Intelligent Security Operations: A Staffing Guide
Table of Contents

Introduction ................................................................. 1
Staffing Considerations ................................................... 1
SOC Roles and Responsibilities .......................................... 2
SIEM Content Authors or Engineers ................................. 5
Hunting ................................................................. 8
Other Roles ............................................................. 10
Metrics ................................................................. 12
Automation ............................................................. 13
Staffing Models ......................................................... 14
Scheduling ............................................................. 17
Roadmap for Growth ................................................... 19
Summary ............................................................... 21
About Micro Focus Security ........................................... 21
Micro Focus Security Products Services ............................ 21
Introduction

The number one issue facing security operations organizations is finding the resources needed to run the business. Often, optimal staffing is not achievable. As an organization tackles the challenge of building a security operations center (SOC), one of the important questions that arises is, “what does it take to staff a SOC?” Other questions, such as, “how to get started?”; “how to prioritize?”; and “how to utilize resources?”, will come into play. The ability to utilize resources effectively helps to facilitate a smooth startup and allows for service build-out and maturation over time.

Building a security operations center from scratch can be a daunting task for organizations that do not have a security intelligence capability. Fortunately, organizations can start with just a few security experts and one-third of the total investment to build the foundation of a SOC. This paper covers the ingredients needed to succeed with security operations: prioritized tactics and metrics to strategically track effectiveness.

Staffing Considerations

For organizations attempting to build a security operations center for the first time, or those expanding their SOC’s capability or coverage, staffing the right people is arguably the most critical aspect of the people, process, or technology puzzle. Hiring experienced analysts from the marketplace presents a number of challenges, especially for a new organization that has not yet established a positive operational culture and established processes.

There is a broad disparity in the quality of existing SOCs in the marketplace. While analysts coming from existing SOCs arrive with valuable experiences, they also come with baggage. If you build a full team of these individuals, the result is often conflict and inconsistency. While being a security operations analyst can be an exciting and flexible role, there is a need for operational consistency and predictability, otherwise, it can wreak havoc on the performance of the SOC. Also, experienced analysts in the market are seeking career progression and are not interested in another level 1 analyst role. Since we know organizations are working very hard to keep their top-performing analysts, there is a chance that those with SOC experience who are actively seeking level 1 security analyst roles are not the top performers on their team.

One question that is often asked by organizations attempting to build a SOC for the first time is how to get started. If you are building a security operations capability from ground zero and have the budget to fill exactly three SOC roles, the pressing question is which roles should they be? Micro Focus recommends focusing on the following areas of expertise:

- SOC manager—expertise in strategic planning, prioritization, accountability, and internal working relationships
Security analyst—expertise in operations, process, threat intelligence, incident response, vendor management, and more

Security information and event management (SIEM) content author or engineer—expertise in SIEM administration, content development, security device engineering, incident response, vendor management, and more

With three people, it would be possible to establish an 8x5 security operations center, but this would require considerable automation and meaningful metrics (which requires significant up-front effort). It could also mean enlisting the help of a third-party niche provider (staff augmentation or subscription-based solution) or managed security service provider. When building a new security program, the more effort dedicated in the beginning to design it well and make it sustainable, the less effort that is needed to demonstrate ROI and receive more backing—specialization and expansion become options.

SOC Roles and Responsibilities

There should be a clear definition of roles and responsibilities within a SOC and governance to hold individuals accountable for those responsibilities. Security issues can become catastrophic when individuals assume that a task is someone else’s responsibility. The most painful after action reviews (AAR) of security breaches often point back to failures in common understanding, ownership, and performance of roles and responsibilities for tasks associated with the incident. In order to address these gaps cyber defense leaders should document the roles and responsibilities of all stakeholders involved in the investigation and response processes of a security incident. These playbooks enumerate the tasks for each role.

