

# Incident Response: Preparation

# Alexis Ahmed

Red Team & Blue Team Instructor @INE

Red Team Lead @HackerSploit

---

# Key Concepts

- + Incident Response Fundamentals
- + Incident Response Teams and Structures
- + The Preparation Phase in Incident Response

# MAJOR TOPICS

- + IR Teams
- + IR Process & Frameworks (NIST, SANS)
- + The Preparation Phase of IR
- + IR Planning & Documentation (RACI, IR Policy, IRPs, Playbooks)
- + Incident Management Process & Platforms
- + Incident Response Toolkit



## LEARNING OUTCOMES

- + Explain the importance of incident response and the risks of unstructured response efforts
- + Identify different types of security incidents and common attack vectors
- + Describe various types of incident response teams, their structures, and their roles
- + Understand and differentiate between major IR frameworks (NIST and SANS)
- + Develop foundational IR artifacts such as policies, plans, playbooks, and responsibility matrices
- + Apply the Hierarchy of Needs model to build incident response readiness
- + Understand the role of technology infrastructure in supporting incident response activities
- + Manage security incidents using an incident management platform (TheHive)
- + Build a basic yet effective Incident Response Toolkit tailored for operational use

# PREREQUISITES

- + A basic understanding of cybersecurity concepts (e.g., threats, vulnerabilities, risk)
- + Familiarity with general IT systems, networks, and common security tools



**LET'S GO!**





# Introduction To Incident Response



# What is Incident Response?

**Incident Response (IR)** is the structured process organizations follow to **detect**, **investigate**, **contain**, **eradicate**, and **recover** from cybersecurity incidents, such as data breaches or malware infections.

*Its goal is to minimize damage, reduce recovery time and costs, and prevent future incidents.*

**But what exactly is an “Incident”?**

# Events & Incidents

An **Event** is any observable occurrence in a system or network. This could be something routine like a user login, a file being accessed, or network traffic. Most events are harmless and part of normal operations.

**Adverse events** are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. — *NIST SP 800-61r2*

# Events & Incidents

Examples of Events:

- + A user successfully logging into their workstation
- + A file being accessed or modified
- + A firewall logging allowed traffic
- + A scheduled system reboot
- + An antivirus scan completing successfully

# Events & Incidents

An **Incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. –  
– *NIST 800-61r2*

An incident is a security event, or a series of related events that indicates a **potential** security breach, policy violation, or malicious activity that threatens the confidentiality, integrity, or availability of systems or data.

In short → ***Every incident is an event, but not every event is an incident.***

# Events & Incidents

Examples of Incidents:

- + Multiple failed login attempts followed by a successful login (possible brute-force attack)
- + Malware detected and quarantined on an endpoint
- + Unusual outbound traffic from a server (possible data exfiltration)
- + Unauthorized access to sensitive files
- + A user account performing privilege escalation without justification

# IR... What is it good for?

The purpose of Incident Response is to help organizations quickly detect, contain, and recover from security incidents in order to minimize damage, reduce downtime, and prevent further compromise.

It's all about **responding** in a ***structured and efficient way*** — so that when something goes wrong, you know exactly what steps to take to protect critical systems, limit the impact, and get operations back to normal as fast as possible.

# IR... What is it good for?

Additionally, Incident Response helps organizations learn from incidents by identifying root causes and security gaps, ultimately improving defenses and reducing the risk/likelihoods of similar attacks/incidents happening again.

It ensures a structured and efficient approach to managing incidents, allowing teams to protect critical systems, limit the impact, and restore normal operations as swiftly as possible.

# Key Objectives of IR

The key objectives of Incident Response are:

- 1. Detect the incident as early as possible**
- 2. Contain the threat to prevent it from spreading**
- 3. Eradicate the root cause of the incident**
- 4. Recover affected systems and restore normal operations**
- 5. Learn from the incident to improve future security**



# Incident Responder

An **Incident Responder** is a cybersecurity professional responsible for managing and handling security incidents within an organization.

*Their primary role is to detect, analyze, contain, and recover from security incidents to minimize damage and restore normal operations.*

An Incident Responder is the **frontline defender during a security incident** — responsible for identifying threats, containing the attack, restoring operations, and ensuring the organization learns from the incident to prevent future occurrences.





# The Need For Incident Response

# The Need For IR

**Incident Response** is a critical part of any organization's cybersecurity strategy. As cyber threats continue to evolve, organizations must be prepared to respond quickly and effectively to security incidents.

*Without a structured response capability, even a small incident can escalate into a major security breach with severe business, financial, and reputational consequences.*

This is why Incident Response is important → it enables organizations to minimize damage, recover faster, meet compliance requirements, and build resilience against future attacks.



# The Need For IR

## 1. Growing Threat Landscape

The **volume** and **complexity** of cyber threats are increasing daily. Attackers are using advanced techniques like ransomware, phishing, zero-day exploits, and supply chain attacks.

***No organization is immune. From small businesses to large enterprises.***

Making a proactive incident response capability critical to defend against modern threats.



# The Need For IR

## 2. Speed of Attacks vs Speed of Response

Cyber attacks can escalate in minutes, a phishing email can lead to credential compromise, lateral movement, and data exfiltration in under an hour.

***If an organization cannot detect and respond quickly, the damage can spiral out of control.***

A well-structured incident response process ensures faster detection, containment, and recovery — reducing the window of opportunity for attackers.



# The Need For IR

## 3. Business & Operational Impact

Security incidents can cause significant disruptions:

- + **System downtime**
- + **Loss of sensitive data**
- + **Financial loss**
- + **Interruption of services**
- + **Damage to brand and customer trust**

IR helps mitigate these impacts by restoring normal operations faster and limiting the reach of the attack.

# The Need For IR

## 4. Regulatory & Compliance Requirements

Regulatory frameworks such as **GDPR**, **HIPAA**, **PCI-DSS**, and **NIS2** require organizations to have an incident response plan and report certain incidents within specific timeframes.

***Non-compliance can lead to heavy fines, lawsuits, and reputational damage.***

Having a robust IR process ensures legal obligations are met and regulatory scrutiny is handled effectively.





# Types of Incidents & Attack Vectors



# Types of Incidents & Attack Vectors

In the context of Incident Response, *incidents can take many forms* depending on how the attacker gains access, their objectives, and the systems targeted.

*Understanding the different types of incidents and attack vectors helps responders classify threats, prioritize actions, and respond effectively.*

# Types of Incidents & Attack Vectors

In the context of Incident Response, attack vectors refer to the specific paths, methods, or techniques that attackers use to gain unauthorized access to a system, network, or application.

***An attack vector is essentially how an attacker gets in.***

# Types of Incidents & Attack Vectors

- *Incident Types describe **what** happened.*
- *Attack Vectors describe **how** it happened.*

# Common Types of Incidents

Incident Type	Description
Malware Infection	Malicious software (ransomware, trojans, spyware) infects systems.
Phishing Attack	Deceptive emails trick users into revealing credentials or downloading malware.
Unauthorized Access	An attacker gains access to systems, networks, or data without permission.
Denial of Service (DoS/DDoS)	Attackers flood systems or networks with traffic to disrupt services.
Insider Threat	A trusted employee misuses access to steal data or cause damage.
Data Breach	Sensitive data is stolen, leaked, or exposed to unauthorized parties.
Web Application Attack	Exploitation of web app vulnerabilities (SQL Injection, XSS, etc.).
Credential Compromise	User credentials (usernames/passwords) are stolen and abused.

# Common Attack Vectors

Attack Vector	Description
Phishing Emails	Malicious emails with attachments or links to steal credentials or deploy malware.
Vulnerability Exploitation	Attacks targeting unpatched software, misconfigurations, or weak security controls.
Brute-Force Attacks	Automated guessing of passwords to gain access.
Drive-By Downloads	Visiting compromised websites that automatically download malware.
Supply Chain Attacks	Compromise of trusted software or service providers.
Removable Media	Malware introduced via USB drives or external storage.
Insider Threats	Malicious or negligent actions by employees or contractors.

# Types of IR Teams

# Types of IR Teams & How They Are Organized

An **Incident Response (IR) team** is a group of cybersecurity and IT professionals responsible for detecting, analyzing, containing, and responding to security incidents to minimize damage and restore normal operations.

**But not all incident response teams are the same.**



# Types of IR Teams & How They Are Organized

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

Organizations structure their Incident Response (IR) teams based on size, resources, and operational requirements.

***There is no one-size-fits-all*** — but typically, IR teams fall into a **few common models**.





# Centralized IR Team

*One dedicated team responsible for handling all incidents across the organization.*

## Characteristics:

- All IR staff are part of a single, centralized team (often within the SOC or Security Department).
- Clear chain of command and standardized processes.

## Suitable For:

- Small to Medium Organizations
- Companies with a single headquarters or minimal remote locations.

# Distributed IR Team

*Multiple smaller IR teams embedded within different departments, regions, or business units.*

## Characteristics:

- Local IR teams handle incidents in their area or region.
- Central coordination for major incidents or escalation.

## Suitable For:

- Large Enterprises
- Multinational Organizations
- Companies with multiple branches/offices.

# Coordinated/Hybrid IR Team

*Combination of centralized command with distributed response teams.*

## Characteristics:

- A central IR team provides policies, guidance, and oversight.
- Local IT/security teams execute initial response.
- Collaboration between central and distributed teams.

## Suitable For:

- Enterprises with global operations
- Organizations requiring flexibility and local presence.

# Outsourced/Managed IR Team (MSSP)

*Incident Response is handled by an external service provider (MSSP or IR Consulting firm).*

## Characteristics:

- Incident Response functions are outsourced.
- Contracts or Service Level Agreements (SLAs) define response times and services.

## Suitable For:

- Small companies without internal security teams.
- Organizations lacking IR expertise or resources.

# Virtual IR Team (VIRT)

*Cross-functional team formed from existing employees across IT, Security, Legal, PR, and Management — activated when an incident occurs.*

## Characteristics:

- Not a full-time dedicated IR team.
- Members are assigned IR roles alongside their normal duties.

## Suitable For:

- Smaller organizations.
- Organizations that experience infrequent incidents.

