Topic 5
Security Operations Centre (SOC)

Dr Diarmuid Ó Briain

12 Mar 2025

setu.ie
INSPIRING FUTURES

Version: 1.0

Licence

Security Operations Centre (SOC)

A SOC is a centralised hub for monitoring, analysing, detecting, and responding to cybersecurity threats.

It serves as the focal point of a cybersecurity posture, providing a 24/7 watch over its IT and OT infrastructure to identify and mitigate potential security breaches.

Learning 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.

Functions of a SOC

- Threat Detection and Analysis
- Incident Response
- Compliance and Risk Management

Components of a SOC

- People
- Technology
- Processes and Procedures

Benefits of implementing a SOC

- Enhanced Security Posture
- Reduced Response Times
- Improved Compliance
- Reduced Risk of Data Breaches
- Enhanced Customer Confidence

Building a SOC

- **People**: The SOC Team
  - Review key SOC roles and responsibilities
  - Examine the SOC skillset matrix
- **Processes and Procedures**
  - Establish the key processes and procedures required to build a SOC
    - Event classification and triage
    - Prioritisation and analysis
    - Remediation and recovery
    - Assessment and audit
    - Examine tools that help centralise these processes and manage them

Building a SOC

- **Tools**
  - Review the essential security monitoring tools required for building a SOC
    - Asset discovery
    - Vulnerability assessment
    - Intrusion detection
    - Behavioural monitoring
    - SIEM/security analytics
    - Explore the real-world benefits of consolidating these tools into a single platform

Building a SOC

- **Intelligence**
  - Understand the differences among the types of intelligence
  - Differentiate between the different types of threat intelligence and their specific applications within the SOC
    - Strategic Intelligence (SI)
    - Tactical Intelligence (TI)
    - Operational Intelligence (OI)
    - Contextual Intelligence (CI)
    - Attribution Intelligence (AI)
    -

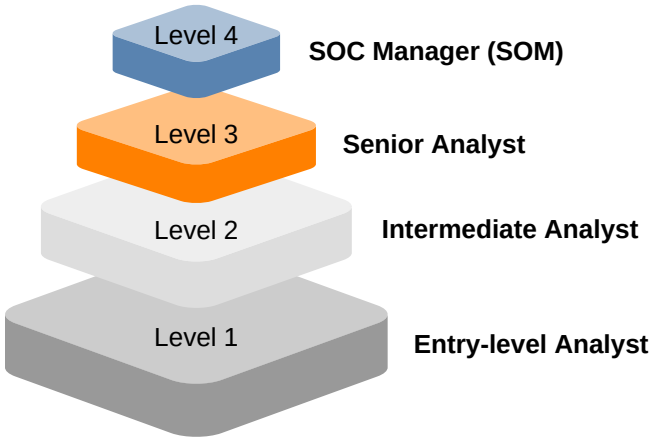
Core SOC tasks

- Establishing a comprehensive data infrastructure
  - Security monitoring tools
  - Centralised log management from infrastructure
- Leveraging Analytic Tools
  - Identify and investigate suspicious or malicious activity
  - Prioritise alerts
  - In-depth investigations
  - Evaluate attribution
  - Share findings

The SOC Team

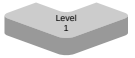
- **Uneven Playing Field**: Cybersecurity budgets often compete with other departments, leaving SOC teams under-resourced.
- **Resource Constraints**: Most SOC teams lack staff, time, and visibility to effectively manage their responsibilities.
- **Focus on Optimisation**: Streamlining tools and structures can maximise efficiency within budgetary limitations.
- **Right Skills, Minimal Resources**: Building a lean, skilled SOC team ensures adequate threat visibility and response.
- **Achieving Goals**: Optimised SOCs are better equipped to defend organisations against cyber threats.

SOC Roles



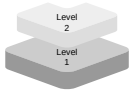
Level 1: Entry-level Analyst

- **Role**: Triage specialist, identifying real threats from false alarms.
- **Skills**: System administration (Linux, macOS, Windows), programming (Python, Ruby, etc.), security certifications (CISSP, etc.).
- **Responsibilities**: Analyse alerts, create incident tickets, conduct vulnerability assessments, manage security monitoring tools.



Level 2: Intermediate Analyst

- **Skills**: Builds on Tier 1 expertise (alerts, tickets, vulnerabilities)
- **Qualities**: Curiosity, strong investigation skills, composure under pressure
- **Bonus**: White hat hacking experience for attacker insights
- **Responsibilities**:
  - Prioritise and escalate critical incidents.
  - Investigate using threat intelligence and identify affected systems.
  - Collect and analyse data to understand the incident scope.
  - Direct remediation and recovery actions.
  - Document findings, steps taken, and lessons learned.

