Title: Executive Briefing (150 words)

Summary

A simulated cyberattack targeting a vulnerable Samba service was detected and contained by the SOC. The attack originated from IP 192.168.1.102 and attempted remote exploitation. Wazuh alerted analysts within two hours (MTTD), and automated playbooks in TheHive initiated IP blocking through CrowdSec, reducing response time to four hours (MTTR). Although containment was successful, the investigation revealed that the vulnerable system was missing from the asset inventory, allowing the exploit to succeed. The incident underscores the need for stronger asset visibility, improved patch management, and expanded SOAR automation. Future enhancements—including automated asset discovery and additional behavioral detection rules—will reduce exposure, minimize dwell time, and strengthen the organization's resilience against similar threats.

Key metrics:

- **MTTD: 2 hours**
- **MTTR: 4 hours**
- **Dwell time: ~6 hours**