IOC Validation Report

Incident: Malware Download Alert
Objective: Validate whether the alert is real or false positive using threat intelligence.

IOC Validation Table

IOC	Platform Used	Result Summary	Decision
Hash 44d8861…	VirusTotal	Marked malicious by many security vendors	Valid Alert (not false positive)
Hash 44d8861…	VirusTotal	Marked malicious by vendors	Valid Alert
VT/TI Detail:		File is a Ransomware X dropper. First seen: 2025-12-01.	True Positive

Context:

- **Source:** EDR/Network Gateway
- **Time:** YYYY-MM-DD HH:MM:SS
- **Asset/User:** Hostname/IP / User ID
- **Malware:** (e.g., Emotet)

Network Traffic: C2 domain/IP

Summary

Threat intelligence confirms the file hash is associated with known malware. The alert is valid and requires immediate incident response.**Recommended Actions**

- **Escalate** to Incident Response Team (Level 2/3 Analyst).
- **Isolate** the affected host (WKSTN-HEMANTH-PC).
- **Perform** forensic image and malware analysis.
- **Block** the malicious hash and associated C2 indicators on perimeter devices.