The Value a Concierge Security Expert™ Brings to Your Team

Sam McLane, a security-operations-center veteran of 20 years and head of security engineering at Arctic Wolf Networks (AWN), answers a few questions about the role of the Concierge Security Engineer™ (CSE) in Arctic Wolf's SOC-as-a-service offering—AWN CyberSOC™.

Here's what the security-operations-center veteran of 20 years has to say:

What is the role of a CSE in Arctic Wolf's SOC-as-a-service offering?

McLane: First and foremost, as CSEs, we're the face of Arctic Wolf to customers. From day one through their entire lifecycle with us, the customer's security engineer is their primary point of contact.

Secondly, CSEs provide all the background security expertise for the service. They review incidents, they review alerts and they generate reports. This is typically done for dedicated customers, but we'll also take turns across the customer base so that we have a variety of eyes looking at different data sources, and no one gets bored or alert-fatigued from reviewing the same data over and over again.

How is AWN's CSE-based service different from other managed SIEM/SOC services?

McLane: Having that personalized service, that one-on-one relationship, really allows us to leverage knowledge and implement customizations in ways that other vendors can't. If you buy into another service, often the tier-one and tier-two support is out-sourced. Or, even if it is local, it's not personalized. So, when you call in, generally they ask "What company are you from?" "Can you describe your environment?" "Have you ever seen this before?"

All of that goes away with Arctic Wolf. Your CSE already knows you and your history, which allows us to be effective and to not waste the end user's time by asking repetitive questions or asking them to explain something multiple times in a given month or quarter if it's an ongoing issue.

Let's home in on one customer example: How do you work together? How often are you in touch with them?

McLane: One of our customers in health care doesn't have a big security team, and has two or three hospitals located throughout their state. On an average month, we'll take in close to 250 million log lines per week, which is what we use to generate our alert data. We go through that, and filter it down to maybe one or two tickets per month. So I'd say we talk to them about incidents every other week.

We also send them a weekly set of reports that they've requested. If they have questions—for instance they might experience extra traffic to Russia in a given month— they can call us up and we'll answer those questions. Every month we sit down with our main point of contact, their director of security, and make sure they understand everything we've seen. We'll also find out if they're doing anything different—for example, adding new security measures or changing policies, or needing to prepare for a HIPAA audit.

Broadly speaking, what are some of the activities CSEs manage for customers?

McLane: We provide managed detection and response, so we collect their data—and our sensors generate a lot of it—and we'll weave through that to generate alerts on anything that we think requires action. We'll also work with the customers to ensure that any malware is cleaned up and that ransomware is contained. If we see data exfiltration, we'll make certain it's blocked, and so on.

On top of that, we provide any reports they have or any alerts they need. Because of the various types of data and the way we collect, organize and structure it, customers might say, for instance, that their Active Directory team needs to know each week how many of their executives get locked out. So we'll supply that report every Monday morning.

Finally, we'll answer general questions. When any security alert comes out in the mainstream media, whether it's Spectre or Meltdown or WannaCry, we get a lot of inbound queries. We walk the customer through it and explain the ramifications in a context they understand.

What threat hunting activities do you perform to keep customers protected from advanced threats such as APTs and zero-days?

McLane: Each team member is assigned a certain amount of research work in a given week. This is part of how we keep team members fresh, so they aren't constantly doing the same type of work, and now have a chance to do something a little more on the cutting edge of threat hunting. Sometimes we have them pick off a type of data such as Active Directory data, or DNS data or firewall data, and look at all of our customer data for a 90-day period or a year in search of anomalies or patterns. They'll look through our different intelligence feeds and align them with what we're doing for customers.

Our CSEs also work with our security research teams—dedicated people from R&D who add in new algorithms and machine-learning techniques for continuous monitoring—to bring certain trends to their attention, maybe an interesting way to look at SSL traffic, so we can always stay sharp.

Otherwise, we just make sure we're getting the right log sources. The day-to-day operational maintenance isn't fun or exciting, but if you do that well you'll catch a lot of the zero-day stuff. For small teams, those are the kinds of tasks that fall off the plate, and that's where you get bit.

If there is a security incident, how does Arctic Wolf inform the customer and ensure that it gets resolved?

McLane: If we see something like ransomware and phishing, we call the customer directly. We open a ticket and track all of those interactions, but we want to talk to a human because time is of the essence. Once we notify the customer, for instance, that a certain machine has ransomware, we can certainly go into our appliances and quarantine that device. But more often than not, it's about dispatching the right person from the customer to that location to unplug the machine and collect the data we need to perform forensics. In those critical scenarios, we're in real time on the phone with the customer.

Most other transactions are conducted over email, and during monthly and quarterly reviews. We summarize all tickets to make sure there aren't any outstanding items. Our customers are often shorthanded and they sometimes forget to update us, so we just want to make certain nothing falls through the cracks.

How do CSEs customize your offering for customers from a monitoring and reporting perspective?

McLane: As customers come on board, we interact closely with them for the first couple of weeks and months to help us fine-tune their service. For instance, if we start sending alerts about older versions of Java that might have software exploits but they aren't concerned about it, we'll suppress that noise. In certain industries, some types of traffic are actually required. There's a law document management system, for example, that 90 percent of law firms use. That software requires certain configurations or versions of Internet Explorer, so we can automatically fine-tune those as they onboard.

Customers realize quickly that the more information they disclose, the better the service works. This lets us add specific customizations so that alerting systems won't fire off anything alarming. We can then provide the right amount of information with a minimum amount of noise.

One final question: What is some of the common feedback you've received about your CSEs?

McLane: The number one thing we hear time and time again is the importance of the relationship our customers have with their security engineers. I probably hear two or three times a day that they wouldn't know what they'd do without "Jonathan" or without "Sarah" on their team. They say that the number of times the CSEs have alerted them to something of which they were completely unaware is invaluable.

Our customers come to us because another solution failed, or they discovered blind spots in their IT security. So, the other thing is we give them peace of mind. During quarterlies, I often hear how much more knowledgeable and assured they are about what's going on, and how they're no longer up at night worrying. When they're asked by executives at management meetings where they are with their security posture, they have confidence that everything is going smoothly and that they're not draining their budget on a variety of tools and services that get away from them. That strong value-to-security ratio from a cost perspective is the icing on the cake.

Learn More: For additional information on the role of the Concierge Security Engineer™ as part of Arctic Wolf's AWN CyberSOC™, read the SANS Institute's review.

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com