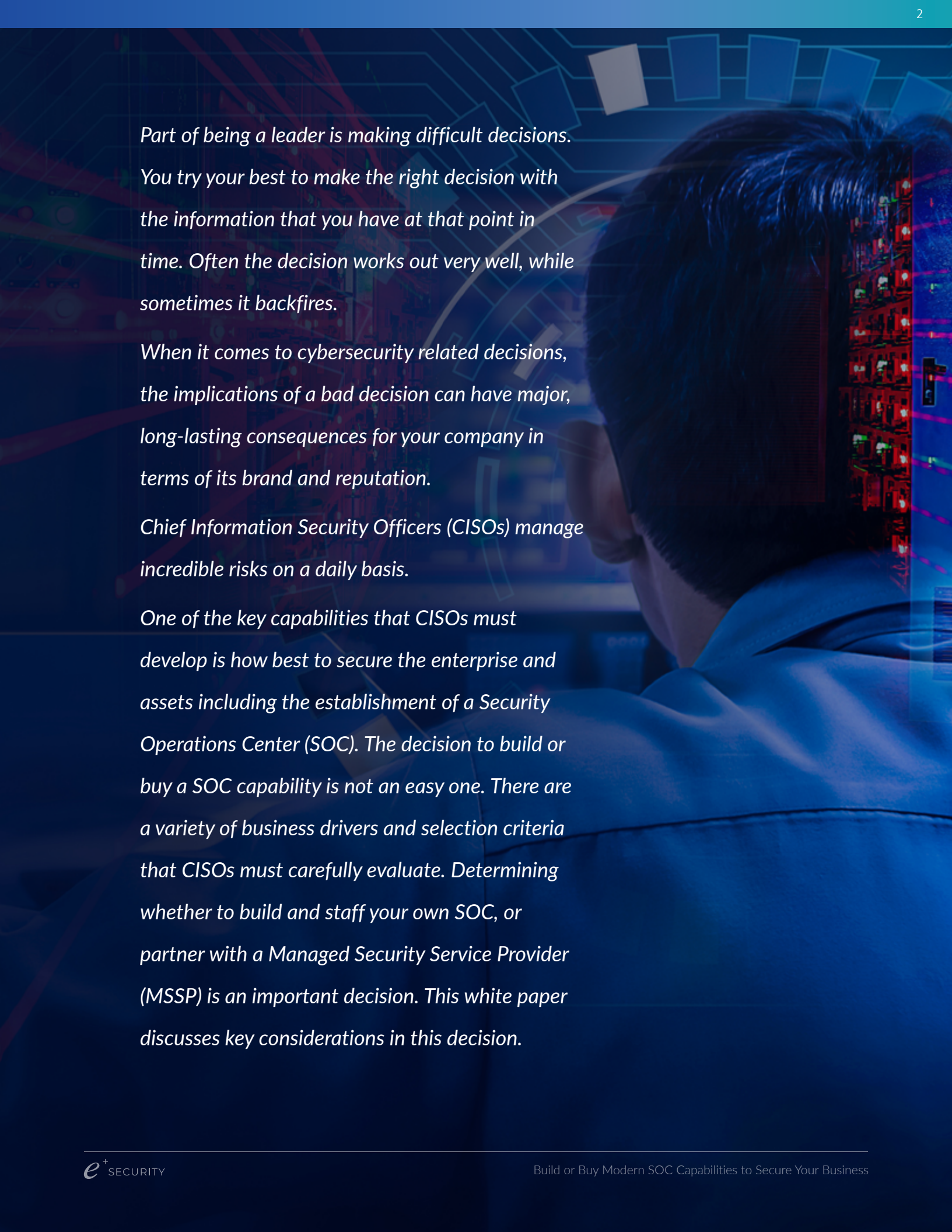
Build or Buy Modern SOC Capabilities to Secure Your Business

Where Technology Means More®



Part of being a leader is making difficult decisions. You try your best to make the right decision with the information that you have at that point in time. Often the decision works out very well, while sometimes it backfires.

