Financial Services

The customer is a 34 year old Financial Services company, managing approximately $7 Billion (as of 31st March 2021) of assets, while providing financial services to more than one million people. Their products and services include mutual funds, equites, insurance, commodities, PMS, and financial planning. The company also pioneered digital products and services, including online trading in 2000 and mobile trading in 2010. By leveraging its multi-channel distribution network and technology backbone, the company has grown considerably over the years.

The Problem and a Failed Solution

While the flexibility, accuracy, and efficiency of the online trading platform has been a game changer for the company, it also introduced the risk of a data breach or malicious cyber attack that could impact users and the brand's reputation. Both external and insider threat actors, could cause data loss or data manipulation. To ensure complete privacy of financial and personal information of its customers, while promoting secure transactions, the company relied heavily on IBM QRadar, a popular SIEM solution based on custom correlation rules created by in-house security expertise. After two years security leaders concluded that the QRadar-based solution fell remarkably short of their expectations. Deployment challenges, operational problems, staffing shortages, poor vendor support resulted in higher than expected Capex and Opex.

Seceon's Cyber Security Solution with aiSIEM

The company selected Seceon's aiSIEM for its ability to ingest a very wide variety of flows, events, identities and logs for threat analysis. Seceon also required minimal operational effort due to automation and advanced analytics (driven by AI and ML).

- Seceon aiSIEM collated events and NetFlow from a wide range of devices - Linux and Windows Servers (Web Services & Back office apps), on-premises Active Directory, Fortinet Firewalls, Radware WAF, and Enterprise Kaspersky EPP. Seceon applied behavioral pattern analytics to create threat indicators from these sources
- They implemented controls for policy violations, such as misuse of software or use of pirated software and they monitored and detected software configuration and postures.

Key Requirements

The company evaluated other enterprise-class SIEM solutions and other necessary point solutions that would address these core requirements and offer comprehensive threat detection:

- Detection and Response coverage for 400+ critical devices
- Aggregate alerts from 3rd party security tools
- Policy violation tracking

Advantage of Seceon aiSIEM over IBM QRadar

Traditional SIEM solutions, like IBM QRadar, are outdated and have many technology and design constraints. Here are some advantages that Seceon aiSIEM brings to threat detection:

- While QRadar requires skilled analysts to initiate remediation, Seceon's aiSIEM generates real-time remediation recommendations through AI/ML threat intelligence enrichment and dynamic threat models, requiring little to no human interaction.
- Being inherently reliant on custom correlation rules, QRadar often struggles to recognize behavioral (user and entity) patterns. Seceon's solution dynamically builds threat profiles on the basis of network traffic patterns and user behavior (baselined) through a continuous learning algorithm, flagging anomalous behavior along the way.

QRadar pricing is based on EPS with the linearly incremental cost for scaling the solution applied through a tier-based EPS license.
This adds unwanted variability to QRadar prices and makes it expensive. Seceon aiSIEM's pricing is based on no. of protected devices, hence quite predictable and all-inclusive.

- QRadar offers a separately priced license extension that enables the use of IBM Security X-Force Threat Intelligence. By default, Seceon's aiSIEM includes Threat Intelligence from 70+ sources at no additional cost.
- QRadar assigns each event type a memory buffer, and once the EPS exceeds the licensed level and the buffer is filled, all new events are queued and processed on a best-effort basis which is not sustainable for longer periods of time. Conversely, an event burst does not affect Seceon's solution and is handled normally with ease

Seceon aiSIEM's low-touch deployment and manageability made it easy for the company to roll out Advanced SIEM across 400+ critical assets within 6-9 months compared to 70 critical assets.

Instant activation of Dynamic Threat Models supported by event correlation and user behavior anomaly detection resulted in rapid alerting for Brute-Force type attacks.

Dedicated product training supplemented by focused Customer Success Engineering ensured value was unlocked from the product continuously to deliver a top-notch customer experience.

About Seceon

Seceon enables organizations to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. The platform delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 7,500 organizations globally are running efficient security programs with automated cyber threat remediation and continuous compliance.

Learn more about Seceon aiXDR and

Schedule a Demo