CERTYX

AUTONOMOUS CERTIFICATE LIFECYCLE MANAGEMENT

Instrukcja użytkownika

Wszystkie widoki konsoli: cel, przebieg, dane, wyniki, uprawnienia i ograniczenia

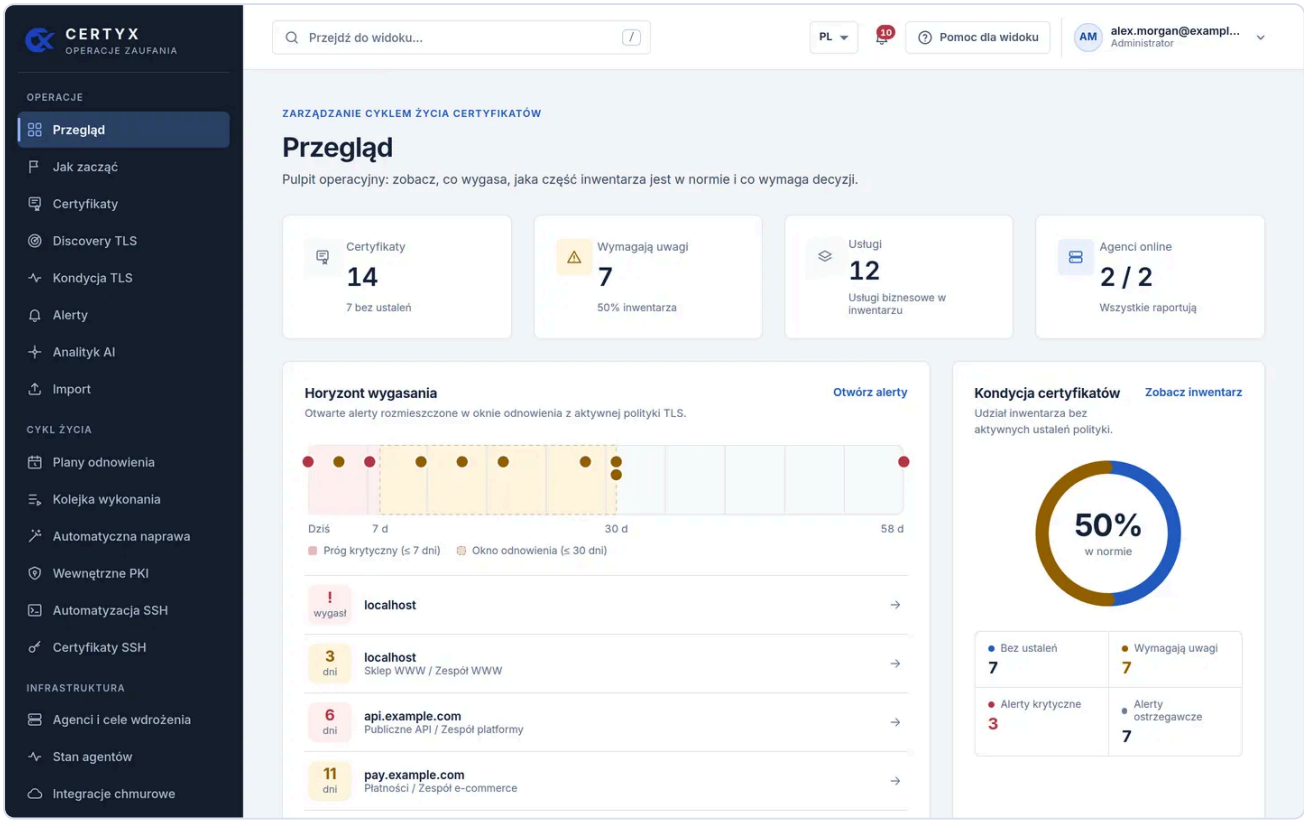
JĘZYK	WERSJA	DATA
Polski	8550060f	1 listopada 2026

Spis treści

1 Przegląd 3
2 Jak zacząć 5
3 Certyfikaty 7
4 Import certyfikatu 10
5 Discovery TLS 12
6 Kondycja TLS 16
7 Plany odnowienia 19
8 Kolejka wykonania 21
9 Automatyczna naprawa 28
10 Polityka TLS 31
11 Bezpieczeństwo i dostęp 33
12 Ślad audytowy 41
13 Alerty 43
14 Analityk AI 45
15 Administracja platformą 48
16 Operatorzy platformy 53
17 Sprzedaż 57
18 Wewnętrzne PKI 62
19 Grupy powiadomień 64
20 Eksport do SIEM 67
21 Agenci i cele wdrożenia 76
22 Graf zależności 83
23 Stan agentów 85
24 Monitoring platformy 89
25 Blokada wysyłki e-mail 92
26 Analityk AI – dostawca 95
27 Integracje chmurowe 97
28 Dziennik zdarzeń bezpieczeństwa 101
29 Certyfikaty SSH 105
30 Automatyzacja SSH 108

1 Przegląd

Pulpit operacyjny: zobacz, co wygasa, jaka część inwentarza jest w normie i co wymaga decyzji.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Zaloguj się, aby zobaczyć rzeczywiste dane organizacji.
2. Karty wskaźników pokazują certyfikaty, certyfikaty wymagające uwagi, usługi oraz agentów online (z aktualnym uwierzytelnionym kontaktem) spośród wszystkich zarejestrowanych. Każda karta jest odnośnikiem: Certyfikaty i Usługi otwierają inwentarz, Wymagają uwagi otwiera inwentarz przefiltrowany do tych certyfikatów, a Agenci online otwiera Stan agentów — od razu przy agencie wymagającym uwagi; karta podaje wtedy agenta, przyczynę (np. Brak raportów, Brak pierwszego kontaktu, Błąd procesu) i od kiedy.
3. Horyzont wygasania rozmieszcza otwarte alerty na osi okna odnowienia z aktywnej polityki TLS; czerwona strefa to próg krytyczny. Lista pod osią pokazuje pięć najbliższych terminów; kliknięcie otwiera Alerty.
4. Kondycja certyfikatów pokazuje udział certyfikatów bez ustaleń polityki oraz liczbę alertów krytycznych i ostrzegawczych.
5. Aktywność operacyjna zlicza zdarzenia ścieżki audytu z ostatnich 7 dni i pokazuje trzy ostatnie.
6. Centrum działań wyprowadza pozycje z bieżących danych, od najpilniejszych, każdą z dokładną przyczyną i odnośnikiem do rekordu, który ją wyjaśnia: wygasłe certyfikaty (przefiltrowany inwentarz), krytyczne alerty, każdy agent wymagający uwagi z przyczyną i wyjaśnieniem (jego karta w Stanie

agentów), nieudane lub wycofane zadania odnowienia z wynikiem agenta (gotowość odnowienia certyfikatu), zadania czekające na drugą osobę, niedziałający eksport SIEM (administratorzy) i niedostarczone powiadomienia z przyczyną, zablokowane plany odnowienia z pierwszą blokadą, przebiegi wykrywania z błędami lub przerwane (historia skanów), certyfikaty w oknie odnowienia, wyłączone MFA na Twoim koncie i pusty inwentarz. Pokazuje do sześciu pozycji.

7. Karta Subskrypcja i uprawnienia pokazuje plan, wykorzystanie limitu zarządzanych rodzin certyfikatów, dostępne rodziny, liczbę certyfikatów w inwentarzu (nierozliczanych) i ostrzeżenia licencyjne. Na liście Rodziny certyfikatów administrator wybiera Obejmij zarządzaniem lub Zakończ zarządzanie; licencję zużywają tylko zarządzane rodziny.
8. Aby szybko przejść do dowolnego widoku, naciśnij „/" lub użyj pola „Przejdź do widoku..." na górze ekranu.
9. Ostatnie wykrywanie pokazuje najnowszy przebieg każdego agenta wykrywającego i najnowszy skan serwera: stan, początek, aktywne hosty, endpointy TLS i znalezione certyfikaty (nowe, wymienione, bez zmian) oraz ostatni błąd; Historia skanów otwiera pełną historię w widoku Discovery TLS.

DANE I PARAMETRY

- Liczniki pochodzą z podsumowania inwentarza (cała organizacja, niezależnie od filtra). Usługi liczone są według unikalnej nazwy.
- Horyzont i centrum działań korzystają z alertów, aktywnej polityki TLS, planów odnowienia i stanu agentów; aktywność — z podsumowania ścieżki audytu przygotowanego przez serwer: liczby zdarzeń w lokalnych dniach przeglądarki (według jej bieżącej różnicy względem UTC) i trzech najnowszych zdarzeń.
- Dane są wczytywane przy wejściu na Przegląd i odświeżane co 30 sekund, dopóki widok jest otwarty; godzina ostatniej aktualizacji jest widoczna pod centrum działań.
- Gdy polityki TLS nie da się odczytać, horyzont używa zastępczego okna odnowienia (30 dni) i progu krytycznego (7 dni).

WYNIK OPERACJI

Pulpit niczego nie zmienia, z jednym wyjątkiem: przełączenie zarządzania rodziną certyfikatów przez administratora zmienia wykorzystanie licencji. Odnośniki prowadzą do widoków, w których wykonuje się działania.

UPRAWNIENIA

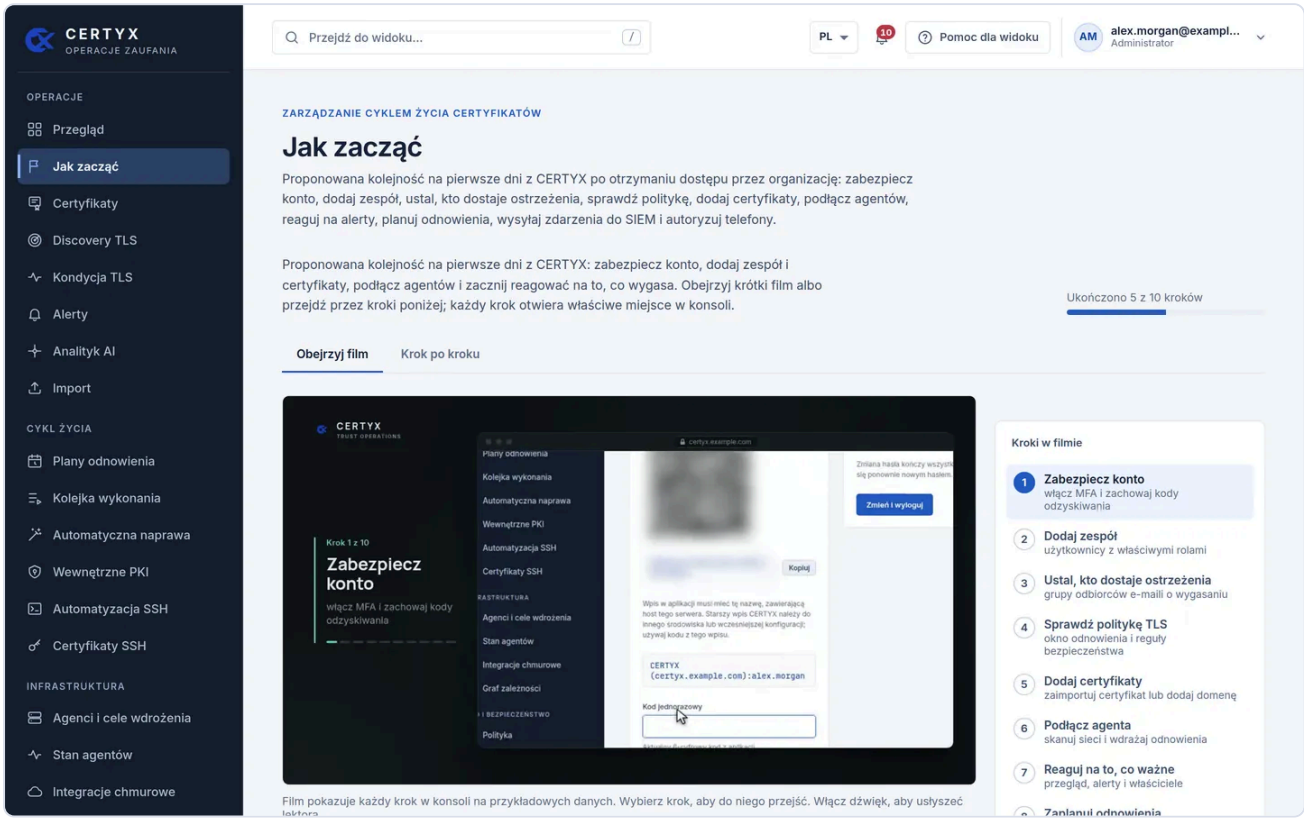
Wszyscy zalogowani użytkownicy organizacji (Audytor, Operator, Admin). Zarządzanie rodzinami certyfikatów przełącza tylko administrator. Jeśli dane źródło jest niedostępne, karta pokazuje „Dane niedostępne" zamiast zera.

OGRANICZENIA

Licznik uwagi dotyczy bazowej polityki, nie potwierdza poprawności wdrożeń. Horyzont pokazuje tylko certyfikaty z otwartymi alertami (w oknie odnowienia). Aktywność obejmuje zdarzenia ścieżki audytu certyfikatów, nie dziennik bezpieczeństwa platformy. Przegląd nie pokazuje zleceń odnowienia ani wdrożenia; śledź je w widoku Kolejka wykonania. Objęcie rodziny zarządzaniem jest odrzucane, gdy limit zarządzanych rodzin został osiągnięty, stan rodziny zmienił się w międzyczasie lub subskrypcja nie pozwala na nowe zarządzane rodziny.

2 Jak zacząć

Proponowana kolejność na pierwsze dni z CERTYX po otrzymaniu dostępu przez organizację: zabezpiecz konto, dodaj zespół, ustal, kto dostaje ostrzeżenia, sprawdź politykę, dodaj certyfikaty, podłącz agentów, reaguj na alerty, planuj odnowienia, wysyłaj zdarzenia do SIEM i autoryzuj telefony.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Obejrzyj film: nagranie dziesięciu kroków w konsoli na przykładowych danych, w języku konsoli, z napisami. Każdy krok omawia lektor: film startuje bez dźwięku w pętli, a po włączeniu dźwięku odtwarza się raz; nie startuje sam, gdy system prosi o ograniczenie ruchu. Wybierz krok z listy obok, aby przejść do tego fragmentu.
2. Albo otwórz Krok po kroku: każdy krok wyjaśnia, dlaczego jest ważny i jak go wykonać, ze zrzutem ekranu odpowiedniego miejsca w konsoli; kroki tylko dla administratorów (zespół, grupy powiadomień, polityka, agenci, eksport do SIEM, telefony) oraz kroki zmieniające dane, wymagające roli operatora lub administratora (certyfikaty, obsługa alertów, plany odnowienia), mają notatkę dla ról, które nie mogą ich wykonać.
3. Przycisk Otwórz przy kroku przenosi prosto do właściwego widoku; pojawia się tylko wtedy, gdy Twoja rola może otworzyć ten widok.
4. Pasek postępu liczy ukończone kroki. Kroki, które konsola rozpoznaje (MFA lub logowanie firmowe, użytkownicy, grupy powiadomień, certyfikaty, agenci, którzy nawiązali kontakt z CERTYX — agent czekający na pierwszy kontakt, unieważniony lub wygasły się nie liczy — plany odnowienia, zapisane

miejsce docelowe SIEM, aktywne urządzenia mobilne), są oznaczane automatycznie. Pozostałe oznaczasz przyciskiem Oznacz jako zrobione, a cofasz przyciskiem Oznacz jako niezrobione.

5. Po wykonaniu kroków konsola spina cały proces operacyjny: przegląd wskazuje, co wymaga uwagi i dlaczego, Stan agentów wyjaśnia przyczynę dla każdego agenta wraz z działaniami, historia skanów pokazuje, co znalazło wykrywanie, a Gotowość odnowienia certyfikatu pokazuje każdy krok od wykrycia do zaktualizowanego inwentarza i co należy skonfigurować.

DANE I PARAMETRY

- Nie trzeba niczego wpisywać. Ręczne oznaczenia są zapisywane tylko w tej przeglądarce dla Twojego konta.

WYNIK OPERACJI

Lista kontrolna pokazująca postęp organizacji i prowadząca do wszystkich potrzebnych miejsc. Ten widok niczego nie zmienia.

UPRAWNIENIA

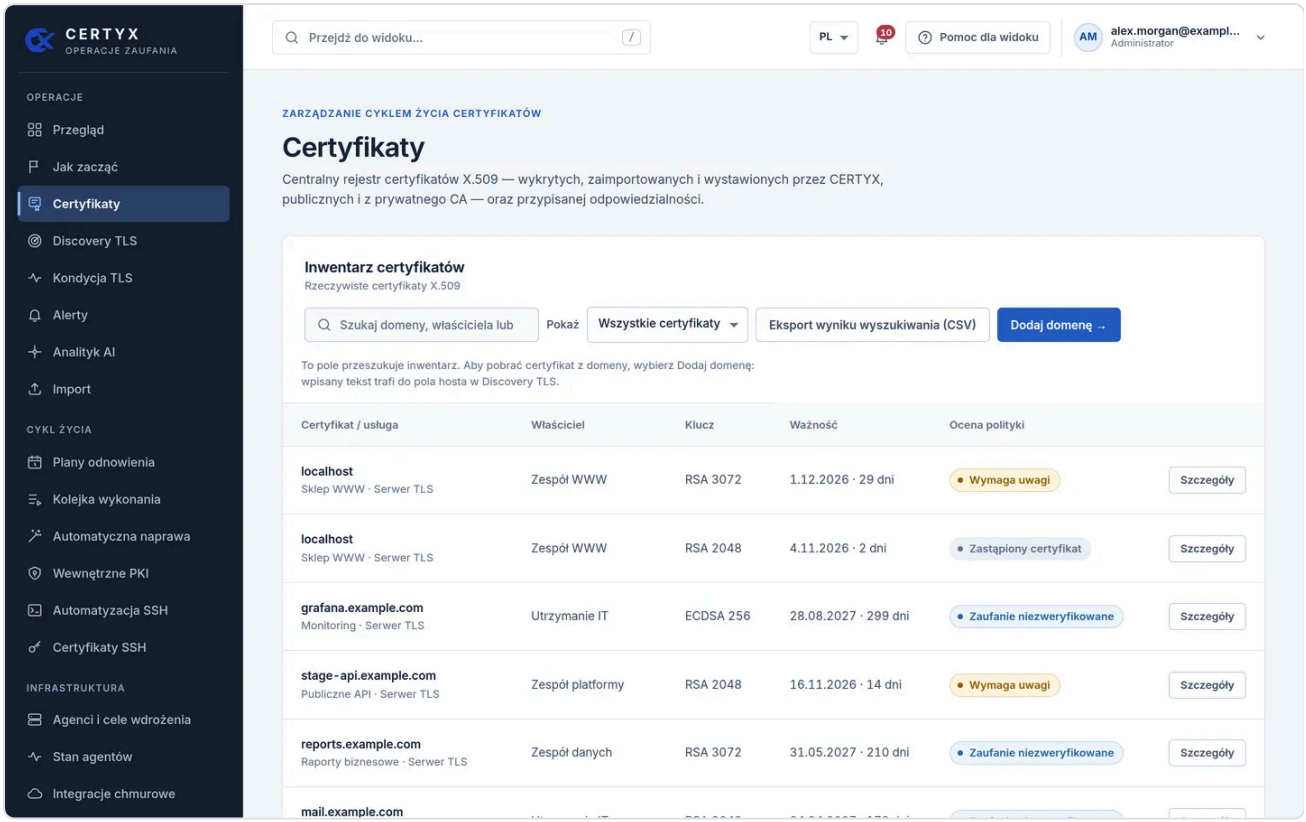
Każdy zalogowany użytkownik organizacji. Kroki tylko dla administratorów albo tylko dla operatorów i administratorów są oznaczone; wykrywanie wymagające uprawnień administratora (użytkownicy, miejsca docelowe SIEM, urządzenia mobilne) widzą tylko administratorzy.

OGRANICZENIA

- Film i zrzuty pokazują przykładowe dane i mogą różnić się szczegółami od Twojej konfiguracji.
- Wykrywanie czyta bieżące dane; krok wykonany inaczej (na przykład certyfikaty z integracji chmurowych) liczy się jako zrobiony, gdy dane istnieją.
- Kroków Sprawdź politykę TLS oraz Reaguj na to, co ważne nie da się wykryć; zawsze oznaczasz je samodzielnie. Użytkowników, miejsca docelowe SIEM i urządzenia mobilne wykrywa się tylko dla administratorów, miejsca docelowe SIEM tylko z bazą platformy, w której jest dziennik bezpieczeństwa, a urządzenia mobilne — tylko gdy platforma udostępnia tę funkcję.
- Jeśli filmu nie da się wczytać, widok wyświetla komunikat, a kroki poniżej opisują te same czynności.
- Ręczne oznaczenia nie są współdzielone ze współpracownikami ani innymi przeglądarkami.

3 Certyfikaty

Centralny rejestr certyfikatów X.509 — wykrytych, zaimportowanych i wystawionych przez CERTYX, publicznych i z prywatnego CA — oraz przypisanej odpowiedzialności.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Wyszukaj domenę, właściciela lub usługę.
2. Aby pobrać certyfikat z domeny, której nie ma w rejestrze, wybierz Dodaj domenę →. Otwiera to formularz sprawdzania w widoku Discovery TLS (sprawdzenie wymaga roli administratora); tekst wpisany w wyszukiwarce jest przenoszony do pola hosta, a puste pole wyszukiwania otwiera pusty formularz.
3. Otwórz Szczegóły, aby zobaczyć podmiot, wystawcę, przeznaczenie, numer seryjny, daty, klucz, ryzyko i SHA-256.
4. Przejrzyj ustalenia polityki. Zmień Właściciel, Usługa, Produkcja i Grupy odpowiedzialności (do 10 niezarchiwizowanych grup; Zarządzaj grupami odbiorców otwiera administrację powiadomień) i wybierz Zapisz odpowiedzialność albo wybierz Zaplanuj odnowienie — plan zostaje utworzony i otwiera się widok Plany odnowienia.
5. Gdy subskrypcja obejmuje funkcję RISK_ENGINE, szczegóły pokazują także Ryzyko biznesowe z jego składnikami i ostrzeżeniami o niepełnym kontekście.
6. Gdy analityk AI jest włączony dla organizacji, Wyjaśnij w szczegółach otwiera go z pytaniem o certyfikat.

7. Każdy certyfikat pokazuje przeznaczenie wynikające z rozszerzonego użycia klucza: serwer TLS, klient TLS, serwer i klient TLS, dowolne użycie (bez ograniczenia EKU) lub inne użycie. Szczegóły zawierają tożsamości e-mail, UPN i URI. Ustalenia dotyczące wyłącznie serwerów (localhost, adres loopback lub IP) nie są zgłaszane dla certyfikatów klienta TLS; publiczny certyfikat dopuszczający uwierzytelnianie klienta otrzymuje ustalenie informacyjne.
8. Pokaż filtruje listę: wszystkie certyfikaty, wymagające uwagi (liczba z przeglądu), wygasłe, w oknie odnowienia lub ważne poza nim. #inventory/validity/<filtr> otwiera przefiltrowaną listę.
9. Gotowość odnowienia w szczegółach pokazuje każdy krok odnowienia: inwentarz (gdzie certyfikat ostatnio zaobserwowano, z usługą rozpoznaną w każdym punkcie, jej wersją TLS i protokołem ALPN, proponowanym sposobem instalacji z pewnością i dowodami oraz certyfikatami wystawców przedstawionymi przez punkt), politykę i okno odnowienia, cel wykonania obejmujący dokładnie jego nazwy, agenta instalującego i jego diagnozę, gdzie i jak agent instaluje (tryb instalacji — agent na hoście albo agent jako przekaźnik SSH z hostem zdalnym —, konektor, katalog wdrożenia, publikowane pliki, np. fullchain.pem, privkey.pem i bundle.p12 lub skonfigurowane ścieżki, polecenia sprawdzenia konfiguracji i przeładowania, zasób chmurowy, sprawdzany endpoint i usługa wykryta przez relay-check — tak jak agent zgłasza miejsca wdrożenia; inny tryb instalacji lub host zdalny blokuje krok), urząd certyfikacji, niezależną weryfikację, co uruchamia wymianę (profil automatyczny, zaplanowane zgłoszenie lub ręcznie), plan odnowienia, zatwierdzenie przez drugą osobę, co agent robi krok po kroku, wynik weryfikacji i zaktualizowany inwentarz. Zablokowany krok mówi dokładnie, co skonfigurować; gdy żaden cel nie obejmuje certyfikatu, administrator wybiera Utwórz cel z tymi wartościami, co otwiera Wykonanie z celem zaproponowanym przez gotowość. Formularz pokazuje pod każdym polem, skąd pochodzi jego wartość i co administrator musi jeszcze wpisać.
10. Następne odnowienie w gotowości odnowienia pokazuje, jak rozpocznie się kolejne odnowienie certyfikatu — Automatyczne (bez zatwierdzania), Wymaga zatwierdzenia lub Planowane ręcznie — oraz które ustawienie automatycznego odnawiania o tym decyduje (domyślne ustawienie instalacji, organizacja, cel lub ten certyfikat). Administrator zmienia wybór Automatyczne odnawianie certyfikatu nad gotowością: Ustawienie organizacji, Odnawiaj automatycznie lub Wymagaj zatwierdzenia; dotyczy on także kolejnych odnowień certyfikatu.

DANE I PARAMETRY

- Szukaj po domenie, podmiocie, zaobserwowanym punkcie, właścicielu, usłudze, wystawcy, numerze seryjnym lub skrócie SHA-256 (do 200 znaków). PostgreSQL filtruje cały rejestr organizacji; strona pokazuje 50 wpisów.
- Właściciel i Usługa: wymagane, 1–200 znaków każde.
- Eksport CSV obejmuje cały wynik wyszukiwania, bez kluczy prywatnych. Formuły arkusza są neutralizowane.

WYNIK OPERACJI

Metadane zostają zapisane i audytowane. Zmiana właściciela lub usługi cofa zatwierdzone plany odnowienia do ponownego zatwierdzenia (Gotowy do zatwierdzenia lub Zablokowany).

UPRAWNIENIA

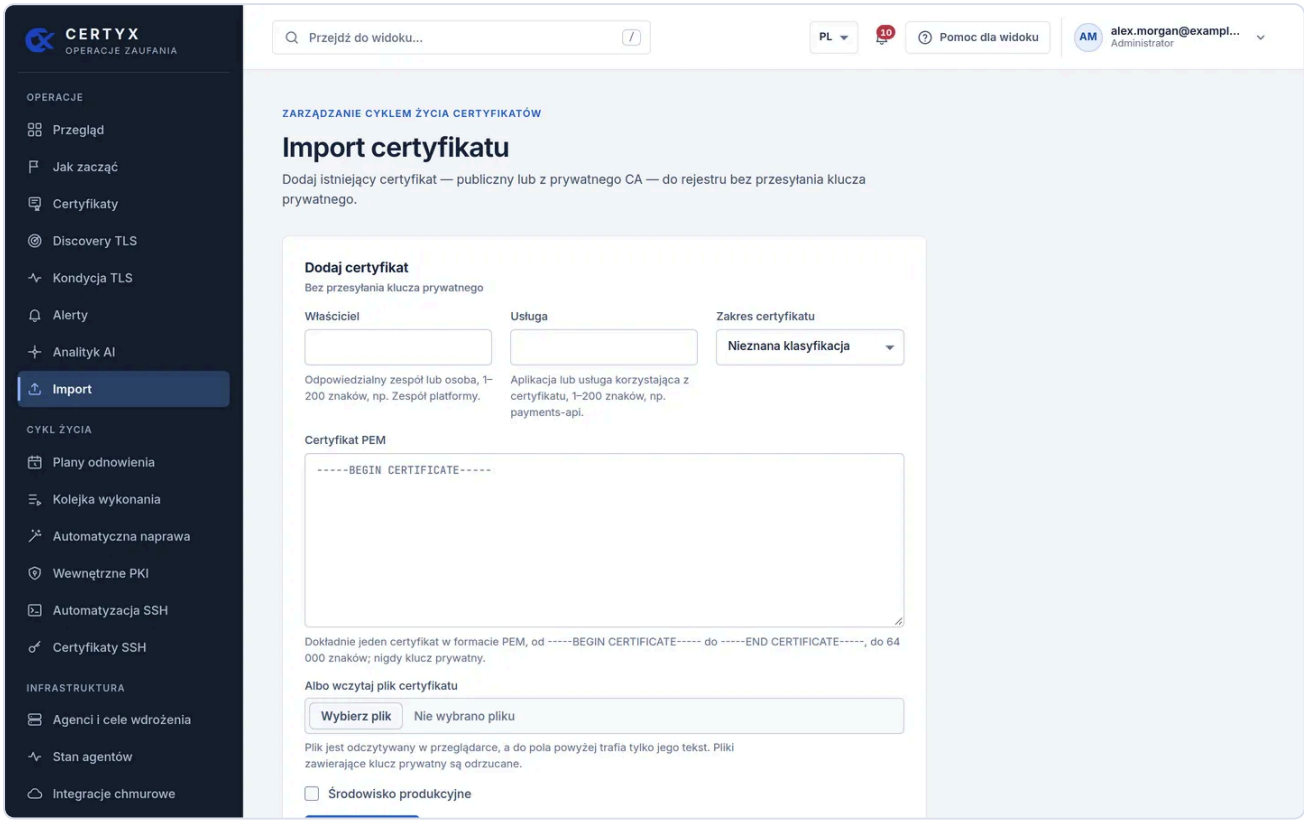
Wszystkie role organizacji: wyszukiwanie, szczegóły i eksport CSV. Operator i administrator: zapis odpowiedzialności i planowanie odnowienia. Ryzyko biznesowe: tylko z funkcją RISK_ENGINE.

OGRANICZENIA

SHA-256 identyfikuje konkretny certyfikat. Wynik ryzyka 0–100 nie jest oceną zaufania CA. Łańcuch, unieważnienie, SAN i poprawność wdrożenia nie są tu potwierdzane.

4 Import certyfikatu

Dodaj istniejący certyfikat — publiczny lub z prywatnego CA — do rejestru bez przesyłania klucza prywatnego.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Podaj Właściciel i Usługa oraz wybierz Zakres certyfikatu: Nieznana klasyfikacja (domyślnie), Certyfikat publiczny lub Certyfikat wewnętrzny.
2. Wklej jeden certyfikat, od -----BEGIN CERTIFICATE----- do -----END CERTIFICATE-----, w pole Certyfikat PEM albo wybierz plik w Albo wczytaj plik certyfikatu (.pem, .crt lub .cer w tekstowej postaci PEM). Plik jest odczytywany w przeglądarce, a do pola trafia tylko jego tekst.
3. Zaznacz Środowisko produkcyjne, jeśli dotyczy, i wybierz Importuj i oceń.
4. Panel Wynik importu pokazuje ocenę, ważność, klucz, ryzyko i liczbę ustaleń polityki. Otwórz inwentarz certyfikatów prowadzi do certyfikatu w inwentarzu. Formularz jest czyszczony, więc możesz od razu zaimportować kolejny certyfikat.

DANE I PARAMETRY

- Certyfikat PEM: dokładnie jeden publiczny certyfikat X.509 w tekstowej postaci PEM, do 64 000 znaków (wybrany plik do 64 000 bajtów). Binarne pliki DER i kontenery PKCS#12/PFX nie są przyjmowane — najpierw przekonwertuj certyfikat do PEM, bez klucza prywatnego. Łańcuch z kilkoma certyfikatami jest odrzucany.
- Właściciel i Usługa: wymagane, 1–200 znaków każde.

- Zakres certyfikatu: Certyfikat wewnętrzny oznacza certyfikat Twojego prywatnego CA — pojawia się on wtedy na liście widoku Wewnętrzne PKI; Certyfikat publiczny i Nieznana klasyfikacja pozostają tylko w inwentarzu.
- Treść z kluczem prywatnym (dowolny blok BEGIN … PRIVATE KEY) jest odrzucana w przeglądarce, zanim zostanie wysłana, i ponownie przez serwer. Certyfikat, który jest już w inwentarzu, jest odrzucany jako duplikat; niepoprawny PEM X.509 jest odrzucany z podaniem przyczyny.

WYNIK OPERACJI

Zapis certyfikatu, wyodrębnienie danych X.509, bieżąca ocena polityki i wpis audytowy (certificate.import).

UPRAWNIENIA

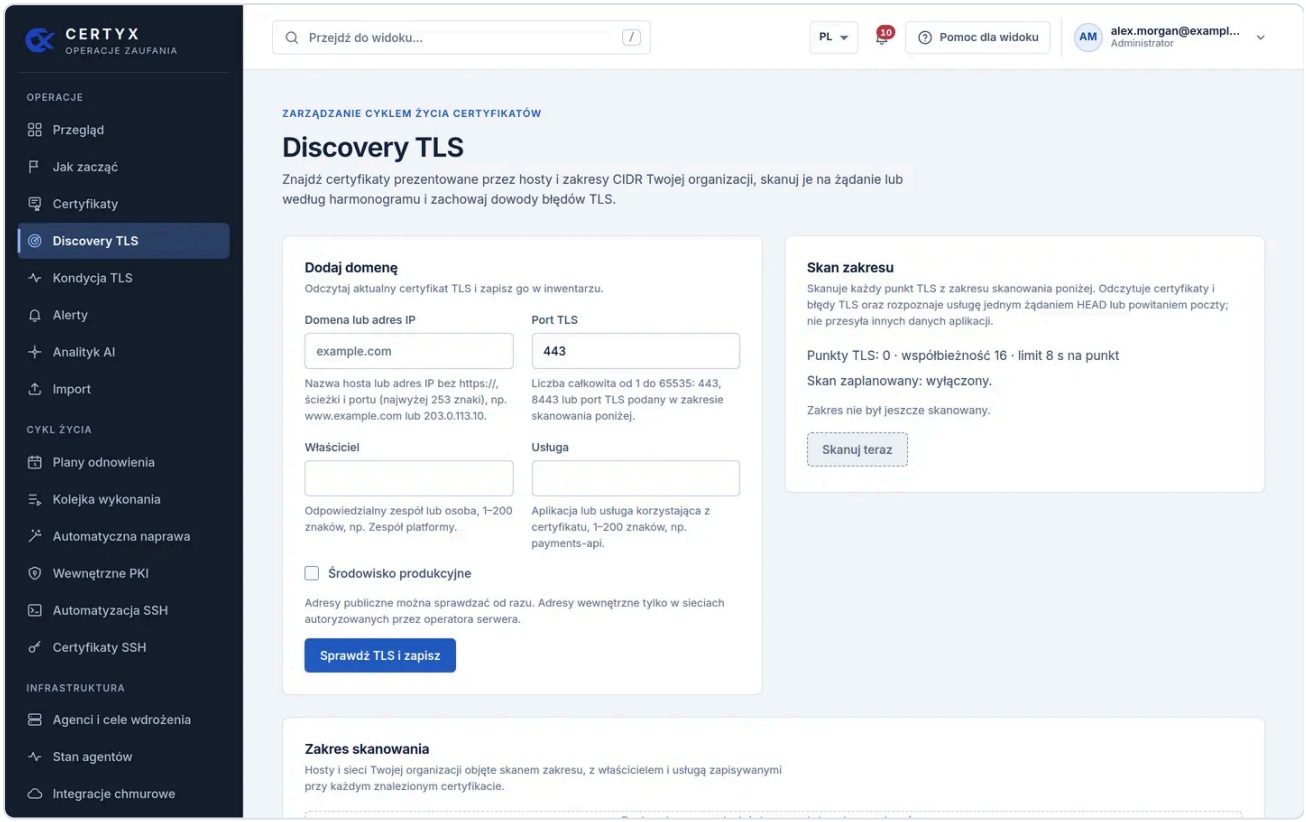
Operator lub administrator. Audytor widzi formularz wyłączony z informacją, że jego rola pozwala tylko przeglądać inwentarz.

OGRANICZENIA

Import nie wydaje ani nie instaluje certyfikatu i nie zapisuje klucza prywatnego ani łańcucha. Certyfikat samopodpisany może zostać zapisany, ale jego zaufanie nie jest potwierdzone. Klasyfikacja jest deklaracją importującego; CERTYX jej nie weryfikuje.

5 Discovery TLS

Znajdź certyfikaty prezentowane przez hosty i zakresy CIDR Twojej organizacji, skanuj je na żądanie lub według harmonogramu i zachowaj dowody błędów TLS.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Ten widok uruchamia wykrywanie po stronie serwera CERTYX dla Twojej organizacji — także na instancjach dedykowanych. Aby znaleźć certyfikaty w sieciach, do których serwer nie ma dostępu, użyj zarejestrowanego agenta: Agenci i cele wdrożenia → Automatyczne wykrywanie w sieci (zgłoszone sieci, zakres, tryb, tempo, okna); wyniki trafiają do inwentarza, a alerty do Alertów.
2. Dla jednej domeny: wpisz nazwę bez https://, wybierz port TLS (domyślnie 443), podaj właściciela i usługę, a następnie Sprawdź TLS i zapisz. Po powodzeniu wybierz Otwórz certyfikat: certyfikat jest już zapisany w inwentarzu.
3. Zakres skanowania (administrator): w sekcji Hosty dodaj nazwę lub adres IP z portem TLS, właścicielem, usługą i oznaczeniem produkcji; w sekcji Sieci dodaj zakres CIDR z jawnymi portami TLS i tymi samymi metadanymi; wykluczenia wpisz po jednym w wierszu.
4. Aby skanować cyklicznie, zaznacz Skanuj automatycznie i podaj interwał w minutach (granice podane pod polem). Wybierz Zapisz zakres. Każdy zapis tworzy nową wersję i trafia do dziennika bezpieczeństwa; jeśli w międzyczasie zakres zmienił inny administrator, odśwież widok i wprowadź zmianę ponownie.
5. Panel Skan zakresu pokazuje liczbę punktów TLS, harmonogram z czasem następnego skanu i ostatni skan. Skanuj teraz uruchamia skan ręczny; postęp odświeża się na bieżąco. Zatrzymaj skan (administrator) zatrzymuje trwający skan organizacji — Twój, innego administratora lub zaplanowany —

na tej instancji, która go wykonuje; kończy się jako anulowany w ciągu kilku sekund, a znalezione już certyfikaty pozostają w inwentarzu. Skan zaplanowany lub uruchomiony przez innego administratora jest widoczny po odświeżeniu stanu.

6. Jeśli instancja wykonująca skan zatrzymała się, skan jest oznaczony jako przerwany. Jest kontynuowany od zapisanego punktu kontrolnego — już przeskanowane punkty nie są sprawdzane ponownie: harmonogram wznawia go automatycznie przy najbliższym przebiegu (chyba że operator serwera to wyłączył), a Wznów skan (administrator) wznawia go od razu. Uwaga pod postępem wyjaśnia, kiedy skanu nie można wznowić (zakres zmienił się od jego startu, osiągnięto limit wznowień, zatrzymał go administrator lub zastąpił go nowszy skan); wtedy uruchom nowy skan.
7. Przejrzyj Wyniki ostatniego skanu (certyfikat albo przyczyna braku odpowiedzi dla każdego punktu), obserwacje oraz certyfikaty dodane do inwentarza. Każdy wynik podaje rozpoznaną usługę; każda obserwacja pokazuje w kolumnie Usługa i instalacja usługę, wersję TLS i wynegocjowany protokół ALPN, proponowany sposób instalacji odnowionego certyfikatu z jego pewnością oraz dowody (na przykład Server: nginx/1.24.0 lub port 6443). Obserwacje agentów bez rozpoznawania usług pokazują Nierozpoznana.
8. Operator serwera ustala limity zakresu, granice interwału i autoryzowane sieci wewnętrzne (Clm:Discovery). Na instancji bez organizacji dedykowanych zakres z CLM_DISCOVERY_TARGETS, CLM_DISCOVERY_CIDRS i CLM_DISCOVERY_EXCLUSIONS jest jednorazowo przejmowany jako zakres organizacji „default”; dalsze zmiany wprowadza się w tym widoku.
9. Wykrywanie przez agenta (Clm.Agent discovery scan na hoście klienta) ponawia przejściowe błędy rotacji tożsamości i komunikacji po Settings.RetrySeconds (domyślnie 30 sekund). Błędy uwierzytelniania, uprawnień lub zaufania TLS zatrzymują proces wykrywania agenta; z --once polecenie zwraca błąd. Na hoście agenta skonfiguruj ścieżki stanu i blokady dostępne tylko dla właściciela. Awaria raportowania może opóźnić diagnostykę, więc monitoruj także brak kontaktu agenta.
10. Historia skanów wymienia każdy przebieg wykrywania agentów i skan serwera w organizacji, od najnowszych: początek, źródło (agent z odnośnikiem do jego stanu albo serwer CERTYX), zakres (sieci, tryb i wykluczenia), stan z fazą i postępem albo zakończenie (zakończony, przerwany z powodu zmiany zakresu, wstrzymania profilu lub ponownego rozpoczęcia przebiegu), aktywne hosty, endpointy TLS, certyfikaty nowe w inwentarzu, wymienione na endpoincie i bez zmian, zgłoszone alerty wykrywania, zmniejszone tempo, ostatnie błędy oraz czy to przebieg bazowy. Wyniki prowadzą do pozycji inwentarza nowych lub wymienionych certyfikatów i do Alertów. #discovery/history otwiera tę sekcję.

DANE I PARAMETRY

- Host: nazwa lub adres IP bez URL, ścieżki i portu; port TLS 1–65535; właściciel i usługa (domyślnie maks. 200 znaków); oznaczenie produkcji.
- Sieć: IPv4/IPv6 CIDR z adresem sieci (np. 203.0.113.0/28) i 1–16 jawnymi portami TLS.
- Wykluczenia: adresy IP lub CIDR; dotyczą również adresu, na który rozwiązuje się nazwa hosta.
- Ten sam punkt TLS (host lub adres i port) podany dwa razy z innym właścicielem, usługą lub oznaczeniem produkcji jest odrzucany.
- Domyślne limity serwera (widoczne pod formularzem): 100 hostów, 64 sieci, 4096 adresów przed wykluczeniami, 16 384 punkty TLS, 1024 wykluczenia. Interwał skanowania domyślnie od 15 minut do 7 dni.

- Adresy: publiczne zawsze; prywatne, lokalne i zarezerwowane tylko w sieciach autoryzowanych przez operatora — zapis zakresu z innymi adresami jest odrzucany, a nazwy hostów rozwiązane do takich adresów kończą się wynikiem „brak odpowiedzi TLS".
- Domyślnie 16 równoległych prób i limit 8 sekund na punkt.
- Pojedyncza domena: port 443 lub 8443 albo port TLS z zakresu skanowania organizacji.

WYNIK OPERACJI

Publiczny certyfikat i błędy TLS zapisane z punktem TLS i czasem obserwacji, razem z odciskiem usługi (wysłana nazwa serwera, wersja TLS, zestaw szyfrów, protokół ALPN, certyfikaty wystawców przedstawione przez punkt, status HTTP z nagłówkami Server i X-Powered-By albo powitanie poczty) i rozpoznaną usługą z proponowanym sposobem instalacji; wyniki każdego punktu przechowywane dla ostatnich 20 skanów organizacji, a trwający skan zapisuje dotychczasowe wyniki jako punkt kontrolny. Zmiany zakresu, start skanu, żądania zatrzymania, wznowienia i zakończenie skanu (ukończony, anulowany, nieudany lub przerwany) są zapisywane w dzienniku bezpieczeństwa i audycie inwentarza.

UPRAWNIENIA

Odczyt zakresu, stanu, wyników i obserwacji: zalogowane role organizacji. Zmiana zakresu, sprawdzenie domeny, uruchomienie, zatrzymanie i wznowienie skanu: administrator.

OGRANICZENIA

Nie jest to skaner wszystkich usług: tylko połączenie TCP i negocjacja TLS na podanych portach oraz, jeśli operator serwera tego nie wyłączył (Clm:Discovery:ServiceIdentification:IdentifyServices), jedno żądanie HEAD / HTTP/1.1 do punktu HTTP albo odczyt powitania SMTPS, IMAPS lub POP3S; żadnych innych danych aplikacyjnych, bez UDP i STARTTLS. Rozpoznana usługa jest propozycją skonfigurowanych reguł: nagłówek Server wskazuje oprogramowanie, które odpowiedziało przez HTTP, a za serwerem pośredniczącym przekazującym nagłówki może to być backend; punkt bez charakterystycznych cech jest pokazywany jako nierozpoznany serwer WWW lub usługa TLS z ogólną instalacją plików PEM i niską pewnością. Jeden skan organizacji naraz. Każda instancja skanuje domyślnie do 4 organizacji jednocześnie (Clm:Discovery:SchedulerConcurrency); gdy termin mija dla większej liczby organizacji, najpierw startują najbardziej zaległe, pozostałe przy kolejnym przebiegu, więc skan może rozpocząć się później niż zaplanowano. Zatrzymanie skanu wykonywanego przez inną instancję działa przy jego najbliższym zapisie postępu (domyślnie co 2 sekundy). Skan, którego instancja padła bez zapisu, jest oznaczany jako przerwany po 10 minutach bez postępu (domyślnie) i wznawiany najwyżej 5 razy (domyślnie). Konsola pokazuje tylko ostatni zakończony skan: pierwsze 100 wyników punktów TLS z łączną liczbą punktów; pełne wyniki punktów pozostają zapisane dla przechowywanych skanów. Pokazuje też 50 najnowszych obserwacji i ich łączną liczbę; serwer przesyła tylko te 50 obserwacji. Dodanie jednej domeny nie dodaje jej do zakresu. Jeśli certyfikat już istnieje, jego właściciel i usługa pozostają bez zmian. Limity serwera nie dotyczą wykrywania przez agenta, które ma własne limity (Clm:Discovery:AgentLimits).

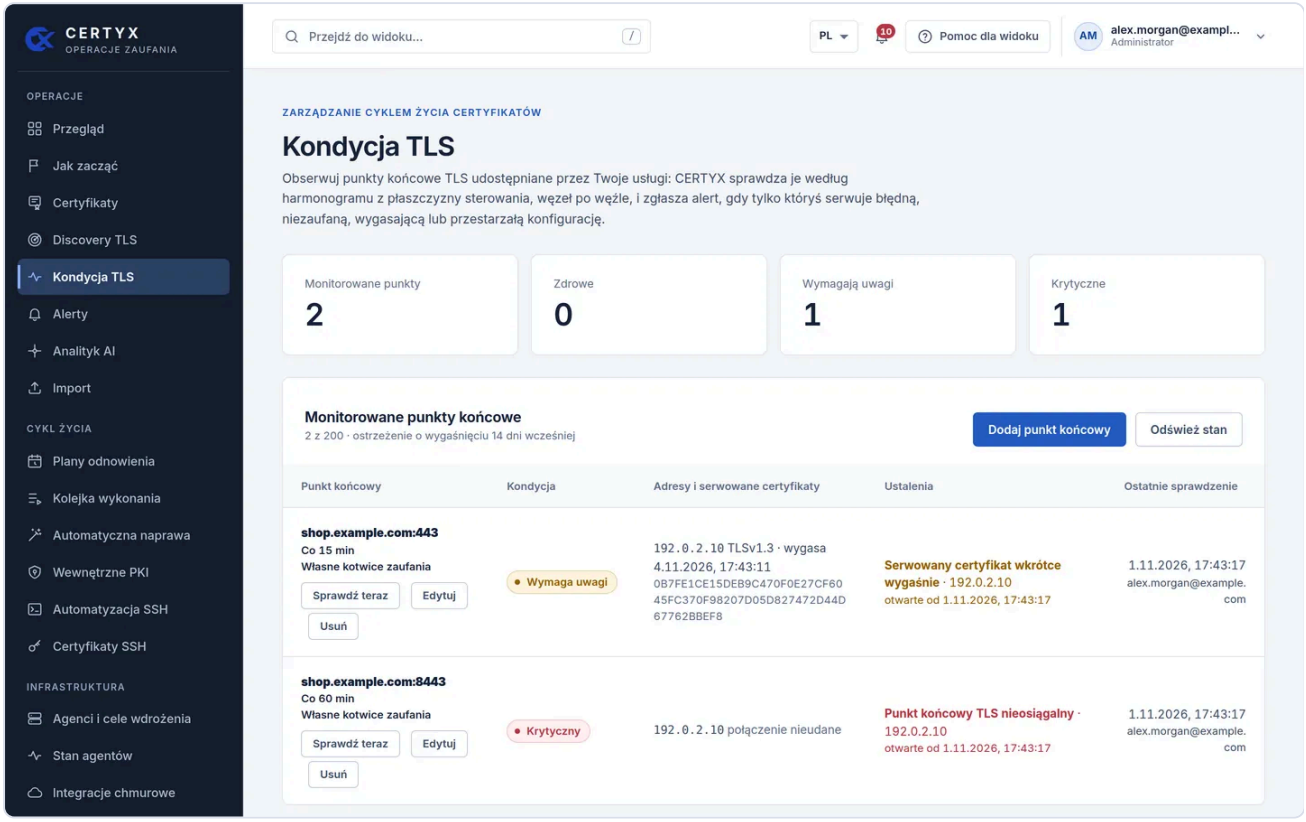
ROZWIĄZYWANIE PROBLEMÓW

- Nie widać przebiegu agenta: agent potrzebuje uprawnienia wykrywania i włączonego, zatwierdzonego profilu (Agenci i cele wdrożenia); sprawdź jego diagnozę w Stanie agentów.
- Przebieg kończy się jako przerwany: zmienił się zatwierdzony zakres lub porty, profil wstrzymano albo agent zaczął przebieg od nowa; następny przebieg rozpocznie się sam.
- Błędy w przebiegu: agent zgłosił stałą przyczynę (np. błąd komunikacji lub lokalnego wejścia/wyjścia albo profil poza lokalną listą dozwolonych sieci); Stan agentów wyjaśnia ją razem z działaniami naprawczymi.

- Brak certyfikatów mimo aktywnych hostów: typowe porty profilu nie obejmują portów TLS usług albo hosty odpowiadają bez TLS; dodaj porty lub użyj trybu pełnego po uzgodnieniu z zespołem bezpieczeństwa.

6 Kondycja TLS

Obserwuj punkty końcowe TLS udostępniane przez Twoje usługi: CERTYX sprawdza je według harmonogramu z płaszczyzny sterowania, węzeł po węźle, i zgłasza alert, gdy tylko któryś serwuje błędną, niezaufaną, wygasającą lub przestarzałą konfigurację.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Administrator wybiera Dodaj punkt końcowy i podaje nazwę hosta lub adres IP (bez https://, ścieżki i portu), port TLS (domyślnie 443) i interwał sprawdzania w minutach (limity są podane w formularzu). Opcjonalnie wpisz oczekiwany odcisk SHA-256 certyfikatu, który musi serwować każdy węzeł, oraz kotwice zaufania (certyfikaty CA w PEM) dla punktów prywatnego CA. Zapisz: punkt zostanie sprawdzony przy najbliższym przebiegu harmonogramu, zwykle w ciągu minuty.
2. Każde sprawdzenie raz rozwiązuje nazwę i samo łączy się z każdym rozwiązanym adresem (każdy węzeł za nazwą DNS lub load balancerem, do Clm:EndpointHealth:MaximumAddresses), więc zmieniająca się odpowiedź DNS nie może go przekierować. Dla każdego adresu zapisuje serwowany certyfikat (odcisk, podmiot, wystawca, wygaśnięcie), wynegocjowaną wersję TLS i szyfr, czy certyfikat obejmuje nazwę hosta, czy łańcuch jest zaufany przy sprawdzaniu unieważnienia online, czy serwer pomija certyfikaty pośrednie i czy nadal akceptuje TLS 1.0 lub 1.1.
3. Ustalenia: nieosiągalny adres, nierozwiązywany host, niezaufany łańcuch (nieznany wystawca, unieważniony, nieprawidłowy), niemożliwy do sprawdzenia status unieważnienia, brak certyfikatu pośredniego, niezgodna nazwa hosta, akceptowany TLS 1.0/1.1, wygasły lub wygasający certyfikat

(ostrzeżenie Clm:EndpointHealth:ExpiringWarningDays wcześniej), inny certyfikat niż oczekiwany odcisk oraz rozjazd węzłów, gdy adresy serwują różne certyfikaty (na przykład po rotacji, która pominęła jeden węzeł).

4. Każde ustalenie jest alertem w widoku Alerty z punktem końcowym i adresem, otwartym od pierwszego wykrycia. Właściciel, usługa i grupy powiadomień pochodzą z inwentarza, gdy serwowany certyfikat jest znany. Otwarte alerty trafiają do kanałów powiadomień organizacji (e-mail, Slack, Microsoft Teams, webhooki, PagerDuty), a krytyczne do aplikacji mobilnej, jak każdy inny alert. Alert można potwierdzić; pozostaje potwierdzony, dopóki ustalenie trwa, i zamyka się sam, gdy sprawdzenie go już nie znajduje. Ponowne wystąpienie to nowy alert.
5. Sprawdź teraz (operatorzy i administratorzy) od razu sprawdza jeden punkt, na przykład zaraz po wdrożeniu. Edytuj zmienia monitor (wersjonowany: jeśli w międzyczasie zmienił go inny administrator, odśwież widok i powtórz zmianę); Usuń kończy monitorowanie i usuwa wyniki oraz otwarte alerty kondycji. Wyłączone monitory nie są sprawdzane i nie wywołują alertów.
6. Tabela pokazuje dla każdego punktu kondycję (Zdrowy, Wymaga uwagi, Krytyczny, Oczekuje na pierwsze sprawdzenie, Wyłączony), każdy adres z wersją TLS, wygaśnięciem i odciskiem albo przyczyną niepowodzenia, ustalenia z czasem, od którego są otwarte, ostatnie sprawdzenie i osobę, która zmieniła monitor. Widok odświeża się automatycznie; Odśwież stan przeładowuje go od razu.

DANE I PARAMETRY

- Nazwa hosta lub adres IP, port 1–65535 i interwał w granicach Clm:EndpointHealth:MinimumIntervalMinutes–MaximumIntervalMinutes (domyślnie DefaultIntervalMinutes, 15).
- Opcjonalny oczekiwany odcisk: 64 znaki szesnastkowe, dwukropki dozwolone. Opcjonalne kotwice zaufania: 1–10 certyfikatów CA w PEM, nigdy klucze prywatne (odrzucane).
- Adresy niepubliczne (prywatne, loopback, link-local, współdzielone, dokumentacyjne i przejściowe) są sprawdzane tylko w sieciach, które operator instalacji wymienia w Clm:Discovery:AuthorizedPrivateNetworks; w przeciwnym razie są zgłaszane jako Adres niepubliczny bez autoryzacji i nigdy nie są kontaktowane.

WYNIK OPERACJI

Dla każdego monitorowanego punktu najnowszy wynik każdego adresu i jego ustalenia, alerty otwierane i zamykane razem z ustaleniami oraz wpisy endpoint-health.monitor.created, .updated i .deleted w dzienniku bezpieczeństwa (eksportowane do SIEM jako CONFIG-035).

