Roles in Response: CSIRT and SOC Overview

# NIST Incident Response Lifecycle Phases:

1. 1. Preparation
2. 2. Detection and Analysis
3. 3. Containment, Eradication, and Recovery
4. 4. Post-Incident Activity

# Command, Control, and Communication

• Command: Leadership and strategic oversight

• Control: Managing technical elements and assigning tasks

• Communication: Keeping all stakeholders informed

# CSIRT (Computer Security Incident Response Team)

A team of specialized professionals who respond to and manage security incidents. CSIRTs may be permanent or ad-hoc and include both security and nonsecurity staff.

## Core Roles:

* Security Analyst

• Monitors for threats, analyzes alerts  
• Performs root-cause investigations  
• Escalates critical issues to Technical Lead

* Technical Lead

• Oversees technical response  
• Identifies root cause  
• Implements containment, eradication, and recovery  
• Coordinates with business units to reduce impact

* Incident Coordinator

• Coordinates communication across departments  
• Ensures nonsecurity teams are aligned and informed

## Additional Possible Roles:

• Communications Lead  
• Legal Lead  
• Planning Lead

Note: Roles and responsibilities may differ by organization. Titles such as 'Incident Commander' or 'Incident Manager' may be used in place of Incident Coordinator.

# SOC (Security Operations Center)

A centralized unit focused on continuous monitoring, threat detection, and incident response. Typically structured by analyst tiers.

## SOC Tier Structure:

* Tier 1 – SOC Analyst L1

• Monitors, reviews, and prioritizes alerts  
• Creates and closes tickets  
• Escalates as needed

* Tier 2 – SOC Analyst L2

• Handles escalated tickets  
• Performs deeper investigations  
• Refines tool configurations

* Tier 3 – SOC Lead L3

• Manages daily team operations  
• Conducts advanced analysis (e.g., forensics, malware)  
• Reports to SOC Manager

* SOC Manager

• Manages team performance and training  
• Reports incidents and audit data to executives

## Specialized Roles:

• Forensic Investigator: Preserves and analyzes evidence (usually L2/L3)

• Threat Hunter: Proactively finds advanced threats using intelligence (typically L3)

# Key Takeaways:

• Understanding the structure of CSIRTs and SOCs is essential for collaboration and incident handling.  
• Recognizing your role and others' roles within the response lifecycle helps ensure clarity and effectiveness.  
• Security analysts must work across teams and with nonsecurity professionals to form effective incident responses.  
• Different perspectives lead to more creative and resilient security solutions.