Alert Management Practice

1. Alert Classification System

Alert classification system that means separation of alerts based on its priority and later mapping it to the MITRE ATT&CK techniques. 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 Mock Alert

Testing mock alert (e.g., “Phishing Email: Suspicious Link”). It includes analysis of alert determining its priority, and classifying it using MITRE ATT&CK framework and updating it in the alert classification table.

Alert ID	Type	Priority	MITRE Tactic
009	Phishing	High	T1110

2. Prioritize Alerts

Prioritize alerts means ranking the alerts based on its impact on finance or business it is important to prioritize alerts that helps in taking the action or to escalate it to the tire 2 team. Simulation of alerts (e.g., “Critical: Log4Shell Exploit Detected” vs. “Low: Port Scan”) and score using CVSS in google sheets. 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 permit

Prioritizing alerts based on the CVSS score along with Asset, Business impact then sum it later compare it with the CVSS and prioritize alert. Formula to find the CVSS score

CVSS score = Asset Criticality + Exploit Likelihood + Business Impact.

Example: Critical: Log4Shell Exploit

Asset = Production database score (3)

Exploit Likelihood = Public POC (2.8)

Business Impact = 4

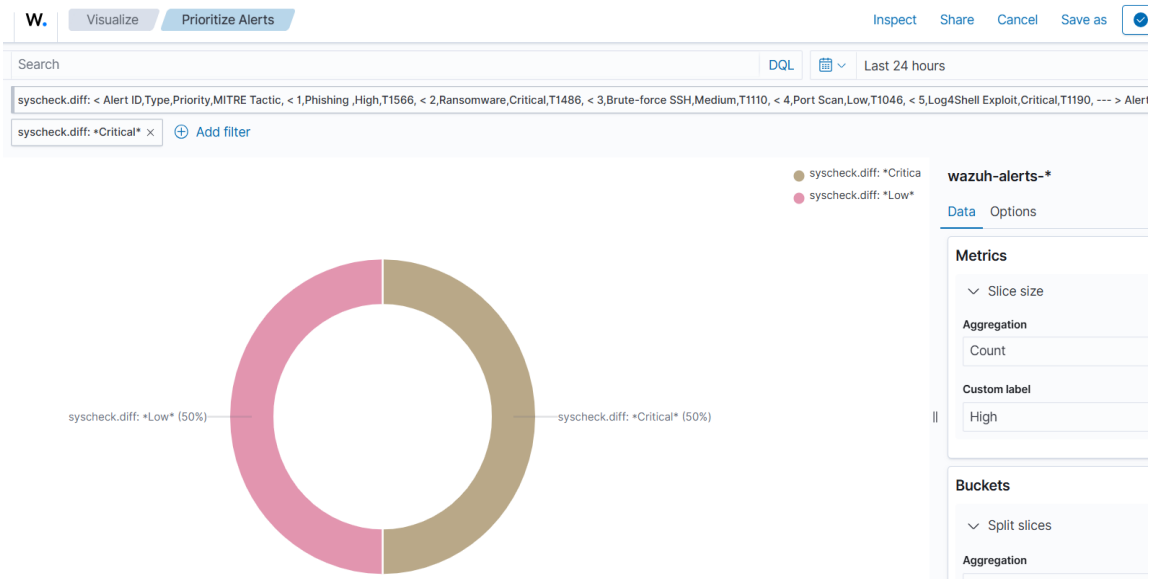
Total = 3 + 2.8 + 4 = 9.8 according to CVSS it’s priority is Critical.

remaining all other alerts given ranking based on this formula only.

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

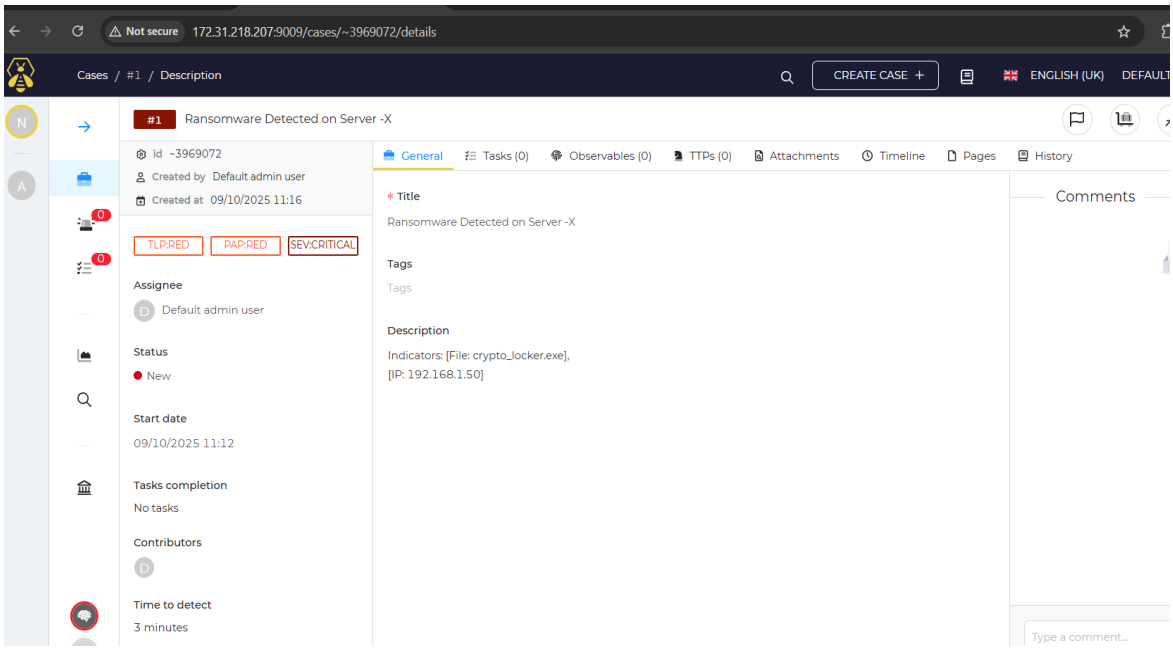
3. Dashboard Creation

Dashboard creation in Wazuh SIEM tool creation of dashboard to visualize alert priorities (e.g., pie chart for Critical vs. High alerts). 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 includes the fields like title, description, priority, and assignee. Incident ticket used as a record for the incident it includes details that helps to analyze and resolve the problems in the IT services and also it is escalated to tire2 team and other higher officials to resolve the issue if it requires higher authorities.



5. Escalation Role-Play

Escalation role-play that comes into the part when the attacks priority is critical and the immediate action required means the tier1 analyst will escalate it to tier2 team by summarizing the incident along with IOCs.
Below provided email is an example of escalating the incident happened to the tire 2 team.

Escalating a critical incident to the tire 2 team

Subject: [CRITICAL] URGENT: Active Ransomware Incident on Server-X

Body:

Tier 2 Team,

We are escalating a Critical incident that is an active ransomware detected on Server-X (192.168.21.10).

The initial alert shown the presence of a malicious file, that is a crypto_locker.exe. The suspected attacker's source IP address is detected as 192.168.1.50.

Action Taken: The affected asset, Server-X, has been successfully isolated from the network to prevent further data encryption and lateral movement.

We require immediate Tier 2 team for deeper analysis, eradication, and confirmation of backup integrity. The full incident ticket in TheHive is **TICKET-001**. Please take action immediately.

Thanks,
Kartheek
Tier 1 SOC Analyst.