UPRAWNIENIA

Wyniki czyta każdy użytkownik organizacji. Administratorzy dodają, zmieniają i usuwają monitory; operatorzy i tokeny API z rolą Operator uruchamiają Sprawdź teraz. Tokeny API nie zarządzają monitorami.

OGRANICZENIA

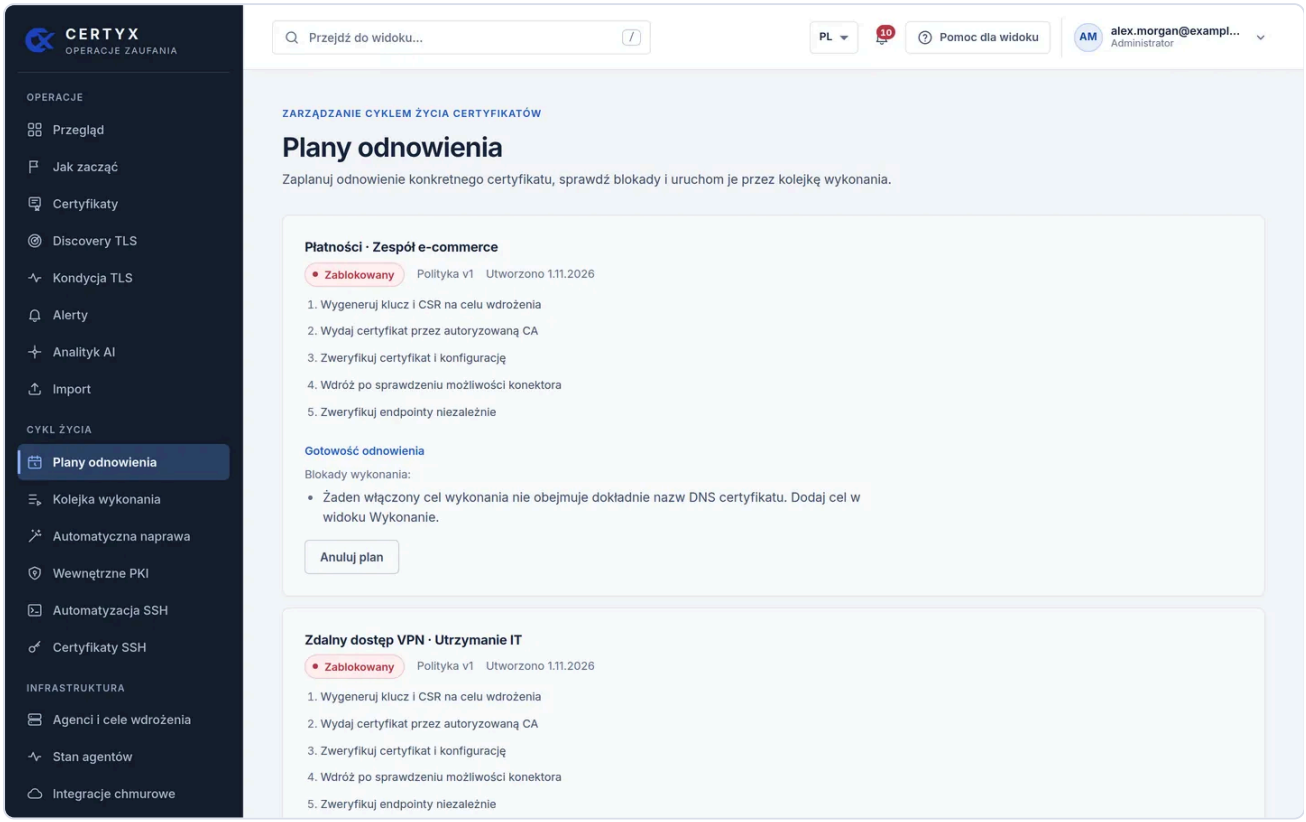
Sprawdzenia działają z płaszczyzny sterowania CERTYX, więc widzą to, co widzi internet (lub dopuszczone sieci wewnętrzne); punkty osiągalne tylko w sieci klienta wymagają dopuszczonej sieci albo pozostają niedozwolone. Organizacja ma najwyżej Clm:EndpointHealth:MaximumMonitors monitorów. Unieważnienie jest sprawdzane online przez adresy CRL lub OCSP zapisane w certyfikatach; bez nich pojawia się ustalenie Nie można sprawdzić statusu unieważnienia. Test TLS 1.0/1.1 wymaga na hoście CERTYX biblioteki TLS, która nadal potrafi zaoferować te wersje; jeśli nie potrafi, wynik pozostaje nieokreślony zamiast zostać zgłoszony jako bezpieczny. Po uzgodnieniu TLS nie są wysyłane żadne żądania aplikacyjne.

ROZWIĄZYWANIE PROBLEMÓW

- Adres niepubliczny bez autoryzacji: nazwa wskazuje na adres wewnętrzny. Poproś operatora instalacji o dopuszczenie tej sieci (Clm:Discovery:AuthorizedPrivateNetworks) albo monitoruj nazwę publiczną.
- Punkt końcowy TLS nieosiągalny: sprawdź zaporę, port i to, czy usługa nasłuchuje na każdym adresie, na który wskazuje nazwa; pojedynczy nieosiągalny węzeł za load balancerem jest zgłaszany tylko dla swojego adresu.
- Niezaufany łańcuch przy prywatnym CA: dodaj certyfikat główny CA jako kotwicę zaufania monitora. Brak certyfikatu pośredniego: skonfiguruj serwer tak, by wysyłał pełny łańcuch (certyfikat końcowy, a po nim pośrednie).
- Węzły serwują różne certyfikaty: wdroż odnowiony certyfikat na pozostałe węzły (Wykonanie) i wybierz Sprawdź teraz.

7 Plany odnowienia

Zaplanuj odnowienie konkretnego certyfikatu, sprawdź blokady i uruchom je przez kolejkę wykonania.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Dopóki automatyczne odnawianie jest włączone dla certyfikatu (Kolejka wykonania, polityka lub szczegóły certyfikatu), odnawia się on bez planu; plany służą certyfikatom odnawianym z zatwierdzeniem lub wymagającym odnowienia poza harmonogramem.
2. Otwórz szczegóły certyfikatu i wybierz Zaplanuj odnowienie.
3. Przejrzyj pięć etapów i Blokady wykonania. Są wyliczane za każdym razem z bieżącego stanu: włączony cel wdrożenia musi mieć dokładnie te same tożsamości co certyfikat (nazwy DNS, a dla certyfikatów klienta także adresy e-mail, nazwy UPN i URI), a rozszerzone użycie klucza certyfikatu musi dopuszczać przeznaczenie celu; agent celu (i agent weryfikujący, jeśli ustawiony) musi kontaktować się z CERTYX w oknie Clm:Lifecycle:AgentContactWindow (domyślnie 10 minut), a cel musi mieć ustawiony urząd certyfikacji. Blokady usuwasz w widokach Kolejka wykonania (cele wdrożenia) oraz Agenci i cele wdrożenia.
4. Administrator wybiera Zatwierdź plan przy planie Gotowy do zatwierdzenia. Zatwierdzenie tworzy zlecenie odnowienia dla pasującego celu w zwykłej kolejce wykonania, zgodnie z bieżącą polityką i subskrypcją.
5. Inny administrator zatwierdza zlecenie (tutaj przyciskiem Zatwierdź zlecenie jako druga osoba albo w widoku Kolejka wykonania); osoba, która zażądała zlecenia, widzi informację, że musi je zatwierdzić inny administrator. Status planu odzwierciedla wtedy zlecenie: W kolejce do agenta, Wykonywany

przez agenta, Wynik wymaga wyjaśnienia, Wdrożony i zweryfikowany, Błąd, Przywrócono poprzednie wdrożenie lub Zlecenie anulowane.

6. Po błędzie, przywróceniu lub anulowaniu zlecenia wybierz Zatwierdź ponownie z nowym zleceniem albo Anuluj plan (po potwierdzeniu; anulowanego planu nie można przywrócić).
7. Każdy plan prowadzi do Gotowości odnowienia swojego certyfikatu (każdy krok z tym, czego brakuje) i do stanu agenta celu.

DANE I PARAMETRY

- Plan odnosi się do certyfikatu, właściciela, usługi i wersji polityki.
- Jeden aktywny plan na certyfikat; powtórne żądanie zwraca istniejący plan.
- Cel jest wybierany automatycznie: spośród włączonych celów o tożsamościach równych tożsamościom certyfikatu i z dopuszczonym przeznaczeniem ten z najmniejszą liczbą blokad (potem o najniższym ID).
- Każda decyzja przesyła wersję planu; jeśli plan zmienił się w międzyczasie, decyzja jest odrzucana i trzeba ją powtórzyć po odświeżeniu.

WYNIK OPERACJI

Wersjonowany i audytowany plan powiązany ze zleceniem wykonania. Zweryfikowane wdrożenie kończy plan; zmiana polityki oraz zmiana właściciela lub usługi certyfikatu przywracają zatwierdzony plan do ponownego zatwierdzenia (Gotowy do zatwierdzenia lub Zablokowany).

UPRAWNIENIA

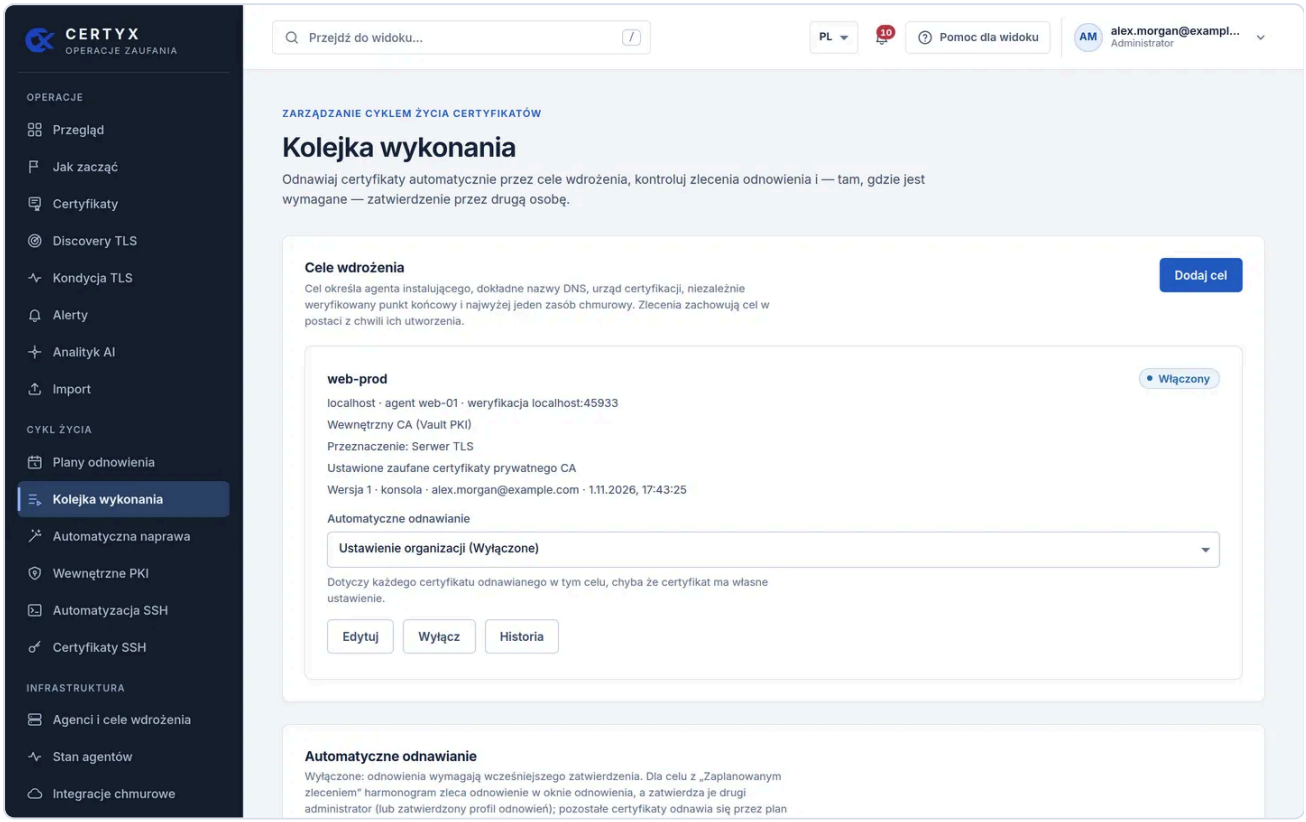
Operator lub administrator: tworzenie planów (w szczegółach certyfikatu). Administrator: zatwierdzanie i anulowanie planów. Inny administrator: zatwierdzenie zlecenia. Audytor i operator: odczyt, z informacją, że plany zatwierdza i anuluje wyłącznie administrator.

OGRANICZENIA

Zatwierdzenie nigdy nie omija zasady dwóch osób: administrator, który zatwierdził plan, nie może zatwierdzić jego zlecenia. Anulowanie planu anuluje zlecenie tylko, dopóki nie przejął go agent; wykonywane zlecenie kończy się lub jest wyjaśniane w widoku Kolejka wykonania. Oczekujące zlecenie z wcześniejszej wersji polityki trzeba anulować w widoku Kolejka wykonania przed ponownym zatwierdzeniem planu. Kontakt agenta jest sprawdzany na podstawie pobierania zleceń i raportów stanu; nie dowodzi powodzenia CA ani wdrożenia — dowodem jest wynik zlecenia i niezależna weryfikacja punktu końcowego. Na usłudze z subskrypcjami zlecenie wymaga funkcji AUTO_DEPLOYMENT, a certyfikat staje się zarządzaną rodziną w ramach limitu subskrypcji; po osiągnięciu limitu zatwierdzenie jest odrzucane.

8 Kolejka wykonania

Odnawiaj certyfikaty automatycznie przez cele wdrożenia, kontroluj zlecenia odnowienia i — tam, gdzie jest wymagane — zatwierdzenie przez drugą osobę.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. W sekcji Cele wdrożenia administrator dodaje cel albo tworzy go z projektu agenta w widoku Agenci i cele wdrożenia (Dodaj cel otwiera formularz; Przeznaczenie certyfikatu — zob. niżej): agent instalujący, dokładne nazwy DNS, host, port i ścieżka kontroli weryfikacji, urząd certyfikacji (wewnętrzny Vault PKI z mount i rolą albo publiczny ACME) z adresem HTTPS, opcjonalne zaufane certyfikaty prywatnego CA (wyłącznie certyfikaty PEM), opcjonalny agent weryfikujący u klienta i najwyżej jeden zasób chmurowy (AWS ACM: ARN certyfikatu i rola obciążenia; Azure Key Vault: adres sejfu, certyfikat, dzierżawa i tożsamość zarządzana; Google Certificate Manager: projekt, lokalizacja, certyfikat i konto usługi). Każdy zapis zwiększa wersję i jest widoczny w Historii; Wyłącz wstrzymuje nowe zlecenia. Zlecenie zachowuje pełny cel z chwili utworzenia, więc późniejsze zmiany nie wpływają na oczekujące zlecenia. Następnie wybierz włączony cel.
2. Instalacja: Agent na hoście, który używa certyfikatu (domyślnie), oznacza, że agent instalujący zapisuje pliki i przeładowuje usługę na własnej maszynie. Agent jako przekaźnik SSH do hosta bez agenta oznacza, że agent instalujący łączy się przez SSH z podanym hostem zdalnym, generuje tam klucz (nigdy nie opuszcza tego hosta), instaluje certyfikat i przeładowuje usługę; agent potrzebuje tego miejsca wdrożenia z Remote w swojej konfiguracji i wpisanego do RelayDestinations, a zadania dla każdego innego hosta odrzuca. Przekaźnik SSH dotyczy certyfikatów serwera TLS bez zasobu chmurowego, dlatego wybór chmury jest ukryty. Bez agenta na hoście lub przekaźnika z dostępem SSH CERTYX nie może automatycznie zainstalować certyfikatu.

3. W sekcji Zleć wystawienie lub odnowienie wybierz włączony Cel wdrożenia. W polu Rodzaj zlecenia / certyfikat wybierz Wystaw nowy certyfikat i podaj Właściciel, Usługa i Produkcja w sekcji Własność nowego certyfikatu albo wybierz do odnowienia bieżący (niezastąpiony) certyfikat z inwentarza; odnowienie zachowuje jego własność.
4. Automatyczne odnawianie (panel nad formularzem zlecenia) jest domyślnie włączone: każdy certyfikat z pasującym, włączonym celem wdrożenia odnawia się bez ręcznego zatwierdzania. W oknie odnowienia polityki harmonogram zleca zadanie, automatyczne odnawianie je zatwierdza (zapisane jako zatwierdzone przez system:auto-renewal), agent wystawia i instaluje certyfikat, CERTYX niezależnie weryfikuje punkt końcowy, a inwentarz zostaje zaktualizowany. Administrator wybiera Wyłącz automatyczne odnawianie, aby wymagać zatwierdzenia w całej organizacji (Włącz automatyczne odnawianie prosi o potwierdzenie). Każda karta celu ma własny wybór Automatyczne odnawianie — Ustawienie organizacji, Odnawiaj automatycznie lub Wymagaj zatwierdzenia — a szczegóły certyfikatu oferują ten sam wybór dla certyfikatu; obowiązuje najbardziej szczegółowy wybór (certyfikat, potem cel, potem organizacja).
5. Wybierz Zleć wystawienie lub odnowienie. Inny administrator zatwierdza zlecenie przyciskiem Zatwierdź jako druga osoba w ramach bieżącej polityki albo anuluje je przyciskiem Anuluj, dopóki nie przejął go agent.
6. Agent generuje klucz i CSR tam, gdzie certyfikat jest używany (na własnym hoście albo, jako przekaźnik SSH, na hoście zdalnym), korzysta z Vault, ACME lub DigiCert i instaluje konektorem miejsca wdrożenia: pem-files, nginx, apache, haproxy, lighttpd, caddy, traefik, envoy, cribl, tomcat, java-keystore, postfix, dovecot, kubernetes-secret, windows-store, iis, albo w zasobie chmurowym celu (AWS ACM, Azure Key Vault, Google Certificate Manager), albo jako pliki dla celu wyłącznie klienckiego. Konektory plikowe publikują skonfigurowane pliki atomowo z właścicielem i trybem, uruchamiają sprawdzenie konfiguracji i przeładowanie oraz weryfikują punkt końcowy przez TLS; błąd przywraca poprzednią generację. CERTYX niezależnie sprawdza cel przed przyjęciem sukcesu.
7. Po wygaśnięciu dzierżawy (zlecenie w uzgadnianiu) administrator wybiera Sprawdź rzeczywisty stan celu, przegląda zaobserwowany dowód, a następnie wybiera Zaakceptuj zweryfikowany certyfikat albo Potwierdź poprzednie wdrożenie. CERTYX ponownie weryfikuje skrót przed rozstrzygnięciem; dopóki agent weryfikujący klienta nie zaobserwował punktu końcowego, przycisk pokazuje oczekiwanie. Wnioskodawca nie rozstrzyga własnego zlecenia.
8. Profile automatycznych odnowień działają, gdy automatyczne odnawianie jest wyłączone: dla celu z Zaplanowanym zleceniem harmonogram zleca należne odnowienia, które czekają na zatwierdzenie. Administrator wybiera Wnioskuj o automatyzację na 90 dni, inny administrator wybiera Zatwierdź jako drugi administrator, a każdy z nich może wybrać Cofnij automatyzację; dopóki profil jest ważny, zatwierdza on zaplanowane zlecenia. Wymaga funkcji subskrypcji AUTO_RENEWAL; zmiana celu lub polityki unieważnia zatwierdzenie.
9. Agent cyklu certyfikatów w Unix wymaga katalogu stanu, plików sekretów i dzienników dostępnych tylko właścicielowi, bez dowiązań symbolicznych w ścieżce i katalogach nadrzędnych. Niebezpieczny lub zbyt duży dziennik zatrzymuje wykonanie do wyjaśnienia przez administratora. Start nie zmienia uprawnień istniejącego katalogu stanu. W Windows agent stosuje tę samą zasadę do plików sekretów i dzienników przez ACL: ich właścicielem i jedynymi podmiotami z dostępem mogą być tylko LocalSystem, Administratorzy lub tożsamość agenta; wszystko inne jest odrzucane. Instalator Windows odpowiednio ogranicza ACL katalogu agenta.
10. Agent cyklu certyfikatów w Unix może odczytywać zatwierdzone sekrety tekstowe Azure Key Vault, AWS Secrets Manager i Google Secret Manager przez lokalną tożsamość CLI klienta. Ustaw dokładne SecretBindings i uruchom Clm.Agent secret-check z chronioną konfiguracją jako konto usługi przed

włączeniem wykonania. Wartości pozostają lokalnie i nie są wyświetlane. Zobacz CUSTOMER-VAULTS.pl.md. Odczyt przez CLI dostawców działa tylko w agentach Unix; w Windows dostępne są wyłącznie sekrety z chronionych plików. Klucze prywatne są generowane i przechowywane programowo na hoście agenta (bez HSM), a agent nie wysyła poczty z hosta klienta.

11. HashiCorp Vault KV obsługuje dokładną referencję HTTPS mount/ścieżka#pole i lokalny token helper klienta. Weryfikacja TLS jest obowiązkowa; przestrzenie nazw nie są obsługiwane. Odczyt kończy się błędem, gdy dostęp jest zabroniony, tożsamość unieważniona lub certyfikat Vault niezaufany. Token Vault pochodzi z token helpera klienta; CERTYX nie tworzy ani nie odnawia tożsamości Vault.
12. Zapisane wyniki wykonania są ponownie przesyłane po przejściowych błędach połączenia, przekroczeniu czasu żądania oraz HTTP 408/429/500/502/503/504, z odstępem PollSeconds i ograniczeniem OperationTimeoutSeconds. Ponowienie zachowuje zadanie, dzierżawę i wynik; nie powtarza wydania ani instalacji certyfikatu. Przy odzyskiwaniu po restarcie agent odnawia dzierżawę podczas przesyłania zapisanego wyniku. Błędy uwierzytelniania, uprawnień, wygasłej lub uzgodnionej dzierżawy i zaufania TLS zatrzymują wykonanie do uzgodnienia. Mechanizm nie przywraca utraconej dzierżawy; awaria dłuższa niż dzierżawa lub limit operacji nadal wymaga uzgodnienia przez administratora.
13. Wszystkie mechanizmy odczytu konfiguracji JSON agenta odrzucają dowiązania pliku lub katalogów nadrzędnych, uprawnienia grupy lub innych użytkowników w Unix, pliki większe niż 1 MiB oraz niepoprawny UTF-8 przed deserializacją. W Unix zabezpiecz konfigurację poleceniem chmod 600. Względne ścieżki argumentów są przekształcane do bezwzględnych i sprawdzane według tych samych reguł. Obsługiwany jest UTF-8 z BOM i bez BOM. Odczyt ustawień i odczyt asynchroniczny stosują te same zasady; komunikaty błędów nie zawierają wartości konfiguracji. W Windows odczyt odrzuca plik, którego właścicielem jest lub który może odczytać albo zmienić inny podmiot niż LocalSystem, Administratorzy lub tożsamość agenta; przed wdrożeniem ustaw restrykcyjne ACL.
14. Prywatne endpointy mogą korzystać z oddzielnego, zarejestrowanego weryfikatora. Operator przypisuje jego ID do celu wykonania; w widoku Agenci i cele wdrożenia, w sekcji Zarejestrowani agenci, wybierz dla instalatora „Włącz wykonywanie cyklu życia certyfikatów", a dla innej tożsamości agenta „Włącz niezależną weryfikację endpointów". Weryfikator sprawdza lokalnie zatwierdzone TLS/HTTP przed akceptacją sukcesu. Konfiguracja to jedno polecenie na hoście weryfikatora: karta celu w Wykonanie → Cele wdrożenia pokazuje Konfiguracja niezależnego weryfikatora endpointu z nadaniem uprawnienia, przyciskiem Pobierz zakres weryfikatora (ID celu, host weryfikacji, port, ścieżka kontroli stanu i zaufane certyfikaty celu; wyłącznie dane publiczne) i poleceniem configure-verifier-linux.sh add-target (Linux, clm-endpoint-verifier.service na koncie agenta) lub configure-verifier-windows.ps1 add-target (Windows, zadanie harmonogramu CERTYX Endpoint Verifier jako LOCAL SERVICE). Skrypt zapisuje konfigurację dostępną tylko dla właściciela z własnej tożsamości agenta, wykonuje jeden sprawdzony cykl, uruchamia usługę i czeka do dziesięciu minut na nadanie uprawnienia, dopóki CERTYX odpowiada HTTP 403; remove-target, disable i status nią zarządzają, a deinstalator ją usuwa. Nowy agent otrzymuje tę rolę przy instalacji (CLM_AGENT_ENDPOINT_VERIFIER w Linuksie, -EndpointVerifierTarget w Windows). Bez zaufanych certyfikatów w celu host weryfikatora musi sam ufać CA wystawcy.
15. Zarejestrowani instalatorzy raportują własną pracę agenta cyklu życia (Praca agenta cyklu życia w widoku Stan agentów: uruchamianie, bezczynność lub błąd). Brak raportów jest widoczny również przy działającym discovery. Zdrowie procesu nie zastępuje wyniku wykonania i niezależnego dowodu endpointu. Przy zatrzymaniu do uzgodnienia sprawdź chronione lokalne dzienniki.

16. Przeznaczenie certyfikatu: każdy cel jest celem serwera TLS (domyślnie), klienta TLS albo serwera i klienta TLS. Certyfikat klienta TLS uwierzytelnia użytkownika, urządzenie lub usługę wobec serwera w mutual TLS (EKU clientAuth). Wybierz Wewnętrzny CA (Vault PKI) z rolą ustawiającą client_flag (dla samego klienta server_flag=false); publiczne CA są odrzucane, bo ACME i produkty TLS DigiCert wystawiają tylko certyfikaty serwera. Tożsamości podaj w sekcji Tożsamości klienta: nazwy DNS, adresy e-mail, nazwy UPN i URI oraz opcjonalnie nazwę pospolitą podmiotu. Cel wyłącznie kliencki nie ma hosta weryfikacji, agenta weryfikującego ani zasobu chmurowego: agent generuje klucz lokalnie, CSR żąda dokładnie tych tożsamości, agent instaluje fullchain.pem i privkey.pem (oraz bundle.p12, gdy cel agenta wskazuje referencję hasła PKCS#12) i przed raportem lokalnie weryfikuje zainstalowane pliki (klucz, łańcuch do swoich zaufanych certyfikatów, EKU clientAuth). CERTYX przyjmuje publiczny certyfikat tylko z dokładnie tymi tożsamościami i EKU zlecenia. Cel w konfiguracji agenta musi deklarować te same Purpose i tożsamości Client (zob. AGENT-INSTALLATION).
17. Z gotowości odnowienia certyfikatu przycisk Utwórz cel z tymi wartościami otwiera formularz celu wypełniony propozycją; pod każdym wypełnionym polem widać Wypełniono na podstawie: ..., a pod każdym polem, którego CERTYX nie mógł ustalić, co wpisać i dlaczego. ID i przeznaczenie: lokalnego miejsca wdrożenia agenta z dokładnie nazwami certyfikatu (agent wykonuje tylko zadania, których ID celu, nazwy i przeznaczenie odpowiadają lokalnemu miejscu wdrożenia), w przeciwnym razie ID z pierwszej nazwy i przeznaczenie z certyfikatu; nazwy i tożsamości klienta pochodzą z certyfikatu. Agent instalujący: agent tego miejsca wdrożenia, w przeciwnym razie jedyny agent z procesem cyklu życia, w przeciwnym razie jedyny agent, którego zgłoszona mapa sieci zawiera adres, pod którym zaobserwowano certyfikat, o ile ma proces cyklu życia; inaczej pole zostaje puste z podaniem powodu. Host weryfikacji: musi to być nazwa (lub adres IP) zawarta w certyfikacie, bo CERTYX sprawdza certyfikat względem niej. Wykrywanie w sieci obserwuje adresy IP, więc CERTYX rozwiązuje nazwy DNS certyfikatu (bez nazw wieloznacznych, z ograniczoną liczbą i czasem) i wpisuje nazwę, która rozwiązuje się na zaobserwowany adres; gdy żadna nie pasuje — pierwszą nazwę z ostrzeżeniem, by ją sprawdzić; przy samych nazwach wieloznacznych host zostaje pusty; adres IP tylko wtedy, gdy certyfikat go zawiera albo nie ma nazw DNS. Port: tam, gdzie zaobserwowano certyfikat (np. 9000); 443 tylko wtedy, gdy nigdy go nie zaobserwowano. Urząd certyfikacji: gdy włączony cel wystawił już certyfikat z tego samego CA (ten sam wystawca i identyfikator klucza) — jego typ CA, adres URL, punkt montowania i rola Vault oraz zaufane certyfikaty główne; w przeciwnym razie typ z miejsca wdrożenia agenta, typ CA zapisany w inwentarzu albo z obserwacji (niezaufany łańcuch oznacza wewnętrzny CA; zaufany łańcuch oznacza publiczny CA tylko wtedy, gdy wszystkie nazwy są publiczne, a nie w domenach takich jak .internal, .local czy .home.arpa). Dla wewnętrznego CA bez takiego celu wpisz adres URL Vault, punkt montowania i rolę używane przez Twojego agenta. Zaufane certyfikaty główne są wypełniane tylko z tego celu albo rzeczywistym certyfikatem głównym wystawiającego CA z inwentarza; w przeciwnym razie wklej prywatny certyfikat główny (PEM), chyba że host CERTYX lub agent weryfikujący już mu ufa. Przed zapisaniem nic nie jest zapisywane. Agenci cyklu życia zgłaszają lokalne miejsca wdrożenia (konektor, katalog wdrożenia, pliki, polecenia sprawdzenia i przeładowania, zasób chmurowy, endpoint) w telemetrii procesu; sekrety i odwołania do sekretów nigdy nie są zgłaszane.
18. Nieudane lub wycofane zadanie pokazuje wynik agenta i dalsze kroki; każde zadanie prowadzi do gotowości odnowienia swojego certyfikatu i do stanu swojego agenta.

DANE I PARAMETRY

- Cel wdrożenia: włączony cel organizacji. Cele z konfiguracji serwera CLM_EXECUTION_TARGETS (Clm:Execution:Targets) są jednorazowo kopiowane do swojej organizacji przy pierwszym użyciu i odtąd zarządzane tylko tutaj. Ścieżki plików serwera (plik zaufanych certyfikatów, testowe wyłączenie

sprawdzania odwołań, katalog ACME Renewal Information) pochodzą wyłącznie z tej konfiguracji i są zachowywane przy edycji takiego celu. Nieprawidłowe dane są odrzucane z podaniem przyczyny.

- Certyfikat: z inwentarza i niezastąpiony, z dokładnie tymi samymi tożsamościami co cel (nazwy DNS, a dla celów klienckich adresy e-mail, nazwy UPN i URI) i rozszerzonym użyciem klucza dopuszczającym przeznaczenie celu; w przeciwnym razie wniosek jest odrzucany z tą przyczyną.
- Nowe wystawienie: Właściciel i Usługa wymagane, 1–200 znaków każde; rezerwuje zarządzaną rodzinę certyfikatów w ramach limitu subskrypcji.
- Zatwierdzenie używa wersji zlecenia i tożsamości zatwierdzającego.
- Urząd certyfikacji Nieustawiony jest przyjmowany przy zapisie, ale plan odnowienia dla takiego celu pozostaje zablokowany, dopóki urząd nie zostanie wybrany.
- Formaty celu (każde pole ma własną pomoc, a przeglądarka podaje oczekiwany format): identyfikatory 1–100 liter, cyfr, łączników i podkreśleń; 1–100 różnych nazw DNS bez symboli wieloznacznych; host weryfikacji jako nazwa hosta lub adres IP bez https://, ścieżki i portu; ścieżka kontroli zaczynająca się od / (np. /healthz); adres CA zaczynający się od https://; mount i rola Vault do 120 liter, cyfr i znaków . _ / -; zaufane certyfikaty główne jako bloki certyfikatów PEM do 64 KiB; AWS arn:aws:acm:REGION:KONTO:certificate/UUID z rolą arn:aws:iam::TO-SAMO-KONTO:role/NAZWA; Azure https://NAZWA.vault.azure.net/, nazwa certyfikatu z liter, cyfr i łączników, identyfikatory dzierżawy i klienta jako GUID; Google identyfikator projektu, lokalizacja global lub region, np. europe-west1, identyfikator certyfikatu i NAZWA@PROJEKT.iam.gserviceaccount.com.
- Katalogi kluczy i wdrożeń wymagają bezwzględnych ścieżek bez dowiązań. Klucze i dzienniki odzyskiwania wymagają dostępu tylko właściciela; dowiązany, współdzielony lub zbyt duży stan jest odrzucany. Dozwolony jest jedynie zarządzany link current do generacji UUID.
- Formaty tożsamości klienta (każde pole ma pomoc; serwer przy odrzuceniu podaje oczekiwany format): e-mail jan.kowalski@example.com (ASCII, jeden znak @, domena DNS, najwyżej 254 znaki); nazwa UPN jkowalski@corp.example.com (nazwa logowania, @, sufiks DNS katalogu, nie CORP\jkowalski); URI ze schematem, np. spiffe://example.org/ns/prod/sa/payments lub urn:uuid:..., bez spacji i części użytkownik:hasło; nazwa pospolita 1–64 znaki, wymagana, gdy podano tylko URI. Jedna wartość w wierszu; najwyżej 100 tożsamości.
- Host zdalny (przekaźnik SSH): nazwa DNS lub adres IP, najwyżej 253 znaki, dokładnie jak Remote.Host w konfiguracji agenta przekaźnika, np. web-01.internal.example.

WYNIK OPERACJI

Wynik zlecenia, publiczny certyfikat w rejestrze i audyt. Zastąpiony certyfikat ma stan archiwalny.

UPRAWNIENIA

Administrator: tworzenie, edycja, wyłączanie i włączanie celów, anulowanie nieprzejętych zleceń, uzgadnianie zleceń oraz wnioskowanie o profile automatyzacji i ich cofanie. Operator lub administrator: zlecanie (w usłudze z subskrypcjami tylko z funkcją AUTO_DEPLOYMENT). Administrator inny niż wnioskodawca: zatwierdzanie zleceń i profili automatyzacji; wnioskodawca nie może uzgodnić własnego zlecenia. Audytor (oraz operator): odczyt celów, profili i zleceń; dla audytora formularz zlecenia jest tylko do odczytu. Przycisk Historia celu i historię zmian (wersja, zmiana, adres e-mail konta, czas) widzi każda rola; przyciski Edytuj i Wyłącz/Włącz widzi tylko administrator. Administrator: włączanie i wyłączanie automatycznego odnawiania dla organizacji oraz wybór dla celu i certyfikatu; ustawienie widzi każda rola.

OGRANICZENIA

Harmonogram odnowień sprawdza włączone cele każdej organizacji co Clm:Lifecycle:SchedulerInterval (domyślnie 5 minut). Automatyczne odnawianie dotyczy najnowszego certyfikatu z dokładnie tymi tożsamościami co cel; wymaga funkcji subskrypcji AUTO_RENEWAL (bez niej każde odnowienie czeka na zatwierdzenie) i odnawia krótkotrwałe certyfikaty dopiero w ostatniej jednej trzeciej ich ważności. Po nieudanym, wycofanym lub anulowanym zadaniu w celu następne odnowienie czeka na zatwierdzenie; po jego powodzeniu odnowienia znów przebiegają automatycznie. Najwyżej Clm:Lifecycle:AutomaticRenewalsPerDay (domyślnie 200) odnowień na organizację jest zatwierdzanych automatycznie w ciągu 24 godzin; kolejne należne odnowienia czekają na zatwierdzenie. Zanim agent otrzyma automatycznie zatwierdzone zadanie, CERTYX sprawdza je ponownie: zmieniony cel je anuluje, a wyłączone ustawienie przywraca je do zatwierdzenia. Zlecenia ręczne i zadania z planów odnowienia zawsze wymagają drugiego administratora. Domyślne ustawienie instalacji to Clm:Lifecycle:AutomaticRenewalByDefault (true). W usłudze współdzielonej przez wiele organizacji ustaw Clm:Execution:AllowPrivateVerificationEndpoints na false: hosty weryfikacji typu loopback, prywatne i link-local wymagają wtedy agenta weryfikującego u klienta, a panel odmawia weryfikacji hosta rozwiązywanego na taki adres. Rejestracja agentów używa jednorazowych kodów w widoku Agenci; lokalna konfiguracja agenta (poświadczenia CA, ścieżki wdrożenia) pozostaje na hoście klienta. Weryfikacja adresów lokalnych, prywatnych lub link-local przez sam CERTYX wymaga zgody operatora platformy dla Twojej organizacji; w przeciwnym razie przypisz agenta weryfikującego. Certyfikaty klienta TLS są wydawane wyłącznie przez role Vault PKI; ACME, DigiCert i magazyny TLS w chmurze są odrzucane z konkretnym powodem. Certyfikaty klienta są dostarczane w agentach Unix jako pliki PEM i opcjonalny pakiet PKCS#12; magazyn certyfikatów Windows, rejestracja w przeglądarce i karty inteligentne nie są obsługiwane. Ich weryfikacja to lokalne sprawdzenie przez agenta instalującego, a nie niezależna obserwacja punktu końcowego; zlecenia wyłącznie klienckiego w stanie uzgadniania nie da się rozstrzygnąć obserwacją: agent dostarcza zapisany wynik przy następnym uruchomieniu, w przeciwnym razie operator sprawdza katalog wdrożenia na hoście agenta. Przekaźnik SSH instaluje tylko certyfikaty serwera TLS (bez certyfikatów klienta i magazynu Windows) z kluczem RSA-3072 wygenerowanym na hoście zdalnym; jedno zdalne miejsce wdrożenia powinno należeć do jednego przekaźnika. Usługi pocztowe są weryfikowane na portach z niejawnym TLS (465, 993, 995); STARTTLS nie jest obsługiwany.

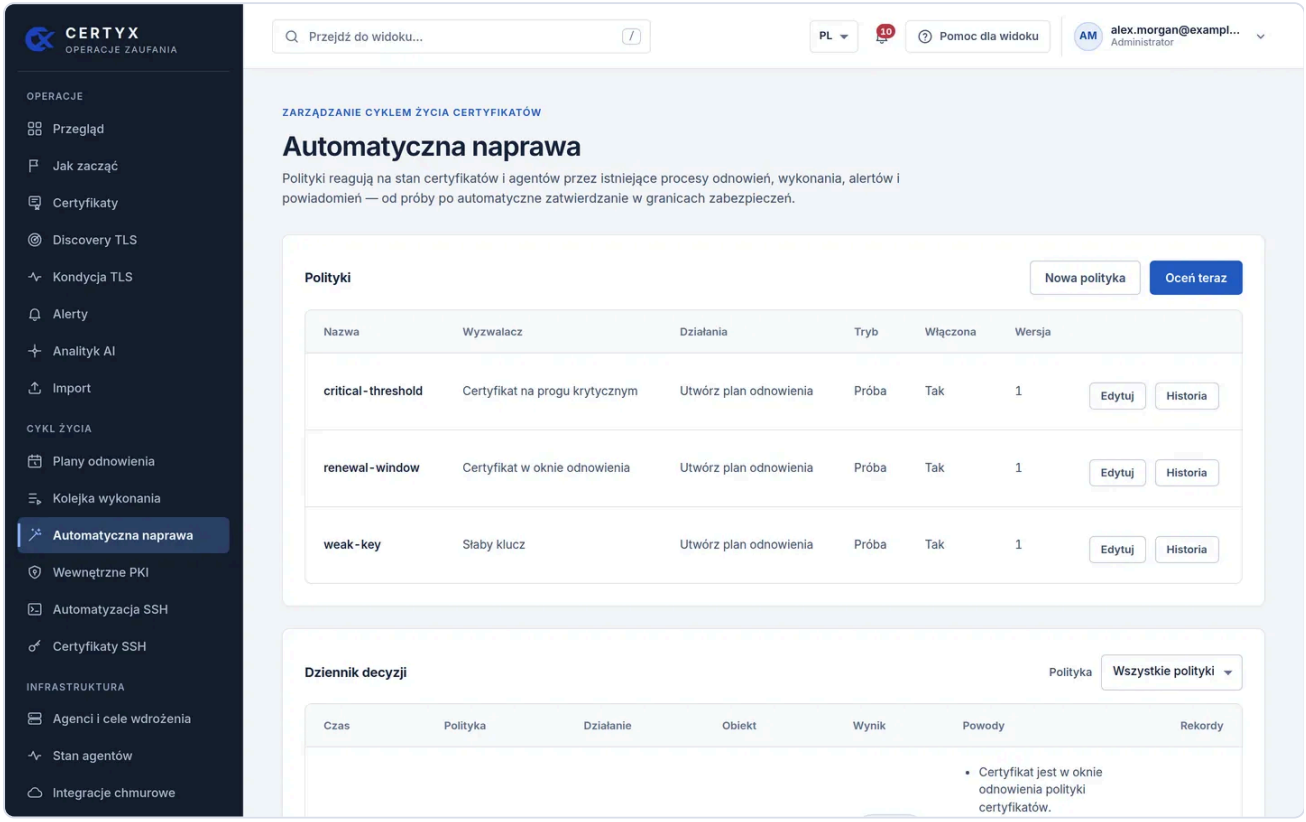
ROZWIĄZYWANIE PROBLEMÓW

- Gotowość informuje, że agent nie ma lokalnego miejsca wdrożenia o ID celu: dodaj do konfiguracji agenta (agent.json, Destinations) miejsce o dokładnie tym ID, tych samych nazwach DNS i przeznaczeniu, uruchom agenta ponownie i poczekaj na jego następny raport.
- Weryfikacja kończy się błędem niezgodności nazwy po utworzeniu celu z gotowości: host weryfikacji musi być nazwą (lub adresem IP) zawartą w certyfikacie. Zastąp adres IP nazwą DNS certyfikatu, która prowadzi do endpointu; jeśli wskazówka mówi, że nazwy nie rozwiązały się na zaobserwowany adres, sprawdź DNS na hoście CERTYX albo wpisz nazwę, którą serwuje endpoint.
- Miejsce wdrożenia agenta ma inne nazwy, przeznaczenie lub rodzaj CA: ujednolić cel i miejsce wdrożenia; cele wewnętrzne wymagają miejsca Vault, publiczne ACME lub DigiCert.
- Agent nie zgłosił miejsc wdrożenia: zgłasza je z każdym raportem procesu cyklu życia, gdy działa z zarejestrowaną tożsamością; sprawdź jego diagnozę w Stanie agentów.
- Wycofano: agent zainstalował nowy certyfikat, ale sprawdzenie endpointu nie powiodło się i przywrócono oraz zweryfikowano poprzednią generację; sprawdź polecenie przeładowania, serwowany host i port oraz zaufane certyfikaty główne, a następnie zatwierdź plan ponownie.

- Uzgodnienie: dzierżawa wygasła przed wynikiem; sprawdź tutaj faktyczne miejsce wdrożenia i przyjmij zweryfikowany certyfikat albo potwierdź pierwotną instalację.
- Gotowość podaje, że agent instaluje w innym trybie: cel wskazuje przekaźnik SSH, a miejsce wdrożenia agenta nie ma Remote (lub odwrotnie). Ujednolić oba: wybierz instalację w celu, dodaj lub usuń Remote i RelayDestinations w konfiguracji agenta i poczekaj na jego następny raport.
- Gotowość podaje, że przekaźnik wdraża na inny host: ustaw host zdalny celu dokładnie na Remote.Host miejsca wdrożenia agenta. Uruchom Clm.Agent relay-check na przekaźniku, aby sprawdzić przypięcie klucza hosta, logowanie SSH, pomocnika, regułę sudo i sprawdzenie konfiguracji bez zmiany certyfikatu.

9 Automatyczna naprawa

Polityki reagują na stan certyfikatów i agentów przez istniejące procesy odnowień, wykonania, alertów i powiadomień — od próby po automatyczne zatwierdzanie w granicach zabezpieczeń.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Wymaga funkcji subskrypcji AUTONOMOUS_REMEDIATION. Administrator wybiera Nowa polityka i podaje identyfikator (1–100 liter, cyfr, łączników lub podkreśleń; nie można go później zmienić), nazwę (1–100 znaków), Włączona, wyzwalacz i obsługiwane przez niego działania, tryb oraz opcjonalnie do 50 usług rozdzielonych przecinkami, do których polityka jest ograniczona (każda do 200 znaków; puste pole oznacza wszystkie usługi), właściciela do przypisania (1–200 znaków, wymagany dla Przypisz właściciela) i grupę odpowiedzialności do powiadomienia (wymagana dla Powiadom grupę).
2. Wyzwalacze: certyfikat w oknie odnowienia, na progu krytycznym, słaby klucz, słaby podpis (także dla wygasłych certyfikatów, gdy ma to zastosowanie), certyfikat wymieniony poza CERTYX (otwarty alert discovery) i agent offline (offline, z błędem lub z wygasłą tożsamością).
3. Podgląd (próba) ocenia szkic na bieżących danych i pokazuje, co by zrobił, niczego nie zmieniając ani nie zapisując. Zapisz politykę tworzy nową wersję; Edytuj otwiera istniejącą politykę; Historia pokazuje każdą wersję i autora zmiany.
4. Tryby: Próba tylko zapisuje, co by się stało. Proponuj tworzy plany odnowień i zleca zadania wykonania, które nadal wymagają zwykłego zatwierdzenia przez drugą osobę, wysyła powiadomienia grup i zapisuje potwierdzenia oraz zmiany właściciela jako zalecenia. Automatyczne zatwierdzanie dodatkowo zatwierdza plany i zadania w granicach zabezpieczeń, w imieniu administratora, który

zapisał politykę po potwierdzeniu ostrzeżenia. Zapis w trybie automatycznym wymaga zaznaczenia Rozumiem i włączam automatyczne zatwierdzanie dla tej polityki, co najmniej jednego okna zmian oraz — gdy polityka tworzy plany odnowień lub zleca zadania — co najmniej jednego dozwolonego celu.

5. Ocena działa co Clm:Remediation:Interval (domyślnie 5 minut) dla każdej aktywnej organizacji z licencją, na jednej instancji aplikacji naraz, chyba że operator serwera ustawił Clm:Remediation:WorkerEnabled na false; Oceń teraz uruchamia ją od razu. Dziennik decyzji pokazuje każdą decyzję z wynikiem (zadziałałaby, zaproponowano, wykonano, pominięto, odmówiono, niepowodzenie), przetłumaczonymi powodami i odnośnikami do celu, planu i zadania; Wyjaśnij otwiera analityka AI, gdy jest włączony.

DANE I PARAMETRY

- Działania według wyzwalacza: wyzwalacze certyfikatów obsługują potwierdzenie alertu, przypisanie właściciela, powiadomienie grupy, utworzenie planu odnowienia i zlecenie zadania wykonania; wymiana poza CERTYX obsługuje potwierdzenie alertu i powiadomienie grupy; agent offline obsługuje powiadomienie grupy.
- Przypisz właściciela zmienia tylko certyfikaty bez właściciela (puste pole lub „unassigned”); certyfikat, który ma już właściciela, jest pomijany z tym powodem.
- Zabezpieczenia automatycznego zatwierdzania: dozwolone cele (do 200 celów wykonania organizacji), maksymalna liczba wykonanych działań w ciągu 24 godzin (od 1 do Clm:Remediation:MaxActionsPerDayLimit, domyślnie 500), do 20 okien zmian w UTC (każde z co najmniej jednym dniem; godzina początku 0–23 przed godziną końca 1–24) oraz czy dozwolone są certyfikaty produkcyjne. Odnowienia są zatwierdzane tylko dla dozwolonego celu z niezależnym punktem weryfikacji.
- Oznaczenie produkcyjne i właściciel pochodzą z metadanych certyfikatu w inwentarzu; powiadomienia trafiają przez przekaźnik SMTP organizacji do grup odpowiedzialności z członkami.

WYNIK OPERACJI

Plany i zadania są tworzone jako system:remediation:<polityka>; zadania zatwierdzone automatycznie mają jako zatwierdzającego potwierdzającego administratora i przechodzą przez zwykły proces wykonania, którego weryfikacja wycofuje nieudane wdrożenie. Każda decyzja trafia do dziennika decyzji (przechowywanego Clm:Remediation:DecisionRetentionDays, domyślnie 400 dni) i do dziennika bezpieczeństwa; identyczna decyzja jest zapisywana najwyżej raz na Clm:Remediation:DecisionRepeatWindow (domyślnie 24 godziny). Zmiany polityk są wersjonowane i dziennikowane.

UPRAWNIENIA

Odczyt polityk, historii i dziennika decyzji: każda rola organizacji. Tworzenie, zmiana, podgląd i ocena: Administrator.

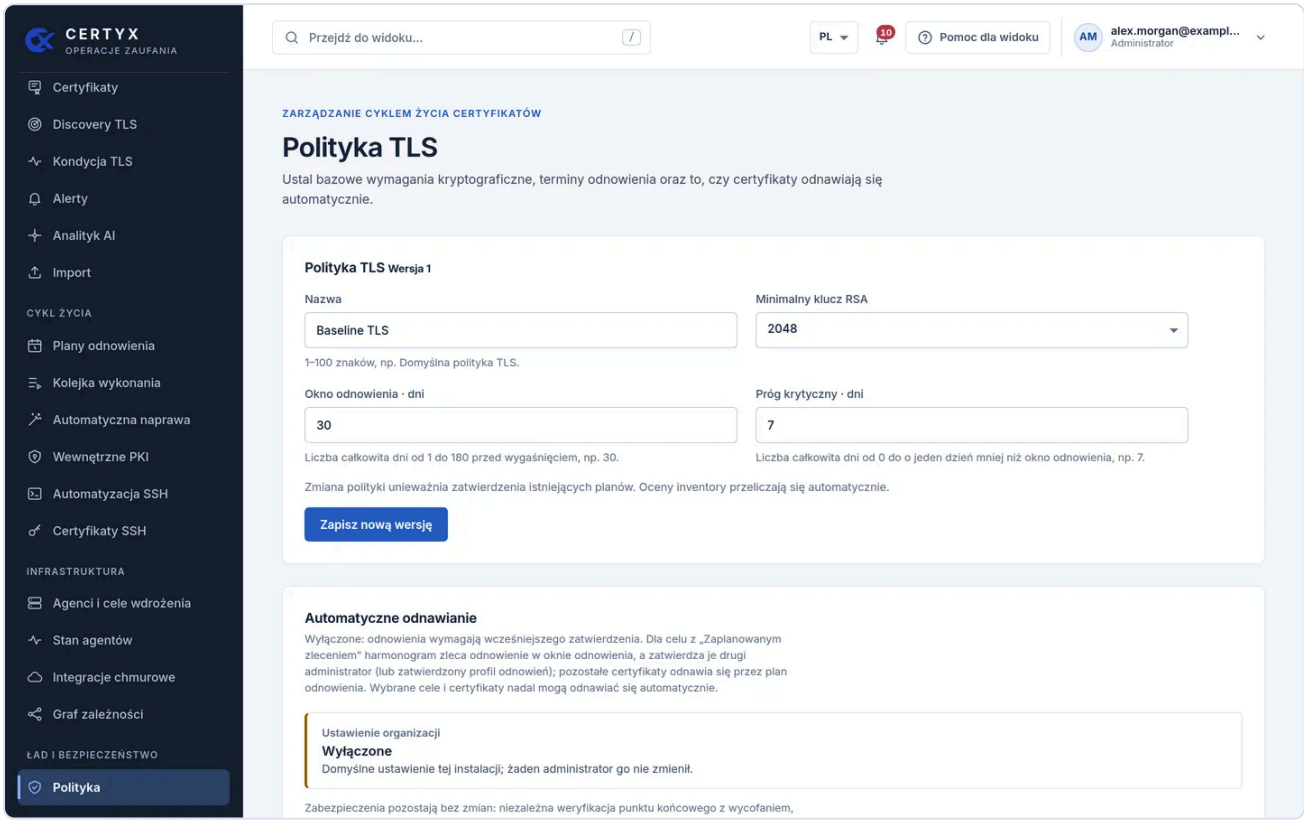
OGRANICZENIA

Unieważnienie jest niedostępne: żaden proces CERTYX nie unieważnia certyfikatów TLS, więc polityka z tym działaniem jest odrzucana. Tryb proponowania nie zmienia właścicieli ani alertów. Odnowienie następuje tylko, gdy plan nie ma blokad (cel z dokładnie tymi samymi tożsamościami co certyfikat i pasującym przeznaczeniem, osiągalny agent, skonfigurowany urząd certyfikacji). Bez funkcji subskrypcji widok informuje, że subskrypcja nie obejmuje automatycznej naprawy, i żadna polityka nie jest oceniana. Automatyczne zatwierdzanie nie sprawdza ponownie roli potwierdzającego administratora w chwili zatwierdzenia; edycja polityki w trybie automatycznym wymaga nowego potwierdzenia przez edytującego

administratora. Najwyżej Clm:Remediation:MaxPoliciesPerOrganization polityk (domyślnie 50) i Clm:Remediation:MaxSubjectsPerPolicy obiektów na politykę i przebieg (domyślnie 200). Wyjaśnienie przez analityka wymaga włączonego analityka AI.

10 Polityka TLS

Ustal bazowe wymagania kryptograficzne, terminy odnowienia oraz to, czy certyfikaty odnawiają się automatycznie.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Sprawdź bieżącą wersję pokazaną obok tytułu.
2. Podaj „Nazwa", „Minimalny klucz RSA", „Okno odnowienia · dni" i „Próg krytyczny · dni".
3. Wybierz „Zapisz nową wersję". Zatwierdzone plany odnowienia wracają do stanu zaplanowanego i wymagają ponownego zatwierdzenia; sprawdź ponownie ocenione certyfikaty.
4. Automatyczne odnawianie pokazuje ustawienie organizacji: Włączone (domyślnie) odnawia w oknie odnowienia każdy certyfikat z pasującym celem wdrożenia bez ręcznego zatwierdzania; Wyłączone wymaga zatwierdzenia każdego odnowienia przez drugiego administratora. Administratorzy wybierają Wyłącz automatyczne odnawianie lub Włącz automatyczne odnawianie; cele i certyfikaty mogą je nadpisać w Kolejce wykonania i w szczegółach certyfikatu.

DANE I PARAMETRY

- Minimalny klucz RSA: 2048, 3072 lub 4096 bitów.
- Okno odnowienia: 1–180 dni. Próg krytyczny: 0–179 dni, mniejszy od okna odnowienia.
- Nazwa: wymagane, 1–100 znaków.
- Polityka domyślna przed pierwszym zapisem: „Baseline TLS", RSA 2048 bitów, okno odnowienia 30 dni, próg krytyczny 7 dni.

WYNIK OPERACJI

Nowa wersja polityki i wpis audytu. Oceny przeliczane przy odczycie; zatwierdzenia planów i zleceń są chronione kontrolą wersji.