# Summary

Team Type	Key Characteristic	Best suited for
Centralized IR	Single dedicated team	Small/Medium Organizations
Distributed IR	Multiple local teams	Large/Global Enterprises
Hybrid IR	Central command + Local response	Enterprises with multiple regions
Outsourced IR	External Provider/MSSP manages IR	Organizations lacking internal capability
Virtual IR	Cross-functional ad-hoc team	Small organizations with limited resources

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 tone is professional and tech-oriented.

# **IR Teams: Same Role, Different Names**

# IR Teams: Same Role, Different Names

Incident Response teams are often referred to by different names, which can sometimes cause confusion or misunderstanding — especially for those new to the field.

Regardless of whether it's called a CIRT, CSIRT, CERT, or simply an Incident Response Team (IRT), **the purpose remains the same:**

***Detect, respond to, and recover from security incidents.***

In the following slides, we'll explore the most commonly used names for Incident Response teams, how they differ, why these differences exist, and how naming conventions often reflect an organization's structure, maturity, or focus.





# Common Names for IR Teams

Different organizations and industries use various names for their Incident Response teams — often based on their structure, function, or focus area.

These names are typically interchangeable but can signal specific roles or responsibilities.

# Common Names for IR Teams

Name	Meaning	Usage Context	Notes / Differences
<b>CSIRT</b>	Computer Security Incident Response Team	Most commonly used modern term in cybersecurity and enterprise environments	Emphasizes both "Security" and "Incident Response" — preferred for formal IR teams focused on prevention, detection, and response. Standard term in industry best practices (NIST, ISO).
<b>CIRT</b>	Computer Incident Response Team	Older or simplified term. Still used by some organizations	Focus is purely on "Incident Response" without explicitly highlighting security operations. Used where the team is primarily reactive rather than proactive.

# Common Names for IR Teams

Name	Meaning	Usage Context	Notes / Differences
<b>SIRT</b>	Security Incident Response Team	Flexible/general term used across different industries	Emphasizes response to any "Security Incident" — whether IT-related or physical security. Used where IR responsibilities cover a broader scope beyond just IT systems.
<b>CERT</b>	Computer Emergency Response Team	Originally coined (trademarked) by Carnegie Mellon CERT/CC — used globally for national, regional, and sector-based IR teams	CERT is often used in government, military, or large sector-wide teams (e.g., US-CERT, CERT-EU). Implies a focus on large-scale incident coordination or emergency response, not just enterprise IR.

# Common Names for IR Teams

Name	Meaning	Usage Context	Notes / Differences
<b>IRT</b>	Incident Response Team	Generic catch-all term	Used in smaller organizations or non-technical environments where simplicity is preferred. Refers to any team responsible for handling incidents — security-related or not.

# How IR Team Names Influence Roles & Structure

While the core mission of all Incident Response teams is the same; detect, respond, and recover from security incidents, the name used for the team often reflects its scope, structure, and responsibilities within the organization.

# Example 1: CSIRT – Computer Security Incident Response Team

## *Enterprise/Internal Security Focus*

A **CSIRT** is typically an internal, dedicated security team responsible for managing and responding to cybersecurity incidents within a single organization.

Their responsibilities are usually technical and operational, such as:

- + Threat detection & monitoring
- + Incident handling & forensics
- + Coordinating containment & recovery
- + Improving security controls & playbooks

A CSIRT operates as part of a Security Operations Center (SOC) or reports directly to the CISO.



## Example 2: CERT– Computer Emergency Response Team

### *National, Sector-Wide, or Public-Facing Focus*

A **CERT** often operates at a ***national or industry-sector level*** (e.g., US-CERT, CERT-EU, CERT-CC).

Their role extends beyond internal incident handling, they also provide:

- + National-level threat intelligence
- + Coordination between multiple organizations
- + Advisories, alerts, and best practices
- + Incident coordination across sectors (government, finance, critical infrastructure)

***CERT teams don't directly manage incidents inside individual companies — they guide, coordinate, and support response efforts across multiple organizations.***



## Example 3: SIRT – Security Incident Response Team

### *Broader Security Scope Beyond IT*

Some organizations use **SIRT** when the team is responsible for responding not only to cybersecurity incidents but also to:

- + Physical security incidents
- + Insider threats
- + Fraud investigations
- + Corporate security breaches

*This name indicates a broader cross-functional team often involving HR, Legal, and Physical Security teams.*



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 "IR Teams: Roles & Responsibilities" is overlaid on the left side of the image.

# IR Teams: Roles & Responsibilities

# IR Teams: Roles & Responsibilities

A **successful Incident Response effort** relies on the **coordination** and **collaboration** of multiple individuals and departments, each fulfilling specific roles that contribute to the overall response effort.

From detection and triage to containment, legal compliance, and public communication, every function within the IR team plays a vital role in managing and resolving security incidents effectively.

In the next set of slides, we'll break down the common roles within an IR team, including technical responders like SOC analysts and forensic specialists, as well as key supporting roles such as legal, PR, and HR.

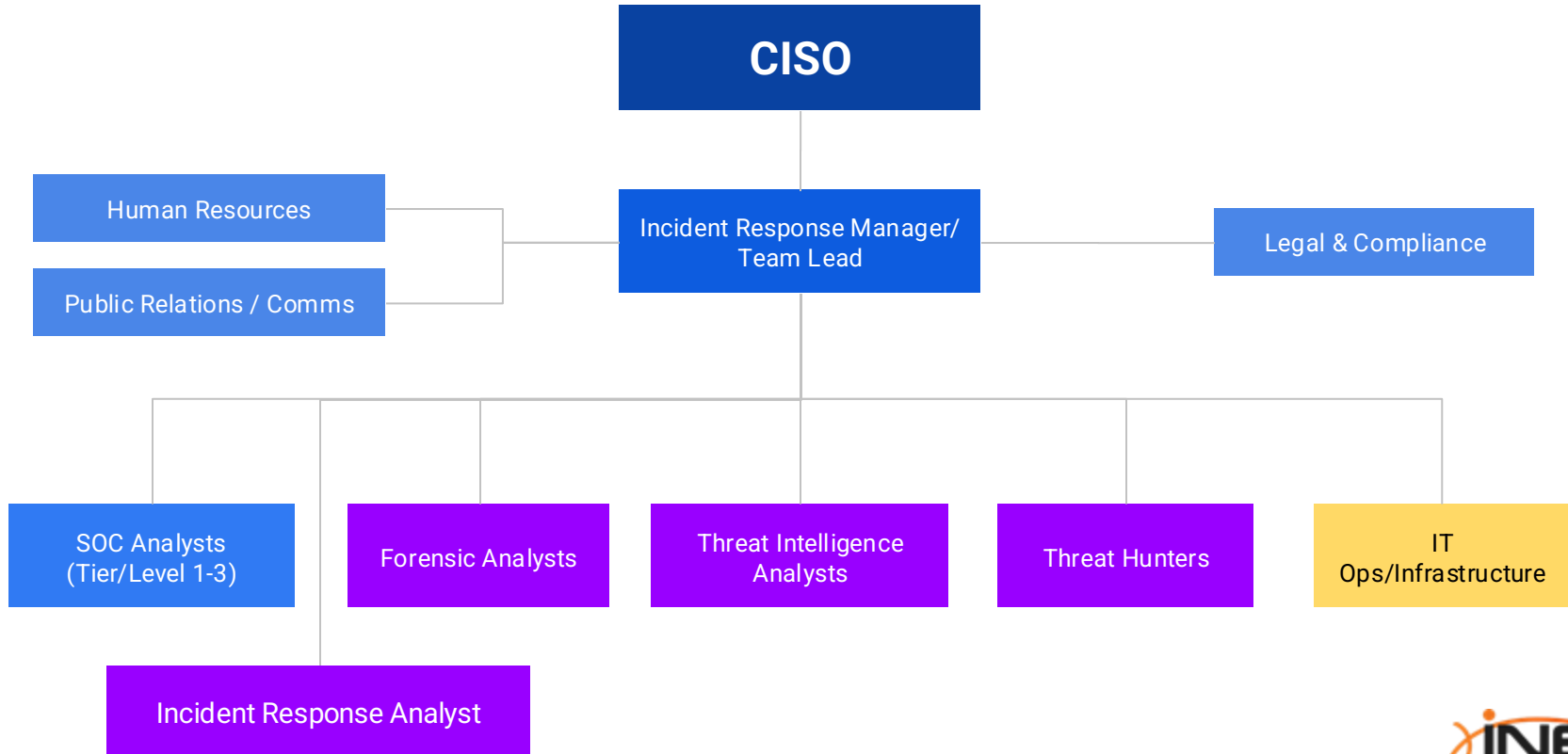


# IR Teams: Roles & Responsibilities

Each role carries unique responsibilities, and together, they form a cohesive response unit capable of handling complex and high-pressure security events.

Understanding these roles is essential for any incident responder. It not only clarifies the scope of one's own responsibilities but also enhances coordination, improves communication during incidents, and ensures that all aspects of the response; technical, legal, and operational are addressed in a timely and effective manner.

# IR Teams: Roles & Responsibilities



# Incident Response Manager / IR Lead

*Leads and coordinates all phases of the incident response process*

## Key Responsibilities:

- + Oversees incident response planning and execution
- + Assigns roles and responsibilities during an incident
- + Ensures response procedures are followed
- + Acts as the main point of contact during major incidents
- + Coordinates post-incident reviews and continuous improvement

# SOC Analysts (Level/Tier 1-3)

*Monitor, detect, escalate, and help investigate potential security incidents*

## Key Responsibilities:

- + Monitor logs, SIEM alerts, and threat intel feeds
- + Triage and validate security events
- + Escalate confirmed incidents to IR Manager
- + Collect initial evidence and context
- + Recommend containment steps

L1/T1 Analysts: Basic triage and alert validation

L2/T2 Analysts: Deeper investigation and correlation

L3/T3 Analysts: Advanced forensics, threat hunting, and containment guidance



# SOC Analysts (Level/Tier 1-3)

*Monitor, detect, escalate, and help investigate potential security incidents*

SOC Tier	Primary Role in Incident Response
Tier 1 (T1)	Monitors alerts, performs initial triage, and escalates potential incidents. They do not typically lead the response.
Tier 2 (T2)	Acts as the Incident Responder. Investigates escalated alerts, confirms incidents, performs deeper analysis, and begins response actions such as containment.
Tier 3 (T3)	Provides expert-level support, performs advanced forensics, threat hunting, and guides complex response efforts. May lead incident response for high-severity cases.

