CASE STUDY

National Leader in Managed Care and Healthcare Solutions Streamlines SOC Operations with SOAR

An award-winning managed care provider—a company that was one of the first such providers to offer an integrated model—includes affordable health insurance, wellness programs, and community involvement programs. This provider has over 6,000 employees and offers its physical and behavioral healthcare and pharmacy solutions to more than 5.3 million customers.

As a growing healthcare provider serving more than 256,000 employers across 15 states and Washington, D.C., the company values innovation and technology as a means to maintain a robust security posture. This is a critical factor for this organization, given its large customer base, reputation, and the company's expansion in offerings.

Too Many Alerts, Too Many Tools

The daily operations of the security incident response team were very inefficient. They had an internal system of tracking incidents and tasks, but they had outgrown it. The security team works 24×7, and with numerous incidents occurring, they were collecting over half a million alerts daily. This led to alert fatigue, and the team found it difficult to keep up. They were using multiple tools, which hampered the process of collecting data for incident and performance reports. As a result, the security team struggled to deliver the reports to executive management in a timely fashion.

Additionally, during shift changes, managers noticed that some employees were deleting information in the system, and they needed a way to mitigate this issue. Tasks were assigned at midnight each day, and managers required a method of capturing the work that had been completed throughout the week.

As the security team was very technically skilled, they sought a solution that would deliver sophisticated security orchestration, automation, and response (SOAR) functionality, without being overly complicated. FortiSOAR was able to meet all of their requirements.

Details

Customer: Leading managed healthcare provider

Industry: Healthcare

Location: USA

Expert Team Demands Sophisticated Capabilities

Recognizing the need for a security orchestration, automation, and response (SOAR) solution to improve their security operations, the company reviewed offerings from multiple vendors before purchasing FortiSOAR. As the security team was very technically skilled, they sought a solution that would deliver sophisticated SOAR functionality that can easily work with their existing tools. FortiSOAR was able to meet all their requirements and was sufficiently customizable, allowing the technical team to leverage their SOAR platform to its fullest potential.

By integrating all of the security team's tools behind a single workbench, FortiSOAR has helped to streamline the analysts' daily operations. The security team can now easily investigate alerts and track security incidents, eliminating alert fatigue and enabling optimal utilization of security operations center (SOC) resources.

The team uses the built-in FortiSOAR Queue Management capability to allocate incident management work across multiple queues and teams, ensuring that no incident or ticket is overlooked. This feature also assists in meeting compliance requirements. Shift change procedures have improved significantly. Ticket logs are timestamped and labeled with the last analyst's name, ensuring that work is completed in an efficient and effective manner.

The FortiSOAR Role-Based Access Control feature allows management to assign specific permissions to teams and individuals, eliminating data deletion and restricting access to those who require it, further securing enterprise assets. This capability enables the security team to meet mandated data privacy requirements, which they would not have been able to achieve with other platforms.

A Transformative Implementation

FortiSOAR has converted the security team's previously manual processes into trackable uniform automated processes. By customizing their FortiSOAR dashboards to monitor the SOC's key performance indicators (KPIs) and service-level agreements (SLAs), the team can easily produce enterprise-level reports for auditors and security leadership.

Both the security team and executive management are pleased with the results of the FortiSOAR implementation. They are particularly happy with the product's configurable incident management and role-based dashboards. Due to the success that they have had with this implementation and their appreciation for the platform, a member of the security team has taken the time to provide valuable feedback that will further the development of the FortiSOAR solution.

Business Impact

- Ability to competently handle a security event stream that generates more than half a million alerts daily
- Timely enterprise-level reporting to auditors and executive management
- Optimized utilization of security operations center (SOC) resources

Solutions

- FortiGate
- FortiSOAR

The security team and executive management are pleased with the FortiSOAR implementation, particularly the product's configurable incident management and role-based dashboards.

FORTINET

www.fortinet.com

February 11, 2020 9:03 AM

592423-0-0-EN

D:\Fortinet\Case Study\HEALTH Anonymous\cs-FA-national-leader-in-managed-care-and-healthcare-solutions