CUSTOMERONE

Symantec

Extending Our Security Operations with Symantec Managed Security Services

On Aug. 22, 2014, at 3 a.m. Eastern time, Symantec Managed Security Services (MSS) detected suspicious activity on the Symantec production network: A computer was connecting to a known command and control server (one associated with malware). The MSS team created a critical alert–the second-highest alert category–and submitted it to Symantec's internal Security Operations Center (SOC) in Herndon, Virginia.

In security operations centers (SOCs) like this one run by Symantec Managed Security Services (MSS), cybersecurity experts provide threat monitoring and customized guidance to clients around the clock.

Jacob Horst, manager of the SOC, saw the alert and launched an investigation. The more he learned, the more his concern grew. The alert came out of Singapore, the hostname for the offending computer (a virtual machine) didn't conform to Symantec standards, and the traffic it generated was associated with an advanced persistent threat. Further correlation and analysis found that the offending virtual machine was infected with commodity malware, appeared to reside on an authorized Symantec computer, and was scanning the network for ways to spread. "We were looking at a machine being utilized as a bot," Jacob recalls. "It was trying to propagate itself, probably for a potential attack down the road."

Perhaps Jacob's most chilling realization was this: The SOC he manages–a brand-new facility with cutting-edge technology–hadn't detected the problem.

Jacob quickly shut down the attack. Postmortem analysis found that a Symantec researcher had created an unauthorized Red Lab–that is, a testing environment that should be completely segregated from the production network–and was using it to experiment with known malware. Our SOC is now on the alert for this type of serious policy violation.

For Jacob, this incident is important for two reasons. First, it demonstrates the importance of having MSS help monitor Symantec's systems 24x7. Secondly, it shows the value of what he calls the "refined architecture and analysis" that MSS employs to protect its customers. "We're the young upstarts, doing all the risky, crazy things with the newest technologies," Jacob says of Symantec's internal SOC. "But MSS detected this problem, and we learned from each other. It's a very symbiotic relationship we have."

Symantec IT operates its own sophisticated Security Operations Center (SOC), and we bolster our defenses by using Symantec's Managed Security Services (MSS). This paper, **Extending Our Security Operations with Symantec Managed Security Services**, gives CIOs, CTOs, CISOs, and other senior managers a transparent look into how we use MSS today. We describe how our relationship with MSS evolved as we launched our own SOC, and how we work and communicate with our MSS colleagues to derive the greatest value from the service. We believe our experiences are relevant to our customers regardless of their information security operations.

You may be surprised to learn that Symantec subscribes to MSS at all, since we operate a sophisticated internal SOC. The fact is, only a few years ago we relied on MSS as our sole source of security monitoring, and our SOC is relatively new—it ramped up in early 2014.

Based on the Red Lab event (and others), we now recognize that the MSS SOC can provide a valued extension of our own capabilities. We've also learned to use its resources more effectively as we increase our internal security capabilities. Tim Fitzgerald, Symantec's chief security officer, characterizes it this way: "We went from consuming the service to deriving serious value from it within the context of our own SOC. Prior to that we treated MSS as a commodity service. That was a big mistake on our part."

This paper explains how and why Symantec IT evolved from using only MSS for security monitoring, to using it in conjunction with an internal SOC. We also explain how you can get the greatest value from an outsourced security management service, regardless of how advanced your own security operations are.

Because the paper references two separate security operations centers, we'll use "internal SOC" when we're talking about the facility Symantec IT operates to protect our own environment, and "MSS SOC" to denote the center that Symantec MSS uses to serve external customers.

Setting a Higher Bar

Before Symantec had its internal SOC, we worked with MSS using a simple, compartmentalized workflow:

- A variety of logs (from endpoint protection, intrusion detection, and other systems) were bundled and sent automatically to the MSS SOC.
- MSS applied its extensive technology and expertise to analyze the logs.
- When MSS detected a potential security issue, it emailed information about the issue to an Incident Response Team (IRT) within Symantec IT.
- The IRT created a ticket for the incident and analyzed the issue to determine its validity and severity. Problems the IRT couldn't remediate on its own were handed off to specialists.

Simplicity was both the blessing and the curse of this workflow. "Companies that aren't in the business of security love this arrangement," Jacob says. "They need security, but they don't want to build a SOC. But for us, as a security company, we needed more."

Our IRT wanted details about the threats and more control over how threats were presented, organized, prioritized, and resolved. To improve its processes, the team also wanted to analyze its response in greater detail than the old workflow allowed.