# Forensic Analyst

*Performs in-depth analysis of compromised systems and digital artifacts*

## Key Responsibilities:

- + Acquire and preserve digital evidence
- + Conduct disk, memory, and file system forensics
- + Analyze malware and attack patterns
- + Reconstruct attacker actions and timelines
- + Support legal/regulatory requirements with proper chain of custody



# Threat Intelligence Analyst

*Provides context and threat data to inform detection, response, and decision-making*

## Key Responsibilities:

- + Collect and analyze threat intelligence (IOCs, TTPs, actors)
- + Correlate intel with current incidents
- + Identify related campaigns or threat actors
- + Recommend defensive actions based on emerging threats

# IT Operations / Infrastructure Team

*Supports containment, eradication, and recovery efforts from a systems and network perspective*

## Key Responsibilities:

- + Isolate affected systems or networks
- + Apply patches and configuration changes
- + Restore systems from backups
- + Rebuild compromised servers or endpoints
- + Implement firewall and network segmentation

# Legal / Compliance

*Provides advice on legal obligations and regulatory implications of incidents*

## Key Responsibilities:

- + Determine breach notification requirements
- + Support evidence handling and incident documentation
- + Coordinate with law enforcement if necessary
- + Ensure regulatory compliance (e.g., GDPR, HIPAA, PCI-DSS)

# Comms / Public Relations

*Manages internal and external communications during and after an incident*

## Key Responsibilities:

- + Develop communication plans and press releases
- + Inform internal stakeholders, customers, and partners
- + Coordinate messaging with legal and executive leadership
- + Help protect brand and public trust during a crisis

# Human Resources (HR)

*Engaged in incidents involving employees (e.g., insider threats, policy violations)*

## Key Responsibilities:

- + Investigate employee involvement
- + Support disciplinary actions or internal investigations
- + Communicate outcomes to staff, if appropriate

# Executive Leadership / CISO

*Provides high-level oversight and strategic decision-making*

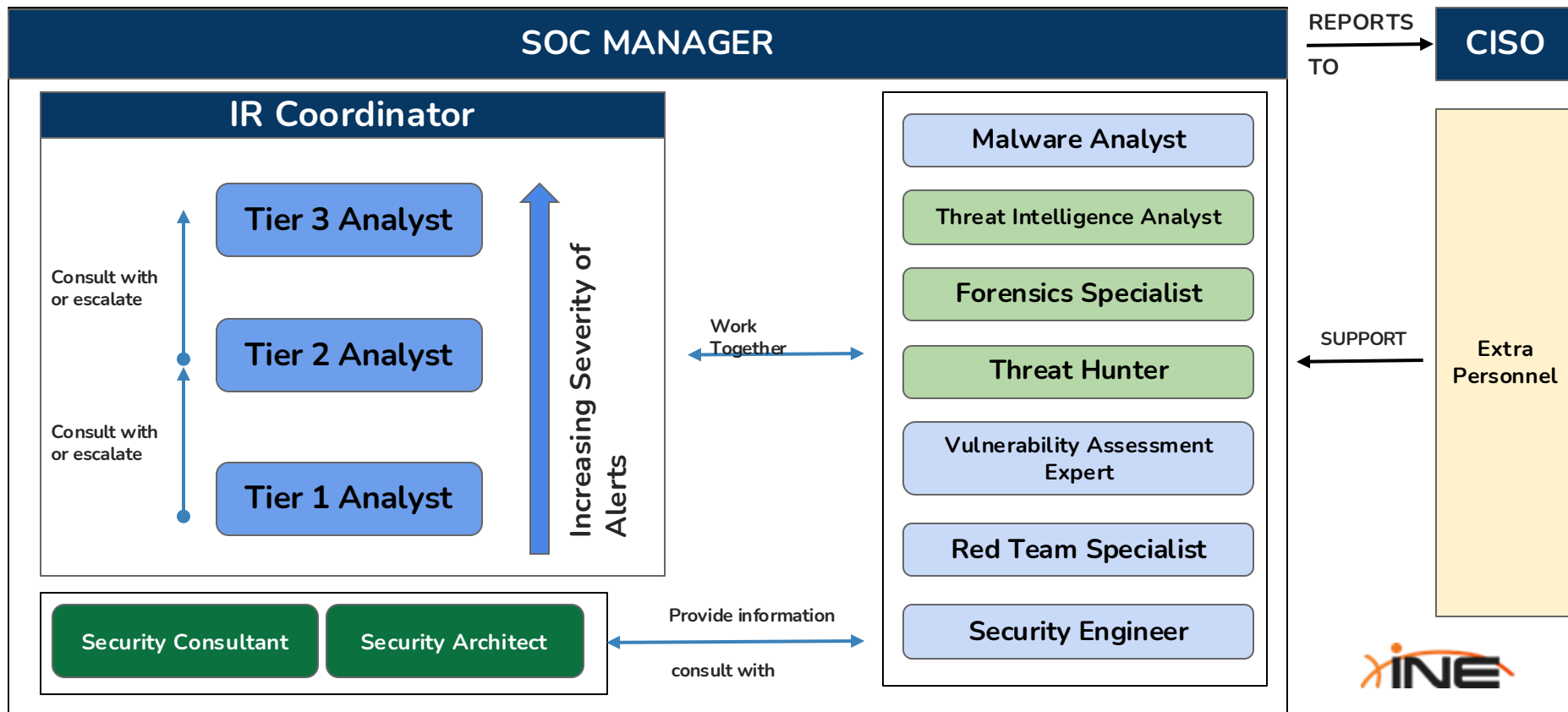
## Key Responsibilities:

- + Approves major containment or shutdown actions
- + Ensures business alignment and continuity
- + Communicates with board members or investors
- + Supports long-term improvements and resource allocation

# Summary Table

ROLE	FOCUS AREA	KEY RESPONSIBILITY
IR Manager	<i>Coordination</i>	Lead IR process & manage team
SOC Analysts	<i>Monitoring &amp; Triage</i>	Detect and escalate threats
Forensic Analyst	<i>Investigation</i>	Analyze systems and evidence
Threat Intel Analyst	<i>Context &amp; Attribution</i>	Enrich investigations with intel
IT Operations	<i>Containment &amp; Recovery</i>	Isolate and restore systems
Legal	<i>Compliance</i>	Advise on legal requirements
PR/Communications	<i>Messaging</i>	Manage internal/external communication
HR	<i>Insider Threats</i>	Address employee-related incidents
CISO / Execs	<i>Oversight</i>	Approve actions and allocate resources

# Interaction of roles within a SOC





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 scene is dimly lit, with the primary light source being the screen. An orange vertical bar is on the left side of the image.

# NIST Incident Response Process

# The Incident Response Process

**Incident Response (IR)** is a *structured* and *systematic* approach to *detecting*, *investigating*, *containing*, *eradicating*, and *recovering* from cybersecurity incidents such as malware infections, data breaches, ransomware attacks, and unauthorized access.

The goal of IR is to:

- + Minimize damage and disruption
- + Restore normal operations as quickly as possible
- + Reduce the risk of future incidents
- + Comply with legal and regulatory requirements

*It's not just about reacting — it's about responding effectively, efficiently, and with purpose.*



# The Importance of a Standardized Framework

*A framework transforms incident response from ad hoc firefighting into a disciplined, professional practice*

**Incident Response is a high-stakes, time-sensitive activity.**

Without a structured and repeatable process, organizations are likely to respond inconsistently, which consequently results in:

- + Delayed containment and recovery
- + Increased damage and downtime
- + Poor communication and role confusion
- + Missed compliance and reporting requirements
- + Failure to learn from past incidents

# The NIST Incident Response Framework

**NIST SP 800-61** is the most widely adopted and recommended framework globally.

It provides a solid foundation for developing, operating, and maturing an IR capability and is compatible with most other standards and tools.

*While several frameworks exist, NIST's IR framework is the global standard due to its clarity, flexibility, and comprehensive approach.*

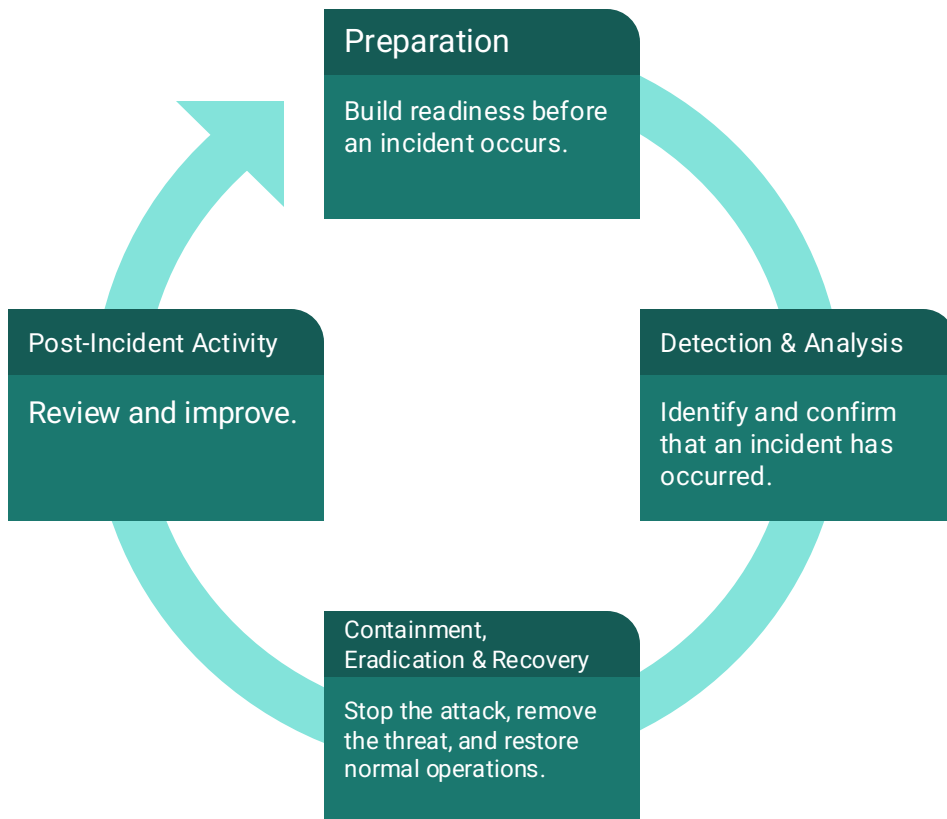


# The NIST Incident Response Framework

The **NIST Special Publication 800-61r2** outlines a standardized incident response lifecycle that organizations should follow to effectively prepare for, detect, respond to, and recover from cybersecurity incidents.

