PenTest magazine

INSIDE THE SECURITY OPERATIONS CENTER

The Red Pill Of SOC Automation

Examining Perspectives: Both Sides of the Line

Future Generation's Security Operations Centres

AND MORE...

What Does a Next-Generation SOC Look Like?

Shiran Grinberg

Shiran Grinberg is a Senior SOC Analyst at CyberProof. Prior to joining CyberProof, Shiran held the position of Forensic Team Leader & Forensic Lab Manager at Cellebrite. Prior to that, Shiran served in an elite defense intelligence unit. Aside from his expertise in all things cyber, Shiran is a passionate sea man who loves to surf and dive. Shiran is married to Lihini and he is a father to Ariel.

Given these many challenges, creating a SOC that's effective and can be maintained successfully is a big job that requires careful planning. If the goal of the SOC is to meet your security needs and manage risk in your organization, you need to keep this knowledge "front and center" – no compromises. Start by defining the structure and processes, and determine appropriate decision-making procedures before you begin.

Introduction

Developing and maintaining an advanced SOC is a crucial step in establishing a safe security perimeter for your organization. But in today's complex business and technology environment, it can be a challenge to set up a SOC that has the capabilities to keep your organization out of harm's way.

If you're building a SOC, there are several factors to take into consideration: a lack of available professionals with the required skill set, the radically extended security perimeter typical of today's IT environment, and a myriad of security solutions that all operate independently.

In addition to dealing with issues of internal security performance, there are also the external challenges – from the growth of cybercrime to a range of new regulations regarding the handling of sensitive data. These challenges increase the complexity of security-related operations and require time and money, drawing resources away from other activities and considerations.

So with all of these issues, how do you create a SOC that has the advanced capabilities your organization requires? When it comes to developing and maintaining an advanced SOC, the key is to balance all of the necessary components – people, processes, and technologies – in order to protect your organization successfully from cyber attack. Let's take a closer look at what this means.

Where'd All the People Go?

Managing security operations in today's age of IoT and the cloud requires having a well-greased team that covers a broad range of disciplines. But currently, we're facing a shortage of talent.

The need for cybersecurity professionals is increasing continuously – as more and more organizations recognize the need for people who can handle monitoring and response, understand policy, and act as compliance experts. And there simply aren't enough cybersecurity professionals to go around.

The shortage is global. According to the (ISC)^2 Cybersecurity Workforce Study (2018), the gap between available jobs and available people grew to almost 3 million in 2018. While the problem is most severe in the Asia/Pacific region, it's also having an impact on countries in regions including North America, EMEA, and Latin America.

Making matters worse is a real problem with burn out. Working as a security professional can be highly stressful – and the problem of alert fatigue, the routine tasks, and an ever-growing technological stack all lead to attrition. As a result, companies that do manage to bring on board real talent never know how long their hires are likely to stay.

The IT Environment – Working with Hybrid IT and Shadow IT

The shift to hybrid IT environments poses additional challenges for SOC performance and robustness. In a hybrid environment, there's a combination of legacy systems that are on-premises, on the one hand – and systems and services in the cloud, on the other. This creates a greater degree of complexity in the IT environment, and it is a complicated set-up that requires better real-time monitoring and incident response.

As Gary Thome points out in InfoWorld, in the distributed environment of an enterprise today, there's no centralized management view. This is a key problem for security professionals working in a hybrid environment: There are multiple systems, and each system has its own management console. Managing and monitoring all of the consoles takes time, and requires having more people on staff.

Another issue that adds to complexity of the environment is shadow IT – which makes it so hard to protect an organization. Shadow IT, i.e., any information-technology systems and solutions used inside organizations without explicit approval, must be uncovered. And make no mistake, uncovering shadow IT is an ongoing battle – one that's essential in ensuring that an organization is aware of everything going on within the system, and can respond when necessary.

Coming Up with a Good Strategy for Advanced SOC Operations

Given these many challenges, creating a SOC that's effective and can be maintained successfully is a big job that requires careful planning. If the goal of the SOC is to meet your security needs and manage risk in your organization, you need to keep this knowledge "front and center" – no compromises. Start by defining the structure and processes, and determine appropriate decision-making procedures before you begin.

One of the first questions that come up in planning a SOC relates to operational coverage. Will your SOC be available 24/7 or only during business hours? If you're limiting the hours of operation, who will be handling security after hours?

