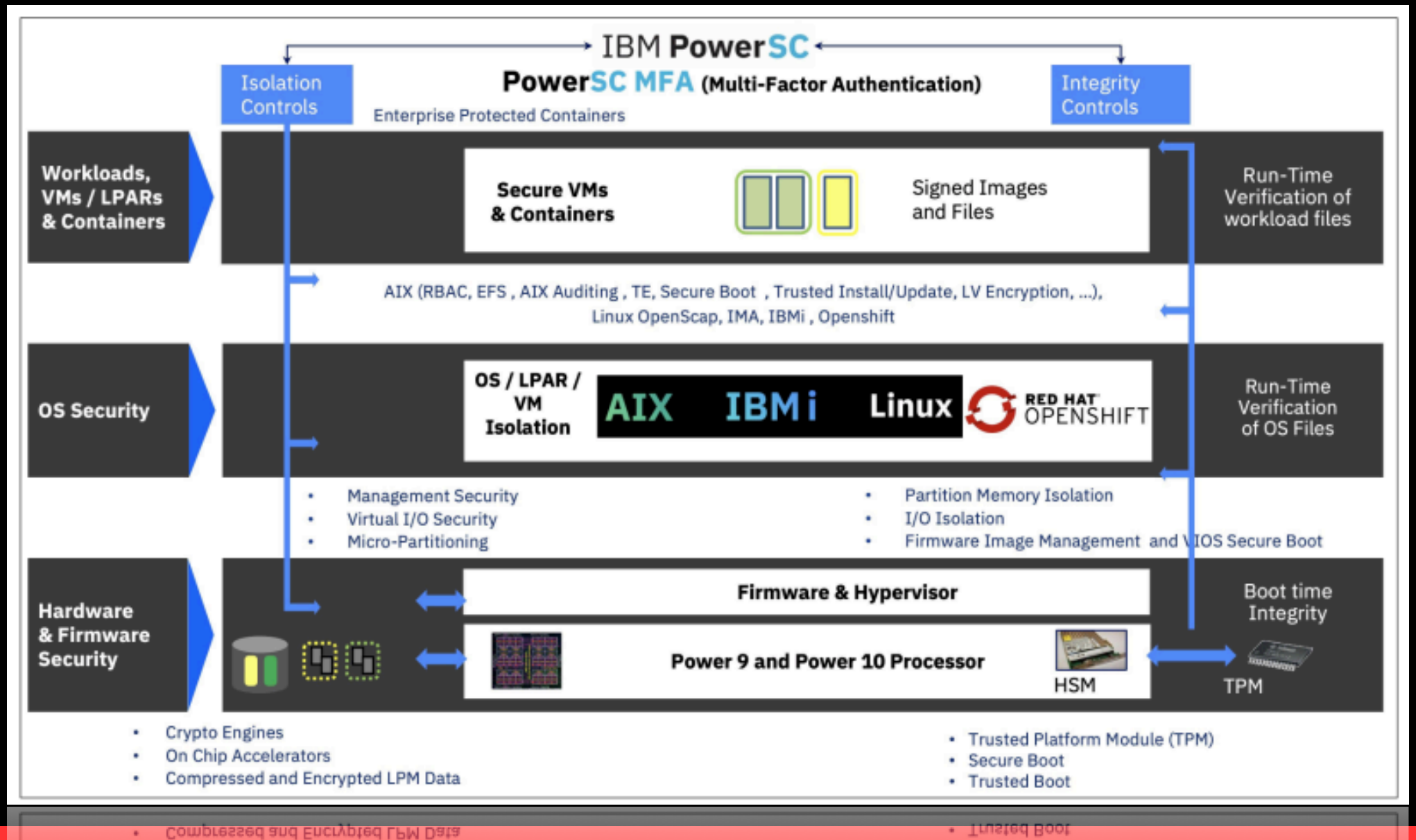
PowerSC - zarządzanie bezpieczeństwem i zgodnością



W świecie pełnym zagrożeń,
zabezpiecz dane w kwantowej twierdzy,
aby Twój biznes i Twoje życie było wolne od dramatów.
#NoDRAMA

