CERTYX



AUTONOMOUS CERTIFICATE LIFECYCLE MANAGEMENT

Benutzerhandbuch

Alle Ansichten der Konsole: Zweck, Ablauf, Eingaben, Ergebnisse, Berechtigungen und Einschränkungen

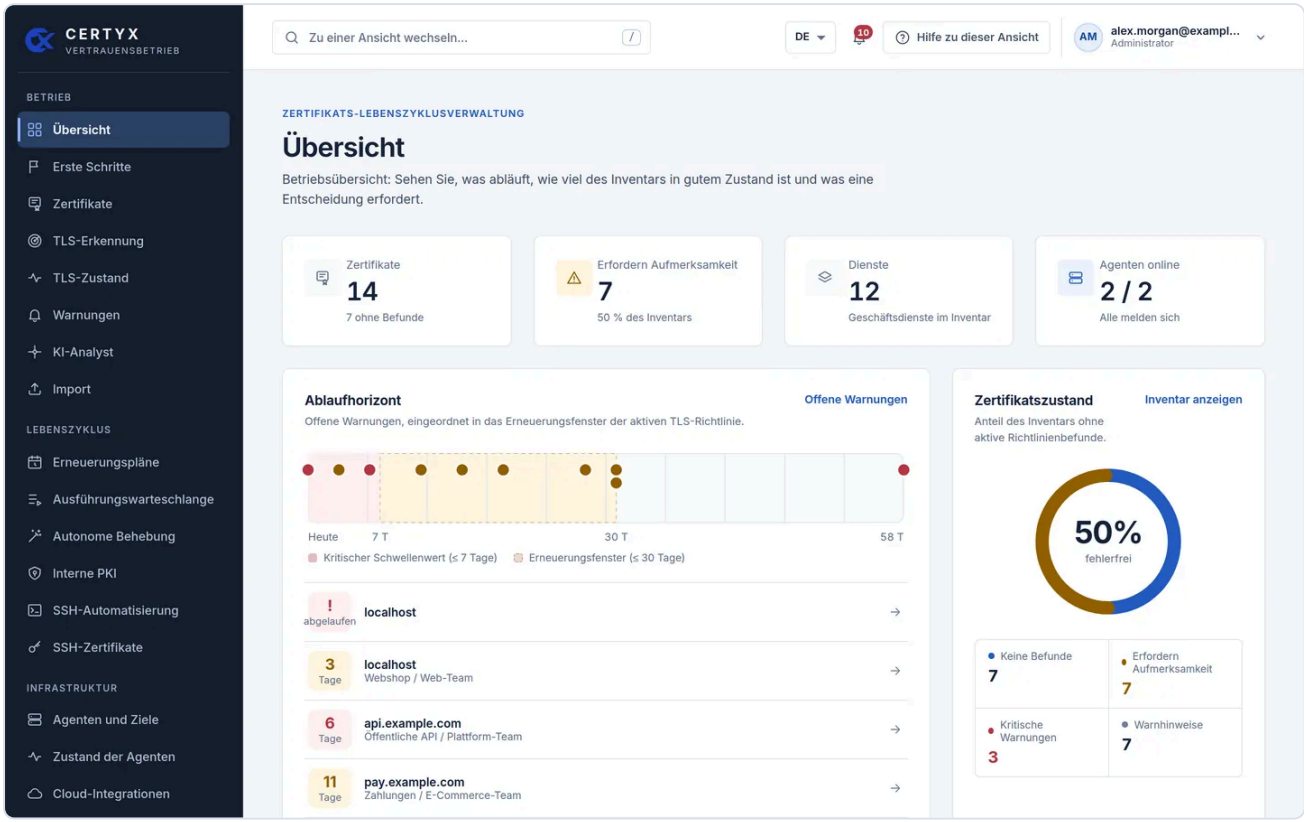
SPRACHE	REVISION	DATUM
Deutsch	8550060f	1. November 2026

Inhalt

1 Übersicht 3
2 Erste Schritte 6
3 Zertifikatsinventar 8
4 Zertifikatsimport 11
5 TLS-Erkennung (Discovery) 13
6 TLS-Zustand 17
7 Erneuerungspläne 20
8 Ausführungswarteschlange 22
9 Autonome Behebung 29
10 TLS-Richtlinie 32
11 Zugriff und Sicherheit 34
12 Prüfprotokoll 42
13 Warnungen 44
14 KI-Analyst 46
15 Plattformverwaltung 49
16 Plattform-Operatoren 55
17 Vertrieb 59
18 Interne PKI 64
19 Benachrichtigungsgruppen 66
20 SIEM-Export 69
21 Agenten und Ziele 78
22 Vertrauensgraph 86
23 Zustand der Agenten 88
24 Plattformbetrieb 92
25 E-Mail-Sperrliste 96
26 KI-Analyst: Anbieter 99
27 Cloud-Integrationen 101
28 Journal der Sicherheitsereignisse 106
29 SSH-Zertifikate 110
30 SSH-Automatisierung 113

1 Übersicht

Betriebsübersicht: Sehen Sie, was abläuft, wie viel des Inventars in gutem Zustand ist und was eine Entscheidung erfordert.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Melden Sie sich an, um die tatsächlichen Daten Ihrer Organisation zu sehen.
2. Die Kennzahlenkarten zeigen Zertifikate, Zertifikate mit Handlungsbedarf, Dienste und Agenten online (mit aktuellem authentifiziertem Kontakt) von allen registrierten Agenten. Jede Karte ist ein Link: Zertifikate und Dienste öffnen das Inventar, Benötigen Aufmerksamkeit öffnet das auf diese Zertifikate gefilterte Inventar und Agenten online öffnet den Agentenzustand — direkt beim Agenten, der Aufmerksamkeit benötigt; die Karte nennt dann diesen Agenten, die Ursache (zum Beispiel Meldet sich nicht, Noch kein erster Kontakt, Prozessfehler) und seit wann.
3. Der Ablaufhorizont ordnet offene Warnungen in das Erneuerungsfenster der aktiven TLS-Richtlinie ein; die rote Zone ist der kritische Schwellenwert. Die Liste darunter zeigt die fünf nächsten Ablaufdaten; die Auswahl eines Eintrags öffnet Warnungen.
4. Der Zertifikatszustand zeigt den Anteil der Zertifikate ohne Richtlinienbefunde sowie die Anzahl kritischer Warnungen und Warnhinweise.
5. Die Betriebsaktivität zählt Ereignisse des Prüfprotokolls der letzten 7 Tage und listet die drei neuesten auf.

6. Das Aktionszentrum leitet Einträge aus aktuellen Daten ab, die dringendsten zuerst, jeweils mit genauer Ursache und einem Link zum erklärenden Datensatz: abgelaufene Zertifikate (gefiltertes Inventar), kritische Warnungen, jeder Agent mit Handlungsbedarf mit Ursache und Erklärung (seine Karte im Agentenzustand), fehlgeschlagene oder zurückgesetzte Erneuerungsaufträge mit dem Ergebnis des Agenten (Erneuerungsbereitschaft des Zertifikats), Aufträge, die auf eine zweite Freigabe warten, ein fehlschlagender SIEM-Export (Administratoren) und nicht zustellbare Benachrichtigungen mit Grund, blockierte Erneuerungspläne mit ihrer ersten Blockade, Erkennungsdurchläufe mit Fehlern oder vorzeitigem Ende (Scanverlauf), Zertifikate im Erneuerungsfenster, deaktivierte MFA Ihres Kontos und ein leeres Inventar. Es zeigt bis zu sechs Einträge.
7. Die Karte „Abonnement und Berechtigungsumfang“ zeigt den Tarif, die Nutzung des Limits verwalteter Zertifikatsfamilien, verfügbare Familien, die Anzahl der Zertifikate im Inventar (nicht abgerechnet) und Lizenzwarnungen. In der Liste „Zertifikatsfamilien“ wählt ein Administrator „Familie verwalten“ oder „Verwaltung beenden“; nur verwaltete Familien verbrauchen Lizenzen.
8. Um zu einer beliebigen Ansicht zu springen, drücken Sie „/“ oder verwenden Sie das Feld „Zu einer Ansicht wechseln…“ oben auf dem Bildschirm.
9. Letzte Erkennung zeigt den neuesten Durchlauf jedes Erkennungsagenten und den neuesten Serverscan: Status, Beginn, aktive Hosts, TLS-Endpunkte und gefundene Zertifikate (neu, ersetzt, unverändert) sowie den letzten Fehler; Scanverlauf öffnet den vollständigen Verlauf unter TLS-Erkennung.

EINGABEN UND PARAMETER

- Die Zahlen stammen aus der Inventarzusammenfassung (gesamte Organisation, unabhängig von Filtern). Dienste werden nach eindeutigem Namen gezählt.
- Horizont und Aktionszentrale verwenden Warnungen, die aktive TLS-Richtlinie, Erneuerungspläne und den Agentenzustand; die Aktivität verwendet eine Serverzusammenfassung des Prüfprotokolls: Ereignisse pro lokalem Tag des Browsers (nach seinem aktuellen UTC-Versatz) und die drei neuesten Ereignisse.
- Die Daten werden beim Öffnen der Übersicht geladen und alle 30 Sekunden aktualisiert, solange die Ansicht geöffnet ist; der Zeitpunkt der letzten Aktualisierung wird unter der Aktionszentrale angezeigt.
- Kann die TLS-Richtlinie nicht gelesen werden, verwendet der Horizont ein Ersatz-Erneuerungsfenster (30 Tage) und einen Ersatz-Schwellenwert (7 Tage).

ERGEBNIS

Das Dashboard ändert nichts, mit einer Ausnahme: Schaltet ein Administrator die Verwaltung einer Zertifikatsfamilie um, ändert sich die Lizenznutzung. Links führen zu den Ansichten, in denen Aktionen ausgeführt werden.

BERECHTIGUNGEN

Alle angemeldeten Benutzer der Organisation (Auditor, Operator, Admin). Nur Administratoren schalten die Verwaltung von Zertifikatsfamilien um. Kann eine Quelle nicht gelesen werden, zeigt ihre Karte „Daten nicht verfügbar“ statt null.

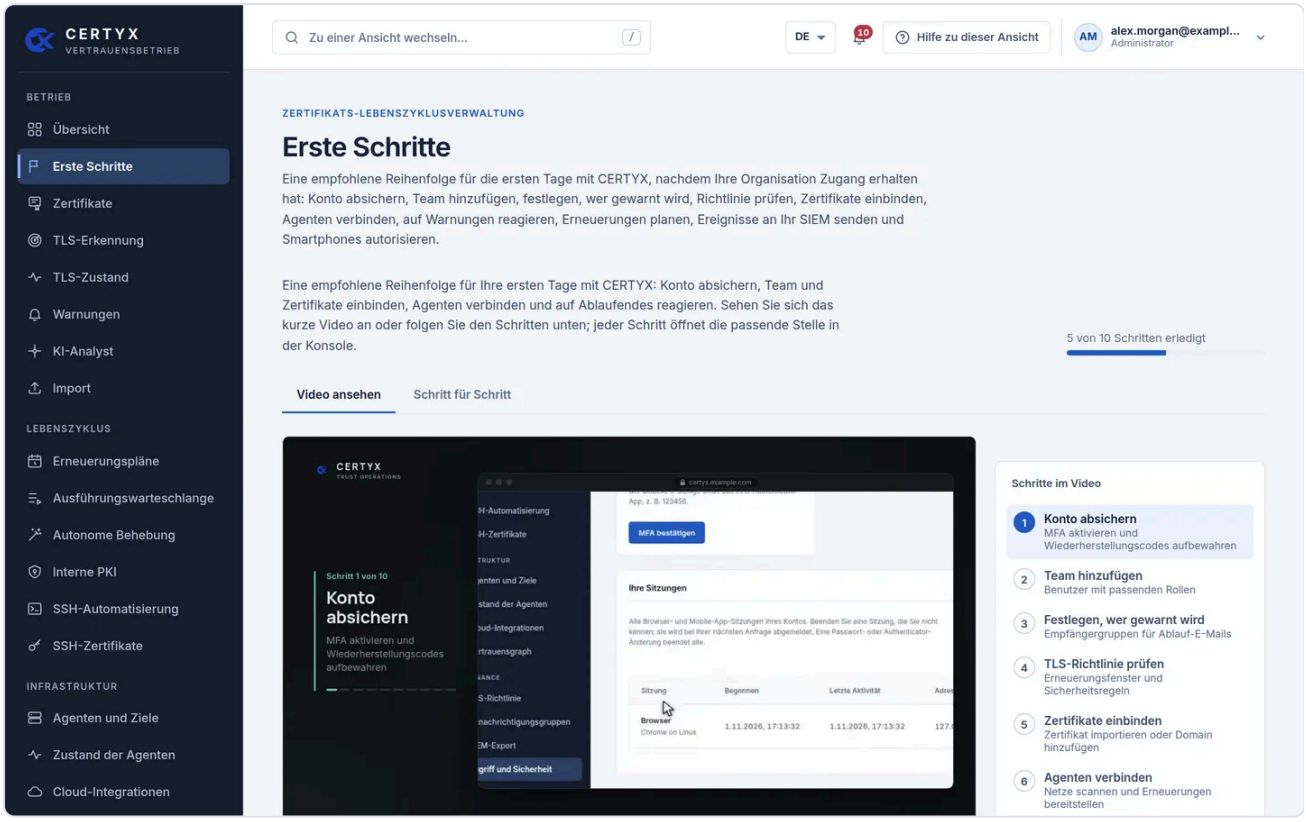
EINSCHRÄNKUNGEN

Die Anzahl der Zertifikate, die Aufmerksamkeit erfordern, spiegelt die Basisrichtlinie wider, nicht verifizierte Bereitstellungen. Der Horizont zeigt nur Zertifikate mit offenen Warnungen (innerhalb des Erneuerungsfensters). Die Aktivität umfasst Ereignisse des Zertifikats-Prüfprotokolls, nicht das

Sicherheitsjournal der Plattform. Die Übersicht zeigt keine Erneuerungs- oder Bereitstellungsaufträge; verfolgen Sie diese unter Ausführungswarteschlange. Das Verwalten einer Familie wird abgelehnt, wenn das Limit verwalteter Familien erreicht ist, sich die Familie inzwischen geändert hat oder das Abonnement keine neuen verwalteten Familien zulässt.

2 Erste Schritte

Eine empfohlene Reihenfolge für die ersten Tage mit CERTYX, nachdem Ihre Organisation Zugang erhalten hat: Konto absichern, Team hinzufügen, festlegen, wer gewarnt wird, Richtlinie prüfen, Zertifikate einbinden, Agenten verbinden, auf Warnungen reagieren, Erneuerungen planen, Ereignisse an Ihr SIEM senden und Smartphones autorisieren.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Sehen Sie sich das Video an: eine Aufzeichnung der zehn Schritte in der Konsole mit Beispieldaten, in der Sprache der Konsole, mit Untertiteln. Ein Sprecher erläutert jeden Schritt: Es startet stumm in einer Schleife, und mit eingeschaltetem Ton läuft die Erläuterung einmal; es startet nicht von selbst, wenn Ihr System reduzierte Bewegung anfordert. Wählen Sie einen Schritt in der Liste daneben, um zu diesem Teil zu springen.
2. Oder öffnen Sie „Schritt für Schritt“: Jeder Schritt erklärt, warum er wichtig ist und wie er geht, mit einem Bildschirmfoto der Stelle in der Konsole; Schritte nur für Administratoren (Team, Benachrichtigungsgruppen, Richtlinie, Agenten, SIEM-Export, Telefone) und Schritte, die Daten ändern und die Rolle Operator oder Administrator brauchen (Zertifikate, Warnungen bearbeiten, Erneuerungspläne), tragen einen Hinweis für Rollen, die sie nicht ausführen können.
3. Mit „... öffnen“ gelangen Sie direkt zur Ansicht des Schritts; die Schaltfläche erscheint nur, wenn Ihre Rolle diese Ansicht öffnen kann.
4. Der Fortschrittsbalken zählt erledigte Schritte. Schritte, die die Konsole erkennt (MFA oder Unternehmensanmeldung, Benutzer, Benachrichtigungsgruppen, Zertifikate, Agenten mit Kontakt zu CERTYX — ein Agent, der noch auf den ersten Kontakt wartet, widerrufen oder abgelaufen ist, zählt

nicht —, Erneuerungspläne, ein gespeichertes SIEM-Ziel, aktive Mobilgeräte), werden automatisch als erledigt markiert. Die übrigen markieren Sie mit „Als erledigt markieren“ und machen dies mit „Als offen markieren“ rückgängig.

5. Nach den Schritten hält die Konsole den Betriebsablauf zusammen: Die Übersicht nennt, was Aufmerksamkeit benötigt und warum, der Agentenzustand erklärt die Ursache jedes Agenten mit den nötigen Schritten, der Scanverlauf zeigt, was die Erkennung gefunden hat, und die Erneuerungsbereitschaft eines Zertifikats zeigt jeden Schritt von der Erkennung bis zum aktualisierten Inventar und was zu konfigurieren ist.

EINGABEN UND PARAMETER

- Keine Eingaben erforderlich. Manuelle Markierungen werden nur in diesem Browser für Ihr Konto gespeichert.

ERGEBNIS

Eine Checkliste, die den Fortschritt Ihrer Organisation zeigt und zu allen benötigten Stellen führt. Diese Ansicht ändert nichts.

BERECHTIGUNGEN

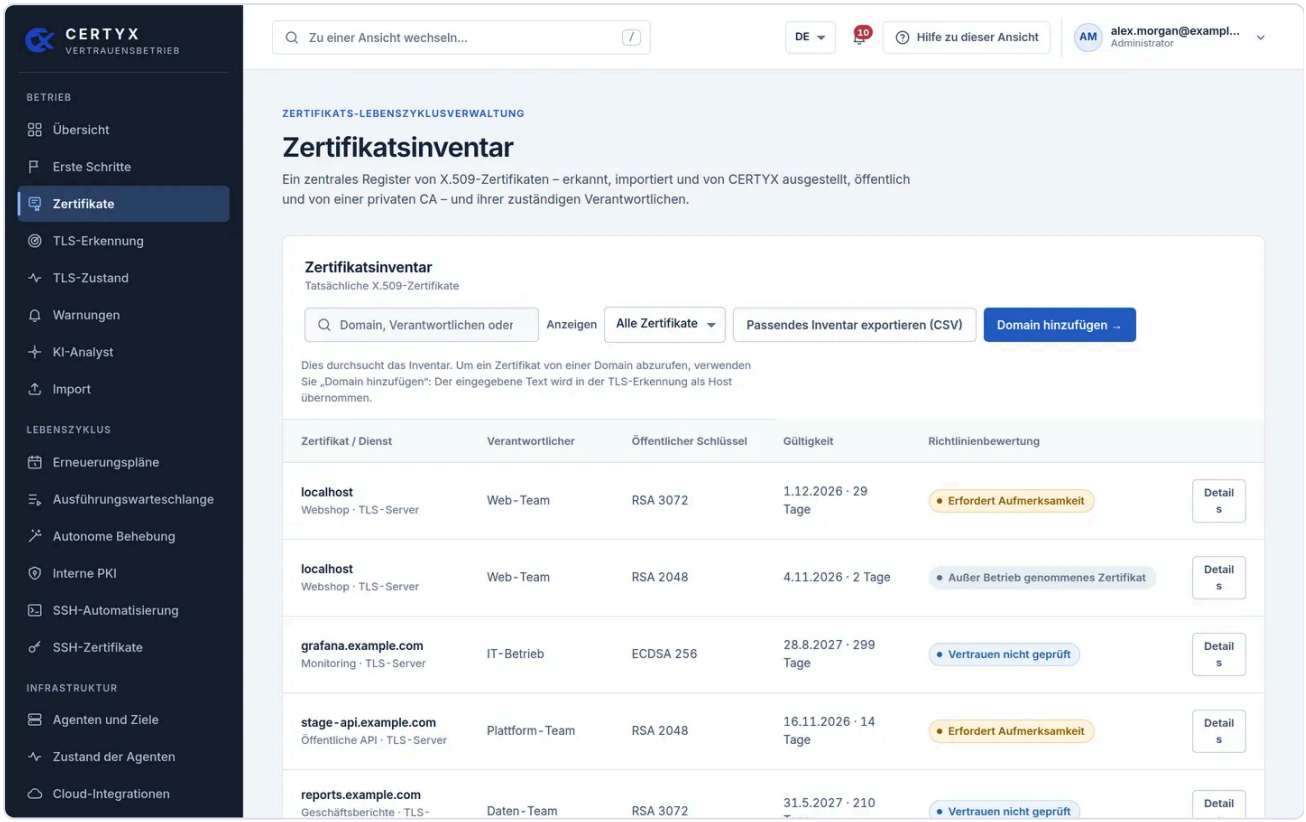
Alle angemeldeten Benutzer der Organisation. Schritte, die nur Administratoren oder nur Operatoren und Administratoren ausführen können, sind gekennzeichnet; Erkennungen, die Administratorrechte erfordern (Benutzer, SIEM-Ziele, Mobilgeräte), sehen nur Administratoren.

EINSCHRÄNKUNGEN

- Video und Bildschirmfotos zeigen Beispieldaten und können im Detail von Ihrer Konfiguration abweichen.
- Die Erkennung liest aktuelle Daten; ein auf anderem Weg erledigter Schritt (zum Beispiel über Cloud-Integrationen eingebundene Zertifikate) gilt als erledigt, sobald die Daten vorhanden sind.
- „TLS-Richtlinie prüfen“ und „Auf Wichtiges reagieren“ lassen sich nicht erkennen; diese markieren Sie immer selbst. Benutzer, SIEM-Ziele und Mobilgeräte werden nur für Administratoren erkannt, SIEM-Ziele nur mit der Plattformdatenbank, die das Sicherheitsjournal enthält, Mobilgeräte zudem nur, wenn die Plattform diese Funktion bereitstellt.
- Kann das Video nicht geladen werden, zeigt die Ansicht einen Hinweis, und die Schritte unten beschreiben dieselben Aktionen.
- Manuelle Markierungen werden nicht mit Kollegen oder anderen Browsern geteilt.

3 Zertifikatsinventar

Ein zentrales Register von X.509-Zertifikaten – erkannt, importiert und von CERTYX ausgestellt, öffentlich und von einer privaten CA – und ihrer zuständigen Verantwortlichen.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Suchen Sie nach einer Domain, einem Verantwortlichen oder einem Dienst.
2. Um das Zertifikat einer nicht inventarisierten Domain abzurufen, wählen Sie Domain hinzufügen →. Das öffnet das Prüfformular der TLS-Erkennung (die Prüfung erfordert die Rolle Admin); der Text im Suchfeld wird als Host übernommen, eine leere Suche öffnet ein leeres Formular.
3. Öffnen Sie Details, um Subjekt, Aussteller, Zweck, Seriennummer, Daten, öffentlichen Schlüssel, Risiko und SHA-256 zu prüfen.
4. Prüfen Sie die Richtlinienbefunde. Ändern Sie Verantwortlicher, Dienst, Produktion und die Verantwortlichkeitsgruppen (bis zu 10 nicht archivierte Gruppen; Empfängergruppen verwalten öffnet die Benachrichtigungsverwaltung) und wählen Sie Verantwortlichkeit speichern, oder wählen Sie Erneuerung planen – der Plan wird erstellt und Erneuerungspläne öffnet sich.
5. Enthält das Abonnement die Funktion RISK_ENGINE, zeigen die Details zusätzlich das Geschäftsrisiko mit seinen Beiträgen und Warnungen zu unvollständigem Kontext.
6. Ist der KI-Analyst für die Organisation aktiviert, öffnet Erklären in den Details ihn mit einer Frage zum Zertifikat.

7. Jedes Zertifikat zeigt seinen Zweck aus den erweiterten Schlüsselverwendungen: TLS-Server, TLS-Client, TLS-Server und -Client, beliebige Verwendung (keine EKU-Einschränkung) oder andere Verwendung. Die Details listen E-Mail-, UPN- und URI-Identitäten. Reine Server-Befunde (localhost, Loopback- oder IP-Identität) werden für TLS-Client-Zertifikate nicht erzeugt; ein öffentliches Zertifikat, das Client-Authentifizierung erlaubt, erhält einen Hinweis.
8. Anzeigen filtert die Liste: alle Zertifikate, solche mit Handlungsbedarf (die Zahl der Übersicht), abgelaufene, solche im Erneuerungsfenster oder solche, die darüber hinaus gültig sind. #inventory/validity/<Filter> öffnet die gefilterte Liste.
9. Die Erneuerungsbereitschaft in den Details zeigt jeden Schritt der Erneuerung: Inventar (wo das Zertifikat zuletzt beobachtet wurde, mit dem an jedem Endpunkt erkannten Dienst, seiner TLS-Version und seinem ALPN-Protokoll, der vorgeschlagenen Installationsart mit Sicherheit und Hinweisen sowie den vom Endpunkt vorgelegten Ausstellerzertifikaten), Richtlinie und Erneuerungsfenster, das Ausführungsziel mit genau seinen Namen, den installierenden Agenten und seine Diagnose, wo und wie der Agent installiert (Installationsmodus — Agent auf dem Host oder Agent als SSH-Relay mit dem Remote-Host —, Konnektor, Bereitstellungsverzeichnis, die veröffentlichten Dateien wie fullchain.pem, privkey.pem und bundle.p12 oder die konfigurierten Pfade, Prüf- und Reload-Befehle, Cloud-Ressource, geprüfter Endpunkt und der von relay-check gefundene Dienst — wie der Agent seine Ziele meldet; ein anderer Installationsmodus oder Remote-Host blockiert den Schritt), die Zertifizierungsstelle, die unabhängige Prüfung, was den Austausch auslöst (automatisches Profil, geplanter Antrag oder manuell), den Erneuerungsplan, die Vier-Augen-Freigabe, was der Agent Schritt für Schritt tut, das Prüfergebnis und das aktualisierte Inventar. Ein blockierter Schritt nennt genau, was zu konfigurieren ist; deckt kein Ziel das Zertifikat ab, wählen Administratoren Ziel mit diesen Werten anlegen, das die Ausführung mit dem vorgeschlagenen Ziel öffnet. Das Formular zeigt unter jedem Feld, woher sein Wert stammt und was der Administrator noch eingeben muss.
10. Nächste Erneuerung in der Erneuerungsbereitschaft zeigt, wie die nächste Erneuerung des Zertifikats beginnt — Automatisch (keine Freigabe nötig), Benötigt Freigabe oder Manuell geplant — und welche Einstellung der automatischen Erneuerung das entscheidet (Standard der Installation, Organisation, Ziel oder dieses Zertifikat). Administratoren ändern die Auswahl Automatische Erneuerung des Zertifikats über der Bereitschaft: Einstellung der Organisation, Automatisch erneuern oder Freigabe verlangen; sie gilt auch für spätere Erneuerungen des Zertifikats.

EINGABEN UND PARAMETER

- Suchen Sie nach Domain, Subjekt, beobachtetem Endpunkt, Verantwortlichem, Dienst, Aussteller, Seriennummer oder SHA-256-Fingerabdruck (bis zu 200 Zeichen). PostgreSQL wendet den Filter auf das gesamte Inventar der Organisation an; pro Seite werden 50 Zeilen angezeigt.
- Verantwortlicher und Dienst: erforderlich, jeweils 1–200 Zeichen.
- Der CSV-Export überträgt das vollständige gefilterte Ergebnis, ohne private Schlüssel. Formelzellen für Tabellenkalkulationen werden neutralisiert.

ERGEBNIS

Metadatenänderungen werden gespeichert und protokolliert. Eine Änderung von Verantwortlichem oder Dienst gibt genehmigte Erneuerungspläne erneut zur Genehmigung zurück (Bereit zur Genehmigung oder Blockiert).

BERECHTIGUNGEN

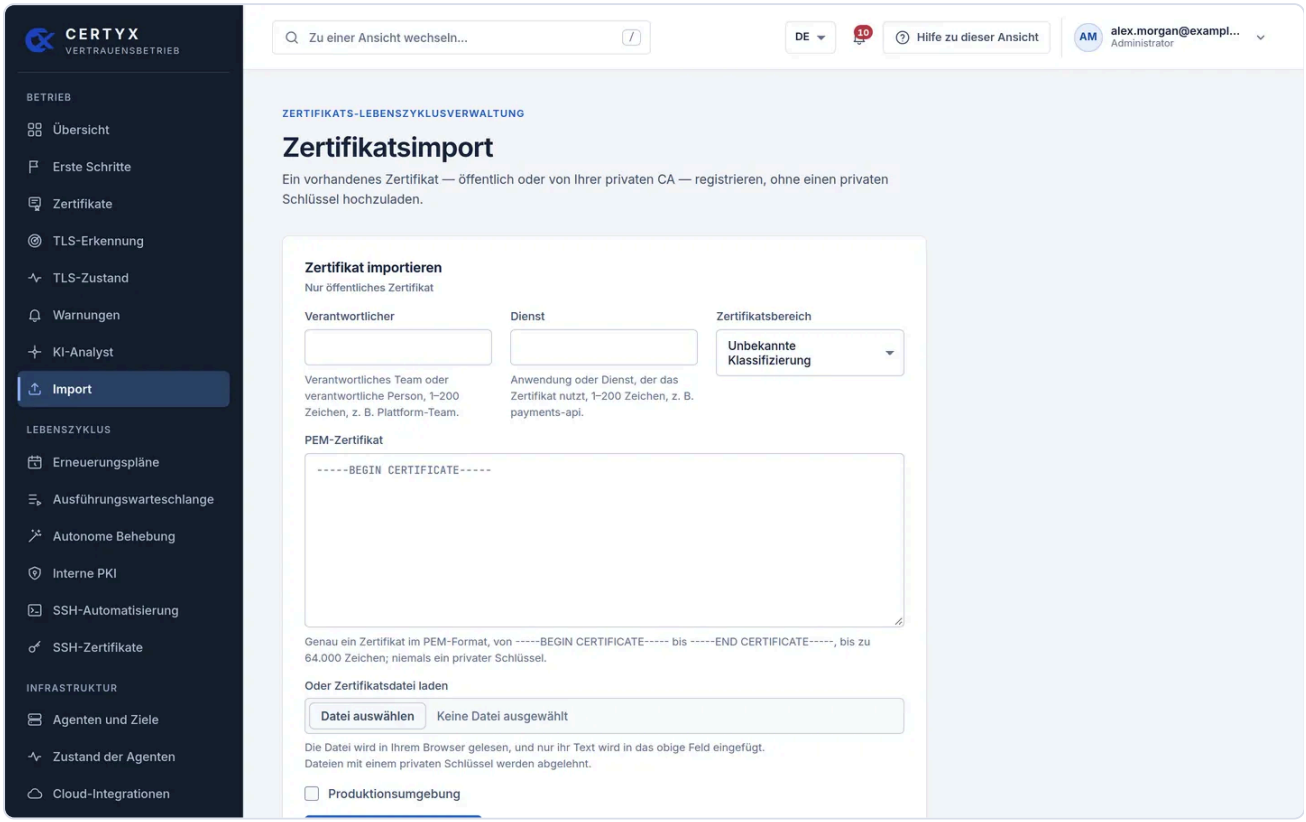
Jede Rolle der Organisation: Suche, Details und CSV-Export. Operator und Admin: Verantwortlichkeit speichern und Erneuerung planen. Geschäftsrisiko: nur mit der Funktion RISK_ENGINE.

EINSCHRÄNKUNGEN

SHA-256 identifiziert ein bestimmtes Zertifikat. Das Risiko 0–100 ist kein CA-Vertrauen. Kette, Widerruf, SAN-Abdeckung und Korrektheit der Bereitstellung werden hier nicht bestätigt.

4 Zertifikatsimport

Ein vorhandenes Zertifikat — öffentlich oder von Ihrer privaten CA — registrieren, ohne einen privaten Schlüssel hochzuladen.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Geben Sie Verantwortlicher und Dienst ein und wählen Sie den Zertifikatsbereich: Unbekannte Klassifizierung (Standard), Öffentliches Zertifikat oder Internes Zertifikat.
2. Fügen Sie ein Zertifikat von -----BEGIN CERTIFICATE----- bis -----END CERTIFICATE----- in PEM-Zertifikat ein oder wählen Sie unter Oder Zertifikatsdatei laden eine Datei (.pem, .crt oder .cer in PEM-Textform). Die Datei wird in Ihrem Browser gelesen, und nur ihr Text wird in das Feld eingefügt.
3. Aktivieren Sie gegebenenfalls Produktionsumgebung und wählen Sie Importieren und bewerten.
4. Der Bereich Importergebnis zeigt Bewertung, Gültigkeit, Schlüssel, Risiko und die Anzahl der Richtlinienbefunde. Zertifikatsinventar öffnen führt zum Zertifikat im Inventar. Das Formular wird geleert, sodass Sie sofort ein weiteres Zertifikat importieren können.

EINGABEN UND PARAMETER

- PEM-Zertifikat: genau ein öffentliches X.509-Zertifikat in PEM-Textform, bis zu 64.000 Zeichen (eine gewählte Datei bis zu 64.000 Byte). Binäre DER-Dateien und PKCS#12/PFX-Container werden nicht angenommen – konvertieren Sie das Zertifikat zuerst in PEM, ohne privaten Schlüssel. Eine Kette aus mehreren Zertifikaten wird abgelehnt.
- Verantwortlicher und Dienst: erforderlich, jeweils 1–200 Zeichen.

- Zertifikatsbereich: Internes Zertifikat kennzeichnet ein Zertifikat Ihrer privaten CA – es erscheint dann in der Liste der Ansicht Interne PKI; Öffentliches Zertifikat und Unbekannte Klassifizierung bleiben nur im Inventar.
- Inhalte mit privatem Schlüssel (jeder Block BEGIN … PRIVATE KEY) werden im Browser vor dem Senden und erneut vom Server abgelehnt. Ein bereits inventarisiertes Zertifikat wird als Duplikat abgelehnt; ein ungültiges X.509-PEM wird mit Begründung abgelehnt.

ERGEBNIS

Das Zertifikat wird gespeichert, X.509-Metadaten werden extrahiert, die aktuelle Richtlinie wird bewertet und ein Eintrag im Prüfprotokoll (certificate.import) wird geschrieben.

BERECHTIGUNGEN

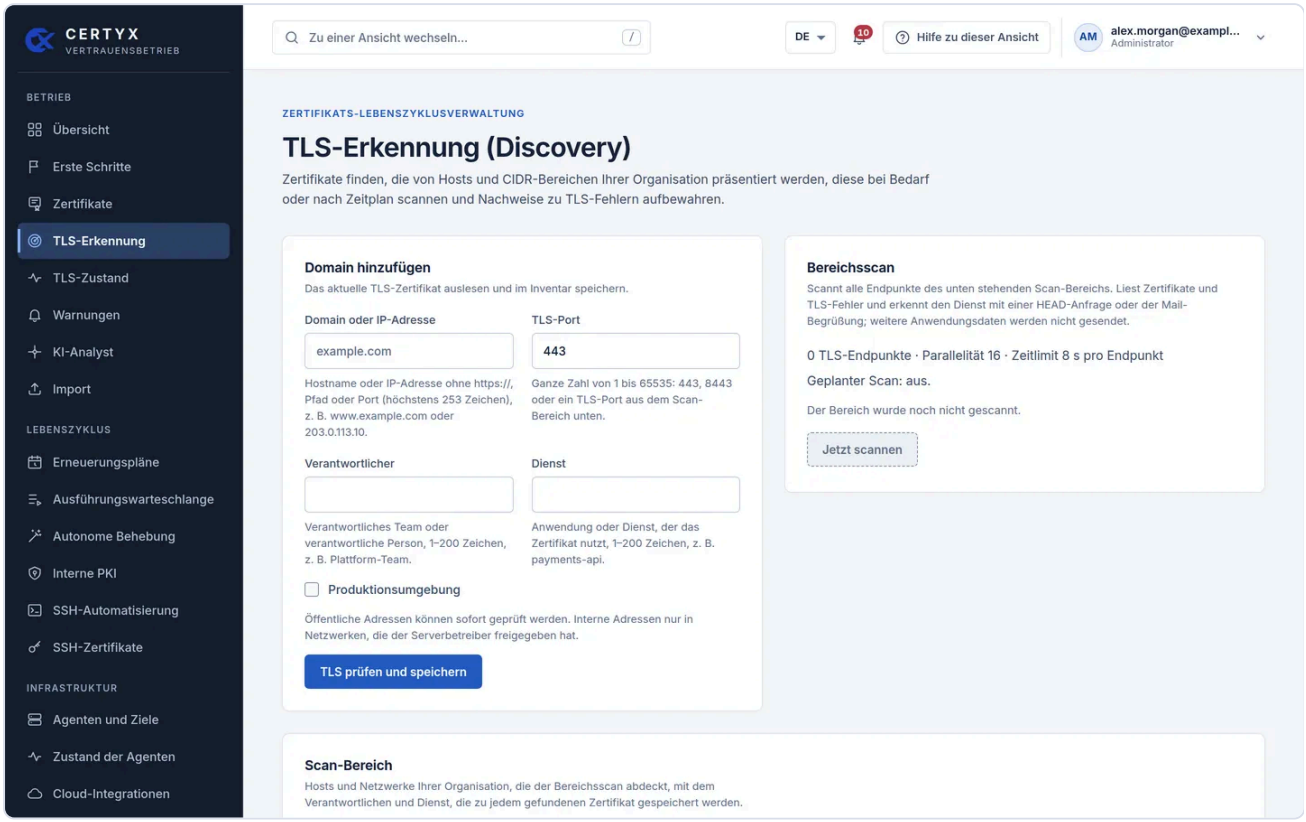
Operator oder Admin. Ein Auditor sieht das Formular deaktiviert, mit dem Hinweis, dass seine Rolle das Inventar nur einsehen kann.

EINSCHRÄNKUNGEN

Der Import stellt kein Zertifikat aus, installiert keines und speichert weder einen privaten Schlüssel noch eine Kette. Ein selbstsigniertes Zertifikat kann inventarisiert werden, sein Vertrauen wird jedoch nicht bestätigt. Die Klassifizierung ist eine Angabe des Importierenden; CERTYX prüft sie nicht.

5 TLS-Erkennung (Discovery)

Zertifikate finden, die von Hosts und CIDR-Bereichen Ihrer Organisation präsentiert werden, diese bei Bedarf oder nach Zeitplan scannen und Nachweise zu TLS-Fehlern aufbewahren.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Diese Ansicht führt die serverseitige Erkennung vom CERTYX-Server für Ihre Organisation aus, auch auf dedizierten Instanzen. Um Zertifikate in Netzwerken zu finden, die der Server nicht erreicht, verwenden Sie einen registrierten Agent: Agenten und Ziele → Automatische Netzwerkerkennung (gemeldete Netzwerke, Umfang, Modus, Rate, Zeitfenster); die Ergebnisse erscheinen im Inventar und die Warnungen unter Warnungen.
2. Für eine einzelne Domain: Geben Sie ihren Hostnamen ohne https:// ein, wählen Sie einen TLS-Port (standardmäßig 443), geben Sie Verantwortlichen und Dienst ein und wählen Sie dann TLS prüfen und speichern. Wählen Sie danach Zertifikat öffnen: Das Zertifikat ist bereits im Inventar gespeichert.
3. Scan-Bereich (Admin): Fügen Sie unter Hosts einen Namen oder eine IP-Adresse mit TLS-Port, Verantwortlichem, Dienst und Produktionskennzeichen hinzu; fügen Sie unter Netzwerke einen CIDR-Bereich mit expliziten TLS-Ports und denselben Metadaten hinzu; geben Sie Ausschlüsse zeilenweise ein.
4. Für regelmäßige Scans aktivieren Sie Automatisch scannen und geben ein Intervall in Minuten ein (die erlaubten Grenzen stehen unter dem Feld). Wählen Sie Bereich speichern. Jede Speicherung erzeugt eine neue Version und wird im Sicherheitsjournal erfasst; hat inzwischen ein anderer Administrator gespeichert, laden Sie die Ansicht neu und wiederholen Sie Ihre Änderung.

5. Das Feld Bereichsscan zeigt die Anzahl der TLS-Endpunkte, den Zeitplan mit dem nächsten Scan und den letzten Scan. Jetzt scannen startet einen manuellen Scan; der Fortschritt wird laufend aktualisiert. Scan stoppen (Admin) stoppt den laufenden Scan der Organisation — Ihren, den eines anderen Administrators oder einen geplanten — auf der Instanz, die ihn ausführt; er endet innerhalb von Sekunden als abgebrochen, bereits gefundene Zertifikate bleiben im Inventar. Ein geplanter oder von einem anderen Administrator gestarteter Scan erscheint, sobald der Status aktualisiert wird.
6. Wurde die Instanz, die einen Scan ausführte, beendet, wird der Scan als unterbrochen angezeigt. Er wird ab dem gespeicherten Prüfpunkt fortgesetzt — bereits gescannte Endpunkte werden nicht erneut geprüft: Der Planer setzt ihn beim nächsten Durchlauf automatisch fort (sofern der Serverbetreiber dies nicht ausgeschaltet hat), und Scan fortsetzen (Admin) setzt ihn sofort fort. Der Hinweis unter dem Fortschritt erklärt, wann ein Scan nicht fortgesetzt werden kann (Bereich seit dem Start geändert, Fortsetzungslimit erreicht, von einem Administrator gestoppt oder durch einen neueren Scan ersetzt); starten Sie dann einen neuen Scan.
7. Prüfen Sie die Ergebnisse des letzten Scans (Zertifikat oder Grund für fehlende TLS-Antwort pro Endpunkt), die Beobachtungen und die dem Inventar hinzugefügten Zertifikate. Jedes Ergebnis nennt den erkannten Dienst; jede Beobachtung zeigt unter Dienst und Installation den Dienst, die TLS-Version und das ausgehandelte ALPN-Protokoll, die für ein erneuertes Zertifikat vorgeschlagene Installationsart mit ihrer Sicherheit und die Hinweise (zum Beispiel Server: nginx/1.24.0 oder Port 6443). Beobachtungen von Agenten ohne Diensterkennung zeigen Nicht erkannt.
8. Der Serverbetreiber legt die Bereichsgrenzen, die Intervallgrenzen und die freigegebenen internen Netzwerke fest (Clm:Discovery). Auf einer Instanz ohne dedizierte Organisationen wird ein in CLM_DISCOVERY_TARGETS, CLM_DISCOVERY_CIDRS und CLM_DISCOVERY_EXCLUSIONS konfigurierter Bereich einmalig als Bereich der Organisation „default“ übernommen; spätere Änderungen erfolgen in dieser Ansicht.
9. Die Agent-Erkennung (Clm.Agent discovery scan auf dem Kundenhost) wiederholt vorübergehende Fehler bei der Identitätsrotation und der Kommunikation nach Settings.RetrySeconds (standardmäßig 30 Sekunden). Authentifizierungs-, Autorisierungs- und TLS-Vertrauensfehler stoppen den Erkennungsprozess des Agents; mit --once meldet der Befehl einen Fehler. Konfigurieren Sie auf dem Agent-Host nur für den Eigentümer zugängliche Zustands- und Sperrpfade. Ein Ausfall der Berichterstattung kann Diagnosen verzögern; überwachen Sie auch ausbleibende Kontakte des Agents.
10. Der Scanverlauf listet jeden Erkennungsdurchlauf der Agenten und jeden Serverscan der Organisation, neueste zuerst: Beginn, Quelle (der Agent, verlinkt mit seinem Zustand, oder der CERTYX-Server), Umfang (Netze, Modus und Ausschlüsse), Status mit Phase und Fortschritt oder Ende (abgeschlossen, unterbrochen wegen geändertem Umfang, pausiertem Profil oder neu begonnenem Durchlauf), aktive Hosts, TLS-Endpunkte, neue, an einem Endpunkt ersetzte und unveränderte Zertifikate, ausgelöste Erkennungswarnungen, reduzierte Rate, die letzten Fehler und ob es der Basisdurchlauf ist. Ergebnisse verlinken die Inventareinträge neuer oder ersetzter Zertifikate und die Warnungen. #discovery/history öffnet ihn.

EINGABEN UND PARAMETER

- Host: Name oder IP-Adresse ohne URL, Pfad oder Port; TLS-Port 1–65535; Verantwortlicher und Dienst (standardmäßig höchstens 200 Zeichen); Produktionskennzeichen.
- Netzwerk: IPv4/IPv6-CIDR mit der Netzwerkadresse (zum Beispiel 203.0.113.0/28) und 1–16 expliziten TLS-Ports.
- Ausschlüsse: IP-Adressen oder CIDRs, die auch auf die aufgelöste Adresse eines Hostnamens angewendet werden.

- Derselbe Endpunkt (Host oder Adresse und Port), der zweimal mit einem anderen Verantwortlichen, Dienst oder Produktionskennzeichen angegeben ist, wird abgelehnt.
- Standardgrenzen des Servers (unter dem Formular angezeigt): 100 Hosts, 64 Netzwerke, 4.096 Adressen vor Ausschlüssen, 16.384 TLS-Endpunkte, 1.024 Ausschlüsse. Scan-Intervall standardmäßig von 15 Minuten bis 7 Tage.
- Adressen: öffentliche immer; private, lokale und reservierte nur in Netzwerken, die der Serverbetreiber freigegeben hat — ein Bereich mit anderen solchen Adressen wird abgelehnt, und Hostnamen, die dorthin aufgelöst werden, enden als „keine TLS-Antwort“.
- Standardmäßig 16 gleichzeitige Prüfungen mit einem Timeout von 8 Sekunden pro Endpunkt.
- Einzelne Domain: Port 443 oder 8443 oder ein TLS-Port aus dem Scan-Bereich der Organisation.

ERGEBNIS

Öffentliche Zertifikate und TLS-Fehler werden mit Endpunkt und Beobachtungszeitpunkt gespeichert, zusammen mit dem Dienst-Fingerabdruck (gesendeter Servername, TLS-Version, Cipher-Suite, ALPN-Protokoll, die vom Endpunkt vorgelegten Ausstellerzertifikate, HTTP-Status mit den Headern Server und X-Powered-By oder die Mail-Begrüßung) und dem erkannten Dienst mit der vorgeschlagenen Installationsart; Ergebnisse pro Endpunkt werden für die letzten 20 Scans der Organisation aufbewahrt, und ein laufender Scan speichert die bisherigen Ergebnisse als Prüfpunkt. Bereichsänderungen, Scanstart, Stopp-Anforderungen, Fortsetzungen und das Ende eines Scans (abgeschlossen, abgebrochen, fehlgeschlagen oder unterbrochen) werden im Sicherheitsjournal und im Inventar-Audit erfasst.

BERECHTIGUNGEN

Bereich, Status, Ergebnisse und Beobachtungen lesen: angemeldete Rollen der Organisation. Bereich ändern, Domain prüfen, Scan starten, stoppen oder fortsetzen: Admin.

EINSCHRÄNKUNGEN

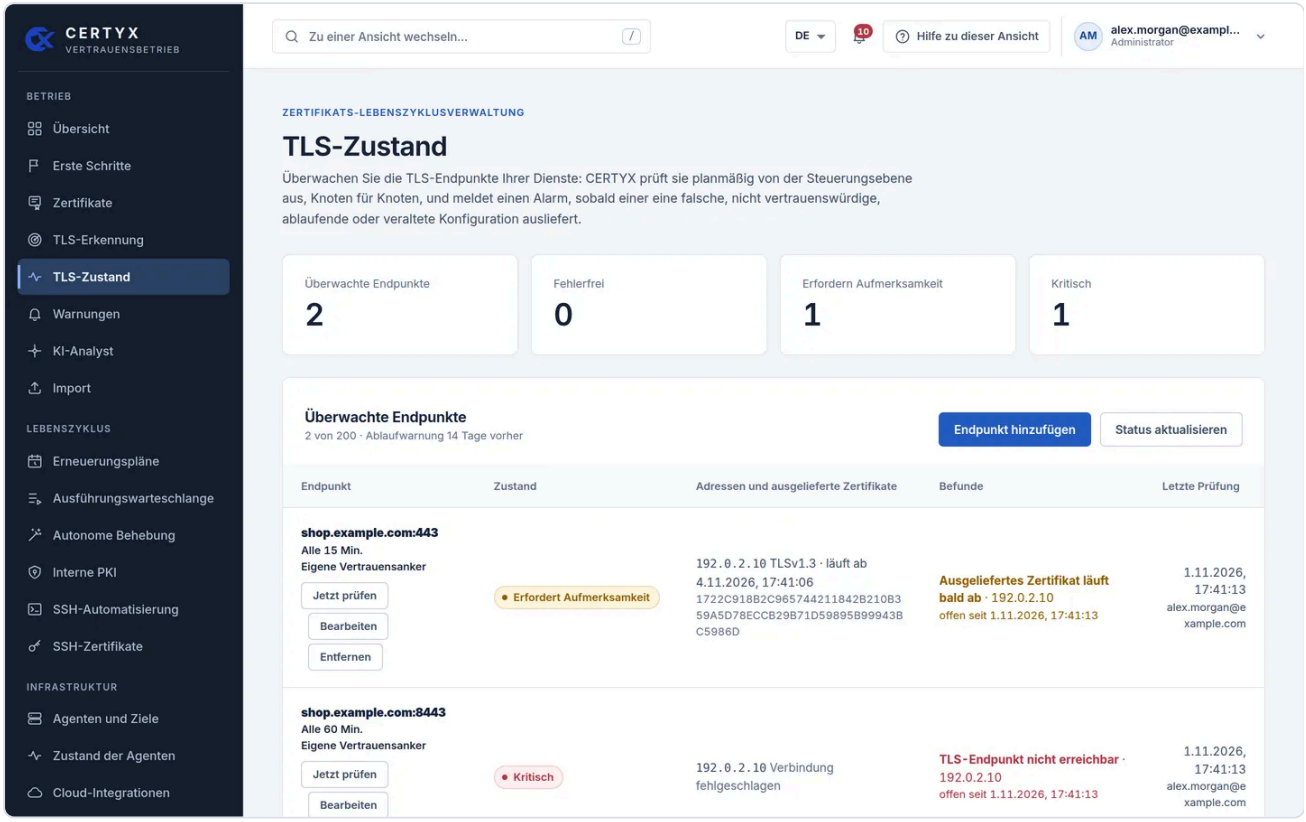
Dies ist kein Scanner für alle Dienste: nur TCP-Verbindung und TLS-Handshake auf den angegebenen Ports und, sofern der Serverbetreiber es nicht abgeschaltet hat (Clm:Discovery:ServiceIdentification:IdentifyServices), eine HEAD-/-HTTP/1.1-Anfrage an einen HTTP-Endpunkt oder das Lesen der SMTPS-, IMAPS- oder POP3S-Begrüßung; keine weiteren Anwendungsdaten, kein UDP oder STARTTLS. Der erkannte Dienst ist ein Vorschlag der konfigurierten Regeln: Der Server-Header nennt die Software, die HTTP beantwortet hat, hinter einem Proxy, der Header durchreicht, also womöglich das Backend; ein Endpunkt ohne eindeutige Merkmale erscheint als nicht erkannter Webserver oder TLS-Dienst mit der allgemeinen Installation als PEM-Dateien und geringer Sicherheit. Ein Scan pro Organisation gleichzeitig. Jede Instanz scannt standardmäßig bis zu 4 Organisationen gleichzeitig (Clm:Discovery:SchedulerConcurrency); sind mehr Organisationen fällig, starten die am längsten überfälligen zuerst und die übrigen in einem späteren Durchlauf, daher kann ein Scan später als geplant beginnen. Ein Stopp für einen Scan, den eine andere Instanz ausführt, wirkt bei dessen nächster Fortschrittsspeicherung (standardmäßig alle 2 Sekunden). Ein Scan, dessen Instanz ohne Speichern ausfiel, wird nach 10 Minuten ohne Fortschritt (Standard) als unterbrochen angezeigt und höchstens 5-mal (Standard) fortgesetzt. Die Konsole zeigt nur den letzten abgeschlossenen Scan: seine ersten 100 Endpunktergebnisse mit der Gesamtzahl der Endpunkte; die vollständigen Ergebnisse pro Endpunkt bleiben für die aufbewahrten Scans gespeichert. Außerdem zeigt sie die neuesten 50 Beobachtungen mit ihrer Gesamtzahl; der Server sendet nur diese 50 Beobachtungen. Das Prüfen einer einzelnen Domain fügt sie nicht dem Bereich hinzu. Ein vorhandenes Zertifikat behält seinen aktuellen Verantwortlichen und Dienst. Die serverseitigen Grenzen gelten nicht für die Agent-Erkennung, die eigene Grenzen hat (Clm:Discovery:AgentLimits).

FEHLERBEHEBUNG

- Kein Agentendurchlauf erscheint: Der Agent benötigt die Erkennungsberechtigung und ein aktiviertes, genehmigtes Profil (Agenten und Ziele); seine Diagnose im Agentenzustand prüfen.
- Ein Durchlauf endet unterbrochen: Genehmigter Umfang oder Ports wurden geändert, das Profil pausiert oder der Agent hat den Durchlauf neu begonnen; der nächste Durchlauf startet von selbst.
- Fehler in einem Durchlauf: Der Agent hat einen festen Grund gemeldet (zum Beispiel Kommunikations- oder lokaler E/A-Fehler oder ein Profil jenseits der lokalen Positivliste); der Agentenzustand erklärt ihn mit Abhilfen.
- Keine Zertifikate trotz aktiver Hosts: Die gängigen Ports des Profils enthalten nicht die TLS-Ports der Dienste oder die Hosts antworten ohne TLS; Ports ergänzen oder nach Abstimmung mit dem Sicherheitsteam den vollständigen Modus nutzen.

6 TLS-Zustand

Überwachen Sie die TLS-Endpunkte Ihrer Dienste: CERTYX prüft sie planmäßig von der Steuerungsebene aus, Knoten für Knoten, und meldet einen Alarm, sobald einer eine falsche, nicht vertrauenswürdige, ablaufende oder veraltete Konfiguration ausliefert.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Administratoren wählen Endpunkt hinzufügen und geben Hostname oder IP-Adresse (ohne https://, Pfad oder Port), den TLS-Port (standardmäßig 443) und das Prüfintervall in Minuten ein (die Grenzen stehen im Formular). Optional geben Sie den erwarteten SHA-256-Fingerabdruck des Zertifikats an, das jeder Knoten liefern muss, sowie Vertrauensanker (PEM-CA-Zertifikate) für Endpunkte einer privaten CA. Speichern: Der Endpunkt wird beim nächsten Durchlauf des Planers geprüft, meist innerhalb einer Minute.
2. Jede Prüfung löst den Namen einmal auf und verbindet sich selbst mit jeder aufgelösten Adresse (jeder Knoten hinter einem DNS-Namen oder Load Balancer, bis zu Clm:EndpointHealth:MaximumAddresses), sodass eine wechselnde DNS-Antwort sie nicht umleiten kann. Pro Adresse werden das ausgelieferte Zertifikat (Fingerabdruck, Subjekt, Aussteller, Ablauf), die ausgehandelte TLS-Version und Cipher-Suite, die Abdeckung des Hostnamens, das Vertrauen in die Kette mit Online-Sperrprüfung, fehlende Zwischenzertifikate und die Annahme von TLS 1.0 oder 1.1 erfasst.
3. Befunde: nicht erreichbare Adresse, nicht auflösbarer Host, nicht vertrauenswürdige Kette (unbekannter Aussteller, gesperrt, ungültig), nicht prüfbarer Sperrstatus, fehlendes Zwischenzertifikat, abweichender Hostname, akzeptiertes TLS 1.0/1.1, abgelaufenes oder bald ablaufendes Zertifikat

(Warnung Clm:EndpointHealth:ExpiringWarningDays vorher), ein anderes Zertifikat als der erwartete Fingerabdruck und Knotenabweichung, wenn Adressen unterschiedliche Zertifikate liefern (zum Beispiel nach einer Rotation, die einen Knoten ausgelassen hat).

4. Jeder Befund ist ein Alarm unter Alarme mit Endpunkt und Adresse, offen seit dem ersten Auftreten. Verantwortlicher, Dienst und Benachrichtigungsgruppen stammen aus dem Inventar, wenn das ausgelieferte Zertifikat bekannt ist. Offene Alarme erreichen die Benachrichtigungskanäle der Organisation (E-Mail, Slack, Microsoft Teams, Webhooks, PagerDuty) und kritische die mobile App, wie jeder andere Alarm. Ein Alarm kann bestätigt werden; er bleibt bestätigt, solange der Befund besteht, und schließt sich von selbst, wenn eine Prüfung ihn nicht mehr findet. Ein erneutes Auftreten ist ein neuer Alarm.
5. Jetzt prüfen (Operatoren und Administratoren) prüft einen Endpunkt sofort, zum Beispiel direkt nach einer Bereitstellung. Bearbeiten ändert den Monitor (versioniert: Hat ein anderer Administrator ihn inzwischen geändert, laden Sie neu und wiederholen Sie die Änderung); Entfernen beendet die Überwachung und entfernt Ergebnisse und offene Zustandsalarme. Deaktivierte Monitore werden nicht geprüft und lösen keine Alarme aus.
6. Die Tabelle zeigt pro Endpunkt den Zustand (Fehlerfrei, Erfordert Aufmerksamkeit, Kritisch, Erste Prüfung ausstehend, Deaktiviert), jede Adresse mit TLS-Version, Ablauf und Fingerabdruck oder dem Grund des Fehlschlags, die Befunde mit dem Zeitpunkt seit dem sie offen sind, die letzte Prüfung und wer den Monitor geändert hat. Die Ansicht aktualisiert sich automatisch; Status aktualisieren lädt sie sofort neu.

EINGABEN UND PARAMETER

- Hostname oder IP-Adresse, Port 1–65535 und ein Intervall zwischen Clm:EndpointHealth:MinimumIntervalMinutes und MaximumIntervalMinutes (Standard DefaultIntervalMinutes, 15).
- Optionaler erwarteter Fingerabdruck: 64 Hexadezimalzeichen, Doppelpunkte erlaubt. Optionale Vertrauensanker: 1 bis 10 CA-Zertifikate im PEM-Format, niemals private Schlüssel (abgelehnt).
- Nicht öffentliche Adressen (privat, Loopback, Link-Local, Shared, Dokumentations- und Übergangsbereiche) werden nur in den Netzen geprüft, die der Betreiber der Installation in Clm:Discovery:AuthorizedPrivateNetworks freigibt; sonst werden sie als Nicht öffentliche Adresse nicht freigegeben gemeldet und nie kontaktiert.

ERGEBNIS

Pro überwachtem Endpunkt das letzte Ergebnis jeder Adresse und ihre Befunde, Alarme, die sich mit den Befunden öffnen und schließen, sowie die Einträge endpoint-health.monitor.created, .updated und .deleted im Sicherheitsjournal (als CONFIG-035 an das SIEM exportiert).

BERECHTIGUNGEN

Alle Benutzer der Organisation lesen die Ergebnisse. Administratoren fügen Monitore hinzu, ändern und entfernen sie; Operatoren und Operator-API-Tokens starten Jetzt prüfen. API-Tokens können keine Monitore verwalten.

