# Week 02: Theory Notes

## Alert Priority Levels:

SOC teams face alert overload (thousands/day). Without priority scoring, critical threats (e.g., ransomware encryption) may be buried under noise (e.g., routine scans). Prioritization ensures high-severity + high-impact alerts get the fastest response.

**Priority Categories:**

- **Critical** → Active exploitation with severe business impact (e.g., ransomware spreading on production servers).
- **High** → Unauthorized admin access, malware persistence attempts.
- **Medium** → Suspicious behavior with moderate risk (e.g., malware on a non-critical host).
- **Low** → Reconnaissance, failed logins, benign scans.

**CVSS 4.0:**

The **Common Vulnerability Scoring System (CVSS) v4.0** is the latest standard for evaluating the severity of vulnerabilities. It provides a numerical score (0.0–10.0) based on how easily a vulnerability can be exploited and the potential **impact on** confidentiality, integrity, and availability **(CIA)**. Unlike earlier versions, CVSS 4.0 introduces more flexibility and precision by adding threat metrics (exploit maturity, safety, and environmental context), which help SOC teams adapt scores to their own environment.

In practice, CVSS 4.0 separates metrics into:

- **Base Metrics** → inherent characteristics of the vulnerability (attack vector, complexity, privileges, user interaction, CIA impact).
- **Threat Metrics** → how actively the vulnerability is being exploited in the wild.
- **Environmental Metrics** → business-specific factors like asset criticality, safety implications, and organizational impact.

By combining these, analysts can move beyond a “one-size-fits-all” score and prioritize alerts more realistically. For example, a CVSS 9.8 vulnerability on a test VM may not be as urgent as a CVSS 7.5 on a production database server.

**Elements to Consider for Rating (CVSS v4.0):**

These are some of the important elements that we need to consider which rating an incident:

**1. Attack Vector (AV)**

- How an attacker reaches the target:
    - **Network (N)** → Exploitable remotely over the internet (highest risk).
    - **Adjacent (A)** → Exploitable on same subnet or VPN.
    - **Local (L)** → Requires access to system/console.
    - **Physical (P)** → Needs physical access (lowest risk).

**2. Attack Complexity (AC)**

- Extra conditions required for exploitation:
    - **Low (L)** → Easy to exploit, no special conditions (public exploit available).
    - **High (H)** → Requires specific setup, timing, or conditions.

**3. Privileges Required (PR)**

- **None (N)** → Attacker doesn’t need creds → more dangerous.
- **Low (L)** → User-level access required.
- **High (H)** → Already admin/root required → less impactful unless combined.

**4. User Interaction (UI)**

- **None (N)** → No action required (self-propagating malware, worms).
- **Required (R)** → User must click/download/open (phishing, malicious docs).

**5. Impact on CIA (Confidentiality, Integrity, Availability)**

- **Confidentiality (VC)**: Data exposure, leaks.
- **Integrity (VI)**: Unauthorized modifications.
- **Availability (VA)**: System/service downtime.
- Rated as **High (H), Low (L), or None (N)**.

**6. Scope (S)**

- **Unchanged (U)** → Attack only affects same security boundary.
- **Changed (C)** → Compromise extends to other components (e.g., exploit on VM escapes to hypervisor).

**Example CVSS 4.0 Rating:**

- Log4Shell (CVE-2021-44228).
- **Vector**: AV:N/AC:L/PR:N/UI:N/VC:H/VI:H/VA:H/S:U
- **Breakdown**:
  - Remote (Network) → accessible over internet.
  - Low Complexity → trivial exploit.
  - No Privileges → attacker doesn't need login.
  - No User Interaction → auto-triggered via logging.
  - High CIA Impact → data theft, modification, and denial possible.
- **Base Score**: 9.8 / 10 → **Critical**.
- **SOC Response**: Immediate patching, monitoring, and threat hunting.

## Incident Classification

Incident classification is the process of identifying and labeling security events based on type, impact, and context so that analysts can respond appropriately and consistently. Proper classification ensures faster triage, streamlined workflows, and accurate reporting.

