InfoWorld

February 25, 2016

GET TECHNOLOGY RIGHT®

INSIDER

Exclusive: Go inside a security operations center

A tour of managed security services provider Alert Logic reveals how proactive monitoring detects breaches and accelerates incident response

Credit: Thinkstock

Walk into a security operations center (SOC) and the first impression you get is of an immense war room, with large screens across the entire front wall displaying a world map and endless rows of tabular data.

Analysts sit in rows facing the screens as they scrutinize streams of data on their own monitors. Most of the light comes from the wall screens, creating a cavelike atmosphere. The overall feel is one of quiet efficiency.

Welcome to Alert Logic's 24/7 security operations center in Houston, Texas. This is where Alert Logic's analysts monitor customer applications and networks, hunting for signs of an attack or a breach. For organizations with limited budgets and a small (or not) dedicated security team, working with a managed security services provider like Alert Logic helps close the security gap.

"They [customers] are thinking, 'We have too much valuable data not to have better security capabilities," says Gray Hall, CEO of Alert Logic. It's a shift from investing in specific technologies and hoping it's enough to prevent a breach to a proactive approach where the goal is to find attackers before they cause much damage.

That's not to say traditional point solutions such as antivirus on the endpoint, firewall, and IPS/IDS have lost their usefulness. But hunt teams — SOC personnel who look for signs of an infection or a breach — help organizations identify attackers who've broken past traditional security measures. At their best, SOCs offer a consummate combination of vigilance, expertise, and advanced security tech.

Security central

To protect customers' IT infrastructure, SOCs needs to correlate data from different sources into a centralized platform — along with experts who know how to respond to security events.

Gray Hall, CEO of Alert Logic

Analysts look for network anomalies as part of the monitoring service, such as a file transfer from an internal system to an IP address in a country where the customer nor-

mally doesn't do business. In one real situation for a customer, Alert Logic analysts discovered a machine — a printer, actually — communicating with a Russian IP address. As soon as the analysts alerted the customer, the connection was shut down.

"That [printer incident] was one of the cooler ones we've seen," says Jason Payne, senior director of ActiveWatch Services at Alert Logic. At Alert Logic, analysts rely on a platform that collects security events from applications, event data, logs, and appliances in customer data centers. The service also extends to public cloud workloads, such as workloads running on AWS. If the customer has deployed a Web application firewall, analysts pull the Web transaction data, too.

The analytics platform correlates the information along with other sources, bubbles up what it identifies as an indicator of compromise, and puts it in front of the analyst for further investigation. The alert appears on the big screen in the front of the room, along with various pieces of customer information. Analysts have 15 minutes to analyze the issue, validate whether or not the attack was successful, understand the impact, and escalate to the customer.

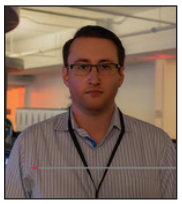
"It [the screen] will have a countdown and will change colors as it gets closer to 15 minutes," Payne says.

Genomic informatics company GenomeNext relies on Alert Logic to monitor both its development and production environments on Amazon Web Services and is notified immediately whenever an unexpected event occurs. When instances go offline, GenomeNext receives alerts within 15 minutes saying the appliance is down and should be checked. In another recent case, one of the developers wrote test code — it was never going to be released into production — where passwords were sent in clear text. The SOC team caught it, validated the alert, assessed the potential damage, and sent an email describing the issue and how to fix it.

"That was within 30 minutes of us writing the code," says James Hirmas, co-founder and CEO of GenomeNext. "It was a very short turnaround."

Alert Logic's security operations center in Houston, Texas

Working with customers


Jason Payne, senior director of ActiveWatch Services at Alert Logic

SOCs are large, complex operations. To mount effective defenses, SOC personnel must understand each customer's business and why certain decisions were made, so they can prioritize alerts and make appropriate recommendations. Alert Logic asks customers which information is most valuable, so the team knows what to focus on. It's a group effort.

"If a customer calls in and they just need help with something, we do our best to help," Payne says. "We make sure that our analysts understand we don't log into anything [customer systems]. That's where the line is."

Alert Logic does not provide incident response capabilities. Instead, along with alerts, it delivers complete records to customers: where the incident occurred, the actual payload executed, and the responses from the system. The customer can see all the data the analysts saw and why it was flagged, as well as remediation advice. In the case of an SQL injection attack, for example, the analyst would include the actual attack string and the resulting output. If the analyst suspected someone was trying to brute-force a password, the incident record would show the IP addresses associated with failed login attempts.

"We are not just saying, 'Hey, this happened,' to the customer. We tell a story, 'Hey, this is what we initially see. This is where we'd go and investigate an event. This is what's in the payload, and this is what that indicates.' We work collaboratively to make sure the customer understands what happened and why we flagged the incident," Payne says.

The analyst is responsible for making sure the right person on the customer team is notified, gets a complete rundown of what happened, and receives concrete recommendations. If malware was exfiltrating data, the analyst may recommend blocking the IP address at the firewall or closing down a remote desktop port, for example.

The customers handle cleanup and remediation based on the information the SOC analyst has collected and provided, while Alert Logic's SOC continues monitoring to make sure the repairs are sufficient and effective. "We could have specific people coordinating with them [the customer] and watching from that [compromised] host and say, 'OK, I saw it stop.' Communication goes both ways," Payne says.

More than monitoring

Most managed security providers, including Alert Logic, have an active intelligence team researching the latest threats and analyzing actual attacks. Indicators of compromise and other threat intelligence are fed back into the analytics platform that the SOC uses as part of its monitoring. The intelligence team can ask SOC analysts to keep an eye out for specific types of threats.

