digital craftsmen™ ARMOR

MARCH 2020

WHITE PAPER

SECURITY OPERATIONS CENTER: BUILD IT OR BUY IT

Digital Craftsmen Ltd

info@digitalcraftsmen.com

INTRODUCTION

Organizations of all sizes have come to realize the only way to protect their networks and data around the clock is with a security operations center (SOC) that operates 24/7/365. A SOC, according to Gartner, can be defined both as a team, often operating in shifts around the clock, and a facility dedicated to and organized to prevent, detect, assess, and respond to cybersecurity threats and incidents, as well as to fulfill and assess regulatory compliance.

Although nothing can ensure a threat never enters a network, a SOC can act instantaneously to prevent a significant loss of data from ever occurring. Most organizations know they need a SOC but don't understand all the resources needed to operate one. Before deciding whether to build or buy—also referred to as outsourcing—organizations need to know the staff roles, technology, and costs needed to operate a successful SOC.

> The only way to protect your network and data is with a security operations center that functions 24/7/365.

THE NEED FOR AN EFFECTIVE SOC

A successful SOC supports business objectives and consists of technology, current actionable threat intelligence, and expert warriors who can defend their network in the cloud and on premises. The SOC needs the ability to aggregate, normalize, correlate, prioritize, and remediate security events. To do that, large enterprises will typically implement a security incident event management (SIEM) solution. Operating a SIEM is labor-intensive, expensive, and difficult to fully operate. A SIEM must continually be tuned, updated, patched, and monitored. With annual costs that run anywhere from $10,000 to more than $100,000 and a lack of funds to hire the talent to maintain it, most small and midsized businesses (SMBs) outsource their SIEM service.

A SIEM solution or similar technology is necessary to combine security events and look at them as a whole. Without one, companies would receive alerts from different devices. Analysts would review each alert separately, preventing them from easily seeing correlations between alerts. For example, by itself an alert regarding each one of the below events probably would not attract the concern of an analyst:

- 20 login attempts within a couple of minutes on one computer
- A search in the cache for administrator credentials
- A computer that starts up the macros application

However, if those three events were combined into one picture, an analyst would gain a better understanding of what is going on. Together, those three events would provide clear indications that a threat actor has broken into a user's computer, searched for the administrator's login credentials and started up macros to record the authentic user's login credentials each time the user logs into a website.

Taking similar data of interest coming from the above sources, the SIEM aggregates the data and provides a summary of the security events of interest. The SIEM also correlates that data, establishing connections among different logs from different devices and applications. For example, an IDS/IPS log shows packets and streams of data, while application logs show sessions, users, and requests. So, if the IDS/IPS and the application logs are both showing suspicious activity, it probably means something malicious is occurring, and the SIEM will send an alert to the SOC. An analyst must then review the logs to discern whether the alert is a false positive, meaning it was just some anomalous activity and is harmless, or whether it is a true positive, meaning it is indeed a threat. Log messages use technical languages and differ from one another depending upon the vendor and device, so analysts must have years of experience to fully understand the logs. Although many people call themselves analysts, that does not mean they have the experience needed to comprehend logs.

Once analysts discover threats, they feed their threat-related findings back into the SIEM so that it becomes smarter over time, can better discern what is and is not a threat, and will block anything known to be a threat. This process takes an inordinate amount of time, stresses resources, and may require the company to hire more security experts. The SIEM is only effective when people constantly pay attention to its input and output. If it puts out alerts and no one analyzes each alert and remediates each threat, the company environment gets breached and threats can stay hidden for months or longer. One of the most highly publicized breaches from a big-box store occurred not because the SIEM didn't put out an alert, but because no one took the time or had the knowledge to properly analyze the logs. Having quality analysts on hand who can make time to adequately review the logs is difficult for enterprises, but it's much more difficult for SMBs. Finding quality people is the most difficult part of running a SOC. Build it, but the people might not come.