Management

Establishing effective leadership is a top priority for building intelligent security operations. Leadership begins with the SOC manager. The manager is responsible for achieving the goals of the SOC program through the implementation of processes, procedures, and performance indicators related to security incidents and prevention management.
The SOC manager will take ownership of the SOC and be responsible for maintaining smooth operations, ensuring service-level agreements (SLAs) are met, and following policies and procedures. Additionally, the SOC manager will:

- Manage the overall day-to-day operations. They are responsible for ensuring events and/or incidents are detected and responded to in adherence to established process as well as procedures.
- Oversee the analysts’ daily tasking.
- Manage the team’s scheduling.
- Ensure effective incident management.
- Identify chronic operational and security issues, and ensure they are managed appropriately.
- Manage and escalate roadblocks that may jeopardize security monitoring operations, infrastructure, and SLAs.
- Serve as a senior mentor to SOC staff.
- Interface and collaborate with outside teams.
- Track tactical issues in execution of SOC responsibilities.
- Document and track analyst training requirements.
- Ensure analysts follow existing procedures and all procedures are documented in accordance with local guidelines.
- Manage the process improvement program for SOC processes.
- Serve as an incident manager for the SOC, along with other responsibilities.

**Level 1 Security Analysts**

A level 1 analyst executes operations procedures as a matter of daily responsibility. The role of a SOC analyst is the detailed and repeatable execution of all operational tasks as documented in processes and subordinate procedures. Specifically, the level 1 analyst will be responsible for monitoring the SOC situational awareness and automation systems for security events and closing or escalating those events as necessary. Level 1 analysts will maintain the group email address and distribution lists, answer SOC main phone lines, and update all relevant documentation such as shift logs and tickets.

Specifically the SOC level 1 analyst will identify, categorize, prioritize, and investigate events rapidly utilizing triage and response guidelines for the enterprise using commonly available SOC log sources that include:

- Firewalls and network devices
- Infrastructure server and end-user systems
- Threat intelligence platforms
- Web proxies
- Application logs and web-application firewalls
- Identity and access management systems
- Cloud and hybrid-IT provisioning, access, and infrastructure systems
- Antivirus systems
Intrusion detection and prevention systems
- Monitor incoming event queues for potential security incidents using the Micro Focus® Security ArcSight Enterprise Security Management (ESM) tool per operational procedures.
- Perform initial investigation and triage of potential incidents, and escalate or close events as applicable.
- Monitor SOC ticket (or email) queue for potential event reporting from outside entities and individual users.
- Maintain SOC shift logs with relevant activity from the shift.
- Document investigation results, ensuring relevant details are passed to tier 2 for final event analysis.
- Update or reference SOC collaboration tool as necessary for changes to SOC process and procedure as well as ingest SOC daily intelligence reports and previous shift logs.
- Conduct security research and intelligence gathering on emerging threats and exploits.
- Perform additional auxiliary responsibilities as outlined in the console monitoring procedure.

Level 2 Security Analysts
Level 2 security analysts own the successful completion of all procedures executed during their presence in the SOC. The level 2 analysts own the documentation and measurement of all subordinate procedures as well as the continual improvements to them. They are also responsible for the execution of the information fusion procedure, where various data inputs are fed to both operations and engineering to automate detection of new indicators and to filter out conditions that are not actionable for their organizations.

These senior analysts will gather information, collate it into an accessible format, and ensure its full dissemination. Level 2 analysts are responsible for the subtle event process—long-term analysis and deep dive investigation into network activity.

Specifically, the level 2 analyst will:
- Monitor level 1 analyst performance by investigating incoming events using SOC-available tools.
- Ensure level 1 event(s) are addressed in a timely manner using available reporting and metrics.
- Approve and, if necessary, further investigate level 1-escalated events.
- Mentor level 1 analysts to improve detection capability within the SOC.
- Manage SOC event and information intake to include gathering intelligence reports, monitoring ticket queues, investigating reported incidents, and interacting with other security and network groups as necessary.
- Serve as detection authority for initial incident declaration.
- Function as shift subject-matter experts (SMEs) on incident detection and analysis techniques, providing guidance to junior analysts and making recommendations to organizational managers.
- Drive and monitor shift-related metrics processes ensuring applicable reporting is gathered and disseminated per SOC requirements.
- Conduct security research and intelligence gathering on emerging threats and exploits.
- Serve as a backup analyst for any potential coverage gaps to ensure business continuity.
SIEM Content Authors or Engineers

ArcSight is an established SIEM product that automates the detection of emerging security threats at leading SOCs worldwide. An ArcSight SIEM Engineer is primarily responsible for infrastructure deployment and upkeep and content development. The ArcSight SIEM scope of responsibilities includes all administration, management, configuration, testing, and integration tasks related to the ArcSight system, focusing primarily on content development to include reports, dashboards, real-time rules, filters, and active channels.