Architektura bezpieczeństwa IBM Power Systems

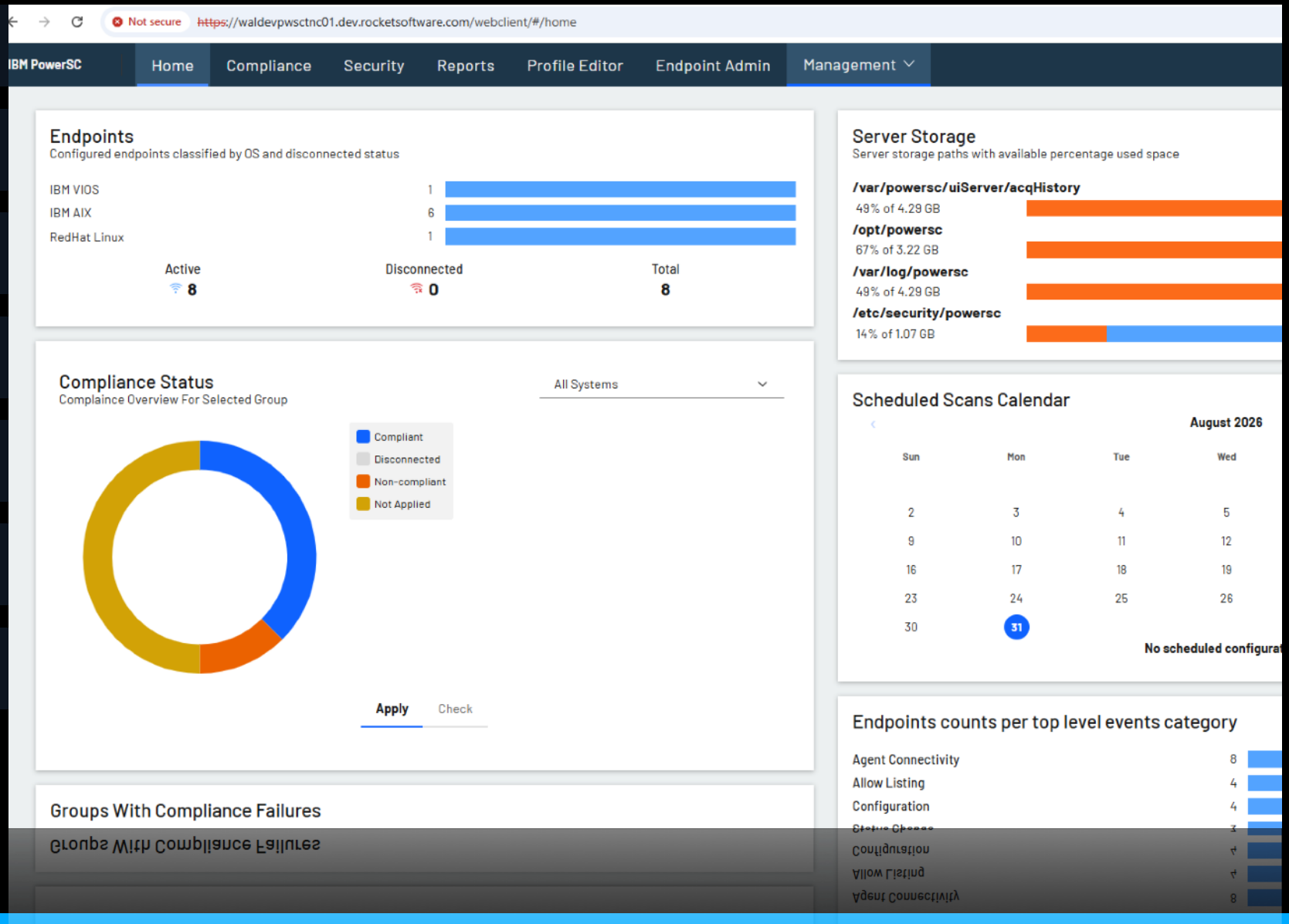


Zgodność (Compliance)

Automatyczna zgodność i analiza bezpieczeństwa

Panel zarządzania zgodnością PowerSC

- Panel zgodności
- Ogólny status zgodności
- Automatyczne egzekwowanie
- Sprawdzanie i symulacja profili
- Analiza błędów
- Dostosowywanie profili
- Alerty przy braku zgodności



