SafeAeon

SECURITY OPERATION CENTRE

Inhouse Vs Outsource

WHITEPAPER

www.safeaeon.com

BUILDING A SOC

An organization must hire, train, and retain enough employees to continuously monitor security alerts, analyze them, and eliminate cybersecurity risks. To promptly address risks, the SOC requires a dedicated area, a wide range of security and remediation technologies, highly skilled analysts, and incident response specialists. In-house SOCs, who lack a comprehensive understanding of the threat landscape and only have knowledge of risks they have personally encountered, must subscribe to threat intelligence services that offer practical guidance on dealing with both existing and emerging threats. Because threats are continually evolving, SOC staff members must regularly attend internal and external training sessions on the latest security tools and techniques for preventing and retaliating against assaults. Although SOC members are supposed to share information among teams, this is frequently not the case. Employees frequently quit their jobs to pursue possibilities in government or commercial cybersecurity businesses, where they can collaborate with other team members and gain knowledge from leading authorities in the field.

As per the Global Research Report "2022 Cybersecurity Skills Gap" by Fortinet, Security Operation Centre is the second most challenging area for recruitment, and 52% of organizations struggle with retention of different cybersecurity roles. Globally, 88% of organizations' board reports state they need to hire cybersecurity professionals immediately. Even though this is a decline from 53% in 2019, 51% in 2018, and 45% in 2017, Jon Oltsik, senior principal analyst, ESG fellow, and founder of ESG's cybersecurity services, claims that the cybersecurity skills gap is not getting better. According to him, security executives are now experimenting with new types of analytics, embracing automation, expanding their teams with professional and managed services, investing in training, and consolidating security technology after many years of dealing with the cybersecurity skills shortage.

In addition, 2020 demonstrated that all projections are merely guesses, just as Cybersecurity Ventures, a research organization focusing on the global cyber economy, forecasted in 2019 that there would be 3.5 million cybersecurity positions open by 2021. The skills gap decreased in 2020, from 4.07 million in 2019 to 3.12 million, according to (ISC)2, which has been monitoring the cyber workforce since 2014. This is because 700,000 more workers were entering the profession in 2020, but also because the COVID-19 epidemic caused a decrease in demand. 5 See what the remaining months of 2021 reveal. Cybersecurity Ventures estimates that by 2025, cybercrime will cost the globe $10.5 trillion, up from $3 trillion in 2015.

OUTSOURCING A SECURITY OPERATIONS CENTER

Outsourcing a SOC will help reduce the cost of SIEM license ownership and the hassle of training and developing an in-house team. Outsourced SOCs are fully staffed 24X7 and use their platforms to correlate threats. They have a highly skilled workforce that regularly monitors the environment and analyses alerts, as well as its security and repair solutions. To avoid having to do it themselves or engage incident response staff, several outsourced SOCs also remove threats. Outsourced SOCs have direct access to threat intelligence gathered from hundreds of thousands of clients in addition to leveraging external threat intelligence services. When a threat is identified in one environment, the SOC develops countermeasures to find and stop it, thereby defending all its clients. An outsourced SOC can safeguard clients much better than any internal SOC, which only has access to its limited understanding of the threat environment, thanks to the global community-powered threat insight. When an internal SOC first detects a threat, a global SOC has already identified it and developed countermeasures to block it.

There is still cause for concern; even FireEye and Mandiant state in their M-Trends 2021 special report that the dwell duration—the time between a threat entering and exiting an environment—fell by half to an average of 24 days in 2020. Compared to 416 days in 2011, 24 days is a considerable decrease from 56 days, although experts note a steep rise in ransomware cases from 14% in 2019 to 25% in 2020. Attackers are increasingly at ease with taking big risks since ransomware attacks may do much harm in a brief period.

Many MSSPs warn businesses about cyber threats, but they do not always intervene to handle incident response. They offer to alert and impose exorbitant incident response fees, returning responsibility for remediation to their clients. To reduce risk and economic loss, swift remediation is essential. However, only some businesses have in-house security specialists capable of resolving attacks in hybrid, cloud, and on-premises settings.

The costs will be reduced the sooner a data breach is discovered and contained. According to the 2020 IBM/Ponemon cost of a Data Breach study, there is a direct correlation between how soon a company can detect and contain data breach occurrences and the resulting financial costs. From the report from the prior year, a lot has stayed the same. In comparison to 279 days in 2019, it took an average of 207 days to identify a breach and 73 days to contain it. Threat remediation requires not just top-notch technology but also qualified personnel. If cleanup is improperly carried out, the attacker can be alerted and resort to more extreme actions. Any SOC's effectiveness is influenced by its personnel, equipment, and procedures.