Specifically, the ArcSight Engineer will:
- Develop, implement, and execute the standard procedures for the administration, backup, disaster recovery, and operation of the ArcSight systems infrastructure, including:
  - Operating system security hardening
  - Backup management
  - Capacity planning
  - Change management
  - Version or patch management
  - Lifecycle upgrade management
- Develop and maintain the technical architecture of the ArcSight system, enabling all the components to perform as expected and meeting established service-level objectives for system uptime.
- Perform routine equipment checks and preventative maintenance.
- Maintain up-to-date documentation of designs or configurations.
- Respond to after hours (on-call support) infrastructure issues as required.
- Be responsible for new product release management, policy and integration testing, security testing, and vendor management.
- Maintain hardware or software revisions, ArcSight content, security patches, hardening, and documentation.
- Develop and deploy content for the ArcSight infrastructure, including use cases for dashboards, active channels, reports, rules, filters, trends, and active lists.
- Monitor and help optimize data flow using aggregation, filters, and use cases to improve the SOC monitoring and response capabilities.
- Coordinate and conduct event collection, log management, event management, compliance automation, and identity monitoring activities.
- Respond to day-to-day security change requests related to ArcSight operations.
- Perform collateral duties and responsibilities as a backup to the security engineering role.

Incident Handlers
The SOC incident response manager (SOC IRM) is responsible for achieving the goals of the SOC security incident management program through the implementation of processes, procedures, and performance indicators related to security incident and prevention management. The IRM will work with senior management
to ensure that emergency response and crisis management plans and procedures are tested for viability, and to ensure that plan currency is maintained based upon lessons learned as well as business requirements. The IRM is responsible for handling incident escalations from the SOC to the respective business units and managing incidents throughout the incident lifecycle. The IRM will direct forensics analysis on systems and ensure root cause and resolution for metrics, tracking, and lessons learned are compiled, documented, and disseminated. Additional responsibilities include:

- Interfacing with senior management, activating the incident management team, establishing communications with appropriate team members and business units, providing status updates.
- Reporting, tracking, monitoring, and closing out incident response issues.
- Interacting with internal business units to address incidents and support investigations.
- Being the focal point for critical security events and incidents. The IRM will serve as an SME while providing recommendations and guidance to the respective business units and to the SOC lead for escalation and remediation.
- Handling, responding, and documenting all events or incidents that require escalation from level 2 or level 1 analysts.
- Analyzing and reviewing escalated cases until closure. This includes investigating and recommending appropriate corrective actions for data security incidents, which includes communicating with the implementation staff.
- Establishing and maintaining a mature incident management program.
- Leading efforts in monitoring, reporting, and responding to information security incidents. Based upon external threat indicators, industry trends, and lessons learned, the IRM recommends controls and process improvements.
- Being responsible for facilitating incident management team exercises and events.

Security Engineers
A security engineer is primarily responsible for the security infrastructure such as firewalls, anti-virus, intrusion detection or prevention, and other technologies. The infrastructure scope of responsibilities includes architecture and system performance of the respective infrastructure applications. The engineer performs all development, management, and configuration tasks related to the respective infrastructure system. The security engineer’s scope of responsibilities also includes all administration, management, configuration, testing, and integration.

Specifically, the security engineer will:

- Develop, implement, and execute the standard procedures for the administration, backup, disaster recovery, and operation of the systems infrastructure, including:
  - Operating system security hardening
  - Backup management
  - Capacity planning
The incident response manager is responsible for handling incident escalations from the SOC to the respective business units and managing incidents throughout the incident lifecycle.

- Change management
- Version and patch management
- Lifecycle upgrade management

- Develop and maintain the technical architecture of the infrastructure systems, along with ensuring all components perform as expected to meet established service-level objectives for system uptime.
- Perform routine equipment checks and preventative maintenance.
- Create and maintain up-to-date documentation of designs and configurations.
- Be responsible for new product release management, policy and integration testing, security testing, and vendor management.
- Maintain hardware or software revisions, applicable content, security patches, hardening, and documentation.
- Deploy content (policies, signatures, or rules) for the security infrastructure.
- Coordinate and conduct event collection, log management, event management, and compliance automation.
- Respond to day-to-day security change requests related to security operations.
- Act on after hours (on-call support) infrastructure issues as required.
- Perform collateral duties and responsibilities as a backup to the ArcSight SIEM engineering role.

