LMNTRIX

BE THE HUNTER I NOT THE PREY

WHAT DOES IT REALLY COST TO BUILD A 24/7 SOC?

A Security Operations Centre (SOC) is an effective solution for managing a business's security concerns. A SOC centralizes the business's information security monitoring and incident response functions and computer network defenses, taking responsibility for detecting and remediating external malicious attacks and internal security breaches.

SOC's can go by many names, including Cybersecurity Operations Center (CSOC), Computer Incident Response Team (CIRT), Computer Security Incident Response Capability (CSIRC), or Network Operations and Security Center (NOSC). Whatever the name, the mission is the same - computer network defenses organized to detect, analyze, respond, report, and prevent security incidents.

DO YOU NEED A SOC?

Maybe the question should be, can you afford not to have a SOC? Businesses need to take a proactive approach when it comes to cybersecurity in today's threat landscape. Security breaches can be extremely costly, both in terms of direct financial losses and indirect after-shocks from reputational damage. Attacks can come from a broad range of sources, from the bored teenager looking to cause mischief through to organized criminal gangs seeking to steal valuable data, from competitors seeking advantage through to nation-states seeking to acquire intellectual property. Attackers have access to ever more sophisticated hacking tools, and attacks can come at any time and from anywhere in the world, requiring businesses to be always on guard to meet these challenges.

Addressing this challenge is where a SOC comes in, the services of a capable SOC, and the trained analysts that staff it is crucial for any business that needs to maintain a sound security posture and prevent any attacks from causing adverse damage to the company. In today's threat laden environment. SOC's are becoming a popular solution for businesses of all sizes and shapes.

A SOC is more than a facility. It is the integration of security analysts, practical procedures, and the latest technology into a comprehensive service for the monitoring and protection of a business's information systems from external and internal threats. The principle behind the operation of a SOC is the collation and consolidation of data into a central location where it can be processed and analyzed.

WHAT WILL A SOC DO FOR YOU?

SOC's protect corporate information systems by collecting internal and external threat intelligence data and performing analysis to identify any suspicious or abnormal behavior of users, endpoints and networked devices, or network traffic.

SOC's are built around a core Security Information and Event Management (SIEM) technology that performs the threat intelligence and behavioral analysis. The consolidation of these results with the collated IT infrastructure event and log data delivers an exhaustive threat detection service. The primary purpose of the analysis is to identify if a threat is actively attempting to find and exploit a security weakness and neutralize that threat before it can compromise the system. The output of the automated processes is incident reporting of irregular events, prioritized for investigation by the trained team of security analysts. Their role is to determine the actual cause and significance of events and initiate countermeasures or corrective actions, as necessary.

SOC's employ a range of tools that not only facilitate security breach identification but also provide the necessary information to allow detailed forensic investigation of each breach. An additional benefit of a SOC is that it can perform the mandatory log monitoring and compliance reporting for organizations that need to demonstrate IT security compliance with legislation, regulations, or standards such as PCI DSS.

LMNTRIX
BE THE HUNTER I NOT THE PREY

WHY SHOULD I BUILD A SOC?

SOC's are vital to maintaining secure information systems, and access to your own dedicated and bespoke SOC will provide your business with the capability to manage security precisely in accordance with your corporate security strategy against the threats that are relevant to your company and cognizant of the board's risk appetite. You also have direct control over the evolution and expansion of your SOC capability in response to changes to your business, the threat landscape, and the availability of new technological developments.

Building a SOC should come with a word of caution; such a venture can be extremely time-consuming and expensive to build from scratch. Especially for a business that does not currently have an in-house security monitoring capability. Expenditure to consider includes a physically secure location, IT infrastructure and connectivity, software, and hardware tools, and last and not least, the staffing costs – recruitment, employment, and training.

For a SOC to be continuously effective, it must operate 24/7/365. Staffing requirements must ensure there are sufficient numbers available to cover round-the-clock shifts, including the ability to cover planned and unplanned absences, periods of high workloads due to active and significant scale incidents, and natural turnover. The availability of suitably trained, qualified, and experienced analysts will depend on the geographic location of the SOC and the employee benefits on offer.

Third-party owned and managed SOC's are available as a managed service for those businesses that cannot build, staff, and maintain a SOC. These provide an invaluable resource for those businesses that cannot afford to attract, retain, and support the specialist team required by a SOC on a continuous basis.

WHAT DO I NEED TO BUILD A SOC?

Building a SOC is much more than just buying all the latest tools and equipment, followed by hiring a team of analysts. SOC's require ongoing effort to stay on top of threats, to stay up to date with emerging technology and trends, and keeping the analyst skills of the current.