The SOC needs the ability to put into context log data generated from a broad range of the following sources such as:

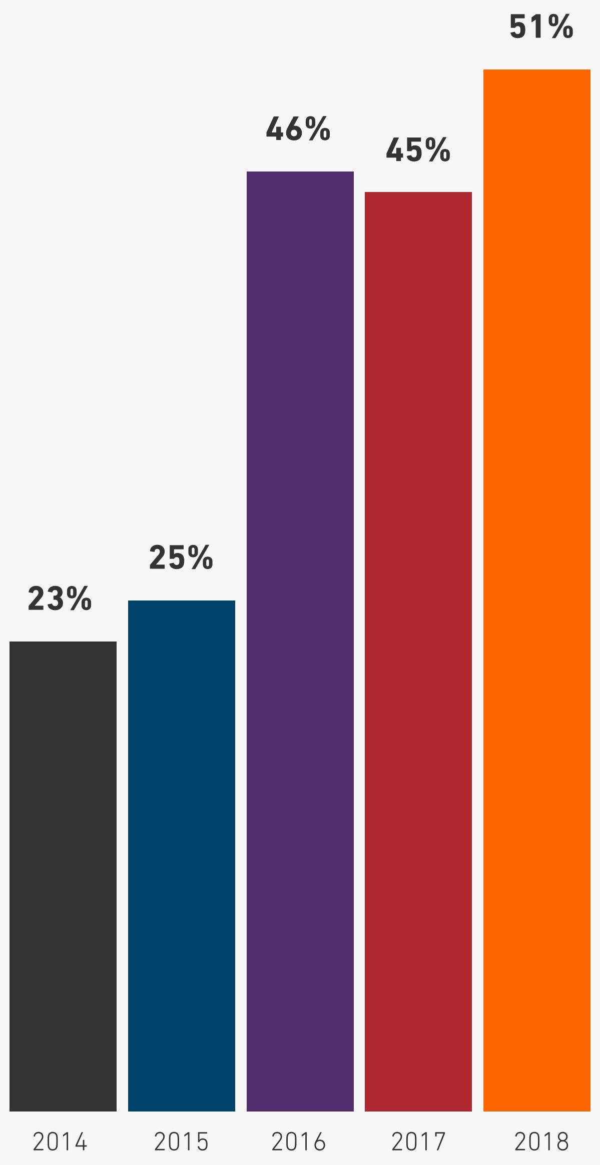
- **Antivirus software**
- **Firewalls**
- **Key servers**
- **VPN concentrators**
- **Web filters**
- **Honeypots**
- **Intrusion detection and prevention system**
- **Routers**
- **Switches**
- **Domain controllers**
- **Wireless access points**
- **Application servers**
- **Databases**
- **Intranet applications**

BUILDING A SOC

Organizations that want to build their own in-house SOC need to be able to hire, train, and maintain enough staff to continuously monitor and analyze alerts and remediate threats. The SOC needs its own space as well as a variety of security and remediation tools, highly experienced analysts, and incident response specialists so they can quickly remediate threats. In-house SOCs, which don't have a global view of the threat landscape, only have knowledge of threats that they have seen and need to subscribe to threat intelligence services that provide actionable advice to combat current and emerging threats. Because threats are always changing, SOC employees must constantly attend internal and external training courses on new security technologies and new ways to prevent and respond to attacks. Although SOC members should be sharing information among teams, often they don't. Employees often leave companies to find other opportunities within government or professional cybersecurity organizations, where team members work together and can learn from top experts in the industry.

In-house SOC managers must be prepared to continually search for new security experts. Enterprise Strategy Group (ESG), an IT research and analyst firm, found in 2018 that 51 percent of respondents (620 IT and cybersecurity professional across all industries, with respondents working in North America and Western Europe) claimed that their organization had a problematic shortage of cybersecurity skills. That's an increase from 45 percent in 2017, 46 percent in 2016, 25 percent in 2015, and 23 percent in 2014. In a study ESG conducted in 2017 with the Information Systems Security Association (ISSA), 70 percent of cybersecurity professionals claimed that their organization was impacted by the cybersecurity skills shortage, resulting in increased workloads on cybersecurity staff, the need to hire and train junior personnel rather than experienced cybersecurity professionals, and cybersecurity teams spending most of their time dealing with daily emergencies rather than training and preparing for the latest defense strategies. Cybersecurity Ventures, a research firm covering the global cyber economy, predicts that by 2021 there will be 3.5 million unfilled cybersecurity jobs, up from 1 million in 2014. Cybercrime is expected to cost the world $6 trillion by 2021, up from $3 trillion in 2015.

Percentage of ESG Survey Respondents Claiming a Shortage of Cybersecurity Skills in Their Organization Since 2013:



OUTSOURCING A SECURITY OPERATIONS CENTER

Buying, or outsourcing, a SOC removes the need for purchasing a SIEM and building a SOC. Outsourced SOCs use their own platforms to correlate threats and are fully staffed 24/7/365. They have their own security and remediation tools as well as highly experienced staff who continuously monitor environments and analyze alerts. Some outsourced SOCs also remediate threats so companies don't have to do it themselves or hire an incident response team. In addition to using external threat intelligence services, outsourced SOCs have first-hand threat intelligence gathered from hundreds of thousands of clients. Once a threat is seen in one environment, the SOC creates countermeasures to detect and block that threat, protecting all its customers. This global community-powered threat insight allows an outsourced SOC to protect customers far better than could any in-house SOC, which has only its own narrow view of the threat environment. By the time an in-house SOC sees a threat for the first time, a global SOC has not only seen it but already created countermeasures to block it.