Forensic Investigator

The forensic investigator is responsible for the development and maturity of the forensic and investigations program. The forensic investigator performs a variety of highly technical analyses and procedures dealing with the collection, processing, preservation, and presentation of computer-related evidence.

The forensic investigators examine malicious code (malware), attack vectors, and network communication methods, as well as analyze against target systems and networks. They also determine target network capabilities and vulnerabilities; support development and maintenance of new tools and techniques to exploit specific targets; and produce technical, after-action reports in support of the SOC.

Additional responsibilities include:

- Conducting forensic analysis of systems and ensuring root cause and resolution for metrics, tracking and lessons learned are compiled, documented, and disseminated.
- Using forensic tools and investigative methods to find specific electronic data, including internet use history, processing documents, images, and other files.
- Disseminating and reporting cyber-related activities, conducting vulnerability analyses, conducting risk management of computer systems, and recovering information from computers and data storage devices.
- Analyzing and reviewing escalated cases until closure. This includes investigating and recommending appropriate corrective actions for data security incidents, which includes communicating with the implementation staff.
Performing postmortem analysis on logs, traffic flows, and other activities to identify malicious activity.

Researching, developing, and keeping abreast of testing tools, techniques, and process improvements in support of security event detection and incident response.

Reverse engineering and analyzing binaries, files, and other malicious attack artifacts.

Establishing, maintaining, and ensuring complete chain of custody of forensic evidence.

Recovering and examining data from computers and other electronic storage devices in order to use the data as evidence in criminal prosecutions.

Dismantling and rebuilding the system in order to recover lost data, when a device is damaged.

Detailing how the computer evidence was discovered and all of the steps taken during the retrieval process.

Giving testimony in court regarding the evidence the analyst collected. The analyst keeps current on new methodologies and forensic technology and trains law enforcement officers on proper procedure with regard to computer evidence.

Contributing to the design and development of innovative research projects, as well as attending and participating in professional conferences to stay abreast of new trends and innovations in the field of information systems and cyber security.

Being proficient in the latest forensic response and reverse engineering skills, along with astute interest in the latest exploit methodologies.

Providing significant input into the design and development of the business groups working on information security systems operations. Maintaining strategy and methodology to comply with the organization’s cyber security standards and mission.

Hunt Analyst

While hunting can be considered the main job for a member of a hunting team, the reality is a hunt analyst has to perform many different roles and tasks. This section will describe a few of these roles and provide some tips and tricks for each role when applicable.

Note: Depending on how mature or developed a hunting program is, dedicated personnel instead of the team as a whole can perform some of these jobs.

Hunting

This goes without saying, the hunt analyst needs to be able to hunt. Most of a hunt analyst’s time will revolve around designing queries, models, and hypotheses to identify anomalies and find evidence of compromise, intrusions, and malicious activity on the network. Hunt analysts are focused on detecting new threats, vulnerabilities, and potential weaknesses.
Hunt analysts primarily use manual methods and techniques for threat detection that lead to additional intelligence, more precise filtering, and automated detection of suspicious conditions and risks to business assets. A hunt starts with some form of cyber threat intelligence or internal awareness as a basis for the formation of a hypothesis. This hypothesis is an educated guess based on prior knowledge and observation that the hunt tests or validates by collecting and analyzing the necessary data.

Many skill sets compliment hunt operations. Matching individual talents to the hunting process allows for more specialized concentrations. It's difficult or impossible to find individuals that carry complete security knowledge in every domain and analysts always have a work preference.

Larger enterprise operations have the capability to fill the specialized hunting roles. For example, the team could consist of intelligence analysts, network security analysts, data scientists, and incident responders. The hunt incident responder could also be a shared resource with Computer Security Incident Response Team (CSIRT) to help bridge the gap in joint remediation efforts. It is important that the entire team has full transparency on all hunts from start to finish. Formal channels should exist for feedback loops and lessons learned, which enable continuous improvement.

