HOW TO BUILD A SOC

A GUIDE FOR EFFECTIVE SECURITY OPERATIONS

WWW.RIVERSAFE.CO.UK

RIVERSAFE

CONTENTS

1. INTRODUCTION TO SOC

In today's digital age, organisations are becoming increasingly vulnerable to cyber threats. A SOC is an essential element of an organisation's cybersecurity architecture. It provides real-time monitoring of security events and alerts, enabling organisations to respond to threats quickly. The SOC is responsible for identifying and responding to cyber threats, protecting critical assets, and ensuring the confidentiality, integrity, and availability of data.

THE DIFFERENT SOC CATEGORIES

There are different types of SOC's available, ranging from small, five-person operations to large, national coordination centres. The type of SOC that an organisation chooses to implement depends on the size of the organisation, the complexity of its IT infrastructure, and the level of cybersecurity risk it faces.

IN-HOUSE SOC

- An In-House SOC is a centralised unit that is fully owned and managed by the organisation. This model provides full control to the organisation over its security operations and may operate around the clock (24/7) to ensure constant vigilance.

CO-MANAGED SOC

- A Co-Managed SOC (also known as a hybrid-SOC) is a model where the organisation shares responsibility for managing the SOC with a third-party provider. In this model, in-house resources typically operate during normal business hours (9-5), while out of office hours are handled by a Managed Security Service Provider (MSSP). This allows for a balance between in-house control and external expertise.

FULLY MANAGED SOC

- A Fully Managed SOC is a model where the organisation outsources the management of the SOC to a third-party provider. The service provider typically operates 24/7, offering the organisation access to advanced tools and expertise without the need to manage the SOC internally.

THE ROLE OF THE CISO

The role of the Chief Information Security Officer (CISO) is critical in the construction and management of a SOC. The CISO is responsible for ensuring that the SOC is staffed, trained, and equipped to respond to cybersecurity incidents. In order to accomplish this, they must work closely with other departments to integrate the SOC into the organisation's overall cybersecurity strategy.

2. PLANNING AND DESIGNING A SOC

UNDERSTANDING THE BUSINESS DRIVERS

Before building a SOC, it is important to understand the core business drivers that are motivating the creation of the SOC. This will help you define the scope and objectives of the SOC based on the organisation's specific needs and risk profile.

THREATS

When building out a SOC, it is essential to consider various threats that can impact its effectiveness. Some common threats to consider when building a SOC include:

- Insider Threats
- External Attacks
- Advanced Persistent Threats (APTs)
- Data Breaches
- Malware and Ransomware
- Denial-of-Service (DoS) Attacks
- Vulnerability Exploitation
- Lack of Security Awareness and Training
- Third-Party Risks
- Physical Security Threats

RISK MANAGEMENT

When it comes to risk management, there are several factors to consider based on your organisation. Here are some common examples to help you in the risk management process:

- Risk Identification and Assessment
- Risk Prioritisation
- Risk Mitigation Strategies
- Risk Tolerance and Decision-Making
- Implementation of Risk Controls
- Ongoing Monitoring and Review
- Incident Response Planning
- Employee Awareness and Training
- Continuous Improvement
- Compliance and Regulations

BRAND REVENUE AND PROTECTION

Areas of consideration to safeguard revenue streams and protect the brand reputation of the organisation include:

- Counterfeit and Intellectual Property Protection
- Brand Reputation Management
- Product and Service Quality Assurance
- Pricing and Revenue Optimization
- Customer Data Protection
- Distribution Channel Control
- Competitive Landscape Analysis
- Brand and Marketing Strategy
- Compliance and Legal Considerations

INSURERS

Finally you also have insurers to consider such as:

- Insurance-Specific Threats
- Customer Trust and Reputation
- Regulatory Compliance
- Incident Response and Business Continuity
- Claims Fraud Detection
- Underwriting Risk Assessment
- Cyber Insurance Offerings
- Third-Party Risk Management
- Business Impact Analysis
- Compliance with Industry Standards

SOC TECHNOLOGIES AND TOOLS

After gaining a clear understanding of the business drivers, it's crucial to identify the necessary resources and tools for building the SOC. These include hardware, software, and personnel. To ensure that the resources and tools are suitable for the organisation's needs and budget, you could map them out. This exercise will help you determine which resources are required and how they should be allocated.

