CASE STUDY

Business Soars When MSSP Leverages FortiSOAR for Threat-alert Case Management

Five and a half years ago, Secure Cyber Defense started up with the sole purpose of ratcheting down customers' cybersecurity practices. The managed security service provider (MSSP) located outside of Dayton, Ohio, provides Fortinet solutions as a service to industry sectors such as government, manufacturing, finance, education, and healthcare. Its flagship offerings include a managed firewall using FortiGate next-generation firewall (NGFW) appliances and virtual machines (VMs), as well as managed FortiMail email security systems. Those products proved to be highly effective and easy to manage, yielding a valuable and profitable set of managed security services.

However, as the cyber threat landscape continued to evolve with more sophisticated attacks, customers came back to Secure Cyber Defense asking for more expert security monitoring services. To meet this demand, Secure Cyber Defense turned to the Fortinet FortiSIEM security information and event management (SIEM) system—and more recently to the FortiEDR advanced endpoint detection and response (EDR) solution—to deliver higher-value security operations center (SOC) services, all the way through to incident response. "FortiSIEM is the foundation of our managed services," says Shawn Waldman, CEO of Secure Cyber Defense. "And FortiEDR, which feeds into FortiSIEM, provides essential threat detection and validation in real time."

This business model has turned out to be an especially good fit for Secure Cyber Defense's small to midsize client base in 2020. "The automation capabilities of FortiSIEM and FortiSOAR have allowed us to maximize the efforts of our team and to better serve our growing client base," says Waldman. "Automation is helping us grow, and we are hiring people to keep up with the demand."

Staffing Challenges and Alert Fatigue Challenged Business Growth

Like many cybersecurity companies, Secure Cyber Defense was having difficulty finding enough qualified security staff to evaluate and respond to the overwhelming number of alerts generated across all its client networks. "Anywhere from 150 to 300 alerts would come in each day," Waldman says. "They would automatically create tickets in our ticketing system, and the team would have to investigate each and every one of those by the end of the day. The next day, it would start all over again. Our staff was suffering from alert fatigue, which was the same challenge for our larger enterprise clients."

With an overwhelming number of alerts pouring in, some low-level alerts were getting passed over during the busiest days. "MSSPs cannot humanly process all the alerts coming from all the systems they are monitoring, without the aid of automation," Waldman says. "Our team excels when we triage alerts. So, they had the ability to see attacks in progress, for example, but there was some risk that they might not spot the reconnaissance phase of an attack right away. The

SECURECYBER DEFENSE

"Having such robust automation in our case management system, facilitated by our FortiSOAR playbooks, makes us comfortable our analysts are investigating everything that truly needs a human look—our team is no longer waking up in the middle of the night unless it is absolutely necessary."

– Shawn Waldman, CEO,
Secure Cyber Defense

Details

Customer: Secure Cyber Defense

Industry: MSSP/Service Provider

Location: Miamisburg, Ohio

Business Impact

- Enabled seven-figure revenue stream with new, value-add SOC services
- Rapid time to market with complete multi-tenancy solution for managed detection and response
- Accelerated response to perceived threats (from 45 minutes to 2 minutes in some cases)
- Improved efficiency by automating low-level alert response, freeing up team to pursue more strategic work

fact that we were already dealing with alert fatigue compounded the issue." To streamline detection and response processes and free up staff time for more critical activities, the company began developing a custom security orchestration, automation, and response (SOAR) solution based on the FortiAnalyzer platform. A SOAR system is an automated framework that pulls all the tools used by the SOC together into a unified case management system.

Plans changed when Secure Cyber Defense discovered that Fortinet had begun offering the FortiSOAR solution. "We decided it did not make sense to build an internal solution, even one based on the powerful FortiAnalyzer platform, when we could just buy the same capabilities in FortiSOAR," Waldman says.

Automated Case Management Improves Threat Response Efficiency

Secure Cyber Defense launched a FortiSOAR proof-of-concept (POC). "Our analysts dropped everything to do this POC for three months," Waldman says. "It went so well that at the end of three months, we started using the FortiSOAR case management functionality and turned off our ticketing system on the same day. Now, three months later, we are using FortiSOAR for 100 percent of our threat detection and response case management."

Out-of-the-box connectors enable FortiSOAR to receive alerts from more than 350 non-Fortinet security products, so all of a company's security events can be investigated and processed within the centralized case management solution. Because Secure Cyber Defense is a Fortinet-focused MSSP, its FortiSOAR deployment pulls in alerts from clients' FortiGate NGFWs, FortiEDR solution, FortiWeb web application firewall (WAF) and FortiMail installations, and the Secure Cyber Defense FortiSIEM system.

All these inflowing events become cases in FortiSOAR. The solution automatically triages alerts, prioritizing them based on content and correlating them with other alerts that represent similar threats in different areas of the network or across multiple clients.

In addition to leveraging threat intelligence from FortiGuard Labs, Secure Cyber Defense has an internally developed system that consolidates data from a wide range of external sources. Secure Cyber Defense integrated FortiSOAR with FortiGuard Labs and built a custom connector to its internal intelligence database. If a threat detected in one client environment matches certain criteria in the intel databases, FortiSOAR can send out a companywide block command within minutes, so that FortiGate NGFWs at any Secure Cyber Defense client site deny entry to traffic from a specific IP address, country, or other characteristic identified as problematic.

Secure Cyber Defense has long taken advantage of the multitenancy capabilities within its FortiGate and Fortinet security-management solutions. "Obviously, we do not want to stand up a separate device on the back end for every client if we do not need to," Waldman says. "FortiAnalyzer, FortiManager, FortiSIEM, FortiEDR, and FortiSOAR enable us to give each customer their own virtual domain that is segmented from other customers." Waldman's team has used FortiSOAR to build on this capability to create proprietary custom dashboards through which clients can view security information about their own environment.