1. Preparation
2. Detection & Analysis
3. Containment, Eradication & Recovery
4. Post-Incident Activity (Lessons Learned)

# The NIST Incident Response Process Lifecycle



# Preparation

*Build readiness before an incident occurs*

**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

*Identify and confirm that an incident has occurred*

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

*Stop the attack, remove the threat, and restore normal operations*

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)

*Learn from the incident to enhance defenses and refine the IR process*

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.



# SANS Incident Response Process

# SANS Incident Response Process

The SANS Institute, through its Incident Handler's Handbook, outlines a six-phase incident response lifecycle that is widely used by security professionals, especially in operational environments and IR training.

This process emphasizes a hands-on, tactical approach to incident handling — breaking down each step from preparation to lessons learned.

Its clarity and simplicity make it a favorite among IR practitioners, especially those working in SOCs, MSSPs, and operational response teams.

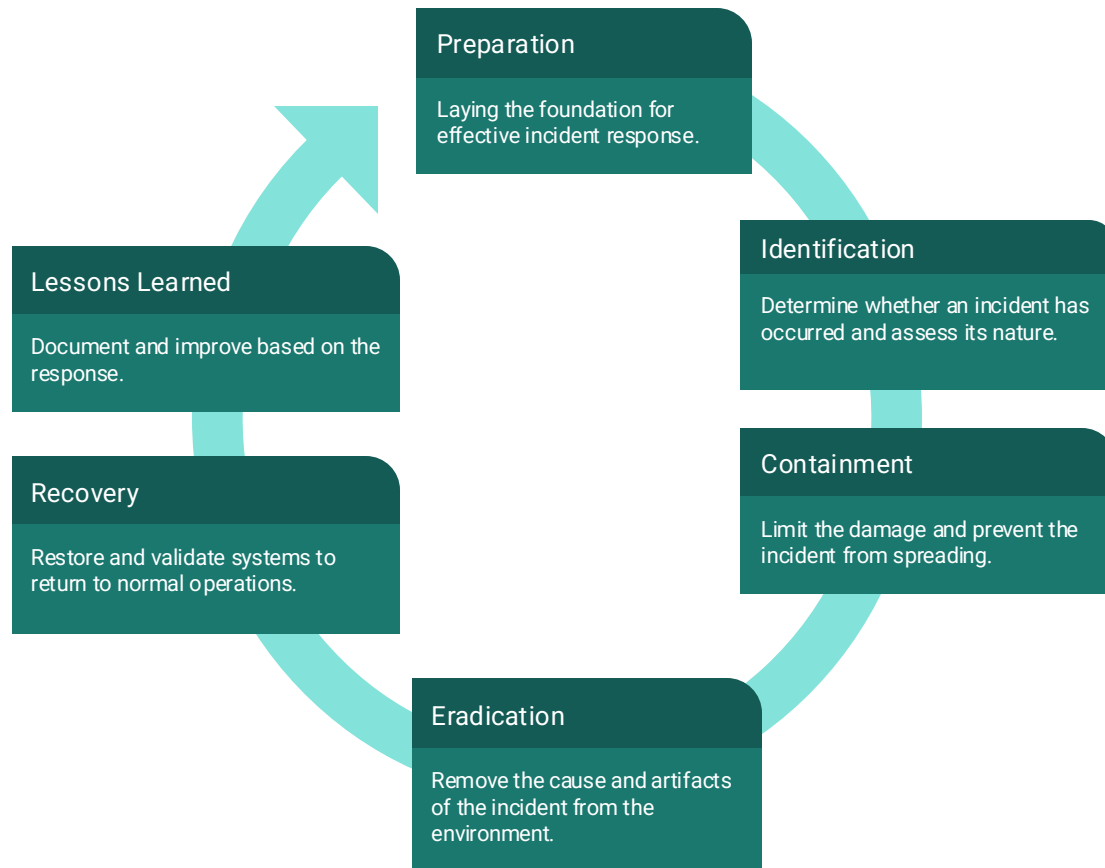


# SANS Incident Response Process

The **SANS Incident Response process**, outlines a clear, **six-phase** lifecycle designed to help organizations effectively detect, respond to, and recover from security incidents.

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

# The SANS Incident Response Cycle



# Preparation

*Laying the foundation for effective incident response*

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

## **Key Activities:**

- + Develop IR policies, plans, and playbooks
- + Define team roles, responsibilities, and communication paths
- + Set up logging, monitoring, and alerting systems
- + Train staff and run tabletop exercises
- + Establish secure configurations, asset inventories, and backups

# Identification

*Determine whether an incident has occurred and assess its nature*

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

## Key Activities:

- + Monitor security tools (SIEM, EDR, IDS, logs) for suspicious activity
- + Validate alerts and classify potential incidents
- + Determine the scope, severity, and impact of the incident
- + Record evidence and assign incident severity levels
- + Decide whether to escalate or initiate full response



# Containment

*Limit the damage and prevent the incident from spreading*

## Key Activities:

- + Isolate affected systems (e.g., network segmentation, disconnecting devices)
- + Apply short-term containment measures to stop further attacker activity
- + Consider long-term containment steps for continued business operations
- + Preserve volatile data for later analysis

# Eradication

*Remove the cause and artifacts of the incident from the environment*

## Key Activities:

- + Identify the root cause (e.g., malware, vulnerable software, stolen credentials)
- + Remove malicious files, backdoors, and persistence mechanisms
- + Patch systems or change passwords
- + Re-image compromised systems if needed

# Recovery

*Restore and validate systems to return to normal operations*

## Key Activities:

- + Restore systems from clean backups
- + Monitor systems to confirm they are functioning properly and free of threats
- + Reintroduce affected systems to the network in a controlled manner
- + Verify system integrity and user access controls

# Post-Incident Activity (Lessons Learned)

*Learn from the incident to enhance defenses and refine the IR process*

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

## Key Activities:

- + Conduct a post-incident review or debrief
- + Document the timeline, actions taken, and outcomes
- + Identify what worked and where improvements are needed
- + Update IR plans, policies, and detection tools
- + Share findings with stakeholders and relevant teams

# SANS vs. NIST IR Frameworks

Phase	SANS IR Process	NIST SP 800-61	Comparison
1	Preparation	Preparation	Both begin with readiness planning, tools, and training
2	Identification	Detection and Analysis	SANS separates detection into its own phase; NIST combines detection and analysis
3	Containment	Containment, Eradication, and Recovery	SANS breaks these into 3 distinct phases for clarity; NIST groups them for flexibility
4	Eradication		Same goal: remove root cause and attacker artifacts
5	Recovery		Restore and validate systems
6	Lessons Learned	Post-Incident Activity	Both conclude with review, documentation, and improvement

# SANS vs. NIST IR Frameworks

SANS IR Process offers a more granular, operational breakdown, ideal for hands-on incident response teams.

NIST IR Framework is more formal and flexible, aligning with policy, compliance, and enterprise-level governance.

***Both are widely accepted and compatible. Many organizations use SANS for execution and NIST for structure and policy alignment.***

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 tech-oriented.

# The IR Responsibility Matrix

# Why Roles & Responsibilities Matter

When responding to security incidents, **time** is critical, and so is **clarity of responsibility**. Without clearly defined roles and responsibilities, even a well-prepared organization can suffer from delays, confusion, and poor coordination during a response.

Defining who is **responsible**, who is **accountable**, and **who needs to be consulted** or **informed** ensures that every action is deliberate, timely, and effective. This, in turn, reduces overlap, eliminates gaps, and enables teams to work together efficiently under pressure.

In the next set of slides, we'll explore how clearly assigning responsibilities using frameworks like **RACI** can enhance communication, streamline decision-making, and ultimately lead to a faster, more efficient incident response.





# The RACI Responsibility Matrix

**RACI** is a widely used ***responsibility assignment matrix*** that helps organizations clearly define who is involved in what when it comes to completing tasks, making decisions, or executing processes — such as those involved in the **Incident Response (IR) process**.

Letter	Definition
<b>R - Responsible</b>	The person or role <b><i>who performs the work</i></b> . There can be multiple people responsible for executing the task.
<b>A - Accountable</b>	The person who is <b><i>ultimately answerable</i></b> for the task being completed correctly and thoroughly. Only one person should be accountable for each task.
<b>C - Consulted</b>	Individuals who <b><i>provide input, guidance, or expertise during the task</i></b> . This involves two-way communication.
<b>I - Informed</b>	Individuals who are <b><i>kept updated on progress or outcomes</i></b> . They are not directly involved but need to know. This is one-way communication.

# Benefits Of Using RACI

- + Eliminates ambiguity about who is doing what.
- + Improves accountability across cross-functional teams.
- + Ensures nothing falls through the cracks during time-sensitive operations.
- + Simplifies/streamlines communication during complex or high-stress incidents.
- + Aligns everyone involved in the IR process; technical, legal, PR, and leadership.

# Why a RACI Matrix is Important in IR

**Incident Response (IR)** is often complex, fast-paced, and involves multiple teams, from SOC analysts and IT staff to legal, PR, and executive leadership.

*Without clearly defined roles, confusion and delays* can occur at the worst possible time.

*That's where a RACI matrix becomes invaluable.*

A **RACI matrix** brings structure, clarity, and accountability to incident response. It ensures the right people are involved at the right time, reduces confusion, improves response speed, and helps organizations learn and improve after an incident.



# 1 - Clarifying Roles and Responsibilities

*Everyone knows what they're expected to do*

A **RACI matrix** removes ambiguity by clearly identifying:

- + Who is doing the work (**Responsible**)
- + Who is ultimately in charge (**Accountable**)
- + Who should be consulted for advice or approval (**Consulted**)
- + Who needs to be informed of progress or outcomes (**Informed**)

*This ensures tasks don't fall through the cracks or get duplicated.*

# 2 - Improve Coordination Across Teams

*Streamlines collaboration across technical and non-technical functions*

**Incident response** often involves cross-functional teams:

- + SOC or IR team (technical response)
- + IT operations (containment & recovery)
- + Legal (compliance, breach notification)
- + PR (public communication)
- + HR (insider threats)
- + Executives (approval, oversight)

*RACI helps ensure everyone knows when and how to engage.*



# 3 - Speeds Up Decision-Making

*Removes delays caused by unclear ownership*

When dealing with high-pressure incidents, *time is of the essence*.