When it comes to cybersecurity related decisions, the implications of a bad decision can have major, long-lasting consequences for your company in terms of its brand and reputation.

Chief Information Security Officers (CISOs) manage incredible risks on a daily basis.

One of the key capabilities that CISOs must develop is how best to secure the enterprise and assets including the establishment of a Security Operations Center (SOC). The decision to build or buy a SOC capability is not an easy one. There are a variety of business drivers and selection criteria that CISOs must carefully evaluate. Determining whether to build and staff your own SOC, or partner with a Managed Security Service Provider (MSSP) is an important decision. This white paper discusses key considerations in this decision.

Defining a Modern SOC

What is a SOC

According to Sid Deshpande, a former Gartner Analyst: "A SOC can be defined both as a team, often operating in shifts around the clock, and a facility dedicated and organized to prevent, detect, assess and respond to cybersecurity threats and incidents." More simply put, a SOC monitors an organization's environment for Indicators of Compromise (IOCs). SOC analysts monitor and validate potential malicious traffic and act to stop it before it causes harm, or if a breach has occurred, limit exposure and mitigate the threat.

A SOC also serves as a center of risk definition for the organization. Data derived from the SOC is utilized by the CISO to make risk-based decisions.

What a SOC is Not

A SOC is not a complete security program in and of itself. A SOC should not be responsible for development of security policies and programs, as these are the responsibility of the security leadership team. Though it can provide valuable insight, a SOC is not responsible for the architecture and implementation of security technology controls. Those are typically a joint effort between the security architecture and engineering team with the help of information technology resources. A SOC is not responsible for the assessment and maintenance of the organization's compliance with regulatory and industry requirements. Since the SOC generally operates many of the controls necessary to meet these requirements, an independent part of the organization is more appropriate for the assessment of the state of compliance provided through these requirements.

Further, a SOC is not focused on the same issues that a Network and IT Operations Center are: routing issues, capacity issues, uptime issues, and the like are not generally considered part of security operations.

What is a Modern SOC

A Modern SOC analyzes significant volumes of data, contextualizes and correlates this data and delivers critical insights into security logs and alerts in "real time." This cannot be done by manually reviewing the output of a Security Information and Event Management (SIEM) or log aggregation solution. A Modern SOC requires significant automation, a view of the company's security that goes beyond internal logs by incorporating knowledge of the world outside the organization's borders, and visibility into the logs generated by sources that legacy SOCs would have never ingested in the first place. Modern SOCs focus on team coordination and automation in order to handle the increased event load to be reviewed. It is our opinion that the largest jump between legacy SOCs and modern SOCs are:

Legacy

+ Events from Perimeter and Endpoint
+ Detection Technologies
+ Manual Investigation or Analysis
+ 8x5x5 Operations
+ Endpoint, Network, and Patch/Vuln separated responsibilities

Modern

+ Correlation of Events from multiple logging areas, e.g., on-premises and cloud
+ Threat Intelligence
+ Automation
+ 24x7x365 Activity
+ Monitor, Manage and Advise

Correlation of Events from Multiple Logging Areas

Security operations are built out of the collection and analysis of logs from different sources or areas. Historically these "areas" have been the perimeter and endpoint spaces. Whether it was logs from the firewalls, IDS/IPS, and/or from endpoint antivirus, these are the logs sources and areas that Security Operations Centers grew up on.

As new "areas" (External Environments) have arrived, like Public Cloud, Software as a Service, remote devices, Internet of Things, and a plethora of other sources, Security Operations has had to onboard and attempt to understand or correlate alerts from the significant increase in log volume from these sources to understand the state of an organization's security and react to incidents.

