

Introduction to Security Operations Center (SOC)

Alexis Ahmed

Red Team & Blue Team Instructor @INE

Red Team Lead @HackerSploit

Key Concepts

- + Introduction to Security Operations
- + Key Functions & Services of a SOC
- + SOC Structure & Roles
- + SOC Workflows & Processes

MAJOR TOPICS

- + Key Functions & Services of a SOC
- + Types of SOC
- + SOC Roles & Responsibilities
- + Incident Detection & Incident Response
- + SOC Workflows & Processes
- + SOC Tools & Technologies
- + SOC Automation



LEARNING OUTCOMES

- + Understand the Fundamentals of a SOC: Explain the purpose, structure, and key functions of a SOC, including different SOC models (In-house, Managed, Hybrid) and SOC tiers (Tier 1, 2, 3).
- + Identify Key Roles and Teams in a SOC: Describe the roles and responsibilities of SOC analysts, threat hunters, digital forensics teams, CSIRT, IRT, red teams, and threat intelligence teams.
- + Understand SOC Frameworks and Maturity Models: Compare various SOC maturity models and frameworks to assess and improve SOC effectiveness.
- + Explain the Incident Response Lifecycle: Detail the phases of the Incident Response Lifecycle according to NIST 800-61, including detection, containment, eradication, recovery, and lessons learned.
- + Incident Detection & Response Techniques: Describe IR techniques like event triage, investigation workflows, escalation protocols, and response strategies.
- + SOC Tools & Automations: Have an understanding of essential SOC tools, technologies, and automation techniques, including SOAR platforms, threat intelligence feeds, and the use of AI & Machine Learning to enhance SOC efficiency.


PREREQUISITES

- + Basic understanding of cybersecurity concepts and terminology.
- + Foundational knowledge of threat types and attack vectors.



LET'S GO!





What is a Security Operations Center (SOC)?

What is a SOC?

A **Security Operations Center (SOC)** is a centralized unit/team in an organization that is responsible for **monitoring, detecting, analyzing,** and **responding** to cybersecurity threats across applications, devices, systems, networks and locations.

Fundamentally speaking, the SOC is an organization's **first line of defense**, functioning as the nerve center for all cybersecurity efforts.

Given the critical role a SOC plays within an organization, it must operate **around the clock (24/7)** to provide **continuous security monitoring** and **rapid incident response**.



What is a SOC?

A SOC is built upon **four essential pillars: people, processes, tools, and intelligence.**

- Skilled analysts and engineers form the human foundation, using established protocols and workflows to guide operations.
- Advanced security platforms and technologies enable real-time monitoring, detection, and analysis of potential threats.
- Finally, up-to-date threat intelligence keeps the SOC informed about emerging attack methods, ensuring a proactive and adaptive defense posture.

A SOC relies on these pillars to effectively protect an organization, Each pillar is critical to the SOC's effectiveness.



What is a SOC?

1 - People (The SOC Team):

The individuals/roles required to operate a functional SOC.

A SOC requires skilled security analysts and engineers in order to operate effectively. A functional SOC organizes and classifies members of a SOC team based on their role and responsibilities, for example; Tier 1, Tier 2 and Tier 3 analyst.

2 - Processes:

Processes establish consistency and clarity, ensuring incidents are handled methodically.

A functional SOC has defined workflows, protocols, and best practices help ensure consistency and efficiency. This includes procedures for incident response, threat intelligence sharing, and compliance reporting.

What is a SOC?

3 - Tools/Technology:

The technical capabilities to detect, analyze, and mitigate threats at scale.

This refers to the range of solutions/tools required for the SOC to perform its primary functions, for example: asset discovery, vulnerability assessment, intrusion detection, SIEM platforms, endpoint detection, and security analytics.

4 - Intelligence:

Supplying the SOC with intelligence them to remain one step ahead of adversaries.

Up-to-date threat intelligence equips the SOC with insights into emerging attack vectors, tactics, and indicators of compromise, guiding proactive and reactive measures effectively.

SOC Services

A SOC is typically responsible for a broad range of services/functions like:

- + Real-Time Security Monitoring
- + Threat Detection & Intelligence
- + Incident Response
- + Vulnerability Management
- + Forensics
- + Reporting and Compliance

The services/functions outlined above represent categories of services that a SOC provides and is not representative of all the functions/activities that fall under each of the categories. We will take a closer look at the primary SOC services in the next set of slides

Core SOC Services

- + **Security Monitoring** – Continuous log collection & network monitoring
- + **Threat Intelligence** – Analyzing emerging threats & attack trends
- + **Threat Hunting** – Proactive hunting for undetected threats
- + **Incident Response** – Detecting, containing, and eradicating threats
- + **Digital Forensics** – Investigating security incidents post-breach
- + **Compliance & Reporting** – Meeting regulatory and audit requirements

SOC Services

SOC services are usually categorized based on the nature of the operations they entail i.e ***are they reactive or proactive?***

- **Reactive services** are the tasks triggered ***after an intrusion*** or malicious event is detected.
- **Proactive services** involve tasks performed by the SOC in the ***absence of any clear indicators of intrusion.***

SOC Services

REACTIVE SERVICES	PROACTIVE SERVICES
Alert Handling & Triage	Cyber Threat Intelligence (CTI)
Incident Response & Analysis	Threat Hunting
Intrusion Detection	Network Security Monitoring
Vulnerability Management	Logging & SIEM Management (Platform Health Monitoring)
Digital Forensics	Baseline & Policy Management
Malware Analysis	Proactive Monitoring
Reporting & Compliance	
Recovery & Remediation	

Key Characteristics of a SOC

Understanding the key characteristics of a SOC is essential because it provides a foundational framework for how security operations function and how **SOCs should operate**.

More importantly, these characteristics will be very useful in establishing a baseline that can be used to **determine whether a SOC is indeed functional and more importantly, to identify where improvements can be made**.

Centralized Command Center

1 - Centralized Command Center

A SOC operates as a single, centralized unit/team responsible for an organization's cybersecurity defense.

- + **24/7 Operations:** A SOC should function around the clock (24/7) to detect and respond to threats immediately.
- + **Unified Security Infrastructure:** A SOC should integrate multiple security tools, such as SIEM, EDR, IDS/IPS, and firewalls, to provide a holistic view of security events.
- + **Real-time Threat Intelligence:** Centralized visibility allows the SOC team to correlate events, detect attack patterns, and respond proactively.
- + **Incident Coordination:** Security teams, IT teams, and executive stakeholders rely on the SOC for security event updates and response actions.



Continuous Monitoring

2 – Continuous Monitoring

A SOC is responsible for real-time monitoring of network traffic, system logs, endpoints, and cloud environments to detect malicious activity.

- + **Log Collection & Analysis:** A SOC should aggregate logs from firewalls, intrusion detection systems (IDS), servers, and endpoints.
- + **Alerting & Threat Prioritization:** A SOC should utilize Security Information & Event Management (SIEM) systems to generate alerts and prioritize security incidents.
- + **Threat Intelligence Feeds:** A SOC should incorporate global threat intelligence sources to detect known Indicators of Compromise (IOCs).
- + **Behavioral Analytics & Machine Learning:** A SOC should have anomaly-based detection capabilities in order to monitor user behavior and insider threats through User and Entity Behavior Analytics (UEBA).
- + **Network & Endpoint Monitoring:** A SOC should integrate Network Detection & Response (NDR) and Endpoint Detection & Response (EDR) tools to track suspicious activity.

Incident Response & Containment

3 – Incident Response & Containment

*One of the SOC's most critical functions is **rapidly responding** to cybersecurity incidents to minimize damage, contain the threat, and prevent escalation.*

- + **Incident Handling:** SOC analysts should follow a structured incident response process based on **NIST 800-61** or **SANS** guidelines.
- + **Containment Strategies:** A SOC team should be able to quarantine compromised systems, revoke access, or block malicious IPs/domains.
- + **Eradication & Remediation:** A SOC team should be able to remove malware, patch vulnerabilities, and strengthen security controls.
- + **Forensic Investigation:** A SOC team should be able to collect digital evidence, analyze malware, and trace the origin of an attack.
- + **Incident Documentation & Reporting:** A SOC should be able to prepare post-incident reports for executive stakeholders and legal teams.

Coordination & Collaboration

4 – Coordination & Collaboration

A SOC **does not operate in isolation**. It requires close collaboration with multiple departments to ensure an effective security posture.

Key Features:

- + **Collaboration with IT Teams:** The SOC should be able to work with system administrators, DevOps, and network engineers to apply patches, enforce security controls, and maintain business continuity.
- + **Communication with Executive Leadership:** SOC managers should be able to provide security reports, risk assessments, and incident impact analyses to the executive team.
- + **Compliance & Legal Coordination:** A SOC should ensure compliance with industry regulations (GDPR, HIPAA, PCI-DSS, ISO 27001) and be able to work with legal teams for incident disclosure.
- + **Security Awareness & Training:** A SOC should be able to work with HR and employees to reduce human risk, such as phishing attacks and social engineering scams.
- + **Continuous Security Improvement:** A SOC should share lessons learned from past incidents to refine security policies and defense strategies.

A man with glasses and a beard is shown in profile, working on a computer in a dark room. The screen displays some code or data. The overall atmosphere is professional and focused.

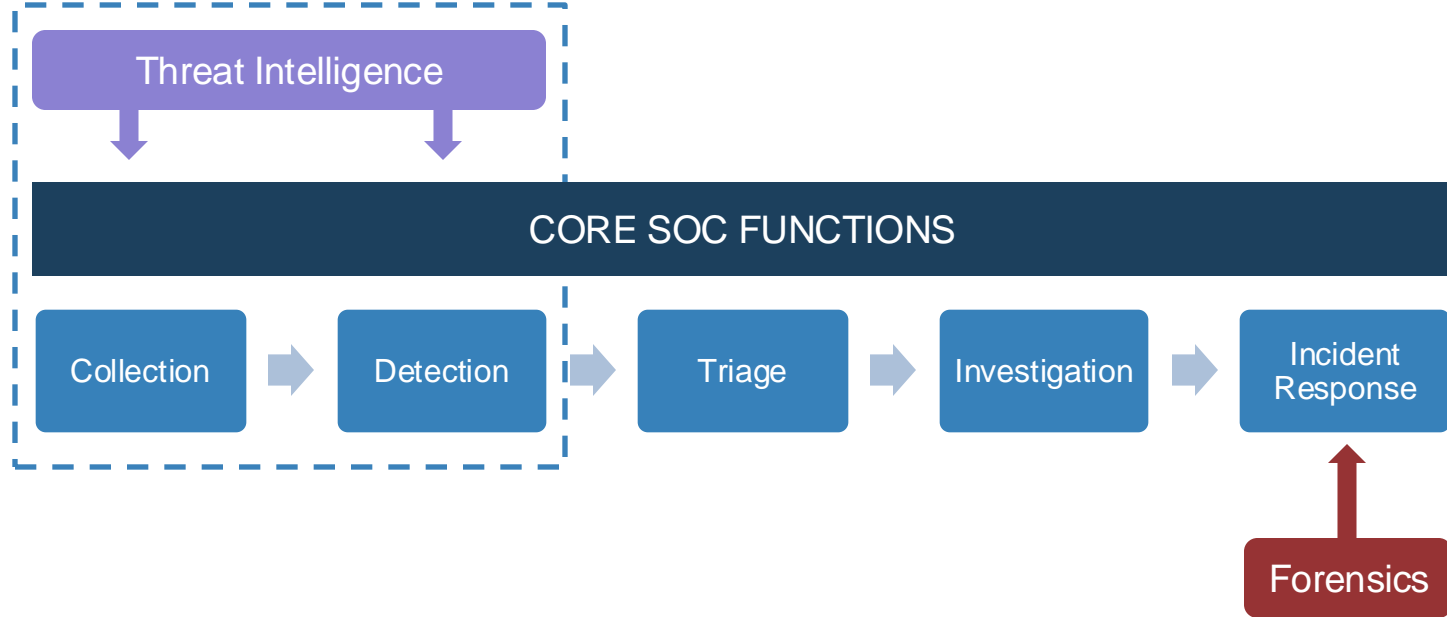
Key Functions of a SOC

Key Functions of a SOC

When analyzing how a SOC functions, breaking down the complex workflow of security events into modular/atomic functions provides clarity on inputs, outputs, goals, and interactions with other teams.

This decomposition/modularization enables organizations to assess performance, optimize operations, and ensure effective cyber defense.

Key Functions of a SOC



Key Functions of a SOC

The image shown in this slide represents the fundamental components of operating a SOC, categorized as core activities essential to the responsibilities of a typical SOC team.

The next set of slides will explore each function in detail, outlining its objectives and methods for evaluating its effectiveness.



1 – Data Collection & Aggregation

What is Data Collection & Aggregation?

- + Data collection and aggregation is the foundation of a SOC. It involves gathering, normalizing, and centralizing security-related data from various sources across an organization's IT infrastructure.
- + This process ensures that SOC analysts and security tools have the necessary visibility to detect, investigate, and respond to security incidents effectively.

Inputs:

- + Security logs from firewalls, IDS/IPS, EDR, SIEM, cloud services, and network devices
- + User activity logs (Windows Event Logs, Linux Syslog, Active Directory logs)
- + Application and database logs
- + Threat intelligence feeds (Indicators of Compromise - IOCs, Indicators of Attack - IOAs)

Process & Goals:

- + Ensure complete visibility across IT assets by collecting logs from all security-relevant sources.
- + Normalize and aggregate log data for efficient analysis.
- + Maintain data integrity for forensic analysis and compliance.

Outputs:

- + Centralized and structured logs
- + Enriched logs with threat intelligence
- + Real-time alerts for suspicious activities

2 – Detection & Correlation

What is Detection & Correlation?

- + Detection and correlation are core functions of a SOC that enable security teams to identify, analyze, and connect disparate security events to detect malicious activities before they escalate into full-blown security incidents.
- + Detection focuses on identifying suspicious or malicious activity using security tools, log analysis, and behavioral analytics.
- + Correlation involves linking related events across multiple data sources to identify attack patterns, reduce false positives, and gain contextual insight into potential security incidents.

Inputs:

- + Aggregated logs from data collection sources
- + Threat intelligence feeds (known IOCs, IPs, domains, and hashes)
- + Behavioral analytics data (UEBA, anomaly detection)

Process & Goals:

- + Detect suspicious activities, anomalies, and security policy violations.
- + Utilize Security Information and Event Management (SIEM) and Machine Learning (ML) models to correlate security events and identify patterns.
- + Reduce false positives while maintaining high-fidelity alerts.

Outputs:

- + Security event alerts with correlation data
- + Prioritized list of potential threats
- + Escalation of confirmed threats to triage and investigation

3 – Triage

What is Alert Triage and Prioritization?

- + Alert triage and prioritization is the process of analyzing, categorizing, and ranking security alerts based on their severity, impact, and likelihood of being an actual security incident.
- + Triage refers to sorting and assessing alerts to determine whether they indicate a real security threat or a false positive.
- + Prioritization assigns an urgency level to alerts, ensuring that the most critical threats are addressed first while filtering out low-risk or irrelevant alerts.

Inputs:

- + Security event alerts from SIEM, IDS/IPS, EDR
- + Correlated alerts from threat detection systems
- + Threat intelligence and historical attack data

Process & Goals:

- + Categorize alerts based on severity, likelihood, and potential impact.
- + Reduce alert fatigue by filtering false positives and benign events.
- + Escalate confirmed threats for further investigation and containment.

Outputs:

- + Categorized alerts (Low, Medium, High, Critical)
- + Escalation to Tier 2 analysts for deep investigation
- + Incident documentation and reporting

4 – Incident Investigation

What is Incident Investigation?

- + Incident investigation and threat analysis are critical functions in a SOC, responsible for determining the full scope, impact, and cause of a security incident.
- + Incident Investigation is the process of analyzing security alerts and correlated events to determine whether a real security breach has occurred and how it unfolded.
- + Threat Analysis involves examining attacker tactics, techniques, and procedures (TTPs) to understand how the attack was executed and how to prevent similar incidents in the future.

Inputs:

- + Escalated alerts from Tier 1 SOC Analysts
- + Network and host logs, forensic data
- + Malware samples and reverse-engineering reports

Process & Goals:

- + Determine the full scope of an incident (entry point, affected assets, impact).
- + Conduct log analysis, endpoint investigation, and threat hunting.
- + Identify malware behaviors, attack vectors, and attacker TTPs (Tactics, Techniques, and Procedures).

Outputs:

- + Incident reports with root cause analysis
- + Attack chain mapping using MITRE ATT&CK framework
- + Recommendations for containment and mitigation

5 – Incident Response

What is Incident Response?

- + Incident containment and response are critical phases in the incident response lifecycle where SOC teams take immediate action to stop an active attack, prevent further damage, and restore normal operations.
- + Containment focuses on isolating the threat to limit its spread and impact.
- + Response involves removing the threat, remediating vulnerabilities, and implementing preventive security measures to ensure the attacker cannot return.

Inputs:

- + Investigated incidents and confirmed threats
- + Forensic data, malware samples, affected systems information

Process & Goals:

- + Contain active threats to prevent further spread (network segmentation, account disablement).
- + Eradicate threats by removing malicious files, revoking attacker persistence, and patching vulnerabilities.
- + Implement real-time response actions via SOAR (Security Orchestration, Automation, and Response).

Outputs:

- + Systems isolated from the network
- + Mitigated threats with remediation plans
- + Containment reports for stakeholders

A man with glasses and a beard is shown in profile, working on a computer in a dark room. The background is dark, and the man is wearing a dark shirt. The text "SOC Maturity Models & Frameworks" is overlaid on the image in white. There is a small orange vertical bar on the left side of the image.

SOC Maturity Models & Frameworks

SOC Maturity Models & Frameworks

What is SOC Maturity?

- + A Security Operations Center (SOC) Maturity Model **defines the capability, effectiveness, and operational maturity** of a SOC in detecting, responding to, and mitigating security incidents.
- + Organizations evolve their SOC capabilities based on their security needs, available resources, and risk tolerance.
- + A mature SOC is **proactive, automated, and aligned** with industry frameworks to detect, investigate, and mitigate advanced threats efficiently.

