CERTYX



AUTONOMOUS CERTIFICATE LIFECYCLE MANAGEMENT

Jak zacząć

Dziesięć kroków od pierwszego logowania do Twojego SIEM

JĘZYK
Polski

WERSJA
8550060f

DATA
1 listopada 2026

Spis treści

1 Zabezpiecz konto 3
2 Dodaj zespół 4
3 Ustal, kto dostaje ostrzeżenia 5
4 Sprawdź politykę TLS 6
5 Dodaj certyfikaty 7
6 Podłącz agenta 8
7 Reaguj na to, co ważne 9
8 Zaplanuj odnowienia 10
9 Wysyłaj zdarzenia do SIEM 11
10 Weź CERTYX ze sobą 12

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.

> Zrzuty i film pokazują przykładowe dane.

1 Zabezpiecz konto

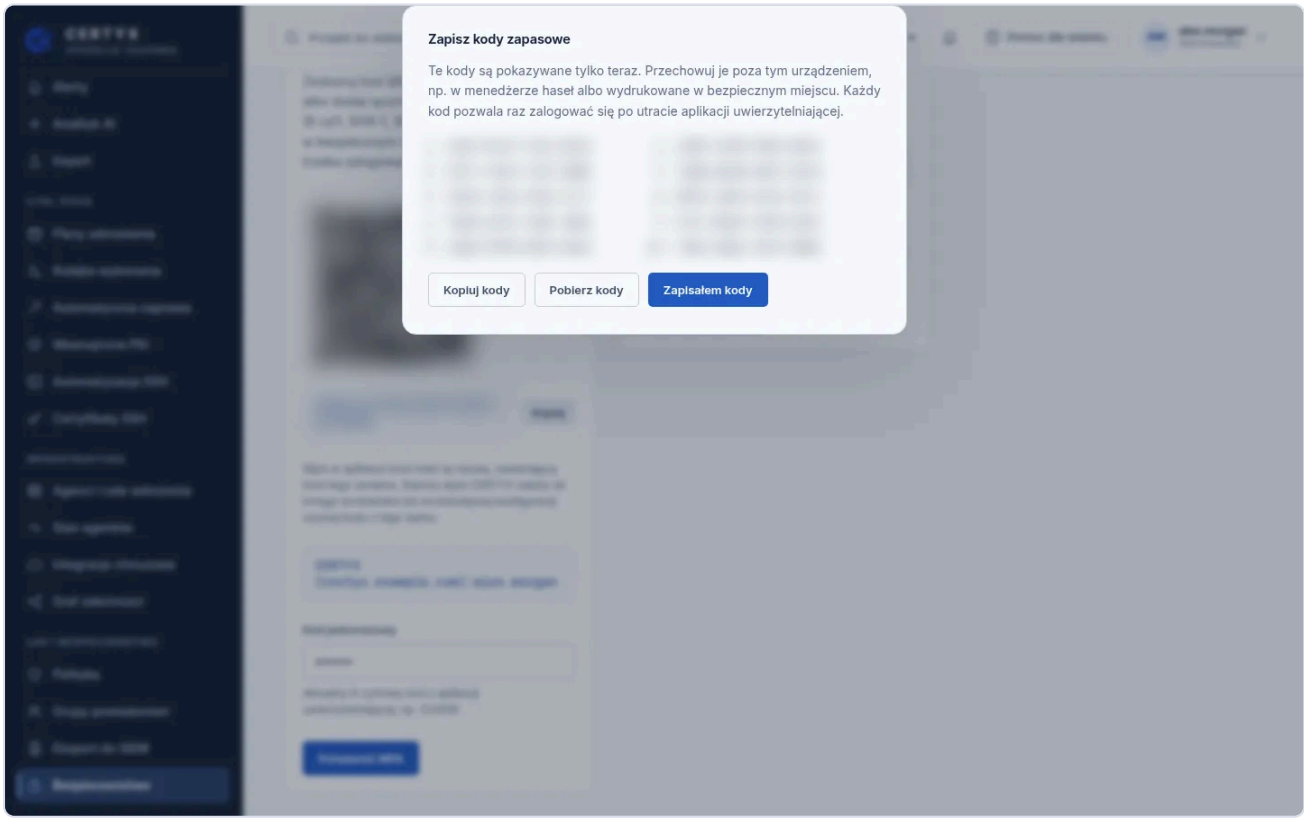
Włącz MFA i zachowaj kody odzyskiwania

DLACZEGO

Twoje konto zarządza certyfikatami i zatwierdzeniami organizacji. Drugi składnik zatrzyma każdego, kto pozna Twoje hasło.

JAK

1. Otwórz Bezpieczeństwo. Jeśli logujesz się przez logowanie firmowe (SSO), MFA zarządza dostawca tożsamości, a ten krok liczy się jako zrobiony.
2. Wybierz Włącz MFA i dodaj sekret do aplikacji uwierzytelniającej.
3. Wpisz sześciocyfrowy kod z aplikacji i wybierz Potwierdź MFA.
4. Skopiuj lub pobierz dziesięć kodów odzyskiwania, przechowuj je offline i wybierz Zapisałem kody.
5. Zaloguj się ponownie hasłem i kodem MFA.