The **RACI matrix** identifies who is authorized to make key decisions (Accountable) so teams aren't waiting on unnecessary approvals or second-guessing their actions.

# 4 - Supports Regulatory Compliance

*Ensures the right people are involved in breach handling and reporting*

For compliance with regulations like **GDPR**, **HIPAA**, or **PCI-DSS**, it's essential to involve the correct stakeholders at the right time.

RACI ensures:

- + Legal teams are consulted when needed
- + Reporting obligations are not missed
- + Incident documentation is thorough and complete

# Example: IR RACI Matrix

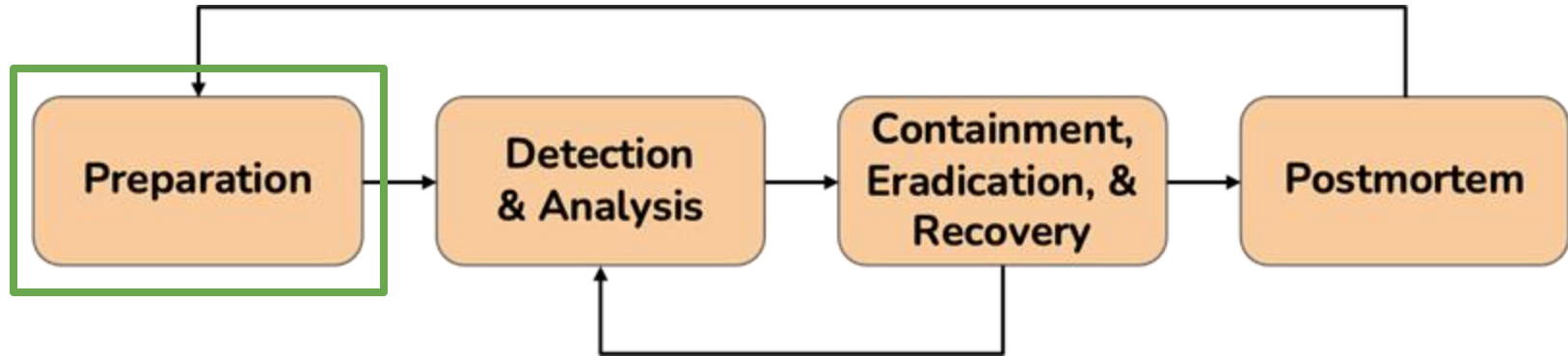
RACI Matrix					
Incident Response Role	Phase				
	Preparation	Identification	Containment	Eradication	Recovery
Incident Response Manager	A	A	A	A	A
SOC Analyst	R	R	R	R	R
Incident Responder	C	C	R	R	R
IT Specialist	R	R	R	R	R
Management	I	I	I	I	I
Legal	I	I	C	C	C





# Preparing for Cybersecurity Incidents

# The Preparation Phase



# The Preparation Phase

The **Preparation Phase** is the **first** and **foundational** phase of the Incident Response (IR) process and lifecycle.

It involves establishing and developing the capabilities, policies, tools, people, and processes that an organization needs before an incident occurs — ***In preparation for an Incident.***

The goal of this phase is to ensure that ***an organization is equipped*** and ***ready to handle*** a potential security incident effectively, minimizing damage and ensuring a coordinated, timely response.

***This phase of the IR process is not reactive, it is proactive.***



# The Preparation Phase

The Preparation phase typically encompasses the following activities:

- + Establishing and training the incident response team (IRT).
  - + Ensuring all responders understand their roles, responsibilities, and escalation paths.
- + Developing incident response plans, policies and playbooks.
- + Deployment and configuration of monitoring and detection systems.
- + Deployment of tools, security controls, countermeasures, etc
  - + Based on needs of org and risk analysis/assessments
- + User awareness training and skills development.
  - + Running tabletop exercises and simulations.

# The Importance of Good Preparation

Without proper preparation, even the most skilled response team can be *crippled by confusion, delays*, and *poor coordination* when an incident occurs.

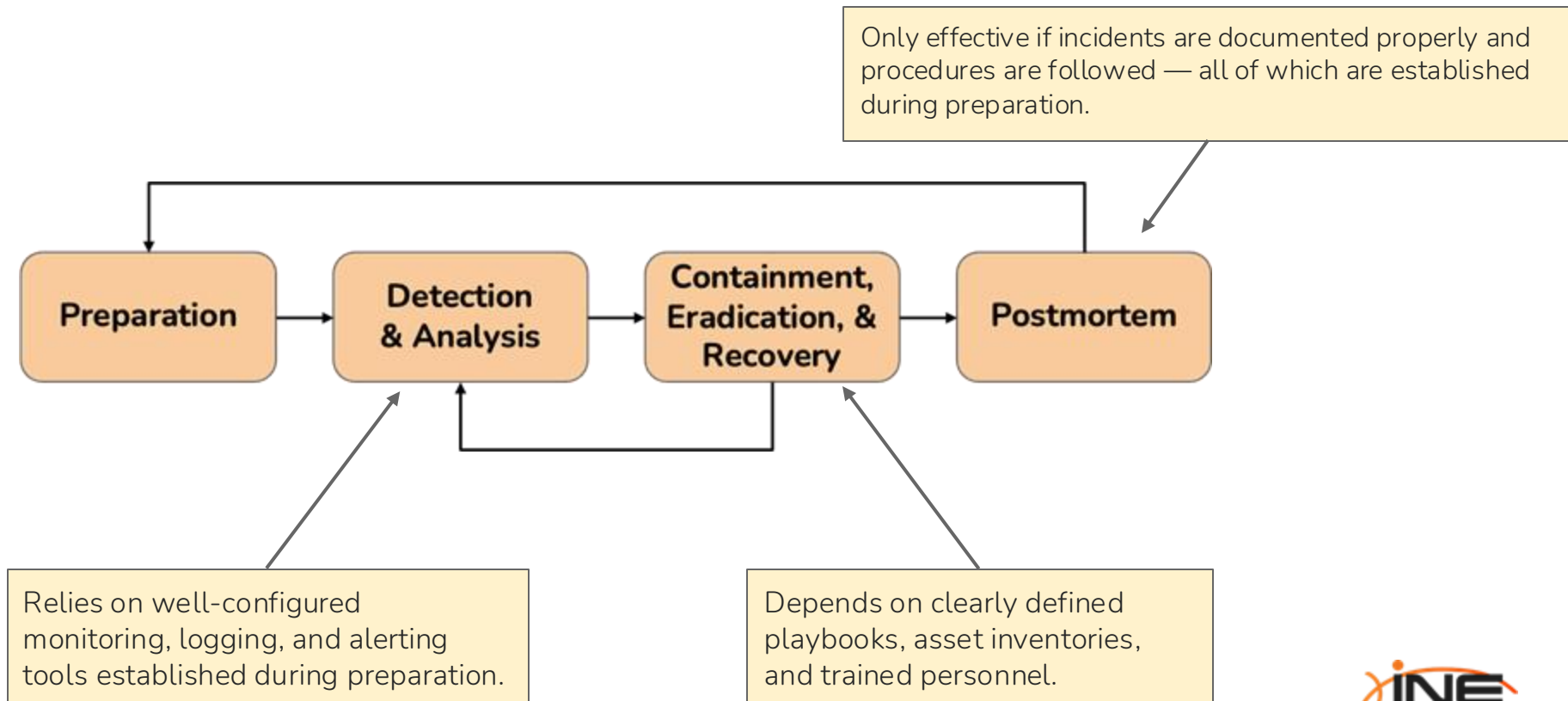
## Well Prepared Organizations

- Detect incidents faster
- Respond more efficiently
- Minimize the impact on business operations
- Meet legal and regulatory obligations
- Improve recovery times
- Learn and adapt through documentation and review

## Unprepared Organizations

- Disorganized responses
- Communication breakdowns
- Missed reporting deadlines
- Greater financial and reputational damage

# How Preparation Affects Other Phases





# **People, Processes & Technology**

# People, Processes & Technology

To better understand the components of the Preparation Phase, we can apply the ***People, Processes, and Technology*** framework.

This approach helps break down the complexity of **preparation** into ***manageable*** and ***interrelated categories***.

By organizing preparation activities into these three domains, we create a structured view of what needs to be in place; from trained personnel and defined workflows to properly configured tools and systems.

***This categorization not only enhances clarity and alignment across teams, but also ensures that the preparation phase is comprehensive, well-organized, and actionable.***





# People, Processes & Technology

This triad reflects the core components that must be in place before an incident ever occurs:

Component	Explanation
<b>People</b>	Represents the trained individuals (IR Team) who will detect, assess, and respond when threats arise.
<b>Processes</b>	Ensure there is a well-defined, repeatable structure for how incidents are handled.
<b>Technology</b>	Provides the tools and systems necessary to monitor, detect, investigate, and respond to threats.

# 1 - People

## *Building the Human Element of Readiness*

The foundation of any successful incident response capability begins with the right people in the right roles, properly trained and prepared to respond under pressure.

### Key Focus Areas:

- + Incident Response Team (IRT): Define team structure, roles, and escalation paths
- + Role Clarity: Use frameworks like RACI to define who is responsible, accountable, consulted, and informed
- + Training & Drills: Conduct tabletop exercises, red/blue team simulations, and hands-on tool training
- + Awareness: Ensure all staff (not just security) know how to report suspicious activity and follow response protocols

# 2 - Processes

## *Establishing Playbooks, Policies & Communication Paths*

Processes provide the structure and repeatability required for a consistent and coordinated response. ***The preparation phase defines and documents these processes.***

Key Focus Areas:

- + IR Policy & Plan: Formal documents outlining how the organization detects, reports, escalates, and responds to incidents
- + Incident Classification & Severity: Define how incidents are categorized and prioritized
- + Playbooks & Runbooks: Predefined workflows for specific incident types (e.g., ransomware, insider threat)
- + Communication Protocols: Internal war room channels, external disclosure pathways, legal/regulatory reporting timelines
- + Post-Incident Review Process: Define how lessons learned are captured and used to improve

# 3 - Technology

## *Detection, Analysis & Response Capabilities*

Technology empowers the team to ***monitor, detect, investigate, and respond*** — but it must be properly deployed, configured, and accessible before the incident.

