

Topic 8

Incident Response Fundamentals

Slides developed by



What you will
learn in these
slides...

Importance of incident response
procedures

NIST Incident Response Life Cycle

Common response plans used

- IRP, DRP, BCP


The need for incident response (IR) in organizations



Purpose of IR procedures

- Familiarize employees with common cyber incidents that may affect the organization
- Detect and respond to these incidents in a timely and effective manner
- Ensure employees fully understand the SOPs within the organization
 - Remember, **each and every employee** is vital to the success of proper response procedures!
 - Any individual can propose improvement strategies and take notes during execution of the plan

Incidents that can trigger/activate an IR plan

A dark, abstract image featuring a hand with glowing red digital lines and binary code, symbolizing technical incidents.

Technical incidents

- Malware
- Data Breaches
- DoS / DDoS attacks

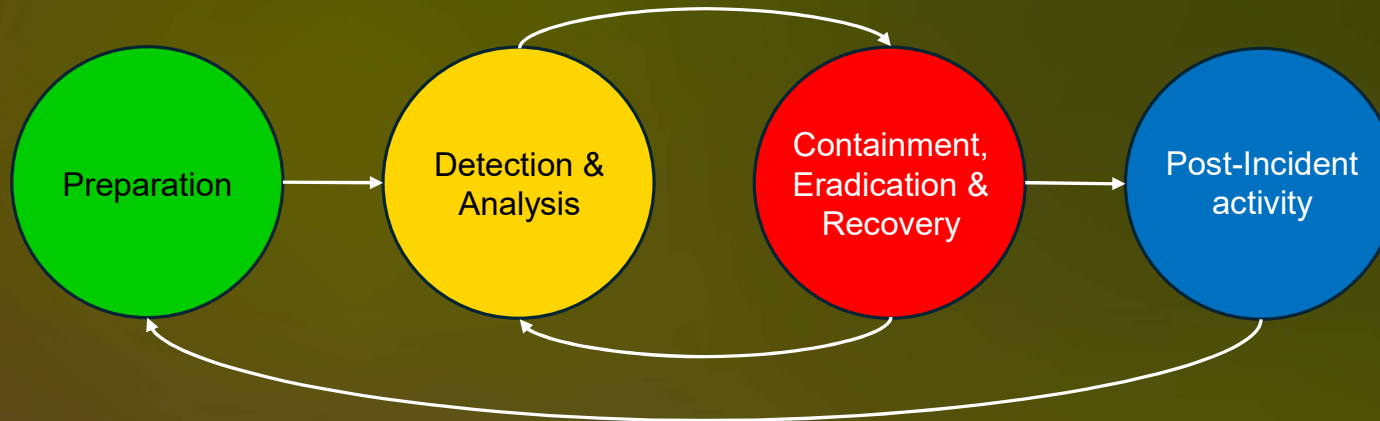
A dramatic image of a road leading towards a massive, dark storm cloud with a bright light source, symbolizing non-technical incidents.

Non-technical incidents

- Fires
- Blackouts
- Natural Disasters

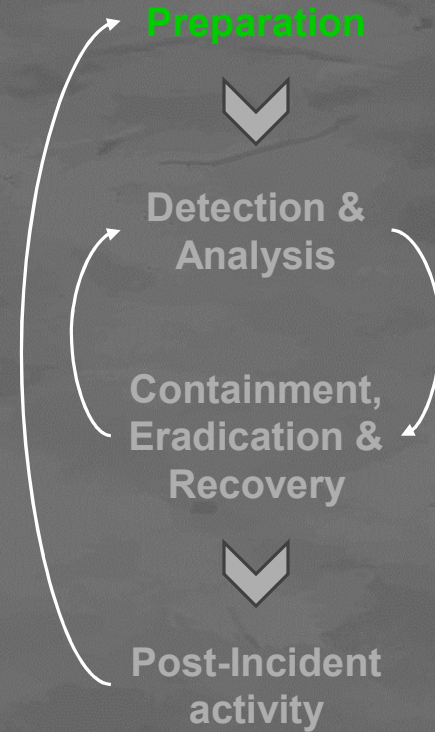
NIST Incident Response Life Cycle

- In Topic 3 we learned about NIST and its guidelines for good passwords
- For incident response, NIST also developed a 4-step process for organizations to follow
- Allows organizations to adopt a common framework to handle cybersecurity incidents
- Promotes consistency and reliability in response efforts



