

The top challenges of today's SOC

In today's increasingly connected world, corporate security operations centers (SOCs) are more important than ever.



SOC teams are on the front line of protecting the company operations and confidential data from the myriad of rapidly evolving cyber threats organizations face everyday. SOC teams are tasked with more responsibility than ever before. As a result, they are drowning in systems that don't provide enough information or context to empower analysts to make informed decisions. As a result, SOC teams are spending too much time on analysis and validation and not enough time on problem solving.

This ebook takes a closer look at the top 6 challenges that impede the effectiveness of SOC operations and how advanced analytics technologies can address these challenges and streamline analyst efforts.

There are many factors impacting the modern SOC team that can reduce their effectiveness. This eBook looks at some of the key challenges, including:

- 1. SOC analysts are working on the wrong problem**
- 2. Cyberthreats are evolving faster than defenses**
- 3. Cost control in the SOC**
- 4. Staffing challenges in the SOC**
- 5. SOC operations models**
- 6. Compliance impact to SOC operations**

It also introduces the value of applying advanced analytics to facilitate event analysis and alleviate these pressing challenges.

“Today’s typical SOC is not adequately lowering risk or getting the right return on investment. Team members must spend valuable cycles on validation instead of problem solving . There are too many things to respond to and very limited data upon which to make a good decision. This needs to change.”

1. SOC analysts are working on the wrong problem

Everyday, analysts are flooded in alerts, many of which are false, while at the same time lacking the necessary visibility and context to properly make decisions, and are forced to spend much of their time hunting down information on alerts rather than identifying risk, responding to incidents, identifying incident impact, and reducing the time to the detection of breaches.

According to the Cisco 2019 CISO benchmark Study, an average of 49% of security alerts are not investigated. Of those that are investigated, only 24% are deemed legitimate. Of the legitimate alerts, only 43% are actually remediated.

This is in large part due to the sheer volume of alerts that SOC teams receive on a regular basis, especially since a significant portion of companies manually review cybersecurity alerts. In fact, 66 percent of companies receive up to 10,000 alerts per day and 21 percent of companies receive up to 100,000 daily alerts.¹

2. Cyber threats are evolving faster than defenses

The environment in the enterprise changes daily, cyber threats change moment-by-moment, and cyberdefenses lag behind. Significant updates to the cyber defense environment might change quarterly, at best. How can one expect an enterprise to be sufficiently protected when defenses stand still while threats and even the environments being protected are evolving at such rapid paces? Attackers will get in, and you have less and less time to detect and defend against them.

Attack velocity (i.e., the speed of the attack) is increasing as the average time from the initial breach to data exfiltration or other targeted activity is decreasing. For example, the Microsoft Global Incident Response and Recovery Team saw a phishing email attack go from initial infection to full and complete domain control in less than 24 hours.²

Corporate SOC's must detect and defend against attacks at a faster rate and scale to keep pace with cybercriminals.

3. Cost control in the SOC

Cost control is certainly not an issue unique to security, but the nature of SOC's and the realities of today's security landscape create distinctive difficulties when budgeting for it. The hiring of knowledgeable SOC team members with the necessary background to address the current cybersecurity landscape is constrained by both rising salary levels and an acute shortage of candidates. You need to be able to pay your security personnel enough that they aren't attracted by higher paying positions at other companies, a real risk as long as there continues to be a major shortage of skilled cybersecurity professionals.

While dealing with all of this, you also need to maintain continuous training among your SOC staff which may lack necessary basic training. The SOC staff needs both the time and the resources to keep up with this rapidly-changing landscape, even while continuing to provide needed defense and analysis on an operational basis around-the-clock.

SOC's must also maintain up-to-date technology. Each SOC has a unique set-up and most of the smaller teams don't have well-formalized processes. Determining which new technologies will properly augment your personnel and current technology is a challenge all its own, and one that is not helped by the speed at which the cybersecurity and threat landscapes change. You need to select technology that is worth the investment, that is of actual use to the SOC staff without further complicating their jobs.



4. Staff challenges in the SOC

As noted earlier, the shortage of such security personnel is widespread and shows every indication of increasing substantially over the next few years. More than half (53%) of companies report they have a problematic shortage of cybersecurity skills in the organization, and there will be an estimated 3.5 million unfilled cybersecurity positions by 2021.³

Many organizations don't have enough SOC staff to assign each only one role, necessitating the personnel you do have to juggle the duties and specialties. This would be a problem even if it wasn't complicated by the high turnover rates of SOC staff. Because many important SOC tasks often depend on a few key individuals, when those people leave for greener pastures, the SOC is left in a lurch, left without the skills and familiarity

provider (MSSP)? Use a combination? Should you use managed detection and response (MDR) technology to supplement your team instead? What about the variety of security information and event management (SIEM) software?