Cyber Threat Intelligence

With the significant increase in data to analyze, coupled with the ever-increasing number of threats against the organization, the SOC must use contextual knowledge to better prioritize and make decisions on the event that could be the most impactful to the business. Cyber Threat Intelligence provides valuable insight by enriching the alerts with information about both present and future attacks and threat actors. With internal sources providing information about the systems and applications and external sources providing details about attack campaigns, Cyber Threat Intelligence increases the efficacy of the SOC.

Automation

The increase in the number of detection and protection technologies in place, along with the addition of the outside perspective of Threat Intelligence, has caused a dramatic increase in the number of logs that need to be analyzed and validated by security operations teams. Coupled with the ongoing lack of security talent in the industry, we have seen a tremendous increase in the use and dependence on orchestration and automation applied to event analysis and security operations in general. Automation can be as simple as task creation and resolution, to as complex as multi-step phishing analysis, verification and system remediation.

Automation is one of those areas that gets more complex the deeper you go, but also offers greater potential value and return on time. Furthermore, automated workflows and responses, and the skill sets required to continuously build and improve them, have become a foundational requirement to delivering a modern SOC of ever-increasing maturity.

24/7/365 Activity

This one is simple. Attackers don't work 9 to 5. They don't take off weekends, and they may not celebrate the same holidays that you or your company does. In reality, those are often the times when most attacks occur. Monitoring needs to not only be consistent in eyes on glass, but the eyes on glass need to be of equal caliber across the hours of the day. Long gone are the days of the Senior Analysts answering the once-in-a-blue-moon ring of the afterhours on-call phone.

Monitor, Manage, and Advise

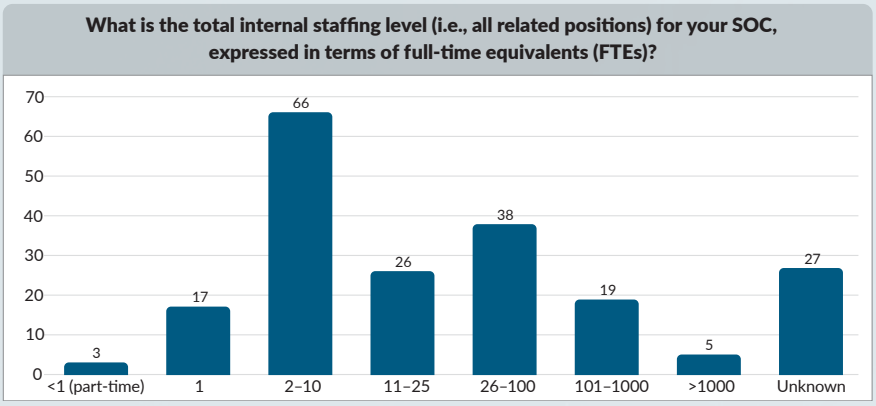
Security operations have matured and specialized over the years. Security operations traditionally are based around a tiered model of Tier 1, Tier 2, and Tier 3. These tiers are based not only on specialization of differing tools or detection/protection types, but also from experience and oversight capabilities. Tier 1 and Tier 2 are generally focused on the traditional security environment of Firewalls (Perimeter), Endpoints (User Land), and Infrastructure (DMZ or Server Land). Tier 3 is usually the team lead and is focused on the forensics and incident resolution capabilities. Think of it like this: Tier1 sees it, Tier 2 validates it, Tier 3 attempts to fix it.

The average SOC has 75 security tools to manage. They are almost constantly in the midst of at least one technology change or major upgrade. The sheer number of events, along with the project management of a roll out, can overwhelm even well performing SOCs; meaning they don't have the time to get in front of event analysis, or time to make anything other than reaction-based changes to the tool they monitor and manage.