Before you start to build your SOC, its vital that you fully understand precisely what capabilities your business requires both on day one and going forward into the near future. The core business objectives in concert with regulatory and legislative requirements will drive the strategy that the SOC must satisfy, which defines its concept of operations (CONOPS). The IT infrastructure, information processing environment, and the information assets that the SOC is protecting will influence the detailed requirements.

An inadequate or inaccurate assessment of your SOC capabilities will result in a weak SOC strategy that does not align with the goals of the organization. At best, you will end up with an inadequate SOC, and at worst, you will spend a significant amount of cash on a SOC that does not work.

SOC FACILITY

SOCs are often portrayed in the media as a "war room" with monitors covering the walls and rows of desks behind each is an analyst in deep thought as they stare at columns of random characters. The reality is usually far more modest.

The critical point to remember is that the SOC is the point where all the security-related data for a business is collected and consolidated into one central location. From an attacker's point of view, being able to sit inside the SOC or remotely access its systems would effectively give them the keys to everything that is of value within the business. This criticality is why the SOC must be physically and logically secure to prevent its compromise. Physical security includes sufficient access controls, so only authorized personnel are allowed inside, breaking into the facility through doors, windows, or other means should never be possible without detection. Strict controls are a must for visitors, contractors, and other third-parties. The list of physical security controls will go on and on.

Logical security includes technology to ensure that the consolidated security-related data cannot leave the SOC unless explicitly authorized. All data must be protected to ensure that inadvertent or malicious deletion or alteration of evidence is not possible.

Secure retention of security-related data in the event of loss or damage using standard data backup, business continuity, and disaster recovery processes must consider the unique security requirements of security-related data.

It is here that using a standard for the management of the security of the SOC itself is invaluable. Certification and continuous audits against an international standard such as ISO/IEC 27001 can be a step in the right direction for safeguarding your SOC.

SOC STAFFING

The critical component of any SOC is the team that staff it, responsible for monitoring the systems, identifying any security issues and events, and responding to incidents. Other duties can include security policy and compliance monitoring and reporting, change management, patch management, and security testing. The SOC team, depending on the size and nature of your business, will typically include:

SOC MANAGEMENT TEAM

The SOC Chief is responsible for managing operations, overseeing incident response planning, allocating resources, and planning future development.

SECURITY ANALYST TEAM (TIER-1)

The Security Analyst Team is the SOC front-line staff, monitoring the IT systems, and handling incoming queries and requests for assistance. They are responsible for organizing and interpreting collated logging and event data and integrating with threat intelligence data to generate real-time threat analysis and breach reporting. Once a breach is verified, the Incident Response Team takes responsibility for further investigation and identifying actions to halt, resolve, and mitigate the breach.

INCIDENT RESPONSE TEAM (TIER-2)

Responsible for triage of the information provided by the Security Analyst Team, they react to breaches, deploy counter-measures to halt any violation, and resolve the exploited vulnerabilities used to carry out the attack.

FORENSIC INVESTIGATION TEAM (TIER-2)

Responsible for analyzing incident data to identify the nature and severity of any breaches, including any consequential effects and collateral damage assessment.

SECURITY TEST TEAM

Responsible for conducting proactive vulnerability scanning and penetration testing to identify and resolve vulnerabilities before a malicious attacker can exploit them or allow an inadvertent operation to cause undesirable consequences to the integrity of the systems. They may also fulfill the role of threat hunters, working proactively to study available data to identify potential security breaches that do not register as suspicious or abnormal behavior.

COMPLIANCE AUDITORS

Responsible for ensuring processes comply with applicable legislation and regulations and generating compliance reports.

TEAM TASK ALLOCATION

It is not unusual for SOC staff to fulfill several roles within the teams to perform a combination of unprogrammed event-driven response tasks and scheduled day to day routine operational tasks. This situation is especially true for a simple SOC where financial resources are limited, so tier-1 analysts may be required to take on tier-2 roles as well as administration and engineering support roles.

SOC SYSTEM ADMIN AND ENGINEERING

Responsible for managing the SOC infrastructure operations and maintenance activities, tool deployment, and management, scripting, and automation plus data collection, control, and storage.

SOC PROCESSES

The SOC teams rely on having effective processes, policies, and standards against which to operate to do their jobs. The documented procedures should describe each stage of the monitoring, analysis, investigation, and resolution lifecycle for security incidents. Procedures should detail the hand-off procedures between each step to prevent the inadvertent overlooking of security issues.

Typical processes should cover the operating procedures for threat monitoring and detection, incident logging, threat escalation, analysis, incident response, compliance monitoring, and reporting. The NIST SP800-61 Computer Security Incident Handling Guide provides advice as to industry best practices that can help develop the framework for the SOC processes.