SOC ANALYSTS

The world's leading information security training and certification body, SANS Institute, advises that a SOC team consists of at least four roles: Tier 1 analysts, Tier 2 incident responders, Tier 3 threat hunters, and a SOC manager (Tier 4). Anomaly activity on networks, servers, endpoints, databases, and online applications is regularly monitored by analysts. They look for weaknesses in an environment to reduce risk before a breach happens, and they look through the logs to discover what unusual activities have taken place.

To ascertain whether a threat is present in their system, Tier 1 analysts need to be proficient log interpreters. If so, they must ascertain what kind of threat it is. That is challenging because numerous risks are like one another, but each might lead to various issues. Businesses that lack the cybersecurity firms' comprehensive threat intelligence frequently need more expertise to identify the precise sort of danger present in their system. Companies frequently categorize threats improperly, lacking information on the threat's characteristics, the kind of data it seeks, and the havoc it has already wreaked.

When the SOC is not receiving any warnings, analysts look for threatening behavior and attempt to stop it as soon as they are aware. Analysts interact with the Tier 2 incident response team when they find dangers within the network. To aid incident responders in comprehending the threat and delving deeper into the situation to ascertain whether a crucial system or data set has been impacted, they provide as much comprehensive, context-rich attack data as possible. Threats are removed by incident responders, who also inform analysts of their findings.

The most difficult component of cybersecurity is often responding to and resolving attacks; most firms need to improve in this area. Most businesses need a thorough understanding of threat remediation. They might believe they have eliminated a threat, yet there could still be remnants of it in another system. Or else, the danger might have developed a backdoor that makes it simple to get back into the network. Professional incident responders who have received forensics training and can provide recommendations regarding the best ways to address the underlying cause of the compromise to stop future attacks are frequently the best people to handle incident response.

Threat hunters are Tier 3 of the SOC. They are truly knowledgeable in forensics, threat hunting, networks, and malware reverse engineering. Threat hunters are adept at employing tools to find sophisticated dangers hiding in the network unseen using the most recent threat intelligence and indicators of compromise.

The Tier 4 SOC manager also finds, employs, and evaluates staff and completes the SOC team by managing personnel, budgets, and scheduling. Additionally, the manager oversees all new initiatives, training, and business-critical incidents. A well-managed SOC team collaborates to respond quickly, and a playbook guides each position for addressing issues.

SOC PROCESSES

SOCs must have systems in place to ensure that all actions are taken to properly prevent, detect, and remediate breaches and have the newest intrusion detection and prevention technologies and highly qualified personnel. The SOC should include playbooks to detect and respond to threats without interfering with business operations, carrying out routine tasks like filtering emails, network traffic, and endpoints, and engaging with clients to evaluate lessons learned after an incident. A standardized, repeatable workflow offers direction for dealing with any circumstance, including the actions that must be completed to satisfy SOX, FERPA, FISMA, PCI DSS, GDPR, and HIPAA compliance regulations. To save businesses time from having to spend hours designing reports, a SOC should be able to offer help in meeting each compliance standard's requirements. It should offer each customer an Attestation of Compliance that is customized and audit ready.

SOC TECHNOLOGY

To detect and eliminate threats, SOCs require the most up-to-date techniques, including machine learning and artificial intelligence. There is a constant flow of data from workstations, routers, servers, mobile devices, and many other security technologies, but analysts can only process so much data simultaneously. Machine learning can complete tasks that would take people hours in a matter of seconds. Additionally, it can immediately identify unusual activity. It can, for instance, spot unusual occurrences like a U.S.-based employee connecting to the network from a device with a Chinese IP address. To aid in the detection of fraud, machine learning can also highlight emails from a domain that is like one it is familiar with. For instance, it might reject emails that are sent from Amazon.com instead of Amazzon.com. Artificial intelligence algorithms use machine learning to identify threats and classify them according to their seriousness.

SOC tools need to spot attacks on-premises and in the cloud. Virtually all organizations have data in the cloud, even those that do not know it. Employees may use cloud apps such as SalesForce, Dropbox, or Google Docs. Or they may be using their emails for business and exfiltrating company data.