"Essentially, all the metrics we had [under the old system] were based on when we received the alert from MSS and when we closed it," but not on the important steps in between, Jacob explains. "Also, we relied on one internal team for identification, escalation, and investigation. The IRT had to say if a ticket was legit, whether it should be escalated, and how we fixed the problem." This sometimes slowed our response. We needed and wanted to set a higher bar for ourselves.

Finding Our Focus

Part of the challenge lay in the fact that, as a vendor to Symantec, the MSS SOC didn't have complete visibility into the context of issues, Tim says. "They could always tell us when something looked bad, and why it looked bad, but they couldn't always tell us what it meant in the context of my environment, or what the risk might be based on the value of the affected asset. That was something that needed to get corrected."

Symantec opened its internal SOC in early 2014, leveraging the advice of our colleagues in the MSS SOC. (In fact, Symantec's internal SOC resides in the same Herndon, Virginia building as one MSS SOC; others are in India, Japan, Singapore, and the UK, and more are slated.)

We had several reasons to continue using MSS as we ramped up our internal SOC. First and foremost, it allowed our internal team to focus its efforts on higher-order detection and analysis. This also made sense because, frankly, the MSS analysts are much better at the Tier 1 analysis than our internal team.

According to SOC designer Frank Riccardelli, senior manager in the Symantec Global Security Office, using MSS "allows for a leaner number of analysts." More important, the pre-vetting of alerts and incidents by MSS lets our internal team work smarter. "That means we can focus, and look at things that are more specific to us, rather than generic in nature," he says. "And that means we can move them through to incident response quicker."

Initially, our internal SOC focused its efforts on two things: source code protection and payment card industry (PCI) regulations. "Source code makes Symantec who we are, and PCI allows us to sell our products and be profitable," Jacob explains. "So we built our first use cases around them." (For more about how we protect our source code, see the CustomerONE story, "Source Code Security the Symantec Way.")

The lesson for you, whether you run information security programs in-house or leverage an outside service, is this: Identify the security issues that are truly important to your business and align your security efforts to address them first.

Not sure where to start? "Embracing GRC [governance, risk, and compliance] is always the key to success," Frank says. "If you have solutions that are under compliance—like HIPAA, SOX, and PCI—the focus would be on those products and the security solutions that layer on top of them."

Extending Our Team

Our internal SOC has since matured and expanded its view to encompass 174 separate use cases. Each use case is a collection of logic that results in an alert; a single use case could be as simple as the presence of a virus on a known endpoint, or as complicated as the unauthorized Red Lab scenario. "As we build out our own use cases, we try to avoid things that MSS does better than we do, so we don't duplicate effort," explains Javier Santoyo, Symantec's senior director of security intelligence.

Avoiding duplication enables us to continue to leverage MSS like an extension of our own internal SOC team. "They're very mature in their operations," Javier says of MSS. "Their ability to ingest data and correlate with threats they see across their other customers gives them a unique perspective."

> **"Their ability to ingest data and correlate with threats they see across their other customers gives [MSS] a unique perspective."**
>
> — Javier Santoyo, Senior Director, Security Intelligence

Jacob likes working with MSS for two main reasons.

- **To strengthen our 24x7 coverage:** Like many of you, we find that SOC analysts can be expensive and difficult to come by. MSS provides high-quality eyes on our environment around the clock.
- **To provide feedback:** Our internal SOC communicates candidly with the MSS teams that run the service and develop new capabilities. "We provide them with the kind of direct feedback that they don't typically get from other customers," Jacob says.

The feedback we provide to MSS falls into three broad categories:

1. **Ongoing communication about the service.** Every week the staff of our internal SOC and IRT meets with MSS services delivery manager Prajakta Kulkarni and technical services coordinator Kenny Piontek to discuss the service. "We talk through any issues they're seeing, and any recommendations on how we can tune the incident escalation on our side," she explains. Prajakta also meets quarterly with Javier to discuss performance metrics and ongoing collaborative projects. "We review categories of critical incidents and engineering efforts," she says, "and if there were false positives, we ask for feedback—what do we need to change on our side so we don't alert on false positives?"

   Our communication is greatly enhanced by the fact that MSS aligns its teams by customer, rather than using a "next available agent" queue for incidents. This customer-centered alignment using dedicated teams enables MSS analysts to understand the specifics of our environment, and use that information when analyzing potential threats. It also deepens the professional relationship between the teams, leading to even better communication and understanding of needs and priorities.

