# Capstone Incident Report

Executive Summary: On 2025-08-18 we conducted a controlled SOC capstone simulation combining an adversary emulation and exploitation sequence to exercise detection, automation, escalation, and post-incident analysis. The simulation used two concurrent TTPs: a spearphishing vector (MITRE T1566) to obtain initial access and a subsequent Samba usermap exploit (MITRE T1210) to attempt lateral movement. Detection: Wazuh generated alerts for suspicious email delivery patterns and the exploit activity; threat intelligence enrichment flagged external IPs as malicious, and the SOAR playbook auto-blocked identified C2 IPs. Response: Tier 1 triaged and escalated confirmed malicious activity to Tier 2 in TheHive. CrowdSec was invoked to block attacker IPs and the affected VM was isolated. Post-Incident: A rapid RCA using the 5 Whys identified gaps in email filtering and a missing enrichment rule; a fishbone diagram captured contributing factors across People, Process, and Technology. Metrics: MTTD observed 2 hours, MTTR 4 hours, dwell time estimated 6 hours. Recommendations included integrating additional telemetry, improving playbook coverage for chained TTPs, and scheduling targeted training. Conclusion: The exercise validated core SOC capabilities, highlighted automation strengths, and produced prioritized remediation actions to reduce detection windows and prevent similar attack chains. Detailed artifact collection included memory and network captures stored with documented chain-of-custody; artifacts were hashed (SHA256) and retained for analysis. A follow-up plan schedules a re-test after implementing improved detection rules and playbook updates to confirm closure of identified gaps.