2 Dodaj zespół

Użytkownicy z właściwymi rolami

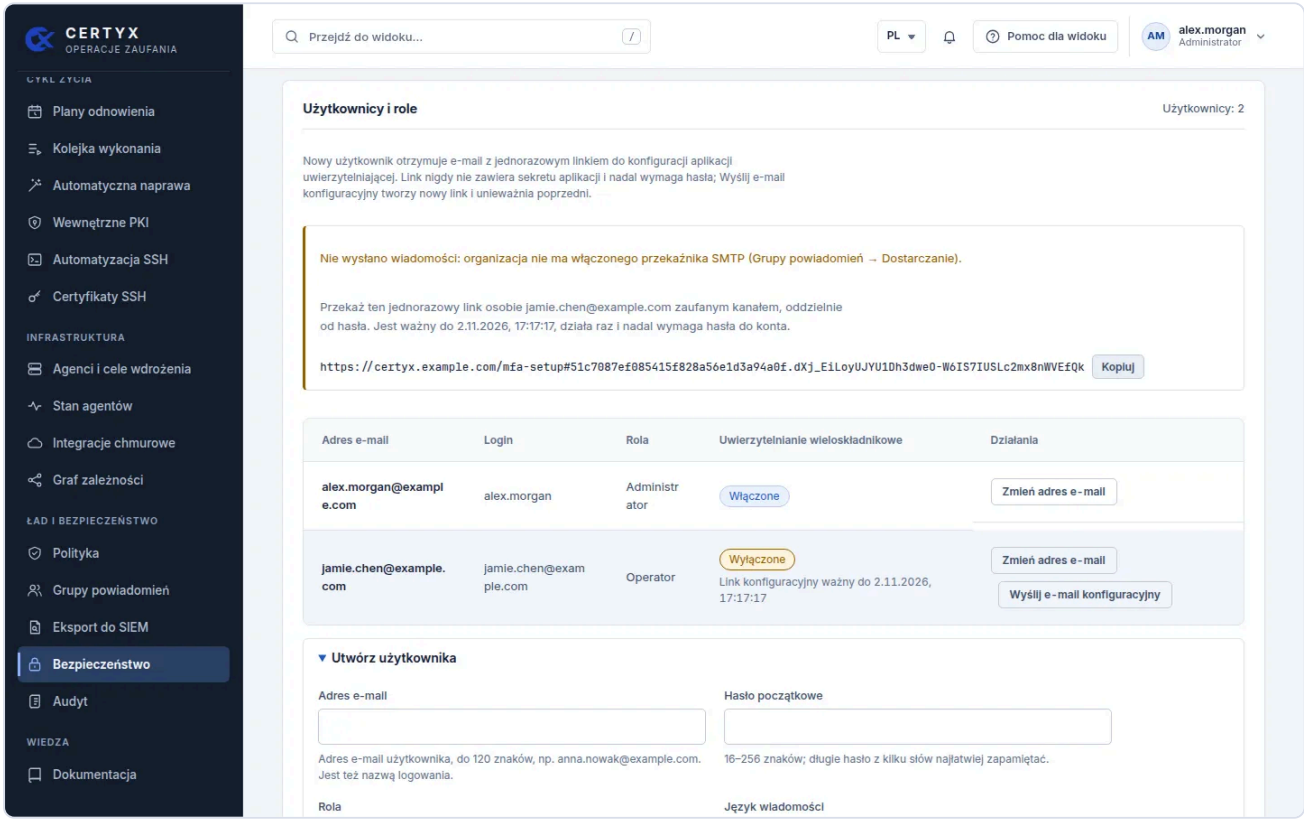
DLACZEGO

Każda osoba pracuje na własnym koncie, więc każda zmiana i zatwierdzenie ma autora.

JAK

1. W Bezpieczeństwie przejdź do Użytkownicy i role.
2. Rozwiń Utwórz użytkownika i wpisz e-mail współpracownika, hasło początkowe (co najmniej 16 znaków) i rolę: Audytor czyta, Operator zarządza inwentarzem i planami, Administrator zatwierdza.
3. Wybierz Utwórz użytkownika i przekaż hasło początkowe osobiście.
4. Opcjonalnie: w Logowanie firmowe (SSO) połącz Microsoft Entra ID, Okta, innego dostawcę OpenID Connect lub SAML 2.0, aby współpracownicy logowali się kontem firmowym.

> Ten krok wykonuje administrator. Jeśli nie masz tej roli, poproś administratora.



