SECUREVISIO

Wdrożenie SecureVisio - Case Study

„Nowy Szpital Wojewódzki" Sp. z o.o.

„Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UoKSC) nakłada na operatorów usług kluczowych, w tym szpitale, szereg obowiązków. Uznaliśmy, że musimy stworzyć usługę SOC (ang. Security Operations Center) i zbudować ją w oparciu o kompleksową platformę, która będzie czymś więcej niż SIEM (ang. Security Information and Event Management). Wcześniej korzystaliśmy z QRadar, ale nie spełniał naszych oczekiwań – zdawaliśmy sobie sprawę, że SOC to nie tylko SIEM i że wyłącznie współpraca kliku narzędzi może stworzyć kompletną platformę do zarządzania bezpieczeństwem.

SecureVisio (SV) to kompleksowa platforma składająca się ze SIEM, SOAR (ang. Security Orchestration, Automation and Response), UEBA (ang. User and Entity Behavior Analytics), analizy ryzyka, zarządzania podatnościami oraz incydentami, która wprost adresuje obowiązki wynikające z ustawy o KSC.

W związku z tym w maju 2020 roku wdrożyliśmy SecureVisio, które jest nie tylko SIEMem – oprócz samej korelacji logów i zdarzeń SV pozwala na zarządzanie podatnościami i analizę ryzyka, a wbudowany SOAR minimalizuje czas potrzebny na obsługę zdarzeń.

Analiza ryzyka cyberzagrożeń jest prowadzona w sposób dynamiczny i aktualny oraz uwzględnia rolę procesów w organizacji. Wbudowana baza zasobów informacyjno–usługowych pozwala na priorytetyzowanie kontekstu organizacji oraz sprawne i szybkie zarządzanie bezpieczeństwem.

Platforma pozwala na automatyzację i orkiestrację optymalizacji czasu i kosztów zarządzania bezpieczeństwem – SecureVisio ma wbudowany system rozpoznawania najważniejszych zasobów wspierających krytyczne procesy biznesowe oraz wrażliwe dane, i zasoby te chroni w pierwszej kolejności. W praktyce oznacza to, że dzięki SV posiadamy pełną wiedzę o naszej infrastrukturze IT, gdzie dla każdego zasobu określiliśmy jego krytyczność dla organizacji, zarówno pod kątem technicznym, jak i biznesowym. SV posiada również moduł ochrony danych osobowych, pozwalający na spełnienie wymogów ustawowych poprzez dostarczenie pełnej analizy ryzyka utraty poufności, dostępności oraz integralności danych.

Dzięki SV wiemy, który system w szpitalu jest kluczowy, które elementy powinny zostać zabezpieczone i które są najważniejsze z punktu widzenia analizy ryzyka.

SV 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.

Ważna dla nas jest również dostępność zatrudnionych przez producenta ekspertów ds. cyberbezpieczeństwa, z którymi w ramach wykupionego wsparcia możemy na bieżąco konsultować wpływ naszych modyfikacji na skuteczność działania systemu oraz rozwiązywać problemy techniczne komunikując się w języku polskim. "

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