EINSCHRÄNKUNGEN

Die Prüfungen laufen von der CERTYX-Steuerungsebene aus und sehen daher, was das Internet (oder die freigegebenen internen Netze) sieht; nur im Kundennetz erreichbare Endpunkte benötigen ein freigegebenes Netz oder bleiben nicht zulässig. Eine Organisation hat höchstens Clm:EndpointHealth:MaximumMonitors Monitore. Der Sperrstatus wird online über die CRL- oder OCSP-

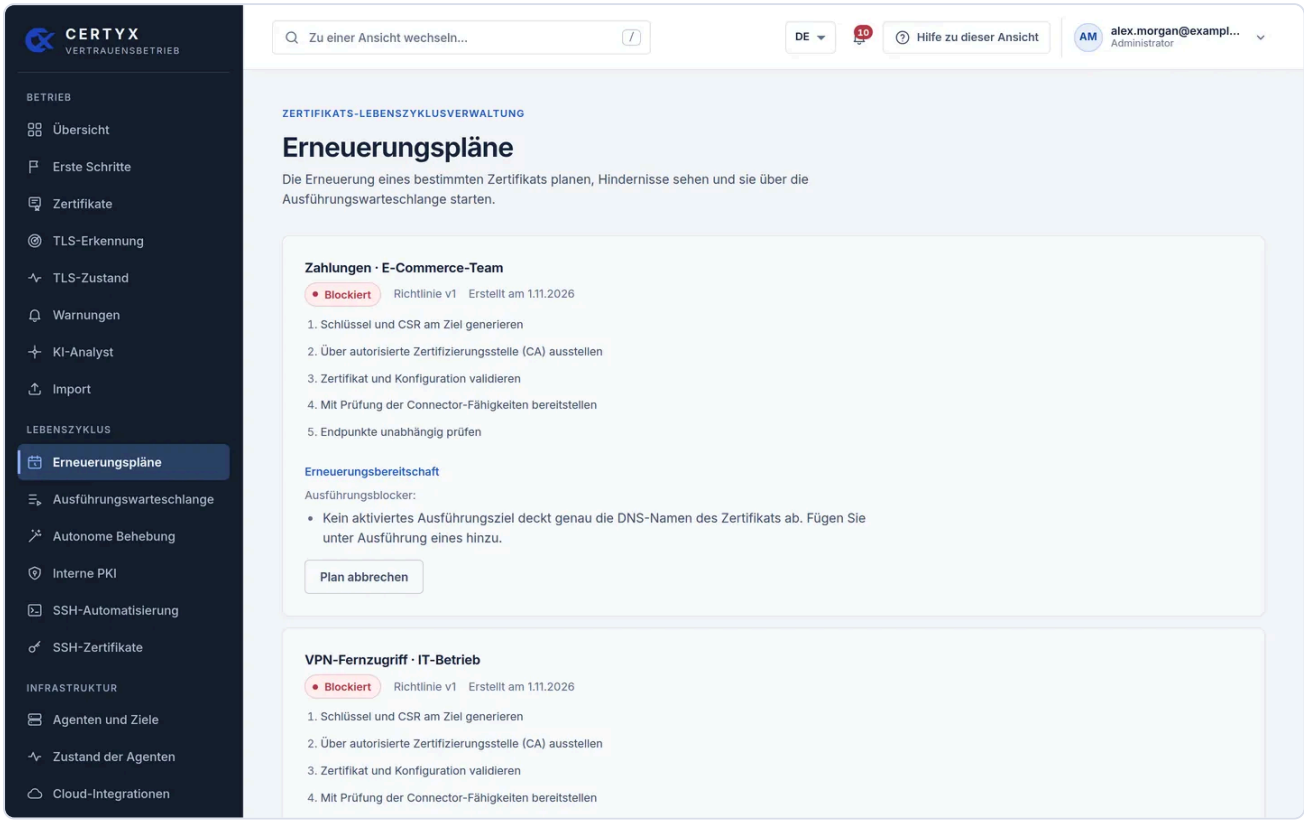
Adressen der Zertifikate geprüft; ohne sie erscheint der Befund Sperrstatus nicht prüfbar. Der Test auf TLS 1.0/1.1 benötigt auf dem CERTYX-Host eine TLS-Bibliothek, die diese Versionen noch anbieten kann; wo das nicht geht, bleibt das Ergebnis offen, statt als sicher gemeldet zu werden. Nach dem TLS-Handshake werden keine Anwendungsanfragen gesendet.

FEHLERBEHEBUNG

- Nicht öffentliche Adresse nicht freigegeben: Der Name wird zu einer internen Adresse aufgelöst. Bitten Sie den Betreiber der Installation, dieses Netz freizugeben (Clm:Discovery:AuthorizedPrivateNetworks), oder überwachen Sie einen öffentlichen Namen.
- TLS-Endpunkt nicht erreichbar: Prüfen Sie Firewall und Port und ob der Dienst auf jeder Adresse lauscht, zu der der Name aufgelöst wird; ein einzelner nicht erreichbarer Knoten hinter einem Load Balancer wird nur für diese Adresse gemeldet.
- Nicht vertrauenswürdige Kette bei einer privaten CA: Hinterlegen Sie das Stammzertifikat der CA als Vertrauensanker des Monitors. Fehlendes Zwischenzertifikat: Konfigurieren Sie den Server so, dass er die vollständige Kette sendet (Endzertifikat, gefolgt von den Zwischenzertifikaten).
- Knoten liefern unterschiedliche Zertifikate: Stellen Sie das erneuerte Zertifikat auf den übrigen Knoten bereit (Ausführung) und wählen Sie Jetzt prüfen.

7 Erneuerungspläne

Die Erneuerung eines bestimmten Zertifikats planen, Hindernisse sehen und sie über die Ausführungswarteschlange starten.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Solange die automatische Erneuerung für ein Zertifikat eingeschaltet ist (Ausführungswarteschlange, Richtlinie oder Zertifikatsdetails), wird es ohne Plan erneuert; Pläne sind für Zertifikate gedacht, die mit Freigabe erneuert werden oder eine Erneuerung außerhalb des Planers benötigen.
2. Öffnen Sie die Zertifikatsdetails und wählen Sie Erneuerung planen.
3. Prüfen Sie die fünf Phasen und die Ausführungsblocker. Sie werden jedes Mal aus dem aktuellen Zustand berechnet: Ein aktiviertes Bereitstellungsziel muss genau die Identitäten des Zertifikats enthalten (DNS-Namen, bei Client-Zertifikaten auch E-Mail-Adressen, UPNs und URIs) und einen Zweck haben, den die erweiterten Schlüsselverwendungen des Zertifikats erlauben, sein Agent (und gegebenenfalls der Verifizierungsagent) muss CERTYX innerhalb von Clm:Lifecycle:AgentContactWindow (standardmäßig 10 Minuten) kontaktiert haben, und das Ziel muss seine Zertifizierungsstelle angeben. Beheben Sie Hindernisse unter Ausführungswarteschlange (Bereitstellungsziele) oder Agenten und Ziele.
4. Ein Administrator wählt Plan freigeben bei einem Plan, der bereit zur Genehmigung ist. Die Genehmigung fordert über die reguläre Ausführungswarteschlange einen Erneuerungsauftrag für das passende Ziel an, gemäß aktueller Richtlinie und Subskription.

5. Ein anderer Administrator genehmigt den Auftrag (hier mit Auftrag als zweite Person genehmigen oder in der Ausführungswarteschlange); wer den Auftrag angefordert hat, sieht den Hinweis, dass ein anderer Administrator ihn genehmigen muss. Der Planstatus folgt dann dem Auftrag: In der Warteschlange für den Agenten, Wird vom Agenten ausgeführt, Ergebnis muss abgeglichen werden, Bereitgestellt und verifiziert, Fehlgeschlagen, Zurückgesetzt oder Auftrag storniert.
6. Wählen Sie nach einem fehlgeschlagenen, zurückgesetzten oder stornierten Auftrag Erneut mit neuem Auftrag genehmigen oder Plan abbrechen (nach Bestätigung; ein abgebrochener Plan kann nicht wiederhergestellt werden).
7. Jeder Plan verlinkt die Erneuerungsbereitschaft seines Zertifikats (jeder Schritt mit dem, was fehlt) und den Zustand des Agenten des Ziels.

EINGABEN UND PARAMETER

- Pläne verweisen auf ein Zertifikat, einen Verantwortlichen, einen Dienst und eine Richtlinienversion.
- Ein aktiver Plan pro Zertifikat; wiederholte Anfragen liefern den vorhandenen Plan zurück.
- Das Ziel wird automatisch gewählt: unter den aktivierten Zielen, deren Identitäten und Zweck zum Zertifikat passen, das mit den wenigsten Hindernissen (dann die niedrigste ID).
- Jede Entscheidung überträgt die Version des Plans; wurde der Plan inzwischen geändert, wird die Entscheidung abgelehnt und muss nach dem Aktualisieren der Liste wiederholt werden.

ERGEBNIS

Ein versionierter, protokollierter Plan, verknüpft mit seinem Ausführungsauftrag. Eine verifizierte Bereitstellung schließt den Plan ab; eine Richtlinienänderung oder eine Änderung von Verantwortlichem oder Dienst des Zertifikats gibt einen genehmigten Plan erneut zur Genehmigung zurück (Bereit zur Genehmigung oder Blockiert).

BERECHTIGUNGEN

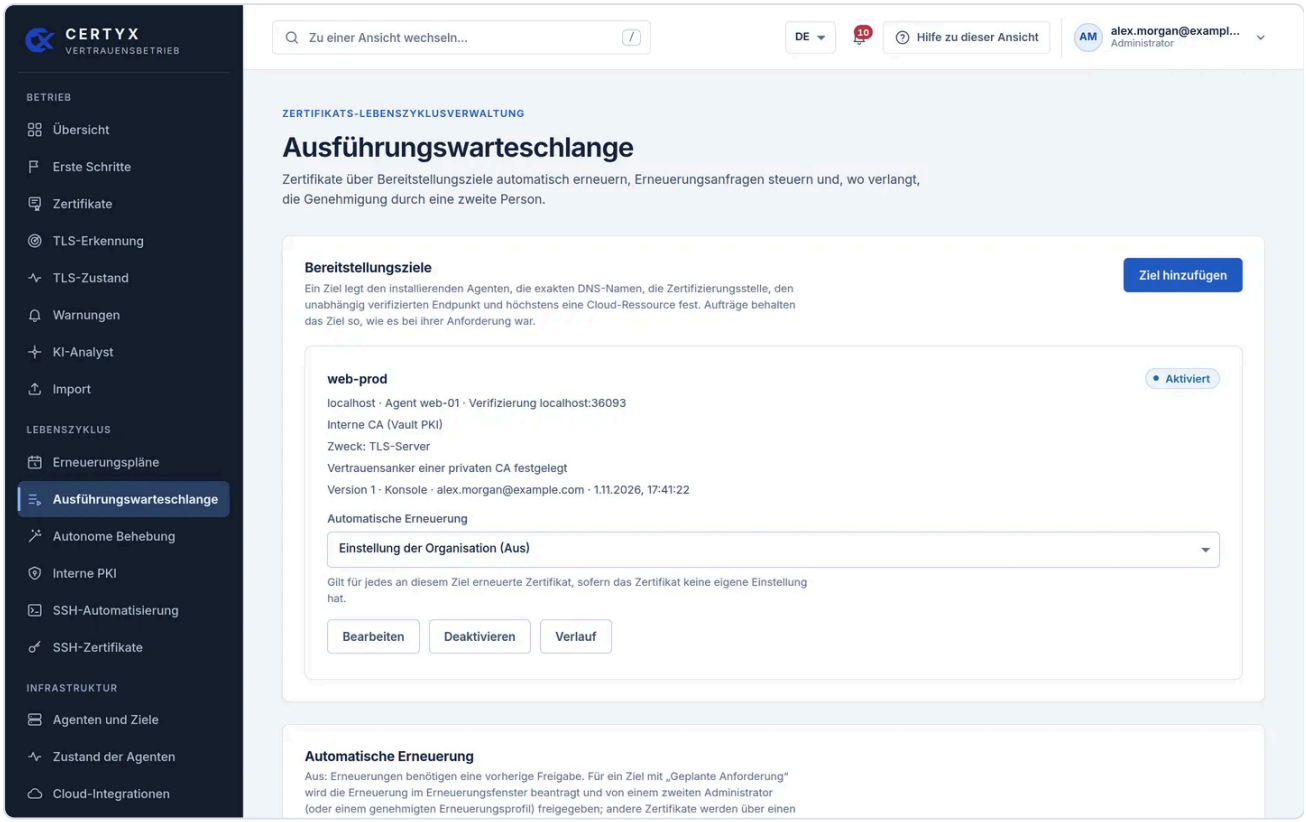
Operator oder Admin: Pläne erstellen (in den Zertifikatsdetails). Admin: Pläne genehmigen und abbrechen. Ein anderer Admin: den Auftrag genehmigen. Auditor und Operator: lesen, mit dem Hinweis, dass nur Administratoren Pläne genehmigen oder abbrechen.

EINSCHRÄNKUNGEN

Die Genehmigung umgeht nie das Vier-Augen-Prinzip: Der Administrator, der den Plan genehmigt hat, kann dessen Auftrag nicht genehmigen. Das Abbrechen eines Plans storniert den Auftrag nur, solange ihn kein Agent übernommen hat; ein laufender Auftrag wird beendet oder in der Ausführungswarteschlange abgeglichen. Ein ausstehender Auftrag aus einer früheren Richtlinienversion muss in der Ausführungswarteschlange storniert werden, bevor der Plan erneut genehmigt wird. Der Agentenkontakt wird aus Auftragsabfragen und Zustandsberichten geprüft; er beweist nicht, dass CA oder Bereitstellung gelingen — das belegen das Auftragsergebnis und die unabhängige Endpunktverifizierung. Das Anfordern des Auftrags erfordert die Funktion automatisierte Bereitstellung im Abonnement und macht die Zertifikatsfamilie verwaltet; ist das Limit verwalteter Familien des Abonnements erreicht, wird die Genehmigung abgelehnt.

8 Ausführungswarteschlange

Zertifikate über Bereitstellungsziele automatisch erneuern, Erneuerungsanfragen steuern und, wo verlangt, die Genehmigung durch eine zweite Person.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Unter Bereitstellungsziele fügt ein Administrator ein Ziel hinzu oder erstellt es aus einem Agentenentwurf unter Agenten und Ziele (Ziel hinzufügen öffnet das Formular; Zertifikatszweck siehe unten): installierender Agent, exakte DNS-Namen, Verifizierungshost, Port und Health-Pfad, die Zertifizierungsstelle (interne Vault PKI mit Mount und Rolle oder öffentliche ACME-CA) mit ihrer HTTPS-URL, optionale Vertrauensanker einer privaten CA (nur PEM-Zertifikate), ein optionaler Verifizierungsagent beim Kunden und höchstens eine Cloud-Ressource (AWS ACM: Zertifikat-ARN und Workload-Rolle; Azure Key Vault: Vault-URL, Zertifikat, Mandant und verwaltete Identität; Google Certificate Manager: Projekt, Standort, Zertifikat und Dienstkonto). Jedes Speichern erhöht die Version und erscheint unter Verlauf; Deaktivieren stoppt neue Aufträge. Ein Auftrag behält das vollständige Ziel aus dem Zeitpunkt der Anforderung, spätere Änderungen wirken also nicht auf ausstehende Aufträge. Wählen Sie dann ein aktiviertes Ziel.
2. Installation: Agent auf dem Host, der das Zertifikat nutzt (Standard), bedeutet, dass der installierende Agent die Dateien auf seinem eigenen Rechner schreibt und den Dienst neu lädt. Agent als SSH-Relay zu einem Host ohne Agent bedeutet, dass sich der installierende Agent per SSH mit dem eingegebenen Remote-Host verbindet, dort den Schlüssel erzeugt (er verlässt diesen Host nie), das Zertifikat installiert und den Dienst neu lädt; der Agent braucht dieses Ziel mit Remote in seiner Konfiguration und

in RelayDestinations aufgeführt und lehnt Aufträge für jeden anderen Host ab. SSH-Relay gilt für TLS-Server-Zertifikate ohne Cloud-Ressource, daher wird die Cloud-Auswahl ausgeblendet. Ohne Agent auf dem Host oder ein Relay mit SSH-Zugang kann CERTYX das Zertifikat nicht automatisch installieren.

3. Wählen Sie unter Ausstellung oder Erneuerung anfordern ein aktiviertes Bereitstellungsziel. Wählen Sie in Anfragetyp / Zertifikat Neues Zertifikat ausstellen und geben Sie unter Verantwortlichkeit für das neue Zertifikat Verantwortlicher, Dienst und Produktion ein, oder wählen Sie ein aktuelles (nicht ersetztes) Zertifikat aus dem Inventar zur Erneuerung; die Erneuerung behält dessen Verantwortlichkeit.
4. Die automatische Erneuerung (Bereich über dem Anfrageformular) ist standardmäßig eingeschaltet: Jedes Zertifikat mit einem passenden aktivierten Bereitstellungsziel wird ohne manuelle Freigabe erneuert. Im Erneuerungsfenster der Richtlinie beantragt der Planer den Auftrag, die automatische Erneuerung gibt ihn frei (vermerkt als freigegeben von system:auto-renewal), der Agent stellt das Zertifikat aus und installiert es, CERTYX prüft den Endpunkt unabhängig und das Inventar wird aktualisiert. Ein Administrator wählt Automatische Erneuerung ausschalten, um für die ganze Organisation eine Freigabe zu verlangen (Automatische Erneuerung einschalten fragt nach einer Bestätigung). Jede Zielkarte hat eine eigene Auswahl Automatische Erneuerung — Einstellung der Organisation, Automatisch erneuern oder Freigabe verlangen —, und die Zertifikatsdetails bieten dieselbe Auswahl je Zertifikat; die spezifischste Auswahl gilt (Zertifikat, dann Ziel, dann Organisation).
5. Wählen Sie Ausstellung oder Erneuerung anfordern. Ein anderer Administrator genehmigt den Auftrag mit Als zweite Person freigeben gemäß der aktuellen Richtlinie oder storniert ihn mit Abbrechen, solange ihn kein Agent übernommen hat.
6. Der Agent erzeugt Schlüssel und CSR dort, wo das Zertifikat genutzt wird (auf seinem eigenen Host oder als SSH-Relay auf dem Remote-Host), signiert über Vault, ACME oder DigiCert und installiert mit dem Connector des Ziels: pem-files, nginx, apache, haproxy, lighttpd, caddy, traefik, envoy, cribl, tomcat, java-keystore, postfix, dovecot, kubernetes-secret, windows-store, iis, oder in der Cloud-Ressource des Ziels (AWS ACM, Azure Key Vault, Google Certificate Manager) oder als Dateien bei einem reinen Client-Ziel. Dateibasierte Connectoren veröffentlichen die konfigurierten Dateien atomar mit Besitzer und Modus, führen Konfigurationsprüfung und Reload aus und prüfen den Endpunkt per TLS; bei einem Fehler wird die vorherige Generation erneut veröffentlicht. CERTYX verifiziert den konfigurierten Endpunkt unabhängig, bevor der Erfolg akzeptiert wird.
7. Bei einer abgelaufenen Lease (Auftrag im Abgleich) wählt ein Administrator Tatsächliches Ziel prüfen, prüft den beobachteten Nachweis und wählt dann Geprüftes Zertifikat übernehmen oder Ursprüngliche Installation bestätigen. CERTYX prüft den Fingerabdruck vor der Auflösung erneut; solange ein Kunden-Verifizierungsagent den Endpunkt noch nicht beobachtet hat, zeigt die Schaltfläche das Warten an. Der Anfragende kann seinen eigenen Auftrag nicht abgleichen.
8. Profile für automatische Erneuerung gelten bei ausgeschalteter automatischer Erneuerung: Für ein Ziel mit Geplanter Anforderung beantragt der Planer fällige Erneuerungen, die auf Freigabe warten. Ein Administrator wählt 90-Tage-Automatisierung anfordern, ein anderer Administrator wählt Als separater Administrator freigeben, und jeder von beiden kann Automatisierung widerrufen wählen; solange das Profil gilt, gibt es die geplanten Anforderungen frei. Erfordert die Abonnementfunktion AUTO_RENEWAL; eine Änderung des Ziels oder der Richtlinie macht die Freigabe ungültig.
9. Unix-Lebenszyklus-Agenten erfordern nur für den Eigentümer zugängliche Zustandsdaten, Secret-Dateien und Ausführungsjournale ohne symbolische Pfade oder symbolische übergeordnete Verzeichnisse. Unsichere oder übergroße Journale stoppen die Ausführung zum Abgleich durch einen Administrator. Der Start ändert keine Berechtigungen eines vorhandenen Zustandsverzeichnisses. Unter Windows wendet der Agent dieselbe Regel über ACLs auf Secret-Dateien und Journale an: Nur

LocalSystem, Administratoren oder die eigene Identität des Agenten dürfen sie besitzen und darauf zugreifen; alles andere wird abgelehnt. Das Windows-Installationsprogramm schränkt die ACL des Agentenverzeichnisses entsprechend ein.

10. Unix-Lebenszyklus-Agenten können genehmigte Text-Secrets aus Azure Key Vault, AWS Secrets Manager und Google Secret Manager über die kundenlokale Provider-CLI-Identität auflösen. Konfigurieren Sie exakte SecretBindings und führen Sie Clm.Agent secret-check mit der geschützten Lebenszykluskonfiguration als Dienstidentität aus, bevor Sie die Ausführung aktivieren. Werte bleiben lokal und werden nie ausgegeben. Siehe CUSTOMER-VAULTS.en.md. Die Auflösung über Provider-CLIs läuft nur auf Unix-Agenten; unter Windows stehen nur Secrets aus geschützten Dateien zur Verfügung. Private Schlüssel werden in Software auf dem Agent-Host erzeugt und gehalten (kein HSM), und der Agent versendet keine E-Mails vom Kundenhost.
11. HashiCorp Vault KV wird ebenfalls über eine exakte HTTPS-Bindung mount/path#field und einen kundenlokalen nativen Token-Helper unterstützt. TLS-Verifizierung ist erforderlich; Namespaces werden nicht unterstützt. Ein Lesevorgang schlägt fehl, wenn der Zugriff verweigert wird, die Identität widerrufen ist oder dem Vault-Zertifikat nicht vertraut wird. Das Vault-Token stammt aus dem Token-Helper des Kunden; CERTYX erstellt oder erneuert keine Vault-Identitäten.
12. Gespeicherte Lebenszyklusergebnisse werden nach vorübergehenden Verbindungsfehlern, Zeitüberschreitungen von Anfragen und HTTP 408/429/500/502/503/504 erneut übertragen, unter Verwendung von PollSeconds und der Grenze OperationTimeoutSeconds. Derselbe Auftrag, dieselbe Lease und dasselbe Ergebnis werden wiederverwendet; Ausstellung und Installation werden nie wiederholt. Die Wiederherstellung nach einem Neustart erneuert die Lease, während das gespeicherte Ergebnis zugestellt wird. Authentifizierungs- und Autorisierungsfehler, abgelaufene/abgeglichene Leases und TLS-Vertrauensfehler stoppen zum Abgleich. Eine verlorene Lease kann durch diesen Mechanismus nicht erneuert werden; ein Ausfall, der die Lease- oder Vorgangsgrenze überschreitet, erfordert weiterhin einen Abgleich durch einen Administrator.
13. Alle JSON-Konfigurationsleser des Agenten lehnen symbolische Dateien oder übergeordnete Verzeichnisse, Unix-Gruppen-/Andere-Berechtigungen, Dateien über 1 MiB und ungültiges UTF-8 vor der Deserialisierung ab. Schützen Sie die Konfiguration unter Unix mit chmod 600. Relative Befehlszeilenpfade werden in einen absoluten Pfad aufgelöst und denselben Prüfungen unterzogen. UTF-8 mit oder ohne BOM wird unterstützt. Einstellungen und asynchrone Leser verwenden dieselben Regeln; Fehlerausgaben enthalten keine Konfigurationswerte. Unter Windows lehnen die Leser eine Datei ab, die ein anderer Prinzipal als LocalSystem, Administratoren oder die eigene Identität des Agenten besitzt, lesen oder ändern kann; richten Sie vor der Bereitstellung restriktive ACLs ein.
14. Private Endpunkte können einen separaten registrierten Endpunkt-Verifizierer verwenden. Der Operator bindet dessen ID an das Ausführungsziel; wählen Sie unter Agenten und Ziele → Registrierte Agents beim Installer „Ausführung des Zertifikatslebenszyklus aktivieren“ und bei einer anderen Agentenidentität „Unabhängige Endpunktverifizierung aktivieren“. Der Verifizierer prüft genehmigte lokale TLS/HTTP-Endpunkte, bevor der Erfolg akzeptiert wird. Die Einrichtung ist ein Befehl auf dem Prüfhost: Die Zielkarte unter Ausführung → Bereitstellungsziele zeigt Unabhängigen Endpunkt-Prüfer einrichten mit der Erteilung, Prüfumfang herunterladen (Ziel-ID, Prüfhost, Port, Health-Pfad und Vertrauensanker des Ziels; nur öffentliche Daten) und dem Befehl configure-verifier-linux.sh add-target (Linux, clm-endpoint-verifier.service unter dem Agent-Konto) bzw. configure-verifier-windows.ps1 add-target (Windows, geplante Aufgabe CERTYX Endpoint Verifier als LOCAL SERVICE). Das Skript schreibt die nur für den Besitzer lesbare Konfiguration aus der eigenen Identität des Agents, führt einen geprüften Zyklus aus, startet den Dienst und wartet bis zu zehn Minuten auf die Erteilung, solange CERTYX mit HTTP 403 antwortet; remove-target, disable und status verwalten ihn, das

Deinstallationsprogramm entfernt ihn. Ein neuer Agent erhält die Rolle bei der Installation (CLM_AGENT_ENDPOINT_VERIFIER unter Linux, -EndpointVerifierTarget unter Windows). Ohne Vertrauensanker im Ziel muss der Prüfhost der ausstellenden CA selbst vertrauen.

15. Registrierte Installer melden ihre eigene Lebenszyklus-Workload in Zustand der Agenten (starting, idle oder error). Ausbleibende Meldungen bleiben auch bei funktionierender Erkennung sichtbar. Der Prozesszustand ersetzt weder das Ausführungsergebnis noch den unabhängigen Endpunktnachweis. Prüfen Sie die geschützten lokalen Journale, wenn ein Zyklus zum Abgleich stoppt.
16. Zertifikatszweck: Jedes Ziel ist ein TLS-Server- (Standard), TLS-Client- oder TLS-Server-und-Client-Ziel. Ein TLS-Client-Zertifikat authentifiziert einen Benutzer, ein Gerät oder einen Dienst gegenüber einem Server per Mutual TLS (EKU clientAuth). Wählen Sie Interne CA (Vault PKI) mit einer Rolle, die client_flag setzt (für reine Clients server_flag=false); öffentliche CAs werden abgelehnt, weil ACME und DigiCert-TLS-Produkte nur Server-Zertifikate ausstellen. Geben Sie die Identitäten unter Client-Identitäten an: DNS-Namen, E-Mail-Adressen, Benutzerprinzipalnamen und URIs sowie optional einen allgemeinen Namen des Antragstellers. Ein reines Client-Ziel hat keinen Verifizierungshost, keinen Prüf-Agenten und keine Cloud-Ressource: Der Agent erzeugt den Schlüssel lokal, der CSR beantragt genau diese Identitäten, der Agent installiert fullchain.pem und privkey.pem (sowie bundle.p12, wenn sein Ziel eine PKCS#12-Passwortreferenz nennt) und prüft die installierten Dateien lokal (Schlüssel, Kette zu seinen Vertrauensankern, EKU clientAuth), bevor er meldet. CERTYX akzeptiert das öffentliche Zertifikat nur mit genau den Identitäten und EKUs des Auftrags. Das Agentenziel muss denselben Purpose und dieselben Client-Identitäten deklarieren (siehe AGENT-INSTALLATION).
17. Aus der Erneuerungsbereitschaft eines Zertifikats öffnet Ziel mit diesen Werten anlegen das Zielformular mit dem Vorschlag; unter jedem ausgefüllten Feld steht Übernommen aus: … und unter jedem Feld, das CERTYX nicht bestimmen konnte, was einzugeben ist und warum. ID und Zweck: die des lokalen Agentenziels mit genau den Namen des Zertifikats (der Agent führt nur Aufträge aus, deren Ziel-ID, Namen und Zweck einem lokalen Ziel entsprechen), andernfalls eine ID aus dem ersten Namen und der Zweck aus dem Zertifikat; Namen und Client-Identitäten stammen aus dem Zertifikat. Installierender Agent: der Agent dieses Ziels, andernfalls der einzige Agent mit Lebenszyklusprozess, andernfalls der einzige Agent, dessen gemeldete Netzwerkkarte die Adresse enthält, an der das Zertifikat beobachtet wurde, sofern er den Lebenszyklusprozess hat; sonst leer mit dem Grund. Prüfhost: Er muss ein Name (oder eine IP-Adresse) im Zertifikat sein, weil CERTYX das Zertifikat gegen ihn prüft. Die Netzwerkerkennung beobachtet IP-Adressen, daher löst CERTYX die DNS-Namen des Zertifikats auf (ohne Platzhalternamen, begrenzte Anzahl und Zeit) und trägt den Namen ein, der zur beobachteten Adresse aufgelöst wird; trifft keiner zu, den ersten Namen mit dem Hinweis, ihn zu prüfen; bei nur Platzhalternamen bleibt der Host leer; eine IP-Adresse nur, wenn das Zertifikat sie enthält oder keine DNS-Namen hat. Port: wo das Zertifikat beobachtet wurde (z. B. 9000); 443 nur, wenn es nie beobachtet wurde. Zertifizierungsstelle: Hat ein aktiviertes Ziel bereits ein Zertifikat derselben CA ausgestellt (gleicher Aussteller und Schlüsselbezeichner), dessen CA-Typ, URL, Vault-Mount und -Rolle und Vertrauensanker; andernfalls der Typ aus dem Agentenziel, der im Inventar erfasste CA-Typ oder die Beobachtung (eine nicht vertrauenswürdige Kette bedeutet eine interne CA; eine vertrauenswürdige Kette eine öffentliche CA nur, wenn alle Namen öffentlich sind und nicht unter Endungen wie .internal, .local oder .home.arpa liegen). Für eine interne CA ohne solches Ziel geben Sie Vault-URL, Mount und Rolle ein, die Ihr Agent verwendet. Vertrauensanker werden nur aus diesem Ziel oder mit dem tatsächlichen Stammzertifikat der ausstellenden CA aus dem Inventar gefüllt; sonst fügen Sie die private Stammzertifizierungsstelle (PEM) ein, sofern der CERTYX-Host oder der Verifizierungsagent ihr nicht schon vertraut. Vor dem Speichern wird nichts gespeichert.

Lebenszyklusagenten melden ihre lokalen Ziele (Konnektor, Bereitstellungsverzeichnis, Dateien, Prüf- und Reload-Befehle, Cloud-Ressource, Endpunkt) mit ihrer Prozesstelemetrie; Geheimnisse und Geheimnisreferenzen werden nie gemeldet.

18. Ein fehlgeschlagener oder zurückgesetzter Auftrag zeigt das Ergebnis des Agenten und die nächsten Schritte; jeder Auftrag verlinkt die Erneuerungsbereitschaft seines Zertifikats und den Zustand seines Agenten.

EINGABEN UND PARAMETER

- Bereitstellungsziel: ein aktiviertes Ziel der Organisation. Ziele aus der Serverkonfiguration CLM_EXECUTION_TARGETS (Clm:Execution:Targets) werden bei der ersten Verwendung einmalig in ihre Organisation übernommen und danach nur hier verwaltet. Serverdateipfade (Vertrauensanker-Datei, Test-Hilfe ohne Sperrprüfung, ACME-Renewal-Information-Verzeichnis) stammen nur aus dieser Konfiguration und bleiben beim Bearbeiten eines solchen Ziels erhalten. Ungültige Eingaben werden mit Begründung abgelehnt.
- Zertifikat: im Inventar und nicht ersetzt, mit genau den Identitäten des Ziels (DNS-Namen und bei Client-Zielen E-Mail-Adressen, UPNs und URIs) und erweiterten Schlüsselverwendungen, die den Zweck des Ziels erlauben; sonst wird die Anfrage mit dieser Begründung abgelehnt.
- Neuausstellung: Verantwortlicher und Dienst erforderlich, jeweils 1–200 Zeichen; sie reserviert eine verwaltete Zertifikatsfamilie innerhalb der Kapazität des Abonnements.
- Die Zertifizierungsstelle Nicht festgelegt wird beim Speichern angenommen, aber ein Erneuerungsplan für ein solches Ziel bleibt blockiert, bis die Zertifizierungsstelle gewählt ist.
- Die Genehmigung verwendet die Auftragsversion und die Identität des Genehmigenden.
- Schlüssel- und Bereitstellungswurzeln müssen absolut und frei von Links sein. Private Schlüssel und Wiederherstellungsjournale erfordern Berechtigungen nur für den Eigentümer; verlinkte, gemeinsam genutzte oder übergroße Zustandsdaten werden abgelehnt. Nur der verwaltete UUID-Link der aktuellen Generation ist zulässig.
- Formate der Ziele (jedes Feld zeigt seine eigene Hilfe, der Browser nennt das erwartete Format): IDs 1–100 Buchstaben, Ziffern, Bindestriche und Unterstriche; 1–100 unterschiedliche DNS-Namen ohne Platzhalter; Verifizierungshost als Hostname oder IP-Adresse ohne https://, Pfad oder Port; Health-Pfad beginnend mit / (z. B. /healthz); CA-URL beginnend mit https://; Vault-Mount und -Rolle bis zu 120 Buchstaben, Ziffern und . _ / -; Vertrauensanker als PEM-Zertifikatsblöcke bis 64 KiB; AWS arn:aws:acm:REGION:KONTO:certificate/UUID mit einer Rolle arn:aws:iam::GLEICHES-KONTO:role/NAME; Azure https://NAME.vault.azure.net/, Zertifikatsname aus Buchstaben, Ziffern und Bindestrichen, Mandanten- und Client-ID als GUID; Google Projekt-ID, Standort global oder eine Region wie europe-west1, Zertifikats-ID und NAME@PROJEKT.iam.gserviceaccount.com.
- Formate der Client-Identitäten (jedes Feld zeigt seine Hilfe; der Server nennt bei Ablehnung das erwartete Format): E-Mail erika.mustermann@example.com (ASCII, ein @, DNS-Domäne, höchstens 254 Zeichen); Benutzerprinzipalname emustermann@corp.example.com (Anmeldename, @, DNS-Suffix des Verzeichnisses, nicht CORP\emustermann); URI mit Schema wie spiffe://example.org/ns/prod/sa/payments oder urn:uuid:..., ohne Leerzeichen oder Benutzer:Passwort; allgemeiner Name 1–64 Zeichen, erforderlich, wenn nur URIs angegeben sind. Ein Wert pro Zeile; höchstens 100 Identitäten.
- Remote-Host (SSH-Relay): ein DNS-Name oder eine IP-Adresse, höchstens 253 Zeichen, genau wie Remote.Host in der Konfiguration des Relay-Agenten, z. B. web-01.internal.example.

ERGEBNIS

Dauerhaftes Ausführungsergebnis, zurückgegebenes öffentliches Zertifikat im Inventar und Prüfnachweise. Das ersetzte Zertifikat wird außer Betrieb genommen.

BERECHTIGUNGEN

Admin: Ziele erstellen, bearbeiten, deaktivieren und aktivieren, nicht übernommene Aufträge stornieren, Aufträge abgleichen sowie Automatisierungsprofile anfordern und widerrufen. Operator oder Admin: Aufträge anfordern (auf einem Dienst mit Abonnements nur mit der Funktion AUTO_DEPLOYMENT). Ein anderer Admin als der Anfragende: Aufträge und Automatisierungsprofile genehmigen; der Anfragende kann seinen Auftrag nicht abgleichen. Auditor (und Operator): Ziele, Profile und Aufträge lesen; für einen Auditor ist das Anfrageformular schreibgeschützt. Jede Rolle sieht die Schaltfläche Verlauf eines Ziels und dessen Änderungsverlauf (Version, Änderung, E-Mail-Adresse des Kontos, Zeit); die Schaltflächen Bearbeiten und Deaktivieren/Aktivieren sehen nur Administratoren. Admin: automatische Erneuerung für die Organisation ein- oder ausschalten und je Ziel und Zertifikat wählen; jede Rolle sieht die Einstellung.

EINSCHRÄNKUNGEN

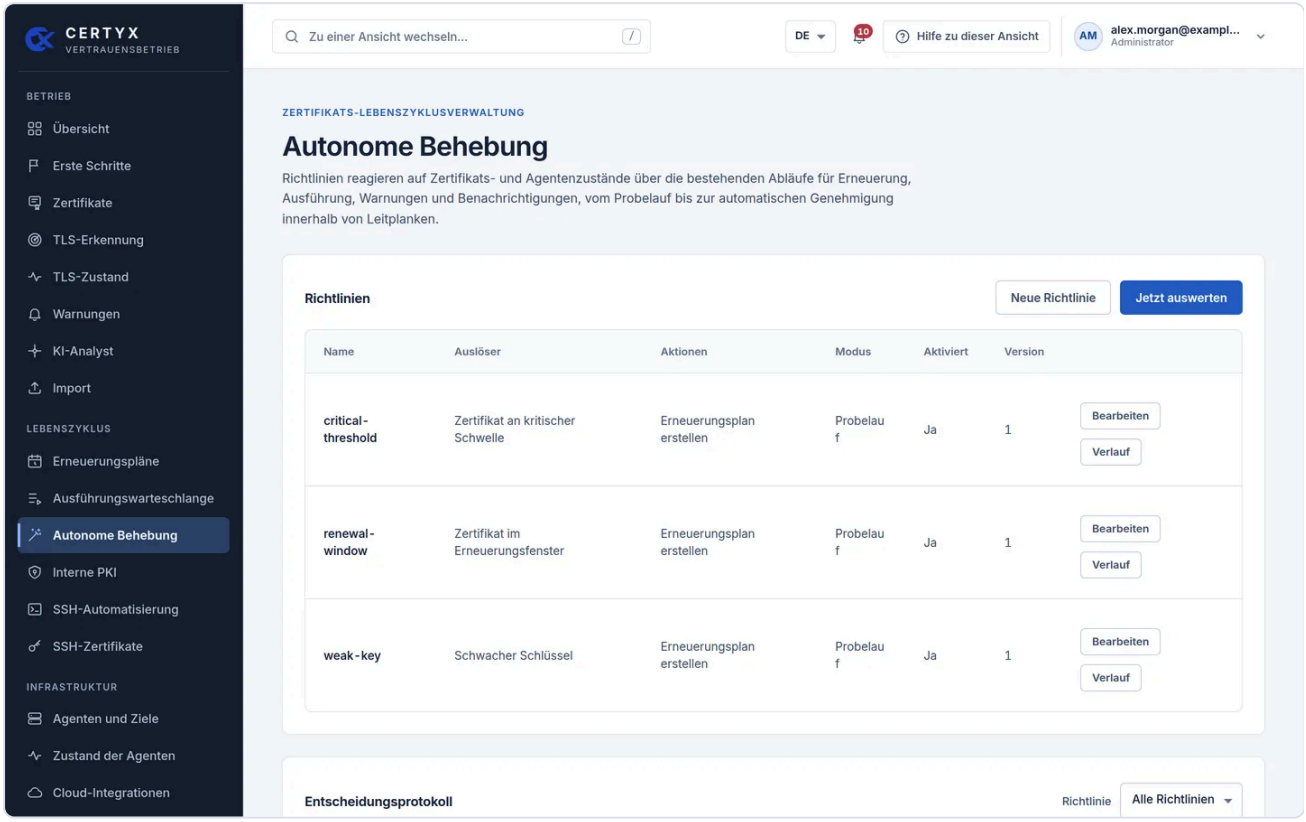
Der Erneuerungsplaner prüft die aktivierten Ziele jeder Organisation alle Clm:Lifecycle:SchedulerInterval (standardmäßig 5 Minuten). Die automatische Erneuerung gilt für das neueste Zertifikat mit genau den Identitäten eines Ziels; sie erfordert die Abonnementfunktion AUTO_RENEWAL (ohne sie wartet jede Erneuerung auf Freigabe) und beginnt kurzlebige Zertifikate erst im letzten Drittel ihrer Laufzeit. Nach einem fehlgeschlagenen, zurückgesetzten oder abgebrochenen Auftrag an einem Ziel wartet die nächste Erneuerung auf Freigabe; nach deren Erfolg laufen Erneuerungen wieder automatisch. Höchstens Clm:Lifecycle:AutomaticRenewalsPerDay (standardmäßig 200) Erneuerungen je Organisation werden innerhalb von 24 Stunden automatisch freigegeben; weitere fällige Erneuerungen warten auf Freigabe. Bevor der Agent einen automatisch freigegebenen Auftrag erhält, prüft CERTYX ihn erneut: Ein geändertes Ziel bricht ihn ab, eine ausgeschaltete Einstellung schickt ihn zurück zur Freigabe. Manuell angeforderte Aufträge und Aufträge aus Erneuerungsplänen benötigen immer einen zweiten Administrator. Der Standard der Installation ist Clm:Lifecycle:AutomaticRenewalByDefault (true). Setzen Sie auf einem von mehreren Organisationen gemeinsam genutzten Dienst Clm:Execution:AllowPrivateVerificationEndpoints auf false: Loopback-, private und Link-Local-Verifizierungshosts benötigen dann einen Verifizierungsagenten beim Kunden, und die Steuerungsebene verweigert die Verifizierung eines Hosts, der auf eine solche Adresse auflöst. Die Agentenregistrierung nutzt Einmalcodes unter Agenten; die lokale Konfiguration des installierten Agenten (CA-Anmeldedaten, Bereitstellungspfade) bleibt auf dem Kundenhost. Die Prüfung von Loopback-, privaten oder Link-Local-Endpunkten durch CERTYX selbst erfordert die Erlaubnis des Plattformbetreibers für Ihre Organisation; andernfalls weisen Sie einen Prüf-Agenten zu. TLS-Client-Zertifikate werden nur über Vault-PKI-Rollen ausgestellt; ACME, DigiCert und Cloud-TLS-Speicher werden mit konkretem Grund abgelehnt. Client-Zertifikate werden auf Unix-Agenten als PEM-Dateien und optionales PKCS#12-Bündel bereitgestellt; Windows-Zertifikatsspeicher, Browser-Enrollment und Smartcard-Bereitstellung werden nicht unterstützt. Ihre Prüfung ist die lokale Prüfung des installierenden Agenten, keine unabhängige Endpunktbeobachtung, und ein reiner Client-Auftrag im Abgleich kann nicht durch Beobachtung gelöst werden: Der Agent liefert ein gespeichertes Ergebnis beim nächsten Lauf, andernfalls prüft der Betreiber das Bereitstellungsverzeichnis auf dem Agent-Host. Das SSH-Relay installiert nur TLS-Server-Zertifikate (keine Client-Zertifikate, kein Windows-Speicher) mit einem auf dem Remote-Host erzeugten RSA-3072-Schlüssel; ein Remote-Ziel sollte genau einem Relay gehören. Maildienste werden auf Ports mit implizitem TLS (465, 993, 995) geprüft; STARTTLS wird nicht gesprochen.

FEHLERBEHEBUNG

- Die Bereitschaft meldet, dass der Agent kein lokales Ziel mit der Ziel-ID hat: ein Ziel mit genau dieser ID, denselben DNS-Namen und demselben Zweck in die Agentenkonfiguration (agent.json, Destinations) aufnehmen, den Agenten neu starten und auf seine nächste Meldung warten.
- Die Verifizierung schlägt nach dem Anlegen eines Ziels aus der Bereitschaft mit einem Namensfehler fehl: Der Prüfhost muss ein Name (oder eine IP-Adresse) im Zertifikat sein. Ersetzen Sie eine IP-Adresse durch den DNS-Namen des Zertifikats, der den Endpunkt erreicht; meldet der Hinweis, dass die Namen nicht zur beobachteten Adresse aufgelöst wurden, prüfen Sie DNS auf dem CERTYX-Host oder geben Sie den Namen ein, den der Endpunkt ausliefert.
- Das Agentenziel nennt andere Namen, einen anderen Zweck oder eine andere CA-Art: Ziel und Agentenziel angleichen; interne Ziele benötigen ein Vault-Ziel, öffentliche ACME oder DigiCert.
- Der Agent hat seine Ziele nicht gemeldet: Er meldet sie mit jeder Meldung des Lebenszyklusprozesses, sobald er mit registrierter Identität läuft; seine Diagnose im Agentenzustand prüfen.
- Zurückgesetzt: Der Agent hat das neue Zertifikat installiert, die Endpunktprüfung schlug aber fehl und die vorherige Generation wurde wiederhergestellt und geprüft; Reload-Befehl, ausgelieferten Host und Port sowie Vertrauensanker prüfen und den Plan erneut freigeben.
- Abstimmen: Die Lease lief vor einem Ergebnis ab; hier das tatsächliche Ziel prüfen und das geprüfte Zertifikat übernehmen oder die ursprüngliche Installation bestätigen.
- Die Bereitschaft meldet, dass der Agent in einem anderen Modus installiert: Das Ziel nennt SSH-Relay, aber das Agentenziel hat kein Remote (oder umgekehrt). Gleichen Sie beides an: Wählen Sie die Installation im Ziel, ergänzen oder entfernen Sie Remote und RelayDestinations in der Agentenkonfiguration und warten Sie auf die nächste Meldung.
- Die Bereitschaft meldet, dass das Relay auf einem anderen Host bereitstellt: Setzen Sie den Remote-Host des Ziels genau auf Remote.Host des Agentenziels. Führen Sie Clm.Agent relay-check auf dem Relay aus, um Host-Schlüssel-Festlegung, SSH-Anmeldung, Helfer, sudo-Regel und Konfigurationsprüfung ohne Änderung eines Zertifikats zu testen.

9 Autonome Behebung

Richtlinien reagieren auf Zertifikats- und Agentenzustände über die bestehenden Abläufe für Erneuerung, Ausführung, Warnungen und Benachrichtigungen, vom Probelauf bis zur automatischen Genehmigung innerhalb von Leitplanken.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Erfordert die Abonnementfunktion AUTONOMOUS_REMEDIATION. Ein Administrator wählt Neue Richtlinie und gibt Kennung (1–100 Buchstaben, Ziffern, Bindestriche oder Unterstriche; später nicht änderbar), Namen (1–100 Zeichen), Aktiviert, Auslöser und die von ihm unterstützten Aktionen, den Modus sowie optional bis zu 50 durch Kommas getrennte Dienste, auf die die Richtlinie beschränkt ist (je bis zu 200 Zeichen; leer bedeutet alle Dienste), den zuzuweisenden Verantwortlichen (1–200 Zeichen, erforderlich für Verantwortlichen zuweisen) und die zu benachrichtigende Zuständigkeitsgruppe (erforderlich für Gruppe benachrichtigen) an.
2. Auslöser: Zertifikat im Erneuerungsfenster, an der kritischen Schwelle, schwacher Schlüssel, schwache Signatur (jeweils auch für abgelaufene Zertifikate, wo zutreffend), Zertifikat außerhalb von CERTYX ersetzt (offene Discovery-Warnung) und Agent offline (offline, fehlerhaft oder Identität abgelaufen).
3. Vorschau (Probelauf) wertet den Entwurf mit den aktuellen Daten aus und zeigt, was er tun würde, ohne etwas zu ändern oder aufzuzeichnen. Richtlinie speichern legt eine neue Version an; Bearbeiten öffnet eine vorhandene Richtlinie; Verlauf listet jede Version mit dem Ändernden.
4. Modi: Probelauf zeichnet nur auf, was geschehen würde. Vorschlagen erstellt Erneuerungspläne und fordert Ausführungsaufträge an, die weiterhin die normale Vier-Augen-Genehmigung benötigen, sendet Gruppenbenachrichtigungen und hält Bestätigungen und Verantwortlichenänderungen als

Empfehlungen fest. Automatische Genehmigung genehmigt Pläne und Aufträge zusätzlich innerhalb der Leitplanken, im Namen des Administrators, der die Richtlinie nach Bestätigung der Warnung gespeichert hat. Das Speichern im automatischen Modus erfordert das Ankreuzen von „Ich verstehe dies und aktiviere die automatische Genehmigung für diese Richtlinie“, mindestens ein Änderungsfenster und, wenn die Richtlinie Erneuerungspläne erstellt oder Aufträge anfordert, mindestens ein zulässiges Ziel.

5. Die Auswertung läuft alle Clm:Remediation:Interval (Standard 5 Minuten) für jede aktive, lizenzierte Organisation auf jeweils einer Anwendungsinstanz, sofern der Serverbetreiber Clm:Remediation:WorkerEnabled nicht auf false gesetzt hat; Jetzt auswerten startet sie sofort. Das Entscheidungsprotokoll listet jede Entscheidung mit Ergebnis (würde handeln, vorgeschlagen, ausgeführt, übersprungen, abgelehnt, fehlgeschlagen), übersetzten Gründen und Verweisen auf Ziel, Plan und Auftrag; Erklären öffnet den KI-Analysten, wenn er aktiviert ist.

EINGABEN UND PARAMETER

- Aktionen je Auslöser: Zertifikatsauslöser unterstützen Warnung bestätigen, Verantwortlichen zuweisen, Gruppe benachrichtigen, Erneuerungsplan erstellen und Ausführungsauftrag anfordern; außerhalb von CERTYX ersetzt unterstützt Warnung bestätigen und Gruppe benachrichtigen; Agent offline unterstützt Gruppe benachrichtigen.
- Verantwortlichen zuweisen ändert nur Zertifikate ohne Verantwortlichen (leer oder „unassigned“); ein Zertifikat mit Verantwortlichem wird mit diesem Grund übersprungen.
- Leitplanken der automatischen Genehmigung: zulässige Ziele (bis zu 200 Ausführungsziele der Organisation), maximale ausgeführte Aktionen in 24 Stunden (1 bis Clm:Remediation:MaxActionsPerDayLimit, Standard 500), bis zu 20 Änderungsfenster in UTC (je mindestens ein Tag; Startstunde 0–23 vor Endstunde 1–24) und ob Produktionszertifikate erlaubt sind. Erneuerungen werden nur für ein zulässiges Ziel mit unabhängigem Verifizierungsendpunkt genehmigt.
- Produktionskennzeichen und Verantwortlicher stammen aus den Zertifikatsmetadaten im Inventar; Benachrichtigungen gehen über das SMTP-Relay der Organisation an Zuständigkeitsgruppen mit Mitgliedern.

ERGEBNIS

Pläne und Aufträge werden als system:remediation:<Richtlinie> erstellt; automatisch genehmigte Aufträge tragen den bestätigenden Administrator als Genehmigenden und laufen durch die normale Ausführung, deren Verifizierung eine fehlgeschlagene Bereitstellung zurücksetzt. Jede Entscheidung wird im Entscheidungsprotokoll (aufbewahrt Clm:Remediation:DecisionRetentionDays, Standard 400 Tage) und im Sicherheitsjournal gespeichert; eine identische Entscheidung wird höchstens einmal pro Clm:Remediation:DecisionRepeatWindow (Standard 24 Stunden) festgehalten. Richtlinienänderungen werden versioniert und protokolliert.

BERECHTIGUNGEN

Richtlinien, Verlauf und Entscheidungsprotokoll lesen: jede Rolle der Organisation. Erstellen, ändern, Vorschau und Auswertung: Administrator.

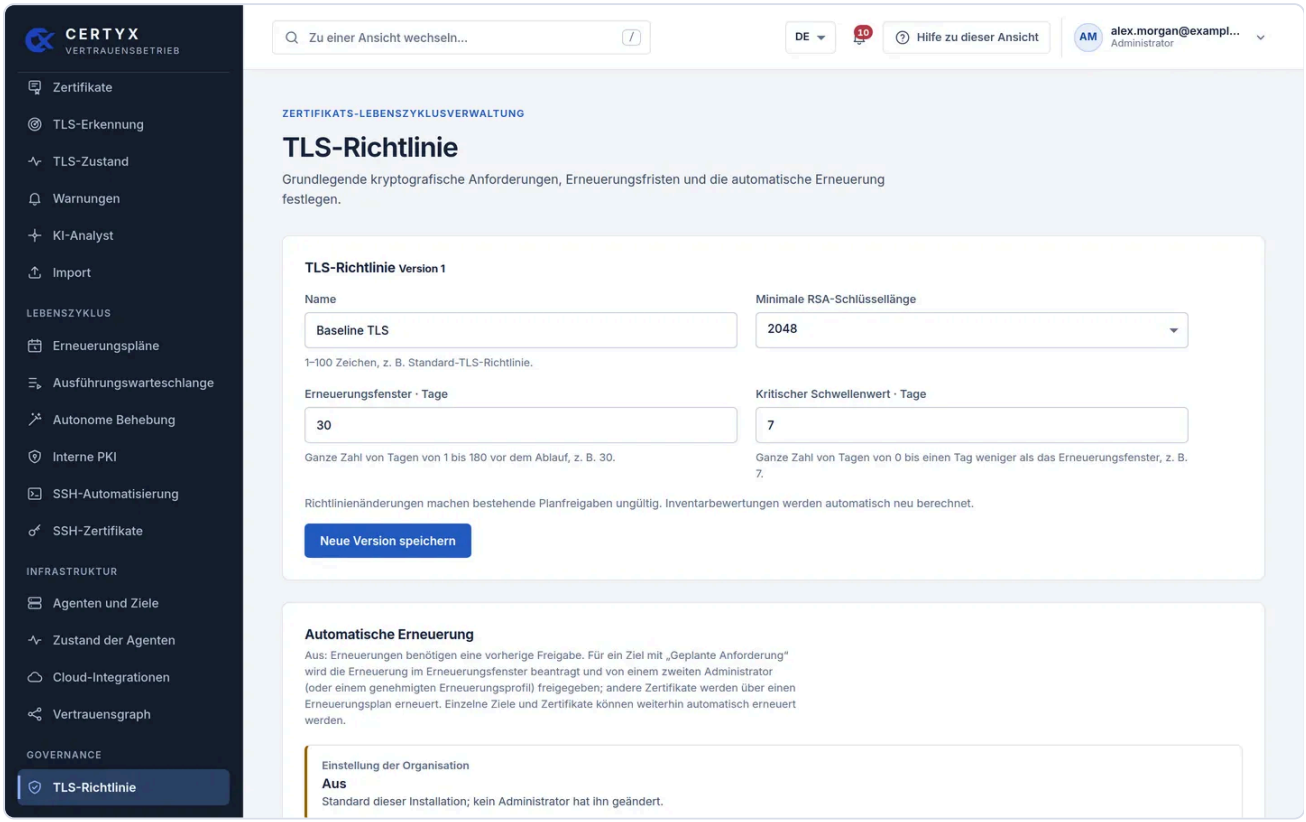
EINSCHRÄNKUNGEN

Widerruf ist nicht verfügbar: Kein CERTYX-Ablauf widerruft TLS-Zertifikate, daher wird eine Richtlinie mit dieser Aktion abgelehnt. Der Vorschlagsmodus ändert weder Verantwortliche noch Warnungen. Eine Erneuerung erfolgt nur, wenn der Plan keine Blocker hat (Ziel mit genau den Identitäten des Zertifikats und passendem Zweck, erreichbarer Agent, konfigurierte Zertifizierungsstelle). Ohne die Abonnementfunktion

meldet die Ansicht, dass das Abonnement keine autonome Behebung enthält, und keine Richtlinie wird ausgewertet. Die automatische Genehmigung prüft die Rolle des bestätigenden Administrators zum Genehmigungszeitpunkt nicht erneut; das Bearbeiten einer Richtlinie im automatischen Modus erfordert eine neue Bestätigung durch den Bearbeitenden. Höchstens Clm:Remediation:MaxPoliciesPerOrganization Richtlinien (Standard 50) und Clm:Remediation:MaxSubjectsPerPolicy Gegenstände pro Richtlinie und Durchlauf (Standard 200). Die Erklärung durch den Analysten erfordert einen aktivierten KI-Analysten.

10 TLS-Richtlinie

Grundlegende kryptografische Anforderungen, Erneuerungsfristen und die automatische Erneuerung festlegen.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Prüfen Sie die aktuelle Version neben dem Titel.
2. Geben Sie „Name“, „Minimale RSA-Schlüssellänge“, „Erneuerungsfenster · Tage“ und „Kritischer Schwellenwert · Tage“ ein.
3. Wählen Sie „Neue Version speichern“. Genehmigte Erneuerungspläne kehren in den Status geplant zurück und müssen erneut genehmigt werden; prüfen Sie die neu bewerteten Zertifikate.
4. Automatische Erneuerung zeigt die Einstellung der Organisation: Ein (Standard) erneuert jedes Zertifikat mit passendem Bereitstellungsziel im Erneuerungsfenster ohne manuelle Freigabe; Aus verlangt für jede Erneuerung die Freigabe durch einen zweiten Administrator. Administratoren wählen Automatische Erneuerung ausschalten oder Automatische Erneuerung einschalten; Ziele und Zertifikate können sie unter Ausführungswarteschlange und in den Zertifikatsdetails übersteuern.

EINGABEN UND PARAMETER

- Minimale RSA-Schlüssellänge: 2.048, 3.072 oder 4.096 Bit.
- Erneuerungsfenster: 1–180 Tage. Kritischer Schwellenwert: 0–179 Tage, unterhalb des Erneuerungsfensters.
- Name: erforderlich, 1–100 Zeichen.

- Standardrichtlinie vor dem ersten Speichern: „Baseline TLS“, RSA 2.048 Bit, Erneuerungsfenster 30 Tage, kritischer Schwellenwert 7 Tage.

ERGEBNIS

Eine neue Richtlinienversion und ein Eintrag im Prüfprotokoll. Bewertungen werden beim Lesen neu berechnet; Genehmigungen von Plänen und Aufträgen sind durch Versionsprüfungen geschützt.

BERECHTIGUNGEN

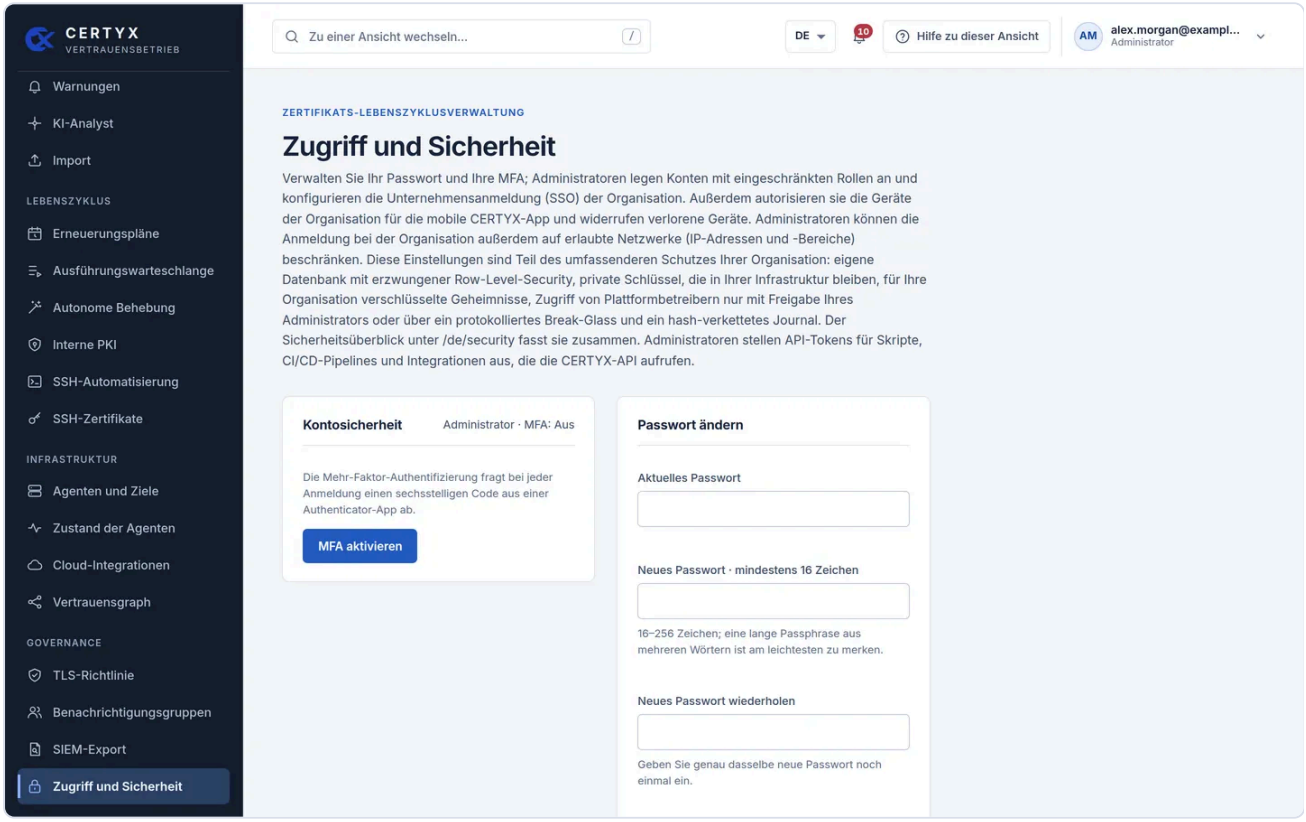
Lesen: alle Rollen. Schreiben (Richtlinie und automatische Erneuerung): Admin.

