**INCIDENT RESPONSE**

**📌 What is Incident Response in a SOC?**

**Incident Response (IR)** in a **Security Operations Center (SOC)** is the **process of detecting, investigating, containing, and recovering from security incidents** such as cyberattacks, data breaches, or malware infections.

SOC teams follow a **structured approach** to minimize damage, restore normal operations, and prevent future incidents.

**📌 Why is Incident Response Important?**

✅ **Minimizes damage** from cyber threats (e.g., ransomware, phishing).  
✅ **Ensures quick recovery** to reduce downtime.  
✅ **Identifies root causes** to prevent similar attacks.  
✅ **Helps meet compliance** requirements (e.g., GDPR, NIST, ISO 27001).  
✅ **Improves security posture** by learning from past incidents.

**📌 6 Phases of Incident Response (NIST Framework)**

| **Phase** | **Description** |
| --- | --- |
| **1️⃣ Preparation** | Develop an **incident response plan (IRP)**, train staff, and set up tools (SIEM, EDR, IDS). |
| **2️⃣ Detection & Analysis** | Identify potential security incidents using logs, alerts, and threat intelligence. |
| **3️⃣ Containment** | Stop the spread of the attack (e.g., isolate infected devices, block malicious IPs). |
| **4️⃣ Eradication** | Remove malware, delete compromised accounts, patch vulnerabilities. |
| **5️⃣ Recovery** | Restore affected systems, monitor for any reinfection. |
| **6️⃣ Lessons Learned** | Document the incident, update security policies, improve defenses. |

**📌 Common Security Incidents in SOC**

🔴 **Malware Infection** → Ransomware, trojans, keyloggers.  
🔴 **Phishing Attack** → Employees tricked into revealing credentials.  
🔴 **DDoS Attack** → Overloading servers to disrupt services.  
🔴 **Unauthorized Access** → Hackers exploiting weak passwords.  
🔴 **Data Breach** → Sensitive data stolen by attackers.

**📌 Tools Used in Incident Response**

| **Tool** | **Purpose** |
| --- | --- |
| **SIEM (e.g., Splunk, QRadar, ELK)** | Detects suspicious activities & logs incidents. |
| **EDR (e.g., CrowdStrike, SentinelOne, Microsoft Defender)** | Monitors and responds to endpoint threats. |
| **IDS/IPS (e.g., Snort, Suricata, Zeek)** | Detects & blocks network intrusions. |
| **Threat Intelligence (e.g., VirusTotal, AlienVault OTX)** | Identifies known malware & attack patterns. |
| **Forensics Tools (e.g., Velociraptor, Volatility, Autopsy)** | Analyzes memory dumps & compromised systems. |

**📌 Example: Incident Response in Action**

**🚨 Scenario:** A **SOC alert** detects unusual outbound traffic from a workstation.

✔ **Step 1: Detect & Analyze** → Check SIEM logs for suspicious connections.  
✔ **Step 2: Contain** → Isolate the machine from the network.  
✔ **Step 3: Eradicate** → Scan for malware and remove it.  
✔ **Step 4: Recover** → Restore system from a clean backup.  
✔ **Step 5: Lessons Learned** → Update firewall rules, train employees on phishing awareness.

**📌 Key Takeaways**

✔ **Incident Response (IR)** = **Handling and mitigating security incidents in SOC**.  
✔ Follows a **structured 6-phase process** (NIST framework).  
✔ Uses **SIEM, EDR, IDS, Threat Intelligence, and Forensics tools**.  
✔ Helps **minimize damage, restore operations, and prevent future attacks**.

Would you like a **detailed Incident Response Playbook** for a specific attack scenario? 🚀