UPRAWNIENIA

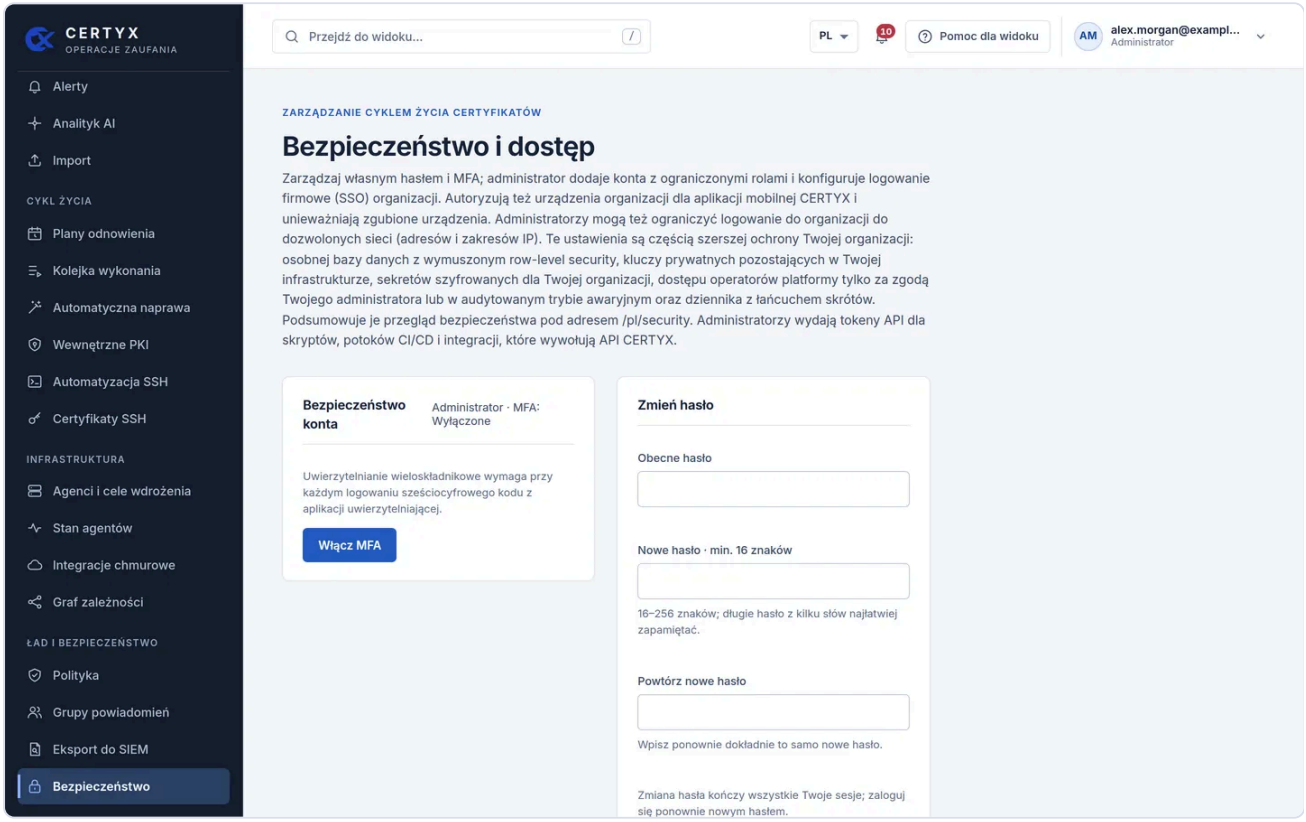
Odczyt: wszystkie role. Zapis (polityka i automatyczne odnawianie): administrator.

OGRANICZENIA

Obecnie jest to bazowa polityka ważności i kluczy, a nie pełny silnik reguł organizacji. Stałe reguły bazowe nie są edytowalne: klucze ECDSA poniżej 256 bitów, inne algorytmy niż RSA i ECDSA oraz podpisy SHA-1 lub MD5 są zawsze krytyczne. Jeśli w międzyczasie ktoś zapisał inną wersję, zapis jest odrzucany z prośbą o ponowne wczytanie. Zmiana nie modyfikuje wydanych certyfikatów.

11 Bezpieczeństwo i dostęp

Zarządzaj własnym hasłem i MFA; administrator dodaje konta z ograniczonymi rolami i konfiguruje logowanie firmowe (SSO) organizacji. Autoryzują też urządzenia organizacji dla aplikacji mobilnej CERTYX i unieważniają zgubione urządzenia. Administratorzy mogą też ograniczyć logowanie do organizacji do dozwolonych sieci (adresów i zakresów IP). Te ustawienia są częścią szerszej ochrony Twojej organizacji: osobnej bazy danych z wymuszonym row-level security, kluczy prywatnych pozostających w Twojej infrastrukturze, sekretów szyfrowanych dla Twojej organizacji, dostępu operatorów platformy tylko za zgodą Twojego administratora lub w audytowanym trybie awaryjnym oraz dziennika z łańcuchem skrótów. Podsumowuje je przegląd bezpieczeństwa pod adresem /pl/security. Administratorzy wydają tokeny API dla skryptów, potoków CI/CD i integracji, które wywołują API CERTYX.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Menu konta: kliknij swój awatar i nazwę w prawym górnym rogu. Profil pokazuje login, adres e-mail, rolę, organizację, sposób logowania i stan MFA; pozwala zmienić hasło (nowe hasło wpisujesz dwa razy) oraz własny adres e-mail, który jest też nazwą logowania – zmianę potwierdzasz obecnym hasłem i, przy włączonym MFA, kodem MFA lub zapasowym. Obie zmiany kończą wszystkie Twoje sesje. Wyloguj kończy bieżącą sesję.

2. Włącz MFA, a następnie zeskanuj kod QR aplikacją uwierzytelniającą albo wpisz klucz ręcznie. Sprawdź nazwę wpisu: to CERTYX i host tego serwera w nawiasie, na przykład CERTYX (certyx.example.com). Starszy wpis o nazwie CLM, samo CERTYX lub z innym hostem należy do innego środowiska albo wcześniejszej konfiguracji i jego kody są tu odrzucane.
3. Potwierdź bieżącym sześciocyfrowym kodem. Dziesięć kodów zapasowych pojawi się tylko raz: skopiuj je lub pobierz i przechowuj poza urządzeniem, potem zaloguj się ponownie.
4. Po utracie aplikacji uwierzytelniającej wpisz przy logowaniu jeden kod zapasowy zamiast kodu MFA. Każdy kod działa raz; sekcja Kody zapasowe pokazuje, ile zostało. Wygeneruj nowe kody zapasowe (hasło i bieżący kod MFA) zastępuje wszystkie wcześniejsze.
5. Administrator zalogowany z MFA może użyć Resetuj MFA dla innego użytkownika organizacji po potwierdzeniu tożsamości tej osoby poza systemem. Sesje użytkownika zostają zakończone; loguje się hasłem i ponownie włącza MFA.
6. Panel Zmień hasło w tym widoku również zmienia hasło: podaj obecne hasło i dwa razy nowe, a Zmień i wyloguj kończy wszystkie Twoje sesje. Kolejne nieudane logowania blokują konto na 15 minut, a każda następna nieudana próba po zakończeniu blokady podwaja jej czas (domyślnie do 24 godzin; wartości ustawia operator). Sesja kończy się po 30 minutach albo po 15 minutach bez aktywności (domyślnie). W środowisku produkcyjnym funkcje administratora wymagają sesji zalogowanej z MFA: dopóki administrator nie włączy MFA i nie zaloguje się ponownie z kodem, widoki administracyjne odpowiadają, że MFA jest wymagane, a profil i włączanie MFA pozostają dostępne.
7. Użytkownicy i role (administrator): Utwórz użytkownika przyjmuje adres e-mail, login, hasło początkowe i rolę. Lista pokazuje adres e-mail, rolę i stan MFA każdego użytkownika; Zmień adres e-mail ustawia adres, którym użytkownik się loguje (unikalny w instalacji), i kończy sesje tego użytkownika.
8. Logowanie firmowe (administrator zalogowany z MFA): wybierz dostawcę – Microsoft Entra ID, Okta, inny OpenID Connect albo SAML 2.0. Dla OpenID Connect zarejestruj u dostawcy pokazany adres przekierowania i wpisz adres wystawcy, identyfikator klienta i sekret. Dla SAML zaimportuj u dostawcy metadane dostawcy usługi (albo wpisz identyfikator jednostki i adres odbioru asercji), a w CERTYX wpisz adres logowania SAML, identyfikator jednostki dostawcy i jego certyfikat podpisu.
9. Opcje SAML: w sekcji Klucz dostawcy usług (SAML) wygeneruj klucz; widoczny jest jego odcisk SHA-256 i okres ważności, a klucz prywatny nigdy nie opuszcza serwera. Ponownie zaimportuj metadane u dostawcy (zawierają teraz certyfikat podpisu i szyfrowania oraz usługę pojedynczego wylogowania), a następnie włącz Podpisuj żądania uwierzytelnienia i Wymagaj zaszyfrowanych asercji, jeśli dostawca to obsługuje, oraz wpisz adres pojedynczego wylogowania dostawcy. Rotacja: wybierz Przygotuj następny klucz, pozwól dostawcy ponownie zaimportować metadane, potem Aktywuj następny klucz; poprzedni klucz nadal odszyfrowuje w okresie zakładki (domyślnie 30 dni), a Odrzuć następny klucz usuwa przygotowany, nieaktywowany klucz. Wylogowanie z konsoli wylogowuje wtedy także u dostawcy, a podpisane żądanie wylogowania od dostawcy kończy sesje użytkownika w CERTYX.
10. Zmapuj grupy dostawcy na role Admin, Operator lub Auditor i zapisz. Dodaj domenę e-mail, opublikuj pokazany rekord TXT _certyx-verification i wybierz Zweryfikuj. Od tej chwili użytkownicy z tej domeny widzą na stronie logowania przycisk logowania firmowego. Nazwa użytkownika podana przez dostawcę (preferred_username, email lub upn) musi należeć do zweryfikowanej domeny albo jej subdomeny, gdy organizacja ma już zweryfikowaną domenę (wcześniej nazwy są akceptowane i trafiają do dziennika jako niezweryfikowane): nazwa z innej domeny jest odrzucana (strona logowania informuje, że dostawca tożsamości podał użytkownika z niezweryfikowaną domeną e-mail; przyczyna w dzienniku sso-unverified-domain), chyba że administrator zaznaczy Akceptuj nazwy użytkowników spoza zweryfikowanych domen — wtedy logowanie trafia do dziennika z użytkownikiem oznaczonym jako niezweryfikowany. Nazwy bez domeny (login) są akceptowane.

11. Opcjonalnie wygeneruj token SCIM i wpisz go z adresem SCIM w ustawieniach provisioningu dostawcy: wtedy logować się mogą tylko użytkownicy założeni i aktywni w katalogu, a wyłączenie użytkownika kończy jego sesje. Dostawca może też przekazywać grupy (SCIM Groups); Grupy z provisioningu pokazuje je z liczbą członków i przypisaną rolą. Grupę mapuje się jej nazwą lub identyfikatorem zewnętrznym, tak jak grupę z tokenu. Opcja Tylko logowanie firmowe blokuje hasła lokalne organizacji. Zmiana grupy SCIM, która podnosi rolę użytkownika, trafia do dziennika jako osobny wpis identity.scim.role-raised z grupą, przypisaną do niej rolą oraz rolą każdego użytkownika przed i po zmianie.
12. Logowanie firmowe (Microsoft Entra ID, Okta, inny OpenID Connect, SAML 2.0) konfiguruje administrator w panelu Logowanie firmowe (SSO) tego widoku. Użytkownicy wybierają potem na stronie logowania „Zaloguj się kontem firmowym"; logowanie startuje, gdy ich e-mail należy do zweryfikowanej domeny.
13. Urządzenia mobilne (administrator): wybierz użytkownika (lub dowolnego użytkownika organizacji) i opcjonalną etykietę, a następnie Wygeneruj kod aktywacyjny. Kod i kod QR są pokazywane jeden raz i działają jeden raz w skonfigurowanym czasie (Clm:Mobile:EnrollmentCodeLifetime, domyślnie 15 minut). Gdy certyfikat serwera pochodzi z własnego (prywatnego) urzędu certyfikacji organizacji, operator konfiguruje jego odcisk SHA-256 (Clm:Mobile:TrustedServerCertificates lub Clm:Mobile:TrustedServerCertificateFile); kod QR zawiera go wtedy, panel pokazuje go pod kodem, a aplikacja ufa temu urzędowi certyfikacji wyłącznie dla tego serwera – w takim przypadku zeskanuj kod QR zamiast wpisywać kod. Na urządzeniu zainstaluj CERTYX ze sklepu organizacji (Custom App przez Apple Business Manager lub prywatna aplikacja w zarządzanym Google Play), zeskanuj kod QR lub wpisz kod, a potem zaloguj się kontem użytkownika (e-mail, hasło i, gdy konto ma MFA, jego kod) albo logowaniem firmowym; aplikacja pokazuje logowanie firmowe tylko wtedy, gdy organizacja ma je skonfigurowane ze zweryfikowaną domeną. W aplikacji użytkownik widzi przegląd, certyfikaty, alerty, zatwierdzenia, stan agentów i certyfikaty SSH; alerty potwierdza się, a zatwierdzenia udziela z tymi samymi rolami co w konsoli. Autoryzowane urządzenia pokazują etykietę nadaną przy kodzie razem z nazwą i modelem zgłoszonymi przez telefon. Oczekujące kody można anulować. Unieważnij dostęp natychmiast blokuje urządzenie: aplikacja zostaje odrzucona przy kolejnym żądaniu, jeszcze przed logowaniem, i wymaga ponownej aktywacji nowym kodem. Usuń to urządzenie w ustawieniach aplikacji unieważnia urządzenie także na serwerze (lista pokazuje wtedy Usunięte na urządzeniu); gdy telefon nie ma połączenia, aplikacja i tak usuwa swoje dane i informuje, że administrator musi unieważnić urządzenie tutaj.
14. Tokeny API (administrator zalogowany z MFA): podaj nazwę, wybierz rolę – Audytor odczytuje, Operator dodatkowo zleca odnowienia, wdrożenia i importy – oraz ważność w dniach, a potem Utwórz token. Token (cx_...) jest pokazywany tylko raz: skopiuj go do menedżera sekretów i wysyłaj jako nagłówek Authorization: Bearer <token> do API CERTYX (/api/...); ciasteczko ani token CSRF nie są potrzebne. Lista pokazuje rolę, kto i kiedy utworzył token, datę wygaśnięcia, ostatnie użycie i stan (aktywny, wygasł, odwołany); Odwołaj blokuje token natychmiast.
15. E-mail konfiguracji aplikacji uwierzytelniającej (administrator): Utwórz użytkownika pyta też o język e-maila (English, Deutsch lub Polski; domyślnie język konsoli). Nowy użytkownik otrzymuje przez przekaźnik SMTP organizacji (Grupy powiadomień → Dostarczanie) e-mail z jednorazowym linkiem do konfiguracji aplikacji uwierzytelniającej. Wiadomość zawiera link jako tekst i jako kod QR, który otwiera go w telefonie, nigdy sekret aplikacji ani hasło; hasło początkowe przekaż osobno. Bez włączonego przekaźnika albo gdy wysyłka się nie powiedzie, panel pokazuje przyczynę i link do skopiowania: przekaż go zaufanym kanałem. Lista użytkowników pokazuje „Link konfiguracyjny ważny do ...", dopóki link czeka na użycie; Wyślij e-mail konfiguracyjny tworzy nowy link (poprzedni przestaje działać) dla włączonego użytkownika z adresem e-mail i bez MFA.

16. Strona konfiguracji: osoba otwiera link, wpisuje hasło do konta, skanuje kod QR (albo wpisuje klucz; wpis nazywa się CERTYX z hostem tego serwera w nawiasie), potwierdza bieżącym sześciocyfrowym kodem i zachowuje dziesięć kodów zapasowych pokazanych jeden raz; jej sesje się kończą, a każde kolejne logowanie wymaga kodu.
17. Dozwolone sieci logowania (administrator zalogowany z MFA): wpisz adresy i zakresy, z których łączą się Twoi użytkownicy, po jednym w wierszu – pojedynczy adres (203.0.113.7, 2001:db8::7) albo zakres CIDR zaczynający się od pierwszego adresu (203.0.113.0/24, 2001:db8::/48) – i wybierz Zapisz sieci logowania. Panel pokazuje adres, z którego jesteś połączony, i czy lista go obejmuje. Jeśli nie, zapis jest odrzucany z ostrzeżeniem: upewnij się, że możesz połączyć się z dozwolonej sieci, zaznacz potwierdzenie, podaj bieżący kod z aplikacji uwierzytelniającej i zapisz ponownie. Od tej chwili każde logowanie hasłem i logowaniem firmowym, każda aktywacja urządzenia i logowanie w aplikacji mobilnej oraz każde żądanie sesji przeglądarki są sprawdzane z listą; sesja z adresu spoza listy kończy się przy kolejnym żądaniu. Aby usunąć ograniczenie, wyczyść listę i zapisz.
18. Aplikacja mobilna a sieci logowania: domyślnie (opcja Sprawdzaj także każde żądanie zalogowanych aplikacji mobilnych wyłączona) aktywacja urządzenia i każde logowanie w aplikacji muszą pochodzić z dozwolonej sieci, a już zalogowana aplikacja działa z dowolnej sieci do końca sesji (Clm:Mobile:SessionLifetime, domyślnie 30 minut) – na przykład w sieci komórkowej. Włącz opcję, aby sprawdzać też każde żądanie aplikacji; aplikacja działa wtedy tylko w dozwolonych sieciach, na przykład przez VPN.
19. Wnioski operatora platformy (Admin zalogowany z MFA): operatorzy platformy CERTYX nie mogą samodzielnie tworzyć kont, podnosić ról, ponownie włączać kont ani resetować MFA w Twojej organizacji, dopóki ma ona włączonego Admina. Taka zmiana jest tu widoczna z wnioskowaną zmianą, czasem i stanem, aż Admin ją zatwierdzi (zostanie wykonana od razu; jeśli przekaźnik platformy nie wysłał e-maila konfiguracyjnego nowego konta, zobaczysz jednorazowy link) albo odrzuci; domyślnie wygasa po 72 godzinach. Break-glass wykonany przez dwóch różnych operatorów jest pokazany z powodem; każdy Admin dostaje e-mail, a przyznany dostęp domyślnie kończy się po 24 godzinach, chyba że zmienisz konto. Działania operatora platformy pokazują ostatnie zmiany operatorów w Twojej organizacji z jej dziennika bezpieczeństwa (wysyłane też do Twoich miejsc docelowych SIEM).
20. Klucze dostępu (konta lokalne z włączonym MFA): wpisz nazwę i bieżący kod z aplikacji uwierzytelniającej, wybierz Dodaj klucz dostępu i postępuj zgodnie z oknem przeglądarki (urządzenie, telefon lub klucz bezpieczeństwa). Potem Zaloguj się kluczem dostępu na stronie logowania przyjmuje hasło i klucz zamiast kodu, a każde pole kodu i okno potwierdzenia centrum sterowania oferują Potwierdź kluczem dostępu. Zasada określa, czym może być drugi składnik: kod z aplikacji lub klucz dostępu (domyślnie), tylko klucz dostępu (kody są odrzucane; wymaga klucza) albo tylko kod z aplikacji. Kody odzyskiwania działają przy każdej zasadzie. Usuń klucz dostępu wymaga wskazania klucza i kodu; po usunięciu ostatniego obowiązuje znów kod lub klucz.
21. Twoje sesje: wszystkie sesje przeglądarki i aplikacji mobilnej Twojego konta z klientem, początkiem, ostatnią aktywnością, adresem i stanem, z oznaczoną bieżącą. Zakończ sesję wylogowuje ją przy następnym żądaniu; Zakończ wszystkie inne sesje zostawia tylko tę. Administratorzy organizacji widzą też Sesje w organizacji (wszyscy użytkownicy, przy sesji mobilnej z nazwą urządzenia) i mogą zakończyć każdą; każde zakończenie trafia do dziennika bezpieczeństwa.

DANE I PARAMETRY

- TOTP: 6 cyfr, SHA-1, okres 30 sekund; potwierdź konfigurację w ciągu 10 minut, w przeciwnym razie zacznij Włącz MFA od nowa.

- Kod zapasowy: 16 znaków w czterech grupach (litery i cyfry); wielkość liter, spacje i myślniki nie mają znaczenia.
- Hasło: 16–256 znaków. Login: do 120 znaków.
- Audytor czyta; operator zarządza inwentarzem i planuje; administrator zarządza politykami i zatwierdza.
- Entra: adres wystawcy https://login.microsoftonline.com/<ID katalogu>/v2.0 (jeden katalog). OpenID Connect: adres HTTPS bez zapytania. SAML: adres HTTPS logowania (powiązanie HTTP-Redirect), identyfikator jednostki dostawcy i certyfikat podpisu w PEM lub base64 (nieprzeterminowany, klucz RSA lub ECDSA).
- Adres pojedynczego wylogowania SAML: adres HTTPS SingleLogoutService dostawcy (HTTP-Redirect). Grupy SCIM: nazwa unikalna w organizacji (do 256 znaków), członkami mogą być tylko użytkownicy już założeni przez SCIM; filtry displayName, externalId lub id eq "wartość".
- Mapowanie grup: jedna linia „grupa = rola”, do 100 linii. Domeny: do 20 na organizację; domena zweryfikowana przez inną organizację nie może zostać przejęta.
- Kod aktywacyjny urządzenia: 16 znaków w czterech grupach; jednorazowy; powiązanie z użytkownikiem ogranicza logowanie na tym urządzeniu do wybranej osoby.
- Link konfiguracyjny: ważny przez Clm:Identity:MfaSetupLinkLifetime (domyślnie 24 godziny), działa raz, wymaga hasła do konta; nowszy link, zmiana hasła lub włączone MFA go unieważniają. Nowy link dla tego samego użytkownika najwyżej raz na Clm:Identity:MfaSetupResendInterval (domyślnie 1 minuta).
- Dozwolone sieci logowania: IPv4 w zapisie dziesiętnym z kropkami (cztery części, bez zer wiodących) lub IPv6, opcjonalnie z długością prefiksu (/0–/32, /0–/128); adres musi być pierwszym adresem zakresu (203.0.113.0/24, nie 203.0.113.5/24); wpis IPv6 mapujący IPv4 (::ffff:203.0.113.0/120) jest zapisywany jako zakres IPv4. Wpisy można też rozdzielać przecinkami lub spacjami; duplikaty są usuwane. Najwyżej Clm:Identity:MaximumSignInNetworks wpisów (domyślnie 100).
- Zasady logowania firmowego: Akceptuj nazwy użytkowników spoza zweryfikowanych domen jest domyślnie wyłączone (odrzucanie); po włączeniu takie nazwy są akceptowane i zapisywane w dzienniku jako niezweryfikowane.
- Klucz dostępu: nazwa (do 64 znaków) i bieżący kod z aplikacji; zasada: kod z aplikacji lub klucz dostępu, tylko klucz dostępu albo tylko kod z aplikacji.
- Token API: nazwa do 80 znaków; rola Audytor lub Operator; ważność od 1 dnia do Clm:Identity:ApiTokens:MaximumLifetimeDays (domyślnie 365, proponowane 90); najwyżej Clm:Identity:ApiTokens:MaximumPerOrganization aktywnych tokenów (domyślnie 25).

WYNIK OPERACJI

Włączenie MFA, zmiana hasła i reset MFA kończą sesje konta. Kody zapasowe są przechowywane wyłącznie jako skróty; użycie, wygenerowanie i reset trafiają do dziennika bezpieczeństwa. Role są egzekwowane przez API niezależnie od widoczności przycisków. Logowanie firmowe tworzy sesję z rolą z najwyżej uprawnionej zmapowanej grupy; jest odrzucane bez zmapowanej grupy, bez MFA (gdy jest wymagane), z innego katalogu Entra, przy zbyt wielu grupach w tokenie, a przy SCIM – dla użytkownika niezałożonego lub wyłączonego. Każda zmiana ustawień kończy istniejące sesje firmowe. Odpowiedź SAML jest przyjmowana tylko z podpisem przypiętego certyfikatu, dla właściwego odbiorcy i wystawcy, w czasie ważności i jako odpowiedź na żądanie rozpoczęte w tej samej przeglądarce; ponowne użycie tej samej odpowiedzi jest odrzucane. Przy grupach SCIM rola jest najwyższą rolą zmapowaną łącznie z grup w tokenie i grup SCIM; zmiana członkostwa, nazwy lub usunięcie grupy, które zmienia efektywną rolę użytkownika, kończy jego sesje przy następnym żądaniu, a każda zmiana trafia do dziennika wraz z

użytkownikami, których rola się zmieniła. Przy opcji Wymagaj zaszyfrowanych asercji niezaszyfrowana asercja jest odrzucana; zaszyfrowane asercje muszą używać AES-GCM lub AES-CBC z transportem klucza RSA-OAEP (RSA PKCS#1 v1.5 jest odrzucane). Przy opcji Podpisuj żądania uwierzytelnienia każde AuthnRequest jest podpisane RSA-SHA256. Pojedyncze wylogowanie: wylogowanie z konsoli od razu kończy sesję na każdej instancji, potem wysyła do dostawcy podpisane żądanie wylogowania; podpisane, świeże żądanie wylogowania od dostawcy (sprawdzane względem przypiętego certyfikatu, wystawcy i adresata, odrzucane przy powtórzeniu) kończy sesje tego użytkownika na każdej instancji i otrzymuje podpisaną odpowiedź. Urządzenia mobilne: każde żądanie aplikacji, łącznie z logowaniem, jest podpisane kluczem, który nie opuszcza urządzenia, i sprawdzane względem autoryzowanego urządzenia, więc unieważnienie działa od razu; kody są przechowywane tylko jako skróty, a wygenerowanie kodu, autoryzacja i unieważnienie urządzenia trafiają do dziennika bezpieczeństwa. Wysłanie, użycie i wygasły link są zapisywane w dzienniku bezpieczeństwa (mfa-setup.mail.sent, .used, .expired) bez linku i trafiają do eksportu SIEM organizacji. Użytkownicy logowania firmowego (SSO i SCIM) nie dostają e-maila konfiguracyjnego; przy Tylko logowanie firmowe nie jest on wysyłany, bo MFA wymusza dostawca tożsamości. Dozwolone sieci logowania: każda zmiana (przed i po, wykonawca) i każda odrzucona zmiana trafia do dziennika bezpieczeństwa (identity.signin-networks.changed, .refused); każde odrzucone logowanie, aktywacja urządzenia lub żądanie aplikacji spoza listy jest zdarzeniem logowania z powodem network-not-allowed, adresem źródłowym i – jeśli jest znany – użytkownikiem w dzienniku i eksporcie SIEM organizacji, a sesja zakończona w ten sposób jest wylogowaniem z tym powodem. Strona logowania i aplikacja informują użytkownika, że jego sieć nie jest dozwolona, nie ujawniając listy. Tokeny API są przechowywane wyłącznie jako skróty SHA-256; utworzenie, odwołanie i odrzucone użycia (na przykład spoza sieci logowania) trafiają do dziennika bezpieczeństwa i są eksportowane do SIEM jak inne zdarzenia tożsamości, a lista pokazuje ostatnie użycie.

UPRAWNIENIA

Własne konto: zalogowany użytkownik lokalny. Tworzenie kont i reset MFA: Admin; reset wymaga też logowania administratora z MFA i nie dotyczy własnego konta. Administratorzy platformy resetują MFA kont klientów w Administracji platformą. Konta SSO zarządzają hasłem i MFA u dostawcy tożsamości. Logowanie firmowe, domeny i token SCIM: Admin zalogowany z MFA; dotyczą wyłącznie jego organizacji. Klucze dostawcy usług (generowanie, aktywacja, odrzucenie) również wymagają Admina zalogowanego z MFA; lista grup SCIM jest dla Adminów tylko do odczytu. Zmiana własnego hasła i adresu e-mail: każdy zalogowany użytkownik lokalny dla swojego konta; nieudane potwierdzenie liczy się do blokady konta. Urządzenia mobilne: Admin organizacji; generowanie kodów i unieważnianie urządzeń wymaga własnego logowania administratora z MFA. Aplikacja jest tylko dla użytkowników klienta; operatorzy platformy nie mogą się w niej zalogować. Dozwolone sieci logowania: Admin organizacji; zapis wymaga własnego logowania administratora z MFA, a lista bez bieżącego adresu administratora dodatkowo bieżącego kodu z aplikacji uwierzytelniającej konta lokalnego (administratorzy zalogowani przez logowanie firmowe muszą pozostawić swój adres na liście). Wnioski operatora platformy: tylko Admini tej organizacji; zatwierdzenie i odrzucenie wymagają własnego logowania Admina z MFA. Klucze dostępu i lista własnych sesji: każdy zalogowany użytkownik lokalny z MFA dla własnego konta (sesje także użytkownicy logowania firmowego). Sesje w organizacji: Admin organizacji. Tokeny API: tworzenie i odwoływanie wymaga administratora zalogowanego z MFA w przeglądarce; sam token działa wyłącznie jako Audytor lub Operator w swojej organizacji i jest odrzucany przez każdy punkt administracyjny (zatwierdzenia, ustawienia, użytkownicy, urządzenia, tokeny), więc zatwierdzanie przez dwie osoby pozostaje w rękach ludzi.

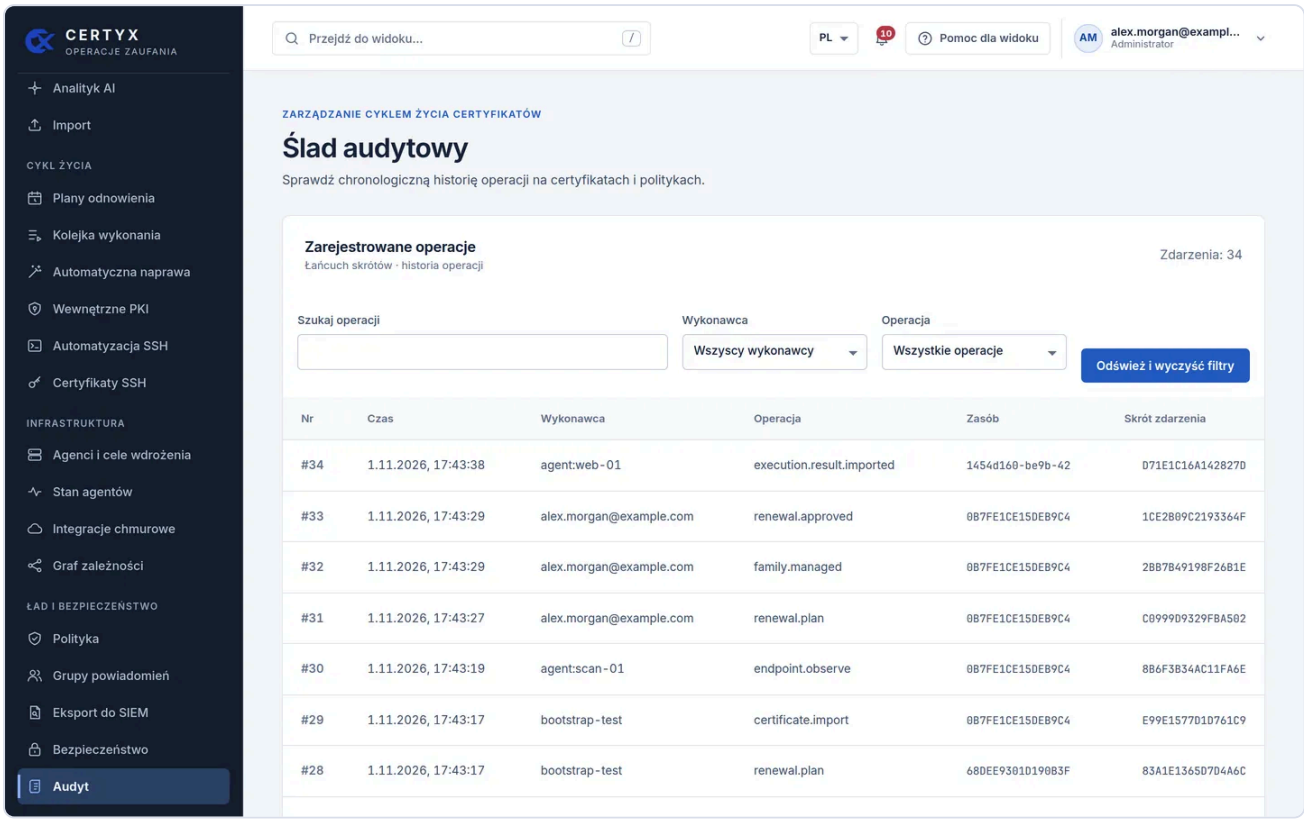
OGRANICZENIA

Brak samodzielnej rejestracji. Sesja konsoli kończy się po Clm:Identity:SessionLifetime (domyślnie 30 minut) niezależnie od aktywności, a sesja aplikacji mobilnej po Clm:Mobile:SessionLifetime (domyślnie 30 minut); potem trzeba zalogować się ponownie. Sesje kończą się też przez wylogowanie, zmianę hasła, adresu e-mail lub MFA, reset MFA albo unieważnienie urządzenia mobilnego. Listy sesji wymagają bazy platformy; bez niej informują, że sesje nie są rejestrowane. Klucze dostępu wymagają skonfigurowanej strony ufającej instalacji (Clm:Identity:Passkeys) i przeglądarki z WebAuthn pod adresem https konsoli; klucz działa tylko dla adresu, pod którym go zarejestrowano. Sesje mobilne rozpoczęte przed tą wersją nie są wyświetlane. Administrator, który utracił aplikację uwierzytelniającą i wszystkie kody zapasowe, potrzebuje innego administratora organizacji; administratora platformy w takiej sytuacji odzyskują offline dwie osoby narzędziem tools/Clm.OperatorBootstrap reset-mfa przy zatrzymanej usłudze. Konta utworzone przed wprowadzeniem kodów zapasowych otrzymują je przez Wygeneruj nowe kody zapasowe. Przy bazie platformy konta, stan MFA i klucze ochrony danych są wspólne dla wszystkich instancji aplikacji; bez niej pozostają w lokalnym katalogu danych jednej instancji. Nigdy nie udostępniaj sekretu TOTP, kodów zapasowych ani hasła. Poświadczenia i klucze prywatne klientów pozostają pod ich kontrolą. Agenci odczytują sekrety klienta z chronionych plików, HashiCorp Vault KV, Azure Key Vault, AWS Secrets Manager i Google Secret Manager; inne sejfy nie są obsługiwane, a agenci nie wysyłają poczty z hosta klienta. W Windows chronione pliki są akceptowane tylko wtedy, gdy należą do LocalSystem, grupy Administratorzy lub tożsamości agenta i tylko te podmioty mają do nich dostęp. Uprawnienia tokenu Vault na Unix są sprawdzane przy każdym użyciu. Logowanie firmowe: organizacja operatorów platformy zawsze zachowuje lokalne logowanie awaryjne i nie może włączyć trybu Tylko logowanie firmowe. SAML: przed rotacją klucza u dostawcy wklej jego nowy certyfikat podpisu. Podpisywanie żądań, wymagane szyfrowanie i pojedyncze wylogowanie wymagają klucza dostawcy usług, a wylogowanie także adresu wylogowania dostawcy; przygotowany następny klucz musi zostać zaimportowany u dostawcy przed aktywacją, inaczej odrzuci on podpisane żądania. Jeśli dostawca nie potwierdzi wylogowania z konsoli, sesja CERTYX i tak jest zakończona, a strona logowania o tym informuje. Zagnieżdżone grupy SCIM nie są obsługiwane (członkami są tylko użytkownicy), a operacje zbiorcze SCIM (bulk) nie są dostępne. SAML wymaga HTTPS, ponieważ ciasteczko żądania jest oznaczone Secure. Brak grup w odpowiedzi Entra (przekroczenie limitu grup) kończy się odmową – ogranicz grupy do przypisanych do aplikacji. Urządzenia mobilne wymagają bazy platformy; bez niej panel o tym informuje. Powiadomienia push są wysyłane tylko, gdy operator usługi skonfigurował Firebase Cloud Messaging; nigdy nie zawierają nazw certyfikatów. Dozwolone sieci logowania wymagają bazy danych platformy; bez niej panel o tym informuje, a logowanie nie jest ograniczone. Adres klienta to adres połączenia albo – z Clm:Ingress:TrustedProxies – adres przekazany przez zaufane proxy (X-Forwarded-For od każdego innego nadawcy jest ignorowany); użytkownicy za wspólnym NAT lub proxy mają jego adres publiczny. Agenci (wzajemne TLS) i tokeny SCIM nie są logowaniem użytkownika i nie są sprawdzane. Jeśli wszyscy administratorzy stracili dostęp, operator platformy może usunąć ograniczenie (karta klienta → Dostęp); to usunięcie widać w dzienniku bezpieczeństwa i eksporcie SIEM tej organizacji. Wniosek można rozpatrzyć tylko, gdy jest otwarty, i w pokazanej wersji; zatwierdzona zmiana konta nie zostanie wykonana, jeśli konto zmieniło się po złożeniu wniosku, nazwa jest zajęta lub osiągnięto limit aktywnych kont z umowy (wniosek pokazuje wtedy Niewykonane). Działania operatora platformy pokazują 50 najnowszych wpisów bez szczegółów przed/po; odczyty operatorów nie są wymieniane. Opcja MFA wymuszane przez politykę dostawcy sprawia, że każde logowanie firmowe liczy się jako MFA, choć dostawca tego nie zgłasza: panel pokazuje ostrzeżenie, dopóki opcja jest zaznaczona, a każdy zapis z nią trafia do dziennika jako identity.sso.mfa-delegated. Utworzenie konta lub przypisanie adresu e-mail, który jest już używany, w tej lub innej organizacji, jest odrzucane tym samym komunikatem; tylko dziennik platformy zapisuje rzeczywistą przyczynę (account.create-refused, account.email-refused), więc administratorzy nie dowiedzą się, czy adres istnieje gdzie indziej. Tokeny API wymagają bazy danych platformy; bez niej panel informuje, że są niedostępne. Każdy token wygasa i nie

można go przedłużyć – utwórz nowy i odwołaj stary. Token podlega liście sieci logowania organizacji (poza nią 403 network-not-allowed). Żądania z nieznanym, błędnym, odwołanym lub wygasłym tokenem dostają 401 invalid-token i nigdy nie korzystają z sesji przeglądarki.

12 Ślad audytowy

Sprawdź chronologiczną historię operacji na certyfikatach i politykach.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Otwórz widok po zalogowaniu.
2. Wyszukuj operacje, filtruj według wykonawcy lub operacji i przeglądaj listę stronami po 50 operacji, od najnowszych; stronicowanie pozostaje na tej samej migawce, dopóki Odśwież i wyczyść filtry nie wczyta najnowszych operacji. Sprawdź sekwencję, datę, wykonawcę, rodzaj operacji i identyfikator zasobu.
3. Porównaj zdarzenia z planami, polityką lub obserwacją endpointu.
4. Eksportuj CSV lub Eksportuj JSON pobiera wszystkie operacje zgodne z bieżącym wyszukiwaniem i filtrami, od najnowszych, z powiązaniami łańcucha skrótów; każdy eksport jest zapisywany w dzienniku bezpieczeństwa. Eksport i przechowywanie pokazuje obowiązujące zasady przechowywania, liczbę i zakres czasu zapisanych operacji oraz limit eksportu.
5. Operator może dodatkowo eksportować podpisane kotwice audytu inwentarza poleceniem tools/Clm.Backup anchor --tenant <identyfikator-organizacji>, z chronionym kluczem podpisującym i jawną tożsamością bazy bez obejścia RLS. verify-anchors --tenant sprawdza podpis związany z organizacją, segment i łańcuch; --db-env dodatkowo porównuje żywą bazę. Klucz i niezmienne kopie należy utrzymywać niezależnie od hosta bazy.

DANE I PARAMETRY

- Zdarzenia tworzy serwer podczas zmian; widok nie pozwala ich edytować.

- Sekwencja i hash wiążą kolejne zdarzenia. Daty są wyświetlane w lokalnej strefie przeglądarki.
- Serwer weryfikuje cały łańcuch skrótów przy każdej zmianie najnowszego zdarzenia i co najmniej co 5 minut; przy niespójnym łańcuchu odmawia odczytu inwentarza.

WYNIK OPERACJI

Historia umożliwia odtworzenie, kto zmienił dane i kiedy. Weryfikacja łańcucha wykrywa niespójność zapisanej historii.

UPRAWNIENIA

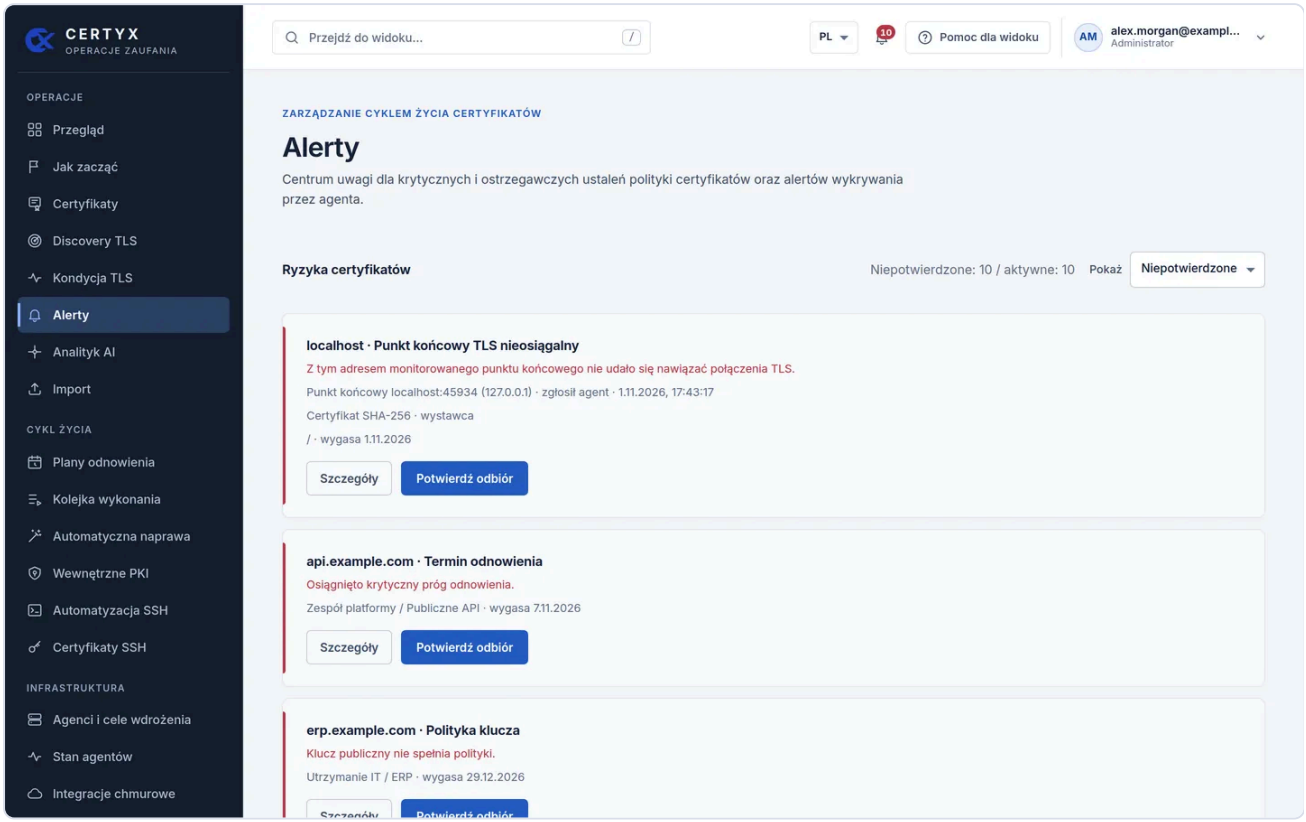
Wszystkie zalogowane role przeglądają i eksportują.

OGRANICZENIA

Sam łańcuch skrótów w bazie nie zapewnia niezaprzeczalności wobec administratora bazy. Zmiana wcześniejszego zdarzenia wykonana bezpośrednio w bazie jest wykrywana przy następnej pełnej weryfikacji (najpóźniej po 5 minutach). Niezależne podpisane kotwice wykrywają zmianę zakotwiczonej historii; ochrona przed usunięciem wymaga zewnętrznej niezmiennej retencji i niezależnej weryfikacji. Przechowywanie: operacje są przechowywane przez cały okres istnienia organizacji bez automatycznego usuwania, a rola aplikacji może je tylko dodawać i odczytywać. Konfigurowalny okres retencji nie jest oferowany, ponieważ usunięcie wpisów przerwałoby łańcuch skrótów. Jeden eksport obejmuje najwyżej Clm:AuditExport:MaxRows operacji (domyślnie 100 000); przy większych widokach zawęź filtry.

13 Alerty

Centrum uwagi dla krytycznych i ostrzegawczych ustaleń polityki certyfikatów oraz alertów wykrywania przez agenta.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Przejrzyj alerty niepotwierdzone, uporządkowane według ważności i daty wygaśnięcia.
2. Szczegóły otwierają certyfikat w inwentarzu, gdzie fakty, ustalenia, odpowiedzialność i odnowienie pokazują dowody stojące za alertem. Każda karta pokazuje już ustalenie, jego wyjaśnienie, właściciela i usługę, datę wygaśnięcia, a po potwierdzeniu także, kto i kiedy je potwierdził.
3. Wybierz Potwierdź odbiór. Aby zobaczyć również potwierdzone ryzyka, ustaw Wszystkie aktywne ryzyka.
4. Kolejka i historia powiadomień poniżej pokazuje ostatnie 100 powiadomień organizacji (alerty dla kanałów, wiadomości do grup i powiadomienia push) z kanałem, stanem, liczbą prób, czasem doręczenia i przyczyną ostatniego błędu; Podgląd wiadomości otwiera wiadomość do grupy z kolejki w postaci, w jakiej zostanie wysłana.
5. Każdy wpis podaje typ zdarzenia (alert certyfikatu, alert eskalowany, zdarzenia zadań i odnowień). Administrator wybiera Wyślij ponownie przy dostarczonym, porzuconym lub anulowanym wpisie kanału, aby dostarczyć go jeszcze raz (licznik prób od zera, zapis w dzienniku bezpieczeństwa); wpisów wiadomości grupowych i powiadomień mobilnych nie wysyła się ponownie, a ponowne wysłanie zdarzenia PagerDuty ponownie otwiera incydent.
6. Gdy analityk AI jest włączony dla organizacji, Wyjaśnij otwiera go z pytaniem o alert.

DANE I PARAMETRY

- Alert powstaje z bieżącej oceny polityki: ważność, próg odnowienia, klucz lub podpis.
- Identyfikator obejmuje certyfikat, wersję polityki, kod i poziom ryzyka. Zmiana poziomu lub polityki wymaga nowego potwierdzenia.
- Wykrywanie przez agenta wywołuje alerty po przebiegu bazowym profilu (pierwszym pełnym przebiegu): Znaleziono nieznany certyfikat (ostrzeżenie; krytyczny, gdy certyfikat jest samopodpisany lub pochodzi od wystawcy nigdy niewidzianego w organizacji), Certyfikat na punkcie końcowym został zastąpiony (ostrzeżenie; nie powstaje, gdy zadanie wykonania CERTYX wdrożyło dokładnie ten certyfikat na ten punkt końcowy lub w miejsce poprzedniego w oknie Clm:Discovery:ReplacementSuppressionWindow, domyślnie 7 dni) oraz Nowy punkt końcowy TLS (informacja). Karty pokazują punkt końcowy, zgłaszającego agenta oraz odcisk SHA-256 i wystawcę nowego i poprzedniego certyfikatu. Powstają raz na punkt końcowy i certyfikat, są zapisywane w dzienniku i wysyłane skonfigurowanymi kanałami powiadomień jak inne otwarte alerty.

WYNIK OPERACJI

Potwierdzenie jest trwałe, idempotentne i audytowane razem z tożsamością i czasem. Nie zmienia certyfikatu ani poziomu ryzyka.

UPRAWNIENIA

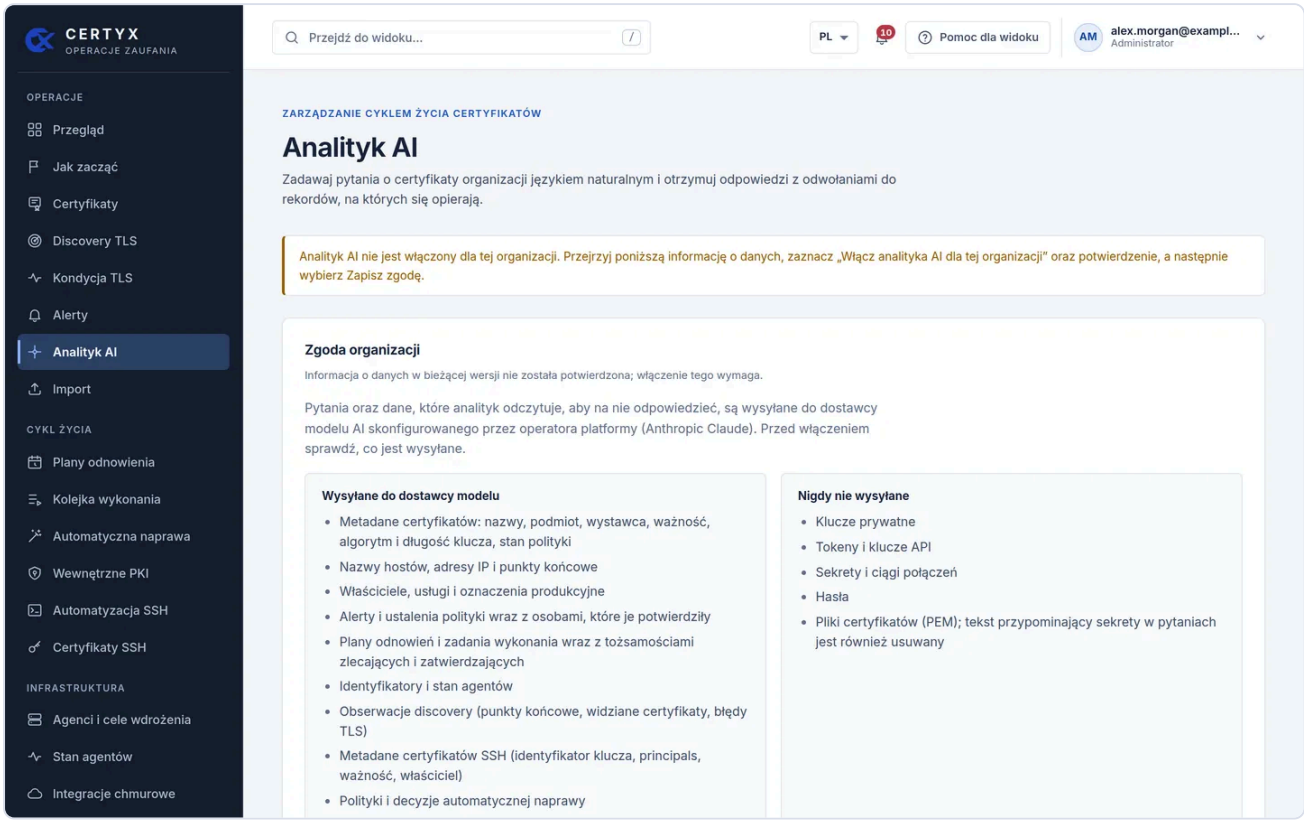
Odczyt: wszystkie zalogowane role. Potwierdzanie: operator lub administrator.

OGRANICZENIA

Potwierdzenie nie usuwa ryzyka. Otwarte alerty trafiają do kolejki każdego włączonego kanału organizacji (webhook, Microsoft Teams, Slack, PagerDuty) i są doręczane co najmniej raz; kanały eskalacji otrzymują tylko krytyczne alerty nadal niepotwierdzone po ich opóźnieniu. Kanały i przekaźnik SMTP konfiguruje się w Grupach powiadomień → Wysyłka, gdzie każdy pokazuje oczekujące i nieudane wiadomości. Gdy operator usługi skonfigurował powiadomienia push, otwarte krytyczne alerty i alerty wygaśnięcia trafiają też na autoryzowane urządzenia mobilne organizacji z włączonymi powiadomieniami, jako ogólna wiadomość bez nazw certyfikatów. Lista pokazuje ostatnie 100 powiadomień. Alert wykrywania pozostaje na liście po potwierdzeniu; aby zareagować, przypisz właściciela certyfikatu lub zbadaj punkt końcowy. Zastąpienie innym narzędziem albo wdrożenie CERTYX, którego punkt weryfikacji różni się od obserwowanego adresu, jest zgłaszane.

14 Analityk AI

Zadawaj pytania o certyfikaty organizacji językiem naturalnym i otrzymuj odpowiedzi z odwołaniami do rekordów, na których się opierają.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Warunki: subskrypcja obejmuje AI_ANALYST; operator platformy podłącza analityka w widoku centrum sterowania Analityk AI – dostawca (klucz API Anthropic, model, Testuj połączenie, „Udostępnij analityka AI organizacjom"), a w samodzielnej instalacji bez bazy danych platformy osoba ją utrzymująca ustawia Clm:Analyst w konfiguracji; Administrator organizacji włącza go tutaj po przeczytaniu i potwierdzeniu informacji o danych. „Zapisz zgodę" zapisuje potwierdzenie informacji o danych także wtedy, gdy analityk pozostaje wyłączony; karta pokazuje wtedy zaznaczone pole (nie można go odznaczyć) z administratorem i czasem potwierdzenia, a obok przycisku pojawia się potwierdzenie zapisu. Potwierdzenie obowiązuje do zmiany informacji o danych; nową wersję trzeba potwierdzić ponownie.
2. Dopóki wszystko nie jest gotowe, widok wskazuje brakujący krok i kto musi działać: brak w subskrypcji (dział sprzedaży lub operator platformy), nieudostępniony przez operatora, brak klucza API lub klucz nieczytelny (operator platformy w widoku Analityk AI – dostawca albo konfiguracja instalacji), niewłączony dla organizacji (Administrator, w karcie zgody organizacji w tym widoku). Administratorzy widzą kartę zgody i informację o danych jeszcze przed skonfigurowaniem dostawcy.
3. Wpisz pytanie, na przykład które certyfikaty produkcyjne wygasają w ciągu 30 dni i kto za nie odpowiada, i wybierz Zapytaj. Analityk odczytuje dane wyłącznie przez narzędzia tylko do odczytu tej organizacji: wyszukiwanie i szczegóły certyfikatów (ustalenia oraz, jeśli objęte licencją, ryzyko

biznesowe), alerty, plany odnowień, zadania wykonania, stan agentów, obserwacje discovery, inwentarz SSH oraz polityki i decyzje automatycznej naprawy.