3 Ustal, kto dostaje ostrzeżenia

Grupy odbiorców e-maili o wygasaniu

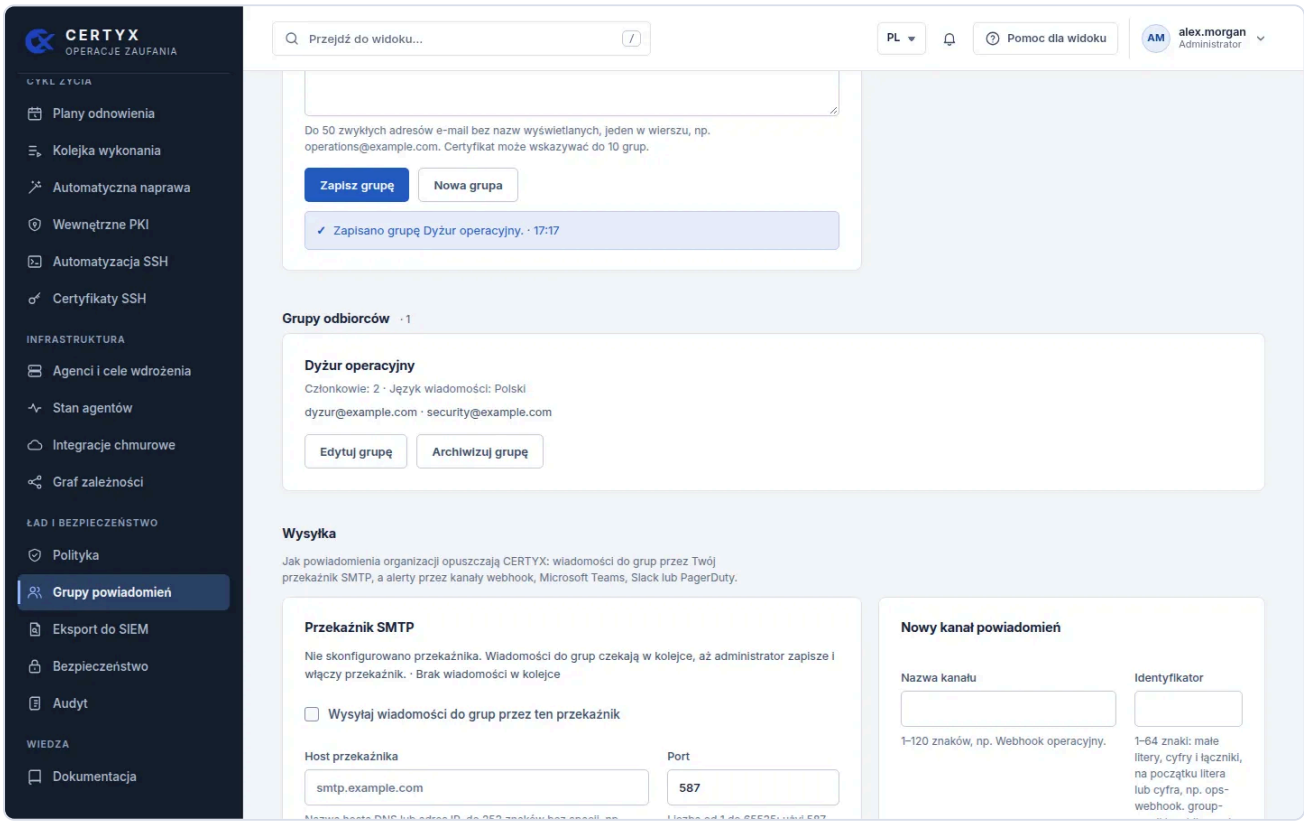
DLACZEGO

Ostrzeżenia o wygasaniu trafiają do osób, które mogą działać, w ich języku, a nie do jednej wspólnej skrzynki.

JAK

1. Otwórz Grupy powiadomień. Formularz Nowa grupa odbiorców jest na górze; Nowa grupa czyści formularz.
2. Wpisz Nazwę grupy, na przykład Dyżur operacyjny, i do 50 adresów e-mail w polu Adresy odbiorców, po jednym w wierszu.
3. Wybierz Język wiadomości i Zapisz grupę.
4. Przypisz grupę do certyfikatów w ich szczegółach, w sekcji Grupy odpowiedzialności. E-maile są wysyłane, gdy administrator zapisze i włączy przekaźnik SMTP w sekcji Wysyłka.

> Ten krok wykonuje administrator. Jeśli nie masz tej roli, poproś administratora.



