Topic 5

Security Operations Centre (SOC)

Dr Diarmuid Ó Briain

Version: 1.0

SETU
Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University

Dr Diarmuid Ó Briain

CEng, FIEI

CISSP®

Table of Contents

Illustration Index

1 Introduction

In today's increasingly digital world, organisations are facing a growing number of cybersecurity threats. To protect their data and systems, many organisations are turning to Security Operations Centres (SOC).

A SOC is a centralised hub for monitoring, analysing, detecting, and responding to cybersecurity threats. It serves as the focal point of an organisation's cybersecurity posture, providing a 24/7 watch over its Informational Technology (IT) and Operational Technology (OT) infrastructure to identify and mitigate potential security breaches.

There are many benefits to implementing a SOC, including enhanced security posture, reduced risk of cyberattacks, improved compliance, and increased business continuity. SOCs can be built and maintained in-house or outsourced to a Managed Security Service Provider (MSSP).

The key components of a SOC are people, processes, tools, intelligence, and core SOC tasks. The SOC team is the heart of any SOC, and it is made up of security analysts, managers, and other professionals with expertise in cybersecurity. SOCs also have a set of well-defined processes that guide their operations, including incident response procedures, threat hunting protocols, and vulnerability management methodologies.

SOCs employ a variety of security tools to collect, analyse, and correlate security data, including Security Information and Event Management (SIEM), Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), threat intelligence platforms, and vulnerability management software. SOCs also rely on threat intelligence to stay informed about the latest threats and emerging attack techniques.

1.1 Objectives

By the end of this topic, you will be able to:

- define a SOC and understand its role in an organisation's cybersecurity strategy.
- identify the core components of a SOC, including people, processes, tools, intelligence, and core SOC tasks.
- describe the different levels of SOC analysts and their respective responsibilities.
- explain the importance of threat intelligence in a SOC and how to collect, analyse, and use threat intelligence to enhance cybersecurity posture.

2 Secure Operations Centre

2.1 Functions of a SOC

2.1.1 Threat Detection and Analysis

SOC analysts continuously monitor security logs, network traffic, and other data feeds to identify suspicious activity or anomalies that could indicate a cyberattack. They employ a variety of tools and techniques, including SIEM systems, IDS/IPS, to analyse and assess potential threats.

2.1.2 Incident Response

When a potential threat is detected, the SOC team rapidly initiates incident response procedures to contain, investigate, and remediate the issue. This may involve isolating affected systems, restoring backups, forensically analysing attack patterns, and notifying relevant stakeholders.

2.1.3 Compliance and Risk Management

SOCs play a crucial role in ensuring that organisations adhere to relevant cybersecurity regulations and industry standards. They conduct regular vulnerability assessments, penetration testing, and compliance audits to identify and address security gaps.

2.2 Components of a SOC

2.2.1 People

A SOC comprises skilled IT and OT security professionals with expertise in threat detection, analysis, incident response, and compliance. They possess a deep understanding of cybersecurity threats, tools, and techniques.

2.2.2 Technology

SOCs rely on a suite of security technologies to collect, analyse, and correlate threat data. This includes SIEM systems, IDS/IPS, network monitoring tools, log management tools, and threat intelligence platforms.

2.2.3 Processes and Procedures

SOCs establish clear and documented processes for handling security incidents, investigations, and remediation. These processes ensure that security teams can effectively respond to threats and minimise the impact of cyberattacks.

2.3 Benefits of Implementing a SOC

2.3.1 Enhanced Security Posture

A SOC can significantly improve an organisation's cybersecurity posture by proactively detecting and addressing threats before they can cause significant damage.

2.3.2 Reduced Response Times

SOCs enable faster and more effective incident response, minimising the impact of cyberattacks on operations and data.

2.3.3 Improved Compliance

SOCs help organisations maintain compliance with relevant cybersecurity regulations and standards, reducing the risk of legal and financial penalties.

2.3.4 Reduced Risk of Data Breaches

By detecting and remediating threats early on, SOCs can help organisations significantly reduce the risk of data breaches, protecting sensitive information and customer privacy.

2.3.5 Enhanced Customer Confidence

A robust cybersecurity posture supported by a SOC can instil confidence in customers and partners, demonstrating the organisation's commitment to protecting their data and systems.

3 Building a SOC

The establishment of a SOC can pose a significant challenge for many organisations, particularly those with limited resources in terms of time, personnel, and financial constraints. The complexity of integrating multiple security monitoring technologies and real-time threat intelligence necessitates a comprehensive approach that goes beyond a Do It Yourself (DIY) solution. The ability to effectively implement and manage these diverse tools on an ongoing basis is crucial for maintaining a robust SOC infrastructure. To address these challenges, organisations should seek methodologies for simplifying and unifying security monitoring practices, thereby optimising SOC processes and team effectiveness.

A SIEM platform can provide a solid foundation upon which to build a SOC, obviating the need for costly implementation services or the deployment of large teams to manage its operations. A SIEM system powered by a threat intelligence engine can effectively orchestrate the integration of people, processes, tools, and threat intelligence, thereby encompassing all the fundamental components essential for establishing a successful SOC. The main considerations are people, processes, tools and intelligence.

3.1 People: The SOC Team

Review key SOC roles and responsibilities: Comprehend the essential roles and responsibilities within a SOC team, including security analysts, threat hunters, incident responders, and SOC managers. Understand the skills and experience required for each role.

Examine the SOC skillset matrix: Analyse the SOC skillset matrix to assist with identification and recruitment of the right talent to assemble a strong SOC team. This matrix provides a comprehensive overview of the skills and experience required for each SOC role.

3.2 Processes and Procedures

Establish the key processes and procedures required to build a SOC: Define the critical processes and procedures that underpin an effective SOC, including:

- **Event classification and triage**: Efficiently categorise and prioritise security alerts to ensure prompt and appropriate attention.
- **Prioritisation and analysis**: Analyse incoming security events to assess their severity and potential impact.
- **Remediation and recovery**: Implement corrective actions to address detected threats and restore normal system operations.
- **Assessment and audit**: Conduct regular assessments and audits to evaluate the SOC's effectiveness and identify areas for improvement.
- **Examine tools that help centralise these processes and manage them**: Explore tools that can automate and streamline SOC processes, enabling efficient and centralised management of security events and incident responses.

