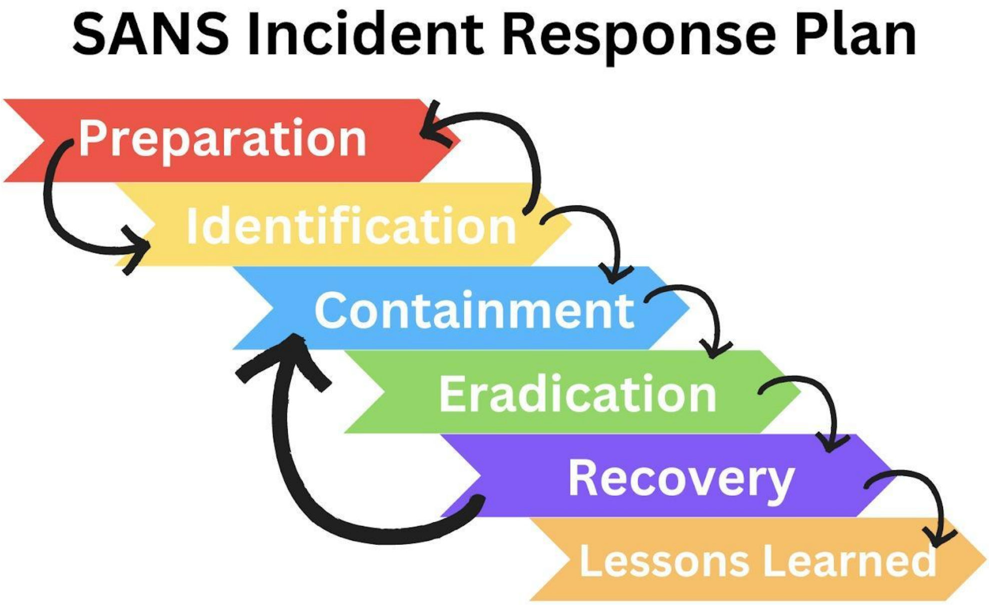
Incident Response in Cybersecurity



Yasemin AĞIRBAŞ

1. Preparation

The foundation of a successful incident response is preparation. This ensures quick and efficient action when a security event occurs.