SOC Maturity Models & Frameworks

Why SOC Maturity Matters

- + Ensures scalability and adaptability to evolving cyber threats.
- + Reduces incident response time and enhances detection capabilities.
- + Aligns SOC operations with industry best practices and compliance standards.
- + Helps organizations measure progress and identify gaps in security operations.

SOC Maturity Models

SOC maturity is often evaluated using structured maturity models that assess an organization's security capabilities from basic (reactive) to advanced (proactive and automated).

It is, therefore, vitally important to familiarize yourself with these models before you begin implementing them.

Gartner SOC Maturity Model

Gartner classifies SOC maturity into five levels, ranging from minimal capabilities to fully automated threat intelligence-driven SOC.

Maturity Level	Description	Key Characteristics
Level 1 – Minimal (Ad Hoc SOC)	No formal SOC	No 24/7 monitoring, security handled reactively.
Level 2 – Developing (Reactive SOC)	Basic SOC with manual processes	Security monitoring exists but lacks automation and proactive threat hunting.
Level 3 – Defined (Operational SOC)	Established SOC	Security incidents are detected, triaged, and responded to systematically.
Level 4 – Managed (Proactive SOC)	Advanced SOC with automation and analytics	Incorporates threat intelligence, behavioral analytics, and proactive threat hunting.
Level 5 – Optimized (Intel-Driven SOC)	Fully integrated and automated SOC	Uses AI/ML-driven threat detection, SOAR, and automated response actions.

NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) provides a roadmap for SOC maturity based on five security functions:

SOC Alignment with NIST CSF:

- + Basic SOC focus on detecting & responding to security threats.
- + Mature SOC integrates threat intelligence, automated detection, and proactive defense measures across all five functions.

Function	Description
Identify	Understanding business risks, asset inventory, and threat landscape.
Protect	Implementing access control, data security, and endpoint protection.
Detect	Monitoring, detecting anomalies, and identifying threats.
Respond	Containment, eradication, and mitigation of security incidents.
Recover	Restoring operations, lessons learned, and continuous improvement.

Capability Maturity Model Integration (CMMI) for SOCs

CMMI measures SOC maturity across five levels, similar to Gartner but with an emphasis on process optimization and continuous improvement.

Maturity Level	Description
Level 1 – Initial	No structured SOC, ad hoc incident handling.
Level 2 – Managed	Basic incident response procedures, minimal automation.
Level 3 – Defined	Standardized SOC processes, monitoring, and threat detection.
Level 4 – Quantitatively Managed	Data-driven incident response, automated analytics.
Level 5 - Optimizing	Fully automated, AI-powered SOC with continuous improvement.

MITRE ATT&CK-Based SOC Maturity


MITRE ATT&CK is an adversary tactics, techniques, and procedures (TTPs) framework that helps SOCs enhance threat detection, intelligence-driven defense, and adversary emulation.

SOC Maturity Level	Characteristics
Basic (Level 1)	Detects commodity malware and known attack signatures.
Intermediate (Level 2 - 3)	Detects known TTPs mapped to MITRE ATT&CK, incorporates behavioral analytics.
Advanced (Level 4 – 5)	Conducts proactive threat hunting, adversary simulation, and MITRE ATT&CK-based detections.

SOC-CMM (SOC Capability Maturity Model)

The SOC-CMM framework provides a structured assessment model for SOC maturity across five domains:

SOC-CMM Domains	Evaluation Criteria
Business	SOC alignment with business & compliance goals.
People	Training, skill sets, and staff certifications.
Process	Defined and repeatable incident response workflows.
Technology	Use of SIEM, SOAR, EDR, threat intelligence platforms.
Metrics	Data-driven decision-making & KPI tracking.

A man with glasses and a beard is shown in profile, working on a computer in a dark room. The background is dark, and the man is wearing a dark shirt. The text is overlaid on the left side of the image.

Types of SOCs (In-house, Managed, Hybrid)

Types of Security Operations Centers (SOCs)

- + Organizations choose different types of Security Operations Centers (SOCs) based on budget, expertise, security needs, and compliance requirements.
- + SOCs typically fall into three main categories:
 - + **In-House SOC** (Dedicated Internal Team)
 - + **Managed SOC** (Outsourced to a Managed Security Service Provider - MSSP)
 - + **Hybrid SOC** (Combination of In-House & Managed Services)

Each type has its own advantages and challenges, and organizations must choose the one that aligns with their security strategy, resources, and risk profile.



In-House SOC (Dedicated Internal Team)

- + An In-House SOC is a fully owned and operated security center within an organization.
- + It consists of an internal cybersecurity team that is responsible for monitoring, detecting, analyzing, and responding to threats.

Key Characteristics:

- + Staffed by the organization's security analysts (SOC Tier 1, Tier 2, Tier 3, Incident Responders).
- + Uses internally managed security tools (SIEM, EDR, SOAR, Threat Intelligence).
- + Operates 24/7 or on a predefined schedule.
- + Compliant with organizational security policies and regulatory requirements.

Pros & Cons of an In-House SOC

Advantages	Disadvantages
Full control over security operations (policies, procedures, incident response).	High cost (salaries, tools, infrastructure, training, 24/7 staffing).
Customization & flexibility in implementing detection rules and response strategies.	Requires skilled security professionals (hiring and retaining talent is difficult).
Better alignment with business objectives & compliance requirements.	Managing & maintaining SIEM, threat intelligence feeds, and forensic tools is resource-intensive.
Stronger internal visibility into threats targeting the organization.	Alert fatigue (if not automated, SOC analysts may get overwhelmed).

In-House SOC (Dedicated Internal Team)

An In-House SOC is best suited to meet the needs of Large enterprises, government organizations, critical infrastructure sectors (e.g., financial institutions, healthcare, defense) that require full control over security operations.

Managed SOC (Outsourced Security Operations)

- + A Managed SOC is fully or partially outsourced to a third-party Managed Security Service Provider (**MSSP**).
- + The MSSP provides **24/7 security monitoring, detection**, and **incident response** on behalf of the organization.

Key Characteristics:

- + SOC services are provided remotely by MSSPs (IBM Security, Secureworks, Palo Alto, AT&T Cybersecurity, Arctic Wolf).
- + Uses cloud-based SIEM, EDR, and threat intelligence solutions managed by the provider.
- + Security analysts from the MSSP monitor and investigate threats based on service-level agreements (SLAs).
- + Threat intelligence & global attack insights are provided by the MSSP.



Pros & Cons of a Managed SOC

Advantages	Disadvantages
Lower operational costs compared to maintaining an in-house SOC.	Limited control over security policies & incident response procedures.
24/7 expert security monitoring without needing an internal security team.	Third-party dependency (<i>delays in response if the provider is overwhelmed</i>).
Rapid deployment & scalability (instant access to security expertise).	Potential data privacy concerns (<i>outsourcing security operations means sharing logs and sensitive information</i>).
Threat intelligence from multiple clients & industries improves detection accuracy.	Standardized security models (<i>may not be fully tailored to a specific business</i>).

Managed SOC (Outsourced Security Operations)

A Managed SOC is best suited to meet the needs of Small-to-medium businesses (SMBs), startups, and organizations that lack an internal security team but require 24/7 monitoring and threat detection.

Hybrid SOC (In-House & Managed SOC)

- + A Hybrid SOC combines in-house SOC operations with external MSSP support, allowing organizations to maintain control over critical security functions while outsourcing specific tasks such as threat monitoring, intelligence, or incident triage.

Characteristics:

- + Internal SOC analysts handle strategic cybersecurity functions (incident response, digital forensics, vulnerability management).
- + MSSP provides external support for log collection, event monitoring, SIEM management, and 24/7 coverage.
- + Flexible SOC model that adapts to business needs and security budgets.
- + Leverages MSSP threat intelligence while keeping sensitive investigations in-house.

Pros & Cons of a Hybrid SOC

Advantages	Disadvantages
Balances cost-effectiveness with internal control over security operations.	Complex coordination between the in-house team and MSSP.
24/7 monitoring without hiring a full-time night shift security team.	Integration challenges when merging MSSP security tools with existing in-house systems.
More efficient incident response (internal team investigates high-priority alerts).	Data security concerns when sharing logs & alerts with an external provider.
Best of both worlds (customized security approach with expert external support).	

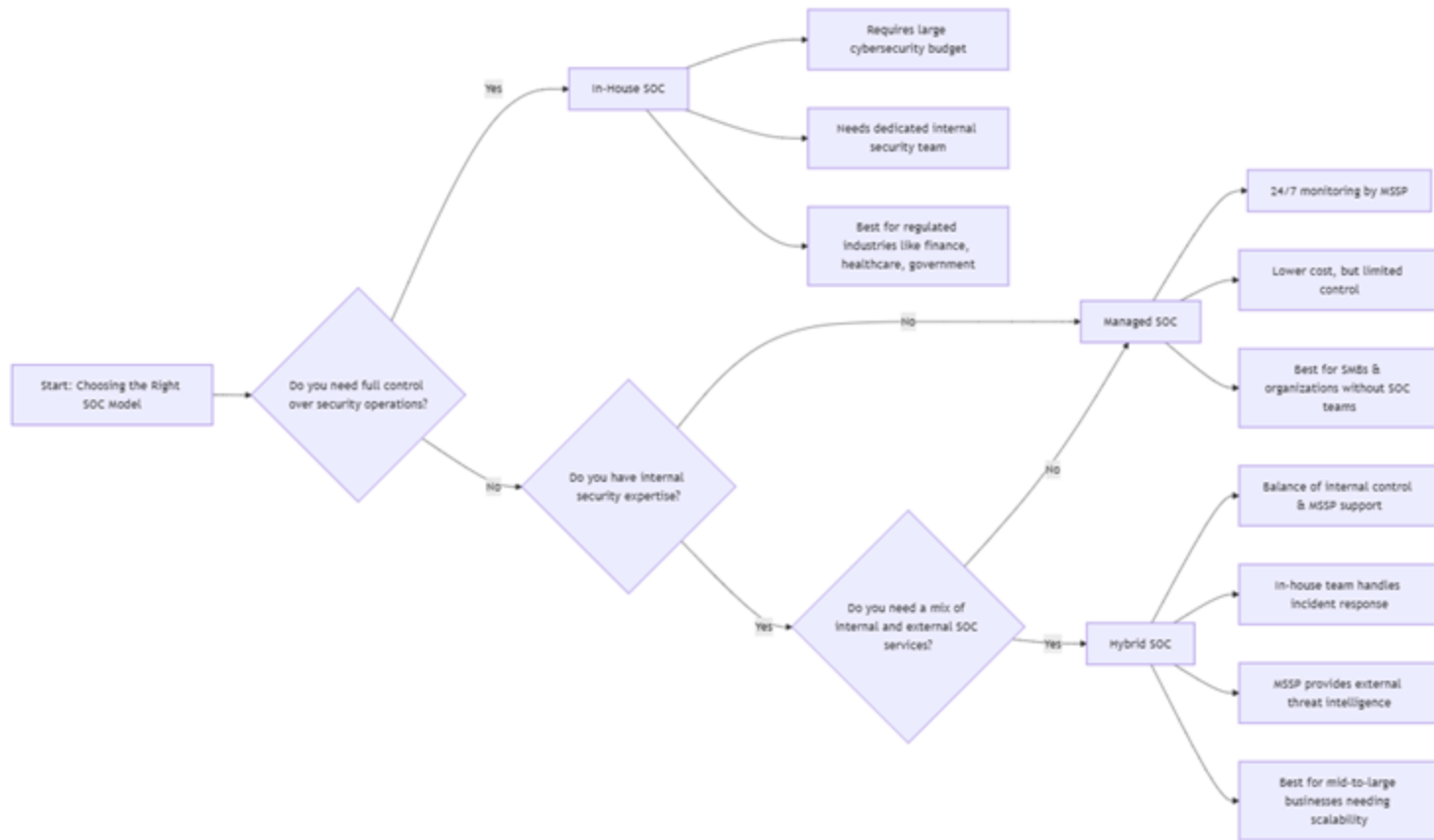
Hybrid SOC (In-House & Managed SOC)

A Managed SOC is best suited to meet the needs of Mid-sized to large enterprises that require a balance of in-house security operations and outsourced expertise. Suitable for businesses with strict compliance needs but limited internal resources.

Comparing In-House, Managed & Hybrid SOC

Feature	In-House	Managed	Hybrid
Control	Full Control	Limited control	Balanced control
Cost	High	Lower	Moderate
Staffing	Requires Internal Analysts	MSSP provides analysts	Mix of internal and external staff
Threat Intelligence	Org-Specific Intelligence	MSSP provides intel	Both internal and MSSP intelligence
24/7 Coverage	Requires dedicated shifts	Provided by MSSP	Shared responsibility
Incident Response	Fully internal	MSSP handles initial response	Internal team escalates critical incidents
Best For	Large enterprises, critical sectors	SMBs, organizations with no SOC	Mid-to-large businesses that require scalability

Choosing The Right SOC Model



A man with glasses and a beard is shown in profile, looking at a computer screen in a dark room. The screen displays some code or data. The overall atmosphere is professional and focused.

SOC Tiers & Roles (Tier 1, 2, 3 Analysts)

SOC Tiers & Roles

A SOC is structured into ***tiers*** to ensure **efficient** and **effective *incident detection, analysis, response, and remediation.***

- + SOC Tiers define the levels of expertise, responsibilities, and workflow in a SOC.
- + Each tier handles incidents based on complexity, severity, and required technical skills.

This tiered approach allows for scalability, specialization, and faster incident response.

SOC Tiers Structure Overview

SOC Tier	Role	Primary Responsibilities
Tier 1 - SOC Analyst (Alert Monitoring & Triage)	Entry-Level	First line of defense, monitors security alerts, performs initial triage, escalates serious threats.
Tier 2 - Incident Responder (Investigation & Response)	Mid-Level	Conducts in-depth analysis, investigates confirmed threats, mitigates incidents.
Tier 3 - Threat Hunter / Senior Analyst (Advanced Threat Analysis & Hunting)	Senior-Level	Proactively hunts threats, reverse-engineers malware, creates detection rules, fine-tunes SIEM/SOAR.

Tier 1 – SOC Analyst (Alert Monitoring & Triage)

A **Tier 1 SOC Analyst** is the first line of defense responsible for monitoring security alerts, triaging incidents, and escalating serious threats to Tier 2 or 3.

Required Skills:

- + Basic knowledge of SIEM, IDS/IPS, endpoint security solutions.
- + Familiarity with log analysis and threat intelligence platforms.
- + Strong analytical and decision-making skills.
- + Understanding of cyber attack patterns (MITRE ATT&CK, Cyber Kill Chain).

Common Tools Used by Tier 1 Analysts:

- + SIEM Platforms: Splunk, ELK, QRadar, Microsoft Sentinel
- + Threat Intelligence Feeds: AlienVault OTX, VirusTotal, Recorded Future
- + Endpoint Security Solutions: CrowdStrike, SentinelOne, Microsoft Defender



Tier 1 – SOC Analyst (Alert Monitoring & Triage)

Responsibility	Activities
Continuous Monitoring	Monitor SIEM alerts, IDS/IPS logs, firewall logs, endpoint security logs for potential security incidents.
	Use real-time dashboards to track anomalies and suspicious activities.
Alert Triage & Categorization	Review incoming alerts, filters out false positives, and classify threats based on severity.
	Use MITRE ATT&CK mapping to determine if an alert matches known attack patterns.
Initial Threat Analysis	Conduct basic investigation by checking logs, IP reputation, and threat intelligence feeds.
	Correlate alerts to determine if multiple security events indicate a larger attack.
Documentation & Escalation	Create detailed incident reports for Tier 2 analysts.
	Escalate incidents only when they exceed predefined risk thresholds.
Containment & Response	May perform simple response actions, such as blocking an IP address or disabling compromised accounts.

Tier 2 – Incident Responder (Investigation & Response)

A Tier 2 SOC Analyst (Incident Responder) investigates escalated alerts, determines the attack scope, and takes direct action to contain and mitigate incidents.

Required Skills:

- + Advanced log analysis, forensic investigation, and network security expertise.
- + Understanding of malware reverse engineering & exploit analysis.
- + Experience with incident handling frameworks (NIST, SANS, ISO 27035).

Common Tools Used by Tier 2 Analysts:

- + Forensics: Volatility, Autopsy, FTK Imager
- + Threat Hunting: Splunk, ELK, Zeek, Suricata
- + Malware Analysis: IDA Pro, Ghidra, Cuckoo Sandbox

Tier 2 – Incident Responder (Investigation & Response)

Responsibility	Activities
Threat Investigation & Root Cause Analysis	Investigates escalated incidents to determine: <ul style="list-style-type: none">• How did the attacker gain access?• Which systems are affected?• What actions did the attacker perform?
	Conducts forensic log analysis to trace attacker movement across the network.
Incident Containment & Remediation	Isolates compromised endpoints, blocks malicious IPs, disables compromised accounts.
	Works with IT teams to remove malware, restore affected systems, and apply security patches.
Digital Forensics & Malware Analysis	Uses memory forensics tools (Volatility, Rekall) to analyze active threats.
	Dissects malware samples in sandboxes (Cuckoo, Any.Run) to understand how they behave.
Incident Documentation & Reporting	Writes detailed forensic investigation reports for security leadership.
	Provides recommendations to prevent similar incidents in the future.

Tier 3 – Threat Hunter / Senior Analyst

A Tier 3 SOC Analyst (Threat Hunter / Senior Analyst) is responsible for proactively hunting for undetected threats, performing advanced forensic analysis, and developing new detection techniques.

Required Skills:

- + Expert knowledge of network forensics, malware analysis, and adversary emulation.
- + Proficiency in scripting (Python, PowerShell) for automation.
- + Deep understanding of MITRE ATT&CK and threat intelligence methodologies.