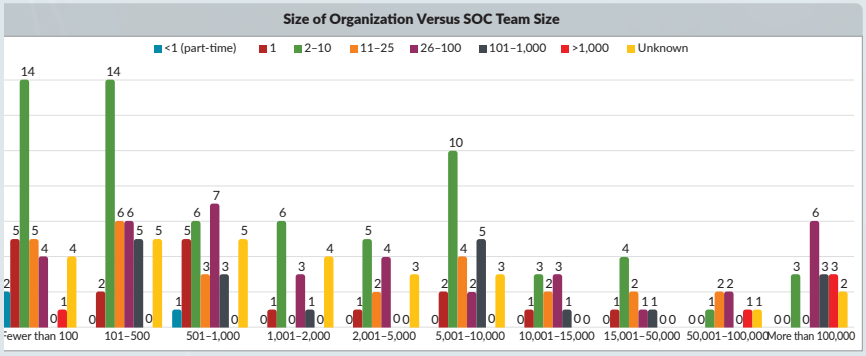
A modern SOC takes advantage of differing correlation and automation techniques and technology to reduce manual analysis and get more time on the clock. This time allows for a modern SOC to more accurately schedule the eyes on glass they need, with the appropriate Tiers of users to keep the analysis assembly line moving. The modern SOC isn't only focused on handling the event load in an accurate manner, but also in partnering with other operating groups to make suggestions on managing security tangential technologies, or advising in appropriate next steps for resolution, remediation or mitigation.

SOCs by the Numbers

A recent SANS study can be used to put some numbers together on the difference between traditional and modern Security Operations Groups. A minimal 24x7x365 Modern Security Operations Group employs Analysts, SIEM/ Network/ Forensics Engineers, Threat Hunters, Project Managers and Leadership. Viable staffing for this availability and capabilities requires a headcount of 14-20 individuals. These estimates include the need for addressing coverage in each role as employees take time away from work. SANS numbers suggest that Modern Security Operations are not the standard across the industry. Research suggests that most companies do not attain this level of staffing, nor are they able to provide true 24x7x365 coverage internally. According to the SANS Institute 2022 SOC Survey, the typical SOC today usually employs two to ten analysts, with more respondents in the SANS study reporting their staffing levels in this range (please see graphic), scaled by organizational size.



As found in the SANS surveys of previous years, organizations with between 10,000 to 15,000 employees generally run a SOC with 6 to 10 employees; organizations from 15,001 employees up to 100,000 employees put together SOC teams of approximately 11-25 analysts; and very large enterprises with over 100,000 employees stand up SOCs with 26 to 100 analysts.



Two other factors to consider when working on the numbers for Security Operations Groups are the Compliance and audit requirements the company is operating under and the current cybersecurity talent and skills gap. There have been volumes written around the gap and the current focus on getting more people into the field, but the thing that has been missing from the discussion is the location of these people. Security Operations Center staffing issues can be exacerbated by the location and the amount of local talent available, especially with the push by many organizations to return to corporate offices. Compliance requirements add more complexity to hiring and staffing numbers in regulated industries. Security mandates can vary based on the industry sector. Retail businesses need to meet PCI DSS, for example. Healthcare providers must comply with the Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements; publicly traded companies must comply with Sarbanes-Oxley (SOX) constraints; and Financial Institutions must adhere to FFIEC regulations. Staffing a knowledgeable team to meet and keep up with the requirements of these mandates can be challenging.

Build or Buy?

In order to acquire Modern Security Operations capabilities, customers can choose to either build from scratch or upgrade/update existing Security Operation Groups. Another option is to Buy Modern Security Operations from an MSSP (Managed Security Services Provider).

Build

If the goal is to operate or build a Modern Security Operations Group let's start with some of the requirements around operational needs.

