CYBERSECURITY INCIDENT RESPONSE PLAN

Created by : Raushan

Linkedin : https://www.linkedin.com/in/raushan-patel-8823b3241/

Incident Response Plan process

Preparation

- Creating Guidelines to enable seamless communications.

Containment

- Adopt mitigations actions
- Coordinated shutdowns.

Recovery

- Develop strategies to mitigate risks.

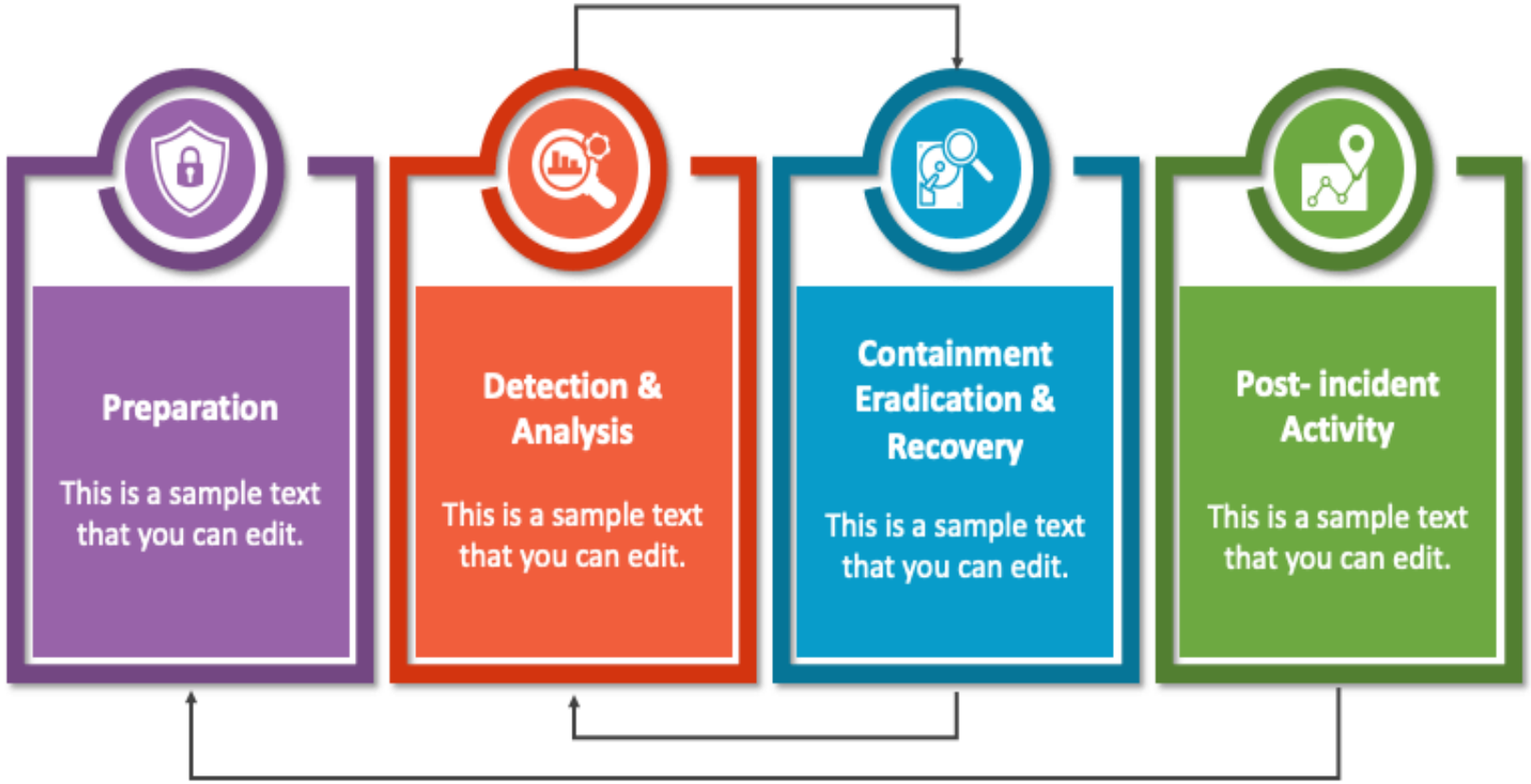
Detection & analysis

- Monitors networks and system to
- Gather information and prioritize individual incidents

Eradication

- Remove existing threats from network.

CYBER INCIDENT RESPONSE PLAN



What Is Cybersecurity incident response plan?

- A cybersecurity Incident Response Plan (CIRP) is a strategic and systematic approach that an organization follows to effectively manage and mitigate the impact of a cybersecurity incident.
- A cybersecurity incident refers to any event that compromises the confidently, integrity, or availability of an organization's information systems and data. Incidents can range from a malware infection and unauthorized access to a data breach or a distributed denial-of-service (DDoS) attack.

What Is An Incident Response?

- Incident response refers to the systematic approach taken to address and handle the consequences of a security breach or attack, aiming to minimize harm and restore regular operations promptly.
- The incident response process encompasses various measures, including identifying the origin of the attack, containing the breach, reducing the impact, and implementing preventive measures against future attacks.
- It represents a proactive approach to security.