EINSCHRÄNKUNGEN

Dies ist eine Basisrichtlinie für Gültigkeit und öffentliche Schlüssel, keine vollständige Regel-Engine für die Organisation. Feste Basisregeln sind nicht bearbeitbar: ECDSA-Schlüssel unter 256 Bit, andere Algorithmen als RSA und ECDSA sowie SHA-1- oder MD5-Signaturen sind immer kritisch. Hat zwischenzeitlich jemand eine andere Version gespeichert, wird das Speichern mit der Aufforderung zum Neuladen abgelehnt. Eine Änderung verändert keine bereits ausgestellten Zertifikate.

11 Zugriff und Sicherheit

Verwalten Sie Ihr Passwort und Ihre MFA; Administratoren legen Konten mit eingeschränkten Rollen an und konfigurieren die Unternehmensanmeldung (SSO) der Organisation. Außerdem autorisieren sie die Geräte der Organisation für die mobile CERTYX-App und widerrufen verlorene Geräte. Administratoren können die Anmeldung bei der Organisation außerdem auf erlaubte Netzwerke (IP-Adressen und -Bereiche) beschränken. Diese Einstellungen sind Teil des umfassenderen Schutzes Ihrer Organisation: eigene Datenbank mit erzwungener Row-Level-Security, private Schlüssel, die in Ihrer Infrastruktur bleiben, für Ihre Organisation verschlüsselte Geheimnisse, Zugriff von Plattformbetreibern nur mit Freigabe Ihres Administrators oder über ein protokolliertes Break-Glass und ein hash-verkettetes Journal. Der Sicherheitsüberblick unter /de/security fasst sie zusammen. Administratoren stellen API-Tokens für Skripte, CI/CD-Pipelines und Integrationen aus, die die CERTYX-API aufrufen.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Kontomenü: Wählen Sie oben rechts Ihren Avatar und Namen. Das Profil zeigt Ihr Login, Ihre E-Mail-Adresse, Rolle, Organisation, Anmeldemethode und den MFA-Status; dort ändern Sie Ihr Passwort (das neue zweimal eingeben) und Ihre eigene E-Mail-Adresse, die zugleich Ihr Anmeldename ist – bestätigen Sie mit Ihrem aktuellen Passwort und, bei aktivierter MFA, mit einem MFA- oder Wiederherstellungscode. Beide Änderungen beenden alle Ihre Sitzungen. Abmelden beendet die aktuelle Sitzung.

2. Aktivieren Sie MFA, scannen Sie dann den QR-Code mit einer Authenticator-App oder geben Sie den Schlüssel von Hand ein. Prüfen Sie den Namen des Eintrags: CERTYX, gefolgt vom Host dieses Servers in Klammern, zum Beispiel CERTYX (certyx.example.com). Ein älterer Eintrag namens CLM, nur CERTYX oder mit einem anderen Host gehört zu einer anderen Umgebung oder einer früheren Einrichtung; seine Codes werden hier abgelehnt.
3. Bestätigen Sie mit dem aktuellen sechsstelligen Code. Zehn Wiederherstellungscodes werden einmalig angezeigt: Kopieren oder laden Sie sie herunter, bewahren Sie sie offline auf und melden Sie sich dann erneut an.
4. Wenn Sie den Authenticator verlieren, geben Sie bei der Anmeldung statt des MFA-Codes einen Wiederherstellungscode ein. Jeder Code funktioniert einmal; Wiederherstellungscodes zeigt, wie viele noch übrig sind. Neue Wiederherstellungscodes erzeugen (Passwort und aktueller MFA-Code) ersetzt alle früheren Codes.
5. Ein Administrator, der sich mit MFA angemeldet hat, kann MFA zurücksetzen für einen anderen Benutzer der Organisation verwenden, nachdem er die Identität dieser Person außerhalb des Systems bestätigt hat. Die Sitzungen des Benutzers werden beendet; er meldet sich mit dem Passwort an und aktiviert MFA erneut.
6. Auch der Bereich Passwort ändern dieser Ansicht ändert Ihr Passwort: Geben Sie das aktuelle und zweimal das neue Passwort ein; Ändern und abmelden beendet alle Ihre Sitzungen. Wiederholte fehlgeschlagene Anmeldungen sperren das Konto für 15 Minuten, und jeder weitere Fehlversuch nach Ablauf einer Sperre verdoppelt sie (standardmäßig bis zu 24 Stunden; die Werte legt der Betreiber fest). Eine Sitzung endet nach 30 Minuten oder nach 15 Minuten ohne Aktivität (Standardwerte). In der Produktion erfordern Administratorfunktionen eine mit MFA angemeldete Sitzung: Bis ein Administrator MFA aktiviert und sich erneut mit einem Code anmeldet, melden Administratoransichten, dass MFA erforderlich ist; Profil und MFA-Einrichtung bleiben verfügbar.
7. Benutzer und Rollen (Administrator): Benutzer erstellen nimmt E-Mail-Adresse, Benutzername, initiales Passwort und Rolle entgegen. Die Benutzerliste zeigt E-Mail-Adresse, Rolle und MFA-Status jedes Benutzers; E-Mail-Adresse ändern legt die Adresse fest, mit der sich der Benutzer anmeldet (in der Installation eindeutig), und beendet die Sitzungen dieses Benutzers.
8. Unternehmensanmeldung (mit MFA angemeldeter Administrator): Wählen Sie den Anbieter – Microsoft Entra ID, Okta, einen anderen OpenID-Connect-Anbieter oder SAML 2.0. Registrieren Sie für OpenID Connect die angezeigte Weiterleitungsadresse beim Anbieter und geben Sie Aussteller-Adresse, Client-ID und Geheimnis ein. Importieren Sie für SAML die Metadaten des Dienstanbieters beim Anbieter (oder geben Sie die Entity-ID und die Assertion-Consumer-Adresse ein) und geben Sie dann die SAML-Anmelde-URL, die Entity-ID und das Signaturzertifikat des Anbieters in CLM ein.
9. SAML-Optionen: Erzeugen Sie unter Dienstanbieter-Schlüssel (SAML) einen Schlüssel; angezeigt werden sein SHA-256-Fingerabdruck und seine Gültigkeit, der private Schlüssel verlässt den Server nie. Importieren Sie die Metadaten beim Anbieter erneut (sie enthalten nun das Signatur- und Verschlüsselungszertifikat und den Single-Logout-Dienst), aktivieren Sie dann Authentifizierungsanfragen signieren und Verschlüsselte Assertions verlangen, soweit der Anbieter dies unterstützt, und tragen Sie für Single Logout die Logout-URL des Anbieters ein. Zum Rotieren Nächsten Schlüssel vorbereiten wählen, den Anbieter die Metadaten erneut importieren lassen, dann Nächsten Schlüssel aktivieren; der bisherige Schlüssel entschlüsselt während der Überlappungszeit (standardmäßig 30 Tage) weiter, und Nächsten Schlüssel verwerfen entfernt einen vorbereiteten, nicht aktivierten Schlüssel. Die Abmeldung in der Konsole meldet dann auch beim Anbieter ab, und eine signierte Abmeldeanfrage des Anbieters beendet die CERTYX-Sitzungen des Benutzers.

10. Ordnen Sie Anbietergruppen Admin, Operator oder Auditor zu und speichern Sie. Fügen Sie eine E-Mail-Domain hinzu, veröffentlichen Sie den angezeigten TXT-Eintrag _certyx-verification und wählen Sie Verifizieren. Ab dann sehen Benutzer dieser Domain auf der Anmeldeseite die Schaltfläche für die Unternehmensanmeldung. Der vom Anbieter übermittelte Benutzername (preferred_username, email oder upn) muss zu einer verifizierten Domain oder einer ihrer Subdomains gehören, sobald die Organisation eine Domain verifiziert hat (vorher werden Namen akzeptiert und als nicht verifiziert protokolliert): Ein Name einer anderen Domain wird abgelehnt (die Anmeldeseite meldet, dass der Identitätsanbieter einen Benutzer mit nicht verifizierter E-Mail-Domain genannt hat; Journalgrund sso-unverified-domain), außer der Administrator wählt Benutzernamen außerhalb der verifizierten Domains akzeptieren; dann wird die Anmeldung mit dem Benutzer als nicht verifiziert protokolliert. Namen ohne Domain (ein Anmeldename) werden akzeptiert.
11. Erzeugen Sie optional ein SCIM-Token und tragen Sie es zusammen mit der SCIM-Adresse in den Bereitstellungseinstellungen des Anbieters ein: Dann können sich nur Benutzer anmelden, die im Verzeichnis bereitgestellt und aktiv sind, und das Deaktivieren eines Benutzers beendet seine Sitzungen. Der Anbieter kann auch Gruppen bereitstellen (SCIM Groups); Bereitgestellte Gruppen zeigt sie mit Mitgliederzahl und zugeordneter Rolle. Eine Gruppe wird wie eine Token-Gruppe über ihren Namen oder ihre externe ID zugeordnet. Nur Unternehmensanmeldung sperrt lediglich die lokalen Passwörter der Organisation. Eine SCIM-Gruppenänderung, die die Rolle eines Benutzers erhöht, wird als eigener Eintrag identity.scim.role-raised protokolliert, mit der Gruppe, ihrer zugeordneten Rolle und der Rolle jedes Benutzers vorher und nachher.
12. Die Firmenanmeldung (Microsoft Entra ID, Okta, anderes OpenID Connect, SAML 2.0) richtet ein Administrator im Bereich Unternehmensanmeldung (SSO) dieser Ansicht ein. Benutzer wählen dann auf der Anmeldeseite „Mit Firmenkonto anmelden“; sie startet, sobald ihre E-Mail-Adresse zu einer verifizierten Domain gehört.
13. Mobilgeräte (Administrator): Wählen Sie einen Benutzer (oder jeden Benutzer der Organisation) und optional eine Bezeichnung, dann „Aktivierungscode erzeugen“. Code und QR-Code werden einmal angezeigt und funktionieren einmal innerhalb der konfigurierten Gültigkeit (Clm:Mobile:EnrollmentCodeLifetime, standardmäßig 15 Minuten). Stammt das Zertifikat des Servers von einer eigenen (privaten) Zertifizierungsstelle der Organisation, konfiguriert der Betreiber dessen SHA-256-Fingerabdruck (Clm:Mobile:TrustedServerCertificates oder Clm:Mobile:TrustedServerCertificateFile); der QR-Code enthält ihn dann, das Panel zeigt ihn unter dem Code, und die App vertraut dieser Zertifizierungsstelle nur für diesen Server – scannen Sie in diesem Fall den QR-Code, statt den Code einzutippen. Installieren Sie CERTYX auf dem Gerät aus dem App-Store der Organisation (Custom App über Apple Business Manager oder private App in Managed Google Play), scannen Sie den QR-Code oder geben Sie den Code ein und melden Sie sich mit dem Konto des Benutzers (E-Mail, Passwort und, wenn das Konto MFA nutzt, dessen Code) oder der Firmenanmeldung an; die App bietet die Firmenanmeldung nur an, wenn die Organisation sie mit einer verifizierten Domain eingerichtet hat. In der App sieht der Benutzer Übersicht, Zertifikate, Warnungen, Freigaben, Agentenzustand und SSH-Zertifikate; Warnungen werden mit denselben Rollen wie in der Konsole bestätigt und Freigaben erteilt. „Freigegebene Geräte“ zeigt die beim Code vergebene Bezeichnung zusammen mit Namen und Modell, die das Telefon gemeldet hat. Wartende Codes können verworfen werden. „Zugriff widerrufen“ sperrt ein Gerät sofort: Die App wird bei ihrer nächsten Anfrage, noch vor der Anmeldung, abgelehnt und muss mit einem neuen Code erneut aktiviert werden. „Dieses Gerät entfernen“ in den Einstellungen der App widerruft das Gerät auch auf dem Server (die Liste zeigt dann „Auf dem Gerät entfernt“); hat das Telefon keine Verbindung, löscht die App ihre Daten trotzdem und weist darauf hin, dass ein Administrator das Gerät hier widerrufen muss.

14. API-Tokens (Administrator mit MFA angemeldet): Namen eingeben, Rolle wählen – Auditor liest, Operator fordert zusätzlich Erneuerungen, Bereitstellungen und Importe an – sowie die Gültigkeit in Tagen, dann Token erstellen. Der Token (cx_...) wird nur einmal angezeigt: Kopieren Sie ihn in Ihren Secret-Manager und senden Sie ihn als Header Authorization: Bearer <Token> an die CERTYX-API (/api/...); Cookie oder CSRF-Token sind nicht nötig. Die Liste zeigt Rolle, wer den Token wann erstellt hat, Ablauf, letzte Verwendung und Zustand (aktiv, abgelaufen, widerrufen); Widerrufen sperrt ihn sofort.
15. E-Mail zur Einrichtung des Authenticators (Administration): Benutzer anlegen fragt auch nach der E-Mail-Sprache (English, Deutsch oder Polski; die Konsolensprache ist vorausgewählt). Die neue Person erhält dann über das SMTP-Relay der Organisation (Benachrichtigungsgruppen → Zustellung) eine E-Mail mit einem einmaligen Link zur Einrichtung einer Authenticator-App. Die E-Mail enthält den Link als Text und als QR-Code, der ihn auf dem Telefon öffnet, nie das Geheimnis der App oder das Passwort; geben Sie das Anfangspasswort getrennt weiter. Ohne eingeschaltetes Relay oder wenn das Senden fehlschlägt, zeigt der Bereich den Grund und den Link zum Kopieren: Geben Sie ihn über einen vertrauenswürdigen Kanal weiter. Die Benutzerliste zeigt „Einrichtungslink gültig bis ...“, solange ein Link offen ist; Einrichtungs-E-Mail senden erstellt einen neuen Link (der vorherige funktioniert nicht mehr) für eine aktivierte Person mit E-Mail-Adresse und ohne MFA.
16. Einrichtungsseite: Die Person öffnet den Link, gibt das Kontopasswort ein, scannt den QR-Code (oder tippt den Schlüssel ab; der Eintrag heißt CERTYX mit dem Host dieses Servers in Klammern), bestätigt mit dem aktuellen sechsstelligen Code und bewahrt die einmalig angezeigten zehn Wiederherstellungscodes auf; ihre Sitzungen enden und jede weitere Anmeldung verlangt den Code.
17. Erlaubte Anmeldenetzwerke (Administrator mit MFA angemeldet): Geben Sie die Adressen und Bereiche ein, von denen sich Ihre Benutzer verbinden, eine pro Zeile – eine einzelne Adresse (203.0.113.7, 2001:db8::7) oder einen CIDR-Bereich, der mit seiner ersten Adresse beginnt (203.0.113.0/24, 2001:db8::/48) – und wählen Sie Anmeldenetzwerke speichern. Das Panel zeigt die Adresse, von der Sie verbunden sind, und ob die Liste sie enthält. Enthält sie sie nicht, wird das Speichern mit einer Warnung abgelehnt: Stellen Sie sicher, dass Sie sich aus einem erlaubten Netzwerk verbinden können, setzen Sie die Bestätigung, geben Sie Ihren aktuellen Authenticator-Code ein und speichern Sie erneut. Danach wird jede Passwort- und Unternehmensanmeldung, jede Geräteaktivierung und Anmeldung in der Mobil-App und jede Anfrage einer Browsersitzung gegen die Liste geprüft; eine Sitzung von einer Adresse außerhalb endet bei ihrer nächsten Anfrage. Leeren Sie die Liste und speichern Sie, um die Einschränkung aufzuheben.
18. Mobil-App und Anmeldenetzwerke: Standardmäßig (Auch jede Anfrage angemeldeter Mobil-Apps prüfen aus) müssen die Aktivierung eines Geräts und jede Anmeldung in der App aus einem erlaubten Netzwerk kommen, und eine bereits angemeldete App funktioniert aus jedem Netzwerk weiter, bis ihre Sitzung endet (Clm:Mobile:SessionLifetime, standardmäßig 30 Minuten) – zum Beispiel im Mobilfunknetz. Schalten Sie die Option ein, um auch jede Anfrage der App zu prüfen; die App funktioniert dann nur in erlaubten Netzwerken, zum Beispiel über Ihr VPN.
19. Anfragen des Plattformbetreibers (Admin mit MFA angemeldet): CERTYX-Plattformbetreiber können in Ihrer Organisation keine Konten anlegen, Rollen erhöhen, Konten wieder aktivieren oder MFA zurücksetzen, solange sie einen aktivierten Admin hat. Eine solche Änderung steht hier mit angefragter Änderung, Zeit und Status, bis ein Admin sie freigibt (sie wird sofort ausgeführt; konnte das Plattform-Relay die Einrichtungs-E-Mail eines neuen Kontos nicht senden, wird Ihnen der einmalige Link angezeigt) oder ablehnt; sie läuft standardmäßig nach 72 Stunden ab. Ein Break-Glass durch zwei verschiedene Betreiber wird mit seinem Grund angezeigt; jeder Admin erhält eine E-Mail, und

gewährter Zugriff endet standardmäßig nach 24 Stunden, sofern Sie das Konto nicht ändern. Aktivität des Plattformbetreibers zeigt die letzten Änderungen der Betreiber an Ihrer Organisation aus ihrem Sicherheitsjournal (auch an Ihre SIEM-Ziele gesendet).

20. Passkeys (lokale Konten mit aktivierter MFA): Geben Sie einen Namen und Ihren aktuellen Authenticator-Code ein, wählen Sie Passkey hinzufügen und folgen Sie der Abfrage Ihres Browsers (Gerät, Telefon oder Sicherheitsschlüssel). Danach nimmt Mit Passkey anmelden auf der Anmeldeseite Ihr Passwort und den Passkey statt des Codes, und jedes Codefeld sowie der Bestätigungsdialog des Kontrollraums bieten Mit Passkey bestätigen an. Die Richtlinie legt fest, was der zweite Faktor sein darf: Authenticator-Code oder Passkey (Standard), nur Passkey (Codes werden abgelehnt; braucht einen Passkey) oder nur Authenticator-Code. Wiederherstellungscodes funktionieren mit jeder Richtlinie. Passkey entfernen nimmt den Passkey und einen Code; nach dem Entfernen des letzten gilt wieder Code oder Passkey.
21. Ihre Sitzungen: alle Browser- und Mobile-App-Sitzungen Ihres Kontos mit Client, Beginn, letzter Aktivität, Adresse und Status, die aktuelle markiert. Sitzung beenden meldet diese Sitzung bei ihrer nächsten Anfrage ab; Alle anderen Sitzungen beenden behält nur diese. Organisationsadministratoren sehen zusätzlich Sitzungen der Organisation (alle Benutzer, bei mobilen Sitzungen mit Gerätebezeichnung) und können jede beenden; jedes Beenden wird im Sicherheitsjournal erfasst.

EINGABEN UND PARAMETER

- TOTP: 6 Ziffern, SHA-1, 30-Sekunden-Intervall; bestätigen Sie die Einrichtung innerhalb von 10 Minuten, sonst starten Sie MFA aktivieren erneut.
- Wiederherstellungscode: 16 Zeichen in vier Gruppen (Buchstaben und Ziffern); Groß-/Kleinschreibung, Leerzeichen und Bindestriche werden ignoriert.
- Passwort: 16–256 Zeichen. Benutzername: bis zu 120 Zeichen.
- Auditor liest; Operator verwaltet Inventar und Pläne; Admin verwaltet Richtlinien und Genehmigungen.
- Entra: Aussteller https://login.microsoftonline.com/<directory ID>/v2.0 (ein Verzeichnis). OpenID Connect: eine HTTPS-Adresse ohne Query. SAML: die HTTPS-Anmeldeadresse (HTTP-Redirect-Binding), die Entity-ID des Anbieters und sein Signaturzertifikat in PEM oder Base64 (nicht abgelaufen, RSA- oder ECDSA-Schlüssel).
- SAML-Single-Logout-URL: die HTTPS-Adresse des SingleLogoutService des Anbieters (HTTP-Redirect). SCIM-Gruppen: Anzeigename eindeutig pro Organisation (bis 256 Zeichen), Mitglieder müssen bereits per SCIM bereitgestellte Benutzer sein; Filter displayName, externalId oder id eq "Wert".
- Gruppenzuordnung: eine Zeile "group = role", bis zu 100 Zeilen. Domains: bis zu 20 pro Organisation; eine von einer anderen Organisation verifizierte Domain kann nicht beansprucht werden.
- Mobiler Aktivierungscode: 16 Zeichen in vier Gruppen; einmal verwendbar; eine Benutzerbindung beschränkt die Anmeldung auf diesem Gerät auf den gewählten Benutzer.
- Einrichtungslink: gültig für Clm:Identity:MfaSetupLinkLifetime (Standard 24 Stunden), funktioniert einmal, verlangt das Kontopasswort; ein neuerer Link, eine Passwortänderung oder aktiviertes MFA machen ihn ungültig. Ein neuer Link für dieselbe Person höchstens einmal pro Clm:Identity:MfaSetupResendInterval (Standard 1 Minute).
- Erlaubte Anmeldenetzwerke: IPv4 in Punktschreibweise (vier Teile, keine führenden Nullen) oder IPv6, optional mit Präfixlänge (/0–/32, /0–/128); die Adresse muss die erste ihres Bereichs sein (203.0.113.0/24, nicht 203.0.113.5/24); ein IPv4-gemappter IPv6-Eintrag (::ffff:203.0.113.0/120) wird als

sein IPv4-Bereich gespeichert. Einträge dürfen auch durch Kommas oder Leerzeichen getrennt sein; Duplikate werden entfernt. Höchstens Clm:Identity:MaximumSignInNetworks Einträge (standardmäßig 100).

- Anmelderegeln der Unternehmensanmeldung: Benutzernamen außerhalb der verifizierten Domains akzeptieren ist standardmäßig aus (ablehnen); eingeschaltet werden solche Namen akzeptiert und als nicht verifiziert protokolliert.
- Passkey: ein Name (bis 64 Zeichen) und der aktuelle Authenticator-Code; die Richtlinie: Authenticator-Code oder Passkey, nur Passkey oder nur Authenticator-Code.
- API-Token: Name bis 80 Zeichen; Rolle Auditor oder Operator; Gültigkeit 1 Tag bis Clm:Identity:ApiTokens:MaximumLifetimeDays (Standard 365, vorgeschlagen 90); höchstens Clm:Identity:ApiTokens:MaximumPerOrganization aktive Tokens (Standard 25).

ERGEBNIS

Das Aktivieren von MFA, eine Passwortänderung und ein MFA-Reset beenden die Sitzungen des Kontos. Wiederherstellungscodes werden nur als Hashes gespeichert; Verwendung, Neuerzeugung und Zurücksetzen werden im Sicherheitsjournal erfasst. Rollen werden von der API durchgesetzt, unabhängig von der Sichtbarkeit von Schaltflächen. Die Unternehmensanmeldung erstellt eine Sitzung mit der Rolle der am höchsten berechtigten zugeordneten Gruppe; sie wird abgelehnt ohne zugeordnete Gruppe, ohne MFA, wenn diese erforderlich ist, aus einem anderen Entra-Verzeichnis, bei zu vielen Gruppen für das Token sowie bei SCIM für einen nicht bereitgestellten oder deaktivierten Benutzer. Jede Änderung der Einstellungen beendet bestehende Sitzungen der Unternehmensanmeldung. Eine SAML-Antwort wird nur akzeptiert, wenn sie mit dem hinterlegten Zertifikat signiert ist, für die richtige Zielgruppe und den richtigen Aussteller gilt, innerhalb ihrer Gültigkeit liegt und die Antwort auf eine im selben Browser gestartete Anfrage ist; die Wiederverwendung derselben Antwort wird abgelehnt. Mit SCIM-Gruppen ist die Rolle die höchste, die aus Token-Gruppen und SCIM-Gruppen zusammen zugeordnet wird; eine Mitgliedschaftsänderung, Umbenennung oder Löschung, die die effektive Rolle eines Benutzers ändert, beendet dessen Sitzungen bei der nächsten Anfrage, und jede Änderung wird mit den Benutzern protokolliert, deren Rolle sich geändert hat. Mit Verschlüsselte Assertions verlangen wird eine unverschlüsselte Assertion abgelehnt; verschlüsselte Assertions müssen AES-GCM oder AES-CBC mit RSA-OAEP-Schlüsseltransport verwenden (RSA PKCS#1 v1.5 wird abgelehnt). Mit Authentifizierungsanfragen signieren wird jeder AuthnRequest mit RSA-SHA256 signiert. Single Logout: Die Abmeldung in der Konsole beendet die Sitzung sofort auf jeder Instanz und sendet dann eine signierte Abmeldeanfrage an den Anbieter; eine signierte, aktuelle Abmeldeanfrage des Anbieters (geprüft gegen das hinterlegte Zertifikat, Aussteller und Ziel, bei Wiederholung abgelehnt) beendet die Sitzungen des Benutzers auf jeder Instanz und wird mit einer signierten Abmeldeantwort beantwortet. Mobilgeräte: Jede Anfrage der App, auch die Anmeldung, wird mit einem Schlüssel signiert, der das Gerät nicht verlässt, und gegen das autorisierte Gerät geprüft – ein Widerruf wirkt daher sofort; Codes werden nur als Hashes gespeichert, und Codeerzeugung, Geräteautorisierung und Widerruf werden im Sicherheitsprotokoll erfasst. Senden, Verwenden und ein abgelaufener Link werden ohne den Link im Sicherheitsjournal erfasst (mfa-setup.mail.sent, .used, .expired) und erreichen den SIEM-Export der Organisation. Personen mit Firmenanmeldung (SSO und SCIM) erhalten keine Einrichtungs-E-Mail; bei Nur Firmenanmeldung wird keine gesendet, weil der Identitätsanbieter MFA erzwingt. Erlaubte Anmeldenetzwerke: Jede Änderung (vorher und nachher, Akteur) und jede abgelehnte Änderung wird im Sicherheitsjournal protokolliert (identity.signin-networks.changed, .refused); jede abgelehnte Anmeldung, Geräteaktivierung oder App-Anfrage von außerhalb der Liste ist ein Anmeldeereignis mit dem Grund network-not-allowed, der Quelladresse und, soweit bekannt, dem Benutzer im Journal und SIEM-Export der Organisation, und eine so beendete Sitzung ist eine Abmeldung mit diesem Grund. Anmeldeseite und App teilen dem Benutzer mit,

dass sein Netzwerk nicht erlaubt ist, ohne die Liste preiszugeben. API-Tokens werden nur als SHA-256-Hashes gespeichert; Erstellung, Widerruf und abgelehnte Verwendungen (etwa von außerhalb der Anmeldenetze) werden im Sicherheitsjournal erfasst und wie andere Identitätsereignisse an das SIEM exportiert; die Liste zeigt die letzte Verwendung.

BERECHTIGUNGEN

Eigenes Konto: angemeldeter lokaler Benutzer. Kontoerstellung und MFA-Reset: Admin; der Reset erfordert zusätzlich die eigene MFA-Anmeldung des Administrators und kann nicht auf das eigene Konto angewendet werden. Plattformadministratoren setzen die MFA von Kundenkonten in der Plattformverwaltung zurück. SSO-Konten verwalten Passwort/MFA beim Identitätsanbieter. Unternehmensanmeldung, Domains und SCIM-Token: mit MFA angemeldeter Admin; sie gelten nur für die Organisation dieses Administrators. Dienstanbieter-Schlüssel (erzeugen, aktivieren, verwerfen) erfordern ebenfalls einen mit MFA angemeldeten Admin; die Liste der SCIM-Gruppen ist für Admins schreibgeschützt. Eigenes Passwort und eigene E-Mail-Adresse ändern: jeder angemeldete lokale Benutzer für sein eigenes Konto; eine fehlgeschlagene Bestätigung zählt zur Kontosperrung. Mobilgeräte: Admin der Organisation; Codeerzeugung und Widerruf erfordern die eigene MFA-Anmeldung des Administrators. Die App ist nur für Kundenbenutzer; Plattformbetreiber können sich darin nicht anmelden. Erlaubte Anmeldenetzwerke: Admin der Organisation; das Speichern erfordert die eigene MFA-Anmeldung des Administrators, und eine Liste ohne die aktuelle Adresse des Administrators zusätzlich einen aktuellen Authenticator-Code eines lokalen Kontos (über die Unternehmensanmeldung angemeldete Administratoren müssen ihre eigene Adresse in der Liste behalten). Anfragen des Plattformbetreibers: nur Admins dieser Organisation; Freigeben und Ablehnen erfordern die eigene MFA-Anmeldung des Admins. Passkeys und die eigene Sitzungsliste: jeder angemeldete lokale Benutzer mit MFA für sein eigenes Konto (Sitzungen auch Benutzer der Firmenanmeldung). Sitzungen der Organisation: Organisations-Admin. API-Tokens: Erstellen und Widerrufen erfordert einen im Browser mit MFA angemeldeten Admin; ein Token selbst handelt nur als Auditor oder Operator in seiner Organisation und wird von jedem Administrator-Endpunkt abgelehnt (Genehmigungen, Einstellungen, Benutzer, Geräte, Tokens), sodass Vier-Augen-Genehmigungen bei Menschen bleiben.

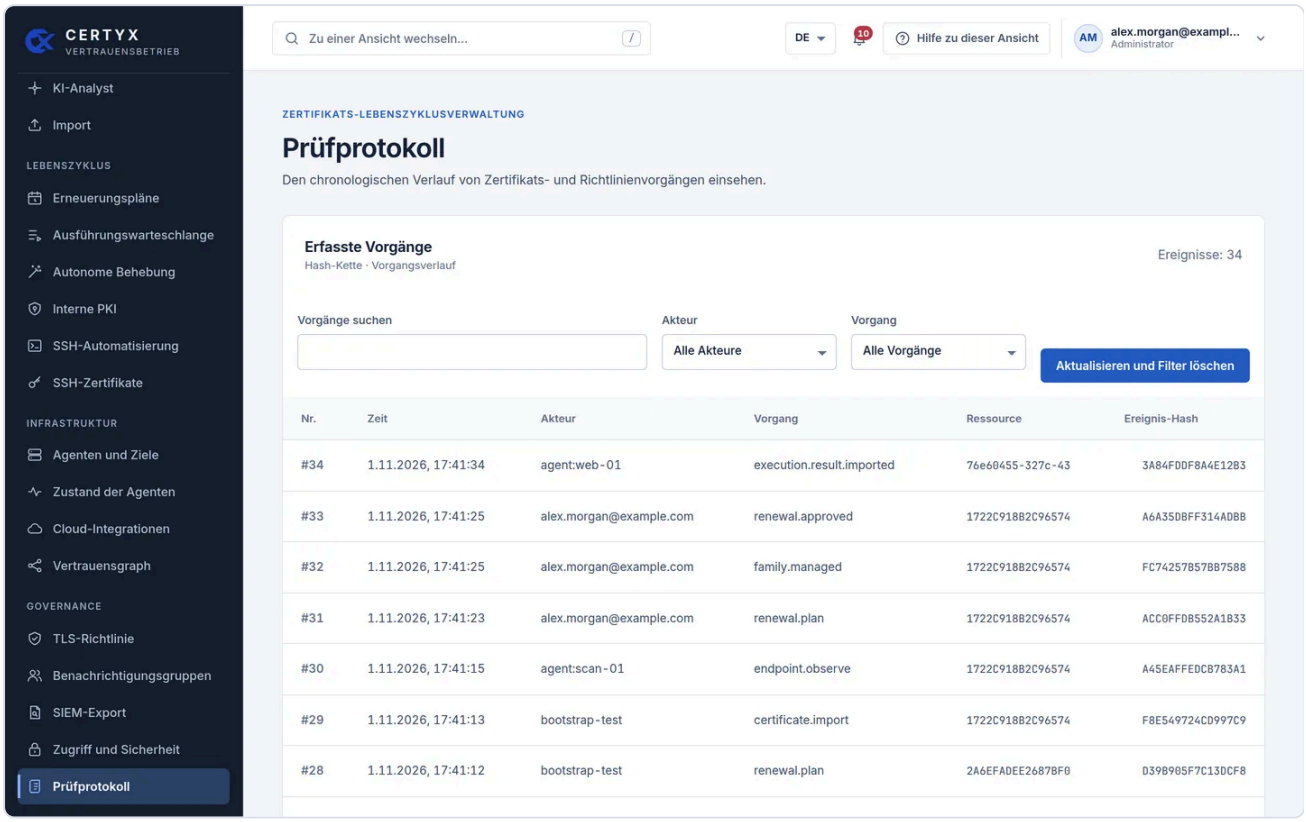
EINSCHRÄNKUNGEN

Keine Selbstregistrierung. Eine Konsolensitzung endet nach Clm:Identity:SessionLifetime (Standard 30 Minuten) unabhängig von der Aktivität, eine Sitzung der mobilen App ebenso nach Clm:Mobile:SessionLifetime (Standard 30 Minuten); danach melden Sie sich erneut an. Sitzungen enden außerdem durch Abmelden, Passwort-, E-Mail- oder MFA-Änderungen, einen MFA-Reset oder den Widerruf eines Mobilgeräts. Die Sitzungslisten brauchen die Plattformdatenbank; ohne sie melden sie, dass Sitzungen nicht erfasst werden. Passkeys brauchen die Relying Party der Installation (Clm:Identity:Passkeys) und einen Browser mit WebAuthn auf der https-Adresse der Konsole; ein Passkey gilt nur für die Adresse, auf der er registriert wurde. Mobile Sitzungen, die vor dieser Version begonnen haben, erscheinen nicht. Ein Administrator, der sowohl den Authenticator als auch alle Wiederherstellungscodes verloren hat, benötigt einen anderen Administrator der Organisation; ein Plattformadministrator in dieser Situation wird offline von zwei Personen mit tools/Clm.OperatorBootstrap reset-mfa wiederhergestellt, während der Dienst gestoppt ist. Konten, die vor Einführung der Wiederherstellungscodes angelegt wurden, erhalten diese über Neue Wiederherstellungscodes erzeugen. Mit der Plattformdatenbank werden Konten, MFA-Status und Datenschutzschlüssel von allen Anwendungsinstanzen gemeinsam genutzt; ohne sie verbleiben sie im lokalen Datenverzeichnis einer einzelnen Instanz. Geben Sie Ihr TOTP-Geheimnis, Ihre Wiederherstellungscodes oder Ihr Passwort niemals weiter. Kundenzugangsdaten und private Schlüssel bleiben unter Kontrolle des Kunden. Agenten lesen Kunden-Secrets aus geschützten Dateien, HashiCorp Vault KV, Azure Key Vault, AWS Secrets Manager und

Google Secret Manager; andere Tresorprodukte werden nicht unterstützt, und Agenten versenden keine E-Mails vom Kundenhost. Unter Windows werden geschützte Dateien nur akzeptiert, wenn LocalSystem, Administrators oder die eigene Identität des Agenten Eigentümer sind und darauf zugreifen. Die Berechtigungen des Unix-Vault-Tokens werden bei jeder Verwendung erneut geprüft. Unternehmensanmeldung: Die Organisation der Plattformbetreiber behält immer die lokale Notfallanmeldung (Break-Glass) und kann Nur Unternehmensanmeldung nicht aktivieren. SAML: Fügen Sie das neue Signaturzertifikat des Anbieters ein, bevor er seinen Schlüssel rotiert. Signierte Anfragen, verlangte Verschlüsselung und Single Logout erfordern einen Dienstanbieter-Schlüssel, Single Logout zusätzlich die Logout-URL des Anbieters; ein vorbereiteter nächster Schlüssel muss vor der Aktivierung beim Anbieter importiert sein, sonst lehnt dieser signierte Anfragen ab. Bestätigt der Anbieter eine Abmeldung aus der Konsole nicht, ist die CERTYX-Sitzung trotzdem beendet und die Anmeldeseite weist darauf hin. Verschachtelte SCIM-Gruppen werden nicht unterstützt (Mitglieder sind nur Benutzer), und SCIM-Bulk-Operationen werden nicht angeboten. SAML erfordert HTTPS, da das Anfrage-Cookie als Secure markiert ist. Eine Entra-Gruppenüberschreitung (Group Overage) wird abgelehnt – beschränken Sie das Token auf die der Anwendung zugewiesenen Gruppen. Mobilgeräte erfordern die Plattformdatenbank; ohne sie weist der Bereich darauf hin. Push-Benachrichtigungen werden nur gesendet, wenn der Dienstbetreiber Firebase Cloud Messaging eingerichtet hat; sie enthalten nie Zertifikatsnamen. Erlaubte Anmeldenetzwerke benötigen die Plattformdatenbank; ohne sie meldet das Panel dies und die Anmeldung ist nicht eingeschränkt. Die Client-Adresse ist die Adresse der Verbindung oder mit Clm:Ingress:TrustedProxies die vom vertrauenswürdigen Proxy weitergegebene Adresse (X-Forwarded-For von jedem anderen Absender wird ignoriert); Benutzer hinter einem gemeinsamen NAT oder Proxy teilen dessen öffentliche Adresse. Agenten (gegenseitiges TLS) und SCIM-Provisioning-Token sind keine Benutzeranmeldung und werden nicht geprüft. Sind alle Administratoren ausgesperrt, kann ein Plattform-Operator die Einschränkung aufheben (Kundenkarte → Zugriff); diese Aufhebung erscheint im Sicherheitsjournal und SIEM-Export dieser Organisation. Eine Anfrage kann nur entschieden werden, solange sie offen ist und in der angezeigten Version; eine freigegebene Kontoänderung wird nicht ausgeführt, wenn das Konto nach der Anfrage geändert wurde, der Name vergeben ist oder das Limit aktiver Konten aus dem Vertrag erreicht ist (die Anfrage zeigt dann Nicht ausgeführt). Aktivität des Plattformbetreibers zeigt die neuesten 50 Einträge ohne Vorher/Nachher-Details; Lesezugriffe der Betreiber werden nicht aufgeführt. MFA wird durch die Richtlinie unseres Anbieters erzwungen lässt jede Unternehmensanmeldung als MFA zählen, ohne dass der Anbieter sie meldet: Das Panel zeigt eine Warnung, solange die Option gewählt ist, und jedes Speichern damit wird als identity.sso.mfa-delegated protokolliert. Das Anlegen eines Kontos oder das Zuweisen einer bereits verwendeten E-Mail-Adresse, in dieser oder einer anderen Organisation, wird mit derselben Meldung abgelehnt; nur das Plattformjournal hält den tatsächlichen Grund fest (account.create-refused, account.email-refused), sodass Administratoren nicht erfahren, ob eine Adresse anderswo existiert. API-Tokens erfordern die Plattformdatenbank; ohne sie meldet das Panel, dass sie nicht verfügbar sind. Jeder Token läuft ab und kann nicht verlängert werden – erstellen Sie einen neuen und widerrufen Sie den alten. Ein Token unterliegt der Liste der Anmeldenetze der Organisation (außerhalb 403 network-not-allowed). Anfragen mit unbekanntem, fehlerhaftem, widerrufenem oder abgelaufenem Token erhalten 401 invalid-token und greifen nie auf eine Browsersitzung zurück.

12 Prüfprotokoll

Den chronologischen Verlauf von Zertifikats- und Richtlinienvorgängen einsehen.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Öffnen Sie den Arbeitsbereich nach der Anmeldung.
2. Durchsuchen Sie Vorgänge, filtern Sie nach Akteur oder Vorgang und blättern Sie seitenweise mit 50 Vorgängen pro Seite, neueste zuerst; das Blättern bleibt auf demselben Stand, bis Aktualisieren und Filter löschen die neuesten Vorgänge lädt. Prüfen Sie Sequenz, Zeitstempel, Akteur, Vorgang und Ressourcenkennung.
3. Vergleichen Sie Ereignisse mit Plänen, Richtlinienänderungen oder Endpunktbeobachtungen.
4. CSV exportieren oder JSON exportieren lädt alle Vorgänge herunter, die der aktuellen Suche und den Filtern entsprechen, neueste zuerst, mit den Verknüpfungen der Hash-Kette; jeder Export wird im Sicherheitsjournal erfasst. Export und Aufbewahrung zeigt die geltende Aufbewahrung, Anzahl und Zeitraum der erfassten Vorgänge und das Exportlimit.
5. Der Betreiber kann zusätzlich signierte Inventar-Audit-Prüfpunkte mit tools/Clm.Backup anchor --tenant <Organisations-ID>, einem geschützten Signaturschlüssel und einer Datenbankidentität ohne RLS-Umgehung exportieren. verify-anchors --tenant prüft die organisationsgebundene Signatur, das Segment und die Kette; --db-env vergleicht zusätzlich die laufende Datenbank. Schlüssel und unveränderliche Kopien müssen vom Datenbankhost unabhängig bleiben.

EINGABEN UND PARAMETER

- Der Server erstellt Ereignisse bei Änderungen; dieser Arbeitsbereich kann sie nicht bearbeiten.

- Sequenz und Hashes verknüpfen aufeinanderfolgende Ereignisse. Zeiten verwenden die lokale Zeitzone des Browsers.
- Der Server prüft die gesamte Hashkette bei jeder Änderung des neuesten Ereignisses und mindestens alle 5 Minuten und verweigert Inventarzugriffe bei inkonsistenter Kette.

ERGEBNIS

Der Verlauf hilft nachzuvollziehen, wer Daten wann geändert hat. Die Validierung der Hash-Kette erkennt inkonsistent gespeicherten Verlauf.

BERECHTIGUNGEN

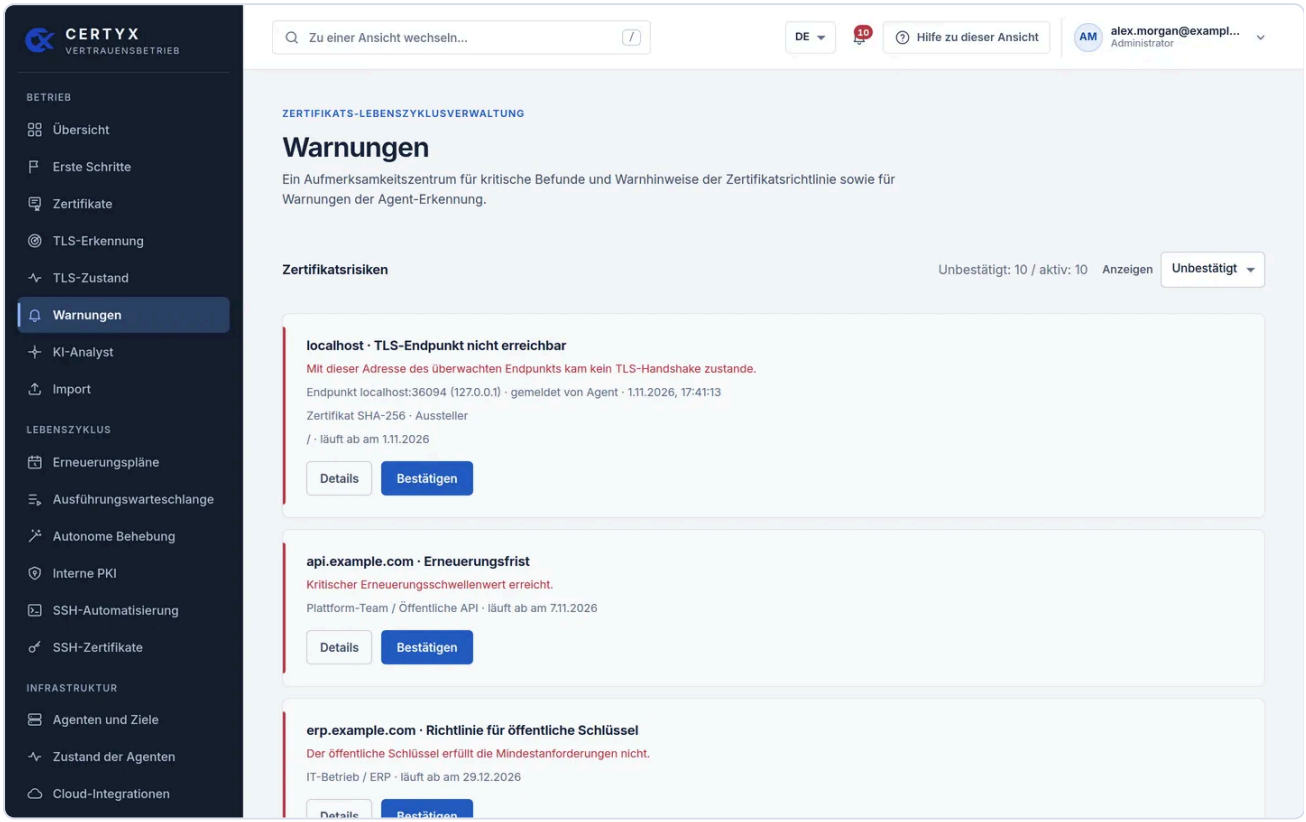
Alle angemeldeten Rollen sehen und exportieren.

EINSCHRÄNKUNGEN

Die Hashkette in der Datenbank allein beweist keine Nichtabstreitbarkeit gegenüber einem Datenbankadministrator. Eine direkt in der Datenbank vorgenommene Änderung eines früheren Ereignisses wird bei der nächsten vollständigen Prüfung erkannt (spätestens nach 5 Minuten). Unabhängige signierte Prüfpunkte erkennen Änderungen bereits verankerter Historie; gegen Löschung sind externe unveränderliche Aufbewahrung und unabhängige Prüfung erforderlich. Aufbewahrung: Vorgänge bleiben für die Lebensdauer der Organisation ohne automatisches Löschen erhalten, und die Anwendungsrolle kann sie nur hinzufügen und lesen. Eine konfigurierbare Aufbewahrungsfrist wird nicht angeboten, da das Löschen von Einträgen die Hash-Kette unterbrechen würde. Ein Export enthält höchstens Clm:AuditExport:MaxRows Vorgänge (Standard 100.000); schränken Sie bei größeren Ansichten die Filter ein.

13 Warnungen

Ein Aufmerksamkeitszentrum für kritische Befunde und Warnhinweise der Zertifikatsrichtlinie sowie für Warnungen der Agent-Erkennung.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Prüfen Sie unbestätigte Warnungen, sortiert nach Schweregrad und Ablauf.
2. Details öffnet das Zertifikat im Inventar, wo Fakten, Befunde, Verantwortung und Erneuerung die Nachweise hinter der Warnung zeigen. Jede Karte zeigt bereits den Befund, seine Erklärung, Verantwortlichen und Dienst, den Ablauf und nach einer Bestätigung, wer sie wann bestätigt hat.
3. Wählen Sie Bestätigen. Wählen Sie Alle aktiven Risiken, um bestätigte Risiken einzubeziehen.
4. Benachrichtigungs-Outbox und Verlauf darunter listet die neuesten 100 Benachrichtigungen der Organisation (Warnungen für Outbox-Kanäle, Gruppen-E-Mails und mobile Push-Nachrichten) mit Kanal, Status, Versuchen, Zustellzeit und letztem Fehlergrund; E-Mail-Vorschau öffnet eine eingereihte Gruppen-E-Mail so, wie sie gesendet wird.
5. Jeder Eintrag nennt seinen Ereignistyp (Zertifikatswarnung, eskalierte Warnung, Auftrags- und Erneuerungsereignisse). Ein Administrator wählt Erneut senden bei einem zugestellten, aufgegebenen oder abgebrochenen Kanaleintrag, um ihn noch einmal zuzustellen (Versuche zurückgesetzt, im Sicherheitsjournal erfasst); Gruppen-E-Mails und Mobile-Push-Einträge können nicht erneut gesendet werden, und das erneute Senden eines PagerDuty-Triggers öffnet den Vorfall wieder.
6. Ist der KI-Analyst für die Organisation aktiviert, öffnet Erklären ihn mit einer Frage zur Warnung.

EINGABEN UND PARAMETER

- Warnungen stammen aus aktuellen Richtlinienbewertungen: Gültigkeit, Erneuerungsschwellenwerte, öffentliche Schlüssel oder Signaturen.
- Die Identität umfasst Zertifikat, Richtlinienversion, Befundcode und Schweregrad. Eine Änderung der Richtlinie oder des Schweregrads erfordert eine neue Bestätigung.
- Die Agent-Erkennung löst nach der Ausgangsbasis des Profils (seinem ersten vollständigen Durchlauf) Warnungen aus: Unbekanntes Zertifikat gefunden (Warnhinweis; kritisch, wenn selbstsigniert oder von einem in der Organisation nie gesehenen Aussteller), Zertifikat am Endpunkt ersetzt (Warnhinweis; nicht ausgelöst, wenn ein CERTYX-Ausführungsauftrag genau dieses Zertifikat innerhalb von Clm:Discovery:ReplacementSuppressionWindow, standardmäßig 7 Tage, auf diesen Endpunkt oder anstelle des vorherigen bereitgestellt hat) und Neuer TLS-Endpunkt (Information). Diese Karten zeigen den Endpunkt, den meldenden Agent sowie SHA-256-Fingerabdruck und Aussteller des neuen und des vorherigen Zertifikats. Sie entstehen einmal pro Endpunkt und Zertifikat, werden protokolliert und wie andere offene Warnungen über die konfigurierten Benachrichtigungskanäle gesendet.

ERGEBNIS

Die Bestätigung ist dauerhaft, idempotent und wird mit Identität und Zeitstempel protokolliert. Sie verändert das Zertifikat nicht und behebt das Risiko nicht.

BERECHTIGUNGEN

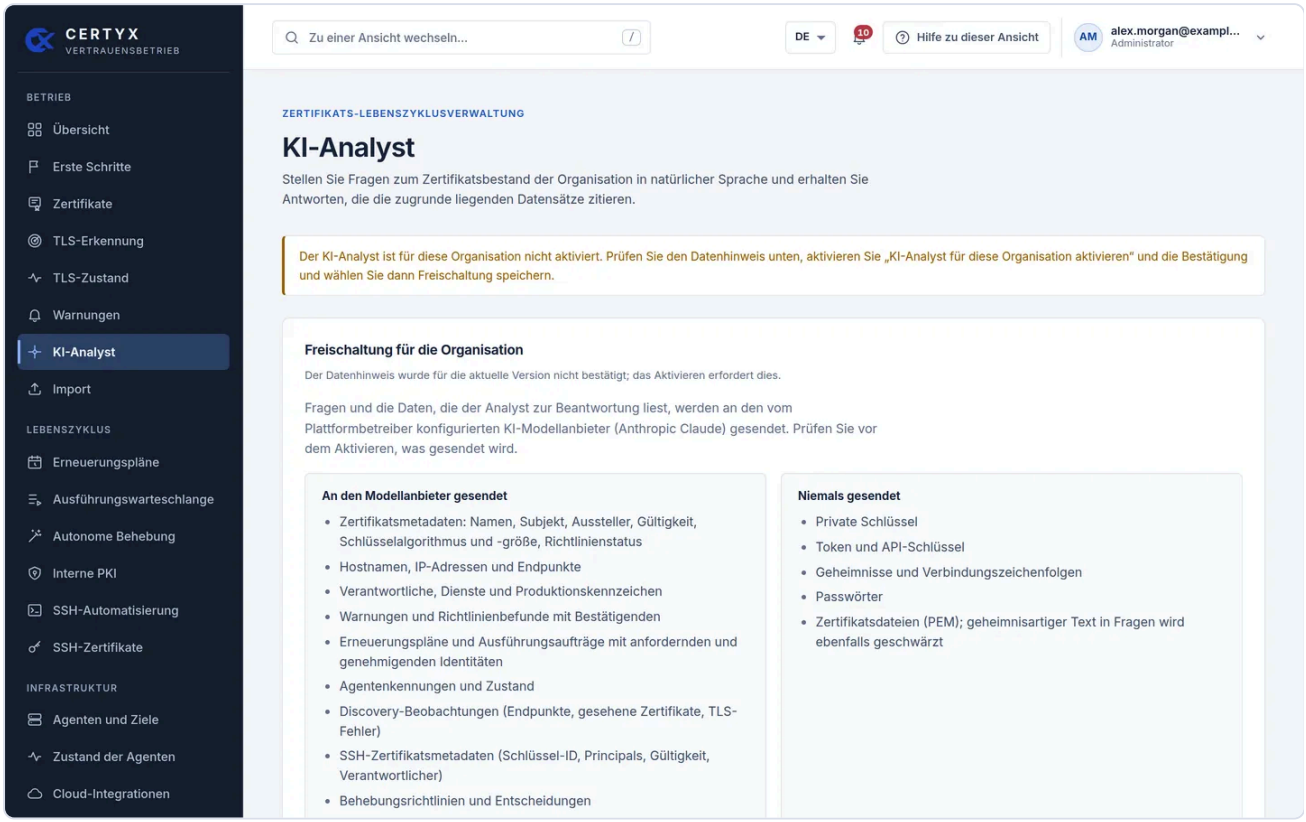
Lesen: alle angemeldeten Rollen. Bestätigen: Operator oder Admin.

EINSCHRÄNKUNGEN

Eine Bestätigung beseitigt das Risiko nicht. Offene Warnungen werden für jeden aktivierten Outbox-Kanal der Organisation (Webhook, Microsoft Teams, Slack, PagerDuty) eingereiht und mindestens einmal zugestellt; Eskalationskanäle erhalten nur kritische Warnungen, die nach ihrer Verzögerung noch unbestätigt sind. Kanäle und das SMTP-Relay werden unter Benachrichtigungsgruppen → Zustellung eingerichtet, wo jeweils wartende und fehlgeschlagene Nachrichten angezeigt werden. Hat der Dienstbetreiber Push-Benachrichtigungen eingerichtet, erreichen offene kritische und Ablaufwarnungen auch die autorisierten Mobilgeräte der Organisation mit eingeschalteten Benachrichtigungen, als allgemeine Nachricht ohne Zertifikatsnamen. Die Liste zeigt die neuesten 100 Benachrichtigungen. Eine Erkennungswarnung bleibt nach der Bestätigung gelistet; weisen Sie dem Zertifikat einen Verantwortlichen zu oder untersuchen Sie den Endpunkt. Ein Austausch durch ein anderes Werkzeug oder eine CERTYX-Bereitstellung, deren Prüfendpunkt von der beobachteten Adresse abweicht, wird gemeldet.

14 KI-Analyst

Stellen Sie Fragen zum Zertifikatsbestand der Organisation in natürlicher Sprache und erhalten Sie Antworten, die die zugrunde liegenden Datensätze zitieren.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Voraussetzungen: Das Abonnement enthält AI_ANALYST; der Plattformbetreiber verbindet den Analysten in der Kontrollraum-Ansicht KI-Analyst: Anbieter (Anthropic-API-Schlüssel, Modell, Verbindung testen, „KI-Analyst den Organisationen anbieten“) – in einer eigenständigen Installation ohne Plattformdatenbank setzt der Betreiber CIm:Analyst in der Konfiguration –; und ein Admin der Organisation schaltet ihn hier nach Lesen und Bestätigen des Datenhinweises frei. „Freischaltung speichern“ speichert die Bestätigung des Datenhinweises auch dann, wenn der Analyst deaktiviert bleibt; die Karte zeigt das Kästchen danach angekreuzt (es lässt sich nicht abwählen) mit Administrator und Zeitpunkt der Bestätigung, und neben der Schaltfläche erscheint eine Bestätigung. Die Bestätigung gilt, bis sich der Datenhinweis ändert; eine neue Fassung muss erneut bestätigt werden.
2. Solange nicht alles eingerichtet ist, nennt die Ansicht den fehlenden Schritt und wer zuständig ist: nicht im Abonnement (Vertrieb oder Plattformbetreiber), vom Betreiber nicht angeboten, kein oder ein nicht lesbarer API-Schlüssel (Plattformbetreiber unter KI-Analyst: Anbieter oder die Konfiguration der Installation), für die Organisation nicht freigeschaltet (ein Admin in der Karte Freischaltung der Organisation dieser Ansicht). Administratoren sehen die Freischaltungskarte und den Datenhinweis schon, bevor der Anbieter eingerichtet ist.

3. Geben Sie eine Frage ein, zum Beispiel welche Produktionszertifikate in 30 Tagen ablaufen und wer verantwortlich ist, und wählen Sie Fragen. Der Analyst liest Daten nur über schreibgeschützte Werkzeuge dieser Organisation: Zertifikatssuche und -details (Befunde und, falls lizenziert, Geschäftsrisiko), Warnungen, Erneuerungspläne, Ausführungsaufträge, Agentenzustand, Discovery-Beobachtungen, SSH-Inventar sowie Behebungsrichtlinien und -entscheidungen.
4. Die Antwort enthält nummerierte Verweise; jeder führt zum zitierten Datensatz (Zertifikatsdetails, Warnungen, Erneuerungspläne, Ausführung, Agentenzustand, Discovery, SSH oder Autonome Behebung). Zitiert werden können nur Datensätze, die ein Werkzeug tatsächlich geliefert hat. Unter der Antwort sehen Sie, welche Daten gelesen wurden, und die Tokenanzahl.
5. Erklären in den Zertifikatsdetails, bei einer Warnung und bei einer Behebungsentscheidung öffnet diese Ansicht mit einer vorbereiteten Frage zu diesem Datensatz; prüfen Sie sie und wählen Sie Fragen.
6. Unterhaltungen werden für die Aufbewahrungsdauer der Organisation gespeichert und sind nur für Sie sichtbar: Öffnen Sie eine, um fortzufahren, löschen Sie sie oder beginnen Sie eine Neue Unterhaltung. Administratoren sehen das Anfrageprotokoll der Organisation.

EINGABEN UND PARAMETER

- Frage mit bis zu Clm:Analyst:MaxQuestionLength Zeichen (Standard 4000). Eine Folgefrage sendet höchstens Clm:Analyst:MaxHistoryTurns frühere Beiträge (Standard 10).
- An den Modellanbieter gesendet (Anthropic Claude, vom Betreiber gewählt): Zertifikatsmetadaten, Hostnamen und Endpunkte, Verantwortliche und Dienste, Warnungen und Befunde, Pläne und Aufträge mit anfordernder und genehmigender Identität, Agentenzustand, Discovery-Beobachtungen, SSH-Zertifikatsmetadaten, Behebungsentscheidungen und der Fragetext.
- Niemals gesendet: private Schlüssel, Token, Geheimnisse, Passwörter und Zertifikatsdateien (PEM). Die Werkzeuge projizieren Datensätze ohne diese Angaben, und eine Schwärzung entfernt geheimnisartigen Text (PEM-Blöcke, API- und Zugriffsschlüssel, Bearer-Token, JWTs, password=-Zuweisungen, lange codierte Daten) aus Werkzeugergebnissen, Fragen und früheren Beiträgen.

