Adversary Emulation Practice – Spearphishing Simulation (T1566)

Adversary emulation was conducted to test SOC detection capabilities against spearphishing techniques. Using MITRE Caldera, a simulated spearphishing scenario aligned with **MITRE ATT&CK technique T1566 (Phishing)** was executed to evaluate monitoring and alerting effectiveness.

The emulation scenario involved delivery of a malicious email payload designed to trigger endpoint activity and generate detection logs within the SIEM environment.

Detection Results

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

Wazuh successfully generated an alert upon detection of suspicious email behavior and associated endpoint activity. The alert was classified as High severity and reviewed by SOC analysts.

Emulation Report

The adversary emulation exercise demonstrated effective detection of spearphishing activity aligned with MITRE ATT&CK technique T1566. Wazuh generated timely alerts upon identifying suspicious email behavior and endpoint indicators. While detection controls functioned properly, analysis revealed potential improvement areas, including faster automated containment and enhanced user awareness training. The exercise validated SOC monitoring capabilities and highlighted the importance of continuous adversary emulation to identify detection gaps, refine alert rules, and strengthen defensive posture against phishing-based attacks.