Notes

1. Objective

This notes contains the details of the task including Threat Hunting Methodologies, Advanced SOAR Automation, Post-Incident Analysis and Continuous Improvement, Adversary Emulation Techniques, and Security Metrics and Executive Reporting. The goal of this task is to:

- Develop skills to proactively identify threats using structured methodologies and data analysis.
- Build proficiency in automating repetitive SOC tasks to improve efficiency and response times.
- Master post-incident analysis to drive continuous improvement in SOC operations.
- Develop skills to simulate adversary behaviors to enhance SOC preparedness and validate controls.
- Build proficiency in measuring SOC performance and communicating results to leadership.

2. Introduction

Evidence preservation and analysis is a digital forensic process for performing Investigation it involves collection of evidence, preservation of evidence, and analyzing the evidence to know the attackers tactics, and techniques. Performing further legal proceedings.

3. Tools

- Velociraptor setup using its official documentation.
  https://docs.velociraptor.app/downloads/
- Elastic Security setup using documentation.
  https://www.elastic.co/docs/solutions/search
- TheHive setup using its official documentation.
  https://docs.strangebee.com/thehive/installation/installation-methods/
- CrowdSec setup using documentation
  https://docs.crowdsec.net/

4. Threat Hunting Methodologies

- **Proactive Threat Hunting:** Hypothesis-driven approach focusing on attacker TTPs.
  For example searching for TTPs like T1078 - Valid accounts misuse.
- **Reactive Threat Hunting:** Responding to the incident after it occurred. For example hunting privilege escalation in logs.

- **Frameworks:** SqRR (Search, Query, Retrieve, Respond), TaHiTI (Threat Intelligence integrated hunting) these frameworks are structured in a clean manner to provide guidance in threat hunting.
- **Data Sources:** EDR logs, network traffic, threat intelligence feeds, email security logs, and SIEM logs.
- **Goal:** Identify unknown and hidden threats proactively.
- **Learn From:** SANS Threat Hunting papers, Elastic Threat Hunting guide.

5. Advanced SOAR Automation

- **SOAR:** Security Orchestration, Automation, Response working together for efficiency.
- **Playbooks:** Automate repetitive SOC tasks like phishing, malware triage. A structured Automation work flow that decides when to trigger, what actions to take, and when to involve.
- **Integration:** Works best with SIEM + EDR for better decision making.
- **Learn From:** Splunk SOAR docs, TheHive playbook examples.

6. Post-Incident Analysis & Continuous Improvement

- **Post-Incident Analysis:** Analysts do post-incident to know what happened, how did analysts detect it, how did the attacker move, what failed, and how to stop next time.
- **Incident Reports and Knowledge Sharing:** Incident reports and knowledge sharing Helps everyone in the organization especially for analysts like what should be documented exactly, providing timelines, explaining impact and business risk, showing how the threat was stopped, and recommended improvements.
- **SOC Metrics and Maturity:** MTTD stands for Mean Time To Detect that means how much time it is taking to respond, MTTA stands for Mean Time To Acknowledge means the time taken to acknowledge when it detects the incident, Compliance, and Automation Coverage.
- **Learn From:** NIST SP 800-61, CISA Cybersecurity Metrics guides.

7. Adversary Emulation Techniques

- **Emulation:** Simulate realistic attacker TTPs (for example, Phishing T1566 or Valid accounts T1078) to test whether defenses detect and respond as expected. Run controlled scenarios that mirror attacker goals and constraints so blue teams face believable trade-offs and

noise. measure coverage gaps, false negatives, and response times to prioritize detection and remediation work.

- **Frameworks:** Use purpose-built platforms like MITRE Caldera to automate and scale emulation runs, chaining modules that represent adversary behaviors. Leverage community plugins, playbooks, and mappings to ATT&CK so emulations remain consistent and auditable. Automated frameworks make repeatable regression tests are possible and help track improvements across detection rules and controls.
- **Collaboration:** Pair red and blue teams in iterative exercises where red handoffs include telemetry and hypothesis details that blue can use to tune detections. Run post-exercise reviews that turn attack traces into concrete detection rules, playbooks, and prioritized engineering tickets. Shared metrics (dwell time, detection rate, mean time to respond) keep both teams aligned on realistic improvement goals.
- **Learn From:** MITRE Caldera docs, Red Canary emulation guides.

8. Security Metrics & Executive Reporting

- **Key Metrics:** Focus on measurable indicators like MTTD, MTTR, dwell time, and false positive rates to show how quickly and accurately threats are found and resolved. track trends over time to highlight whether tooling and process changes truly improve defensive posture. Tie alerts and incidents to severity so metrics reflect meaningful risk reduction, not just activity volume.
- **Purpose:** Translate technical SOC results into outcomes that matter to executives, like reduced business disruption and minimized regulatory exposure. Show where investments in tools or staffing are paying off and where gaps remain. Build trust by demonstrating accountability and continuous improvement across detection and response.
- **Reporting:** Use concise dashboards, heat maps, and timelines that spotlight what leadership

needs to act on, not raw event noise. Frame data with clear business context: financial impact, affected assets, and likelihood of recurrence. Include short narratives and recommended actions so decisions can be made swiftly and confidently.

- **Learn From:** SANS SOC reporting templates, CISA metric frameworks.