esecure | SECURE VISIO

SOAR

Automatyzacja zarządzania
i reagowania na incydenty

NextGen SIEM

Wykrywanie incydentów
i zagrożeń bezpieczeństwa

Jedna platforma do wykrywania i zarządzania incydentami, podatnościami i ryzykiem

SecureVisio SOAR

to specjalistyczne rozwiązanie Security Orchestration, Automation and Response służące do automatyzacji zarządzania i reagowania na incydenty oraz usprawnienia innych procesów zarządzania bezpieczeństwem.

Funkcje i korzyści rozwiązania:

- Uporządkowana praca ludzi – proces zarządzania incydentami (Workflow) odbywa się etapowo, zgodne z obowiązującymi standardami (m.in. ISO/IEC 27035)
- Unifikacja narzędzi - jedna graficzna konsola zawiera wszystkie narzędzia i informacje potrzebne do wyjaśniania i obsługi incydentów
- Automatyzacja pracy ludzi - gotowe do użycia scenariusze obsługi incydentów (Playbooki) dla wielu rodzajów incydentów
- Integracja narzędzi i źródeł danych - Plabooki automatycznie uruchamiają narzędzia i pozyskują dane ze źródeł zewnętrznych (m.in. Threat Intelligence)
- Priorytetyzacja biznesowa - incydenty są automatycznie priorytetyzowane w odniesieniu do ważności zasobów dla organizacji (tzn. wspomaganych procesów, wrażliwych informacji)
- Świadomość skutków incydentu - proces obsługi incydentów odbywa się ze świadomością ryzyka (norma ISO/IEC 27005) i biznesowych skutków naruszenia bezpieczeństwa
- Zunifikowane zarządzanie podatnościami – współpraca z narzędziami Vulnerability Assessment i CVE oraz zintegrowane narzędzia Workflow i Playbook do zarządzania podatnościami
- Symulacja i wizualizacja zagrożeń - analiza incydentów i podatności jest wspomagana za pomocą graficznych narzędzi symulacji ataków i innych zagrożeń
- Metryki efektywności z kontekstem biznesowym - narzędzia obliczają kluczowe wskaźniki efektywności KPI (key performance indicator) oraz kluczowe wskaźniki ryzyka KRI (key risk indicator)

SecureVisio NextGen SIEM

to nowej generacji rozwiązanie Security Information and Event Management zaprojektowane pod kątem spełnienia współczesnych wymagań bezpieczeństwa umożliwiające szybkie wykrywanie incydentów i innych zagrożeń.

Funkcje i korzyści rozwiązania:

- Wiele metod detekcji – reguły korelacji SIEM, analiza behawioralna użytkowników i systemów (UEBA), Threat Intelligence
- Dynamiczne reguły SIEM – reguły korelacji zdarzeń automatycznie dostosowują się do zmian sieci i systemów wykrywanych za pomocą funkcji Auto-Discovery
- Kontekst biznesowy – analiza logów w SIEM odbywa się w kontekście aktualnego ryzyka dla procesów organizacji i wrażliwych informacji
- Szeroki zakres analizy – SIEM poddaje analizie zdarzenia bezpieczeństwa (logi), aktualne podatności, informacje Threat Intelligence oraz oszacowane wielkości ryzyka
- Repozytorium zdarzeń – specjalistyczna baza plikowa do długoterminowego składowania i szybkiego wyszukiwania zdarzeń bezpieczeństwa
- Wiele metod odczytu logów – Syslog, e-mail, Windows Event Forwarding, a także możliwość odczytu logów z baz danych oraz plików płaskich
- Graficzny edytor parserów - predefiniowany zestaw parserów może zostać rozszerzony o nowe parsery tworzone za pomocą graficznego edytora
- Efektywność kosztowa - licencjonowanie oparte jest na rzeczywistej liczbie monitorowanych zasobów IT bez ograniczeń na wielkość analizowanych danych