Common Tools Used by Tier 3 Analysts:

- + Reverse Engineering: IDA Pro, Radare2, Ghidra
- + Threat Hunting: Velociraptor, Zeek, Splunk
- + SOAR Automation: Cortex XSOAR, Phantom



Tier 3 – Threat Hunter / Senior Analyst

Responsibility	Activities
Threat Hunting & Adversary Emulation	Uses proactive hunting techniques to detect stealthy attacks before they cause damage.
	Maps adversary behavior to MITRE ATT&CK and conducts Purple Team exercises.
Malware Reverse Engineering	Deconstructs zero-day malware and ransomware strains to understand their impact.
	Develops custom YARA rules to detect new malware variants.
SIEM & SOAR Rule Development	Writes custom correlation rules to improve SOC detection capabilities.
	Automates repetitive incident response tasks using SOAR playbooks.
Threat Intelligence & Attack Attribution	Analyzes nation-state APT groups and tracks evolving TTPs.
	Collaborates with external CTI teams to enrich SOC threat intelligence.



Threat Hunters & Digital Forensics Teams

Speciality Roles in the SOC

In the context of a SOC, **Threat Hunters** and **Digital Forensics** teams are **specialty roles** that **complement** core SOC functions like monitoring, detection, and incident response.

Threat Hunters, typically aligned with Tier 2 operations, actively search for threats within the organization's environment. Although Tier 3 analysts also engage in threat detection, a specialized role may focus on reviewing logs, conducting proactive threat hunts, and analyzing publicly available threat intelligence to identify potential risks originating both internally and externally.

While they may not be directly involved in every incident response process, their contributions significantly strengthen the organization's ability to detect, analyze, and understand threats.



Threat Hunters & Digital Forensics Teams

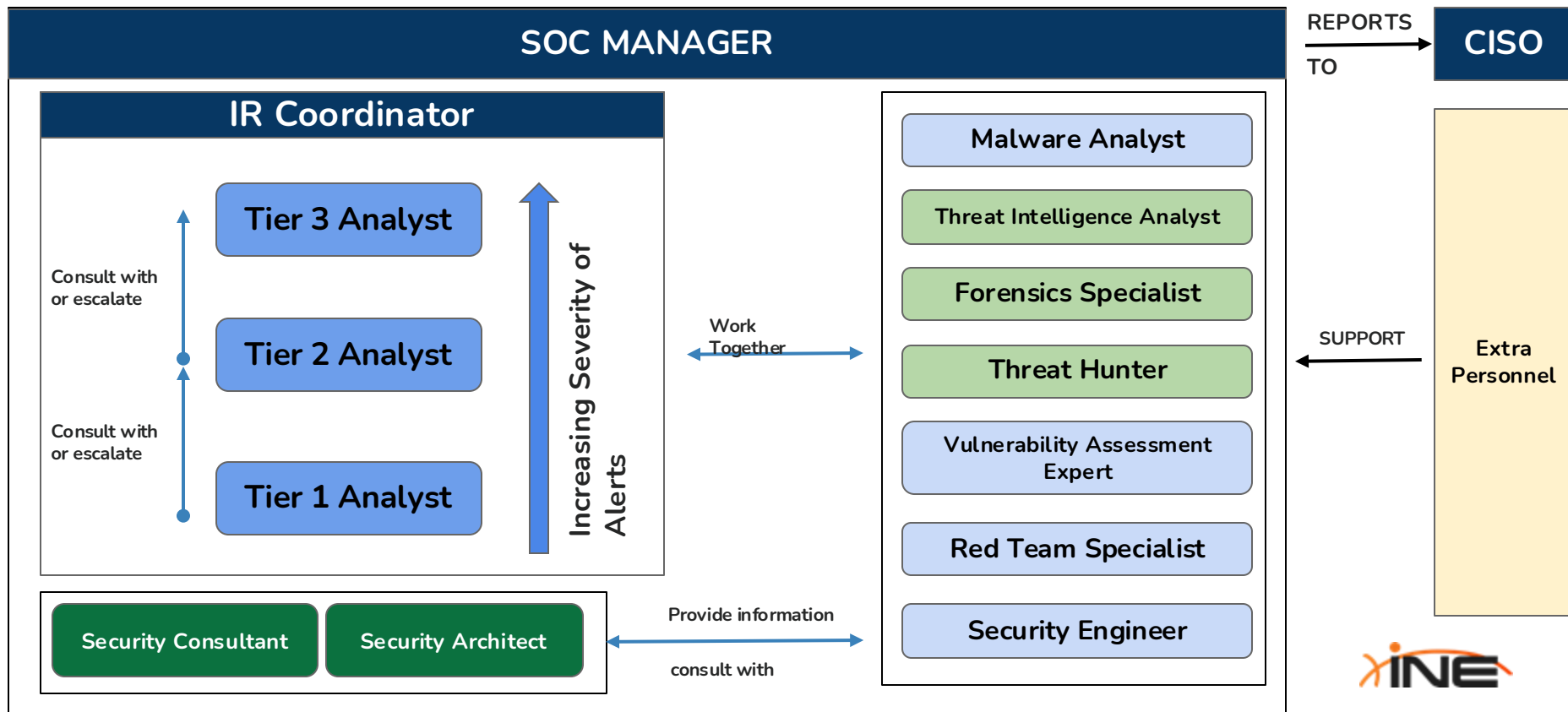
These two highly specialized roles play a crucial part in ***proactive defense*** and ***post-incident investigation***:

- + **Threat Hunters** – Focused on proactively seeking out threats that have evaded traditional detection mechanisms.
- + **Digital Forensics Teams** – Specialize in investigating and analyzing security incidents, gathering digital evidence, and determining the root cause of attacks.

Both teams are essential in enhancing an organization's cyber resilience, incident response capabilities, and post-incident analysis.



Interaction of roles within a SOC



Threat Hunters

Threat Hunters are cybersecurity experts who **proactively search** for **hidden threats** and **adversaries** within an organization's environment that have bypassed existing security controls. Their role is **proactive** and **hypothesis-driven**, aiming to detect and mitigate threats before they escalate into full-scale security incidents.

Common Tools Used by Threat Hunters:

- + SIEM Platforms: Splunk, ELK, QRadar, Microsoft Sentinel
- + EDR Solutions: CrowdStrike, SentinelOne, Microsoft Defender ATP
- + Threat Intelligence Platforms (TIPs): MISP, Recorded Future, OpenCTI
- + Network Analysis: Zeek, Wireshark, Suricata
- + MITRE ATT&CK Navigator – For mapping and tracking adversary behavior.
- + Custom Scripting: Python, PowerShell, Bash for automating detection processes.

Threat Hunter – Key Responsibilities

Responsibility	Activities
Proactive Threat Hunting	Develop hypotheses based on threat intelligence, attack trends, and organizational risk factors.
	Actively seek out advanced threats (like fileless malware, zero-day attacks, and insider threats) that traditional security tools may miss.
	Leverage SIEM data, endpoint telemetry, and network traffic to identify abnormal patterns or suspicious behaviors.
Adversary TTP Analysis	Map observed behaviors and attack patterns to the MITRE ATT&CK Framework.
	Identify gaps in detection and recommend strategies to close those gaps.
Threat Detection Engineering	Develop custom detection rules and alerts for SIEM, EDR, and SOAR platforms.
	Refine existing detection use-cases to reduce false positives and Create behavioral analytics models to detect sophisticated attack patterns.
Automation & Playbook Development	Work with SOC and engineering teams to automate detection and response workflows.
	Develop custom playbooks for responding to advanced attacks.
Collaboration with Threat Intelligence Team(s)	Use threat intelligence feeds to stay ahead of emerging threats and validate hypotheses by correlating data with known IOCs (Indicators of Compromise) and adversary techniques.

Digital Forensics Team

The **Digital Forensics team** is responsible for *investigating security incidents, analyzing digital artifacts, and determining the root cause of an attack.*

They specialize in data recovery, malware analysis, and evidence preservation for legal or internal use.

Common Tools Used by Digital Forensics Teams:

- + Memory Forensics: Volatility, Rekall
- + Disk Forensics: FTK Imager, Autopsy, EnCase
- + Malware Analysis: Ghidra, IDA Pro, Cuckoo Sandbox, Any.Run
- + Packet Analysis: Wireshark, Zeek
- + Log Analysis: SIEM Platforms (Splunk, QRadar, ELK)
- + Cloud Forensics: AWS CloudTrail, Azure Security Center




Digital Forensics Team – Key Responsibilities

Responsibility	Activities
Evidence Collection & Preservation	Collect digital evidence from endpoints, servers, networks, and cloud services.
	Ensure the chain of custody is maintained to preserve evidence integrity. Use forensic imaging tools to create copies of affected systems for analysis.
Forensic Analysis	Perform disk, memory, and network forensics to uncover indicators of compromise (IOCs).
	Investigate how the attacker gained access, what data was accessed, and whether the attack is ongoing. Recover deleted files and analyze file system artifacts (timestamps, registry changes).
Malware Analysis	Analyze suspicious files to determine if they are malicious or benign.
	Conduct static and dynamic malware analysis to understand malware behavior. Reverse-engineer malware using tools like Ghidra, IDA Pro, or sandbox environments.

Digital Forensics Team – Key Responsibilities

Responsibility	Activities
Incident Documentation & Reporting	Document every step of the forensic investigation process.
	Provide detailed reports outlining how the incident occurred, which systems were compromised, and recommendations for remediation.
	Support legal or regulatory compliance by providing forensic evidence for audits or legal cases.
Support Incident Response Teams	<p>Collaborate with Tier 2/3 SOC analysts and threat hunters to contain and eradicate threats.</p> <p>Provide insights on how attackers operated within the environment.</p> <p>Assist in root cause analysis and recommend security improvements.</p>



Types of Incident Response Teams (CSIRT & IRT)

Types of Incident Response Teams

Incident response is a ***critical function*** within any organization's cybersecurity strategy, ***but not all*** incident response teams are the same.

Depending on the ***size, maturity,*** and ***structure*** of an organization, different types of teams may be responsible for handling security incidents.

Types of Incident Response Teams

The **Computer Security Incident Response Team (CSIRT)** is one of the most well-known types of Incident Response teams, however, it is not the only approach to incident response.

Organizations may have dedicated, distributed, or hybrid incident response teams, each with its own scope, function, and responsibilities.

The next set of slides explores the various types of incident response teams, including CSIRTs, traditional Incident Response Teams (IRTs), and other organizational response structures.

Types of Incident Response Teams

In a SOC, both the **Computer Security Incident Response Team (CSIRT)** and **Incident Response (IR) Teams** are critical to managing and mitigating cybersecurity incidents.

Although their functions often overlap, they serve distinct roles in the incident response lifecycle.

CSIRT (Computer Security Incident Response Team)

A **Computer Security Incident Response Team (CSIRT)** is a ***dedicated*** group within an organization that is responsible for handling cybersecurity incidents.

CSIRTs are typically ***structured teams*** that follow a ***defined process to detect, respond to, mitigate, and recover*** from security incidents affecting an organization's systems, networks, or data.

Their primary goal is to minimize damage and restore normal operations as quickly as possible.



Key Responsibilities of a CSIRT

Responsibility	Activities
Incident Management & Coordination	Acts as the primary point of contact during a cybersecurity incident.
	Coordinates the entire incident response lifecycle, ensuring communication between stakeholders (SOC, IT, legal, executive teams).
	Ensures incidents are prioritized and handled according to severity and business impact.
Incident Detection & Analysis	Monitoring and analyzing security alerts, logs, and reports to identify potential security incidents.
Incident Response & Mitigation	Containing, eradicating, and mitigating threats to reduce impact on business operations.
Threat Intelligence & Monitoring	Gathering and analyzing intelligence on emerging threats and vulnerabilities to improve defense strategies.
Forensic Analysis	Investigating security breaches by analyzing logs, malware samples, and other digital evidence to determine attack vectors and root causes.
Recovery & Remediation	Assisting affected teams in restoring compromised systems and ensuring they are secured before returning to production.

Key Responsibilities of CSIRT

Responsibility	Activities
Documentation & Compliance	Documents every phase of the incident response process for internal records and audits.
	Ensures regulatory compliance by managing reporting requirements for data breaches.
Stakeholder Communication & Reporting	<p>Conducts post-mortem analyses to identify gaps and recommend corrective actions.</p> <p>Works with security leadership to develop strategic improvements to strengthen cybersecurity defenses.</p>
Policy & Procedure Development	Creating incident response plans, playbooks, and best practices to improve preparedness.

Key Responsibilities of CSIRT



Incident Response Teams (IRT) (General)

The **IRT** is a tactical group of security professionals that responds to security incidents by investigating, containing, and eradicating threats.

A standard **Incident Response Team (IRT)** is **broader** than a **CSIRT** and may handle both cybersecurity and non-cybersecurity incidents.

This type of team is often assembled from IT, legal, HR, and public relations to manage security breaches, service outages, and compliance-related incidents.

Their primary focus is on technical incident resolution.



Incident Response Teams (IRT) (General)

Unlike a CSIRT, which is a formally established team with a predefined structure, an **IRT** can be ad hoc or cross-functional, pulling in specialists from IT, legal, compliance, public relations, and other departments as needed.

Some organizations use the term IRT interchangeably with CSIRT, while others consider IRTs to be broader teams that include external stakeholders.

Incident Response Teams (IRT) (General)

Key Characteristics:

- + ***Handles a Broad Range of Incidents*** – Not limited to cybersecurity; may handle IT system failures, data privacy breaches, and business continuity issues.
- + ***Multi-Disciplinary*** – Often includes IT staff, legal representatives, compliance officers, and business stakeholders.
- + ***Reactive in Nature*** – Primarily activated in response to an incident, rather than operating proactively like a CSIRT.
- + ***May Lack Deep Cybersecurity Expertise*** – Unlike a CSIRT, a general IRT may not have dedicated cyber security specialists, relying instead on IT teams for technical response.

SOC Incident Response Team (Embedded)

A **SOC-based Incident Response Team** is *embedded within a SOC* and is responsible for *real-time monitoring, detection*, and *response* to security threats.

Unlike a standalone **CSIRT**, which may function separately from a SOC, this type of team directly responds to alerts from SIEM (Security Information and Event Management) systems and other monitoring tools.

SOC Incident Response Team (Embedded)

Key Characteristics:

- + ***Real-Time Response*** – Operates 24/7 to detect and mitigate security threats as they occur.
- + ***Integrates with Other SOC Functions*** – Works closely with SOC analysts, threat hunters, and vulnerability management teams.
- + ***Tactical & Fast-Paced*** – Focused on immediate containment and mitigation rather than deep forensic analysis.

Distributed Incident Response Team (DIRT)


A **Distributed Incident Response Team (DIRT)** consists of *multiple teams* spread across different locations or business units.

Large enterprises, government agencies, and multinational organizations often use this model to ensure incident response coverage across multiple regions.

Distributed Incident Response Team (DIRT)

Key Characteristics:

- + ***Geographically Distributed*** – Operates across different time zones and regions to provide global incident response capabilities.
- + ***Decentralized Approach*** – Local teams handle incidents independently, but follow standardized response procedures.
- + ***Highly Scalable*** – Works well for large organizations that require incident response at multiple sites.



Red Teams & Threat Intelligence Teams

Red Teams & Threat Intelligence Teams

In a mature cybersecurity environment, the SOC team, Red Team, and Threat Intelligence Team work collaboratively to enhance an organization's detection, response, and defense capabilities.

Their interaction ensures that security controls are continuously tested, refined, and improved based on real-world threats and attack techniques.

Interaction Between SOC & Red Team

A Red Team simulates real-world cyberattacks to test and challenge an organization's security defenses.

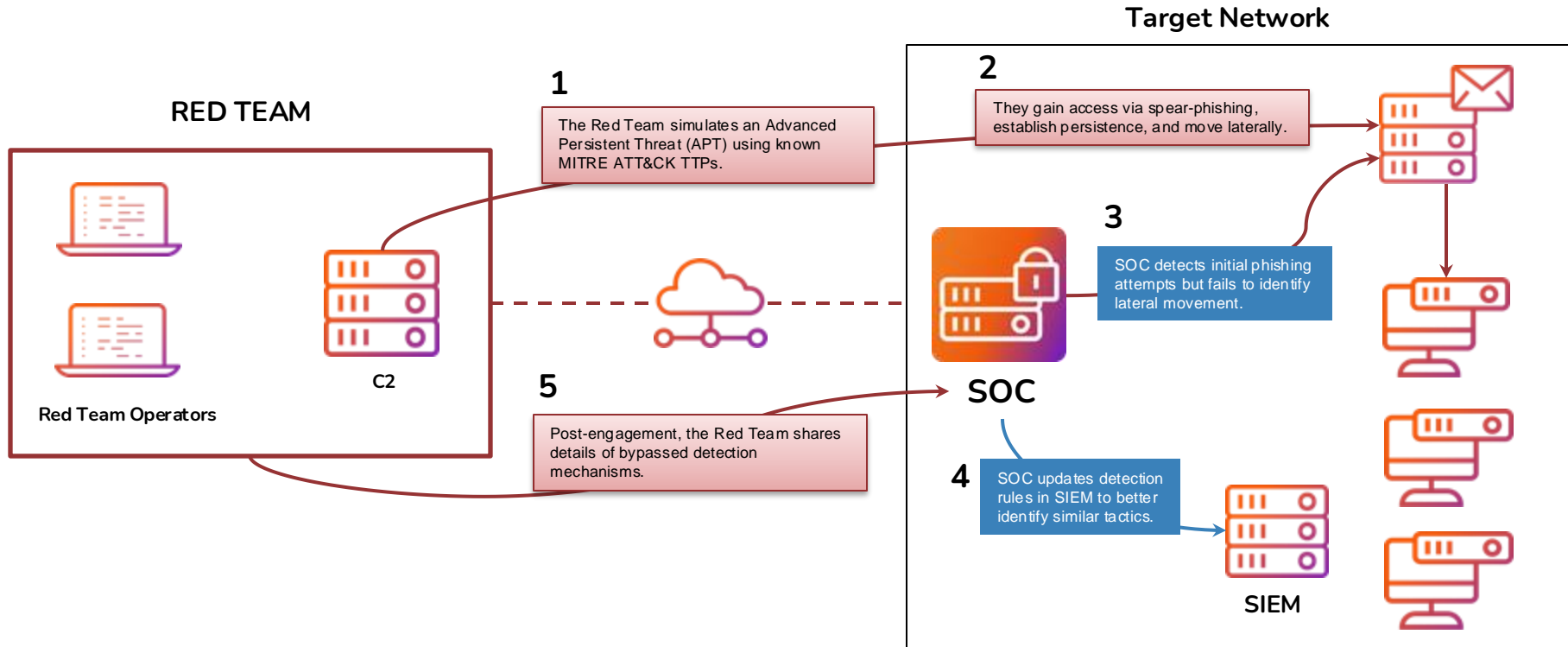
Their goal is to identify weaknesses by emulating the tactics, techniques, and procedures (TTPs) used by actual threat actors.