4 Sprawdź politykę TLS

Okno odnowienia i reguły bezpieczeństwa

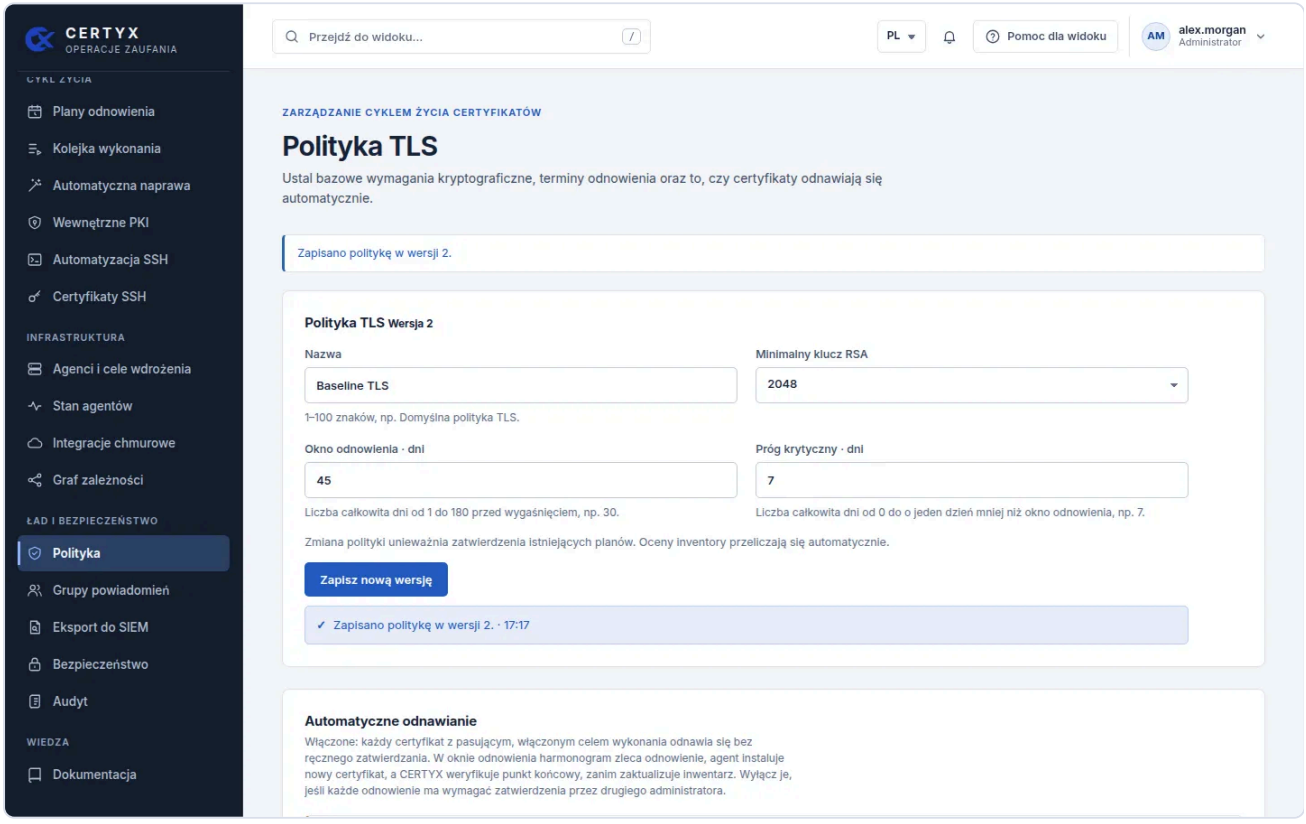
DLACZEGO

Polityka decyduje, kiedy certyfikat wymaga uwagi i jakie klucze oraz podpisy są akceptowane.

JAK

1. Otwórz widok Polityka.
2. Sprawdź okno odnowienia i próg krytyczny w dniach.
3. Wybierz minimalny klucz RSA. Zawsze obowiązują też stałe reguły: klucze ECDSA co najmniej P-256, brak podpisów SHA-1 i MD5 oraz kontrola ważności.
4. Wybierz Zapisz nową wersję; każdy certyfikat jest oceniany według niej, a zatwierdzenia istniejących planów odnowienia tracą ważność.

> Ten krok wykonuje administrator. Jeśli nie masz tej roli, poproś administratora.