ERGEBNIS

Eine Antwort mit nummerierten Verweisen auf Datensätze dieser Organisation. Jede Frage wird im Anfrageprotokoll (E-Mail-Adresse des Benutzers, Zeit, verwendete Werkzeuge, Tokenanzahl, Ergebnis) und im Sicherheitsjournal festgehalten, beide ohne Frage- oder Antworttext. Änderungen der Freischaltung werden mit dem bestätigenden Administrator protokolliert, dessen E-Mail-Adresse die Karte der Organisationsfreischaltung zeigt.

BERECHTIGUNGEN

Jeder angemeldete Benutzer der Organisation sieht den Status. Ist der Analyst aktiviert, können Prüfer, Operatoren und Administratoren fragen. Aktivieren, Aufbewahrung festlegen und Anfrageprotokoll lesen: Administrator.

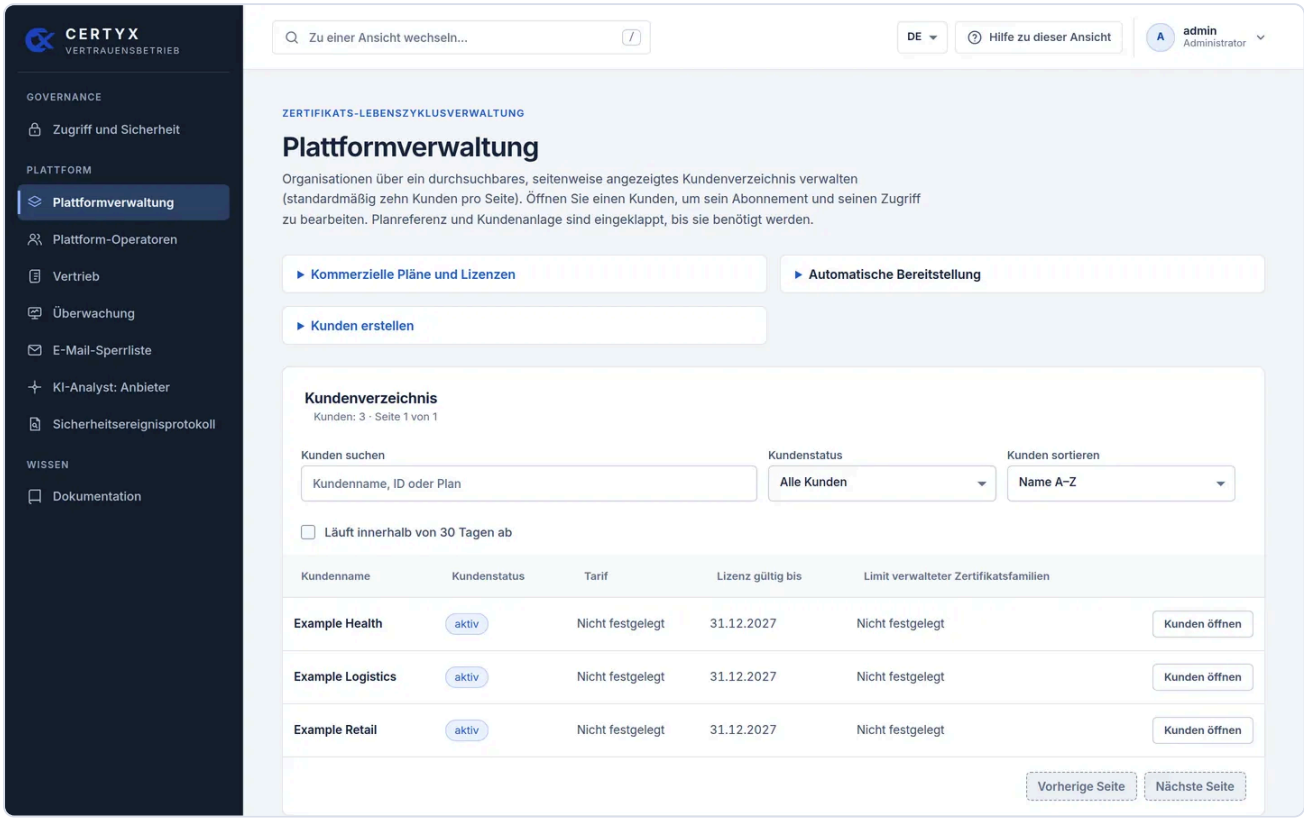
EINSCHRÄNKUNGEN

Antworten werden von einem KI-Modell erzeugt und können falsch oder unvollständig sein; prüfen Sie die zitierten Datensätze, bevor Sie handeln. Der Analyst ist schreibgeschützt und kann nichts ändern. Vom Betreiber festgelegte Kontingente (Standard: 30 Fragen pro Benutzer und Stunde, 300 pro Organisation und 2.000.000 Token in 24 Stunden) lehnen weitere Fragen mit einer Meldung ab. Eine Antwort nutzt höchstens Clm:Analyst:MaxToolRounds Modellaufrufe (Standard 6) und Clm:Analyst:Timeout (Standard 2 Minuten); sonst wird sie als unvollständig markiert oder eine Zeitüberschreitung angezeigt. Jedes Werkzeug liefert höchstens 25 Datensätze und 40.000 Zeichen. Antworten erscheinen vollständig (kein

Streaming). Ein Anbieterfehler oder eine Ablehnung wird als Meldung angezeigt und protokolliert. Bei Aufbewahrung 0 wird nichts gespeichert; abgelaufene Unterhaltungen löscht ein stündlicher Durchlauf. Ihre Unterhaltungsliste zeigt Ihre neuesten Clm:Analyst:ConversationListLimit Unterhaltungen (Standard 50); das Anfrageprotokoll zeigt die neuesten 50 Anfragen der Organisation und bewahrt Einträge Clm:Analyst:RequestJournalDays auf (Standard 400 Tage). Jede hier genannte Zahl ist ein konfigurierbarer Standardwert: Die Kontingente legt der Plattformbetreiber unter „KI-Analyst: Anbieter“ fest, die übrigen Werte die Installationskonfiguration (Clm:Analyst).

15 Plattformverwaltung

Organisationen über ein durchsuchbares, seitenweise angezeigtes Kundenverzeichnis verwalten (standardmäßig zehn Kunden pro Seite). Öffnen Sie einen Kunden, um sein Abonnement und seinen Zugriff zu bearbeiten. Planreferenz und Kundenanlage sind eingeklappt, bis sie benötigt werden.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Suchen Sie nach Name, ID oder Plan; filtern Sie nach Status oder nach Lizenzen, die innerhalb des konfigurierten Zeitfensters ablaufen (standardmäßig 30 Tage; das Kontrollkästchen zeigt die Anzahl der Tage), sortieren Sie und wechseln Sie die Seiten. Kunden öffnen zeigt nur die ausgewählte Organisation; schließen Sie deren Details, um zum Verzeichnis zurückzukehren.
2. Legen Sie einen Kunden mit einem Lizenzzeitraum an.
3. Stellen Sie seine dedizierte Instanz bereit: Bei eingeschalteter automatischer Bereitstellung (Standard der Container-Bereitstellung) beginnt sie mit dem Anlegen des Kunden von selbst, und der Kunde wird aktiv, sobald der Reiter Instanz und Bereitstellung den Auftrag als abgeschlossen zeigt; ist der automatische Start ausgeschaltet, wählen Sie Automatisch bereitstellen. Ohne automatische Bereitstellung bereiten Sie die Instanz über den serverseitigen Ablauf vor und wählen Instanz prüfen und aktivieren.
4. Legen Sie Kundenkonten mit Kundenrollen an: Auf der Registerkarte Zugriff nimmt Kundenkonto erstellen die Anmelde-E-Mail-Adresse, ein Initialpasswort und die Rolle (Administrator, Operator oder Auditor) entgegen. Jedes aufgeführte Konto hat eine eigene Rolle, Konto aktiviert und Zugriff speichern.

5. Verwalten Sie Lizenzzeiträume und sperren Sie den Zugriff bei Bedarf: Ändern Sie unter Übersicht → Kundendetails den Namen, das Lizenzende oder den Kundenstatus (aktiv, Gesperrt oder Archiviert) und wählen Sie Kunden speichern. Der Detaileditor wird nicht angezeigt, solange der Kunde bereitgestellt wird (die Aktivierung erfolgt über die Instanz-Registerkarte); ein archivierter Kunde zeigt nur seine Übersicht.
6. Legen Sie Abonnementplan, Status, Daten, Grenze für verwaltete Familien, Kulanzkontingent, Abrechnungszeitraum, Vertragsbetrag, Währung (PLN, EUR oder USD) sowie Funktions- und Zusatzmodulberechtigungen fest und wählen Sie Abonnement speichern. Die Wahl eines Plans übernimmt dessen Funktionsvorgabe und behält optionale Module bei; Discovery ist immer enthalten. Betrieb und Erkennung erhöhen keine nutzungsabhängigen Gebühren.
7. Vertrag und Abrechnung auf der Kundenkarte zeigen den unterzeichneten Vertrag aus dem Vertrieb, überfällige und nächste Zahlungen sowie eine Sperrung wegen Nichtzahlung; Im Vertrieb öffnen öffnet den Vertrag. Solange ein Vertrag in Kraft ist, folgen Plan, Zertifikatsgrenze, Gültigkeit, Abrechnungszeitraum, Betrag, Währung und Lizenzende diesem: Ein abweichender Wert wird nur mit einer Begründung für die Ausnahme gespeichert, die im Sicherheitsjournal erfasst wird.
8. Auf der Registerkarte Zugriff entfernt MFA zurücksetzen (bei Konten mit eingeschalteter MFA angezeigt) die MFA von einem Kundenkonto, das seinen Authenticator und seine Wiederherstellungscodes verloren hat, nach Bestätigung der Identität außerhalb des Systems. Die Sitzungen des Kontos werden beendet, und die Aktion wird in das Plattform-Prüfprotokoll und das Sicherheitsjournal geschrieben.
9. Automatische Bereitstellung: Das Feld Automatische Bereitstellung über dem Verzeichnis zeigt, ob sie eingeschaltet ist und bei neuen Kunden von selbst startet, die konfigurierten Infrastruktur- und Migrationsbefehle, ob diese feste, von anderen nicht änderbare Programme sind, das Zustandsverzeichnis und die Wiederholungsgrenzen. Ein im Feld oder durch einen unterzeichneten Vertrag angelegter Kunde sowie ein Kunde, der wartete, während die Bereitstellung ausgeschaltet war, wird automatisch bereitgestellt: Die Plattform erstellt die eigene Datenbank und die Rollen des Kunden, migriert die Datenbank und erfasst die Kundenidentität, speichert das nur für den Eigentümer lesbare Verbindungsgeheimnis, verifiziert die Instanz und aktiviert den Kunden. Status, Schritt und ein eventueller Abbruchgrund werden im Reiter Instanz und Bereitstellung aktualisiert; jeder Abbruchgrund nennt Ursache und Abhilfe, danach wählen Sie Bereitstellung wiederholen. Instanz prüfen und aktivieren nennt die genaue fehlgeschlagene Prüfung und ihre Abhilfe; bei einer nie vorbereiteten Instanz startet es stattdessen die automatische Bereitstellung. In der Container-Bereitstellung führt der separate Bereitstellungsauftrag (Container provisioner) die Aufträge aus, der einzige Teil der Bereitstellung mit der Berechtigung zum Anlegen von Datenbanken, sodass die Anwendung selbst keine Datenbanken oder Rollen anlegen kann; das Feld zeigt dann unter Ausgeführt von die letzte Meldung dieses Auftrags und warnt, wenn sie fehlt oder älter als fünf Minuten ist (prüfen Sie, ob der Container provisioner läuft).
10. Die Kundenkarte hat die Registerkarten Übersicht, Abonnement und Berechtigungsumfang, Zugriff, Cloud-Quellen und Instanz und Bereitstellung (letztere nur während der Bereitstellung; ein archivierter Kunde hat nur die Übersicht); die gewählte Registerkarte bleibt geöffnet, während die Karte nach einer Änderung neu geladen wird, aber nicht beim Neuladen der Seite oder beim erneuten Öffnen der Ansicht. Die Übersicht zeigt die Kundendaten, Vertrag und Abrechnung, die Abonnementnutzung eines aktiven oder gesperrten Kunden und den Editor der Kundendetails. Im Abonnement hat jede Funktion eine Auswahl: nicht enthalten, im Plan enthalten oder optionales Modul. Schließen Sie die Kundendetails mit der Schaltfläche im Kopf der Karte.

11. Cloud-Quellen: Weisen Sie die Collector-Eingangsdatei des Kunden mit Quellen-ID, Anbieter (AWS, Azure, Google Cloud oder DigiCert CertCentral), dem Bereich genau wie vom Collector gemeldet (Azure: der Vault-Name; AWS: KONTO:REGION, z. B. 123456789012:eu-central-1; Google Cloud: PROJEKT:STANDORT, z. B. my-project:global; DigiCert: account:<Ziel-ID>), der Eingangsdatei (absoluter Pfad der nur für den Eigentümer lesbaren Datei auf dem Plattform-Host oder eine Eingangs-ID, wenn die Bereitstellung ein Eingangsverzeichnis hat) und dem maximalen Snapshot-Alter (5–1440 Minuten) zu. Der nächste Synchronisierungsdurchlauf importiert sie in Inventar und Vertrauensgraph des Kunden. Die Tabelle zeigt den Zustand (wartet auf die erste Synchronisierung, funktioniert, Teilergebnis, fehlgeschlagen mit Grund, pausiert), Zertifikate, letzten Erfolg und letzten Versuch; eine Quelle kann bearbeitet, pausiert, fortgesetzt oder entfernt werden. Jede Änderung wird versioniert und im Sicherheitsjournal erfasst. Die Organisation sieht ihre Quellen und deren Zustand unter Cloud-Integrationen, nie den Ort der Eingangsdatei.
12. Registerkarte Zugriff → Prüfung privater Endpunkte: CERTYX erlauben, Bereitstellungen der Organisation auf Loopback-, privaten oder Link-Local-Adressen selbst zu prüfen (Bestätigung und Eintrag im Sicherheitsprotokoll). Ohne diese Erlaubnis prüft die Organisation solche Endpunkte mit einem eigenen Prüf-Agenten.
13. E-Mail zur Einrichtung von Kundenkonten: Kundenkonto anlegen sendet dem neuen Konto über das technische Mail-Relay der Plattform (Plattformbetrieb → E-Mail-Relay für Alarme; nie das Vertriebs-Relay) in der gewählten E-Mail-Sprache einen einmaligen Link zur Einrichtung der Authenticator-App. Die E-Mail enthält den Link als Text und als QR-Code des Links, nie das Geheimnis der App oder das Passwort. Solange dieses Relay keinen Host oder Absender hat oder fehlschlägt, zeigt die Registerkarte Zugriff den Grund und, nur bei einer Organisation ohne aktivierten Admin, den Link zum Kopieren; geben Sie ihn über einen vertrauenswürdigen Kanal und getrennt vom Anfangspasswort an den Kunden weiter. Einrichtungs-E-Mail senden in einer Kontozeile erstellt einen neuen Link (der vorherige funktioniert nicht mehr) und wird im Plattform-Audit erfasst.
14. Anmeldenetzwerke eines Kunden (Kundenkarte → Zugriff): zeigt die Adressen, die die Administratoren der Organisation für die Anmeldung erlauben. Haben sie sich ausgesperrt (zum Beispiel ein falscher Bereich oder eine geänderte Büroadresse), geben Sie Ihren Authenticator-Code ein und wählen Sie Einschränkung aufheben: Die Liste wird geleert (die Einstellung für die Mobil-App bleibt), die Änderung wird im Plattform-Audit protokolliert (customer.signin-networks.cleared mit vorher und nachher) und erscheint als identity.signin-networks.cleared-by-operator im eigenen Sicherheitsjournal der Organisation; als Plattformeintrag wird es nicht an die SIEM-Ziele der Organisation gesendet. Die Administratoren der Organisation legen danach unter Zugriff und Sicherheit eine korrekte Liste fest.
15. Freigabe durch den Kunden und Break-Glass: In einer aktiven Organisation, die bereits einen aktivierten Admin hat, ändern Kundenkonto anlegen (jede Rolle), Zugriff speichern mit Rollenerhöhung oder Wiederaktivierung und MFA zurücksetzen das Konto nicht. Sie erzeugen eine Zugriffsanfrage (die Konsole meldet das), die der Tab Zugriff unter Zugriffsanfragen mit angefragter Änderung, Zeit und Status anzeigt; ein Admin des Kunden gibt sie unter Zugriff und Sicherheit → Anfragen des Plattformbetreibers frei oder lehnt sie ab, eine freigegebene Anfrage wird sofort ausgeführt. Eine Anfrage läuft nach Clm:Platform:AccessRequests:RequestLifetime ab (Standard 72 Stunden). Eine Organisation ohne aktivierten Admin (neue Bereitstellung) oder die nicht aktiv ist, behält den direkten Ablauf. Rollen senken und Konten deaktivieren laufen immer direkt.
16. Break-Glass nur im Notfall (zum Beispiel hat der einzige Admin der Organisation den Authenticator verloren): Geben Sie in der Zeile der Anfrage den Grund (10–500 Zeichen, für den Kunden sichtbar) und Ihren aktuellen Authenticator-Code ein und wählen Sie Break-Glass starten. Ein zweiter, anderer Betreiber gibt seinen eigenen aktuellen Code ein und wählt Break-Glass bestätigen innerhalb von

Clm:Platform:AccessRequests:BreakGlassConfirmationWindow (Standard 1 Stunde). Dann wird die Aktion ausgeführt; ein angelegtes Konto, eine erhöhte Rolle oder ein wieder aktiviertes Konto wird nach BreakGlassAccessDuration (Standard 24 Stunden) zurückgenommen, sofern kein Admin des Kunden das Konto zwischenzeitlich geändert hat; jeder aktivierte Admin des Kunden (und bei einer Zugriffsänderung oder MFA-Zurücksetzung das Konto selbst) erhält über das Plattform-Relay eine E-Mail in seiner Sprache, die jede Minute erneut versucht wird (NoticeAttempts, Standard 30), bis sie zugestellt ist.

EINGABEN UND PARAMETER

- Kundenname, Lizenzenddatum, Konto-E-Mail-Adresse, Initialpasswort und Kundenrolle (Administrator, Operator oder Auditor).
- Formate: Kundenname 1–200 Zeichen; Lizenzende ein Datum von heute bis höchstens 5 Jahre im Voraus, gespeichert als 23:59:59 UTC; Abonnementlimit eine ganze Zahl von 1 bis 10.000.000, Kulanz 0–100 %, Abrechnungszeitraum 1–36 Monate, Vertragsbetrag 0–1.000.000.000 mit bis zu 2 Nachkommastellen, eine Testphase höchstens 30 Tage; Konto-E-Mail bis zu 120 Zeichen und Initialpasswort 16–256 Zeichen; Cloud-Quellen-ID 1–100 Buchstaben, Ziffern, - oder _, Bereich bis zu 300 Zeichen, Eingangsdatei bis zu 1024 Zeichen, Höchstalter 5–1440 Minuten. Der Hilfetext unter jedem Feld nennt sein Format, und ein abgelehnter Wert nennt das erwartete Format.
- Bezeichnungen für Plan und Abonnementstatus folgen der gewählten Sprache; ihre gespeicherten API-Kennungen bleiben stabil.
- Begründung für die Abweichung vom Vertrag (10–500 Zeichen), nur erforderlich, wenn ein vertraglich geregelter Wert vom unterzeichneten Vertrag abweicht.
- Break-Glass: Grund mit 10–500 Zeichen; der 6-stellige Code Ihres eigenen Authenticators (Step-up, ein Code gilt einmal; wiederholte falsche Codes sperren Ihr Konto).
- Reservierte Organisationsnamen: *, platform, platform-control, unattributed und default (beliebige Groß-/Kleinschreibung) werden beim Anlegen oder Umbenennen eines Kunden abgelehnt, weil Journal und SIEM-Export sie für die Plattform verwenden. Ein Kunde, der bereits einen solchen Namen hat, zeigt auf seiner Karte eine Warnung, bis er umbenannt ist.

ERGEBNIS

Ein versioniertes Kundenregister und Plattform-Prüfprotokoll. Jede ändernde Aktion an einem Kunden (Konten, Anfragen, Break-Glass, Abonnement und Status, Aktivierung, Bereitstellung, Cloud-Quellen, private Prüfung) wird zusätzlich im Sicherheitsjournal dieses Kunden mit dem Akteur platform:<Konto-ID des Betreibers> erfasst, dem Kunden unter Zugriff und Sicherheit → Aktivität des Plattformbetreibers angezeigt und nur über die eigenen SIEM-Bereiche der Plattform exportiert, nie an die Ziele des Kunden; Kontoaktionen speichern im Plattform-Audit die ID des Zielkontos.

BERECHTIGUNGEN

Ausdrücklich freigegebener Plattformadministrator mit einer MFA-authentifizierten Sitzung. Ein Kunden-Admin reicht nicht aus. Break-Glass erfordert zwei verschiedene Betreiber, die jeweils mit einem aktuellen Authenticator-Code bestätigen; über Firmenanmeldung angemeldete Betreiber können nicht bestätigen (kein lokaler Authenticator). Die Freigabe einer Anfrage ist den Admins des Kunden selbst vorbehalten. Step-up: Jede Änderung in dieser Ansicht (außer Tests, Verbindungsprüfungen und dem Bestätigen eines Vorfalls) fragt nach dem aktuellen 6-stelligen Code Ihres eigenen Authenticators; ein bestätigter Code gilt für Clm:Identity:OperatorStepUpWindow (Standard 5 Minuten) auch für Ihre weiteren Änderungen im Kontrollraum. Ein falscher oder bereits verwendeter Code wird abgelehnt, zählt zur Kontosperre und wird protokolliert; Abbrechen verwirft die Änderung. Über Firmenanmeldung angemeldete Betreiber haben

keinen lokalen Authenticator und können diese Änderungen nicht vornehmen. Operator-Rollen: Jede Rolle liest Kunden; Kunden anlegen, der Detaileditor, Abonnements und die Bereitstellung brauchen Vertrieb oder Administrator, Kundenkonten, Zugriffsanträge, Break-Glass, Anmeldenetze, Cloud-Quellen und die private Prüfung brauchen Sicherheitsadministrator oder Administrator, Vertrag und Abrechnung brauchen Vertrieb oder Administrator; die Karte zeigt nur, was die Rolle nutzen darf.

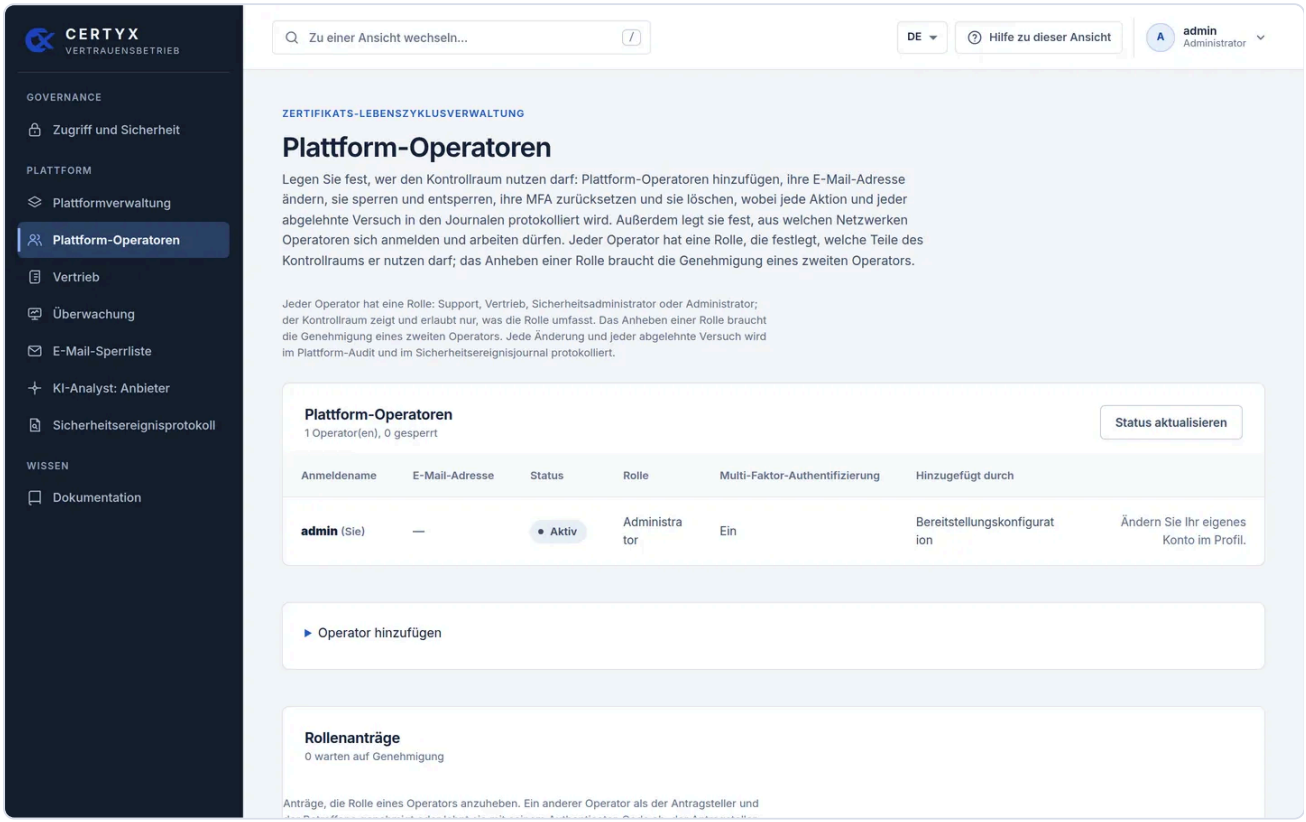
EINSCHRÄNKUNGEN

- Die Plattformverwaltung benötigt die Plattformdatenbank (Clm:Database:Platform). Das Anlegen eines Kunden benötigt zusätzlich ein absolutes Verzeichnis für Kundengeheimnisse (Clm:Storage:CustomerSecretDirectory), in dem das Verbindungsgeheimnis des Kunden erwartet wird; ohne dieses wird das Anlegen als nicht verfügbar abgelehnt.
- Bereitstellungsbefehle, Zustandsverzeichnis, automatischer Start und Wiederholungsgrenzen sind Einstellungen der Bereitstellung (Container-Bereitstellung: CERTYX_PROVISIONING-Einstellungen in certyx.env) und werden im Feld Automatische Bereitstellung schreibgeschützt angezeigt. Solange die Bereitstellung ausgeschaltet ist, bereiten Sie die Instanz manuell vor; die Aktivierung verifiziert sie. Ein Kunde, dessen Verbindungsgeheimnis ein Betreiber bereits abgelegt hat, wird nicht automatisch bereitgestellt; aktivieren Sie ihn mit Instanz prüfen und aktivieren.
- Mit der Plattformdatenbank werden Kundenkonten in deren gemeinsamer Kontotabelle gespeichert und sind auf jeder Anwendungsinstanz gleich; ohne sie verbleiben sie im lokalen Datenverzeichnis einer einzelnen Instanz. Jede Organisation verbindet ihre Unternehmensanmeldung (Microsoft Entra ID, Okta, OpenID Connect oder SAML 2.0) und die SCIM-Bereitstellung selbst unter Zugriff und Sicherheit.
- Der Vertragsbetrag ist eine erfasste kaufmännische Bedingung, keine Rechnung, keine automatische Belastung und keine feste Preisliste. Suche, Filter, Sortierung und Paginierung des Verzeichnisses laufen auf dem Server: Der Browser lädt nur die aktuelle Seite und den geöffneten Kunden. Suchtext wird wörtlich abgeglichen (% und _ sind keine Platzhalter). Der Betreiber legt Seitengröße und Ablaufzeitfenster in Clm:Platform:Directory fest.
- Die automatische Bereitstellung erfordert einen konfigurierten Infrastrukturbefehl und läuft nur auf Unix-Hosts. Die Container-Bereitstellung erstellt die Datenbank jedes Kunden mit eigener Eigentümer- und Laufzeitrolle auf dem Mandanten-Datenbankserver der Bereitstellung, über TLS mit vollständiger Zertifikatsprüfung; die Anmeldedaten eines Kunden öffnen nie die Datenbank eines anderen. Lokal kann sie je Kunde ein Docker-PostgreSQL anlegen, in der Cloud dienen die Terraform-Module für AWS RDS, Azure Flexible Server und Cloud SQL. Eine gleichnamige Datenbank oder Rolle, die nicht von der Bereitstellung angelegt wurde, eine Datenbank eines anderen Kunden und ein vorhandenes abweichendes Geheimnis werden ohne Änderungen abgelehnt. Das Löschen der Infrastruktur eines Kunden ist nicht automatisiert.
- Eingangsdateien von Cloud-Quellen sind Dateien auf dem Plattform-Host, die der Collector des Kunden schreibt; die Bereitstellung kann sie auf ein Eingangsverzeichnis beschränken, und eine Eingangsdatei außerhalb davon wird als nicht gelesen angezeigt. Eine bisher verwendete Registrierungsdatei der Synchronisierung wird einmal in die Kundenkarten übernommen. Eine Quelle eines Kunden ohne Lizenz für den Vertrauensgraphen schlägt mit diesem Grund fehl. Die Katalogfunktionen HSM integration und On-premise sind in der Planübersicht und der Berechtigungstabelle als Nicht implementiert gekennzeichnet; ihre Freischaltung aktiviert keine Funktion.
- Einrichtungslinks gelten für Clm:Identity:MfaSetupLinkLifetime (Standard 24 Stunden), funktionieren einmal und verlangen weiterhin das Kontopasswort; setzen Sie Clm:Identity:PublicConsoleUrl, damit Links die öffentliche Konsolenadresse verwenden.

- Von Betreibern angelegte und wieder aktivierte Kundenkonten zählen zum Limit aktiver Konten aus dem Vertrag des Kunden (das Benutzerlimit des Pakets, beim Übernehmen eines unterschriebenen Vertrags aus dem Plan übernommen, 5 bei einem Kunden ohne übernommenen Vertrag); von den eigenen Admins des Kunden und per SCIM angelegte Konten werden dagegen noch nicht geprüft. Bei einer Organisation mit Admin wird der Einrichtungslink eines Kundenkontos im Kontrollraum nie angezeigt: Ohne funktionierendes Plattform-Relay meldet die Konsole das, und der Admin des Kunden sendet oder erhält den Link. Eine Break-Glass-E-Mail, die nach den konfigurierten Versuchen nicht zugestellt werden kann, bleibt in der Anfrage und im Journal des Kunden erfasst.

16 Plattform-Operatoren

Legen Sie fest, wer den Kontrollraum nutzen darf: Plattform-Operatoren hinzufügen, ihre E-Mail-Adresse ändern, sie sperren und entsperren, ihre MFA zurücksetzen und sie löschen, wobei jede Aktion und jeder abgelehnte Versuch in den Journalen protokolliert wird. Außerdem legt sie fest, aus welchen Netzwerken Operatoren sich anmelden und arbeiten dürfen. Jeder Operator hat eine Rolle, die festlegt, welche Teile des Kontrollraums er nutzen darf; das Anheben einer Rolle braucht die Genehmigung eines zweiten Operators.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Melden Sie sich am Operator-Zugang (/operator-access) als aktiver Plattform-Operator mit MFA an und öffnen Sie im Kontrollraum Plattform-Operatoren. Die Liste zeigt Anmeldename, E-Mail-Adresse, Status (Aktiv oder Gesperrt), ob MFA eingerichtet ist und ob der Operator aus der Bereitstellungskonfiguration stammt (der Bootstrap-Operator, Clm:Platform:AdminIds) oder im Kontrollraum hinzugefügt wurde. Ihre eigene Zeile hat keine Aktionen.
2. Jede Änderung (Hinzufügen, E-Mail-Änderung, Sperren, Entsperren, MFA-Zurücksetzung, Einrichtungs-E-Mail, Löschen) wird mit dem aktuellen 6-stelligen Code Ihres eigenen Authenticators bestätigt (Step-up): Geben Sie ihn im Formular ein oder im Bestätigungsdialog einer Zeilenaktion, der auch die Folge nennt. Ein fehlender, falscher oder bereits verwendeter Code lehnt die Änderung mit dem Grund ab; die Ablehnung wird protokolliert.
3. Operator hinzufügen: Geben Sie Anmeldename, E-Mail-Adresse, ein Anfangspasswort und die E-Mail-Sprache ein und wählen Sie Operator hinzufügen. CERTYX legt das Konto in der Operator-Organisation (platform-control) an und stellt einen einmaligen Einrichtungslink für den Authenticator aus. Ist das

Plattform-Mail-Relay konfiguriert (Monitoring-Einstellungen), wird der Link per E-Mail gesendet; sonst zeigt die Ansicht ihn mit dem Grund zur Weitergabe über einen vertrauenswürdigen Kanal. Geben Sie das Anfangspasswort getrennt weiter. Der neue Operator öffnet den Link, gibt das Passwort ein, fügt den Authenticator hinzu, bestätigt einen Code und meldet sich dann am Operator-Zugang mit Passwort und Code an.

4. Rollen: Support (Kunden nur lesen, Überwachung und Vorfälle), Vertrieb (Vertrieb, Abonnements und Kunden-Lebenszyklus), Sicherheitsadministrator (Operatoren, Kundenkonten und Zugriffsanträge, Integrationen, SIEM, Journale, Alarmierung, Sitzungen) und Administrator (alles; der Bootstrap-Operator und die konfigurierten). Der Kontrollraum zeigt nur die Ansichten und Aktionen Ihrer Rolle, der Server lehnt alles andere mit Begründung ab. Operator hinzufügen bietet eine Rolle an: Ein neuer Operator beginnt immer als Support, jede andere Rolle wird ein Antrag unter Rollenanträge. Rolle ändern in einer Zeile senkt eine Rolle sofort ab; das Anheben erzeugt einen Antrag.
5. Rollenanträge: Ein anderer Operator als der Antragsteller und der Betroffene genehmigt oder lehnt einen offenen Antrag mit seinem eigenen Code oder Passkey ab; seine eigene Rolle muss die beantragte umfassen (nur ein Administrator genehmigt einen Administrator). Der Antragsteller sieht stattdessen Zurückziehen. Unbeantwortet läuft ein Antrag ab (Standard 3 Tage). Der letzte aktive Administrator kann nicht gesperrt, gelöscht oder einer anderen Rolle zugewiesen werden, und einen Operator mit höherer Rolle als Ihrer können Sie nicht ändern.
6. Sitzungen (Sicherheitsadministrator und Administrator): Sitzungen anzeigen listet die Browser- und Mobile-App-Sitzungen der Operatoren oder, nach Eingabe ihrer Kennung, die einer Organisation mit Client, Beginn, letzter Aktivität, Adresse und Status. Sitzung beenden (mit Ihrem Code oder Passkey bestätigt) meldet sie bei ihrer nächsten Anfrage ab und erfasst das im Sicherheitsjournal dieser Organisation.
7. E-Mail ändern: Wählen Sie E-Mail ändern, geben Sie die neue Adresse ein und speichern Sie. Die Sitzungen des Operators enden; der Anmeldename bleibt gleich.
8. Sperren: Wählen Sie Sperren und bestätigen Sie. Die Sitzungen des Operators enden sofort (bei seiner nächsten Anfrage), die Anmeldung wird abgelehnt, und die Sperre gilt auch dann, wenn die ID des Operators noch in der konfigurierten Liste steht. Entsperren und bestätigen gibt den Zugang zurück; der Operator meldet sich wieder mit Passwort und Authenticator an.
9. MFA zurücksetzen (ein Operator hat den Authenticator verloren): Bestätigen Sie das Zurücksetzen; Authenticator und Wiederherstellungscodes werden entfernt und die Sitzungen enden. Wählen Sie dann Einrichtungs-E-Mail senden, damit der Operator einen neuen Authenticator einrichten kann. Einrichtungs-E-Mail senden wird auch für einen Operator angeboten, der die Einrichtung nie abgeschlossen hat.
10. Löschen: Bestätigen Sie das Löschen. Der Operator verschwindet aus der Liste, die Sitzungen enden und das Konto wird dauerhaft deaktiviert. Die Mitgliedschaft bleibt als Grabstein erhalten, sodass ein erneutes Eintragen der ID in die konfigurierte Liste den Operator nicht zurückbringt, und der Anmeldename bleibt reserviert, damit die Journale ihn weiter nennen.
11. Jede Aktion und jeder abgelehnte Versuch wird im Plattform-Audit (Sicherheitsereignisjournal → Plattform-Audit: Aktion platform.operator.<Aktion>, Zielkonto und Ergebnis, refused:<Grund> bei einer Ablehnung; Vorher und Nachher werden mit dem Eintrag gespeichert) und im hashverketteten Sicherheitsereignisjournal mit handelndem Operator, Ziel, Vorher, Nachher und Ergebnis protokolliert.
12. Anmeldenetzwerke des Kontrollraums: Geben Sie die Adressen und Bereiche ein, von denen sich Operatoren verbinden, eine pro Zeile (203.0.113.7, 203.0.113.0/24, 2001:db8::/48), geben Sie Ihren Authenticator-Code ein und speichern Sie. Solange hier keine Liste gespeichert ist, gilt die

Bereitstellungseinstellung Clm:Platform:AllowedNetworks (angezeigt als Bereiche aus der Bereitstellungskonfiguration); danach hat die gespeicherte Liste Vorrang. Das Panel zeigt Ihre eigene Adresse und ob die Liste sie enthält; eine Liste ohne sie wird abgelehnt, bis Sie die Bestätigung setzen und einen frischen Code eingeben. Danach wird jede Operator-Anmeldung am Operator-Zugang und jede Anfrage einer Operator-Sitzung geprüft; eine Sitzung von außerhalb der Liste endet bei ihrer nächsten Anfrage. Leeren Sie die Liste und speichern Sie, um die Einschränkung aufzuheben.

EINGABEN UND PARAMETER

- Anmeldename: bis zu 120 Zeichen ohne Leerzeichen, eindeutig über alle Konten; er kann später nicht geändert werden.
- E-Mail-Adresse: eine gültige Adresse, eindeutig über alle Konten; sie erhält den Einrichtungslink.
- Anfangspasswort: 16 bis 256 Zeichen.
- E-Mail-Sprache: English, Deutsch oder Polski, für die Einrichtungs-E-Mail.
- Ihr Authenticator-Code: der aktuelle 6-stellige Code Ihres eigenen Authenticators, bei jeder Änderung abgefragt; Wiederherstellungscodes werden nicht akzeptiert.
- Bereitstellungseinstellungen (nicht in der Konsole): Clm:Platform:AdminIds (CLM_PLATFORM_ADMIN_IDS), die Konto-IDs, die Operatoren sind, bis eine gespeicherte Mitgliedschaft existiert (vom Bootstrap bei der Bereitstellung geschrieben); das Plattform-Mail-Relay (Monitoring-Einstellungen) für Einrichtungs-E-Mails.
- Anmeldenetzwerke des Kontrollraums: IPv4- oder IPv6-Adressen oder CIDR-Bereiche, die mit ihrer ersten Adresse beginnen, höchstens Clm:Identity:MaximumSignInNetworks Einträge (standardmäßig 100); Clm:Platform:AllowedNetworks in der Bereitstellungskonfiguration ist die Ausgangsliste (ungültige Einträge stoppen den Start).
- Rolle: Support, Vertrieb, Sicherheitsadministrator oder Administrator; jede Rolle über Support ist ein Antrag, bis ein zweiter Operator ihn genehmigt.

ERGEBNIS

Eine Mitgliedschaft je Operator in der Plattformdatenbank (aktiv, gesperrt oder gelöscht, mit Version), ein Konto in platform-control für hier hinzugefügte Operatoren, beendete Sitzungen nach Sperren, Löschen, E-Mail-Änderung oder MFA-Zurücksetzung und ein Eintrag im Plattform-Audit und im Sicherheitsereignisjournal für jede Aktion und jeden abgelehnten Versuch. Jede Änderung der Anmeldenetzwerke des Kontrollraums wird im Plattform-Audit (platform.signin-networks.changed, Ziel platform-control, vorher und nachher) und im Sicherheitsjournal protokolliert; abgelehnte Operator-Anmeldungen und Anfragen von außerhalb der Liste sind Anmeldeereignisse mit dem Grund network-not-allowed und der Quelladresse.

BERECHTIGUNGEN

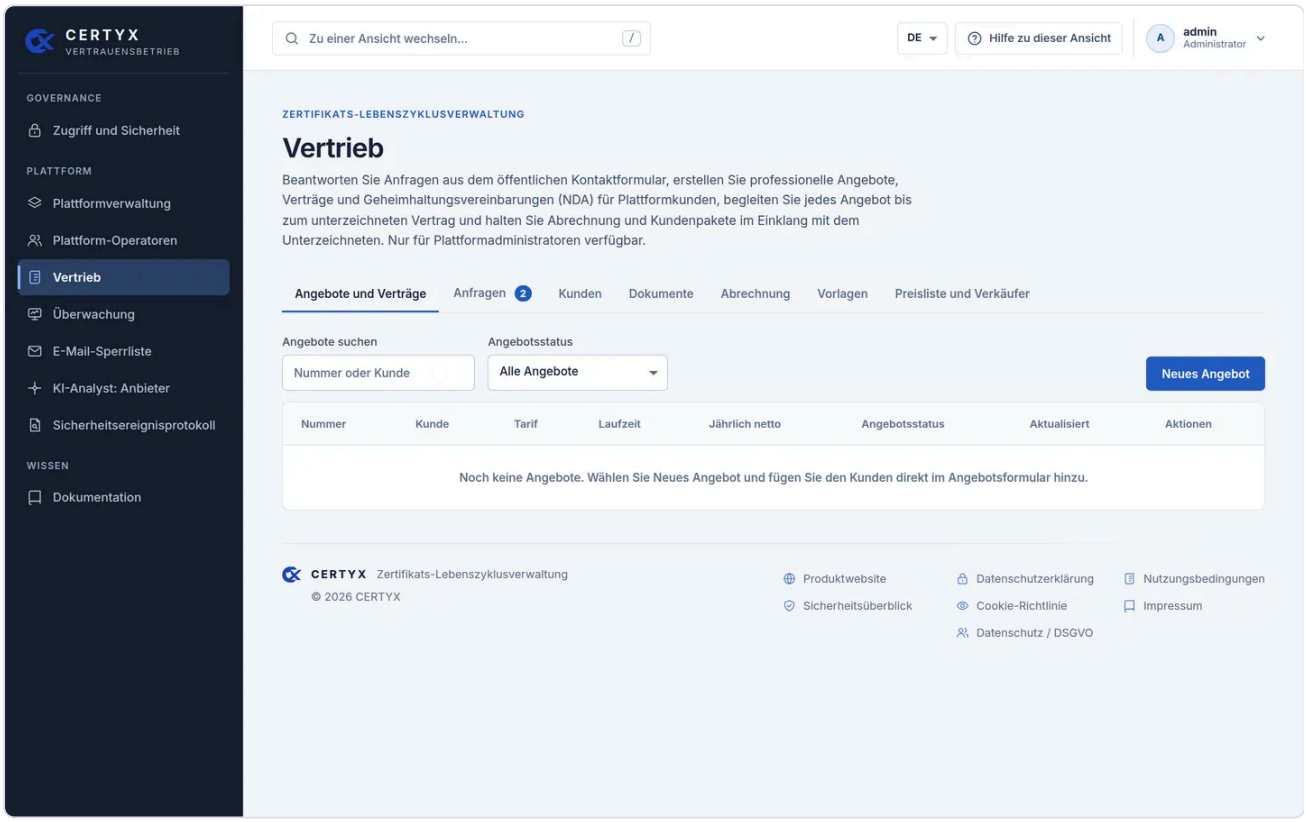
Nur aktive Plattform-Operatoren mit MFA-Anmeldung öffnen diese Ansicht und nutzen ihre API; Kundenadministratoren sowie gesperrte oder gelöschte Operatoren werden abgewiesen (403) und erreichen sie nicht. Diese Ansicht braucht die Rolle Sicherheitsadministrator oder Administrator; andere Rollen sehen sie nicht. Ein Operator ändert nur Operatoren, deren Rolle seine eigene umfasst, und genehmigt nie seinen eigenen Rollenantrag. Ein Operator ändert hier nie sein eigenes Konto (kein Selbstsperren, Selbstlöschen oder Zurücksetzen der eigenen MFA; die eigene E-Mail und den eigenen Authenticator ändern Sie im Profil), daher behält der letzte aktive Operator immer den Zugang. Die Anmeldenetzwerke des Kontrollraums: jeder aktive, mit MFA angemeldete Operator, mit einem aktuellen Authenticator-Code eines lokalen Operator-Kontos für jede Änderung.

EINSCHRÄNKUNGEN

Benötigt die Plattformdatenbank; ohne sie antworten die Anfragen der Ansicht mit 503. Eine Änderung aus einer veralteten Liste wird als Konflikt abgelehnt: Aktualisieren und wiederholen. Der Anmeldename kann nicht umbenannt werden. Gelöschte Operatoren können nicht wiederhergestellt werden; fügen Sie stattdessen einen neuen Operator hinzu. Jeder Code bestätigt eine Änderung: Ein Code eines Zeitschritts, der bereits eine Änderung (oder die Anmeldung) bestätigt hat, wird abgelehnt; warten Sie auf den nächsten Code. Falsche Codes zählen wie fehlgeschlagene Anmeldungen zur Sperre Ihres Kontos. Über die Firmenanmeldung angemeldete Operatoren haben keinen lokalen Authenticator und können keine Änderungen bestätigen: Ein lokales Operator-Konto mit Authenticator muss sie vornehmen. Der Zeitpunkt der letzten Anmeldung wird nicht angezeigt; Anmeldungen finden Sie im Sicherheitsereignisjournal. Ohne Mail-Relay muss der Einrichtungslink von Hand weitergegeben werden. Wiederherstellung, wenn sich kein Operator mehr anmelden kann: das Offline-Bootstrap-Werkzeug (reset-mfa), beschrieben in DEPLOYMENT.md. Operatoren, die die Firmenanmeldung der Plattform nutzen (eine ID sso:platform-control:<Subjekt> in der konfigurierten Liste), haben kein lokales Konto: Sie werden ohne Aktionen aufgeführt, und ihr Zugang endet, wenn die ID aus Clm:Platform:AdminIds entfernt wird. Anmeldenetzwerke lassen sich hier nur mit der Plattformdatenbank speichern; ohne sie gilt nur Clm:Platform:AllowedNetworks. Sperrt die gespeicherte Liste alle Operatoren aus dem Kontrollraum aus, entfernt der Dienstbetreiber die gespeicherte Liste in der Plattformdatenbank (DELETE FROM platform_settings WHERE key='signin-networks:platform-control' als Datenbankeigentümer, siehe PLATFORM-OPERATIONS.md); dann gilt wieder die konfigurierte Liste. Operatoren, die schon vor Einführung der Rollen bestanden, haben die Rolle Administrator. Kann sich kein Administrator mehr anmelden, setzt der Eigentümer eine Rolle in der Plattformdatenbank (Offline-Wiederherstellung).

17 Vertrieb

Beantworten Sie Anfragen aus dem öffentlichen Kontaktformular, erstellen Sie professionelle Angebote, Verträge und Geheimhaltungsvereinbarungen (NDA) für Plattformkunden, begleiten Sie jedes Angebot bis zum unterzeichneten Vertrag und halten Sie Abrechnung und Kundenpakete im Einklang mit dem Unterzeichneten. Nur für Plattformadministratoren verfügbar.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Prüfen Sie unter Preisliste und Verkäufer die Verkäuferangaben, die auf jedem Dokument erscheinen, sowie die Preisliste: Planentgelte, Zertifikatsstaffeln, SSH, Zusatzleistungen, Laufzeitrabatte, Genehmigungsschwelle und Mindestmarge. Schalten Sie unter Vertriebs-E-Mail-Versand den E-Mail-Versand ein und tragen Sie das SMTP-Relay (Host, STARTTLS-Port, Absender, optional Benutzername und ein nur schreibbares Passwort oder secret:<Name>), die optionale Betreiberkopie (Abrechnungshinweise) und bis zu 10 Empfänger der Anfragebenachrichtigung ein; Test-E-Mail senden sendet sofort eine Nachricht und nennt bei einem Fehler den Grund.
2. „Anfragen“ listet Anfragen aus dem Kontaktformular der öffentlichen Website (allgemeine Frage, Präsentationsanfrage, Angebotsanfrage, Pilotanfrage), neueste zuerst; das Symbol am Reiter zählt neue Anfragen. „Details“ zeigt Kontakt, Nachricht und Antworten des Fragebogens und erlaubt, den Status (Neu, Kontaktiert, Übernommen, Geschlossen) mit einer internen Notiz zu setzen. Bei Präsentations-, Angebots- und Pilotanfragen legt „Angebot erstellen“ den Kunden aus der Anfrage an (einmalig; weitere Klicks verwenden ihn wieder), markiert die Anfrage als „Übernommen“ und öffnet ein neues Angebot, vorausgefüllt mit Tarif, verwalteten Zertifikaten, SSH-Hosts (mindestens das SSH-

Minimum), zusätzlichen Organisationen, Onboarding, Premium-Support, Laufzeit, monatlicher Abrechnung (sofern der Tarif sie erlaubt), Währung, Startmonat, Pilotkennzeichen sowie Referenz und Nachricht der Anfrage in den Notizen. Prüfen Sie die Kalkulation und speichern Sie das Angebot.

3. Jede neue Anfrage sendet über das Vertriebs-Relay zwei E-Mails, meist innerhalb von Sekunden: Jeder Empfänger der Anfragebenachrichtigung erhält eine Benachrichtigung in der Sprache von Clm:Sales:Inquiries:NotifyLanguage (standardmäßig Englisch) mit Überschrift, Farbe und Priorität je Art (allgemeine Anfrage: normal, Antwort innerhalb 1 Werktag; Präsentationsanfrage: hoch, Präsentationstermine innerhalb 1 Werktag; Angebotsanfrage: hoch, Preisangebot innerhalb 1 Werktag; Pilotanfrage: höchste, Kontakt innerhalb 4 Geschäftsstunden), allen Formularangaben (Kontakt, Position, Unternehmen, E-Mail, Telefon, Land, Steuernummer, Sprache, Antworten des Fragebogens einschließlich bevorzugtem Betrieb und gewünschtem Start, Pilotziele, Nachricht, Einwilligung, Referenz und Eingangszeit in UTC), empfohlenen nächsten Schritten (bei einem Piloten zusätzlich eine Checkliste der Voraussetzungen), <Name> antworten (Reply-To ist der Interessent) und In der Konsole öffnen, das diese Anfrage unter Vertrieb › Anfragen öffnet. Der Interessent erhält eine Bestätigung in seiner Antwortsprache mit Referenz, nächsten Schritten und der Absenderadresse des Vertriebs. Beide sind HTML mit Textalternative und eingebettetem Logo; sie laden nichts aus dem Internet.
4. Kunden werden mit Neuer Kunde angelegt: auf der Registerkarte Kunden oder direkt neben dem Kundenfeld eines Angebots oder einer NDA; dort wird der neue Kunde nach dem Speichern sofort ausgewählt, und die bereits eingegebenen Werte bleiben erhalten. Erfassen Sie Rechtsangaben, Kontakt- und Rechnungs-E-Mail, Dokumentsprache und die Kennzeichnung öffentlicher Sektor. Verknüpfen Sie optional einen bestehenden Plattformkunden; andernfalls legt der erste unterzeichnete Vertrag einen an.
5. Optionales Pilotprojekt: Erzeugen Sie unter Dokumente vor Beginn des Pilotprojekts eine NDA für den Kunden.
6. Wählen Sie unter Angebote und Verträge Neues Angebot: Das Formular beginnt mit dem Plan Professional, einer Laufzeit von 24 Monaten und Onboarding. Wählen Sie den Kunden aus oder legen Sie ihn an und passen Sie dann Paket, Laufzeit, Abrechnung und Rabatt an. Die Kalkulation rechts wird während der Eingabe neu berechnet und warnt vor Mindestlaufzeit, Rabattgenehmigung, Höchstrabatt und Marge. Speichern Sie, um die Nummer OF/Jahr/laufende Nummer zu vergeben.
7. Wählen Sie Angebots-PDF erstellen. Jedes PDF ist mit AES-256 und einem eigenen Passwort verschlüsselt, das nach der Erzeugung einmal angezeigt wird und später über Passwort anzeigen abrufbar ist. Senden Sie PDF und Passwort über verschiedene Kanäle.
8. Führen Sie das Angebot durch seine Phasen: Als gesendet markieren, Kunde hat angenommen, Vertrag vorbereiten (vergibt UM/Jahr/laufende Nummer), dann Vertrags-PDF erstellen in der Sprache des Kunden (verfügbar ab Kunde hat angenommen). Letzte Änderungen sind möglich, bis das Angebot unterzeichnet ist. Weitere Übergänge: Zurück zum Entwurf, Kunde hat abgelehnt, Als abgelaufen markieren und Angebot stornieren; ein abgelehntes oder abgelaufenes Angebot kann als Entwurf wieder geöffnet werden, Stornieren, Ablehnen und Unterzeichnen verlangen eine Bestätigung, und eine Stornierung ist endgültig.
9. Öffnen Sie nach der Unterzeichnung Unterzeichneter Vertrag und Konfiguration: Erfassen Sie die Bedingungen so, wie sie im Vertrag stehen (möglich, solange das Angebot angenommen oder der Vertrag vorbereitet ist), laden Sie den Scan hoch, vergleichen Sie mit Bedingungen prüfen Angebot, Vertrag und Kundenkonfiguration und wählen Sie dann Als unterzeichnet markieren; die Schaltfläche bleibt deaktiviert, bis die unterzeichneten Bedingungen erfasst sind. Dadurch wird das Angebot

gesperrt, der Zahlungsplan erstellt und der Plattformkunde anhand der Bedingungen angelegt oder konfiguriert: Plan, Funktionen, Zertifikatslimit mit Toleranz, Gültigkeit, Abrechnungszeitraum, Vertragsbetrag und Benutzerlimit.

10. Ein neu angelegter Plattformkunde beginnt im Status Bereitstellung: Stellen Sie seine Instanz in der Plattformadministration bereit und prüfen Sie sie (Plattformkunden öffnen). Ist die Konfiguration bei der Unterzeichnung fehlgeschlagen, wiederholt Auf Kundenabonnement anwenden sie; damit werden die unterzeichneten Bedingungen auch später erneut angewendet.
11. Erfassen Sie unter Abrechnung Zahlungen mit Datum und Referenz. Wird die Zahlung erfasst, die einen überfälligen Posten ausgleicht, wird ein durch die Abrechnung gesperrter Kunde automatisch wieder freigeschaltet. Das Feld Erfordert Aufmerksamkeit über den Registerkarten (nur sichtbar, wenn etwas fällig ist) listet fällige Zahlungen, überfällige Posten, gesperrte Kunden und auslaufende Verträge auf; Verlängerungsangebot vorbereiten erstellt einen Entwurf, der am Tag nach Vertragsende beginnt.
12. Bearbeiten Sie unter Vorlagen die Texte von Angebot, Vertrag und NDA für jede Sprache, fügen Sie Datenfelder und generierte Blöcke ein, zeigen Sie eine PDF-Vorschau an und speichern Sie eine neue Version.
13. Erfassen Sie eine Zahlung mit Zahlung erfassen in einem Dialog mit Zahlungsdatum und Referenz (bis zu 120 Zeichen). Die Preisliste zeigt jeden Plan als eigene Karte mit Zusammenfassung (Entgelt, Limits, Marge, Vollständigkeit der PL/EN/DE-Texte) und aufklappbarer Bearbeitung; eine Karte warnt vor fehlenden oder abweichenden PL/EN/DE-Listen und Supporttexten, einer Marge unter dem Minimum und einer Marge, die beim maximalen Vertriebsrabatt unter das Minimum fällt. Speichern oder verwerfen Sie Preislistenänderungen über die Leiste, die beim Scrollen sichtbar bleibt.

EINGABEN UND PARAMETER

- Anfrage (aus dem öffentlichen Formular): Art, Name, Unternehmen, geschäftliche E-Mail, optional Telefon, Land, Position und Steuernummer, Sprache für Antwort und Dokumente (EN, DE oder PL), Nachricht (Pflicht bei einer allgemeinen Frage), Einwilligung sowie bei Angebots- und Pilotanfragen der optionale Fragebogen: Tarif, verwaltete Zertifikate, SSH-Hosts, Organisationen, bevorzugter Betrieb (von CERTYX betrieben, eigene Umgebung oder noch offen), Startmonat, Laufzeit in Jahren, jährliche oder monatliche Abrechnung, Währung, Onboarding, Premium-Support, öffentlicher Sektor, Zertifikatsquellen und Ziele des Pilotprojekts.
- Kunde: Firmenname, Anschrift, Steuernummer, Registernummer, Vertreter, Kontakt- und Rechnungs-E-Mail, Sprache, öffentlicher Sektor, verknüpfter Plattformkunde.
- Angebot: Plan, verwaltete Zertifikate, SSH-Hosts, zusätzliche Organisationen, Onboarding, zusätzliche Tage, Premium-Support, Pilotprojekt, Laufzeit (standardmäßig mindestens 12 Monate, 24 empfohlen, höchstens 60), jährliche oder monatliche Rechnungsstellung, Vertriebsrabatt und Genehmigender, Startdatum, Gültigkeit, Notizen, PLN, EUR oder USD (EUR und USD zu den Kursen der Preisliste). Ein Rabatt über der Genehmigungsschwelle der Preisliste erfordert einen Genehmigenden, und kein Rabatt darf den maximalen Vertriebsrabatt überschreiten.
- Formate: verwaltete Zertifikate und SSH-Hosts sind ganze Zahlen von 0 bis 10.000.000, zusätzliche Organisationen 0–50, zusätzliche Tage 0–365; Vertriebsrabatt 0–100 % mit bis zu 2 Nachkommastellen, Genehmigender bis zu 300 Zeichen, Notizen bis zu 4.000 Zeichen; Textfelder des Kunden bis zu 300 Zeichen; Zahlungsziel 1–120 Tage; Beträge mit bis zu 2 Nachkommastellen; SMTP-Host ein Hostname oder eine IP-Adresse ohne Schema und Port, Port 1–65535, Absender und Betreiberkopie einzelne E-Mail-Adressen, Empfänger der Anfragebenachrichtigung bis zu 10 durch Kommas getrennte Adressen; Felder des Verkäuferprofils bis zu 300 Zeichen; Vorlagen bis zu 200.000 Zeichen. Fragebogen der Anfrage: verwaltete Zertifikate und SSH-Hosts ganze Zahlen ab 0 (bis

Clm:Sales:Inquiries:MaxQuantity), Organisationen ab 1 (bis MaxOrganizations, standardmäßig 100), Laufzeit 1–3 Jahre; Nachricht und Pilotziele bis Clm:Sales:Inquiries:MaxMessageLength (standardmäßig 4.000 Zeichen); Name, Unternehmen, Telefon, Land, Position und Steuernummer bis zu 300 Zeichen. Der Hilfetext unter jedem Feld nennt sein Format, und ein abgelehnter Wert nennt Feld und erwartetes Format.

