OTAVA

OTAVA® Ends Alert Fatigue for Technology Solutions Company

OTAVA® SIEM & SOC provides a comprehensive security solution against cyber threats

About The Client

The technology solutions provider is part of a 150-year legacy company in the communication industry. Based in the Midwest, the company has approximately 150 employees.

Specializing in delivering advanced technology solutions, the company caters to mid-market businesses across various industries with a strong focus in healthcare, finance, and insurance. The company has a customer base that serves around 600 clients in the US and abroad.

Cyber threats are everywhere. It's not a matter of **if** a company will get hit. It's a matter of **when**.

The Challenge

The company provides complex, multi-tenant technology solutions to its customers. These solutions must meet a plethora of compliance requirements, including HIPAA, HITECH, PCI, SOC1-3, ISO 27001, and HITRUST.

The company needed to implement a security solution that would allow them to protect not only their internal assets but also the external assets of their customers.

Due to the large number of assets needing to be managed, the company recognizes the need for an AI component within the solution to provide clear visibility into all internal and external devices to assess behavioral patterns, gather analytical insights, streamline data management, and automate actions as needed.

Given its customer base, the company needed to reduce the time it would take to identify and respond to any kind of threat.

The Solution

The company turned to OTAVA to deploy a SIEM (Security Information and Event Management) and SOC (Security Operations Center) solution that would meet their unique needs. OTAVA was able to customize and deploy a SOC & SIEM solution that would solve the complexity of the customer's multi-tenant environment and address the volume of assets that needed to be protected.

OTAVA® SIEM & SOC provided the customer with 24x7x365 monitoring, detection, and response capabilities to protect the customer's internal and external assets against threats and attacks. The solution provides the customer with real-time alerting and utilizes AI and machine learning to reduce alert fatigue by creating actionable rules and validating security controls.

The deployment included an advanced configuration and fine-tuning of alerts to reduce false positives and create more actionable alerts.

The Results

Implementing OTAVA® SIEM & SOC proved highly effective for the company, offering numerous benefits and resolving several critical challenges.

> “If OTAVA can solve my problems using this solution, they can **solve anyone's problems.**”

> “OTAVA provided us with an **elevated security posture,** not just a security product.”

The company enhanced its overall security posture and improved its **Mean Time to Detection (MTTD)** and Mean **Time to Response (MTTR)** by gaining real-time visibility of all assets and potential threats.

Previously, the company was inundated with a staggering 250,000 alert messages every 15 minutes, resulting in more than **700 million messages** per month. With OTAVA® SIEM & SOC in place, this was drastically **reduced to only 18 events** that demanded attention in a 30-day period. This reduction **eliminated the alert fatigue** the company was experiencing. It alleviated the company's resource burdens by filtering out the noise and allowing them to focus on **crucial security incidents**.

The solution allowed the company to create **Role Based Access Controls (RBAC)** for its users in different departments. This allowed them to set user privileges and permissions based on specific needs, allowing them to see only relevant data.

The new solution also allowed the company to generate **compliance reporting** faster and on time. Previously, these reports were often delayed by several months.

“Our problems are every other customer's problems but amplified times 100 because we have all *their* problems, and *ours*, in one environment,” a company executive said. “If OTAVA can solve my problems using this solution, they can solve anyone's problems.”

Contact OTAVA today to learn more about how we can help your organization reach your objectives with the power of cloud technology.

OTAVA® is a global and recognized leader in delivering secure multi-cloud solutions with a personal touch. Its extensive portfolio is powered by world-class technology partners, backed with expert intelligence, and tailored to help businesses and service providers achieve their individual goals while protecting mission-critical data. With its flexible solutions, fortified security, colocation offerings, and professional services, OTAVA empowers its clients with everything they need to thrive in the cloud and stay focused on what they do best.