4. Odpowiedź zawiera numerowane odwołania; każde prowadzi do cytowanego rekordu (szczegóły certyfikatu, Alerty, Plany odnowień, Wykonanie, Stan agentów, Discovery, SSH lub Automatyczna naprawa). Cytować można tylko rekordy, które narzędzie faktycznie zwróciło. Pod odpowiedzią widać, jakie dane odczytano, oraz liczbę tokenów.
5. Wyjaśnij w szczegółach certyfikatu, przy alercie i przy decyzji naprawy otwiera ten widok z przygotowanym pytaniem o ten rekord; sprawdź je i wybierz Zapytaj.
6. Rozmowy są przechowywane przez okres ustalony w organizacji i widoczne tylko dla Ciebie: otwórz rozmowę, aby ją kontynuować, usuń ją lub rozpocznij Nową rozmowę. Administratorzy widzą dziennik zapytań organizacji.

DANE I PARAMETRY

- Pytanie o długości do Clm:Analyst:MaxQuestionLength znaków (domyślnie 4000). Pytanie uzupełniające wysyła najwyżej Clm:Analyst:MaxHistoryTurns wcześniejszych wypowiedzi (domyślnie 10).
- Wysyłane do dostawcy modelu (Anthropic Claude, wybrany przez operatora): metadane certyfikatów, nazwy hostów i punkty końcowe, właściciele i usługi, alerty i ustalenia, plany i zadania wraz z tożsamościami zlecających i zatwierdzających, stan agentów, obserwacje discovery, metadane certyfikatów SSH, decyzje naprawy i treść pytania.
- Nigdy nie wysyłane: klucze prywatne, tokeny, sekrety, hasła i pliki certyfikatów (PEM). Narzędzia przekazują rekordy bez nich, a redakcja usuwa tekst przypominający sekrety (bloki PEM, klucze API i dostępu, tokeny Bearer, JWT, przypisania password=, długie dane zakodowane) z wyników narzędzi, pytań i wcześniejszych wypowiedzi.

WYNIK OPERACJI

Odpowiedź z numerowanymi odwołaniami do rekordów tej organizacji. Każde pytanie trafia do dziennika zapytań (adres e-mail użytkownika, czas, użyte narzędzia, liczba tokenów, wynik) i do dziennika bezpieczeństwa, oba bez treści pytania i odpowiedzi. Zmiany zgody są dziennikowane wraz z potwierdzającym administratorem, którego adres e-mail pokazuje karta zgody organizacji.

UPRAWNIENIA

Stan widzi każdy zalogowany użytkownik organizacji. Gdy analityk jest włączony, pytać mogą Audytorzy, Operatorzy i Administratorzy. Włączenie, ustawienie przechowywania i odczyt dziennika zapytań: Administrator.

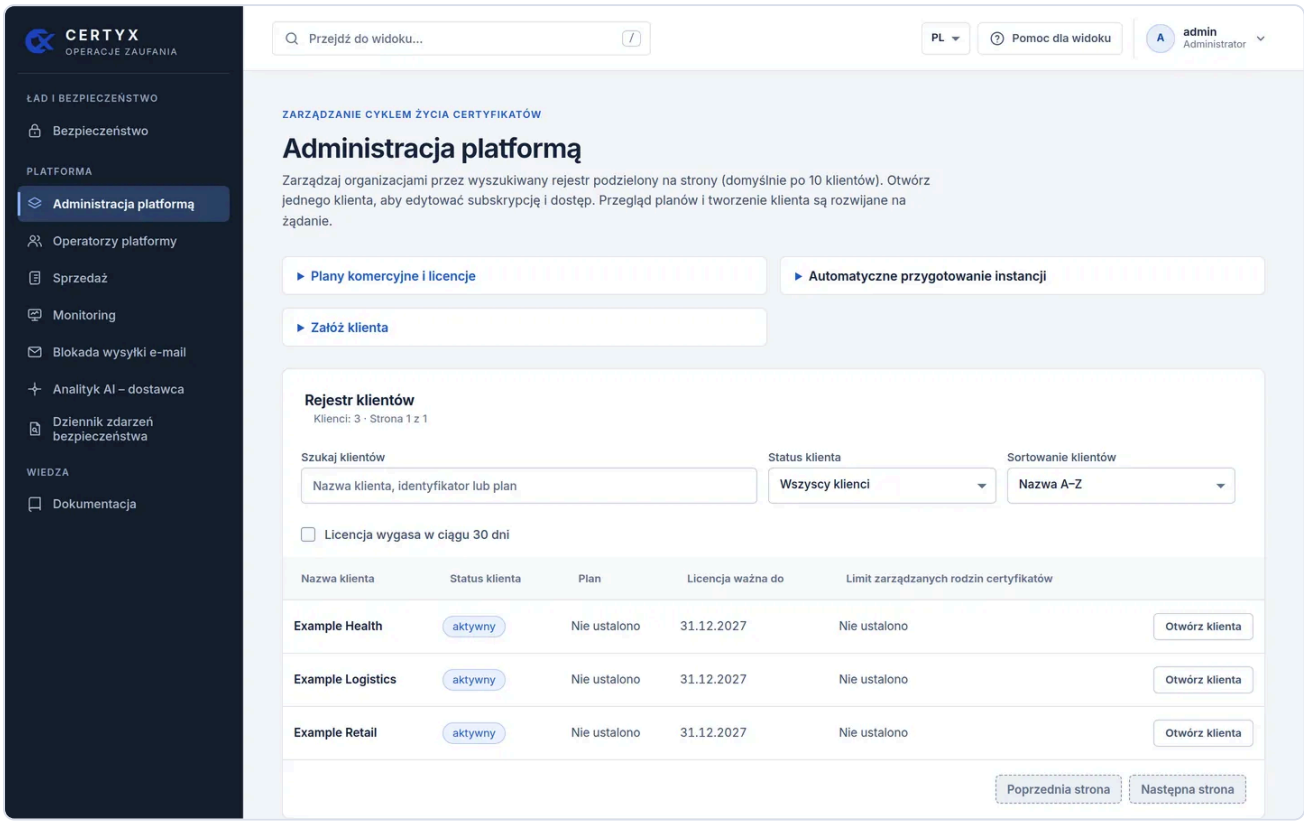
OGRANICZENIA

Odpowiedzi generuje model AI i mogą być błędne lub niepełne; przed działaniem sprawdź cytowane rekordy. Analityk działa tylko do odczytu i niczego nie zmienia. Limity ustawione przez operatora (domyślnie: 30 pytań na użytkownika na godzinę, 300 na organizację i 2 000 000 tokenów w ciągu 24 godzin) odrzucają kolejne pytania z komunikatem. Jedna odpowiedź wykorzystuje najwyżej Clm:Analyst:MaxToolRounds wywołań modelu (domyślnie 6) i Clm:Analyst:Timeout (domyślnie 2 minuty); w przeciwnym razie jest oznaczona jako niepełna lub pojawia się przekroczenie czasu. Każde narzędzie zwraca najwyżej 25 rekordów i 40 000 znaków. Odpowiedzi pojawiają się w całości (bez strumieniowania). Błąd lub odmowa dostawcy jest pokazywana jako komunikat i dziennikowana. Przy przechowywaniu 0 nic nie jest zapisywane; wygasłe rozmowy usuwa cogodzinny przebieg. Lista rozmów pokazuje Twoje najnowsze rozmowy w liczbie Clm:Analyst:ConversationListLimit (domyślnie 50); dziennik zapytań

pokazuje 50 najnowszych zapytań organizacji i przechowuje wpisy przez Clm:Analyst:RequestJournalDays (domyślnie 400 dni). Każda podana tu liczba jest konfigurowalną wartością domyślną: limity zapytań ustawia operator platformy w widoku Analityk AI – dostawca, pozostałe wartości konfiguracja instalacji (Clm:Analyst).

15 Administracja platformą

Zarządzaj organizacjami przez wyszukiwany rejestr podzielony na strony (domyślnie po 10 klientów). Otwórz jednego klienta, aby edytować subskrypcję i dostęp. Przegląd planów i tworzenie klienta są rozwijane na żądanie.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Szukaj po nazwie, identyfikatorze lub planie; filtruj status i licencje wygasające w skonfigurowanym oknie (domyślnie 30 dni; liczba dni jest pokazana przy filtrze), sortuj i zmieniaj strony. Otwórz klienta pokazuje tylko wybraną organizację; zamknij szczegóły, aby wrócić do rejestru.
2. Załóż klienta i określ termin licencji.
3. Utwórz osobną instancję: przy włączonym automatycznym tworzeniu (domyślnie we wdrożeniu kontenerowym) rusza ono samo po utworzeniu klienta, a klient staje się aktywny, gdy karta Instancja i wdrożenie pokaże zakończone zadanie; gdy automatyczny start jest wyłączony, wybierz Utwórz instancję automatycznie. Bez automatycznego tworzenia przygotuj instancję procedurą serwerową i wybierz Zweryfikuj i aktywuj instancję.
4. Załóż konta z rolami klienta: w zakładce Dostęp formularz Załóż konto klienta przyjmuje adres e-mail logowania, hasło początkowe i rolę (Administrator, Operator lub Audytor). Każde konto na liście ma własną rolę, pole Konto aktywne i przycisk Zapisz uprawnienia.
5. Zarządzaj terminami licencji i zawieszaj dostęp: w Przegląd → Dane klienta zmień nazwę, koniec licencji lub Stan klienta (aktywny, Zawieszony lub Archiwalny) i wybierz Zapisz klienta. Edytor szczegółów nie jest pokazywany, gdy klient jest w stanie tworzenia (aktywacja odbywa się w zakładce instancji); klient zarchiwizowany ma tylko zakładkę Przegląd.

6. Ustaw plan, status, daty subskrypcji, limit zarządzanych rodzin, margines przekroczenia, okres rozliczeniowy, kwotę umowy, walutę (PLN, EUR lub USD) i uprawnienia modułów, a następnie wybierz Zapisz subskrypcję. Wybór planu ustawia jego zestaw funkcji i zachowuje moduły dodatkowe; Discovery jest zawsze objęte. Discovery oraz operacje nie zwiększają opłat.
7. Umowa i rozliczenia na karcie klienta pokazuje podpisaną umowę ze Sprzedaży, zaległe i następne płatności oraz zawieszenie za brak płatności; Otwórz w Sprzedaży otwiera umowę. Gdy umowa obowiązuje, plan, limit certyfikatów, ważność, okres rozliczeniowy, kwota, waluta i koniec licencji wynikają z niej: inną wartość zapisuje się tylko z powodem wyjątku, zapisanym w dzienniku bezpieczeństwa.
8. W zakładce Dostęp przycisk Resetuj MFA (widoczny przy kontach z włączonym MFA) usuwa MFA z konta klienta, które utraciło aplikację uwierzytelniającą i kody zapasowe, po potwierdzeniu tożsamości poza systemem. Sesje konta zostają zakończone, a działanie trafia do audytu platformy i dziennika bezpieczeństwa.
9. Automatyczne tworzenie instancji: panel Automatyczne przygotowanie instancji nad rejestrem pokazuje, czy jest włączone i czy startuje samo dla nowych klientów, skonfigurowane polecenia infrastruktury i migracji, czy są to stałe pliki wykonywalne, których inni nie mogą zmienić, katalog stanu i limity ponowień. Klient utworzony w panelu lub przez podpisaną umowę, a także klient, który czekał, gdy tworzenie było wyłączone, otrzymuje instancję automatycznie: platforma tworzy własną bazę i role klienta, wykonuje migrację z zapisem tożsamości klienta, zapisuje sekret połączenia dostępny tylko dla właściciela, weryfikuje instancję i aktywuje klienta. Status, krok i ewentualny powód zatrzymania odświeżają się na karcie Instancja i wdrożenie; każdy powód zatrzymania podaje przyczynę i sposób naprawy, po naprawie wybierz Ponów tworzenie instancji. Zweryfikuj i aktywuj instancję podaje dokładnie, która kontrola nie przeszła i co zrobić; dla instancji nigdy nieprzygotowanej uruchamia zamiast tego automatyczne tworzenie. We wdrożeniu kontenerowym zadania wykonuje osobne zadanie przygotowania (kontener provisioner), jedyna część wdrożenia z poświadczeniem do tworzenia baz danych, więc sama aplikacja nie może tworzyć baz ani ról; panel pokazuje wtedy w polu Wykonywane przez ostatni raport tego zadania i ostrzega, gdy raportu brak lub jest starszy niż pięć minut (sprawdź, czy działa kontener provisioner).
10. Karta klienta ma zakładki Przegląd, Subskrypcja i uprawnienia, Dostęp, Źródła chmurowe oraz Instancja i wdrożenie (ta ostatnia tylko w stanie tworzenia; klient zarchiwizowany ma tylko Przegląd); wybrana zakładka pozostaje otwarta, gdy karta przeładowuje się po zmianie, ale nie po przeładowaniu strony ani ponownym otwarciu widoku. Przegląd pokazuje dane klienta, Umowa i rozliczenia, wykorzystanie subskrypcji klienta aktywnego lub zawieszonego oraz edytor szczegółów klienta. W subskrypcji każda funkcja ma jeden wybór: nieobjęta, w planie albo moduł dodatkowy. Zamknij szczegóły klienta wyraźnym przyciskiem w nagłówku karty.
11. Źródła chmurowe: przypisz skrzynkę kolektora klienta, podając identyfikator źródła, dostawcę (AWS, Azure, Google Cloud lub DigiCert CertCentral), zakres dokładnie taki, jak raportuje kolektor (Azure: nazwa magazynu; AWS: KONTO:REGION, np. 123456789012:eu-central-1; Google Cloud: PROJEKT:LOKALIZACJA, np. my-project:global; DigiCert: account:<identyfikator miejsca docelowego>), skrzynkę (bezwzględną ścieżkę pliku dostępnego tylko dla właściciela na hoście platformy albo identyfikator skrzynki, gdy wdrożenie ma katalog skrzynek) i maksymalny wiek migawki (5–1440 minut). Następny przebieg synchronizacji importuje ją do inwentarza i grafu zaufania klienta. Tabela pokazuje stan (oczekuje na pierwszą synchronizację, działa, częściowy wynik, błąd z przyczyną, wstrzymane), certyfikaty, ostatni sukces i ostatnią próbę; źródło można edytować,

wstrzymać, wznowić lub usunąć. Każda zmiana jest wersjonowana i zapisywana w dzienniku bezpieczeństwa. Organizacja widzi swoje źródła i ich stan w Integracjach chmurowych, nigdy lokalizacji skrzynki.

12. Zakładka Dostęp → Weryfikacja adresów wewnętrznych: pozwól CERTYX samodzielnie weryfikować wdrożenia organizacji na adresach lokalnych, prywatnych i link-local (z potwierdzeniem i wpisem w dzienniku bezpieczeństwa). Bez tego organizacja weryfikuje takie punkty końcowe własnym agentem weryfikującym.
13. E-mail konfiguracyjny konta klienta: Utwórz konto klienta wysyła nowemu kontu przez techniczny przekaźnik poczty platformy (Monitoring platformy → Przekaźnik e-mail alertów; nigdy przekaźnik sprzedaży), w wybranym języku, jednorazowy link do konfiguracji aplikacji uwierzytelniającej. Wiadomość zawiera link jako tekst i jako kod QR linku, nigdy sekret aplikacji ani hasło. Gdy przekaźnik nie ma hosta ani nadawcy albo wysyłka się nie powiedzie, zakładka Dostęp pokazuje przyczynę i, tylko w organizacji bez włączonego Admina, link do skopiowania; przekaż go klientowi zaufanym kanałem, oddzielnie od hasła początkowego. Wyślij e-mail konfiguracyjny w wierszu konta tworzy nowy link (poprzedni przestaje działać) i jest zapisywane w audycie platformy.
14. Sieci logowania klienta (karta klienta → Dostęp): pokazuje adresy, które administratorzy organizacji dopuszczają do logowania. Jeśli stracili dostęp (na przykład przez błędny zakres lub zmieniony adres biura), podaj kod z aplikacji uwierzytelniającej i wybierz Usuń ograniczenie: lista zostaje wyczyszczona (ustawienie aplikacji mobilnej pozostaje), zmiana trafia do audytu platformy (customer.signin-networks.cleared z wartościami przed i po) oraz pojawia się jako identity.signin-networks.cleared-by-operator we własnym dzienniku bezpieczeństwa organizacji; jako zapis platformy nie jest wysyłane do miejsc docelowych SIEM organizacji. Administratorzy organizacji ustawiają potem poprawną listę w widoku Bezpieczeństwo.
15. Zgoda klienta i break-glass: w aktywnej organizacji, która ma już włączonego Admina, Utwórz konto klienta (dowolna rola), Zapisz dostęp podnoszący rolę lub ponownie włączający konto oraz Resetuj MFA nie zmieniają konta. Tworzą wniosek o dostęp (konsola to komunikuje), widoczny w karcie Dostęp w sekcji Wnioski o dostęp z wnioskowaną zmianą, czasem i stanem; Admin klienta zatwierdza go lub odrzuca w widoku Bezpieczeństwo → Wnioski operatora platformy, a zatwierdzony wniosek jest wykonywany od razu. Wniosek wygasa po Clm:Platform:AccessRequests:RequestLifetime (domyślnie 72 godziny). Organizacja bez włączonego Admina (świeże udostępnienie) lub nieaktywna zachowuje bezpośredni przebieg. Obniżenie roli i wyłączenie konta zawsze działają bezpośrednio.
16. Break-glass tylko w sytuacji awaryjnej (na przykład jedyny Admin organizacji utracił aplikację uwierzytelniającą): w wierszu wniosku wpisz powód (10–500 znaków, widoczny dla klienta) i swój bieżący kod uwierzytelniający, a następnie wybierz Rozpocznij break-glass. Drugi, inny operator wpisuje własny bieżący kod i wybiera Potwierdź break-glass w czasie Clm:Platform:AccessRequests:BreakGlassConfirmationWindow (domyślnie 1 godzina). Działanie zostaje wtedy wykonane; utworzone konto, podniesiona rola lub ponownie włączone konto są cofane po BreakGlassAccessDuration (domyślnie 24 godziny), chyba że Admin klienta zmienił w tym czasie konto; każdy włączony Admin klienta (a przy zmianie dostępu lub resecie MFA także samo konto) dostaje e-mail w swoim języku przez przekaźnik platformy, ponawiany co minutę (NoticeAttempts, domyślnie 30) aż do doręczenia.

DANE I PARAMETRY

- Nazwa klienta, koniec licencji, adres e-mail konta, hasło początkowe i rola klienta (Administrator, Operator lub Audytor).

- Formaty: nazwa klienta od 1 do 200 znaków; koniec licencji to data od dziś do 5 lat naprzód, zapisywana jako 23:59:59 UTC; limit subskrypcji to liczba całkowita od 1 do 10 000 000, tolerancja 0–100 %, okres rozliczeniowy 1–36 miesięcy, kwota umowy 0–1 000 000 000 z maksymalnie 2 miejscami po przecinku, okres próbny najwyżej 30 dni; e-mail konta do 120 znaków i hasło początkowe 16–256 znaków; identyfikator źródła chmurowego 1–100 liter, cyfr, - lub _, zakres do 300 znaków, skrzynka do 1024 znaków, maksymalny wiek 5–1440 minut. Podpowiedź pod każdym polem podaje jego format, a odrzucona wartość wskazuje oczekiwany format.
- Nazwy planów i statusów subskrypcji są wyświetlane w wybranym języku; identyfikatory zapisywane w API pozostają stałe.
- Powód odstępstwa od umowy (10–500 znaków), wymagany tylko, gdy wartość wynikająca z umowy różni się od podpisanej umowy.
- Break-glass: powód 10–500 znaków; 6-cyfrowy kod Twojej własnej aplikacji uwierzytelniającej (step-up, kod działa raz; powtarzane błędne kody blokują Twoje konto).
- Zarezerwowane nazwy organizacji: *, platform, platform-control, unattributed i default (bez względu na wielkość liter) są odrzucane przy tworzeniu klienta lub zmianie nazwy, bo dziennik i eksport SIEM używają ich dla platformy. Klient, który już ma taką nazwę, pokazuje ostrzeżenie na swojej karcie, dopóki nazwa nie zostanie zmieniona.

WYNIK OPERACJI

Wersjonowany rejestr klientów i audyt platformy. Każde zmieniające działanie na kliencie (konta, wnioski, break-glass, subskrypcja i stan, aktywacja, udostępnianie, źródła chmurowe, weryfikacja prywatna) jest też zapisywane w dzienniku bezpieczeństwa tego klienta z aktorem platform:<ID konta operatora>, pokazywane klientowi w widoku Bezpieczeństwo → Działania operatora platformy i eksportowane wyłącznie przez własne zakresy SIEM platformy, nigdy do miejsc docelowych klienta; działania na kontach zapisują w audycie platformy ID konta docelowego.

UPRAWNIENIA

Jawnie wskazany administrator platformy z sesją uwierzytelnioną przez MFA. Rola administratora klienta nie wystarcza. Break-glass wymaga dwóch różnych operatorów, z których każdy potwierdza bieżącym kodem uwierzytelniającym; operatorzy logujący się przez logowanie firmowe nie mogą potwierdzać (brak lokalnej aplikacji uwierzytelniającej). Zatwierdzanie wniosku jest zarezerwowane dla Adminów samego klienta. Step-up: każda zmiana w tym widoku (poza testami, sprawdzeniami połączenia i potwierdzeniem incydentu) prosi o bieżący 6-cyfrowy kod Twojej aplikacji uwierzytelniającej; potwierdzony kod obejmuje także kolejne zmiany w centrum sterowania przez Clm:Identity:OperatorStepUpWindow (domyślnie 5 minut). Błędny lub już użyty kod jest odrzucany, wlicza się do blokady konta i jest zapisywany w dzienniku; Anuluj porzuca zmianę. Operatorzy logujący się przez logowanie firmowe nie mają lokalnej aplikacji uwierzytelniającej i nie mogą wprowadzać tych zmian. Role operatorów: każda rola odczytuje klientów; zakładanie klientów, edytor danych, subskrypcje i przygotowanie instancji wymagają roli sprzedaży lub administratora, konta klientów, wnioski o dostęp, break-glass, sieci logowania, źródła chmurowe i weryfikacja prywatna — administratora bezpieczeństwa lub administratora, umowa i rozliczenia — sprzedaży lub administratora; karta pokazuje tylko to, z czego rola może korzystać.

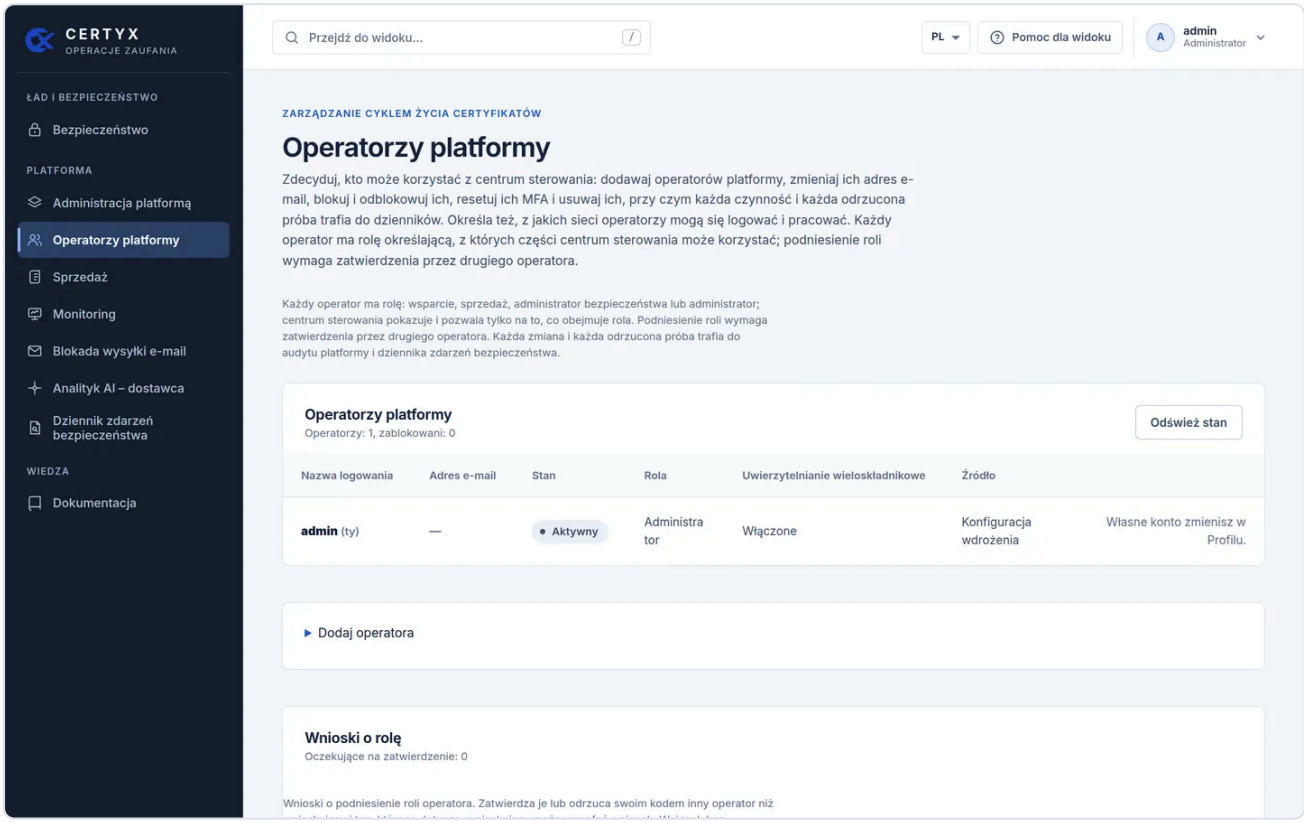
OGRANICZENIA

- Administracja platformą wymaga bazy platformy (Clm:Database:Platform). Założenie klienta wymaga ponadto bezwzględnego katalogu sekretów klientów (Clm:Storage:CustomerSecretDirectory), w którym oczekiwany jest sekret połączenia klienta; bez niego założenie jest odrzucane jako niedostępne.

- Polecenia tworzenia instancji, katalog stanu, automatyczny start i limity ponowień są ustawieniami wdrożenia (we wdrożeniu kontenerowym: ustawienia CERTYX_PROVISIONING w certyx.env) i są pokazane tylko do odczytu w panelu Automatyczne przygotowanie instancji. Gdy tworzenie jest wyłączone, przygotuj instancję ręcznie; aktywacja ją weryfikuje. Klient, któremu operator już umieścił sekret połączenia, nie jest tworzony automatycznie; aktywuj go przyciskiem Zweryfikuj i aktywuj instancję.
- Przy bazie platformy konta klientów są przechowywane w jej wspólnej tabeli kont i są takie same w każdej instancji aplikacji; bez niej pozostają w lokalnym katalogu danych jednej instancji. Każda organizacja sama podłącza logowanie firmowe (Microsoft Entra ID, Okta, OpenID Connect lub SAML 2.0) i provisioning SCIM w widoku Bezpieczeństwo i dostęp.
- Kwota umowy jest zapisem warunków handlowych, a nie fakturą, automatyczną płatnością ani stałym cennikiem. Wyszukiwanie, filtry, sortowanie i stronicowanie rejestru wykonuje serwer: przeglądarka pobiera tylko bieżącą stronę i otwartego klienta. Wyszukiwany tekst jest porównywany dosłownie (znaki % i _ nie są symbolami wieloznacznymi). Rozmiar strony i okno wygasania ustawia operator w Clm:Platform:Directory.
- Automatyczne tworzenie instancji wymaga skonfigurowanego polecenia infrastruktury i działa tylko na hostach Unix. Wdrożenie kontenerowe tworzy bazę każdego klienta z własną rolą właściciela i rolą runtime na serwerze baz klientów tego wdrożenia, przez TLS z pełną weryfikacją certyfikatu; dane logowania jednego klienta nie otwierają bazy innego. Lokalnie może tworzyć osobny Docker PostgreSQL dla klienta, w chmurze służą moduły Terraform dla AWS RDS, Azure Flexible Server i Cloud SQL. Baza lub rola o tej samej nazwie, której nie utworzył mechanizm tworzenia, baza należąca do innego klienta i istniejący inny sekret są odrzucane bez zmian. Usuwanie infrastruktury klienta nie jest zautomatyzowane.
- Skrzynki źródeł chmurowych to pliki na hoście platformy zapisywane przez kolektor klienta; wdrożenie może ograniczyć je do katalogu skrzynek, a skrzynka spoza niego jest oznaczona jako nieodczytywana. Wcześniej używany plik rejestru synchronizacji jest jednorazowo przejmowany do kart klientów. Źródło klienta bez licencji grafu zaufania kończy się błędem z tą przyczyną. Funkcje katalogu HSM integration i On-premise są w zestawieniu planów i tabeli uprawnień oznaczone jako Funkcja niewdrożona; ich przyznanie nie włącza żadnej funkcji.
- Linki konfiguracyjne są ważne przez Clm:Identity:MfaSetupLinkLifetime (domyślnie 24 godziny), działają raz i nadal wymagają hasła do konta; ustaw Clm:Identity:PublicConsoleUrl, aby linki używały publicznego adresu konsoli.
- Konta klienta utworzone lub ponownie włączone przez operatora wliczają się do limitu aktywnych kont z umowy klienta (limit użytkowników pakietu, przejmowany z planu przy zastosowaniu podpisanej umowy, 5 dla klienta bez zastosowanej umowy); konta tworzone przez własnych Adminów klienta i przez SCIM nie są jeszcze z nim porównywane. W organizacji z Adminem link konfiguracyjny konta klienta nigdy nie jest pokazywany w centrum sterowania: bez działającego przekaźnika platformy konsola to komunikuje, a link wysyła lub otrzymuje Admin klienta. E-mail break-glass, którego nie udało się doręczyć po skonfigurowanej liczbie prób, pozostaje zapisany we wniosku i w dzienniku klienta.

16 Operatorzy platformy

Zdecyduj, kto może korzystać z centrum sterowania: dodawaj operatorów platformy, zmieniaj ich adres e-mail, blokuj i odblokowuj ich, resetuj ich MFA i usuwaj ich, przy czym każda czynność i każda odrzucona próba trafia do dzienników. Określa też, z jakich sieci operatorzy mogą się logować i pracować. Każdy operator ma rolę określającą, z których części centrum sterowania może korzystać; podniesienie roli wymaga zatwierdzenia przez drugiego operatora.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Zaloguj się przez wejście dla operatorów (/operator-access) jako aktywny operator platformy z MFA i otwórz w centrum sterowania Operatorzy platformy. Lista pokazuje nazwę logowania, adres e-mail, stan (Aktywny lub Zablokowany), czy MFA jest skonfigurowane oraz czy operator pochodzi z konfiguracji wdrożenia (operator bootstrap, Clm:Platform:AdminIds), czy został dodany w centrum sterowania. Twój własny wiersz nie ma czynności.
2. Każdą zmianę (dodanie, zmiana e-maila, blokada, odblokowanie, reset MFA, e-mail konfiguracyjny, usunięcie) potwierdzasz bieżącym 6-cyfrowym kodem z własnej aplikacji uwierzytelniającej (step-up): wpisz go w formularzu albo w oknie potwierdzenia czynności w wierszu, które opisuje też jej skutek. Brakujący, błędny lub już użyty kod odrzuca zmianę z podaniem przyczyny; odrzucenie trafia do dziennika.
3. Dodaj operatora: podaj nazwę logowania, adres e-mail, hasło początkowe i język e-maili, a następnie wybierz Dodaj operatora. CERTYX zakłada konto w organizacji operatorów (platform-control) i wystawia jednorazowy link konfiguracji aplikacji uwierzytelniającej. Gdy przekaźnik poczty platformy

jest skonfigurowany (ustawienia Monitoringu), link jest wysyłany e-mailem; w przeciwnym razie widok pokazuje go z przyczyną, do przekazania zaufanym kanałem. Hasło początkowe przekaż osobno. Nowy operator otwiera link, podaje hasło, dodaje aplikację uwierzytelniającą, potwierdza kod, a następnie loguje się przez wejście dla operatorów hasłem i kodem.

4. Role: wsparcie (klienci tylko do odczytu, monitoring i incydenty), sprzedaż (sprzedaż, subskrypcje i cykl życia klienta), administrator bezpieczeństwa (operatorzy, konta klientów i wnioski o dostęp, integracje, SIEM, dzienniki, alerty, sesje) oraz administrator (wszystko; operator startowy i skonfigurowani). Centrum sterowania pokazuje tylko widoki i akcje Twojej roli, a serwer odrzuca wszystko inne z podaniem powodu. Dodaj operatora pozwala wybrać rolę: nowy operator zawsze zaczyna z rolą wsparcia, a każda inna rola staje się wnioskiem w Wnioskach o rolę. Zmień rolę w wierszu obniża rolę od razu; podniesienie tworzy wniosek.
5. Wnioski o rolę: oczekujący wniosek zatwierdza lub odrzuca własnym kodem albo kluczem dostępu inny operator niż wnioskujący i ten, którego dotyczy; jego rola musi obejmować wnioskowaną (administratora zatwierdza tylko administrator). Wnioskujący widzi zamiast tego Wycofaj. Wniosek bez odpowiedzi wygasa (domyślnie po 3 dniach). Ostatniego aktywnego administratora nie można zablokować, usunąć ani zmienić mu roli, a operatora z rolą wyższą niż Twoja nie możesz zmieniać.
6. Sesje (administrator bezpieczeństwa i administrator): Pokaż sesje wyświetla sesje przeglądarki i aplikacji mobilnej operatorów albo, po podaniu identyfikatora, organizacji, z klientem, początkiem, ostatnią aktywnością, adresem i stanem. Zakończ sesję (potwierdzone Twoim kodem lub kluczem dostępu) wylogowuje ją przy następnym żądaniu i zapisuje to w dzienniku bezpieczeństwa tej organizacji.
7. Zmień e-mail: wybierz Zmień e-mail, podaj nowy adres i zapisz. Sesje operatora się kończą; nazwa logowania pozostaje bez zmian.
8. Zablokuj: wybierz Zablokuj i potwierdź. Sesje operatora kończą się natychmiast (przy jego następnym żądaniu), logowanie jest odrzucane, a blokada obowiązuje także wtedy, gdy identyfikator operatora nadal jest na skonfigurowanej liście. Odblokuj i potwierdź, aby przywrócić dostęp; operator loguje się ponownie hasłem i aplikacją uwierzytelniającą.
9. Resetuj MFA (operator utracił aplikację uwierzytelniającą): potwierdź reset; aplikacja uwierzytelniająca i kody odzyskiwania są usuwane, a sesje się kończą. Następnie wybierz Wyślij e-mail konfiguracyjny, aby operator mógł skonfigurować nową aplikację. Wyślij e-mail konfiguracyjny jest dostępne także dla operatora, który nigdy nie dokończył konfiguracji.
10. Usuń: potwierdź usunięcie. Operator znika z listy, sesje się kończą, a konto zostaje trwale wyłączone. Członkostwo pozostaje jako nagrobek, więc ponowne wpisanie identyfikatora na skonfigurowaną listę nie przywraca operatora, a nazwa logowania pozostaje zarezerwowana, aby dzienniki nadal ją wskazywały.
11. Każda czynność i każda odrzucona próba trafia do audytu platformy (Dziennik zdarzeń bezpieczeństwa → Audyt platformy: czynność platform.operator.<czynność>, konto docelowe i wynik, refused: <przyczyna> przy odrzuceniu; stan przed i po jest zapisany przy wpisie) oraz do łańcuchowanego hashami dziennika zdarzeń bezpieczeństwa z działającym operatorem, celem, stanem przed, po i wynikiem.
12. Sieci logowania centrum sterowania: wpisz adresy i zakresy, z których łączą się operatorzy, po jednym w wierszu (203.0.113.7, 203.0.113.0/24, 2001:db8::/48), podaj kod z aplikacji uwierzytelniającej i zapisz. Dopóki nie zapiszesz tu listy, obowiązuje ustawienie wdrożenia Clm:Platform:AllowedNetworks (pokazywane jako zakresy z konfiguracji wdrożenia); potem pierwszeństwo ma zapisana lista. Panel pokazuje Twój adres i czy lista go obejmuje; lista bez niego jest odrzucana, dopóki nie zaznaczysz

potwierdzenia i nie podasz nowego kodu. Od tej chwili sprawdzane jest każde logowanie operatora przez wejście dla operatorów i każde żądanie sesji operatora; sesja spoza listy kończy się przy kolejnym żądaniu. Aby usunąć ograniczenie, wyczyść listę i zapisz.

DANE I PARAMETRY

- Nazwa logowania: do 120 znaków bez spacji, unikalna wśród wszystkich kont; nie można jej później zmienić.
- Adres e-mail: poprawny adres, unikalny wśród wszystkich kont; otrzymuje link konfiguracji.
- Hasło początkowe: od 16 do 256 znaków.
- Język e-maili: English, Deutsch lub Polski, dla e-maila konfiguracji.
- Twój kod z aplikacji uwierzytelniającej: bieżący 6-cyfrowy kod z własnej aplikacji, wymagany przy każdej zmianie; kody odzyskiwania nie są akceptowane.
- Ustawienia wdrożenia (poza konsolą): Clm:Platform:AdminIds (CLM_PLATFORM_ADMIN_IDS), identyfikatory kont, które są operatorami, dopóki nie istnieje zapisane członkostwo (zapisywane przez bootstrap przy wdrożeniu); przekaźnik poczty platformy (ustawienia Monitoringu) dla e-maili konfiguracji.
- Sieci logowania centrum sterowania: adresy IPv4 lub IPv6 albo zakresy CIDR zaczynające się od pierwszego adresu, najwyżej Clm:Identity:MaximumSignInNetworks wpisów (domyślnie 100); Clm:Platform:AllowedNetworks w konfiguracji wdrożenia jest listą początkową (niepoprawne wpisy zatrzymują start).
- Rola: wsparcie, sprzedaż, administrator bezpieczeństwa lub administrator; każda rola powyżej wsparcia jest wnioskiem do czasu zatwierdzenia przez drugiego operatora.

WYNIK OPERACJI

Członkostwo każdego operatora w bazie danych platformy (aktywne, zablokowane lub usunięte, z wersją), konto w platform-control dla operatorów dodanych tutaj, zakończone sesje po blokadzie, usunięciu, zmianie e-maila lub resecie MFA oraz wpis w audycie platformy i dzienniku zdarzeń bezpieczeństwa dla każdej czynności i każdej odrzuconej próby. Każda zmiana sieci logowania centrum sterowania trafia do audytu platformy (platform.signin-networks.changed, cel platform-control, przed i po) i do dziennika bezpieczeństwa; odrzucone logowania i żądania operatorów spoza listy są zdarzeniami logowania z powodem network-not-allowed i adresem źródłowym.

UPRAWNIENIA

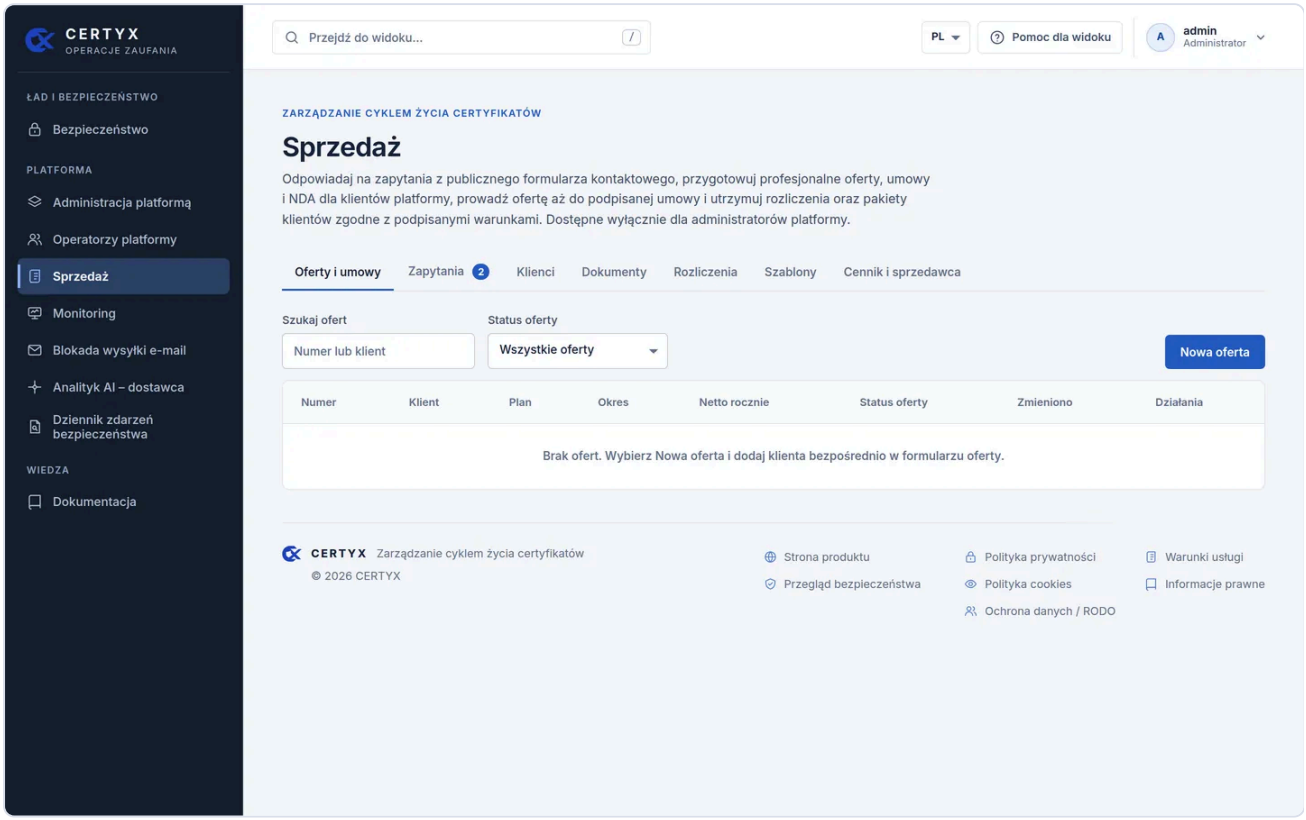
Tylko aktywni operatorzy platformy zalogowani z MFA otwierają ten widok i używają jego API; administratorzy klientów oraz zablokowani lub usunięci operatorzy są odrzucani (403) i nie mają do niego dostępu. Ten widok wymaga roli administratora bezpieczeństwa lub administratora; inne role go nie widzą. Operator zmienia tylko operatorów, których rolę obejmuje jego własna, i nigdy nie zatwierdza własnego wniosku o rolę. Operator nigdy nie zmienia tutaj własnego konta (bez samoblokady, samousunięcia i resetu własnego MFA; własny e-mail i aplikację uwierzytelniającą zmienisz w Profilu), dlatego ostatni aktywny operator zawsze zachowuje dostęp. Sieci logowania centrum sterowania: każdy aktywny operator zalogowany z MFA, z bieżącym kodem z aplikacji uwierzytelniającej lokalnego konta operatora przy każdej zmianie.

OGRANICZENIA

Wymaga bazy danych platformy; bez niej żądania widoku odpowiadają 503. Zmiana wykonana na nieaktualnej liście jest odrzucana jako konflikt: odśwież i powtórz. Nazwy logowania nie można zmienić. Usuniętych operatorów nie można przywrócić; dodaj zamiast tego nowego operatora. Każdy kod potwierdza jedną zmianę: kod z kroku czasowego, który już potwierdził zmianę (lub logowanie), jest odrzucany, więc poczekaj na następny kod; błędne kody liczą się do blokady konta tak jak nieudane logowania. Operatorzy zalogowani przez logowanie firmowe nie mają lokalnej aplikacji uwierzytelniającej i nie mogą potwierdzać zmian: musi je wykonać lokalne konto operatora z aplikacją uwierzytelniającą. Czas ostatniego logowania nie jest pokazywany; logowania znajdziesz w Dzienniku zdarzeń bezpieczeństwa. Bez przekaźnika poczty link konfiguracji trzeba przekazać ręcznie. Odzyskiwanie, gdy żaden operator nie może się już zalogować: narzędzie bootstrap offline (reset-mfa) opisane w DEPLOYMENT.md. Operatorzy korzystający z logowania firmowego platformy (identyfikator sso:platform-control:<podmiot> na skonfigurowanej liście) nie mają konta lokalnego: są wyświetlani bez czynności, a ich dostęp kończy się po usunięciu identyfikatora z Clm:Platform:AdminIds. Sieci logowania można tu zapisać tylko z bazą danych platformy; bez niej obowiązuje tylko Clm:Platform:AllowedNetworks. Jeśli zapisana lista odcina od centrum sterowania wszystkich operatorów, właściciel usługi usuwa zapisaną listę w bazie danych platformy (DELETE FROM platform_settings WHERE key='signin-networks:platform-control' jako właściciel bazy, zob. PLATFORM-OPERATIONS.md); wtedy znów obowiązuje lista z konfiguracji. Operatorzy istniejący przed wprowadzeniem ról mają rolę administratora. Gdy żaden administrator nie może się zalogować, właściciel ustawia rolę w bazie platformy (odzyskiwanie offline).

17 Sprzedaż

Odpowiadaj na zapytania z publicznego formularza kontaktowego, przygotowuj profesjonalne oferty, umowy i NDA dla klientów platformy, prowadź ofertę aż do podpisanej umowy i utrzymuj rozliczenia oraz pakiety klientów zgodne z podpisanymi warunkami. Dostępne wyłącznie dla administratorów platformy.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. W zakładce Cennik i sprzedawca sprawdź dane sprzedawcy widoczne na każdym dokumencie oraz cennik: opłaty planów, progi certyfikatów, SSH, dodatki, rabaty za okres, próg akceptacji rabatu i minimalną marżę. W sekcji Wysyłka e-mail sprzedaży włącz e-mail i wpisz przekaźnik SMTP (host, port STARTTLS, nadawca, opcjonalnie użytkownik i hasło tylko do ustawienia albo secret:<nazwa>), opcjonalną kopię dla operatora (powiadomienia rozliczeniowe) i do 10 odbiorców powiadomień o zapytaniach; Wyślij e-mail testowy wysyła od razu jedną wiadomość i podaje przyczynę niepowodzenia.
2. Zapytania to lista zgłoszeń z formularza kontaktowego na stronie publicznej (pytanie ogólne, prośba o prezentację, prośba o ofertę, prośba o pilotaż), od najnowszych; znacznik zakładki liczy nowe. Szczegóły pokazują kontakt, wiadomość i odpowiedzi z ankiety oraz pozwalają ustawić status (Nowe, W kontakcie, Przekształcone, Zamknięte) z notatką wewnętrzną. Dla prośby o prezentację, ofertę lub pilotaż Utwórz ofertę dodaje klienta z zapytania (jednorazowo; kolejne kliknięcia używają tego samego), oznacza zapytanie jako Przekształcone i otwiera nową ofertę wypełnioną pakietem, liczbą zarządzanych certyfikatów, hostów SSH (co najmniej minimum SSH), dodatkowymi organizacjami,

wdrożeniem, wsparciem premium, okresem, rozliczeniem miesięcznym (jeśli pakiet na nie pozwala), walutą, miesiącem startu, znacznikiem pilotażu oraz numerem i treścią zapytania w notatkach. Sprawdź wycenę i zapisz ofertę.

3. Każde nowe zapytanie wysyła przez przekaźnik sprzedaży dwa e-maile, zwykle w ciągu kilku sekund: każdy odbiorca powiadomień o zapytaniach dostaje powiadomienie w języku z Clm:Sales:Inquiries:NotifyLanguage (domyślnie angielski) z nagłówkiem, kolorem i priorytetem zależnym od rodzaju (zapytanie ogólne: standardowy, odpowiedź w ciągu 1 dnia roboczego; prośba o prezentację: wysoki, terminy prezentacji w ciągu 1 dnia roboczego; prośba o ofertę: wysoki, wyceniona oferta w ciągu 1 dnia roboczego; wniosek o pilotaż: najwyższy, kontakt w ciągu 4 godzin roboczych), wszystkimi danymi z formularza (kontakt, stanowisko, firma, e-mail, telefon, kraj, NIP, język, odpowiedzi z ankiety łącznie z preferowanym wdrożeniem i startem, cele pilotażu, wiadomość, zgoda, numer zgłoszenia i czas otrzymania w UTC), zalecanymi kolejnymi krokami (przy pilotażu także listą wymagań), przyciskiem Odpowiedz: <imię> (Reply-To to klient) i Otwórz w konsoli, który otwiera to zapytanie w Sprzedaż › Zapytania. Klient dostaje potwierdzenie w swoim języku odpowiedzi z numerem zgłoszenia, kolejnymi krokami i adresem nadawcy działu sprzedaży. Oba są w HTML z wersją tekstową i osadzonym logo; nie pobierają niczego z internetu.
4. Klientów dodaje się przyciskiem Nowy klient: w zakładce Klienci albo bezpośrednio przy polu klienta w ofercie lub NDA, gdzie nowy klient zostaje wybrany zaraz po zapisaniu, a wpisane już wartości zostają. Podaj dane rejestrowe, kontakt i e-mail do faktur, język dokumentów i oznaczenie sektora publicznego. Opcjonalnie wskaż istniejącego klienta platformy; w przeciwnym razie pierwsza podpisana umowa go utworzy.
5. Opcjonalny pilotaż: w zakładce Dokumenty wygeneruj NDA dla klienta przed rozpoczęciem pilotażu.
6. W zakładce Oferty i umowy wybierz Nowa oferta: formularz startuje z planem Professional, okresem 24 miesięcy i wdrożeniem. Wybierz lub dodaj klienta, potem dostosuj pakiet, okres, fakturowanie i rabat. Wycena po prawej przelicza się na bieżąco i ostrzega o minimalnym okresie, akceptacji rabatu, maksymalnym rabacie i marży. Zapis nadaje numer OF/rok/kolejny.
7. Wybierz Generuj PDF oferty. Każdy PDF jest szyfrowany AES-256 własnym hasłem, pokazywanym po wygenerowaniu i dostępnym później przez Pokaż hasło. PDF i hasło wysyłaj różnymi kanałami.
8. Prowadź ofertę przez etapy: Oznacz jako wysłaną, Klient zaakceptował, Przygotuj umowę (nadaje UM/rok/kolejny), a następnie Generuj PDF umowy w języku klienta (dostępne od etapu Klient zaakceptował). Ostatnie poprawki są możliwe do momentu podpisania. Pozostałe przejścia: Przywróć jako szkic, Klient odrzucił, Oznacz jako wygasłą i Anuluj ofertę; ofertę odrzuconą lub wygasłą można przywrócić jako szkic, anulowanie, odrzucenie i podpisanie wymagają potwierdzenia, a anulowanie jest ostateczne.
9. Po podpisaniu otwórz Podpisana umowa i konfiguracja: wpisz warunki z umowy (możliwe, gdy oferta jest zaakceptowana lub umowa przygotowana), wgraj skan, użyj Sprawdź warunki, aby porównać ofertę, umowę i konfigurację klienta, potem Oznacz jako podpisaną — przycisk jest nieaktywny, dopóki nie wpiszesz podpisanych warunków. To blokuje ofertę, tworzy harmonogram płatności oraz tworzy lub konfiguruje klienta platformy według warunków: plan, funkcje, limit certyfikatów z tolerancją, ważność, okres rozliczeniowy, kwotę umowy i limit użytkowników.
10. Nowo utworzony klient platformy zaczyna w stanie provisioning: udostępnij i zweryfikuj jego instancję w Administracji platformą (Otwórz klienta platformy). Jeśli konfiguracja przy podpisaniu się nie powiodła, Zastosuj w subskrypcji klienta ją ponawia; służy też do ponownego zastosowania podpisanych warunków.

11. W zakładce Rozliczenia księguj płatności z datą i referencją. Zaksięgowanie płatności, która usuwa zaległość, automatycznie przywraca klienta zawieszonego przez rozliczenia. Panel Wymaga uwagi nad zakładkami (widoczny tylko, gdy coś jest wymagalne) pokazuje zbliżające się płatności, zaległości, zawieszonych klientów i umowy bliskie końca; Przygotuj ofertę odnowienia tworzy szkic od dnia po końcu umowy.
12. W zakładce Szablony edytuj treść oferty, umowy i NDA w każdym języku, wstawiaj pola danych i bloki generowane, oglądaj podgląd PDF i zapisuj nową wersję.
13. Płatność rejestrujesz przyciskiem Zaksięguj płatność w oknie z datą zapłaty i numerem referencyjnym (do 120 znaków). Cennik pokazuje każdy plan jako osobną kartę z podsumowaniem (opłata, limity, marża, kompletność tekstów PL/EN/DE) i rozwijaną edycją; karta ostrzega o brakujących lub niezgodnych listach i tekstach wsparcia PL/EN/DE, marży poniżej minimum oraz marży spadającej poniżej minimum przy maksymalnym rabacie handlowym. Zmiany cennika zapisujesz paskiem Zapisz/Odrzuć widocznym przy przewijaniu.

DANE I PARAMETRY

- Zapytanie (z formularza publicznego): rodzaj, imię i nazwisko, firma, służbowy e-mail, opcjonalnie telefon, kraj, stanowisko i NIP, język odpowiedzi i dokumentów (EN, DE lub PL), wiadomość (wymagana przy pytaniu ogólnym), zgoda, a przy prośbie o ofertę lub pilotaż opcjonalna ankieta: pakiet, zarządzane certyfikaty, hosty SSH, organizacje, preferowane wdrożenie (hostowane przez CERTYX, własne środowisko lub nie zdecydowano), miesiąc startu, okres w latach, rozliczenie roczne lub miesięczne, waluta, wdrożenie, wsparcie premium, sektor publiczny, źródła certyfikatów i cele pilotażu.
- Klient: pełna nazwa, adres, NIP, numer rejestrowy, reprezentant, kontakt i e-mail do faktur, język, sektor publiczny, powiązany klient platformy.
- Oferta: plan, zarządzane certyfikaty, hosty SSH, dodatkowe organizacje, wdrożenie, dodatkowe dni, wsparcie premium, pilotaż, okres (domyślnie minimum 12 miesięcy, zalecane 24, najwyżej 60), fakturowanie roczne lub miesięczne, rabat handlowy i osoba zatwierdzająca, data startu, ważność, uwagi, PLN, EUR lub USD (EUR i USD po kursach z cennika). Rabat powyżej progu akceptacji z cennika wymaga osoby zatwierdzającej, a żaden rabat nie może przekroczyć maksymalnego rabatu handlowego.
- Formaty: zarządzane certyfikaty i hosty SSH to liczby całkowite od 0 do 10 000 000, dodatkowe organizacje 0–50, dodatkowe dni 0–365; rabat handlowy 0–100 % z maksymalnie 2 miejscami po przecinku, osoba zatwierdzająca do 300 znaków, uwagi do 4000 znaków; pola tekstowe klienta do 300 znaków; termin płatności 1–120 dni; kwoty z maksymalnie 2 miejscami po przecinku; host SMTP to nazwa hosta lub adres IP bez schematu i portu, port 1–65535, nadawca i kopia operatora to pojedyncze adresy e-mail, odbiorcy powiadomień o zapytaniach to do 10 adresów rozdzielonych przecinkami; pola profilu sprzedawcy do 300 znaków; szablony do 200 000 znaków. Kwestionariusz zapytania: zarządzane certyfikaty i hosty SSH to liczby całkowite od 0 (do Clm:Sales:Inquiries:MaxQuantity), organizacje od 1 (do MaxOrganizations, domyślnie 100), okres 1–3 lata; wiadomość i cele pilotażu do Clm:Sales:Inquiries:MaxMessageLength (domyślnie 4000 znaków); imię i nazwisko, firma, telefon, kraj, stanowisko i NIP do 300 znaków. Podpowiedź pod każdym polem podaje jego format, a odrzucona wartość wskazuje pole i oczekiwany format.
- Podpisane warunki: plan, ilości, początek i koniec okresu (koniec po początku), okres rozliczeniowy (miesięczny lub roczny), kwota netto rocznie, waluta (PLN, EUR lub USD), termin płatności (1–120 dni) i uzgodnione zmiany. Skan: PDF, JPEG lub PNG, rozpoznawany po treści, w skonfigurowanym limicie rozmiaru (Clm:Sales:MaxSignedScanBytes, domyślnie 20 MB).

