Adversary Emulation Report: T1566 Spearphishing Simulation

This adversary emulation exercise utilized **MITRE Caldera** to simulate the **Spearphishing (T1566)** technique against the security stack monitored by **Wazuh**. The primary objective was to validate the Security Operations Center's (SOC) capability to detect initial access vectors.

The simulation, logged on 2025-09-27, was **successful** at the initial detection phase, with the malicious email being blocked and noted in the Wazuh logs. This confirms robust **email gateway** and **endpoint protection** against this specific initial access method.

However, the emulation highlighted a potential **detection gap** in post-compromise lateral movement visibility. While the initial threat was contained, the simulation did not test the system's ability to detect the *execution* of a potential payload or subsequent persistence techniques had the email *not* been blocked. Future emulation should focus on a full kill-chain sequence to fully test **behavioral analysis** and **endpoint detection and response (EDR)** capabilities.