CASE STUDY

Consumer Financial Pioneer Invests in SOAR That Empowers Security Operations Team

One of the largest providers of private label credit cards in the U.S., this Fortune 500 company offers consumer financing products that include credit, promotional financing, loyalty programs, installment lending, and FDIC insured savings products through its banking services. This organization boasts over 85 years of experience with over 16,000 employees. "With more than $140 billion in sales financed and 80.3 million active accounts, our enterprise brings deep industry expertise, actionable data insights, innovative solutions, and differentiated digital experiences to improve the success of every business we serve and the quality of each life we touch," says a cybersecurity executive with the company.

SOC Overwhelmed and Distracted by False-positive Alerts

Considering the critical nature of the financial services industry, it was important for the company to ensure robust security that encompassed all of its varied digital assets. Given the vast network of digital assets and varied security products used, the security operations center (SOC) team was constantly battling a huge influx of security alerts from security information and event management (SIEM), firewall, endpoint detection and response (EDR) tools, and email gateways. They were unable to keep pace with the alert volume, and increasing the SOC team's staff did not resolve the issue.

Additionally, a massive number of false positives consumed precious analyst time and added to the considerable noise in alert volume. Analysts were also bogged down by manual methods of alert tracking and incident management, which was based primarily on spreadsheets. As the SOC team struggled to provide timely incident and performance reports to top-level management, it became evident that they required a more robust security operations approach.

> *"The timely reports the team generates through FortiSOAR have played a critical role in the company's revenue growth, as executives are now able to track their desired metrics in greater detail."*
>
> *– Cybersecurity Team Executive*

Details

Customer: Consumer Financial Services Leader

Industry: Financial Services

Location: USA

Ease of Use and Maintenance Were Key Decision Factors

Having explored multiple security orchestration, automation, and response (SOAR) solutions, the company decided on FortiSOAR for several reasons. First, FortiSOAR licensing offered unlimited usage to the SOAR features that do not require coding and the ability to perform any number of actions or automations daily, as opposed to some others evaluated that had licensing restrictions on usage. As a financial company, they needed the ability to quickly and easily take the necessary actions to resolve incidents without the worry of being charged more or having a specified number of resources or actions available to them.

Another factor that made FortiSOAR stand out was its ability to create complex workflows that can be easily maintained internally by their in-house security team. The SOC team found that competitors' platforms were unnecessarily difficult to use at a higher level, and much more difficult to maintain internally. As a result, the total cost of ownership (TCO) goes very high.

The team also appreciated the ease with which FortiSOAR enabled them to add new data tables, which could be integrated into the platform and used within the playbooks. These tables are searchable and can be used to generate key metrics.

Finally, the ability to create a new data source, which could contain specific information, was an important feature that they found only in the FortiSOAR solution.

Automation Relieves Operational Complexity

Automation in FortiSOAR has helped reduce the SOC team's alert fatigue. Through customized investigation, triaging, and automation playbooks, the SOC team can filter out the false positives and focus on the real suspected threats, enabling timelier incident response. This has boosted their return on investment (ROI)—and the team's morale—considerably. The analysts can now focus on mitigating actual threats. Built-in approval processes in FortiSOAR ensure adherence to security protocols.

Integration has also reduced operational complexity, as the team was able to ingest data from almost all of their existing security products using FortiSOAR connectors. In this manner, they can run investigations, remediation, and containment processes right from the FortiSOAR console. The reporting framework enables them to track overall progress and build necessary reports with ease.

SOC Team Gains in Productivity and Compliance

After implementing the FortiSOAR solution, the SOC team saw significant increase in productivity, resulting in an anticipated savings of several millions of dollars over the course of the following year.

Now, the SOC team is no longer concerned with the overwhelming alert volume and is able to adequately manage and track all of their work. Managers leverage the built-in FortiSOAR Queue Management capability to handle automatic work assignments across multiple queues and teams, never allowing an incident or ticket to fall through the cracks. Additionally, shift changes in their 24×7 SOC have been significantly streamlined. The fact that ticket logs are timestamped and labeled with the last analyst's name ensures that work is completed in an efficient and effective manner.

Managers have also assigned individual permissions to each member of the SOC team with the FortiSOAR Role-based Access Control feature, so that each analyst has access only to what they require or are assigned to. Access permissions can be modified as needed, further securing company assets and valuable data.

Additionally, the SOC team configured FortiSOAR to follow their specific incidence response framework in monitoring security operations key performance indicators (KPIs) and service-level agreements (SLAs). This made it easier for the team to meet standards and track compliance. With their manual processes converted into uniform automated processes in FortiSOAR, the team can easily produce enterprise-level reports for auditors and security leadership.

Business Impact

- Improved efficiency of security operations by automating alert triage and response
- Decreased time to respond to incidents due to playbook automation
- Cost savings of million dollars due to increased security operations team productivity

Solutions

- FortiGate
- FortiSOAR

Using FortiSOAR connectors to ingest data from almost all of their existing security products, the SOC team runs investigations, remediation, and containment processes right from the FortiSOAR Workbench.

After implementing the FortiSOAR solution, the SOC team saw a significant increase in productivity, resulting in an anticipated savings of several millions of dollars over the course of the following year.

After using FortiSOAR for only a few months, the team was so pleased with the product that they started managing all their physical security incidents (including theft, unauthorized door entry, etc.) through the FortiSOAR platform. The cybersecurity executive was impressed as well, noting that the timely reports the team generates through FortiSOAR have played a critical role in the company's revenue growth, as executives are now able to track their desired metrics in greater detail.

FERTINET

www.fortinet.com

February 8, 2020 12:44 AM