TOOL	PURPOSE	RISK MITIGATION	VENDOR EXAMPLES
SIEM	Collect and analyse log data to detect threats	Identify suspicious activity early to prevent breaches	Splunk, Sentinel, Exabeam, LogRhythm, IBM QRadar
IDS/IPS	Monitor network traffic and systems to detect malicious activity	Block malicious traffic and attacks	AWS (AWS Network Firewall), GCP (Google Cloud Armor), Cisco, Fortinet, Palo Alto
EDR	Detect threats on endpoints and provide response capabilities	Quickly isolate compromised endpoints to prevent lateral movement	SentinelOne, Carbon Black, CrowdStrike
Vulnerability Scanning	Scan networks and systems to find vulnerabilities	Identify and patch vulnerable systems before they can be exploited	Tenable, Qualys, Rapid7
UEBA	Analyse user behaviour to detect anomalies	Detect compromised accounts or insider threats	Exabeam, Securonix, Gurucul
Incident Response	Orchestrate and automate incident response	Accelerate investigation and containment of incidents	Splunk (Splunk Phantom), IBM SOAR, Swimlane

TOOL	PURPOSE	RISK MITIGATION	VENDOR EXAMPLES
SOAR	Automate and orchestrate security operations and incident response	Reduce response times and increase efficiency in handling threats	Splunk SOAR, Palo Alto Networks XSOAR, IBM Resilient
Threat Intelligence	Provide context on latest threats and adversary tactics	Proactively hunt for emerging threats targeting the organisation	DomainTools, Recorded Future, Anomali
NDR	Detect threats on the network	Identify threats earlier by detecting anomalies and threats on the network	Vectra AI, ExtraHop, FireEye
Compliance	Automate compliance auditing processes and reporting requirements	Simplify compliance work-flows and audits to meet regulatory requirements	ServiceNow, RSA, Qualys, MetricStream

DESIGNING THE SOC ARCHITECTURE

Next, you should design the SOC architecture, including the physical layout, network topology, and data flows. This will help ensure that the SOC is optimised for efficiency and effectiveness.

CONSIDERATIONS FOR THE PHYSICAL LAYOUT:

- Locate the SOC in a secure area with controlled access. Use physical security measures like access cards, biometric scanners.
- Design workspaces to enable collaboration among analysts. Include huddle spaces for quick discussions.
- Have a large video wall for displaying dashboards and security event data.
- Set up the analyst workstations ergonomically to enable long periods of work. Provide multiple monitors.

FOR THE NETWORK TOPOLOGY:

- Segment the SOC network into security zones with firewalls and access controls. Isolate the management network.
- Implement redundant internet connections from different providers for failover.
- Use a mesh topology within the SOC for high availability.

FOR THE DIFFERENT DATA FLOWS:

- Ensure security event logs from endpoints, servers, firewalls etc. are forwarded to the SOC's SIEM system.
- Integrate threat intelligence feeds into the SIEM for correlation with events.
- Enable automated data sharing between SOC systems like the SIEM, SOAR platform, and ticketing system.
- Implement controls around sensitive data like encryption, access controls, and auditing.

POLICIES AND PROCEDURES

Establishing policies and procedures is also critical for the success of the SOC. This includes incident response, threat hunting, and other SOC activities. Policies and procedures should be well-documented and communicated to all relevant stakeholders.

POLICY/PROCEDURE	DESCRIPTION
Incident Response	Outlines the steps the SOC will take when responding to a security incident. Should cover triage, containment, eradication, recovery and lessons learned.
Threat Hunting	Defines the SOC's threat hunting strategy including hunting objectives, tools/data sources, frequency/ scheduling, reporting and more.
Alert Triage	Provides guidance on evaluating and prioritising incoming security alerts. May include severity categorisation, enrichment, escalation procedures etc.
Vulnerability Management	Covers the process for identifying, prioritising, scanning for and remediating vulnerabilities within the environment.
Access Management	Specifies how access will be provisioned, reviewed and revoked for systems and data within the SOC's scope.
Third Party Management	Defines how third party risk will be assessed and managed including due diligence, monitoring and audit.
Incident Documentation	Outlines required documentation for security incidents including summary, timeline, impact, etc.
SOC Reporting	Describes key performance and risk metrics the SOC will report on regularly to stakeholders.

DEVELOP A PROJECT PLAN

To ensure that the SOC is built and implemented successfully, it is important to develop a project plan and timeline. This will help ensure that all necessary tasks are completed on time and within budget.

PLANNING AND DESIGNING A SOC CHECKLIST

- [x] **Understand the business drivers**
- [x] **Define the scope and objectives**
- [x] **Identify necessary resources and tools**
- [x] **Design the SOC architecture**
- [x] **Establish policies and procedures**
- [x] **Develop a project plan and timeline**

3. BUILDING AND IMPLEMENTING THE SOC

Now that you have planned and designed your SOC, it's time to build and implement it. This section will provide you with a guide to help you build and implement an effective SOC.