- Unterzeichnete Bedingungen: Plan, Mengen, Laufzeitbeginn und -ende (Ende nach Beginn), Abrechnungszeitraum (monatlich oder jährlich), jährlicher Nettobetrag, Währung (PLN, EUR oder USD), Zahlungsziel (1–120 Tage) und vereinbarte Änderungen. Scan: PDF, JPEG oder PNG, am Inhalt erkannt, innerhalb der konfigurierten Größengrenze (Clm:Sales:MaxSignedScanBytes, standardmäßig 20 MB).
- Vorlagen: Überschriften (#), Aufzählungen (-), nummerierte Punkte (1.), **fett**, {{Datenfelder}}, {{#if Bedingung}}-Passagen und Blöcke wie [[pricing-table]], [[payment-schedule]] und [[signatures]].

ERGEBNIS

Nummerierte Angebote und Verträge mit erfasstem Lebenszyklus; passwortgeschützte PDFs mit Logo, Kopfzeilen und Seitenzahlen, gespeichert mit Vorlagenversion und SHA-256; ein Zahlungsplan mit Erinnerungen; und ein anhand der unterzeichneten Bedingungen angelegter oder konfigurierter Plattformkunde, dessen Vertrag anschließend sein Abonnement in der Plattformadministration bestimmt. Dokumenterzeugung, Passwortanzeige, Bedingungen, Scans, Statusänderungen, Kundenkonfiguration, Sperrungen und Wiederfreischaltungen werden im Sicherheitsjournal erfasst.

BERECHTIGUNGEN

Plattformadministrator mit einer per MFA authentifizierten Sitzung. Kundenkonten, einschließlich Kunden-Admin, können diese Ansicht und ihre API nicht öffnen. Step-up: Das Unterzeichnen eines Angebots (das den Kunden anlegt oder konfiguriert), das Übernehmen eines Vertrags ins Abonnement, das Erfassen einer Zahlung und das Ändern des Vertriebs-Mail-Relays fragen nach dem aktuellen 6-stelligen Code Ihres Authenticators (einige Minuten durch einen bestätigten Code abgedeckt); Kalkulationen, Angebote, Parteien, Dokumente und Vorlagen nicht.

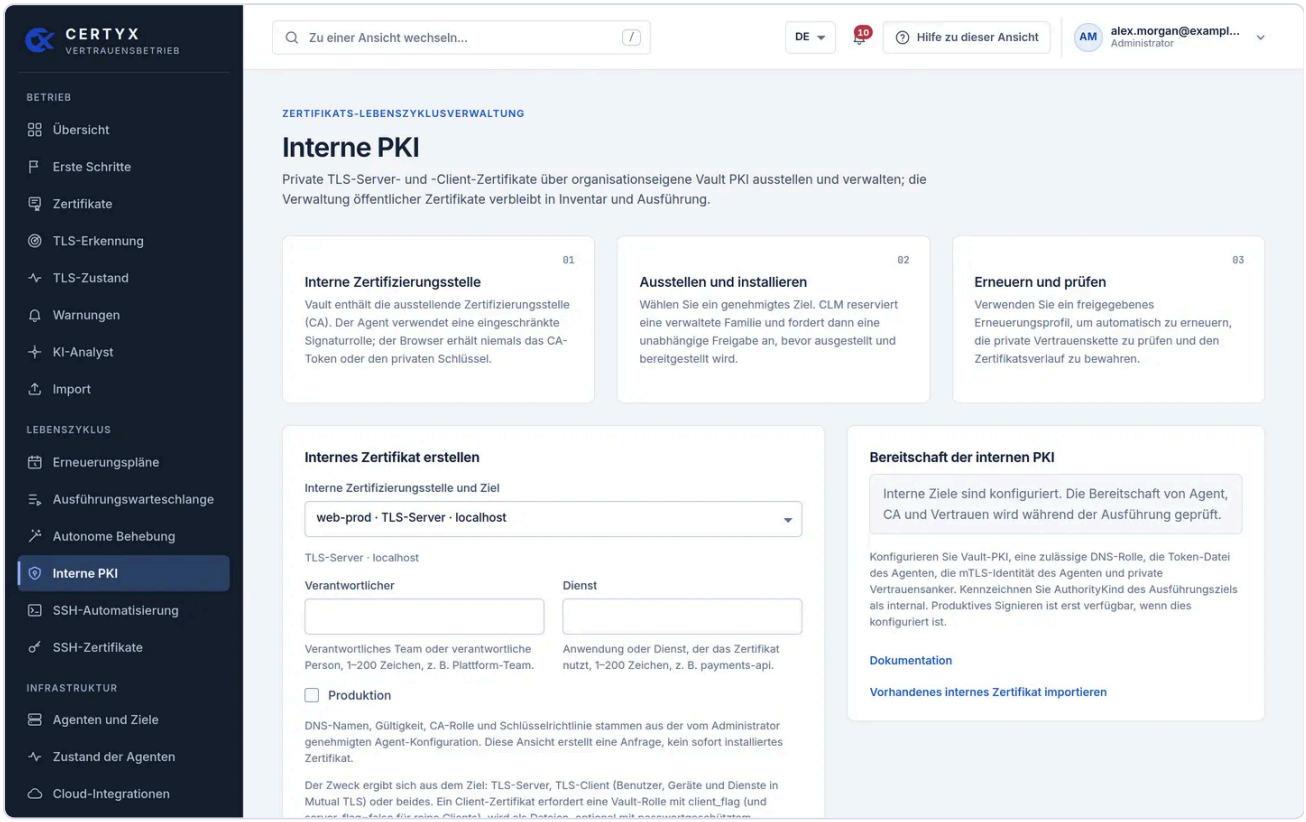
EINSCHRÄNKUNGEN

- Erfordert die Plattformdatenbank (Clm:Database:Platform) mit dem aktuellen platform/schema.sql; ohne sie meldet die Ansicht, dass der Vertrieb nicht verfügbar ist.
- Das öffentliche Kontaktformular benötigt die Plattformdatenbank; ohne sie meldet das Formular, dass es nicht verfügbar ist. Es nimmt 10 Anfragen pro Minute und Adresse an (Clm:Http:InquiriesPerWindow), verlangt ein CSRF-Token und verwirft stillschweigend Einsendungen, die das versteckte Honeypot-Feld ausfüllen. Benachrichtigung und Bestätigung werden nur bei eingeschaltetem Vertriebs-E-Mail-Versand gesendet; bis dahin warten sie unter Abrechnung und werden nach dem Einschalten gesendet (die Warteschlange wird alle Clm:Sales:NoticeInterval, standardmäßig 30 Sekunden, und sofort nach einer neuen Anfrage geprüft). Ohne Empfänger der Anfragebenachrichtigung geht die Benachrichtigung an die Kontakt-E-Mail des Verkäufers; fehlt auch diese, wird nur die Bestätigung eingereiht. In der Konsole öffnen verwendet Clm:Sales:Inquiries:ConsoleUrl oder, wenn leer, die Adresse, von der das Formular gesendet wurde, und erfordert die Anmeldung eines Plattformadministrators. Jeder Besucher sieht die Referenz auf dem Bildschirm; eine gefilterte Honeypot-Einsendung sendet keine E-Mail.
- Die Standardvorlagen für Vertrag, AVV (DPA) und NDA sind Entwürfe und müssen vor der Verwendung von einem Juristen geprüft werden.
- Monatsbeträge in Angeboten dienen nur der Veranschaulichung; Verträge werden für die gesamte Laufzeit geschlossen.

- Die Plattform stellt keine Umsatzsteuerrechnungen aus und ist nicht mit einer Bank verbunden: Zahlungen werden manuell erfasst, Rechnungen stammen aus Ihrem Buchhaltungssystem.
- E-Mail-Erinnerungen und -Hinweise werden nur gesendet, solange der Vertriebs-E-Mail-Versand eingeschaltet ist; andernfalls bleiben sie in der Warteschlange unter Abrechnung sichtbar und werden nach dem Einschalten gesendet. Werte der Konfigurationsdatei werden einmal in die Konsole übernommen; die Zeitgrenze des Relays bleibt eine Einstellung der Bereitstellung. TLS ist immer erforderlich.
- Ein unbezahlter Posten sperrt den verknüpften Plattformkunden nach der internen Kulanzfrist, die in Clm:Sales:SuspensionGraceDays konfiguriert ist; die Kulanzfrist wird in Erinnerungen nicht genannt. Wenn die Zahlung erfasst wird und nichts anderes über die Kulanzfrist hinaus überfällig ist, wird der Kunde automatisch wieder freigeschaltet. Eine von einem Operator in der Plattformadministration gesetzte Sperrung wird durch die Abrechnung nie aufgehoben, und ein Operator, der einen Kunden reaktiviert, während eine Zahlung noch über die Kulanzfrist hinaus überfällig ist, sieht ihn bei der nächsten Abrechnungsprüfung erneut gesperrt.
- Unterzeichnete Scans werden zum Vergleich gespeichert; die Plattform liest ihren Text nicht. Die Bedingungen werden mit den von Ihnen erfassten Werten verglichen.
- Das Anlegen des Plattformkunden bei der Unterzeichnung erfordert Clm:Storage:CustomerSecretDirectory; die dedizierte Instanz wird weiterhin in der Plattformadministration bereitgestellt und geprüft.
- Ist der laufende Server älter als die Konsolendateien, weist die Ansicht darauf hin, statt leere Listen anzuzeigen; starten Sie die Anwendung neu und laden Sie die Seite erneut.

18 Interne PKI

Private TLS-Server- und -Client-Zertifikate über organisationseigene Vault PKI ausstellen und verwalten; die Verwaltung öffentlicher Zertifikate verbleibt in Inventar und Ausführung.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Konfigurieren Sie Vault PKI mit einer ausstellenden Zertifizierungsstelle (CA) und einer auf DNS beschränkten Signierrolle. Speichern Sie ihr Token in einer privaten Datei auf der Agent-Seite.
2. Konfigurieren Sie den ausgehenden mTLS-Agenten und private Vertrauensanker. In Ausführungswarteschlange → Bereitstellungsziele legt ein Administrator das Ziel mit der Zertifizierungsstelle Interne CA (Vault PKI), deren CA-URL, Mount und Rolle an (AuthorityKind internal). Das Agent-Ziel verwendet AuthorityKind vault.
3. Bereitschaft der internen PKI zeigt, ob interne Ziele vorhanden sind und wie viele deaktiviert sind; ohne aktiviertes Ziel ist das Formular deaktiviert. Deaktivierte Ziele bleiben in der Liste, als deaktiviert markiert und nicht wählbar, weil der Server für sie keine neuen Aufträge annimmt. Wählen Sie unter Internes Zertifikat erstellen das Ziel in Interne Zertifizierungsstelle und Ziel (jedes Ziel mit interner CA wird mit Zweck und Identitäten aufgeführt), geben Sie Verantwortlicher, Dienst und Produktion ein und wählen Sie Interne Ausstellung anfordern. CERTYX reserviert eine verwaltete Familie, bevor die Ausstellungsanforderung erstellt wird; die Bestätigung zeigt die Auftrags-ID.
4. Ein anderer Administrator genehmigt den Auftrag in der Ausführungswarteschlange (Freigabe- und Ausführungswarteschlange öffnen). Der Agent erzeugt seinen privaten Schlüssel/CSR, signiert über Vault, stellt bereit und prüft TLS.

5. Prüfen Sie das resultierende Zertifikat unter Inventar interner Zertifikate (50 pro Seite). Dort stehen nur als intern klassifizierte Zertifikate: über ein internes Ziel ausgestellt oder als Internes Zertifikat importiert (Vorhandenes internes Zertifikat importieren). Konfigurieren Sie für die Automatisierung ein separat genehmigtes Erneuerungsprofil in der Ausführungswarteschlange.
6. Für Client-Zertifikate legen Sie das Ziel unter Ausführung mit dem Zweck TLS-Client (oder Server und Client) und seinen Identitäten an. Verwenden Sie eine eigene Vault-Rolle: client_flag=true, server_flag=false für reine Clients, allowed_domains für E-Mail-/DNS-Domänen, allowed_other_sans für Benutzerprinzipalnamen (1.3.6.1.4.1.311.20.2.3;UTF8:*@corp.example.com) und allowed_uri_sans für URIs; cn_validations=disabled nur bei einem frei gewählten allgemeinen Namen wie einem Personennamen. Eine Rolle ohne client_flag wird mit Nennung dieser Einstellung abgelehnt, ebenso eine reine Client-Anfrage, wenn die Rolle zusätzlich Server-Authentifizierung gewähren würde.

EINGABEN UND PARAMETER

- DNS-Namen, Client-Identitäten, Zweck, CA-URL und Vault-Mount/-Rolle stammen aus dem Ausführungsziel; Gültigkeit und Schlüsselrichtlinie stammen aus der Vault-Rolle und der Agent-Konfiguration. Importierte Zertifikate können ausdrücklich als intern klassifiziert werden.
- Verantwortlicher und Dienst: erforderlich, jeweils 1–200 Zeichen. Das Ziel muss aktiviert sein; eine Anfrage für ein deaktiviertes Ziel wird abgelehnt (aktivieren Sie es in der Ausführungswarteschlange).

ERGEBNIS

Ein prüfbarer Ausstellungsauftrag, gefolgt von einem inventarisierten internen Zertifikat nach nachweislich erfolgreicher Ausführung. Die Erneuerung übernimmt seine Familie.

BERECHTIGUNGEN

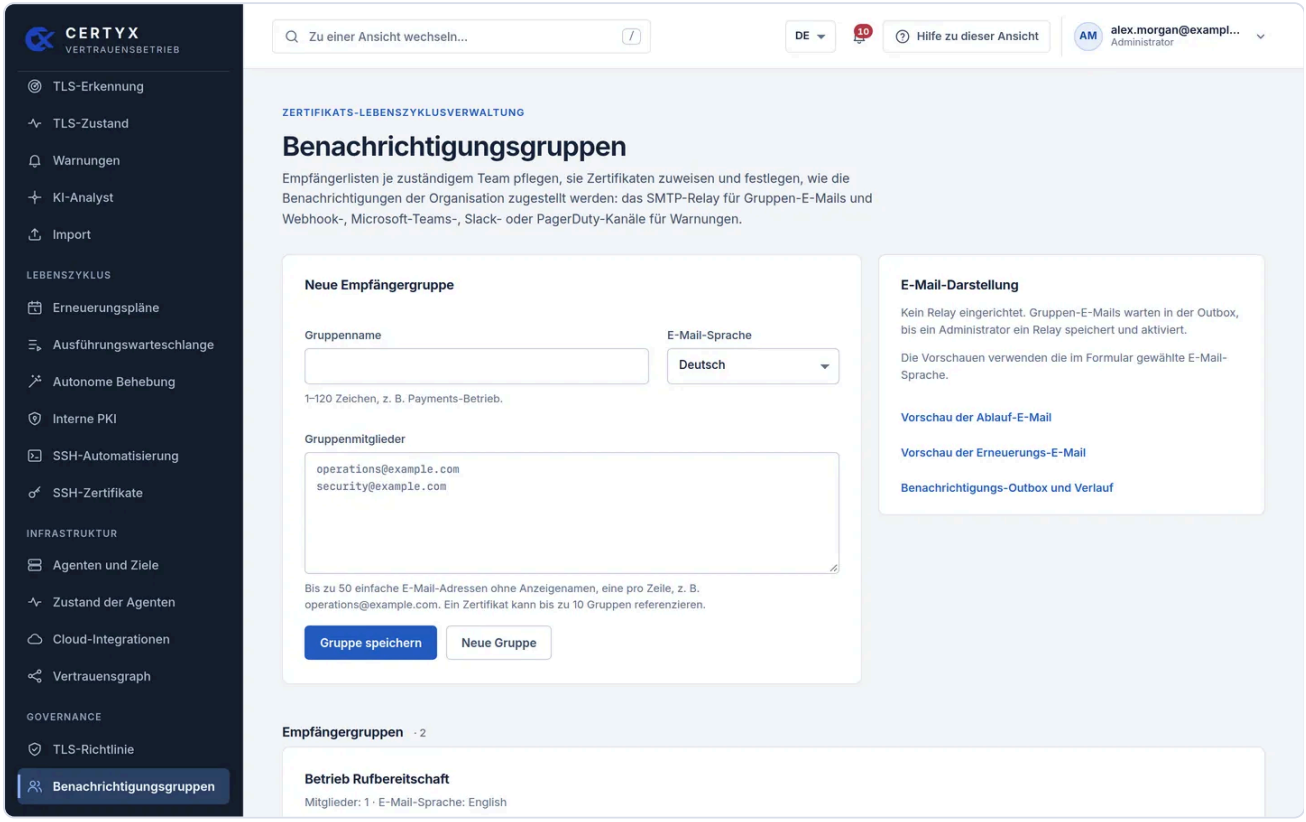
Operator oder Admin fordert die Ausstellung an (auf einem Dienst mit Abonnements nur mit der Funktion AUTO_DEPLOYMENT und freier Kapazität verwalteter Familien); ein anderer Admin genehmigt den Auftrag; Auditor hat nur Lesezugriff (das Formular ist deaktiviert). Organisationsspezifische Ziele und Agent-Identitäten werden durchgesetzt.

EINSCHRÄNKUNGEN

Erfordert eine konfigurierte Vault-Instanz und einen Agenten. Diese Ansicht initialisiert keine Stamm-CA, verteilt keine Vertrauensanker an alle Clients und stellt keine Codesignaturzertifikate aus. Client-Zertifikate (Benutzer, Geräte, Dienste in Mutual TLS) werden ausgestellt, wenn der Zweck des Ziels TLS-Client oder Server und Client ist und die Vault-Rolle client_flag setzt; sie werden nur als Dateien auf Unix-Agenten bereitgestellt (kein Windows-Zertifikatsspeicher, kein Browser- oder Smartcard-Enrollment). Öffentliche Importe werden nie automatisch als vertrauenswürdig eingestuft.

19 Benachrichtigungsgruppen

Empfängerlisten je zuständigem Team pflegen, sie Zertifikaten zuweisen und festlegen, wie die Benachrichtigungen der Organisation zugestellt werden: das SMTP-Relay für Gruppen-E-Mails und Webhook-, Microsoft-Teams-, Slack- oder PagerDuty-Kanäle für Warnungen.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Erstellen Sie eine Empfängergruppe mit Namen, E-Mail-Sprache (Englisch, Deutsch oder Polnisch) und bis zu 50 einfachen Adressen; weisen Sie Gruppen in den Zertifikatsdetails zu. Gruppe archivieren nimmt eine Gruppe außer Betrieb: Sie erhält keine E-Mails mehr und kann Zertifikaten nicht mehr zugewiesen werden, bleibt aber mit ihren Mitgliedern gelistet (als Archiviert markiert); Gruppe wiederherstellen aktiviert sie wieder. Beim Bearbeiten bleibt der Archivstatus erhalten. Ein abgelehntes Speichern nennt den Grund (Kennung oder Name zu lang, nicht unterstützte Sprache, ungültige Mitglieder, inzwischen geändert).
2. Eine Gruppe erhält E-Mails, wenn ein ihr zugewiesenes Zertifikat eine Ablaufschwelle erreicht oder abgelaufen ist, nach einer verifizierten Erneuerung dieses Zertifikats, bei SSH-Zertifikatsereignissen ihr zugewiesener SSH-Profile und wenn eine Behebungsrichtlinie sie benachrichtigt. E-Mail-Darstellung → Vorschau der Ablauf-E-Mail und Vorschau der Erneuerungs-E-Mail zeigen das Layout der Nachricht mit Beispieldaten in der im Formular gewählten E-Mail-Sprache (bis zur Auswahl die Konsolensprache, beim Bearbeiten die Sprache der Gruppe); Gruppen-E-Mails warten in der Outbox, bis ein aktiviertes SMTP-Relay vorhanden ist.

3. Zustellung → SMTP-Relay: Geben Sie Host, Port (587), Absenderadresse und, falls das Relay es verlangt, Benutzername und Passwort ein. STARTTLS wird immer verwendet und das Zertifikat des Relays geprüft. Aktivieren Sie das Relay und speichern Sie.
4. Test-E-Mail senden schickt über das gespeicherte Relay eine kurze Nachricht an die eingegebene Adresse und zeigt, ob das Relay sie angenommen hat; das Ergebnis wird beim Relay gespeichert.
5. Zustellung → Outbox-Kanäle: Fügen Sie einen Webhook (HTTPS-JSON, optional mit HMAC-SHA256 in X-Certyx-Signature signiert), einen eingehenden Microsoft-Teams-Webhook oder eine Workflows-URL, einen eingehenden Slack-Webhook (https://hooks.slack.com/…; Warnungsinhalte kommen als reiner Text an, ohne Erwähnungen oder Links) oder einen PagerDuty-Integrationsschlüssel (Routing Key) hinzu. Eskalationsverzögerung 0 sendet jede offene Warnung sofort; eine Verzögerung macht daraus einen Eskalationskanal, der nur kritische Warnungen erhält, die nach dieser Zeit noch unbestätigt sind. Test senden prüft den Kanal (ein PagerDuty-Test wird sofort wieder aufgelöst).
6. Ereignisse eines Kanals: Zertifikatswarnungen sind standardmäßig gewählt; aktivieren Sie Auftrag angefordert, Auftrag genehmigt, Zertifikat bereitgestellt und verifiziert, Auftrag fehlgeschlagen, Bereitstellung zurückgerollt, Auftrag abgebrochen und Zertifikat erneuert, damit Pipelines, Chat-Kanäle oder ITSM-Werkzeuge jede Erneuerung verfolgen. Jedes Ereignis wird einmal pro Kanal gesendet, sobald es eintritt (innerhalb Clm:Notifications:LifecycleEventWindow, ein Tag); ein Webhook erhält { eventId, type, version 1, event { id, at, actor, jobId, targetId, certificateId, domains, state } }, Teams und Slack einen kurzen Text, PagerDuty nur Warnungen sowie fehlgeschlagene oder zurückgerollte Aufträge.
7. Jedes Relay und jeder Kanal zeigt wartende und unzustellbare Nachrichten, die letzte Zustellung und den letzten Fehlergrund; Warnungen → Benachrichtigungs-Outbox und Verlauf listet die einzelnen Einträge.
8. Vor dem Versand von Gruppen-E-Mails wird die aktive Gruppenmitgliedschaft erneut geprüft: Entfernte Empfänger erhalten keine Nachrichten aus der Warteschlange, neue Empfänger übernehmen keine älteren, und eine Nachricht ohne berechtigte Empfänger wird storniert. Empfänger werden per Bcc beliefert; die Absenderadresse wird nicht hinzugefügt.
9. Empfänger, die keine E-Mails mehr erhalten, listet die Mitglieder Ihrer Gruppen, die auf der E-Mail-Sperrliste der Plattform stehen (vom E-Mail-Anbieter gemeldete dauerhafte Unzustellbarkeit oder Beschwerde), mit Grund, Datum und Gruppen; die Gruppenkarten zeigen, wie viele Mitglieder gesperrt sind. CERTYX sendet ihnen über kein Relay etwas, bis ein Plattformbetreiber sie entfernt. Korrigieren oder ersetzen Sie die Adresse in der Gruppe, oder lassen Sie das Postfach reparieren und bitten Sie Ihren Plattformbetreiber (Support), sie zu entfernen. Es gelten nur plattformweite Einträge und Einträge, die durch E-Mails Ihrer eigenen Organisation entstanden sind; ein Bounce der E-Mail einer anderen Organisation sperrt Ihre Empfänger nie.

EINGABEN UND PARAMETER

- Gruppenname (1–120 Zeichen), E-Mail-Sprache und Mitglieder (einfache Adressen ohne Anzeigenamen, höchstens 50 pro Gruppe). Auch Kanalnamen haben 1–120 Zeichen.
- Relay-Host, Port, Absenderadresse, optional Benutzername und Passwort; Transportsicherheit STARTTLS (ein Loopback-Relay im Klartext wird nur in der Development-Umgebung angeboten).
- Kanalname, Kennung (1–64 Kleinbuchstaben, Ziffern und Bindestriche, beginnend mit einem Buchstaben oder einer Ziffer; group-email und mobile-push sind reserviert), Art, Eskalationsverzögerung (0–1440 Minuten), HTTPS-Adresse ohne Benutzername oder Passwort oder PagerDuty-Routing-Key (20–64 Buchstaben und Ziffern), optional Signaturgeheimnis des Webhooks (bis zu 256 Zeichen).

ERGEBNIS

Protokollierte, versionierte Zustellkonfiguration der Organisation und tatsächliche Zustellung von Gruppen-E-Mails und Warnungen. Passwörter, Kanaladressen, Routing Keys und Signaturgeheimnisse werden verschlüsselt gespeichert, nie wieder angezeigt und weder ins Journal noch in Protokolle geschrieben; lassen Sie ein Geheimnisfeld leer, um den gespeicherten Wert beizubehalten, oder wählen Sie Gespeichertes Passwort entfernen bzw. Gespeichertes Signaturgeheimnis entfernen, um ihn zu löschen. Das SMTP-Relay sendet auch die E-Mail zur Einrichtung des Authenticators für in Zugriff & Sicherheit angelegte Benutzer, sofort und nur an diese Person. Ohne eingeschaltetes Relay zeigt die Konsole stattdessen den Einrichtungslink zum Kopieren.

BERECHTIGUNGEN

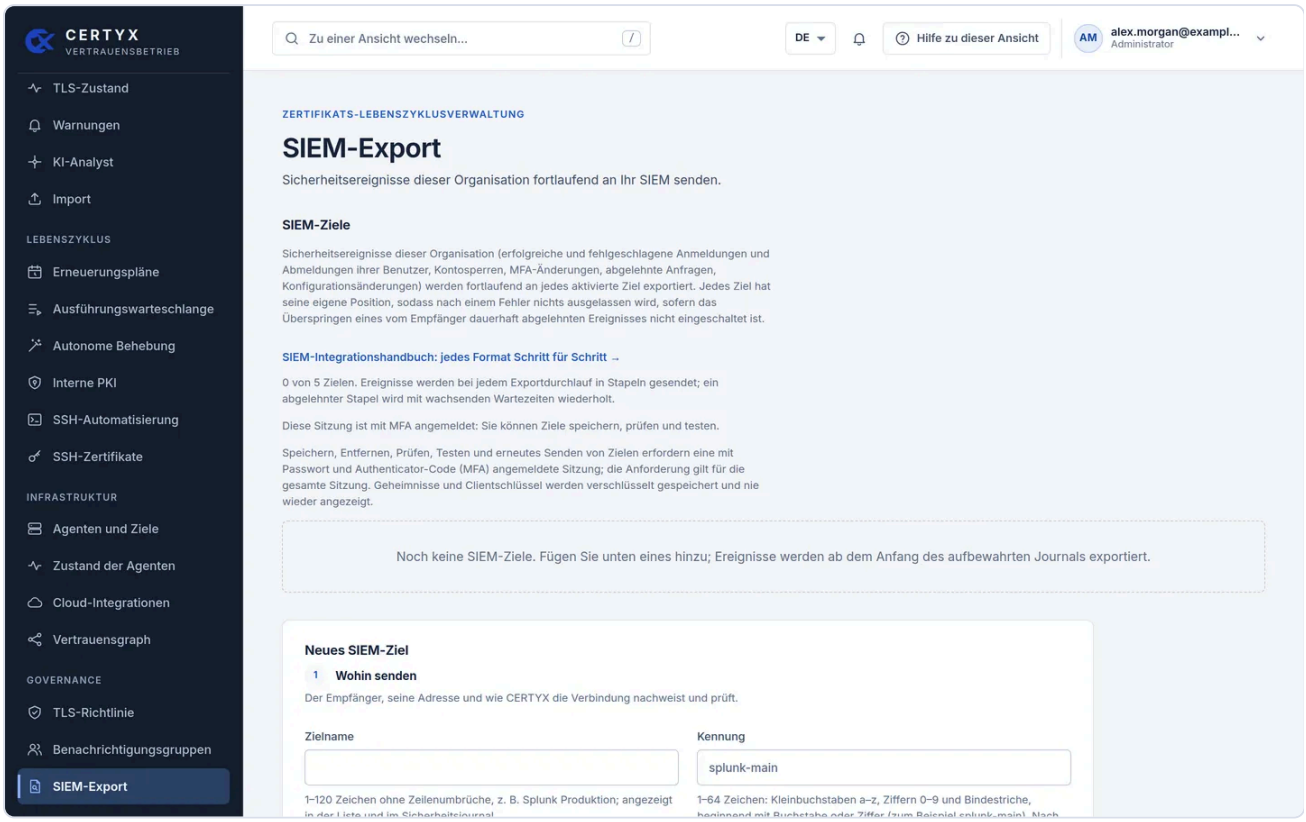
Admin erstellt, ändert, archiviert und reaktiviert Empfängergruppen, ändert und testet das SMTP-Relay (das deaktiviert statt entfernt wird) und fügt Outbox-Kanäle hinzu, ändert, testet und entfernt sie; andere angemeldete Rollen lesen sie. Empfängergruppen werden archiviert statt entfernt, damit Zertifikate und das Journal weiter auf sie verweisen.

EINSCHRÄNKUNGEN

Die Zustellung erfolgt mindestens einmal: Ein Relay oder Kanal, der eine Nachricht kurz vor einem Fehler angenommen hat, kann sie erneut erhalten (X-CLM-Event-Id und X-Certyx-Event-Id kennzeichnen sie). Fehlgeschlagene Nachrichten werden mit wachsenden Pausen (höchstens eine Stunde) wiederholt und nach 10 Versuchen als unzustellbar markiert. Eine Organisation kann höchstens Clm:Notifications:MaxChannelsPerOrganization Outbox-Kanäle festlegen (Standard 20). Implizites TLS (SMTPS, Port 465), OAuth2-SMTP-Authentifizierung und SMTP-Clientzertifikate werden nicht unterstützt. Einmalig aus der Serverkonfiguration übernommene Einstellungen sind gekennzeichnet; danach gelten die hier gespeicherten Werte. Nachrichten in der Warteschlange behalten die Empfänger vom Zeitpunkt der Einreihung, abzüglich inzwischen aus der Gruppe entfernter Empfänger. Das Entfernen eines Kanals storniert seine nicht zugestellten Nachrichten. Zustelleinstellungen, Outbox und Verlauf benötigen die Organisationsdatenbank; ohne sie sind sie nicht verfügbar. Empfänger auf der E-Mail-Sperrliste der Plattform werden übersprungen: Eine Gruppen-E-Mail, deren Empfänger alle gesperrt sind, wird mit diesem Grund abgebrochen, und eine Testnachricht oder Einrichtungs-E-Mail an eine gesperrte Adresse wird nicht gesendet.

20 SIEM-Export

Sicherheitsereignisse dieser Organisation fortlaufend an Ihr SIEM senden.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Melden Sie sich als Admin der Organisation mit Passwort und Authenticator-Code (MFA) an. Oben in der Ansicht steht, ob diese Sitzung die MFA-Anforderung erfüllt; ohne sie sind das Formular und die Schaltflächen Verbindung prüfen, Testereignis senden, Erneut senden ab..., Neues Geheimnis und Entfernen deaktiviert, und der Hinweis sagt genau, was zu tun ist (zum Beispiel: Profil öffnen, MFA aktivieren mit dem aktuellen 6-stelligen Code abschließen und erneut mit Code anmelden). Die Anforderung gilt für die gesamte Sitzung; es gibt kein Zeitfenster.
2. Fügen Sie ein Ziel mit Namen und Kennung (1–64 Kleinbuchstaben, Ziffern und Bindestriche, nach dem Speichern fest) hinzu und wählen Sie dann den Transport (HTTPS, Splunk HTTP Event Collector, Syslog über TLS, Azure Monitor Logs Ingestion für Microsoft Sentinel, OpenTelemetry Logs (OTLP/HTTP) oder Dateiarchiv auf dem Server), ein Format und ein Schemaprofil. Angeboten werden nur die Formate und Profile, die der Server für den gewählten Transport zulässt: HTTPS sendet den JSON-Datensatz (Felder des CERTYX-Journals) oder NDJSON (kanonisches Ereignis); Splunk HEC den JSON-Datensatz oder NDJSON; Syslog über TLS RFC-5424-Syslog mit strukturierten Daten, CEF, LEEF 1.0, LEEF 2.0, Schlüssel=Wert (Generic KV), den JSON-Datensatz oder die CEF- und LEEF-Layouts der ersten Version; Azure Monitor die Zeilen der Microsoft-Sentinel-Tabelle; das Dateiarchiv CSV (kanonisch oder im Layout der ersten Version) oder NDJSON. NDJSON und RFC 5424 bieten die Profile Natives CERTYX-Ereignis, OCSF 1.1.0 (geprüfte Klasse) und ECS 8.11.0, Splunk HEC mit NDJSON zusätzlich Splunk-CIM-Felder; alle anderen Formate verwenden das native Ereignis. Der Kasten Was die Empfangsseite braucht nennt die Empfängereinstellungen für Transport und Format; jedes Feld nennt

sein erwartetes Format, und abgelehnte Eingaben nennen das Feld. Ohne Häkchen bei An dieses Ziel exportieren ist das Ziel pausiert, ohne seine Position zu verlieren. Vor dieser Version gespeicherte Ziele senden weiter dasselbe (plus Ereignis-ID): Beim Bearbeiten sind Transport, Format und Profil vorausgewählt, für die ihre frühere Art steht.

3. Die Schritt-für-Schritt-Einrichtung jedes Formats auf der Empfängerseite und in CERTYX steht im SIEM-Integrationshandbuch: Splunk HTTP Event Collector (Token, Index, Sourcetype, Zertifikat), Cribl Stream (Syslog-TLS-Quelle, Route und Index), ein Splunk-TCP-SSL-Eingang mit Zeilenumbruch-Framing, IBM QRadar (Universal LEEF, TLS Syslog), ArcSight (Syslog NG Daemon SmartConnector mit TLS), Microsoft Sentinel (Datensammlungsendpunkt und -regel, Tabellenspalten, Entra-Anwendung mit der Rolle Monitoring Metrics Publisher) und Webhook-Empfänger mit Code zur Signaturprüfung. Jedes Feld und der Kasten Was die Empfangsseite braucht verlinken auf den passenden Abschnitt, eine fehlgeschlagene Prüfstufe auf ihre Abhilfe, und die Seite des Handbuchs bietet denselben Inhalt als PDF auf Englisch, Deutsch und Polnisch (auch unter Dokumentation).
4. Anmeldeereignisse: Kreuzen Sie unter Zu exportierende Ergebnisse Anmeldeereignisse (Anmeldung, Abmeldung, Sperre, MFA-Änderungen) an oder lassen Sie alle Felder leer. Die Ziele der Organisation erhalten dann jede erfolgreiche und fehlgeschlagene Anmeldung ihrer Benutzer (Passwort, Passwort mit MFA oder Wiederherstellungscode, Firmenanmeldung mit OIDC oder SAML, mobile App), Abmeldungen (auch durch Ablauf, Passwortänderung oder Abmeldung beim Identitätsanbieter beendete Sitzungen), Kontosperren sowie MFA-Einrichtung, -Bestätigung, Zurücksetzen durch einen Administrator und neue Wiederherstellungscodes. Jedes Ereignis nennt die E-Mail-Adresse des Benutzers, die Quell-IP, den User-Agent, die Methode, das Ergebnis (Erfolg oder Fehler) und einen festen Grundcode; das eingegebene Passwort oder der Code wird nie gesendet.
5. Splunk: Wählen Sie den Transport Splunk HTTP Event Collector. Aktivieren Sie in Splunk HEC (Global Settings: All Tokens Enabled, Enable SSL, Port 8088), erstellen Sie ein Token, dessen Allowed indexes den Zielindex enthalten, und geben Sie dann https://<splunk-host>:8088/services/collector/event, den Tokenwert, den Index (zum Beispiel clm) und optional einen Sourcetype ein. Das Format JSON-Datensatz verwendet den Standard-Sourcetype certyx:security; NDJSON (kanonisches Ereignis, Profil nativ, OCSF, ECS oder Splunk-CIM-Felder) verwendet certyx:event und überträgt event_id als indiziertes Feld; geben Sie diesem Sourcetype in props.conf KV_MODE = json. Das HEC-Zertifikat muss auf den Hostnamen ausgestellt sein (Splunks Standardzertifikat SplunkServerDefaultCert wird abgelehnt); eine private CA fügen Sie unter Vertrauenswürdige Stammzertifikate ein.
6. Syslog über TLS: Geben Sie nur den Hostnamen und den Port ein und wählen Sie das Framing: Oktettzählung (RFC 5425; Cribl-Syslog-Quelle, syslog-ng, rsyslog, QRadar, ArcSight) oder Zeilenumbruch (Splunk-Eingang [tcp-ssl:<port>]). Der Empfangseingang muss TLS verwenden. Für LEEF 2.0 geben Sie das LEEF-Trennzeichen ein (ein Zeichen wie ^ oder sein Hexadezimalcode wie x5E; leer bedeutet TAB) und verwenden dasselbe Trennzeichen in der QRadar-Protokollquelle; LEEF 1.0 verwendet immer TAB. Die Zeile unter dem Framing zeigt den vom Serverbetreiber festgelegten Syslog-Kopf (Facility, APP-NAME und IANA-Enterprise-Nummer; ohne Nummer wird kein Strukturdatenelement certyx@ gesendet). Über Cribl wird der Index (zum Beispiel clm) in der Cribl-Route oder -Pipeline gesetzt, nicht von CERTYX.
7. HTTPS (POST eines JSON-Arrays oder NDJSON, HMAC-SHA256 des Inhalts in X-Certyx-Signature) und Azure Monitor Logs Ingestion für Microsoft Sentinel (Datensammlungsendpunkt, unveränderliche ID und Stream der Datensammlungsregel, Microsoft-Entra-Mandant, Anwendungs-ID und geheimer Clientschlüssel) verwenden dasselbe Formular. Bei einem ohne Geheimnis hinzugefügten HTTPS-Ziel

erzeugt CERTYX das Signaturgeheimnis und zeigt es einmal zum Kopieren in den Empfänger an; Neues Geheimnis ersetzt es bei einem HTTPS-Ziel sofort (das bisherige wird ungültig) und zeigt das neue einmal an.

8. OpenTelemetry Logs (OTLP/HTTP): Wählen Sie den Transport OpenTelemetry Logs und das Format OTLP Protobuf (application/x-protobuf, der Standard von OTLP/HTTP) oder OTLP/JSON, geben Sie die vollständige Logs-URL des Empfängers ein (nur https, zum Beispiel https://collector.example.com:4318/v1/logs für den OpenTelemetry Collector), den Inhalt (Body) des Log-Eintrags (die Nachricht oder das ganze kanonische Ereignis als Schlüssel-Wert-Liste), optional einen Namen des Authentifizierungs-Headers (leer ist Authorization) und dessen Wert als Geheimnis (zum Beispiel Bearer <Token>; verschlüsselt gespeichert, nie wieder angezeigt) und Anfragen mit gzip komprimieren. Jeder Stapel ist eine ExportLogsServiceRequest: Ressource service.name certyx, service.version, deployment.environment.name, host.name, host.ip und certyx.organization.id/name/kind; ein Log-Eintrag je Ereignis mit Timestamp, ObservedTimestamp, SeverityNumber/SeverityText (niedrig INFO 9, mittel WARN 13, hoch ERROR 17, sehr hoch FATAL 21), Body, TraceId und SpanId der Anfrage und den Attributen (Semantikkonventionen event.name, user.id, user.name, user.roles, session.id, client.address/port, server.address/port, http.request.method, http.route, http.response.status_code, error.type; certyx.event.id und die übrigen certyx.*-Felder). TLS, vertrauenswürdige Stammzertifikate, Clientzertifikat (mTLS), Sperrprüfung, Zustellrichtlinie, Filter, Prüfung und Testereignis funktionieren wie bei den anderen HTTPS-Transporten; ein Teilerfolg mit abgelehnten Log-Einträgen wird nicht erneut gesendet (OTLP-Spezifikation), sondern als siem.event.rejected mit den Ereignis-IDs der Anfrage und der Meldung des Empfängers protokolliert, mit dem Vorfall siem-rejected; Erneut senden ab sendet die Einträge erneut. Ein Retry-After bei 429 oder 503 wird bis zur längsten Wartezeit beachtet.
9. Feldzuordnung (Netzwerkziele mit kanonischem Format: NDJSON, RFC 5424, CEF, LEEF, Generic KV, OTLP): Regel hinzufügen fügt eine geordnete Regel auf dem kanonischen Ereignis hinzu, bevor es geschrieben wird: Umbenennen (ein kanonisches Feld unter einem neuen Namen), Entfernen (Negativliste), Behalten (Positivliste: mit mindestens einer Behalten-Regel wird jedes andere optionale Feld entfernt) oder Konstante hinzufügen (ein neues Feld mit festem Wert von höchstens 256 Zeichen). event_id, schema_version, die drei Zeitstempel, event_code, category, action, outcome, severity und message können nicht entfernt oder umbenannt werden; ein neuer Name hat 1–64 Buchstaben, Ziffern, Unterstriche und Punkte (CEF nur Buchstaben und Ziffern, ECS und OCSF ohne Punkte), darf nicht mit certyx beginnen und keinem kanonischen Feld oder einem Feld entsprechen, das das Format selbst schreibt (zum Beispiel dst in CEF oder server.address in OTLP). Neue Felder folgen den eigenen Feldern des Formats: inline in JSON, unter labels in ECS, unter unmapped in OCSF, als Erweiterungen in CEF und LEEF, als Schlüssel in KV und als Attribute in OTLP. Höchstens 32 Regeln; sie werden mit dem Ziel gespeichert, versioniert und protokolliert (vorher und nachher). Vorschau des Testereignisses zeigt, was das Formular im aktuellen Zustand für das Testereignis im gewählten Format und in der gewählten Kodierung senden würde (OTLP-Protobuf in seiner JSON-Kodierung, mit der Größe des binären Inhalts); es wird nichts gesendet oder gespeichert, und ungültige Regeln werden mit dem Grund abgelehnt.
10. Speichern Sie und wählen Sie dann Verbindung prüfen (DNS, TCP und TLS, ohne etwas zu senden; bei einem Dateiarchiv, ob sein Verzeichnis beschreibbar ist) und Testereignis senden. Jede Stufe wird mit ihrem Ergebnis aufgeführt: aufgelöste Adressen, verbundene Adresse und Port, TLS-Version sowie Antragsteller, Aussteller und Ablauf des Zertifikats, dann der HTTP-Status oder der Splunk-HEC-Code mit Bedeutung und Abhilfe. Das Testereignis gehört zur Kategorie Integration und hat eine zufällige UUID als event_id, die das Ergebnis nennt; suchen Sie beim Empfänger nach dieser Ereignis-ID (Akteur siem-test). Ein Dateiarchiv hat kein Testereignis.

11. Die Liste zeigt für jedes Ziel Transport, Format und Profil, die Position im Journal, wartende und zugestellte Ereignisse, den letzten Erfolg, den Grund des letzten Fehlers, die Fehler in Folge und den Zeitpunkt des nächsten Versuchs, ein Ereignis, das der Empfänger weiter ablehnt (Sequenz und Versuche), und die letzte Prüfung. Bearbeiten lädt ein Ziel in das Formular: Ein leeres Geheimnis- oder Clientschlüsselfeld behält den gespeicherten Wert, ein Wechsel des Transports erfordert jedoch die erneute Eingabe des Geheimnisses. Entfernen löscht das Ziel samt Position; erneutes Hinzufügen beginnt am Anfang des Journals. Ziele, die der Plattformbetreiber für die Organisation konfiguriert hat, werden schreibgeschützt aufgeführt. Jede Karte listet außerdem die gespeicherte Konfiguration auf: Transport, Format und Profil, Ziel, Framing und Trennzeichen, die gesendeten Ereignisse, die Zustellrichtlinie (Serverstandards als solche benannt), Splunk- und Sentinel-Einstellungen, Stammzertifikate, Clientzertifikat, Sperrprüfung und ob ein Geheimnis gespeichert ist. Beim Öffnen der Ansicht zeigt das Formular das erste Ziel mit seinen gespeicherten Werten; ein gespeichertes Geheimnis oder ein Clientschlüssel wird nie angezeigt und erscheint als „Gespeichert – leer lassen zum Beibehalten“. Bearbeiten öffnet ein anderes Ziel, Neu beginnt ein leeres Formular, und nach dem Speichern behält das Formular das gespeicherte Ziel.
12. Nur senden verringert, was ein Netzwerkziel erhält, um die Lizenznutzung des SIEM zu senken: Die angekreuzten Ergebnisse werden mit oder verknüpft (zum Beispiel Zugriff verweigert, Serverfehler, Anmeldeereignisse sowie Konfigurations- und Geschäftsänderungen, das jedes Ereignis mit einer Konfigurations- oder Geschäftsänderung hinzufügt). Die Kategorien (Authentifizierung, Autorisierung, Benutzerverwaltung, Konfigurationsänderung, Datenzugriff, Administration, Sicherheit, Anwendungsfehler, System, Integration) und die gewählten Codes des Ereigniscode-Katalogs werden untereinander mit oder verknüpft und schränken die Ergebnisauswahl weiter ein. Mindestschweregrad sendet nur Ereignisse ab dem gewählten Schweregrad (empfangen 2, Erfolg 3, abgelehnt 5, verweigert und fehlgeschlagene Anmeldung 7, Serverfehler und Sperre 8). Jede Anfrage hat im Journal zwei Datensätze, einen Empfangsdatensatz vor der Ausführung (kein fehlgeschlagener Versuch) und ein Ergebnis danach; ein Ziel erhält nur das Ergebnis, sofern Empfangene Anfragen nicht angekreuzt ist. Der Empfangsdatensatz bleibt im Journal und in einem Dateiarchiv erhalten. Gesendete Felder (unter Form und Größe) führt jedes Feld des gewählten Formats mit einem Kontrollkästchen auf, sodass ein Ziel genau die angekreuzten Felder erhält und die SIEM-Lizenz nichts anderes zählt; aktiv bleiben nur die vom Format verlangten Felder, und die Kompatibilitäts-Layouts CEF und LEEF der ersten Version sind fest, stellen Sie dort also das Format CEF oder LEEF ein. Health- und Readiness-Prüfungen werden nicht gesendet. Ausgelassene Ereignisse gehen nicht verloren: Sie bleiben im Journal und in einem Dateiarchiv.
13. Das Zielformular hat vier nummerierte Abschnitte: 1 Wohin senden (Name, Transport, Format, Adresse, Geheimnis, TLS), 2 Was senden (Ergebnisse, Kategorien, Ereigniscodes, Schweregrad und die eingeklappten Weiteren Filter), 3 Form und Größe jedes Ereignisses (Vorgabe-Karten, eingeklappte Detaileinstellungen und Feldzuordnung) und 4 Zustellung (eingeklappte Zustellrichtlinie, An dieses Ziel exportieren). Eingeklappte Teile öffnen sich per Klick auf ihren Titel.
14. Weitere Filter: Nur diese Routen senden und Diese Routen nie senden (eine pro Zeile; eine Route umfasst jede Route, die mit ihr beginnt, zum Beispiel /agent/v1/discovery/telemetry für die regelmäßigen Berichte der Agenten), Ereignisse dieser Akteure nie senden (zum Beispiel pending, Anfragen vor der Authentifizierung), Diese Kategorien nie senden und Diese Ereigniscodes nie senden. Ein Ausschluss gilt immer vorrangig.
15. Die Ereignisgestaltung bestimmt, wie groß jedes Ereignis ist, weil viele SIEMs nach indexiertem Volumen abrechnen: Vollständig sendet jedes Feld und den vollständigen Vorher- und Nachher-Zustand jeder Änderung (wie bisher); Ausgewogen sendet nur die geänderten Werte, keine leeren Felder und die Standardfelder; Sparsam sendet Aktion und Kennungen einer Änderung, die minimalen Felder und

höchstens 2 KB pro Ereignis; Benutzerdefiniert verwendet die Detaileinstellungen. Eine Vorgabe füllt die Detaileinstellungen; jede Änderung daran wählt Benutzerdefiniert. Detaileinstellungen: Änderungen (vollständig, nur geänderte Werte, Aktion und Kennungen, keine), Felder (alle, Standard, minimal; Pflichtfelder werden immer gesendet), Leere Felder weglassen, Größtes Ereignis (0 oder 512–1048576 Byte; ein längeres Ereignis verliert Änderungsdetails, dann werden seine längsten Texte gekürzt, und es wird als gekürzt markiert), Stil der Feldnamen und Zeitformat (nur JSON-Dokumente des nativen oder Splunk-CIM-Profils), Syslog-MSGID (standardmäßig Ereigniskategorie, Ereigniscode, eigener Text wie security-journal oder keine) und Syslog-APP-NAME (leer ist clm). Vorschau des Testereignisses zeigt die Größe mit und ohne Gestaltung. Gemessen an einer Agentenbeobachtung von drei Zertifikaten (json): Vollständig 4578 Byte, Ausgewogen 591, Sparsam 378.

16. Zustellrichtlinie (Netzwerkziele): Versuche bis zur kritischen Warnung, Erste und Längste Wartezeit (Sekunden), Stapelgröße und Rückstandswarnung ab; ein leeres Feld verwendet den unter den Feldern angezeigten Serverstandard. Ein fehlgeschlagener Stapel wird mit exponentiellem Backoff und Jitter wiederholt; nach den Versuchen wird der Vorfall siem-delivery kritisch und die Wiederholung geht weiter. Einen Stapel, den der Empfänger wegen seines Inhalts ablehnt, teilt CERTYX bis zum einzelnen abgelehnten Ereignis auf; alles davor wird zugestellt, und dieses Ereignis wird wiederholt und gemeldet. Ein Ereignis überspringen, das der Empfänger weiter ablehnt, ist standardmäßig aus; eingeschaltet wird das Ereignis nach den Versuchen übersprungen und als siem.event.skipped mit seiner event_id protokolliert. Bei einem Rückstand wird nichts verworfen: Das Journal ist die Warteschlange, und oberhalb der Rückstandsgrenze wird der Vorfall siem-backlog ausgelöst.
17. TLS der Netzwerkziele: Das Zertifikat des Empfängers wird immer gegen den Systemspeicher oder die hier eingegebenen Vertrauenswürdigen Stammzertifikate geprüft. Für gegenseitiges TLS geben Sie ein Clientzertifikat (PEM) mit seinem unverschlüsselten privaten Schlüssel (RSA oder EC) ein; der Schlüssel wird verschlüsselt gespeichert und nie wieder angezeigt, und ein leeres Schlüsselfeld behält den gespeicherten Schlüssel, solange das Zertifikat unverändert ist. Sperrprüfung: Soft-Fail (Standard) lehnt ein als gesperrt gemeldetes Zertifikat ab und akzeptiert einen unbekannten Status (keine CRL- oder OCSP-Adresse, Responder nicht erreichbar); Hard-Fail lehnt auch einen unbekannten Status ab.
18. Erneut senden ab… auf der Karte eines Netzwerkziels öffnet einen Dialog: Wählen Sie eine Journalsequenz (1 oder höher) oder Datum und Uhrzeit, lesen Sie, dass jedes Ereignis ab dort erneut gesendet wird, und bestätigen Sie mit Erneut senden. Die Position geht auf kurz vor diesen Punkt zurück, Backoff und Ablehnungszustand werden zurückgesetzt, und der Hinweis nennt die neue Position; der Empfänger muss nach event_id deduplizieren. Die Position rückt nie vor (ein Punkt, den das Ziel noch nicht erreicht hat, wird abgelehnt), ein Dateiarchiv kann nicht erneut senden, und jedes erneute Senden wird mit bisheriger und neuer Position protokolliert (siem.destination.replayed).
19. Das Syslog-Framing muss auf beiden Seiten gleich sein. Oktettzählung sendet jeden Datensatz als <Länge> <Nachricht> (UTF-8-Bytelänge, kein Zeilenumbruch) in einem Schreibvorgang; eine Cribl-Syslog-Quelle braucht dann Octet count framing = Yes (Standard ist No) und eingeschaltetes TLS, eine Quelle je CERTYX-Port, Index und Sourcetype per Eval-Funktion. Ein Empfänger, der an Zeilenumbrüchen trennt, zeigt Bruchstücke wie 412 <84>1 …; ein Empfänger ohne TLS zeigt binäre Ereignisse, die mit \x16\x03 beginnen und seinen eigenen Hostnamen enthalten. Ein erfolgreicher Syslog-Test nennt, was der empfangende Eingang mit dem gewählten Framing tun muss.
20. Dateiarchiv: Wählen Sie den Transport Dateiarchiv auf dem Server (Tagesdateien) und ein Format: CSV (Layout der ersten Version, certyx-security-JJJJ-MM-TT.csv), CSV (kanonisches Ereignis, certyx-events-JJJJ-MM-TT.csv mit versioniertem Kopf) oder NDJSON (ein Dokument des gewählten Profils je Zeile, certyx-events-JJJJ-MM-TT.ndjson). Geben Sie die Aufbewahrung (Tage, 1–3650) ein, kreuzen Sie optional Abgeschlossene Tage mit gzip komprimieren an, speichern Sie und wählen Sie Verbindung

prüfen, das prüft, ob das Archivverzeichnis beschreibbar ist, und die Dateien sowie belegten und freien Speicher zeigt. Das Archiv schreibt jedes Ereignis der Organisation in eine Datei je UTC-Tag im eigenen Bereich der Organisation unter dem vom Plattformbetreiber konfigurierten Archivstamm; Filter, Zustellrichtlinie, Clientzertifikat und Sperrprüfung gelten nicht. Ein abgeschlossener Tag wird versiegelt (optional .gz) mit seinem SHA-256 im Manifest SHA256SUMS, und Tage, die älter als die Aufbewahrung sind, werden gelöscht und protokolliert (siem.archive.expired).

21. Archivdateien auf der Karte des Archivs listet jede Datei mit Größe, Versiegelung und SHA-256; Herunterladen holt eine Datei, Alle herunterladen (ZIP) alle Dateien mit dem Manifest. Prüfen Sie einen Download mit sha256sum -c SHA256SUMS. Downloads erfordern die MFA-Sitzung und werden protokolliert (siem.archive.downloaded).

EINGABEN UND PARAMETER

- Exportierte Felder: Sequenz, Zeit, Ereigniskategorie und Ereigniscode, Organisation, Akteur, Quell-IP, Agent-Fingerabdruck, Methode, Route, HTTP-Status, Ergebnis, Trace-ID, Fehlertyp, geschäftliche Änderungen und der Ereignis-Hash, der den Eintrag im hashverketteten CERTYX-Journal identifiziert.
- CEF-Zuordnung: rt, suser, src, requestMethod, request, outcome, externalId (Sequenz), dvchost (Instanz), cn1 httpStatus, cs1 organization, cs2 traceId, cs3 eventHash, cs4 agentFingerprint, cs5 errorType, cs6 changes; Schweregrad 2–8 je nach Ergebnis. LEEF 2.0 überträgt dieselben Werte als devTime, usrName, src, cat, sev, method, resource, httpStatus, organization, traceId, sequence, eventHash, agentFingerprint, errorType, instance und changes mit ^ als Trennzeichen.
- Anmeldeereignisse (Ergebnis authentication) sind eigene Journaleinträge mit den Namen authentication.sign-in.succeeded, authentication.sign-in.failed, authentication.sign-out, authentication.locked, authentication.mfa.enrolled, authentication.mfa.confirmed, authentication.mfa.reset und authentication.mfa.recovery-codes-regenerated. Methoden: password, password+mfa, password+recovery-code, oidc, saml, mobile-password (mit +mfa oder +recovery-code), mobile-oidc, mobile-saml, mobile-sso und totp. Grundcodes sind unter anderem unknown-account, invalid-credentials, disabled, locked, too-many-failures, mfa-required, mfa-invalid, mfa-enrollment-required, enrollment-expired, sso-required, not-operator, operator-entry, organization-unavailable, organization-mismatch, account-not-allowed, ticket-invalid, device-refused, invalid-request, sso-error, sso-disabled, sso-no-subject, sso-group-overage, sso-not-provisioned, sso-no-role, sso-expired, sso-not-configured, sso-unverified-domain und für Abmeldungen user, credentials-changed, idp-logout, session-ended und administrator-reset.
- Anmeldefelder je Format: Der JSON-Datensatz (Webhook, Syslog-JSON, Splunk-HEC-Ereignis) ergänzt SignIn {Action, User, UserVerified, Organization, Method, Result, Reason, UserAgent}; CEF verwendet den Ereignisnamen als Klassen-ID, suser = E-Mail des Benutzers, suid = Konto, src, outcome = success oder failure, cat = authentication, act = Ereignisname, reason, requestClientApplication = User-Agent, flexString1 authMethod und flexString2 userVerified, mit Schweregrad 3 bei Erfolg, 7 bei Fehler und 8 bei einer Sperre; LEEF verwendet usrName = E-Mail des Benutzers, src, actor, action, authMethod, result, reason, userAgent und userVerified; Sentinel ergänzt die Spalten User, UserVerified (boolean), UserOrganization, AuthAction, AuthMethod, AuthResult, Reason und UserAgent.
- Microsoft Sentinel: Die Spalten des Streams sind TimeGenerated, Sequence, Organization, Actor, SourceIp, AgentFingerprint, Method, Route, Status, Outcome, TraceId, ErrorType, Instance, EventHash und Changes sowie die oben genannten Anmeldespalten (eine Regel, die sie nicht deklariert, speichert nur die übrigen Spalten); die Anwendung benötigt die Rolle Monitoring Metrics Publisher auf der Datensammlungsregel.

