

Author: P. Rajeev

Date: 04-11-2025

Alert Management Practice

1.Alert Classification System

An **Alert Classification System** is a method used in cybersecurity monitoring (like in **Wazuh**, **TheHive**, or **SIEMs**) to organize and prioritize security alerts based on their type, severity, and context.

It helps analysts quickly determine which alerts need immediate attention and which can be handled later or automatically.

Here created a google sheets table with the data includes alert ID, type, priority, and MITRE Tactic.

Alert ID	Type	Priority	MITRE Tactic
001	Log4Shell Exploit	Critical	T1190
002	Ransomware	Critical	T1486
003	Phishing	High	T1110
004	Command and Scripting Interpreter	High	T1059
005	Brute-Force SSH	Medium	T1130
006	Encryption of Data for Impact	Medium	T1486
007	Port Scan	Low	T1046
008	Remote System Discovery	Low	T1018

1.1 Testing with a Mock Alert

Testing a mock alert like “**Phishing Email: Suspicious Link**” involves analyzing the alert, determining its severity and type, classifying it under Phishing (High Priority), mapping it to MITRE ATT&CK T1110, and updating the Alert Classification Table for proper tracking and response.

Alert ID	Type	Priority	MITRE Tactic
009	Phishing	High	T1110

2. Prioritize Alerts

Prioritizing alerts involves ranking them based on their impact and severity using the CVSS (Common Vulnerability Scoring System). Simulated alerts such as “Critical: Log4Shell Exploit Detected” and “Low: Port Scan” are analyzed and scored in Google Sheets. For example, Log4Shell (CVSS 9.8) is categorized as Critical, requiring immediate action.

This process helps analysts evaluate the risk, assign response urgency, and update the alert table accordingly to ensure that the most severe threats are addressed first.

Example: Log4Shell CVSS 9.8 = Critical.

CVSS means Common Vulnerability Scoring System that helps to rank the alerts then analyze, react to the alerts based on the CVSS.

CVSS Score	Priority Level	Action
9.0–10.0	Critical	Immediate action required
7.0–8.9	High	Containment is required quickly
4.0–6.9	Medium	Investigate and then schedule remediation
0.0–3.9	Low	Triage when time permits

Prioritizing alerts is done based on the CVSS score, which is calculated by summing up three key factors:

1. asset criticality
2. exploit likelihood
3. business impact.

The formula used is:

$$\text{CVSS score} = \text{Asset Criticality} + \text{Exploit Likelihood} + \text{Business Impact}$$

For example, consider the critical Log4Shell exploit alert. Here, the asset is a production database with a score of 3, the exploit likelihood is public proof of concept (POC) with a score of 2.8, and the business impact is 4. Adding these gives a total CVSS score of 9.8, which classifies the alert as critical.

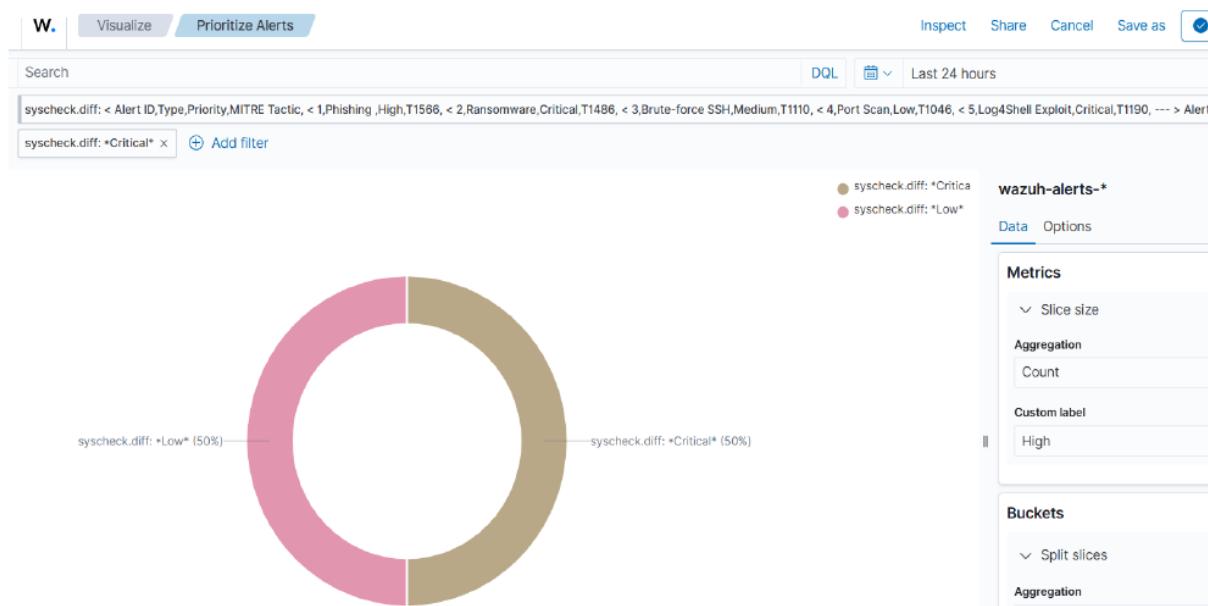
All other alerts are similarly evaluated and ranked based on this formula to determine their priority levels.