The Role of Cybersecurity in Incident Response

- In the realm of incident response, cybersecurity measures play a critical role in preventing and responding to incidents effectively. With the right tools and strategies in place, organizations can:
- This includes personal information like:

- Detect and thwart attacks in advance
- Recognize vulnerabilities and essential assets
- Limit losses
- Execute risk management procedures

Phase 1: Preparing for Potential Incidents

- During the preparation stage, organizations establish the foundation for effective incident response. This includes developing and documenting incident response plans and procedures that outline the roles, responsibilities, and actions to be taken when an incident occurs.
- Conduct risk assessments to determine where they have weaknesses and prioritize assets
- Evaluate potential vulnerabilities
- Establish appropriate communication channels
- Ensure that business continuity plans are in place
- Develop and document incident response plans and procedures that outline the roles, responsibilities, and actions to be taken when an incident occurs.

Phase 2:Detection And Analysis

- In this phase, the focus is on identifying and assessing security incidents to understand their nature, scope, and potential impact on the organization.
- The incident response team analyzes relevant data, logs, system configurations, and any other available information to gain insights into the incident's characteristics and potential consequences.
- Monitor your networks, systems, and connected devices to identify potential threats.
- Produce reports on a regular basis and document events and potential incidents.
- Analyze these occurrences and determine whether you need to activate your incident response plan.
- Determine the frequency and intensity of your monitoring.
- Begin analyzing the incident and determining how it happened.
- Validate and confirm that a reported event is, indeed, a security incident.
- Collect initial triage data used for developing IOC detections.

Phase 3: Containment

- Once an incident has been identified, the next step is to contain its impact and prevent it from spreading to other areas of the organization's network.
- The following criteria are useful in determining a suitable strategy for incident containment:
  - Potential for damage to IT assets or loss thereof
  - Loss of availability of critical services (e.g., networks, externally rendered services)
  - Need for time and resources to implement containment
  - Level of containment effectiveness
  - Loss of service during containment period
- It is crucial, however, not to delete the malware during this phase, as doing so may hinder the response team's ability to conduct an investigation and restore the files.

Phase 4: Investigating and Eradicating Threats

- With the incident contained, the next step is to investigate the root cause and eradicate any threats from the system.
- The Eradication phase has one goal: to make sure the threat is no longer present in the organization's network.
- To achieve this, organizations must employ a range of techniques, including:
- Designing and implementing policies and rules regarding data usage
- Implementing network access control
- Utilizing antivirus software consistently
- Monitoring data usage to combat threats
- Enhancing physical security
- Monitoring and instructing users about being mindful with downloads from third-party sites
- Thoroughly investigating and eradicating threats enables organizations to take a significant step towards restoring normal operations.

Phase 5: Recovering and Restoring Operations

- The Recovery phase of an incident response plan is all about getting back to business as usual. After the threat has been eradicated, organizations must restore the affected systems to their pre-incident state.
- Files lost during the incident or cyberattack may require a data recovery service to restore them.
- To develop and coordinate an incident recovery plan, you need to be familiar with the standard phases
- Incident response planning begins with the initial preparation phase.
- Threats, attacks, and malicious actors are identified in the second phase.
- Threat containment and control comprise the third stage.
- Cyberattacks and threats are eradicated in the fourth stage.
- The recovery phase of incident response occurs in the fifth stage.

Examples Of Real-Life Incident Response Scenarios

- Real-life incident response scenarios can vary greatly depending on the type of incident and the organization's response plan. However, there are some common scenarios that organizations should be aware of and prepared for.
- Data Breach: A company discovers that its customer database has been compromised, resulting in the theft of sensitive customer information such as names, addresses, and credit card details.
- Malware Outbreak: An organization's network gets infected with a new strain of malware that spreads rapidly, causing disruptions and potentially compromising sensitive information.
- Distributed Denial of Service (DDoS) Attack: A popular e-commerce website experiences a sudden surge in incoming traffic, overwhelming its servers and causing the site to become inaccessible to legitimate users.
- Ransomware Attack: A manufacturing company's network is compromised by ransomware, resulting in the encryption of essential production systems and intellectual property.
- Insider Threat: An employee with privileged access intentionally or inadvertently compromises critical systems or data.

The Benefits of Following an Incident Recovery Process

- While remediation standards of the past weren't as comprehensive as the methods used today, they seldom resulted in a permanent solution.
- Given the modern reliance on IT today, a standardized incident recovery plan has many benefits.
- Identifying trouble areas, weak points, and security gaps in your current cyberdefense.
- Clarifying employee roles and responsibilities before an incident occurs
- Educating your staff on common threats and online hazards
- Establishing lines of communication, including backups in the case of widespread system failure
- Detecting certain incidents and events in real-time
- Predicting and preparing for future threats
- Ensuring the security of consumer data during an active incident
- Easing the concerns of key stakeholders

References !

- How to Execute the Containment Phase of Incident Response (rsisecurity.com)
- 7 Phases of Incident Response: Essential Steps for a Comprehensive Response Plan – TitanFile
- Step-By-Step Guide To An Effective Incident Response Plan (wirexsystems.com)
- Incident Response Plan: Frameworks and Steps - CrowdStrike

Thank you

Github:- raushanpatel1 (Raushan patel) (github.com)