Skills to look for in a hunter include:
- Core business knowledge.
- Security analysis (networking devices and operating systems, endpoint analysis, network attacks).
- Content engineering.
- Analytical models and paradigms.
- Data science basics.
- Forensics and incident response (general incident handling, breach frameworks, malware analysis, tools and techniques, memory analysis, and forensic tools).

Data Management
Hunting involves large amounts of data, and that data needs to be managed. Management can include schema management (the names of the tables and the names of the columns), size management or retention, and format or storage management (compression algorithms, data formats such as TSV or CSV, and others).

Data Source Management or Extract, Transform, and Load Development
Many data sources used for hunting come from external sources or people (networking devices, systems administrators, and more). It is highly recommended that this data be accepted “as-is” and no extra conditions be placed on the data source owner. Accepting data sources in this manner places the burden of data transformation and loading on the hunting team, which is where it belongs. Data will often have to be transformed or altered before it is loaded into a data warehouse.
Research
Hunting relies heavily on knowledge of current and emerging threats. Hunt analysts are expected to be able to design queries and models that can detect new threats. Hunt analysts must remain up to date on the latest information security news, the newest vulnerabilities, and on how to detect them.

Other Roles

Security Data Scientist
This role supports the security intelligence needs of the security operations center (SOC) to collaborate with hunt analysts to explore indicators of threat within security data lakes, build algorithms for threat detection, and provide a variety of business intelligence reporting based on SOC and enterprise needs.

Vendor Liaison
This role performs operational vendor management from a real-time security perspective interacting with all vendors including cloud providers. Risks to the business have become so dispersed that it has become necessary to have a person whose job is to work with the vendors to make sure they are providing the required controls. They should also make sure the service level is provided as contracted. The person filling this role will require expertise in governance, investigation, and incident response and must be able to work incidents and investigations for environments they don’t own. This is an expanding role as businesses grow and take on more vendor as well as third-party relationships.

Watch Officer (Public Sector Only)
The watch officer manages, motivates, develops, and supports the security operations team. The officer may also manage the incident response team. Responsibilities include overseeing the development and maintenance of standard operating procedures (SOPs) for the SOC.

The watch officer also ensures staffing coverage in each shift, coordinates escalation for security issues, as well as oversees technology implementation, automation, and maintenance of monitoring and administrative tools. The officer is responsible for tracking key metrics such as performance indicators and security-level agreements, along with accountability for the overall performance of the departmental staff. This includes the development of goals and objectives, recruitment of qualified personnel, standardized training, and performance evaluations.

The other responsibilities of a watch officer are to:

- Provide strategic advisement to the government as the security operations SME.
- Develop and maintain SIEM or SOC leading practices and expertise.
Be responsible for the successful delivery of the SOC operations from a day-to-day tasking perspective.

Complete all tactical security intelligence tasks associated with the people and process aspects of this engagement.

Lead the effort and work to identify, document, and test processes and procedures required for security intelligence.

Maintain appropriate communication with all involved parties to include regular status updates.

Contribute to ESM content (rules, reports, and such) and be the primary contact for review of existing use cases and new use case development.

Provide project management and strategic oversight to the SOC and engineering resources for onboarding new Lines of Business (LoBs).

Manage resource schedule to meet coverage requirements and budget.

Improve performance and effectiveness of SOC resources management.

Boost risks, issues, and decisions management.

Work with LoBs to assess the impact and authorize changes in scope and mission of the SOC.

Act as escalation management for all SOC related issues.

---

**Figure 2. SOC roles**

<table>
<thead>
<tr>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
</tr>
<tr>
<td>Level 1 analyst (L1)</td>
</tr>
<tr>
<td>Level 2 analyst (L2)</td>
</tr>
<tr>
<td>Security engineer</td>
</tr>
<tr>
<td>Incident handler</td>
</tr>
<tr>
<td>SIEM content author</td>
</tr>
<tr>
<td>Forensic investigator</td>
</tr>
<tr>
<td>Hunt analyst</td>
</tr>
<tr>
<td>Others (security data scientist, vendor liaison, watch officer, and more)</td>
</tr>
</tbody>
</table>

---
Metrics

The reporting, metrics, and key performance indicators (KPIs) of an organization’s event and case management will provide a volume of wealth in analyzing long-term trends. The following metrics are a subset of the Micro Focus SIOC services leveraging ArcSight solution:

- Cases by status (Stage)
- Monthly cases by severity
- Monthly cases by event category
- Monthly closure reasons
- Monthly time to resolution (TTR) by severity

3.1 Events Per Analyst Hour

Metrics such as events per analyst hour (EPAH), the number of events annotated, the number of events versus events of interest, case open time or time to close, and even the number of cases opened each week can be helpful if used appropriately.