YOUR TEAM: SKILLS AND EXPERIENCE

Your SOC is only as good as the people who run it. Therefore, it's crucial to hire and train staff with the appropriate skills and experience. You should look for candidates who have experience in threat intelligence, incident response, and security operations. Additionally, you should ensure that your staff has the necessary certifications.

ROLE	RELEVANT CERTIFICATIONS	EXAMPLE JOB DUTIES	
SOC Manager	CISM, CRISC, CISSP	Manage SOC staff, budget, technologies; liaise with leadership	
Security Architect	SSCP, TOGAF	Design security infrastructure and solutions; create security policies and standards	
Security Analyst	Security+, GCIA, GCIH	Monitor security tools and systems; triage and escalate incidents	
Incident Responder	GCIH, GCFA, CISSP	Lead investigation and remediation of incidents; develop mitigation strategies	
Threat Hunter	GCIA, GCIH	Proactively search for IOCs; identify advanced threats through data analysis	
Security Engineer	CISSP, Security+, GSEC	Implement and maintain security tools and systems; support architectural designs	
Forensics Investigator	GCFA, GCIH	Perform malware analysis and reverse engineering; gather evidence for investigations	
Malware Analyst	GCIA, GMON	Analyse malware samples; e xtract IOCs and TTPs; maintain threat intelligence	

HARDWARE AND SOFTWARE COMPONENTS

After hiring and training your staff, you need to configure and deploy the hardware and software components of your SOC. In a hybrid environment, this might include a mix of on-premise and cloud-based tools, such as firewalls, intrusion detection systems (IDS), security information and event management (SIEM) systems, among others. It's also crucial to ensure that your SOC has sufficient computing power, storage, and network bandwidth to manage the traffic and data generated by your organisation.

To help you configure and deploy your SOC's hardware and software components, you can use a table like the one below:

COMPONENT	FUNCTION	VENDOR	MODEL
XDR	Extended Detection and Response	Exabeam	Exabeam Fusion
Domain Intelligence	Threat Intelligence	DomainTools	Iris
Intelligent routing and Filtering	Log Filtering and Management	Cribl	Cribl Stream
Security Awareness	Training	KnowBe4	N/A
SOAR	Security Orchestration, Automation and Response	Splunk	Splunk SOAR
SIEM	Log Management	Microsoft	Microsoft Sentinel
Vuln Management	Vulnerability Scanning	Tenable	Nessus
DDoS	DDos Protection	Cloudflare	Standard DDoS Protection
Firewall	UTM	Palo Alto	Next Generation Firewalls
IDS	Threat Detection	Cisco	Firepower 9300
EDR	Malware Defence	CrowdStrike	Falcon
Network TAP	Traffic Monitoring	Gigamon	GigaVUE-HC3

TEST AND VALIDATE THE SOC'S FUNCTIONALITY AND PERFORMANCE

Before you go live with your SOC, you need to test and validate its functionality and performance. This includes testing your SOC's incident response procedures, validating your SOC's threat intelligence feeds, and ensuring that your SOC's tools and systems are working correctly.

- Test your SOC's incident response procedures with mock scenarios
- Validate your SOC's threat intelligence feeds by comparing them to external sources
- Conduct a comprehensive review of your SOC's policies and procedures to ensure they align with industry standards and best practices

CONDUCT TRAINING AND AWARENESS PROGRAMS FOR EMPLOYEES

Finally, although not directly related to building a SOC, you should consider conducting training and awareness programs for employees and other stakeholders to ensure that they understand the importance of cybersecurity and their role in protecting your organisation. This includes providing regular security awareness training, conducting phishing simulations, and ensuring that employees are aware of your SOC's incident response procedures.

Building and implementing a SOC requires careful planning, hiring and training staff with the appropriate skills and experience, configuring and deploying hardware and software components, testing and validating the SOC's functionality and performance, and conducting training and awareness programs for employees and other stakeholders. By following these steps, you can build and implement an effective SOC that helps protect your organisation from cyber threats.

4. OPERATING AND MANAGING THE SOC

Once your SOC is up and running, it's essential that you effectively manage and operate it to ensure it's providing the necessary protection and value to your organisation. This section will cover some key considerations for operating and managing your SOC.

DEFINING KEY PERFORMANCE INDICATORS (KPIs)

Defining KPIs for your SOC is essential to measure its effectiveness and demonstrate its value to stakeholders. Some key KPIs for SOC operations include Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Acknowledge (MTTA), and Dwell Time.

