trecom | atman non-stop-data | secureVISIO

Wdrożenie usługi Security Operations Center oraz platformy SecureVisio w Atman

Case Study

Atman

Największy w Polsce dostawca usług kolokacji, cloud computingu oraz bezpieczeństwa danych.

Infrastruktura Atman

- Trzy centra danych o łącznej powierzchni **19,5 tys. m²**.
- W budowie czwarte centrum danych WAW-3 o powierzchni **19 972 m²** i mocy docelowej **43 MW IT** (otwarcie w 2025 r.).
- **Ogólnopolska** sieć światłowodowa, transmisja danych i sieć MPLS.
- Punkt wymiany ruchu Thinx.
- Symetryczny Internet dla firm i instytucji.
- Farma serwerów dedykowanych i platformy chmury obliczeniowej w technologii Open Stack i VMware.

Wyzwanie

- Wdrożenie platformy SIEM jako kompleksowego orkiestratora w zarządzaniu ryzykiem, podatnościami oraz dostarczającą funkcjonalności automatycznych reakcji na wykryte zdarzenia.
- Znalezienie zaufanego partnera do skutecznego wykrywania i reagowania na incydenty.
- Integracja i przetwarzanie dużej ilości danych telemetrycznych z różnych systemów IT w ramach rozproszonej infrastruktury.

Zastosowane rozwiązania

- Monitoring bezpieczeństwa **Trecom SOC** – usługa zarządzana, zapewniająca monitoring, analizę i reakcję na incydenty 24/7/365.
- Platforma **SecureVisio** – wdrożona w modelu Software as a Service (SaaS), zapewniająca:
  - Zbieranie i analizę zagrożeń w czasie rzeczywistym dzięki rozwiązaniom SIEM, UEBA i telemetrii agentowej.
  - Priorytetyzację incydentów i podatności w oparciu o wbudowaną analizę ryzyka.
  - Automatyzację reakcji na zagrożenia poprzez predefiniowane playbooki w SOAR.
  - Stworzenie bazy zasobów (CMDB) wspomagającej działania prewencyjne dzięki informacjom o zasobach IT, ich relacjach i właścicielach oraz pozostałych danych operacyjnych.
  - Analizę ryzyka poszczególnych aktywów oraz automatyczne sugestie reakcji na ryzyko.
  - Unikalne kompetencje w wizualizacji potencjalnych ścieżek ataku w ramach MITRE ATT&CK wspierane przez analizę Business Impact Analysis (BIA).

Korzyści dla Atman

Wykrywanie, analiza i reagowanie na zagrożenia w trybie 24/7/365.

Minimalizacja ryzyka przestojów i strat finansowych.

Optymalizacja kosztów i skalowalność dzięki rozwiązaniu w modelu SaaS oraz konsolidacji analizy ryzyka, incydentów i podatności w jednej platformie.

Podniesienie poziomu świadomości o zagrożeniach dzięki bazie CMDB oraz analizie ryzyka.

Atman

Od 2011 roku Atman jest liderem rynku data center w Polsce* działającym na rynku ICT nieprzerwanie od 1997 roku. Firma oferuje usługi kolokacji i bezpieczeństwa danych, cloud computingu i serwerów dedykowanych, oraz dostępu do Internetu i szerokopasmowej transmisji danych. Spółka opiera swoje portfolio na własnej infrastrukturze, obejmującej ogólnopolską sieć światłowodową, punkt wymiany ruchu Thinx oraz trzy centra danych o łącznej powierzchni 19,5 tys. m^2 brutto. Powierzchnia, którą dysponuje Atman, niebawem niemal się podwoi, w związku z budową trzeciego centrum danych Atmana - WAW-3, składającego się z trzech budynków, o łącznej powierzchni 19,972 m^2 i docelowej mocy 43 MW IT. Otwarcie pierwszego budynku planowane jest na pierwszą połowę 2025 roku.

W związku z dynamicznym rozwojem oraz wymogami nowych dyrektyw DORA i NIS 2 Atman szukał partnera, któremu zleci zadania związane z monitoringiem i zarządzaniem incydentami w ramach **Security Operations Center w trybie 24/7/365**.

Wykrywanie, analiza i reagowanie na incydenty bezpieczeństwa w czasie rzeczywistym jest szczególnie ważne dla organizacji, takich jak Atman, który zarządza serwerami zawierającymi dane tysięcy klientów. Incydent cyber pozostawiony bez reakcji mógłby przerodzić się w przestój w działaniu systemów Atmana, który wiązałby się ze stratą finansową oraz szkodami refutacyjnymi.

Z tego względu Atman określił wysokie wymagania dla potencjalnego dostawcy usługi SOC. Wśród warunków do spełnienia znalazły się między innymi – dostępność usługi w trybie 24/7/365, SLA 99,9% w skali roku, obsługa peeków EPS, czy lista certyfikatów analityków i audytorów zawierająca m.in. CISM, CISSP, CCSP czy audytora wiodącego SZBI zgodnie z normą ISO 27001.

> Biorąc pod uwagę mnogość rozwiązań typu SIEM na rynku, wydawać by się mogło, że wybór nie będzie wyzwaniem. **Naszym celem jednak było znalezienie rzetelnego i sprawdzonego partnera**, który wraz z systemem SIEM byłby w stanie dostarczyć nam usługę SOC realizowaną przez doświadczony zespół i dojrzałe procedury. Kompetencje Trecom pozwoliły nam w krótkim czasie znaleźć wspólny mianownik w procesach i procedurach obu spółek oraz z powodzeniem wdrożyć je w operacyjne działanie.
>
> **Krzysztof Majcherski**
> Dyrektor Działu XaaS w Atmanie

* według danych PMR Research

Trecom

Wybór Atmana padł na **Trecom,** integratora rynku IT z ponad 25-letnim doświadczeniem, który poza współpracą z ponad 70 dostawcami rozwiązań technologicznych oferuje usługi zarządzania w tym Security Operations Center.