In addition, FortiSOAR uses application programming interfaces (APIs)—some of which came with the solution, while others were custom built by Secure Cyber Defense—to query external sources for information used by the automated

Solutions

- FortiSOAR
- FortiSIEM
- FortiGate
- FortiMail
- FortiEDR
- FortiWeb
- FortiManager
- FortiAnalyzer

"I have used all of Fortinet's competitors over the course of my career, and Fortinet security is just the best. Now, FortiSOAR has advanced our threat detection and response capabilities by five years. It gives us this tremendous Swiss Army knife of functionality that we are excited to capitalize on."

– Shawn Waldman, CEO,
Secure Cyber Defense

prioritization and response workflows. Waldman explains how FortiSOAR responds when a FortiGate NGFW goes down: “We have a playbook for that,” he says. “First, FortiSOAR takes the latitude and longitude of the FortiGate. We have an API to a national power grid database, which FortiSOAR will query to determine whether the firewall fell victim to a power outage. If not, the next thing it does is query our National Weather Service [NWS] API to check the current conditions of the weather station closest to the FortiGate.” FortiSOAR will receive data on temperature, sky conditions, and wind speed, as well as NWS severe weather warnings. If those data points indicate a storm in the area, FortiSOAR will determine that the alert is likely weather-related.

“For a firewall outage caused by a broader power outage, we will not wake up the analyst on call,” Waldman says. “The customer will receive an automated email letting them know that the problem is weather-related and that the analysts will contact them the next business day. We have always been up-front with our customers that our facilities are not manned 24×7×365. Having such robust automation in our case management system, facilitated by our FortiSOAR playbooks, makes us more comfortable that our analysts are investigating everything that truly needs a human look—our team is not waking up in the middle of the night unless it is absolutely necessary.”

Automation Makes FortiSOAR a Security “Force Multiplier”

Secure Cyber Defense has had FortiSOAR in production for about three months. Not surprisingly, staff reaction was immediately positive. “The outcome is going to be much bigger than I imagined,” Waldman reports. “Our team are in it all day, everyday—they are so excited to have this here. Its capabilities are far beyond what we realized when we first installed it.” He cites the fact that FortiSOAR can integrate with Microsoft Active Directory (AD). “If we come to the conclusion that someone’s account has been compromised, we can reach right into AD from FortiSOAR and lock the account, or we can reset the password.”

When a threat arises, Secure Cyber Defense staff can now respond more quickly, both because FortiSOAR reviews, sorts, and prioritizes alerts faster than a human can, and because Secure Cyber Defense analysts and engineers now have more time to dedicate to the tasks that require manual intervention. “For instance,” Waldman says, “the average ticket for a phishing scheme might have taken 45 minutes to resolve with our legacy process. With FortiSOAR, it takes two minutes—or less.”

Accelerated threat response improves overall security and it enables staff to more efficiently address alerts that receive lower-level priority, enhancing long-term threat protection. Moreover, FortiSOAR case management automation has helped Secure Cyber Defense overcome the skills gap that is the bane of many MSSPs that might have impeded the company’s ability to grow if it were heavily reliant on manual workflows. “It is hard to find senior-level talent right now,” Waldman says. “FortiSOAR is a force multiplier that makes our small staff more effective. It eliminates the alert fatigue that was plaguing our team enabling them to focus only on the problems that actually require human intervention.”

> *“FortiSIEM is the foundation of our managed services. And FortiEDR, which feeds into FortiSIEM, provides essential threat detection and validation in real time.”*
>
> – Shawn Waldman, CEO, Secure Cyber Defense

New Line of Business With Seven-Figure Revenue Stream

Perhaps most important, FortiSOAR, in combination with FortiSIEM and FortiEDR, has enabled Secure Cyber Defense to pursue new business opportunities that would not have been possible if the firm were still more reliant on manual investigations. “Historically, we have found that large enterprises are typically not interested in using an MSSP,” Waldman says. “They have internal staff who want to manage most aspects of their security solutions. However, FortiSOAR gives us the ability to co-manage the firewall with an internal security team. We provide a managed detection and response [MDR] service, processing and responding to security events, while the client continues to manage the FortiGate firewall on a day-to-day basis.”

Another option for large customers is to engage Secure Cyber Defense as a FortiSOAR consultant. “Providing professional services around FortiSOAR is already generating more consulting revenue than we have had in the past,” Waldman says. “We are installing the SOAR, writing playbooks and APIs, and integrating the solution with our proprietary intelligence databases. All told, FortiSOAR has created a new, seven-figure revenue stream for our firm.”

Since its inception, Secure Cyber Defense has focused exclusively on Fortinet security solutions. Waldman believes strongly in the Fortinet product line, and FortiSOAR further bolsters his confidence. “I have almost 30 years in IT,” he says. “I have used all of Fortinet’s competitors over the course of my career, and Fortinet security is just the best. Now, I feel like FortiSOAR has advanced our threat detection and response capabilities by five years. It gives us this tremendous Swiss Army knife of functionality that we are excited to capitalize on.”

FORTINET®

www.fortinet.com

February 19, 2021 1:53 AM

D:\Fortinet\2021 Rebranded templates\Case Studies\February\Secure Cyber\cs-business-soars-when-mssp-leverages-fortisoar-2192021\cs-business-soars-when-mssp-leverages-fortisoar-2192021

828037-0-0-EN