Taking Threat Detection and Response to the Next Level

An expanding attack surface, massive volumes of event data and aggressive adversaries are stretching threat detection and response capabilities. ***Barry Hensley,*** *chief threat intelligence officer for Secureworks, hones in on strategies to scale security initiatives.*

How has the pandemic changed risk management for state and local governments?

A lot of the change comes from having to support a large remote workforce. Regular system maintenance tasks like vulnerability scanning and software patching have changed dramatically. In the past, patching technologies assumed that systems were physically on the same network or would ultimately be connected via a virtual private network. As users' machines move off the network, they get scanned less often, if at all. Remote work and increasing reliance on SaaS have really highlighted the need for zero-trust networks, where services require not only a trusted user but also protection of the data viewed and saved from these services.

What are the keys to effective threat detection and response?

The first key is having sufficiently accurate detections so the security team doesn't develop alert fatigue from chasing false positives. This capability must be coupled with comprehensive visibility into the environments and data sets the organization is defending. Once the team can detect threats effectively, knowing how to respond in various threat scenarios is also critical. Incident response playbooks, reinforced with table-top exercises, are a great way to ensure teams understand their roles, the actions they should take and who they should communicate with throughout the process. Experienced incident response teams can reduce the overall time of an incident; get the business up and running again faster; and advise on remediation of architecture, policies and controls to prevent future incidents.

How can machine learning (ML) complemented by human intelligence help organizations better manage threats?

No matter how good an ML algorithm is, the goal is never to replace humans. It's to augment our top-tier security analysts with the best that machine learning can provide. ML improves operational efficiency through various models. One, it greatly improves the scale of data you can process and the likelihood of greater consistency than a team of humans can reasonably produce. This often results in a reduction of false positives and improves detection by sifting through vast amounts of data and detecting known patterns of malicious behaviors. Two, ML can greatly help with security analyst workflow augmentation and automation by optimizing complex tasks. For example, it can reduce the number of alerts the Security Operations Center must process by removing easy-to-identify benign traffic coming from various security controls. Lastly, ML can learn from past human validated actions and then automate those decisions for future similar alerts.

Is it realistic for today's state or local government security organizations to retain their own internal threat research staff?

The costs associated with highly skilled threat researchers and the advanced tools they leverage are often beyond a state or local government's budget. A good compromise is to partner with a Managed Security Service Provider (MSSP) that can leverage its economies of scale and infuse very deep and robust threat intelligence into its detection and response platforms. This allows organizations to focus on high-severity risks versus day-to-day incident investigation.

How can organizations optimize the effectiveness of managed security services?

It's important to ensure that the onsite team has workflows in place to consume the outputs from the MSSP. Using the case of managed threat detection services, for example, if the organization can't digest, draw insights from and act on what the MSSP detects, the value is lost. Second, the organization needs a dedicated direct liaison between the MSSP and the in-house team tasked with remediating threats and vulnerabilities. This improves responsiveness and accountability on both sides, and ensures that alerts are properly tracked from discovery to complete remediation.

You've led top cybersecurity organizations in the military and the private sector. What advice do you have for CISOs and other cybersecurity professionals as they lead through the pandemic and into the future?

As leaders, it's our job to ensure our team members have the appropriate resources to do their jobs and maintain their peak effectiveness. Especially now, we have to focus on innovative ways to maintain team cohesion and improve communications. In addition, it's important to encourage team members to be cognizant of work-life balance, both in terms of delineating between work and personal time as well as not letting work and professionalism slip when they are out of a more formal environment.

Learn more at **Carah.io/Cyber-Secureworks**

We’re Revolutionizing Cybersecurity.

Secureworks combines machine learning with human intelligence to detect faster, respond smarter, and predict and prevent more threats altogether.

4,100
Customers in 50+ Countries

300+
Expert Security Analysts, Researchers and Responders

20+
Years of Attack and Threat Actor Group Data

Request a demo. Learn more at secureworks.com

Secureworks®