This decision is connected to another question: What happens when an event requires escalation? Who is contacted, and under what circumstances? Are senior managers brought into the loop and if yes, at what point in the process?

A third question involves the crucial need for continuous iteration and improvement. How do you ensure the ongoing development of the SOC? A SOC that is not developing quickly becomes hopelessly out of synch. To prevent this, processes should be determined from the beginning that, for example, push the development and improvement of digital playbooks and ensure the SOC stays on top of changes in the threat landscape.

Finding Security Professionals Who Have the Right Approach

Security professionals need a different attitude than that of IT professionals. The work requires thinking like a hacker – and figuring out how to protect an organization effectively.

The best SOC professionals are creative, out-of-the-box problem solvers who excel at lateral thinking. They don't just look at the data but rather, they look beyond it, asking, "What else do we need to do?"

There's also the question of the SOC's structure – which is related to a team's knowledge level. Most SOCs are staffed primarily by individuals with relatively little experience. Frequently, the work is viewed as a student job – something that's entry-level.

An alternative way of staffing a SOC involves taking fewer people, but making sure they are individuals with significant professional experience. This allows the SOC to operate at a higher level – with greater cooperation and quicker turnaround. But high-level people may be hard to find.

To sidestep this issue of obtaining access to real talent, you may want to consider working with an MSSP (Managed Security Services Provider) – using outsourced resources that give you access to the expertise you need, while increasing return on investment in legacy systems.

Leveraging Technologies that Support Orchestration & Automation

SOCs work with so many different technologies. And using each one separately is inefficient, requiring time and expertise. This problem is a deal breaker – because speed and accuracy is essential; a SOC needs the capacity to detect and respond to malicious behaviors and incidents in near real-time.

The goal of a SOC is to handle an incident optimally, i.e., with maximum speed in order to mitigate any damage caused, whenever and however the incident occurs. Multiple systems make this hard to achieve.

As a case in point, consider the common situation of a virus alert. Investigating a virus alert requires a SOC to use the SIEM, the EDR (Endpoint Detection and Response), and network forensic technologies designed to provide advanced threat detection. We're talking about interfacing with these systems just to get a good picture of what's going on.

So what's the solution?

Orchestration & automation – using advanced technologies that make the work easier and faster, maximizing efficiency. By integrating orchestration & automation capabilities into SOC functionality and processes, a SOC cuts out the number of false positives – the "noise" – leaving the SOC team free to focus on alerts that really do need attention.

The Advantages of AI and ML

The efficiency of an advanced SOC is connected to the use of artificial intelligence (AI) and machine learning (ML). These tools allow creation of smart insights that correlate and enrich log alerts, providing the extra context that makes them "smart alerts." And of course, the self-learning capabilities facilitate continuous improvement.

Used in tandem with big data, AI and ML predict and automate detection and remediation, and can significantly shorten the time to incident response and recovery. The extra data means that detection and remediation can take place in hours – rather than weeks.

Conclusion

Maintaining a SOC that has advanced capabilities is not an easy task. Multiple challenges stand in the way: For one, we simply do not have enough excellent security professionals to meet the world's current needs. There's a shortage of people internationally, and the people we do have frequently suffer from burn-out.

In addition, today's technological landscape makes it more difficult to secure an organization, as the IT environment becomes increasingly diluted. Examples of challenges include the growing existence of hybrid IT environments and shadow IT.

Given these complexities, it's essential to take time out before you start building a SOC to define what you're looking for – to figure out what you need in order to effectively protect your organization. Consider who you want on staff – exploring options for combining the skills of entry-level workers and higher-level professionals, or working in tandem with an MSSP. And put into place – right from the beginning – workable procedures for review and improvement of processes and for ongoing playbook updates.

Advanced technologies are key. Explore how to leverage technology to provide the SOC with orchestration & automation capacities, and learn how to integrate AI and ML. These capabilities are game-changers, reducing the "noise" of false positives so that the SOC team can do what they need to do – and drastically shortening the time required for incident detection and response.

About CyberProof

CyberProof aims to give clarity and confidence to businesses worldwide with a new risk-based approach to cyber security services. CyberProof is part of UST Global, serving some of the world's largest enterprises with their digital transformations. As trusted partners throughout the entire cyber journey, we promise companies around the world measurable risk reduction and justified ROI. For more about CyberProof, please visit our website at: www.cyberproof.com

CyberProof™
A UST Global Company