

Capstone Incident Report

Executive Summary: Simulated Samba exploit detected by Wazuh.

Timeline: Attack detected at 14:00, blocked by CrowdSec.

Recommendations: Apply patches, enable anomaly monitoring.

Incident demonstrated full SOC workflow.