Red Team Role	SOC Role	Interaction Purpose
Simulate realistic cyberattacks (e.g., phishing, lateral movement, data exfiltration).	Detect and respond to simulated attacks in real time.	To test the SOC's detection and response capabilities.
Identify vulnerabilities and provide post-engagement reports.	Analyze attack patterns and improve detection rules.	To enhance SOC's ability to identify advanced threats.
Provide insights into gaps in defenses and bypass techniques.	Update and fine-tune SIEM rules, SOAR playbooks, and detection strategies.	To improve the accuracy of alerting and reduce false positives.
Conduct adversary emulation exercises based on known APTs.	Use the attack data to strengthen response strategies and playbooks.	To test and validate SOC response processes.

Collaboration Points

Collaboration Point	Description
Attack Simulation & Emulation	<ul style="list-style-type: none">• Red Teams conduct covert attack simulations to test SOC's real-time detection and response.• If the SOC fails to detect an attack, Red Teams provide detailed post-engagement reports.
Purple Teaming	<ul style="list-style-type: none">• Red and SOC (Blue) Teams collaborate closely to simulate, detect, and improve defenses in real time.• The Red Team executes an attack while the SOC Team observes, detects, and tunes systems to enhance detection capabilities.• This collaborative approach helps to identify detection gaps and improve alert accuracy.
Feedback & Process Improvement	<p>Red Teams share findings from their simulated attacks with the SOC to help:</p> <ul style="list-style-type: none">• Fine-tune SIEM correlation rules.• Develop new SOAR playbooks.• Improve incident triage and response workflows.

Example Scenario of SOC & Red Team Interaction



Interaction Between SOC & Threat Intelligence Teams

What is a Threat Intelligence Team?

A Threat Intelligence Team **gathers, analyzes, and distributes** threat intelligence (TI) to help the organization **understand, detect, and respond** to emerging threats.

Their role is to enrich security data, inform detection strategies, and support proactive threat hunting.

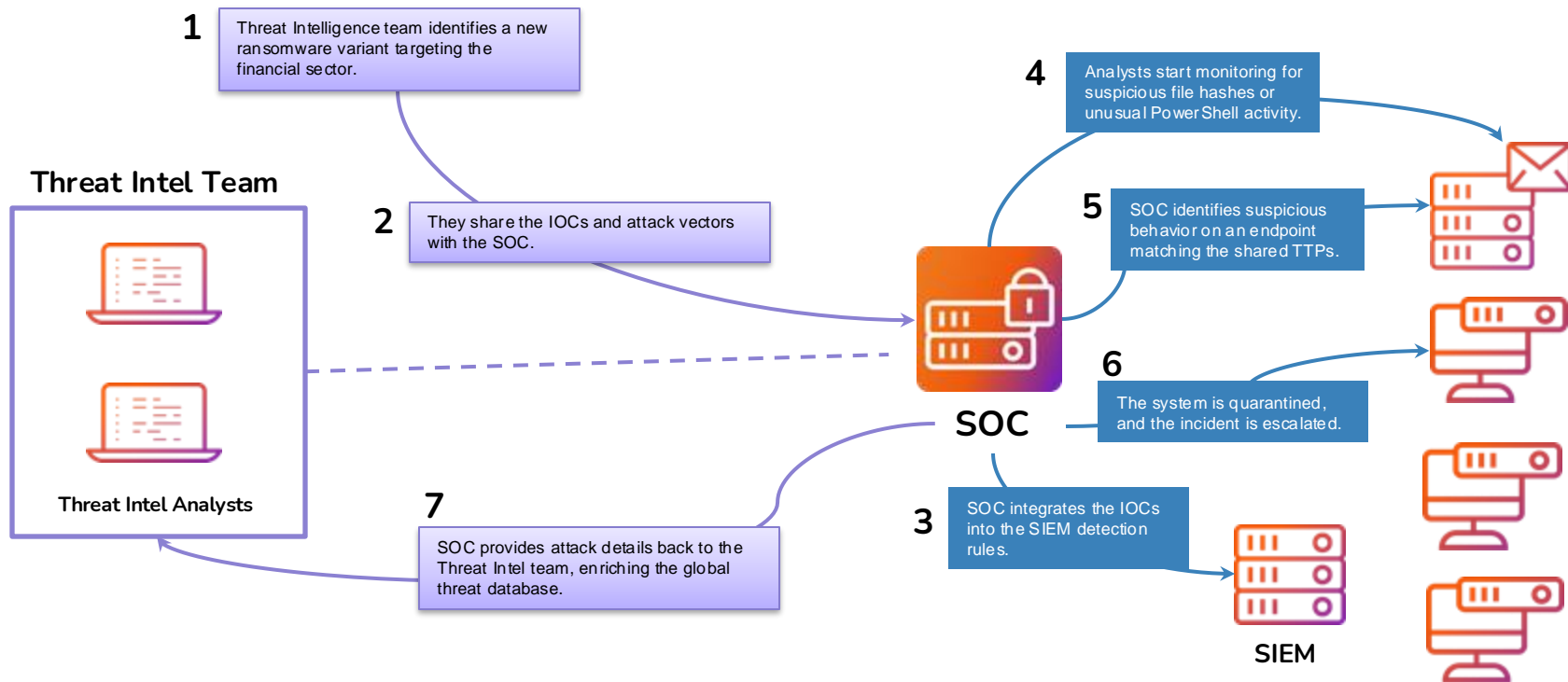
How SOC & Threat Intelligence Teams Interact

Threat Intelligence Role	SOC Role	Interaction Purpose
Collects Indicators of Compromise (IOCs), TTPs, and threat actor profiles.	Uses IOCs and TTPs to enrich SIEM alerts and improve threat detection.	To enhance the accuracy of alerting and correlation.
Analyzes global threat landscapes and tracks adversary behavior.	Uses this intelligence to prioritize alerts and conduct more effective investigations.	To improve threat identification and response processes.
Provides early warnings about emerging threats.	Prepares detection systems to identify and block threats proactively.	To reduce the time to detection (TTD) and response (TTR).
Shares intelligence reports on new vulnerabilities and exploits.	Ensures that vulnerable systems are identified and patched.	To reduce exposure to known attack vectors.

Collaboration Points

Collaboration Point	Description
IOC Sharing & Enrichment	<ul style="list-style-type: none">Threat Intelligence Teams provide SOC with IOCs (malicious IPs, domains, file hashes) for integration into SIEM systems.SOC uses this data to enhance alert correlation and detection accuracy.
Threat Landscape Analysis	<ul style="list-style-type: none">Threat Intel teams provide reports about emerging threats and attack campaigns.SOC uses these insights to prioritize investigations and fine-tune detection rules.
Vulnerability Alerts	<ul style="list-style-type: none">Threat Intel teams identify zero-day vulnerabilities or exploits targeting specific industries.SOC ensures vulnerable systems are isolated, patched, or monitored closely.
Adversary Profiling	<ul style="list-style-type: none">Threat Intel teams provide details about APT groups and their preferred attack techniques.SOC uses this information to map detection rules to adversary TTPs using frameworks like MITRE ATT&CK.

Example Scenario of SOC & Threat Intel Interaction



A man with glasses and a beard is shown in profile, looking at a computer screen in a dark room. The screen displays some code or data. The overall atmosphere is professional and focused.

Incident Detection & Incident Response

Incident Detection & Incident Response

In security operations, **Incident Detection** and **Incident Response** are critical phases of the incident management lifecycle.

While both are essential for protecting organizational assets, ***they serve distinct purposes but are interconnected*** in ensuring an effective security posture.

What is Incident Detection?

Incident Detection is the process of *identifying* and *recognizing potential security incidents* by analyzing logs, monitoring alerts, and detecting anomalies that indicate malicious activity.

It involves the use of automated security tools, continuous monitoring, and proactive threat hunting to detect unauthorized or suspicious behaviors before they escalate.

Key Components of Incident Detection

Component	Description
Log Collection & Aggregation	Collecting logs from systems, endpoints, network devices, and applications.
Real-Time Monitoring	<ul style="list-style-type: none">Utilizing SIEM (Security Information and Event Management) systems to detect anomalies.Monitoring firewall, IDS/IPS, EDR, and cloud security solutions.
Threat Intelligence Integration	Enriching data with IOCs (Indicators of Compromise) to detect known threats.
Correlation & Alerting	Using SIEM and EDR tools to correlate events and generate alerts for suspicious behaviors.
Threat Hunting	Proactively searching for advanced persistent threats (APTs) that evade standard security controls.

Incident Detection Responsibility Matrix

Tier 1 SOC Analyst	Threat Intel Team
Continuously monitor alerts, triage events, and escalate serious threats.	Provide insights into evolving threats and update detection mechanisms.
Security Engineers	Threat Hunters
Ensure security systems (SIEM, EDR) are tuned to capture relevant security telemetry.	Conduct hypothesis-driven searches for hidden or undetected threats.

What is Incident Response?

Incident Response (IR) is the process of *investigating*, *containing*, *eradicating*, and *recovering* from confirmed security incidents.

It ensures that threats are effectively neutralized and that systems are restored to normal operations while minimizing damage.

IR also involves post-incident reviews and process improvements to enhance future responses.

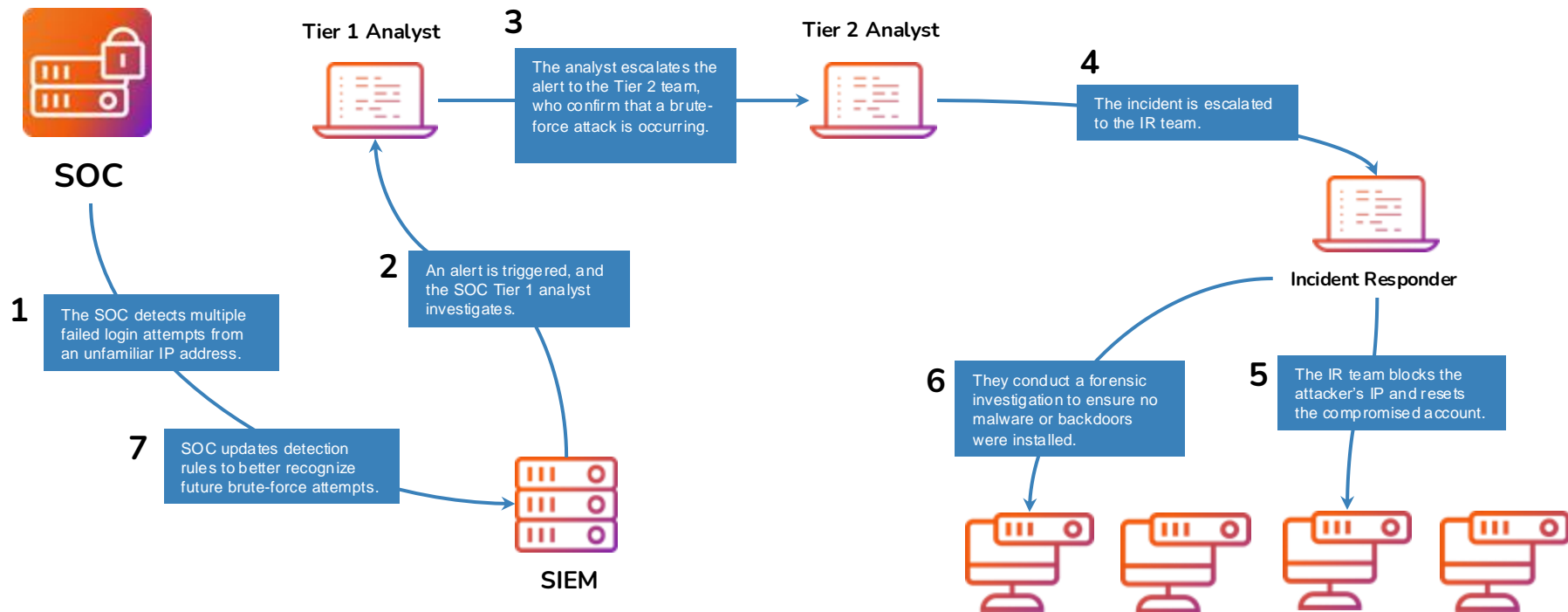
Key Components of Incident Response


Component	Description
Preparation	Establishing an incident response plan, playbooks, and procedures.
Identification & Validation	Confirming the presence of an actual security incident.
Containment	Isolating affected systems and blocking malicious activity to limit the attack's impact.
Eradication	Removing malware, closing vulnerabilities, and ensuring attackers cannot regain access.
Recovery	Restoring affected systems and services while validating their security.
Post-Incident Review	Conducting lessons-learned sessions to refine incident response procedures.

Incident Response Responsibility Matrix

Incident Response Team	CSIRT	Forensics	IT Teams
Conduct technical investigation, containment, eradication, and recovery.	Coordinates the overall response process, communicates with stakeholders, and ensures regulatory compliance.	Investigate digital artifacts to determine attack vectors and gather evidence.	Assist in system recovery, patching, and applying remediation actions.

Example Scenario: Detection & Response in Action





The Incident Response Lifecycle (NIST 800-61)

The Incident Response Lifecycle (NIST 800-61)

The **NIST Special Publication 800-61** outlines a ***standardized incident response lifecycle*** that organizations should follow to effectively ***prepare for, detect, respond to***, and ***recover*** from cybersecurity incidents.

The life cycle is divided into four main phases:

- + Preparation
- + Detection & Analysis
- + Containment, Eradication & Recovery
- + Post-Incident Activity (Lessons Learned)

Preparation

The Preparation Phase involves establishing ***policies, procedures, tools,*** and ***resources*** necessary to effectively detect and respond to incidents.

Key Activities:

- + Develop an incident response policy and define team roles.
- + Establish communication plans and escalation processes.
- + Deploy and configure security tools (SIEM, EDR, IDS/IPS). Conduct employee security awareness training.
- + Create and test incident response playbooks for common scenarios.
- + Perform threat modeling and risk assessments.

Detection & Analysis

This phase focuses on ***identifying*** potential security incidents and ***analyzing*** them to confirm their legitimacy and impact.

Key Activities:

- + Monitor security systems for alerts and suspicious activities.
- + Triage and categorize alerts based on severity and potential impact.
- + Use threat intelligence and forensic analysis to confirm incidents.
- + Document all findings for escalation and investigation.
- + Determine the scope, affected systems, and attacker behavior.

Containment, Eradication & Recovery

This phase focuses on **stopping** the attack, once an **incident is confirmed** and involves **eliminating** the threat, and **restoring systems** to normal operations.

Key Activities:

- + Contain the threat by isolating affected systems and blocking malicious traffic.
- + Eradicate the threat by removing malware, patching vulnerabilities, and ensuring no persistence mechanisms remain.
- + Recover systems by restoring data from backups and verifying system integrity.
- + Perform post-recovery validation to ensure the attacker has been fully removed.

Post-Incident Activity (Lessons Learned)

This phase ensures that ***lessons are learned*** from the incident to ***improve*** future ***detection*** and ***response*** capabilities.

Key Activities:

- + Conduct a post-incident review to analyze what went well and what failed.
- + Update incident response plans and detection rules based on findings.
- + Share findings with threat intelligence teams to enrich data.
- + Provide training for SOC teams on identified weaknesses.
- + Prepare reports for regulatory and compliance requirements.



Event Triage & Investigation Workflow

Event Triage

Event triage is the process of ***analyzing*** and ***categorizing*** security ***alerts*** or ***events*** to determine whether they indicate a potential security incident, a false positive, or a benign activity.

The goal is to quickly assess the relevance and severity of an event and decide on the appropriate next steps.

Event Triage Activities

Activity	Description
Alert Review	<ul style="list-style-type: none">Analyze alerts generated by security tools like SIEM, EDR, IDS/IPS.
Filtering False Positives	<ul style="list-style-type: none">Identify and dismiss non-threatening or routine events.
Severity Assessment	<ul style="list-style-type: none">Classify the event based on potential impact and risk level.
Initial Investigation	<ul style="list-style-type: none">Check logs, user activity, and system behavior for anomalies.
Escalation Decision	<ul style="list-style-type: none">Decide whether the event should be escalated for further investigation.

Event Investigation

Event investigation is the process of **conscientiously analyzing validated security events** to determine the **root cause**, **scope**, and **impact** of a potential security incident.

The objective is to gather enough information to understand the attack, mitigate the threat, and prevent future occurrences.