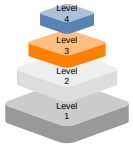


Level 3: Senior Analyst

- **Skills**: Cybersecurity knowledge, security tools expertise, data visualisation, creative thinking, strong communication.
- **Additional Skills**: Threat intelligence, penetration testing, industry best practices.
- **Responsibilities**: Assess risks, develop threat hunting campaigns, conduct penetration tests, recommend security tools, stay informed on threats, collaborate on strategy.
- **Experience**: Masters degree in computer science/cybersecurity (or related field) and 3+ years cybersecurity experience with 1+ year in threat hunting.

Level 4: SOC Manager

- **Leads SOC team**: Manages and inspires SOC team, ensuring alignment with security policies and effective incident response.
- **Security & Operations Expert**: Possesses deep understanding of cybersecurity, incident response, and operations management.
- **Communication Master**: Motivates team, communicates effectively with stakeholders, develops crisis communication plans.
- **Compliance Champion**: Ensures SOC adherence to industry standards and regulations, supports audit processes.
- **Metrics & Value Driven**: Tracks performance, showcases SOC's impact on business continuity and risk mitigation.



Threat Intelligence Team

- **Dedicated Threat Intel Team (Large SOCs)**: Analyses and shares threat data, collaborates with the wider community.
- **Automated Threat Intel (Smaller SOCs)**: Integrates data from reliable threat intelligence providers.
- **Benefits of Automated Solutions**: Saves resources, ensures constant threat awareness.
- **Variety of Providers**: Cyberhaven, IBM X-Force, or Recorded Future.
- **Tailored Approach**: Size the SOC solution to the organisations needs and the available resources.

Managed Security Service Provider

- Security monitoring and threat detection
- Incident response
- Vulnerability management
- Compliance

The case for a SOC

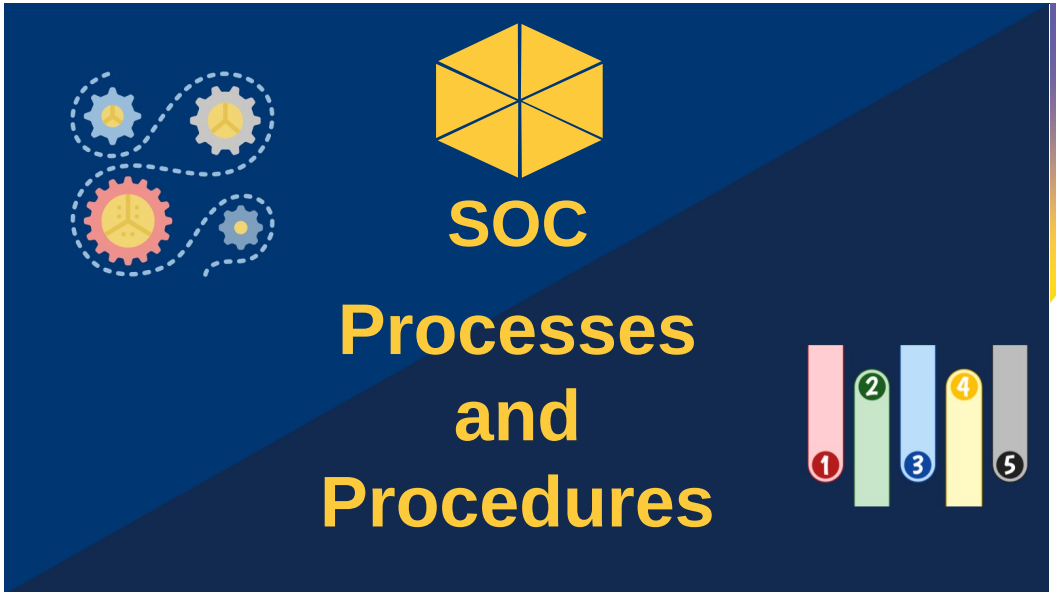
- **Advantages**
  - Full control over security operations
  - Deeper understanding of the organisation's environment
  - Greater flexibility in service offerings
- **Disadvantages**
  - High upfront costs
  - Ongoing operational costs
  - Limited scalability

The case for a MSSP

- **Advantages**
  - Reduced upfront costs
  - Scalability
  - Access to expertise
- **Disadvantages**
  - Loss of control
  - Limited customisation
  - Potential for communication gaps

Key differences between the SOC and MSSP

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



SOC Processes and Procedures

- Event Classification and Triage
- Prioritisation and Analysis
- Remediation and Recovery
- Assessment and Audit

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
  - Prioritisation and analysis
  - Remediation and recovery
  - Assessment and audit

Benefits of Implementing SOC Processes

- Increased security
- Reduced risk
- Improved incident response
- Enhanced compliance
- Reduced costs

SOC Toolkit

- **Importance**: Specialised tools are crucial for SOCs to efficiently monitor, analyse, and respond to security threats.
- **Functionality**: These tools work together to provide a comprehensive view of an organisation's security posture.
- **Benefits**: Enable SOC teams to quickly identify and remediate threats.
- **SIEM**: The central component, collecting and analysing data from various sources to identify potential threats.
- **SIEM capabilities**: Generating alerts, automating incident response procedures.