It's important that an outsourced SOC automatically remediates threats rather than just alerts a customer that its environment has been breached. Companies that use a managed security service provider (MSSP) are often alerted to threats, yet because they don't have the ability to remediate threats, those threats stay hidden in environments for months. A 2019 Ponemon Cost of Data Breach report found that the dwell time, the time period between a threat entering and leaving an environment, averages 99 days.

Many MSSPs alert companies to threats but don't automatically step in to perform incident response. They only provide alerting and charge high incident response fees, putting the onus of remediation back onto their customers. Quick remediation is paramount to minimizing risk and financial loss, but few companies have security experts in-house equipped to remediate threats in hybrid, cloud, and on-premises environments.

The faster a data breach can be identified and contained, the lower the costs. The 2019 IBM/Ponemon Cost of a Data Breach Study reports the relationship between how quickly an organization can identify and contain data breach incidents and the financial consequences. The mean time to identify (MTTI) a threat was 279 days. The mean time to contain (MTTC) a threat was 73 days. Threat remediation not only takes superior technology but people who have the right skills. If remediation is not done properly, it could tip off the attacker who might then take more drastic measures. The effectiveness of any SOC depends on its people, tools, and processes.

It's important that an outsourced SOC automatically remediates threats rather than just alerting a customer that its environment has been breached.

PEOPLE

SANS Institute, the world's largest information security training and certification organization, recommends that a SOC team contain at least four roles: analysts (Tier 1), incident responders (Tier 2), threat hunters (Tier 3), and a SOC manager (Tier 4). Analysts continuously monitor anomalous activity on networks, servers, endpoints, databases, and web applications. They try to identify vulnerabilities in an environment to mitigate risk before a breach occurs, and they review the logs to see what type of anomalous activities have occurred.

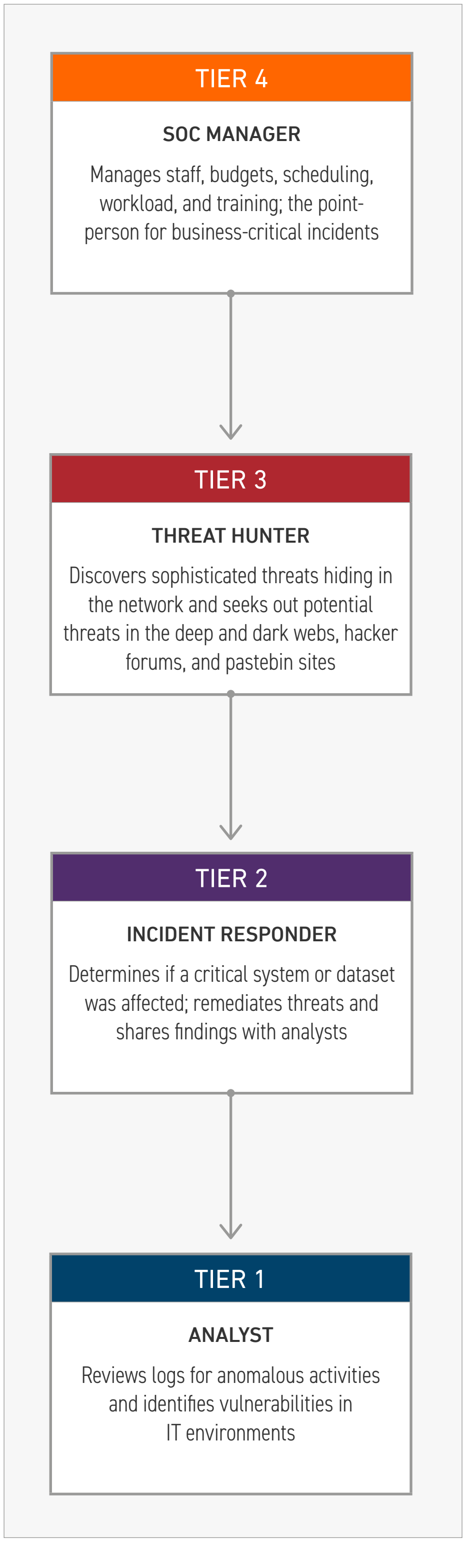
Analysts, Tier 1, must be skilled at interpreting logs to determine whether a threat is in their system. If one is, they need to determine what type of threat it is. That's difficult as many threats resemble one another, but each one can cause different problems. Companies that don't have the extensive threat intelligence that cybersecurity organizations have often lack the skill set needed to determine the exact type of threat in their system. Companies often incorrectly categorize the threat, thereby missing information about what the threat is, what type of data it's after, and what type of havoc it has already created.

