Week 2 Task: Report on a simulation on incident (Capstone) by Mohammed Touheed Patel

1. Alert Priority Levels

1.1 Understanding SOC Alert Prioritization

As a SOC analyst, it's crucial to evaluate alerts quickly and assign risk levels to ensure prompt attention where required. The main considerations for alert severity are **business impact**, **likelihood of exploitation**, and **system criticality**.

Severity Levels

Level	Description	Example
Critical	Ongoing or high-probability compromise, severe operational impact	Network-wide ransomware detected
High	Significant unauthorized activity, high risk but limited scope	Unauthorized admin login from TOR
Medium	Suspicious activity, mitigations possible, moderate risk	Macro malware in email attachment
Low	Low probability or impact, benign or preliminary reconnaissance	Continuous ICMP scan from subnet

Assignment Criteria

- **Asset value:** Is the affected host a production database or a test system?
- **Exploitability:** Does the incident relate to a CVE with public PoC or automated exploit kits?
- **Potential Impact:** Data breach, regulatory risk, financial impact.

Scoring Systems

- **CVSS (Common Vulnerability Scoring System):** Used to quantify vulnerability risk.

- CVSS Base Score, Temporal Score, and Environmental Score—refer to the [FIRST CVSS Guide] for metric details.

Example:

A CVSS 9.7 critical vulnerability (Spring4Shell, CVE-2022-22965) on a payment gateway server is assigned “Critical” priority, while a CVSS 5.6 vulnerability on an archived demo server is “Medium.”

1.2 Practical Alert Management (Google Sheets Example)

Alert Table (Fictitious Sample)

Alert ID	Type	CVSS	Priority	MITRE Tactic
1001	SQL Injection Attempt	8.5	High	T1190
1002	Phishing Email Detected	4.2	Medium	T1566
1003	Privilege Escalation	9.1	Critical	T1068
1004	Port Scan from External	2.6	Low	T1046

1.3 Incident Ticket

Example (TheHive or ServiceNow format)

Title: [Critical] Privilege Escalation Detected – WebSrv-Prod3

Description: Alert flagged a successful exploitation of local privilege escalation (T1068) by user svc_backup on WebSrv-Prod3. Forensic artifacts: suspicious binary /tmp/.escalate.sh, Source IP: 10.1.2.45.

Priority: Critical

Assigned To: Security Response Team

1.5 Escalation Email (SOC Tier 2)

Subject: Escalation: [Critical] Privilege Escalation on WebSrv-Prod3
Dear Tier 2 SOC Team,

A critical incident has been observed on WebSrv-Prod3, where a local privilege escalation exploit was detected. The incident involves user `svc_backup` and was traced to file `/tmp/.escalate.sh` from IP `10.1.2.45`. Host isolation is urgent to contain the threat. All relevant evidence, logs, and IOCs have been compiled in TheHive ticket. Further response actions are advised pending your review.

Regards,
Tier 1 SOC Analyst

2. Incident Classification

2.1 Understanding Incident Classes

- **Malware:** Unauthorized code execution or malicious software detected.
- **Phishing:** Deceptive emails intending credential theft or malware delivery.
- **DDoS:** Excessive illegitimate traffic to disrupt services.
- **Insider Threat:** Legitimate user misusing access for unauthorized data actions.
- **Data Exfiltration:** Sensitive information transferred to unauthorized third parties.

2.2 Use of Standardized Taxonomies

- **MITRE ATT&CK:** Assign tactic/technique for each incident (e.g., T1566 for phishing).
- **ENISA, VERIS:** Broader context and consistency across SOC reporting.
- **Enrich with metadata:** Attach affected device names, time of alert, user names, and IOCs.

Incident Classification Table (Sample)

Incident	Type	Technique	Host	User	IOC	Timestamp

INC-442	Phishing	T1566	HR-Laptop-2	jsmith	md5: a928...	2025-08-21 10:03:31

3. Basic Incident Response

3.1 Response Lifecycle

- **Preparation:** Build and maintain playbooks, contacts, and forensics toolkits.
- **Identification:** Confirm through alert triage or user reports.
- **Containment:** Unplug affected systems from the network ASAP.
- **Eradication:** Remove malware, revoke compromised creds, or block malicious traffic.
- **Recovery:** Restore operations/services, monitor for re-infection.
- **Lessons Learned:** Conduct post-incident reviews, update protocols and awareness.