Event Investigation Activities

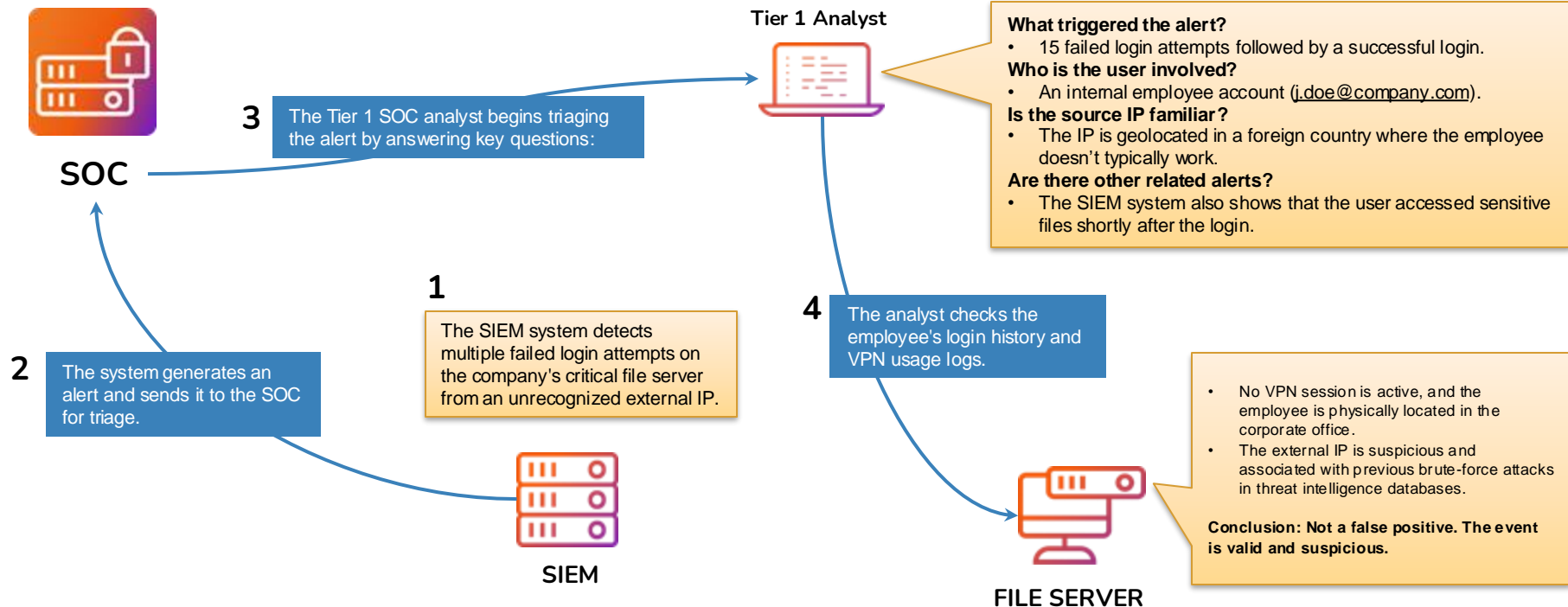
Activity	Description
Root Cause Analysis	<ul style="list-style-type: none">• Determine how the event originated (e.g., phishing, malware).
Attack Scope Determination	<ul style="list-style-type: none">• Identify affected systems, users, and data.
Threat Hunting	<ul style="list-style-type: none">• Search for related suspicious activity or attacker footprints.
Forensics – Collection	<ul style="list-style-type: none">• Gather logs, memory dumps, and network captures for analysis.
Incident Classification	<ul style="list-style-type: none">• Confirm whether the event qualifies as an incident and document it.

Example: Event Triage & Investigation Workflow

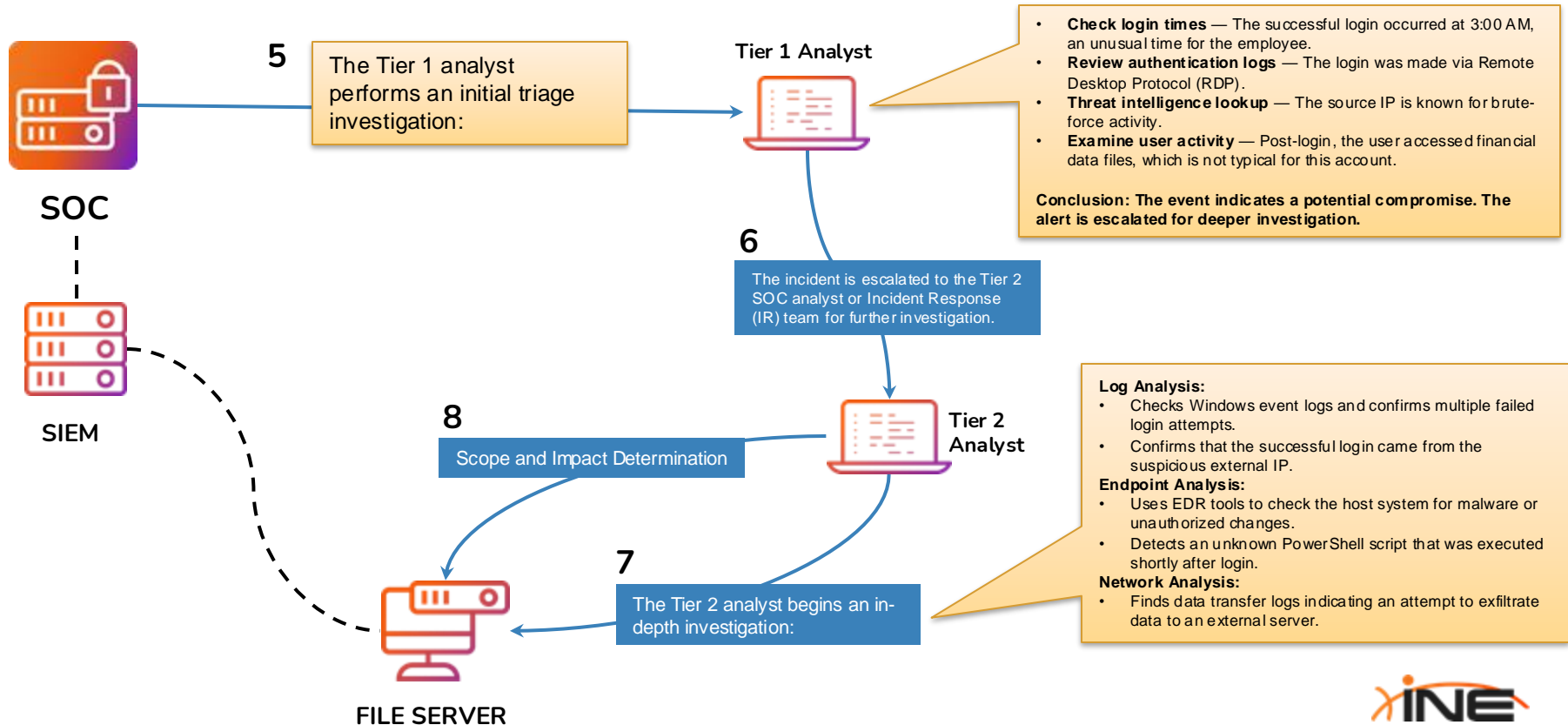
An alert is triggered in the SOC by the SIEM system, indicating multiple failed login attempts on an internal server from an external IP address, followed by a successful login.

The concern is whether this is a brute-force attack or a legitimate activity.

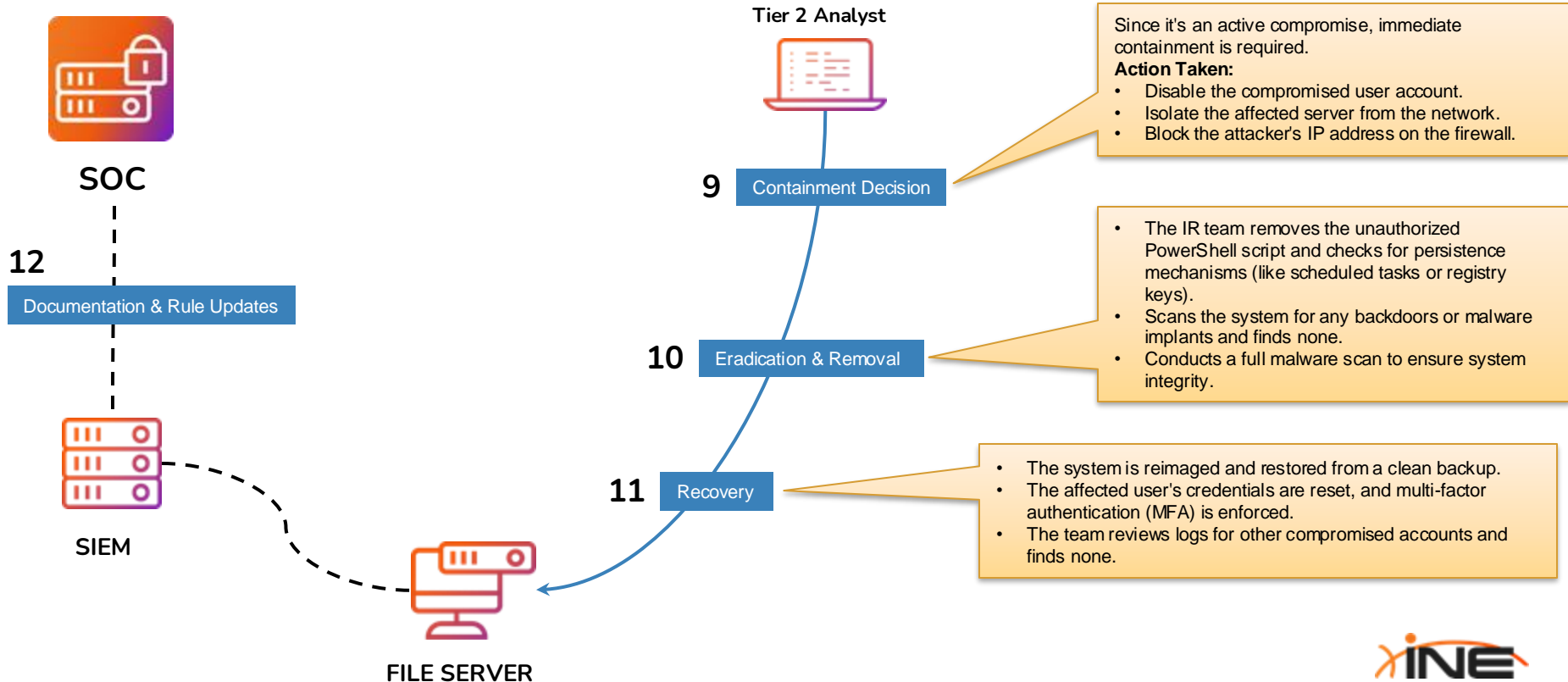
Event Triage Workflow



Investigation Workflow



Investigation Workflow



A man with glasses and a beard is shown in profile, working on a computer in a dark room. The screen displays some code or data. The overall tone is professional and technical.

Escalation & Communication Protocols

Escalation & Communication Protocols

In security operations, **escalation** and **communication protocols** are critical for ensuring that **security incidents** are handled **efficiently, effectively, and transparently**.

These protocols define how and when incidents are escalated within the organization and who needs to be informed at each stage.

Importance of Escalation & Communication Protocols

- + **Speed Up Incident Response:** Ensures incidents are escalated to the right team at the right time.
- + **Minimize Damage:** Helps contain and mitigate the impact of incidents more quickly.
- + **Ensure Consistency:** Standardizes how incidents are managed and communicated.
- + **Meet Compliance Requirements:** Ensures proper documentation and notification to stakeholders, regulators, and legal entities.
- + **Maintain Trust:** Ensures timely and accurate communication to internal and external stakeholders.

Escalation Protocols

What is Escalation in Incident Response?

Escalation is the process of handing over an incident to the appropriate team or authority when its complexity, severity, or potential impact exceeds the initial responder's capabilities.

When should an Incident be escalated?

- + The incident exceeds the capability or authority of the current responder.
- + The incident affects critical infrastructure or sensitive data.
- + The incident is spreading rapidly or impacts multiple systems.
- + When external stakeholders or regulatory bodies need to be involved.
- + If the incident could cause reputational, financial, or legal damage.

Escalation Levels & Criteria

Escalation Levels	Criteria for Escalation	Who to Notify
Level 1 – Low Severity	Minor, routine security events. Easily contained with no significant impact.	SOC Tier 1 Analysts
Level 2 – Moderate Severity	Events requiring more in-depth analysis or multiple system involvement.	SOC Tier 2 or Tier 3 Analysts
Level 3 – High Severity	Confirmed security incidents affecting critical systems or data.	Escalate to Incident Response Team (IR), CSIRT, and management.
Level 4 – Critical Severity	Large-scale incidents involving significant data loss, system outages, or potential regulatory impact.	Notify executive leadership, legal teams, PR, and regulators if needed.

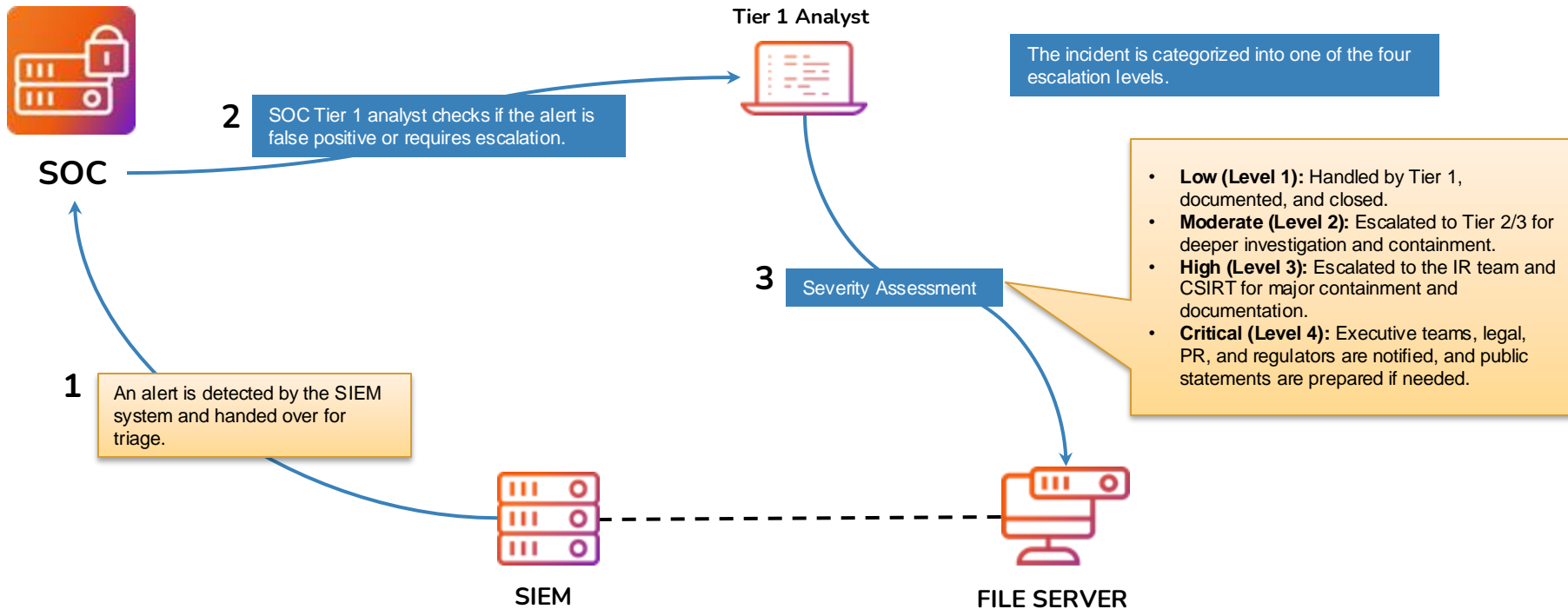
Communication Protocols

Communication protocols define who needs to be informed, what information is shared, and how communication is conducted throughout the incident lifecycle.

Key Elements of Communication Protocols

- + **Communication Channels:** Define approved channels for internal and external communication (e.g., email, secure chat, phone calls, incident management systems).
- + **Roles & Responsibilities:** Identify who is responsible for communicating with internal teams, executives, stakeholders, and regulatory bodies.
- + **Message Consistency:** Ensure consistent, accurate, and timely communication to avoid misinformation.
- + **Confidentiality & Compliance:** Ensure sensitive information is only shared with authorized personnel.
- + **Frequency of Updates:** Define how frequently updates should be provided (e.g., every hour for critical incidents).

Example: Escalation & Communication Workflow



Escalation & Communication Responsibilities

Role	Escalation Responsibility	Communication Responsibility
SOC Tier 1 Analyst	Escalate low-level incidents to Tier 2/3.	Communicate internally within the SOC team.
SOC Tier 2/3 Analyst	Escalate moderate to high-severity incidents to IR Team.	Provide updates to IR Team and CSIRT.
Incident Response Team (IR)	Escalate high and critical incidents to CSIRT and management.	Communicate with internal leadership and technical teams.
CSIRT	Manage escalation of critical incidents to external bodies.	Communicate with executive leadership, legal, and compliance.
Executive Leadership	Escalate incidents that could impact business operations.	Communicate with shareholders, media, and external stakeholders.
Legal & Compliance Team	Ensure regulatory requirements are met.	Handle communications with regulatory bodies.
PR & Communication Team	Manage public-facing communication.	Prepare statements for public disclosure if necessary.



Incident Containment & Eradication

Containment & Eradication

In the incident response lifecycle, the **Containment** and **Eradication** phase is crucial for *minimizing damage, preventing lateral movement, and eliminating threats from the environment.*

Effective containment and eradication strategies ensure that incidents are handled quickly and prevent attackers from re-entering or causing further harm.

This phase occurs after the Detection and Analysis phase and lays the groundwork for successful Recovery.

Containment

Containment involves taking immediate actions to *limit* the *scope* and *impact* of a *security incident*.

The goal is to isolate affected systems, prevent the attacker from moving laterally, and ensure the organization can maintain operations while preparing for full threat eradication.

Objectives of Containment:

- + Isolate affected systems to prevent the spread of malware or unauthorized access.
- + Limit the attacker's ability to access additional systems or data.
- + Preserve forensic evidence for further investigation.
- + Maintain business continuity by minimizing downtime.

Containment

Short-term Containment:

- + Immediate actions to ***stop the attack from spreading.***
- + Temporary measures meant to quickly isolate the compromised systems.
- + Examples:
 - + Disconnecting affected devices from the network.
 - + Blocking malicious IP addresses or domains.
 - + Disabling compromised user accounts.
 - + Applying temporary network segmentation (e.g., VLAN isolation).

Containment

Long-term Containment:

- + More comprehensive measures designed to allow business operations to continue while planning eradication.
- + Focuses on enhancing security posture before a full remediation effort is conducted.
- + Examples:
 - + Patching vulnerable systems to prevent exploitation.
 - + Rebuilding systems with hardened configurations.
 - + Implementing more robust monitoring mechanisms

Eradication

Eradication is the process of *removing* the *root cause* of the incident and ensuring that the attacker's access or persistence mechanisms are fully eliminated.


The goal is to clean the environment and ensure that the threat cannot reoccur.

Objectives of Eradication:

- + Identify and remove malware or any other malicious artifacts.
- + Patch exploited vulnerabilities and close attack vectors.
- + Remove any backdoors or persistence mechanisms used by attackers.
- + Validate that the threat has been fully removed from the environment.