3.3 Tools

Review the essential security monitoring tools required for building a SOC: Understand the necessity of various security monitoring tools, including:

- **Asset discovery**: Identify and inventory all assets within the organisation's IT infrastructure.
- **Vulnerability assessment**: Identify and prioritise vulnerabilities in IT assets to mitigate potential attack vectors.
- **Intrusion detection**: Detect and alert on suspicious network traffic and unauthorised access attempts.
- **Behavioural monitoring**: Monitor user and system behaviour to detect anomalies that may indicate malicious activity.
- **SIEM/security analytics**: Consolidate and correlate security data from various sources to gain a comprehensive view of the security posture.
- **Explore the real-world benefits of consolidating these tools into a single platform**: Examine the advantages of adopting a SIEM platform that integrates multiple security monitoring tools into a single, unified solution. This can streamline operations, improve efficiency, and enhance visibility into the security environment.

3.4 Intelligence

Understand the differences among the types of threat intelligence: Differentiate between these types of threat intelligence and their specific applications within the SOC:

- **Strategic Intelligence (SI):** Provides long-term analysis of emerging threats and trends to inform risk management strategies.
- **Tactical Intelligence (TI)**: Provides real-time, actionable insights into ongoing threats and attacks.
- **Operational Intelligence (OI)**: Provides contextual information about specific threats and attack vectors to guide incident response efforts.
- **Contextual Intelligence (CI)**: Provides information about the context of a threat, such as the motivations of the threat actor, their target, and their potential impact.
- **Attribution Intelligence (AI)**: Provides evidence that can be used to identify the perpetrator of a threat.

3.5 Core SOC tasks

The core functionalities of a SOC revolve around two primary tasks:

Establishing a Comprehensive Data Infrastructure:

- Efficiently configure security monitoring tools to receive raw, security-relevant data generated by various IT components, including firewall logs, login/logoff events, persistent outbound data transfers, firewall allows/denies, and more.

- Ensure that all critical cloud and on-premises infrastructure, such as firewalls, database servers, file servers, domain controllers, Domain Name System (DNS) servers, email servers, web servers, and Active Directory, are seamlessly sending their logs to a centralised log management, log analytics, or SIEM platform.

Leveraging Analytic Tools to Detect and Investigate Security Threats

- **Identify and investigate suspicious or malicious activity**: Employ these tools to identify and investigate suspicious or malicious activity by analysing security alerts, analysing Indicators Of Compromise (IOC) such as file hashes, IP addresses, domains, and other digital fingerprints, and reviewing and editing event correlation rules to enhance threat detection capabilities.
- **Prioritise alerts**: Prioritise alerts based on their criticality and scope of impact to ensure timely and effective response.
- **In-depth investigations**: Conduct in-depth investigations to determine the source, nature, and extent of any potential intrusion.
- **Evaluate attribution**: Evaluate attribution, identifying the responsible parties or threat actors, to gain a better understanding of the attack methods and tactics.
- **Share findings**: Share findings with the broader threat intelligence community, contributing to the collective knowledge base and enhancing the overall security posture.

4 People

Security operations organisations need to optimise their resources and staffing to effectively manage the ever-growing threat landscape.

4.1 Introduction

Security operations organisations are as diverse as the companies they serve. In some organisations, the executive team fully grasps the significance of cybersecurity to the organisation's financial well-being. Consequently, the SOC team enjoys a favourable position, with ample funding for high quality tools, adequate personnel to manage them, and the "human capital" of executive visibility and support.

However, this is not the reality for most organisations. Security teams often find themselves vying for budgetary resources against other departments, frequently those responsible for developing products and solutions that directly contribute to the organisation's profits. Most SOC teams are constantly battling fires, lacking the staff, time, and visibility to effectively manage their responsibilities.

4.2 The SOC Team

This is why it is crucial to focus on streamlining the SOC toolset and optimising the SOC team's structure. By creating a SOC team equipped with the right skills and utilising the minimal amount of resources while maintaining comprehensive visibility into active and emerging threats, organisations can achieve their cybersecurity goals.

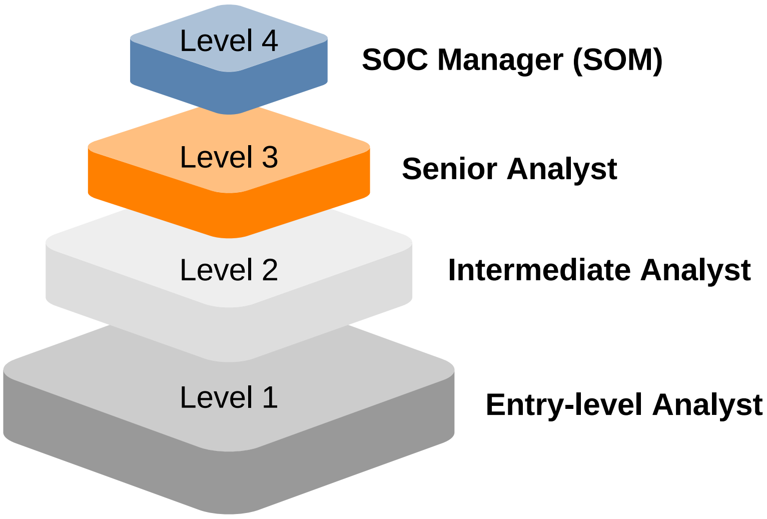

Figure 1: SOC roles

As illustrated in Figure 1, consider the SOC staff under four levels. The bulk of the initial work is carried out by Security Analysts under a SOC Manager (SOM).

4.2.1 Level 1: Entry-level Analyst

This role is the triage specialist who discern real threats from false alarms. This role is similar to that of a nurse in the first stage of Accident & Emergency (A&E) at a hospital. Such analysts require the following competencies:

- **System Administration:** Expertise in GNU/Linux, macOS, and Windows environments.
- **Programming:** Proficient in programming languages such as Python, Ruby, PHP, C, C++, Java, Perl.
- **Security:** Possesses training as Information Systems Security Professional, Intrusion Analyst Certification, Incident Handler, Forensic Analyst, Forensic Examiner.