- Splunk-HEC-Anfrage: POST mit Authorization: Splunk <token>, X-Splunk-Request-Channel (eine stabile GUID je Ziel) und aneinandergereihten Umschlägen {time, host, source certyx:security-journal, sourcetype, index, event}. Mit Indexer acknowledgement am Token fragt CERTYX /services/collector/ack ab, bis Splunk die Indizierung bestätigt (Clm:Siem:HecAckTimeout, Standard 30 Sekunden); ein unbestätigter Stapel wird erneut gesendet.
- Organisationskennung in jedem Format: JSON, Splunk HEC und Syslog-JSON enthalten Tenant (Organisations-ID), OrganizationName, OrganizationKind (organization, platform oder unattributed) und Instance; CEF ergänzt certyxOrganizationName und certyxOrganizationKind neben cs1 organization und dvchost; LEEF ergänzt organizationName und organizationKind; Sentinel ergänzt die Spalten OrganizationName und OrganizationKind. Name und Art werden beim Export ergänzt; der hashverkettete Journaleintrag bleibt unverändert. Der RFC-5424-HOSTNAME der Syslog-Nachrichten ist die Instanz-ID der CERTYX-Instanz, die das Ereignis erfasst hat.
- Spalten des CSV-Archivs: Sequence, At, OrganizationId, OrganizationName, OrganizationKind, Instance, Actor, SourceIp, AgentFingerprint, Method, Route, Status, Outcome, Severity, TraceId, ErrorType, SignInAction, SignInUser, SignInMethod, SignInResult, SignInReason, Changes, PreviousHash und Hash; UTF-8, Kopfzeile, Zellen in Anführungszeichen, CRLF-Zeilenenden; eine Zelle, die mit = + - @, einem Tabulator oder Wagenrücklauf beginnt, erhält einen Apostroph davor, damit Tabellenkalkulationen sie als Text zeigen.
- Kanonisches Ereignis (NDJSON, CEF, LEEF 1.0/2.0, KV, RFC 5424, kanonisches CSV): event_id (<Installations-ID>:<Sequenz>; eine UUID bei Testereignissen), event_code aus dem Ereigniscode-Katalog, Kategorie, Aktion, Ergebnis, Schweregrad 0–10, Zeit, Organisation, Akteur, Quell-IP und Anfragedetails; die Profile OCSF 1.1.0 (Authentication 3002, Account Change 3001, API Activity 6003, sonst Base Event 0, wenn Pflichtattribute einer Klasse fehlen), ECS 8.11.0 und Splunk-CIM-Felder (Datenmodelle Authentication und Change als indizierte HEC-Felder) bilden dasselbe Ereignis ab. Der JSON-Datensatz, die Sentinel-Zeilen und die Layouts der ersten Version behalten ihre Felder und fügen die Ereignis-ID hinzu.
- Die Anreicherungsfelder trace_id, span_id, src_port, host_ip, dst_ip, dst_port, user_role und session_id sind für Journaleinträge gefüllt, die seit dieser Version erfasst wurden (span_id und dst_port seit der OTLP-Version); ältere Einträge senden sie leer.
- Zieladresse dst_ip und dst_port: bei einer Anfrage die Serveradresse und der Port, die die Verbindung angenommen haben (der Listener des CERTYX-Servers; hinter einem Reverse Proxy oder in einem Containernetz ist das die lokale Schnittstellenadresse mit Port, nicht der öffentliche Name, weil ein weitergeleiteter Host-Header vom Client gesetzt werden kann), bei einem Agenten- oder Endpunktereignis das beobachtete Ziel, das das Ereignis nennt (zum Beispiel der Endpunkt einer Discovery-Warnung); sonst unbekannt. Abgebildet als CEF dst/dpt, LEEF dst/dstPort, ECS destination.ip/port, OCSF dst_endpoint, Splunk CIM dest/dest_port, OTLP server.address/port und dst_ip/dst_port in KV, CSV und NDJSON.

ERGEBNIS

Fortlaufender Export der Ereignisse der Organisation (mindestens einmal) mit dauerhafter Position je Ziel und eine stufenweise Diagnose jedes Ziels. Geheimnisse (HMAC-Schlüssel, HEC-Token, geheimer Clientschlüssel) und Clientschlüssel werden verschlüsselt gespeichert, nie wieder angezeigt und nicht protokolliert; jede Änderung, Prüfung, jeder Test und jedes erneute Senden wird im Sicherheitsjournal erfasst (siem.destination.created, updated, deleted, checked, tested, secret-rotated, replayed), ein

übersprungenes abgelehntes Ereignis als siem.event.skipped mit seiner event_id. Ein Dateiarchiv behält den vollständigen Bestand für seine Aufbewahrung auf dem Server, mit einem SHA-256-Manifest jedes abgeschlossenen Tages, sodass das SIEM weniger erhalten kann (Nur senden).

BERECHTIGUNGEN

Admin der Organisation, dessen Sitzung mit MFA angemeldet wurde: ein lokales Konto mit bestätigtem Authenticator oder eine Unternehmensanmeldung, deren Identitätsanbieter MFA meldet (oder deren Organisation erklärt, dass der Anbieter MFA erzwingt). Andere Rollen sehen diese Ansicht nicht. Änderungen, Prüfungen, Tests, erneutes Senden und neue Geheimnisse werden für Sitzungen der mobilen CERTYX-App abgelehnt.

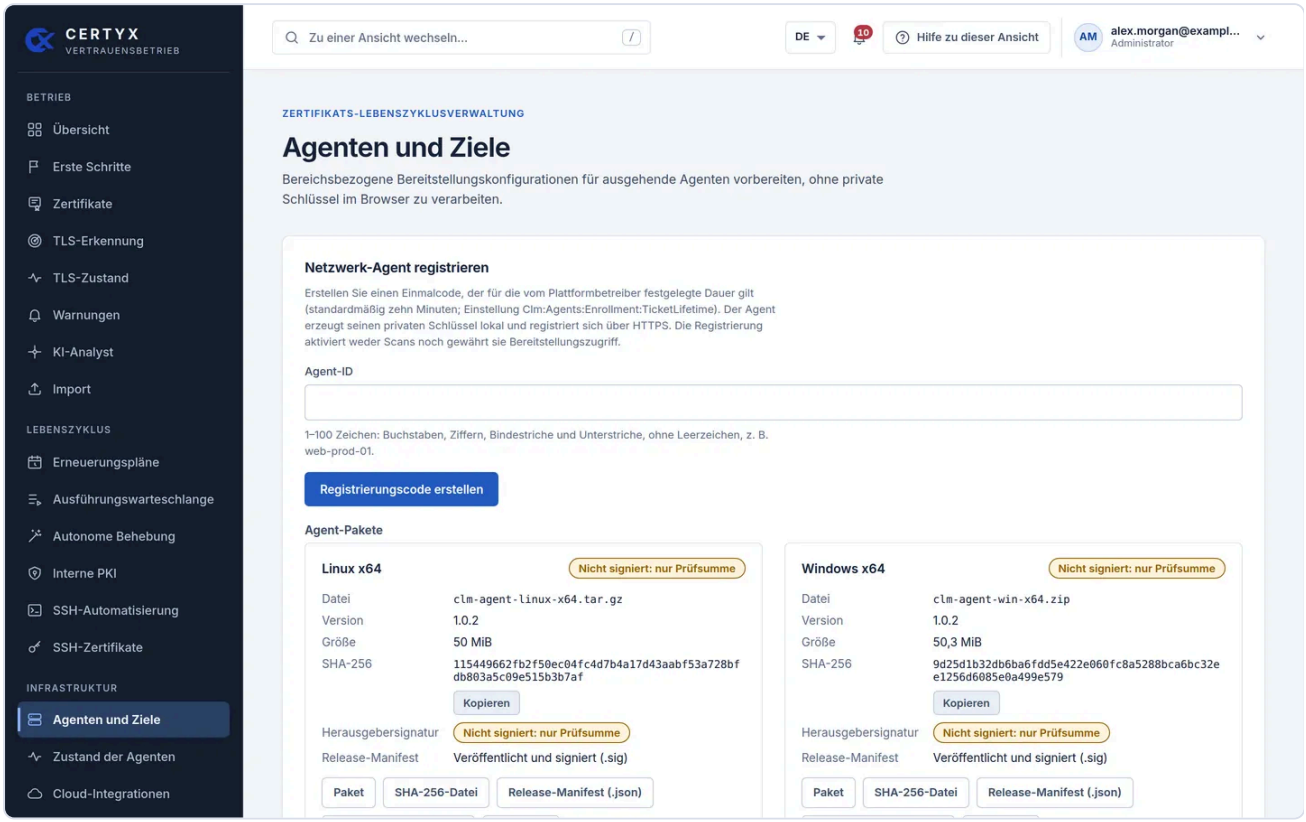
EINSCHRÄNKUNGEN

Erfordert die Plattformdatenbank, die das Sicherheitsjournal enthält; andernfalls zeigt die Ansicht an, dass der Export nicht verfügbar ist. Höchstens Clm:Siem:MaxDestinationsPerOrganization Ziele (Standard 5). Die Zustellung erfolgt mindestens einmal: Ein abgelehnter Stapel wird mit exponentiellem Backoff und Jitter wiederholt (Exportdurchläufe alle Clm:Siem:Interval, Standard 30 Sekunden), und erneutes Senden sendet Ereignisse noch einmal, daher muss der Empfänger nach event_id deduplizieren (<Installations-ID>:<Sequenz>; eine UUID bei Testereignissen). TLS-Zertifikate werden immer geprüft; ein Clientzertifikat wird nur vorgelegt, wenn eines eingegeben ist, und die Sperrprüfung akzeptiert im Modus Soft-Fail einen unbekannten Status, während Hard-Fail ihn ablehnt. Sentinel verwendet die öffentliche Microsoft-Entra-Cloud, sofern der Betreiber nicht Clm:Siem:SentinelAuthorityHost setzt. Ein neues Ziel beginnt am Anfang des aufbewahrten Journals der Organisation. Syslog hat keine Zustellbestätigung: Ein erfolgreicher Syslog-Test belegt nur DNS, TCP, TLS und das Schreiben; Routing und Index müssen beim Empfänger geprüft werden. Reines TCP- und UDP-Syslog wird nicht unterstützt. Eine fehlschlagende Stufe (Name auf dem CERTYX-Server nicht auflösbar, Verbindung abgelehnt oder verworfen, TLS-Handshake, Zertifikatsname oder -vertrauen, HTTP-Status oder HEC-Code) wird mit Abhilfe angezeigt und als letzte Prüfung gespeichert. Ziele unter privaten, Loopback- oder Link-Local-Adressen (zum Beispiel ein interner Splunk- oder Cribl-Empfänger) sind standardmäßig erlaubt (Clm:Siem:AllowPrivateDestinations, Standard true). Der Serverbetreiber einer gemeinsam genutzten Installation kann die Option auf false setzen, um die Ziele von Organisationen auf öffentliche Unicast-Adressen zu beschränken: Dann muss jede Adresse, in die der Host aufgelöst wird, öffentlich sein (abgelehnt werden private, Loopback-, Link-Local-, der gemeinsam genutzte Bereich 100.64.0.0/10, Dokumentations-, Benchmark-, Multicast- und nicht globale IPv6-Bereiche), die Verbindung geht an die geprüfte Adresse, und Weiterleitungen werden nicht befolgt. Die Prüfung endet dann in der DNS-Stufe mit dem Hinweis, dass die Adresse privat ist, und der Export an dieses Ziel schlägt mit demselben Grund fehl (Incident siem-delivery, Position unverändert), bis eine öffentliche Adresse verwendet wird. Die Option beschränkt nie Ziele des Plattformbetreibers oder der Serverkonfiguration. Anmeldeereignisse gehören zur Organisation des Kontos oder der Firmenanmeldung; eine fehlgeschlagene Anmeldung, deren E-Mail-Adresse zu keinem Konto passt, wird der Organisation zugeordnet, zu deren bestätigter Firmenanmeldungs-Domain sie gehört, sonst der Plattform, sodass diese Organisation sie nicht erhält. Vor der Anwendung blockierte Anmeldungen (TLS, Firewall, Ratenbegrenzung am Ingress) werden nicht erfasst, und hinter einem Proxy ist die Quell-IP die Adresse des Proxys. Ein CSV-Archiv wird im Exporttempo geschrieben (Clm:Siem:BatchSize Ereignisse je Clm:Siem:Interval) und nutzt dieselbe dauerhafte Position: Nach einem Absturz setzt es nach der letzten vollständigen Zeile fort, sodass eine Datei keine Zeile doppelt enthält. Planen Sie den Speicherplatz (etwa 0,5–1 KB je Ereignis unkomprimiert, mit gzip etwa ein Zehntel); ein voller Datenträger, ein fehlendes Volume oder ein Archivpfad mit symbolischem Link lässt das Archiv mit dem auf der Karte genannten Grund und dem Vorfall siem-delivery fehlschlagen, und die Position bleibt, bis die Ursache behoben ist. Die Organisation kann den Archivort nicht wählen. Das Entfernen eines Archivs beendet das Schreiben; seine Dateien bleiben, bis der Betreiber

sie löscht. CSV-Archive können nicht in der Serverkonfiguration definiert werden. Der OTLP-Export nutzt nur OTLP/HTTP (kein gRPC) und einen Authentifizierungs-Header; ein Teilerfolg wird nicht erneut gesendet (OTLP-Spezifikation): er wird als siem.event.rejected mit den Ereignis-IDs der Anfrage protokolliert und löst siem-rejected aus, und Erneut senden ab sendet die Einträge nach der Korrektur des Empfängers erneut. Die Feldzuordnung gilt nur für die kanonischen Formate von Netzwerkzielen; Dateiarchive behalten das vollständige Ereignis, und die Formate der ersten Version behalten ihr Layout. Die Anreicherungsfelder trace_id, span_id, src_port, host_ip, dst_ip, dst_port, user_role und session_id sind nur für Einträge vorhanden, die seit dieser Version erfasst wurden (span_id und dst_port seit der OTLP-Version). Die Ziele und das Archiv einer Organisation erhalten nur ihre eigenen Ereignisse. Plattformeinträge erhalten sie nie, auch wenn diese die Organisation betreffen: Aktionen und Anfragen von Betreibern, Sperrung und Wiederherstellung wegen Abrechnung, Bereitstellung und Neuverschlüsselung gespeicherter Geheimnisse. Die Organisation liest sie in ihrer Konsole; das System verlassen sie nur über die eigenen Bereiche der Plattform, die der Plattformbetreiber einrichtet.

21 Agenten und Ziele

Bereichsbezogene Bereitstellungskonfigurationen für ausgehende Agenten vorbereiten, ohne private Schlüssel im Browser zu verarbeiten.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Geben Sie eine Agent-ID ein und wählen Sie „Registrierungscode erstellen“. Die Konsole zeigt die Frist des Codes (einmalig; standardmäßig zehn Minuten; der Plattformbetreiber ändert sie mit Clm:Agents:Enrollment:TicketLifetime), die Adresse, die Agents verwenden müssen (den konfigurierten Agenten-Host und -Port, sonst die HTTPS-Adresse dieser Konsole), Ihre Organisations-ID und nummerierte Installationsschritte mit kopierfertigen Befehlen für Linux (systemd, x64) und Windows (x64): Verwendet die Agent-Adresse die eigene CA des Betreibers, laden Sie zuerst deren Stammzertifikat herunter und prüfen die neben dem Befehl angezeigte SHA-256-Prüfsumme (unter Linux vertrauen ihm die folgenden Downloads desselben Terminals, und das Installationsprogramm fügt es über CLM_AGENT_TRUST_ROOT selbst dem System-Zertifikatsspeicher hinzu und entfernt es wieder, wenn seine Verbindungsprüfung fehlschlägt; unter Windows importiert der Schritt es vor dem Download in den Computerspeicher); die heruntergeladene clm-enrollment.token in ein leeres Arbeitsverzeichnis auf dem Server kopieren; dort das Paket herunterladen (das Archiv wird nur mit einem gültigen Registrierungscode ausgeliefert, den der Befehl aus der Datei liest, oder an eine angemeldete Konsolensitzung über deren eigene Download-Links; ein fehlender, abgelaufener oder verbrauchter Code oder eine falsche Organisations-ID endet mit HTTP 401 und erfordert einen neuen Code), Prüfsumme prüfen, Herausgebersignatur mit verify-agent-package prüfen (ersetzen Sie <PUBLISHER-SHA256> in den Befehlen durch den Fingerabdruck des Herausgeberzertifikats von Ihrem CLM-Anbieter; die Konsole zeigt ihn nie an), entpacken, im Verzeichnis clm-agent das

Installationsprogramm mit ../clm-enrollment.token (Windows ..\clm-enrollment.token) und die Statusprüfung ausführen (unter Linux sudo clm-agent status). Laden Sie die Token-Datei im ersten Schritt herunter; sie wird nie angezeigt. Unter den Schritten verfolgt die Konsole den neuen Agenten: Warten auf die Registrierung, registriert und Warten auf den ersten Kontakt, dann „erster Kontakt empfangen“ mit Uhrzeit.

2. SSH-Workload: Derselbe Agent führt die SSH-Automatisierung aus. Erteilen Sie „SSH-Vorgänge“ (und für Installationen „Bereitstellung von SSH-Identitäten“) hier oder unter SSH-Automatisierung → SSH-Agent installieren und verbinden; dort stehen auch die Downloads, die Host-Befehle (configure-ssh-linux.sh / configure-ssh-windows.ps1 init, add-profile, trust-user-ca) und der Bericht des SSH-Workloads jedes Agents. sudo clm-agent status gibt die erteilten Berechtigungen aus.
3. Unter „Agent-Pakete“ zeigt die Konsole eine Karte je Plattform (Linux x64, Windows x64) mit dem Dateinamen des Archivs, der Release-Version, der Größe, dem SHA-256-Wert (mit Kopieren-Schaltfläche), dem Stand der Herausgebersignatur („Signiert (.p7s veröffentlicht)“ oder „Nicht signiert: nur Prüfsumme“) und dem Stand des Release-Manifests sowie einer Download-Schaltfläche für jede Datei, die der Server veröffentlicht: das Paket, seine .sha256-Datei, die .p7s-Signatur, einen .tsr-Zeitstempel, das Release-Manifest mit seiner .sig-Signatur und den separaten Prüfer (verify-agent-package.sh oder verify-agent-package.ps1). Jede Schaltfläche speichert die Datei unter ihrem eigenen Namen. Die Karte zeigt, welche Signaturdateien veröffentlicht sind; sie prüft sie nicht, das übernimmt der Prüfer auf dem Host. Ein Paket, das der Betreiber nicht veröffentlicht hat, wird als „Auf diesem Server nicht veröffentlicht“ mit dem Veröffentlichungsschritt des Betreibers statt eines Links angezeigt. Vergleichen Sie den SHA-256-Wert der Karte mit sha256sum (Linux) oder Get-FileHash (Windows) der heruntergeladenen Datei. Das Archiv selbst erfordert einen gültigen Registrierungscode (die Befehle der Konsole) oder eine angemeldete Konsolensitzung, Prüfsummen, Signaturen und Prüfer sind öffentlich. Prüfen Sie es gegen den Fingerabdruck des Herausgeberzertifikats, den Sie von Ihrem CLM-Anbieter über einen unabhängigen Kanal erhalten haben; installieren Sie kein abgelehntes Paket. Folgen Sie der verlinkten Installationsanleitung und übergeben Sie denselben Fingerabdruck an das Installationsprogramm (CLM_AGENT_PUBLISHER_SHA256 oder -PublisherSha256); verwenden Sie eine vertrauenswürdige HTTPS-Adresse der Steuerungsebene.
4. Führen Sie die Befehle vor Ablauf der angezeigten Frist auf dem Zielserver aus: Die Gültigkeit umfasst Download und Installation zusammen; die Prüfung beim Download verbraucht den Code nicht, erst die Registrierung. Das Installationsprogramm prüft jedes Argument, bevor es etwas ändert, und nennt ein falsches Argument mit dem nächsten Schritt (fehlende Token-Datei, Platzhalter oder Beispieladresse, Adresse ohne HTTPS, bestehende Installation). Dann prüft es die Verbindung, ohne den Code zu verbrauchen (Namensauflösung, TCP, TLS-Vertrauen einschließlich Online-Sperrprüfung, Uhrzeitabweichung, ob die Adresse Agents bedient), und stoppt mit der Ursache des ersten fehlgeschlagenen Schritts, erklärt Registrierungsfehler (abgelaufener oder verbrauchter Code) und prüft am Ende, dass CERTYX die neue Identität akzeptiert und ihren ersten Kontakt erfasst hat. Führen Sie die Statusprüfung jederzeit erneut aus: Jede Zeile muss mit [OK] beginnen und die letzte „Result: connected“ lauten; eine [FAIL]-Zeile nennt die Ursache und den nächsten Schritt, und die Installationsanleitung beschreibt jede Meldung unter Fehlerbehebung. Nur wenn Ihr Betreiber einen Release-Signaturschlüssel veröffentlicht, geben Sie ./release-signing.pub als viertes Linux-Argument an (täglicher clm-agent-update.timer) oder unter Windows -ReleaseKeyFile .\release-signing.pub (tägliche geplante Aufgabe CERTYX Agent Update, LocalSystem); das aktiviert automatische signierte Updates.
5. Voraussetzungen der Agent-Adresse: HTTPS, vom Agent-Host erreichbar, ein Zertifikat für genau diesen Hostnamen bzw. diese Adresse, dem der Host vertraut und dessen Sperrliste er abrufen kann, und Uhren mit höchstens wenigen Minuten Abweichung. Ist die Konsole über unverschlüsseltes HTTP ohne konfigurierten Agenten-Host (zum Beispiel das lokale ./start.sh) oder über einen Proxy ohne ihn

geöffnet, wird keine Agent-Adresse angeboten und die Ansicht erklärt den Grund. Für einen lokalen Test starten Sie CERTYX mit CLM_AGENT_HOST=<Adresse dieses Computers, die der Agent-Host erreicht> ./start.sh: Es fügt einen HTTPS-Listener für Agents mit lokaler CA und Sperrliste hinzu, und die Konsole zeigt dann die Adresse und den Vertrauensschritt. Der Agent erzeugt einen lokalen privaten Schlüssel und registriert seine öffentliche Identität; Discovery ist standardmäßig erlaubt. Registrierte Agents zeigen den ersten und letzten Kontakt oder dass noch kein Kontakt eingegangen ist. Der Agent meldet beim Start und danach stündlich (NetworkMapIntervalMinutes) eine Netzwerkkarte: die privaten IPv4-Netzwerke seiner Schnittstellen und Routing-Tabelle sowie private Nachbaradressen. Öffentliche Bereiche werden nie gemeldet oder vorgeschlagen.

6. Wählen Sie unter Automatische Netzwerkerkennung den Agent. Erkannte Netzwerke listet die gemeldeten Netzwerke; verwenden Sie Zum Umfang hinzufügen pro Netzwerk oder Alle hinzufügen (privat). Netzwerke, die breiter als das erlaubte Präfix sind (Standard /16), können nicht hinzugefügt werden; geben Sie engere Bereiche ein. Ergänzen Sie Ausschlüsse und geben Sie öffentliche Bereiche nur manuell ein, wenn sie Ihnen gehören. Die Erneuerungsbereitschaft nutzt die gemeldeten Netzwerke ebenfalls: Enthält genau das Netzwerk eines Agenten die Adresse, an der ein Zertifikat beobachtet wurde, und hat dieser Agent den Lebenszyklusprozess, wird er als installierender Agent eines neuen Ziels vorgeschlagen.
7. Wählen Sie den Modus: Standard prüft auf den Erreichbarkeitsports, welche Hosts erreichbar sind, und versucht dann die gängigen TLS-Ports; Vollständig versucht zusätzlich jeden verbleibenden TCP-Port 1–65535 auf erreichbaren Hosts. Legen Sie die Verbindungsversuche pro Sekunde (1–2000), die gleichzeitigen Verbindungen pro Host (1–4), die Batch-Limits und optional wöchentliche Scan-Zeitfenster fest (Tage, von, bis, IANA-Zeitzone; ein Ende vor dem Beginn reicht in den nächsten Tag, 24:00 endet um Mitternacht; ohne Zeitfenster jederzeit).
8. Prüfen Sie vor dem Speichern „Was ein Durchlauf prüft“ unter den Ports. Die Übersicht zählt die Adressen eines Durchlaufs genau wie der Agent (Bereiche mit 4 oder mehr Adressen lassen Netz- und Broadcast-Adresse aus, Überlappungen zählen einmal, Ausschlüsse werden abgezogen) und schätzt die Dauer bei der genehmigten Rate: die Erreichbarkeitsprüfung (jede Adresse wird auf den Erreichbarkeits-Ports geprüft, bis einer antwortet; eine Adresse ohne Antwort wartet pro Port das Verbindungs-Timeout der Agents ab, standardmäßig 500 ms, Clm:Discovery:AgentDefaults:ConnectTimeoutMilliseconds), die üblichen TLS-Ports pro erreichbarem Host und im vollständigen Modus jeden weiteren TCP-Port pro erreichbarem Host. Beispiel bei 50 Versuchen pro Sekunde: Ein /24 (254 Adressen) braucht 5–25 s für die Erreichbarkeit und deutlich unter einer Sekunde pro erreichbarem Host für 16 übliche Ports, der vollständige Modus dagegen mindestens etwa 22 Minuten pro erreichbarem Host und bis zu etwa 9 Stunden für einen Host, dessen Firewall Verbindungen verwirft statt sie abzulehnen; antworteten alle 254 Adressen, dauerte ein vollständiger Durchlauf Tage. Beginnen Sie mit dem Standardmodus und führen Sie den vollständigen Modus in einem Scan-Zeitfenster außerhalb der Arbeitszeit aus. Ein Umfang ohne zu prüfende Adresse wird abgelehnt; eine einzelne Adresse auf .0 oder .255 (etwa 10.10.10.0/32, die Netzadresse von 10.10.10.0/24) und das Speichern eines Profils im vollständigen Modus verlangen eine Bestätigung mit der Schätzung.
9. Der vollständige Modus, ein Bereich kürzer als /20 oder ein öffentlicher Bereich öffnet einen Hinweis, der bestätigt werden muss: Die vollständige Erkennung verbindet sich mit jeder Adresse und jedem Port, daher werden Systeme zur Angriffserkennung sie sehen und können den Agent blockieren oder Ihr Sicherheitsteam alarmieren. Stimmen Sie den Scan mit Ihrem Sicherheitsteam ab und nennen Sie die Adressen des Agents, die Zeitfenster und die Rate, damit es ihn als genehmigten Scanner registrieren

kann. Der Server speichert, wer wann bestätigt hat; das Profil zeigt es an. Ein solches Profil wird ohne Bestätigung nicht gespeichert. Eine frühere Bestätigung bleibt gültig, solange Sie nichts hinzufügen, das eine neue erfordert.

10. Aktivieren Sie das Profil und speichern Sie. Der Erkennungsfortschritt zeigt die Phase (Erreichbarkeit, gängige Ports, alle Ports), den Fortschritt, erreichbare Hosts, gefundene Zertifikate, das Warten auf ein Scan-Zeitfenster (mit dem nächsten Zeitfenster) und eine reduzierte Rate nach vielen Verbindungs-Zeitüberschreitungen. Der erste vollständige Durchlauf eines Umfangs ist die Ausgangsbasis und löst keine Warnungen aus; danach erscheinen unbekannte Zertifikate, ersetzte Zertifikate und neue TLS-Endpunkte unter Warnungen. Änderungen an Netzwerken, Ausschlüssen, Modus oder Ports starten eine neue Ausgangsbasis; Änderungen an Rate, Zeitfenstern oder Batch-Limits nicht. Nach einem Durchlauf zeigen der Fortschritt und das Agent-Protokoll (journalctl -u clm-discovery.service) dessen Ergebnis: geprüfte Adressen, antwortende Adressen und gefundene TLS-Zertifikate; der Scanverlauf unter TLS-Erkennung (Discovery) behält jeden Durchlauf.
11. Unix-Lebenszyklus-Agenten erfordern nur für den Eigentümer zugänglichen Zustand, Secret-Dateien und Ausführungsjournale ohne symbolische Pfade oder symbolische übergeordnete Verzeichnisse. Unsichere oder übergroße Journale stoppen die Ausführung für einen Abgleich durch den Administrator. Beim Start werden die Berechtigungen eines bestehenden Zustandsverzeichnisses nicht geändert. Unter Windows wendet der Agent dieselbe Regel über ACLs auf Secret-Dateien und Journale an: Nur LocalSystem, Administratoren oder die eigene Identität des Agenten dürfen sie besitzen und darauf zugreifen; alles andere wird abgelehnt. Das Windows-Installationsprogramm schränkt die ACL des Agentenverzeichnisses entsprechend ein.
12. Unix-Lebenszyklus-Agenten können genehmigte Text-Secrets aus Azure Key Vault, AWS Secrets Manager und Google Secret Manager über die kundenlokale CLI-Identität des Anbieters auflösen. Konfigurieren Sie exakte SecretBindings und führen Sie Clm.Agent secret-check mit der geschützten Lebenszyklus-Konfiguration als Dienstidentität aus, bevor Sie die Ausführung aktivieren. Die Werte bleiben lokal und werden nie ausgegeben. Siehe CUSTOMER-VAULTS.en.md. Die Auflösung über Provider-CLIs läuft nur auf Unix-Agenten; unter Windows stehen nur Secrets aus geschützten Dateien zur Verfügung. Private Schlüssel werden in Software auf dem Agent-Host erzeugt und gehalten (kein HSM), und der Agent versendet keine E-Mails vom Kundenhost.
13. HashiCorp Vault KV wird ebenfalls über eine exakte HTTPS-Bindung mount/path#field und einen kundenlokalen nativen Token-Helper unterstützt. TLS-Verifizierung ist erforderlich; Namespaces werden nicht unterstützt. Ein Lesevorgang schlägt fehl, wenn der Zugriff verweigert wird, die Identität widerrufen ist oder dem Vault-Zertifikat nicht vertraut wird. Das Vault-Token stammt aus dem Token-Helper des Kunden; CERTYX erstellt oder erneuert keine Vault-Identitäten.
14. Für eine kundengesteuerte entfernte KRL-Übertragung führen Sie ssh publish-krl mit geschützter Publisher-Konfiguration aus und stellen nur dessen öffentlichen Umschlag über eine separate HTTPS-Relay-Identität bereit. Führen Sie ssh sync-krl mit einem geschützten Consumer-Abonnement aus. Signierte Veröffentlichungen laufen nach einer Stunde ab und werden automatisch aktualisiert; Weiterleitungen, fehlerhaftes Vertrauen, übergroße Daten, Manipulationen und abgelaufene Veröffentlichungen werden abgelehnt. Bestehende Widerrufe bleiben nach Fehlern erhalten. OpenSSH erzwingt den Ablauf des Umschlags nicht selbst. Den Zustand melden zentral nur Consumer, die für die KRL-Meldung registriert sind; CERTYX legt nicht fest, welche Hosts die KRL verwenden sollen. Alte Umschläge ohne signierte Zeitgrenzen müssen erneut exportiert werden. Eine neue CA kann vor der Ausstellung eine leere KRL initialisieren; der Verlust der KRL bei einer bereits verwendeten CA erfordert eine Wiederherstellung.

15. Für zentrale Sichtbarkeit registrieren Sie eine separate Consumer-Identität und aktivieren ausdrücklich die KRL-Consumer-Berichterstattung; sie gewährt keine Berechtigung zur SSH-Ausstellung oder Host-Installation. Führen Sie ssh monitor-krl mit der geschützten Identitäts- und Abonnementkonfiguration aus. Agent-Zustand zeigt die gemeldete Revision, den Ablauf der signierten Veröffentlichung, Synchronisierungsfehler und versäumte Berichtsfenster; eine fehlerfreie Erkennung kann einen KRL-Fehler nicht verdecken. Die Plattformüberwachung umfasst diese Agent-Fehler. Es handelt sich um authentifizierte Beobachtungen des Agenten, nicht um einen unabhängigen Nachweis, dass jeder Host die widerrufene Identität ablehnt. Verwenden Sie eine registrierte Identität je Consumer.
16. Gespeicherte Lebenszyklus-Ergebnisse werden nach vorübergehenden Verbindungsfehlern, Anforderungs-Timeouts und HTTP 408/429/500/502/503/504 erneut übertragen, unter Verwendung von PollSeconds und der Grenze OperationTimeoutSeconds. Derselbe Auftrag, dieselbe Lease und dasselbe Ergebnis werden wiederverwendet; Ausstellung und Installation werden nie wiederholt. Die Wiederherstellung nach einem Neustart verlängert die Lease, während das gespeicherte Ergebnis zugestellt wird. Fehler bei Authentifizierung, Autorisierung, abgelaufene/abgeglichene Leases und TLS-Vertrauensfehler stoppen für einen Abgleich. Eine verlorene Lease kann durch diesen Mechanismus nicht verlängert werden; ein Ausfall, der die Lease- oder Operationsgrenze überschreitet, erfordert weiterhin einen Abgleich durch den Administrator.
17. Alle JSON-Konfigurationsleser des Agenten lehnen vor der Deserialisierung symbolische Dateien oder übergeordnete Verzeichnisse, Unix-Gruppen-/Andere-Berechtigungen, Dateien über 1 MiB und ungültiges UTF-8 ab. Schützen Sie die Konfiguration unter Unix mit chmod 600. Relative Befehlszeilenpfade werden in einen absoluten Pfad aufgelöst und denselben Prüfungen unterzogen. UTF-8 mit oder ohne BOM wird unterstützt. Einstellungen und asynchrone Leser verwenden dieselben Regeln; Fehlerausgaben enthalten keine Konfigurationswerte. Unter Windows lehnen die Leser eine Datei ab, die ein anderer Prinzipal als LocalSystem, Administratoren oder die eigene Identität des Agenten besitzt, lesen oder ändern kann; richten Sie vor der Bereitstellung restriktive ACLs ein.
18. Private Endpunkte können einen separat registrierten Endpunkt-Prüfer verwenden. Der Operator bindet dessen ID an das Ausführungsziel; wählen Sie unter Registrierte Agents beim Installer „Ausführung des Zertifikatslebenszyklus aktivieren" und bei einer anderen Agent-Identität „Unabhängige Endpunktverifizierung aktivieren". Der Prüfer kontrolliert genehmigte lokale TLS/HTTP-Endpunkte, bevor ein Erfolg akzeptiert wird. Die Einrichtung ist ein Befehl auf dem Prüfhost: Die Zielkarte unter Ausführung → Bereitstellungsziele zeigt Unabhängigen Endpunkt-Prüfer einrichten mit der Erteilung, Prüfumfang herunterladen (Ziel-ID, Prüfhost, Port, Health-Pfad und Vertrauensanker des Ziels; nur öffentliche Daten) und dem Befehl configure-verifier-linux.sh add-target (Linux, clm-endpoint-verifier.service unter dem Agent-Konto) bzw. configure-verifier-windows.ps1 add-target (Windows, geplante Aufgabe CERTYX Endpoint Verifier als LOCAL SERVICE). Das Skript schreibt die nur für den Besitzer lesbare Konfiguration aus der eigenen Identität des Agents, führt einen geprüften Zyklus aus, startet den Dienst und wartet bis zu zehn Minuten auf die Erteilung, solange CERTYX mit HTTP 403 antwortet; remove-target, disable und status verwalten ihn, das Deinstallationsprogramm entfernt ihn. Ein neuer Agent erhält die Rolle bei der Installation (CLM_AGENT_ENDPOINT_VERIFIER unter Linux, -EndpointVerifierTarget unter Windows). Ohne Vertrauensanker im Ziel muss der Prüfhost der ausstellenden CA selbst vertrauen.
19. Registrierte Installer melden ihre eigene Lebenszyklus-Workload (startet, inaktiv oder Fehler). Versäumte Meldungen bleiben auch bei fehlerfreier Erkennung sichtbar. Der Prozesszustand ersetzt weder das Ausführungsergebnis noch den unabhängigen Endpunktnachweis. Prüfen Sie die geschützten lokalen Journale, wenn ein Zyklus für einen Abgleich anhält.

20. Die Erkennung wiederholt vorübergehende Fehler bei der Identitätsrotation und Kommunikation nach Settings.RetrySeconds. Fehler bei Authentifizierung, Autorisierung und TLS-Vertrauen stoppen den Worker; --once gibt einen Fehler zurück. Konfigurieren Sie nur für den Eigentümer zugängliche Zustands- und Sperrpfade. Ein Berichtsausfall kann die Diagnose verzögern; überwachen Sie auch ausbleibenden Kontakt.
21. Zielentwürfe: Speichern Sie einen Entwurf (Agent, Ziel-ID, DNS-Namen, CA-Typ und -URL, Vault-Mount und -Rolle, Verifizierungsendpunkt, Laufzeit, Bereitstellungsconnector und Installation; für ein SSH-Relay zusätzlich Remote-Host, SSH-Konto und Port), laden Sie sein Konfigurationspaket für den Agentenhost herunter und wählen Sie Ziel aus diesem Agenten erstellen, um das Bereitstellungsziel der Organisation mit demselben Umfang und Installationsmodus unter Ausführung anzulegen. Das Paket enthält die dokumentierten Standarddateien und -befehle des Connectors und für ein Relay das Remote-Objekt und RelayDestinations; ersetzen Sie seine Platzhalter (SET-HOST-KEY-FINGERPRINT, SET-ACCOUNT-EMAIL, YOUR-CLM-HOST) vor der Installation. Die Erstellung wird abgelehnt, wenn ein Ziel mit dieser ID existiert oder der Entwurf die Zielvalidierung nicht besteht; spätere Änderungen (z. B. Vertrauensanker einer privaten CA) nehmen Sie unter Ausführung vor.
22. SSH-Relay zu Hosts ohne Agent: Gewähren Sie dem Relay-Agenten Ausführung des Zertifikatslebenszyklus aktivieren. Führen Sie auf dem Remote-Host configure-relay-host-linux.sh aus dem Agentenpaket mit dem öffentlichen Schlüssel des Relays und dem von Clm.Agent relay-helper ausgegebenen Helfer aus (Konto nur mit Schlüssel-Anmeldung, authorized_keys mit restrict und from=, Helfer, erlaubte Verzeichnisse, minimale sudoers-Regel); legen Sie den ausgegebenen Host-Schlüssel-Fingerabdruck in HostKeyFingerprints und in der known_hosts-Datei auf dem Relay fest; führen Sie dann Clm.Agent relay-check aus. SSH-Identität und known_hosts-Datei des Relays bleiben nur für den Besitzer lesbar auf dem Relay und werden nie an CERTYX gesendet; Meldungen enthalten nur den Namen des Remote-Hosts. Schritt für Schritt: Installationsanleitung des Agenten, „SSH-Relay“.
23. Jeder registrierte Agent zeigt seine Diagnose (Ursache und Erklärung, mit Warum, und was zu tun ist zum Agentenzustand) und seinen letzten Erkennungsdurchlauf (Beginn, Status, aktive Hosts, gefundene Endpunkte und Zertifikate, mit Scanverlauf).

EINGABEN UND PARAMETER

- Organisationsbezogene Einstellungen; private Schlüssel oder CA-Anmeldedaten werden nicht angenommen.
- Schlüssel-/Bereitstellungsstammverzeichnisse müssen absolut und frei von Links sein. Private Schlüssel und Wiederherstellungsjournale erfordern Berechtigungen nur für den Eigentümer; verlinkter/gemeinsam genutzter/übergroßer Zustand wird abgelehnt. Nur der verwaltete UUID-Link der aktuellen Generation ist zulässig.
- Die Erkennungsgrenzen stammen aus der Serverkonfiguration Clm:Discovery:AgentLimits (Standard: Präfix mindestens /16, höchstens 65.536 Adressen pro Bereich und 262.144 pro Profil, 64 Bereiche, 256 Ausschlüsse); Standardports, Rate und Zeitzone stammen aus Clm:Discovery. Loopback-, Link-Local-, Multicast- und reservierte Bereiche werden abgelehnt. Gescannt wird nur IPv4; IPv6-Nachbarn dienen nur als Erreichbarkeitshinweise.
- Formate (jedes Feld zeigt seine eigene Hilfe): Agenten- und Ziel-IDs 1–100 Buchstaben, Ziffern, Bindestriche und Unterstriche (web-prod-01); Netze und Ausschlüsse ein IPv4-CIDR pro Zeile mit Netzwerkadresse (10.20.0.0/16, eine einzelne Adresse als 10.20.0.1/32); Ports als Liste wie 443, 8443 (1–64 gängige, 1–16 Erreichbarkeitsports, jeweils 1–65535); Zeiten der Scan-Fenster HH:mm (24:00 nur als Ende); IANA-Zeitzone wie Europe/Berlin; DNS-Namen ohne Platzhalter, URLs, Ports oder IP-Adressen; CA-API-URL beginnend mit https://. Netzwerkprofil: Verbindungsversuche pro Sekunde 1–

2000, Gleichzeitige Verbindungen pro Host 1–4; unter Batch-Limits Parallele Verbindungen 1–64, Versuche pro Durchlauf 1–10000 und Pause zwischen Durchläufen 10–86400 Sekunden. Zielentwürfe: Prüf-Port 1–65535 und Zertifikatslaufzeit in Stunden 1–8760.

ERGEBNIS

Im Prüfprotokoll erfasste, dauerhaft gespeicherte Administrationskonfiguration.

BERECHTIGUNGEN

Administratoren erstellen Registrierungscodes, sehen registrierte Agents und erkannte Netzwerke, gewähren oder entziehen Fähigkeiten, widerrufen Agents, bearbeiten Netzwerkprofile und speichern Zielentwürfe oder erstellen daraus Ziele. Andere angemeldete Benutzer der Organisation sehen nur die Konfigurationsentwürfe für Ziele und einen Hinweis, dass Administratoren den Rest verwalten; Zustand der Agenten bleibt für sie verfügbar.

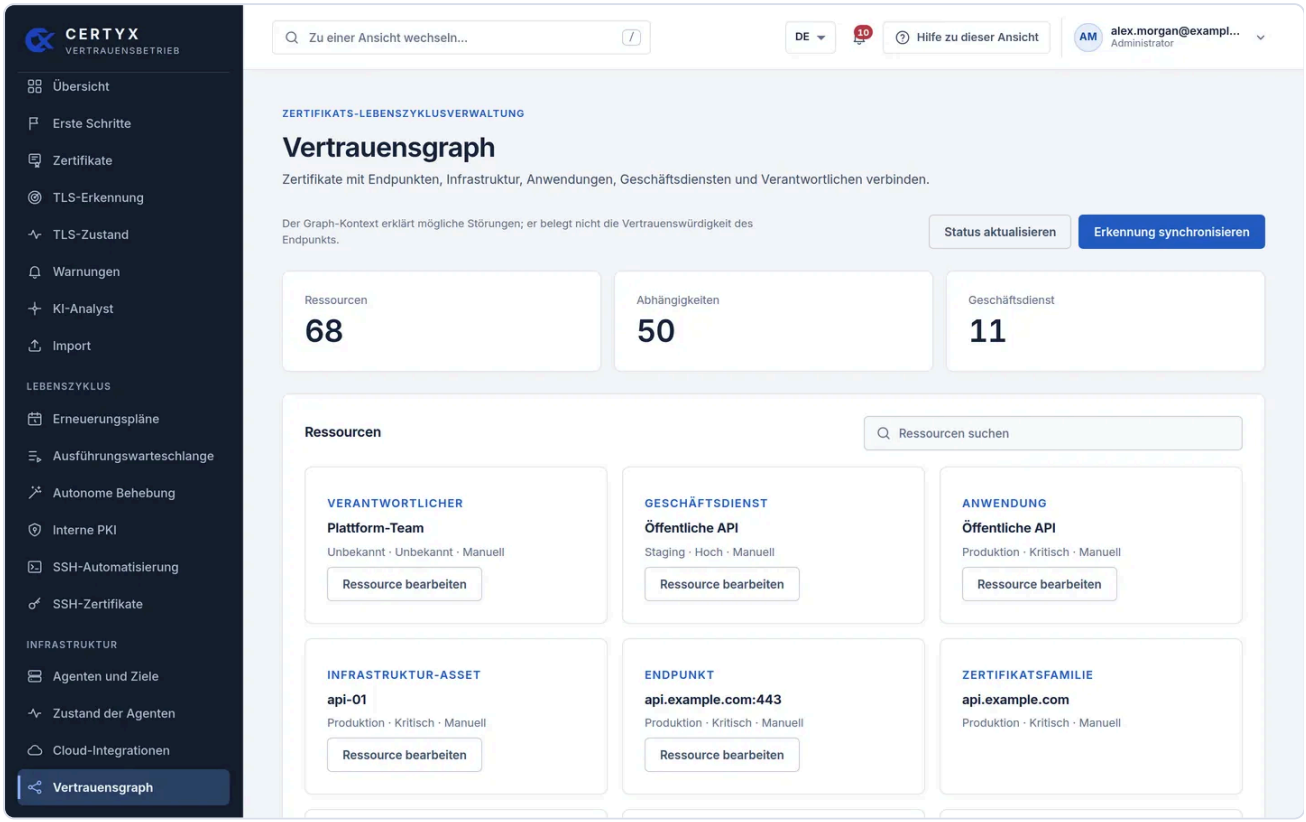
EINSCHRÄNKUNGEN

Die direkte TLS-Erkennung unterstützt IPv4-TCP. Der Agent scannt in einer festen, dokumentierten Reihenfolge mit gleichmäßiger Rate; Rate, Zeitfenster und die reduzierte Rate nach Zeitüberschreitungen begrenzen die Last in Ihrem Netzwerk und sollen den Scan nicht vor Sicherheitswerkzeugen verbergen. Der Server prüft jede Beobachtung erneut gegen das genehmigte Profil. Zur Diensterkennung sendet der Agent nach dem TLS-Handshake eine HEAD-/-HTTP/1.1-Anfrage an einen Endpunkt, der ein HTTP-Protokoll ausgehandelt hat (oder keines auf einem HTTP-Port; h2-Endpunkte erhalten sie über eine weitere HTTP/1.1-Verbindung), oder liest die SMTPS-, IMAPS- oder POP3S-Begrüßung; Settings.ServiceIdentification.IdentifyServices false in der Scan-Konfiguration schaltet das ab. Der Agent prüft keine UDP- oder STARTTLS-Dienste und zählt keine virtuellen SNI-Hosts auf. Eine Agent-ID kann nur einmal registriert werden: Ein Code für eine bereits registrierte ID wird abgelehnt, ein Ersatz-Agent braucht daher eine neue ID; entfernen Sie die alte Installation zuerst mit uninstall-linux.sh (in /opt/clm-agent/current) oder uninstall-windows.ps1, die jede von den CERTYX-Skripten angelegte Unit oder Aufgabe, Datei, jeden Vertrauensanker und das Konto löschen. Wenn der Betreiber einen Release-Signaturschlüssel veröffentlicht, enthalten Releases zusätzlich ein offline signiertes Manifest: Prüfen Sie es vor der Installation mit verify-release.sh (unter /downloads/ der Konsolenadresse und einer separaten Agent-Adresse, zusammen mit den Paketen, ihren Signaturdateien und verify-agent-package.sh/.ps1); mit dem Release-Schlüssel installierte Linux- und Windows-Agenten aktualisieren sich täglich selbst (Linux clm-agent-update.timer, Windows geplante Aufgabe CERTYX Agent Update), nur auf eine neuere signierte Version, und kehren zur vorherigen Version zurück, wenn der neu gestartete Agent nicht fehlerfrei ist. Pakete sind vom Herausgeber signiert: eine CMS-Signatur über den Archiv-Hash und über SHA256SUMS aller Paketdateien sowie Authenticode auf ausführbaren Windows-Dateien, CLM-Assemblys und PowerShell-Skripten. Die Linux- und Windows-Installationsprogramme prüfen das Paket gegen den fixierten Herausgeber-Fingerabdruck und verweigern die Installation unsignierter, veränderter oder fremder Pakete; die Entwicklungsausnahme (CLM_AGENT_ALLOW_UNSIGNED=1 oder -AllowUnsignedDevelopment) gibt eine Warnung aus und darf nicht produktiv verwendet werden. Ohne Release-Schlüssel installierte Agenten werden mit den unten genannten Upgrade-Skripten direkt aktualisiert, weil die Installationsprogramme einen Host mit bereits registriertem Agent ablehnen. Kunden-Anmeldedaten und private Schlüssel bleiben unter Kontrolle des Kunden. Secrets werden aus geschützten Dateien, HashiCorp Vault KV, Azure Key Vault, AWS Secrets Manager und Google Secret Manager aufgelöst; andere Tresorprodukte werden nicht unterstützt, Provider-CLIs laufen nur auf Unix-Agenten, und der Agent versendet keine E-Mails vom Kundenhost. Die Berechtigungen des Unix-Vault-Tokens werden bei jeder Verwendung erneut geprüft. Erkennungsidentitäten rotieren standardmäßig automatisch 30 Tage vor Ablauf (IdentityRenewalDays in den Settings der Agent-Konfiguration); die Schlüssel bleiben lokal, und

verlorene Bestätigungen werden wiederhergestellt. Deployment-Identitäten in der Dateiregistrierung erfordern eine kontrollierte manuelle Rotation. Kundenlokale Connector-Sperrdateien müssen unter Unix reguläre, nur für den Eigentümer zugängliche Dateien ohne symbolische übergeordnete Verzeichnisse sein. Unsichere bestehende Sperrdateien werden abgelehnt; ein Administrator muss die Speicherberechtigungen korrigieren, bevor ein neuer Versuch erfolgt. Diese Konnektoren laufen nur auf Unix-Agenten. Für einen ausdrücklich konfigurierten Unix-AWS-CLI-Transport setzen Sie AwsCliExecutable im kundenlokalen AWS-Ziel auf einen vertrauenswürdigen absoluten Pfad zur ausführbaren Datei. Der CLI-Verlauf muss deaktiviert sein. Zertifikatsimporte verwenden eine private Standardeingabe; Anmeldedaten bleiben lokal. SDK bleibt der Standardtransport. Der GCP-Lebenszyklus verwendet eine kundenlokale Ressourcen-/Identitätskonfiguration und die Baseline-Vorbereitung mit gcp-adopt; siehe GCP-LIFECYCLE.md. Anmeldedaten sind keine Auftragsfelder. Das Google-Certificate-Manager-Ziel selbst wird unter Ausführung in den Bereitstellungszielen registriert. Veröffentlicht dieser Server ein Paket ohne Herausgebersignatur (einen unsignierten Entwicklungsbuild), sagen die Installationsbefehle das, lassen die Signaturdatei aus und prüfen nur die Prüfsumme, mit den Entwicklungsoptionen von Prüfer und Installationsprogramm; verwenden Sie solche Pakete nur in der Entwicklung. Installierte Agenten werden mit upgrade-linux.sh oder upgrade-windows.ps1 aus einem neueren Paket direkt aktualisiert (Installationsanleitung, „Direktes Upgrade“), ohne neuen Registrierungscode; laden Sie das neuere Archiv über die angemeldete Konsole herunter und kopieren Sie es auf den Host. upgrade-linux.sh ergänzt außerdem AgentConfigurationFile in einer update.json eines älteren Installationsprogramms, sodass dessen signierte Updates wieder Archive herunterladen können. Ein SSH-Relay installiert nur TLS-Server-Zertifikate und braucht SSH-Zugang, OpenSSL 1.1.1 oder neuer und eine POSIX-Shell auf dem Remote-Host; Windows-Speicher und IIS installieren nur auf einem Windows-Agent-Host.

22 Vertrauensgraph

Zertifikate mit Endpunkten, Infrastruktur, Anwendungen, Geschäftsdiensten und Verantwortlichen verbinden.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Wählen Sie Erkennung synchronisieren (Administratoren), um beobachtete TLS-Endpunkte zu übernehmen: Für jede Endpunktbeobachtung eines inventarisierten Zertifikats erhält der Graph ein Infrastruktur-Asset (Server), seinen Endpunkt (Host und Port) und die Zertifikatsfamilie, verknüpft als Asset → Endpunkt → Familie; eine neuere Beobachtung verschiebt den Endpunkt zur neu beobachteten Familie. Der Server führt diese Synchronisierung für lizenzierte Organisationen auch automatisch aus (CIm:Assets:SynchronizationInterval, Standard jede Minute). Bestehende Ressourcen behalten ihre manuellen Daten.
2. Wählen Sie unter Geschäftskontext verwalten Ressource hinzufügen: Ressourcenart (Infrastruktur-Asset, Endpunkt, Anwendung, Geschäftsdienst oder Verantwortlicher), Name, Umgebung, Kritikalität, Status und Verantwortlicher; Endpunkte brauchen Hostname und Port, Verantwortliche eine E-Mail-Adresse und einen Typ. Ressource speichern; Ressource bearbeiten auf einer Karte der Liste Ressourcen lädt sie in das Formular (Zertifikatsfamilien stammen aus der Erkennung und sind nicht bearbeitbar).
3. Fügen Sie unter Abhängigkeiten eine Abhängigkeit von der Abhängigen Ressource zum Abhängigkeitsziel hinzu, von dem sie abhängt (zum Beispiel Anwendung → Endpunkt, Geschäftsdienst → Anwendung).

4. Geben Sie unter CMDB-Anreicherung die CMDB-Quelle an, wählen Sie eine CMDB-JSON-Datei (bis 100 KB, Format wie im Beispiel für das JSON-Schema) und dann CMDB-JSON importieren. Importe sind inkrementell: Dieselbe Quelle und dieselben externen IDs aktualisieren dieselben Ressourcen, manuelle Kritikalitätsüberschreibungen bleiben erhalten.
5. Wählen Sie unter Geschäftliche Auswirkung eine Zertifikatsfamilie und Auswirkung analysieren, um betroffene Ressourcen, Abhängigkeitspfade, Verantwortliche, die resultierende Kritikalität und Warnungen zu unvollständigem Kontext zu sehen.

EINGABEN UND PARAMETER

- Versionierte typisierte Ressourcen; inkrementelle CMDB-JSON-Anreicherung mit Quellidentität.
- Voraussetzung: Das Abonnement der Organisation enthält den Vertrauensgraphen (TRUST_GRAPH). Ohne ihn zeigt die Ansicht nur einen Hinweis, und der Server lehnt die Anfragen an den Vertrauensgraphen ab.

ERGEBNIS

Nachvollziehbare geschäftliche Auswirkungen mit Kritikalität, Verantwortlichen und Warnungen bei unvollständigem Kontext.

BERECHTIGUNGEN

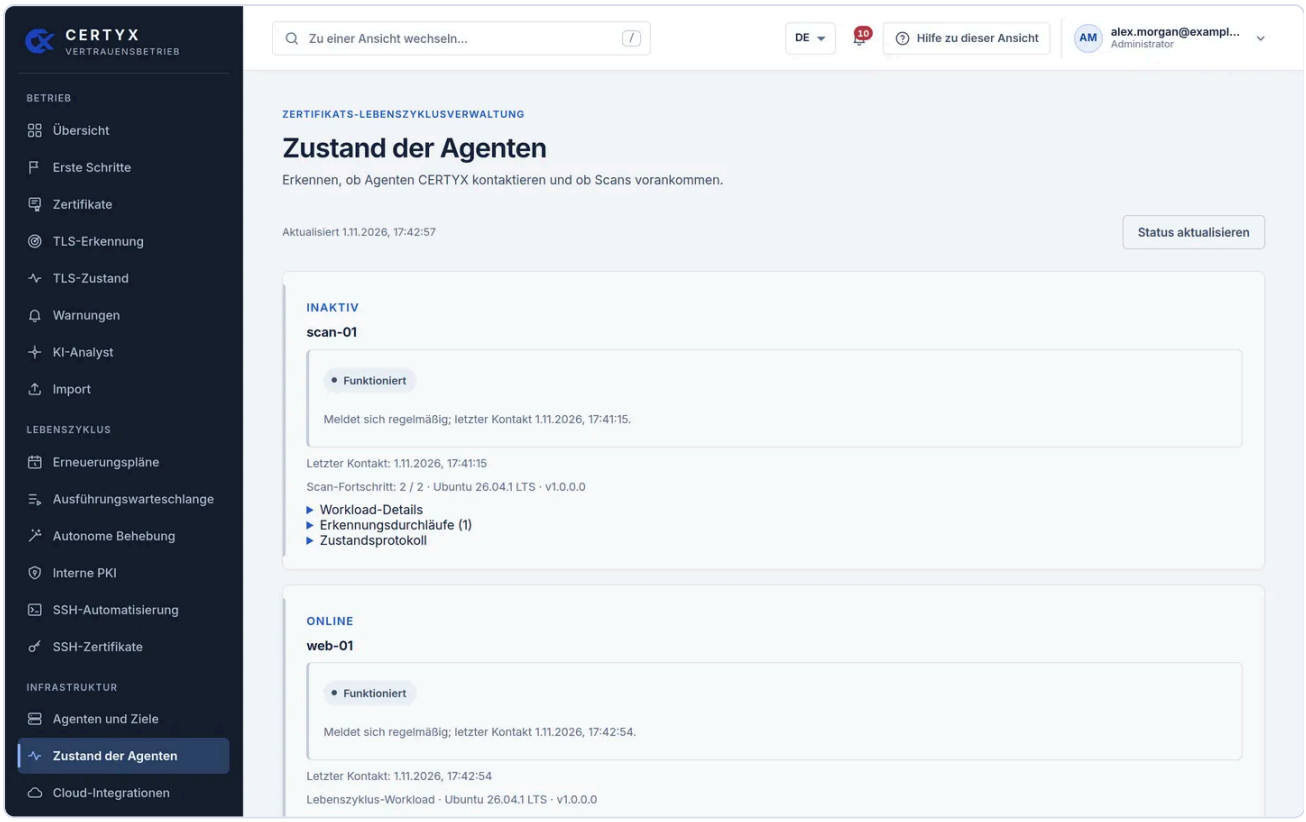
Erfordert die Lizenz für den Vertrauensgraphen. Administratoren synchronisieren die Erkennung, bearbeiten Ressourcen und Abhängigkeiten und importieren CMDB-Daten; andere angemeldete Benutzer der Organisation durchsuchen Ressourcen und analysieren Auswirkungen nur lesend.

EINSCHRÄNKUNGEN

Der CMDB-Import ist ein normalisierter Push-Connector. Herstellerspezifische Pull-Adapter sind nicht implementiert. Unbekannte Kritikalität bedeutet kein geringes Risiko; der Graphkontext verifiziert kein TLS-Vertrauen.

23 Zustand der Agenten

Erkennen, ob Agenten CERTYX kontaktieren und ob Scans vorankommen.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Registrieren und installieren Sie einen Netzwerk-Agenten.
2. Weisen Sie ein genehmigtes Profil zu.
3. Prüfen Sie den letzten authentifizierten Kontakt, den Fortschritt und die Fehlerursachen.
4. Erweitern Sie die Workload-Details eines Erkennungs-Agents, um Phase (Erreichbarkeit, gängige Ports, alle Ports), erreichbare Hosts, eine reduzierte Rate nach Verbindungs-Zeitüberschreitungen, das nächste Scan-Zeitfenster während des Wartens außerhalb der genehmigten Zeitfenster (Zustand Wartet auf ein Scan-Zeitfenster) und den Abschluss der Ausgangsbasis zu sehen.
5. Reine SSH-Agenten benötigen kein Erkennungsprofil. Online bedeutet einen kürzlichen authentifizierten Kontakt, nicht eine erfolgreiche Installation. Prüfen Sie SSH-Aufträge und Widerrufsergebnisse separat; bei ausbleibendem Kontakt wird der Agent offline.
6. Managed SSH meldet seinen eigenen sicheren Zyklusstatus. Ein fehlerfreier Erkennungsprozess kann einen fehlgeschlagenen oder stummen SSH-Worker nicht verdecken. Prüfen Sie den Fehler unter Agent-Zustand und in den geschützten lokalen Journalen; feste Zusammenfassungen enthalten keine Secrets. Ein Verbindungsverlust kann eine sofortige Meldung verhindern, daher ist auch eine Überwachung auf ausbleibenden Kontakt erforderlich.
7. Klappen Sie Workload-Details auf, um den SSH-Zyklusstatus und die letzte Meldung zu sehen; SSH-Metadaten werden nicht als Scan-Fortschritt bezeichnet.