### Key Focus Areas:

- + Monitoring & Detection Tools: SIEM, EDR, IDS/IPS, log aggregation
- + Forensics & Triage Tools: Memory analysis, disk imaging, network capture tools
- + Access Management: Ensure IR team has the necessary permissions to act without delay
- + IR Toolkit: Curated collection of tools for investigation, containment, and recovery
- + Asset Inventory & Network Visibility: Knowing what systems exist and what “normal” looks like

# People, Processes & Technology



## People

Ensure every team member knows what to do before an incident occurs, and is confident in doing it.

*Do we have the right team and skills?*



## Processes

Create a reliable framework that guides action during chaos — reducing delays, missteps, and uncertainty.

*Do we have the right plans and workflows?*



## Technology

Ensure that responders are equipped with the tools and access they need and that those tools are tested, documented, and ready to use.

*Do we have the right tools and access?*



# The Incident Response Hierarchy of Needs

# The Incident Response Hierarchy of Needs

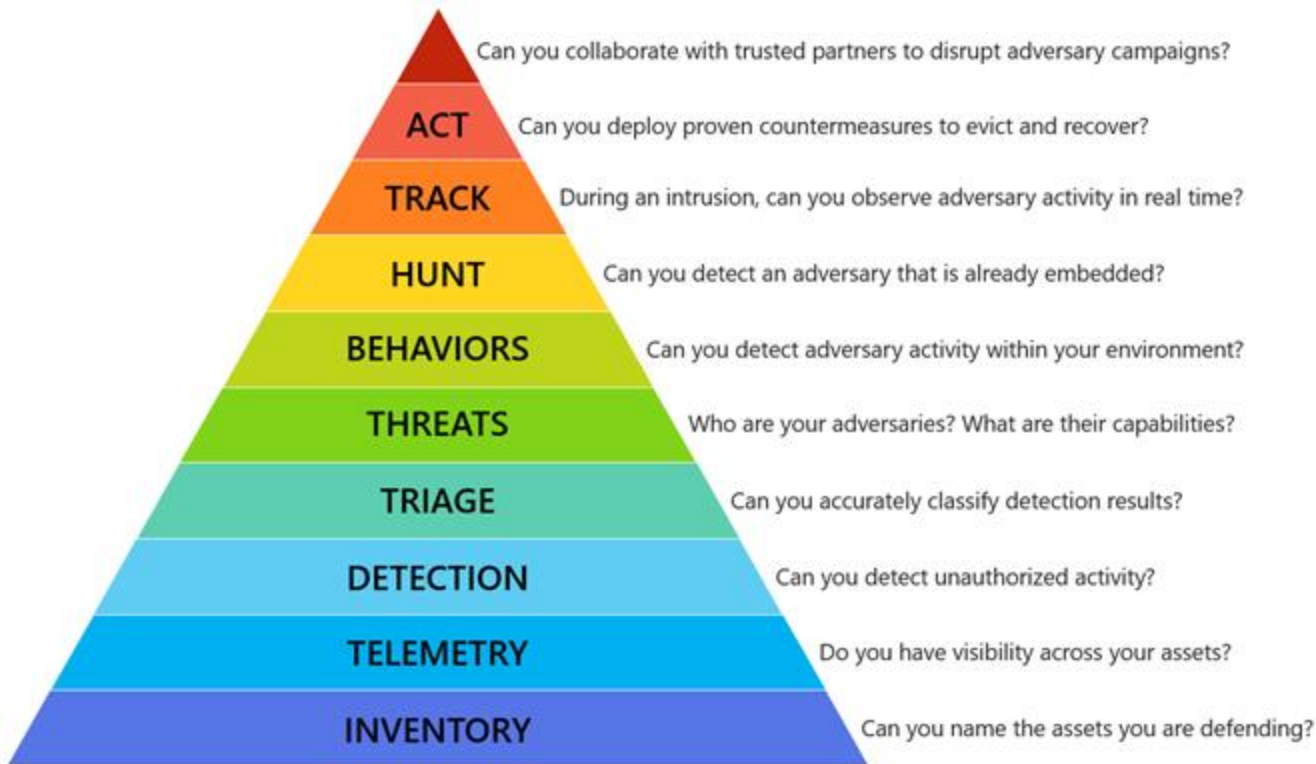
The **Incident Response Hierarchy of Needs**, is a conceptual model created by **Matt Swannman**. It is used to describe the **layers (levels) of readiness** that must be established for an organization to effectively respond to security incidents.

This model offers a structured approach to building an effective incident response program, with a clear emphasis on the layers that must be established before advanced functions like SOC or threat hunting can thrive.

**The pyramid consists of 10 layers**, each having been built on the one below it. Coupled with this pyramid is Swannman's Plateaus Model, which tracks an organization's progression through different levels of maturity in its security operations.



# The Incident Response Hierarchy of Needs





# The Incident Response Hierarchy of Needs

**Swannman's Pyramid** is a visual framework designed to help organizations understand *how to progressively enhance their security posture*.

Each layer of the pyramid represents a level of capability, starting with *foundational needs at the base* and advancing toward more *sophisticated, proactive strategies at the top*.

Threat hunting sits near the top of the pyramid, highlighting that it is a highly specialized activity that relies on the presence of strong foundational elements such as tools, visibility, and well-defined processes, which is established in the lower layers.

# The Incident Response Hierarchy of Needs

#	Layer	Description
1	<b>Asset Inventory</b>	The base of the pyramid is an accurate inventory of assets. Organizations must first identify and classify their assets, including hardware, software, and sensitive data. Understanding what needs protection is critical before any detection or response strategies can be implemented.
2	<b>Telemetry</b>	Telemetry encompasses the collection of system, network, and endpoint data that is essential for security monitoring. This layer ensures that organizations have the necessary data to identify potential threats and observe normal and abnormal activities.
3	<b>Detection</b>	Detection focuses on the tools and mechanisms used to identify threats. This could include intrusion detection systems (IDS), SIEM solutions, and other automated detection tools that generate alerts for suspicious activity. This layer is vital for providing visibility into potential security incidents.
4	<b>Triage</b>	Triage involves the process of analyzing and prioritizing detected incidents to determine their severity and potential impact. Security teams assess the alerts and focus on the most critical incidents that need immediate attention. Efficient triage is crucial for avoiding alert fatigue and ensuring a quick response to genuine threats.

# The Incident Response Hierarchy of Needs

#	Layer	Description
5	<b>Threats</b>	At this stage, organizations actively monitor for specific threat actors, tactics, techniques, and procedures (TTPs). This layer uses threat intelligence to identify known and emerging threats, enabling security teams to stay ahead of adversaries.
6	<b>Behaviors</b>	The “Behaviors” layer involves analyzing anomalous or suspicious behaviors that could indicate a security incident. Rather than relying solely on signature-based detection, organizations focus on identifying abnormal activity patterns and deviations from normal behavior.
7	<b>Hunt</b>	Threat hunting is a proactive approach to cybersecurity, where security teams actively search for hidden threats across networks, endpoints, and data sources. Rather than waiting for alerts to be triggered, threat hunters dig deeper into the data to uncover signs of compromise that may have evaded traditional detection systems.
8	<b>Track</b>	Tracking involves continuously monitoring and following the actions of adversaries once they have been identified. Organizations maintain visibility over the threat’s movement and evolution, providing the context needed to anticipate the adversary’s next steps.

# The Incident Response Hierarchy of Needs

#	Layer	Description
9	<b>Act</b>	The “Act” layer involves taking appropriate actions in response to identified threats. This could include containment, remediation, and recovery efforts. At this stage, security teams take decisive steps to neutralize the threat and prevent further damage.
10	<b>Collaboration</b>	The final layer emphasizes the importance of collaboration with trusted partners, such as industry peers, government agencies, and threat intelligence groups. By working together, organizations can share valuable insights and intelligence to disrupt adversary campaigns and improve defenses on a broader scale.

# Resources & References

- + Incident Response Hierarchy of Needs:  
<https://github.com/swannman/ircapabilities>
- + Hierarchy of Needs – Predefender:  
<https://huntbook.predefender.com/part-1/introduction/hierarchy-of-needs/index.html>



# Incident Response Policy

# IR Processes

In the context of the **Preparation Phase**, *processes* refer to the ***formalized, documented, and repeatable procedures*** that guide how an organization will detect, respond to, and recover from security incidents.

***These processes*** serve as ***the backbone of the IR function***, ensuring that response efforts are not improvised, but ***structured, coordinated, and aligned*** with business goals and regulatory requirements.

# Key Components of IR Processes in the Preparation Phase

1. Incident Response Policy
2. Incident Response Plan (IRP)
3. Playbooks and Runbooks
4. Incident Classification and Severity models/frameworks
5. Escalation and Notification procedures
6. Post-Incident Review Procedures



# Key Components of IR Processes in the Preparation Phase

*In the Preparation Phase, processes are the documented structures that guide how people operate and how technology is used.*

*They ensure that the organization isn't just capable of responding, but prepared to respond in a coordinated, repeatable, and effective way.*

# Incident Response Policy

An **Incident Response Policy** is a foundational document that outlines an organization's **strategy** and **procedures** for **detecting**, **responding** to, and **recovering** from cybersecurity incidents.

*It serves as a blueprint for managing incidents effectively, ensuring that all stakeholders understand their roles and responsibilities.*

# Key Components of an Incident Response Policy

1. Purpose and Scope
  - + Defines the objectives of the policy and the systems, data, and personnel it covers.
1. Definitions
  - + Clarifies terminology such as "security incident," "breach," and "vulnerability" to ensure a common understanding.
1. Roles and Responsibilities
  - + Identifies the incident response team members and their specific duties during an incident.
1. Incident Classification
  - + Establishes criteria for categorizing incidents based on severity and impact.

# Key Components of an Incident Response Policy

## 5. Communication Plan

- + Details internal and external communication protocols, including notification requirements to stakeholders and authorities.

## 5. Training and Awareness

- + Emphasizes the importance of regular training and awareness programs to prepare staff for potential incidents.

## 5. Review, Revisions and Updates

- + Specifies the frequency and process for reviewing and updating the policy to adapt to evolving threats and organizational changes.