- Szablony: nagłówki (#), punktory (-), punkty numerowane (1.), **pogrubienie**, {{pola danych}}, fragmenty {{#if warunek}} oraz bloki, np. [[pricing-table]], [[payment-schedule]] i [[signatures]].

WYNIK OPERACJI

Numerowane oferty i umowy z zapisanym przebiegiem; chronione hasłem PDF z logo, nagłówkami i numeracją stron, przechowywane z wersją szablonu i SHA-256; harmonogram płatności z przypomnieniami oraz klient platformy utworzony lub skonfigurowany według podpisanych warunków, którego umowa wyznacza potem subskrypcję w Administracji platformą. Generowanie dokumentów, wyświetlenie hasła, warunki, skany, zmiany statusu, konfiguracja klienta, zawieszenia i przywrócenia trafiają do dziennika bezpieczeństwa.

UPRAWNIENIA

Administrator platformy w sesji uwierzytelnionej MFA. Konta klientów, w tym Admin klienta, nie mają dostępu do tego widoku ani jego API. Step-up: podpisanie oferty (które rejestruje lub konfiguruje klienta), zastosowanie umowy do subskrypcji, zapisanie płatności i zmiana przekaźnika poczty sprzedaży wymagają bieżącego 6-cyfrowego kodu aplikacji uwierzytelniającej (przez kilka minut obejmuje je potwierdzony kod); wyceny, oferty, strony, dokumenty i szablony nie.

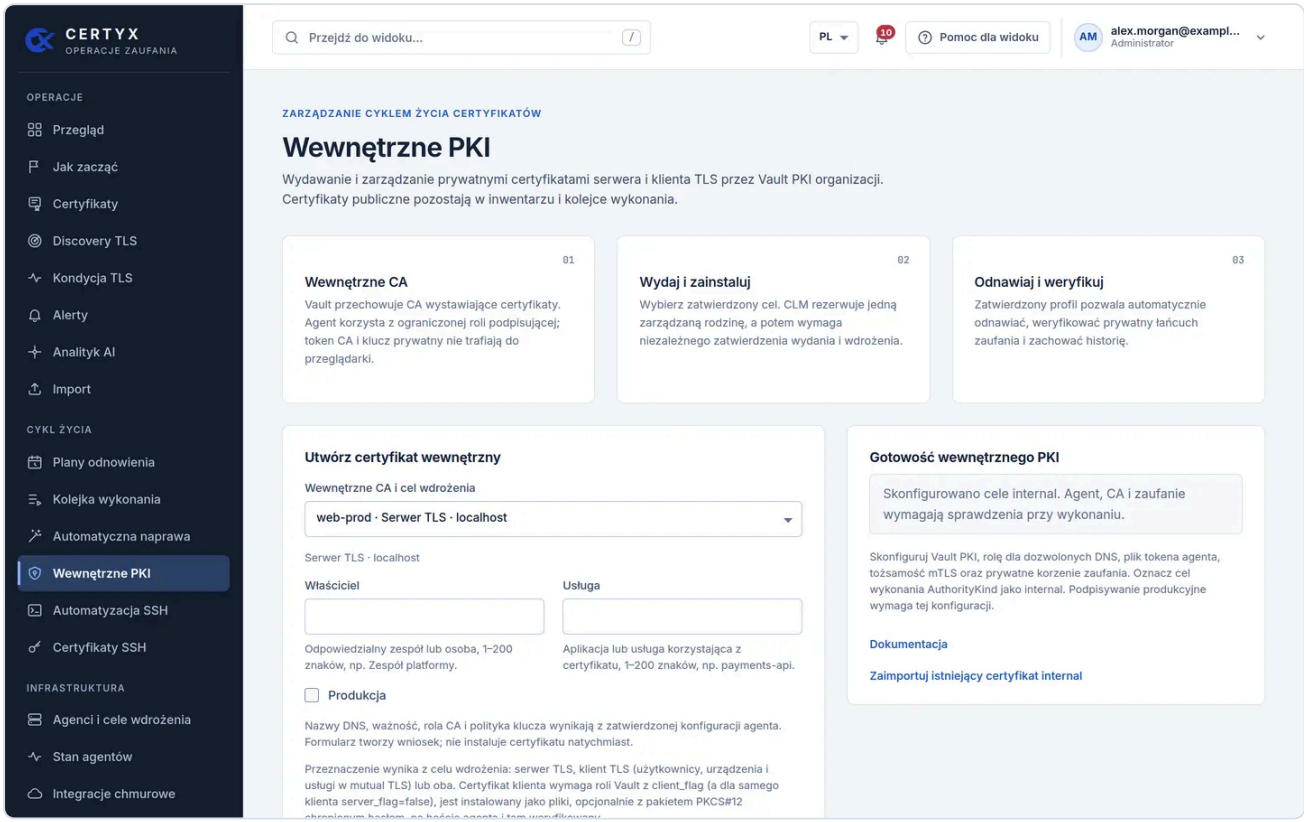
OGRANICZENIA

- Wymaga bazy platformy (Clm:Database:Platform) z aktualnym platform/schema.sql; bez niej widok informuje, że sprzedaż jest niedostępna.
- Publiczny formularz kontaktowy wymaga bazy platformy; bez niej formularz informuje, że jest niedostępny. Przyjmuje 10 zgłoszeń na minutę z jednego adresu (Clm:Http:InquiriesPerWindow), wymaga tokenu CSRF i po cichu odrzuca zgłoszenia z wypełnionym ukrytym polem honeypot. Powiadomienie i potwierdzenie są wysyłane tylko przy włączonej wysyłce e-mail sprzedaży; do tego czasu czekają w zakładce Rozliczenia i zostaną wysłane po jej włączeniu (kolejka jest sprawdzana co Clm:Sales:NoticeInterval, domyślnie 30 sekund, oraz od razu po nowym zapytaniu). Bez odbiorców powiadomień o zapytaniach powiadomienie trafia na e-mail kontaktowy sprzedawcy; bez obu w kolejce jest tylko potwierdzenie. Otwórz w konsoli używa Clm:Sales:Inquiries:ConsoleUrl, a gdy jest puste — adresu, z którego wysłano formularz, i wymaga logowania administratora platformy. Każdy odwiedzający widzi numer zgłoszenia na ekranie; odfiltrowane zgłoszenie honeypot nie wysyła e-maili.
- Domyślne szablony umowy, DPA i NDA są projektami i przed użyciem wymagają weryfikacji prawnika.
- Kwoty miesięczne w ofertach są wyłącznie poglądowe; umowy są zawierane na cały okres.
- Platforma nie wystawia faktur VAT ani nie łączy się z bankiem: płatności księguje się ręcznie, a faktury pochodzą z systemu księgowego.
- Przypomnienia i powiadomienia e-mail są wysyłane tylko przy włączonej Wysyłce e-mail sprzedaży; w przeciwnym razie czekają w kolejce widocznej w Rozliczeniach i zostaną wysłane po jej włączeniu. Wartości z pliku konfiguracji są jednorazowo przejmowane do konsoli; limit czasu przekaźnika pozostaje ustawieniem wdrożenia. TLS jest zawsze wymagany.
- Nieopłacona pozycja zawiesza powiązanego klienta platformy po wewnętrznym okresie karencji ustawionym w Clm:Sales:SuspensionGraceDays; okres karencji nie jest podawany w przypomnieniach. Po zaksięgowaniu płatności, jeśli nic innego nie zalega dłużej niż karencja, klient jest przywracany automatycznie. Zawieszenia ustawionego przez operatora w Administracji platformą rozliczenia nigdy nie znoszą, a klient ponownie aktywowany przez operatora mimo zaległości dłuższej niż karencja zostanie znów zawieszony przy następnym sprawdzeniu rozliczeń.

- Skany podpisanych umów są przechowywane do porównania; platforma nie odczytuje ich treści. Warunki są porównywane z wartościami, które wpiszesz.
- Utworzenie klienta platformy przy podpisaniu wymaga Clm:Storage:CustomerSecretDirectory; dedykowaną instancję nadal udostępnia się i weryfikuje w Administracji platformą.
- Jeśli działający serwer jest starszy niż pliki konsoli, widok informuje o tym zamiast pokazywać puste listy; uruchom ponownie aplikację i odśwież stronę.

18 Wewnętrzne PKI

Wydawanie i zarządzanie prywatnymi certyfikatami serwera i klienta TLS przez Vault PKI organizacji. Certyfikaty publiczne pozostają w inwentarzu i kolejce wykonania.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Skonfiguruj Vault PKI z CA wystawiającym certyfikaty i rolą ograniczoną do DNS. Token przechowuj w prywatnym pliku na agencie.
2. Skonfiguruj agenta mTLS i prywatne korzenie zaufania. W Kolejka wykonania → Cele wdrożenia administrator tworzy cel z urzędem certyfikacji Wewnętrzny CA (Vault PKI), jego adresem CA, mount i rolą (AuthorityKind internal). Cel agenta używa AuthorityKind vault.
3. Gotowość wewnętrznego PKI pokazuje, czy istnieją cele internal i ile z nich jest wyłączonych; bez włączonego celu formularz jest wyłączony. Wyłączone cele pozostają na liście, oznaczone jako wyłączone i niemożliwe do wybrania, ponieważ serwer odrzuca dla nich nowe zlecenia. W sekcji Utwórz certyfikat wewnętrzny wybierz cel w polu Wewnętrzne CA i cel wdrożenia (lista obejmuje każdy cel z wewnętrznym CA, z przeznaczeniem i tożsamościami), podaj Właściciel, Usługa i Produkcja i wybierz Zleć wydanie certyfikatu internal. CERTYX rezerwuje jedną zarządzaną rodzinę przed utworzeniem wniosku; potwierdzenie pokazuje identyfikator zlecenia.
4. Inny administrator zatwierdza zlecenie w Kolejce wykonania (Otwórz kolejkę zatwierdzania i wykonania). Agent generuje klucz/CSR, podpisuje przez Vault, wdraża i weryfikuje TLS.
5. Sprawdź wynikowy certyfikat w sekcji Inwentarz certyfikatów internal (50 na stronę). Lista obejmuje tylko certyfikaty sklasyfikowane jako internal: wydane przez cel internal albo zaimportowane jako Certyfikat wewnętrzny (Zaimportuj istniejący certyfikat internal). Dla automatyzacji zatwierdź oddzielny

profil odnowień w Kolejce wykonania.

6. Dla certyfikatów klienta utwórz cel w Kolejce wykonania z przeznaczeniem Klient TLS (lub Serwer i klient) i jego tożsamościami. Użyj osobnej roli Vault: client_flag=true, server_flag=false dla samego klienta, allowed_domains obejmujące domeny e-mail/DNS, allowed_other_sans dla nazw UPN (1.3.6.1.4.1.311.20.2.3;UTF8:*@corp.example.com) i allowed_uri_sans dla URI; cn_validations=disabled tylko przy dowolnej nazwie pospolitej, np. imieniu i nazwisku. Rola bez client_flag jest odrzucana ze wskazaniem tego ustawienia, a żądanie wyłącznie klienckie — gdy rola nadałaby też uwierzytelnianie serwera.

DANE I PARAMETRY

- Nazwy DNS, tożsamości klienta, przeznaczenie, adres CA oraz mount/rola Vault pochodzą z celu wykonania; ważność i polityka klucza wynikają z roli Vault i konfiguracji agenta. Importowany certyfikat można oznaczyć jako internal.
- Właściciel i Usługa: wymagane, 1–200 znaków każde. Cel musi być włączony; wniosek dla wyłączonego celu jest odrzucany (włącz go w Kolejce wykonania).

WYNIK OPERACJI

Audytowany wniosek wydania, a po udanym zweryfikowanym wykonaniu certyfikat internal w inwentarzu. Odnowienie dziedziczy rodzinę.

UPRAWNIENIA

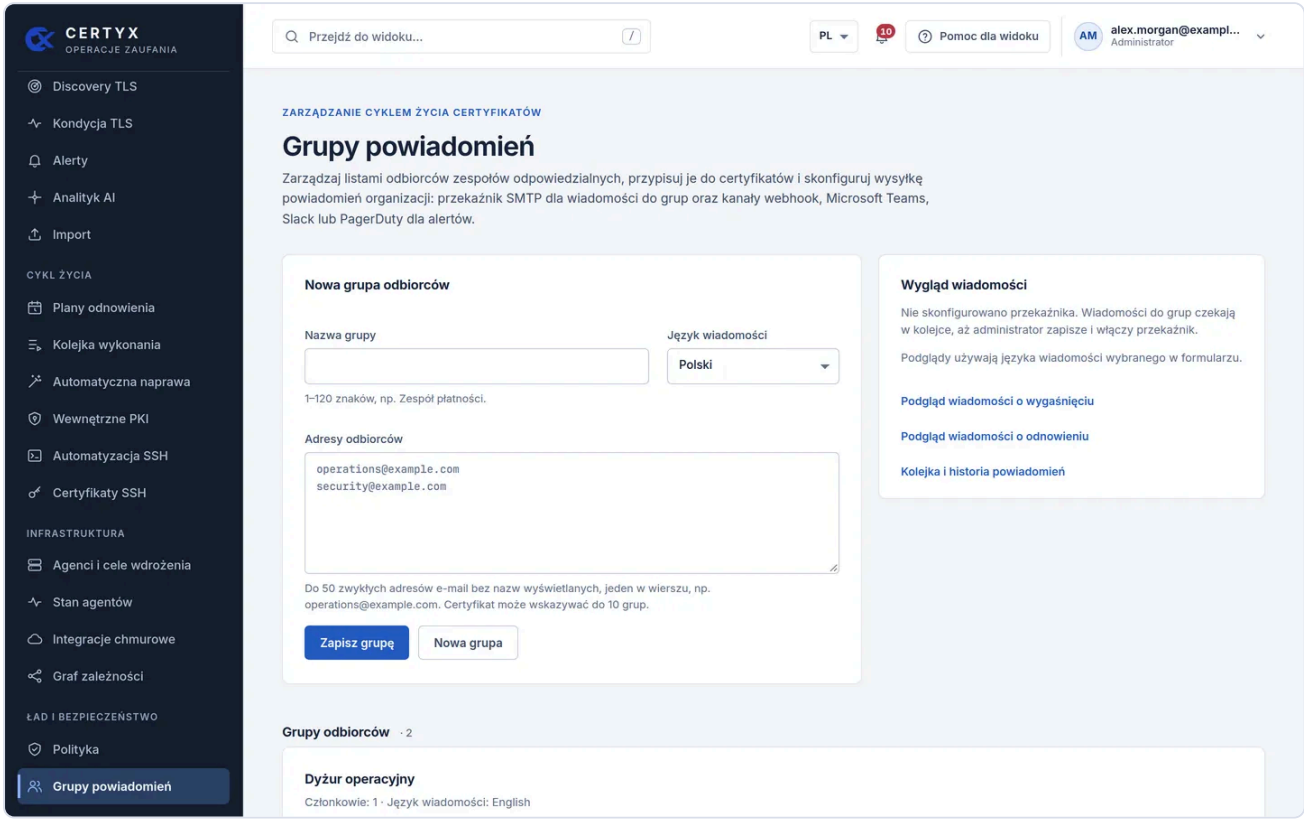
Operator lub administrator zleca wydanie (w usłudze z subskrypcjami tylko z funkcją AUTO_DEPLOYMENT i wolnym limitem zarządzanych rodzin); inny administrator zatwierdza zlecenie; Audytor tylko odczytuje (formularz jest wyłączony). Cele i tożsamości agentów są ograniczone do organizacji.

OGRANICZENIA

Wymaga skonfigurowanego Vault i agenta. Widok nie tworzy CA root, nie dystrybuuje zaufania do wszystkich klientów i nie wydaje certyfikatów code-signing. Certyfikaty klienta (użytkownicy, urządzenia, usługi w mutual TLS) są wydawane, gdy przeznaczeniem celu jest klient TLS albo serwer i klient, a rola Vault ustawia client_flag; są dostarczane wyłącznie jako pliki w agentach Unix (bez magazynu certyfikatów Windows, przeglądarki i kart inteligentnych). Import nie potwierdza zaufania.

19 Grupy powiadomień

Zarządzaj listami odbiorców zespołów odpowiedzialnych, przypisuj je do certyfikatów i skonfiguruj wysyłkę powiadomień organizacji: przekaźnik SMTP dla wiadomości do grup oraz kanały webhook, Microsoft Teams, Slack lub PagerDuty dla alertów.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Utwórz grupę odbiorców z nazwą, językiem wiadomości (angielski, niemiecki lub polski) i maksymalnie 50 zwykłymi adresami; przypisz grupy w szczegółach certyfikatu. Archiwizuj grupę wycofuje grupę z użycia: nie otrzymuje już wiadomości i nie można jej przypisać do certyfikatów, ale pozostaje na liście (oznaczona jako Zarchiwizowana) wraz z członkami; Przywróć grupę ponownie ją aktywuje. Edycja grupy zachowuje stan archiwizacji. Odrzucony zapis podaje powód (zbyt długi identyfikator lub nazwa, nieobsługiwany język, nieprawidłowi członkowie, zmiana w międzyczasie).
2. Grupa otrzymuje wiadomość, gdy przypisany do niej certyfikat osiąga próg wygaśnięcia lub wygasł, po zweryfikowanym odnowieniu tego certyfikatu, przy zdarzeniach certyfikatów SSH przypisanych do niej profili SSH oraz gdy powiadamia ją polityka naprawcza. Wygląd wiadomości → Podgląd wiadomości o wygaśnięciu i Podgląd wiadomości o odnowieniu pokazują układ wiadomości z przykładowymi danymi w języku wiadomości wybranym w formularzu (do czasu wyboru w języku konsoli, podczas edycji w języku grupy); wiadomości do grup czekają w kolejce, dopóki nie zostanie włączony przekaźnik SMTP.
3. Wysyłka → Przekaźnik SMTP: podaj host, port (587), adres nadawcy oraz, jeśli przekaźnik tego wymaga, nazwę użytkownika i hasło. Zawsze używany jest STARTTLS, a certyfikat przekaźnika jest weryfikowany. Włącz przekaźnik i zapisz.

4. Wyślij testowy e-mail wysyła krótką wiadomość przez zapisany przekaźnik na podany adres i pokazuje, czy przekaźnik ją przyjął; wynik jest zapisywany przy przekaźniku.
5. Wysyłka → Kanały powiadomień: dodaj webhook (HTTPS JSON, opcjonalnie podpisany HMAC-SHA256 w X-Certyx-Signature), przychodzący webhook Microsoft Teams lub adres Workflows, przychodzący webhook Slack (https://hooks.slack.com/...; treść alertu trafia jako zwykły tekst, bez wzmianek i linków) albo klucz integracji (routing key) PagerDuty. Opóźnienie eskalacji 0 wysyła każdy otwarty alert od razu; opóźnienie tworzy kanał eskalacji, który otrzymuje tylko krytyczne alerty nadal niepotwierdzone po tym czasie. Wyślij test sprawdza kanał (test PagerDuty jest od razu rozwiązywany).
6. Zdarzenia kanału: domyślnie wybrane są alerty certyfikatów; zaznacz zlecone zadanie, zatwierdzone zadanie, certyfikat wdrożony i zweryfikowany, nieudane zadanie, wycofane wdrożenie, anulowane zadanie i odnowiony certyfikat, aby potoki, kanały czatu lub narzędzia ITSM śledziły każde odnowienie. Każde zdarzenie trafia do kanału raz, gdy wystąpi (w oknie Clm:Notifications:LifecycleEventWindow, jeden dzień); webhook otrzymuje { eventId, type, version 1, event { id, at, actor, jobId, targetId, certificateId, domains, state } }, Teams i Slack krótki tekst, a PagerDuty tylko alerty oraz nieudane lub wycofane zadania.
7. Każdy przekaźnik i kanał pokazuje oczekujące i niedostarczalne wiadomości, ostatnie doręczenie i przyczynę ostatniego błędu; Alerty → Kolejka i historia powiadomień zawiera poszczególne wpisy.
8. Przed wysłaniem wiadomości do grupy system ponownie sprawdza aktualny skład grupy: usunięci adresaci nie otrzymują wiadomości z kolejki, nowi nie otrzymują starszych, a wiadomość bez uprawnionych adresatów jest anulowana. Adresaci otrzymują wiadomość przez Bcc; adres nadawcy nie jest dodawany.
9. Odbiorcy, którzy nie otrzymują już e-maili, to lista członków Twoich grup znajdujących się na liście blokad e-mail platformy (trwałe odbicie lub skarga zgłoszone przez dostawcę poczty), z przyczyną, datą i grupami; karty grup pokazują, ilu członków jest zablokowanych. CERTYX nic do nich nie wysyła, żadnym przekaźnikiem, dopóki operator platformy ich nie usunie. Popraw lub zastąp adres w grupie albo napraw skrzynkę i poproś operatora platformy (wsparcie) o usunięcie blokady. Obowiązują tylko wpisy ogólnoplatformowe i wpisy spowodowane pocztą Twojej organizacji; odbicie poczty innej organizacji nigdy nie blokuje Twoich odbiorców.

DANE I PARAMETRY

- Nazwa grupy (1–120 znaków), język wiadomości i członkowie (zwykłe adresy bez nazw wyświetlanych, najwyżej 50 w grupie). Nazwy kanałów również mają 1–120 znaków.
- Host przekaźnika, port, adres nadawcy, opcjonalnie nazwa użytkownika i hasło; zabezpieczenie STARTTLS (nieszyfrowany przekaźnik loopback jest dostępny tylko w środowisku Development).
- Nazwa kanału, identyfikator (1–64 małe litery, cyfry i łączniki, na początku litera lub cyfra; group-email i mobile-push są zastrzeżone), rodzaj, opóźnienie eskalacji (0–1440 minut), adres HTTPS bez nazwy użytkownika i hasła lub klucz integracji PagerDuty (20–64 liter i cyfr), opcjonalny sekret podpisu webhooka (do 256 znaków).

WYNIK OPERACJI

Audytowana, wersjonowana konfiguracja wysyłki organizacji i rzeczywiste doręczanie wiadomości do grup oraz alertów. Hasła, adresy kanałów, klucze integracji i sekrety podpisu są przechowywane w postaci zaszyfrowanej, nigdy nie są ponownie wyświetlane i nie trafiają do dziennika ani logów; pozostaw pole sekretu puste, aby zachować zapisaną wartość, albo wybierz Usuń zapisane hasło lub Usuń zapisany

sekret podpisu, aby ją usunąć. Przekaźnik SMTP wysyła też e-mail konfiguracji aplikacji uwierzytelniającej dla użytkowników utworzonych w Bezpieczeństwie i dostępie, od razu i tylko do tej osoby. Bez włączonego przekaźnika konsola pokazuje zamiast tego link konfiguracyjny do skopiowania.

UPRAWNIENIA

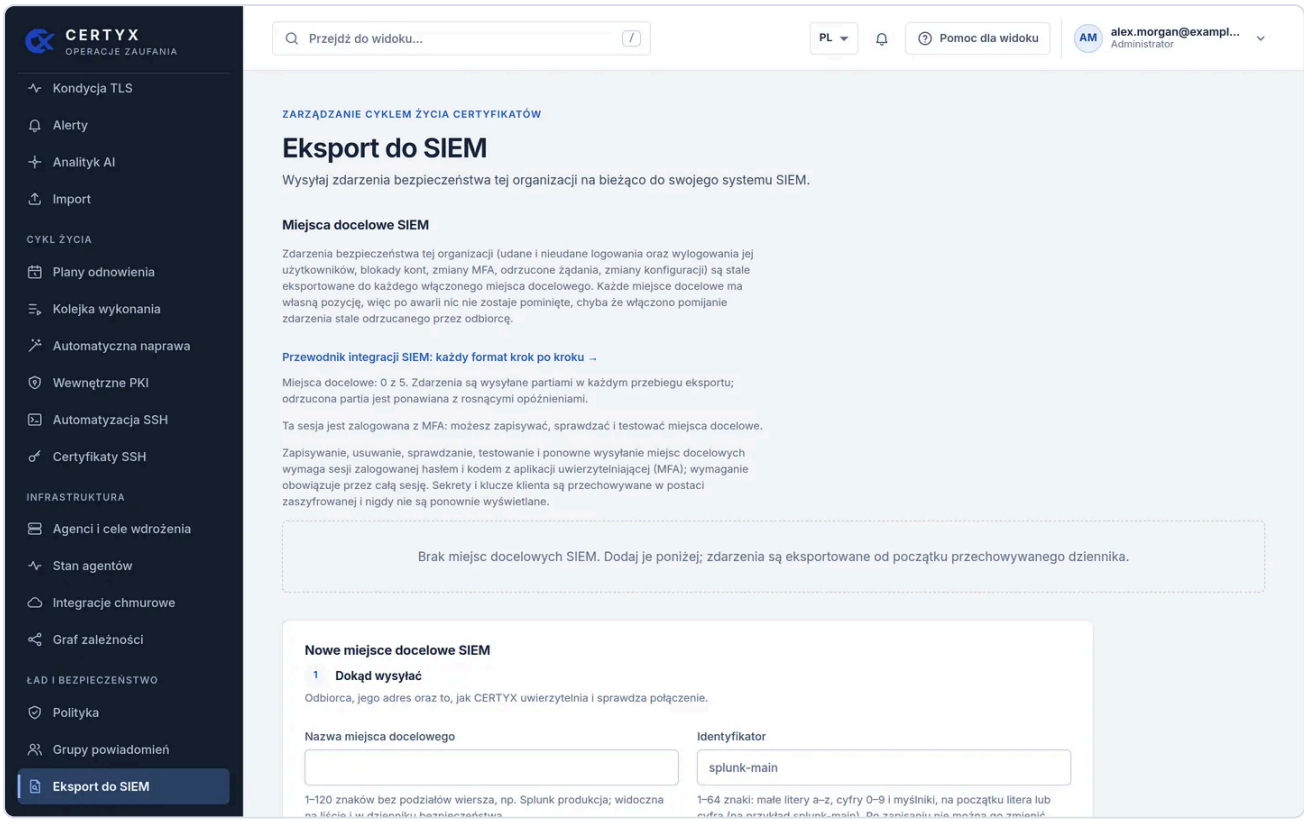
Administrator tworzy, zmienia, archiwizuje i przywraca grupy odbiorców, zmienia i testuje przekaźnik SMTP (który wyłącza się zamiast usuwać) oraz dodaje, zmienia, testuje i usuwa kanały powiadomień; pozostałe zalogowane role je odczytują. Grupy odbiorców są archiwizowane zamiast usuwane, aby certyfikaty i dziennik nadal mogły się do nich odwoływać.

OGRANICZENIA

Doręczanie odbywa się co najmniej raz: przekaźnik lub kanał, który przyjął wiadomość tuż przed awarią, może otrzymać ją ponownie (identyfikują ją X-CLM-Event-Id i X-Certyx-Event-Id). Nieudane wiadomości są ponawiane z rosnącym odstępem (najwyżej godzina) i po 10 próbach oznaczane jako niedostarczalne. Organizacja może zdefiniować najwyżej Clm:Notifications:MaxChannelsPerOrganization kanałów powiadomień (domyślnie 20). Niejawny TLS (SMTPS, port 465), uwierzytelnianie SMTP OAuth2 i certyfikaty klienta SMTP nie są obsługiwane. Ustawienia skopiowane jednorazowo z konfiguracji serwera są oznaczone; później obowiązują wartości zapisane tutaj. Wiadomości w kolejce zachowują adresatów z chwili dodania, z pominięciem osób usuniętych od tego czasu z grupy. Usunięcie kanału anuluje jego niedostarczone wiadomości. Ustawienia wysyłki, kolejka i jej historia wymagają bazy danych organizacji; bez niej są niedostępne. Odbiorcy z listy blokad e-mail platformy są pomijani: e-mail grupowy, którego wszyscy odbiorcy są zablokowani, jest anulowany z tą przyczyną, a wiadomość testowa lub e-mail konfiguracyjny na zablokowany adres nie jest wysyłany.

20 Eksport do SIEM

Wysyłaj zdarzenia bezpieczeństwa tej organizacji na bieżąco do swojego systemu SIEM.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Zaloguj się jako administrator organizacji hasłem i kodem z aplikacji uwierzytelniającej (MFA). Na górze widoku widać, czy ta sesja spełnia wymaganie MFA; jeśli nie, formularz oraz przyciski Sprawdź połączenie, Wyślij zdarzenie testowe, Wyślij ponownie od..., Nowy sekret i Usuń są wyłączone, a komunikat mówi dokładnie, co zrobić (na przykład: otwórz Profil, dokończ Włącz MFA bieżącym 6-cyfrowym kodem i zaloguj się ponownie z kodem). Wymaganie obowiązuje przez całą sesję; nie ma okna czasowego.
2. Dodaj miejsce docelowe z nazwą i identyfikatorem (1–64 małe litery, cyfry i myślniki, niezmienny po zapisaniu), a następnie wybierz Transport (HTTPS, Splunk HTTP Event Collector, Syslog przez TLS, Azure Monitor Logs Ingestion dla Microsoft Sentinel, OpenTelemetry Logs (OTLP/HTTP) albo Archiwum plików na serwerze), Format i Profil schematu. Oferowane są tylko formaty i profile, na które serwer pozwala dla wybranego transportu: HTTPS wysyła rekord JSON (pola dziennika CERTYX) lub NDJSON (zdarzenie kanoniczne); Splunk HEC rekord JSON lub NDJSON; Syslog przez TLS syslog RFC 5424 z danymi strukturalnymi, CEF, LEEF 1.0, LEEF 2.0, klucz=wartość (Generic KV), rekord JSON albo układy CEF i LEEF pierwszego wydania; Azure Monitor wiersze tabeli Microsoft Sentinel; archiwum plików CSV (kanoniczne lub w układzie pierwszego wydania) albo NDJSON. NDJSON i RFC 5424 oferują profile Natywne zdarzenie CERTYX, OCSF 1.1.0 (zweryfikowana klasa) i ECS 8.11.0, a Splunk HEC z NDJSON dodatkowo Pola Splunk CIM; pozostałe formaty używają zdarzenia natywnego. Ramka Czego potrzebuje strona odbierająca podaje ustawienia odbiorcy dla wybranego transportu i formatu; każde pole opisuje oczekiwany format, a odrzucone dane wskazują pole. Odznaczenie Eksportuj do tego

miejsca docelowego wstrzymuje miejsce docelowe bez utraty jego pozycji. Miejsca docelowe zapisane przed tym wydaniem wysyłają to samo co wcześniej (plus identyfikator zdarzenia): przy edycji wybrane są transport, format i profil, które odpowiadają ich dawnemu rodzajowi.

3. Konfiguracja każdego formatu krok po kroku, po stronie odbiorcy i w CERTYX, jest w przewodniku integracji SIEM: Splunk HTTP Event Collector (token, indeks, sourcetype, certyfikat), Cribl Stream (źródło syslog TLS, trasa i indeks), wejście Splunk TCP-SSL z ramkowaniem znakiem nowej linii, IBM QRadar (Universal LEEF, TLS Syslog), ArcSight (SmartConnector Syslog NG Daemon z TLS), Microsoft Sentinel (punkt końcowy i reguła zbierania danych, kolumny tabeli, aplikacja Entra z rolą Monitoring Metrics Publisher) oraz odbiorcy webhooków z kodem weryfikacji podpisu. Każde pole i ramka Czego potrzebuje strona odbierająca prowadzą do właściwej sekcji, nieudany etap sprawdzenia — do sposobu naprawy, a strona przewodnika udostępnia tę samą treść jako PDF po angielsku, niemiecku i polsku (także w Dokumentacji).
4. Zdarzenia logowania: zaznacz Zdarzenia logowania (logowanie, wylogowanie, blokada, zmiany MFA) w polu Eksportowane wyniki albo pozostaw wszystkie pola niezaznaczone. Miejsca docelowe organizacji otrzymują wtedy każde udane i nieudane logowanie jej użytkowników (hasło, hasło z MFA lub kodem odzyskiwania, logowanie firmowe OIDC lub SAML, aplikacja mobilna), wylogowania (także sesje zakończone przez wygaśnięcie, zmianę hasła lub wylogowanie u dostawcy tożsamości), blokady kont oraz rozpoczęcie, potwierdzenie i reset MFA przez administratora oraz wygenerowanie nowych kodów odzyskiwania. Każde zdarzenie zawiera adres e-mail użytkownika, adres IP źródła, agenta użytkownika, metodę, wynik (powodzenie lub niepowodzenie) i stały kod przyczyny; wpisane hasło ani kod nigdy nie są wysyłane.
5. Splunk: wybierz transport Splunk HTTP Event Collector. W Splunk włącz HEC (Global Settings: All Tokens Enabled, Enable SSL, port 8088), utwórz token, którego Allowed indexes zawierają indeks docelowy, a następnie wpisz https://<host-splunk>:8088/services/collector/event, wartość tokenu, indeks (na przykład clm) i opcjonalnie sourcetype. Format Rekord JSON używa domyślnego sourcetype certyx:security; NDJSON (zdarzenie kanoniczne, profil natywny, OCSF, ECS lub Pola Splunk CIM) używa certyx:event i przenosi event_id jako pole indeksowane; ustaw dla tego sourcetype KV_MODE = json w props.conf. Certyfikat HEC musi być wystawiony na nazwę hosta (domyślny certyfikat Splunk SplunkServerDefaultCert jest odrzucany); prywatne CA wklej w polu Zaufane certyfikaty główne.
6. Syslog przez TLS: wpisz samą nazwę hosta i port oraz wybierz ramkowanie: zliczanie oktetów (RFC 5425; źródło Syslog w Cribl, syslog-ng, rsyslog, QRadar, ArcSight) lub nowa linia (wejście Splunk [tcp-ssl:<port>]). Wejście odbierające musi używać TLS. Dla LEEF 2.0 wpisz Separator LEEF (jeden znak, np. ^, lub jego kod szesnastkowy, np. x5E; puste oznacza TAB) i użyj tego samego separatora w źródle logów QRadar; LEEF 1.0 zawsze używa TAB. Wiersz pod ramkowaniem pokazuje nagłówek syslog ustawiony przez operatora serwera (facility, APP-NAME i numer przedsiębiorstwa IANA; bez numeru element danych strukturalnych certyx@ nie jest wysyłany). Przy Cribl indeks (na przykład clm) ustawia się w trasie lub potoku Cribl, nie w CERTYX.
7. HTTPS (POST tablicy JSON lub NDJSON, HMAC-SHA256 treści w X-Certyx-Signature) i Azure Monitor Logs Ingestion dla Microsoft Sentinel (punkt zbierania danych, niezmienny identyfikator i strumień reguły zbierania danych, dzierżawa Microsoft Entra, identyfikator aplikacji i klucz tajny klienta) korzystają z tego samego formularza. Dla miejsca docelowego HTTPS dodanego bez sekretu CERTYX generuje sekret podpisu i pokazuje go jeden raz do skopiowania do odbiorcy; Nowy sekret przy miejscu docelowym HTTPS natychmiast go zastępuje (poprzedni przestaje działać) i pokazuje nowy jeden raz.
8. OpenTelemetry Logs (OTLP/HTTP): wybierz transport OpenTelemetry Logs i format OTLP protobuf (application/x-protobuf, domyślny dla OTLP/HTTP) albo OTLP/JSON, wpisz pełny adres dzienników odbiorcy (tylko https, na przykład https://collector.example.com:4318/v1/logs dla OpenTelemetry

Collector), Treść (Body) rekordu dziennika (komunikat albo całe zdarzenie kanoniczne jako lista klucz-wartość), opcjonalnie Nazwę nagłówka uwierzytelniania (puste oznacza Authorization) i jego wartość jako sekret (na przykład Bearer <token>; przechowywana w postaci zaszyfrowanej, nigdy ponownie niewyświetlana) oraz Kompresuj żądania gzip. Każda partia to jedno ExportLogsServiceRequest: zasób service.name certyx, service.version, deployment.environment.name, host.name, host.ip i certyx.organization.id/name/kind; jeden rekord na zdarzenie z Timestamp, ObservedTimestamp, SeverityNumber/SeverityText (niska INFO 9, średnia WARN 13, wysoka ERROR 17, bardzo wysoka FATAL 21), Body, TraceId i SpanId żądania oraz atrybutami (konwencje semantyczne 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 i pozostałe pola certyx.*). TLS, zaufane certyfikaty główne, certyfikat klienta (mTLS), sprawdzanie odwołania, zasady dostarczania, filtry, sprawdzenie i zdarzenie testowe działają jak w pozostałych transportach HTTPS; częściowy sukces z odrzuconymi rekordami nie jest wysyłany ponownie (specyfikacja OTLP), lecz zapisywany w dzienniku jako siem.event.rejected z identyfikatorami zdarzeń żądania i komunikatem odbiorcy, z incydentem siem-rejected; Wyślij ponownie od wysyła rekordy jeszcze raz. Retry-After przy 429 lub 503 jest respektowany do najdłuższego opóźnienia.

9. Mapowanie pól (sieciowe miejsca docelowe z formatem kanonicznym: NDJSON, RFC 5424, CEF, LEEF, Generic KV, OTLP): Dodaj regułę dodaje uporządkowaną regułę na zdarzeniu kanonicznym przed jego zapisaniem: Zmień nazwę (pole kanoniczne pod nową nazwą), Usuń (lista zabronionych), Zachowaj (lista dozwolonych: przy co najmniej jednej regule Zachowaj każde inne pole opcjonalne jest usuwane) albo Dodaj stałą (nowe pole ze stałą wartością o długości najwyżej 256 znaków). event_id, schema_version, trzech znaczników czasu, event_code, category, action, outcome, severity i message nie można usunąć ani przemianować; nowa nazwa ma 1–64 litery, cyfry, podkreślenia i kropki (CEF tylko litery i cyfry, ECS i OCSF bez kropek), nie może zaczynać się od certyx ani być równa polu kanonicznemu lub polu zapisywanemu przez sam format (na przykład dst w CEF albo server.address w OTLP). Nowe pola następują po własnych polach formatu: w treści JSON, pod labels w ECS, pod unmapped w OCSF, jako rozszerzenia w CEF i LEEF, jako klucze w KV i jako atrybuty w OTLP. Najwyżej 32 reguły; są zapisywane, wersjonowane i rejestrowane w dzienniku razem z miejscem docelowym (przed i po). Podgląd zdarzenia testowego pokazuje, co formularz w obecnym stanie wysłałby jako zdarzenie testowe w wybranym formacie i kodowaniu (OTLP protobuf w kodowaniu JSON, z rozmiarem binarnej treści); nic nie jest wysyłane ani zapisywane, a nieprawidłowe reguły są odrzucane z podaniem przyczyny.
10. Zapisz, a następnie wybierz Sprawdź połączenie (DNS, TCP i TLS bez wysyłania czegokolwiek; dla archiwum plików — czy do jego katalogu można zapisywać) oraz Wyślij zdarzenie testowe. Każdy etap jest pokazany z wynikiem: rozwiązane adresy, połączony adres i port, wersja TLS oraz podmiot, wystawca i ważność certyfikatu, a potem status HTTP lub kod Splunk HEC ze znaczeniem i zaleceniem. Zdarzenie testowe należy do kategorii Integracja i ma losowy UUID jako event_id, który podaje wynik; wyszukaj u odbiorcy ten identyfikator zdarzenia (wykonawca siem-test). Archiwum plików nie ma zdarzenia testowego.
11. Lista pokazuje dla każdego miejsca docelowego transport, format i profil, pozycję w dzienniku, oczekujące i dostarczone zdarzenia, ostatni sukces, przyczynę ostatniego błędu, kolejne niepowodzenia i czas następnej próby, zdarzenie stale odrzucane przez odbiorcę (sekwencja i liczba prób) oraz ostatnie sprawdzenie. Edytuj wczytuje miejsce docelowe do formularza: puste pole sekretu lub klucza klienta zachowuje zapisaną wartość, ale zmiana transportu wymaga ponownego wpisania sekretu. Usuń kasuje miejsce docelowe wraz z jego pozycją; ponowne dodanie zaczyna od początku dziennika. Miejsca docelowe skonfigurowane dla organizacji przez operatora platformy są widoczne tylko do odczytu. Każda karta pokazuje też zapisaną konfigurację: transport, format i profil, cel,

ramkowanie i separator, wysyłane zdarzenia, zasady dostarczania (wartości domyślne serwera oznaczone jako takie), ustawienia Splunk i Sentinel, certyfikaty główne, certyfikat klienta, sprawdzanie odwołania oraz to, czy zapisano sekret. Po otwarciu widoku formularz pokazuje pierwsze miejsce docelowe z zapisanymi wartościami; zapisany sekret ani klucz klienta nigdy nie są wyświetlane i występują jako „Zapisane – pozostaw puste, aby zachować". Edytuj otwiera inne miejsce docelowe, Nowe zaczyna pusty formularz, a po zapisaniu formularz pozostaje przy zapisanym miejscu docelowym.

12. Wysyłaj tylko ogranicza to, co otrzymuje sieciowe miejsce docelowe, aby zmniejszyć zużycie licencji SIEM: zaznaczone wyniki łączy „lub" (na przykład Odmowy dostępu, Błędy serwera, Zdarzenia logowania oraz Zmiany konfiguracji i biznesowe, które dodaje każde zdarzenie ze zmianą konfiguracji lub biznesową). Kategorie (Uwierzytelnianie, Autoryzacja, Zarządzanie użytkownikami, Zmiana konfiguracji, Dostęp do danych, Administracja, Bezpieczeństwo, Błąd aplikacji, System, Integracja) i wybrane kody z katalogu kodów zdarzeń łączy między sobą „lub" i dodatkowo zawężają wybór wyników. Minimalna ważność wysyła tylko zdarzenia o wybranej lub wyższej ważności (odebrane 2, sukces 3, odrzucenie 5, odmowa i nieudane logowanie 7, błąd serwera i blokada 8). Każde żądanie ma w dzienniku dwa rekordy: odebrane żądanie (zapis przed wykonaniem, nie nieudana próba) i wynik po nim; miejsce docelowe otrzymuje tylko wynik, chyba że zaznaczono Odebrane żądania. Rekord odebranego żądania pozostaje w dzienniku i w archiwum plikowym. Wysyłane pola (w sekcji kształtu i rozmiaru) wypisują każde pole wybranego formatu z polem wyboru, więc miejsce docelowe otrzymuje dokładnie zaznaczone pola i licencja SIEM nie liczy nic więcej; włączone zostają tylko pola wymagane przez format, a zgodnościowe układy CEF i LEEF pierwszego wydania są stałe, więc tam ustaw format CEF lub LEEF. Sondy health i readiness nie są wysyłane. Pominięte zdarzenia nie giną: pozostają w dzienniku i w archiwum plików.
13. Formularz miejsca docelowego ma cztery numerowane sekcje: 1 Dokąd wysyłać (nazwa, transport, format, adres, sekret, TLS), 2 Co wysyłać (wyniki, kategorie, kody zdarzeń, ważność i zwinięte Więcej filtrów), 3 Kształt i rozmiar zdarzenia (karty gotowych ustawień, zwinięte Ustawienia szczegółowe i Mapowanie pól) oraz 4 Dostarczanie (zwinięte zasady dostarczania, Eksportuj do tego miejsca docelowego). Zwinięte części otwierają się po kliknięciu ich tytułu.
14. Więcej filtrów: Wysyłaj tylko te trasy i Nigdy nie wysyłaj tych tras (jedna w wierszu; trasa obejmuje każdą trasę, która od niej się zaczyna, np. /agent/v1/discovery/telemetry dla regularnych raportów agentów), Nigdy nie wysyłaj zdarzeń tych aktorów (np. pending, żądania przed uwierzytelnieniem), Nigdy nie wysyłaj tych kategorii i Nigdy nie wysyłaj tych kodów zdarzeń. Wykluczenie zawsze wygrywa.
15. Kształtowanie zdarzeń decyduje, jak duże jest każde zdarzenie, bo wiele systemów SIEM rozlicza licencję od indeksowanej ilości danych: Pełne wysyła każde pole i pełny stan przed i po każdej zmianie (jak dotąd); Zrównoważone wysyła tylko zmienione wartości, bez pustych pól, z polami standardowymi; Oszczędne wysyła akcję i identyfikatory zmiany, pola minimalne i najwyżej 2 KB na zdarzenie; Własne używa ustawień szczegółowych. Gotowe ustawienie wypełnia Ustawienia szczegółowe; zmiana któregoś z nich wybiera Własne. Ustawienia szczegółowe: Zmiany (pełne, tylko zmienione wartości, akcja i identyfikatory, brak), Pola (wszystkie, standardowe, minimalne; pola wymagane są wysyłane zawsze), Pomijaj puste pola, Największe zdarzenie (0 albo 512–1048576 bajtów; dłuższe zdarzenie traci szczegóły zmian, potem skracane są jego najdłuższe teksty i jest oznaczane jako skrócone), Styl nazw pól i Format czasu (tylko dokumenty JSON profilu natywnego lub Splunk CIM), MSGID syslog (domyślnie kategoria zdarzenia, kod zdarzenia, własny tekst, np. security-journal, albo brak) i APP-NAME syslog (puste to clm). Podgląd zdarzenia testowego pokazuje rozmiar z kształtowaniem i bez niego. Zmierzone na obserwacji trzech certyfikatów przez agenta (json): Pełne 4578 bajtów, Zrównoważone 591, Oszczędne 378.

16. Zasady dostarczania (sieciowe miejsca docelowe): Próby przed alertem krytycznym, Pierwsze i Najdłuższe opóźnienie ponowienia (sekundy), Rozmiar partii i Alert zaległości powyżej; puste pole oznacza wartość domyślną serwera pokazaną pod polami. Nieudana partia jest ponawiana z wykładniczym wycofaniem i losowym rozrzutem; po wyczerpaniu prób incydent siem-delivery staje się krytyczny, a ponawianie trwa dalej. Partię odrzuconą przez odbiorcę z powodu treści CERTYX dzieli aż do pojedynczego odrzuconego zdarzenia; wszystko przed nim jest dostarczane, a to zdarzenie jest ponawiane i zgłaszane. Pomiń zdarzenie, które odbiorca nadal odrzuca, jest domyślnie wyłączone; po włączeniu zdarzenie jest pomijane po wyczerpaniu prób i zapisywane w dzienniku jako siem.event.skipped z jego event_id. Zaległości niczego nie usuwają: kolejką jest dziennik, a powyżej limitu zaległości zgłaszany jest incydent siem-backlog.
17. TLS sieciowych miejsc docelowych: certyfikat odbiorcy jest zawsze weryfikowany względem systemowego magazynu zaufania albo wpisanych tu Zaufanych certyfikatów głównych. Dla wzajemnego TLS wpisz Certyfikat klienta (PEM) z jego niezaszyfrowanym kluczem prywatnym (RSA lub EC); klucz jest przechowywany w postaci zaszyfrowanej, nigdy nie jest ponownie wyświetlany, a puste pole klucza zachowuje zapisany klucz, dopóki certyfikat się nie zmienia. Sprawdzanie odwołania: Soft-fail (domyślnie) odrzuca certyfikat zgłoszony jako odwołany i akceptuje nieznany status (brak adresu CRL lub OCSP, niedostępny responder); Hard-fail odrzuca także nieznany status.
18. Wyślij ponownie od... na karcie sieciowego miejsca docelowego otwiera okno: wybierz sekwencję dziennika (1 lub więcej) albo datę i godzinę, przeczytaj, że każde zdarzenie od tego miejsca zostanie wysłane ponownie, i potwierdź przyciskiem Wyślij ponownie. Pozycja cofa się tuż przed ten punkt, stan wycofania i odrzuconego zdarzenia jest czyszczony, a komunikat podaje nową pozycję; odbiorca musi usuwać duplikaty według event_id. Pozycja nigdy nie przesuwa się do przodu (punkt, do którego miejsce docelowe jeszcze nie doszło, jest odrzucany), archiwum plików nie może wysyłać ponownie, a każde ponowne wysłanie jest zapisywane w dzienniku (siem.destination.replayed) z poprzednią i nową pozycją.
19. Ramkowanie syslog musi być takie samo po obu stronach. Zliczanie oktetów wysyła każdy rekord jako <długość> <komunikat> (długość w bajtach UTF-8, bez znaku nowej linii) jednym zapisem; źródło syslog w Cribl wymaga wtedy Octet count framing = Yes (domyślnie No) i włączonego TLS, jednego źródła na port CERTYX, a indeks i sourcetype ustawia funkcja Eval. Odbiorca dzielący na znakach nowej linii pokazuje fragmenty typu 412 <84>1 ...; odbiorca bez TLS pokazuje binarne zdarzenia zaczynające się od \x16\x03 i zawierające jego własną nazwę hosta. Udany test syslog podaje, co wejście odbierające musi zrobić przy wybranym ramkowaniu.
20. Archiwum plików: wybierz transport Archiwum plików na serwerze (pliki dzienne) i format: CSV (układ pierwszego wydania, certyx-security-RRRR-MM-DD.csv), CSV (zdarzenie kanoniczne, certyx-events-RRRR-MM-DD.csv z wersjonowanym nagłówkiem) lub NDJSON (jeden dokument wybranego profilu na wiersz, certyx-events-RRRR-MM-DD.ndjson). Wpisz Okres przechowywania (dni, 1–3650), opcjonalnie zaznacz Kompresuj zamknięte dni gzip, zapisz i wybierz Sprawdź połączenie, które sprawdza, czy do katalogu archiwum można zapisywać, i pokazuje pliki oraz zajęte i wolne miejsce. Archiwum zapisuje każde zdarzenie organizacji do jednego pliku na dobę UTC we własnym obszarze organizacji pod katalogiem archiwum skonfigurowanym przez operatora platformy; filtry, zasady dostarczania, certyfikat klienta i sprawdzanie odwołania nie mają zastosowania. Zamknięty dzień jest pieczętowany (opcjonalnie .gz) z sumą SHA-256 w manifeście SHA256SUMS, a dni starsze niż okres przechowywania są usuwane i zapisywane w dzienniku (siem.archive.expired).
21. Pliki archiwum na karcie archiwum pokazują każdy plik z rozmiarem, stanem zapieczętowania i SHA-256; Pobierz pobiera jeden plik, Pobierz wszystkie (zip) wszystkie pliki z manifestem. Pobrane pliki sprawdzisz poleceniem sha256sum -c SHA256SUMS. Pobieranie wymaga sesji z MFA i jest

zapisywane w dzienniku (siem.archive.downloaded).

DANE I PARAMETRY

- Eksportowane pola: sekwencja, czas, kategoria i kod zdarzenia, organizacja, wykonawca, adres IP źródła, odcisk agenta, metoda, ścieżka, status HTTP, wynik, identyfikator żądania, typ błędu, zmiany biznesowe i skrót zdarzenia, który identyfikuje wpis w łańcuchu skrótów dziennika CERTYX.
- Mapowanie CEF: rt, suser, src, requestMethod, request, outcome, externalId (sekwencja), dvchost (instancja), cn1 httpStatus, cs1 organization, cs2 traceId, cs3 eventHash, cs4 agentFingerprint, cs5 errorType, cs6 changes; ważność 2–8 zależnie od wyniku. LEEF 2.0 przenosi te same wartości jako devTime, usrName, src, cat, sev, method, resource, httpStatus, organization, traceId, sequence, eventHash, agentFingerprint, errorType, instance i changes z separatorem ^.
- Zdarzenia logowania (wynik authentication) to osobne wpisy dziennika o nazwach authentication.sign-in.succeeded, authentication.sign-in.failed, authentication.sign-out, authentication.locked, authentication.mfa.enrolled, authentication.mfa.confirmed, authentication.mfa.reset i authentication.mfa.recovery-codes-regenerated. Metody: password, password+mfa, password+recovery-code, oidc, saml, mobile-password (z +mfa lub +recovery-code), mobile-oidc, mobile-saml, mobile-sso i totp. Kody przyczyn to m.in. 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, a dla wylogowań user, credentials-changed, idp-logout, session-ended i administrator-reset.
- Pola logowania w poszczególnych formatach: rekord JSON (webhook, syslog JSON, zdarzenie Splunk HEC) dodaje SignIn {Action, User, UserVerified, Organization, Method, Result, Reason, UserAgent}; CEF używa nazwy zdarzenia jako identyfikatora klasy, suser = e-mail użytkownika, suid = konto, src, outcome = success lub failure, cat = authentication, act = nazwa zdarzenia, reason, requestClientApplication = agent użytkownika, flexString1 authMethod i flexString2 userVerified, z ważnością 3 dla powodzenia, 7 dla niepowodzenia i 8 dla blokady; LEEF używa usrName = e-mail użytkownika, src, actor, action, authMethod, result, reason, userAgent i userVerified; Sentinel dodaje kolumny User, UserVerified (boolean), UserOrganization, AuthAction, AuthMethod, AuthResult, Reason i UserAgent.
- Microsoft Sentinel: kolumny strumienia to TimeGenerated, Sequence, Organization, Actor, SourceIp, AgentFingerprint, Method, Route, Status, Outcome, TraceId, ErrorType, Instance, EventHash i Changes oraz wymienione wyżej kolumny logowania (reguła, która ich nie deklaruje, zapisuje tylko pozostałe kolumny); aplikacja potrzebuje roli Monitoring Metrics Publisher na regule zbierania danych.
- Żądanie Splunk HEC: POST z Authorization: Splunk <token>, X-Splunk-Request-Channel (stały GUID dla miejsca docelowego) i sklejonymi kopertami {time, host, source certyx:security-journal, sourcetype, index, event}. Gdy token ma włączone indexer acknowledgement, CERTYX odpytuje /services/collector/ack, aż Splunk potwierdzi indeksowanie (Clm:Siem:HecAckTimeout, domyślnie 30 sekund); niepotwierdzona partia jest wysyłana ponownie.
- Identyfikacja organizacji w każdym formacie: JSON, Splunk HEC i syslog JSON zawierają Tenant (identyfikator organizacji), OrganizationName, OrganizationKind (organization, platform lub unattributed) i Instance; CEF dodaje certyxOrganizationName i certyxOrganizationKind obok cs1 organization i dvchost; LEEF dodaje organizationName i organizationKind; Sentinel dodaje kolumny

OrganizationName i OrganizationKind. Nazwa i rodzaj są dodawane przy eksporcie; wpis dziennika powiązany łańcuchem skrótów pozostaje bez zmian. HOSTNAME RFC 5424 komunikatów syslog to identyfikator instancji CERTYX, która zapisała zdarzenie.