2. **Specific feedback on new services and upgrades.** MSS teams leverage their colleagues in Symantec's internal SOC for technical feedback when onboarding new devices and log types. We're currently starting to test the next version of the Log Collection Platform (LCP), the proprietary MSS solution that collects, parses, compresses, encrypts, and forwards log files for analysis. The new version includes support for Amazon Web Services, automated device onboarding, and high availability features. We're also helping test LCP installation and upgrade scenarios. "We're going to point tens of thousands of logs per second at the new LCP," Frank says, "to ensure its stability, reliability, and performance. Live production data is the best test, since labs don't equate to what happens in reality."

3. **Providing technical resources.** Not long ago, MSS developed an API to enable incidents to automatically enter customers' security workflow without relying on email, an MSS portal, or manual intervention. The first API version experienced latency problems, occasional trouble parsing feeds, and unexpected halts. Jacob partnered with the MSS team to improve and test the API.

What Our Experience Means for You

You may wonder why we're explaining our working relationship with MSS in such detail. Admittedly, the typical company is not going to be as deeply embedded with its managed security service provider as we are with ours. But there are lessons to learn, and benefits to gain, from our experience.

The first lesson—perhaps the most obvious one—is that candid communication helps to improve service. "You have to be overt about what's important to you," Jacob says. "You can't just say, 'All of my logs are important.' You have to say, 'My PCI is important,' or, 'This subnet is important.'"

Javier adds that the job of identifying what's important falls to the customer—not to MSS—and is just good business. "It's on us, as customers, to do that," he says. "Because MSS is something we're paying for, we absolutely want to get the most out of it. I put that responsibility on me and the team." (Yes, Symantec's internal SOC pays for MSS, just as Symantec's external customers do, and holds MSS to specific service levels and obligations just like any other paying customer.)

The second lesson is related to the first: Being a pushy customer—but smart about it—can be good for both you and your service provider. "Symantec is a very difficult customer for MSS," says John Lionato, vice president of Information Security Service Operations responsible for MSS. "Symantec is demanding, it is knowledgeable, and it has high expectations. But it is that difficulty that drives us to new ideas, new perspectives, and a continual review of what we do and how we operate."

And by being demanding yet collaborative MSS subscribers, we think our internal SOC helps MSS provide better service to everyone. We know the regular back-and-forth helps our internal SOC teams do their jobs better. If you'd like to learn more about Symantec's Managed Security Services, contact your Symantec representative.

Same Feeds, More Actionable Results

It's important to note that the logs and feeds that we send to MSS for analysis today are the same ones we sent to MSS before we built our internal SOC. The difference is that, by using MSS as an extension of our internal SOC, and by communicating regularly with the MSS team, we are getting better, more actionable results from the same information. The percentage of false positives has decreased significantly over time, and early problems with miscategorized alerts have been eliminated.

In addition to addressing some specific issues we have raised with its service, MSS is expanding its analytics and integration. New technologies are regularly added to the service, including advanced URL analytics, stream query–based analytics, machine-learned log processing, and machine-learned event clustering (known as Smoke Detector, because it enables MSS to detect and extinguish security "fires" when no flames are visible). MSS now receives feeds from Symantec Advanced Threat Protection, and our internal SOC helped MSS fine-tune its service offering for ATP. (To learn more, see the CustomerONE story, "Symantec Advanced Threat Protection: What We Learned as the First and Best Customer of Symantec ATP.")

Those changes and more demonstrate how our relationship with MSS will continue to evolve and how we'll derive even more value from the service. "It's not a set-and-forget type of service," Javier says of MSS. "It's something that needs to be nurtured. The more MSS knows about your environment, your goals, and your priorities, the better they can tailor that service to you."

> **"The more MSS knows about your environment, your goals, and your priorities, the better they can tailor that service to you."**
>
> – Javier Santoyo, Senior Director, Security Intelligence

Learn More from the Managed Security Services Team

This brief is intended to give you a broad look at how we use Symantec Managed Security Services. Your Symantec representative can help you adapt our blueprint to protect your own confidential information.

Contact Symantec today.

SYMANTEC SOLUTIONS AND PRODUCTS IN THIS PAPER

Managed Security Services: MSS provides 24x7 advanced threat monitoring by Symantec security experts who analyze and correlate with the global threat landscape, so you can detect, assess, and respond to threats faster.

customer_one@symantec.com

CustomerONE Team
350 Ellis Street
Mountain View, CA 94043
800-745-6054

Symantec's CustomerONE team can facilitate discussions between you and our IT security practitioners to help you address your security questions and concerns. Please contact us directly or through your Symantec sales team.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.