Security Analytics Case Study Series - Government Contractor

Major Government Defense Contractor Speeds Incident Response with Symantec

Organization

Government Defense Contractor

Challenges

- Lack of visibility into what was happening on their network
- Inability to quickly resolve security incidents – typically took three to four people more than 30 hours

Solution

Symantec Security Analytics

Benefits

- Visibility – finally understand exactly what is going on to get the answers they need to the tough questions around an incident
- Accelerated Incident Resolution – reduced time to resolve an incident by 75%
- Enhanced Security – have the ability to adjust policies, improve security education and fortify the network in other ways to better protect the business

When the Senior Cyber Defense Engineer for a major government defense contractor found himself continually telling management he couldn't prevent or even explain the barrage of security incidents they were experiencing, he set out to find a solution. What he found was the network forensics capabilities of Symantec Security Analytics, which finally provided the answers he was looking for to the tough questions, such as "How did this happen?", "Who did this to us?", "What systems were impacted?", "Is it over?", and "Are we prepared if this happens again?"

The Challenge: Getting the visibility they needed to quickly resolve security incidents

Despite having "best-of-breed" security tools that claimed to provide complete network defenses, they had no visibility into what was actually crossing the network. For example, their last line of defense – the endpoint firewall – was not only unable to prevent zero-day threats, but couldn't even show them what had been compromised. They needed a comprehensive solution that could make sense of the "unknowns" and give them concrete answers to the questions they had around their security incidents.

The time-to-resolution for an individual security incident was frequently over 30 hours, with three to four people each spending 4-8 hours on the investigation. Not only was this threat window unacceptable from a security perspective, giving an attacker ample time to complete their objectives, but also from a financial perspective, costing them the time and resources required to recover from the breach. Management was calling for a dramatic cut in this resource drain, as well as in time-to-resolution for each incident.

Solution: Symantec Security Analytics

The Incident Response Team put the Symantec Security Analytics appliance to the test, and the results were immediately clear. "With one click, I instantly had my answers and was able to quickly complete investigations," the Senior Cyber Defense Engineer reported. With Symantec, the team could quickly search on an infected machine's IP address, narrow the time slice and then drill down into the payload to see exactly what was going on and get the answers they needed.

Symantec

The open integration capabilities of the Security Analytics Appliance further enhanced their overall security infrastructure, providing tight coupling with their IPS solution from Sourcefire and firewall from Dell SonicWALL. The integration enabled them to follow the path of a zero-day threat from start to finish, finally providing the answers upper management wanted, lowering costs and simplifying the investigation and remediation of an attack.

Benefits: Visibility and answers

In one instance, a zero-day attack had entered the company's network through a poisoned Google image search. Using Security Analytics, the defense engineer determined exactly what the image search was, which link was clicked on, which specific image contained the embedded redirect, and the HTML landing page for the redirect. Having these critical pieces of information enabled the defense engineer to quickly identify and take care of devices that had been infected and prevent future access to the infected site to strengthen the entire network's defenses.

"It got in because it was a zero-day attack, but I was able to pinpoint it, once I found the sites that were injecting the malware, and put rules in place so, if people were redirected to the same exact site, we would block it." By doing so, the defense engineer was able to show management exactly what was going on, what users were accessing and, upon review, determine whether this was an internal threat, a breach of an acceptable use policy or simply a misdirected, legitimate image search.

Before Symantec, these simple answers were unavailable. The defense engineer confirms that, "Being able to send reports up the chain that clearly explain where the problem came in, and what we've done to fix it is a thousand times better than the shrugging of the shoulders saying, 'I don't know how it got in!'"

This newfound visibility quickly helped justify the decision to implement the Symantec solution. One of the challenges of deploying any security tool, is management generally focuses on the cost, but the data they now had at their fingertips made the benefits of Symantec Security Analytics clear. The defense engineer confirmed, "In today's world, you have to know."

Results: Accelerated incident resolution

With the Symantec Security Analytics Appliance, the government contractor has reduced their incident resolution time by 75%, down from 30 man hours to less than eight. And, instead of waiting for days, the team can now answer critical questions in less than four hours.

"It's a huge asset, not only from a security perspective," said the Senior Cyber Defense Engineer, "but it also gives me the visibility into how the users are using my network. It gives me the data I need to adjust policy, improve security education or fortify the network in other ways. We get insights that sometimes hit very close to home: like 'this is how close we came to a user sending themselves source code, HR data or bringing down the entire security infrastructure of our company'."

"With Symantec, I can rest assured that regardless of the virility of APT's, zero-day infections, unknown malware or internal threats – we are prepared to face the unknown, knowing the solution is providing always-on, full visibility behind the scenes. Symantec helps me figure out exactly how the breach happened, so I can do my job and protect everyone else."

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

SYMC_cs_SAP_Government_Contractor_EN_v2a