The relationship also goes the other way, as the analysts load up events, logs, and netflow data to look for indicators warranting further investigation. On average, the SOC team generates five to 15 of these manual incidents, which are then sent to the intelligence team, Payne says. The intelligence team creates signatures and adds it to the analytics platforms so that similar incidents are flagged automatically for other customers.


Misha Govshteyn, chief security officer and co-founder of Alert Logic

It's an "ongoing cycle" of manual analysis, identifying threats across different customer environments and applying the information back to the detection platform, says Misha Govshteyn, chief security officer and co-founder of Alert Logic. "A small customer gets the benefit of having a SOC that has visibility on thousands of networks."

If the incident turns out to be more complex or the customer comes back needing more information, Alert Logic can escalate the incident to other specialists on the team. If the crisis at hand is a Web application attack, an analyst really good at digging into code and understanding how to remediate attacks may be tapped to assist. Or if there are anomalies in the logs, a specialist who excels at understanding system logs can help set security policies to get the right data to better understand what is going on.

Alert Logic also offers an ActiveWatch Premier team, which is a "white-glove service" of sorts, where an analyst is assigned to a specific customer. The analysts perform manual analysis by "combing through weird indicators," which they compare against information collected from other environments.

Continuous monitoring is a serious commitment. The last thing a customer wants to hear is that a breach occurred during off hours. Alert Logic has two SOCs: one in Houston, and the other in Cardiff, United Kingdom. The U.K. team goes offline when Houston wakes up and vice versa. The Houston SOC displays a Welsh flag in the corner of the room, and the Cardiff center displays an American flag, to remind the analysts they are extensions of the same team.

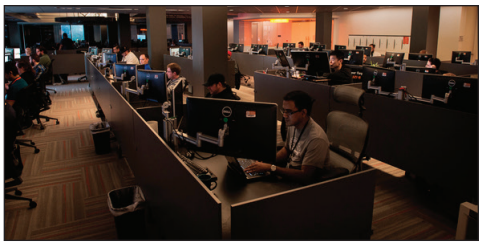
Not everyone needs SOCs

After touring the SOC and learning about the team's continuous monitoring efforts, it's easy to start thinking that everyone needs to invest in SOCs. Well, not exactly — Alert Logic and other providers make it possible for more organizations to work with SOCs, but doing so makes sense only if they've already made other security investments.

Organizations have different security maturity levels; whether or not they're ready for SOCs depends on where they fall on the spectrum, Hall says. Companies with basic security controls are at the lowest level of the maturity model, as they deploy endpoint security tools such as antivirus, network defenses such as firewalls, and VPNs to protect remote connections. These activities are typically managed by the IT staff, and the primary focus is doing just enough to not be considered negligent.

As the organization matures and realizes it needs to do more than the basics, the question becomes how to expand its security expertise. The organization typically looks at specialized systems such as IDS/IPS, SIEM, WAF, and vulnerability management, but the IT team may not know how to respond to the alerts generated by these systems. This is when the organization may build out its own internal security team, hire external security staff, or even buy security as a service.

"This is the level where you say, 'OK, I want to do more than the basics, but I can't really go all the way to a full-blown SOC. Maybe I'll have a couple of dedicated security people on my IT team,'" Hall says.



Alert Logic's security operations center in Houston, Texas

Alert Logic actually picks up a lot of customers in this phase, as these organizations tend to look at ways to beef up their security capabilities, Hall says. This was the case for GenomeNext, which originally used Alert Logic for Web application firewall, log management, and threat management capabilities before moving to the 24/7 SOC.

Once the organization has dedicated security teams implementing policies such as ensuring employees have endpoint security software on their machines and the firewall is configured correctly, they look for other ways to improve their operations. That's the time to start thinking about SOCs.

"The customer says, 'We want to get better, and we want to raise our game in security,'" Hall says.

While it's possible for a company on the lower end of the security model to benefit from SOCs, it will take considerable time and budget to be successful. It's not only a technology investment, but a shift in mindset, since the organization has to prioritize security. The nearly endless stream of data breaches are actually pushing organizations along the maturity model faster, as senior executives and boards see the impact of "just enough" security, Hall says.

Different set of concerns

On the day of the visit, parts of Houston suffered a power outage, which impacted the Alert Logic SOC. Customers weren't affected since Alert Logic temporarily shifted monitoring back to the Cardiff center while waiting for power to be restored. The company has plans in place for handling outages, hurricanes, and other disruptions.

For most organizations, a large-scale attack, such as a breach that resulted in stolen data, or applications and instances deleted from AWS, would be considered catastrophic. For Alert Logic, the worst-case scenario would be incidents spanning multiple customers, Payne says. That could be a coordinated attack or a large worm outbreak threatening to take down an organization. For that kind of a situation, the SOC may assemble a dedicated team that regularly confers with affected customers and make recommendations on how to mitigate the threat.

With so much security becoming automated, would it makes sense to bypass the SOC entirely in favor of automatic detection? Automation can only go so far, especially since the threat landscape is continually changing. New threats are being discovered and new attack methods devised. If the organizations don't have security staff capable of translating the automated alerts into actionable moves, then they may as well as not have any detection capabilities at all.

"There's too many variables to think that you can automate your way out of security," Hall says. "The only way we keep on top of things is by watching and being vigilant."

Many organizations now realize traditional approaches of buying security technology alone is not enough. Prevention needs to go hand in hand with detection, and the security operations center is one way to tap in to skilled security personnel, advanced analytics tools, and continuous monitoring. "It's easy to do the wrong thing if you don't know what you are doing," Govshteyn says.

— Fahmida Y. Rashid — Senior Writer

Fahmida Y. Rashid is a senior writer at InfoWorld, whose coverage focuses on information security.