It is easy to get caught in the Hamster Wheel of Pain. This is the cycle in which you implement a new tool, later realize it does not work for you, spend time assessing new tools, implement one, realize it doesn't work for you, on and on (and on).



necessary to implement necessary tasks and processes. According to (ISC)², it takes 55% of organizations three to six months to fill vacant cybersecurity positions. And, once they are filled, there is a good chance the new analyst will require months to learn some of the basic skills for the position.⁴

5. SOC operations

There are several different approaches to running a SOC. Tactical technology solutions, of varying quality, show up at your doors daily, while new strategies to better manage and operate the SOC, however, are rarely seen and less often implemented.

This doesn't mean that there aren't options, though, but how do you find which one fits your company? Should you stick with an entirely in-house SOC? Outsource to a managed security service

6. Compliance impact to SOC operations

Compliance regulations drive baseline SOC performance requirements but don't guarantee improved security. Many requirements make operations even more complex, especially for multinationals.

In the U.S., there are also state-level laws that impact cybersecurity. Colorado expanded a statute on data privacy to add a 30-day breach notification from the time that the company determines that one has occurred. New York state's department of financial services revised a cybersecurity regulation requiring risk assessments by application, policies that limit the retention of data, monitoring access to information, and encryption for all nonpublic (private) information at rest and in transit.



All of this follows the enacted General Data Protection Regulation in the European Union, the U.S. Cloud Act, the U.S. Encrypt Act, and California's Consumer Privacy Act. Most companies are not tracking the U.S. Data Breach Prevention and Compensation Act.

These regulations create many requirements for U.S. and European companies. Formal risk assessments take considerable time. All of this adds to the SOC's administrative and planning burdens as team members must spend more time in meetings with the compliance and governance teams and less time identifying and resolving threats.

SOC teams must be acutely aware of these challenging regulations and must be able to accommodate the best practices and technologies necessary to meet compliance. Adding to the challenge of meeting all of these requirements is the need for cloud security, as regulations place the burden of security is placed on the cloud customers rather than the cloud providers.

The Imperative for advanced analytics in the SOC

As discussed, the sheer number of alerts received everyday overwhelms SOC personnel, and the lack of context for those alerts keeps analysts focused on the wrong problems.

Your most valuable resources in the SOC are wasting time and not resolving the problems. Advanced analytics to provide alert analysis and context holds the keys to delivering the very best return on investment for your SOC team investments.

“The SOC is drowning in systems that are providing information but lacking enough context to make good decisions. The power of automated alert analysis that employs advanced analytics, such as machine learning and artificial intelligence, is without peer.”

Sumo Logic

Greg Martin
VP/General Manager

Advanced analysis techniques can facilitate the analysis of all of the information regarding an incident, something analysts alone cannot do. By using human analytical processes encoded in machines to validate and contextualize alerts, analysts are freed to focus on more important problem-solving.

Automated analysis ensures all critical alerts are analyzed and that they are resolved in a timely and effective way. This approach provides the essential bridge that can enable the SOC team to efficiently manage the rapidly growing workload, while at the same time resolving important threats in a timely way.

What's next?

Threat detection and analysis represents the singular weakest point and greatest opportunity for organizations to advance their SOC practices. Ready to learn more about how Sumo Logic can help?

1 Cisco. 2019 CISO Benchmark Report. March 2019.

2 <https://cloudblogs.microsoft.com/microsoftsecure/2017/08/03/top-5-best-practices-to-automate-security-operations/>

3 CSO. Cybersecurity skills shortage is getting worse. January 2019.

4 Cybersecurity Ventures. Cybersecurity Jobs Report 2018-2021.



s

u

Continuous Intelligence Platform™

m

o



sumo logic

Toll-Free: 1.855.LOG.SUMO | Int'l: 1.650.810.8700
305 Main Street, Redwood City, CA 94603

www.sumologic.com

© Copyright 2020 Sumo Logic, Inc. Sumo Logic is a trademark or registered trademark of Sumo Logic in the United States and in foreign countries. All other company and product names may be trademarks or registered trademarks of their respective owners.

Updated 06/2020