Chinyere Chinekezi
XDR Security Analyst

# MASTER INCIDENT RESPONSE: ELEVATE EFFICIENCY WITH PLAYBOOKS

CONF42.COM INCIDENT MANAGEMENT 2024

# Agenda

- Understanding Incident Response
- Challenges in Incident Management
- What is an Incident Response Playbook?
- Benefits of Using Incident Response Playbook
- Guides to Creating Your own Playbook
- Key Elements of an Effective Incident Playbook
- Examples of Playbook
- Tools and Technologies
- Conclusion

# Understanding Incident Response

**What is Incident Response?**
**NIST** defines IR as a systematic process for handling cybersecurity incidents
Incidents like data breaches or malware infections.

**Why is it Important?**
IR reduce damage and downtime, ensures business continuity, and protects sensitive data from exploitation.

**Incident Response Phases**

IR involves preparation, detection, analysis, containment, eradication, recovery, and post-incident review.

# Challenges in Incident Management

- **Lack of clear procedures:** Without a clear process, there is a risk of confusion, delays, and errors in the incident management process.
- **Inadequate incident categorization and prioritization**.
- **Lack of tools and resources**
- **Inadequate training**
- **Lack of communication and collaboration**

# What is Incident Response Playbook?

An Incident Response Playbook is a detailed and structured set of procedures that outlines how an organisation will detect, respond to, and recover from cybersecurity incidents..

The primary goal of an incident response playbook is to help organizations minimize the impact of breaches and to quickly restore normal operations

There are different types of playbook that can be developed by organization depending on the nature, size, and potential threat of the organization

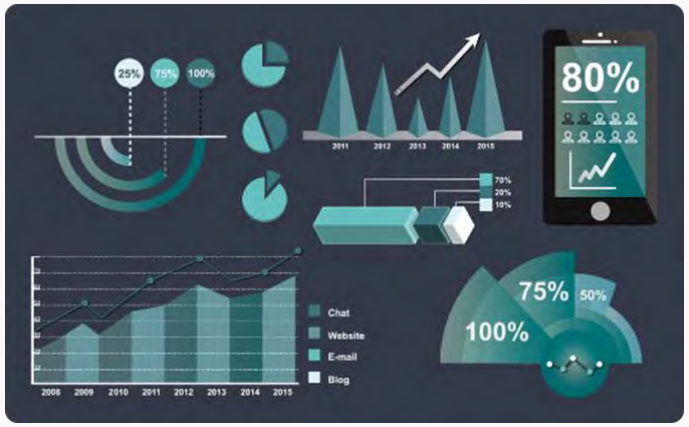
**Common Types of Incident Playbooks.**

- **Ransomware playbook.**
- **Data breach or data loss playbook.**
- **Malware playbook**
- **Denial-of-service playbook.**
- **Insider threat playbook**
- **Social engineering playbook.**
- **Website compromise playbook**
- **Zero-day vulnerability playbook**

# Benefits of Incident Response Playbook

## Improved Efficiency

Streamlined processes for quicker response times and reduced downtime.




## Enhanced Effectiveness

Clear procedures for better decision-making and more impactful actions.

## Increased Collaboration

Well-defined roles and responsibilities for smoother coordination between teams.

# Guides to Creating Incident Playbook

- Define what constitute an incident: This involves identifying potential vulnerabilities and threats that are specific to the organisation and its operations by performing penetration testing and vulnerability assessments.
- Create Reporting Checklists: This checklist is a template for gathering initial incident details, steps carried out during the response, and the outcome of those activities.
- Define clear procedure: This involves developing a process for detecting and investigating Incident to identify potential security incident and prioritising them based on their severity and impact.
- Establish Roles and Responsibilities
- Develop Communication Plans
- Test : This can be done by performing a Tabletop exercise
- Refine: This is allowed for improvement of the defined process

# NIST Four Phase Explained

## Prepartion

- This process involves establishing the right tools and policies, and procedures ahead of any incident. It also includes the training of staff, the creation of incident response protocols, and the establishment of communication strategies for both internal and external purposes.