# Incident Response Policy Templates

- + **FRSecure** Incident Response Policy Template: Provides a comprehensive framework, including roles, responsibilities, and response procedures.
  - + Access it here: [FRSecure Incident Response Policy Template](#)
- + **PurpleSec** Incident Response Policy Template: Offers a detailed policy structure with definitions, scope, and incident handling procedures.
  - + Available at: [PurpleSec Incident Response Policy Template](#)
- + **Center for Internet Security (CIS)** Incident Response Policy Template: Aligns with CIS Controls and provides guidance on developing an effective incident response policy.
  - + Download from: [CIS Incident Response Policy Template](#)
- + **iCIMS** Incident Response Policy & Procedures:
  - + [https://www.icims.com/wp-content/uploads/2020/09/Incident\\_Response\\_Policy\\_and\\_Procedures\\_2020.pdf](https://www.icims.com/wp-content/uploads/2020/09/Incident_Response_Policy_and_Procedures_2020.pdf)



# Example: Incident Response Policies



# Incident Response Plans (IRPs)

# Key Components of IR Processes in the Preparation Phase

1. Incident Response Policy
2. Incident Response Plan (IRP)
3. Playbooks and Runbooks
4. Incident Classification and Severity models/frameworks
5. Escalation and Notification procedures
6. Post-Incident Review Procedures



# Incident Response Plans

When a cybersecurity incident occurs, many organizations, particularly small and medium-sized businesses are often unprepared to respond effectively.

***Developing formal Incident Response Plans (IRPs)*** and playbooks is critical, as they define **how** an organization will detect, respond to, and recover from security breaches.

***Effective incident response goes beyond simply acquiring tools or following generic IR guidelines.***

It requires building from a well-defined baseline that reflects the organization's current security maturity, while ensuring that the IR program is aligned with the business's goals, requirements, and risk tolerance.



# Incident Response Plans

An **Incident Response Plan (IRP)** is a structured document that outlines the **procedures** an organization follows to **detect, respond** to, and **recover** from cybersecurity incidents.

The IRP generally defines a route to follow when a security incident occurs. This plan must be consistent with existing organizational capacity, resources, and infrastructure.

*It serves as a roadmap for managing incidents effectively, minimizing damage, and restoring normal operations promptly.*



# Key Components of an Incident Response Plan

## 1. Introduction

- + Purpose of the plan: Why the plan exists and what it aims to achieve.
- + Scope: Defines what systems, data, departments and types of incidents the plan applies to.
- + Assumptions: Any prerequisites or assumed conditions (Logging and monitoring is already established, IR team is already in place etc)
- + References: Links to related policies, standards and external regulations (IR Policy, GDPR requirements etc.

# Key Components of an Incident Response Plan

## 2. Roles and Responsibilities

- + IR Team Structure: Identification of core IR team members and their roles.
- + Specific/Specialist Roles: Roles like IR manager, SOC Analysis, Forensic Analyst, Legal, Communications/PR etc.
- + Escalation Contacts: Who must be notified at different incident severity levels (including executive leadership).

# Key Components of an Incident Response Plan

## 3. Incident Classification and Severity Levels

- + Incident Categories: Define types of incidents (e.g. Malware infections, Insider threats etc.)
- + Severity Levels: Severity Scale (Low, Medium, High, Critical) based on impact, urgency and scope.
- + Criteria for Classification: How to categorize incidents based on initial evidence/markers.

# Key Components of an Incident Response Plan

## 4. IR Process & Procedures - *Typically based on the NIST or SANS IR frameworks.*

- + Preparation: Review of tools, training, access, and IR readiness requirements.
- + Detection and Analysis:
  - i. How to detect potential incidents (SIEM alerts etc.)
  - ii. Triage process, initial evidence gathering, event correlation.
  - iii. Initial incident logging and ticket creation.
- + Containment:
  - i. Short-term and long-term containment strategies.
  - ii. Criteria for isolating systems or restricting access.

# Key Components of an Incident Response Plan

## 4. IR Process & Procedures - *Typically based on the NIST or SANS IR frameworks.*

- + Eradication:
  - i. Removing the threat (e.g., malware removal, patching vulnerabilities).
  - ii. Verification steps post-eradication.
- + Recovery:
  - i. Restoring systems and validating security post-incident.
- + Post-Incident Activity:
  - i. Conducting a post-incident review (PIR).
  - ii. Capturing lessons learned and updating the IRP or security controls.

# Key Components of an Incident Response Plan

## 5. Communication and Reporting

- + Internal Communication Procedures:
  - i. Who needs to know and when (within technical teams, leadership).
- + External Communication Procedures:
  - i. Regulatory authorities, law enforcement, clients, partners.
- + Public Relations/Disclosure Procedures:
  - i. Press releases, breach notification obligations, media handling.



# Key Components of an Incident Response Plan

## 6. Documentation and Evidence Handling

- + Evidence Handling Protocols:
  - i. Chain of custody procedures, forensic imaging etc.
- + Incident Tracking and Ticketing:
  - i. Systems or methods used to log, track, and close incidents.
- + Retention Requirements:
  - i. How long incident records are kept (often driven by legal/regulatory mandates).

# Key Components of an Incident Response Plan

## 7. Plan Testing and Review

- + Tabletop Exercises (TTX) and Simulations:
  - i. Schedule and structure for regular IR testing.
- + Plan Review Cycle:
  - i. Frequency of reviews (e.g., annually, post-major incidents).

## 8. Appendices

- + Contact Lists: IR team, escalation paths, external support (ISPs, forensics firms, vendors).
- + Glossary: Definitions of technical or legal terms used in the plan.
- + Templates and Forms: Incident reporting forms, checklists, notification templates.

# Summary

- + An **Incident Response Policy** is a high-level, formal document that establishes an organization's intent and commitment to managing cybersecurity incidents.
- + An **Incident Response Plan (IRP)** is a detailed, operational document that ***describes how*** the organization will detect, respond to, contain, and recover from incidents.

**Policy = Strategic Directive**  
**Plan = Tactical Execution Guide**

# References

- + CISA Incident Response Plan (IRP) Basics:
  - + [https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics\\_508c.pdf](https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf)
- + GovRAMP - Incident Response Plan (IRP) Template
  - + <https://govramp.org/blog/document/incident-response-plan-irp-template/>
- + University of Connecticut (UConn) – Incident Response Plan
  - + <https://security.uconn.edu/incident-response-plan/>



# Incident Response Playbooks

# Incident Response Playbooks

An **Incident Response (IR) Playbook** is a *specific, actionable, step-by-step* guide designed to handle a particular type of security incident.

**Incident Response (IR) playbooks** are detailed action guides that outline the specific steps to be taken when responding to particular types of security incidents.

Unlike broader Incident Response Plans (IRPs), playbooks function more like checklists designed for targeted scenarios, such as phishing attacks, information leaks, ransomware infections, denial-of-service (DoS) attacks, website defacements, and similar threats.

# Incident Response Playbooks

A playbook provides ***prescriptive instructions tailored*** to that specific incident type, including:

- + How to detect the incident
- + How to analyze it
- + How to contain and eradicate it
- + Specific evidence to collect
- + Specific communication/escalation steps

***Think of it as a detailed response manual for a specific incident category.***

# Incident Response Playbooks

A typical IR playbook includes:

- + Trigger conditions that define when the playbook should be initiated
- + Step-by-step workflows outlining the actions responders must follow
- + Criteria for incident closure to determine when the response effort is considered complete

There are several publicly available resources offering IR playbook templates.

These templates can serve as valuable starting points, allowing you to customize and build your own playbooks tailored to your organization's environment and threat landscape.






# Summary

- + The **IR Plan** is like a fire department's emergency handbook.
- + The **IR Playbook** is like the exact procedure for responding to a house fire or a chemical spill.

*Both are essential, but one defines the overall system, and the other provides tactical execution for specific threats.*

# Playbook Examples & Templates


- + Incident Playbook: Incident Response Playbooks Mapped to MITRE Attack Tactics and Techniques.
  - + <https://github.com/austinsonger/Incident-Playbook>
- + Public Playbooks: Repository of playbooks and workflows based on the NIST 800.61 r2 guide.
  - + <https://gitlab.com/syntax-ir/playbooks>

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 scene is dimly lit, with the primary light source being the screen.

# **IR Playbook Example: Responding to a Phishing Attack**

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 tone is dark and professional.

# Demo: Phishing Playbook



# Building a Technological Backbone for Incident Response

# Technology In The Preparation Phase

***Before an incident ever occurs***, incident responders must ensure that the ***right technologies are in place***, properly configured, and ready to support detection, investigation, containment, and recovery.

In this video, we'll break down the key technological preparations every incident responder needs to understand, and why these preparations are critical to successful incident handling.

# Technology In The Preparation Phase

Technology provides the **visibility**, **access**, and **tools** that incident responders **rely on during** a security incident.

Without the right technology, even the best-trained response teams can find themselves blind, slow, and ineffective.

*In the preparation phase, technology needs to be ready before the breach happens.*

# Technology In The Preparation Phase

The technologies supporting incident response consist of the systems, tools, and platforms used by security analysts ***to conduct investigations, execute response actions, and manage incidents.***

Effective incident response relies on having the necessary infrastructure, hardware, and software in place to support all activities required during a security breach.



# Technology In The Preparation Phase

An effective incident response capability should be supported by a range of essential tools and resources, including:

- + Incident response management software
- + A threat intelligence platform
- + A well-equipped incident response toolkit
- + Computers with specialized investigation software
- + Isolated network segments for secure responder operations
- + Basic network equipment and cabling
- + Sanitized storage drives for evidence collection
- + Secure communication tools (voice, messaging, and email)
- + Encryption software to protect sensitive information during investigations



# Incident Management With TheHive

# What is Incident Management?

Incident management is the ***structured process*** of ***identifying, managing, and resolving*** security ***incidents*** in a way that minimizes impact, restores normal operations, and preserves evidence.

***It is a core function within the broader discipline of Incident Response (IR).***

# What is Incident Management?

*The primary goal of incident management is to:*

- + **Detect and respond** to incidents quickly and efficiently
- + **Contain** the threat before it spreads
- + **Restore** normal operations as soon as possible
- + Ensure all actions are **documented** and traceable
- + **Learn** from incidents to improve defenses and response capabilities

# Incident Management Platforms

An **Incident Management Platform** is a dedicated software solution that **enables** security teams to centrally manage, track, and coordinate their response to cybersecurity incidents in a structured and consistent manner.

