Adversary Emulation

The adversary emulation of T1566 (Spearphishing) was conducted using MITRE Caldera to simulate phishing-based payload execution within a monitored environment. Wazuh successfully detected suspicious script execution and abnormal process creation activity associated with the simulated attack. However, the initial phishing vector itself was not directly identified due to limited email telemetry integration. Encoded command activity was only partially logged, reducing visibility into obfuscated payload behavior. Alert severity required manual analysis, and no automated response action was triggered. The exercise revealed detection gaps in email monitoring, command-line logging depth, and correlation rule tuning, highlighting areas for improved monitoring and response capability.