Analysts at this level are responsible for:

- **Alert Analysis:** Promptly reviews incoming alerts to assess their relevance and urgency.
- **Incident Ticket Creation:** Raises new trouble tickets for alerts indicating potential incidents requiring Tier 2 or Incident Response scrutiny.
- **Vulnerability Assessment:** Conducts vulnerability scans and evaluates vulnerability assessment reports.
- **Security Monitoring Tool Management:** Manages and configures security monitoring tools, such as IDS and correlation rules.

4.2.2 Level 2: Intermediate Analyst

This is the incident responder role whose competencies are:

- **Triage Specialist**: Possesses the skills and experience of a Tier 1 Analyst, including alert analysis, incident ticket creation, and vulnerability assessment.
- **Curiosity and Investigative Prowess**: Exhibits a natural ability to dig deep, tenacity to uncover the root cause of incidents, and the composure to think clearly under pressure.
- **White Hat Hacking Experience**: Prior experience as a white hat hacker provides unique insights into attacker techniques and methodologies, enabling effective incident response.

Responsibilities for such incident responders are:

- **Incident Triage**: Assesses trouble tickets generated by Tier 1 Analysts, prioritising and escalating critical incidents.
- **Incident Investigation**: Leverages emerging threat intelligence, including IOCs and updated rules, to identify affected systems and the scope of the attack.
- **System Data Acquisition**: Collects and analyses asset data, such as system configurations, running processes, and logs, to gain a comprehensive understanding of the incident.

- **Incident Remediation and Recovery**: Determines and directs remediation and recovery actions to mitigate the impact of the attack and restore normal system operations.
- **Incident Documentation**: Maintains detailed incident documentation, including investigative findings, remediation steps, and lessons learned, to inform future incident responses and improve overall security posture.

4.2.3 Level 3: Senior Analyst

The Senior Analyst role is that of a threat hunter who hunts for stealthy threats that may have found their way inside an organisation's network, often using advanced tools and techniques. The threat hunter role also defends against known and emerging threats by proactively identifying and neutralising them. This is the threat hunter role whose competencies are:

- **Strong understanding of cybersecurity principles and practices**: Possesses a comprehensive grasp of cybersecurity concepts, methodologies, and best practices to effectively identify, assess, and mitigate cyber threats.
- **Expertise in security tools and technologies**: Demonstrates proficiency in utilising various security tools and technologies, including SIEM, Endpoint Detection and Response (EDR), and penetration testing tools, to gather, analyse, and interpret security data.
- **Familiarity with data visualisation tools**: Capable of employing data visualisation tools effectively to translate complex security data into clear and actionable insights.
- **Creative and analytical thinking**: Exhibits the ability to think creatively and outside the box to uncover anomalous patterns and suspicious activities indicative of potential threats.
- **Exceptional communication and collaboration skills**: Possesses strong communication and collaboration skills to effectively interact with other security professionals, stakeholders, and external parties.

Additional Skills associated with the role are:

- **Threat intelligence familiarity**: Possesses a working knowledge of threat intelligence sources and methodologies to stay informed about emerging threats and trends.
- **Penetration testing and vulnerability assessment experience**: Demonstrates experience in conducting penetration tests and vulnerability assessments to evaluate system security posture and identify weaknesses.
- **Industry best practices for threat hunting**: Possesses knowledge of industry best practices for threat hunting methodologies and techniques.

The Senior Analyst has the following responsibilities:

- **Asset discovery and vulnerability assessment review**: Reviews asset discovery and vulnerability assessment data to identify potential security risks and prioritise remediation efforts.
- **Threat hunting campaign development and execution**: Develops and implements threat hunting campaigns to proactively identify and neutralise hidden threats lurking within the organisation's network.
- **Penetration testing on production systems**: Conducts penetration tests on production systems to validate security posture, identify vulnerabilities, and assess potential attack vectors.
- **Security monitoring tool and technique recommendations**: Recommends and implements security monitoring tools and techniques based on threat-hunting findings to enhance overall security visibility.
- **Staying up-to-date on threat intelligence and emerging threats**: Continuously monitors and stays abreast of the latest threat intelligence and emerging threat trends to proactively address evolving cyber threats.
- **Collaboration with security professionals for cybersecurity strategy**: Collaborates with other security professionals to develop and maintain a comprehensive cybersecurity strategy that aligns with the organisation's risk profile and business objectives.

A Senior Analyst would be expected to have a Masters degree in computer science, cybersecurity, or a related field as well as certifications and/or experience in Cyber Threat Hunting methodologies and practices. Additionally, a minimum of at least 3 years of experience in the cybersecurity domain, encompassing various aspects of security operations, incident response, and threat mitigation plus a year or more in threat hunting, applying proactive techniques to identify and neutralise hidden threats within the organisation's environment.

4.2.4 Level 4: SOC Manager

The SOM plays the role of Chief Operating Officer for Operations and Management and is expected to have the following competencies:

- **Thorough understanding of cybersecurity principles, practices, and methodologies**: Possesses a comprehensive grasp of cybersecurity concepts, methodologies, and best practices to effectively manage and lead the SOC team.
- **Expertise in security operations and incident response**: Demonstrates proficiency in managing security operations, incident response, and threat mitigation strategies to protect the organisation's IT infrastructure and data.
- **Strong leadership and communication skills**: Exhibits exceptional leadership qualities to motivate, guide, and inspire the SOC team, effectively communicating security strategies and incident updates to stakeholders.
- **Exceptional organisational and time management skills**: Possesses strong organisational and time management skills to oversee the SOC's operations, ensuring efficient task execution and timely resolution of security incidents.

- **Demonstrated ability to prioritise and manage multiple tasks simultaneously**: Demonstrates the ability to handle multiple tasks concurrently, prioritising critical issues and delegating tasks effectively to maintain operational efficiency.