People

+ Recruiting
+ Education
  - Prepare, plan, design, implement, operate, and optimize technology stacks
  - Security Analysts
  - Threat Hunters
  - Continuing Education
+ Burnout

Process

+ Runbooks
+ Threat Hunting
+ Incident Response
+ Consumption of Threat Intelligence Feeds
+ Participation and contribution to security communities
+ Use Cases

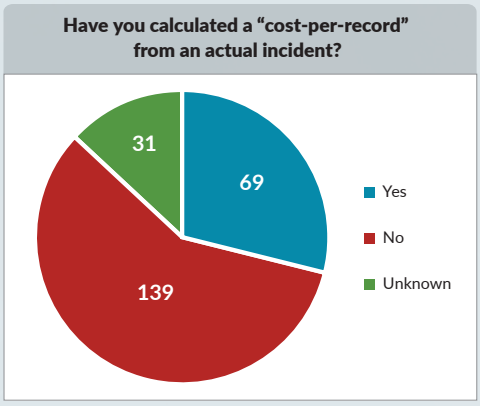
With Those Requirements in Mind, What Might it Cost to Procure the Technology, People, Training?

FTE Function	**Annual (avg)**
Analyst Internal cybersecurity analyst resource capable of investigating and validating notable events	**$100,000**
Engineer Internal cybersecurity engineering resource capable ofconfiguring log sources and setting up and maintaining an advanced SIEM	**$150,000**
Team Implementing a SIEM and staffing a 24x7 SOC with cybersecurity talent resources for single-depth, non-redundant resources	**>$1,000,000**

Technology

+ Security Platform
  - Security Incident and Event Management (SIEM)
  - Security Orchestration Automation and Response (SOAR)
  - Extended Detection and Response (XDR)
  - IT Service Management (ITSM)
+ Border Security
  - Firewalls
  - Proxy
  - Web Application Firewalls
  - Mail Gateways
  - ...any other traditional perimeter-based security controls that all need to be logged for visibility and correlation into the SIEM
+ User/Data Security
  - Endpoint
  - HID/HIPS
  - Anti-Virus
  - Endpoint Detection and Response (EDR)
  - Data Loss Prevention (DLP)
  - Whitelisting
  - Identity and Access Management (IAM), Privileged Access Management (PAM)
  - Multi-Factor Authentication (MFA)
+ Cloud Security
  - Cloud Access Security Broker (CASB)
  - Email
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SSPM)
+ Other Sources of Telemetry
  - Threat Intelligence Platform
  - Dark Web Monitoring
  - Digital Risk Protection Services (DRPS)
  - External Attack Surface Management (EASM)

If you note the table on the previous page is looking strictly at the people cost of Modern 24x7x365 Security Operations. Security Tooling, support, updates, and Intelligence sources and training costs have not calculated into the greater than 1 million per year number. So now a Security Operations Group has been built out. Your company has acquired, implemented the necessary technologies and trained the hired analysts in their capabilities while acquiring or writing out the company's playbooks or runbooks to make sure that the analysis process and false positive vs true positive identification. The next step in building out a Security Operations Group is to determine how to make things better, or how to further refine your Modern Security Operations.



"To gain management support for resources, SOC managers need to move beyond quantity-based metrics — how many raindrops hit the roof — to business-relevant metrics — zero production downtime due to rain getting through the roof," SANS concludes. Currently, the number one used metric to track and report SOC performance is the number of incidents handled. Only a very slim number of SOCs track monetary cost per incident or losses accrued versus losses prevented. As we see in the graph below, a supporting metric of assigning cost per record is still not done by the majority of respondents.

Managing Burnout

A June 2022 Trellix report cited several challenges leading to employee burnout including:

+ Limited support for skills development
+ Lack of recognition
+ Unclear career paths
+ Diversity
+ Pay gaps

The report went on to state "85% of respondents believe the workforce shortage is impacting their organization's abilities to secure increasingly complex information systems and networks, while almost a third (30%) of the current workforce plans to change professions in the future."

For those desiring to build and operate their own modern SOC, it's important to ensure plans are in-place to address these challenges. Those planning to buy modern SOC capabilities via outsourcing should seek to understand the staffing and automation strategies as part of their vendor due diligence. The skills shortage and exodus are significant global challenges that won't be addressed by simply competing for resources in the market, or offshoring.