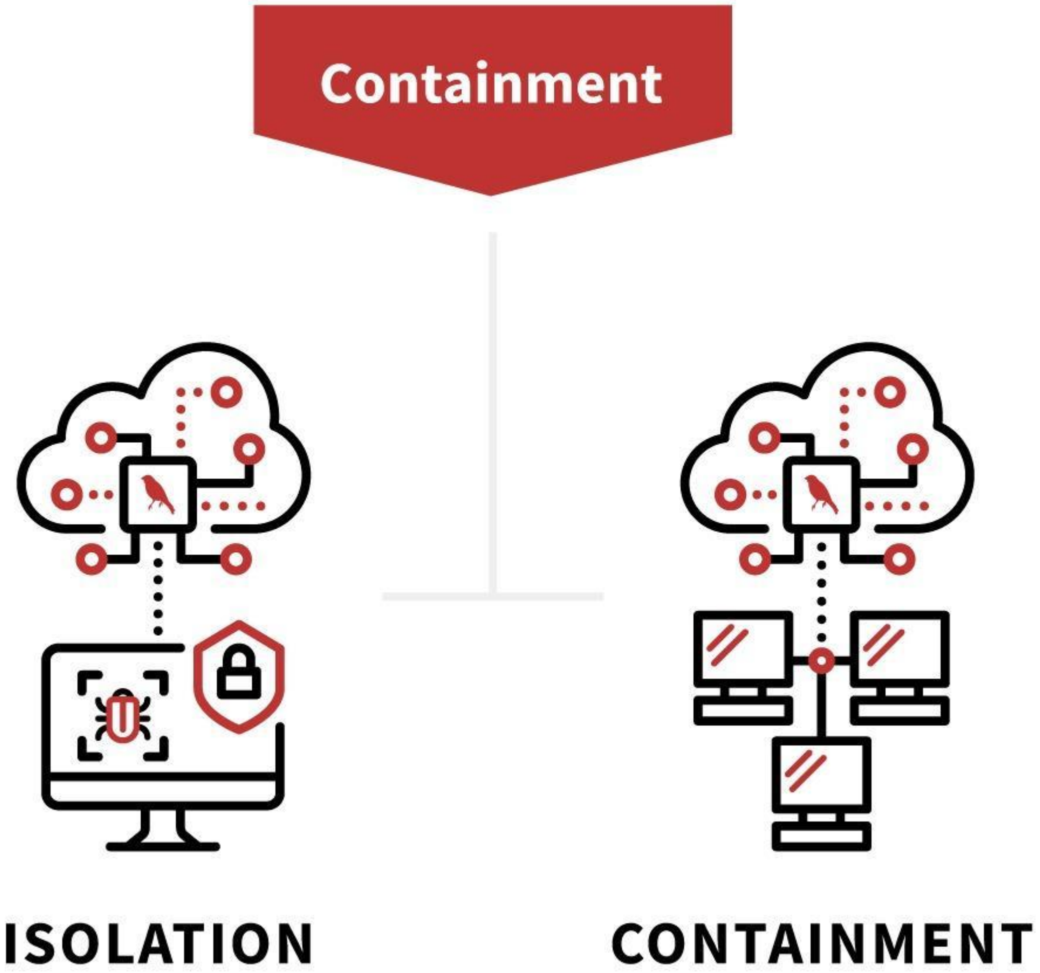
- **Incident Response Team (IRT)**: The IRT should comprise various specialists:
    - **Manager**: Oversees the response, ensuring coordination and effective communication.
    - **First Responders**: The frontline team members who assess and initially tackle the incident.
    - **Subject Matter Experts**: Individuals with deep knowledge in specific areas, such as network forensics, malware analysis, legal implications, and public relations.
- **Training**: Regular drills should simulate various attack scenarios, ensuring team readiness and refining procedures. This also helps in identifying gaps in the current response plan.
- **Tools & Infrastructure**:
    - **Detection Tools**: Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) tools, and endpoint detection and response (EDR) solutions.
    - **Communication Tools**: Encrypted channels for internal team communication.
    - **Forensic Tools**: For data collection and analysis.

2. Identification

Recognizing an incident early can significantly reduce potential damage.

- **Detection Tools**: Regularly review logs and alerts from IDS and SIEM solutions.
- **Alert Triage**: Not all alerts indicate a genuine incident. The team must assess and prioritize them based on potential impact and validity.
- **Analysis**:
    - **Initial Analysis**: Understand the type of attack, its origin, and its potential impact.
    - **Scope Determination**: Identify affected systems and data.

3. Containment



Containment limits the immediate impact and stops further propagation.

- **Short-term containment**:
  - **Network Isolation**: Disconnect affected systems from the network.
  - **Account Suspension**: Temporarily suspend compromised user accounts.
- **Long-term containment**:
  - **Patching**: Apply security patches to vulnerabilities.
  - **Improved Security Measures**: Strengthen security configurations to prevent similar breaches.

4. Eradication

After containment, the root cause must be fully addressed.

- **Root Cause Analysis**:
  - **Threat Hunting**: Proactively search for signs of adversaries within the network.
  - **Vulnerability Assessment**: Identify and address security gaps.
- **Malware Removal**: Use advanced malware removal tools and techniques.

5. Recovery

Post-incident, systems are restored to operational status.

- **System Restoration**: This may involve reimaging systems, restoring from backups, or rebuilding systems.
- **Monitoring**: Enhanced monitoring after an incident ensures no remnants of the threat remain and confirms the integrity of systems.

6. Lessons Learned

A retrospective analysis is crucial for continuous improvement.

- **Debrief Meeting**: The IRT discusses what went right, challenges faced, and potential improvements.
- **Documentation**: Maintain a detailed incident report, including timelines, affected systems, response actions, and findings for future reference.
- **Plan Update**: Based on learnings, update the incident response plan, protocols, and tools.