Post-Mortem Summary: SMB Brute-Force Incident

File Name: 2.4_Post-Mortem_Summary.pdf
Prepared by: Abhishek Tiwary – SOC Analyst (Tier 1)
Date: 11 Oct 2025

Post-Mortem: Lessons from SMB Brute-Force

The automated containment via CrowdSec proved highly effective, instantly banning the attacker and confirming successful containment (**Time to Contain: under 45 seconds**). This validates our SOAR capability. However, Velociraptor acquisition failed due to VM kernel incompatibility, severely limiting forensic evidence. Future priority must shift to **asset inventory validation** and using **stable Windows 10/11 evaluation images** for IR tooling reliability.

Purpose of This Draft

Objective	Explanation
Acknowledge Success	CrowdSec automation worked effectively, providing rapid containment and validating SOAR readiness.
Acknowledge Failure	Velociraptor evidence collection failed due to VM kernel compatibility issues.
Focus on Improvement	Future IR environments must ensure validated asset inventories and stable Windows evaluation images for reliable forensic tooling.