Alert ID	Type	Priority	MITRE Tactic	CVSS Score
001	Log4Shell Exploit	Critical	T1190	9.8
002	Ransomware	Critical	T1486	9.2
003	Phishing	High	T1110	8.9
004	Command and Scripting Interpreter	High	T1059	8.2
005	Brute-Force SSH	Medium	T1130	6.5
006	Encryption of data for impact	Medium	T1486	5.8
007	Port Scan	Low	T1046	0.1
008	Remote System Discovery	Low	T1018	0.1

3.Dashboard Creation

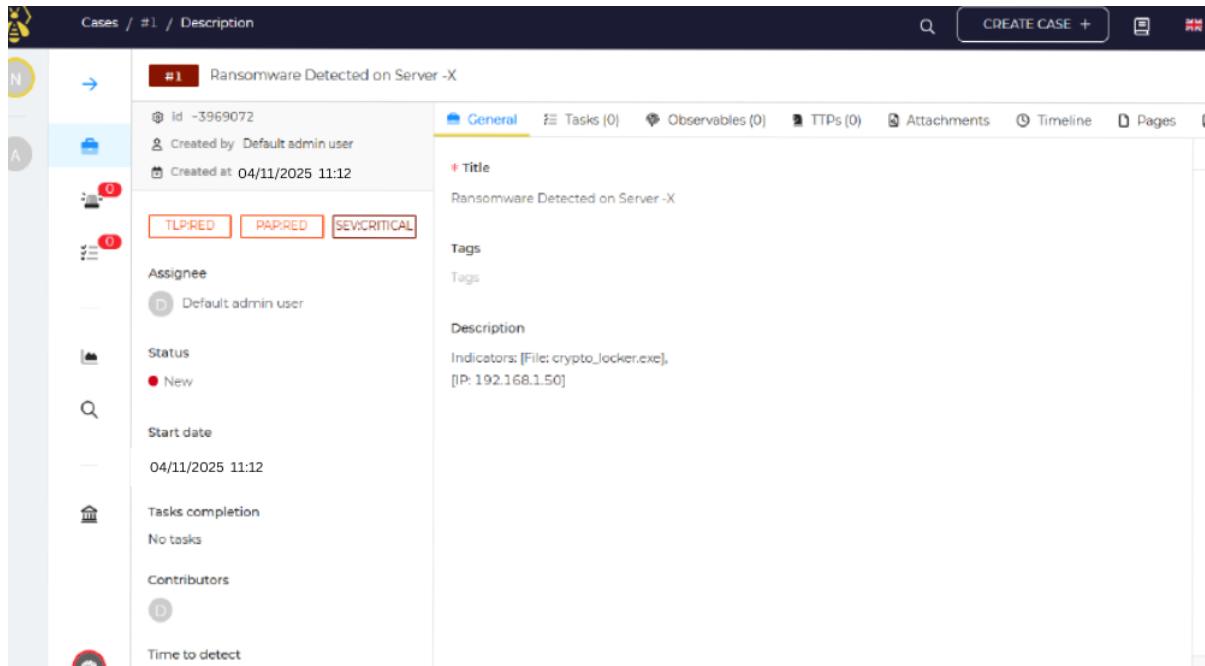
Dashboard creation in Wazuh involves building visual charts, such as a pie chart, to display alert priorities like critical, high, medium, and low. It uses data from the alert classification table to help analysts quickly identify and focus on the most severe alerts for faster incident response.

Here a dashboard is created in Wazuh SIEM tool that includes creation of pie chart to visualize priority of alert for this analyzed the alerts classification table.



4.Incident Ticket

Incident ticket creation in TheHive involves documenting alert details for tracking and response. A ticket is drafted with fields such as title, description, priority, and assignee. For example, the ticket titled “[Critical] Ransomware Detected on Server-X” includes indicators like the file “crypto_locker.exe” and the IP “192.168.1.50.” The priority is marked as critical, and it is assigned to a SOC analyst for immediate investigation and remediation.



The screenshot shows a case entry in the CYART system. The title of the case is "#1 Ransomware Detected on Server -X". Key details include:

- General:** ID: -3969072, Created by: Default admin user, Created at: 04/11/2025 11:12.
- Severity:** TLP:RED, PAP:RED, SEV:CRITICAL.
- Assignee:** Default admin user.
- Status:** New.
- Description:** Indicators: [File: crypto_locker.exe], [IP: 192.168.1.50].
- Tags:** None listed.
- Timeline:** No tasks, no contributors, and no time to detect.

5.Escalation Role-Play

Escalation role-play involves simulating the process of reporting a critical security incident from the Tier 1 SOC analyst to the Tier 2 team. When a high-severity alert, such as a ransomware attack, is detected, the Tier 1 analyst summarizes the incident details and Indicators of Compromise (IOCs) in an email and escalates it for advanced investigation. This step ensures quick communication, faster response, and proper documentation of the event, enabling Tier 2 analysts to perform deeper analysis, containment, and recovery actions efficiently.

Subject: [CRITICAL] Ransomware Incident Detected on Server-X

Dear Tier 2 Team,

We have detected a critical ransomware incident on **Server-X (192.168.21.10)**. The initial alert shows the presence of a malicious file **crypto_locker.exe**, and the attacker's source IP is **192.168.1.50**. The affected server has been isolated to prevent further spread and data encryption. Immediate analysis and containment are required to verify the extent of compromise and restore affected systems.

Please review the incident details in TheHive ticket **TICKET-001** and take necessary action to ensure network integrity.

Regards,

Rajeev

Tier 1 SOC Analyst