When the SOC is receiving no alerts, analysts search for threat activity and try to block it upon detection. When they discover threats inside the network, analysts engage with the incident response team, Tier 2. They provide as much detailed context-rich attack data as possible to help incident responders understand the threat and dive deeper into the incident to determine if a critical system or data set has been impacted. Incident responders remediate threats and share with analysts their findings.

Responding to and resolving threats is typically the most challenging aspect of cybersecurity, and it's the area in which most businesses fall short. Most companies don't fully understand threat remediation. They may think they've removed a threat, but other traces of that threat may be hiding in another system. Or, the threat may have created a backdoor that allows easy reentry into the network. Incident response is often best handled by professional incident responders who are trained in forensics and can recommend the best ways to address the root cause of the compromise to prevent similar attacks.

At Tier 3 of the SOC are threat hunters. They possess in-depth knowledge of networks, forensics, threat hunting and malware reverse engineering. Using up-to-date threat intelligence and indicators of compromise, threat hunters are skilled at using tools to discover sophisticated threats hiding in the network undiscovered.

Rounding out the SOC team is the SOC manager, Tier 4, who manages personnel, budgets, and scheduling, as well as recruits, hires, and assesses the staff. The manager also oversees all new projects and training and is the point-person for business-critical incidents. A well-managed SOC team works together to respond in a timely manner and has a playbook that guides each role in the process handling incidents.



TIER 4

SOC MANAGER

Manages staff, budgets, scheduling, workload, and training; the point-person for business-critical incidents

TIER 3

THREAT HUNTER

Discovers sophisticated threats hiding in the network and seeks out potential threats in the deep and dark webs, hacker forums, and pastebin sites

TIER 2

INCIDENT RESPONDER

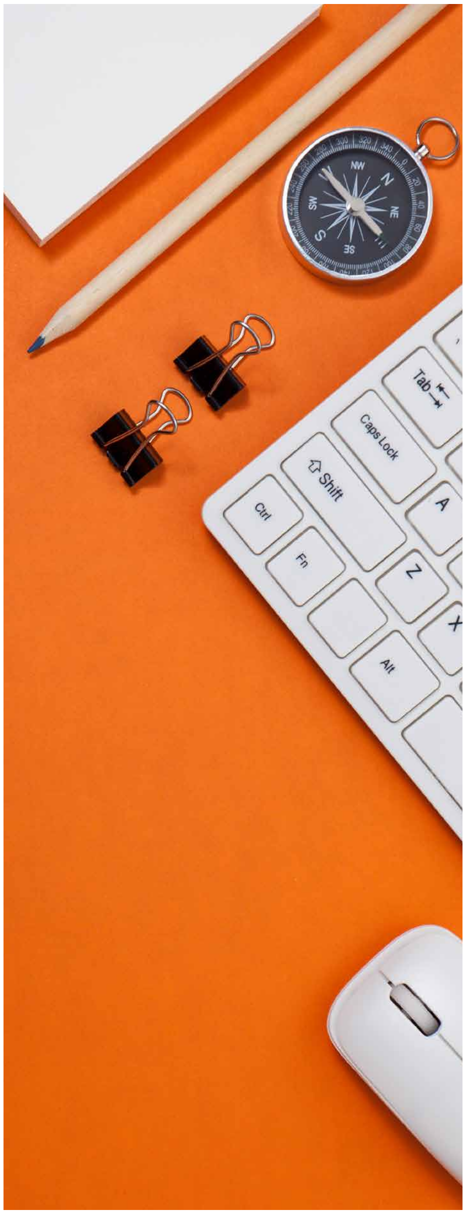
Determines if a critical system or dataset was affected; remediates threats and shares findings with analysts

TIER 1

ANALYST

Reviews logs for anomalous activities and identifies vulnerabilities in IT environments

PROCESSES



As well as having the latest intrusion detection and prevention technologies and highly skilled people, SOCs must have processes in place to make sure all steps are followed to effectively prevent, detect, and remediate breaches. In addition to conducting regular duties such as filtering emails, network traffic, and endpoints, and working with clients to review lessons learned after an incident, the SOC also should have playbooks to detect and respond to threats without disrupting the business. A standardized repeatable workflow provides guidance for handling any type of situation, including steps that must be taken to meet compliance requirements for SOX, FERPA, FISMA, PCI DSS, GDPR, and HIPAA. A SOC should be able to provide guidance in meeting each compliance standard's requirements, and should be able to provide each customer with a personalized audit-ready document, an Attestation of Compliance, to show what it has done to meet the requirements so companies don't have to waste hours customizing reports.