The SOC Manager has the following responsibilities:

- **Supervising the activity of the SOC team**: Provides direct supervision to the SOC team, ensuring that team members are aligned with security policies, procedures, and incident response protocols.
- **Recruiting, hiring, training, and assessing staff**: Oversees the recruitment, hiring, training, and performance assessment of SOC personnel, ensuring the team possesses the necessary skills and expertise to effectively handle security threats.
- **Managing the escalation process and reviewing incident reports**: Establishes and manages the escalation process for security incidents, ensuring timely and appropriate escalation to senior management or external parties when necessary.
- **Developing and executing a crisis communication plan**: Develops and implements a comprehensive crisis communication plan to effectively handle security breaches and communicate incident details to the Chief Information Security Officer (CISO), other stakeholders, and the public when necessary.
- **Running compliance reports and supporting the audit process**: Compiles and analyses security compliance reports, ensuring alignment with industry standards and regulatory requirements. Collaborates with auditors to support audit activities and demonstrate SOC's compliance posture.
- **Measuring SOC performance metrics and communicating the value of security operations to business leaders**: Regularly tracks and analyses SOC performance metrics, such as response times, incident resolution rates, and compliance adherence. Communicates the value of SOC operations to business leaders, demonstrating the impact of security measures on business continuity and risk mitigation.

4.3 The Threat Intelligence team

Very well resourced SOC teams may develop a separate dedicated threat intelligence function. This team, staffed by one or more analysts, involves managing multiple sources of threat intelligence data, verifying its relevance, and collaborating with the larger threat intelligence community on indicators artefacts, attribution, and other details surrounding an adversary's Tools, Tactics and Procedures (TTP). For smaller SOC teams it is necessary to automate the consumption of threat intelligence from a reliable cyber threat intelligence service provider such as CyberCube, Cyberhaven, Cybersixgill, IBM X-Force Intelligence, CrowdStrike Falcon X, Mandiant Threat Intelligence, Recorded Future amongst others.

4.4 Managed Security Service Provider

A MSSP, is a company that provides outsourced cybersecurity services to other organisations. MSSPs typically offer a wide range of services, including:

- **Security monitoring and threat detection**: MSSPs use a variety of tools and technologies to monitor their clients' networks and systems for signs of compromise. This includes monitoring for suspicious activity, such as malware infections or unauthorised access attempts.
- **Incident response**: If a security incident occurs, MSSPs are able to respond quickly and effectively to contain the incident, minimise its impact, and restore normal operations.
- **Vulnerability management**: MSSPs help their clients identify and remediate vulnerabilities in their systems and software. This helps to reduce the risk of cyberattacks.
- **Compliance**: MSSPs can help their clients meet their compliance requirements with various regulations, such as PCI (PCI DSS), General Data Protection Regulation (GDPR)[1], and System and Organisation Controls for Cybersecurity[2].
- **Threat intelligence**: MSSPs provide their clients with threat intelligence, which is information about the latest threats and vulnerabilities. This helps their clients to make informed decisions about their security posture. Ekco, Cyber Risk Alliance, NCC Group, Securicon are all organisations that offer such services.

4.4.1 SOC or MSSP?

The decision of whether to establish an in-house SOC or to outsource cybersecurity to an MSSP depends on various factors, including the size and complexity of the organisation, its budget, its security expertise, and its risk tolerance.

The case for in-house SOC

An in-house SOC provides several advantages, including:

- **Full control over security operations**: The organisation has full control over its security operations, which may be important for organisations with highly sensitive data or critical infrastructure.
- **Deeper understanding of the organisation's environment**: The SOC team has a deep understanding of the organisation's environment, which can help them to identify and respond to threats more effectively.
- **Greater flexibility in service offerings**: The organisation can tailor the services offered by the SOC to meet its specific needs.

However, there are also some disadvantages to an in-house SOC, including:

- **High upfront costs**: Establishing and maintaining an in-house SOC can be expensive, as it requires the hiring and training of security professionals, as well as the purchase of security tools and equipment.
- **Ongoing operational costs**: Maintaining an in-house SOC requires ongoing operational costs, such as salaries, training, and software maintenance.
- **Limited scalability**: An in-house SOC may not be able to scale up quickly to meet the demands of a growing organisation.

The case for MSSP

An MSSP can offer several advantages, including:

- **Reduced upfront costs**: Outsourcing cybersecurity to an MSSP can significantly reduce upfront costs, as the organisation does not need to hire and train security professionals or purchase security tools and equipment.
- **Scalability**: MSSPs can scale up or down quickly to meet the demands of a growing organisation.
- **Access to expertise**: MSSPs have access to a pool of experienced security professionals who can provide 24/7 monitoring and protection.

However, there are also some disadvantages to an MSSP, including:

- **Loss of control**: The organisation relinquishes control over its security operations to the MSSP.
- **Limited customisation**: The organisation may not be able to customise the services offered by the MSSP to meet its specific needs.
- **Potential for communication gaps**: Communication gaps can occur between the organisation and the MSSP, which can hinder incident response and decision-making.

The best approach for an organisation to choosing between an in-house SOC, and an MSSP, depends on its specific needs and circumstances. Organisations with highly sensitive data or critical infrastructure may want to consider establishing an in-house SOC to maintain full control over its security operations. However, organisations with limited resources or expertise may want to consider outsourcing cybersecurity to an MSSP to save costs and gain access to expertise. Figure 2 lists the key differences between an in-house SOC and an MSSP. Ultimately, the decision of whether to establish an in-house SOC or outsource cybersecurity to an MSSP is a business decision that should be made based on the specific needs and circumstances of the organisation.

Feature	In-house SOC	MSSP
Control over security operations	Full	Limited
Depth of understanding of the organisation's environment	Deep	Limited
Flexibility in service offerings	High	Low
Upfront costs	High	Low
Ongoing operational costs	High	Low
Scalability	Limited	High
Access to expertise	Limited	High
Customisation	High	Low
Communication	Direct	At-arm's length

Figure 2: Summary of the key differences between an in-house SOC and an MSSP

4.5 Summary

Securing an organisation's data and infrastructure against evolving cyber threats requires a robust SOC. However, the establishment and maintenance of an in-house SOC can be a costly and resource-intensive endeavour, especially for smaller organisations with limited budgets and expertise.