Profile zgodności PowerSC

Profile można dostosowywać

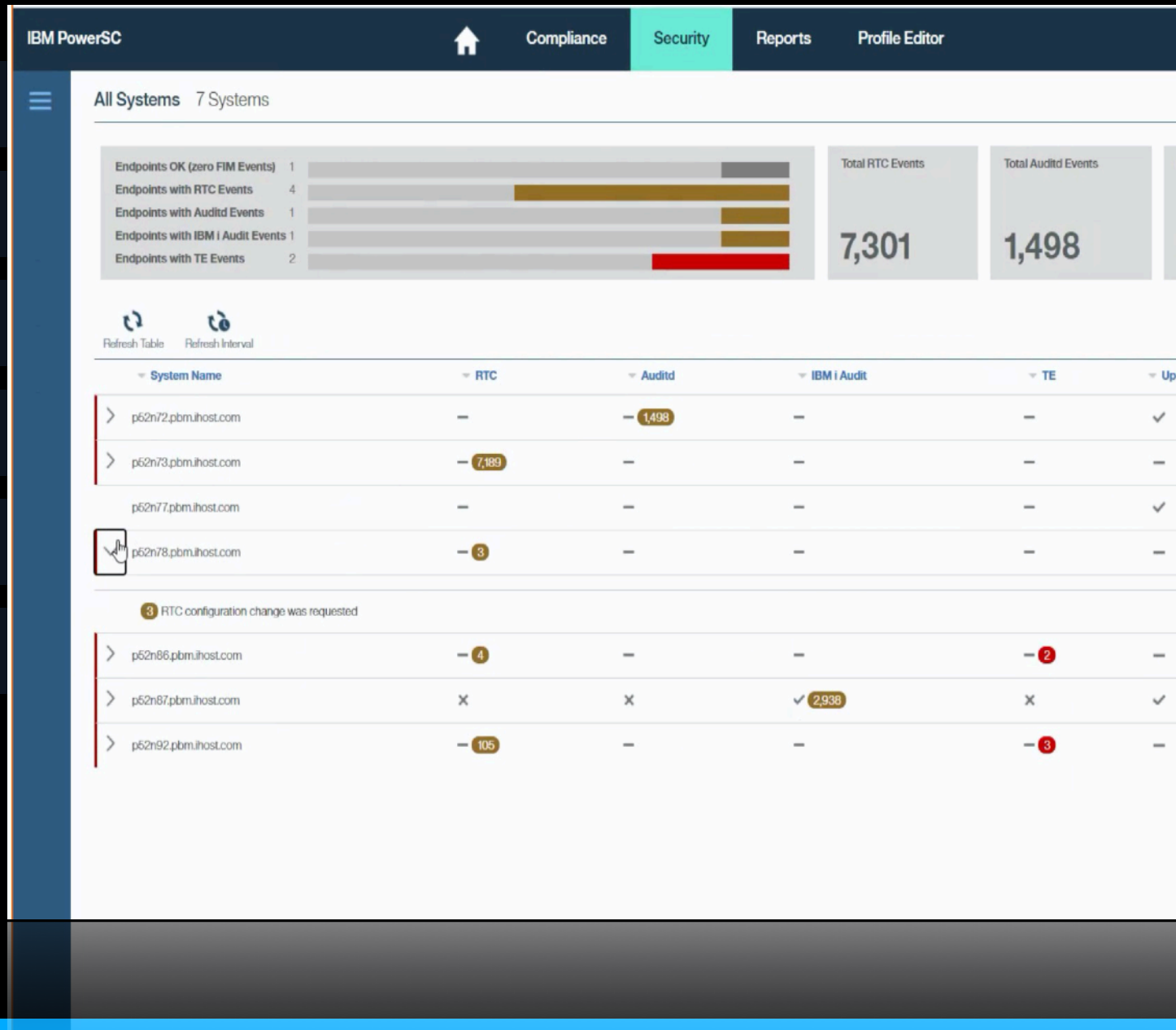
Profile AIX	Profile Linux	Profile IBM i
GDPR	GDPR	Hartowanie IBM i
PCI	PCI	CIS
CIS	Hartowanie SAP	PCI
HIPAA	CIS	
NERC	Hartowanie HMC	
DoD STIG		
Hartowanie SAP		
Hartowanie Oracle		