COSTS

Companies that want to create a SOC must set aside initial and continuing funding. Companies considering building a SOC should compare the costs and benefits of outsourcing a SOC. The average annual salary for an incident responder, threat hunter, SOC manager, and cybersecurity analyst in the United States is over $80,000. Even at the smallest businesses, the SOC must always contain at least one security analyst. t the very least, a small company needs to staff its SOC with seven people: four security analysts, one incident responder, one threat hunter, and one SOC manager.

A SIEM costs, on average, around $50,000, plus annual maintenance, and support fees. Not addition, the cost of the detecting equipment comes to $610,000.

"Building a SOC—or generally developing some kind of internal security operations capabilities—is a costly and time-consuming exercise that requires continual attention to be effective," says Siddharth Deshpande, principal research analyst at Gartner.

Many businesses—including some big companies—decide against having a SOC. They choose alternative security monitoring methods, such as hiring a managed security service provider (MSSP).

OUTSOURCING SECURITY OPERATION CENTRE

Businesses do not need to purchase additional security products, engage additional staff, and invest in further training is reduced when they outsource their SOC. The products that firms have already invested in will run at their peak efficiency since they will be monitored and maintained round-the-clock by qualified cybersecurity professionals. All alerts will be reviewed by analysts who are well-versed in log outputs, and incident responders will provide recommendations for repair based on their experience and knowledge. Customers continue to be able to see via a single pane of glass, govern their whole environment, and access all policy enforcement.

CONCLUSION

Running a SOC is very labor-intensive. It requires elite talent, challenging to find and keep, and cohesive teams that can share knowledge. The SOC's primary responsibility is always to play defense. Companies should assess the issues they are attempting to solve before investing in a SOC and determine whether they require an internal SOC, an external SOC, or a combination of both. Some industries might need their SOC, and some big businesses already have the facilities, funds, and innovative equipment required to create one.

However, SMBs and businesses who need more resources to create their own SOC can still

benefit from the best cybersecurity protection available without having to spend a fortune on pricey gear, manage it, or worry about finding, employing, and keeping security specialists. Today, even the tiniest businesses can have a SOC staffed around the clock.

COMMON CUSTOMER CHALLENGES AND HOW WE SOLVE THEM

Important Factors	Common Challenges Faced While Building Your Own SOC	How to overcome Challenges within minutes by outsouring SOC as a Service from SafeAeon?
Security Team		
Finding and recruiting talented applicants	SOC experts are hard to find and harder to keep.	Within a click, have rapid access to industry leading security experts without the burden of recruiting, employing, and retaining internally.
Filling Cybersecurity Skills Gap	Filling gap is challenging for nearly 80% of organizations	
	COST	
Licensing fees	Costs hundreds of thousands of dollars.	SOC as a service works on Monthly Subscription model. You Pay based on Consumption only. No Lock-in Contracts. $0 Onboarding and Transition.
Total Cost of Ownership	Deploying, maintaining, and operating in-house SOC is expensive.	
	Time	
24/7 Monitoring	Hackers attack usually out of working hours.	SafeAeon's 24×7 Security Team work around the clock
Dwell Time and Economical Impact	Average industry Dwell time is in months	Reduce dwell time from months to minutes, lowering the financial effect
Build a SOC from scratch	Take years to mature SOC processes and scale operations	Within Minutes! Just Call us at 1.855.684.1313
	Tools and Process	
Facilities and Tools	You need to purchase, install, run and maintain all SOC tools	We've all the updated facilities, tools and knowledge to do the job perfectly.
Up-to-Date Security	Keeping up-to-date with the latest SOC tools and capabilities is difficult	
Faster detection and remediation	You create and manage these processes at your organization instead of focusing on your core business	Our team take away all your worries to let you focus on your revenue growth. Just within a call, you can get the capabilities of a modern SOC without the cost and headache of managing one.
Managed security with monitoring		
Events, Alerts, and Incidents Management		
Incident & event reporting		
Threat Detection		

Why is it beneficial to Outsource the SOC than to build inhouse

Vulnerability assessment		
Root cause analysis		
Incident Response		
Compliance Management		
	Certification	
Compliance & Certification	A SOC must be aligned with ISO 27001 or SOC II Type 2.	We're both ISO 27001 or SOC II Type 2 certified

CONTACT US

CONTACT US NOW!

1855-684-1313 | info@safeaeon.com | www.safeaeon.com