Monitoring the effectiveness of the SOC is invaluable in determining whether it is achieving the desired results and providing the required levels of security protection, and give a pointer to any deficiencies, areas for improvement, or future capability enhancement. Typical key performance indicator metrics for monitoring SOC effectiveness include:

- Number of incidents
- Average time for incident detection
- Average time for incident remediation

It is usual to break incident data reporting down into incident types, severity, threat source, time, attack vectors, and other information useful in trend analysis.

SOC TOOLS

The SOC is only as capable as the tools available to the analysts, centralized and integrated suite of compatible tools will minimize the risk of losing track of incident-related data. Asking the team to assess data received piecemeal from a diverse range of incompatible tools that manage individual devices will render their task impractical and risk attacks being unidentified until it is too late. The display of information across multiple dashboards, or worse available in log form only, will be much more difficult to correlate and cross-reference.

For a SOC to deliver comprehensive and effective monitoring and analysis, it will require tools to automate the initial stages of event monitoring, including the data collection, parsing, collation, storage, and triage steps.

The selected toolset should include the ability to manage endpoint protection, firewall configuration, network management, as well as automated application security and monitoring solutions. The beating heart of the SOC is the SIEM system, around which are the supporting applications and systems that typically include some of the following features, depending on the nature of the IT systems requiring protection:

- Data Backup and Recovery
- Data Log Collection
- Endpoint Detection and Response
- File Integrity Monitoring
- Firewall Management
- Forensic Analysis
- Governance, Risk, and Compliance
- Intrusion Detection System (IDS)
- Intrusion Protection System (IPS)
- Log Management
- Malware Quarantine and Analysis
- Patching and Update Test and Rollback
- Penetration Testing
- Security Orchestration, Automation, and Response
- User and Entity Behavior Analytics
- User Request Ticketing
- Vulnerability Scanning
- Wireless Intrusion Prevention

SOC TOOLS

While there is a diverse range of security technologies available to choose from, selecting layered defensive capabilities will deliver the best results. The failure of any single defense measure to detect an attack should be countered by a second independent defense measure being available to prevent the attack. The independence between layers is the key, relying on an intrusion-prevention system (IPS), and anti-virus scanning will not meet this criterion as both rely on signature-based detection methods and so could both potentially miss an attack. The recommended approach would be to consider using layered defensive/detection capabilities such as the following:

- Content filtering against malicious web sources
- IDS/IPS to detect and prevent attacks
- Breach-detection technology focused on threats unknown to the IDS/IPS
- Network baselining and monitoring to detect atypical data trends

To keep one step ahead of evolving threats, the SOC team should, as part of the threat intelligence activities, utilize third-party threat report services such as Information Sharing and Analysis Centers (ISACs). Threat sharing and warning services are a crucial keystone for the threat intelligence function if a SOC is to be proactive rather than reactive.

COST ESTIMATES

The costs to build, operate, and maintain a SOC depend on the type of SOC a business requires, which in terms depends upon its specific needs and requirements.

Starting at the bare minimum for a 24/7/365 capability, you are probably going to need two analysts on duty at any time just to get started. The recommendation is always to have at least two people working at any one time to avoid the issues around lone working and to provide continuous eyes-on monitoring when an analyst needs a comfort break or another coffee. That equates to over 17,500 working hours, so with each analyst working eight-hour shifts for five days a week and with six weeks of absences each year for leave, illness, and training, then that predicates a team size of ten analysts. If you do decide that the single-person operation of the SOC is adequate, the 8,760 working hours for 24/7/365 service requires a team of five analysts as a minimum based on the same shifts and availability.

While there are many different shift schedules to choose from, each with their pros and cons, as an absolute minimum, the team of at least ten analysts is a bare minimum if they are going to work reasonable hours that are sustainable over the long term. This team size allows for standard levels of absenteeism, both planned and unplanned, but no room for adapting to significant changes in workload, work scope, or staff turnover. Considering that a typical security analyst will cost over $130,000 per annum to employ (salary, benefits, taxation), it can be seen straight away that any budget will start well above a million dollars before we consider the facilities, the equipment, and support staff.

COST ESTIMATES

To provide indicative figures, we have postulated three types of SOC, which are typical of the kinds commonly seen.