Bezpieczeństwo

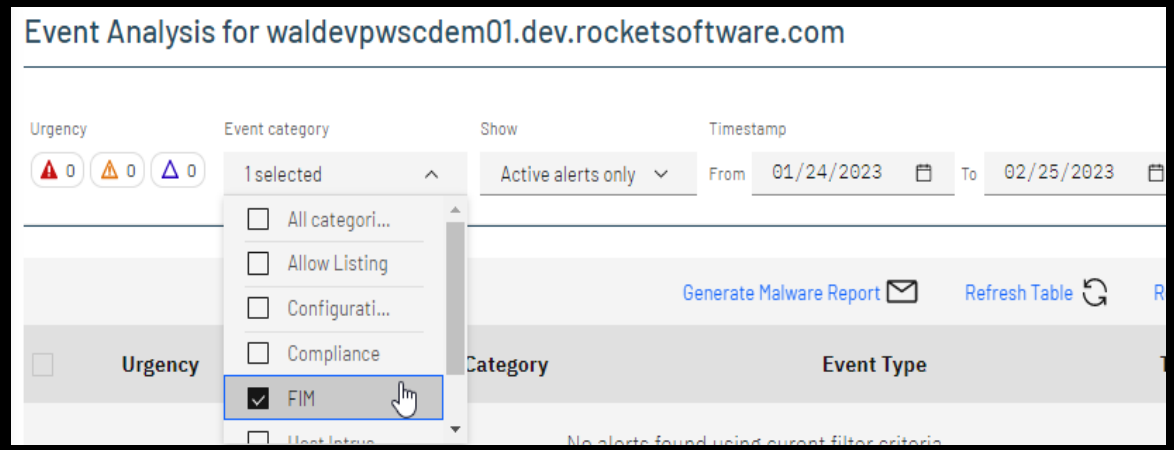
Ochrona w czasie rzeczywistym

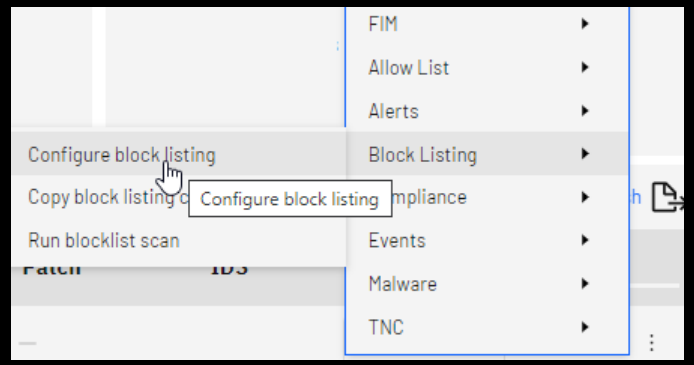
Panel bezpieczeństwa PowerSC

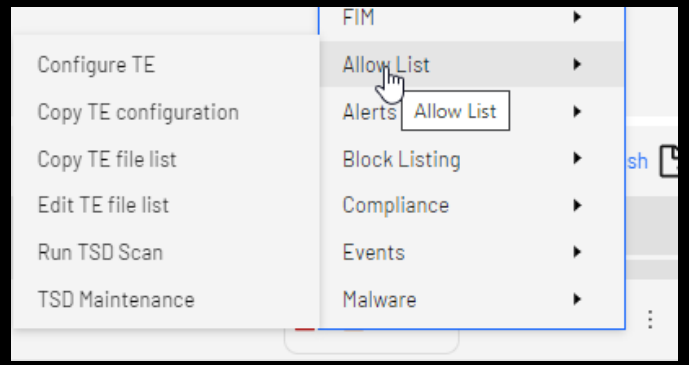
- Panel bezpieczeństwa w czasie rzeczywistym
- Ogólny status bezpieczeństwa
- Opis punktów końcowych
- Kategorie zdarzeń
- Szczegółowe typy zdarzeń
- Monitorowanie z jednego pulpitu

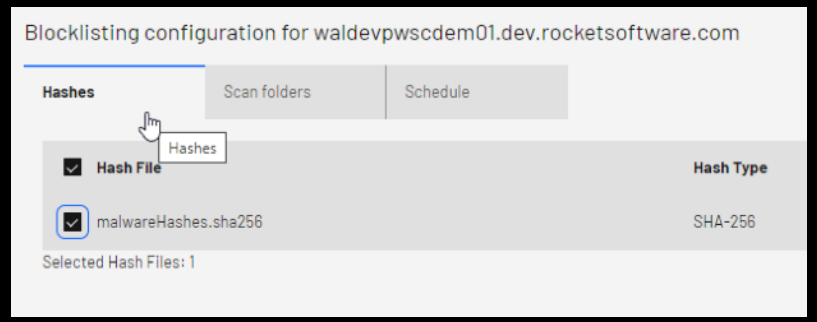


Funkcje bezpieczeństwa PowerSC





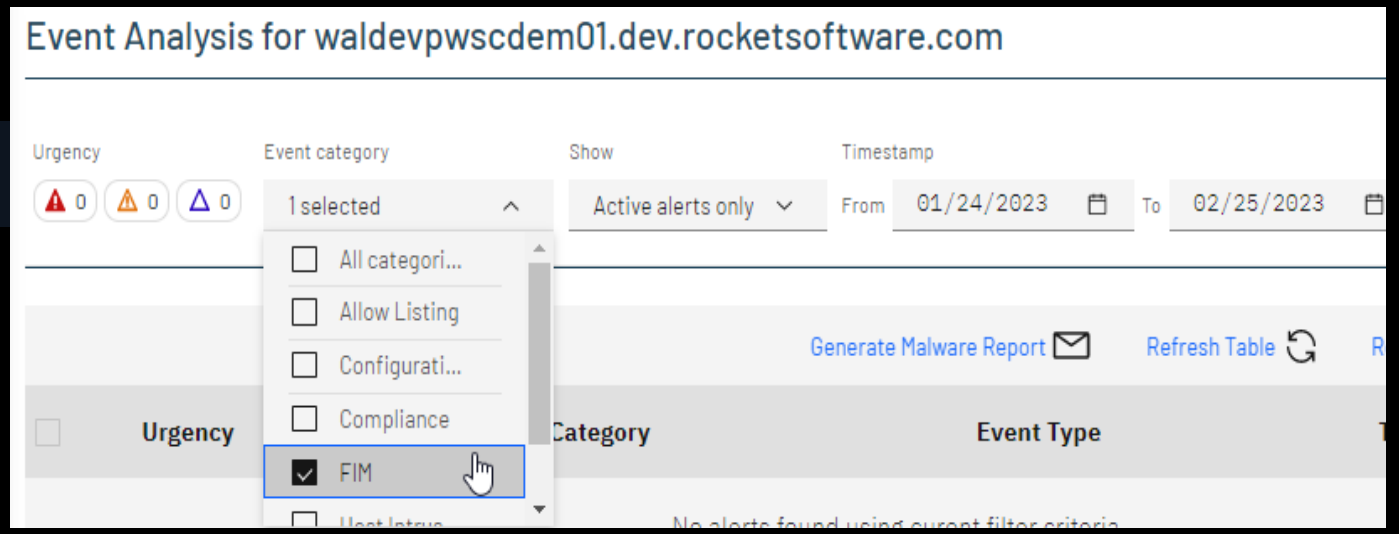




- Monitorowanie integralności plików (FIM)
- Biała lista (kontrola aplikacji)
- Czarna lista (polowanie na zagrożenia)
- Ochrona przed złośliwym oprogramowaniem (ClamAV)
- Integracja z SIEM
- Integracja z IBM Safeguarded Copy
- Możliwości EDR

