2023

secureVISIO

Commercial

Esecure Sp. z o.o.

ul. Hofftamanowej 19, PL-35016 Rzeszów, Polska

www.securevisio.com

SecureVisio to zintegrowana platforma do kompleksowego i efektywnego zarządzania bezpieczeństwem. Kompleksowe zarządzanie cyberbezpieczeństwem w SecureVisio odbywa się na trzech płaszczyznach:

PREWENCJI DETEKCJI REAKCJI (PDR)

PREWENCJA

CMDB IRM TVM

W ramach prewencji SecureVisio pozwala automatycznie stworzyć i utrzymać centralną e-dokumentację zasobów IT (**funkcjonalność CMDB** – Configuration Management Database), prowadzić analizę ryzyka cyberzagrożeń (**narzędzia klasy IRM** – Integrated Risk Management) oraz zarządzać podatnościami z uwzględnieniem kluczowych procesów i zasobów organizacji (**mechanizm TVM** – Threat and Vulnerability Management).

DETEKCJA

SIEM UEBA

Z perspektywy detekcji, SecureVisio wspomaga użytkowników w wykrywaniu zaawansowanych zagrożeń poprzez działanie kontekstowych reguł korelacyjnych (**funkcjonalność SIEM** – Security Information and Event Management) oraz wykrywania anomalii w zachowaniu użytkowników oraz systemów (**narzędzie klasy UEBA** – User and Entity Behavior Analysis).

REAKCJA

SOAR

W obszarze reakcji platforma SecureVisio dostarcza gotowe, automatyczne scenariusze reakcji, które pozwalają szybko obsłużyć wykryte zagrożenia (**funkcjonalność typu SOAR** – Security Automation and Response).

SecureVisio - podsumowanie korzyści

- Zintegrowana platforma do zarządzania bezpieczeństwem z wbudowanymi i gotowymi do użycia narzędziami do PREWENCJI, DETEKCJI I REAKCJI (PDR) względem kluczowych zagrożeń;
- Szerokie pokrycie wymagań prawnych: UoKSC, RODO, KRI – pełna zgodność z kluczowymi wytycznymi dla jednostek publicznych w zakresie cyberbezpieczeństwa;
- Zgodność systemu z metodykami: ISO27001, ISO27005, ISO27035;
- Wbudowane w system narzędzia klasy: CMDB, IRM, SIEM, UEBA, SOAR, TVM eliminują konieczność indywidualnych zakupów i wdrożeń kilku systemów oraz ich kosztownej i długotrwałej integracji;
- Lokalne wsparcie posprzedażowe w zakresie utrzymania systemu – dedykowany konsultant producenta do dyspozycji klientów przez cały okres wsparcia;
- Interfejs systemu w języku polskim i angielskim – czytelny i przejrzysty sposób prezentacji danych;
- Szybkie i nieangażujące użytkowników wdrożenie – już w pierwszym miesiącu instalacji system skutecznie podnosi poziom bezpieczeństwa organizacji;
- Elastyczne i korzystne licencjonowanie oparte o model licencji wieczystej;
- Optymalizacja wydatków na bezpieczeństwo – wdrożenie matrycy analizy ryzyka pozwala obiektywnie i racjonalnie spojrzeć na konieczność zakupu nowych technologii bezpieczeństwa (zobrazowanie ryzyk dla kluczowych procesów);
- Priorytetyzacja z wykorzystaniem kontekstu – wbudowane narzędzia inwentaryzacji zasobów i procesów IT w połączeniu z silnikiem analizy ryzyka, pozwalają operatorom skoncentrować się na kluczowych zagrożeniach i wykorzystać dostępny czas na obsługę najważniejszych alarmów;
- Użytkownicy z poziomu jednego narzędzia mają dostęp do elektronicznej dokumentacji, analizy ryzyka cyberzagrożeń, przeglądarki logów bezpieczeństwa, widoku obługi incydentów, podatności oraz obszaru zarządzania danymi osobowymi.