- Kolumny archiwum CSV: Sequence, At, OrganizationId, OrganizationName, OrganizationKind, Instance, Actor, SourceIp, AgentFingerprint, Method, Route, Status, Outcome, Severity, TraceId, ErrorType, SignInAction, SignInUser, SignInMethod, SignInResult, SignInReason, Changes, PreviousHash i Hash; UTF-8, wiersz nagłówka, komórki w cudzysłowach, końce wierszy CRLF; komórka zaczynająca się od = + - @, tabulatora lub powrotu karetki dostaje apostrof na początku, aby arkusze kalkulacyjne pokazywały ją jako tekst.
- Zdarzenie kanoniczne (NDJSON, CEF, LEEF 1.0/2.0, KV, RFC 5424, kanoniczny CSV): event_id (<identyfikator instalacji>:<sekwencja>; UUID dla zdarzeń testowych), event_code z katalogu kodów zdarzeń, kategoria, akcja, wynik, ważność 0–10, czas, organizacja, wykonawca, adres IP źródła i szczegóły żądania; profile OCSF 1.1.0 (Authentication 3002, Account Change 3001, API Activity 6003, w przeciwnym razie Base Event 0, gdy brakuje wymaganych atrybutów klasy), ECS 8.11.0 i Pola Splunk CIM (modele danych Authentication i Change jako indeksowane pola HEC) odwzorowują to samo zdarzenie. Rekord JSON, wiersze Sentinel i układy pierwszego wydania zachowują swoje pola i dodają identyfikator zdarzenia.
- Pola wzbogacenia trace_id, span_id, src_port, host_ip, dst_ip, dst_port, user_role i session_id są wypełnione dla wpisów dziennika zapisanych od tego wydania (span_id i dst_port od wydania z OTLP); starsze wpisy wysyłają je puste.
- Adres docelowy dst_ip i dst_port: dla żądania adres i port serwera, które przyjęły połączenie (nasłuch serwera CERTYX; za odwrotnym proxy lub w sieci kontenerów jest to adres i port lokalnego interfejsu, a nie nazwa publiczna, bo przekazywany nagłówek hosta może ustawić klient), dla zdarzenia agenta lub punktu końcowego obserwowany cel podany w zdarzeniu (na przykład punkt końcowy alertu wykrywania); w przeciwnym razie nieznany. Mapowanie: CEF dst/dpt, LEEF dst/dstPort, ECS destination.ip/port, OCSF dst_endpoint, Splunk CIM dest/dest_port, OTLP server.address/port oraz dst_ip/dst_port w KV, CSV i NDJSON.

WYNIK OPERACJI

Ciągły eksport zdarzeń organizacji (co najmniej raz) z trwałą pozycją dla każdego miejsca docelowego oraz diagnostyka etap po etapie. Sekrety (klucz HMAC, token HEC, klucz tajny klienta) i klucze klienta są przechowywane w postaci zaszyfrowanej, nigdy nie są ponownie wyświetlane i nie trafiają do dziennika; każda zmiana, sprawdzenie, test i ponowne wysłanie są zapisywane w dzienniku bezpieczeństwa (siem.destination.created, updated, deleted, checked, tested, secret-rotated, replayed), a pominięte odrzucone zdarzenie jako siem.event.skipped z jego event_id. Archiwum plików przechowuje pełny zapis na serwerze przez swój okres przechowywania, z manifestem SHA-256 każdego zamkniętego dnia, dzięki czemu SIEM może otrzymywać mniej (Wysyłaj tylko).

UPRAWNIENIA

Administrator organizacji, którego sesja została zalogowana z MFA: konto lokalne z potwierdzoną aplikacją uwierzytelniającą albo logowanie firmowe, dla którego dostawca tożsamości zgłasza MFA (lub organizacja deklaruje, że dostawca je wymusza). Inne role nie widzą tego widoku. Zmiany, sprawdzenia, testy, ponowne wysłania i nowe sekrety są odrzucane dla sesji aplikacji mobilnej CERTYX.

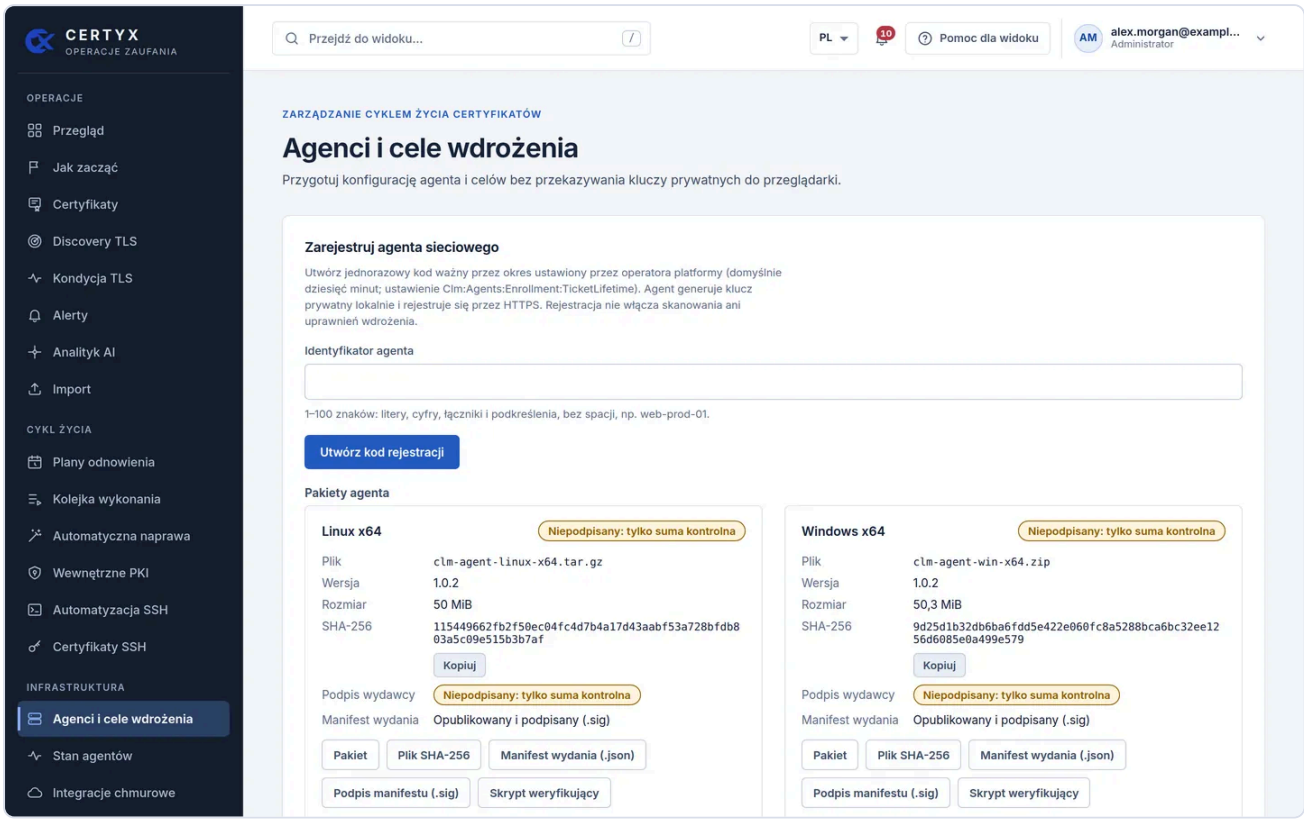
OGRANICZENIA

Wymaga bazy platformy, w której jest dziennik bezpieczeństwa; w przeciwnym razie widok informuje, że eksport jest niedostępny. Najwyżej Clm:Siem:MaxDestinationsPerOrganization miejsc docelowych (domyślnie 5). Doręczanie odbywa się co najmniej raz: odrzucona partia jest ponawiana z wykładniczym wycofaniem i losowym rozrzutem (przebiegi eksportu co Clm:Siem:Interval, domyślnie 30 sekund), a ponowne wysłanie wysyła zdarzenia jeszcze raz, dlatego odbiorca musi usuwać duplikaty według event_id (<identyfikator instalacji>:<sekwencja>; UUID dla zdarzeń testowych). Certyfikaty TLS są zawsze weryfikowane; certyfikat klienta jest przedstawiany tylko wtedy, gdy został wpisany, a sprawdzanie odwołania w trybie soft-fail akceptuje nieznany status, natomiast hard-fail go odrzuca. Sentinel używa publicznej chmury Microsoft Entra, chyba że operator ustawi Clm:Siem:SentinelAuthorityHost. Nowe miejsce docelowe zaczyna od początku przechowywanego dziennika organizacji. Syslog nie potwierdza dostarczenia: udany test syslog dowodzi tylko DNS, TCP, TLS i zapisu, więc trasowanie i indeks trzeba sprawdzić u odbiorcy. Zwykły syslog TCP i UDP nie jest obsługiwany. Nieudany etap (nazwa nierozwiązywalna na serwerze CERTYX, połączenie odrzucone lub porzucone, uzgadnianie TLS, nazwa lub zaufanie certyfikatu, status HTTP lub kod HEC) jest pokazywany z zaleceniem i zapisywany jako ostatnie sprawdzenie. Miejsca docelowe pod adresami prywatnymi, pętli zwrotnej lub link-local (na przykład wewnętrzny odbiornik Splunk lub Cribl) są domyślnie dozwolone (Clm:Siem:AllowPrivateDestinations, domyślnie true). Operator serwera współdzielonej instalacji może ustawić tę opcję na false, aby ograniczyć miejsca docelowe organizacji do publicznych adresów unicast: każdy adres, na który rozwiązuje się host, musi być wtedy publiczny (odrzucane są zakresy prywatne, pętli zwrotnej, link-local, współdzielony 100.64.0.0/10, dokumentacyjne, testowe, multicast i nieglobalne zakresy IPv6), połączenie idzie na sprawdzony adres, a przekierowania nie są wykonywane. Sprawdzenie kończy się wtedy na etapie DNS z informacją, że adres jest prywatny, a eksport do tego miejsca kończy się błędem z tą samą przyczyną (incydent siem-delivery, pozycja bez zmian), dopóki nie zostanie użyty adres publiczny. Opcja nigdy nie ogranicza miejsc docelowych operatora platformy ani zdefiniowanych w konfiguracji serwera. Zdarzenia logowania należą do organizacji konta lub logowania firmowego; nieudane logowanie, którego adres e-mail nie pasuje do żadnego konta, jest przypisywane organizacji, do której należy zweryfikowana domena logowania firmowego, a w przeciwnym razie platformie, więc ta organizacja go nie otrzymuje. Logowania zablokowane przed aplikacją (TLS, zapora, limit żądań na ingressie) nie są rejestrowane, a za serwerem proxy adresem IP źródła jest adres proxy. Archiwum CSV jest zapisywane w tempie eksportu (Clm:Siem:BatchSize zdarzeń na Clm:Siem:Interval) z tą samą trwałą pozycją: po awarii kontynuuje za ostatnim kompletnym wierszem, więc plik nigdy nie zawiera wiersza dwa razy. Zaplanuj miejsce na dysku (około 0,5–1 KB na zdarzenie bez kompresji, z gzip około jednej dziesiątej); pełny dysk, brak woluminu lub ścieżka archiwum z dowiązaniem symbolicznym powodują błąd archiwum z przyczyną na jego karcie i incydentem siem-delivery, a pozycja pozostaje bez zmian do usunięcia przyczyny. Organizacja nie może wybrać lokalizacji archiwum. Usunięcie archiwum kończy zapis; jego pliki pozostają, dopóki operator ich nie usunie. Archiwów CSV nie można zdefiniować w konfiguracji serwera. Eksport OTLP używa tylko OTLP/HTTP (bez gRPC) i jednego nagłówka uwierzytelniania; częściowy sukces nie jest wysyłany ponownie (specyfikacja OTLP): jest zapisywany w dzienniku jako siem.event.rejected z identyfikatorami zdarzeń żądania i zgłasza siem-rejected, a Wyślij ponownie od wysyła rekordy jeszcze raz po naprawie odbiorcy. Mapowanie pól dotyczy tylko formatów kanonicznych sieciowych miejsc docelowych; archiwa plików przechowują pełne zdarzenie, a formaty pierwszego wydania zachowują swój układ. Pola wzbogacenia trace_id, span_id, src_port, host_ip, dst_ip, dst_port, user_role i session_id są obecne tylko we wpisach zapisanych od tego wydania (span_id i dst_port od wydania z OTLP). Miejsca docelowe i archiwum organizacji otrzymują wyłącznie jej własne zdarzenia. Nigdy nie otrzymują zapisów platformy, także tych dotyczących tej organizacji: działań i wniosków operatorów, zawieszenia i przywrócenia z

powodu rozliczeń, udostępniania ani ponownego szyfrowania zapisanych sekretów. Organizacja czyta je w swojej konsoli, a poza system wychodzą wyłącznie przez własne zakresy platformy, które ustawia operator platformy.

21 Agenci i cele wdrożenia

Przygotuj konfigurację agenta i celów bez przekazywania kluczy prywatnych do przeglądarki.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Wpisz identyfikator agenta i wybierz „Utwórz kod rejestracji”. Konsola pokaże termin ważności kodu (jednorazowy; domyślnie dziesięć minut; operator platformy zmienia go ustawieniem Clm:Agents:Enrollment:TicketLifetime), adres, którego muszą używać agenci (skonfigurowany host i port agentów, a w przeciwnym razie adres HTTPS tej konsoli), identyfikator organizacji i ponumerowane kroki instalacji z gotowymi do skopiowania poleceniami dla Linux (systemd, x64) i Windows (x64): gdy adres agentów używa własnego CA operatora, najpierw pobierz jego certyfikat główny i sprawdź sumę SHA-256 pokazaną obok polecenia (w Linuksie kolejne pobrania w tym samym terminalu mu ufają, a instalator sam dodaje go przez CLM_AGENT_TRUST_ROOT do systemowego magazynu zaufanych certyfikatów i usuwa go ponownie, gdy sprawdzenie połączenia się nie powiedzie; w Windows krok importuje go do magazynu komputera przed pobraniem); skopiuj pobrany clm-enrollment.token do pustego katalogu roboczego na serwerze; tam pobierz pakiet (archiwum jest udostępniane tylko z ważnym kodem rejestracji, który polecenie odczytuje z pliku, albo w zalogowanej sesji konsoli przez jej własne linki; brak, wygaśnięcie lub zużycie kodu albo błędny identyfikator organizacji kończy się HTTP 401 i wymaga nowego kodu), sprawdź sumę kontrolną, zweryfikuj podpis wydawcy skryptem verify-agent-package (zastąp <PUBLISHER-SHA256> w poleceniach odciskiem certyfikatu wydawcy od dostawcy CERTYX; konsola nigdy go nie pokazuje), rozpakuj go, w katalogu clm-agent uruchom instalator z ../clm-enrollment.token (Windows ..\clm-enrollment.token) i sprawdzenie stanu (w Linux

sudo clm-agent status). Plik kodu pobierz w pierwszym kroku; kod nigdy nie jest wyświetlany. Pod krokami konsola śledzi nowego agenta: oczekiwanie na rejestrację, zarejestrowany i oczekiwanie na pierwszy kontakt, a potem „pierwszy kontakt odebrany" z godziną.

2. Zadanie SSH: ten sam agent wykonuje automatyzację SSH. Nadaj „Operacje SSH" (oraz „Wdrażanie tożsamości SSH" do instalacji) tutaj lub w Automatyzacja SSH → Instalacja i podłączenie agenta SSH, gdzie są też pliki do pobrania, polecenia dla hosta (configure-ssh-linux.sh / configure-ssh-windows.ps1 init, add-profile, trust-user-ca) i raport zadania SSH każdego agenta. sudo clm-agent status wypisuje nadane uprawnienia.
3. W sekcji „Pakiety agenta" konsola pokazuje kartę dla każdej platformy (Linux x64, Windows x64) z nazwą pliku archiwum, wersją wydania, rozmiarem, wartością SHA-256 (z przyciskiem Kopiuj), stanem podpisu wydawcy („Podpisany (opublikowano .p7s)" albo „Niepodpisany: tylko suma kontrolna") i stanem manifestu wydania oraz przyciskiem pobierania dla każdego pliku opublikowanego przez serwer: pakietu, pliku .sha256, podpisu .p7s, znacznika czasu .tsr, manifestu wydania i jego podpisu .sig oraz osobnego weryfikatora (verify-agent-package.sh lub verify-agent-package.ps1). Każdy przycisk zapisuje plik pod jego własną nazwą. Karta pokazuje, które pliki podpisów są opublikowane; nie weryfikuje ich, robi to weryfikator na hoście. Pakiet, którego operator nie opublikował, jest pokazany jako „Nieopublikowany na tym serwerze" z krokiem publikacji operatora zamiast linku. Porównaj wartość SHA-256 z karty z wynikiem sha256sum (Linux) lub Get-FileHash (Windows) dla pobranego pliku. Samo archiwum wymaga ważnego kodu rejestracji (polecenia konsoli) lub zalogowanej sesji konsoli, a sumy kontrolne, podpisy i weryfikatory są publiczne. Sprawdź go względem odcisku certyfikatu wydawcy otrzymanego od dostawcy CERTYX niezależnym kanałem; nie instaluj odrzuconego pakietu. Wykonaj podlinkowaną instrukcję instalacji i przekaż ten sam odcisk instalatorowi (CLM_AGENT_PUBLISHER_SHA256 lub -PublisherSha256); użyj zaufanego adresu HTTPS platformy.
4. Wykonaj polecenia na serwerze docelowym przed upływem pokazanego terminu: ważność obejmuje łącznie pobranie i instalację; sprawdzenie kodu przy pobieraniu go nie zużywa, zużywa go rejestracja. Instalator sprawdza każdy argument przed jakąkolwiek zmianą i wskazuje błędny razem z kolejnym krokiem (brak pliku kodu, symbol zastępczy lub adres przykładowy, adres bez HTTPS, istniejąca instalacja). Potem sprawdza połączenie bez zużywania kodu (rozwiązywanie nazwy, TCP, zaufanie TLS ze sprawdzeniem unieważnienia online, różnica zegarów, czy adres obsługuje agentów) i zatrzymuje się z przyczyną pierwszego nieudanego kroku, objaśnia błędy rejestracji (kod wygasły lub zużyty), a na końcu sprawdza, że CERTYX akceptuje nową tożsamość i zapisał jej pierwszy kontakt. Sprawdzenie stanu możesz powtórzyć w dowolnym momencie: każdy wiersz musi zaczynać się od [OK], a ostatni brzmieć „Result: connected"; wiersz [FAIL] podaje przyczynę i kolejny krok, a instrukcja instalacji opisuje każdy komunikat w sekcji Rozwiązywanie problemów. Tylko gdy operator publikuje klucz podpisywania wydań, dodaj ./release-signing.pub jako czwarty argument w Linuksie (codzienny clm-agent-update.timer) lub -ReleaseKeyFile .\release-signing.pub w Windows (codzienne zaplanowane zadanie CERTYX Agent Update, LocalSystem); włącza to automatyczne podpisane aktualizacje.
5. Wymagania adresu dla agentów: HTTPS osiągalny z hosta agenta, certyfikat dokładnie dla tej nazwy hosta lub adresu, któremu host ufa i którego listę odwołań może pobrać, oraz zegary różniące się najwyżej o kilka minut. Gdy konsola jest otwarta przez nieszyfrowany HTTP bez skonfigurowanego hosta agentów (na przykład lokalny ./start.sh) albo przez proxy bez niego, adres dla agentów nie jest podawany, a widok wyjaśnia dlaczego. Do lokalnego testu uruchom CERTYX poleceniem CLM_AGENT_HOST=<adres tego komputera osiągalny z hosta agenta> ./start.sh: dodaje ono nasłuch HTTPS dla agentów z lokalnym CA i listą odwołań, a konsola pokazuje wtedy adres i krok zaufania. Agent generuje lokalny klucz prywatny i rejestruje publiczną tożsamość; wykrywanie jest domyślnie dozwolone. Zarejestrowani agenci pokazują pierwszy i ostatni kontakt albo informację, że kontaktu

jeszcze nie było. Agent zgłasza mapę sieci przy starcie, a potem co godzinę (NetworkMapIntervalMinutes): prywatne sieci IPv4 swoich interfejsów i tablicy routingu oraz prywatne adresy sąsiadów. Zakresy publiczne nigdy nie są zgłaszane ani proponowane.

6. W sekcji Automatyczne wykrywanie w sieci wybierz agenta. Lista Wykryte sieci pokazuje zgłoszone sieci; użyj Dodaj do zakresu przy sieci albo Dodaj wszystkie (prywatne). Sieci szerszych niż dozwolony prefiks (domyślnie /16) nie można dodać; wpisz węższe zakresy. Dodaj wykluczenia, a zakresy publiczne wpisuj ręcznie tylko wtedy, gdy należą do Ciebie. Gotowość odnowienia również korzysta ze zgłoszonych sieci: gdy dokładnie sieć jednego agenta zawiera adres, pod którym zaobserwowano certyfikat, a agent ma proces cyklu życia, jest on proponowany jako agent instalujący nowego celu.
7. Wybierz tryb: Standardowy sprawdza, które hosty są aktywne na portach dostępności, a potem próbuje typowych portów TLS; Pełny próbuje dodatkowo każdego pozostałego portu TCP 1–65535 na aktywnych hostach. Ustaw liczbę prób połączeń na sekundę (1–2000), jednoczesne połączenia na host (1–4), limity partii oraz opcjonalnie tygodniowe okna skanowania (dni, od, do, strefa IANA; koniec przed początkiem przechodzi na następny dzień, 24:00 kończy o północy; brak okien oznacza dowolną porę).
8. Przed zapisaniem sprawdź sekcję „Co sprawdza jeden przebieg” pod portami. Liczy ona adresy jednego przebiegu dokładnie tak jak agent (zakresy z co najmniej 4 adresami pomijają adres sieci i rozgłoszeniowy, nakładające się zakresy liczą się raz, wykluczenia są odejmowane) i szacuje czas przy zatwierdzonym tempie: sprawdzenie dostępności (każdy adres jest próbowany na portach dostępności, aż któryś odpowie; adres bez odpowiedzi czeka na każdym porcie limit czasu połączenia agentów, domyślnie 500 ms, Clm:Discovery:AgentDefaults:ConnectTimeoutMilliseconds), typowe porty TLS na każdy aktywny host oraz w trybie pełnym każdy pozostały port TCP na każdy aktywny host. Przykład przy 50 próbach na sekundę: sieć /24 (254 adresy) potrzebuje 5–25 s na sprawdzenie dostępności i znacznie poniżej sekundy na aktywny host dla 16 typowych portów, natomiast tryb pełny co najmniej około 22 minut na aktywny host i do około 9 godzin na host, którego zapora odrzuca połączenia bez odpowiedzi zamiast ich odmawiać; gdyby odpowiedziały wszystkie 254 adresy, jeden pełny przebieg trwałby dni. Zacznij od trybu standardowego, a tryb pełny uruchamiaj w oknie skanowania poza godzinami pracy. Zakres bez żadnego adresu do sprawdzenia jest odrzucany; pojedynczy adres kończący się na .0 lub .255 (np. 10.10.10.0/32, adres sieci 10.10.10.0/24) oraz zapis profilu w trybie pełnym wymagają potwierdzenia z szacunkiem.
9. Tryb pełny, zakres krótszy niż /20 lub zakres publiczny otwiera ostrzeżenie, które trzeba potwierdzić: pełne wykrywanie łączy się z każdym adresem i portem, więc systemy wykrywania włamań to zobaczą i mogą zablokować agenta lub zaalarmować zespół bezpieczeństwa. Uzgodnij skanowanie z zespołem bezpieczeństwa i przekaż mu adresy agenta, okna i tempo, aby zarejestrował go jako zatwierdzony skaner. Serwer zapisuje, kto i kiedy potwierdził; profil to pokazuje. Zapis takiego profilu bez potwierdzenia jest odrzucany. Wcześniejsze potwierdzenie pozostaje ważne, dopóki nie dodasz niczego, co wymaga nowego.
10. Włącz profil i zapisz. Postęp wykrywania pokazuje fazę (dostępność, typowe porty, wszystkie porty), postęp, aktywne hosty, znalezione certyfikaty, oczekiwanie na okno skanowania (z następnym oknem) oraz zmniejszone tempo po wielu przekroczeniach czasu połączeń. Pierwszy pełny przebieg zakresu jest bazowy i nie wywołuje alertów; później nieznane certyfikaty, zastąpione certyfikaty i nowe punkty końcowe TLS pojawiają się w Alertach. Zmiana sieci, wykluczeń, trybu lub portów rozpoczyna nowy przebieg bazowy; zmiana tempa, okien lub limitów partii nie. Po zakończonym przebiegu postęp i dziennik agenta (journalctl -u clm-discovery.service) pokazują jego wynik: sprawdzone adresy, adresy, które odpowiedziały, i znalezione certyfikaty TLS; Historia skanów w widoku Discovery TLS przechowuje każdy przebieg.

11. Agent cyklu certyfikatów w Unix wymaga katalogu stanu, plików sekretów i dzienników dostępnych tylko właścicielowi, bez dowiązań symbolicznych w ścieżce i katalogach nadrzędnych. Niebezpieczny lub zbyt duży dziennik zatrzymuje wykonanie do wyjaśnienia przez administratora. Start nie zmienia uprawnień istniejącego katalogu stanu. W Windows agent stosuje tę samą zasadę do plików sekretów i dzienników przez ACL: ich właścicielem i jedynymi podmiotami z dostępem mogą być tylko LocalSystem, Administratorzy lub tożsamość agenta; wszystko inne jest odrzucane. Instalator Windows odpowiednio ogranicza ACL katalogu agenta.
12. Agent cyklu certyfikatów w Unix może odczytywać zatwierdzone sekrety tekstowe Azure Key Vault, AWS Secrets Manager i Google Secret Manager przez lokalną tożsamość CLI klienta. Ustaw dokładne SecretBindings i uruchom Clm.Agent secret-check z chronioną konfiguracją jako konto usługi przed włączeniem wykonania. Wartości pozostają lokalnie i nie są wyświetlane. Zobacz CUSTOMER-VAULTS.pl.md. Odczyt przez CLI dostawców działa tylko w agentach Unix; w Windows dostępne są wyłącznie sekrety z chronionych plików. Klucze prywatne są generowane i przechowywane programowo na hoście agenta (bez HSM), a agent nie wysyła poczty z hosta klienta.
13. HashiCorp Vault KV obsługuje dokładną referencję HTTPS mount/ścieżka#pole i lokalny token helper klienta. Weryfikacja TLS jest obowiązkowa; przestrzenie nazw nie są obsługiwane. Odczyt kończy się błędem, gdy dostęp jest zabroniony, tożsamość unieważniona lub certyfikat Vault niezaufany. Token Vault pochodzi z token helpera klienta; CERTYX nie tworzy ani nie odnawia tożsamości Vault.
14. Zdalne przekazywanie KRL pod kontrolą klienta: uruchom ssh publish-krl z chronioną konfiguracją i udostępnij wyłącznie publiczny zestaw przez osobną tożsamość relaya HTTPS. Na odbiorcy uruchom ssh sync-krl z chronioną subskrypcją. Podpisana publikacja wygasa po godzinie i odświeża się automatycznie; przekierowania, brak zaufania, zbyt duże dane, manipulacje i stare publikacje są odrzucane. Błąd zachowuje istniejące unieważnienia. OpenSSH sam nie egzekwuje terminu zestawu. Stan centralnie raportują tylko odbiorcy zarejestrowani do raportowania KRL; CERTYX nie ustala, które hosty powinny korzystać z KRL. Stare zestawy bez podpisanych terminów wymagają ponownego eksportu. Nowa CA inicjalizuje pusty KRL przed wystawieniem; utrata listy używanej CA wymaga odzyskania.
15. Dla centralnej widoczności zarejestruj osobną tożsamość odbiorcy i jawnie włącz raportowanie KRL; nie nadaje ono prawa wystawiania ani instalowania SSH. Uruchom ssh monitor-krl z chronioną tożsamością i konfiguracją subskrypcji. Stan agentów pokazuje zgłoszoną wersję, podpisany termin publikacji, błędy synchronizacji i brak raportów; poprawne skanowanie nie ukrywa błędu KRL. Monitoring platformy uwzględnia te błędy. To uwierzytelnione obserwacje agenta, nie niezależny dowód odrzucenia certyfikatu na wszystkich hostach. Używaj osobnej zarejestrowanej tożsamości dla każdego odbiorcy.
16. Zapisane wyniki wykonania są ponownie przesyłane po przejściowych błędach połączenia, przekroczeniu czasu żądania oraz HTTP 408/429/500/502/503/504, z odstępem PollSeconds i ograniczeniem OperationTimeoutSeconds. Ponowienie zachowuje zadanie, dzierżawę i wynik; nie powtarza wydania ani instalacji certyfikatu. Przy odzyskiwaniu po restarcie agent odnawia dzierżawę podczas przesyłania zapisanego wyniku. Błędy uwierzytelniania, uprawnień, wygasłej lub uzgodnionej dzierżawy i zaufania TLS zatrzymują wykonanie do uzgodnienia. Mechanizm nie przywraca utraconej dzierżawy; awaria dłuższa niż dzierżawa lub limit operacji nadal wymaga uzgodnienia przez administratora.
17. Wszystkie mechanizmy odczytu konfiguracji JSON agenta odrzucają dowiązania pliku lub katalogów nadrzędnych, uprawnienia grupy lub innych użytkowników w Unix, pliki większe niż 1 MiB oraz niepoprawny UTF-8 przed deserializacją. W Unix zabezpiecz konfigurację poleceniem chmod 600. Względne ścieżki argumentów są przekształcane do bezwzględnych i sprawdzane według tych samych reguł. Obsługiwany jest UTF-8 z BOM i bez BOM. Odczyt ustawień i odczyt asynchroniczny stosują te

same zasady; komunikaty błędów nie zawierają wartości konfiguracji. W Windows odczyt odrzuca plik, którego właścicielem jest lub który może odczytać albo zmienić inny podmiot niż LocalSystem, Administratorzy lub tożsamość agenta; przed wdrożeniem ustaw restrykcyjne ACL.

18. Prywatne endpointy mogą korzystać z oddzielnego, zarejestrowanego weryfikatora. Operator przypisuje jego ID do celu wykonania; w sekcji Zarejestrowani agenci wybierz dla instalatora „Włącz wykonywanie cyklu życia certyfikatów", a dla innej tożsamości agenta „Włącz niezależną weryfikację endpointów". Weryfikator sprawdza lokalnie zatwierdzone TLS/HTTP przed akceptacją sukcesu. Konfiguracja to jedno polecenie na hoście weryfikatora: karta celu w Wykonanie → Cele wdrożenia pokazuje Konfiguracja niezależnego weryfikatora endpointu z nadaniem uprawnienia, przyciskiem Pobierz zakres weryfikatora (ID celu, host weryfikacji, port, ścieżka kontroli stanu i zaufane certyfikaty celu; wyłącznie dane publiczne) i poleceniem configure-verifier-linux.sh add-target (Linux, clm-endpoint-verifier.service na koncie agenta) lub configure-verifier-windows.ps1 add-target (Windows, zadanie harmonogramu CERTYX Endpoint Verifier jako LOCAL SERVICE). Skrypt zapisuje konfigurację dostępną tylko dla właściciela z własnej tożsamości agenta, wykonuje jeden sprawdzony cykl, uruchamia usługę i czeka do dziesięciu minut na nadanie uprawnienia, dopóki CERTYX odpowiada HTTP 403; remove-target, disable i status nią zarządzają, a deinstalator ją usuwa. Nowy agent otrzymuje tę rolę przy instalacji (CLM_AGENT_ENDPOINT_VERIFIER w Linuksie, -EndpointVerifierTarget w Windows). Bez zaufanych certyfikatów w celu host weryfikatora musi sam ufać CA wystawcy.
19. Zarejestrowani instalatorzy raportują własny proces „Praca agenta cyklu życia" (rozpoczęcie, bezczynność lub błąd). Brak raportów jest widoczny również przy działającym discovery. Zdrowie procesu nie zastępuje wyniku wykonania i niezależnego dowodu endpointu. Przy zatrzymaniu do uzgodnienia sprawdź chronione lokalne dzienniki.
20. Discovery ponawia przejściowe błędy rotacji tożsamości i komunikacji po Settings.RetrySeconds. Błędy uwierzytelniania, uprawnień lub zaufania TLS zatrzymują agenta; --once zwraca błąd. Stan i blokada wymagają ochrony tylko dla właściciela. Awaria raportowania może opóźnić diagnostykę, więc monitoruj także brak kontaktu.
21. Projekty celów: zapisz projekt (agent, ID celu, nazwy DNS, typ i adres CA, mount i rola Vault, punkt weryfikacji, czas życia, Konektor wdrożenia i Instalacja; dla przekaźnika SSH także host zdalny, konto SSH i port), pobierz pakiet konfiguracji dla hosta agenta i wybierz Utwórz cel z tego agenta, aby dodać cel wdrożenia organizacji o tym samym zakresie i trybie instalacji w widoku Wykonanie. Pakiet zawiera udokumentowane domyślne pliki i polecenia konektora, a dla przekaźnika obiekt Remote i RelayDestinations; przed instalacją zastąp jego znaczniki (SET-HOST-KEY-FINGERPRINT, SET-ACCOUNT-EMAIL, YOUR-CLM-HOST). Utworzenie jest odrzucane, gdy cel o tym ID istnieje albo projekt nie przechodzi walidacji celu; dalsze zmiany (np. zaufane certyfikaty prywatnego CA) wprowadzisz w widoku Wykonanie.
22. Przekaźnik SSH do hostów bez agenta: nadaj agentowi przekaźnika uprawnienie Włącz wykonywanie cyklu życia certyfikatów. Na hoście zdalnym uruchom configure-relay-host-linux.sh z pakietu agenta z kluczem publicznym przekaźnika i pomocnikiem wypisanym przez Clm.Agent relay-helper (konto tylko z logowaniem kluczem, authorized_keys z restrict i from=, pomocnik, dozwolone katalogi, minimalna reguła sudoers); przypnij wypisany odcisk klucza hosta w HostKeyFingerprints i w pliku known_hosts na przekaźniku; następnie uruchom Clm.Agent relay-check. Tożsamość SSH i plik known_hosts przekaźnika pozostają dostępne tylko dla właściciela na przekaźniku i nigdy nie trafiają do CERTYX; raporty zawierają tylko nazwę hosta zdalnego. Krok po kroku: instrukcja instalacji agenta, „Przekaźnik SSH".

23. Każdy zarejestrowany agent pokazuje swoją diagnozę (przyczynę i wyjaśnienie, z odnośnikiem Dlaczego i co zrobić do Stanu agentów) oraz ostatni przebieg wykrywania (początek, stan, aktywne hosty, znalezione endpointy i certyfikaty, z Historią skanów).

DANE I PARAMETRY

- Ustawienia organizacji; klucze prywatne i dane uwierzytelniające CA nie są przyjmowane.
- Katalogi kluczy i wdrożeń wymagają bezwzględnych ścieżek bez dowiązań. Klucze i dzienniki odzyskiwania wymagają dostępu tylko właściciela; dowiązany, współdzielony lub zbyt duży stan jest odrzucany. Dozwolony jest jedynie zarządzany link current do generacji UUID.
- Limity wykrywania pochodzą z konfiguracji serwera Clm:Discovery:AgentLimits (domyślnie: prefiks co najmniej /16, najwyżej 65 536 adresów na zakres i 262 144 na profil, 64 zakresy, 256 wykluczeń); domyślne porty, tempo i strefa czasowa pochodzą z Clm:Discovery. Zakresy loopback, link-local, multicast i zarezerwowane są odrzucane. Skanowane jest tylko IPv4; sąsiedzi IPv6 służą wyłącznie jako wskazówki dostępności.
- Formaty (każde pole ma własną pomoc): identyfikatory agenta i miejsca docelowego 1–100 liter, cyfr, łączników i podkreśleń (web-prod-01); sieci i wykluczenia po jednym CIDR IPv4 w wierszu zapisanym adresem sieci (10.20.0.0/16, pojedynczy adres jako 10.20.0.1/32); porty jako lista, np. 443, 8443 (1–64 typowych, 1–16 portów dostępności, każdy 1–65535); godziny okien skanowania HH:mm (24:00 tylko jako koniec); strefa czasowa IANA, np. Europe/Warsaw; nazwy DNS bez symboli wieloznacznych, adresów URL, portów i adresów IP; adres API urzędu certyfikacji zaczynający się od https://. Profil sieci: Próby połączeń na sekundę 1–2000, Jednoczesne połączenia na host 1–4; w sekcji Limity partii Połączenia równoległe 1–64, Próby w jednej partii 1–10000 i Przerwa między przejściami 10–86400 sekund. Szkice miejsc docelowych: Port weryfikacji 1–65535 i Ważność certyfikatu w godzinach 1–8760.

WYNIK OPERACJI

Trwała, audytowana konfiguracja administracyjna.

UPRAWNIENIA

Administratorzy tworzą kody rejestracji, widzą zarejestrowanych agentów i wykryte sieci, nadają lub odbierają uprawnienia, unieważniają agentów, edytują profile sieciowe i zapisują projekty celów lub tworzą z nich cele. Pozostali zalogowani użytkownicy organizacji widzą tylko projekty konfiguracji celów i informację, że resztą zarządzają administratorzy; widok Stan agentów pozostaje dla nich dostępny.

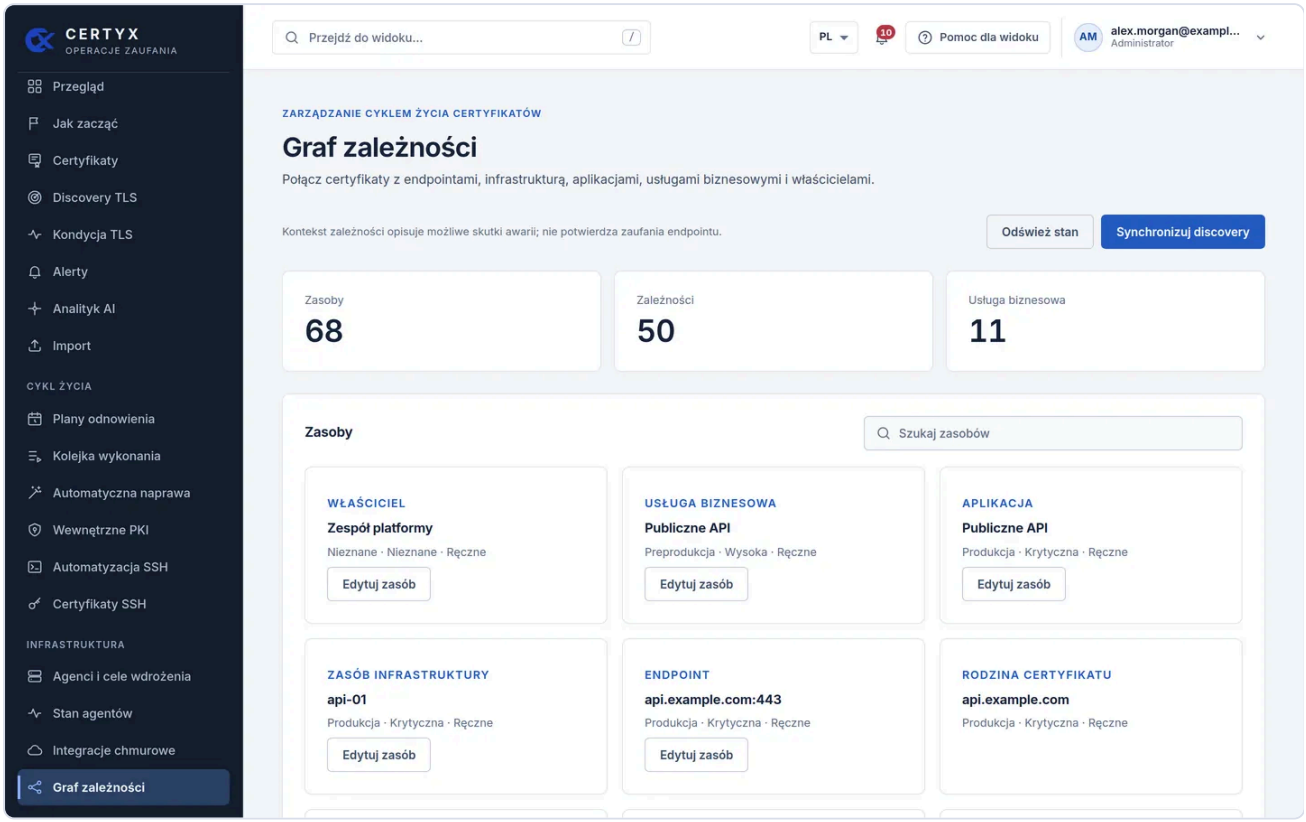
OGRANICZENIA

Wykrywanie bezpośredniego TLS obsługuje IPv4 TCP. Agent skanuje w stałej, udokumentowanej kolejności i w stałym tempie; tempo, okna i zmniejszanie tempa po przekroczeniach czasu ograniczają obciążenie sieci i nie służą ukrywaniu skanowania przed narzędziami bezpieczeństwa. Serwer ponownie sprawdza każdą obserwację względem zatwierdzonego profilu. Aby rozpoznać usługę, po negocjacji TLS agent wysyła jedno żądanie HEAD / HTTP/1.1 do punktu, który wynegocjował protokół HTTP (albo żaden na porcie HTTP; punkty h2 dostają je przez jeszcze jedno połączenie HTTP/1.1), lub odczytuje powitanie SMTPS, IMAPS albo POP3S; Settings.ServiceIdentification.IdentifyServices false w konfiguracji skanu to wyłącza. Agent nie sprawdza usług UDP ani STARTTLS i nie wylicza hostów wirtualnych SNI. Identyfikator agenta można zarejestrować tylko raz: kod dla już zarejestrowanego identyfikatora jest odrzucany, więc agent zastępczy wymaga nowego identyfikatora; najpierw usuń starą instalację skryptem uninstall-linux.sh (w /opt/clm-agent/current) lub uninstall-windows.ps1, które usuwają każdą jednostkę lub zadanie, plik, wpis zaufania i konto utworzone przez skrypty CERTYX. Gdy operator publikuje klucz podpisu wydań,

wydania mają dodatkowo podpisany offline manifest: przed instalacją sprawdź go skryptem verify-release.sh (dostępnym w /downloads/ pod adresem konsoli i pod osobnym adresem agentów, razem z pakietami, ich plikami podpisów i verify-agent-package.sh/.ps1); agenci Linux i Windows zainstalowani z kluczem wydań (Linux: clm-agent-update.timer, Windows: zaplanowane zadanie CERTYX Agent Update) aktualizują się codziennie wyłącznie do nowszej podpisanej wersji i wycofują zmianę, gdy zrestartowany agent nie jest zdrowy. Pakiety są podpisane przez wydawcę: podpis CMS skrótu archiwum i pliku SHA256SUMS ze skrótami wszystkich plików pakietu, a także Authenticode na plikach wykonywalnych Windows, bibliotekach CLM i skryptach PowerShell. Instalatory Linux i Windows weryfikują pakiet względem przypiętego odcisku wydawcy i odmawiają instalacji pakietu niepodpisanego, zmienionego lub od innego wydawcy; obejście deweloperskie (CLM_AGENT_ALLOW_UNSIGNED=1 lub -AllowUnsignedDevelopment) wyświetla ostrzeżenie i nie może być używane produkcyjnie. Agentów zainstalowanych bez klucza wydań aktualizuje się w miejscu opisanymi niżej skryptami aktualizacji, ponieważ instalatory odrzucają host z już zarejestrowanym agentem. Poświadczenia i klucze prywatne pozostają pod kontrolą klienta. Sekrety są odczytywane z chronionych plików, HashiCorp Vault KV, Azure Key Vault, AWS Secrets Manager i Google Secret Manager; inne sejfy nie są obsługiwane, CLI dostawców działają tylko w agentach Unix, a agent nie wysyła poczty z hosta klienta. Uprawnienia pliku tokenu Vault w Unix są sprawdzane przy każdym użyciu. Tożsamości agentów wykrywających rotują automatycznie domyślnie 30 dni przed wygaśnięciem (IdentityRenewalDays w obiekcie Settings konfiguracji agenta), z kluczami lokalnymi i odzyskiwaniem utraconych potwierdzeń. Tożsamości wdrożeniowe w rejestrze plikowym wymagają kontrolowanej rotacji ręcznej. Lokalne blokady konektorów muszą być zwykłymi plikami tylko dla właściciela w Unix, bez dowiązań w katalogach nadrzędnych. Niebezpieczne istniejące blokady są odrzucane; administrator musi poprawić uprawnienia magazynu przed ponowieniem. Te konektory działają tylko w agentach Unix. Dla jawnie wybranego transportu AWS CLI na Unix ustaw AwsCliExecutable w lokalnej konfiguracji celu AWS na zaufaną bezwzględną ścieżkę programu. Historia CLI musi być wyłączona. Import używa prywatnego standardowego wejścia, poświadczenia pozostają lokalne. Domyślnym transportem pozostaje SDK. Cykl GCP wymaga lokalnej konfiguracji zasobu/tożsamości i przygotowania poprzedniej generacji przez gcp-adopt; patrz GCP-LIFECYCLE.md. Poświadczenia nie są polami zadania. Sam cel Google Certificate Manager rejestruje się w widoku Wykonanie, w sekcji Cele wdrożenia. Gdy ten serwer publikuje pakiet bez podpisu wydawcy (niepodpisaną kompilację deweloperską), polecenia instalacji mówią o tym, pomijają plik podpisu i sprawdzają tylko sumę kontrolną, z obejściami deweloperskimi weryfikatora i instalatora; takich pakietów używaj tylko do prac deweloperskich. Zainstalowanych agentów aktualizuje się w miejscu skryptem upgrade-linux.sh lub upgrade-windows.ps1 z nowszego pakietu (instrukcja instalacji, „Aktualizacja w miejscu”), bez nowego kodu rejestracji; nowsze archiwum pobierz przez zalogowaną konsolę i skopiuj na host. upgrade-linux.sh dodaje też AgentConfigurationFile do update.json zapisanego przez starszy instalator, dzięki czemu jego podpisane aktualizacje znów mogą pobierać archiwa. Przekaźnik SSH instaluje tylko certyfikaty serwera TLS i wymaga dostępu SSH, OpenSSL 1.1.1 lub nowszego oraz powłoki POSIX na hoście zdalnym; magazyn Windows i IIS instalują tylko na hoście z agentem Windows.

22 Graf zależności

Połącz certyfikaty z endpointami, infrastrukturą, aplikacjami, usługami biznesowymi i właścicielami.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Wybierz Synchronizuj discovery (administratorzy), aby przejąć zaobserwowane endpointy TLS: dla każdej obserwacji endpointu certyfikatu z inwentarza graf otrzymuje zasób infrastruktury (serwer), jego endpoint (host i port) i rodzinę certyfikatu, połączone jako zasób → endpoint → rodzina; nowsza obserwacja przenosi endpoint do nowo zaobserwowanej rodziny. Serwer wykonuje tę synchronizację także automatycznie dla organizacji z licencją (Clm:Assets:SynchronizationInterval, domyślnie co minutę). Istniejące zasoby zachowują dane wprowadzone ręcznie.
2. W sekcji Zarządzaj kontekstem biznesowym wybierz Dodaj zasób: rodzaj zasobu (Zasób infrastruktury, Endpoint, Aplikacja, Usługa biznesowa lub Właściciel), nazwę, środowisko, krytyczność, status i właściciela; endpoint wymaga nazwy hosta i portu, właściciel adresu e-mail i typu. Zapisz zasób; Edytuj zasób na karcie listy zasobów wczytuje go do formularza (rodziny certyfikatów pochodzą z discovery i nie podlegają edycji).
3. W sekcji Zależności dodaj zależność od Zasobu zależnego do Celu zależności, od którego zależy (np. aplikacja → endpoint, usługa biznesowa → aplikacja).
4. W sekcji Uzupełnianie z CMDB podaj źródło CMDB, wybierz plik JSON CMDB (do 100 KB, format jak w przykładzie schematu JSON) i wybierz Importuj JSON CMDB. Importy są przyrostowe: to samo źródło i te same identyfikatory zewnętrzne aktualizują te same zasoby, a ręcznie ustawiona krytyczność zostaje zachowana.

5. W sekcji Wpływ biznesowy wybierz rodzinę certyfikatu i Analizuj wpływ, aby zobaczyć dotknięte zasoby, ścieżki zależności, właścicieli, wynikową krytyczność i ostrzeżenia o niepełnym kontekście.

DANE I PARAMETRY

- Wersjonowane zasoby z klasyfikacją; przyrostowy import JSON CMDB z tożsamością źródła.
- Warunek: subskrypcja organizacji obejmuje graf zależności (TRUST_GRAPH). Bez niej widok pokazuje tylko informację, a serwer odrzuca żądania grafu.

WYNIK OPERACJI

Wyjaśniony wpływ biznesowy z krytycznością, właścicielami i ostrzeżeniami o niepełnym kontekście.

UPRAWNIENIA

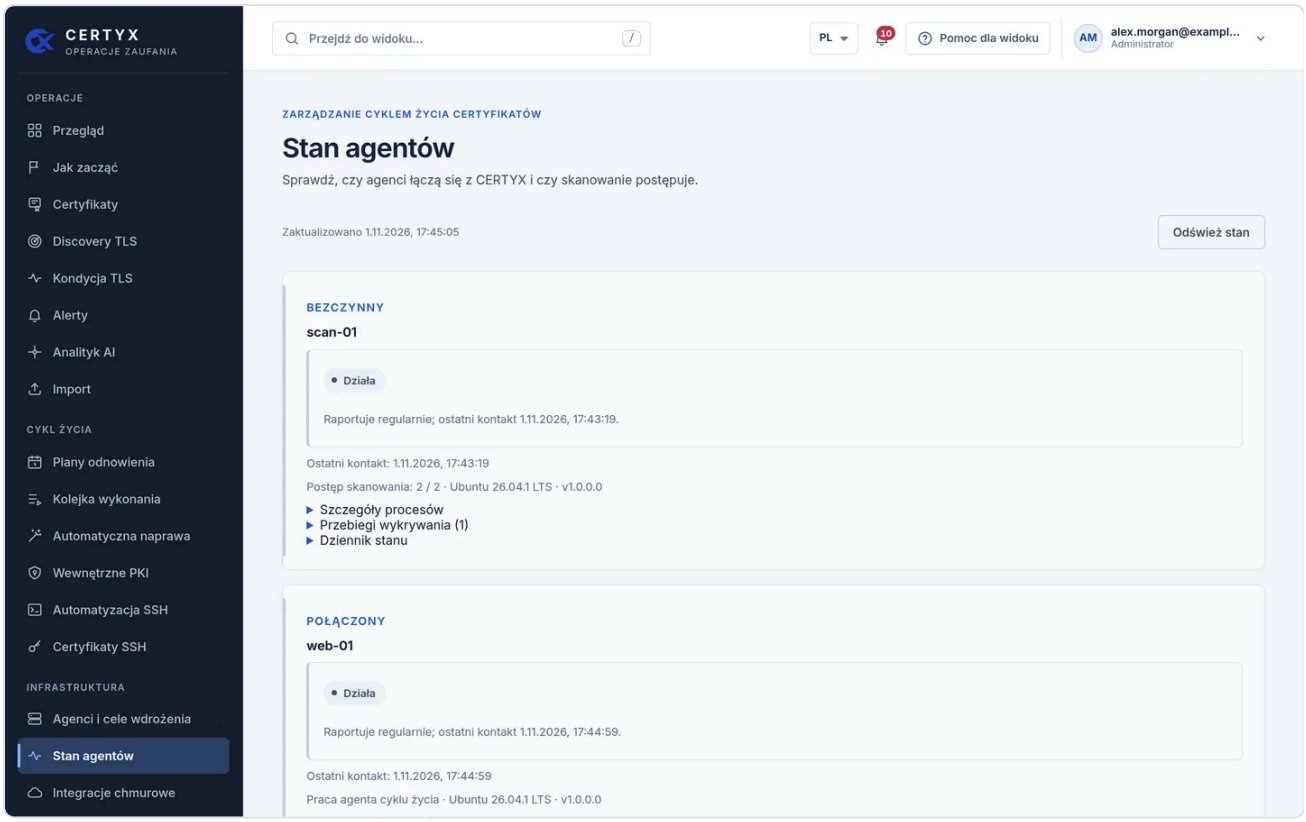
Wymaga licencji na graf zależności. Administratorzy synchronizują discovery, edytują zasoby i zależności oraz importują dane CMDB; pozostali zalogowani użytkownicy organizacji przeszukują zasoby i analizują wpływ tylko do odczytu.

OGRANICZENIA

Import CMDB jest znormalizowanym konektorem push. Adaptery pobierające dane od konkretnych dostawców nie są wdrożone. Nieznana krytyczność nie oznacza niskiego ryzyka, a graf nie weryfikuje zaufania TLS.

23 Stan agentów

Sprawdź, czy agenci łączą się z CERTYX i czy skanowanie postępuje.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Zarejestruj i zainstaluj agenta sieciowego.
2. Przypisz zatwierdzony profil.
3. Sprawdź ostatni uwierzytelniony kontakt, postęp i przyczyny błędów.
4. Rozwiń Szczegóły procesów agenta wykrywania, aby zobaczyć fazę (dostępność, typowe porty, wszystkie porty), aktywne hosty, zmniejszone tempo po przekroczeniach czasu połączeń, następne okno skanowania, gdy agent czeka poza zatwierdzonymi oknami (stan Oczekuje na okno skanowania), oraz czas zakończenia przebiegu bazowego.
5. Agenci wyłącznie SSH nie wymagają profilu skanowania. Online oznacza świeży uwierzytelniony kontakt, nie udaną instalację. Zadania i unieważnienia SSH sprawdzaj osobno; brak kontaktu zmienia stan na offline.
6. Zarządzany proces SSH zgłasza własny bezpieczny stan cyklu. Poprawne skanowanie nie ukrywa błędu ani braku raportów procesu SSH. Sprawdź błąd w stanie agentów i chronione lokalne dzienniki; stałe podsumowania nie zawierają sekretów. Brak połączenia może uniemożliwić natychmiastowy raport, dlatego monitorowany jest również brak kontaktu.
7. Rozwiń Szczegóły procesów, aby sprawdzić stan cyklu SSH i ostatni raport; dane SSH nie są oznaczane jako postęp skanowania.