Funkcje bezpieczeństwa PowerSC

Monitorowanie integralności plików (FIM)

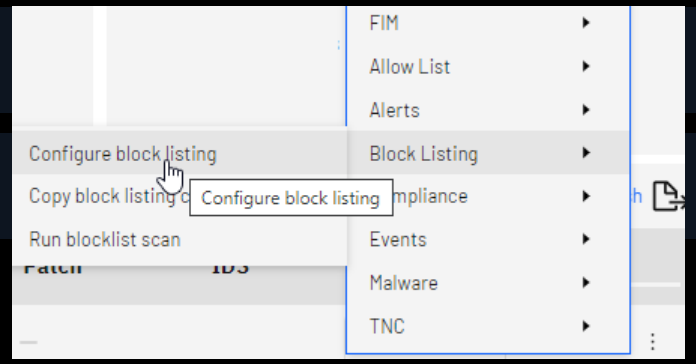


- Audyt zmian
- Uprawnienia
- Zawartość
- Pliki nieulotne
- Hooki OS

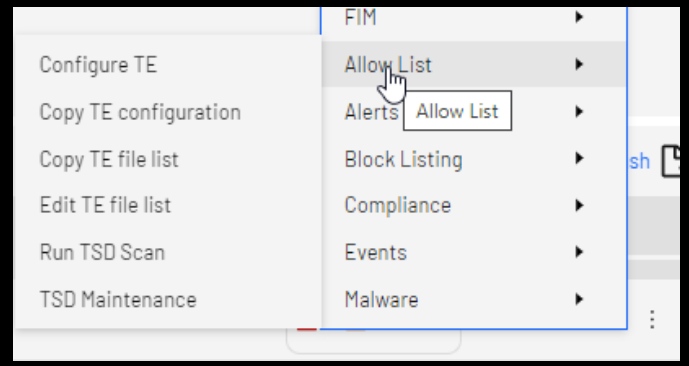
Funkcje bezpieczeństwa PowerSC

Biała lista (kontrola aplikacji)

Czarna lista (polowanie na zagrożenia)



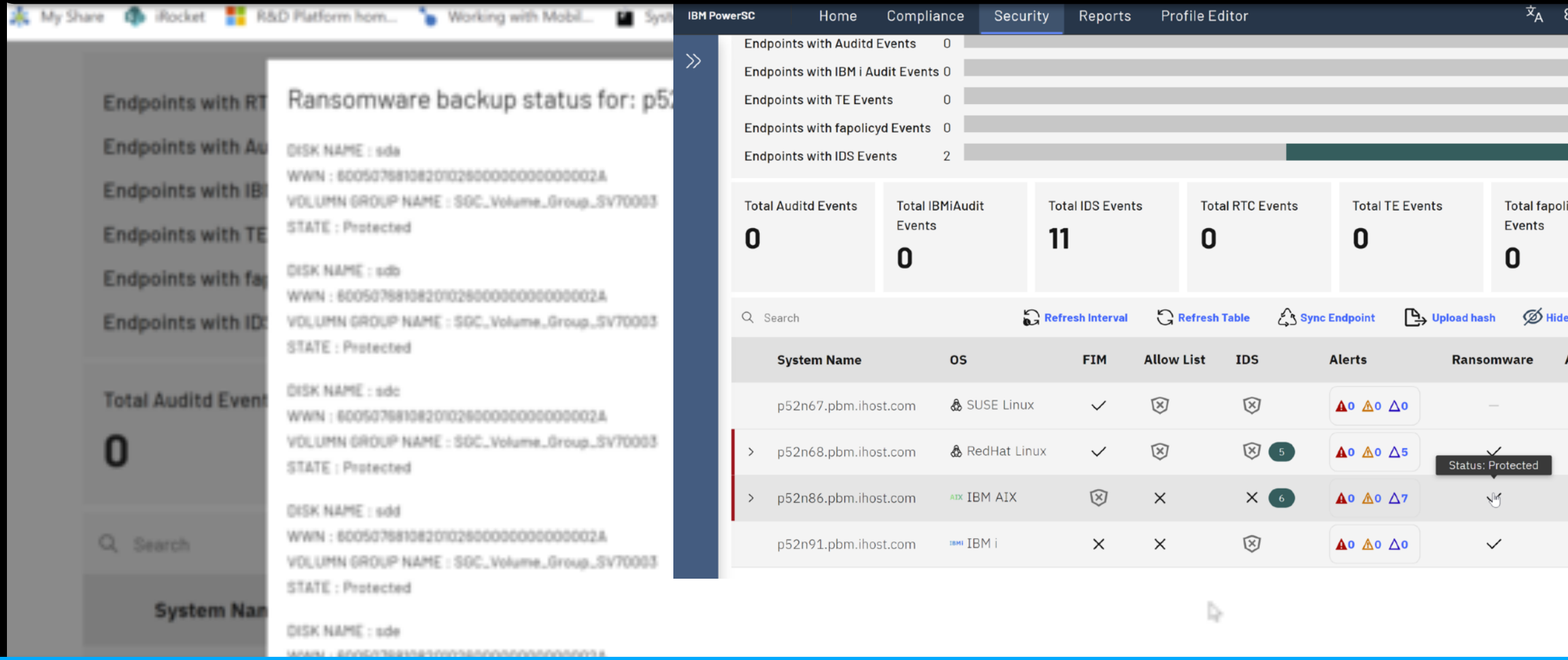
- Podejście zero-trust
- Dozwolone tylko to, co jawnie zaufane
- Może używać porównania skrótów (hash)