- MTTD measures how quickly your SOC can identify a security threat.
- MTTR calculates the average time taken to address and resolve the detected threats.
- MTTA gauges the time taken for your SOC team to acknowledge the detection of a threat.
- Dwell Time refers to the duration a threat remains undetected within your network.

These metrics can help you track how quickly and efficiently your SOC is identifying, acknowledging, and responding to security incidents.

IDENTIFYING METRICS AND MEASUREMENTS

In addition to KPIs, it's important to identify other metrics and measurements that can be used to track SOC performance over time. This can include metrics such as the number of incidents handled, the types of incidents detected, and the effectiveness of your incident response procedures.

DEVELOPING REPORTING AND ANALYSIS CAPABILITIES

To effectively manage your SOC, you need to have the right reporting and analysis capabilities in place. This means developing regular reports that provide updates on SOC performance, incident trends, and other key metrics. These reports should be shared with management and other stakeholders on a regular basis.

KPI	DEFINITION
Mean Time to Detect (MTTD)	The average time it takes to detect a security incident
Mean Time to Respond (MTTR)	The average time it takes to respond to a security incident
Number of Incidents Handled	The total number of security incidents handled by the SOC
Types of Incidents Detected	A breakdown of the types of security incidents detected by the SOC
Effectiveness of Incident Response Procedures	A measure of how effective your incident response procedures are in responding to security incidents

USING CONTINUOUS IMPROVEMENT PROCESSES

Continuous improvement is essential for ensuring that your SOC is always operating at peak efficiency. This means regularly reviewing your processes, procedures, and technologies to identify areas for improvement. Once you've identified areas for improvement, you should implement changes as needed to ensure your SOC is always operating at its best.

THE ROLE OF AUTOMATION AND ORCHESTRATION

Automation and orchestration can play a critical role in SOC operations. By automating routine tasks and orchestrating incident response procedures, you can improve your SOC's efficiency and effectiveness. This can help you detect and respond to security incidents more quickly and effectively, reducing the impact of security breaches on your organisation. out. This exercise will help you determine which resources are required and how they should be allocated.

5. INTEGRATING THE SOC WITH OTHER SECURITY PROCESSES

Integrating the SOC with other security processes is crucial for effective security operations. By sharing information and collaborating with other teams, the SOC can gain a more comprehensive view of the organisation's security posture and respond to threats more efficiently. In this section, we will discuss best practices for integrating the SOC with other security tools and processes.

VULNERABILITY MANAGEMENT

Vulnerability management is a critical component of any security program. By identifying and remediating vulnerabilities in a timely manner, organisations can reduce the risk of successful attacks. The SOC can work closely with the vulnerability management team to ensure that vulnerabilities are prioritised and remediated promptly.

The following table outlines best practices for integrating the SOC with vulnerability management:

- **Regular communication:** The SOC and vulnerability management teams should have regular meetings to discuss vulnerabilities and their potential impact on the organisation.
- **Prioritisation:** Vulnerabilities should be prioritised based on their severity and the potential impact on the organisation. The SOC can provide input on which vulnerabilities pose the greatest risk to the organisation.
- **Escalation:** If a vulnerability poses an immediate threat to the organisation, it should be escalated to the SOC for immediate action.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity and Access Management (IAM) is another critical component of a security program. By ensuring that only authorised users have access to sensitive data and systems, organisations can reduce the risk of unauthorised access. The SOC can work closely with the IAM team to ensure that access controls are properly configured and monitored.

The following best practices should be followed when integrating the SOC with IAM:

- **Regular communication:** The SOC and IAM teams should have regular meetings to discuss access control policies and any changes that may impact security.
- **Monitoring:** The SOC should monitor access logs and activity to detect any unauthorised access attempts or suspicious activity.
- **Escalation:** If the SOC detects any suspicious activity or unauthorised access attempts, they should escalate the incident to the IAM team for further investigation.

INCIDENT RESPONSE

Effective incident response is critical for minimising the impact of security incidents. The SOC should have a well-defined incident response plan that outlines how incidents should be prioritised and escalated based on their severity.

The following best practices should be followed for incident response:

- **Prioritisation:** Incidents should be prioritised based on their severity and the potential impact on the organisation.
- **Escalation:** If an incident poses an immediate threat to the organisation, it should be escalated to the appropriate team for immediate action.
- **Communication:** The SOC should communicate regularly with other teams during incident response to ensure that everyone is aware of the incident and the actions being taken to mitigate it.