Buy

A major reason that companies look to Buy into Managed Security Services (MSS) is to see the benefit of tooling, training, and common experience with the rest of the partner's customer base or that partner's specific capabilities.

MSSPs purchase, deploy and manage leading technologies for their customers. In other words, MSSP customers utilize leading technologies for a fraction of the cost. Therefore, an MSSP has access to best-of-breed technologies and thus is able to continuously enhance its technology platform. The costs for these tools are spread across clients, at a negligible cost to each.

Though MSSPs and the associated capabilities can vary, benefits may include:

+ Standardized technology stack including SIEM, SOAR/XDR, PSA/ITSM, RMM, etc.
+ Integrating with and/or supporting a client's technology stack
+ Capabilities to deliver technology integration between provider's tech stack, border user, data, and cloud security combined with additional sources of telemetry.
+ Transferring responsibility for hiring, retaining, training, etc. of personnel to the provider.
+ Integrating provider's processes and workflows with client's

Threat Analysis, Malware and Forensics, and Threat Intelligence are Modern Security Operations standards, but are some of the most expensive and complex capabilities to do well. These actions are challenging because they require coordination across the different tiers of analysis and a personalized understanding of the context around an event to be analyzed. Generally, a purchased MSS offering of traditional or Modern Security Operations does not have the time, resources or capabilities to offer personalized and effective advanced services for their customers due to scale, cost and time constraints.

It's important to note, a modern MSSP offering MDR capabilities either directly or through partnerships with an MDR provider is different from legacy MSSPs. The difference is found in the amount of connection between the partner and your team and awareness brought to your company's unique needs, events, and expectations.

Partnering with a modern MSSP can help achieve these goals by providing:

Cost savings:

24x7x365 coverage at a fraction of the cost of hiring internal cybersecurity staff, and eliminating the need for large, frequent capital expenditures and licensing costs. Responsiveness and performance metrics defined in a service level agreement ensures your needs are met and you are getting what you are paying for.

A stronger focus on the core business:

Building the internal capabilities to address challenges like dark web monitoring and advanced threat detection can sap resources from core business operations in terms of attention and budget.

Enhanced protection:

Internal teams can get overwhelmed by the noise of actions and incidents, reaching a point of ignoring alerts because they feel they are false positives or don't provide actionable intelligence. A modern MSSP can incorporate machine learning and artificial intelligence to address "noise" issues and synthesize appropriate responses. An modern MSSP uses not only Machine Learning and Automation to reduce noise but also utilizes a deep familiarization with the customer's environment and needs to truly tailor the when and who to communicate with on your team, but to also provide potential next steps or remediation actions based on communal understanding of the environment.

Access to a deep bench of experts:

With capabilities to align with industry-specific standard compliance, a modern MSSP can provide specific responses to address a client's specific risks, challenges, and threats, while helping maximize internal staff resources through ongoing communication. A true MSSP partner will look to provide consistency in contacts between analysts and customers, fostering familiarization and collaborative processes that build trust and expedite responses.
Access to a repository of security use cases: Use cases inform detection and rapid responses with a library of threat detection signatures, risky authentication behavior searches, automated response workflows, anomalous network activity, and other situations that may be unfamiliar to an internal security team.

Access to advanced technology:

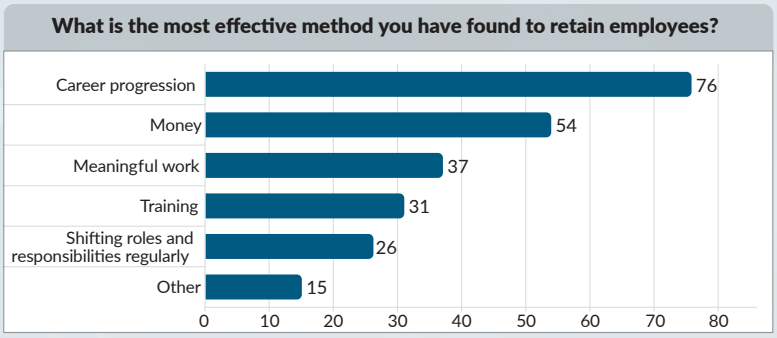
Modern MSSPs have the resources and capability to build tailored, scalable solutions to match clients' needs, while integrating, as needed, technologies that clients currently use. The solutions are service-oriented, thus geared to a specific solution rather than selling a particular technology, and with the ability to communicate across platforms. Modern MSSPs have the ability to not just bring additional resources to bear, but to also tailor these advanced capabilities for the greatest results and effectiveness for their customers.

