SECUREVISIO

Szpital zgodny z KSC, RODO oraz KRI

Jak z wykorzystaniem SecureVisio podnieść poziom cyberbezpieczeństwa

Szpitale stoją przed szansą, ale i wyzwaniem podniesienia poziomu cyberbezpieczeństwa dla swoich kluczowych procesów i usług. Ustawa o Krajowym Systemie Cyberbezpieczeństwa *(UoKSC)*, Rozporządzenie o Ochronie Danych Osobowych *(RODO)* i Rozporządzenie ws. Krajowych Ram Interoperacyjności *(KRI)* wskazują wiele obszarów, które muszą zostać zaadresowane przez dostawcę usług kluczowych w celu spełnienia wymogów ustawowych. System SecureVisio, jako zintegrowana platforma do kompleksowego i efektywnego zarządzania bezpieczeństwem, umożliwia spełnienie tych wymogów.

Kompleksowe zarządzanie cyberbezpieczeństwem w SecureVisio odbywa się na trzech płaszczyznach:
PREWENCJI, DETEKCJI oraz REAKCJI *(PDR)*.

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

Wdrożenie SecureVisio zapewni spełnienie wymagań zdefiniowanych w UoKSC, RODO oraz KRI poprzez:

- Zapewnienie szacowania ryzyka dla usług krytycznych;
- Zapewnienie szacowania ryzyka dla osoby fizycznej;
- Zapewnienie szacowania ryzyka dla rejestrów publicznych, systemów informatycznych oraz wymiany informacji w postaci cyfrowej;
- Wdrożenie adekwatnych do wyników szacowania ryzyka środków technicznych;
- Identyfikowanie i usuwanie podatności;
- Wykrywanie incydentów, klasyfikowanie ich oraz obsługę;
- Zgłaszanie naruszeń bezpieczeństwa;
- Prowadzenie dokumentacji zgodnej ze zdefiniowanymi wymaganiami.

SECUREVISIO

SECUREVISIO

Podsumowanie korzyści dla szpitali:

- 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;
- Wdrożenia w organizacjach służby zdrowia – system sprawdzony w realiach pracy szpitali;
- 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 obsługi incydentów, podatności oraz obszaru zarządzania danymi osobowymi;
- Automatyzacja zarządzania incydentami i podatnościami.

W opinii Naszego Klienta

„SecureVisio stanowi trzon naszego SOC. Od dwóch lat intensywnie korzystamy z tego produktu i nie wyobrażamy sobie teraz pracy w obszarze operacyjnym, a także w wykrywaniu incydentów i zdarzeń bez SecureVisio. To jest narzędzie, które w sposób optymalny pozwala na podniesienie poziomu bezpieczeństwa w każdej organizacji, w tym u operatorów usług kluczowych. Daje szpitalom szansę na efektywne i pełne uzupełnienie braków w cyberbezpieczeństwie."

Michał Hordejuk
Konsultant ds. Cyberbezpieczeństwa
„Nowy Szpital Wojewódzki" Sp. z o.o.