8. Für zentrale Sichtbarkeit registrieren Sie eine separate Consumer-Identität und aktivieren ausdrücklich die KRL-Consumer-Berichterstattung; sie gewährt keine Berechtigung zur SSH-Ausstellung oder Host-Installation. Führen Sie ssh monitor-krl mit der geschützten Identitäts- und Abonnementkonfiguration aus. Agent-Zustand zeigt die gemeldete Revision, den Ablauf der signierten Veröffentlichung, Synchronisierungsfehler und versäumte Berichtsfenster; eine fehlerfreie Erkennung kann einen KRL-Fehler nicht verdecken. Die Plattformüberwachung umfasst diese Agent-Fehler. Es handelt sich um authentifizierte Beobachtungen des Agenten, nicht um einen unabhängigen Nachweis, dass jeder Host die widerrufene Identität ablehnt. Verwenden Sie eine registrierte Identität je Consumer.
9. Ein neu autorisierter KRL-Consumer bleibt bis zu seiner ersten Meldung nicht konfiguriert; eine andere fehlerfreie Workload kann keine Synchronisierung implizieren. Status und Ursache müssen übereinstimmen. Meldungen sind nach Organisationen isoliert, und eine entzogene Fähigkeit lehnt spätere Aktualisierungen ab.
10. Private Endpunkte können einen separat registrierten Endpunkt-Prüfer verwenden. Der Operator bindet dessen ID an das Ausführungsziel; wählen Sie unter Agenten und Ziele → Registrierte Agents beim Installer „Ausführung des Zertifikatslebenszyklus aktivieren" und bei einer anderen Agent-Identität „Unabhängige Endpunktverifizierung aktivieren". Der Prüfer kontrolliert genehmigte lokale TLS/HTTP-Endpunkte, bevor ein Erfolg akzeptiert wird; seine Workload erscheint in den Workload-Details. Die Einrichtung ist ein Befehl auf dem Prüfhost: Die Zielkarte unter Ausführung → Bereitstellungsziele zeigt Unabhängigen Endpunkt-Prüfer einrichten mit der Erteilung, Prüfumfang herunterladen (Ziel-ID, Prüfhost, Port, Health-Pfad und Vertrauensanker des Ziels; nur öffentliche Daten) und dem Befehl configure-verifier-linux.sh add-target (Linux, clm-endpoint-verifier.service unter dem Agent-Konto) bzw. configure-verifier-windows.ps1 add-target (Windows, geplante Aufgabe CERTYX Endpoint Verifier als LOCAL SERVICE). Das Skript schreibt die nur für den Besitzer lesbare Konfiguration aus der eigenen Identität des Agents, führt einen geprüften Zyklus aus, startet den Dienst und wartet bis zu zehn Minuten auf die Erteilung, solange CERTYX mit HTTP 403 antwortet; remove-target, disable und status verwalten ihn, das Deinstallationsprogramm entfernt ihn. Ein neuer Agent erhält die Rolle bei der Installation (CLM_AGENT_ENDPOINT_VERIFIER unter Linux, -EndpointVerifierTarget unter Windows). Ohne Vertrauensanker im Ziel muss der Prüfhost der ausstellenden CA selbst vertrauen.
11. Registrierte Installer melden ihre eigene Lebenszyklus-Workload (startet, inaktiv oder Fehler). Versäumte Meldungen bleiben auch bei fehlerfreier Erkennung sichtbar. Der Prozesszustand ersetzt weder das Ausführungsergebnis noch den unabhängigen Endpunktnachweis. Prüfen Sie die geschützten lokalen Journale, wenn ein Zyklus für einen Abgleich anhält.
12. Die Erkennung wiederholt vorübergehende Fehler bei der Identitätsrotation und Kommunikation nach Settings.RetrySeconds. Fehler bei Authentifizierung, Autorisierung und TLS-Vertrauen stoppen den Worker; --once gibt einen Fehler zurück. Konfigurieren Sie nur für den Eigentümer zugängliche Zustands- und Sperrpfade. Ein Berichtsausfall kann die Diagnose verzögern; überwachen Sie auch ausbleibenden Kontakt.
13. Jede Karte beginnt mit der Diagnose: genaue Ursache (Funktioniert, Meldet sich nicht, Noch kein erster Kontakt, Identität abgelaufen oder läuft bald ab, Uhrzeitabweichung, Prozessfehler, Prozess meldet sich nicht, Konfiguration fehlt, Erkennung pausiert, Wartet auf ein Scanfenster, Reduzierte Scanrate, Beobachtung abgelehnt), eine verständliche Erklärung mit Fakten (letzter Kontakt und verpasstes Meldefenster, Prozess und gemeldeter fester Grund, Ablaufdatum, gemessene Uhrzeitabweichung) und Was zu tun ist: die Abhilfen der Reihe nach, jede mit Link zum Ort der Umsetzung, sowie die Fehlerbehebung der Anleitung. #agent-health/<Agenten-ID> öffnet direkt einen Agenten (aus Übersicht, Agenten und Ziele, Erneuerungsplänen und der Erneuerungsbereitschaft).

14. Das Zustandsprotokoll listet jede Änderung der Diagnose, neueste zuerst, mit Zeit, neuer und vorheriger Ursache und Erklärung. Eine Zustandsüberwachung bewertet jeden Agenten alle Clm:Agents:Health:WatchInterval (standardmäßig 1 Minute) und erfasst jede Änderung; sie wird auch als agent.health.changed mit Erklärung und Abhilfeschritten ins Sicherheitsprotokoll geschrieben, sodass Plattformbetreiber und der SIEM-Export der Organisation sie erhalten. Erkennungsdurchläufe zeigt die letzten Durchläufe des Agenten (siehe TLS-Erkennung, Scanverlauf).

EINGABEN UND PARAMETER

- Empfangszeit auf dem Server, Zertifikatsablauf und begrenzte authentifizierte Agent-Telemetrie.
- Ein Agent wird Offline und eine Workload-Meldung als Fehler markiert, wenn innerhalb seines Berichtsfensters nichts eintrifft: Intervall des Profils oder der Workload plus Clm:Agents:Health:ReportingGrace (Standard 1,5 Minuten), mindestens Clm:Agents:Health:MinimumReportingWindow (Standard 2 Minuten).

ERGEBNIS

Eine Karte je registriertem Agent mit seinem Zustand (Online, Wartet auf ersten Kontakt, Wartet auf Konfiguration, Pausiert, Wartet auf ein Scan-Zeitfenster, Offline, Fehler, Identität abgelaufen, Widerrufen), der Ursache, dem letzten Kontakt, der primären Workload mit Betriebssystem und Agent-Version sowie Workload-Details je gemeldeter Workload. Die Liste wird bei geöffneter Ansicht automatisch aktualisiert; Status aktualisieren lädt sie sofort neu.

BERECHTIGUNGEN

Authentifizierte Benutzer der Organisation.

EINSCHRÄNKUNGEN

Offline bedeutet, dass der Kontakt fehlt; die Plattform kann die genaue Ursache für eine nicht erreichbare Maschine nicht kennen. Das vom Agenten gemeldete Betriebssystem ist keine Hardware-Attestierung. Erkennungsidentitäten rotieren standardmäßig automatisch 30 Tage vor Ablauf (IdentityRenewalDays in den Settings der Agent-Konfiguration); die Schlüssel bleiben lokal, und verlorene Bestätigungen werden wiederhergestellt. Deployment-Identitäten in der Dateiregistrierung erfordern eine kontrollierte manuelle Rotation. Mit dem Release-Signaturschlüssel des Betreibers installierte Linux-Agenten aktualisieren sich täglich aus signierten Releases; andere Linux-Agenten und alle Windows-Agenten haben kein direktes Update: Die Installationsprogramme lehnen einen Host mit bereits registriertem Agent ab, daher wird eine neuere Version installiert, indem Sie den Agent ersetzen (widerrufen, die Installation wie in der Installationsanleitung beschrieben entfernen und das geprüfte neue Paket unter einer neuen Agent-ID registrieren).

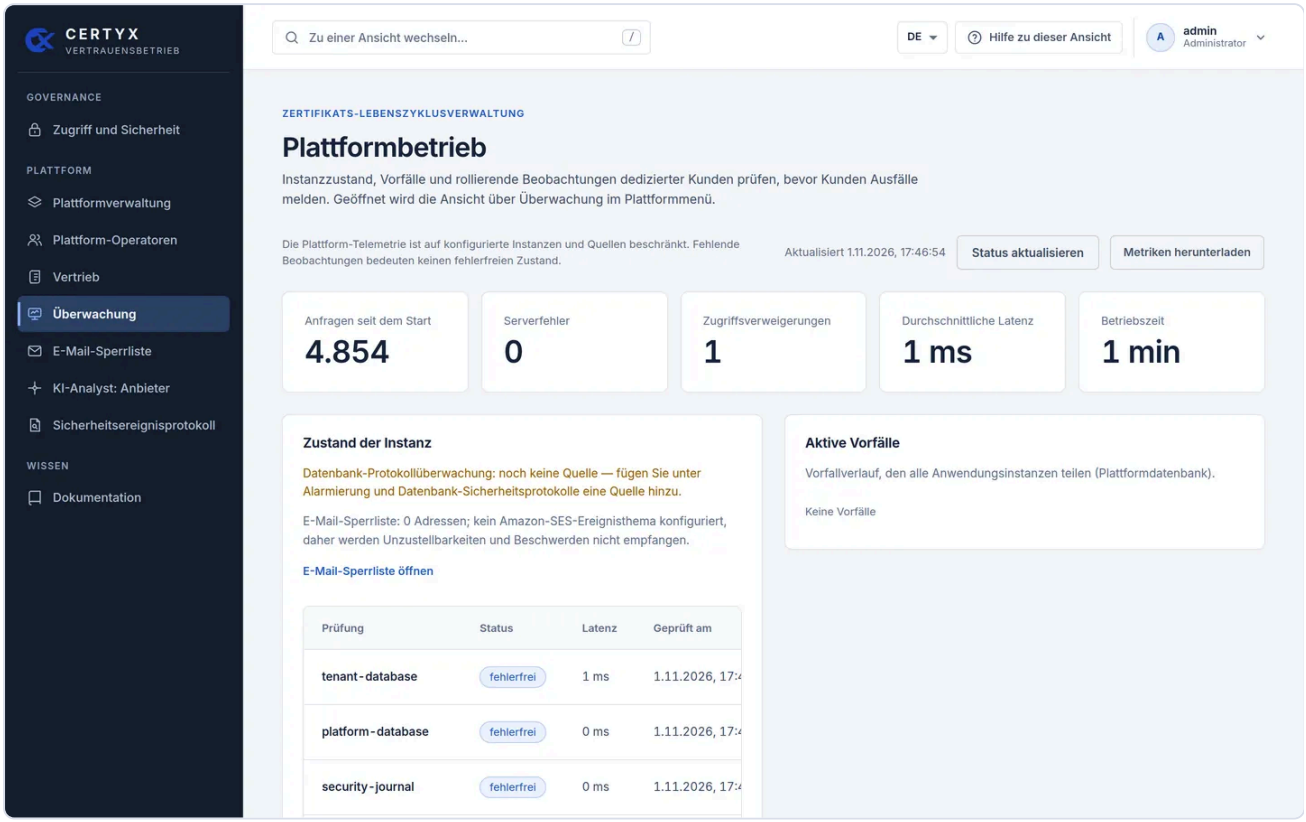
FEHLERBEHEBUNG

- Meldet sich nicht: Dienst starten (sudo systemctl status clm-discovery.service; clm-ssh.service für SSH; die geplante Aufgabe unter Windows) und sudo clm-agent log lesen; sudo clm-agent status ausführen, das den fehlerhaften Schritt nennt (Dienst, Adresse, TLS-Vertrauen mit Sperrprüfung, Uhrzeit, Identität); Firewall, Proxy und DNS zur Agentenadresse prüfen; bei TLS-Vertrauensfehlern das private Stammzertifikat der Agentenadresse installieren; Uhr synchronisieren; prüfen, ob die Identität abgelaufen oder widerrufen ist. Unter Windows die Protokolle der Aufgaben C:\ProgramData\CLM-Agent\state\discovery.log und C:\ProgramData\CLM-SSH\state\ssh-workload.log lesen (Get-Content -Tail 50) und Clm.Agent.exe status agent.json in einer Administrator-PowerShell ausführen.

- Noch kein erster Kontakt: den nach der Registrierung angezeigten Installationsbefehl vor Ablauf des Codes ausführen (Agenten und Ziele); nach Ablauf einen neuen Code erstellen; danach sudo clm-agent status.
- Identität abgelaufen oder läuft bald ab: Die automatische Rotation läuft IdentityRenewalDays (standardmäßig 30) vor Ablauf; ist sie ausgeblieben, den Agenten unter einer neuen Agenten-ID neu registrieren und die alte Identität widerrufen.
- Uhrzeitabweichung: Die Netzwerkkarte des Agenten enthält seine Uhrzeit; den Host per NTP synchronisieren. TLS- und Identitätsprüfungen schlagen bei Minutenabweichungen fehl (Toleranz Clm:Agents:Health:ClockSkewTolerance).
- Prozessfehler: Lebenszyklusprozess fehlgeschlagen — den fehlgeschlagenen Auftrag unter Ausführung und das geschützte lokale Protokoll öffnen; Erkennung fehlgeschlagen — Kommunikation mit sudo clm-agent status prüfen; genehmigtes Profil überschreitet die lokale Positivliste — AllowedCidrs erweitern oder Profil verkleinern; KRL-Synchronisierung fehlgeschlagen — Relay des Kunden und gepinntes Vertrauen prüfen; SSH-Zyklus fehlgeschlagen — SSH-Protokoll und SSH-Automatisierung prüfen.
- Konfiguration fehlt: ein Erkennungsprofil zuweisen und genehmigen oder den Prozess konfigurieren und starten, für den die Berechtigung erteilt wurde (Lebenszyklus, Endpunktprüfung, KRL-Empfänger).
- Reduzierte Scanrate: Verbindungs-Timeouts haben die Rate halbiert; prüfen, ob eine Firewall oder Angriffserkennung den Agenten blockiert, oder Rate und Verbindungen pro Host senken.

24 Plattformbetrieb

Instanzzustand, Vorfälle und rollierende Beobachtungen dedizierter Kunden prüfen, bevor Kunden Ausfälle melden. Geöffnet wird die Ansicht über Überwachung im Plattformmenü.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Melden Sie sich als freigegebener Plattformadministrator mit MFA an.
2. Prüfen Sie die Metrikkacheln dieser Instanz (Anfragen seit dem Start, Serverfehler, Zugriffsverweigerungen, Durchschnittliche Latenz, Betriebszeit), Zustand der Instanz (Prüfungen der Organisations- und der Plattformdatenbank, der Kundenüberwachung und jeder Datenbank-Protokollquelle mit Status, Latenz und Prüfzeit; die Zeile über der Tabelle zeigt die Überwachung der Datenbankprotokolle) und Aktive Vorfälle. Status aktualisieren lädt alles neu; Metriken herunterladen speichert die Prometheus-Metriken dieser Instanz.
3. Fügen Sie unter Alarmierung und Datenbank-Sicherheitsprotokolle das verwaltete PostgreSQL-Protokoll jeder Datenbank hinzu: AWS CloudWatch Logs (vollständiger ARN der RDS-Protokollgruppe), Azure Log Analytics (Arbeitsbereich-GUID|Ressourcen-ID des Flexible Server) oder Google Cloud Logging (Projekt:Cloud-SQL-Instanz), mit der Kunden-ID bei einer dedizierten Kundendatenbank. Jede Quelle wird im nächsten Überwachungszyklus mit der Maschinenidentität des Plattform-Hosts gelesen (CloudWatch über das AWS SDK, der Host braucht also nur Lesezugriff auf die Protokollgruppe; Azure und Google Cloud über die Anbieter-CLI), und Authentifizierungs- und Autorisierungsfehler werden zu Vorfällen. Mit den Datenbankcontainern der Standardbereitstellung muss nichts hinzugefügt werden: Beide Datenbanken schreiben ein JSON-Sicherheitsprotokoll, das die Anwendung liest; die Zeile zum Instanzzustand nennt dann „lokales PostgreSQL-Protokoll“. Auf AWS mit RDS fügen Sie einmal die

CloudWatch-Quelle mit dem ARN der Protokollgruppe hinzu, den die Infrastrukturausgabe database_log_group_arn nennt. Eine nicht lesbare Quelle erscheint als eigene fehlgeschlagene Zustandsprüfung und in der Quellenliste; die Zeile zum Instanzzustand zeigt, wie viele Quellen überwacht werden und ob das lokale PostgreSQL-JSON-Protokoll des Hosts gelesen wird.

4. Zustand der Kunden listet dedizierte Kunden mit Datenbankstatus, Kundenstatus, Agenten offline, fehlgeschlagenen Lebenszyklus-Aufträgen und letzter Beobachtung (Grund beim Überfahren einer Zeile). Wählen Sie nach der Untersuchung Vorfall bestätigen; die Bestätigung hält fest, wer die Untersuchung übernimmt, und behebt den Fehler nicht.
5. Alarmkanäle: Fügen Sie Kanäle für Microsoft Teams (Webhook- oder Workflow-URL), Slack (Incoming-Webhook-URL; Nachrichtenlayout Blocks oder Klartext), PagerDuty (Routing-Schlüssel der Events API v2), HTTPS-Webhook oder E-Mail mit einer Mindestschwere hinzu und wählen Sie Testalarm senden; ein fehlgeschlagener Test nennt den Grund (Relay fehlt, ungültiges Ziel, Geheimnis nicht lesbar, abgelehnt, nicht erreichbar, Zeitüberschreitung). E-Mail-Kanäle verwenden das E-Mail-Relay für Alarme (Host, STARTTLS-Port, Absender, optional Benutzername und Passwort). URLs, Routing-Schlüssel und Passwörter sind nur schreibbar: Geben Sie einen neuen Wert ein, um ihn zu ersetzen, oder secret:<Name>, um ihn aus einer freigegebenen Plattform-Geheimnisbindung zu lesen; ein leeres Feld behält den gespeicherten Wert. Öffnungen und Auflösungen von Vorfällen gehen an jeden Kanal, dessen Mindestschwere sie erreichen; ein Kanal, der wiederholt fehlschlägt, löst den Vorfall zur Warnungszustellung aus. Jeweils eine Instanz sendet Warnungen, und jede Änderung erreicht einen Kanal einmal, auch bei mehreren Instanzen.
6. Für zentrale Sichtbarkeit registrieren Sie eine separate Consumer-Identität und aktivieren ausdrücklich die KRL-Consumer-Berichterstattung; sie gewährt keine Berechtigung zur SSH-Ausstellung oder Host-Installation. Führen Sie ssh monitor-krl mit der geschützten Identitäts- und Abonnementkonfiguration aus. Agent-Zustand zeigt die gemeldete Revision, den Ablauf der signierten Veröffentlichung, Synchronisierungsfehler und versäumte Berichtsfenster; eine fehlerfreie Erkennung kann einen KRL-Fehler nicht verdecken. Die Plattformüberwachung umfasst diese Agent-Fehler. Es handelt sich um authentifizierte Beobachtungen des Agenten, nicht um einen unabhängigen Nachweis, dass jeder Host die widerrufene Identität ablehnt. Verwenden Sie eine registrierte Identität je Consumer.
7. Der Anbieter des KI-Analysten (Anthropic-API-Schlüssel, Modell, Verbindungstest, Kontingente, Angebot an Organisationen) hat eine eigene Kontrollraum-Ansicht: KI-Analyst: Anbieter.
8. Unter der Offline-Zahl listet jede Kundenzeile die Agenten mit Handlungsbedarf mit Ursache und seit wann (dieselbe Diagnose, die die Organisation im Agentenzustand sieht); die Sicherheitsprotokolleinträge agent.health.changed des Kunden enthalten Erklärung und Abhilfeschritte.
9. Technische und Vertriebs-E-Mails sind getrennt: Das E-Mail-Relay für Alarme ist der technische Absender der Plattform (zum Beispiel support@…) für Alarm-E-Mails und die E-Mails zur Einrichtung des Authenticators für Kundenkonten; Vertriebs-E-Mails nutzen ihr eigenes Relay unter Vertrieb (zum Beispiel sales@…). Muster der Einrichtungs-E-Mail senden schickt einem Empfänger über dieses Relay eine Vorschau der Einrichtungs-E-Mail in einer gewählten Sprache; Link und QR-Code darin öffnen keine Einrichtung, und der Versand wird im Sicherheitsjournal erfasst (mfa-setup.mail.sample-sent). Das Relay nutzt STARTTLS (Port 587); implizites TLS auf Port 465 wird nicht unterstützt.
10. Unter Instanzzustand zeigt die Zeile zur E-Mail-Sperrliste, wie viele Adressen gesperrt sind und welches Amazon-SES-Ereignis zuletzt empfangen wurde (noch keines ist normal, Ereignisse sind selten) oder dass kein Ereignisthema konfiguriert ist; E-Mail-Sperrliste öffnen führt zur Liste. Ein Alarm-E-Mail-Kanal mit gesperrter Adresse wird nicht wiederholt und öffnet einen alert-delivery-Vorfall mit der Ursache.

EINGABEN UND PARAMETER

- Instanzzähler seit Prozessstart; authentifizierte Datenbankprüfungen; begrenzter Vorfallverlauf und Kundenbeobachtungen.
- Alarmkanal: Name (1–64 Buchstaben, Ziffern, . _ -, beginnend mit einem Buchstaben oder einer Ziffer), Art, Mindestschwere, Empfänger-E-Mail oder URL/Routing-Schlüssel (eine URL beginnt mit https://; ein PagerDuty-Routing-Schlüssel hat bis zu 200 Zeichen ohne Leerzeichen; beide können stattdessen ein Verweis secret:<name> sein), Slack-Nachrichtenlayout (nur Slack). Relay: Host, Port, Absender, optional Benutzername und Passwort. Datenbank-Protokollquelle: Name, Protokolldienst, Ort im für den Dienst angezeigten Format, optional Kunden-ID (GUID). Die Mindestschwere ist Nur kritisch oder Warnungen und kritisch; höchstens 20 Alarmkanäle und 50 Datenbank-Protokollquellen.

ERGEBNIS

Dauerhafte Vorfälle (bei konfigurierter Plattformdatenbank von allen Instanzen geteilt, sodass ein auf einer Instanz gemeldeter Vorfall auf einer anderen bestätigt oder geschlossen werden kann), geschützte Prometheus-Metriken und Betriebsstatus. Der Vorfallbereich zeigt, ob der Verlauf geteilt, lokal oder nicht verfügbar ist. Versionierte Einstellungen für Alarmkanäle, Relay und Datenbank-Protokollquellen in der Plattformdatenbank.

BERECHTIGUNGEN

Nur freigegebener Plattformadministrator mit einer MFA-authentifizierten Sitzung. Jede Einstellungsänderung und jeder Testalarm wird ohne Geheimniswerte im Sicherheitsjournal erfasst. Step-up: Jede Änderung in dieser Ansicht (außer Tests, Verbindungsprüfungen und dem Bestätigen eines Vorfalls) fragt nach dem aktuellen 6-stelligen Code Ihres eigenen Authenticators; ein bestätigter Code gilt für Clm:Identity:OperatorStepUpWindow (Standard 5 Minuten) auch für Ihre weiteren Änderungen im Kontrollraum. Ein falscher oder bereits verwendeter Code wird abgelehnt, zählt zur Kontosperre und wird protokolliert; Abbrechen verwirft die Änderung. Über Firmenanmeldung angemeldete Betreiber haben keinen lokalen Authenticator und können diese Änderungen nicht vornehmen. Operator-Rollen: Support, Sicherheitsadministrator und Administrator sehen die Überwachung und bearbeiten Vorfälle; die Alarmierungseinstellungen (Kanäle, Relay, Protokollquellen) brauchen Sicherheitsadministrator oder Administrator.

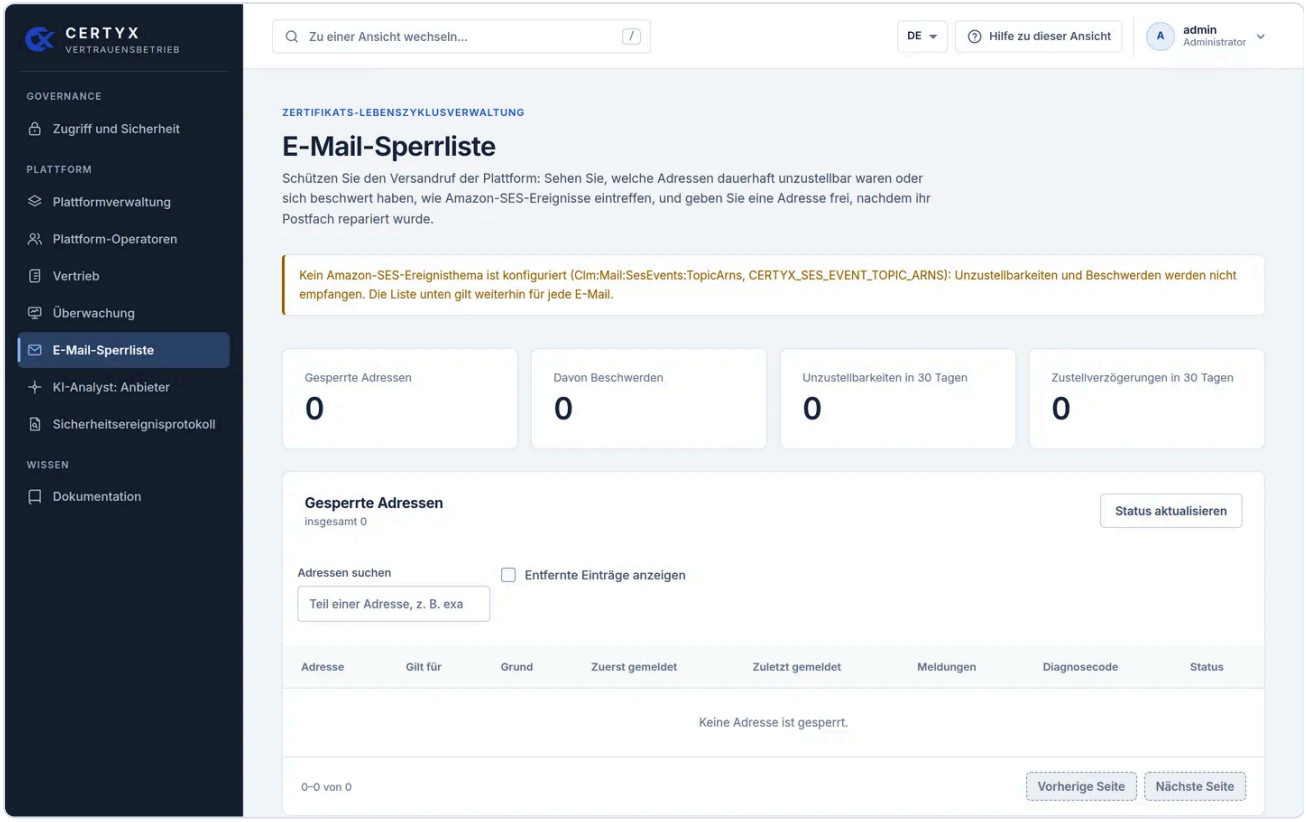
EINSCHRÄNKUNGEN

Zähler werden beim Neustart zurückgesetzt. Es handelt sich um die Erkennung ausgewählter Symptome, nicht um eine vollständige Einbruchsverhinderung. Jede Instanz führt eigene Prüfungen und Metriken aus; ohne Plattformdatenbank führt sie auch einen eigenen Vorfallverlauf und sendet eigene Warnungen, betreiben Sie dann nur eine Instanz. Solange die Plattformdatenbank nicht erreichbar ist, werden neue Vorfälle erst nach ihrer Rückkehr erfasst. Vorfälle aus der Zeit vor dem Update oder aus der Datei importierte werden nicht erneut gemeldet, und ein neuer Kanal erhält nur spätere Änderungen. Cursor für verwaltete Protokolle beginnen nach einem Neustart neu, sodass ein alter Fehler erneut gemeldet werden kann. Das Sicherheitsjournal wird an SIEM-Ziele exportiert, die unter Journal der Sicherheitsereignisse → SIEM-Export (Plattformbereiche) und von jeder Organisation (SIEM-Export) eingerichtet werden; die vollständige Erfassung von Datenbank-Audits ist nicht Teil dieser Ansicht. Dedizierte Kunden werden in rollierenden Stapeln geprüft (Clm:Monitoring:CustomerProbeBatchSize, Standard 10 je Zyklus von Clm:Monitoring:ProbeInterval, Standard 30 Sekunden); Zeitstempel machen veraltete Beobachtungen sichtbar. Der Vorfallverlauf behält höchstens Clm:Monitoring:IncidentRetention Vorfälle (Standard 5.000) und entfernt zuerst gelöste. Alarm- und Protokollquelleneinstellungen benötigen die Plattformdatenbank; die Werte der Konfigurationsdatei werden beim ersten Start einmal übernommen, danach ist die Konsole

maßgeblich. Pfade der Anbieter-CLIs, das lokale PostgreSQL-JSON-Protokoll und die Zeitgrenze der Alarmzustellung sind Einstellungen der Bereitstellung. Ein erfolgreicher Test belegt, dass das Ziel die Nachricht angenommen hat, nicht dass jemand alarmiert wurde.

25 E-Mail-Sperrliste

Schützen Sie den Versandruf der Plattform: Sehen Sie, welche Adressen dauerhaft unzustellbar waren oder sich beschwert haben, wie Amazon-SES-Ereignisse eintreffen, und geben Sie eine Adresse frei, nachdem ihr Postfach repariert wurde.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Melden Sie sich als zugelassener Plattformadministrator mit MFA an und öffnen Sie in der Leitstelle E-Mail-Sperrliste. Die Statuszeile zeigt, ob Amazon-SES-Ereignisse empfangen werden (Anzahl der zugelassenen SNS-Themen und das letzte Ereignis); die Kacheln zeigen gesperrte Adressen, davon Beschwerden, sowie Unzustellbarkeiten und Zustellverzögerungen der letzten 30 Tage.
2. Amazon SES meldet jede Unzustellbarkeit, Beschwerde, Ablehnung und Zustellverzögerung der Plattformpost an das SNS-Thema der Installation, das sie an https://<Konsole>/public/api/mail-events/ses sendet. CERTYX prüft die SNS-Signatur (Zertifikat nur von sns.<Region>.amazonaws.com, Kette zu einer öffentlichen Wurzel, Subjekt sns.amazonaws.com), das Thema gegen Clm:Mail:SesEvents:TopicArns, das Alter der Nachricht und die MessageId (eine Wiederholung ändert nichts) und bestätigt das Abonnement selbst.
3. Eine dauerhafte Unzustellbarkeit oder eine Beschwerde setzt jeden genannten Empfänger auf die Liste (Grund, erste und letzte Meldung, Anzahl der Meldungen, Diagnosecode des Anbieters; nie Nachrichteninhalt) und wird als mail.suppression.added protokolliert. Vorübergehende Unzustellbarkeiten, Zustellverzögerungen und Ablehnungen werden nur gezählt. Jeder Eintrag hat einen Bereich (Spalte Gilt für): E-Mails, die die Plattform für eine Organisation sendet (ihre Authenticator-Einrichtungs-E-Mails), tragen die Organisation im Amazon-SES-Nachrichten-Tag certyx-

scope, sodass ihr Bounce oder ihre Beschwerde die Adresse nur für diese Organisation sperrt; Plattform-E-Mails (Betreiber, Alarme, Vertrieb) und Ereignisse ohne Tag (zum Beispiel SES-Feedback-Benachrichtigungen oder Einträge aus der Zeit vor der Sperre pro Organisation) sperren sie für alle E-Mails. E-Mails einer Organisation prüfen die plattformweiten und die eigenen Einträge, nie die einer anderen Organisation.

4. Jede E-Mail der Plattform prüft vor dem Versand die Liste: Benachrichtigungen der Organisationen (gesperrte Empfänger werden übersprungen; der Outbox-Eintrag vermerkt es oder wird abgebrochen, wenn niemand übrig ist), Testnachrichten, E-Mails zur Einrichtung des Authentifikators (die Konsole zeigt stattdessen den Link mit dem Grund), Alarm-E-Mails (der Kanal öffnet einen Vorfall statt erneut zu senden) und Vertriebs-E-Mails (die Mitteilung wird als Nicht gesendet: Empfänger gesperrt markiert). Die Betreiberkopie von Abrechnungsmitteilungen entfällt, wenn sie gesperrt ist.
5. Suchen Sie nach einem Teil der Adresse; Entfernte Einträge anzeigen listet auch entfernte Adressen mit Person, Zeitpunkt und Grund.
6. Sobald das Postfach wieder funktioniert, wählen Sie Aus der Sperrliste entfernen, geben den Grund ein und bestätigen. Das Entfernen wird als mail.suppression.removed protokolliert und CERTYX sendet sofort wieder an die Adresse; eine neue Unzustellbarkeit oder Beschwerde sperrt sie erneut. Entfernen Sie die Adresse auch aus der kontoweiten Sperrliste von Amazon SES (SES-Konsole → Suppression list oder aws sesv2 delete-suppressed-destination --email-address <Adresse>), sonst verwirft SES Nachrichten an sie weiterhin. Das Entfernen gilt für den Eintrag der gewählten Zeile (seinen Bereich); eine in mehreren Bereichen gesperrte Adresse behält ihre anderen Einträge.

EINGABEN UND PARAMETER

- Suche: Teil einer Adresse (bis 254 Zeichen, ohne Beachtung der Groß-/Kleinschreibung).
- Grund für das Entfernen: 3 bis 500 Zeichen ohne Zeilenumbrüche, zum Beispiel: Postfach am 14. Oktober vom Kunden neu angelegt.
- Installationseinstellungen (nicht in der Konsole): Clm:Mail:SesEvents:TopicArns (auf dem Host CERTYX_SES_EVENT_TOPIC_ARNS), die zugelassenen SNS-Themen-ARNs; MaxMessageAge (Standard 1 Stunde), MaxClockSkew (5 Minuten), MaxBodyBytes (256 KiB), EventRetention (90 Tage) und SigningCertificateSubjects (sns.amazonaws.com).

ERGEBNIS

Eine Sperrliste in der Plattformdatenbank, gemeinsam für alle E-Mail-Wege und alle Organisationen, mit einem Protokolleintrag für jede hinzugefügte (Akteur system:amazon-ses) und entfernte Adresse (der Betreiber). Organisationsadministratoren sehen ihre gesperrten Gruppenmitglieder unter Benachrichtigungsgruppen. Einträge haben einen Bereich: plattformweit oder die Organisation, deren E-Mail sie verursacht hat.

BERECHTIGUNGEN

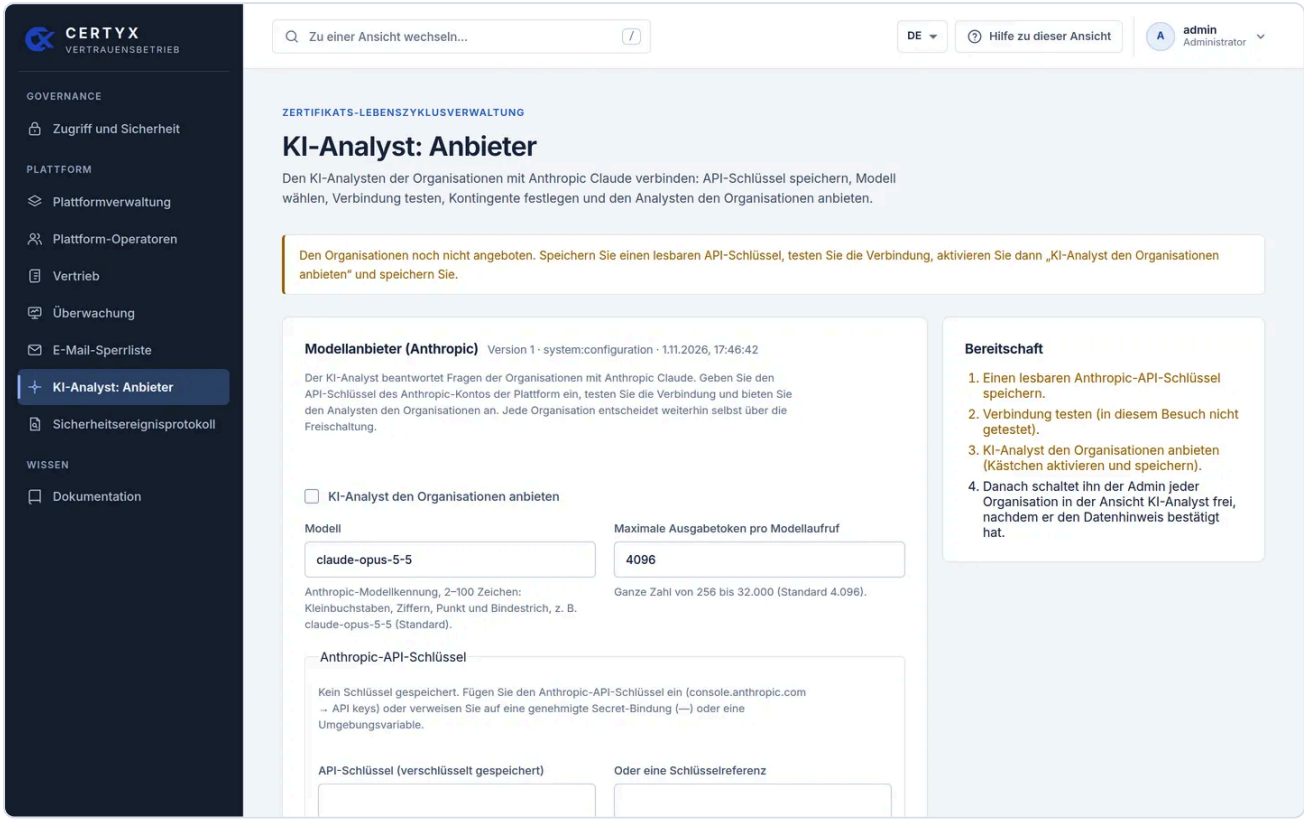
Nur Plattformadministratoren mit MFA sehen die Liste und entfernen Adressen. Benutzer einer Organisation sehen nur die gesperrten Mitglieder ihrer eigenen Empfängergruppen (Benachrichtigungsgruppen) und können sie nicht entfernen: Die Liste schützt den gemeinsamen Versandruf der Plattform. Step-up: Jede Änderung in dieser Ansicht (außer Tests, Verbindungsprüfungen und dem Bestätigen eines Vorfalls) fragt nach dem aktuellen 6-stelligen Code Ihres eigenen Authenticators; ein bestätigter Code gilt für Clm:Identity:OperatorStepUpWindow (Standard 5 Minuten) auch für Ihre weiteren Änderungen im Kontrollraum. Ein falscher oder bereits verwendeter Code wird abgelehnt, zählt zur Kontosperre und wird protokolliert; Abbrechen verwirft die Änderung. Über Firmenanmeldung angemeldete Betreiber haben keinen lokalen Authenticator und können diese Änderungen nicht vornehmen.

EINSCHRÄNKUNGEN

Benötigt die Plattformdatenbank; ohne sie sperrt CERTYX nichts (die Liste wird als nicht verfügbar angezeigt) und SES-Ereignisse können nicht empfangen werden. Ohne zugelassenes Thema antwortet der Endpunkt mit 404 und die Statuszeile meldet, dass keine Ereignisse empfangen werden; die Liste gilt weiterhin. Ereignisse sind selten: Lange kein Ereignis ist normal. Solange die Plattformdatenbank nicht lesbar ist, wird ohne Prüfung gesendet (die kontoweite Sperrliste von Amazon SES gilt weiterhin). Nur Amazon-SES-Ereignisse über SNS werden verstanden; Unzustellbarkeiten anderer Anbieter (beim eigenen Relay einer Organisation) werden nicht empfangen. Das Entfernen hier entfernt die Adresse nicht aus der kontoweiten SES-Liste. Die Sperre gilt je Adresse für alle Organisationen.

26 KI-Analyst: Anbieter

Den KI-Analysten der Organisationen mit Anthropic Claude verbinden: API-Schlüssel speichern, Modell wählen, Verbindung testen, Kontingente festlegen und den Analysten den Organisationen anbieten.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Melden Sie sich als freigegebener Plattformadministrator mit MFA an und öffnen Sie im Kontrollraum KI-Analyst: Anbieter. Statuszeile und Liste Bereitschaft zeigen, was noch fehlt: ein lesbarer Schlüssel, ein erfolgreicher Verbindungstest und das Angebot an die Organisationen.
2. Fügen Sie unter Anthropic-API-Schlüssel den Schlüssel aus console.anthropic.com → API keys in API-Schlüssel (verschlüsselt gespeichert) ein oder geben Sie stattdessen eine Referenz an: secret:<Bindung> für eine genehmigte Plattform-Secret-Bindung oder env:<VARIABLE> für eine Umgebungsvariable der Anwendung. Füllen Sie nur eines der beiden Felder aus; leere Felder behalten den gespeicherten Schlüssel; Gespeicherten Schlüssel entfernen löscht ihn. Ein gespeicherter Schlüssel wird nie wieder angezeigt: Das leere Schlüsselfeld zeigt dann „gespeicherter Schlüssel — neuen eingeben, um ihn zu ersetzen“, und die Zeile über den Feldern nennt die Herkunft des Schlüssels.
3. Wählen Sie Verbindung testen. Es wird eine kurze Anfrage (wenige Ausgabetoken, keine Werkzeuge, keine Organisationsdaten) mit den Werten im Formular – auch einem ungespeicherten Schlüssel oder Modell – oder den gespeicherten Einstellungen gesendet und das Ergebnis gemeldet: Verbindung funktioniert, Schlüssel abgelehnt (401), Nicht berechtigt (403), Modell nicht gefunden (404), Rate-Limit oder Kontingent erreicht (429), Abrechnungsproblem (Guthaben), Anfrage abgelehnt (400), Anbieter

überlastet (529), Fehler beim Anbieter, Anbieter nicht erreichbar (DNS, Firewall, Proxy, TLS) oder Keine Antwort rechtzeitig, mit HTTP-Status, Fehlertyp und Meldung des Anbieters, Modell und Dauer. Ein fehlender oder nicht lesbarer Schlüssel wird gemeldet, ohne etwas zu senden.

4. Prüfen Sie das Modell (Standard claude-opus-5-5) und die Ausgabetoken, aktivieren Sie KI-Analyst den Organisationen anbieten und wählen Sie Einstellungen speichern. Die Statuszeile meldet dann Bereit und nennt die Adresse des Anbieters.
5. Der Admin jeder Organisation schaltet den Analysten weiterhin in der eigenen Ansicht KI-Analyst nach Bestätigung des Datenhinweises frei; erst dann können deren Benutzer Fragen stellen.

EINGABEN UND PARAMETER

- API-Schlüssel: 20–500 Zeichen ohne Leerzeichen (Anthropic-Schlüssel beginnen meist mit sk-ant-). Mit dem Data-Protection-Schlüsselbund der Plattform verschlüsselt (über die Plattformdatenbank von allen Instanzen geteilt) und als protected:<Chiffretext> gespeichert; nie wieder angezeigt, nie von der API zurückgegeben, nie im Journal oder Protokoll.
- Schlüsselreferenz: secret:<Name> einer in Clm:Secrets:Bindings aufgeführten Bindung (beim Senden einer Frage mit der Maschinenidentität gelesen) oder env:<VARIABLE> (Großbuchstaben, Ziffern, Unterstriche).
- Modell: 2–100 Kleinbuchstaben, Ziffern, Punkte oder Bindestriche, z. B. claude-opus-5-5. Maximale Ausgabetoken pro Modellaufruf 256–32.000 (Standard 4.096).
- Kontingente: Fragen pro Benutzer und Stunde 1–10.000 (Standard 30), Fragen pro Organisation und Tag 1–100.000 (Standard 300), Token pro Organisation und Tag 1.000–1.000.000.000 (Standard 2.000.000).

ERGEBNIS

Ein versioniertes Einstellungsdokument in der Plattformdatenbank (Schlüssel analyst); jedes Speichern wird als analyst.settings.updated protokolliert, ein gespeicherter Schlüssel erscheint nur als „stored“, jeder Verbindungstest als analyst.connection.tested mit Ergebnis, HTTP-Status, Modell und Schlüsselquelle. Organisationen sehen den Analysten als verfügbar, sobald er angeboten wird und der Schlüssel lesbar ist.

BERECHTIGUNGEN

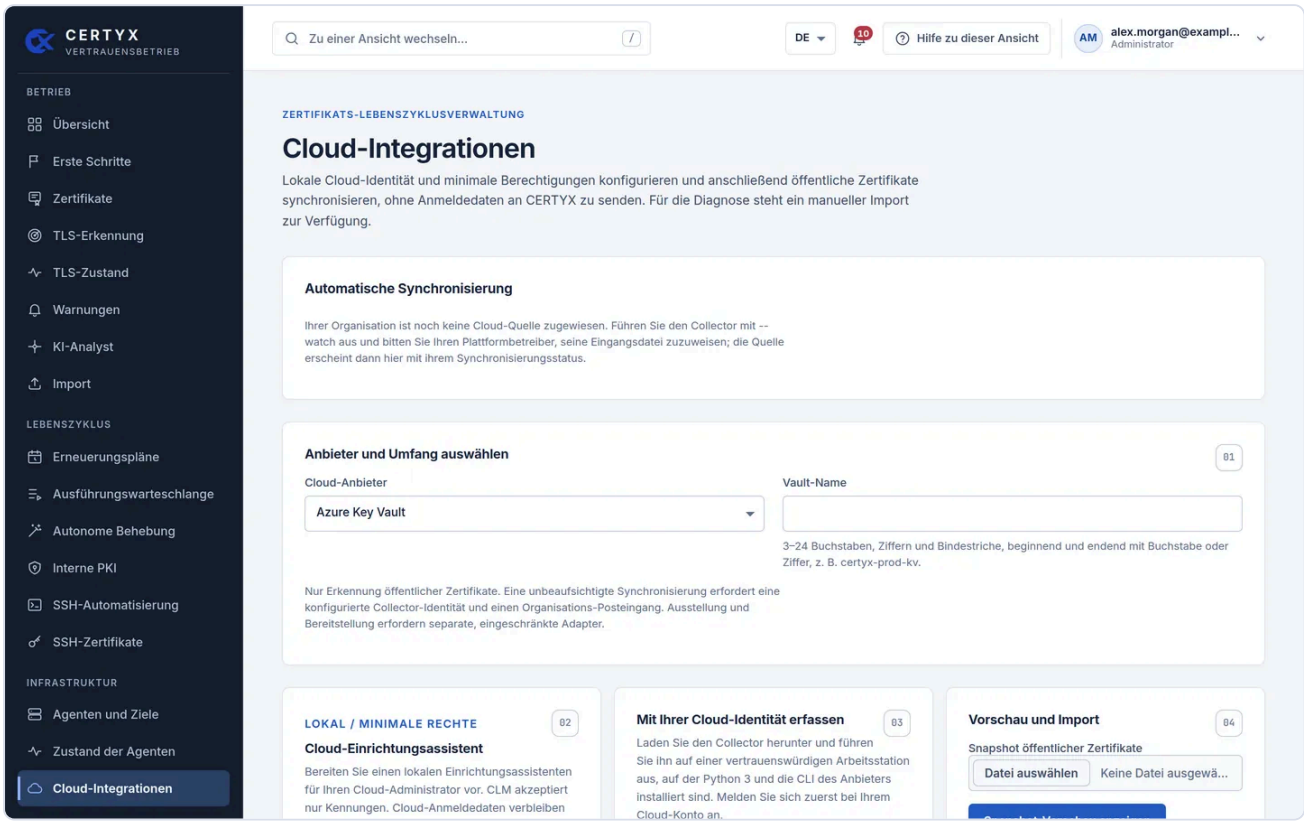
Nur Plattformadministratoren mit MFA. Benutzer der Organisationen sehen weder den Schlüssel noch diese Ansicht. Step-up: Jede Änderung in dieser Ansicht (außer Tests, Verbindungsprüfungen und dem Bestätigen eines Vorfalls) fragt nach dem aktuellen 6-stelligen Code Ihres eigenen Authenticators; ein bestätigter Code gilt für Clm:Identity:OperatorStepUpWindow (Standard 5 Minuten) auch für Ihre weiteren Änderungen im Kontrollraum. Ein falscher oder bereits verwendeter Code wird abgelehnt, zählt zur Kontosperre und wird protokolliert; Abbrechen verwirft die Änderung. Über Firmenanmeldung angemeldete Betreiber haben keinen lokalen Authenticator und können diese Änderungen nicht vornehmen.

EINSCHRÄNKUNGEN

Ohne Plattformdatenbank (eigenständige Installation) werden die Werte aus Clm:Analyst der Konfiguration schreibgeschützt angezeigt und hier kann kein Schlüssel eingegeben werden; Verbindung testen prüft sie dennoch. Ein mit einem anderen Schlüsselbund verschlüsselter Schlüssel ist nicht lesbar und muss erneut eingegeben werden. Die Adresse des Anbieters (Clm:Analyst:BaseUrl, Standard https://api.anthropic.com) wird nur in der Konfiguration gesetzt. Der Verbindungstest wartet höchstens 30 Sekunden und wiederholt nicht. Ein erfolgreicher Test belegt Schlüssel, Modell und Netzwerkpfad zu diesem Zeitpunkt; die Antwortqualität bewertet er nicht. Die Daten verarbeitet Anthropic im Rahmen der Vereinbarung des Betreibers mit Anthropic.

27 Cloud-Integrationen

Lokale Cloud-Identität und minimale Berechtigungen konfigurieren und anschließend öffentliche Zertifikate synchronisieren, ohne Anmeldedaten an CERTYX zu senden. Für die Diagnose steht ein manueller Import zur Verfügung.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Wählen Sie AWS, Azure oder GCP und den Bereich aus. Füllen Sie den lokalen IAM-Einrichtungsassistenten nur mit öffentlichen Kennungen aus. GCP erfordert ein bestehendes Dienstkonto im ausgewählten Projekt; dessen Rolle mit einer einzigen Berechtigung gewährt das öffentliche Auflisten, ohne Kontoschlüssel oder Föderation zu erstellen.
2. Wählen Sie „Einrichtungskonfiguration herunterladen“ (clm-cloud-setup.json; eine falsche Kennung wird mit dem erwarteten Format abgelehnt) und „Lokalen Assistenten herunterladen“ (cloud-setup.py). Führen Sie plan lokal aus, um minimale Richtlinien vorzubereiten, ohne Ihre Cloud zu ändern.
3. Prüfen Sie die Richtlinien. Führen Sie apply mit einer autorisierten Cloud-Administratoridentität aus und bestätigen Sie den Bereich ausdrücklich. Dadurch werden nur Berechtigungen für die Erkennung erstellt.
4. Konfigurieren Sie die Workload-Identität des Collectors und führen Sie dann doctor unter dieser Identität aus. Fehlgeschlagene Prüfungen liefern einen Exit-Code ungleich null; leere Bereiche werden als nicht vollständig getestet gemeldet.
5. Laden Sie in „Mit Ihrer Cloud-Identität erfassen“ cloud-collect.py herunter und führen Sie nach der Anmeldung mit der Anbieter-CLI den angezeigten Befehl aus; er schreibt eine neue clm-cloud.json und überschreibt keine vorhandene Datei.

6. Für eine unbeaufsichtigte Synchronisierung führen Sie den Collector mit --watch SEKUNDEN (mindestens 300) aus und bitten Ihren Plattformbetreiber, dessen nur für den Eigentümer zugängliche Eingangsdatei dieser Organisation zuzuweisen. Automatische Synchronisierung listet dann jede zugewiesene Quelle mit ihrem Zustand auf: wartet auf die erste Synchronisierung, funktioniert, Teilergebnis, fehlgeschlagen mit Grund oder vom Betreiber pausiert, zusammen mit Zertifikatsanzahl, letztem Erfolg und letztem Versuch. Das Feld wird alle 30 Sekunden aktualisiert, solange die Ansicht geöffnet ist. Ist noch keine Quelle zugewiesen, zeigt das Feld dies an. Manuelle Momentaufnahmen bleiben zur Fehlerbehebung verfügbar.
7. Manueller Import („Vorschau und Import“): Wählen Sie die Snapshot-Datei und „Snapshot-Vorschau anzeigen“. Der Server prüft sie, ohne etwas zu speichern, und zeigt Anbieter, Bereich, Zertifikatsanzahl, Warnungen und die Zertifikate. „In diese Organisation importieren“ fügt dann neue Zertifikate hinzu und meldet hinzugefügte, bereits vorhandene und Teilergebnisse. Ohne Vertrauensgraphen im Abonnement ist nur die Vorschau verfügbar.
8. Unix-Lebenszyklus-Agenten können genehmigte Text-Secrets aus Azure Key Vault, AWS Secrets Manager und Google Secret Manager über die kundenlokale CLI-Identität des Anbieters auflösen. Konfigurieren Sie exakte SecretBindings und führen Sie CIm.Agent secret-check mit der geschützten Lebenszyklus-Konfiguration als Dienstidentität aus, bevor Sie die Ausführung aktivieren. Die Werte bleiben lokal und werden nie ausgegeben. Siehe CUSTOMER-VAULTS.en.md. Die Auflösung über Provider-CLIs läuft nur auf Unix-Agenten; unter Windows stehen nur Secrets aus geschützten Dateien zur Verfügung. Private Schlüssel werden in Software auf dem Agent-Host erzeugt und gehalten (kein HSM), und der Agent versendet keine E-Mails vom Kundenhost.
9. HashiCorp Vault KV wird ebenfalls über eine exakte HTTPS-Bindung mount/path#field und einen kundenlokalen nativen Token-Helper unterstützt. TLS-Verifizierung ist erforderlich; Namespaces werden nicht unterstützt. Ein Lesevorgang schlägt fehl, wenn der Zugriff verweigert wird, die Identität widerrufen ist oder dem Vault-Zertifikat nicht vertraut wird. Das Vault-Token stammt aus dem Token-Helper des Kunden; CERTYX erstellt oder erneuert keine Vault-Identitäten.
10. Der AWS-Lebenszyklus verwaltet in ACM importierte Zertifikate. Auf dem Unix-Host des Kunden bereitet aws-adopt <protected-agent-config> <target-id> <protected-key-reference-json> eine geschützte Rollback-Baseline vor, nachdem der passende Schlüssel, der reale TLS-Endpunkt und der unveränderte ACM-Fingerabdruck geprüft wurden. Dieser Befehl liest AWS nur; er ersetzt das Cloud-Zertifikat nicht. Bestehender verwalteter Zustand erfordert eine Wiederherstellung statt einer Übernahme.
11. Das AWS-Paket enthält agent.aws-vault.json, aws-baseline-key.json und AWS-LIFECYCLE.md. Ersetzen Sie Platzhalter lokal; das Vault-Beispiel stellt Zertifikate einer privaten CA aus. Ein Erneuerungsauftrag ist erst erfolgreich, wenn ACM das neue Zertifikat enthält und die unabhängige TLS-Prüfung des ausgelieferten Endpunkts bestanden ist. In dieser Ansicht werden keine Anmeldedaten eingegeben.
12. Für ein genehmigtes importiertes AWS-Zertifikat erzeugt aws-plan <protected-agent-config> <target-id> eine minimale Ressourcen-Berechtigungsrichtlinie, ohne AWS zu kontaktieren. Es gewährt kein Rollenvertrauen und erstellt keine Infrastruktur. Lesen Sie AWS-LIFECYCLE.md, bevor Sie den Plan anwenden.
13. Die Store-Operationen für AWS ACM und Azure Key Vault ersetzen das Zertifikat, lesen es zurück, stellen die geschützte Baseline wieder her, wenn eine Änderung zurückgenommen werden muss, und lehnen ein Zertifikat mit nicht passendem Schlüssel ab. Die AWS-Erneuerung leitet Schlüsselalgorithmus/-größe und Verwendungseinschränkungen aus der geschützten Baseline ab; inkompatible Migrationen erfordern eine neue Ressource.

14. DigiCert CertCentral: Auf dem Host des Kunden liest Clm.Agent digicert-collect <config> <destination-id> <output.json> erworbene Zertifikate mit dem lokal gehaltenen API-Schlüssel und schreibt eine Momentaufnahme (Anbieter digicert), die hier importiert wird; Warnungen listen Domain- und Organisationsvalidierungen auf, die innerhalb von 60 Tagen ablaufen. Agent-Ziele der Art digicert bestellen Zertifikate oder stellen sie neu aus, innerhalb der konfigurierten Kaufrichtlinie.
15. Für die Azure-Agent-Ausführung konfigurieren Sie den exakten AzureKeyVault-Bereich (VaultUrl, CertificateName, TenantId, ManagedIdentityClientId) auf dem Server und dem Kunden-Agenten sowie einen unabhängigen VerifyHost. Verwenden Sie eine benutzerseitig zugewiesene verwaltete Identität. Auf dem Host des Kunden liest und verifiziert azure-adopt <protected-agent-config> <target-id> <protected-key-reference-json> <protected-public-chain-reference-json> das bestehende Zertifikat und bereitet eine geschützte Rollback-Baseline vor. Beide Referenzen werden lokal aufgelöst. Private Schlüssel werden weder aus Azure exportiert noch zu CERTYX hochgeladen. Siehe AZURE-LIFECYCLE.md. Der bloße Import einer Vault-Version ist keine erfolgreiche Bereitstellung: Der Auftrag ist erst nach unabhängiger TLS-Prüfung erfolgreich, und CERTYX stellt Anwendungsbindungen nutzender Azure-Dienste nicht auf die neue Version um. Dieser Cloud-Generierungs-Workflow läuft nur auf Unix-Agenten.
16. GCP-Erkennung: Wählen Sie Google Certificate Manager und geben Sie die exakte Projekt-ID ein. Führen Sie den angezeigten kundenlokalen Befehl cloud-collect.py gcp PROJECT --location global mit einer genehmigten Leseidentität aus. Importieren Sie die öffentliche Momentaufnahme hier oder verwenden Sie --watch mit einem nur für den Eigentümer zugänglichen Synchronisierungs-Eingangsordner. Verwenden Sie --location für einen separat genehmigten regionalen Standort. Fehlendes öffentliches PEM, auch bei Zertifikaten, die noch bereitgestellt werden, wird als Warnung gemeldet. Der IAM-Assistent erstellt eine projektbezogene Rolle zum öffentlichen Auflisten für das bestehende GCP-Dienstkonto. Führen Sie doctor mit ausdrücklicher Identitätsübernahme (Impersonation) dieses Kontos aus; dies erfordert eine genehmigte Föderation oder eine Berechtigung zur Token-Erstellung, die auf Kundenseite bereits konfiguriert ist. Es werden keine Token-Creator-Berechtigungen oder Kontoschlüssel erstellt.
17. Die GCP-Einrichtung schreibt vor der Änderung von IAM eine nur für den Eigentümer zugängliche gcp-apply-receipt.json. Ein vorhandener Beleg blockiert wiederholte Schreibvorgänge. Führen Sie cloud-setup.py reconcile --config CONFIG.json --output PLAN-DIRECTORY für schreibgeschützte Prüfungen der exakten Berechtigungen und der Bindung aus. IAM-Administratoren des Kunden lösen Teiländerungen anhand der Audit-Protokolle des Anbieters auf; der Abgleich erweitert niemals Berechtigungen.
18. Die Übernahme einer GCP-Baseline (gcp-adopt <protected-agent-config> <target-id> <protected-key-reference-json> [protected-public-chain-reference-json]) akzeptiert als letztes Argument eine optionale geschützte Referenz auf die öffentliche Ausstellerkette. Verwenden Sie sie, wenn Google Aussteller auslässt; der Agent validiert die Kette gegen genehmigte Vertrauensanker, bevor der Rollback-Zustand gespeichert wird. Schlüssel bleiben kundenlokal.
19. Auf Compute Engine kann der Agent ausdrücklich gcpIdentityKind=metadata für das genehmigte angehängte Dienstkonto wählen, ohne Anmeldedatenreferenz oder Kontoschlüssel. IAM und VM-OAuth-Bereich konfiguriert der Kunde. Föderation und Kundentresor bleiben verfügbar.

EINGABEN UND PARAMETER

- Öffentliche PEM-Zertifikate und Referenzen auf Cloud-Ressourcen; keine Anmeldedaten, Secrets oder privaten Schlüssel.

