INCIDENT REPORT

Executive Summary:

On September 12, 2025, our network detected a potential Samba backdoor exploit targeting 192.168.1.36. The exploit, leveraging the Metasploit usermap_script module, was identified through Zeek network monitoring and corroborated by Wazuh logs. Immediate containment actions were initiated using CrowdSec, preventing further compromise. No critical data exfiltration was observed, and the incident was contained within minutes of detection.

Timeline of Events:

- 16:47: Zeek detected unusual SMB traffic from 192.168.1.39 to 192.168.1.36.
- 16:48: Metasploit exploitation attempt successfully executed in a lab environment.
- 16:49: Zeek triggered a custom notice (Samba_Backdoor) logged in Kibana.
- 16:51: Case created in TheHive, observables added, and containment task executed.
- 17:30: CrowdSec firewall bouncer blocked the malicious IP.
- 17:32: Incident marked as contained; no lateral movement detected.

Root Cause Analysis (RCA):

The incident originated from an external test host exploiting the Samba usermap_script vulnerability. The attack leveraged legacy SMB functionality exposed on the target system. Lack of continuous SMB vulnerability monitoring delayed automated detection until Zeek custom scripting captured the exploit attempt.

Recommendations:

- Patch Management: Apply Samba security updates and disable legacy scripts where possible.
- Network Segmentation: Restrict SMB access to authorized hosts only.

- Automated Containment: Enhance integration between Zeek, TheHive, and CrowdSec for real-time response.
- Monitoring & Metrics: Implement dashboards to track MTTD, MTTR, and dwell time for all criticl alerts.
- Training & Playbooks: Maintain up-to-date incident response playbooks for known SMB exploits.