Eradication

Activity	Description
Root Cause Analysis	<ul style="list-style-type: none">• Identifying how the attacker gained access and understanding their tactics, techniques, and procedures (TTPs).• Determining if persistence mechanisms were established.
Artifact Removal	<ul style="list-style-type: none">• Deleting malware, scripts, tools, backdoors, or any other malicious code from systems.• Removing unauthorized user accounts or network connections.
Patch Management & Hardening	<ul style="list-style-type: none">• Applying patches to eliminate vulnerabilities.• Strengthening security configurations on affected systems.
Credential Reset & Management	<ul style="list-style-type: none">• Resetting compromised credentials and enhancing authentication mechanisms.• Implementing Multi-Factor Authentication (MFA) where applicable.
Log Analysis & Monitoring	<ul style="list-style-type: none">• Reviewing logs to confirm that all signs of compromise have been addressed.• Ensuring continuous monitoring for signs of reinfection.

A man with glasses and a beard is shown in profile, looking at a computer monitor in a dark room. The monitor displays some code or data. The overall atmosphere is dark and focused.

Case Study: Ransomware Detection & Response

Case Study: Ransomware Detection & Response

A multinational financial organization experiences a ransomware attack targeting its internal systems.

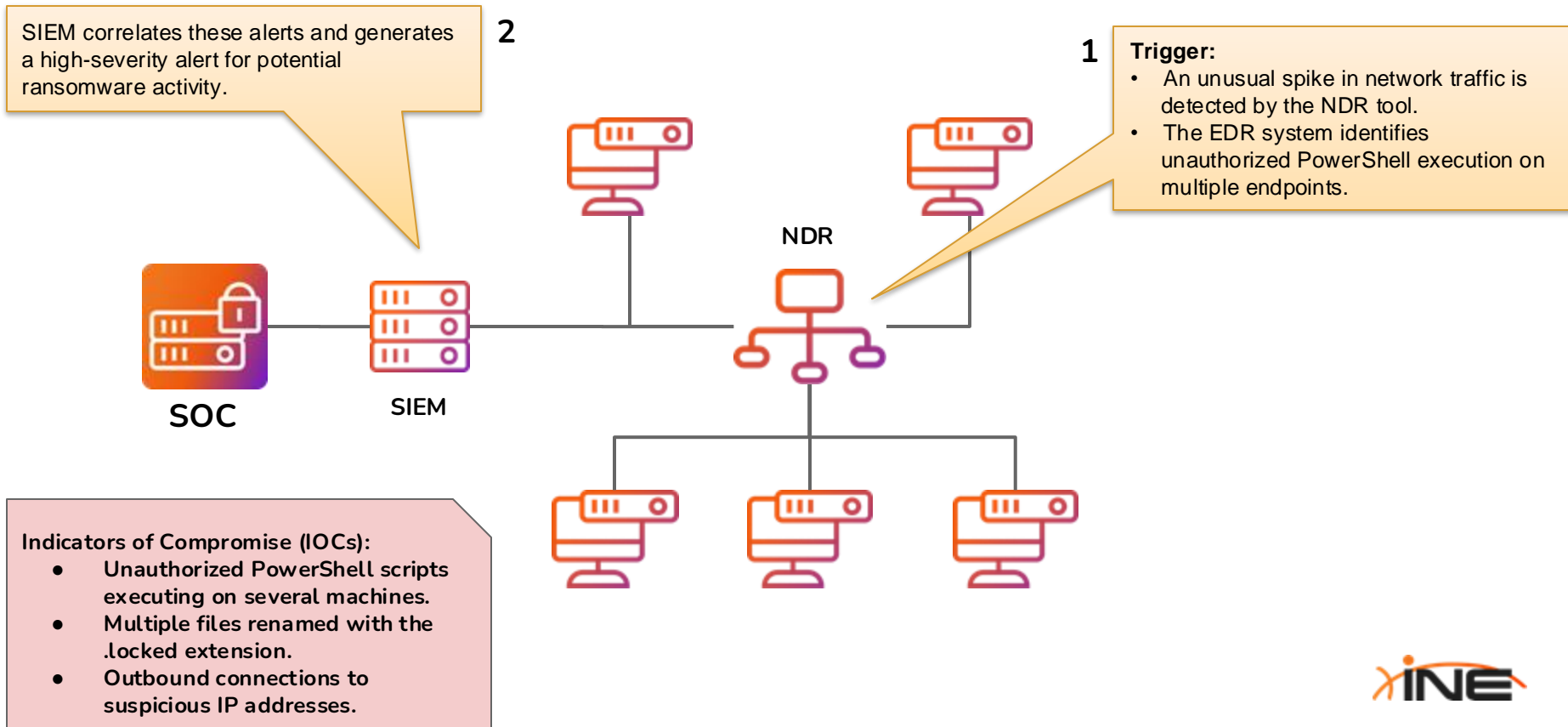
The incident is detected by the organization's Security Operations Center (SOC), which employs a combination of SIEM, EDR, and SOAR tools to identify, contain, and respond to the attack.

Case Study: Ransomware Detection & Response

Company Background:

- + Industry: Financial Services
- + Infrastructure:
 - + Windows-based systems.
 - + Centralized Active Directory for authentication.
 - + EDR (CrowdStrike Falcon), SIEM (Splunk), and SOAR (Palo Alto Cortex XSOAR).

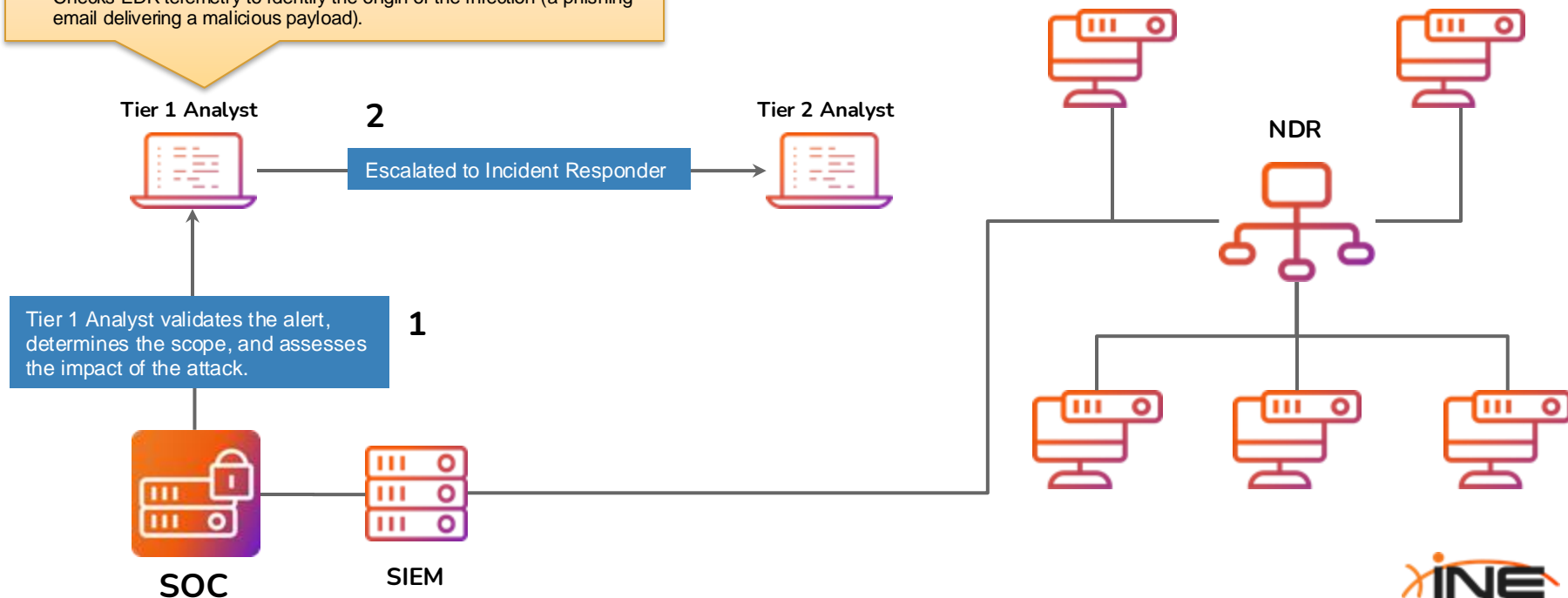
Phase 1: Detection & Alerting (Initial Detection)



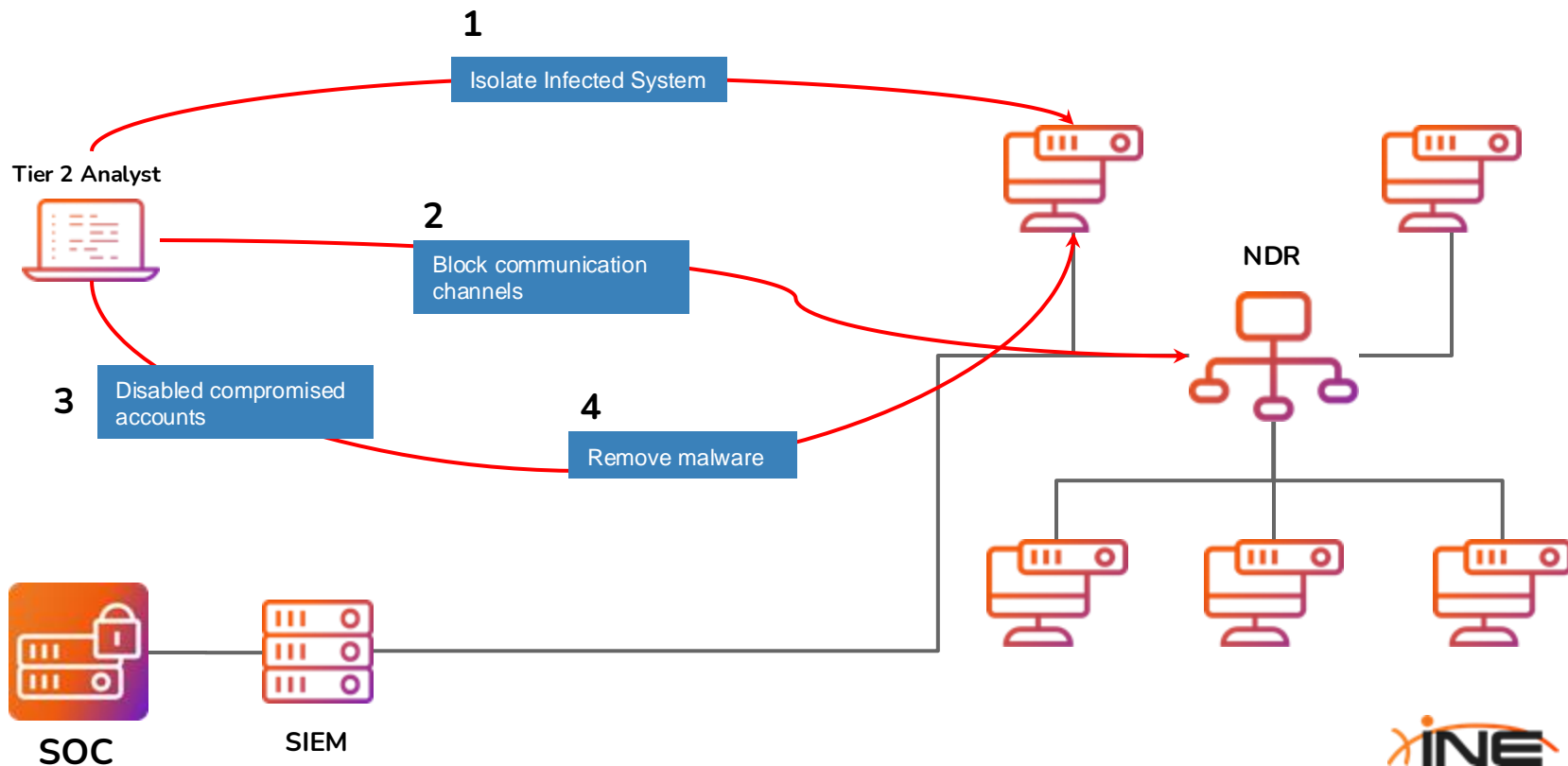
Phase 2: Triage & Analysis (Initial Investigation)

SOC Analyst Actions:

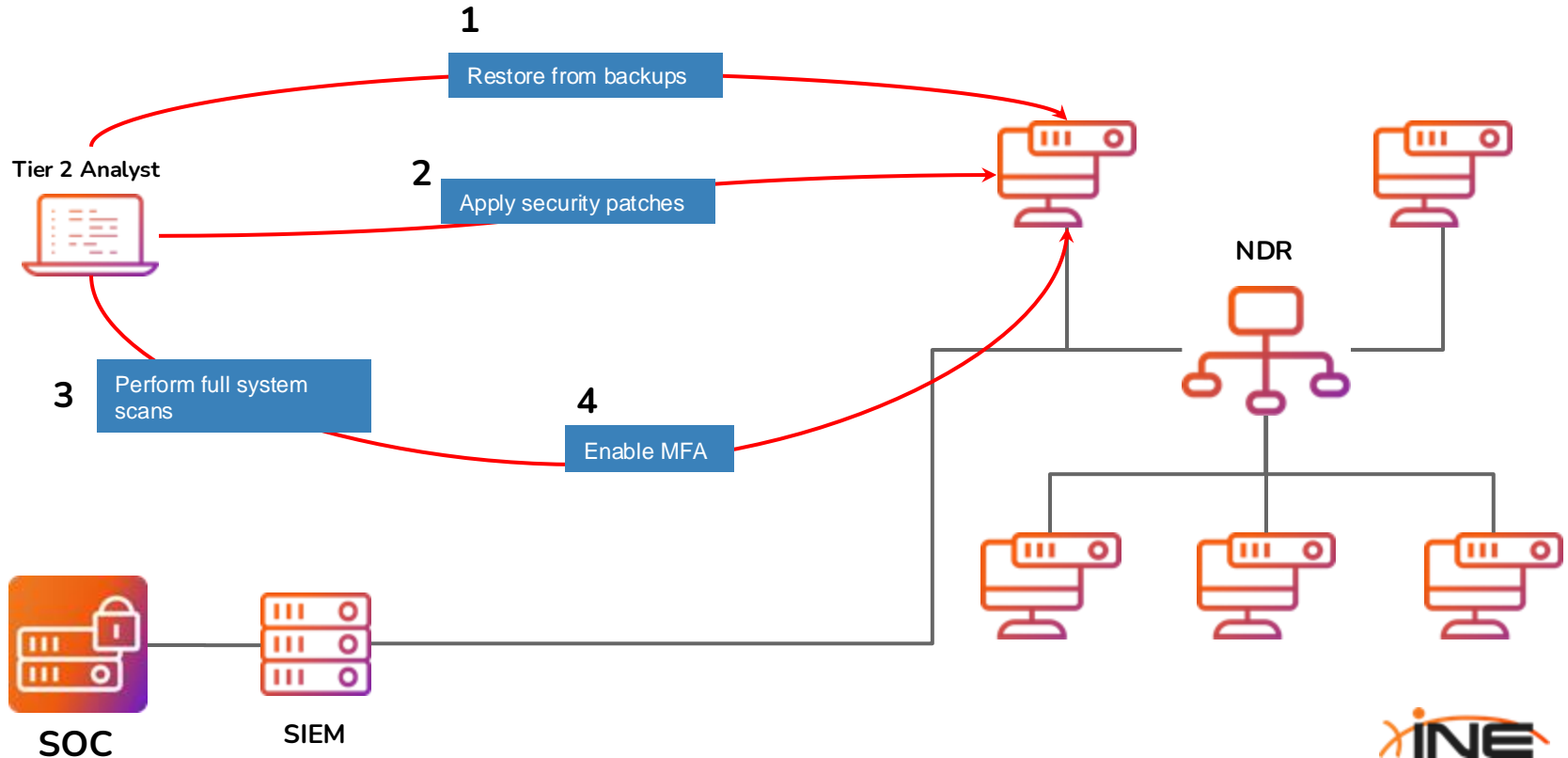
- Reviews SIEM alerts and logs.
- Identifies the source of the PowerShell execution.
- Confirms multiple endpoints are affected with similar symptoms.
- Checks EDR telemetry to identify the origin of the infection (a phishing email delivering a malicious payload).



Phase 3: Containment & Eradication (Response & Mitigation)



Phase 4: Recovery (Restoration & Validation)



Phase 5: Post-Incident Activity (Lessons Learned & Improvement)

Objective: Review the incident, identify gaps, and enhance defenses.

Actions Taken:

- + Conduct a Post-Mortem Review: Analyze what detection mechanisms worked and what failed and Identify areas for improvement in detection and response processes.
- + Update Playbooks: Enhance SOAR playbooks to better detect and respond to similar threats.
- + Improve Detection Rules: Refine SIEM and EDR detection rules for identifying ransomware activity.
- + Enhance User Awareness Training: Educate employees on identifying phishing attempts.
- + Update Backup Policies: Ensure regular backups are performed and stored securely.

Phase 5: Post-Incident Activity (Lessons Learned & Improvement)

Category	What Worked	What Needs Improvement
Detection	EDR and SIEM quickly detected ransomware activity.	Improved visibility into lateral movement needed.
Containment	Automated isolation of infected systems was effective.	Some endpoints were not isolated immediately.
Eradication	Malware was successfully removed using automated playbooks.	Better correlation between SIEM and EDR needed.
Recovery	Backup restoration was successful.	Faster backup validation processes required.
Post-Incident	Lessons learned were well-documented.	Improved training for phishing detection needed.

Lessons Learned

- + **Improve Endpoint Monitoring:** Enhance detection rules for unusual processes like PowerShell execution.
- + **Better Network Segmentation:** Limit exposure of critical assets to unauthorized network access.
- + **Refine Playbooks:** Update SOAR playbooks to include more robust malware detection procedures.
- + **Enhance User Training:** Increase awareness of phishing tactics through periodic training.
- + **Improve Backup Strategy:** Ensure that backups are stored securely and regularly tested for integrity.



Essential SOC Tools & Technologies

Essential SOC Tools & Technologies

In a SOC, various tools and technologies are utilized to ***detect***, ***analyze***, ***respond to***, and ***mitigate*** security threats.

Each tool plays a specific role in strengthening an organization's security posture.