8. Dla centralnej widoczności zarejestruj osobną tożsamość odbiorcy i jawnie włącz raportowanie KRL; nie nadaje ono prawa wystawiania ani instalowania SSH. Uruchom ssh monitor-krl z chronioną tożsamością i konfiguracją subskrypcji. Stan agentów pokazuje zgłoszoną wersję, podpisany termin publikacji, błędy synchronizacji i brak raportów; poprawne skanowanie nie ukrywa błędu KRL. Monitoring platformy uwzględnia te błędy. To uwierzytelnione obserwacje agenta, nie niezależny dowód odrzucenia certyfikatu na wszystkich hostach. Używaj osobnej zarejestrowanej tożsamości dla każdego odbiorcy.
9. Nowy odbiorca KRL pozostaje nieskonfigurowany do pierwszego raportu; inny poprawny proces nie potwierdza synchronizacji. Stan i powód muszą być zgodne. Raporty są izolowane dla organizacji, a odebranie uprawnienia odrzuca dalsze aktualizacje.
10. Prywatne endpointy mogą korzystać z oddzielnego, zarejestrowanego weryfikatora. Operator przypisuje jego ID do celu wykonania; w widoku Agenci i cele wdrożenia, w sekcji Zarejestrowani agenci, wybierz dla instalatora „Włącz wykonywanie cyklu życia certyfikatów", a dla innej tożsamości agenta „Włącz niezależną weryfikację endpointów". Weryfikator sprawdza lokalnie zatwierdzone TLS/HTTP przed akceptacją sukcesu; jego proces widać w Szczegółach procesów. Konfiguracja to jedno polecenie na hoście weryfikatora: karta celu w Wykonanie → Cele wdrożenia pokazuje Konfiguracja niezależnego weryfikatora endpointu z nadaniem uprawnienia, przyciskiem Pobierz zakres weryfikatora (ID celu, host weryfikacji, port, ścieżka kontroli stanu i zaufane certyfikaty celu; wyłącznie dane publiczne) i poleceniem configure-verifier-linux.sh add-target (Linux, clm-endpoint-verifier.service na koncie agenta) lub configure-verifier-windows.ps1 add-target (Windows, zadanie harmonogramu CERTYX Endpoint Verifier jako LOCAL SERVICE). Skrypt zapisuje konfigurację dostępną tylko dla właściciela z własnej tożsamości agenta, wykonuje jeden sprawdzony cykl, uruchamia usługę i czeka do dziesięciu minut na nadanie uprawnienia, dopóki CERTYX odpowiada HTTP 403; remove-target, disable i status nią zarządzają, a deinstalator ją usuwa. Nowy agent otrzymuje tę rolę przy instalacji (CLM_AGENT_ENDPOINT_VERIFIER w Linuksie, -EndpointVerifierTarget w Windows). Bez zaufanych certyfikatów w celu host weryfikatora musi sam ufać CA wystawcy.
11. Zarejestrowani instalatorzy raportują własny proces „Praca agenta cyklu życia" (rozpoczęcie, bezczynność lub błąd). Brak raportów jest widoczny również przy działającym discovery. Zdrowie procesu nie zastępuje wyniku wykonania i niezależnego dowodu endpointu. Przy zatrzymaniu do uzgodnienia sprawdź chronione lokalne dzienniki.
12. Discovery ponawia przejściowe błędy rotacji tożsamości i komunikacji po Settings.RetrySeconds. Błędy uwierzytelniania, uprawnień lub zaufania TLS zatrzymują agenta; --once zwraca błąd. Stan i blokada wymagają ochrony tylko dla właściciela. Awaria raportowania może opóźnić diagnostykę, więc monitoruj także brak kontaktu.
13. Każda karta zaczyna się od diagnozy: dokładnej przyczyny (Działa, Brak raportów, Brak pierwszego kontaktu, Tożsamość wygasła lub wkrótce wygaśnie, Rozbieżność zegara, Błąd procesu, Proces nie raportuje, Brak konfiguracji, Wykrywanie wstrzymane, Oczekuje na okno skanowania, Zmniejszone tempo skanowania, Obserwacja odrzucona), wyjaśnienia z faktami (ostatni kontakt i pominięte okno raportowania, proces i zgłoszona stała przyczyna, data wygaśnięcia, zmierzona różnica zegara) oraz sekcji Co zrobić: działań naprawczych po kolei, każde z odnośnikiem do miejsca wykonania, i odnośnika do rozwiązywania problemów. #agent-health/<ID agenta> otwiera wybranego agenta (z przeglądu, Agentów i celów, Planów odnowienia i gotowości odnowienia).
14. Dziennik stanu wymienia każdą zmianę diagnozy, od najnowszej, z czasem, nową i poprzednią przyczyną oraz wyjaśnieniem. Monitor stanu ocenia każdego agenta co Clm:Agents:Health:WatchInterval (domyślnie 1 minuta) i zapisuje każdą zmianę; trafia ona też do

dziennika bezpieczeństwa jako agent.health.changed z wyjaśnieniem i krokami naprawczymi, więc otrzymują ją operator platformy i eksport SIEM organizacji. Przebiegi wykrywania pokazują ostatnie przebiegi agenta (zob. Discovery TLS, Historia skanów).

DANE I PARAMETRY

- Czas odbioru na serwerze, ważność certyfikatu i ograniczona telemetria uwierzytelnionego agenta.
- Agent przechodzi w stan Brak kontaktu, a raport procesu jest oznaczany jako błąd, gdy w oknie raportowania nic nie dotrze: interwał profilu lub procesu plus Clm:Agents:Health:ReportingGrace (domyślnie 1,5 minuty), co najmniej Clm:Agents:Health:MinimumReportingWindow (domyślnie 2 minuty).

WYNIK OPERACJI

Jedna karta na zarejestrowanego agenta z jego stanem (Połączony, Oczekuje na pierwszy kontakt, Oczekuje na konfigurację, Wstrzymany, Oczekuje na okno skanowania, Brak kontaktu, Błąd, Tożsamość wygasła, Unieważniony), przyczyną, ostatnim kontaktem, głównym procesem z systemem operacyjnym i wersją agenta oraz Szczegółami procesów dla każdego zgłoszonego procesu. Lista odświeża się automatycznie, gdy widok jest otwarty; Odśwież stan wczytuje ją natychmiast.

UPRAWNIENIA

Użytkownicy organizacji po zalogowaniu.

OGRANICZENIA

Brak kontaktu nie pozwala platformie ustalić dokładnej przyczyny niedostępności maszyny. Zgłoszony system operacyjny nie stanowi atestacji sprzętu. Tożsamości agentów wykrywających rotują automatycznie domyślnie 30 dni przed wygaśnięciem (IdentityRenewalDays w obiekcie Settings konfiguracji agenta), z kluczami lokalnymi i odzyskiwaniem utraconych potwierdzeń. Tożsamości wdrożeniowe w rejestrze plikowym wymagają kontrolowanej rotacji ręcznej. Agenci Linux zainstalowani z kluczem podpisu wydań operatora aktualizują się codziennie z podpisanych wydań; pozostali agenci Linux i wszyscy agenci Windows nie mają aktualizacji w miejscu: instalatory odrzucają host z już zarejestrowanym agentem, więc nowszą wersję instaluje się, zastępując agenta (unieważnij go, usuń instalację zgodnie z instrukcją instalacji i zarejestruj zweryfikowany nowy pakiet pod nowym identyfikatorem agenta).

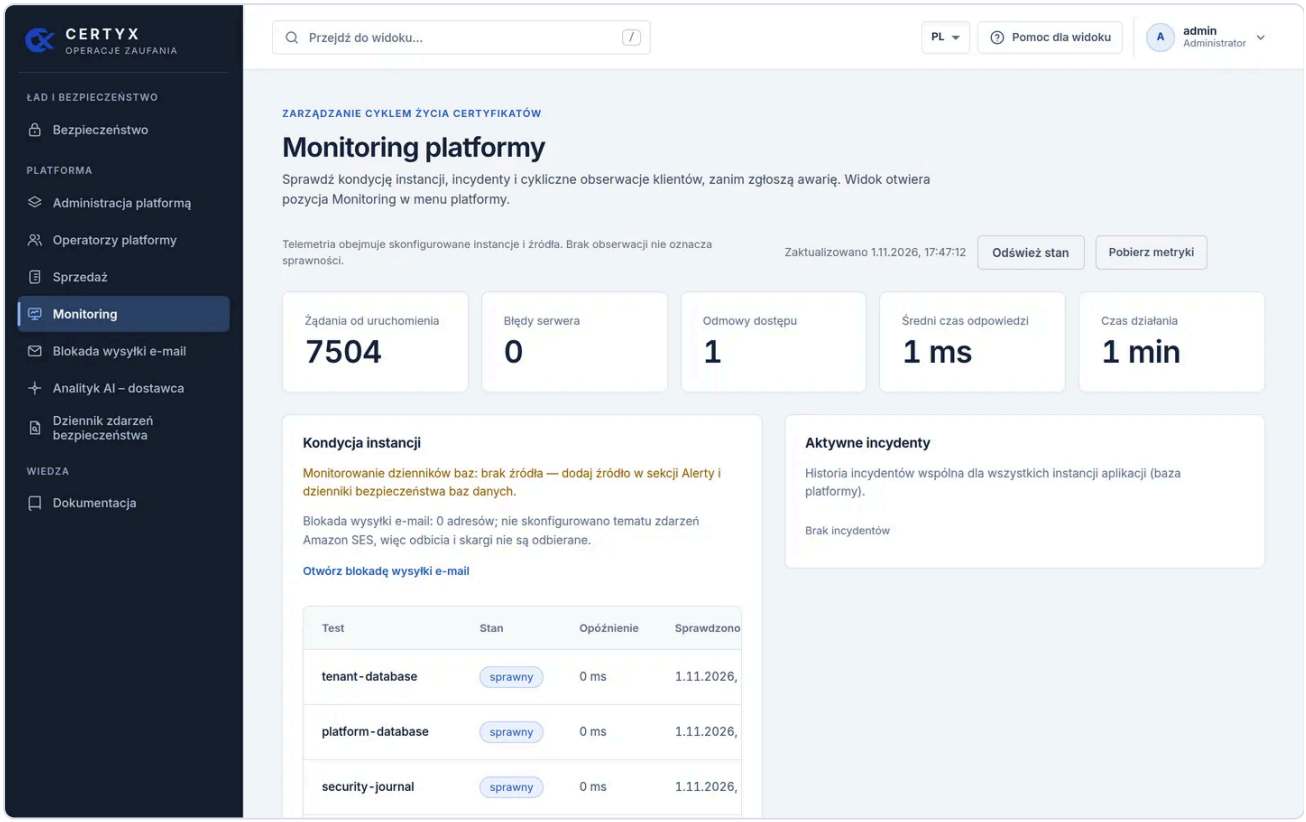
ROZWIĄZYWANIE PROBLEMÓW

- Brak raportów: uruchom usługę (sudo systemctl status clm-discovery.service; clm-ssh.service dla SSH; zadanie harmonogramu w Windows) i przeczytaj sudo clm-agent log; uruchom sudo clm-agent status, który wskazuje błędny krok (usługa, adres, zaufanie TLS z unieważnieniem, zegar, tożsamość); sprawdź zaporę, proxy i DNS w kierunku adresu agentów; przy błędzie zaufania TLS zainstaluj prywatny certyfikat główny adresu agentów; zsynchronizuj zegar; sprawdź, czy tożsamość nie wygasła lub nie została unieważniona. W Windows przeczytaj logi zadań C:\ProgramData\CLM-Agent\state\discovery.log i C:\ProgramData\CLM-SSH\state\ssh-workload.log (Get-Content -Tail 50) i uruchom Clm.Agent.exe status agent.json w PowerShell administratora.
- Brak pierwszego kontaktu: uruchom polecenie instalacji pokazane po rejestracji, zanim kod wygaśnie (Agenci i cele wdrożenia); po wygaśnięciu utwórz nowy kod; następnie sudo clm-agent status.
- Tożsamość wygasła lub wkrótce wygaśnie: automatyczna rotacja działa IdentityRenewalDays (domyślnie 30) dni przed wygaśnięciem; jeśli nie zadziałała, zarejestruj agenta ponownie z nowym ID i unieważnij starą tożsamość.

- Rozbieżność zegara: mapa sieci agenta zawiera jego czas; zsynchronizuj host przez NTP. Kontrole TLS i tożsamości zawodzą przy różnicy minut (tolerancja Clm:Agents:Health:ClockSkewTolerance).
- Błąd procesu: proces cyklu życia nie powiódł się — otwórz nieudane zadanie w widoku Wykonanie i chroniony lokalny dziennik; wykrywanie nie powiodło się — sprawdź komunikację przez sudo clm-agent status; zatwierdzony profil wykracza poza lokalną listę dozwolonych sieci — rozszerz AllowedCidrs lub zawęź profil; synchronizacja KRL nie powiodła się — sprawdź przekaźnik klienta i przypięte zaufanie; cykl SSH nie powiódł się — sprawdź dziennik SSH i Automatyzację SSH.
- Brak konfiguracji: przypisz i zatwierdź profil wykrywania albo skonfiguruj i uruchom proces, dla którego nadano uprawnienie (cykl życia, weryfikator endpointów, odbiorca KRL).
- Zmniejszone tempo skanowania: przekroczenia czasu połączeń zmniejszyły tempo o połowę; sprawdź, czy zapora lub IPS nie blokuje agenta, albo obniż tempo i liczbę połączeń na host.

24 Monitoring platformy

Sprawdź kondycję instancji, incydenty i cykliczne obserwacje klientów, zanim zgłoszą awarię. Widok otwiera pozycja Monitoring w menu platformy.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Zaloguj się jako dopuszczony zarządca platformy z MFA.
2. Przejrzyj kafelki metryk tej instancji (Żądania od uruchomienia, Błędy serwera, Odmowy dostępu, Średni czas odpowiedzi, Czas działania), Kondycję instancji (sprawdzenia bazy organizacji i bazy platformy, monitorowania klientów i każdego źródła dziennika bazy, ze stanem, czasem odpowiedzi i czasem sprawdzenia; wiersz nad tabelą pokazuje monitorowanie dzienników baz) oraz Aktywne incydenty. Odśwież stan wczytuje wszystko ponownie; Pobierz metryki zapisuje metryki Prometheus tej instancji.
3. W sekcji Alerty i dzienniki bezpieczeństwa baz danych dodaj zarządzany dziennik PostgreSQL każdej bazy: AWS CloudWatch Logs (pełny ARN grupy dzienników RDS), Azure Log Analytics (GUID obszaru roboczego|identyfikator zasobu Flexible Server) lub Google Cloud Logging (projekt:instancja Cloud SQL), z identyfikatorem klienta dla dedykowanej bazy klienta. Każde źródło jest odczytywane w następnym cyklu monitorowania z tożsamością maszyny hosta platformy (CloudWatch przez AWS SDK, więc host potrzebuje tylko prawa odczytu grupy dzienników; Azure i Google Cloud przez CLI dostawcy), a nieudane uwierzytelnienia i autoryzacje stają się incydentami. Przy kontenerach baz danych standardowego wdrożenia nie trzeba niczego dodawać: obie bazy zapisują dziennik bezpieczeństwa JSON, który aplikacja czyta; wiersz kondycji instancji pokazuje wtedy „lokalny dziennik PostgreSQL”. Na AWS z RDS dodaj raz źródło CloudWatch z ARN grupy dzienników podanym w wyniku

infrastruktury database_log_group_arn. Nieczytelne źródło pojawia się jako osobny nieudany test zdrowia i na liście źródeł; wiersz kondycji instancji pokazuje, ile źródeł jest obserwowanych i czy odczytywany jest lokalny dziennik JSON PostgreSQL hosta.

4. Kondycja klientów pokazuje dedykowanych klientów ze stanem bazy, statusem klienta, agentami offline, nieudanymi zadaniami cyklu życia i ostatnią obserwacją (przyczyna po najechaniu na wiersz). Po analizie wybierz Potwierdź incydent; potwierdzenie zapisuje, kto prowadzi analizę, i nie usuwa awarii.
5. Kanały alertów: dodaj kanał Microsoft Teams (adres webhooka lub przepływu), Slack (adres Incoming Webhook; układ wiadomości bloki lub zwykły tekst), PagerDuty (klucz routingu Events API v2), webhook HTTPS lub e-mail z minimalną ważnością, a następnie wybierz Wyślij alert testowy; nieudany test podaje przyczynę (brak przekaźnika, błędne miejsce docelowe, nieczytelny sekret, odmowa, brak połączenia, przekroczony czas). Kanały e-mail korzystają z przekaźnika e-mail alertów (host, port STARTTLS, nadawca, opcjonalnie użytkownik i hasło). Adresy URL, klucze routingu i hasła można tylko ustawić: wpisz nową wartość, aby ją zastąpić, albo secret:<nazwa>, aby odczytać ją z zatwierdzonego powiązania sekretu platformy; puste pole zachowuje zapisaną wartość. Otwarcie i zamknięcie incydentu trafia do każdego kanału, którego minimalną ważność osiąga; kanał, który stale zawodzi, otwiera incydent alert-delivery. Alerty wysyła jedna instancja naraz i każda zmiana trafia do kanału raz, także przy kilku instancjach.
6. Dla centralnej widoczności zarejestruj osobną tożsamość odbiorcy i jawnie włącz raportowanie KRL; nie nadaje ono prawa wystawiania ani instalowania SSH. Uruchom ssh monitor-krl z chronioną tożsamością i konfiguracją subskrypcji. Stan agentów pokazuje zgłoszoną wersję, podpisany termin publikacji, błędy synchronizacji i brak raportów; poprawne skanowanie nie ukrywa błędu KRL. Monitoring platformy uwzględnia te błędy. To uwierzytelnione obserwacje agenta, nie niezależny dowód odrzucenia certyfikatu na wszystkich hostach. Używaj osobnej zarejestrowanej tożsamości dla każdego odbiorcy.
7. Dostawca analityka AI (klucz API Anthropic, model, test połączenia, limity, udostępnienie organizacjom) ma własny widok w centrum sterowania: Analityk AI – dostawca.
8. Pod liczbą agentów offline każdy wiersz klienta wymienia agentów wymagających uwagi z przyczyną i od kiedy (ta sama diagnoza, którą organizacja widzi w Stanie agentów); wpisy agent.health.changed w dzienniku bezpieczeństwa klienta zawierają wyjaśnienie i kroki naprawcze.
9. Poczta techniczna i sprzedażowa są rozdzielone: przekaźnik e-mail alertów to techniczny nadawca platformy (na przykład support@...) dla e-maili alertów i e-maili konfiguracji aplikacji uwierzytelniającej kont klientów; poczta sprzedaży ma własny przekaźnik w Sprzedaży (na przykład sales@...). Wyślij przykładowy e-mail konfiguracyjny wysyła odbiorcy przez ten przekaźnik podgląd e-maila konfiguracyjnego w wybranym języku; jego link i kod QR nie otwierają konfiguracji, a wysyłka jest zapisywana w dzienniku bezpieczeństwa (mfa-setup.mail.sample-sent). Przekaźnik używa STARTTLS (port 587); niejawny TLS na porcie 465 nie jest obsługiwany.
10. W sekcji Kondycja instancji wiersz blokady wysyłki e-mail pokazuje, ile adresów jest zablokowanych i jakie zdarzenie Amazon SES odebrano ostatnio (brak zdarzeń jest normalny, są rzadkie) albo że nie skonfigurowano tematu zdarzeń; Otwórz blokadę wysyłki e-mail prowadzi do listy. Kanał e-mail alertów z zablokowanym adresem nie jest ponawiany i otwiera incydent alert-delivery z przyczyną.

DANE I PARAMETRY

- Liczniki od uruchomienia procesu; uwierzytelnione sondy bazy; ograniczona historia incydentów i obserwacje klientów.

- Kanał alertów: nazwa (1–64 litery, cyfry, . _ -, na początku litera lub cyfra), rodzaj, minimalna ważność, e-mail odbiorcy albo URL/klucz routingu (URL zaczyna się od https://; klucz routingu PagerDuty ma do 200 znaków bez spacji; zamiast nich można podać odwołanie secret:<name>), układ wiadomości Slack (tylko Slack). Przekaźnik: host, port, nadawca, opcjonalnie użytkownik i hasło. Źródło dziennika bazy: nazwa, usługa dzienników, lokalizacja w formacie podanym dla usługi, opcjonalnie identyfikator klienta (GUID). Minimalna ważność to Tylko krytyczne albo Ostrzeżenia i krytyczne; najwyżej 20 kanałów alertów i 50 źródeł dzienników baz.

WYNIK OPERACJI

Trwałe incydenty (wspólne dla wszystkich instancji, gdy skonfigurowano bazę platformy; wtedy incydent zgłoszony na jednej instancji można potwierdzić lub zamknąć na innej), chronione metryki Prometheus i stan operacyjny. Panel incydentów pokazuje, czy historia jest wspólna, lokalna czy niedostępna. Wersjonowane ustawienia kanałów alertów, przekaźnika i źródeł dzienników baz w bazie platformy.

UPRAWNIENIA

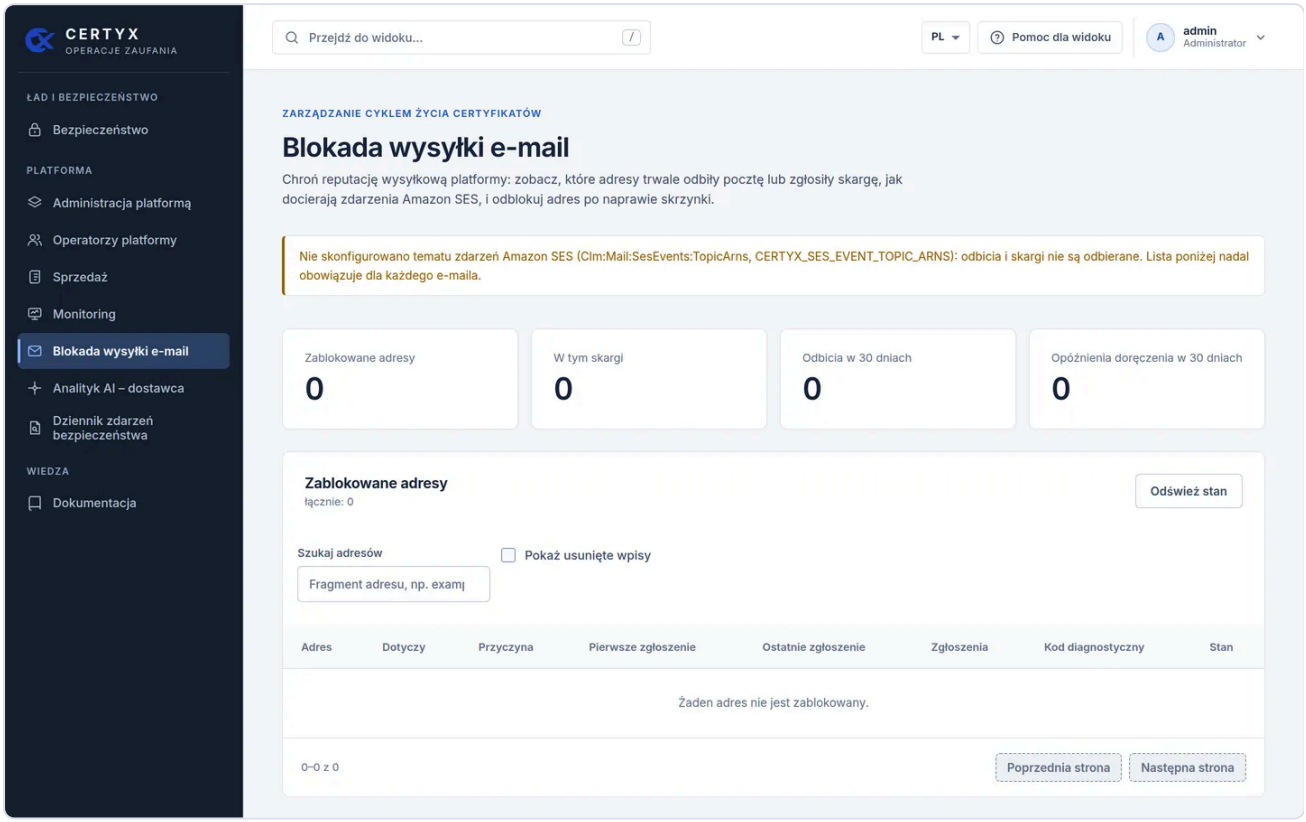
Wyłącznie dopuszczony zarządca platformy z sesją uwierzytelnioną przez MFA. Każda zmiana ustawień i każdy alert testowy trafia do dziennika bezpieczeństwa bez wartości sekretów. Step-up: każda zmiana w tym widoku (poza testami, sprawdzeniami połączenia i potwierdzeniem incydentu) prosi o bieżący 6-cyfrowy kod Twojej aplikacji uwierzytelniającej; potwierdzony kod obejmuje także kolejne zmiany w centrum sterowania przez Clm:Identity:OperatorStepUpWindow (domyślnie 5 minut). Błędny lub już użyty kod jest odrzucany, wlicza się do blokady konta i jest zapisywany w dzienniku; Anuluj porzuca zmianę. Operatorzy logujący się przez logowanie firmowe nie mają lokalnej aplikacji uwierzytelniającej i nie mogą wprowadzać tych zmian. Role operatorów: wsparcie, administrator bezpieczeństwa i administrator widzą monitoring i obsługują incydenty; ustawienia alertów (kanały, relay, źródła dzienników) wymagają administratora bezpieczeństwa lub administratora.

OGRANICZENIA

Liczniki zerują się po restarcie. To wykrywanie wybranych objawów, nie pełna ochrona przed włamaniem. Każda instancja sama wykonuje sondy i liczy metryki; bez bazy platformy ma też własną historię incydentów i sama wysyła alerty, więc wtedy uruchamiaj jedną instancję. Gdy baza platformy jest niedostępna, nowe incydenty nie są zapisywane do czasu jej powrotu. Incydenty sprzed aktualizacji i zaimportowane z pliku nie są alarmowane ponownie, a nowy kanał dostaje tylko późniejsze zmiany. Kursory dzienników baz zarządzanych startują od nowa po restarcie, więc stara awaria może zostać zgłoszona ponownie. Dziennik bezpieczeństwa jest eksportowany do miejsc docelowych SIEM skonfigurowanych w Dzienniku zdarzeń bezpieczeństwa → Eksport do SIEM (zakresy platformy) oraz przez każdą organizację (Eksport do SIEM); pełny audyt bazy nie jest częścią tego widoku. Dedykowani klienci są sprawdzani cyklicznie partiami (Clm:Monitoring:CustomerProbeBatchSize, domyślnie 10 w każdym cyklu Clm:Monitoring:ProbeInterval, domyślnie 30 sekund); znaczniki czasu pokazują nieaktualne obserwacje. Historia incydentów przechowuje najwyżej Clm:Monitoring:IncidentRetention incydentów (domyślnie 5000), usuwając najpierw rozwiązane. Ustawienia alertów i źródeł dzienników wymagają bazy platformy; wartości z pliku konfiguracji są przejmowane jednorazowo przy pierwszym uruchomieniu, a potem rozstrzyga konsola. Ścieżki CLI dostawców, lokalny dziennik JSON PostgreSQL i limit czasu doręczenia alertu są ustawieniami wdrożenia. Udany test dowodzi przyjęcia wiadomości przez miejsce docelowe, a nie powiadomienia dyżurnego.

25 Blokada wysyłki e-mail

Chroń reputację wysyłkową platformy: zobacz, które adresy trwale odbiły pocztę lub zgłosiły skargę, jak docierają zdarzenia Amazon SES, i odblokuj adres po naprawie skrzynki.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Zaloguj się jako dopuszczony administrator platformy z MFA i otwórz w centrum sterowania Blokada wysyłki e-mail. Wiersz stanu mówi, czy zdarzenia Amazon SES są odbierane (liczba dozwolonych tematów SNS i ostatnie zdarzenie), a kafelki pokazują zablokowane adresy, w tym skargi, oraz odbicia i opóźnienia doręczenia z ostatnich 30 dni.
2. Amazon SES zgłasza każde odbicie, skargę, odrzucenie i opóźnienie doręczenia poczty platformy do tematu SNS instalacji, który przesyła je na https://<konsola>/public/api/mail-events/ses. CERTYX sprawdza podpis SNS (certyfikat tylko z sns.<region>.amazonaws.com, łańcuch do publicznego urzędu głównego, podmiot sns.amazonaws.com), temat względem Clm:Mail:SesEvents:TopicArns, wiek wiadomości i MessageId (powtórzenie niczego nie zmienia) oraz sam potwierdza subskrypcję.
3. Trwałe odbicie lub skarga dodaje każdego wskazanego odbiorcę do listy (przyczyna, pierwsze i ostatnie zgłoszenie, liczba zgłoszeń, kod diagnostyczny dostawcy; nigdy treść wiadomości) i trafia do dziennika jako mail.suppression.added. Tymczasowe odbicia, opóźnienia doręczenia i odrzucenia są tylko zliczane. Każdy wpis ma zakres (kolumna Dotyczy): poczta, którą platforma wysyła dla organizacji (e-maile konfiguracji uwierzytelniacza), niesie organizację w tagu wiadomości Amazon SES certyx-scope, więc jej odbicie lub skarga blokuje adres tylko dla tej organizacji; poczta platformy (operatorzy,

alerty, sprzedaż) i zdarzenia bez tagu (np. powiadomienia zwrotne SES albo wpisy sprzed blokad per organizacja) blokują go dla całej poczty. Poczta organizacji sprawdza wpisy ogólnoplatformowe i własne, nigdy innej organizacji.

4. Każdy e-mail platformy przed wysłaniem sprawdza listę: powiadomienia organizacji (zablokowani odbiorcy są pomijani; wpis skrzynki nadawczej to odnotowuje albo jest anulowany, gdy nikt nie pozostał), wiadomości testowe, e-maile konfiguracji aplikacji uwierzytelniającej (konsola pokazuje wtedy odnośnik z przyczyną), e-maile alertów (kanał otwiera incydent zamiast ponawiać) i e-maile sprzedaży (komunikat jest oznaczony Nie wysłano: odbiorca zablokowany). Kopia operatora powiadomień rozliczeniowych jest pomijana, gdy jest zablokowana.
5. Szukaj po fragmencie adresu; Pokaż usunięte wpisy pokazuje także usunięte adresy z informacją, kto, kiedy i dlaczego je usunął.
6. Gdy skrzynka znowu działa, wybierz Usuń z blokady, wpisz powód i potwierdź. Usunięcie trafia do dziennika jako mail.suppression.removed, a CERTYX od razu znowu wysyła na ten adres; nowe odbicie lub skarga zablokuje go ponownie. Usuń adres także z listy blokad na poziomie konta Amazon SES (konsola SES → Suppression list albo aws sesv2 delete-suppressed-destination --email-address <adres>), inaczej SES nadal odrzuca wiadomości do niego. Usunięcie dotyczy wpisu wybranego wiersza (jego zakresu); adres zablokowany w kilku zakresach zachowuje pozostałe wpisy.

DANE I PARAMETRY

- Wyszukiwanie: fragment adresu (do 254 znaków, bez rozróżniania wielkości liter).
- Powód usunięcia: od 3 do 500 znaków bez podziałów wiersza, na przykład: skrzynka ponownie utworzona przez klienta 14 października.
- Ustawienia instalacji (poza konsolą): Clm:Mail:SesEvents:TopicArns (na hoście CERTYX_SES_EVENT_TOPIC_ARNS), dozwolone ARN tematów SNS; MaxMessageAge (domyślnie 1 godzina), MaxClockSkew (5 minut), MaxBodyBytes (256 KiB), EventRetention (90 dni) i SigningCertificateSubjects (sns.amazonaws.com).

WYNIK OPERACJI

Jedna lista blokad w bazie danych platformy, wspólna dla wszystkich ścieżek e-mail i wszystkich organizacji, z wpisem w dzienniku dla każdego dodanego (aktor system:amazon-ses) i usuniętego adresu (operator). Administratorzy organizacji widzą zablokowanych członków swoich grup w widoku Grupy powiadomień. Wpisy mają zakres: cała platforma albo organizacja, której poczta je spowodowała.

UPRAWNIENIA

Tylko administratorzy platformy z MFA widzą listę i usuwają adresy. Użytkownicy organizacji widzą wyłącznie zablokowanych członków własnych grup odbiorców (Grupy powiadomień) i nie mogą ich usuwać: lista chroni wspólną reputację wysyłkową platformy. Step-up: każda zmiana w tym widoku (poza testami, sprawdzeniami połączenia i potwierdzeniem incydentu) prosi o bieżący 6-cyfrowy kod Twojej aplikacji uwierzytelniającej; potwierdzony kod obejmuje także kolejne zmiany w centrum sterowania przez Clm:Identity:OperatorStepUpWindow (domyślnie 5 minut). Błędny lub już użyty kod jest odrzucany, wlicza się do blokady konta i jest zapisywany w dzienniku; Anuluj porzuca zmianę. Operatorzy logujący się przez logowanie firmowe nie mają lokalnej aplikacji uwierzytelniającej i nie mogą wprowadzać tych zmian.

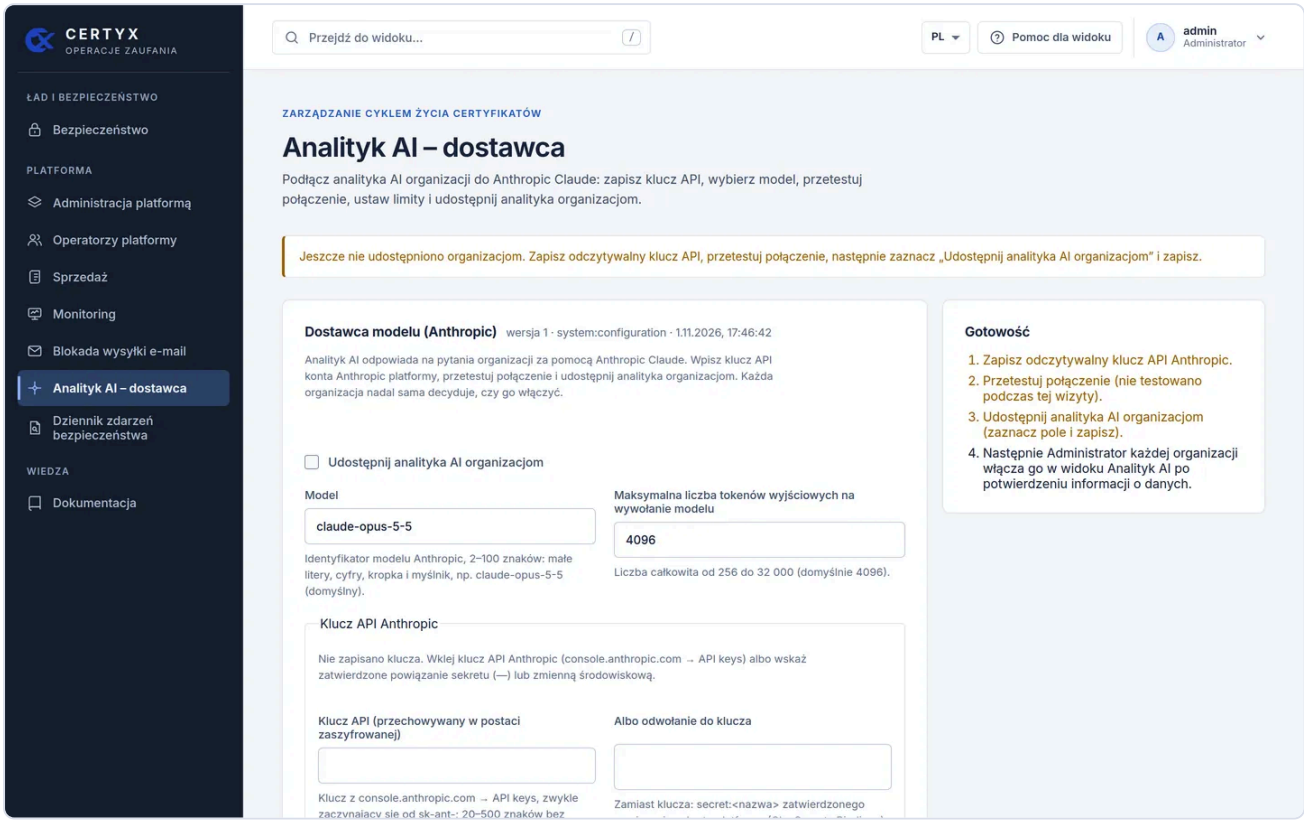
OGRANICZENIA

Wymaga bazy danych platformy; bez niej CERTYX niczego nie blokuje (lista jest pokazywana jako niedostępna), a zdarzeń SES nie da się odbierać. Bez dozwolonego tematu punkt końcowy odpowiada 404, a wiersz stanu informuje, że zdarzenia nie są odbierane; lista nadal obowiązuje. Zdarzenia są rzadkie: długi

brak zdarzeń jest normalny. Gdy bazy danych platformy nie da się odczytać, poczta jest wysyłana bez sprawdzenia (nadal działa lista blokad na poziomie konta Amazon SES). Rozumiane są tylko zdarzenia Amazon SES przez SNS; odbicia innych dostawców (przy własnym przekaźniku organizacji) nie są odbierane. Usunięcie tutaj nie usuwa adresu z listy na poziomie konta SES. Blokada dotyczy adresu we wszystkich organizacjach.

26 Analityk AI – dostawca

Podłącz analityka AI organizacji do Anthropic Claude: zapisz klucz API, wybierz model, przetestuj połączenie, ustaw limity i udostępnij analityka organizacjom.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Zaloguj się jako dopuszczony administrator platformy z MFA i otwórz w centrum sterowania Analityk AI – dostawca. Wiersz stanu i lista Gotowość pokazują, czego jeszcze brakuje: odczytywalnego klucza, udanego testu połączenia i udostępnienia organizacjom.
2. W sekcji Klucz API Anthropic wklej klucz z console.anthropic.com → API keys w pole Klucz API (przechowywany w postaci zaszyfrowanej) albo zamiast tego podaj odwołanie: secret:<powiązanie> dla zatwierdzonego powiązania sekretu platformy lub env:<ZMIENNA> dla zmiennej środowiskowej aplikacji. Wypełnij tylko jedno z pól; puste pola zachowują zapisany klucz; Usuń zapisany klucz go kasuje. Zapisany klucz nigdy nie jest ponownie wyświetlany: puste pole klucza pokazuje wtedy „klucz zapisany — wpisz nowy, aby go zastąpić", a wiersz nad polami podaje, skąd pochodzi klucz.
3. Wybierz Testuj połączenie. Wysyłane jest jedno krótkie żądanie (kilka tokenów wyjściowych, bez narzędzi, bez danych organizacji) z wartościami z formularza — także niezapisanym kluczem lub modelem — albo z zapisanymi ustawieniami, a wynik jest raportowany: Połączenie działa, Klucz odrzucony (401), Brak uprawnień (403), Nie znaleziono modelu (404), Osiągnięto limit lub przydział (429), Problem z rozliczeniem (saldo środków), Żądanie odrzucone (400), Dostawca przeciążony (529), Błąd dostawcy, Dostawca nieosiągalny (DNS, zapora, proxy, TLS) lub Brak odpowiedzi na czas, wraz ze statusem HTTP, typem błędu i komunikatem dostawcy, modelem i czasem. Brak klucza lub nieczytelny klucz jest zgłaszany bez wysyłania czegokolwiek.

4. Sprawdź model (domyślnie claude-opus-5-5) i tokeny wyjściowe, zaznacz Udostępnij analityka AI organizacjom i wybierz Zapisz ustawienia. Wiersz stanu pokaże Gotowe i adres dostawcy.
5. Administrator każdej organizacji nadal włącza analityka we własnym widoku Analityk AI po potwierdzeniu informacji o danych; dopiero wtedy jej użytkownicy mogą zadawać pytania.

DANE I PARAMETRY

- Klucz API: 20–500 znaków bez spacji (klucze Anthropic zwykle zaczynają się od sk-ant-). Szyfrowany pękiem kluczy ochrony danych platformy (wspólnym dla wszystkich instancji przez bazę danych platformy) i zapisywany jako protected:<szyfrogram>; nigdy ponownie wyświetlany, zwracany przez API, dziennikowany ani logowany.
- Odwołanie do klucza: secret:<nazwa> powiązania z Clm:Secrets:Bindings (odczytywanego tożsamością maszyny przy wysyłaniu pytania) albo env:<ZMIENNA> (wielkie litery, cyfry, podkreślenia).
- Model: 2–100 małych liter, cyfr, kropek lub myślników, np. claude-opus-5-5. Maksymalna liczba tokenów wyjściowych na wywołanie 256–32 000 (domyślnie 4096).
- Limity: pytania na użytkownika na godzinę 1–10 000 (domyślnie 30), pytania na organizację na dzień 1–100 000 (domyślnie 300), tokeny na organizację na dzień 1 000–1 000 000 000 (domyślnie 2 000 000).

WYNIK OPERACJI

Wersjonowany dokument ustawień w bazie danych platformy (klucz analyst); każdy zapis trafia do dziennika jako analyst.settings.updated, a zapisany klucz widnieje tylko jako „stored”; każdy test połączenia jako analyst.connection.tested z wynikiem, statusem HTTP, modelem i źródłem klucza. Organizacje widzą analityka jako dostępnego, gdy jest udostępniony, a klucz daje się odczytać.

UPRAWNIENIA

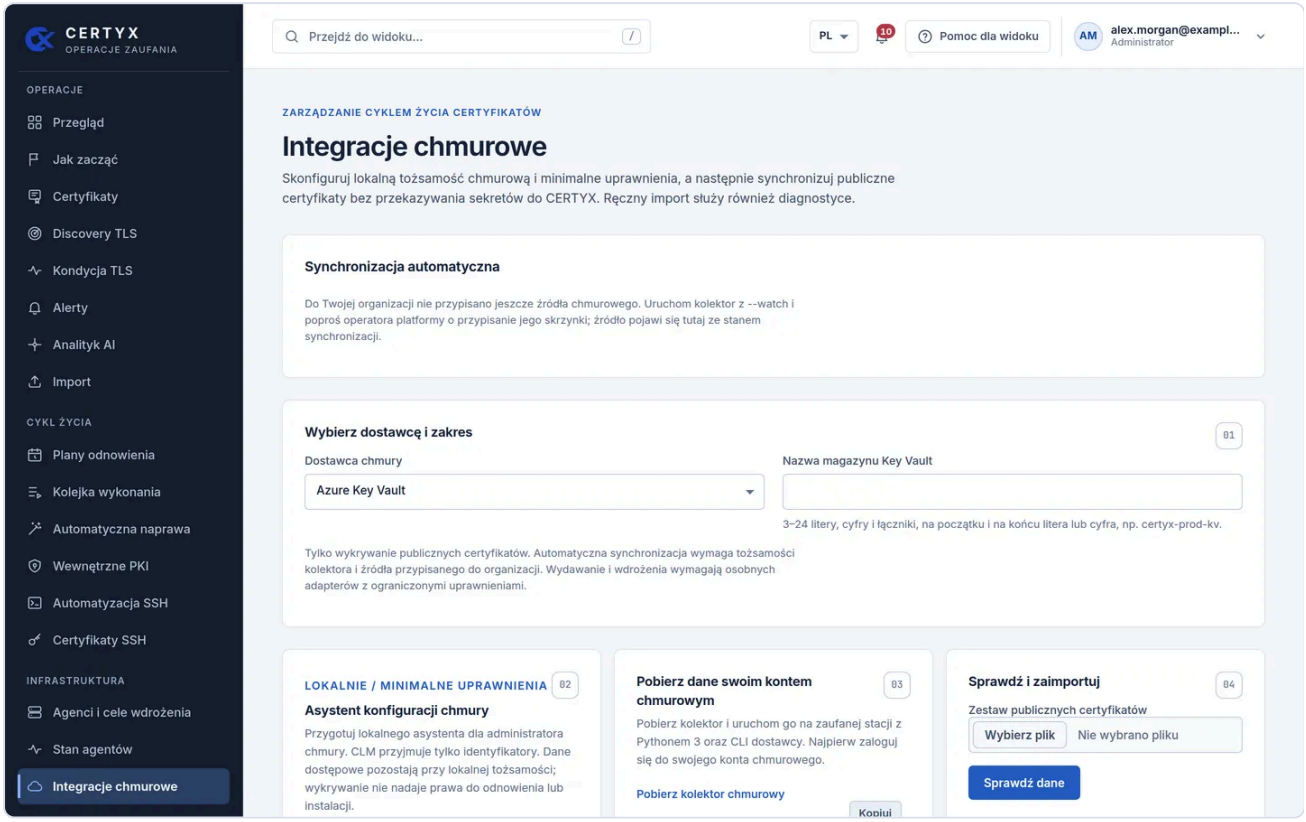
Tylko administratorzy platformy z MFA. Użytkownicy organizacji nie widzą klucza ani tego widoku. Step-up: każda zmiana w tym widoku (poza testami, sprawdzeniami połączenia i potwierdzeniem incydentu) prosi o bieżący 6-cyfrowy kod Twojej aplikacji uwierzytelniającej; potwierdzony kod obejmuje także kolejne zmiany w centrum sterowania przez Clm:Identity:OperatorStepUpWindow (domyślnie 5 minut). Błędny lub już użyty kod jest odrzucany, wlicza się do blokady konta i jest zapisywany w dzienniku; Anuluj porzuca zmianę. Operatorzy logujący się przez logowanie firmowe nie mają lokalnej aplikacji uwierzytelniającej i nie mogą wprowadzać tych zmian.

OGRANICZENIA

Bez bazy danych platformy (samodzielna instalacja) wartości z Clm:Analyst w konfiguracji są pokazywane tylko do odczytu i nie można tu wpisać klucza; Testuj połączenie nadal je sprawdza. Klucza zaszyfrowanego innym pękiem kluczy nie da się odczytać i trzeba go wpisać ponownie. Adres dostawcy (Clm:Analyst:BaseUrl, domyślnie https://api.anthropic.com) ustawia się wyłącznie w konfiguracji. Test połączenia czeka najwyżej 30 sekund i nie ponawia prób. Udany test potwierdza klucz, model i ścieżkę sieciową w danej chwili; nie ocenia jakości odpowiedzi. Dane przetwarza Anthropic na podstawie umowy operatora z Anthropic.

27 Integracje chmurowe

Skonfiguruj lokalną tożsamość chmurową i minimalne uprawnienia, a następnie synchronizuj publiczne certyfikaty bez przekazywania sekretów do CERTYX. Ręczny import służy również diagnostyce.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Wybierz AWS, Azure lub GCP i zakres. Wypełnij lokalnego asystenta IAM wyłącznie publicznymi identyfikatorami. GCP wymaga istniejącego konta usługi w wybranym projekcie; rola z jednym uprawnieniem pozwala listować publiczne certyfikaty, bez tworzenia kluczy konta i federacji.
2. Wybierz „Pobierz konfigurację asystenta” (clm-cloud-setup.json; błędny identyfikator jest odrzucany z podaniem oczekiwanego formatu) i „Pobierz lokalnego asystenta” (cloud-setup.py). Uruchom plan lokalnie, aby przygotować minimalne polityki bez zmian w chmurze.
3. Sprawdź polityki. Uruchom apply jako uprawniony administrator chmury i jawnie potwierdź zakres. Powstają tylko uprawnienia wykrywania.
4. Skonfiguruj tożsamość usługi kolektora i uruchom doctor jako ta tożsamość. Nieudane testy zwracają kod błędu; pusty zakres jest oznaczony jako nie w pełni sprawdzony.
5. W kroku „Pobierz dane swoim kontem chmurowym” pobierz cloud-collect.py i po zalogowaniu CLI dostawcy uruchom wyświetlone polecenie; zapisuje ono nowy plik clm-cloud.json i nie nadpisuje istniejącego.

6. Do automatycznej synchronizacji uruchom kolektor z --watch SEKUNDY (co najmniej 300) i poproś operatora platformy o przypisanie jego prywatnej skrzynki do tej organizacji. Synchronizacja automatyczna pokazuje wtedy każde przypisane źródło ze stanem: oczekuje na pierwszą synchronizację, działa, częściowy wynik, błąd z przyczyną lub wstrzymane przez operatora, wraz z liczbą certyfikatów, ostatnim sukcesem i ostatnią próbą. Panel odświeża się co 30 sekund, gdy widok jest otwarty. Gdy nie przypisano jeszcze źródła, panel to wyraźnie pokazuje. Ręczny import pozostaje do diagnostyki.
7. Ręczny import („Sprawdź i zaimportuj”): wybierz plik z danymi i „Sprawdź dane”. Serwer sprawdza plik bez zapisywania i pokazuje dostawcę, zakres, liczbę certyfikatów, ostrzeżenia i certyfikaty. „Importuj do tej organizacji” dodaje nowe certyfikaty i podaje liczbę dodanych, już istniejących oraz informację o wyniku częściowym. Bez grafu zaufania w subskrypcji dostępny jest tylko podgląd.
8. Agent cyklu certyfikatów w Unix może odczytywać zatwierdzone sekrety tekstowe Azure Key Vault, AWS Secrets Manager i Google Secret Manager przez lokalną tożsamość CLI klienta. Ustaw dokładne SecretBindings i uruchom Clm.Agent secret-check z chronioną konfiguracją jako konto usługi przed włączeniem wykonania. Wartości pozostają lokalnie i nie są wyświetlane. Zobacz CUSTOMER-VAULTS.pl.md. Odczyt przez CLI dostawców działa tylko w agentach Unix; w Windows dostępne są wyłącznie sekrety z chronionych plików. Klucze prywatne są generowane i przechowywane programowo na hoście agenta (bez HSM), a agent nie wysyła poczty z hosta klienta.
9. HashiCorp Vault KV obsługuje dokładną referencję HTTPS mount/ścieżka#pole i lokalny token helper klienta. Weryfikacja TLS jest obowiązkowa; przestrzenie nazw nie są obsługiwane. Odczyt kończy się błędem, gdy dostęp jest zabroniony, tożsamość unieważniona lub certyfikat Vault niezaufany. Token Vault pochodzi z token helpera klienta; CERTYX nie tworzy ani nie odnawia tożsamości Vault.
10. Cykl życia AWS obsługuje certyfikaty importowane do ACM. Na hoście Unix klienta komenda aws-adopt <chroniona-konfiguracja-agenta> <id-celu> <chroniona-referencja-klucza-json> przygotowuje chroniony stan do rollbacku po sprawdzeniu klucza, rzeczywistego endpointu TLS i niezmienionego odcisku ACM. Komenda tylko odczytuje AWS; nie podmienia certyfikatu w chmurze. Istniejący stan wymaga odzyskiwania zamiast ponownego przejęcia.
11. Paczka AWS zawiera agent.aws-vault.json, aws-baseline-key.json i AWS-LIFECYCLE.md. Podmień lokalnie wartości zastępcze; przykład Vault wystawia certyfikaty prywatnej CA. Zadanie odnowienia kończy się sukcesem dopiero wtedy, gdy ACM przechowuje nowy certyfikat, a niezależna weryfikacja TLS obsługiwanego punktu końcowego przechodzi pomyślnie. Ten widok nie przyjmuje poświadczeń.
12. Dla zatwierdzonego importowanego certyfikatu AWS komenda aws-plan <chroniona-konfiguracja-agenta> <id-celu> generuje minimalną politykę uprawnień zasobu bez kontaktu z AWS. Nie nadaje zaufania roli i nie tworzy infrastruktury. Przed zastosowaniem planu przeczytaj AWS-LIFECYCLE.md.
13. Operacje magazynów AWS ACM i Azure Key Vault zastępują certyfikat, odczytują go ponownie, przywracają chronioną wersję bazową, gdy zmianę trzeba wycofać, i odrzucają certyfikat z niepasującym kluczem. Odnowienie AWS zachowuje algorytm, rozmiar klucza i zastosowania z chronionej wersji bazowej; migracja wymaga nowego zasobu.
14. DigiCert CertCentral: na hoście klienta polecenie Clm.Agent digicert-collect <konfiguracja> <id-celu> <wynik.json> odczytuje zakupione certyfikaty kluczem API przechowywanym lokalnie i zapisuje migawkę (provider digicert) do importu tutaj; ostrzeżenia wskazują walidacje domen i organizacji wygasające w ciągu 60 dni. Cele agenta typu digicert zamawiają lub ponownie wystawiają certyfikaty w granicach skonfigurowanej polityki zakupów.

15. Dla wykonania przez agenta Azure ustaw identyczny zakres AzureKeyVault (VaultUrl, CertificateName, TenantId, ManagedIdentityClientId) na serwerze i u klienta oraz niezależny VerifyHost. Użyj jednej tożsamości zarządzanej przypisanej przez użytkownika. Na hoście klienta polecenie azure-adopt <chroniona-konfiguracja-agenta> <id-celu> <chroniona-referencja-klucza-json> <chroniona-referencja-publicznego-łańcucha-json> odczytuje i weryfikuje istniejący certyfikat oraz przygotowuje chronioną generację do wycofania wdrożenia. Referencje są rozwiązywane lokalnie. Klucz nie jest eksportowany z Azure ani przesyłany do CERTYX. Patrz AZURE-LIFECYCLE.md. Sam import wersji do sejfu nie oznacza poprawnego wdrożenia: zadanie kończy się sukcesem dopiero po niezależnej weryfikacji TLS, a CERTYX nie przełącza powiązań aplikacji w korzystających usługach Azure na nową wersję. Ten przepływ generacji chmurowych działa tylko w agentach Unix.
16. Wykrywanie GCP: wybierz Google Certificate Manager i wpisz dokładny identyfikator projektu. Uruchom wyświetlone cloud-collect.py gcp PROJEKT --location global lokalnie u klienta z zatwierdzoną tożsamością do odczytu. Zaimportuj publiczny plik tutaj albo użyj --watch i chronionej skrzynki synchronizacji. Parametr --location wskazuje osobno zatwierdzoną lokalizację regionalną. Brak publicznego PEM, także przy oczekiwaniu na wydanie, jest ostrzeżeniem. Asystent IAM tworzy projektową rolę odczytu publicznej listy dla istniejącego konta usługi GCP. Uruchom doctor z jawną impersonacją konta; wymaga to wcześniej zatwierdzonej federacji lub prawa do uzyskania krótkotrwałego tokenu u klienta. Asystent nie nadaje token-creator ani nie tworzy kluczy konta.
17. Asystent GCP zapisuje chroniony gcp-apply-receipt.json przed zmianą IAM. Istniejący zapis blokuje powtórne zmiany. Uruchom cloud-setup.py reconcile --config KONFIGURACJA.json --output KATALOG-PLANU, aby tylko sprawdzić dokładne uprawnienia i powiązanie. Częściowe zmiany uzgadnia administrator IAM klienta na podstawie audytu dostawcy; reconcile nie rozszerza uprawnień.
18. Przy przejmowaniu stanu GCP (gcp-adopt <chroniona-konfiguracja-agenta> <id-celu> <chroniona-referencja-klucza-json> [chroniona-referencja-publicznego-łańcucha-json]) możesz dodać na końcu chronioną referencję publicznego łańcucha, jeśli Google nie zwraca wystawców. Agent sprawdza łańcuch względem zatwierdzonych korzeni przed zapisem stanu do rollbacku. Klucz pozostaje u klienta.
19. Na Compute Engine agent może jawnie wybrać gcpIdentityKind=metadata dla zatwierdzonego konta przypisanego do maszyny, bez referencji poświadczeń i klucza konta. Klient konfiguruje IAM i zakres OAuth maszyny. Nadal dostępne są federacja i sejf klienta.