**Core Elements:**

1. **Incident Categories**
   - **Malware:** Viruses, ransomware, trojans.
   - **Phishing:** Malicious emails with links/attachments (e.g., MITRE ATT&CK T1566).
   - **DDoS:** Flooding services to disrupt availability.
   - **Insider Threats:** Authorized users misusing access (e.g., data theft).
   - **Data Exfiltration:** Unauthorized transfer of sensitive data.
   - **Credential Compromise:** Stolen or brute-forced login details.
2. **Taxonomy Frameworks**
   - **MITRE ATT&CK:** Maps incidents to adversary tactics & techniques (e.g., phishing → Initial Access).
   - **ENISA Incident Taxonomy:** Standard categories for EU SOCs (e.g., system intrusion, availability issues).
   - **VERIS Framework:** Vocabulary for structured incident recording (actors, actions, assets, impact).
3. **Contextual Metadata**
   - **System Affected:** e.g., Production DB server vs. Employee laptop.
   - **Timestamps:** Timeline of malicious activity.

    - **Indicators of Compromise (IOCs):** IP addresses, file hashes, domains, registry keys.
    - **Business Impact:** Data loss, downtime, financial cost.

**Key Objective:**
To consistently **categorize and enrich incidents** with metadata, helping SOC teams align alerts with playbooks, prioritize response, and feed threat intelligence systems.

**Learning References:**

- **MITRE ATT&CK Navigator** → map incidents to tactics.
- **ENISA & VERIS documentation** → standard taxonomies.
- **Case Studies:** e.g., phishing campaigns in SANS Reading Room to practice classification.

## Basic Incident Response

**Definition:**
Incident Response (IR) is a structured process used by SOC teams to detect, contain, and recover from security incidents while minimizing damage and preventing recurrence.

**Phases of the Incident Response Lifecycle (NIST SP 800-61):**

1. **Preparation**
    - Develop playbooks and incident response plans.
    - Deploy monitoring tools (SIEM, EDR, IDS/IPS).
    - Train SOC analysts on common attack scenarios.
2. **Identification**
    - Detect anomalies via alerts (e.g., suspicious login attempts, malware execution).
    - Validate alerts to filter false positives.
    - Classify incidents (malware, phishing, DDoS, insider, etc.).
3. **Containment**
    - **Short-term:** Isolate infected endpoints (e.g., remove from network).
    - **Long-term:** Apply firewall rules, disable accounts, stop lateral movement.
4. **Eradication**
    - Remove malware, malicious accounts, or persistence mechanisms.
    - Patch exploited vulnerabilities.
    - Validate that threats are eliminated.
5. **Recovery**
    - Restore systems from clean backups.
    - Monitor for reinfection or anomalies.
    - Return systems to normal business operations.
6. **Lessons Learned**
    - Conduct a **post-mortem** (what worked, what failed).
    - Update playbooks, detection rules, and employee training.
    - Feed new IOCs and TTPs into threat intelligence systems.

**Procedures & Tools:**

- **Isolation:** Disconnect compromised host or segment network.

- **Evidence Preservation:** Collect memory dumps, disk images, and logs (hash for integrity).
- **SOAR Automation:** Tools like Splunk Phantom or TheHive streamline triage, response, and escalation.
- **Communication:** Maintain proper escalation channels (Tier-1 → Tier-2 → Incident Manager).

**Observation:**

Most incident response playbooks share a similar base structure — typically following the phases of detection, triage, containment, eradication, recovery, and lessons learned. While the framework and naming convention remain consistent across incidents, the specific actions taken within each phase differ depending on the type of attack (e.g., phishing vs. ransomware vs. insider threat). This ensures standardized workflow while allowing flexibility for tailored responses.

**Key Objective:**

To ensure SOC analysts can quickly detect, contain, and recover from incidents using a repeatable process that limits damage and strengthens defenses against future threats.

**Learning References:**

- NIST SP 800-61 (Computer Security Incident Handling Guide).
- SANS Incident Handler’s Handbook.