Integracja IBM Safeguarded Copy z CSM

Status ochrony przed ransomware

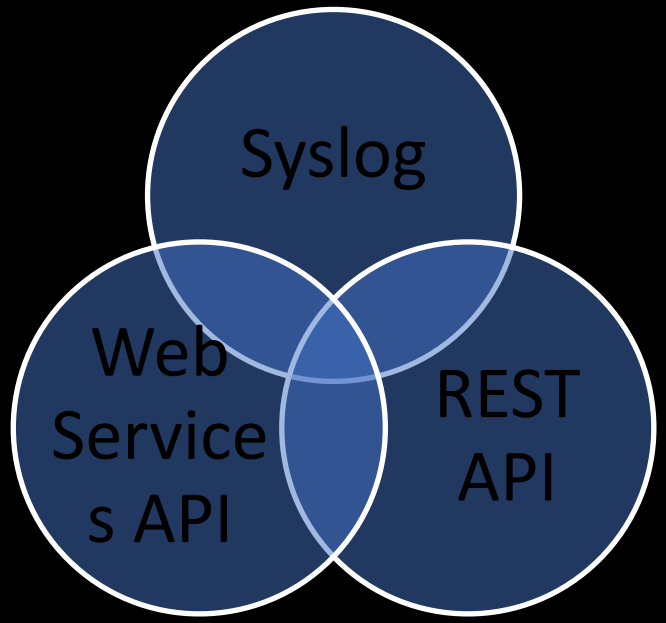
Integracja PowerSC z IBM Safeguarded Copy umożliwia monitorowanie statusu ochrony przed ransomware bezpośrednio z panelu PowerSC.