- Snapshot-Datei: JSON mit höchstens 5 MB und höchstens 250 Zertifikaten; Momentaufnahmen, die älter als 30 Tage sind, werden abgelehnt. In Snapshots akzeptierte Anbieter: azure, aws, gcp und digicert.
- Formate von Umfang und Identität (unter jedem Feld angezeigt; ein falscher Wert wird mit dem erwarteten Format abgelehnt): Azure-Vault-Name 3–24 Buchstaben, Ziffern und Bindestriche; AWS-Region wie eu-central-1, Konto-ID mit 12 Ziffern und Rolle arn:aws:iam::KONTO:role/NAME; GCP-Projekt-ID aus 6–30 Kleinbuchstaben, Ziffern und Bindestrichen; Ressourcen-ID des Azure-Vaults /subscriptions/.../providers/Microsoft.KeyVault/vaults/VAULT-NAME und Objekt-ID als GUID; GCP-Dienstkonto NAME@PROJEKT-ID.iam.gserviceaccount.com des gewählten Projekts.
- Berechtigungen, die der Assistent vorbereitet (plan) und vergibt (apply): AWS — eine Kundenrolle, der nur die angegebene Workload-Rolle mit einer eindeutigen External ID vertraut (sts:AssumeRole), mit acm:ListCertificates in der gewählten Region sowie acm:DescribeCertificate und acm:GetCertificate für Zertifikate dieses Kontos und dieser Region; Azure — eine benutzerdefinierte Rolle mit der einzigen Datenaktion Microsoft.KeyVault/vaults/certificates/read, der verwalteten Identität auf dem einen Vault zugewiesen; Google Cloud — eine Projektrolle mit der einzigen Berechtigung certificatemanager.certs.list, an das vorhandene Dienstkonto gebunden. Es werden keine Berechtigungen für Geheimnisse, private Schlüssel, Ausstellung oder Bereitstellung vergeben. Der Collector meldet den Snapshot-Umfang als Azure-Vault-Namen, AWS KONTO:REGION und GCP PROJEKT:STANDORT.

ERGEBNIS

Zertifikate erscheinen im Inventar und Abhängigkeiten von Cloud-Ressourcen im Vertrauensgraphen. Wiederholte Importe duplizieren keine Zertifikate.

BERECHTIGUNGEN

Einrichtungsassistent und Collector-Befehl stehen jeder Rolle der Organisation zur Verfügung. Synchronisierungsstatus, Snapshot-Vorschau und Import: Admin. Der Import erfordert zusätzlich den Vertrauensgraphen im Abonnement.

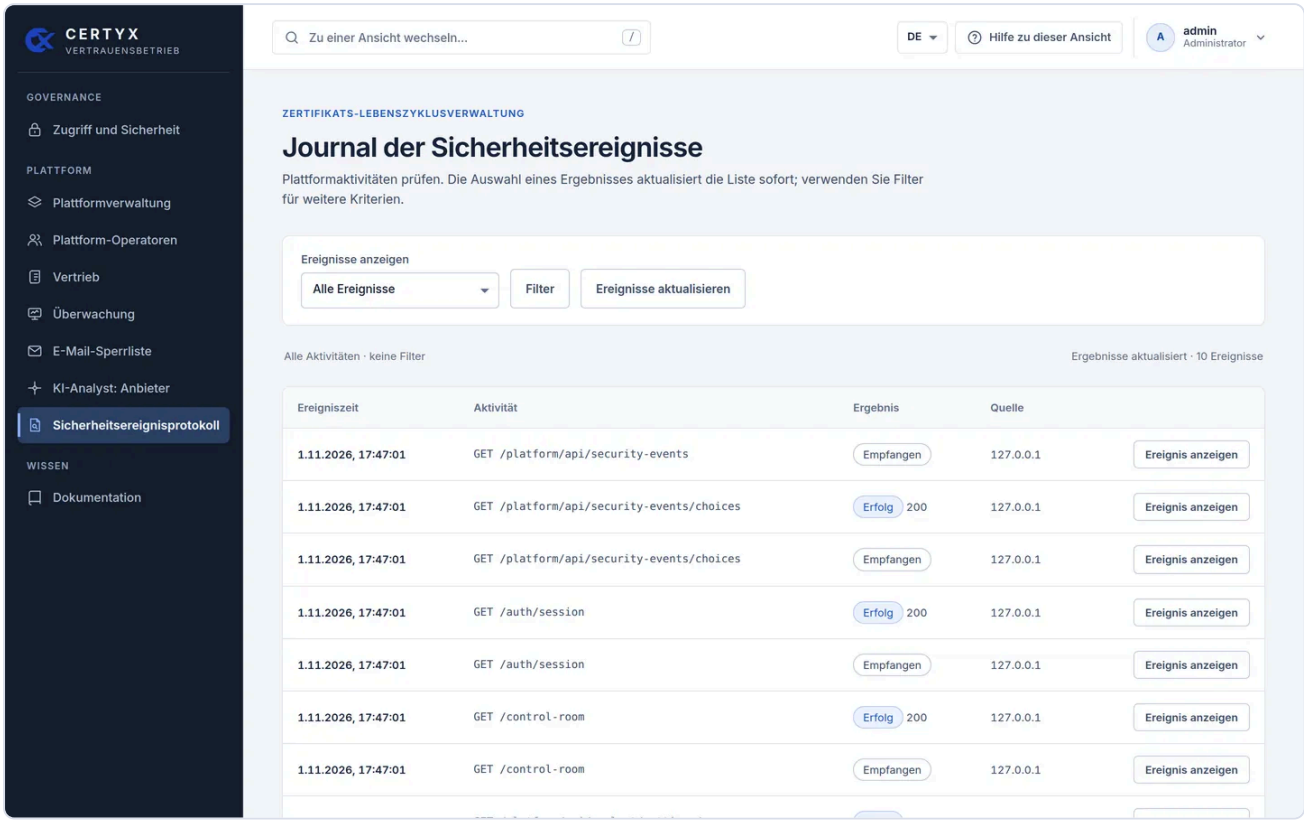
EINSCHRÄNKUNGEN

Der Assistent erfordert Python 3 und die CLI des Anbieters. Er erstellt Rollen für eine bestehende Workload-Identität; er erstellt oder verknüpft keine VM-Identitäten oder Föderationen. Azure erfordert Vaults mit aktiviertem RBAC. Die Cloud-Bereitstellung benötigt lokale Administratorberechtigungen, während der Collector nur Lesezugriff auf Zertifikate benötigt. Werte von Anmeldedaten werden nicht angenommen. Erfolgreiche Lesetests beweisen nicht das Fehlen weitergehender Berechtigungen. Erneuerung und Bereitstellung laufen über den Lebenszyklus-Agenten für ein Ausführungsziel mit einer Cloud-Ressource: AWS ACM (erneuter Import in dieselbe Zertifikat-ARN), Azure Key Vault (neue Version desselben Zertifikats) und Google Certificate Manager (Aktualisierung desselben selbstverwalteten Zertifikats); ein Auftrag gilt erst nach unabhängiger TLS-Verifizierung des ausgelieferten Endpunkts als erfolgreich. Der Import in einen Store stellt nutzende Azure- oder Google-Dienste nicht auf die neue Version um. Kunden-Anmeldedaten und private Schlüssel bleiben unter Kontrolle des Kunden. Secrets werden aus geschützten Dateien, HashiCorp Vault KV, Azure Key Vault, AWS Secrets Manager und Google Secret Manager aufgelöst; andere Tresorprodukte werden nicht unterstützt, Provider-CLIs laufen nur auf Unix-Agenten, und der Agent versendet keine E-Mails vom Kundenhost. Die Berechtigungen des Unix-Vault-Tokens werden bei jeder Verwendung erneut geprüft. Die Azure-Key-Vault-Speicheroperation bewahrt die bestehende Zertifikatsrichtlinie, Tags, den Aktivierungsstatus und das PEM/PFX-Speicherformat. Der Software-Import lehnt fehlende Richtlinien, deaktivierte Zertifikate und HSM-gestützte

Schlüssel ab. Er stellt das Zertifikat nicht auf Azure-Endpunkten bereit. Der Arbeitsbereich stellt keine Load Balancer (ALB) bereit. Die Kunden-Cloud ist optional: Vom Kunden gehostetes Vault KV/PKI bleibt eine Alternative unter Kontrolle des Kunden; geschützte Dateien sind ein Kompatibilitäts-Fallback, kein verschlüsselter Vault. DigiCert ist eine Anbieterwahl, keine Voraussetzung für das Konto. Das Lesen von Google-Secret-Manager-Secrets ist vom Lebenszyklus in Google Certificate Manager getrennt. Felder für den Import öffentlicher Zertifikate dürfen niemals private Schlüssel enthalten. Die AWS-Verifizierung ist durch das Konvergenzfenster des Agenten begrenzt (sechs Minuten für AWS-ACM-Ziele, sofern Settings.Connectors.CloudVerification des Agenten kein anderes ConvergenceWindow festlegt, da ALB TLS während der Propagierung eines erneuten Imports länger als zwei Minuten anhalten kann): aws-store-unread bedeutet, dass innerhalb der Grenze kein ACM-Lesevorgang abgeschlossen wurde; aws-store-not-converged bedeutet, dass der letzte ACM-Lesevorgang nicht mit dem genehmigten Fingerabdruck übereinstimmte; aws-endpoint-not-verified bedeutet, dass ACM übereinstimmte, aber nicht jede aufgelöste Load-Balancer-Adresse es mit gültiger Kette und fehlerfreiem Zustand ausgeliefert hat. Drosselung und abgelaufene Lesevorgänge werden innerhalb der Grenze wiederholt; Zugriffs-, Identitäts- und Validierungsfehler stoppen sofort. Beide erfordern eine Untersuchung; keiner beweist eine erfolgreiche Bereitstellung. Eine Stornierung durch den Kunden bleibt eine Stornierung. Ein unvollendetes AWS-Wiederherstellungsjournal erzwingt einen abgesicherten Import seiner vorherigen geschützten Generation, auch wenn ein ACM-Lesevorgang bereits übereinstimmt. Der Abschluss erfordert weiterhin eine unabhängige TLS-Verifizierung; bei einem Fehler wird das Journal für den Abgleich aufbewahrt. GCP-apply und -reconcile laufen nur unter Unix, weil ihre Belege nur für den Eigentümer zugängliche Unix-Pfade erfordern.

28 Journal der Sicherheitsereignisse

Plattformaktivitäten prüfen. Die Auswahl eines Ergebnisses aktualisiert die Liste sofort; verwenden Sie Filter für weitere Kriterien.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Wählen Sie unter Ereignisse anzeigen oberhalb der Tabelle (Zehn Ereignisse pro Seite, neueste zuerst) Alle Ereignisse, Verweigert, Serverfehler, Abgelehnte Anfrage, Erfolg, Empfangen oder Anmeldung; die Liste wird sofort aktualisiert. Ereignisse aktualisieren lädt die neuesten Ereignisse mit den aktuellen Filtern.
2. Anmeldeereignisse (Anmeldung) werden für jede erfolgreiche und fehlgeschlagene Anmeldung, Abmeldung, Kontosperre und MFA-Änderung erfasst und der Organisation des Benutzers zugeordnet; Anmeldungen von Plattformbetreibern und Anmeldungen ohne passendes Konto werden unter platform erfasst. Ereignis anzeigen zeigt den Ereignisnamen, die E-Mail-Adresse des Benutzers (bei einer fehlgeschlagenen Anmeldung als eingegeben und nicht bestätigt gekennzeichnet), die Anmeldemethode, das Ergebnis, den Grundcode und den User-Agent; das eingegebene Passwort oder der Code wird nie erfasst.
3. Öffnen Sie Filter für Konto, Organisation, IP, UTC-Zeitraum oder technische Kriterien. Filter anwenden kehrt zu den Ergebnissen zurück.
4. Ladeanzeige, Anzahl der Ergebnisse und Anzahl aktiver Filter zeigen, was sich geändert hat. Filter zurücksetzen stellt alle Aktivitäten wieder her.

5. Ereignis anzeigen öffnet fokussierte Details. Diese Anfrage filtern verfolgt eine Anfrage, ohne ihre Kennung zu kopieren. Jede Anfrage hat zwei Einträge: Empfangen, geschrieben beim Eingang der Anfrage, bevor der Server prüft, wer sie gesendet hat (Benutzer und Organisation sind noch nicht ermittelt, Status 0), und den Ergebniseintrag mit Benutzer, Organisation und HTTP-Status. Ein Eintrag Empfangen ist kein fehlgeschlagener Versuch und kein Angriff; er hält eine Anfrage auch dann fest, wenn sie vor der Antwort abbricht. Diese Anfrage filtern zeigt beide Einträge.
6. Ältere Ereignisse ersetzt die Seite. Journal-Werkzeuge enthalten die Integritätsprüfung, den Export aller Ereignisse, die den Filtern entsprechen (CSV oder JSON, nicht nur die sichtbare Seite), und die geltende Aufbewahrung.
7. Wählen Sie nach dem Wechsel zu älteren Seiten Neueste Ereignisse, um zum Anfang zurückzukehren. In den Journal-Werkzeugen prüft Integrität des Journals prüfen die Hash-Kette des gesamten aufbewahrten Journals, und Plattform-Prüfprotokoll listet die letzten 100 geschäftlichen Änderungen der Plattformadministratoren (Kunden, Abonnements, Instanzen und Kundenkonten).
8. SIEM-Export verwaltet die plattformweiten Ziele: Bereich Plattformbetreiber (eigene Ereignisse der Betreiber) oder Alle Ereignisse (jede Organisation), dann den Transport (HTTPS, Splunk HTTP Event Collector, Syslog über TLS, Azure Monitor Logs Ingestion für Microsoft Sentinel, OpenTelemetry Logs (OTLP/HTTP) oder Dateiarchiv), ein Format und ein Schemaprofil unter den vom Server dafür zugelassenen, wie in der SIEM-Export-Ansicht der Organisation. Jedes Ziel zeigt Route, Position, Rückstand, letzten Erfolg und Fehler, Fehler in Folge mit dem nächsten Versuch und ein Ereignis, das der Empfänger weiter ablehnt; Verbindung prüfen testet DNS, TCP und TLS, ohne etwas zu senden, und Testereignis senden stellt zusätzlich ein Testereignis zu (Kategorie Integration, eine UUID als event_id), jeweils mit den Stufen und der Abhilfe. Netzwerkziele haben Filter (Ergebnisse, Kategorien, Ereigniscodes, Mindestschweregrad), eine Zustellrichtlinie, optional ein Clientzertifikat (gegenseitiges TLS) und einen Modus der Sperrprüfung, und Erneut senden ab… setzt die Position auf eine Sequenz oder einen Zeitpunkt zurück (nie vor; Empfänger deduplizieren nach event_id). Änderungen erfordern die MFA-Sitzung. Bei einem ohne Geheimnis hinzugefügten HTTPS-Ziel erzeugt CERTYX das Signaturgeheimnis und zeigt es einmal zum Kopieren in den Empfänger an; Neues Geheimnis ersetzt es sofort (das bisherige wird ungültig) und zeigt das neue einmal an. Jedes Feld verlinkt auf den passenden Abschnitt des SIEM-Integrationshandbuchs (auch als PDF unter Dokumentation).
9. Der Bereich Plattformbetreiber erhält die Anmeldeereignisse der Betreiber und Anmeldungen, die keiner Organisation zugeordnet sind; Alle Ereignisse erhält zusätzlich die Anmeldeereignisse jeder Organisation. Kreuzen Sie unter Zu exportierende Ergebnisse Anmeldeereignisse an, um nur diese zu senden, oder lassen Sie alle Felder leer; die Hilfe zum SIEM-Export der Organisationsansicht nennt die Anmeldefelder jedes Formats.
10. Dateiarchive für die Plattform: Wählen Sie im SIEM-Export den Bereich Plattformbetreiber oder Alle Ereignisse, den Transport Dateiarchiv auf dem Server und das Format CSV (Layout der ersten Version oder kanonisch) oder NDJSON, mit Aufbewahrung und optional gzip. Die Dateien werden unter Clm:Siem:PlatformArchiveDirectory geschrieben (Standard: der Ordner platform in Clm:Siem:ArchiveRoot), unter Archivdateien mit Größe und SHA-256 aufgeführt und einzeln oder als ZIP heruntergeladen; Downloads erfordern die MFA-Sitzung und werden protokolliert. Nutzen Sie Nur senden an den Netzwerkzielen (Ergebnisse, Kategorien, Ereigniscodes, Mindestschweregrad), um dem SIEM weniger zu senden, während das Archiv jedes Ereignis behält; Health-Prüfungen werden nur mit Clm:Siem:ExportHealthProbes gesendet. Exportierte Ereignisse enthalten ID, Name und Art der Organisation sowie die Instanz, sodass der Bereich Alle Ereignisse in einem SIEM nach Organisation getrennt werden kann.

EINGABEN UND PARAMETER

- Wählen Sie ein erfasstes Konto oder einen Systemakteur aus. Eine leere Auswahl schließt alle ein.
- Wählen Sie eine Organisation nach Namen aus; Systemeinträge können technische Bereichsnamen verwenden.
- Wählen Sie eine vom Journal erfasste Instanz aus.
- Wählen Sie einen beobachteten HTTP-Status aus. Null kennzeichnet einen Eintrag Empfangen, der vor der Antwort geschrieben wird.
- Verwenden Sie Diese Anfrage filtern in einem aufgeklappten Ereignis, um dies automatisch auszufüllen, oder geben Sie eine Anfrage-ID ein.
- Optional IP, Routenfragment und UTC-Zeitraum.
- SIEM-Ziel: Transport, Format und Schemaprofil; HTTPS-Adresse oder Syslog-Host, Port, Framing und LEEF-2.0-Trennzeichen; transportspezifische Felder (Splunk-Sourcetype und Index; Sentinel-Datensammlungsregel, Stream, Microsoft-Entra-Mandant und Anwendung); Filter, Zustellrichtlinie, optional vertrauenswürdige Stammzertifikate, Clientzertifikat und -schlüssel (PEM) und Sperrprüfungsmodus; OTLP-Inhalt, Name des Authentifizierungs-Headers und gzip; die Regeln der Feldzuordnung; die Ereignisgestaltung (Vorgabe Vollständig, Ausgewogen, Sparsam oder Benutzerdefiniert mit Änderungsdetail, Feldauswahl, leeren Feldern, größtem Ereignis, Namensstil, Zeitformat, Syslog-MSGID und APP-NAME) und die weiteren Filter (Routen, Akteure, ausgeschlossene Kategorien und Ereigniscodes), beschrieben in der Hilfe zum SIEM-Export; das Geheimnis (HMAC-Schlüssel, HEC-Token, geheimer Clientschlüssel oder Wert des OTLP-Headers) und der Clientschlüssel werden verschlüsselt gespeichert und nie wieder angezeigt.

ERGEBNIS

Gefilterter, begrenzter Zugriff auf das aufbewahrte Sicherheitsjournal, herunterladbare Exporte des gefilterten Journals und fortlaufender Export an SIEM-Ziele. Einrichtungslinks für den Authenticator erscheinen als mfa-setup.mail.sent (Zustellung per E-Mail oder als der Administration angezeigter Link, mit Fehlergrund), mfa-setup.mail.used und mfa-setup.mail.expired, zugeordnet der Organisation des Kontos; der Link selbst wird nie gespeichert.

BERECHTIGUNGEN

Plattformadministrator auf der Betreiber-Zulassungsliste, dessen Sitzung mit MFA angemeldet wurde; andere Identitäten können weder die Ansicht noch ihre API öffnen. SIEM-Änderungen, -Prüfungen, -Tests, erneutes Senden und neue Geheimnisse werden für Sitzungen der mobilen CERTYX-App abgelehnt. Step-up: Jede Änderung in dieser Ansicht (außer Tests, Verbindungsprüfungen und dem Bestätigen eines Vorfalls) fragt nach dem aktuellen 6-stelligen Code Ihres eigenen Authenticators; ein bestätigter Code gilt für Clm:Identity:OperatorStepUpWindow (Standard 5 Minuten) auch für Ihre weiteren Änderungen im Kontrollraum. Ein falscher oder bereits verwendeter Code wird abgelehnt, zählt zur Kontosperre und wird protokolliert; Abbrechen verwirft die Änderung. Über Firmenanmeldung angemeldete Betreiber haben keinen lokalen Authenticator und können diese Änderungen nicht vornehmen.

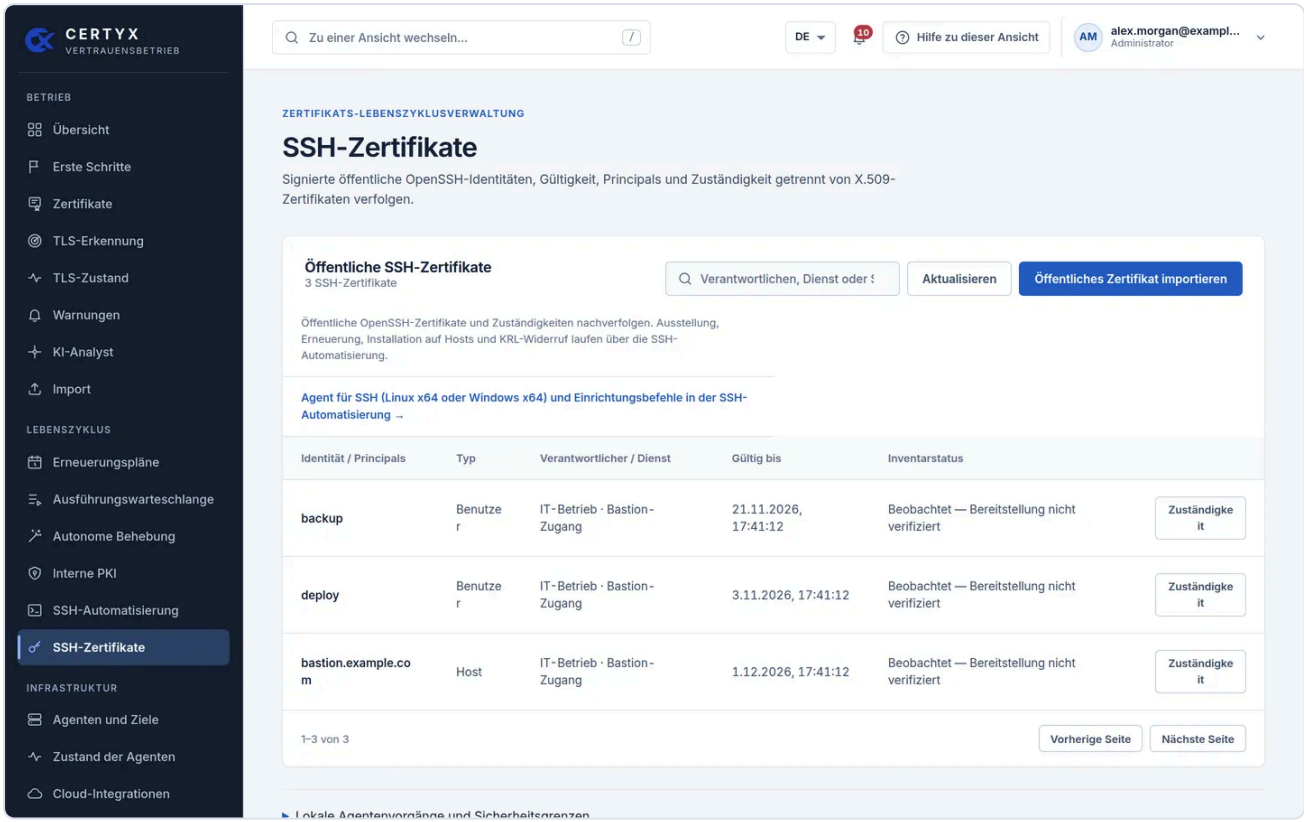
EINSCHRÄNKUNGEN

Die Quell-IP ist kein Nachweis für Person oder Standort. Die Seitenaufteilung löscht keine Ereignisse. Ein Export enthält höchstens Clm:AuditExport:MaxRows Ereignisse (Standard 100.000) und wird selbst protokolliert. Auswahllisten enthalten bis zu 500 unterschiedliche Werte; ohne Plattformdatenbank (lokales Dateiprotokoll) werden die letzten 5.000 Ereignisse untersucht und der SIEM-Export ist nicht verfügbar. Ereignisse werden ohne automatisches Löschen aufbewahrt; die Anwendungsrolle kann sie nur hinzufügen

und lesen. Die SIEM-Zustellung erfolgt mindestens einmal: Ein abgelehnter Stapel wird mit Backoff und Jitter wiederholt und löst den Vorfall siem-delivery aus, der nach den Versuchen kritisch wird; ein Rückstand über seiner Grenze löst siem-backlog aus, und nichts wird verworfen; ein Ereignis, das der Empfänger weiter ablehnt, wird bis zur Annahme wiederholt, sofern das Überspringen nicht eingeschaltet ist (siem.event.skipped). Empfänger deduplizieren nach event_id. Erneut senden ab... rückt nie vor und wird für Dateiarchive abgelehnt; bei Plattformzielen fragt es wie andere Änderungen den Step-up-Code ab. In Clm:Siem definierte Ziele werden schreibgeschützt aufgeführt. Das Zertifikat des Empfängers wird immer geprüft; ein Clientzertifikat (gegenseitiges TLS) wird vorgelegt, wenn eines eingegeben ist, und die Sperrprüfung akzeptiert einen unbekannten Status im Modus Soft-Fail (Standard) und lehnt ihn im Modus Hard-Fail ab. OpenTelemetry Logs nutzen nur OTLP/HTTP; ein Teilerfolg wird nicht erneut gesendet, sondern protokolliert (siem.event.rejected, Vorfall siem-rejected) und kann mit Erneut senden ab erneut gesendet werden. Plattformweite Ziele dürfen private, Loopback- oder Link-Local-Adressen verwenden; Clm:Siem:AllowPrivateDestinations beschränkt nur die Ziele, die Organisationen selbst verwalten. Ein Plattform-CSV-Archiv behält jedes Ereignis seines Bereichs (Alle Ereignisse: jede Organisation) für seine Aufbewahrung; planen Sie den Speicherplatz des Archiv-Volumes und binden Sie dasselbe Verzeichnis auf jeder Instanz ein. Anfragen von Plattformbetreibern werden unter dem Mandanten platform erfasst (wie ihre Anmeldungen), daher exportiert der SIEM-Bereich Plattformbetreiber sie; Einträge vor dem 18.10.2026 behalten den Mandanten platform-control. Jede Änderung eines Betreibers an einem Kunden wird zusätzlich unter diesem Kunden erfasst (Akteur platform:<Konto-ID des Betreibers>).

29 SSH-Zertifikate

Signierte öffentliche OpenSSH-Identitäten, Gültigkeit, Principals und Zuständigkeit getrennt von X.509-Zertifikaten verfolgen.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Den Agent für SSH (Linux x64 oder Windows x64) mit Prüfsummen, Signaturen und Einrichtungsbefehlen erhalten Sie unter SSH-Automatisierung → SSH-Agent installieren und verbinden.
2. Konfigurieren Sie auf einem genehmigten Unix-Host des Kunden die lokale SSH-CA, das geschützte Zustandsverzeichnis und die zulässigen Benutzer-/Host-Principals.
3. Führen Sie Clm.Agent ssh issue <config> <operation-UUID> user|host <principal> <minutes> aus; Wiederholungen mit derselben Operations-ID stellen dasselbe Zertifikat wieder her.
4. Wählen Sie „Öffentliches Zertifikat importieren“ und fügen Sie nur die öffentliche Zeile der identity-cert.pub ein. Weisen Sie Verantwortlichen, Dienst und Umgebung zu. Ein erneuter Import desselben Zertifikats liefert den bestehenden Eintrag ohne Duplikat. Die Suche erfasst Verantwortlichen, Dienst oder Schlüssel-ID; längere Listen blättern Sie mit den Seitenschaltflächen.
5. Verwenden Sie Zuständigkeit, um Verantwortlichen, Dienst, Umgebung zu ändern oder einen Inventareintrag zu archivieren. Der Dialog zeigt den CA-Fingerabdruck; die Signaturprüfung stellt kein Vertrauen in diese CA her. Die Archivierung widerruft nicht den Host-Zugriff. Hat zwischenzeitlich jemand den Eintrag geändert, wird das Speichern abgelehnt; aktualisieren Sie und versuchen Sie es erneut.

6. Für einen lokalen Widerruf führen Sie Clm.Agent ssh revoke <config> <operation-UUID> aus. Veröffentlichen Sie die resultierende revoked.krl über RevokedKeys auf jedem SSH-Server und prüfen Sie, dass der Zugriff abgelehnt wird.
7. Weitere lokale Befehle: ssh list <config> listet die von der lokalen CA ausgestellten Zertifikate; ssh deploy-host oder ssh deploy-user <config> <target-config> <operation-UUID> installiert ein ausgestelltes Host-Zertifikat oder ein Workload-Benutzerzertifikat auf dem lokal konfigurierten Ziel mit Verifizierung und Rollback; ssh export-krl <config> <tenant-ID> <CA-fingerprint> <new-file> schreibt den signierten öffentlichen KRL-Umschlag, und ssh apply-krl <consumer-config> <envelope> wendet einen Umschlag auf einem Consumer an.
8. Eigenständige lokale Erneuerung ohne Meldung an CERTYX: configure-ssh-linux.sh enable-renewal <heruntergeladenes Profil> schreibt renewal.json aus der lokalen CA-Richtlinie und dem Profil, führt einen Zyklus Clm.Agent ssh renew über systemd aus und aktiviert clm-ssh-renewal.timer (ein Zyklus pro Minute, ohne Netzwerkzugriff, Journal-Kennung clm-ssh-renewal); unter Windows registriert configure-ssh-windows.ps1 enable-renewal die Aufgabe CERTYX SSH Renewal. Ein fehlgeschlagenes, blockiertes oder in Konflikt stehendes Profil lässt den Zyklus sichtbar scheitern (failed-Unit bzw. Aufgabenergebnis ungleich null); renewal-status zeigt es, disable-renewal entfernt die Erneuerung. Ein Profil wird entweder mit add-profile oder mit enable-renewal erneuert. ready-local bestätigt nur ein lokales Paket; eine entfernte Installation ist damit nicht verbunden.
9. Für plattformverwaltete Erneuerung und verifizierte Host-Bereitstellung öffnen Sie SSH-Automatisierung. Weisen Sie aktive Benachrichtigungsgruppen zu und prüfen Sie den separaten Zustand der SSH-Workload. Lokale KRL-Consumer können im verwalteten Agenten konfiguriert werden; die Verteilung an eine entfernte Flotte ist weiterhin separat.
10. Für eine kundengesteuerte entfernte KRL-Übertragung führen Sie ssh publish-krl mit geschützter Publisher-Konfiguration aus und stellen nur dessen öffentlichen Umschlag über eine separate HTTPS-Relay-Identität bereit. Führen Sie ssh sync-krl mit einem geschützten Consumer-Abonnement aus. Signierte Veröffentlichungen laufen nach einer Stunde ab und werden automatisch aktualisiert; Weiterleitungen, fehlerhaftes Vertrauen, übergroße Daten, Manipulationen und abgelaufene Veröffentlichungen werden abgelehnt. Bestehende Widerrufe bleiben nach Fehlern erhalten. OpenSSH erzwingt den Ablauf des Umschlags nicht selbst. Den Zustand melden zentral nur Consumer, die für die KRL-Meldung registriert sind; CERTYX legt nicht fest, welche Hosts die KRL verwenden sollen. Alte Umschläge ohne signierte Zeitgrenzen müssen erneut exportiert werden. Eine neue CA kann vor der Ausstellung eine leere KRL initialisieren; der Verlust der KRL bei einer bereits verwendeten CA erfordert eine Wiederherstellung.
11. Für zentrale Sichtbarkeit registrieren Sie eine separate Consumer-Identität und aktivieren ausdrücklich die KRL-Consumer-Berichterstattung; sie gewährt keine Berechtigung zur SSH-Ausstellung oder Host-Installation. Führen Sie ssh monitor-krl mit der geschützten Identitäts- und Abonnementkonfiguration aus. Agent-Zustand zeigt die gemeldete Revision, den Ablauf der signierten Veröffentlichung, Synchronisierungsfehler und versäumte Berichtsfenster; eine fehlerfreie Erkennung kann einen KRL-Fehler nicht verdecken. Die Plattformüberwachung umfasst diese Agent-Fehler. Es handelt sich um authentifizierte Beobachtungen des Agenten, nicht um einen unabhängigen Nachweis, dass jeder Host die widerrufene Identität ablehnt. Verwenden Sie eine registrierte Identität je Consumer.

EINGABEN UND PARAMETER

- Ein Ed25519-OpenSSH-Zertifikat, signiert von einer Ed25519-CA, mit einem endlichen Gültigkeitszeitraum. Private Schlüssel werden abgelehnt.

- Lokale CA-/Zustandspfade müssen absolut, ohne symbolische Links und nur für den Eigentümer zugänglich sein. Weder ein CA-Schlüssel noch ein privater Endpunktschlüssel wird an die SaaS gesendet.
- Importformat: eine Zeile ssh-ed25519-cert-v01@openssh.com AAAA... mit optionalem Kommentar, wie in einer -cert.pub-Datei, höchstens 64.000 Zeichen.

ERGEBNIS

Seitenweises, nach Organisationen isoliertes SSH-Inventar, kryptografisch verifizierte Signaturen, versionierte Zuständigkeit und im Prüfprotokoll erfasste Änderungen. Der Agent stellt Zertifikate lokal aus und erzeugt KRLs. Die lokale Erneuerung verwendet dauerhafte ausstehende Operationen, atomare Paketzeiger und Sperren bei Widerruf/Richtlinienkonflikten.

BERECHTIGUNGEN

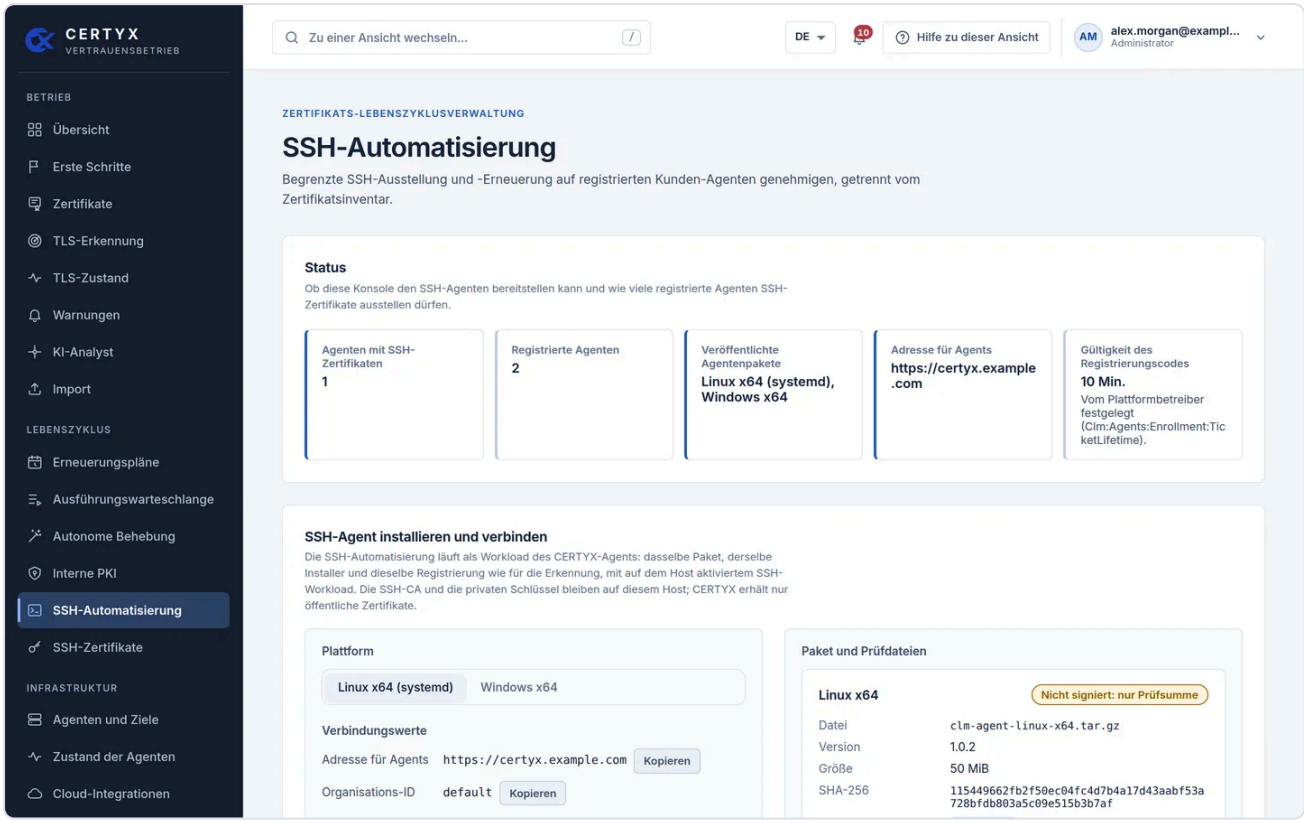
Alle Rollen der Organisation lesen; Admin und Operator importieren und bearbeiten, Auditor liest nur. Die lokale CA-Nutzung erfordert eine ausdrückliche Principal- und Gültigkeitsrichtlinie.

EINSCHRÄNKUNGEN

Die SSH-Automatisierung umfasst plattformgenehmigte Aufträge, unbeaufsichtigte begrenzte Erneuerung, verifizierte Installation/Rollback auf Unix-Hosts, lokale signierte KRL-Consumer und SSH-Benachrichtigungsereignisse. CERTYX konfiguriert weder CA-Vertrauen noch Widerrufslisten in der OpenSSH-Konfiguration entfernter Hosts und verfolgt nicht, welche Hosts die KRL verwenden sollen. Benutzerzertifikate werden nur für kundenlokale Unix-Workload-Identitäten installiert, nicht für Konten von Personen. SSH-Operationen laufen auf Linux- und Windows-Agenten (OpenSSH für Windows), und die SSH-CA verwendet ausschließlich Ed25519-Schlüssel. SSH-Benachrichtigungen werden per E-Mail über das SMTP-Relay der Organisation an die Empfängergruppen des Profils gesendet. Eine gültige Inventarsignatur beweist weder den Auslieferungsstatus noch den Widerruf in der Flotte. Lokale CA-Schlüsseldateien sind kein HSM. Die lokale SSH-Zertifizierungsstelle schreibt den Inhalt des Seriennummernzählers und dessen Verzeichniseintrag vor dem Signieren dauerhaft auf den Datenträger. Ein Fehler bei der Speichersynchronisierung blockiert die Ausstellung; prüfen Sie den geschützten lokalen Speicher und wiederholen Sie nach der Reparatur dieselbe Operations-ID. Signiert wird auf einem Host; verteiltes Signieren wird nicht unterstützt. Kundenlokale Connector-Sperrdateien müssen unter Unix reguläre, nur für den Eigentümer zugängliche Dateien ohne symbolische übergeordnete Verzeichnisse sein. Unsichere bestehende Sperrdateien werden abgelehnt; ein Administrator muss die Speicherberechtigungen korrigieren, bevor ein neuer Versuch erfolgt. Diese Konnektoren laufen nur auf Unix-Agenten.

30 SSH-Automatisierung

Begrenzte SSH-Ausstellung und -Erneuerung auf registrierten Kunden-Agenten genehmigen, getrennt vom Zertifikatsinventar.



Beispieldaten: Organisationen, Personen, Hosts und Adressen sind fiktiv.

SO FUNKTIONIERT ES

1. Die Ansicht ist in Karten gegliedert: Status (Agenten mit SSH-Zertifikaten, registrierte Agenten, veröffentlichte Pakete, die Adresse für Agenten und die konfigurierte Gültigkeit des Registrierungscodes), SSH-Agent installieren und verbinden, Agenten und SSH-Berechtigungen sowie Profile, Auftragsverlauf und Sperrungen. Wählen Sie in „SSH-Agent installieren und verbinden“ Linux x64 (systemd) oder Windows x64: Der Bereich zeigt die Paketkarte dieser Plattform (dieselbe Karte wie unter „Agenten und Ziele“: Dateiname, Version, Größe, SHA-256 mit Kopieren-Schaltfläche, Stand der Herausgebersignatur und des Release-Manifests sowie Download-Schaltflächen für das Paket, seine .sha256-Datei, die .p7s-Signatur und den .tsr-Zeitstempel, sofern veröffentlicht, das Release-Manifest mit seiner Signatur und den Prüfer, jeweils unter dem eigenen Dateinamen gespeichert) oder meldet, dass das Paket auf diesem Server nicht veröffentlicht ist, zusammen mit dem Veröffentlichungsschritt des Betreibers. Administratoren erstellen hier den Einmal-Registrierungscode und laden die Token-Datei herunter; die nummerierten Schritte enthalten kopierfertige Befehle aus der Adresse für Agents und Ihrer Organisations-ID: Vertrauensschritt für eine private Agent-CA, Kopieren der Token-Datei in ein leeres Arbeitsverzeichnis auf dem Host, Download (das Archiv wird nur mit einem gültigen Registrierungscode ausgeliefert, den der Befehl aus der Datei liest; der Download-Link im Bereich funktioniert in Ihrer angemeldeten Konsolensitzung) und Prüfung (ersetzen Sie <PUBLISHER-SHA256>

durch den unabhängig erhaltenen Herausgeber-Fingerabdruck), Installer im Verzeichnis clm-agent mit ../clm-enrollment.token und Statusprüfung. Es gibt ein Agent-Paket; SSH ist ein Workload dieses Agents.

2. Die nummerierten Installationsschritte (jeder ein eigener Block mit Titel und dem zu kopierenden Befehl) öffnen sich von selbst, solange kein Agent die SSH-Berechtigung hat. Erteilen Sie in „Agenten und SSH-Berechtigungen“ dem registrierten Agent „SSH-Zertifikate“ (ruft genehmigte Profile ab) und für Installationen „SSH-Installation“; die Tabelle zeigt den letzten Kontakt und den letzten Bericht des SSH-Workloads. Führen Sie auf dem Host configure-ssh-linux.sh init (Linux, als root) oder configure-ssh-windows.ps1 init (Windows, Administrator-PowerShell) aus: Es erstellt die Host-CA (/etc/clm-ssh oder C:\ProgramData\CLM-SSH, nur für den Eigentümer) und gibt den CA-Fingerabdruck für das Profil aus. Nach Genehmigung und Download des Profils führt add-profile ./ssh-profile-<ID>.json einen geprüften Zyklus ssh manage --once aus und startet clm-ssh.service (Linux) bzw. die geplante Aufgabe „CERTYX SSH Workload“ (Windows, LocalSystem); ein fehlgeschlagener Zyklus nennt seine Ursache (z. B. HTTP 403 ohne SSH-Berechtigung) und es wird nichts gestartet. Optional lässt trust-user-ca den lokalen sshd Benutzerzertifikate dieser CA akzeptieren (TrustedUserCAKeys, mit sshd -T geprüft, Sicherung wiederhergestellt, wenn sshd nicht neu lädt). Prüfen Sie mit sudo clm-agent status (Zeile Capabilities enthält ssh) und dem Skriptstatus. Unter Windows Server 2025 lässt sshd standardmäßig nur Mitglieder von administrators und OpenSSH Users zu (AllowGroups): Nehmen Sie Konten, die sich mit Benutzerzertifikaten anmelden, in OpenSSH Users auf, und starten Sie den OpenSSH-Server vor trust-user-ca einmal, damit sshd_config existiert.
3. Wählen Sie Neues Profil und geben Sie den registrierten Agenten mit SSH-Fähigkeit, Principal und Typ (Benutzer oder Host), Lebensdauer, Erneuerungsfenster, Gültigkeit der Genehmigung, unabhängig genehmigten CA-Fingerabdruck, Umgebung, zuständigen Verantwortlichen oder Team, Dienst oder Host, der die Identität verwendet, und optional Verantwortlichkeitsgruppen an; dann Genehmigung anfordern. Ohne aktivierten Agenten mit SSH-Fähigkeit weist das Formular darauf hin und kann nicht abgesendet werden.
4. Ein anderer Administrator wählt im Register Profile beim Profil Umfang genehmigen (wer angefordert hat, kann nicht selbst genehmigen). Wählen Sie Öffentliches Profil herunterladen und übernehmen Sie es in die kundenlokale verwaltete Konfiguration; private CA- und Identitätspfade bleiben auf diesem Host.
5. Eigenständige lokale Erneuerung ohne Meldung an CERTYX: configure-ssh-linux.sh enable-renewal <heruntergeladenes Profil> schreibt renewal.json aus der lokalen CA-Richtlinie und dem Profil, führt einen Zyklus Clm.Agent ssh renew über systemd aus und aktiviert clm-ssh-renewal.timer (ein Zyklus pro Minute, ohne Netzwerkzugriff, Journal-Kennung clm-ssh-renewal); unter Windows registriert configure-ssh-windows.ps1 enable-renewal die Aufgabe CERTYX SSH Renewal. Ein fehlgeschlagenes, blockiertes oder in Konflikt stehendes Profil lässt den Zyklus sichtbar scheitern (failed-Unit bzw. Aufgabenergebnis ungleich null); renewal-status zeigt es, disable-renewal entfernt die Erneuerung. Ein Profil wird entweder mit add-profile oder mit enable-renewal erneuert. ready-local bestätigt nur ein lokales Paket; eine entfernte Installation ist damit nicht verbunden.
6. Führen Sie Clm.Agent ssh manage <protected-managed-config> [--once] aus. Der Agent verbindet sich ausgehend über mTLS, ruft dauerhafte Aufträge ab und behält alle privaten Schlüssel lokal.
7. Verwenden Sie die Registerkarten Profile und Auftragsverlauf, um Genehmigung, Ablauf und Fehler zu prüfen. Automatisierung stoppen lehnt weitere Übernahmen/Veröffentlichungen ab.
8. Für die Host-Installation wählen Sie unter Registrierte Agents „Bereitstellung von SSH-Identitäten aktivieren“ und markieren im Profil „Diese SSH-Identität installieren und verifizieren“. Der Kundenadministrator stellt ein geschütztes lokales Ziel, eine bestehende Baseline, feste

Validierungs-/Neuladewerkzeuge und eine CA-gepinnte SSH-Prüfung bereit; unter Linux erlaubt configure-ssh-linux.sh enable-host-deploy dem Agent-Konto genau sshd -t und das Neuladen von sshd über sudo (mit visudo geprüfte Regel und Drop-in des Dienstes; disable-host-deploy entfernt beides). Der Agent installiert ein vollständiges Schlüssel-/Zertifikatspaar, validiert, lädt neu und verifiziert; bei einem Fehler wird das vorherige Paar wiederhergestellt und verifiziert.

9. Der Entzug der Fähigkeit zur SSH-Host-Bereitstellung stoppt ausstehende Host-Aufträge und weitere Übernahmen. Der Agent prüft die Auftragsautorisierung unmittelbar vor der Installation erneut. Ist ein unterbrochenes Aktivierungsjournal vorhanden, stellen Sie vor neuer Arbeit den vorherigen validierten Zustand wieder her.
10. Wählen Sie im Auftragsverlauf Zertifikat widerrufen und bestätigen Sie. Die Plattform stoppt das zugehörige Profil und erstellt eine dauerhafte Anforderung. Der zugewiesene Agent verifiziert das exakte lokale Zertifikat, aktualisiert seine lokale KRL und meldet deren Hash. Prüfen Sie ausstehend, fehlgeschlagen oder revoked-local unter Widerrufe. Offline-Agenten behalten ausstehende Arbeit. Bestehende Sitzungen und andere Hosts werden nicht automatisch widerrufen.
11. Schlägt der lokale Widerruf fehl, prüfen Sie den sicheren Fehlercode und den geschützten Agent-Zustand, beheben Sie die Ursache und verwenden Sie dann Widerruf wiederholen. Eine neue Anforderungs-ID lehnt verspätete Bestätigungen des alten Versuchs ab; die Ausstellung bleibt gestoppt.
12. Weisen Sie beim Anlegen des SSH-Profils bestehende Benachrichtigungsgruppen zu. Der lokale Postausgang erstellt zweisprachige HTML-Nachrichten zu bevorstehendem Ablauf, Ausstellung, Bereitstellung, Rollback, Fehlern und lokalem Widerruf. Wiederholte Verarbeitung dupliziert kein Ereignis. Die Zustellung erfordert einen aktivierten SMTP-Kanal der Organisation; eine Nachricht in der Warteschlange ist kein Zustellnachweis. Der lokale Widerruf verteilt keine KRLs an andere Hosts und beendet keine Sitzungen.
13. Kundenseitige SSH-KRL-Übertragung: Clm.Agent ssh export-krl signiert eine öffentliche Liste mit der lokalen CA; Clm.Agent ssh apply-krl <Consumer-Konfiguration> <Umschlag> verifiziert Organisation, gepinnte CA, Signatur, Digest und monoton steigende Revision. Consumer müssen RevokedKeys oder RevokedHostKeys separat konfigurieren. Verteilen Sie die Liste mit ssh publish-krl und ssh sync-krl auf weitere Hosts; CERTYX prüft nicht, ob jeder Host einen widerrufenen Schlüssel tatsächlich ablehnt.
14. Optionale kundenlokale KrlConsumers in der verwalteten Agent-Konfiguration erhalten nach einem Widerruf automatisch signierte KRL-Aktualisierungen. Versionen bleiben über Neustarts hinweg erhalten. Eine fehlgeschlagene Veröffentlichung ist als fehlgeschlagener Widerruf sichtbar und kann wiederholt werden. Dies konfiguriert weder OpenSSH-Consumer noch deckt es entfernte Flotten-Hosts ab.
15. Der verwaltete Agent gleicht konfigurierte lokale KRL-Consumer in jedem Abfragezyklus ab, auch nach einem Neustart oder einem autorisierten lokalen Widerruf. Consumer-Fehler stoppen den Zyklus sicher. Die nutzende OpenSSH-Identität muss berechtigt sein, ihr bereitgestelltes Ziel zu lesen; der Agent gewährt einem anderen Konto keinen Dateisystemzugriff.
16. Managed SSH meldet seinen eigenen sicheren Zyklusstatus. Ein fehlerfreier Erkennungsprozess kann einen fehlgeschlagenen oder stummen SSH-Worker nicht verdecken. Prüfen Sie den Fehler unter Agent-Zustand und in den geschützten lokalen Journalen; feste Zusammenfassungen enthalten keine Secrets. Ein Verbindungsverlust kann eine sofortige Meldung verhindern, daher ist auch eine Überwachung auf ausbleibenden Kontakt erforderlich.

17. SSH-E-Mail-Ereignisse werden atomar mit der Operation gespeichert. Nachrichten identifizieren das exakte signierte Zertifikat, den Ablauf in UTC, den CA-Fingerabdruck und den sicheren Fehlercode. Die Zustellprojektion verarbeitet begrenzte Stapel und stellt unterbrochene Bestätigungen ohne doppelte E-Mails wieder her.
18. Neue SSH-Ausstellungen erfordern die Berechtigung für automatische Erneuerung. Die Host-Installation erfordert zusätzlich die Berechtigungen für Bereitstellung, Verifizierung und Rollback. Bereits laufende Ergebnisse/Wiederherstellungen werden nicht allein durch eine Funktionsänderung blockiert; Organisationszugriff und Sperren durch Sicherheitswiderruf gelten weiterhin.
19. Für eine kundengesteuerte entfernte KRL-Übertragung führen Sie ssh publish-krl mit geschützter Publisher-Konfiguration aus und stellen nur dessen öffentlichen Umschlag über eine separate HTTPS-Relay-Identität bereit. Führen Sie ssh sync-krl mit einem geschützten Consumer-Abonnement aus. Signierte Veröffentlichungen laufen nach einer Stunde ab und werden automatisch aktualisiert; Weiterleitungen, fehlerhaftes Vertrauen, übergroße Daten, Manipulationen und abgelaufene Veröffentlichungen werden abgelehnt. Bestehende Widerrufe bleiben nach Fehlern erhalten. OpenSSH erzwingt den Ablauf des Umschlags nicht selbst. Den Zustand melden zentral nur Consumer, die für die KRL-Meldung registriert sind; CERTYX legt nicht fest, welche Hosts die KRL verwenden sollen. Alte Umschläge ohne signierte Zeitgrenzen müssen erneut exportiert werden. Eine neue CA kann vor der Ausstellung eine leere KRL initialisieren; der Verlust der KRL bei einer bereits verwendeten CA erfordert eine Wiederherstellung.
20. Für zentrale Sichtbarkeit registrieren Sie eine separate Consumer-Identität und aktivieren ausdrücklich die KRL-Consumer-Berichterstattung; sie gewährt keine Berechtigung zur SSH-Ausstellung oder Host-Installation. Führen Sie ssh monitor-krl mit der geschützten Identitäts- und Abonnementkonfiguration aus. Agent-Zustand zeigt die gemeldete Revision, den Ablauf der signierten Veröffentlichung, Synchronisierungsfehler und versäumte Berichtsfenster; eine fehlerfreie Erkennung kann einen KRL-Fehler nicht verdecken. Die Plattformüberwachung umfasst diese Agent-Fehler. Es handelt sich um authentifizierte Beobachtungen des Agenten, nicht um einen unabhängigen Nachweis, dass jeder Host die widerrufene Identität ablehnt. Verwenden Sie eine registrierte Identität je Consumer.
21. Ausstellungsbestätigungen erfordern eine aktive registrierte Identität mit SSH-Fähigkeit. Bereitstellungsbestätigungen erfordern zusätzlich die Fähigkeit zur SSH-Bereitstellung. Das Entfernen der Berechtigung lehnt ausstehende Ergebnisse ab, auch wenn die Ausstellung bereits begonnen hat; aufbewahrte lokale Journale erfordern einen Abgleich, bevor Berechtigungen wiederhergestellt werden.
22. Installation von Benutzeridentitäten: Wählen Sie Benutzer und aktivieren Sie die Installation, wenn Sie das Profil anfordern. Unabhängige Genehmigung und die Fähigkeit zur SSH-Bereitstellung sind erforderlich. Fügen Sie der aktuellen Unix-Agent-Konfiguration einen passenden UserTargets-Eintrag hinzu: festes entferntes Konto/Principal, Endpunkt und separat gepinnte Host-CA. Der Agent wechselt die lokale vollständige Schlüssel-/Zertifikatsgeneration, weist die Zertifikatsauthentifizierung nach und stellt bei Ablehnung die vorherige Generation wieder her. Ein Rückfall auf den reinen Schlüssel wird nicht als Zertifikatsverifizierung akzeptiert.
23. UserTargets müssen HostRevocationFile enthalten: die geschützte kundenlokale KRL, die für RevokedHostKeys verwendet wird. Der Client lehnt fehlende/unsichere Listen und widerrufene Hosts ab, auch wenn deren CA-Pin übereinstimmt. Halten Sie die Liste über den KRL-Publisher/-Subscriber des Kunden synchron; CERTYX prüft nicht, welche Hosts sie haben sollen.
24. Alle JSON-Konfigurationsleser des Agenten lehnen vor der Deserialisierung symbolische Dateien oder übergeordnete Verzeichnisse, Unix-Gruppen-/Andere-Berechtigungen, Dateien über 1 MiB und ungültiges UTF-8 ab. Schützen Sie die Konfiguration unter Unix mit chmod 600. Relative

Befehlszeilenpfade werden in einen absoluten Pfad aufgelöst und denselben Prüfungen unterzogen. UTF-8 mit oder ohne BOM wird unterstützt. Einstellungen und asynchrone Leser verwenden dieselben Regeln; Fehlerausgaben enthalten keine Konfigurationswerte. Unter Windows lehnen die Leser eine Datei ab, die ein anderer Prinzipal als LocalSystem, Administratoren oder die eigene Identität des Agenten besitzt, lesen oder ändern kann; richten Sie vor der Bereitstellung restriktive ACLs ein.

EINGABEN UND PARAMETER

- Registrierter, aktivierter Agent mit ausdrücklicher SSH-Fähigkeit; HTTPS, dem der Host vertraut.
- Die nur für den Eigentümer zugängliche verwaltete Konfiguration enthält Registrierungsidentität, lokale Zertifizierungsstelle und das Array genehmigter Profile.
- Die Genehmigung erfordert einen anderen Administrator und läuft nach 1–90 Tagen ab.
- Formate des Profils: Prinzipal 1–128 Buchstaben, Ziffern und . _ @ -, beginnend mit Buchstabe oder Ziffer (bastion.example.com oder deploy); CA-Fingerabdruck SHA256: plus 43 Base64-Zeichen wie von ssh-keygen -lf ausgegeben; Lebensdauer 2–10.080 Minuten; Erneuerung vor Ablauf mindestens 1 Minute und kürzer als die Lebensdauer; Genehmigung 1–90 Tage.

ERGEBNIS

Tatsächlich signierte öffentliche SSH-Artefakte werden gegen Auftrags-UUID, Principal, CA und Lebensdauer validiert; das Inventar wird idempotent fortgeschrieben. Verlorene Ergebnisbestätigungen werden ohne neue Schlüssel wiederhergestellt.

BERECHTIGUNGEN

Benutzer der Organisation lesen; Administratoren fordern an/widerrufen, ein anderer Administrator genehmigt. Host-Administratoren des Kunden autorisieren den lokalen CA-Geltungsbereich.

EINSCHRÄNKUNGEN

Die Host-Bereitstellung unterstützt OpenSSH unter Linux und OpenSSH für Windows mit vorkonfigurierter Baseline und lokalem Ziel (Beispiele ssh-host-target.linux.json und ssh-host-target.windows.json). Der Windows-SSH-Workload (ACL-geschützte Dateien, kopiertes current-Paar statt symbolischer Verknüpfung, Restart-Service sshd) läuft als LocalSystem mit OpenSSH für Windows. issued-local bedeutet nur Ausstellung; deployed-verified erfasst die beobachtete SSH-Akzeptanz. rolled-back stoppt automatische Wiederholungen; ein Eingreifen erfordert eine Untersuchung durch den Host-Administrator. CERTYX konfiguriert kein CA-Vertrauen auf entfernten Hosts und verfolgt nicht, welche Hosts die KRL verwenden sollen. SSH-Benachrichtigungen werden per E-Mail über das SMTP-Relay der Organisation versendet. Lokale signierte KRL-Consumer und dauerhafte HTML-Benachrichtigungsereignisse sind verfügbar; der lokale Widerruf begründet keine Abdeckung entfernter Consumer. Das Stoppen eines Profils widerruft weder Zertifikate noch bestehende Sitzungen. Registrierte überwachte Consumer melden den Synchronisierungszustand; dies begründet weder die erwartete Flottenabdeckung noch eine unabhängige Verweigerung des widerrufenen Zugriffs. Die Benutzerinstallation ist derzeit eine kundenlokale Unix-Workload-Identität unter demselben Betriebssystemkonto mit einer bestehenden verifizierten Baseline. Sie stellt weder Home-Verzeichnisse menschlicher Benutzer, Windows-ACLs, Server-CA-Vertrauen noch Live-Sitzungen bereit. Workloads müssen für neue Verbindungen die Bereitstellungspfade current/identity und current/identity-cert.pub verwenden. Aktualisieren Sie die Agenten, bevor Sie Profile mit Benutzerinstallation zuweisen. Veröffentlicht dieser Server ein Paket ohne Herausgebersignatur (einen unsignierten Entwicklungsbuild), sagen die Installationsbefehle das, lassen die Signaturdatei aus und prüfen nur die Prüfsumme, mit den Entwicklungsoptionen von Prüfer und Installationsprogramm; verwenden Sie solche Pakete nur in der Entwicklung.