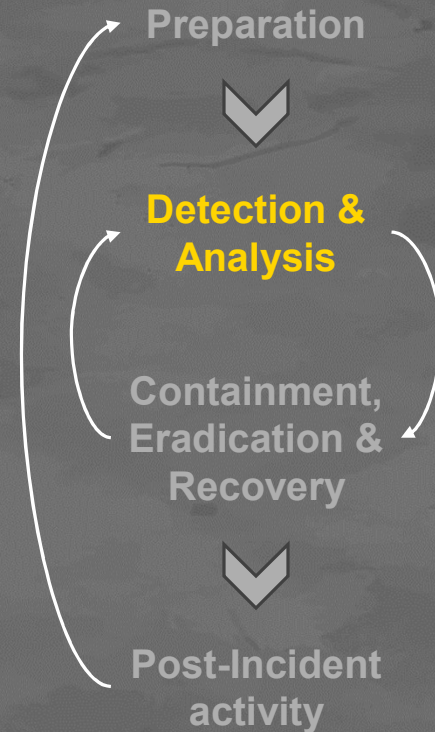
NIST IR Life Cycle (Preparation)

- Implement and establish clear IR policies and roles
- Establish communication protocols and contact lists
 - Implement a call tree
- Conduct training and simulated drills to ensure staff understand their role and steps to follow



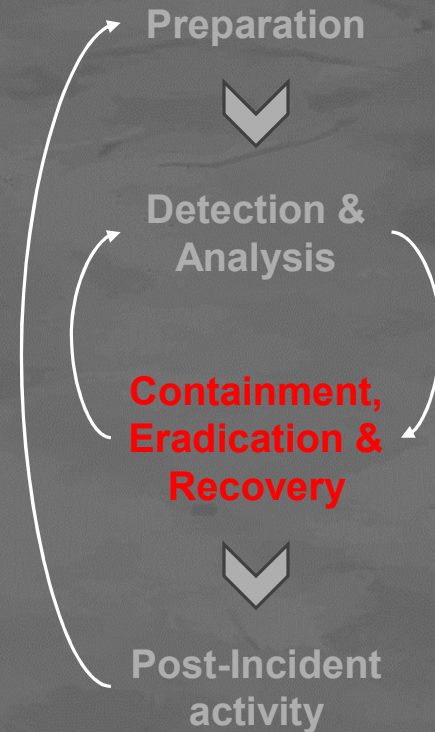
NIST IR Life Cycle (Detection & Analysis)

- Monitor systems for unusual activities
- Utilize intrusion detection systems (IDS) and/or security information and event management (SIEM) systems to analyze alerts and logs for potential incidents



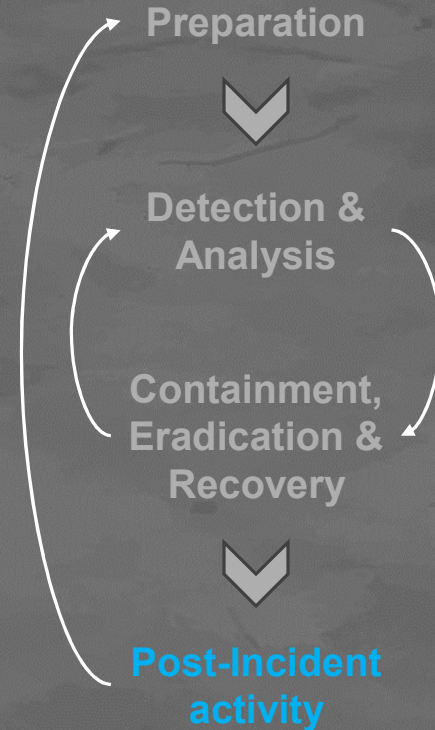
NIST IR Life Cycle (Containment, Eradication & Recovery)

- Isolate affected systems to prevent spread (via sandboxes or other isolation software)
- Remove malicious components from systems
- Restore systems and validate integrity
- If more monitoring of systems is required, go back to **Detection & Analysis**
- If all parties are confident that no more monitoring is required, go to **Post-Incident Activity**



NIST IR Life Cycle (Post-Incident Activity)

- Conduct a thorough incident debrief for affected staff
- Update policies based on lessons learned
- Document and report findings and improvements



Call Tree



- A communication method used in various response and recovery plans
- Helps to quickly disseminate information and instructions during an emergency
- Ensures that critical messages reach all relevant personnel efficiently and effectively
- Expressed as a phone tree diagram with the overall in-charge of the organization at the top of the tree
 - The overall in-charge is often the **CEO**, Chief Information Security Officer (**CISO**) or an **operations manager**, depending on the organization or plan activated
- All employees are required to memorize the call tree for clarity and preparedness

Commonly implemented response plans

- Incident Response Plan (IRP)
- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)



Incident Response Plan (IRP)

- Address and manage the aftermath of a security breach or cyberattack
- Limit damage and reduce recovery time and costs

Objectives of IRP	Recommended teams to assemble
<ul style="list-style-type: none">• Quickly contain and mitigate the impact of security incidents• Rapidly recover affected systems to maintain business operations• From the incident, find ways to strengthen security measures and protocols	<ul style="list-style-type: none">• Head of Departments / Senior Management• Incident Response Team (IRT)• IT Recovery Department (includes IT Recovery Team and Damage Assessment Team)• Engineering Department