Fortunately, outsourced security services offered by MSSPs provide a cost-effective and scalable alternative. MSSPs leverage their deep expertise and specialised tools to monitor, detect, and respond to security threats, freeing up internal resources to focus on core business operations.

Organisations considering the choice between an in-house SOC and an MSSP should carefully evaluate their specific needs, budget, and risk tolerance to make an informed decision that aligns with their long-term security goals.

5 Processes and Procedures

5.1 Introduction

A SOC is a centralised unit within an organisation responsible for monitoring, analysing, and responding to security events. SOC processes are the set of procedures and practices that SOC teams use to effectively manage security risk. These processes typically include event classification and triage, prioritisation and analysis, remediation and recovery, and assessment and audit.

5.2 Overview of SOC Processes and Procedures

5.2.1 Event Classification and Triage

The first step in the SOC process is event classification and triage. This involves identifying and prioritising security events based on their severity and potential impact. SOC analysts use a variety of tools and techniques to classify events, such as threat intelligence, correlation rules, and machine learning algorithms. Once events have been classified, they are prioritised based on their potential impact on the organisation. Critical events are escalated to higher-level analysts for further investigation, while less critical events may be handled by lower-level analysts or automated systems.

5.2.2 Prioritisation and Analysis

After event classification, SOC analysts prioritise and analyse the most critical events. This involves gathering additional information about the events, such as the source, destination, and type of activity. SOC analysts also use a variety of tools and techniques to analyse events, such as IDS/IPS and log analysis tools. The goal of prioritisation and analysis is to determine the root cause of the event and to identify any potential threats or vulnerabilities.

5.2.3 Remediation and Recovery

Once the root cause of an event has been identified, SOC analysts work to remediate the issue and recover from the incident. This may involve patching vulnerabilities, removing malware, or restoring systems from backups. SOC analysts also work to contain the incident and prevent further damage. This may involve isolating affected systems, blocking malicious traffic, or notifying affected stakeholders.

5.2.4 Assessment and Audit

SOC teams regularly assess and audit their processes to ensure that they are effective and efficient. This involves conducting vulnerability assessments, penetration tests, and compliance audits. SOC teams also use data from security events to identify areas for improvement and to develop new mitigation strategies.

5.3 Using SIEM to Support SOC Processes

SIEM platforms that can help SOC teams automate and streamline their processes. SIEM provides a variety of features that support SOC processes, including:

- **Event classification and triage**: SIEM uses threat intelligence, correlation rules, and machine learning algorithms to classify events and prioritise them based on their severity and potential impact.
- **Prioritisation and analysis**: SIEM provides a variety of tools and techniques for analysing events, including IDS, IPS, and log analysis tools.
- **Remediation and recovery**: SIEM can automatically remediate some types of security events, and it can also help SOC teams to recover from incidents.
- **Assessment and audit**: SIEM provides a variety of tools for assessing and auditing SOC processes, including vulnerability assessments, penetration tests, and compliance audits.

SIEM can help SOC teams to improve their efficiency, effectiveness, and overall security posture.

5.4 Benefits of Implementing SOC Processes and Procedures

There are many benefits to implementing SOC processes, including:

- **Increased security**: SOC processes can help to identify and respond to security threats more quickly and effectively.
- **Reduced risk**: SOC processes can help to reduce the risk of data breaches, malware infections, and other security incidents.
- **Improved incident response**: SOC processes can help to improve the organisation's ability to respond to security incidents in a timely and effective manner.
- **Enhanced compliance**: SOC processes can help to ensure that the organisation is compliant with relevant security regulations.
- **Reduced costs**: SOC processes can help to reduce the costs of security incidents by preventing them from happening in the first place.

5.5 Summary

SOC processes are essential for any organisation that wants to protect its data and systems from security threats. By implementing SOC processes, organisations can improve their security posture, reduce risk, and enhance compliance. SIEM can help organisations to automate and streamline their SOC processes, making it easier and more efficient to protect their critical assets.

6 Tools

6.1 Introduction

To effectively monitor, analyse, and respond to security threats, SOCs rely on a suite of specialised tools. These tools work together to provide a comprehensive view of an organisation's security posture and enable SOC teams to identify and remediate threats quickly and efficiently.

6.2 The SOC toolkit

6.2.1 SIEM: The Central Component

SIEM is the cornerstone of a modern SOC. SIEM systems collect, analyse, and correlate security data from a variety of sources, including firewalls, IDS, security logs, network traffic, and endpoint devices. This data is then used to identify patterns and anomalies that may indicate a security threat. SIEM systems also generate alerts to notify SOC teams of potential threats and can be used to automate incident response procedures.

6.2.2 Other Essential SOC Tools

In addition to SIEM, there are a number of other tools that are essential for building a comprehensive SOC. These tools include:

- **Threat Intelligence Management**: Threat intelligence management tools provide SOC teams with access to real-time threat intelligence from a variety of sources, including security vendors, government agencies, and industry experts. This intelligence can be used to identify new threats, prioritise investigations, and develop mitigation strategies.
- **Intrusion Detection and Prevention**: IDS and IPS systems are used to detect and prevent unauthorised access to networks and systems. IDS systems passively monitor network traffic and identify suspicious activity, while IPS systems actively block malicious traffic.
- **Vulnerability Assessment and Management**: Vulnerability Assessment and Management (VulnA&M) tools scan networks and systems for vulnerabilities that could be exploited by attackers. These tools can be used to identify and prioritise vulnerabilities, develop remediation plans, and track the effectiveness of remediation efforts.
- **Endpoint Detection and Response**: EDR tools provide visibility into and control over endpoint security events. EDR tools can be used to detect and respond to malware infections, privilege escalation, and other endpoint threats.
- **Log Management**: Log management tools collect, centralise, and archive security logs from a variety of sources. These tools can be used to search, analyse, and correlate logs to identify patterns and anomalies that may indicate a security threat.

