**SOC Analyst Practical Labs – Hands-On Training Report**

**1. Threat Hunting Practice**

**Tools Used:**

- Elastic Security
- Velociraptor
- AlienVault OTX

**Activities:**

- Developed a threat hunting hypothesis:
  **"Unauthorized privilege escalation in domain accounts."**
- Queried Event ID 4672 in Elastic Security to detect special privilege assignments.

| Timestamp | User | Event ID | Notes |
|---|---|---|---|
| 2025-08-18 15:00:00 | testuser | 4672 | Unexpected admin role |

- Used AlienVault OTX to search for **MITRE T1078** IOCs (e.g., compromised credentials, IPs).
- Cross-referenced IOCs with Velociraptor queries:

---

**2. SOAR Playbook Development**

**Tools Used:**

- Splunk Phantom
- TheHive
- Google Docs

**Activities:**

- Created an automated playbook for phishing alert response:
  - Check IP reputation
  - Block IP using CrowdSec
  - Generate TheHive case

| Playbook Step | Status | Notes |
|---|---|---|
| Check IP | Success | IP flagged as malicious |
| Block IP | Success | CrowdSec blocked 192.168.1.102 |

**Playbook Summary (50 words):**

A Splunk Phantom playbook was developed to automate the response to phishing alerts. It checks the IP reputation, blocks malicious addresses via CrowdSec, and creates a case in TheHive. Testing confirmed successful execution, enhancing response speed and reducing manual workload for SOC analysts.

---

**3. Post-Incident Analysis**

**Tools Used:**

- Google Sheets
- Draw.io

**Activities:**

- Conducted 5 Whys analysis for a mock phishing incident:

| Question | Answer |
|---|---|
| Why was email opened? | User clicked malicious link |
| Why clicked? | Weak email filtering |
| Why weak filtering? | Misconfigured rules |
| Why misconfigured? | No update process |
| Why no updates? | No patch management policy |

- Created a Fishbone Diagram in Draw.io identifying root causes (People, Process, Technology).
- Calculated:
    - **MTTD**: 2 hours

- **MTTR**: 4 hours

**Summary (50 words):**

A root cause analysis revealed that weak email filtering and lack of update processes led to phishing success. Using the 5 Whys and Fishbone Diagram, systemic gaps were identified. SOC metrics show a 2-hour detection and 4-hour response time, indicating moderate maturity in phishing incident handling.

---

**4. Alert Triage with Automation**

**Tools Used:**

- Wazuh
- VirusTotal
- TheHive

**Activities:**

- Triage of mock alert:

| Alert ID | Description | Source IP | Priority | Status |
|---|---|---|---|---|
| 005 | Suspicious Download | 192.168.1.102 | High | Open |

- Automated file hash lookup using VirusTotal via TheHive integration.

**5. Evidence Analysis**

**Tools Used:**

- Velociraptor
- FTK Imager

**Activities:**

- Used Velociraptor to query network connections:

```
SELECT * FROM netstat
```

- Identified suspicious remote connections.
- Maintained evidence chain-of-custody:

| Item | Description | Collected By | Date | Hash Value |
|---|---|---|---|---|
| Network Log | Server-Z Log | SOC Analyst | 2025-08-18 | [SHA256 hash] |

---

**6. Adversary Emulation Practice**

**Tools Used:**

- MITRE Caldera
- Wazuh

**Activities:**

- Simulated **MITRE T1566** (Spearphishing).
- Detection successfully triggered in Wazuh.

| Timestamp | TTP | Detection Status | Notes |
|---|---|---|---|
| 2025-08-18 17:00:00 | T1566 | Detected | Phishing email blocked |

**Summary Report (100 words):**

A spearphishing campaign was simulated using MITRE Caldera to emulate adversary behavior (T1566). The attack was successfully detected by Wazuh, confirming effective email and behavioral monitoring. The test revealed minor detection delays but no false negatives, validating SOC readiness for common phishing vectors.

---

**7. Security Metrics and Executive Reporting**

**Tools Used:**

- Elastic Security
- Google Sheets
- Google Docs

**Activities:**

- Created Elastic dashboard for:
    - MTTD: 2 hours

  - MTTR: 4 hours
  - False Positive Rate: 10%
- Calculated average dwell time: 6 hours

---

**8. Capstone Project: End-to-End SOC Incident Response**

**Tools Used:**

- Metasploit
- Wazuh
- CrowdSec
- TheHive
- Caldera
- Elastic Security
- Google Docs

**Activities:**

- **Simulated Exploit**:
  Used Metasploit's exploit/multi/samba/usermap_script on Metasploitable2.
- **Emulated TTP (T1210)** in Caldera

| Timestamp | Source IP | Alert Description | MITRE Technique |
|---|---|---|---|
| 2025-08-18 16:00:00 | 192.168.1.102 | Samba exploit | T1210 |

- Wazuh alerted on the intrusion; TheHive used for case triage.
- Attacker's IP blocked using CrowdSec.
- Automated response tested via playbook.
- RCA conducted using 5 Whys and Fishbone Diagram.
- Metrics gathered:
  - MTTD: 2 hrs

- MTTR: 4 hrs
- Dwell Time: 6 hrs