Other essential tools in the SOC Toolkit

- Threat Intelligence Management
- Intrusion Detection and Prevention
- Vulnerability Assessment and Management
- Endpoint Detection and Response
- Log Management
- Incident Response
- Security Analytics
- Security Orchestration, Automation, and Response

Commercial Tools

- Enterprise domain tools
  - AlienVault Unified Security Management (USM)
  - Palo Alto Networks Cortex XSOAR
  - Rapid7 InsightIDRMcAfee Enterprise Threat Intelligence Cloud
- Operational Technology (OT) domain tools
  - Nozomi Networks N-SOAR
  - Cisco SecureOT
  - Siemens MindSphere Security

Summary

- **Core SOC tools**: SIEM, threat intelligence management, IDS/IPS, VulnA&M, EDR, and log management. These provide fundamental threat detection, analysis, and response capabilities.
- **Tailored approach**: Specific tool needs depend on organisation size, complexity, and unique security concerns.
- **Flexibility**: Additional tools can be added to address specific security challenges, ensuring a comprehensive approach.
- **Focus on core**: The core set of tools listed above should be prioritised for any SOC, regardless of specific needs.

Threat Intelligence

- Context,
- Attribution
- Action.

Threat Intelligence - Context

- Context provides the essential framework for understanding the significance of threat indicators.
  - 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?

Threat Intelligence - 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?

Threat Intelligence - 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?

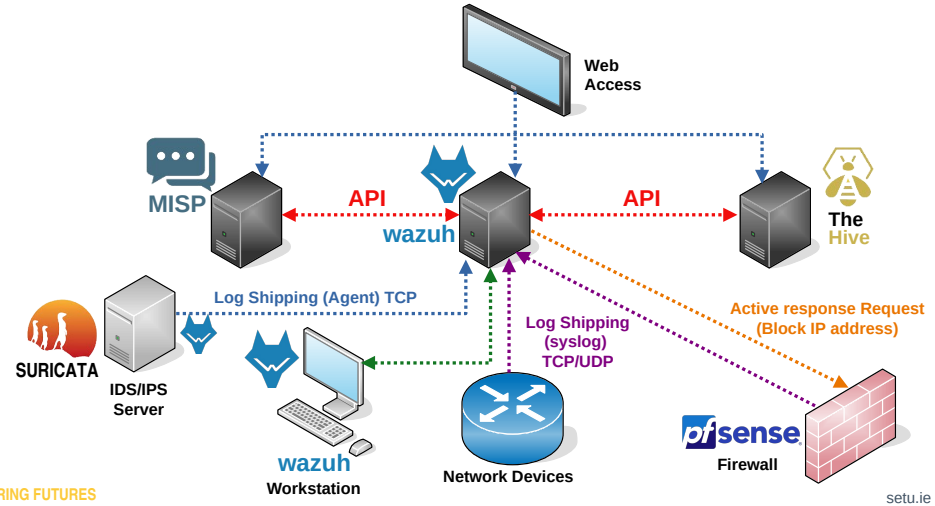
Threat Intelligence Category summary

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.

Threat Intelligence Sources

- **Crowdsourced Intelligence**: This involves leveraging contributions from the cybersecurity community through platforms such as AlienVault - 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.

Open-Source SOC



Wazuh (SIEM/XDR)

- Threat detection, prevention, and response
- Unifies XDR and SIEM protection across various environments,
  - On-premises systems
  - Virtualised
  - Containerised
  - Cloud-based
- Two key components:
  - Central management server
  - Lightweight endpoint security agents

wazuh

Wazuh (SIEM/XDR) detection methods

- Threat detection
- Security Configuration Assessment (SCA)
- Rootkit detection
- File Integrity Monitoring (FIM)
- Malware detection
- Vulnerability scanning
- Log analysis
- Compliance reporting
- Container security
- Open-source and community-driven

wazuh

Suricata (IDS/IPS)