Reference Templates:

- Used NIST SP 800-61 Phase Descriptions for documentation.
- Refered to the SANS Handler’s Handbook for step-by-step checklists.

4. Practical Applications

4.1 Build an Alert Classification Sheet (Google Sheets)

- Map sample alerts with unique IDs, types, assigned CVSS-based priorities, MITRE techniques, and statuses.
- Tag each alert for quick dashboard summary in Wazuh.

Example Sheet:

Alert ID	Threat Type	Priority	MITRE Tactic	Status
5012	Brute-force SSH	Medium	T1110	Open
5013	Macro Malware	High	T1204	Closed

4.2 Triage Table and Threat Intel Checking

- Use Wazuh to simulate "Brute-force SSH" alert from IP 172.16.100.50.
- Query this IP in VirusTotal and AlienVault OTX for threat reputation.

- Example documentation:

Alert ID	Description	Source IP	Priority	Status
5012	Brute-force SSH	172.16.100.50	Medium	Open

Threat Intel Summary (50 words):

IP 172.16.100.50 is flagged on OTX as an active brute-force attacker targeting multiple organizations. VirusTotal finds corresponding SSH dictionary attack patterns. Marked as True Positive. Recommend IP block at network perimeter and further monitoring for persistence.

4.3 Evidence Preservation, Chain of Custody Example

Item	Description	Collected By	Date	Hash Value (SHA256)
Volatile Memory	HR-Laptop-2 RAM Dump	SOC Analyst	2025-08-21	e1eaa...f55e8aa

All evidence preserved using FTK Imager and Velociraptor was hashed and documented for integrity and chain-of-custody compliance.

4.4 Capstone: Simulated Full Response Scenario

- Use Metasploit: exploit unix/webapp/file_upload on vulnerable test server LABWEB02.
- Detection: Wazuh flags alert for suspicious PHP shell upload, MITRE T1190.
- Response: Isolate LABWEB02; ban offending IP via CrowdSec.
- Document everything in a SANS-based IR report (see below).

Incident Report Format (Based on SANS Guidelines)

1. **Executive Summary:**
   On August 21, a file upload vulnerability was exploited on LABWEB02. Attack was detected instantly and neutralized with no production impact. Incident demonstrates importance of timely alerting and asset patching.
2. **Timeline:**

Time	Step	Details
09:31:00	Alert	Malicious upload detected
09:32:30	Validate	IOC matched MITRE T1190, PHP shell hash
09:33:00	Contain	Server isolated from network
09:35:00	Block	Attacker IP blacklisted in CrowdSec

3. **Impact Analysis:**
   Attack targeted a non-production learning server. No data loss occurred. Method could affect real assets if left unpatched.
4. **Recommendations:**
   Routine patching, regular alert tuning, security awareness for admins.

4.5 Stakeholder Briefing (Non-Technical 100 words)

On August 21, our monitoring detected, blocked, and contained an external hacking attempt exploiting a test web server. The system was promptly isolated, and no critical data was impacted. This event underscores our ability to detect and respond to threats in real time. Continued vigilance and regular staff training will be key in maintaining security across the organization.

5. Key Learnings

- Practical setup of Elastic SIEM and Kali VM
  I gained hands-on experience launching a cloud-based Elastic SIEM deployment, installing the Elastic Agent on Kali Linux, and enabling real-time security event collection.

- Event generation and log analysis
  Generating security events via Nmap and observing them directly in the SIEM environment helped me understand how network activity is captured, queried, and visualized—bridging the gap between theory and practice.

References

- https://www.youtube.com/watch?v=exKtmfQisaE
- Step-by-step GitHub guide: Elastic SIEM lab, agent install, log query, alerts
- YouTube walkthrough: SIEM lab setup, Nmap attack simulation, dashboard creation
- Beginner's setup guides with practical screenshots
- Draw.io