Using the total events per second (EPS) volume metrics to either forecast the staffing needs or indicate when to increase staffing numbers is incorrect. The proper way to size and staff a SOC is to focus on the number of hours in a day that have to be monitored. The effectiveness of this monitoring will be directly correlated to the number of people doing the job. However, adding more headcount does not make a SOC more effective.

Using metrics correctly allows a SOC to add more events, devices, and use cases with the same headcount. The EPAH metric is a measurement that shows leadership when it is asking too much or too little in terms of suspicious alert triage from the analysts. This number should be between 8–12, which allows the analysts to triage and escalate events effectively. This metric is not used to size the number of analyst headcount, but rather to measure the effectiveness of existing headcount. If the number is too high either add headcount, reduce or modify SLA requirements, or modify use cases (i.e., tune the system) to get back into a manageable range.
One of the biggest problems that enterprises face today is the ability to keep up with the data explosion and vastly increasing the volume of data. The only way to keep up with the continual data increase is with automation. SIEM platforms today integrate with Big Data platforms that can scale to billions of events per second instead of the millions of events per second. The only way to perform threat detection realistically with this volume of data is through security orchestration, automation, and response (SOAR) systems. Investing in people who know how to make automation function correctly (maintain and manage the automated systems) is going to become increasingly important, more so than investing in people to perform security monitoring.

Additionally, increasing levels of automation with tools that can automate investigatory tasks and incident workflow is becoming a higher priority. Security automation is becoming smarter and more robust in terms of the threat detection information it is providing. Today’s investment in 24x7 real-time analysis is going to shift to automated hunting and performing investigations in a near-time manner instead.

Analytics and SOAR solutions that integrate a SIEM with large data stores and automation provide access to events that can empower a Machine Learning response action. While additional contextual events may not be ingested into the SIEM solution, access to the data via the right-click tools menu option in ESM would empower analysts.

Figure 3. Event management efficiency: Getting from raw events to actionable alerts through repeatable workflow
Additional automation considerations:

- Incorporate IT management tools typically used for managing service performance and availability.
- Consider the value add of using existing tools to augment security team’s capabilities.
- Additional applications such as Micro Focus Asset Manager, Operations Orchestration, a configuration management database (CMDB).

**Staffing Models**

Staffing plans will evolve directly out of the needs of the business (that is, what is the value of what it is you are trying to protect and what is the total cost of recovery for every second, minute, or hour that asset is impacted). Is the SOC a virtual entity where events are collected, analyzed, alerted, and reported? Should the SOC have the full-time personnel to monitor consoles, analyze, alert, and report? Or, does the SOC need full staffing 24x7x365? These needs will dictate the staffing models that must be implemented. Despite the particulars of any given staffing models, there are some guidelines to follow:

- A SOC analyst should never be alone in operating a shift, many safety and performance issues can occur.
- Each shift and role within the SOC should have clearly defined responsibilities and deliverables.
There should be no ambiguity in what is expected from each analyst at any given time during a SOC shift.

Workload and output from each shift should be regularly measured and adjustments to schedules, staffing levels, or task distribution should be modified accordingly. An overloaded SOC analyst will not be able to support the objectives of the SOC.

Most oversights and errors will occur during shift turnover. Therefore, there needs to be a clear and repeatable communication "hand-off" between shifts and overlapping shifts. Each shift should keep a formal log of events documenting those issues that need additional or continual attention.

A significant issue that always shows up on any night shift is that the analysts feel ignored and uninformed. The SOC managers must work hard to ensure they constantly communicate with the night shift and schedule time to work together.

