Incident Report

Executive Summary

On **August 18, 2025**, the Security Operations Center detected a simulated exploitation attempt against a vulnerable Samba service on an ip 192.168.159.138. The activity was identified by Wazuh and confirmed as a true positive through log analysis. The incident was quickly contained and escalated for further review. No sensitive data or production systems were impacted.

Timeline (UTC)

- **2025-08-18 14:00 UTC** – Exploitation activity initiated against the Samba service
- **2025-08-18 14:01 UTC** – Wazuh generated a high-severity alert mapped to MITRE T1210
- **2025-08-18 14:05 UTC** – SOC analyst validated the alert as a true positive
- **2025-08-18 14:10 UTC** – Affected virtual machine isolated and attacker IP blocked using CrowdSec
- **2025-08-18 14:15 UTC** – Incident escalated to Tier 2 via TheHive

Recommendations

Vulnerable services such as Samba should be patched, hardened, or disabled if not required. Network segmentation and host-isolation controls should be strengthened. Continuous monitoring and alert tuning within Wazuh should be maintained to ensure early detection and rapid response to similar exploitation attempts.