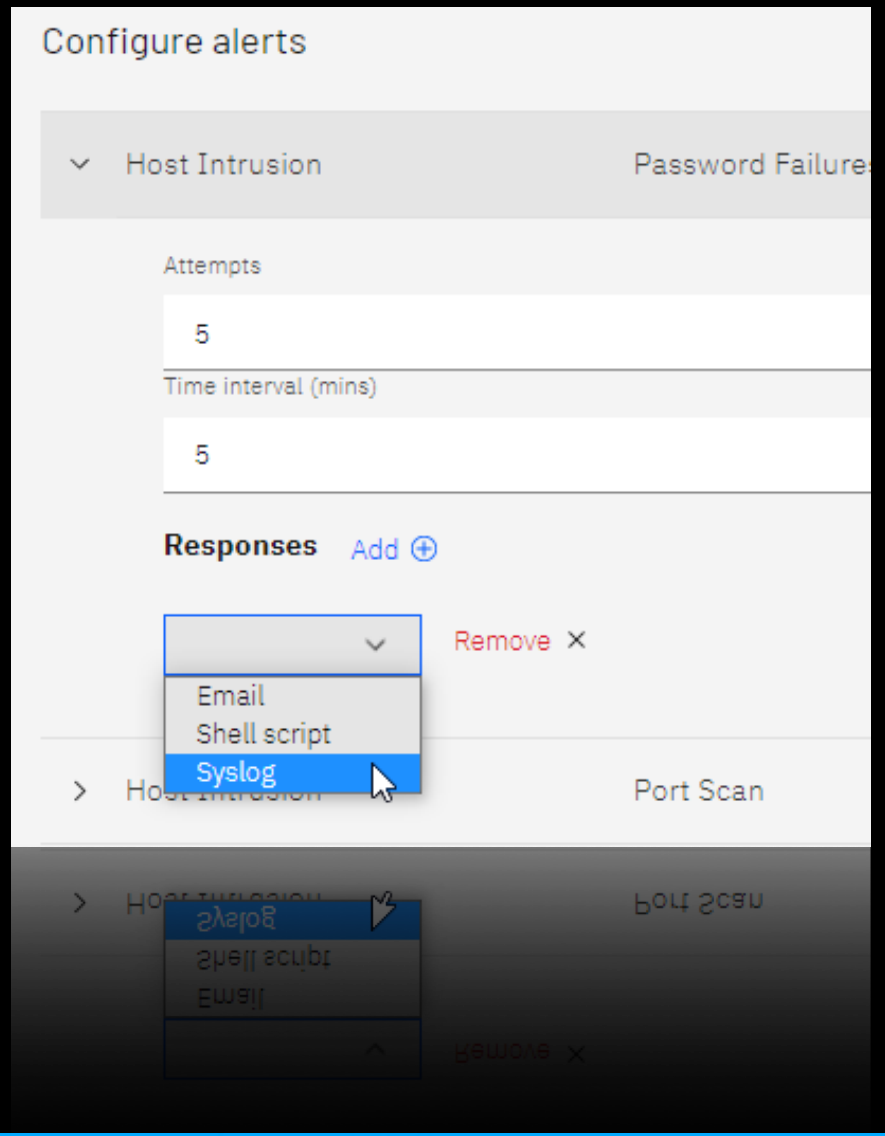


Ochrona punktów końcowych - Integracja z SIEM

EDR - przerywa ataki wcześniej w łańcuchu kill-chain
SIEM - bogatsze źródła danych i analityka

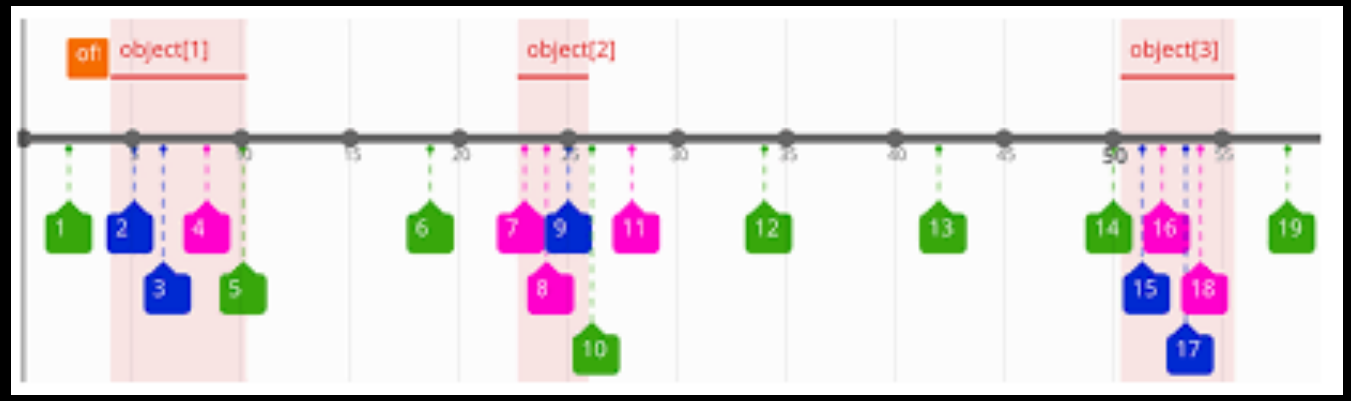
Protokoły wejściowe:
Syslog | REST API | Web Services API





Możliwości wykrywania i reagowania na zagrożenia (EDR)

- Wykrywanie i zapobieganie intruzjom (IDP)
- Inspekcja i analiza logów
- Wykrywanie anomalii, korelacja i reagowanie na incydenty
- Wyzwalacze reakcji
- Kontekst i filtrowanie zdarzeń



- Monitorowanie integralności plików (FIM)
- Biała lista (kontrola aplikacji)
- Czarna lista (polowanie na zagrożenia)
- Ochrona przed złośliwym oprogramowaniem (ClamAV)
- Integracja z SIEM
- Integracja z IBM Safeguarded Copy
- Możliwości EDR

Zarządzanie aktualizacjami (Patch Management)

Wykrywanie i egzekwowanie aktualizacji bezpieczeństwa

Panel zarządzania aktualizacjami PowerSC

Funkcja zarządzania aktualizacjami wykrywa maszyny wirtualne, które nie spełniają polityk zarządzania aktualizacjami.