Benchmarking security operations through a maturity model:

Providing an objective scoring index helps assess the customer's security operational capabilities and yields metrics that are useful to board and auditors in measuring and upgrading security systems and resources.

Efficiencies:

Higher levels of productivity and performance are achieved through a collaborative managed security service, with responsibility for crucial tasks that include threat monitoring and proactive threat hunting, while paring back notable events from thousands down to an average of 4-5 events per day through a rigorous validation process, saving clients many hours, and enabling clients to redirect staff previously performing monitoring and validation activities to undertake other essential tasks within an organization.



As previously mentioned, those planning to buy modern SOC capabilities via outsourcing should seek to understand the staffing and automation strategies as part of their vendor due diligence. Considering the realities in the security talent pool, only exacerbated by the great resignation, if your provider doesn't have a plan beyond the conventional approach of competing in the market for skilled resources...all you've given up is control and will still feel the pain of the skills shortage. Discussion points on methods which the providers' retention plans should include can be seen in the graph below from the SANS Survey.

It's equally important to bear in mind you can outsource responsibility, but you can't outsource accountability. Though you and your organization may or may not be subject to regulatory compliance, you are accountable to the organization and the organization is accountable to shareholders, customers, and the court of public opinion; regardless of whether or not it was outsourced.

+ Clearly define expectations including:
  - SLAs
  - Roles and Responsibilities (RACI Matrix)
  - Escalations
+ Review and coordinate often, not just during QBRs

Build and Buy: a Hybrid SOC

Does establishing a modern SOC have to be a binary choice between Build or Buy? Could you build some and buy the rest?

Building a modern SOC could be addressed employing a hybrid solution. Often success is found assessing current capabilities, determining what can be achieved within your organization with minimal effort, and opting to outsource other aspects in the near-term. This approach allows organizations to determine which of the more complex capabilities they wish to bring in-house at a later date and with more knowledge.

Organizations taking this approach should consider what portion of the provider's tech stack, if any, is transferable to the organization; entire images, configurations, and the like are all important considerations. The same applies to the provider's processes and knowledge. That's not to say if they won't transfer some or all of it, they're not worthy of consideration but rather ensuring you're making today's decisions with an eye to potential future considerations.

In Closing

None of us can know it all. Good leaders know their limits and plus their efforts by surrounding themselves with those that can bridge the knowledge gaps. Work with your trusted advisors to determine what makes the most sense for your organization. If you have any questions or wish to discuss further with a member of our team, we're happy to assist.

About ePlus Security

Backed by extensive certifications and accreditations, an unparalleled bench of technical experts, top industry recognition, and a relentless commitment to innovation on behalf of everyone we serve, ePlus Security offers a comprehensive suite of consulting, advisory and managed security services that provide organizations across every industry with a turnkey approach to mitigating risks, identifying and remediating threats, and building foundationally strong security programs that help prevent and protect all of their important assets, from networks and data to devices and people.

With an independent approach and an unparalleled depth of knowledge stemming from decades of experience helping leading organizations defend against and recover from an increasingly sophisticated attack landscape, ePlus provides tailored, full lifecycle security solutions, spanning strategy and design through to implementation, support, and ongoing management.

If you would like to learn more about how ePlus and Deepwatch can help secure your network, please visit www.eplus.com/gobeyond or reach out to us at security@eplus.com