To staff a repeatable, sustainable 24x7x365 SOC operations, a minimum of 10 analysts are required. The shift schedule that best fits this staffing model leverages four shifts each working 12 hours at a time. A minimum of two analysts should be on schedule at all times. Additionally, two of the more experienced analysts (commonly referred to as level 2 analysts) work an overlapping 8x5 shift and are available to cover shifts for planned and unplanned absences.
Cybersecurity and threat detection programs today account for non-owned and non-managed vendor partner environments such as cloud and hybrid cloud. It also includes highly virtualized and dispersed environments such as bring your own device (BYOD), Internet of Things (IoT), and more. This also has a large impact on the decisions that must be made when building and operating a SOC for an enterprise. Within this highly dispersed and less controlled ecosystem, a SOC must have visibility into vendor partner environments.

Analysts need understanding in not only network traffic and threat detection but also expertise in highly virtualized cloud environments and cloud vendors. Examples of what analysts should request from cloud vendors:

- Visibility into data access and authentication methods
- Visibility into infrastructure traffic
- Processes and procedures

During the past decade or more, there has been a pendulum effect between the roles of third-party managed security service provider SOCs versus on-premises dedicated security operation centers. The analyst monitoring skillset(s) of past years is now shifting toward a hunting and investigation skillset.

Hybrid Staffing Model

Access to skilled security resources continues to be the main concern of enterprises. To deal with this, organizations are moving toward hybrid staffing and hybrid security service models. These new models require less in-house expertise while retaining control over critical pieces of the security organization’s detection capability.
A SOC may be created as a business-hours–only function (8x5), an extended-hours function (12x5, 18x7, and 24x7), or a hybrid of internal staff and outsourcing. The perceived ROI for such hybrid solutions can vary widely based on many factors, but the perception that security can be outsourced completely to a third party has clearly declined in favor of hybrid, niche vendor and provider solutions.

Organizations using this model realize that the level of capability will differ between the in-sourced and outsourced teams. And they have made a risk-based decision that the cost to fully staff with their own people is not worth the more in-depth capability. A managed security services (MSS) provider will not know as much about an organization as an internal team, yet there is still value in leveraging an MSS provider in many situations. Many companies are still building and operating a 24x7 capability in-house. Others are taking the viewpoint that a highly skilled, business hours-centric internal team with effective tools can independently or with the augmentation of a managed service, meet their objectives.

Hybrid, co-managed operations cyber defense teams use a combination of internal and external (professional or managed services) resources to operate their cyber defense capability. These hybrid environments require advanced maturity of their processes to be effective and to avoid mishandling of incidents. Utilizing hybrid staffing models, such as outsourcing first-line analysis, can not only reduce the negative effect of attrition or skills acquisition but also make the total cost of recovery more expensive.

Organizations that use a hybrid staffing model must pay special attention to escalation and shift turnover processes between insourced and outsourced functions. Strictly defined and followed processes ensure that all relevant information is passed between groups and allows for the best capabilities at identifying and isolating breaches.

**Scheduling**

The first hurdle in scheduling is coverage. How many analysts are required to cover a given operational timeframe—24x7x365, 8x5, 12x5, or virtual? How many analysts are needed on shift at any given time? The number of security analysts required per shift will vary throughout the day based on overall security responsibilities and work volume. A good rule of thumb is to have at least two analysts on shift at any given moment to allow for breaks and to prevent a condition commonly known as console burn-out.

It is typical to staff junior analysts with senior analysts or level 1 analysts and level 2 analysts. Best practices call for a staffing ratio of higher number of level 1 analysts to level 2 analysts. For example, ArcSight ESM workflow is designed to leverage a level 1 or level 2 model with the built-in case management and event annotation. This means essentially moving alerts or events of interests through an initial triage stage (level 1) through investigation (level 2) to escalation (Security Incident Response Team).

A SOC shift lead provides senior experience and accountability during a shift and shift turnover. Shift leads also ensure operational tasks are completed by priority. They also ensure analyst training and mentoring is
performed across all shifts while providing coverage during breaks. Shift leads can bridge the gap between each shift turnover. A SOC shift lead role can also fill the level 2 responsibilities.