NIST IR Life Cycle for IRP

Preparation	<ul style="list-style-type: none">• Develop and implement IR policies• Assemble required teams and provide training• Implement a call tree• Conduct regular drills for both IRT and other employees
Detection & Analysis	<ul style="list-style-type: none">• Monitor systems for suspicious activity• Analyze potential threats and identify incidents quickly
Containment, Eradication and Recovery	<ul style="list-style-type: none">• Isolate affected systems• Eliminate any threats• Restore normal operations
Post-Incident Activity	<ul style="list-style-type: none">• Conduct a post-incident review• Document lessons learned• Update IRP with new measures if needed

Disaster Recovery Plan (DRP)

- Ensure the recovery of critical IT systems and data after a disaster
- Applies to both **technical** and/or **non-technical** incidents

Objectives of DRP	Recommended teams to assemble
<ul style="list-style-type: none">• Restore critical IT systems and data promptly after a disaster• Ensure business operations face as little disruption as possible• Safeguard the integrity and availability of data during recovery	<ul style="list-style-type: none">• Head of Departments / Senior Management• Crisis Recovery Department (includes Crisis Management Team and Crisis Communication Team)• IT Recovery Department (includes IT Recovery Team and Damage Assessment Team)

NIST IR Life Cycle for DRP

Preparation	<ul style="list-style-type: none">• Ensure recovery procedures are detailed and maintained• Assemble required teams and provide training• Implement a call tree• Backup all necessary software regularly• Test recovery processes
Detection & Analysis	<ul style="list-style-type: none">• Identify potential technical and non-technical incidents that the organization may face• Assess the potential damage caused and plan recovery actions
Containment, Eradication and Recovery	<ul style="list-style-type: none">• Execute the recovery actions• Restore the systems and data• Ensure data integrity to prevent future unauthorized tampering
Post-Incident Activity	<ul style="list-style-type: none">• Review the recovery process and identify areas for improvement• Improve recovery strategies and analyze effectiveness

Business Continuity Plan (BCP)

- Includes critical information that an organization needs to continue business operations during and after a disruption
- Alternate sites must be set up and ready to allow **continuous operations**

Objectives of BCP	Recommended teams to assemble
<ul style="list-style-type: none">• Ensure essential business functions continue during disruptions• Identify and mitigate risks to business continuity• Establish clear communication channels for stakeholders during incidents	<ul style="list-style-type: none">• Head of Departments / Senior Management• Crisis Recovery Department (includes Crisis Management Team and Crisis Communication Team)• IT Recovery Department (includes IT Recovery Team and Damage Assessment Team)• Emergency Response Team• Command Centre Operation Team

NIST IR Life Cycle for BCP

Preparation	<ul style="list-style-type: none">• Identify critical business functions• Assemble required teams and provide training• Implement a call tree• Develop continuity strategies
Detection & Analysis	<ul style="list-style-type: none">• Recognize potential disruptions and evaluate their impact (using various risk methodologies)
Containment, Eradication and Recovery	<ul style="list-style-type: none">• Implement alternative business processes• Relocate operations to a temporary site if necessary• Ensure continuous communication across all sites
Post-Incident Activity	<ul style="list-style-type: none">• Review continuity efforts• assess overall impact, and enhance the plan for future resilience

Important pointers for each plan

	IRP	DRP	BCP
Key Focus	Handling immediate response to security incidents	Restoring IT systems and data after a disaster	Ensuring all critical business functions continue
Scope	Cybersecurity incidents and breaches	IT infrastructure and data recovery	Entire organization, both tech and non-tech disruptions
Usual duration to complete upon plan activation	Short-term (4-8 hours)	Short to Medium-term (6 hours to 1 week)	Medium to Long-term (1-28 days)
Documentation needed	<ul style="list-style-type: none">IR proceduresIncident logs	<ul style="list-style-type: none">Recovery proceduresSystem backups	<ul style="list-style-type: none">Continuity proceduresCommunication plans
Recommended testing frequency	Every 6 months or upon new updates	Annually	Annually
What can cause the plan to activate	<ul style="list-style-type: none">Data breachesMalware	<ul style="list-style-type: none">Natural disastersTechnical failures	<ul style="list-style-type: none">Natural disastersTechnical failuresSupply chain disruptions

Despite a few minor differences between each plan, all three plans play equally important roles in ensuring an organization knows how to overcome adversity.

Topic 8 Summary

- Importance of incident response procedures
- NIST Incident Response Life Cycle
- Common cybersecurity response plans and their differences
 - IRP, DRP, BCP

We hope you have gained valuable cybersecurity insights from all our eight topics! 😊

Now... are you ready to showcase what you have learnt?

