**Standard Operating Procedure: Kaspersky Endpoint Security Management**

**Prepared by: Chetan Sai C**

**1. Objective**

To ensure the continuous protection and operational integrity of all endpoints using Kaspersky Endpoint Security by regularly monitoring, analysing, and responding to threats and vulnerabilities.

**2. Scope**

Applies to all systems and endpoints in the organization where Kaspersky Endpoint Security is deployed. The SOP is applicable to the SOC team and system administrators.

**3.Kaspersky Dashboard**

The Kaspersky Security Centre Dashboard provides a centralized view of your endpoint security posture. It offers real-time insights and visual summaries about threats, protection status, device health, and administrative tasks.

A screenshot of a computer

AI-generated content may be incorrect.



**Kaspersky Reports**

Reports” section in Kaspersky Security Centre gives detailed insights into various aspects of your endpoint environment. It’s used for auditing, incident response, compliance, and weekly/monthly reporting.

1. **Threat Reports**

Provides insight into detected malicious activity.

* **Detected Threats**: Lists all malware, Trojans, spyware, ransomware, etc.
* **Not Processed**: Threats that could not be cleaned or require manual action.
* **Date & Time of Detection**
* **Affected Hostnames**
* **Threat Category** (e.g., Trojan, Worm, PUA)
* **Action Taken** (Quarantined, Deleted, Failed)
* **Detection Source**: Email, USB, network, web, etc.

**2. Infected Devices Report**

Shows machines that were impacted by malware.

* **Device Name / IP Address**
* **Threat Count**
* **Status** (Cleaned, partially cleaned, Not cleaned)
* **User Logged In**
* **Last Detection Time**

**3. Vulnerability Reports**

Lists OS or application vulnerabilities found via Kaspersky scan.

* **CVE ID / Vulnerability Title**
* **Severity (Low/Medium/High/Critical)**
* **Affected Application or OS**
* **Number of Devices Affected**
* **Remediation Status** (Pending, Installed, Ignored)

A screenshot of a computer

AI-generated content may be incorrect.

In Kaspersky Security Center, under Monitoring & Reporting > Event Selections, you’ll find several predefined event categories. These are designed to help security teams quickly filter and monitor key security events across the network.

Here’s what each of those sections typically means:

1. **User Requests (Predefined selection**): Events generated by user actions through the Kaspersky endpoint agent or Security Center. Examples: Manual scan started by user tried to pause protection User requested to unblock a website or application Use Case: Monitor if users are bypassing or interacting with security settings.

**2.Recent Events (Predefined selection):** A summary of all recent security events, regardless of category. Examples: Threats detected Task executions Update results

Use Case: Quick snapshot of what's happened across your environment in the last few hours or days.

3. **Audit Events (Predefined selection):** Administrative actions and changes within Kaspersky Security Center Examples: Policy changed new device group created User login/logout from console

Use Case: Useful for internal auditing and change tracking for compliance.

4. **Info Events (Predefined selection)**: General informational logs not necessarily tied to security incidents. Examples: Update completed successfully Scan finished with no threats Use Case: For tracking routine system activities and confirming successful operations.

5. **Critical Events (Predefined selection)**: Events that indicate serious security risks or system issues. Examples: Active malware infection not neutralized Failed security update Agent disabled or stopped Use Case: High-priority alerting; needs immediate attention or escalation.

6. **Warnings (Predefined selection**): Medium severity events that may lead to issues if not resolved. Examples: Signature database outdated License nearing expiration Scans skipped or incomplete Use Case: Early detection of problems before they become critical.

7. **Functional Failures** (Predefined selection): Failures in Kaspersky functions or scheduled tasks. Examples: Patch management task failed Update task failed Deployment errors

A screenshot of a computer

AI-generated content may be incorrect.

**Monitoring & reporting Alerts**

In Kaspersky Security Center, the Monitoring & Reporting > Alerts section is used to display and manage real-time alerts generated from across the Kaspersky environment. These alerts are critical for incident response, monitoring system health, and identifying misconfigurations or infections.

A screenshot of a computer

AI-generated content may be incorrect.

**Integrating Kaspersky Security Center with Wazuh**

We can follow the steps outlined in the blog mentioned below to integrate Kaspersky Security Center with Wazuh and successfully receive Kaspersky logs into the Wazuh Manager for centralized monitoring and alerting.

<https://medium.com/@yury.xisto/integrating-kaspersky-security-center-withwazuh-6f4468292e24>