DANE I PARAMETRY

- Publiczne certyfikaty PEM i identyfikatory zasobów chmurowych; bez danych dostępowych, sekretów i kluczy prywatnych.
- Plik danych: JSON o rozmiarze najwyżej 5 MB, do 250 certyfikatów; dane starsze niż 30 dni są odrzucane. Dostawcy przyjmowani w plikach: azure, aws, gcp i digicert.
- Formaty zakresu i tożsamości (pokazane pod każdym polem; błędna wartość jest odrzucana z podaniem oczekiwanego formatu): nazwa magazynu Azure 3–24 litery, cyfry i łączniki; region AWS, np. eu-central-1, identyfikator konta z 12 cyfr i rola arn:aws:iam::KONTO:role/NAZWA; identyfikator projektu GCP z 6–30 małych liter, cyfr i łączników; identyfikator zasobu sejfu Azure /subscriptions/.../providers/Microsoft.KeyVault/vaults/NAZWA-MAGAZYNU i object ID jako GUID; konto usługi GCP NAZWA@ID-PROJEKTU.iam.gserviceaccount.com wybranego projektu.
- Uprawnienia przygotowywane (plan) i nadawane (apply) przez asystenta: AWS — rola klienta zaufana wyłącznie dla podanej roli obciążenia z unikalnym external ID (sts:AssumeRole), z prawem acm:ListCertificates w wybranym regionie oraz acm:DescribeCertificate i acm:GetCertificate dla certyfikatów tego konta i regionu; Azure — rola niestandardowa z jedną akcją danych

Microsoft.KeyVault/vaults/certificates/read, przypisana tożsamości zarządzanej na jednym magazynie; Google Cloud — rola projektu z jednym uprawnieniem certificatemanager.certs.list, przypisana istniejącemu kontu usługi. Nie są nadawane uprawnienia do sekretów, kluczy prywatnych, wystawiania ani wdrażania. Kolektor raportuje zakres migawki jako nazwę magazynu Azure, KONTO:REGION dla AWS i PROJEKT:LOKALIZACJA dla GCP.

WYNIK OPERACJI

Certyfikaty trafiają do inwentarza, a zasoby i zależności do grafu. Powtórzenie importu nie duplikuje certyfikatów.

UPRAWNIENIA

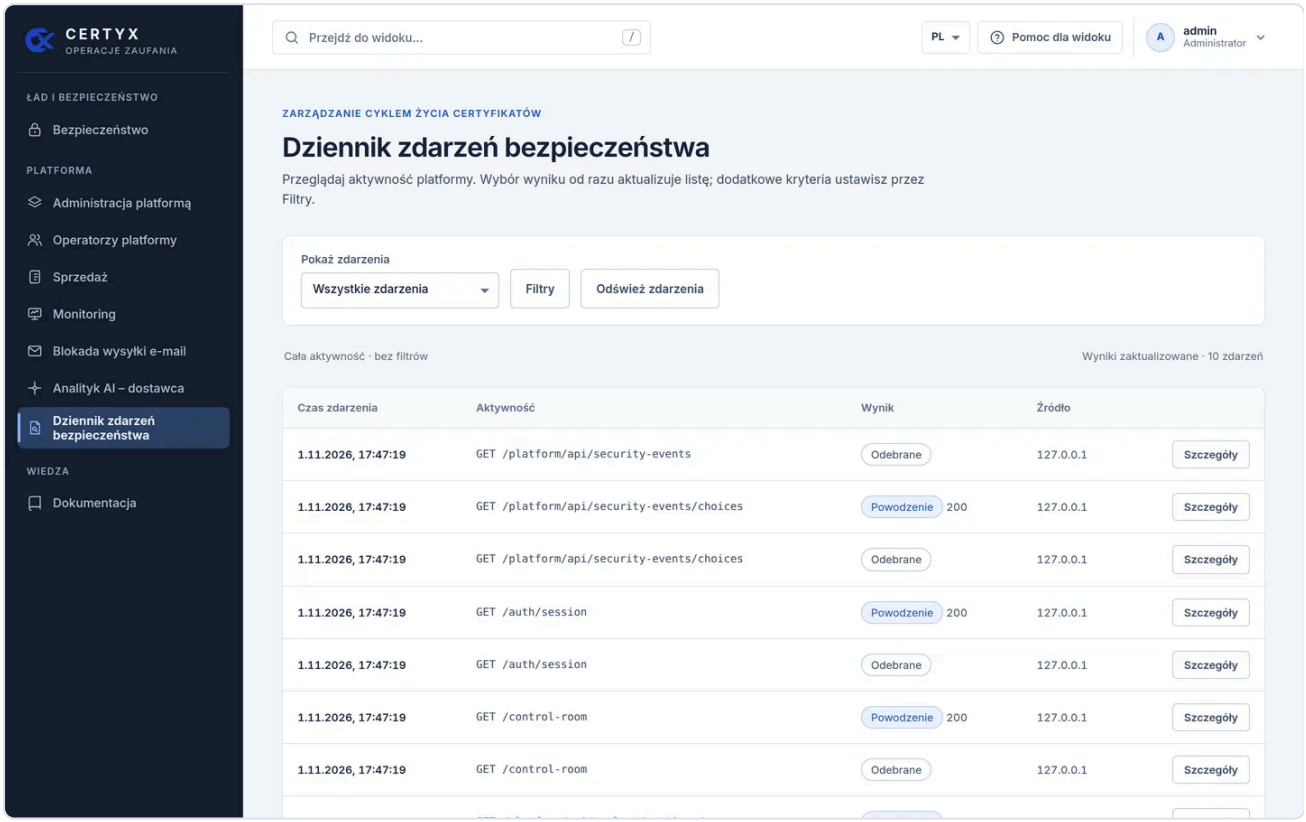
Asystent konfiguracji i polecenie kolektora są dostępne dla każdej roli organizacji. Stan synchronizacji, podgląd i import danych: Admin. Import wymaga dodatkowo grafu zaufania w subskrypcji.

OGRANICZENIA

Asystent wymaga Python 3 i CLI dostawcy. Tworzy role dla istniejącej tożsamości usługi; nie tworzy ani nie przypina tożsamości maszyn ani federacji. Azure wymaga sejfu z RBAC. Konfiguracja chmury wymaga lokalnych uprawnień administratora, a kolektor tylko odczytu certyfikatów. Sekrety nie są przyjmowane. Udany odczyt nie dowodzi braku szerszych uprawnień. Odnowienie i wdrożenie wykonuje agent cyklu życia dla celu wykonania z jednym zasobem chmurowym: AWS ACM (ponowny import do tego samego ARN certyfikatu), Azure Key Vault (nowa wersja tego samego certyfikatu) i Google Certificate Manager (aktualizacja tego samego certyfikatu self-managed); zlecenie kończy się sukcesem dopiero po niezależnej weryfikacji TLS obsługiwanego punktu końcowego. Import do magazynu nie przełącza usług Azure ani Google korzystających z certyfikatu na nową wersję. Poświadczenia i klucze prywatne pozostają pod kontrolą klienta. Sekrety są odczytywane z chronionych plików, HashiCorp Vault KV, Azure Key Vault, AWS Secrets Manager i Google Secret Manager; inne sejfy nie są obsługiwane, CLI dostawców działają tylko w agentach Unix, a agent nie wysyła poczty z hosta klienta. Uprawnienia pliku tokenu Vault w Unix są sprawdzane przy każdym użyciu. Operacja zapisu w Azure Key Vault zachowuje istniejącą politykę certyfikatu, tagi, stan włączenia i format PEM/PFX. Import programowy odmawia zapisu przy braku polityki, wyłączonym certyfikacie oraz kluczu HSM. Adapter nie wdraża certyfikatu na punkty końcowe Azure. Widok nie tworzy load balancerów (ALB). Chmura klienta jest opcjonalna: własny Vault KV/PKI pozostaje alternatywą pod kontrolą klienta; chronione pliki to tryb zgodności, nie szyfrowany sejf. DigiCert jest dostawcą do wyboru, nie warunkiem założenia konta. Odczyt sekretów Google Secret Manager jest niezależny od cyklu życia certyfikatów Google Certificate Manager. Publiczne pola importu certyfikatów nigdy nie mogą zawierać kluczy prywatnych. Weryfikację AWS ogranicza okno zbieżności agenta (dla celów AWS ACM sześć minut, chyba że Settings.Connectors.CloudVerification agenta ustawia inne ConvergenceWindow, ponieważ ALB może wstrzymywać TLS dłużej niż dwie minuty podczas propagacji ponownego importu): aws-store-unread oznacza, że w tym czasie nie zakończył się żaden odczyt ACM; aws-store-not-converged oznacza brak zgodności ostatniego odczytu ACM z zatwierdzonym odciskiem; aws-endpoint-not-verified oznacza zgodny ACM, ale nie każdy adres load balancera serwował certyfikat z poprawnym łańcuchem i stanem usługi. Ograniczenie liczby zapytań (throttling) i przekroczony czas odczytu są ponawiane w tym limicie; błędy dostępu, tożsamości i walidacji przerywają weryfikację od razu. Oba wyniki wymagają analizy i nie potwierdzają wdrożenia. Anulowanie przez klienta pozostaje anulowaniem. Niezakończony dziennik przywracania AWS wymusza kontrolowany import poprzedniej chronionej generacji, nawet gdy pojedynczy odczyt ACM jest już zgodny. Zakończenie nadal wymaga niezależnej weryfikacji TLS; przy błędzie dziennik pozostaje do uzgodnienia. Apply i reconcile GCP działają tylko w Unix, ponieważ ich zapisy wymagają ścieżek Unix dostępnych tylko dla właściciela.

28 Dziennik zdarzeń bezpieczeństwa

Przeglądaj aktywność platformy. Wybór wyniku od razu aktualizuje listę; dodatkowe kryteria ustawisz przez Filtry.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. W polu Pokaż zdarzenia nad tabelą (10 zdarzeń na stronę, najnowsze najpierw) wybierz Wszystkie zdarzenia, Odmowa, Błąd serwera, Odrzucone żądanie, Powodzenie, Odebrane lub Logowanie; lista aktualizuje się od razu. Odśwież zdarzenia wczytuje najnowsze zdarzenia z bieżącymi filtrami.
2. Zdarzenia logowania (Logowanie) są zapisywane dla każdego udanego i nieudanego logowania, wylogowania, blokady konta i zmiany MFA i przypisywane organizacji użytkownika; logowania operatorów platformy i logowania niepasujące do żadnego konta są zapisywane pod platform. Szczegóły wyświetlają nazwę zdarzenia, adres e-mail użytkownika (przy nieudanym logowaniu oznaczony jako wpisany i niezweryfikowany), sposób logowania, wynik, kod przyczyny i agenta użytkownika; wpisane hasło ani kod nigdy nie są zapisywane.
3. Otwórz Filtry, aby wybrać konto, organizację, IP, czas UTC lub kryteria techniczne. Zastosuj filtry wraca do wyników.
4. Komunikat wczytywania, liczba wyników i aktywnych filtrów pokazują zmianę. Wyczyść filtry przywraca całą aktywność.
5. Szczegóły otwierają pojedyncze zdarzenie. Pokaż to żądanie filtruje bez kopiowania identyfikatora. Każde żądanie ma dwa wpisy: Odebrane, zapisany w chwili nadejścia żądania, zanim serwer sprawdzi, kto je wysłał (użytkownik i organizacja są wtedy jeszcze nieustalone, status 0), oraz wpis wyniku z

użytkownikiem, organizacją i statusem HTTP. Wpis Odebrane nie oznacza nieudanej próby ani ataku; dzięki niemu w dzienniku zostaje ślad także żądania, które zostało przerwane przed odpowiedzią. Pokaż to żądanie wyświetla oba wpisy.

6. Starsze zdarzenia zastępują stronę. Narzędzia dziennika zawierają sprawdzenie integralności, eksport wszystkich zdarzeń zgodnych z filtrami (CSV lub JSON, nie tylko widocznej strony) oraz obowiązujące zasady przechowywania.
7. Po przejściu do starszych stron wybierz Najnowsze zdarzenia, aby wrócić na początek. W Narzędziach dziennika Sprawdź integralność dziennika weryfikuje łańcuch skrótów całego przechowywanego dziennika, a Audyt platformy pokazuje ostatnie 100 zmian biznesowych wykonanych przez zarządców platformy (klienci, subskrypcje, instancje i konta klientów).
8. Eksport do SIEM zarządza miejscami docelowymi całej platformy: zakres Operatorzy platformy (własne zdarzenia operatorów) lub Wszystkie zdarzenia (każda organizacja), następnie transport (HTTPS, Splunk HTTP Event Collector, Syslog przez TLS, Azure Monitor Logs Ingestion dla Microsoft Sentinel, OpenTelemetry Logs (OTLP/HTTP) lub Archiwum plików), format i profil schematu spośród dozwolonych przez serwer, jak w widoku Eksport do SIEM organizacji. Każde miejsce docelowe pokazuje trasę, pozycję, zaległości, ostatni sukces i błąd, kolejne niepowodzenia z czasem następnej próby oraz zdarzenie stale odrzucane przez odbiorcę; Sprawdź połączenie testuje DNS, TCP i TLS bez wysyłania czegokolwiek, a Wyślij zdarzenie testowe dodatkowo doręcza jedno zdarzenie testowe (kategoria Integracja, UUID jako event_id), w obu przypadkach z etapami i zaleceniem. Sieciowe miejsca docelowe mają filtry (wyniki, kategorie, kody zdarzeń, minimalna ważność), zasady dostarczania, opcjonalny certyfikat klienta (wzajemne TLS) i tryb sprawdzania odwołania, a Wyślij ponownie od... cofa pozycję do sekwencji lub punktu w czasie (nigdy do przodu; odbiorcy usuwają duplikaty według event_id). Zmiany wymagają sesji MFA. Dla miejsca docelowego HTTPS dodanego bez sekretu CERTYX generuje sekret podpisu i pokazuje go jeden raz do skopiowania do odbiorcy; Nowy sekret natychmiast go zastępuje (poprzedni przestaje działać) i pokazuje nowy jeden raz. Każde pole prowadzi do właściwej sekcji przewodnika integracji SIEM (także jako PDF w Dokumentacji).
9. Zakres Operatorzy platformy otrzymuje zdarzenia logowania operatorów i logowania nieprzypisane do żadnej organizacji; Wszystkie zdarzenia otrzymuje dodatkowo zdarzenia logowania każdej organizacji. Zaznacz Zdarzenia logowania w polu Eksportowane wyniki, aby wysyłać tylko je, albo pozostaw wszystkie pola niezaznaczone; pomoc eksportu do SIEM w widoku organizacji opisuje pola logowania w każdym formacie.
10. Archiwa plików platformy: w Eksporcie do SIEM wybierz zakres Operatorzy platformy lub Wszystkie zdarzenia, transport Archiwum plików na serwerze i format CSV (układ pierwszego wydania lub kanoniczny) albo NDJSON, z okresem przechowywania i opcjonalnym gzip. Pliki są zapisywane w Clm:Siem:PlatformArchiveDirectory (domyślnie folder platform w Clm:Siem:ArchiveRoot), widoczne w Plikach archiwum z rozmiarem i SHA-256 i do pobrania pojedynczo lub jako zip; pobieranie wymaga sesji z MFA i jest zapisywane w dzienniku. Użyj Wysyłaj tylko w sieciowych miejscach docelowych (wyniki, kategorie, kody zdarzeń, minimalna ważność), aby wysyłać do SIEM mniej, podczas gdy archiwum zachowuje każde zdarzenie; sondy health są wysyłane tylko z Clm:Siem:ExportHealthProbes. Eksportowane zdarzenia zawierają identyfikator, nazwę i rodzaj organizacji oraz instancję, więc zakres Wszystkie zdarzenia można w jednym SIEM rozdzielić według organizacji.

DANE I PARAMETRY

- Wybierz konto lub źródło systemowe z dziennika. Pusty wybór uwzględnia wszystkich.
- Wybierz organizację po nazwie; wpisy systemowe mogą używać technicznych nazw zakresu.
- Wybierz instancję zarejestrowaną w dzienniku.

- Wybierz zarejestrowany status HTTP. Zero oznacza wpis Odebrane, zapisany przed odpowiedzią.
- W rozwiniętym wpisie kliknij Pokaż to żądanie, aby uzupełnić pole automatycznie, albo wpisz identyfikator żądania.
- Opcjonalne IP, fragment ścieżki i zakres czasu UTC.
- Miejsce docelowe SIEM: transport, format i profil schematu; adres HTTPS albo host, port, ramkowanie syslog i separator LEEF 2.0; pola zależne od transportu (sourcetype i indeks Splunk; reguła zbierania danych, strumień, dzierżawa i aplikacja Microsoft Entra dla Sentinel); filtry, zasady dostarczania, opcjonalne zaufane certyfikaty główne, certyfikat i klucz klienta (PEM) oraz tryb sprawdzania odwołania; treść OTLP, nazwa nagłówka uwierzytelniania i gzip; reguły mapowania pól; kształtowanie zdarzeń (gotowe ustawienie Pełne, Zrównoważone, Oszczędne lub Własne ze szczegółowością zmian, zestawem pól, pustymi polami, największym zdarzeniem, stylem nazw, formatem czasu, MSGID i APP-NAME syslog) oraz dodatkowe filtry (trasy, aktorzy, wykluczone kategorie i kody zdarzeń), opisane w pomocy eksportu SIEM; sekret (klucz HMAC, token HEC, klucz tajny klienta lub wartość nagłówka OTLP) i klucz klienta są przechowywane w postaci zaszyfrowanej i nigdy nie są ponownie wyświetlane.

WYNIK OPERACJI

Filtrowany, ograniczony widok zachowanego dziennika bezpieczeństwa, pobierane eksporty przefiltrowanego dziennika i ciągły eksport do miejsc docelowych SIEM. Linki konfiguracyjne aplikacji uwierzytelniającej pojawiają się jako mfa-setup.mail.sent (dostarczenie e-mailem albo jako link pokazany administratorowi, z przyczyną błędu), mfa-setup.mail.used i mfa-setup.mail.expired, przypisane do organizacji konta; sam link nigdy nie jest zapisywany.

UPRAWNIENIA

Zarządca platformy z listy dozwolonych operatorów, którego sesja została zalogowana z MFA; inne tożsamości nie otworzą widoku ani jego API. Zmiany, sprawdzenia, testy, ponowne wysłania i nowe sekrety SIEM są odrzucane dla sesji aplikacji mobilnej CERTYX. Step-up: każda zmiana w tym widoku (poza testami, sprawdzeniami połączenia i potwierdzeniem incydentu) prosi o bieżący 6-cyfrowy kod Twojej aplikacji uwierzytelniającej; potwierdzony kod obejmuje także kolejne zmiany w centrum sterowania przez Clm:Identity:OperatorStepUpWindow (domyślnie 5 minut). Błędny lub już użyty kod jest odrzucany, wlicza się do blokady konta i jest zapisywany w dzienniku; Anuluj porzuca zmianę. Operatorzy logujący się przez logowanie firmowe nie mają lokalnej aplikacji uwierzytelniającej i nie mogą wprowadzać tych zmian.

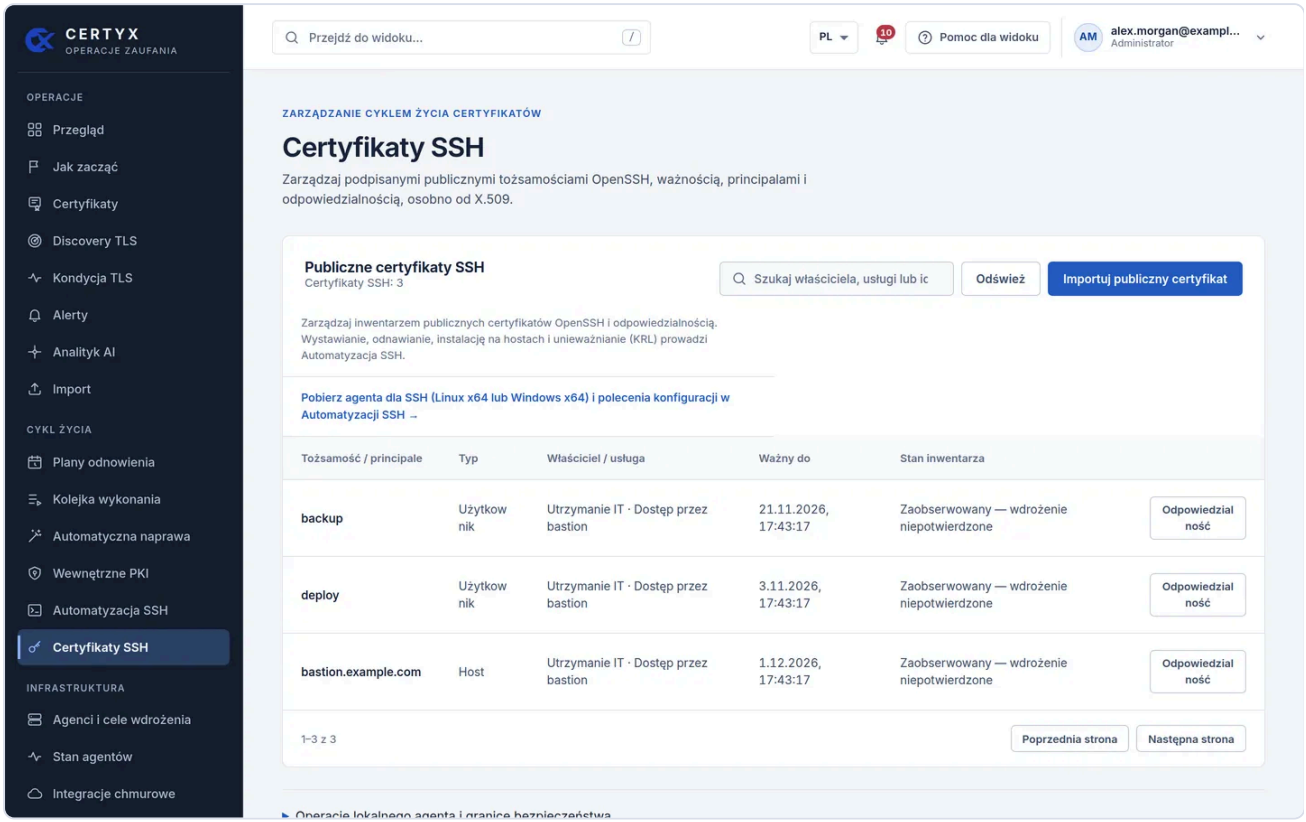
OGRANICZENIA

IP nie dowodzi tożsamości ani lokalizacji. Stronicowanie nie usuwa wpisów. Jeden eksport obejmuje najwyżej Clm:AuditExport:MaxRows zdarzeń (domyślnie 100 000) i sam jest zapisywany w dzienniku. Listy wyboru zawierają do 500 odrębnych wartości; bez bazy platformy (lokalny dziennik plikowy) analizowanych jest ostatnie 5000 wpisów, a eksport do SIEM jest niedostępny. Zdarzenia są przechowywane bez automatycznego usuwania; rola aplikacji może je tylko dodawać i odczytywać. Doręczanie do SIEM odbywa się co najmniej raz: odrzucona partia jest ponawiana z wycofaniem i losowym rozrzutem i otwiera incydent siem-delivery, który po wyczerpaniu prób staje się krytyczny; zaległości powyżej limitu otwierają siem-backlog i nic nie jest usuwane; zdarzenie stale odrzucane przez odbiorcę jest ponawiane aż do przyjęcia, chyba że włączono pomijanie (siem.event.skipped). Odbiorcy usuwają duplikaty według event_id. Wyślij ponownie od... nigdy nie przesuwa pozycji do przodu i jest odrzucane dla archiwów plików; przy miejscach docelowych platformy prosi o kod step-up jak inne zmiany. Miejsca docelowe zdefiniowane w Clm:Siem są widoczne tylko do odczytu. Certyfikat odbiorcy jest zawsze weryfikowany; certyfikat klienta (wzajemne TLS) jest przedstawiany, gdy został wpisany, a sprawdzanie odwołania akceptuje nieznany status w trybie soft-fail (domyślnie) i odrzuca go w trybie hard-fail.

OpenTelemetry Logs używają tylko OTLP/HTTP; częściowy sukces nie jest wysyłany ponownie, lecz zapisywany w dzienniku (siem.event.rejected, incydent siem-rejected) i można go wysłać ponownie przez Wyślij ponownie od. Miejsca docelowe całej platformy mogą używać adresów prywatnych, pętli zwrotnej lub link-local; Clm:Siem:AllowPrivateDestinations ogranicza tylko miejsca docelowe zarządzane przez organizacje. Archiwum CSV platformy zachowuje każde zdarzenie swojego zakresu (Wszystkie zdarzenia: każda organizacja) przez okres przechowywania; zaplanuj miejsce na woluminie archiwum i zamontuj ten sam katalog na każdej instancji. Żądania operatorów platformy są zapisywane pod dzierżawcą platform (jak ich logowania), więc zakres SIEM Operatorzy platformy je eksportuje; wpisy sprzed 18.10.2026 zachowują dzierżawcę platform-control. Każda zmiana operatora u klienta jest dodatkowo zapisywana pod tym klientem (aktor platform:<ID konta operatora>).

29 Certyfikaty SSH

Zarządzaj podpisanymi publicznymi tożsamościami OpenSSH, ważnością, principalami i odpowiedzialnością, osobno od X.509.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Agenta dla SSH (Linux x64 lub Windows x64) z sumami kontrolnymi, podpisami i poleceniami konfiguracji pobierzesz w Automatyzacja SSH → Instalacja i podłączenie agenta SSH.
2. Na zatwierdzonym hoście Unix klienta skonfiguruj lokalną CA SSH, chroniony katalog stanu oraz dozwolone principale użytkowników i hostów.
3. Uruchom Clm.Agent ssh issue <konfiguracja> <UUID-operacji> user|host <principal> <minuty>; powtórzenie tego samego UUID zwraca ten sam certyfikat.
4. Wybierz „Importuj publiczny certyfikat” i wklej wyłącznie publiczny wiersz identity-cert.pub. Przypisz właściciela, usługę i środowisko. Ponowny import tego samego certyfikatu zwraca istniejący wpis bez duplikatu. Wyszukiwanie obejmuje właściciela, usługę lub identyfikator klucza; dłuższe listy przeglądasz przyciskami stron.
5. Przycisk Odpowiedzialność pozwala zmienić właściciela, usługę, środowisko lub archiwizować wpis. Okno pokazuje odcisk CA; weryfikacja podpisu nie potwierdza zaufania do tej CA. Archiwizacja nie unieważnia dostępu na hostach. Jeśli ktoś w międzyczasie zmienił wpis, zapis jest odrzucany; odśwież widok i ponów.
6. Lokalne unieważnienie: Clm.Agent ssh revoke <konfiguracja> <UUID-operacji>. Wdróż wynikowy revoked.krl na każdym serwerze przez RevokedKeys i sprawdź odrzucenie dostępu.

7. Pozostałe polecenia lokalne: ssh list <konfiguracja> wypisuje certyfikaty wystawione przez lokalną CA; ssh deploy-host lub ssh deploy-user <konfiguracja> <konfiguracja-celu> <UUID-operacji> instaluje wystawiony certyfikat hosta lub certyfikat użytkownika procesu na lokalnie skonfigurowanym celu z weryfikacją i wycofaniem; ssh export-krl <konfiguracja> <ID-organizacji> <odcisk-CA> <nowy-plik> zapisuje podpisany publiczny zestaw KRL, a ssh apply-krl <konfiguracja-odbiorcy> <zestaw> stosuje jeden zestaw na odbiorcy.
8. Samodzielne lokalne odnawianie bez raportowania do CERTYX: configure-ssh-linux.sh enable-renewal <pobrany profil> zapisuje renewal.json z lokalnej polityki CA i profilu, wykonuje jeden cykl Clm.Agent ssh renew przez systemd i włącza clm-ssh-renewal.timer (jeden cykl na minutę, bez dostępu do sieci, identyfikator w dzienniku clm-ssh-renewal); w Windows configure-ssh-windows.ps1 enable-renewal rejestruje zadanie CERTYX SSH Renewal. Profil w stanie failed, blocked lub w konflikcie polityki sprawia, że cykl kończy się widocznym błędem (jednostka failed lub niezerowy wynik zadania); renewal-status to pokazuje, a disable-renewal usuwa odnawianie. Profil odnawia albo add-profile, albo enable-renewal. ready-local potwierdza tylko lokalny zestaw; nie oznacza zdalnej instalacji.
9. Odnowienia zarządzane przez platformę i zweryfikowane wdrożenia hosta ustawisz w Automatyzacji SSH. Przypisz aktywne grupy powiadomień i sprawdzaj osobny stan procesu SSH. Lokalnych odbiorców KRL skonfigurujesz w agencie; zdalna dystrybucja do floty pozostaje osobnym wymaganiem.
10. Zdalne przekazywanie KRL pod kontrolą klienta: uruchom ssh publish-krl z chronioną konfiguracją i udostępnij wyłącznie publiczny zestaw przez osobną tożsamość relaya HTTPS. Na odbiorcy uruchom ssh sync-krl z chronioną subskrypcją. Podpisana publikacja wygasa po godzinie i odświeża się automatycznie; przekierowania, brak zaufania, zbyt duże dane, manipulacje i stare publikacje są odrzucane. Błąd zachowuje istniejące unieważnienia. OpenSSH sam nie egzekwuje terminu zestawu. Stan centralnie raportują tylko odbiorcy zarejestrowani do raportowania KRL; CERTYX nie ustala, które hosty powinny korzystać z KRL. Stare zestawy bez podpisanych terminów wymagają ponownego eksportu. Nowa CA inicjalizuje pusty KRL przed wystawieniem; utrata listy używanej CA wymaga odzyskania.
11. Dla centralnej widoczności zarejestruj osobną tożsamość odbiorcy i jawnie włącz raportowanie KRL; nie nadaje ono prawa wystawiania ani instalowania SSH. Uruchom ssh monitor-krl z chronioną tożsamością i konfiguracją subskrypcji. Stan agentów pokazuje zgłoszoną wersję, podpisany termin publikacji, błędy synchronizacji i brak raportów; poprawne skanowanie nie ukrywa błędu KRL. Monitoring platformy uwzględnia te błędy. To uwierzytelnione obserwacje agenta, nie niezależny dowód odrzucenia certyfikatu na wszystkich hostach. Używaj osobnej zarejestrowanej tożsamości dla każdego odbiorcy.

DANE I PARAMETRY

- Jeden certyfikat OpenSSH Ed25519 z podpisem CA Ed25519 i ograniczoną ważnością. Klucze prywatne są odrzucane.
- Ścieżki CA i stanu muszą być absolutne, bez dowiązań, dostępne tylko właścicielowi. Klucze prywatne nie trafiają do SaaS.
- Format importu: jeden wiersz ssh-ed25519-cert-v01@openssh.com AAAA... z opcjonalnym komentarzem, jak w pliku -cert.pub, najwyżej 64 000 znaków.

WYNIK OPERACJI

Stronicowany inwentarz SSH izolowany dla organizacji, kryptograficzna weryfikacja podpisów, wersjonowana odpowiedzialność i audyt zmian. Agent lokalnie wystawia certyfikaty i generuje KRL. Lokalne odnowienia używają trwałych operacji oczekujących, atomowych wskaźników zestawu oraz blokad

po unieważnieniu lub zmianie polityki.

UPRAWNIENIA

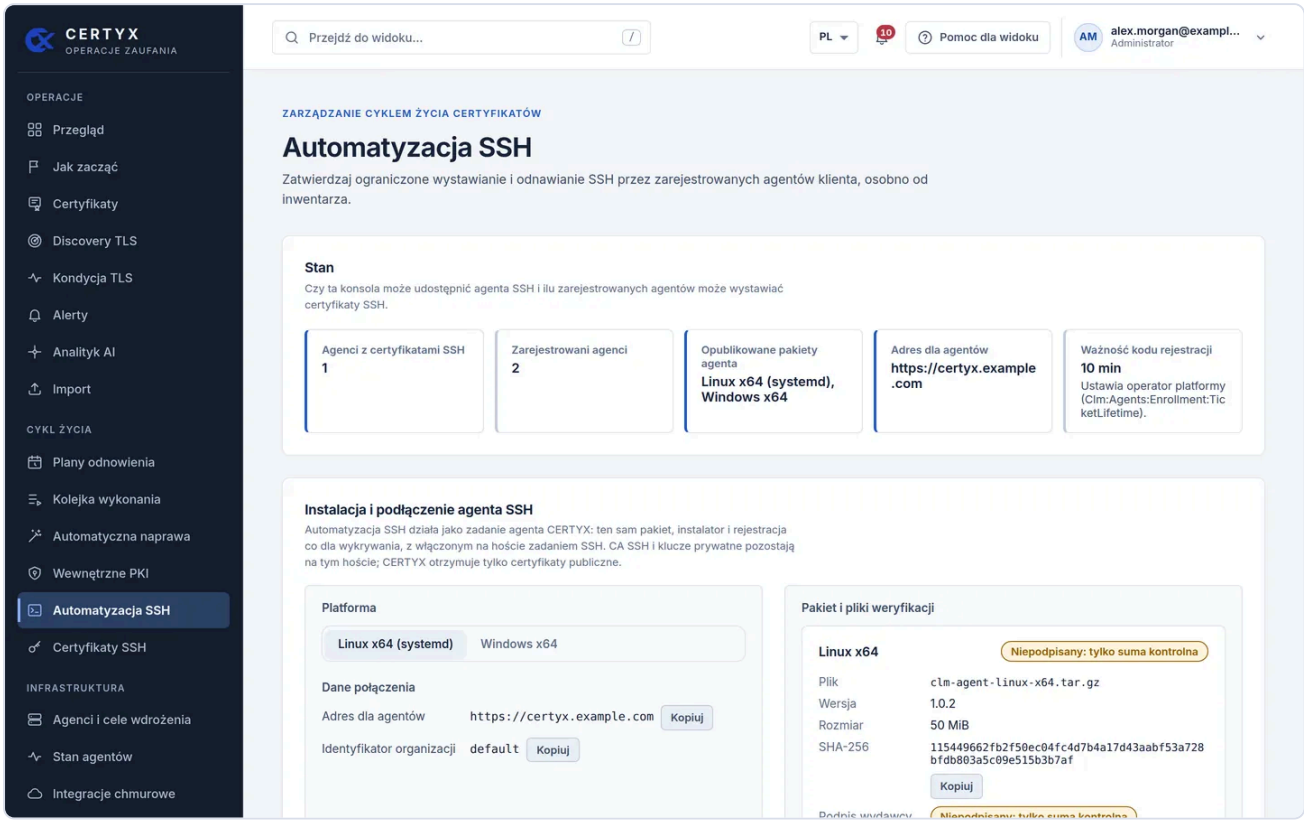
Wszystkie role organizacji odczytują; Admin i Operator importują i edytują, Auditor tylko odczytuje. Użycie lokalnej CA ogranicza polityka principali i ważności.

OGRANICZENIA

Automatyzacja SSH obejmuje zatwierdzane zadania platformy, automatyczne odnowienia w ograniczonym zakresie, zweryfikowane wdrożenie hosta Unix i wycofanie po błędzie, lokalnych odbiorców podpisanego KRL oraz zdarzenia powiadomień SSH. CERTYX nie konfiguruje zaufania CA ani list unieważnień w konfiguracji OpenSSH zdalnych hostów i nie śledzi, które hosty powinny korzystać z KRL. Certyfikaty użytkowników są instalowane tylko dla lokalnych tożsamości procesów Unix klienta, nie dla kont osób. Operacje SSH działają w agentach Linux i Windows (OpenSSH dla Windows), a CA SSH używa wyłącznie kluczy Ed25519. Powiadomienia SSH są wysyłane e-mailem do grup odbiorców profilu przez przekaźnik SMTP organizacji. Podpis wpisu nie potwierdza działania usługi ani unieważnienia we flocie. Lokalny klucz CA nie jest HSM. Lokalny urząd SSH synchronizuje zawartość licznika numerów seryjnych i wpis katalogu przed podpisaniem. Błąd synchronizacji magazynu blokuje wystawienie; sprawdź chroniony magazyn lokalny i po naprawie ponów ten sam identyfikator operacji. Podpisywanie odbywa się na jednym hoście; podpisywanie rozproszone nie jest obsługiwane. Lokalne blokady konektorów muszą być zwykłymi plikami tylko dla właściciela w Unix, bez dowiązań w katalogach nadrzędnych. Niebezpieczne istniejące blokady są odrzucane; administrator musi poprawić uprawnienia magazynu przed ponowieniem. Te konektory działają tylko w agentach Unix.

30 Automatyzacja SSH

Zatwierdzaj ograniczone wystawianie i odnawianie SSH przez zarejestrowanych agentów klienta, osobno od inwentarza.



Dane przykładowe: organizacje, osoby, hosty i adresy są fikcyjne.

JAK TO DZIAŁA

1. Widok jest podzielony na karty: Stan (agenci z certyfikatami SSH, zarejestrowani agenci, opublikowane pakiety, adres dla agentów i skonfigurowana ważność kodu rejestracji), Instalacja i podłączenie agenta SSH, Agenci i uprawnienia SSH oraz Profile, historia zadań i unieważnienia. W karcie „Instalacja i podłączenie agenta SSH” wybierz Linux x64 (systemd) lub Windows x64: panel pokazuje kartę pakietu tej platformy (tę samą kartę co w widoku Agenci i cele wdrożenia: nazwa pliku, wersja, rozmiar, SHA-256 z przyciskiem Kopiuj, stan podpisu wydawcy i manifestu wydania oraz przyciski pobierania pakietu, pliku .sha256, podpisu .p7s i znacznika czasu .tsr, gdy są opublikowane, manifestu wydania z podpisem i weryfikatora, każdy zapisywany pod własną nazwą pliku) albo informuje, że pakiet nie jest opublikowany na tym serwerze, wraz z krokiem publikacji operatora. Administratorzy tworzą tu jednorazowy kod rejestracji i pobierają plik tokenu; ponumerowane kroki zawierają gotowe do skopiowania polecenia zbudowane z adresu dla agentów i identyfikatora organizacji: zaufanie prywatnego CA agentów, skopiowanie pliku tokenu do pustego katalogu roboczego na hoście, pobranie (archiwum jest udostępniane tylko z ważnym kodem rejestracji, który polecenie odczytuje z pliku; link pobierania w panelu działa w zalogowanej sesji konsoli) i weryfikacja (zastąp <PUBLISHER-SHA256> odciskiem wydawcy uzyskanym niezależnie), instalator w katalogu clm-agent z ../clm-enrollment.token i kontrola stanu. Jest jeden pakiet agenta; SSH to zadanie tego agenta.

2. Ponumerowane kroki instalacji (każdy w osobnym bloku z tytułem i poleceniem do skopiowania) otwierają się same, dopóki żaden agent nie ma uprawnienia SSH. W karcie „Agenci i uprawnienia SSH" nadaj zarejestrowanemu agentowi „Certyfikaty SSH" (pobiera zatwierdzone profile) oraz, do instalacji, „Instalacja SSH"; tabela pokazuje ostatni kontakt i ostatni raport zadania SSH. Na hoście uruchom configure-ssh-linux.sh init (Linux, jako root) lub configure-ssh-windows.ps1 init (Windows, PowerShell administratora): tworzy CA hosta (/etc/clm-ssh lub C:\ProgramData\CLM-SSH, tylko dla właściciela) i wypisuje odcisk CA do profilu. Po zatwierdzeniu i pobraniu profilu add-profile ./ssh-profile-<ID>.json wykonuje jeden sprawdzony cykl ssh manage --once i uruchamia clm-ssh.service (Linux) lub zadanie harmonogramu „CERTYX SSH Workload" (Windows, LocalSystem); nieudany cykl podaje przyczynę (np. HTTP 403 bez uprawnienia SSH) i nic nie jest uruchamiane. Opcjonalne trust-user-ca sprawia, że lokalny sshd ufa certyfikatom użytkowników tego CA (TrustedUserCAKeys, sprawdzane przez sshd -T, kopia zapasowa przywracana, gdy sshd się nie przeładuje). Sprawdź poleceniem sudo clm-agent status (wiersz Capabilities zawiera ssh) i statusem skryptu. W Windows Server 2025 sshd domyślnie dopuszcza tylko członków grup administrators i OpenSSH Users (AllowGroups): dodaj konta logujące się certyfikatami użytkownika do OpenSSH Users i uruchom serwer OpenSSH raz przed trust-user-ca, aby istniał sshd_config.
3. Wybierz Nowy profil i podaj zarejestrowanego agenta z uprawnieniem SSH, principal i typ (Użytkownik lub Host), ważność, okno odnowienia, ważność zatwierdzenia, niezależnie zatwierdzony odcisk CA, środowisko, odpowiedzialnego właściciela lub zespół, usługę i opcjonalnie grupy odpowiedzialności, a potem Poproś o zatwierdzenie. Bez aktywnego agenta z uprawnieniem SSH formularz to wyjaśnia i nie da się go wysłać.
4. Inny administrator wybiera przy profilu w zakładce Profile Zatwierdź zakres (wnioskujący nie może zatwierdzić własnego wniosku). Wybierz Pobierz publiczny profil i dodaj go do lokalnej konfiguracji zarządzanej; ścieżki prywatnego CA i tożsamości pozostają na tym hoście.
5. Samodzielne lokalne odnawianie bez raportowania do CERTYX: configure-ssh-linux.sh enable-renewal <pobrany profil> zapisuje renewal.json z lokalnej polityki CA i profilu, wykonuje jeden cykl Clm.Agent ssh renew przez systemd i włącza clm-ssh-renewal.timer (jeden cykl na minutę, bez dostępu do sieci, identyfikator w dzienniku clm-ssh-renewal); w Windows configure-ssh-windows.ps1 enable-renewal rejestruje zadanie CERTYX SSH Renewal. Profil w stanie failed, blocked lub w konflikcie polityki sprawia, że cykl kończy się widocznym błędem (jednostka failed lub niezerowy wynik zadania); renewal-status to pokazuje, a disable-renewal usuwa odnawianie. Profil odnawia albo add-profile, albo enable-renewal. ready-local potwierdza tylko lokalny zestaw; nie oznacza zdalnej instalacji.
6. Uruchom Clm.Agent ssh manage <chroniona-konfiguracja> [--once]. Agent łączy się wychodząco przez mTLS, pobiera trwałe zadania i zachowuje klucze prywatne lokalnie.
7. Zakładki Profile i Historia zadań pokazują zatwierdzenia, terminy i błędy. Przycisk Zatrzymaj automatyzację blokuje dalsze pobrania i publikacje.
8. Dla instalacji na hoście wybierz w sekcji Zarejestrowani agenci „Włącz wdrażanie tożsamości SSH" i zaznacz w profilu „Zainstaluj i zweryfikuj tę tożsamość SSH". Administrator klienta przygotowuje chroniony lokalny cel, istniejącą wersję bazową, stałe narzędzia sprawdzania/przeładowania oraz próbę SSH z przypiętą CA; w Linuksie configure-ssh-linux.sh enable-host-deploy pozwala kontu agenta uruchamiać przez sudo dokładnie sshd -t i przeładowanie sshd (reguła sprawdzona przez visudo i plik drop-in usługi; disable-host-deploy usuwa oba). Agent instaluje pełną parę klucz/certyfikat, sprawdza i przeładowuje usługę; błąd powoduje przywrócenie i sprawdzenie poprzedniej pary.
9. Odebranie uprawnienia instalacji SSH zatrzymuje oczekujące zadania hosta i dalsze pobrania. Agent ponownie sprawdza zgodę bezpośrednio przed instalacją. Jeżeli istnieje dziennik przerwanej aktywacji, najpierw odzyskuje wcześniej sprawdzony stan.

10. W Historii zadań wybierz Unieważnij certyfikat i potwierdź. Platforma zatrzymuje profil i zapisuje jedno trwałe zlecenie. Przypisany agent sprawdza dokładny lokalny certyfikat, aktualizuje lokalny KRL i przekazuje jego skrót. W zakładce Unieważnienia sprawdzisz oczekiwanie, błąd lub lokalne unieważnienie. Nieaktywny agent pozostawia zadanie oczekujące. Istniejące sesje i inne hosty nie są automatycznie unieważniane.
11. Gdy lokalne unieważnienie nie powiedzie się, sprawdź kod błędu i chroniony stan agenta, usuń przyczynę, a następnie wybierz Ponów unieważnienie. Nowy identyfikator odrzuca spóźnione potwierdzenia poprzedniej próby; wystawianie pozostaje zatrzymane.
12. Podczas tworzenia profilu SSH przypisz istniejące grupy powiadomień. Lokalna kolejka tworzy dwujęzyczne wiadomości HTML o zbliżającym się wygaśnięciu, wydaniu, wdrożeniu, wycofaniu wdrożenia, błędach i lokalnym unieważnieniu. Ponowne przetwarzanie nie powiela zdarzenia. Wysyłka wymaga włączonego kanału SMTP organizacji; wpis w kolejce nie potwierdza dostarczenia. Lokalne unieważnienie nie rozprowadza KRL na inne hosty ani nie kończy sesji.
13. Przekazywanie KRL po stronie klienta: Clm.Agent ssh export-krl podpisuje publiczną listę lokalną CA; Clm.Agent ssh apply-krl <konfiguracja-odbiorcy> <koperta> sprawdza organizację, przypiętą CA, podpis, skrót i rosnącą wersję. Odbiorcy muszą osobno skonfigurować RevokedKeys lub RevokedHostKeys. Listę na inne hosty przekazują ssh publish-krl i ssh sync-krl; CERTYX nie sprawdza, czy każdy host faktycznie odrzuca unieważniony klucz.
14. Opcjonalna lista KrlConsumers w konfiguracji agenta automatycznie otrzymuje podpisane aktualizacje KRL po unieważnieniu. Wersje są trwałe między restartami. Błąd publikacji pokazuje nieudane unieważnienie, które można ponowić. Mechanizm nie konfiguruje odbiorców OpenSSH ani zdalnych hostów floty.
15. Agent uzgadnia skonfigurowanych lokalnych odbiorców KRL w każdym cyklu, również po restarcie lub uprawnionym lokalnym unieważnieniu. Błąd odbiorcy bezpiecznie zatrzymuje cykl. Konto odbiorcy OpenSSH musi mieć dostęp do odczytu przygotowanego katalogu; agent nie nadaje innemu kontu uprawnień do plików.
16. Zarządzany proces SSH zgłasza własny bezpieczny stan cyklu. Poprawne skanowanie nie ukrywa błędu ani braku raportów procesu SSH. Sprawdź błąd w stanie agentów i chronione lokalne dzienniki; stałe podsumowania nie zawierają sekretów. Brak połączenia może uniemożliwić natychmiastowy raport, dlatego monitorowany jest również brak kontaktu.
17. Zdarzenie wiadomości SSH jest zapisywane atomowo z operacją. Wiadomość wskazuje dokładny podpisany certyfikat, ważność w UTC, odcisk CA i bezpieczny kod błędu. Kolejka przetwarza ograniczone partie i odzyskuje przerwane potwierdzenia bez powielania wiadomości.
18. Nowe wydanie SSH wymaga uprawnienia do automatycznego odnawiania. Instalacja hosta wymaga również wdrażania, weryfikacji i wycofania wdrożenia. Sama zmiana pakietu nie blokuje rozliczenia ani odzyskiwania rozpoczętej operacji; nadal obowiązują ograniczenia dostępu organizacji i unieważnienie uprawnień.
19. Zdalne przekazywanie KRL pod kontrolą klienta: uruchom ssh publish-krl z chronioną konfiguracją i udostępnij wyłącznie publiczny zestaw przez osobną tożsamość relaya HTTPS. Na odbiorcy uruchom ssh sync-krl z chronioną subskrypcją. Podpisana publikacja wygasa po godzinie i odświeża się automatycznie; przekierowania, brak zaufania, zbyt duże dane, manipulacje i stare publikacje są odrzucane. Błąd zachowuje istniejące unieważnienia. OpenSSH sam nie egzekwuje terminu zestawu. Stan centralnie raportują tylko odbiorcy zarejestrowani do raportowania KRL; CERTYX nie ustala, które

hosty powinny korzystać z KRL. Stare zestawy bez podpisanych terminów wymagają ponownego eksportu. Nowa CA inicjalizuje pusty KRL przed wystawieniem; utrata listy używanej CA wymaga odzyskania.

20. Dla centralnej widoczności zarejestruj osobną tożsamość odbiorcy i jawnie włącz raportowanie KRL; nie nadaje ono prawa wystawiania ani instalowania SSH. Uruchom ssh monitor-krl z chronioną tożsamością i konfiguracją subskrypcji. Stan agentów pokazuje zgłoszoną wersję, podpisany termin publikacji, błędy synchronizacji i brak raportów; poprawne skanowanie nie ukrywa błędu KRL. Monitoring platformy uwzględnia te błędy. To uwierzytelnione obserwacje agenta, nie niezależny dowód odrzucenia certyfikatu na wszystkich hostach. Używaj osobnej zarejestrowanej tożsamości dla każdego odbiorcy.
21. Potwierdzenie wystawienia wymaga aktywnej zarejestrowanej tożsamości z uprawnieniem SSH. Potwierdzenie instalacji wymaga także uprawnienia wdrażania SSH. Odebranie uprawnienia blokuje oczekujące wyniki również po rozpoczęciu wystawiania; zachowane lokalne dzienniki wymagają uzgodnienia przed przywróceniem uprawnień.
22. Instalacja tożsamości użytkownika: wybierz Użytkownik i włącz instalację przy zgłaszaniu profilu. Wymagane są niezależne zatwierdzenie i uprawnienie wdrażania SSH. Dodaj zgodny wpis UserTargets do aktualnej konfiguracji agenta Unix: konkretne konto/principal, endpoint i osobno przypięta CA hosta. Agent przełącza kompletny lokalny zestaw klucza i certyfikatu, potwierdza uwierzytelnienie certyfikatem i przy odrzuceniu odzyskuje poprzednią wersję. Logowanie samym kluczem nie potwierdza wdrożenia certyfikatu.
23. UserTargets musi zawierać HostRevocationFile: chroniony lokalny KRL klienta używany jako RevokedHostKeys. Klient odrzuca brak lub niebezpieczne uprawnienia listy oraz unieważnione hosty mimo zgodnej CA. Synchronizuj listę przez publikację/subskrypcję KRL klienta; CERTYX nie sprawdza, które hosty powinny ją mieć.
24. Wszystkie mechanizmy odczytu konfiguracji JSON agenta odrzucają dowiązania pliku lub katalogów nadrzędnych, uprawnienia grupy lub innych użytkowników w Unix, pliki większe niż 1 MiB oraz niepoprawny UTF-8 przed deserializacją. W Unix zabezpiecz konfigurację poleceniem chmod 600. Względne ścieżki argumentów są przekształcane do bezwzględnych i sprawdzane według tych samych reguł. Obsługiwany jest UTF-8 z BOM i bez BOM. Odczyt ustawień i odczyt asynchroniczny stosują te same zasady; komunikaty błędów nie zawierają wartości konfiguracji. W Windows odczyt odrzuca plik, którego właścicielem jest lub który może odczytać albo zmienić inny podmiot niż LocalSystem, Administratorzy lub tożsamość agenta; przed wdrożeniem ustaw restrykcyjne ACL.

DANE I PARAMETRY

- Zarejestrowany aktywny agent z jawnym uprawnieniem SSH; HTTPS zaufane na hoście.
- Chroniona konfiguracja zawiera tożsamość z rejestracji, lokalną CA i tablicę zatwierdzonych profili.
- Zatwierdza inny administrator; ważność zatwierdzenia wynosi 1–90 dni.
- Formaty profilu: principal 1–128 liter, cyfr i znaków . _ @ -, zaczynający się literą lub cyfrą (bastion.example.com lub deploy); odcisk CA SHA256: i 43 znaki Base64, tak jak wypisuje ssh-keygen -lf; ważność 2–10 080 minut; odnowienie przed wygaśnięciem co najmniej 1 minuta i krócej niż ważność; zatwierdzenie 1–90 dni.

WYNIK OPERACJI

Publiczne certyfikaty SSH są sprawdzane względem UUID zadania, principala, CA i ważności oraz idempotentnie wprowadzane do inwentarza. Utrata potwierdzenia wyniku nie tworzy nowych kluczy.

UPRAWNIENIA

Użytkownicy organizacji odczytują; administratorzy wnioskują i zatrzymują, inny administrator zatwierdza. Administrator hosta klienta dopuszcza lokalny zakres CA.

OGRANICZENIA

Wdrażanie hosta obsługuje OpenSSH w Linuksie i OpenSSH dla Windows z przygotowaną wersją bazową i lokalnym celem (przykłady ssh-host-target.linux.json i ssh-host-target.windows.json). Zadanie SSH w Windows (pliki chronione listą ACL, kopiowana para current zamiast dowiązania, Restart-Service sshd) działa jako LocalSystem z OpenSSH dla Windows. issued-local oznacza samo wystawienie; deployed-verified potwierdza zaobserwowane połączenie SSH. rolled-back zatrzymuje automatyczne próby; interwencja wymaga sprawdzenia przez administratora hosta. CERTYX nie konfiguruje zaufania CA na zdalnych hostach i nie śledzi, które hosty powinny korzystać z KRL. Powiadomienia SSH są wysyłane e-mailem przez przekaźnik SMTP organizacji. Lokalni odbiorcy podpisanego KRL i trwałe zdarzenia wiadomości HTML są dostępne; lokalne unieważnienie nie potwierdza objęcia zdalnych odbiorców. Zatrzymanie profilu nie unieważnia certyfikatów ani sesji. Zarejestrowani monitorowani odbiorcy raportują stan synchronizacji; nie potwierdza to oczekiwanego pokrycia floty ani niezależnego odrzucenia unieważnionego dostępu. Instalacja użytkownika obejmuje lokalną tożsamość procesu Unix pod tym samym kontem systemowym, z istniejącą sprawdzoną wersją bazową. Nie zakłada katalogów domowych użytkowników, ACL Windows, zaufania CA na serwerze ani aktywnych sesji. Procesy muszą używać ścieżek wdrożenia current/identity i current/identity-cert.pub przy nowych połączeniach. Przed przypisaniem profilu instalacji użytkownika zaktualizuj agenta. Gdy ten serwer publikuje pakiet bez podpisu wydawcy (niepodpisaną kompilację deweloperską), polecenia instalacji mówią o tym, pomijają plik podpisu i sprawdzają tylko sumę kontrolną, z obejściami deweloperskimi weryfikatora i instalatora; takich pakietów używaj tylko do prac deweloperskich.