It serves as the **operational hub** during a security incident; where alerts are ingested, cases are created, tasks are assigned, progress is tracked, and collaboration occurs.

# Functions of an Incident Management Platform

Function	Description
Alert Ingestion	Collects alerts from various sources like SIEMs, EDRs, or email reports.
Case Management	Allows responders to convert alerts into structured investigation cases.
Task Assignment & Tracking	Breaks incidents into specific tasks and assigns them to analysts.
Evidence Handling	Centralizes observables (IOCs) and documentation for analysis.
Collaboration	Enables multiple team members to work on a case simultaneously with full visibility.
Audit Logging	Tracks actions, decisions, and timelines for accountability and compliance.
Reporting & Metrics	Generates reports for executives, compliance, and lessons learned.



**TheHive**

# TheHive

**TheHive** is an open-source incident response and case management platform designed to help security operations centers (SOCs), CSIRTs, and incident responders **manage** and **coordinate** their **response to security incidents** in a structured and collaborative way.





# TheHive

**TheHive** acts as a ***centralized workspace*** for handling alerts, tracking investigation tasks, managing evidence (observables), and documenting incident response activities.

***It is designed to streamline and standardize incident response workflows, especially in environments with multiple analysts or high alert volumes.***



# Key Features of TheHive

Feature	Description
Alert Ingestion	Collect alerts from SIEMs, emails, scripts, or manual inputs.
Case Management	Convert alerts into structured cases that contain tasks, observables, and timelines.
Task Tracking	Organize the response process by creating and assigning investigation tasks.
Observables Handling	Track and enrich indicators of compromise (e.g., IPs, hashes, domains).
Collaboration	Multiple analysts can work on the same case, with full visibility into actions and notes.
Integration with Cortex	Optional integration for automated enrichment, analysis, and response actions.
Audit Logging & Reporting	Built-in support for documentation and case reporting for compliance and reviews.

# TheHive Integrations

Integration Type	Examples	Purpose
<b>SIEM Tools</b>	Splunk, Elastic Stack, QRadar	Automatically forward alerts into TheHive as new cases or alerts
<b>Ticketing Systems</b>	ServiceNow, JIRA	Link IR cases with ITSM or engineering workflows
<b>Threat Intelligence</b>	MISP, OpenCTI	Ingest threat intel and IOCs to enrich observables
<b>Security Automation (SOAR)</b>	Cortex (official), TheHive4py (Python client)	Automate enrichment, scanning, and containment actions
<b>EDR/AV</b>	CrowdStrike, SentinelOne, etc.	Alert ingestion or response actions via Cortex analyzers
<b>Email &amp; Phishing Analysis</b>	IMAP, Email Parser Scripts	Automatically create alerts from phishing reports sent to an inbox
<b>ChatOps</b>	Mattermost, Slack (via webhooks)	Notify IR teams of new alerts or case status changes



# What is Cortex?



Cortex is TheHive's official analysis and automation engine. It's a companion application used to automate the enrichment of observables and perform response actions directly from within TheHive.

Cortex acts like the "brains" behind TheHive's automation — it gives responders instant context without leaving the platform.

# Cortex Capabilities

- + Run analyzers on observables (e.g., scan IPs, URLs, hashes)
- + Perform automated actions, like checking an IP against VirusTotal or querying MISP for known IOCs
- + Use responders to take real-world actions (e.g., block an IP on a firewall, notify a system)

# Common Cortex Analyzers

- + VirusTotal
- + URLhaus
- + AbuseIPDB
- + Shodan
- + MISP
- + Whois/RDAP
- + Censys

# TheHive Terminology

- + **Alert:** A security-relevant notification (from a SIEM, analyst, or tool) that may be escalated into an incident case.
- + **Case:** A formal incident investigation that contains tasks, observables, tags, severity levels, and analyst comments.
- + **Task:** A step or action required during the handling of a case (e.g., “Collect logs,” “Analyze malware”).
- + **Observable:** Any indicator that can be analyzed or enriched (e.g., file hash, IP, domain, email address).
- + **Tag:** Custom labels applied to cases or observables for grouping and filtering (e.g., #ransomware, #phishing).



# TLP (Traffic Light Protocol)


TLP is a standard classification scheme used to indicate how sensitive information is and how it can be shared.

TLP Level	Meaning
TLP:RED	Highly sensitive, for named recipients only – no further sharing
TLP:AMBER	Limited sharing within organization or community
TLP:GREEN	Can be shared within the cybersecurity community
TLP:WHITE	Public – no restrictions on distribution

# PAP (Permissible Actions Protocol)

PAP (Permissible Actions Protocol) is a classification system used to define how information may be used, rather than how it may be shared (which is what TLP governs).

PAP Level	Meaning
PAP:WHITE	The information may be used freely, including for attribution, enforcement, or public disclosure.
PAP:GREEN	The information may be used within the organization or community, including for protective actions, but not publicly.
PAP:AMBER	The information is more sensitive; it may be used internally, but not disclosed externally or used for attribution without permission.
PAP:RED	The information is highly sensitive and should not be used for enforcement, attribution, or public exposure — typically used for situational awareness only.

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 Response With TheHive: A Practical Demo



# Incident Response Toolkit

# Incident Response Toolkit

An **Incident Response (IR) Toolkit** is a curated set of tools and utilities that ***incident responders use during security investigations***, containment efforts, and post-incident analysis.

It provides the ***technical capabilities*** responders need to collect evidence, perform forensics, triage alerts, and act quickly during a cyber incident.

# Incident Response Toolkit

Depending on the organization or context, the IR toolkit may also be referred to as:

- + Responder Kit
- + Cyber First Responder Toolkit
- + Digital Forensics Toolkit
- + IR Utility Pack
- + Investigation Toolkit
- + Security Analyst Toolkit

Despite different labels, the goal remains the same: ***equipping responders with ready-to-use tools for efficient, consistent, and effective incident handling.***



# Common Tools Included in an IR Toolkit

IR toolkits typically include a mix of forensics, analysis, collection, and triage tools. Here's a breakdown by category:

- + Evidence Collection & Imaging
  - + FTK Imager – Disk imaging
  - + Magnet RAM Capture / Belkasoft RAM Capturer – Memory acquisition
  - + dd – Command-line disk imaging (Linux)
  
- + Memory and Disk Forensics
  - + Volatility / Rekall – Memory analysis
  - + Autopsy / Sleuth Kit – File system forensics

# Common Tools Included in an IR Toolkit

- + Log and Event Analysis
  - + Log Parser – Windows log analysis
  - + SysmonView – Visualization for Sysmon logs
- + Packet Capture and Network Analysis
  - + Wireshark / tcpdump – Traffic inspection and capture
- + Malware Analysis and IOC Triage
  - + PEStudio – Static malware analysis
  - + VirusTotal Uploader – File and hash scanning
  - + CyberChef – Decode and analyze encoded/obfuscated data
  - + YARA – Pattern matching for malware detection



# Common Tools Included in an IR Toolkit

- + Artifact Collection (Windows)
  - + KAPE (Kroll Artifact Parser and Extractor) – Collects Windows forensic artifacts
  - + EZ Tools (Eric Zimmerman) – Registry Explorer, Timeline Explorer
  
- + System Utilities and Scripting
  - + PsExec / PSKill (Sysinternals) – Remote execution and process termination
  - + PowerShell & Bash scripts – For automation and triage
  - + HashMyFiles – Generate and verify file hashes

# How to Build Your Own IR Toolkit

## 1. Define Your Use Case

- + Are you building for a Windows environment? Linux? Cloud?
- + Will this toolkit be used in the field (USB/live boot) or on dedicated IR workstations?

## 1. Identify Core Capabilities You Need

- + Evidence collection? Memory analysis? Log review?
- + Include tools aligned with your incident response procedures and playbooks.

## 1. Select and Test Tools

- + Choose reliable, well-supported tools (preferably open source or vendor-approved)
- + Test everything in a sandbox environment before relying on it in production
- + Document usage instructions or create a quick reference guide

# How to Build Your Own IR Toolkit

## 4. Package and Organize the Toolkit

- + Create a structured folder system:

```
IR-Toolkit/  
├── Collection/  
├── Forensics/  
├── MalwareAnalysis/  
├── Scripts/  
├── Logs/  
└── Documentation/
```

Consider building:

- + A portable version on a USB drive with write blockers
- + A virtual machine image preloaded with your tools
- + A cloud-hosted toolkit if responding to cloud-native incidents

# How to Build Your Own IR Toolkit

## 5. Maintain and Update

- + Keep tools up to date
- + Regularly review your toolkit based on:
  - + New attack trends
  - + Lessons learned from past incidents
  - + Team feedback

# Incident Response: Preparation - Summary

# Key Concepts - Recap

- + Incident Response Fundamentals
- + Incident Response Teams and Structures
- + The Preparation Phase in Incident Response



## Learning Outcomes Recap

- + Explain the importance of incident response and the risks of unstructured response efforts
- + Identify different types of security incidents and common attack vectors
- + Describe various types of incident response teams, their structures, and their roles
- + Understand and differentiate between major IR frameworks (NIST and SANS)
- + Develop foundational IR artifacts such as policies, plans, playbooks, and responsibility matrices
- + Apply the Hierarchy of Needs model to build incident response readiness
- + Understand the role of technology infrastructure in supporting incident response activities
- + Manage security incidents using an incident management platform (TheHive)
- + Build a basic yet effective Incident Response Toolkit tailored for operational use

# Next Steps

- + Deepen your understanding of IR Frameworks:
  - + NIST Special Publication 800-61 Revision 2 – Computer Security Incident Handling Guide
  - + SANS Incident Handler's Handbook – Practical IR process guidance
- + Practice Incident Management Using Open-Source Tools
  - + Set up a personal lab with:
    - + TheHive (Incident Management Platform)
    - + Simulate handling different types of incidents (e.g., phishing, malware outbreaks)



# Next Steps

- + Create Your Own IR Documents:
  - + A sample Incident Response Policy
  - + A basic Incident Response Plan (IRP)
  - + A few IR Playbooks (e.g., ransomware, insider threat, phishing)

**THANKS FOR WATCHING!**