- **Incident Response**: Incident response tools automate the steps involved in responding to security incidents. These tools can be used to collect evidence, identify the root cause of an incident, and isolate and remediate affected systems.
- **Security Analytics**: Security analytics tools use machine learning and statistical techniques to gain insights from security data. These tools can be used to identify trends, patterns, and anomalies in security data that may indicate a security threat.
- **Security Orchestration, Automation, and Response**: Security Orchestration, Automation, and Response (SOAR) platforms automate security workflows and provide a centralised platform for managing security operations. SOAR platforms can be used to automate tasks such as incident response, threat hunting, and vulnerability management.

Examples of such tool suites in the Enterprise Information Technology (IT) domain include **AlienVault Unified Security Management (USM)**, **Palo Alto Networks Cortex XSOAR, Rapid7 InsightIDR and McAfee Enterprise Threat Intelligence Cloud. These** identify new threats, prioritise investigations, and develop mitigation strategies. For the Operational Technology (OT) domains the following are potential suites that can be considered when establishing a SOC:

- **Nozomi Networks N-SOAR**: Nozomi Networks N-SOAR is a SOAR platform that includes OT-specific threat intelligence management capabilities. Nozomi Networks N-SOAR can automatically ingest threat intelligence from a variety of sources, such as AlienVault OTX, and use it to automate security tasks, such as incident response, threat hunting, and vulnerability management in OT environments.
- **Cisco SecureOT**: Cisco SecureOT is a security platform that includes OT-specific threat intelligence management capabilities. Cisco SecureOT can collect threat intelligence from a variety of sources, such as Cisco Talos, and use it to automate security tasks, such as incident response, threat hunting, and vulnerability management in OT environments.
- **Siemens MindSphere Security**: Siemens MindSphere Security is a security platform that includes OT-specific threat intelligence management capabilities. Siemens MindSphere Security can collect threat intelligence from a variety of sources, such as Siemens Industrial Cyber Security, and use it to automate security tasks, such as incident response, threat hunting, and vulnerability management in OT environments.

There are other solutions such as Deepwatch Industrial Control Systems (ICS) Threat Intelligence, Dragos Edge, ABB Ability Security, Honeywell Forge, Schneider Electric EcoStruxure Security and Rockwell Automation FactoryTalk Security.

6.2.3 Choosing the Right SOC Tools

The specific tools that are needed for a SOC will vary depending on the size, complexity, and specific security needs of the organisation. However, all SOCs should have a core set of tools that includes SIEM, threat intelligence management, IDS/IPS, VulnA&M, EDR, and log management. Additional tools may be needed depending on the organisation's unique requirements.

6.3 Summary

A comprehensive suite of SOC tools is essential for organisations to effectively protect themselves from cyber threats. By collecting, analysing, and correlating security data, SOC teams can identify and respond to threats quickly and efficiently.

7 Threat Intelligence

7.1 Introduction

In the ever-evolving realm of cybersecurity, threat intelligence stands as a crucial pillar of effective defence. It encompasses the collection, analysis, and dissemination of information pertaining to potential threats, providing organisations with the necessary knowledge to proactively mitigate attacks. At its core, threat intelligence hinges on three key elements:

- Context,
- Attribution, and
- Action.

7.2 Threat Intelligence Elements

7.2.1 Context

Context provides the essential framework for understanding the significance of threat indicators. It answers questions such as:

- What role does this indicator play in the overall threat landscape?
- Does its presence signify the beginning of an attack or system compromise?
- Is this threat actor known for this type of behaviour?
- How sophisticated is this particular indicator?

Without context, threat indicators remain mere fragments of information, lacking the necessary depth to inform effective decision-making.

7.2.2 Attribution

Attribution delves into the identification of the threat actor behind a detected activity. Understanding the motivations and TTPs of the adversary is critical for formulating targeted mitigation strategies.

- Who is behind this attack, and what are their motives?
- What tools, infrastructure, and tactics do they employ?

By attributing attacks, organisations can gain valuable insights into the adversary's methods, enabling them to anticipate future attacks and fortify their defences accordingly.

7.2.3 Action

Effective threat intelligence goes beyond mere analysis; it drives proactive action. Organisations must translate intelligence into actionable insights that inform their security posture and response capabilities.

- What specific steps can be taken to detect and block future attacks?
- How can we strengthen our defences against the identified threat actor's TTPs?
- What information can we share with other organisations to improve collective security?

Actionable threat intelligence empowers organisations to move beyond reactive measures and embrace a proactive approach to security.

7.3 Variety of Threat Intelligence

Figure 3 categorises the various types of threat intelligence :

Type	Description	Purpose
Strategic (SI)	Provides a broad overview of the threat landscape, including trends, TTPs of threat actors.	Helps organisations understand the overall threat environment and identify potential threats to their systems and networks.
Tactical (TI)	Provides more specific information about specific threats, such as malware samples, attack vectors, and vulnerabilities.	Helps organisations prioritise their security efforts and develop targeted mitigation strategies.
Operational (OI)	Provides real-time or near real-time information about active threats, such as IOCs and threat alerts.	Helps organisations detect and respond to threats quickly and effectively.
Contextual (CI)	Provides information about the context of a threat, such as the motivations of the threat actor, their target, and their potential impact.	Helps organisations understand the reasoning behind a threat and make informed decisions about how to respond.
Attribution (AI)	Provides evidence that can be used to identify the perpetrator of a threat.	Helps organisations hold threat actors accountable for their actions and deter future attacks.

Figure 3: Types of Threat Intelligence

7.4 Threat Intelligence Sources

Organisations can gather threat intelligence from various sources, including:

- **Crowdsourced Intelligence**: This involves leveraging contributions from the cybersecurity community through platforms such as AlienVault - Open Threat Exchange (OTX).
- **Proprietary Intelligence**: This includes threat intelligence provided by cybersecurity vendors, often based on their own research and analysis.
- **DIY Intelligence**: This involves manually collecting and analysing intelligence from open-source sources.

Effective threat intelligence programmes often employ a combination of these approaches to leverage the strengths of each:

- Crowdsourced intelligence for timely and widespread threat coverage.
- Proprietary intelligence for high-fidelity and credible analysis.
- DIY intelligence for flexibility and tailored insights.

