Endpoint Antivirus Event Triage

Summary

This checklist is designed for enterprise IT teams.

Initial Triage

* Validate alert source and timestamp
* Identify affected device and user
* Determine malware family or signature

Containment

* Isolate device if high risk
* Block malicious hash or URL
* Notify SOC or IT security

Investigation

* Collect logs and process details
* Review recent user activity
* Check for lateral movement

Resolution

* Remove or quarantine artifacts
* Re-scan and validate clean status
* Document findings and close ticket