- Network IDS/IPS monitoring and analysing network traffic in real-time to detect and potentially block malicious activities.
- Key Features of Suricata include:
  - Network traffic analysis
  - Intrusion detection
  - Intrusion prevention
  - Signature-based and anomaly-based detection
  - Multi-threading and performance
  - Open-source and community-driven

Suricata (IDS/IPS) functions

- 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

Wazuh -vs- Suricata

- **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

The Hive Project (SIR)

- Combines multiple tools and functionalities to aid in the management and response to security incidents effectively
- The Hive Project key features are:
  - Case management
  - Collaboration
  - Threat intelligence integration
  - Automation
  - Visualisation
  - Open-Source and Community driven

The Hive Project (SIR)

- 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

Malware Information Sharing Platform

- Collects, stores, shares, and analyses IOCs and other threat intelligence information
- It an be considered as a hub that facilitates:
  - Share threat information
  - Collaborate on analysis
  - Store and organise information
  - Automate threat sharing

MISP

Malware Information Sharing Platform

- Some key features of MISP are:
  - Taxonomies and tagging
  - Relationship linking
  - Attribute-based Access Control (ABAC)
  - Open-source and community-driven

MISP

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.
- pfSense key characteristics:
  - Stateful firewall
  - Network Address Translation
  - Virtual Private Network
  - DHCP
  - DNS server
  - Load balancing

Firewall

pfSense Firewall features

- Flexible and customisable
- High performance
- Advanced security features
- Web-based interface
- Open-source and community-driven

pfsense Firewall

Revision

QUIZ

setu.ie
INSPIRING FUTURES

Question 1

- **What is the primary function of a SOC?**
  - ☐ Data storage and analysis
  - ☐ Monitoring, analysing, and responding to security threats
  - ☐ Network infrastructure management
  - ☐ Software development

Question 1

- **What is the primary function of a SOC?**
  - ☒ Data storage and analysis
  - ☑ Monitoring, analysing, and responding to security threats
  - ☒ Network infrastructure management
  - ☒ Software development

Question 2

- **What is the core component of a modern SOC?**
  - ☐ Vulnerability management tool
  - ☐ Security information and event management
  - ☐ Intrusion detection/prevention system
  - ☐ Threat intelligence platform

Question 2

- **What is the core component of a modern SOC?**
  - ☒ Vulnerability management tool
  - ☑ Security information and event management
  - ☒ Intrusion detection/prevention system
  - ☒ Threat intelligence platform

Question 3

- **What are the benefits of implementing a SOC?**
  - ☐ Reduced costs for security personnel
  - ☐ Increased network downtime
  - ☐ Enhanced security posture and reduced risk of cyberattacks
  - ☐ More complex compliance processes

Question 3

- **What are the benefits of implementing a SOC?**
  - ☒ Reduced costs for security personnel
  - ☒ Increased network downtime
  - ☑ Enhanced security posture and reduced risk of cyberattacks
  - ☒ More complex compliance processes

Question 4

- **Which role within a SOC focuses on identifying and prioritising vulnerabilities?**

☐ Vulnerability assessment and management specialist

☐ Threat intelligence analyst

☐ Incident responder

☐ SOC manager

Question 4

- **Which role within a SOC focuses on identifying and prioritising vulnerabilities?**

☑ Vulnerability assessment and management specialist

☒ Threat intelligence analyst

☒ Incident responder

☒ SOC manager

Question 5

- **What are two factors that influence the specific tools needed by a SOC?**

☐ Brand preference and budget

☐ Pre-existing IT infrastructure

☐ Industry regulations and compliance requirements

☐ Organisation size, complexity, and security needs

Question 5

- **What are two factors that influence the specific tools needed by a SOC?**

☒ Brand preference and budget

☒ Pre-existing IT infrastructure

☑ Industry regulations and compliance requirements

☑ Organisation size, complexity, and security needs

Question 6

- **What are the different levels of expertise within a SOC analyst team?**

☐ Beginner, intermediate, advanced

☐ Entry-level, analyst, senior analyst, SOC manager

☐ Threat hunter, incident responder, vulnerability specialist, intelligence analyst

☐ Entry-level analyst, intermediate analyst, senior analyst, Database analyst

Question 6

- **What are the different levels of expertise within a SOC analyst team?**

☑ Beginner, intermediate, advanced

☑ Entry-level, analyst, senior analyst, SOC manager

☑ Threat hunter, incident responder, vulnerability specialist, intelligence analyst

☒ Entry-level analyst, intermediate analyst, senior analyst, Database analyst

Learning outcomes

- 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 ✓

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir

D +353 59 917 5426 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Thank you

engcore advancing technology