These are some additional considerations regarding scheduling:

- All analysts could effectively work at least one weekend, which provides balance as all persons share equal burden
- Built-in staffing redundancy for vacations, holidays, paid time-off (PTO), and/or unpredictable emergencies
- Holiday coverage should be treated as a normal business day, but with minimal staffing and be in accordance with local labor laws
- Provisioning of on-call services or capabilities for after-hours monitoring of a small subset of critical use case(s) or in the event of an incident
- The business stakeholder(s) will need to partner with the respective human resources (HR) department for SOC locations with consideration of any potential scheduling issues or allowance required to transition to the required workday hours and weekend coverage
Roadmap for Growth

A mature SOC that is fully staffed, operationally mature, and properly aligned with its mission and vision statements, with dedicated engineering resources, should be expected to absorb “spikes” in detections when there are emerging security events and return to a normal state over a short time. Requesting and obtaining headcount is not always the correct answer to resolve symptoms that the organization is experiencing. It’s important that security leaders fully understand the issues and symptoms before they formulate and execute a plan to respond and grow.

Knowing when to increase headcount is a troubling decision that all organizations face. As the business owner of the SOC, security leaders are required to ensure that the business strategies and tactics are aligned and are being executed while also being fiscally responsible.

As the business owner, SOC leaders must conduct the appropriate level of analysis to justify the execution of a plan, which may involve:

- Transition of work items that do not align with the organization mission or vision.
- Development of applications or tools (middleware) to improve workflow efficiencies and enable new levels of automation.
- Incorporate new capabilities that are required to address emerging threats or risks like the establishment of analytics.
- Adopt the business requirement to extend hours of operations, such as 24x7 availability.
Growth inhibitors or roadblocks:

- An inability to prioritize efforts in a SOC results in an overall low capability and maturity—it is difficult and costly to protect everything. Successful SOCs utilize a risk-based approach that results in clear priorities and targeted focus.

- Administrative tasks levied on top of analytical tasks in a SOC degrade overall results. Organizations often gauge that there are not enough events detected in the SOC and assign other non-detective tasks to ensure full utilization of SOC analysts. A more mature response is to discover why there is a lack of detection and implement a plan to improve the SOC’s detection capability.

- Frequently evaluate whether the SOC’s daily responsibilities or tasks are aligned to its mission and vision statement

- Out-of-scope (mission and vision)—whereas these tasks can be re-directed to the appropriate teams, persons or organization as reports, alerts, and such.

Some situations and/or scenarios may require additional resources such as full-time equivalent (FTE) headcount, contingent staffing, budgetary allotments, or organizational realignment to address growing operational issues. For such scenarios:

- Establish comprehensive security monitoring and incident response capabilities.

- Provision dedicated staffing in the SOC for the given shift(s) to maintain security monitoring and operations.

---

**Figure 4. Triggers for increasing SOC headcount**

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase in EPAH (due to addition of technology feeds and more)</td>
<td></td>
</tr>
<tr>
<td>Compliance requirements (for example, General Data Protection Regulation)</td>
<td></td>
</tr>
<tr>
<td>Expanding coverage (24x7 services and more)</td>
<td></td>
</tr>
<tr>
<td>Mergers and acquisitions</td>
<td></td>
</tr>
<tr>
<td>Maturity increase</td>
<td></td>
</tr>
</tbody>
</table>

---

20
Summary

Although every organization is unique in its security expertise, security posture, risk tolerance, compliance requirements, and budget, all organizations share the same goal of effectively hardening their attack surface while detecting, prioritizing, and responding to security threats and incidents. You can establish a successful security operations capability, a critical contributor to your organization’s security posture, with knowledge of the basic SOC elements and a roadmap for where to start and how to mature. Start small and build. Micro Focus Consulting can help.

About Micro Focus Security

Micro Focus is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products including ArcSight, Fortify, Data Security, and Identity and Access Security, the Micro Focus cyber security solutions portfolio uniquely delivers the advanced correlation, application protection, and network defenses to protect today’s hybrid IT infrastructure from sophisticated threats.

Micro Focus Cyber Security Services

Micro Focus Security Intelligence and Operations Consulting (SIOC) services take a holistic approach to building and operating cyber security. Our approach also delivers response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world’s largest enterprises. Micro Focus uses a combination of operational expertise—both from the company and customers—and proven methodologies to deliver fast and effective results to demonstrate ROI. Micro Focus’s proven, use-case driven solutions combine market-leading technology together with sustainable business and technical processes executed by trained and organized people.

Learn More At
www.microfocus.com/sioc