Title: Alert Triage with Automation – Full Report

Date: 24 Nov 2025
Prepared by: Mayuri Sawle

Objective

This document includes all sections: triage table, automation summary, and references.

Triage Simulation

Alert Details:

Alert ID	Description	Source IP	Priority	Status
005	File Download	192.168.1.102	High	Open

Summary (50 words)

Automation was configured in TheHive to automatically submit file hashes to VirusTotal during alert creation. The integration enabled rapid reputation checks, identifying whether the downloaded file was malicious, suspicious, or benign. This reduced analyst workload, improved accuracy, and accelerated triage decisions, resulting in faster containment and improved SOC efficiency.