- The basic threat monitoring facility comprises a senior manager acting as SOC Chief, typically occupying a Chief Information Security Officer (CISO) role, with a team of ten tier-1 security analysts to provide 24/7 operations. The principal function of the SOC is the detection and resolution of attacks, with the security analysts fulfilling the incident response and investigation roles in addition to their primary monitoring responsibilities. Services provided include:

  - Call Center Facility
  - Real-Time Monitoring and Triage
  - Incident Analysis
  - Incident Response

- The intermediate threat monitoring facility with dedicated response capability takes things one step further with a dedicated tier-2 incident response team on hand to perform all incident response and investigation roles, leaving the security analysts to concentrate on their monitoring responsibilities. A second manager, supporting the SOC Chief as the SOC Deputy Chief, helps manage the increased team size and its additional capabilities. Services provided include:

  - Call Center Facility
  - Real-Time Monitoring and Triage
  - Threat Assessment
  - Incident Analysis
  - Incident Response
  - Countermeasure Implementation
  - Malware and Implant Analysis
  - Forensic Artifact Analysis

LMNTRIX
BE THE HUNTER I NOT THE PREY

COST ESTIMATES

- The advanced threat monitoring, response, and hunting facility include a full-time forensic investigation team to support the tier-2 incident response team and includes further capabilities to undertake proactive threat hunting activities. These additional capabilities are carried out under the guidance of a third member of the management team, supporting the SOC Chief and Deputy Chief, with the prerequisite subject matter expertise. Services provided include:

  - Call Center Facility
  - Real-Time Monitoring and Triage
  - Cyber Intel Collection and Analysis
  - Trend Analysis
  - Threat Assessment
  - Incident Analysis
  - Incident Response
  - Countermeasure Implementation
  - Malware and Implant Analysis
  - Forensic Artifact Analysis
  - Vulnerability Scanning and Assessment
  - Penetration Testing

Determining the exact type of SOC that you will need is far from straight forward, though help is available from many sources. We highly recommend NIST's Cybersecurity Framework for its straightforward approach to defining your security requirements using the identify, protect, detect, respond, and recover processes.

Depending on the selected SOC type and the nature of the operations that the SOC will be required to undertake, staffing may require specialist security investigators and auditors. They will typically cost over $160,000 per annum each to employ as well as a CISO and other senior management level specialists at over $210,000 per annum each.

These figures drive the ball-park indicative values below. Actual numbers will vary on geographic location, specific skills and experience required, and marketplace supply and demand fluctuations. A SOC located in northern California is likely to attract more applicants than a SOC located in south Arizona.

COST ESTIMATE SUMMARY

	Basic Threat Momitoring Facility	Intermediate Theart Monitoring With Dedicated Response	Advanced Threat Monitoring, Response And Hunting Facility
SOC Facility Establishment (Building, Equipment, Services, Infrastructure)	$120,000	$160,000	$200,000
SOC Facility Annual Maintenance	$40,000	$60,000	$80,000
SOC Staffing Annual Costs	(11 Employees)	(16 Employees)	(21 Employees)
SOC Management Team (1-3)	$210,000	$420,000	$630,000
Tier-1 Security Analyst Team (10)*1	$1,300,000	$1,300,000	$1,300,000
Tier-2 Incident Response Team (4)	-	$640,000	$640,000
Tier-2 Forensic Investigation Team (2)	-	-	$320,000
Compliance Auditors (2)	-	-	$320,000
Total Staffing Annual Costs	$1,510,000	$2,360,000	$3,210,000
SOC Tools (Purchase, Installation, Dedicated, Equipment, And Services)	$250,000	$300,000	$500,000
SOC Tools (Maintenance And Support)	$50,000	$60,000	$100,000
Total Year 1 Cost	$1,880,000	$2,820,000	$3,910,000
Annual Recurring Costs	$1,600,000	$2,480,000	$3,390,000

*1 Single-Person Operation Of A SOC Will Reduce This Cost Down From $1,300,000 To $650,000 Per Annum

LAST THOUGHTS

Building a SOC, of whatever type you need, will take conservable effort, expertise, and resources to complete successfully. Never underestimate just how long it can take to get from a paper plan to a fully operational facility running at optimal efficiency.

In terms of cost, the estimates show how staffing costs dominate both the first year and the subsequent recurring charges for a SOC. They account for over 90% of all costs, and with the scarcity of suitably qualified resources in today's marketplace, the expectation is that these costs will only increase. These estimates that we have calculated can be considered relatively conservative in terms of running a 24/7/365 operation with just ten analysts. These figures typically only provide for two analysts being in the SOC at any time, with sufficient availability left to increase the team size for short periods during times of exceptionally active threats.

With the extensive requirements for conceiving, developing, building, and staffing a SOC, it is easy to see why SOCs can cost so much and yet still fail to live up to expectations. It is essential to keep in mind before starting this process that no SOC will be perfect, particularly when it first goes live. SOC's need constant maintenance, updating, enhancement, and evolution if they are to become effective and remain viable over the long term.