7.5 Summary

Threat intelligence stands as an invaluable tool in the cybersecurity arsenal, empowering organisations to make informed decisions, strengthen their defences, and proactively mitigate emerging threats. By understanding the core elements of threat intelligence, the spectrum of intelligence sources, and the complementary approaches to threat intelligence gathering, organisations can effectively navigate the ever-evolving threat landscape and safeguard their valuable assets.

8 Open-Source SOC

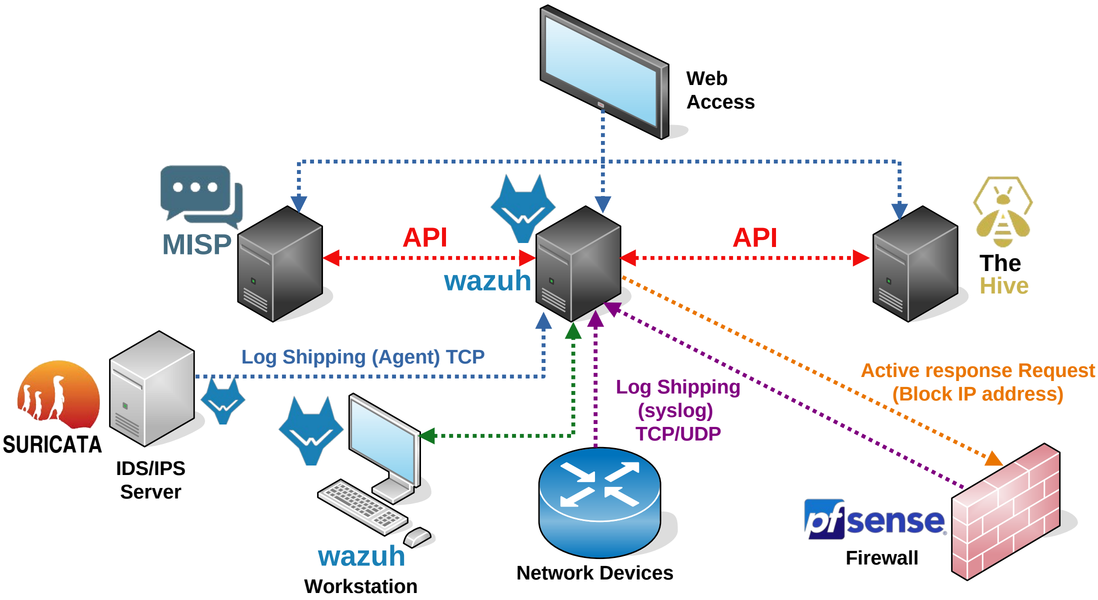

Figure 4: Open-Source SOC

An Open-Source SOC design, in Figure 4, illustrates how integrating multiple open-source solutions can significantly enhance security posture. It illustrates a network security architecture that uses various open-source security tools to protect its servers, workstations, and network devices. The architecture consists of open-source platforms:

- **Wazuh**: An endpoint security platform that collects security data from various sources, including system events, logs, files, and vulnerability information. It analyses this data to detect and respond to threats.
- **Suricata**: A network intrusion detection and prevention system (IDS/IPS) that monitors network traffic in real-time to detect and potentially block malicious activity.
- **TheHive**: A Security Incident Response (SIR) platform that helps teams manage and respond to security incidents effectively.
- **Malware Information Sharing Platform (MISP)**: A threat intelligence platform that facilitates the sharing and collaboration of threat information among security professionals and organisations.
- **pfSense**: A firewall and router software that provides powerful packet filtering, inspection, and security features.

The network devices in the diagram are protected by the firewall, and the workstations and servers are protected by both the firewall and Wazuh agents. Security events from all of these sources are collected and analysed by TheHive and MISP, which helps security teams to identify and respond to threats more effectively.

Overall, this network security architecture appears to be well-designed and leverages a number of powerful open-source tools to provide comprehensive protection for its assets.

8.1 Wazuh (SIEM/XDR)

Wazuh is a popular and versatile open-source platform designed for threat detection, prevention, and response. It unifies Extended Detection and Response (XDR) and SIEM protection across various environments, including, On-premises systems, Virtualised, Containerised and Cloud-based. This is achieved by combining two key components:

- **Central management server**: This server receives data from the agents, analyses it using threat intelligence, and provides actionable insights and alerts. Additionally, it offers a web-based dashboard for visualisation and management.
- **Lightweight endpoint security agents**: These agents are deployed on the systems to be monitored and collect a wide range of data, including system events, logs, files, and vulnerability information.

Wazuh detects malicious activities and IOCs using several methods, including:

- **Security Configuration Assessment (SCA)**: Identifies misconfigurations that could be exploited by attackers.
- **Rootkit detection**: Detects hidden processes and files that attackers might use.
- **File Integrity Monitoring (FIM)**: Monitors critical system files for unauthorised changes.
- **Malware detection**: Analyses logs and system activity for signs of malware infections.
- **Vulnerability scanning**: Wazuh identifies known vulnerabilities in systems and prioritises them based on risk.
- **Log analysis**: Wazuh collects and analyses logs from various sources, providing insights into system activity and potential security incidents.
- **Compliance reporting**: Wazuh helps meet various compliance requirements by generating reports on relevant security activities.
- **Container security**: Wazuh provides visibility into containerised environments, monitoring their behaviour and detecting threats and vulnerabilities.
- **Open-source and community-driven**: Wazuh is freely available and benefits from a large and active community, ensuring continuous development and improvement.

8.2 Suricata (IDS/IPS)

Suricata is a high-performance, open-source network IDS/IPS. It primarily operates at the network level, monitoring and analysing network traffic in real-time to detect and potentially block malicious activities.