These SOC tools work together to streamline the workflow involving the collection of logs, the detection and investigation of suspicious events, and the tracking, handling, and measurement of each incident.

Essential SOC Tools & Technologies

The following is a list of the core tools used in a SOC:

1. **SIEM** – Security Information and Event Management
2. **EDR** – Endpoint Detection and Response
3. **SOAR** – Security Orchestration, Automation, and Response
4. **NDR** – Network Detection and Response
5. **IDS/IPS** – Intrusion Detection and Prevention Systems
6. **Threat Intelligence Platform**
7. **Incident Management System**

SIEM (Security Information and Event Management)

A **SIEM** is a **centralized** platform that **collects**, **aggregates**, and **analyzes** security data from various sources, such as logs, events, network devices, servers, and applications. ***It provides real-time visibility, threat detection, and alerting.***

Key Features of a SIEM:

- + **Log Aggregation:** Collects logs from multiple data sources (firewalls, servers, applications).
- + **Correlation:** Analyzes and correlates security events to detect anomalies and potential threats.
- + **Alerting:** Generates alerts based on predefined or custom detection rules.
- + **Dashboards and Reporting:** Provides visual dashboards for monitoring security posture and generating reports.
- + **Compliance Monitoring:** Helps meet compliance requirements by logging and documenting security events.



SIEM (Security Information and Event Management)

Why is SIEM essential in a SOC?

- + Provides centralized visibility into security events.
- + Enables real-time threat detection through correlation rules.
- + Supports incident investigation by maintaining a historical log of security events.
- + Aids in regulatory compliance (e.g., GDPR, HIPAA, PCI-DSS).

Popular SIEMs: Splunk, Microsoft Sentinel, IBM QRadar, Elastic Stack (ELK), LogRhythm

EDR (Endpoint Detection & Response)

EDR solutions focus on **detecting**, **investigating**, and **responding** to threats on endpoints like workstations, servers, and mobile devices.

Key Features of EDR:

- + **Real-Time Endpoint Monitoring:** Continuously monitors endpoint activity for suspicious behavior.
- + **Threat Detection:** Identifies malware, ransomware, and fileless attacks on endpoints.
- + **Automated Response:** Quarantines affected files or isolates compromised endpoints.
- + **Forensic Capabilities:** Records endpoint activities for post-incident investigation.
- + **Behavioral Analysis:** Uses machine learning to detect anomalous behavior.



EDR (Endpoint Detection & Response)

Why is EDR essential in a SOC?

- + Enables real-time visibility and response to endpoint-based threats.
- + Provides deep forensic analysis for understanding attacker techniques.
- + Helps in automated containment of infected systems.
- + Detects advanced and persistent threats that bypass traditional antivirus.

Popular EDRs: CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint, Carbon Black



SOAR (Security Orchestration, Automation, and Response)

SOAR platforms help **orchestrate** and **automate** incident response processes. They enable SOC teams to **automatically respond to security incidents**, reducing manual efforts and response times.

Key Features of SOAR:

- + **Automation:** Automates repetitive tasks like alert triage, ticket creation, and IP blocking.
- + **Orchestration:** Integrates with other security tools (SIEM, EDR, firewalls) to coordinate responses.
- + **Playbook Execution:** Executes predefined response playbooks automatically or manually.
- + **Case Management:** Provides a centralized system for tracking and managing incidents.
- + **Collaboration:** Facilitates team collaboration for incident investigations.

SOAR (Security Orchestration, Automation, and Response)

Why is SOAR essential in a SOC?

- + Reduces response time by automating common tasks.
- + Minimizes human error during incident response.
- + Standardizes responses through automated playbooks.
- + Increases efficiency and allows analysts to focus on complex threats.

Popular SOAR Solutions: Palo Alto Cortex XSOAR, IBM Resilient, Splunk SOAR (formerly Phantom), Swimlane, FortiSOAR

NDR (Network Detection & Response)

NDR tools provide detailed and ***granular visibility into network traffic*** and use advanced analytics to detect suspicious behavior, lateral movement, and command-and-control (C2) activities within the network.

Key Features of NDR:

- + **Network Traffic Analysis:** Monitors inbound and outbound network traffic.
- + **Anomaly Detection:** Detects abnormal behavior such as data exfiltration or port scanning.
- + **Encrypted Traffic Inspection:** Analyzes encrypted traffic without decrypting it.
- + **Threat Hunting:** Supports proactive threat hunting by identifying hidden threats.
- + **Automated Response:** Can integrate with firewalls and other tools for automated blocking.

NDR (Network Detection & Response)

Why is NDR essential in a SOC?

- + Provides network-level visibility to detect stealthy threats.
- + Identifies lateral movement and suspicious traffic patterns.
- + Complements EDR by detecting attacks that bypass endpoint controls.
- + Helps detect zero-day attacks and unknown threats.

Popular NDR Solutions: Darktrace, Vectra AI, ExtraHop, Cisco, Stealthwatch, Corelight

IDS/IPS (Intrusion Detection and Prevention Systems)

- + **IDS (Intrusion Detection System)** identifies and alerts on suspicious or malicious network activity.
- + **IPS (Intrusion Prevention System)** not only detects but actively blocks or prevents malicious traffic.

Key Features of IDS/IPS Systems:

- + **Signature-Based Detection:** Identifies threats by matching patterns to known attack signatures.
- + **Anomaly-Based Detection:** Detects unknown attacks by identifying anomalous network behavior.
- + **Traffic Analysis:** Monitors network packets for signs of malicious activity.
- + **Active Prevention (IPS):** Automatically blocks malicious packets in real-time.
- + **Alerting and Logging:** Generates alerts and logs suspicious activities.

IDS/IPS (Intrusion Detection and Prevention Systems)

Why is IDS/IPS essential in a SOC?

- + Provides real-time visibility into potential network attacks.
- + Helps block known attack vectors before they reach critical systems.
- + Acts as an additional security layer, complementing SIEM, EDR, and NDR.
- + Reduces false positives by filtering out non-threatening traffic.

Popular IDS/IPS Solutions: Snort (IDS/IPS), Suricata (IDS/IPS), Cisco Firepower (IPS), Palo Alto Networks (IPS), Security Onion (IDS/IPS)

How These Tools Work Together in a SOC

TOOL	PRIMARY FOCUS	ROLE IN SOC
SIEM	Collecting, analyzing, and correlating security data.	Provides centralized visibility and alerting.
EDR	Monitoring endpoints for suspicious behavior.	Detects and responds to endpoint threats.
SOAR	Automating and orchestrating incident response.	Reduces response time and improves efficiency.
NDR	Monitoring network traffic for anomalies.	Detects stealthy threats and lateral movement.
IDS/IPS	Detecting and blocking network-based attacks.	Prevents known attacks and provides real-time detection.



Threat Intelligence Feeds & Platforms

Understanding Threat Intelligence

Threat Intelligence, also known as **Cyber Threat Intelligence (CTI)**, involves the ***collection***, ***analysis***, and ***dissemination*** of information regarding ***potential*** or ***current threats*** targeting an organization.

This intelligence encompasses details about threat actors, their tactics, techniques, procedures (TTPs), and indicators of compromise (IOCs), enabling organizations to proactively defend against cyber threats.

Understanding Threat Intelligence

The following are the key components of threat intelligence:

- + **Indicators of Compromise (IOCs):** Artifacts such as malicious IP addresses, domain names, file hashes, or email headers that signal potential breaches.
- + **Tactics, Techniques, and Procedures (TTPs):** Insight into the methodologies employed by threat actors, aiding in the anticipation and mitigation of future attacks.
- + **Threat Actor Profiles:** Information about adversaries, including their motives, capabilities, and historical activities.

Threat Intelligence Feeds & Platforms

To effectively harness threat intelligence, organizations utilize ***Threat Intelligence Feeds*** and ***Threat Intelligence Platforms (TIPs)***.

Threat Intelligence Feeds

- + These are ***continuous*** streams of data providing ***real-time*** information on emerging threats.
- + They can be sourced from commercial vendors, open-source communities, or industry-specific sharing groups.
- + Integrating these feeds into security systems enhances an organization's ability to detect and respond to threats promptly.

Threat Intelligence Platforms (TIPs)

TIPs are specialized solutions designed to **aggregate**, **analyze**, and **manage** threat intelligence data **from multiple sources**. They enable organizations to contextualize threat information, automate responses, and facilitate collaboration among security teams.

Threat Intelligence Platforms

- + **Recorded Future:** Utilizes machine learning and natural language processing to collect and organize data from various sources, including the open web and dark web. The platform offers real-time threat intelligence, aiding organizations in proactive defense measures.
- + **Anomali ThreatStream:** Anomali ThreatStream aggregates threat data from various sources, utilizing machine learning to rank threats based on severity. It integrates with multiple security systems, including SIEMs and firewalls, to automate threat detection and response.



Threat Intelligence Platforms (TIPs)

Threat Intelligence Platforms

- + **Mandiant Advantage:** Mandiant Advantage offers a free version providing dashboards, threat actor and vulnerability data, and OSINT indicators. It's suitable for organizations seeking basic threat intelligence capabilities without significant investment.
- + **MISP Threat Sharing:** MISP is an open-source platform for collecting, storing, and sharing cybersecurity indicators and malware analysis. It supports multiple data formats and facilitates collaboration among organizations to enhance threat detection and response.
- + **OpenCTI:** OpenCTI is an open-source platform that structures, stores, and visualizes technical and non-technical information about cyber threats. It integrates with other tools like MISP and TheHive to provide a comprehensive threat intelligence solution.



The Role of Incident Response in the SOC

The Role of Incident Response within a SOC

Incident response is a **core** function of the SOC, ensuring that any ***detected security threats*** are ***properly analyzed, managed, and resolved***.

The SOC's primary responsibility is to ensure that incidents are identified early and handled effectively to minimize risk to the organization.

The Role of Incident Response within a SOC

Role	Activities
Threat Detection & Monitoring	<ul style="list-style-type: none">• The SOC continuously monitors the organization's networks, endpoints, and systems for suspicious activities or IOCs using tools like SIEM, EDR, IDS/IPS.• IR teams in the SOC are responsible for analyzing alerts and determining whether they represent a true security incident.
Triage	<ul style="list-style-type: none">• When an alert is triggered, SOC analysts conduct event triage to determine the severity, scope, and potential impact.• IR teams classify incidents based on severity levels (low, moderate, high, critical) and prioritize their response accordingly.
Incident Investigation	<ul style="list-style-type: none">• The IR team conducts deep investigations to identify the root cause, scope, and impact of the incident.• This involves log analysis, endpoint forensics, network analysis, and leveraging threat intelligence for context.
Containment	<ul style="list-style-type: none">• IR teams develop and implement containment strategies to limit the spread of the incident.

The Role of Incident Response within a SOC

Role	Activities
Eradication	<ul style="list-style-type: none">• The SOC IR team ensures that malware is removed, vulnerabilities are patched, and persistence mechanisms (like backdoors) are eliminated.• They conduct thorough system scans to ensure the complete removal of the threat.
Recovery	<ul style="list-style-type: none">• The IR team coordinates with IT teams to restore systems from clean backups and ensure operations are back to normal.• They validate system integrity to ensure that no residual threats remain.
Post-Incident Review & Analysis	<ul style="list-style-type: none">• After an incident is resolved, the SOC conducts a lessons-learned session to evaluate the response process.
Documentation & Reporting	<ul style="list-style-type: none">• The IR team maintains detailed documentation of every incident, including timelines, actions taken, and mitigation steps.• Reports are shared with executive leadership, legal teams, and regulatory bodies as needed.
Coordination with External Stakeholders	<ul style="list-style-type: none">• In severe incidents, the SOC IR team may need to coordinate with law enforcement, regulators, and external consultants.• They ensure compliance with breach notification requirements and assist in legal investigations.

How IR Collaborates with SOC Functions

SOC FUNCTION	IR TEAM COLLABORATION
SOC Analysts	Receives escalated alerts for deeper investigation and action.
Threat Intelligence Team/Analyst	Receives IOCs and TTPs to contextualize incidents and predict attacker behavior.
Red Team	Shares lessons learned from real incidents to refine red team simulations.
SOAR	Automates certain IR tasks like isolating endpoints or blocking IPs.
Management & Compliance	Provides detailed reports to ensure regulatory compliance.

Importance of IR in the SOC

The SOC's primary mission is to detect, respond to, and prevent security incidents.

Incident Response plays a central role in achieving this mission by:

- + Providing a structured approach to managing incidents.
- + Ensuring rapid identification and containment of attacks.
- + Minimizing damage and ensuring timely recovery of operations.
- + Driving continuous improvement in detection, prevention, and response capabilities.

Common Problems faced by IR Team in the SOC

- + **Alert Fatigue:** Managing a high volume of false-positive alerts.
- + **Skill Gaps:** Ensuring the team is skilled in forensics, malware analysis, and containment strategies.
- + **Limited Visibility:** Incomplete data from network or endpoint systems can hamper investigations.
- + **Lack of Automation:** Manual processes can slow down incident response efforts.



Incident Handling vs. Incident Response

Incident Handling vs. Incident Response

In the context of security operations, Incident Response and incident handling are two **distinct** but **interconnected** phases of the incident management process.

Understanding the difference between the two is crucial for building an effective Security Operations Center (SOC) workflow.

It is also important to understand the difference between them as they are often used interchangeably.

What is Incident Handling?

Incident Handling refers to the overall, structured process of managing and preparing for security incidents.

It includes developing **policies**, **procedures**, and **guidelines** to **detect**, **contain**, **eradicate**, and **recover** from incidents.

The primary objective of **Incident Handling** is to ensure that an organization is ready to effectively manage and mitigate incidents **when they occur**.

What is Incident Handling?

Scope:

- + Preparation (creating playbooks, training, establishing communication channels).
- + Detection (identifying potential threats and attacks).
- + Containment (limiting the damage of a security incident).
- + Eradication (removing the threat from the environment).
- + Recovery (restoring normal operations after an incident).

Incident Handling vs. Incident Response

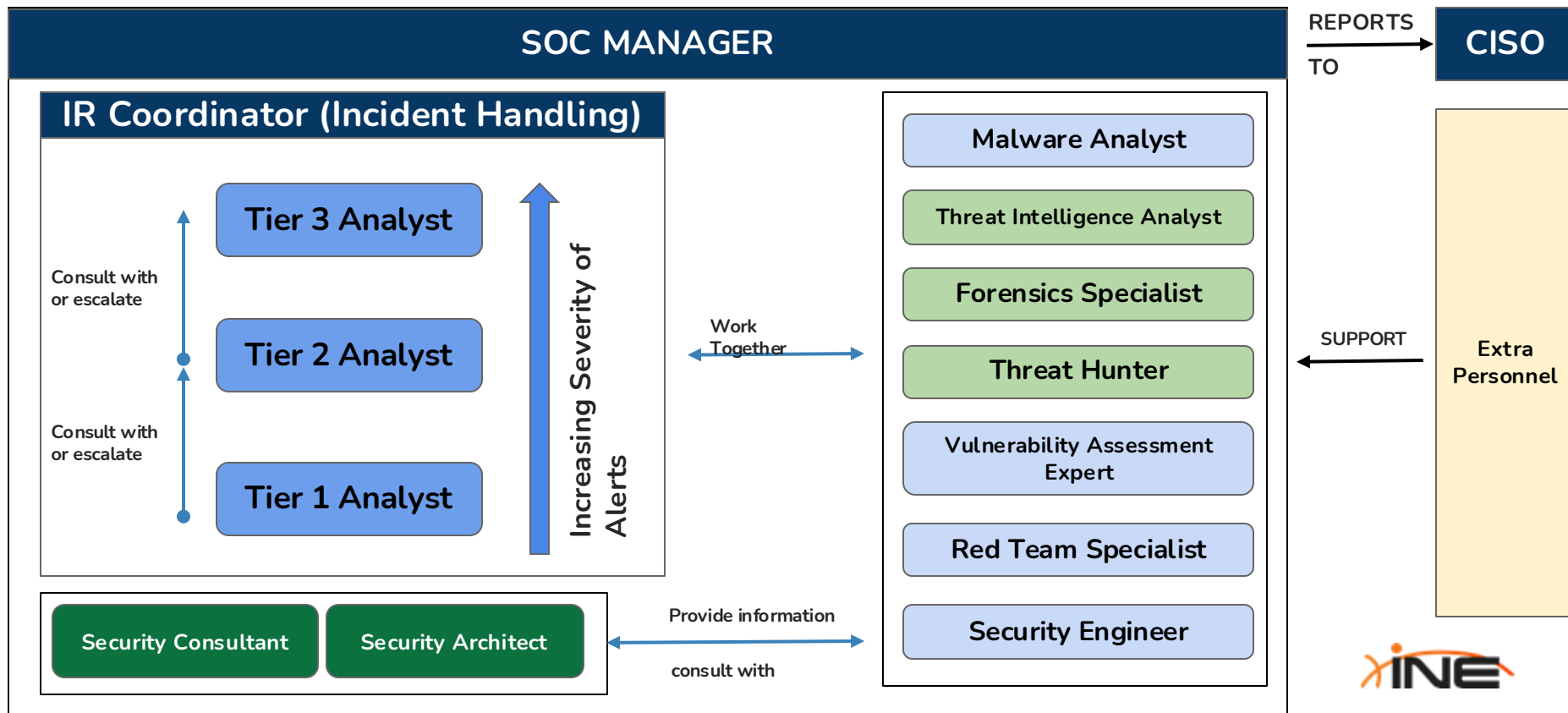
Incident Handling is a broader term that refers to the process of *managing* an incident from start to finish, including *preparation*, *planning* and *coordination* of all activities related to security incidents.

*Incident Response is a subset of incident handling, focusing on the actions taken to mitigate and resolve the incident **after detection**.*

Key Differences

ASPECT	INCIDENT HANDLING	INCIDENT RESPONSE
SCOPE	Broad; Includes planning, detection, response, recovery, and improvement.	Narrow; Primarily focuses on detection, response, containment, and recovery.
EMPHASIS	Preparation, coordination, and overall management of incidents.	Tactical response and remediation of incidents.
GOAL	Building a strong foundation for handling incidents effectively.	Rapidly responding to and mitigating the impact of incidents.
ACTIVITIES	Policies, procedures, training, preparation, and incident management.	Investigation, containment, eradication, recovery, and forensics.
DURATION	Ongoing process.	Event-driven, initiated when an incident occurs.
RESPONSIBILITY	Incident Handling is typically overseen by the Incident Management Team (IMT), which may include SOC Managers, Incident Coordinators, and Compliance/Policy Specialists.	Incident Response is carried out by the Incident Response Team (IRT) or SOC Analysts (Tier 1 - Tier 3), Forensic Analysts, and Threat Hunters.