TECHNOLOGY

SOCs need the latest tools, which now incorporate machine learning and artificial intelligence, to prevent and remediate threats. Tons of data flow from mobile devices, workstations, routers, servers, and numerous other security technologies, but analysts can only process so much information. Machine learning can handle tasks in seconds that would take humans hours. It can also quickly detect anomalous activities. For example, it can identify events that are out of the ordinary, such as an employee based in the U.S. who appears to be logging into the network from a computer with an IP address based in China. Machine learning can also flag emails from a domain that is similar to one it is familiar with to help detect fraud. For example, it could block an email that comes from amazzon.com rather than amazon.com. Artificial Intelligence tools use machine learning to detect threats and categorize them based on their level of severity.

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

COSTS

Organizations that want to build a SOC must allocate initial and ongoing funds. Organizations planning to build a SOC should perform a cost-benefit analysis of creating a SOC to that of outsourcing one.

The national average salaries for a cyber security analyst, an incident responder, threat hunter, and a SOC manager in the U.S. are about $80,000 each. Even at the smallest of organizations, there has to be at least one security analyst in the SOC at all times. At bare minimum, a small company must hire four security analysts, one incident responder, one threat hunter, and one SOC manager, a total of seven SOC employees. That's seven multiplied by $80,000, which is $560,000 for salaries alone. The average price of a SIEM is about $50,000, and there are maintenance and support costs each year. That's $610,000, not including the price of detection tools.

Gartner says: "Building a SOC—or generally creating some form of internal security operations capabilities—is a costly and time-consuming effort that requires ongoing attention in order to be effective. Indeed, a great number of organizations (including some large organizations) choose not to have a SOC. Instead, they choose other security monitoring options, such as engaging a managed security service provider (MSSP)."

$80,000 NATIONAL AVERAGE SALARY FOR SOC EMPLOYEES

AT BARE MINIMUM, A SMALL COMPANY MUST HIRE:

1 SOC Manager

1 Incident Responder
1 Threat Hunter

4 Security Analysts

OUTSOURCING OPTIONS

When organizations outsource their SOC, it minimizes their need to buy more security products, to hire more staff, and to pay for more training. The products organizations have already invested in will be working at their optimal level because they will be managed and operated by professional cybersecurity experts 24/7. Analysts who have a thorough understanding of log outputs will review all alerts, and incident responders offer suggestions for remediation based on experience and expertise. Within a single pane of glass, customers still have visibility into and control of their entire environment and can access all policy enforcements.

Capabilities	Traditional MSSP	Security-As-A-Service
Implementation timeline (DevOps-ready)	Avg 45 days	<2 min
Threat detection and response	Alerting	99.99% threats blocked, response included
Average threat detection and elimination timeline	99 days	1 day
Visibility and threat management across on-premise, cloud, and hybrid environments	On-premise	✓
Audit-ready compliance (HIPAA, PCI, GDPR)	No	✓
Usage-based pricing	Fixed, contract	✓
Patching	Client-owned	✓

CONCLUSION

Operating a SOC is an enormous job. It needs top talent, which is hard to find and keep, and it needs to have teams that work closely with and can learn from one another. The SOC's job is to play defense every second of the day. Before investing in a SOC, companies should think about the problems they are trying to solve and consider whether they need a SOC in-house, outsourced, or some combination of the two. Some industries may need their own SOC, and some large companies may already have the office space, the budgets, and the latest tools to develop one. However, SMBs and enterprises that don't have the funds to build and develop their own SOC can still receive the utmost cybersecurity protection without purchasing, managing, and operating expensive hardware or worrying about finding, hiring, and maintaining security experts. Today, even the smallest organizations can have a fully staffed SOC 24/7/365.

ABOUT ARMOR

Armor is a global cybersecurity software company that simplifies protecting data and applications in private, public, or hybrid cloud environments. We combine workload protection, analytics from cloud-native sources, and other security data to provide unparalleled insights into threats facing organizations. Armor's cybersecurity experts monitor customer environment 24/7/365 and, if an attack takes place, help customers respond quickly and effectively. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple.

ARMOR

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167