THREAT INTELLIGENCE

Threat intelligence can provide valuable insights into the latest threats and attack methods. The SOC can integrate threat intelligence into their workflow to stay up-to-date on the latest threats and improve their ability to detect and respond to attacks.

The following best practices should be followed for integrating threat intelligence into the SOC's workflow:

- **Regular updates:** Threat intelligence should be updated regularly to ensure that the SOC has the latest information on threats and attack methods.
- **Integration with SIEM:** Threat intelligence can be integrated with the SOC's SIEM to improve the accuracy of threat detection and reduce false positives.
- **Analysis:** The SOC should analyse threat intelligence to identify any potential threats to the organisation and take appropriate action to mitigate them.

By following best practices and working closely with other teams, the SOC can improve their ability to detect and respond to threats, ultimately improving the organisation's overall security posture.

6. CONCLUSION

Congratulations on completing this guide on building an effective SOC. At this point, you should have a solid understanding of what a SOC is, why it is a critical component of an organisation's security strategy, and how to build one tailored to your organisation's needs.

HERE ARE THE KEY TAKEAWAYS FROM THIS GUIDE:

- A SOC is a centralised unit that monitors and analyses an organisation's security posture and responds to security incidents.
- A SOC can help you detect and respond to security incidents faster, reducing the impact of a breach and minimising downtime.
- Building a SOC requires careful planning, including defining your objectives, identifying your resources, and selecting the right technology.
- A SOC should be staffed with skilled professionals who can quickly identify and respond to security incidents.
- To build an effective SOC, you need to establish clear processes and procedures for incident response, communicate effectively with stakeholders, and continuously monitor and improve your security posture.

HERE ARE SOME ADDITIONAL RESOURCES:

- The National Cyber Security Centre's (NCSC) guidance on Building a Security Operations Centre (SOC) provides detailed advice on how to design and implement a SOC.
- The Information Security Forum's (ISF) Building a Successful SOC guide offers practical advice on how to set up and run a SOC, including how to measure its effectiveness.

Building a SOC is an ongoing process, and it's important to continuously monitor and improve your security posture. With the right planning, technology, and people, you can build an effective SOC that helps you stay ahead of the ever-evolving threat landscape.

FREQUENTLY ASKED QUESTIONS

WHAT ARE THE KEY COMPONENTS OF A SOC?

A SOC is a facility that houses the team responsible for monitoring, detecting, analysing, and responding to security incidents. The key components of a SOC include people, processes, and technology. The people component includes security analysts, incident responders, and SOC managers. The processes component includes incident response procedures, escalation policies, and reporting mechanisms. The technology component includes security information and event management (SIEM) systems, intrusion detection and prevention systems (IDPS), and other security tools.

WHAT ARE THE BEST PRACTICES FOR DESIGNING AND BUILDING A SOC?

The best practices for designing and building a SOC include conducting a risk assessment, defining the scope and objectives of the SOC, selecting the appropriate team members, defining the roles and responsibilities of each team member, selecting the appropriate technology, defining the incident response process, defining the escalation process, and defining the reporting process. It is also important to establish key performance indicators (KPIs) to measure the effectiveness of the SOC.

WHAT ARE THE REQUIREMENTS FOR SETTING UP A 24X7 SOC?

A 24x7 SOC requires a team of security analysts, incident responders, and SOC managers who are available around the clock to monitor, detect, analyse, and respond to security incidents. The team should be organised into shifts to ensure that there is always someone available to respond to incidents. The SOC should also have a backup team in case the primary team is unavailable.

WHAT IS THE COST OF BUILDING A SOC?

The cost of building a SOC depends on the size and complexity of the organisation, the level of security required, and the technology used. A small organisation may be able to set up a basic SOC with a few security analysts and a SIEM system for a few hundred thousand pounds. A larger organisation may require a more complex SOC with multiple teams, advanced technology, and a budget of several million pounds.

WHAT ARE THE ESSENTIAL TOOLS AND TECHNOLOGIES FOR A SOC?

The essential tools and technologies for a SOC include a SIEM system, IDPS, threat intelligence feeds, and security automation and orchestration tools. These tools help the SOC team monitor, detect, analyse, and respond to security incidents in real-time.

WHAT ARE THE SKILLS AND QUALIFICATIONS REQUIRED TO WORK IN A SOC?

The skills and qualifications required to work in a SOC include a strong understanding of security principles and practices, knowledge of security tools and technologies, experience in incident response, and strong analytical and problem-solving skills. Many SOC roles require a degree in computer science, information security, or a related field, as well as industry certifications such as CompTIA Security+ and Certified Information Systems Security Professional (CISSP).