Interaction of roles within a SOC

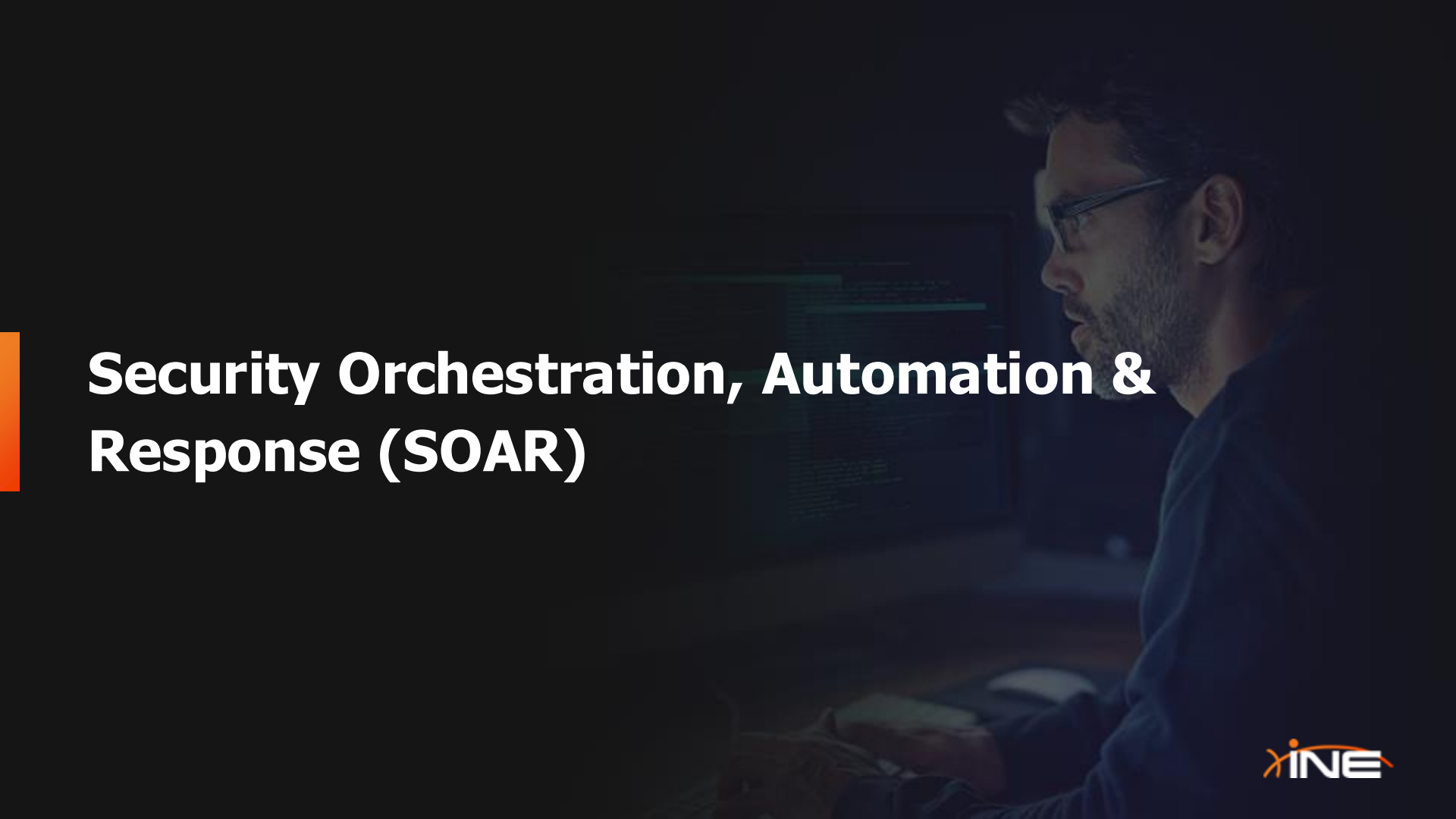


References

“Generally, the terms incident handling and incident response are inconsistently used throughout SOC communities. In some circles, incident handling is considered a broader term than incident response, suggesting it encompasses tracking and reporting, while incident response is specific to responding to the incident itself; although, many SOCs call the function “Incident Response” and include tracking and report writing in the function.”

MITRE. (2022). 11 Strategies of a World-Class Cybersecurity Operations Center. MITRE Corporation.

Retrieved from: <https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf>



Security Orchestration, Automation & Response (SOAR)

Security Orchestration, Automation & Response (SOAR)

SOAR stands for ***Security Orchestration, Automation, and Response***.

It is a cybersecurity solution designed to help organizations **automate**, **coordinate**, and **streamline** their **security operations** and **incident response processes**.

SOAR platforms integrate with existing security tools (like SIEM, EDR, IDS/IPS, firewalls) and enable automated workflows for responding to security threats.

This helps reduce response times, minimize human errors, and enhance operational efficiency.



Security Orchestration, Automation & Response (SOAR)

Orchestration

- + Integrates and coordinates actions across multiple security tools (e.g., SIEM, EDR, firewalls).
- + Ensures security systems work together in a cohesive and efficient manner.

Automation

- + Automates repetitive and manual tasks such as alert triage, enrichment, and response actions.
- + Reduces human intervention in common, low-level security tasks, speeding up the response process.

Response

- + Provides playbooks and workflows for consistent and standardized incident response.
- + Ensures that incidents are responded to quickly and efficiently.

Case Management

- + Centralizes all incident-related information for easy tracking and collaboration.
- + Helps in documenting incidents, tracking progress, and reporting outcomes.



How SOAR Platforms Work

- + **Alert Ingestion** - SOAR ingests security alerts from various sources like SIEM, IDS/IPS, EDR, and threat intelligence platforms.
- + **Automated Triage and Enrichment** - The platform automatically analyzes and enriches alerts with contextual data (e.g., threat intelligence, geolocation, reputation).
- + **Automated Response Execution** - Based on predefined playbooks, SOAR executes automated actions, such as: Isolating infected endpoints, Blocking malicious IPs/domains, Notifying stakeholders.
- + **Case Management and Documentation** - SOAR creates an incident case, logs all actions, and enables analysts to collaborate and track the incident's status.
- + **Post-Incident Review** - Provides analytics and reporting to help improve future response strategies.

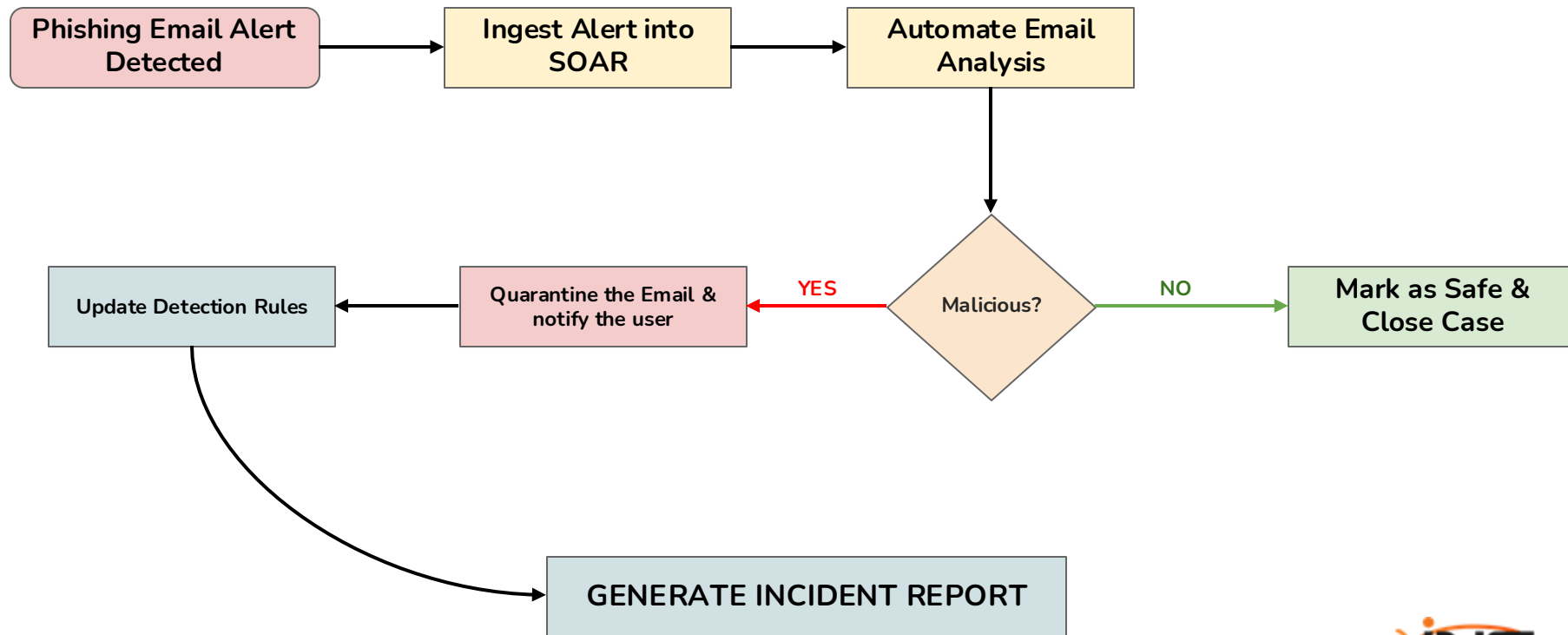
SOAR vs. SIEM

FEATURE	SOAR	SIEM
Primary Role	Automates and orchestrates response processes.	Aggregates and analyzes security event data.
Focus	Response and automation.	Detection and correlation of security events.
Automation Capabilities	Automates response actions using playbooks.	Limited automation, primarily focused on alerting.
Playbook Integration	Provides customized response workflows.	Does not offer response playbooks.
Use Case	Reducing incident response times and improving efficiency.	Detecting security threats through log analysis.

Note: SOAR and SIEM are complementary. SIEM detects and analyzes incidents, while SOAR automates and orchestrates the response.



SOAR Workflow Example: Automated Phishing Response



SOAR Solutions

SOAR Solution	Key Features
Palo Alto Cortex XSOAR	Robust automation, orchestration, and case management capabilities.
Splunk SOAR (Phantom)	Strong integration with Splunk SIEM and other third-party tools.
IBM Resilient	Focuses on flexible and customizable incident response workflows.
Swimlane	Highly scalable with advanced automation capabilities.
FortiSOAR	Offers extensive integrations with Fortinet security solutions.



Automating SOC Workflows with Playbooks

What are Playbooks in the SOC?

In the context of a Security Operations Center (SOC), a playbook is a ***predefined, structured*** set of ***workflows*** and ***actions*** that guide analysts through responding to specific security incidents.

These playbooks help ***standardize*** and ***automate*** the response process, ensuring incidents are handled ***consistently, efficiently, and accurately***.

In essence, Playbooks act as step-by-step guides for responding to security threats, detailing what actions should be taken, in what order, and by whom.

Why use Playbooks in SOC Operations?

- + **Standardization** - Ensures every incident is handled using consistent procedures, reducing errors and oversights.
- + **Speed and Efficiency** - Automates repetitive and time-consuming tasks, accelerating incident response.
- + **Reduces Alert Fatigue** - Automates the triage of low-severity alerts, allowing analysts to focus on critical threats.
- + **Simplifies Decision-Making** - Provides a clear guide for analysts, reducing the need for complex decisions in high-pressure situations.
- + **Enhances Learning** - Helps less-experienced analysts by providing a clear, repeatable response process.
- + **Ensures Compliance** - Supports regulatory and compliance requirements by standardizing documentation and reporting.

How are Playbooks used in the SOC?

- + **Incident Detection** - The SOC detects a potential threat (e.g., a phishing email or a malware alert).
- + **Playbook Triggering** - Based on the type of alert, the corresponding playbook is automatically triggered (via a SOAR platform) or initiated manually by an analyst.
- + **Automated Actions** - The playbook initiates automated tasks such as alert enrichment, triage, or initial containment.
- + **Manual Decision Points** - If needed, the playbook presents decision points where an analyst must review data and choose the next action.
- + **Final Response** - The playbook completes the incident by ensuring containment, eradication, and recovery steps are taken.
- + **Documentation and Reporting** - All actions are logged and reports are generated for compliance and post-incident analysis.

Playbook Examples

Phishing Email Response Playbook

Objective: Automatically analyze and respond to potential phishing emails.

Playbook Procedures:

1. Ingest the Suspicious Email Alert via SIEM or mailbox monitoring.
2. **Automated Analysis:** Check the sender's domain reputation.
 - a. Analyze email headers and attachment hashes against threat intelligence feeds.
 - b. Scan the email body for malicious links.
3. **Containment:** If confirmed malicious, quarantine the email from all mailboxes.
 - a. Block sender's domain in the email security system.
4. **Notify User:** Send an alert to the recipient explaining the malicious nature of the email.
5. **Update Detection Rules:** Add new indicators to block similar attacks in the future.
6. **Document the Incident:** Automatically generate an incident report.

Malware Detection and Containment Playbook

Objective: Automatically detect and contain malware threats on endpoints.

Playbook Procedures:

1. Ingest the Malware Alert from EDR or SIEM systems.
2. **Automated Enrichment:** Scan the file hash in a threat intelligence database.
 - a. Identify the origin of the malware (e.g., phishing, drive-by download).
3. **Containment:**
 - a. Automatically isolate the affected endpoint.
 - b. Block communication with known C2 servers.
4. **Remediation:**
 - a. Run an automated malware scan.
 - b. Remove or quarantine the malicious files.
5. **Recovery and Validation:**
 - a. Ensure the endpoint is clean and reconnect to the network.
6. **Documentation:**
 - a. Record all actions and prepare an incident report.

IR Playbook Examples & Templates

- + Counteractive's Incident Response Plan Template:
<https://github.com/counteractive/incident-response-plan-template>
- + Microsoft Incident Response Playbooks: <https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks>
- + SOCfortress Playbooks for SOC Analysts:
<https://github.com/socfortress/Playbooks>
- + CISA's Cybersecurity Incident & Vulnerability Response Playbooks:
https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf



AI & Machine Learning in SOC Operations

AI & ML in the SOC

In SOCs, Artificial Intelligence (AI) and Machine Learning (ML) are leveraged to ***enhance threat detection, analysis, and incident response.***

These technologies automate routine tasks, identify sophisticated threats, and help security teams respond faster and more effectively to cyberattacks.

AI involves systems designed to mimic human intelligence, while ML (a subset of AI) enables systems to learn from data and improve over time without being explicitly programmed.



Why use AI & ML in the SOC?

CHALLENGE	AI/ML APPLICABILITY
High Alert Volume	Filters out false positives and prioritizes real threats.
Evolving Threats	Detects new and unknown attack patterns using <i>behavioral analysis</i> .
Limited Human Resources	Automates repetitive tasks, reducing analyst workload.
Slow Incident Response Times	Provides real-time insights and accelerates response actions.
Complex Data Analysis	Correlates massive datasets to uncover hidden attack patterns.

How AI & ML Enhances SOC Tools

SOC TOOL/SOLUTION	AI/ML ENHANCEMENT
SIEM	Improves anomaly detection and reduces false positives by analyzing complex data patterns.
EDR	Detects unknown malware and suspicious endpoint behavior using behavioral analysis.
SOAR	Automates decision-making processes and optimizes response workflows.
NDR	Identifies anomalous network traffic and lateral movement across systems.
UEBA	Continuously learns and adapts to user behaviors, identifying deviations that indicate potential threats.

Real-World Examples of AI & ML in SOC

VENDOR/TOOL	AI/ML CAPABILITIES
CrowdStrike Falcon	AI-driven EDR with advanced behavioral detection and threat hunting.
Microsoft Sentinel	Uses AI to analyze security data and identify suspicious activities.
Darktrace	Leverages ML for autonomous response and anomaly detection in network environments.
Splunk	Uses ML to create advanced correlation rules and prioritize security alerts.
Palo Alto Cortex XSOAR	Automates response processes using AI to recommend actions based on incident data.

Introduction to Security Operations Center (SOC) - Summary

Key Concepts - Recap

- + Introduction to Security Operations
- + Key Functions & Services of a SOC
- + SOC Structure & Roles
- + SOC Workflows & Processes



Learning Outcomes Recap

- + Understand the Fundamentals of a SOC: Explain the purpose, structure, and key functions of a SOC, including different SOC models (In-house, Managed, Hybrid) and SOC tiers (Tier 1, 2, 3).
- + Identify Key Roles and Teams in a SOC: Describe the roles and responsibilities of SOC analysts, threat hunters, digital forensics teams, CSIRT, IRT, red teams, and threat intelligence teams.
- + Understand SOC Frameworks and Maturity Models: Compare various SOC maturity models and frameworks to assess and improve SOC effectiveness.
- + Explain the Incident Response Lifecycle: Detail the phases of the Incident Response Lifecycle according to NIST 800-61, including detection, containment, eradication, recovery, and lessons learned.
- + Incident Detection & Response Techniques: Describe IR techniques like event triage, investigation workflows, escalation protocols, and response strategies.
- + SOC Tools & Automations: Have an understanding of essential SOC tools, technologies, and automation techniques, including SOAR platforms, threat intelligence feeds, and the use of AI & Machine Learning to enhance SOC efficiency.

Next Steps

- + Research Incident Response Frameworks: Study the NIST 800-61 Incident Response Lifecycle and compare it with other industry-standard frameworks.
- + Explore SOC Automation Tools: Investigate various SOAR platforms and their capabilities to enhance SOC workflows and response processes.
- + Examine Threat Intelligence Platforms: Review different threat intelligence feeds and platforms to understand how they contribute to proactive threat detection and defense.

THANKS FOR WATCHING!



EXPERTS AT MAKING YOU AN EXPERT

