CS444 – Network Security Operations

Eng. Abdo Saeed

Lecture 1.1 — Introduction to Network Security Operations

What is SOC and NOC?

- SOC (Security Operations Center):

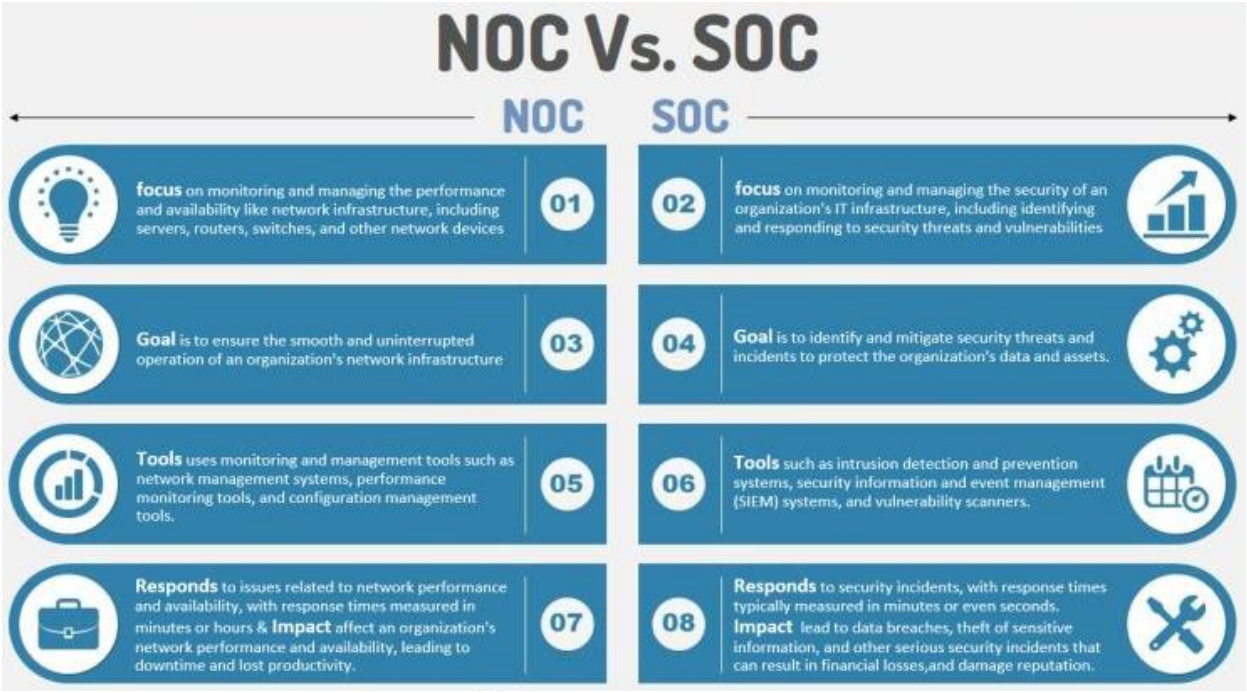
A team of IT security professionals (inside the company or outsourced) that works 24/7 to:

