Briefing: Capstone Project

On 18 September 2025, our team ran a controlled security exercise to test the SOC's ability to detect and respond to a real attack. A known Samba vulnerability was used to compromise a test server. Our monitoring system (Wazuh) quickly detected the attack, and the compromised machine was isolated to prevent further risk. The attacker's IP was blocked using automated protection tools, and a case was escalated for deeper forensic review. No production systems were affected. This exercise confirmed that our detection, containment, and escalation processes are effective, and highlighted areas for continued improvement and automation.