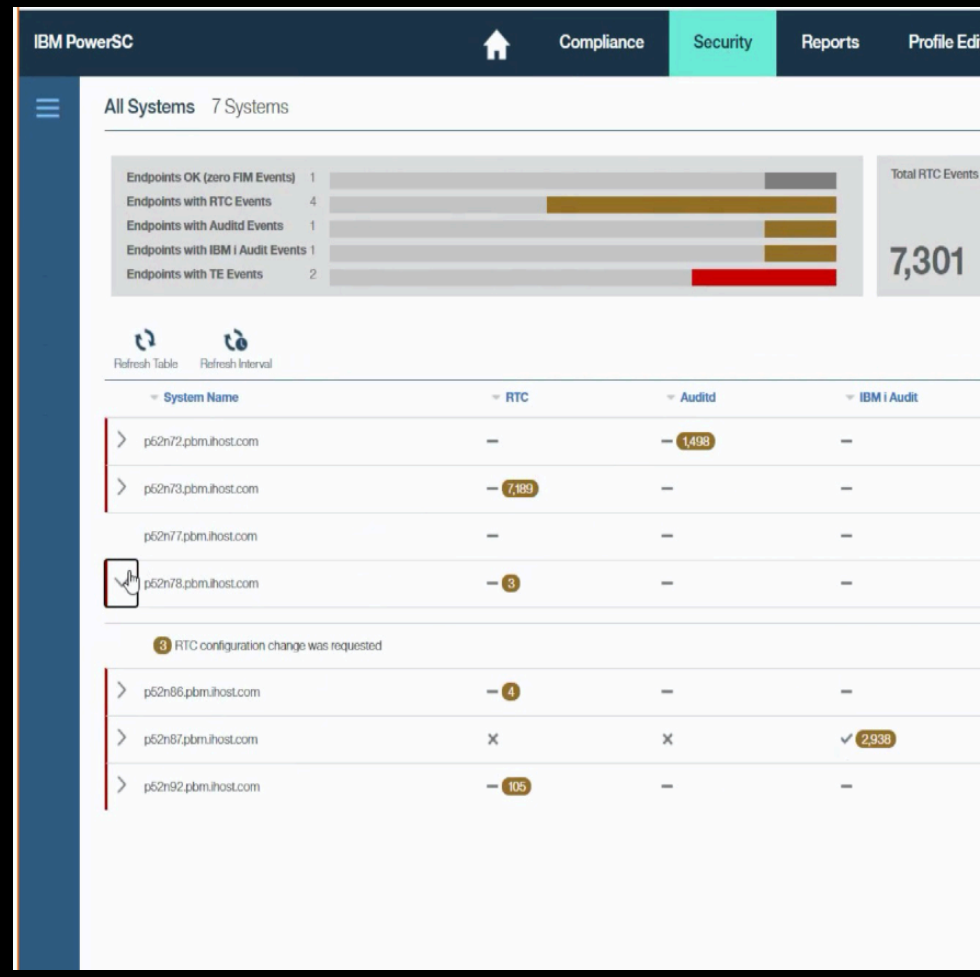
Panel pokazuje maszyny wirtualne z brakującymi poprawkami bezpieczeństwa.

Można je zaktualizować z poziomu panelu

Status zarządzania aktualizacjami

Widok zgodności

Punkty końcowe



Uwierzytelnianie wieloskładnikowe (MFA)

Tylko uwierzytelnieni użytkownicy mają dostęp

Uwierzytelnianie wieloskładnikowe PowerSC

Coś, co znasz

Hasło / kod PIN

Coś, co masz

Karta identyfikacyjna lub klucz kryptograficzny

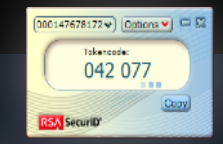
Kim jesteś

Odcisk palca lub inne dane biometryczne

Do potwierdzenia tożsamości i przyznania dostępu do systemu używane są co najmniej dwa czynniki uwierzytelniania.

PowerSC MFA – Metody uwierzytelniania

- RSA SecurID (via fob)
- Certyfikaty chronione PIN-em na kartach PIV/CAC
- TOTP (IBM Verify/ Google Authenticator/Duo Movile)
- Yubikey (via USB, np. na laptopie)
- Protokół RADIUS (Generic, Gemalto Safenet, RSA)
- Hasło / LDAP









Funkcje bezpieczeństwa PowerSC

Feature	PowerSC 2.3
Automatyczna zgodność	✔ Sprawdzanie i zastosowanie
Raportowanie zgodności (w tym harmonogramy)	✔ AIX, Linux, IBM i
Monitorowanie integralności plików	✔ AIX, Linux, IBM i
Biała lista / Kontrola aplikacji	✔ AIX i Linux
Czarna lista / Polowanie na zagrożenia	✔ AIX, Linux, IBM i
Anti-Malware (baza wirusów)	✔ AIX, Linux, IBM i
Zarządzanie aktualizacjami	✔ AIX, Linux
Wykrywanie i reagowanie na zagrożenia (EDR)	✔ AIX, Linux, IBM i
IDS/IPS / Firewall (EDR)	✔ AIX, Linux, IBM i
Inspekcja i analiza logów (EDR)	✔ AIX, Linux, IBM i
Wykrywanie anomalii i korelacja (EDR)	✔ AIX, Linux, IBM i
Wyzwalacze reakcji (EDR)	✔ AIX, Linux, IBM i
Kontekst i filtrowanie zdarzeń (EDR)	✔ AIX, Linux, IBM i
Uwierzytelnianie wieloskładnikowe (MFA)	✔ AIX, Linux, IBM i