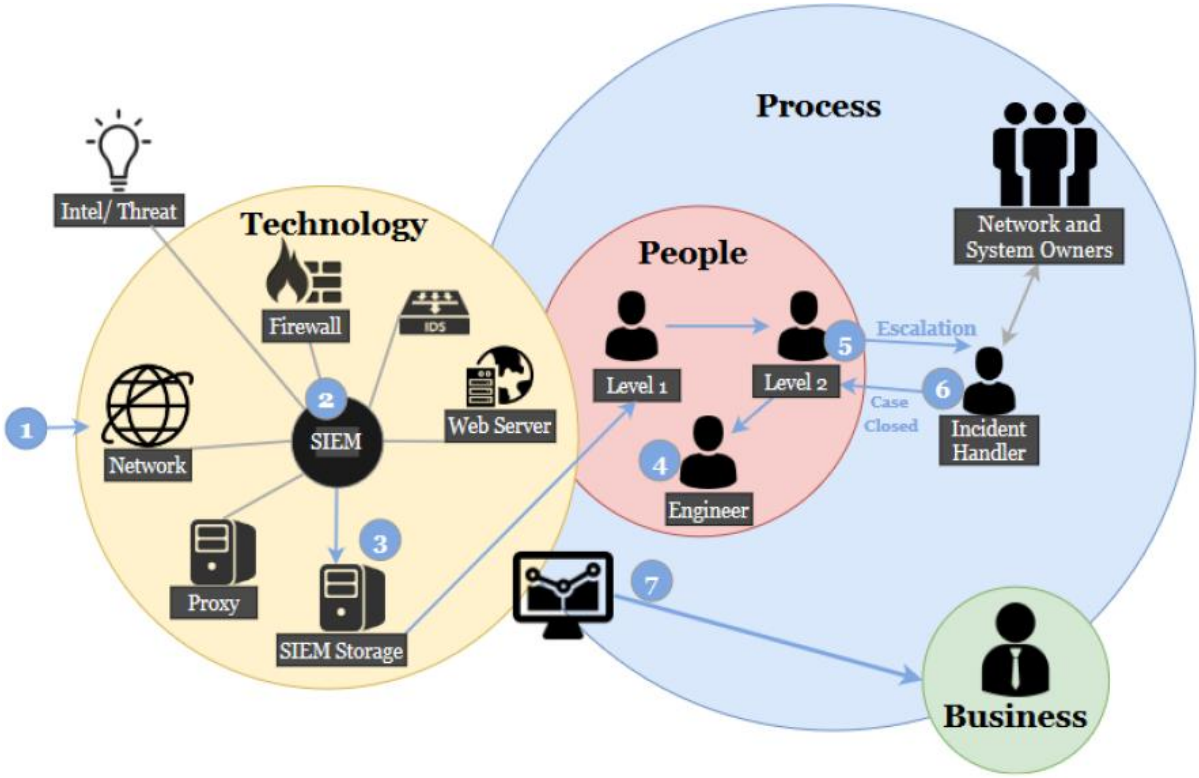
  - Monitor the IT infrastructure,
  - Detect cyberattacks in real time,
  - Respond quickly,
  - Manage security tools, and
  - Analyze threats to continuously improve the organization's security.
  - Also called ISOC (Information Security Operations Center).

- NOC (Network Operations Center):

NOC focuses on network monitoring and performance.

  - Ensures uptime, availability, and network health.
  - Works closely with SOC when incidents overlap (e.g., DDoS).





ALERTS FROM:

- Security Intelligence Platform
- Help Desk
- Other IT departments

Tier 1

- Monitoring
- Opens ticket and closes false positives
- Basic investigation and mitigation

Tier 2

- Deep Investigations
- Mitigation / recommends changes

Tier 3

- Advanced investigations
- Prevention
- Threat hunting
- Forensics
- Counter intelligence
- Malware reverser

Cybersecurity Management & SIEM





A **SIEM solution** supports SOCs in:

- Detecting and stopping threats.
- Proactively improving security.

Structure of a SOC

Level 1 – First Response:

The first line of incident responders. These security professionals **watch for alerts** and determine two things:

- The **urgency** of each alert
- When to **escalate an alert** up to Level 2
  - Level 1 Personnel (Employees) may also **manage security tools** and **run regular reports**.

Level 2 – Incident Resolution:

- Finds the root cause of the problem.
- Assess which part of the infrastructure is at risk.

Level 3 – Proactive Security Operations:

