ALERT TIAGE WITH AUTOMATION

Summary

Alert 005 was triggered for a suspicious file download originating from IP 192.168.1.102, marked as high priority. The file's SHA256 hash **e3b0c44298fc1c149afbf4c8996fb924** was extracted from the ELK alert and manually checked on VirusTotal, which provided threat intelligence including detection ratio and related metadata. Based on this information, a case was manually created in TheHive, with the hash added as an artifact and the alert details documented. This process effectively simulates automated triage and validation, ensuring that threat intelligence is applied to evaluate potential risks before further analysis.