5 Dodaj certyfikaty

Zaimportuj certyfikat lub dodaj domenę

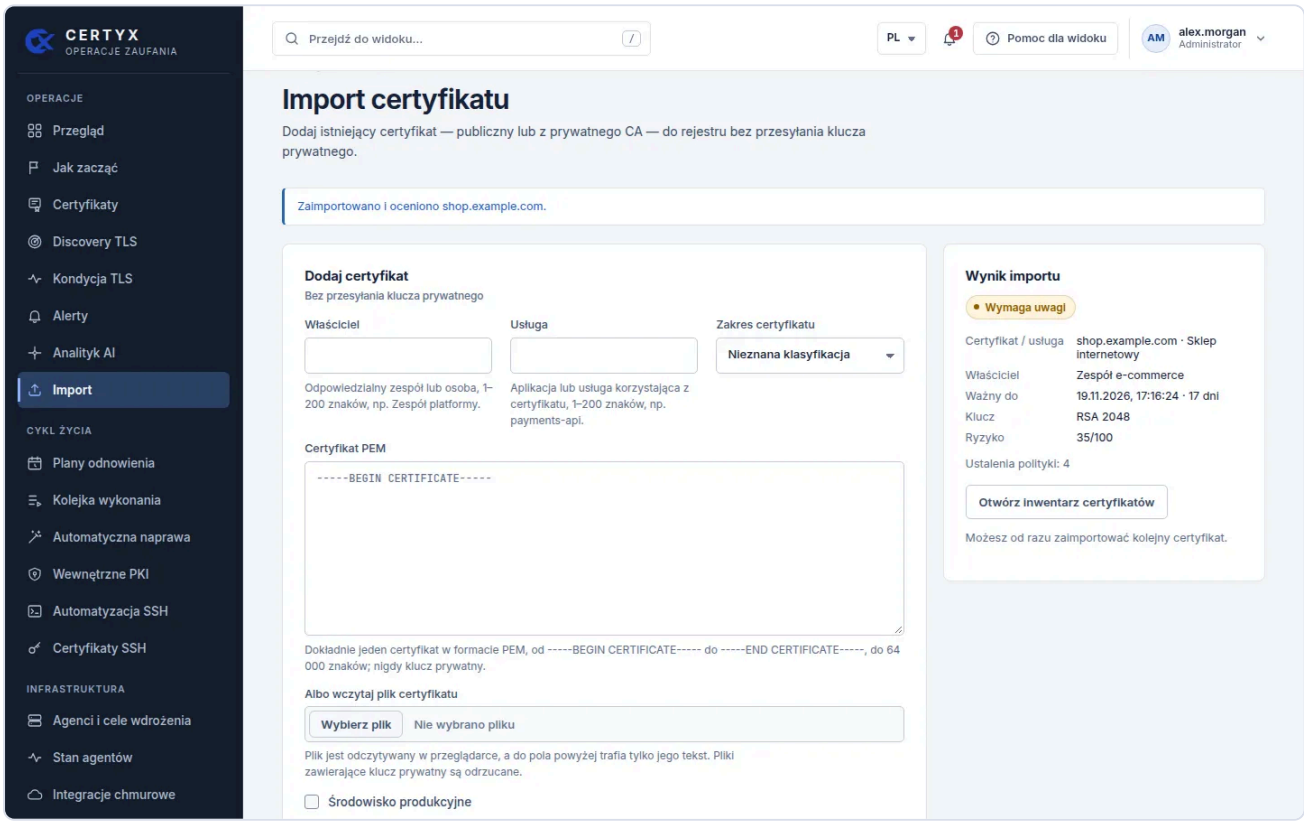
DLACZEGO

Zarządzać można tylko tym, co widać. Zacznij od najważniejszych usług.

JAK

1. Otwórz Import, wklej publiczny certyfikat PEM lub wczytaj plik certyfikatu i wpisz właściciela oraz usługę.
2. Wybierz Importuj i oceń: certyfikat zostaje zapisany i sprawdzony według polityki.
3. Aby odczytać certyfikat z działającego serwera, wybierz Dodaj domenę w Certyfikatach; otworzy się Discovery TLS.
4. Dla całych sieci zarejestruj agenta (następny krok) lub podłącz integracje chmurowe.

> Ten krok wykonuje operator lub administrator. Twoja rola może przeglądać wynik; o zmiany poproś operatora lub administratora.



6 Podłącz agenta

Skanuj sieci i wdrażaj odnowienia

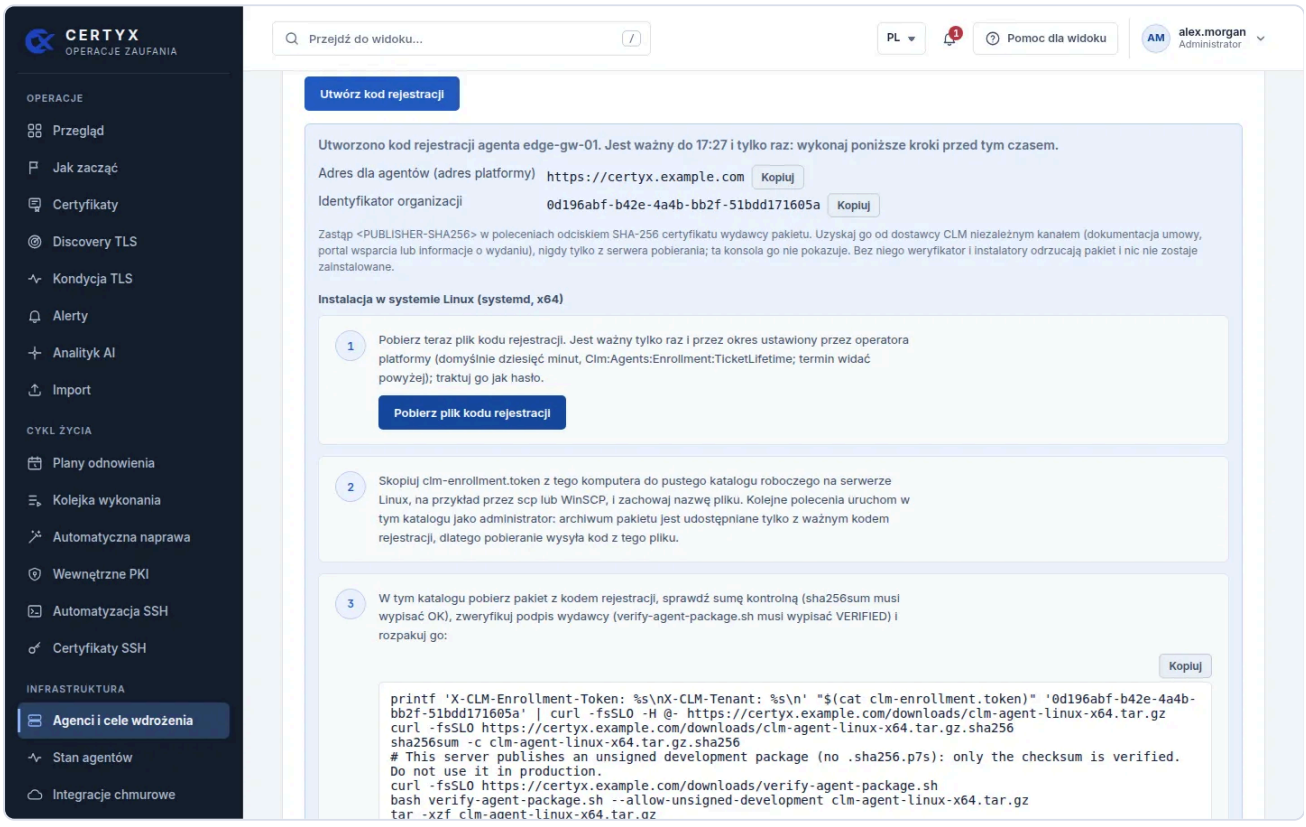
DLACZEGO

Agent w Twojej sieci znajduje certyfikaty na każdym zatwierdzonym hoście i porcie, a później instaluje odnowione.