At Level 3 we begin moving from reactive to **proactive security actions.**

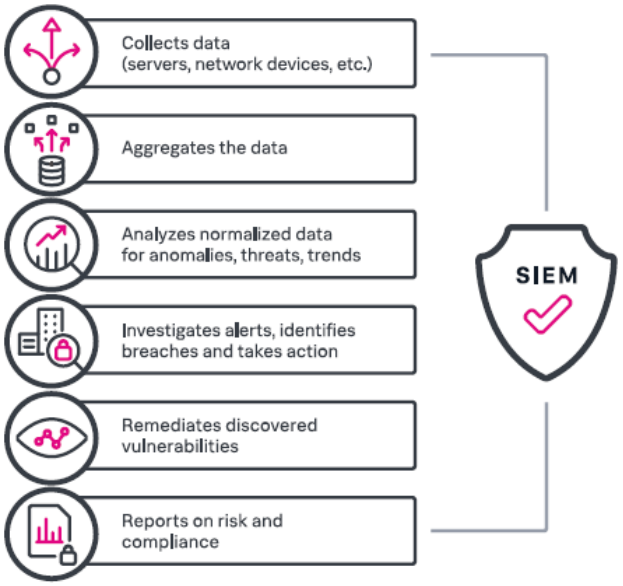
  - Personnel (Employees) are expert security analysts who actively **search for vulnerabilities** within the network and **hunt for threats.**

Level 4 – SOC Performance & Integration with business:

At SOC's most advanced level are **managers and chief officers**.

  - This group **oversees** all SOC team activities
  - Responsible for **hiring and training**.
  - **Evaluating** individual and overall **performance**.

- **A SIEM solution** unifies data from different sources across the network infrastructure.



Incident Response Team Services

Intrusion Detection

- First tier responsibility.
- Analyzes incidents quickly using intrusion detection technologies.

1. ## Incident Response
   - Identify, mitigate, and analyze threats.
   - Goal: Contain and resolve quickly.

Example: A company identifies unauthorized access and immediately blocks the intrusion, investigates the breach source, and restores affected systems.

2. ## Incident Handling
   - A broader term that includes **preparing for**, **managing**, and **recovering** from incidents, ensuring minimal impact.

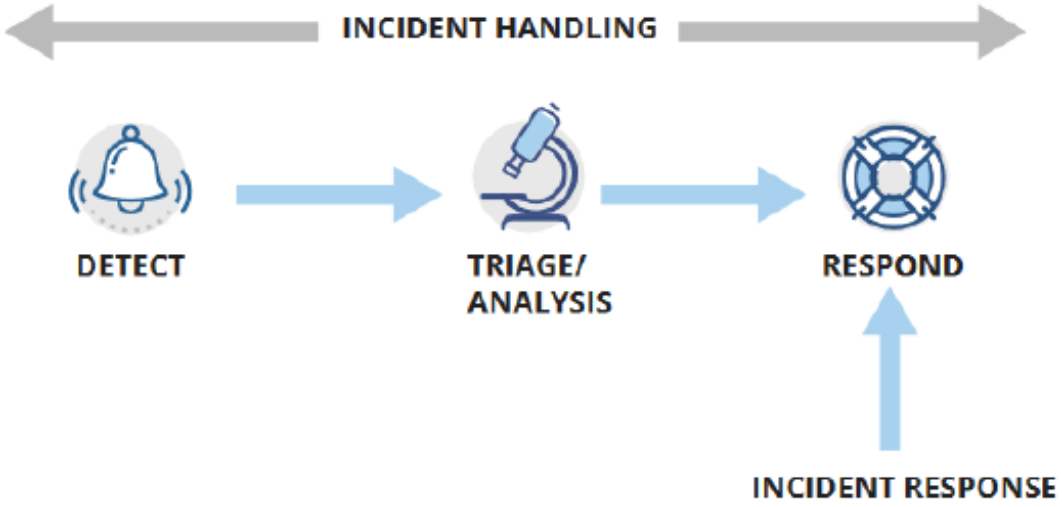
Example: Developing and implementing a comprehensive plan that outlines steps for prevention, detection, response, and post-incident analysis.

3. ## Incident Management
   - The overarching framework that includes the lifecycle management of all incidents.
   - **Focus:** restore services, minimize impact on business operations.

Example: Use ITSM (IT Service Management) tools to track incidents from detection to resolution.

Role and Responsibilities of an Incident Handler

- Conducting **detailed investigations** of security incidents
- Implementing **containment measures**
- **Coordinating with relevant teams** for resolution
- **Analyzing and improving** security controls.



Incident Management Starts Before an Incident Occurs