## Detection &Analysis

- **It involves monitoring and analysing data to detect any anomalies that indicate a security breach**

## Containment, Eradication &Recovery

- **It** focuses on developing strategies to minimise the spread and impact of the incident.
- **Restoration guidelines are implemented**

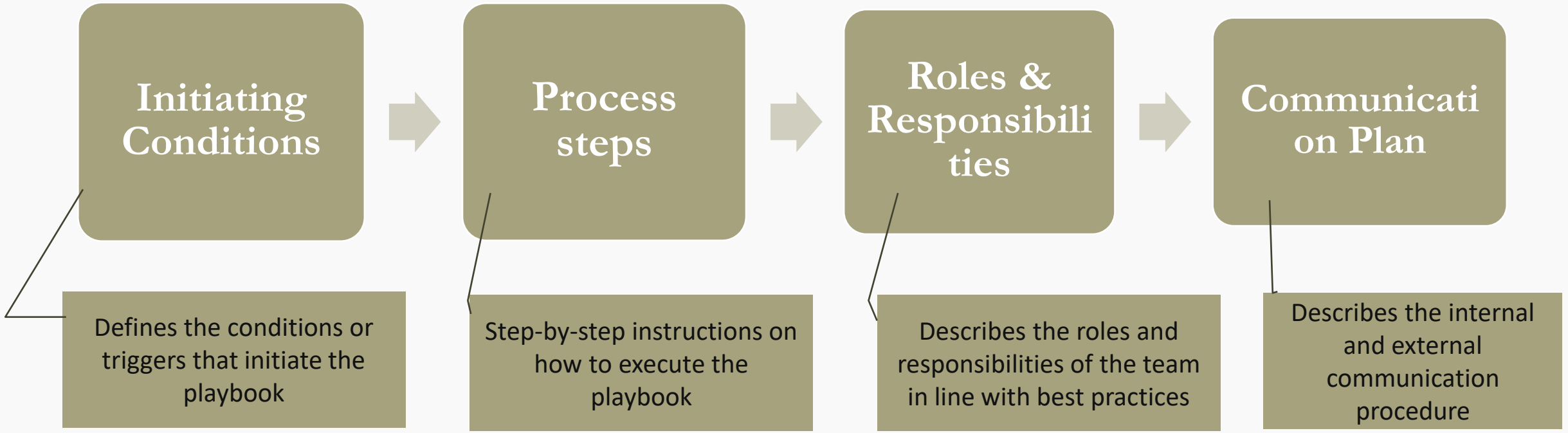
## Post-Incident Activity

**Review of Incident playbook**

**Lessons Learned**

https://csrc.nist.gov/Projects/incident-response

# Key Element of an Effective Incident Playbook



# Example Playbook: Phishing Attack Response

A large financial institution faced a sophisticated phishing attack targeting its employees. The attackers aimed to steal sensitive information and gain unauthorized access to the company's systems.

**Trigger**

Employee reports a suspicious email, or the security team detected unusual login attempts and flagged them as potential phishing attempts

# Phishing Attack Response Playbook

**Detection**

Verify the phishing attempt (e.g., look for malicious links, attachments, or impersonated domains).

**Containment**

- Block the sender's email address and malicious domain across the organization.
- Quarantine affected email accounts and isolate any compromised systems.
- Revoke any access granted via compromised credentials.
- Notify employees to avoid clicking on the phishing email.

**Eradication**

- Scan affected endpoints for malware or suspicious activity.
- Review email logs and identify any other employees who may have received or interacted with the phishing email.
- Reset passwords and enforce multi-factor authentication (MFA) for compromised accounts

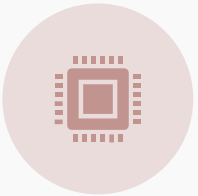
**Recovery**

- Ensure all compromised accounts, systems, and devices are secure.
- Restore any data impacted by the phishing attack.
- Test the security posture by simulating potential phishing exploits to verify containment
- Prevent the spread of the attack or further data compromise.

**Post-incident Activity**

- Document the attack's details, response efforts, and results.
- Conduct a post-incident analysis to determine how the phishing attempt bypassed security controls.
- Implement Improvements: Strengthen email filters, update training protocols, and refine the phishing detection process.
- Employee Awareness Training: Conduct phishing awareness training, using the incident as an educational too

# Tools and Technologies



**Security Information and Event Management (SIEM)**: SIEM tools collect and analyse security data from various sources to detect suspicious activities e.g. Splunk, IBM QRadar, ArcSight

**Endpoint Detection and Response (EDR):** Monitor and respond to threats on endpoints (CrowdStrike Falcon, Carbon Black, Microsoft Defender for Endpoint)

**Security Orchestration, Automation, and Response (SOAR): E.g Microsoft Sentinel, FortinetSOAR, Rapid7 InsightConnect**

**Incident Management Systems: E.g (**TheHive, IBM Resilient, Palo Alto Networks Cortex XSOAR)

**Threat Intelligence Platforms: E.g (RecordedFuture,Shodan, AbuseIPDP, etc)**

# Common Pitfalls to Avoid

**Outdated Playbooks**

**Lack of Testing**

**Poor Communication**

# Conclusion

By using well-designed incident response playbooks, organizations can significantly enhance efficiency, reduce downtime, and improve overall security.