JAK

1. Otwórz Agenci i cele wdrożenia.
2. Wpisz identyfikator agenta i wybierz Utwórz kod rejestracji.
3. Zainstaluj agenta na serwerze Linux lub Windows poleceniami wyświetlonymi po utworzeniu kodu; szczegóły zawiera Instrukcja instalacji agenta.
4. W sekcji Automatyczne wykrywanie w sieci wczytaj profil sieciowy agenta, ustaw Zatwierdzone zakresy CIDR i wybierz Zapisz profil sieciowy; Stan agentów pokazuje, czy agent się zgłasza.

> Ten krok wykonuje administrator. Jeśli nie masz tej roli, poproś administratora.



7 Reaguj na to, co ważne

Przegląd, alerty i właściciele

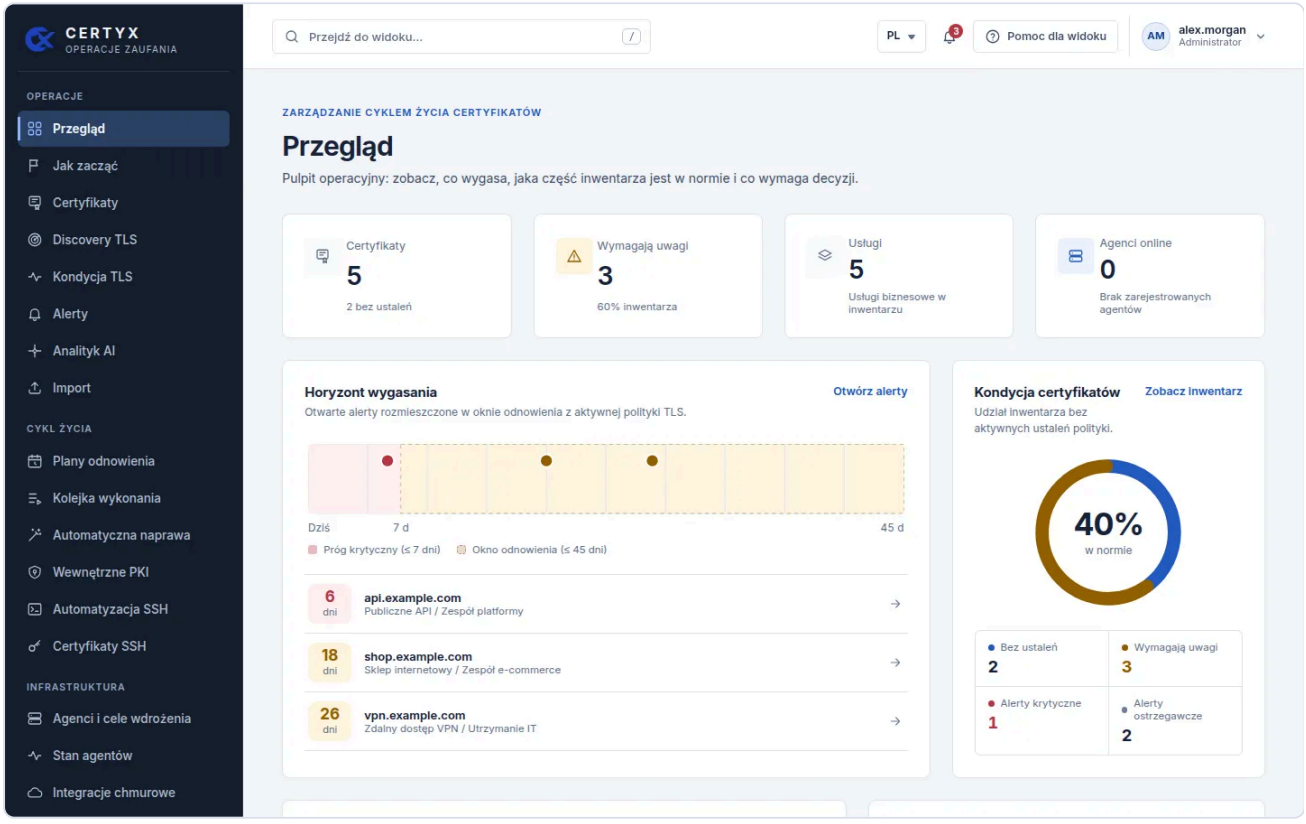
DLACZEGO

Certyfikaty z właścicielem są obsługiwane; przegląd pokazuje, od czego zacząć.