Dlaczego Atman zdecydował się na współpracę z Trecom SOC? Jednym z najważniejszych czynników podczas wyboru partnera do monitoringu bezpieczeństwa jest oferowana dojrzałość procedur, która gwarantuje błyskawiczną i skuteczną reakcję na incydent bezpieczeństwa. **Trecom okazał się dostawca oferującym kompleksowe wdrożenie w krótkim czasie, bazując na doświadczonym zespole projektowym i developerskim.** Bogate referencje potwierdziły słuszność wyboru z perspektywy Atman.

Trecom, jako jeden z nielicznych na Polskim rynku dostawców komercyjnej usługi SOC posiada akredytację Trusted Introducer oraz zgodność z normami ISO 27001, ISO 22301. Akredytacja poświadcza dojrzałość i zgodność usługi z międzynarodowymi standardami. Dodatkową zaletą jest współpraca analityków SOC z ekspertami Trecom specjalizujących w sieciach (m.in. SD-WAN, LAN, WLAN), data center (elementach fizycznych, sieciach ACI, systemach data center czy rozwiązaniach do wirtualizacji), chmurze czy punktowych rozwiązań z zakresu cyberbezpieczeństwa (m.in. firewalle, rozwiązania threat intelligence, content, web czy e-mail security).

Oznacza to, że Atman nie musi szukać kolejnego partnera do wprowadzenia zmian wynikających z raportów przygotowywanych przez zespół SOC.

> Proces wdrożenia usługi Security Operations Center przebiegał w kilku etapach, poprzedzonych dokładną analizą potrzeb klienta. Ze względu na złożoność środowiska IT Atmana, uznaliśmy, że optymalnym rozwiązaniem będzie platforma SecureVisio. Kluczowym elementem weryfikacji gotowości do świadczenia usługi były wizyty referencyjne zarówno w TrecomSOC, jak i u obecnych klientów, które pozwoliły ocenić skuteczność rozwiązania oraz kompetencje zespołu. Dzięki ścisłej współpracy Atmana, SecureVisio i Trecom, **wdrożenie przebiegło sprawnie i zakończyło się sukcesem**, zapewniając klientowi nowoczesne oraz efektywne narzędzie do zarządzania cyberbezpieczeństwem.
>
> **Paweł Sokół**
> Dyrektor Handlowy, Trecom

SecureVisio

Przed rozpoczęciem monitoringu cyberbezpieczeństwa w Atman konieczne było wdrożenie systemu SIEM, który zbiera i integruje logi z różnych systemów, wzbogacając je o kontekst umożliwiający analitykowi SOC podjęcie działania oraz SOAR, który usprawnia reakcję na incydent między innymi, przez zautomatyzowane działania podejmowane na podstawie przygotowanych wcześniej playbooków. Poza standardowym zestawem technologii oferowanych przez vendorów klasy SIEM/SOAR/UEBA SecureVisio zapewnia narzędzia do analizy podatności i ryzyk, bazę CMDB oraz moduł BIA.

Wyzwaniem we wdrożeniu systemu SIEM w Atman była wielkość środowiska jego różnorodność i złożoność systemów IT. Z tego względu zespół Trecom zarekomendował wdrożenie rozwiązania SecureVisio. Secure Visio odpowiadało na wymogi Atman, wśród których zawierały się między innymi: korelacja logów i danych w czasie rzeczywistym, zapewnienie funkcjonalności do analizy zdarzeń, incydentów czy podatności, mapowanie sieci, a także inne kluczowe obszary, takie jak integracje z bazami Cyber Threat Intelligence, zdolność do proaktywnego poszukiwania zagrożeń (Threat Hunting), skuteczna reakcja na zagrożenia oraz rekomendacja środków zaradczych.

> “Przy wdrożeniu w Atmanie kluczowe było zapewnienie spójności i kompletności informacji o środowisku IT oraz ich korelacji w czasie rzeczywistym. SecureVisio pozwala zintegrować dane telemetryczne, analizować ryzyko w kontekście biznesowym i reagować automatycznie, co w przypadku tak dużej i rozproszonej infrastruktury jest podstawą skutecznego cyberbezpieczeństwa. Cieszymy się, że mogliśmy wesprzeć Atmana w podniesieniu poziomu bezpieczeństwa oraz we wdrożeniu skutecznego Security Operations Center (SOC).
>
> **Anna Grzesiakowska-Medygrał**
> Project Manager, SecureVisio

Platforma SecureVisio została wdrożona w modelu Software as a Service, co dla Atman oznacza **optymalizację kosztów i możliwość swobodnego skalowania z rozwojem Atman**.

Dzięki zaawansowanym możliwościom analizy danych oraz automatyzacji reakcji na incydenty Atman może teraz skuteczniej identyfikować i neutralizować zagrożenia w czasie rzeczywistym. SecureVisio zapewnia unikalną widoczność ryzyk, incydentów oraz podatności gwarantując przy tym informacje o kontekście organizacyjnym oraz analizę wpływu na biznes (BIA). Ponadto dzięki integracjom z bazami CTI SecureVisio może stać się centralnym oraz kompletnym źródłem wiedzy o aktualnej ekspozycji na zagrożenia organizacji.