Key Features of Suricata include:

- **Network traffic analysis**: Suricata captures and analyses network packets, looking for patterns that match predefined rules or signatures indicating suspicious or malicious activity.
- **Intrusion detection**: Identifies various threats like malware, Denial-of-Service (DoS) attacks, and unauthorised access attempts, providing alerts and logs for further investigation.
- **Intrusion prevention**: Can be configured to take action upon detecting threats, such as blocking malicious traffic or dropping connections.
- **Signature-based and anomaly-based detection**: Employs both pre-defined signatures for known threats and anomaly detection techniques to identify unusual network behaviour.
- **Multi-threading and performance**: Leverages multi-core processors for efficient analysis of large volumes of network traffic.
- **Open-source and community-driven**: Like Wazuh, Suricata benefits from an active community, ensuring development and updates.

Suricata software can be found:

- Monitoring network traffic for malicious activity in real-time.
- Detecting and preventing various network-based attacks.
- Gaining insights into network behaviour and potential security risks.
- Fulfilling compliance requirements related to network security monitoring.

Suricata and Wazuh, what is the difference:

- **Focus**: Suricata operates at the network level, while Wazuh focuses on endpoint and system security.
- **Functionality**: Suricata excels in real-time network traffic analysis and threat detection, while Wazuh offers broader security features like vulnerability scanning and log analysis.
- **Deployment**: Suricata is typically deployed on network monitoring devices or dedicated servers, while Wazuh agents are installed on individual systems.

Both Suricata and Wazuh are valuable tools that serve different purposes. Suricata's focus is real-time network monitoring and threat detection, while Wazuh provides a broader set of security features across systems and endpoints. Choosing the right tool depends on your specific security needs and the areas you want to prioritise.

8.3 TheHive Project

TheHive Project, is an open-source platform for SIR. It is a platform that combines multiple tools and functionalities to aid in the management and response to security incidents effectively.

The Hive Project key features are:

- **Case management**: Create and manage cases for each incident, tracking details like timeline, observations, tasks, and communication.
- **Collaboration**: Enables teams to work together on investigations, assigning tasks, sharing information, and discussing findings.
- **Threat intelligence integration**: Connects to threat intelligence feeds and platforms, enriching investigations with relevant context.
- **Automation**: Automate repetitive tasks and workflows, streamlining incident response processes.
- **Visualisation**: Provides customisable dashboards and reports to visualise investigation progress and key findings.
- **Open-source and community-driven**: Freely available and backed by a large community, ensuring continuous development and improvement.

The Hive Project, streamlines the investigation process, saves time, and reduces manual effort while enabling SOC teams to work together seamlessly, leading to faster and more effective resolutions. Through increased visibility it provides clear insights into incidents, improving situational awareness and decision-making. The platform encompasses:

- **TheHive**: The core platform for case management and collaboration.
- **Cortex**: An optional add-on for automated threat analysis and response actions.
- **MISP**: A separate platform for sharing threat intelligence, which can be integrated with TheHive.

The Hive is a powerful and versatile platform for managing and responding to security incidents effectively.

8.4 Malware Information Sharing Platform

MISP is an open-source threat intelligence platform. It provides tools and functionalities for collecting, storing, sharing, and analysing cybersecurity IOCs and other threat intelligence information. It an be considered as a hub that facilitates:

- **Share threat information**: Upload and share details about malware, vulnerabilities, attack campaigns, and other security threats.
- **Collaborate on analysis**: Work together to understand threats, identify their scope, and develop mitigation strategies.
- **Store and organise information**: Maintain a structured repository of threat intelligence for future reference and analysis.
- **Automate threat sharing**: Integrate with other security tools and platforms to automate the exchange of threat data.

Some key features of MISP are:

- **Taxonomies and tagging**: Enables consistent classification and organisation of threat information using standardised categories and tags.
- **Relationship linking**: Allows users to connect different pieces of information, revealing broader attack patterns.
- **Attribute-based Access Control (ABAC)**: Provides granular control over who can access and share specific information.
- **Open-source and community-driven**: Freely available and supported by a large and active community of security professionals.

MISP improves threat detection and analysis, through sharing and collaboration, leading to better understanding of threats and faster response times. It provides an enhanced situational awareness of the threat landscape and potential risks. This leads to reduced time to mitigation as collaboration and information sharing are streamlined, enabling quicker response to incidents.

8.5 PfSense Firewall

pfSense is a popular open-source firewall and router software built on the FreeBSD operating system. It is used in various environments, from home networks to large businesses and organisations, providing robust security and advanced networking features. Here is a breakdown of its key characteristics:

- **Stateful firewall**: It provides powerful packet filtering and inspection, controlling inbound and outbound traffic based on pre-defined rules and security policies.
- **Network Address Translation**: Network Address Translation (NAT) enables efficient sharing of a single public IP address among multiple devices on your network.
- **Virtual Private Network**: It supports various Virtual Private Network (VPN) protocols such as OpenVPN and IPsec to create secure encrypted tunnels for remote access.
- **Dynamic Host Configuration Protocol**: pfSense automatically assigns IP addresses to devices on the network using Dynamic Host Configuration Protocol (DHCP), simplifying network management.
- **Domain Name System server**: A Domain Name System (DNS) function resolves domain names to IP addresses, allowing devices to access websites efficiently.
- **Load balancing**: Distributes traffic across multiple Internet connections for improved performance and redundancy.

PfSense has the following key features:

- **Flexible and customisable**: Offers a wide range of configuration options to suit diverse network needs.
- **High performance**: Efficiently handles large volumes of network traffic.
- **Advanced security features**: Supports various security protocols, intrusion detection/prevention, and content filtering.
- **Web-based interface**: Provides a user-friendly interface for configuration and management.
- **Open-source and community-driven**: Freely available with ongoing development and support from a vast community.

PfSense can be deployed in dedicated hardware for optimal performance and security; however, it can also run as a virtual machine on a hypervisor such as VMware or Kernel Virtual Machine (KVM) for flexibility and resource sharing. It is also possible to deploy pfSense in cloud environments like Amazon Web Services (AWS).

9 Bibliography

[1] Regulation (EU) 2016/679, *EU General Data Protection Regulation (GDPR)*. 2016. Accessed: Mar. 10, 2020. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] AICPA and CIMA, ‘SOC for Cybersecurity’, https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-for-cybersecurity. Accessed: Feb. 01, 2024. [Online]. Available: https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-for-cybersecurity

This page is intentionally blank