JAK

1. Otwórz Przegląd: wygasające certyfikaty, otwarte alerty i stan agentów w jednym miejscu.
2. Otwórz Alerty i zacznij od krytycznych.
3. Otwórz certyfikat w Certyfikatach, ustaw właściciela oraz usługę i wybierz Zapisz odpowiedzialność, aby każdy alert miał osobę odpowiedzialną.
4. Wybierz Potwierdź odbiór przy obsłużonych alertach.

> Ten krok wykonuje operator lub administrator. Twoja rola może przeglądać wynik; o zmiany poproś operatora lub administratora.



8 Zaplanuj odnowienia

Zatwierdzane przez drugą osobę

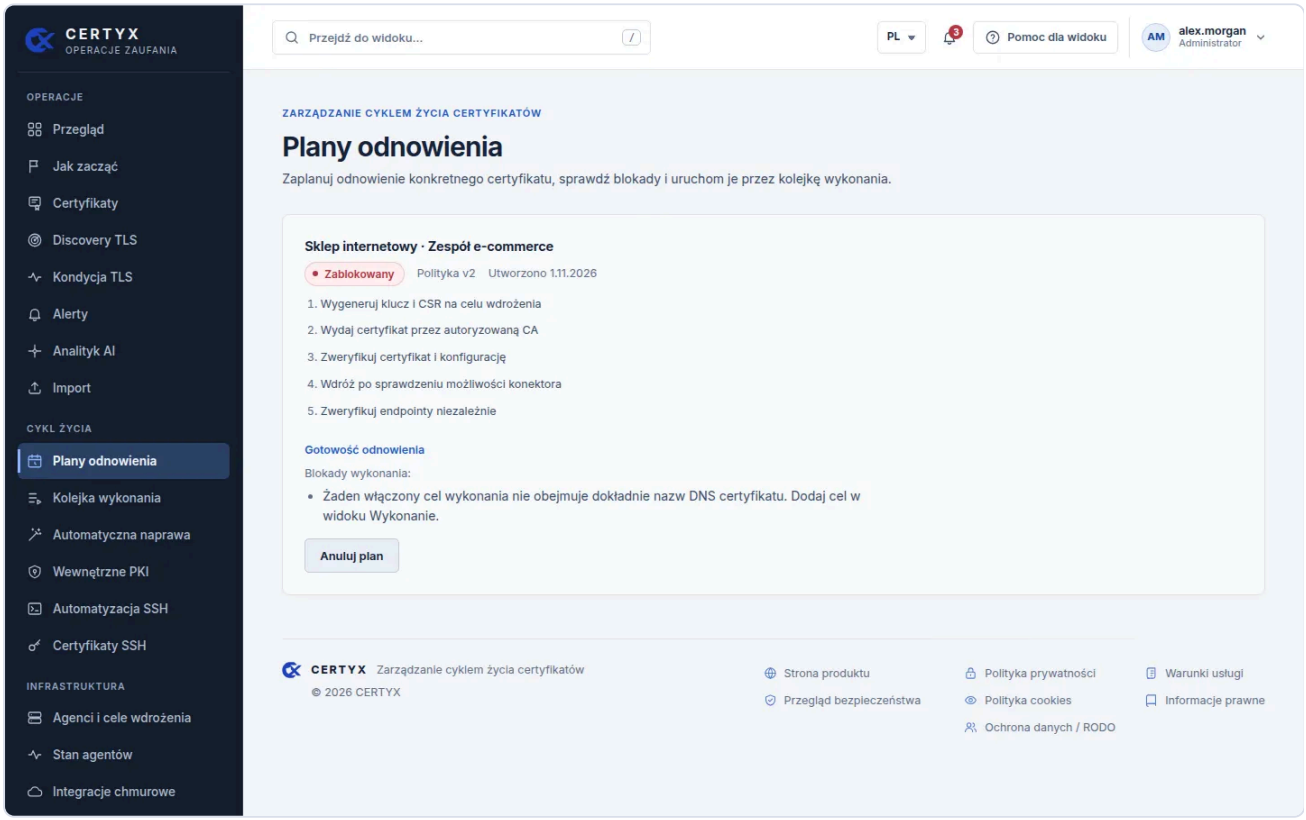
DLACZEGO

Odnowienia są planowane z wyprzedzeniem i zatwierdzane przez drugą osobę, zanim cokolwiek zmieni się na serwerach.

JAK

1. W Certyfikatach otwórz certyfikat, który wkrótce wygaśnie, i wybierz Zaplanuj odnowienie.
2. Otwórz Plany odnowienia: plan pokazuje etapy i to, co go blokuje, na przykład brak celu wdrożenia lub kontaktu z agentem.
3. Administrator wybiera Zatwierdź plan, co tworzy zlecenie wykonania; drugi administrator wybiera Zatwierdź zlecenie jako druga osoba.
4. Gdy agent jest połączony, cel wdrożenia istnieje, a urząd certyfikacji jest skonfigurowany, Kolejka wykonania odnawia, wdraża i weryfikuje certyfikat.

> Ten krok wykonuje operator lub administrator. Twoja rola może przeglądać wynik; o zmiany poproś operatora lub administratora.



