Document 3: Escalation Summary Task 3.1

A. Document Name

Task 3 : Incident Escalation Summary (Tier 2 Handover)

B. Purpose

This summary serves as a Tier 1 Analyst handover note to the Tier 2 team in TheHive, providing details of the simulated Capstone attack involving a reverse shell. It includes detection evidence, initial containment actions, and recommendations for deeper investigation.

C. Summary (100 Words)

Incident Summary: Critical Reverse Shell Foothold – Win10-Victim

A high-priority alert was triggered on Server-Y following unauthorized login activity at 2025-08-18 13:00 from IP address 192.168.1.200. The event maps to MITRE technique T1078 (Valid Accounts) and indicates the possible use of stolen or misused credentials. Initial containment steps included isolating Server-Y from the network, blocking the suspicious IP, and verifying that no lateral movement occurred. Log analysis suggests repeated login attempts across multiple accounts. Due to the severity, potential credential compromise, and risk of privilege escalation, this case is being escalated to Tier 2 for deeper investigation, forensic triage, and further containment actions.