

► Audyt sieci przemysłowych ICS/SCADA

Kompleksowy audyt sieci i urządzeń pod kątem cyberzagrożeń oraz niewłaściwego działania elementów sieci – bez integracji w sieć i zakłóceń jej działania dzięki wykorzystaniu narzędzia CyberX XSense.

Obecne sieci ICS/SCADA działają w oparciu w głównej mierze o technologie sprzed kilkunastu lub kilkudziesięciu lat, gdy zapewnienie bezpieczeństwa nie było priorytetem. Rozbudowa sieci, pojawienie się nowych zagrożeń i coraz częstsze ataki na krytyczną infrastrukturę przemysłową wymagają zwiększenia poziomu bezpieczeństwa.

► Wyzwanie Klienta

Infrastruktura przemysłowa staje się w coraz większym stopniu przedmiotem zainteresowania cyberprzestępców, którzy wykorzystują podatności systemów SCADA oraz brak ich właściwego zabezpieczenia.

Jednocześnie sieci SCADA są krytyczne z punktu widzenia zapewnienia usług krytycznych (np. dostawy energii, wody), zapewnienia ciągłości procesu produkcyjnego czy bezpieczeństwa.

Incydenty związane z sieciami przemysłowymi nie są już rzadkością, a ich skutki mają coraz częściej charakter fizyczny.

Organizacje mają ograniczoną możliwość pełnej identyfikacji zasobów, weryfikacji ich powiązań i poziomu zabezpieczenia przy jednoczesnym niezakłócaniu działania sieci i systemów.

► Zakres świadczonych usług

Audyt ma charakter kompleksowy. W jego ramach identyfikowane są luki i podatności oraz wskazywane są konkretne sposoby ich usunięcia i zabezpieczenia przed wystąpieniem incydentów w przyszłości.

W skład proponowanej usługi wchodzi następujące zadania:

- Analiza zagrożeń i podatności sieci jej elementów
- Ocena obecnego poziomu zabezpieczenia i zarekomendowanie odpowiednich zmian
- Wykrywanie ataków cybernetycznych i błędnego działania poszczególnych elementów (incydenty operacyjne)
- Mapowanie sieci/analiza zasobów i wzajemnych powiązań pomiędzy nimi

Zarekomendowanie odpowiednich zmian w celu podniesienia poziomu bezpieczeństwa

► Wsparcie PBSG

PBSG świadczy usługę audytu sieci ICS/SCADA w oparciu o wiedzę oraz narzędzie CyberX XSense – lidera w zakresie bezpieczeństwa sieci przemysłowych.

CyberX XSense zbiera dane przesyłane w sieci jako moduł pasywny, które następnie podlegają zaawansowanej analizie porównawczej. Zagrożenia i podatności wykrywane są na podstawie analizy tysięcy skanów sieci, badań przeprowadzonych przez CyberX oraz opatentowanej technologii wykrywającej anomalie/zagrożenia typu zero-day.

Rezultatem przeprowadzenia audytu jest kompleksowy raport stanowiący powiązanie wyników analizy technicznej, specjalistycznej wiedzy z zakresu bezpieczeństwa oraz najlepszych standardów ochrony sieci przemysłowych.

► Korzyści dla Klienta

Korzyści wynikające z zastosowania audytu sieci przemysłowej:

- Uniknięcie strat finansowych i wizerunkowych powstałych w wyniku ataku cybernetycznego
- Zapewnienie bezpieczeństwa sieci ICS/SCADA
- Ograniczenie prawdopodobieństwa wystąpienia incydentów operacyjnych powstałych wskutek nieprawidłowego działania elementów infrastruktury
- Przedstawienie wykazu wszystkich urządzeń i połączeń w sieci, w tym połączeń niebezpiecznych (np. połączenie do sieci internet)
- Wykaz luk i podatności wraz ze wskazaniem sposobów ich usunięcia
- Możliwość przeprowadzenia analizy wszystkich elementów infrastruktury; brak urządzeń niewspieranych
- Audyt i analiza infrastruktury bez wpływu na jej działanie, brak jakichkolwiek zakłóceń
- Wykrywanie również podatności typu zero-day

► O CyberX

Dostarczając swoje produkty klientom z całego świata, CyberX umożliwia wykrywanie zagrożeń oraz identyfikację incydentów w czasie rzeczywistym poprzez umożliwienie dokonania pełnego wglądu w sieci przemysłowe. CyberX jest członkiem Industrial Internet Consortium (IIC) i ICS-ISAC oraz został uznany przez Gartnera jako Cool Vendor w zakresie bezpieczeństwa technologicznego (2015). CyberX otrzymał również wiele wyróżnień, włączając nagrodę CDM „Best Product in ICS/SCADA Security Solution of 2016”.