9 Wysyłaj zdarzenia do SIEM

Dopasowane do licencji

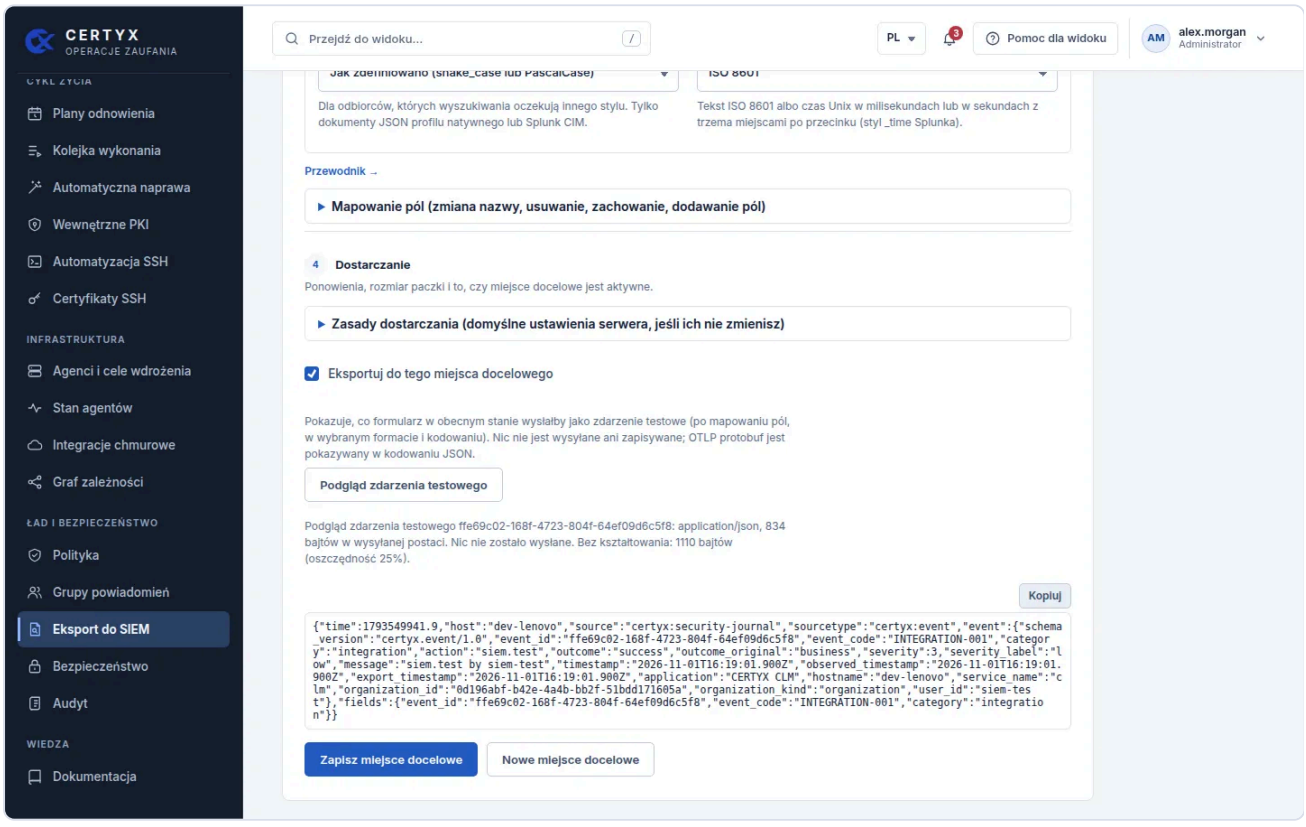
DLACZEGO

Zespół bezpieczeństwa widzi każde logowanie, zmianę i błąd w Splunku, QRadarze, Sentinelu, Elasticu lub dowolnym innym SIEM, a Ty decydujesz, jak duże jest każde zdarzenie, więc licencja SIEM nie jest marnowana.

JAK

1. Otwórz Eksport do SIEM i wpisz nazwę oraz identyfikator miejsca docelowego.
2. Wybierz transport swojego SIEM, np. Splunk HTTP Event Collector, i wpisz jego adres oraz token.
3. W sekcji Kształt i rozmiar wybierz Zrównoważone lub Oszczędne; Podgląd zdarzenia testowego pokazuje, ile bajtów oszczędza każde zdarzenie.
4. Zapisz, potem Sprawdź połączenie i Wyślij zdarzenie testowe.

> Ten krok wykonuje administrator. Jeśli nie masz tej roli, poproś administratora.



10 Weź CERTYX ze sobą

Autoryzuj telefony zespołu

DLACZEGO

Alerty i zatwierdzenia na telefonie — tylko na urządzeniach autoryzowanych przez administratora.

JAK

1. W Bezpieczeństwie przejdź do Urządzenia mobilne.
2. Wybierz użytkownika i Wygeneruj kod aktywacyjny; Twoja sesja musi być zalogowana z MFA.
3. Użytkownik instaluje CERTYX ze sklepu aplikacji organizacji, skanuje kod QR lub wpisuje kod i loguje się swoim kontem z MFA albo logowaniem firmowym.
4. Wybierz Unieważnij dostęp przy zgubionym urządzeniu; aplikacja na nim natychmiast przestaje działać.

> Ten krok wykonuje administrator. Jeśli nie masz tej roli, poproś administratora.

