1. Objective

The objective of this exercise is to simulate real-world adversary techniques using adversary emulation tools and evaluate the effectiveness of SOC detection capabilities. The focus is on spearphishing attacks and validating detection through security monitoring systems.

2. Tools Used

- **MITRE Caldera** – Used to emulate adversary tactics, techniques, and procedures (TTPs)
- **Wazuh** – Used to detect and alert on malicious activities

3. Attack Scenario Overview

- **Attack Type:** Spearphishing
- **MITRE ATT&CK Technique: MITRE ATT&CK – T1566 (Phishing)**
- **Target System:** Windows Virtual Machine
- **Objective:** Test detection of phishing-related indicators and SOC alerting accuracy

4. Emulation Simulation

4.1 Emulation Setup

- MITRE Caldera was configured with a phishing-related ability aligned to **T1566**
- The simulation involved delivering a crafted phishing payload
- Wazuh was configured to monitor:
    - Email security logs
    - Endpoint process creation

- Suspicious file execution

4.2 Detection Results

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

4.3 Detection Analysis

- Wazuh successfully generated alerts based on phishing indicators
- Email filtering rules detected malicious content
- No user interaction with the phishing payload was observed

---

5. Emulation Report (100 Words)

The adversary emulation exercise successfully simulated a spearphishing attack using MITRE Caldera mapped to MITRE ATT&CK technique T1566. Wazuh effectively detected the phishing attempt through email security monitoring and endpoint alerting mechanisms. The attack was blocked before user interaction, demonstrating strong preventive and detective controls. However, limited visibility was observed in user behavior analytics, indicating a detection gap if phishing bypasses email filters. Future improvements include enhancing endpoint telemetry, integrating sandbox analysis for email attachments, and expanding correlation rules to detect delayed or user-triggered phishing activity. Overall, the SOC demonstrated effective initial detection with minor areas identified for enhancement.