CASE STUDY

Sector: Financial Services

The customer is a Financial Services company with over 34 years of experience, managing approximately USD 7.08B (as of 31st March, 2021) of assets, while providing effective financial solutions to more than a million people. Products and services range from mutual funds, equity and derivatives to insurance, commodity, PMS and financial planning. Along with traditional offerings, the company built a comprehensive portfolio of digital products and services, pioneering online trading back in 2000 and launched mobile trading platform in 2010. By leveraging its multichannel distribution network and technology backbone, the company has grown considerably over the years.

The Problem and Failed Solution

While the flexibility, accuracy and efficiency of online trading platform has been a game changer for the company, it also came with its risk of data breach and malicious cyber attacks that could impact the business and brand reputation. Any breach could be instrumented by an external or insider agent, thus adding to the unpredictability of data loss and risk factors.

In order to ensure complete privacy of financial and personal information of its customers, while promoting secure transactions, the company relied heavily on IBM QRadar, a well-known SIEM solution that is based on custom correlation rules that are dependant on security skills and trials. After a few years, they realized that the QRadar based solution fell remarkably short of their expectations, marred by deployment challenges, operational problems and lackadaisical support, despite high Capex and Opex.

Key Requirements

Hence, it was crucial for the company to evaluate other enterprise class SIEM solutions that would address the pain and offer comprehensive threat detection:

- Coverage across 400+ critical devices
- Aggregated alerts from 3rd party security tools
- Policy violation tracking

Seceon's Cyber Security Solution with aiSIEM

The company made a determination that Seceon's aiSIEM was both holistic in gathering datapoints for threat analysis and 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 (running Web Services & Backoffice apps), On-prem Active Directory, Fortinet Firewall, Radware WAF and Enterprise Kaspersky Endpoint Protection – applying behavioral pattern analytics to create threat indicators
- Policy Violations, such as misuse of software or use of pirated software, were tracked effectively through a powerful feature called "User Defined Alert"
- System Health of all collectors and event data streaming from different assets, was monitored from single unified UI (Portal)

Advantage of Seceon aiSIEM over IBM QRadar

Traditional SIEM solutions, like IBM QRadar, carry the burden of outdated functionalities, being hindered by technology and design constraints. Here are some advantages that Seceon aiSIEM brings to threat detection:

- While QRadar requires skilled analysts on the customer premise to initiate remediation, Seceon aiSIEM generates remediation recommendations through automated analytics, requiring negligible 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 linearly incremental cost for scaling the solution applied through 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 separately priced license extension that enables 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, event burst does not affect the Seceon's solution and is handled normally with ease.

Visible Difference with Seceon aiSIEM

1. 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
2. Instant activation of Dynamic Threat Models supported by event correlation and user behavior anomaly detection resulted in rapid alerting for Brute-Force type attacks
3. Simplistic User Interface with operational fluidity resulted in easy adoption of Seceon aiSIEM, causing very little disruption while replacing the older SIEM solution
4. Dedicated product training supplemented by focused Customer Success Engineering ensured value was unlocked from the product continuously to deliver top-notch customer experience