Alert Management Practice

1. Alert Classification System

An alert classification framework that categorizes alerts by priority and links them to the MITRE ATT&CK techniques. For this, a Google Sheets table was created with columns for 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	Port Scan	Low	T1046
005	Remote System Discovery	Low	T1018
006	Encryption of data for impact	Medium	T1486
007	Command and Scripting Interpreter	High	T1059
008	Brute-Force SSH	Medium	T1130

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

Prioritizing alerts involves ranking them by their financial or business impact. This ensures the most significant alerts prompt action or escalation to the Tier-2 team. For simulation, alerts such as 'Critical: Log4Shell Exploit Detected' versus 'Low: Port Scan' are scored using the Common Vulnerability Scoring System (CVSS) within Google Sheets—e.g., Log4Shell has a CVSS 9.8, so it's deemed Critical. CVSS provides a standardized framework to assess, rank, and respond to alerts effectively.

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)

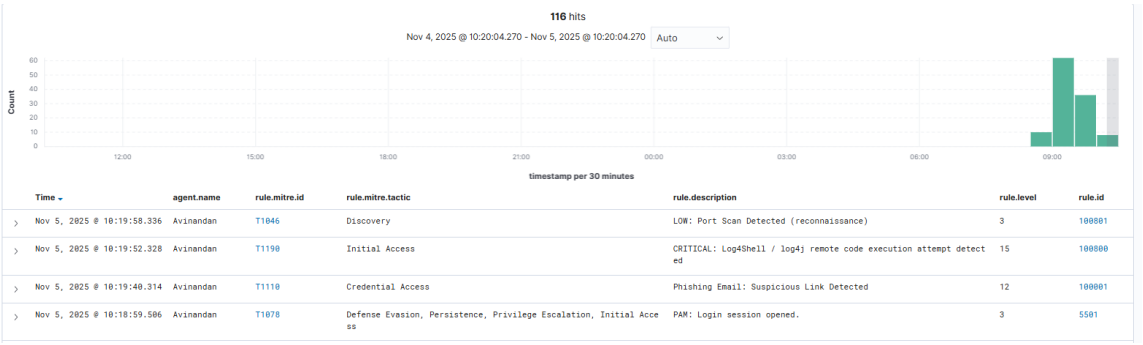
Business Impact = 4

Total = 3 + 2.8 + 4 = 9.8 according to CVSS its 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

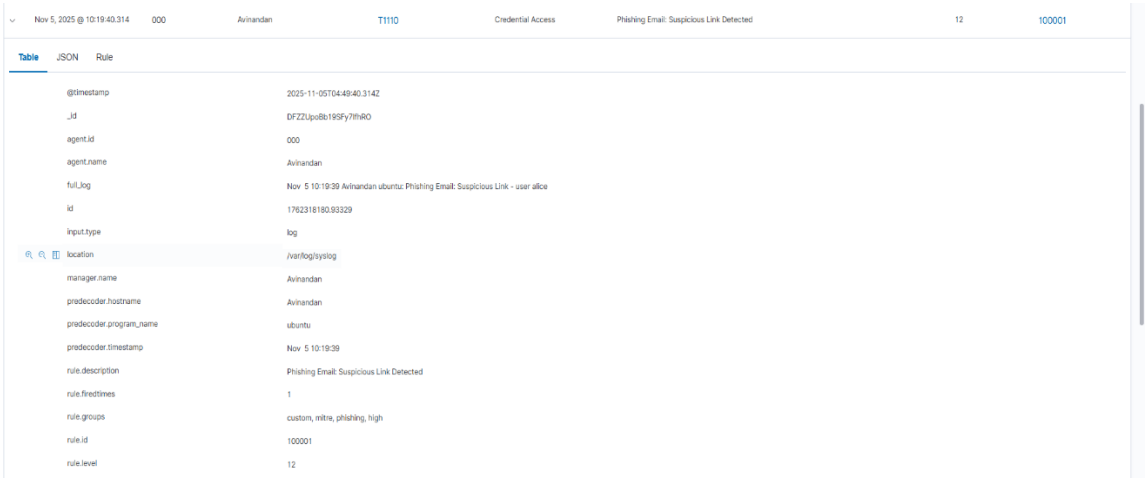
3. Dashboard Creation

The process starts on the main security dashboard. This screen gives a high-level overview of "116 hits" shown on a timeline. The table below lists alerts, allowing you to quickly identify high-priority threats like a **"CRITICAL: Log4Shell"** attempt (level 15) and a **"Phishing Email"** (level 12) alongside lower-level noise like a **"Port Scan"** (level 3).

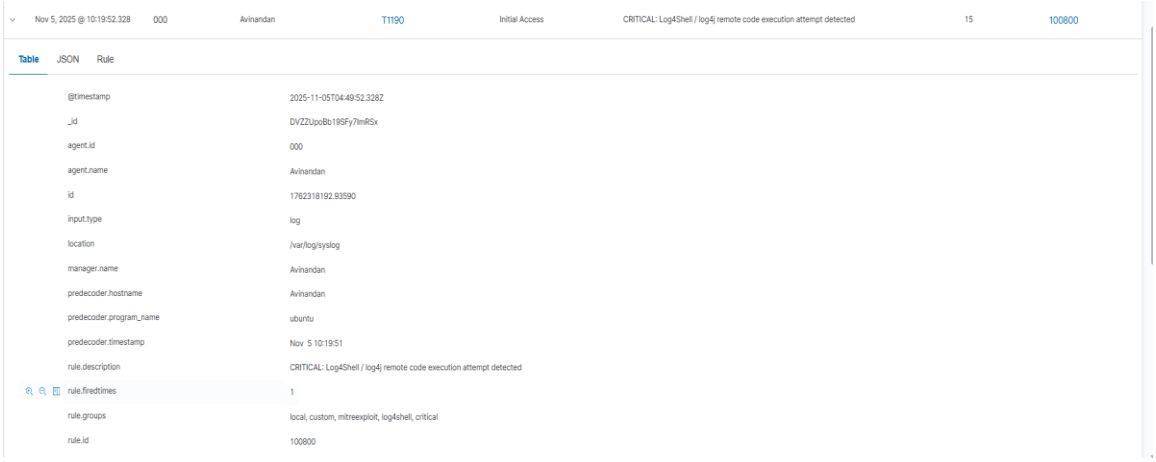


Time	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Nov 5, 2025 @ 10:19:58.336	Avinandan	T1046	Discovery	LOW: Port Scan Detected (reconnaissance)	3	100801
Nov 5, 2025 @ 10:19:52.328	Avinandan	T1190	Initial Access	CRITICAL: Log4Shell / log4j remote code execution attempt detected	15	100800
Nov 5, 2025 @ 10:19:40.314	Avinandan	T1110	Credential Access	Phishing Email: Suspicious Link Detected	12	100001
Nov 5, 2025 @ 10:18:59.506	Avinandan	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501

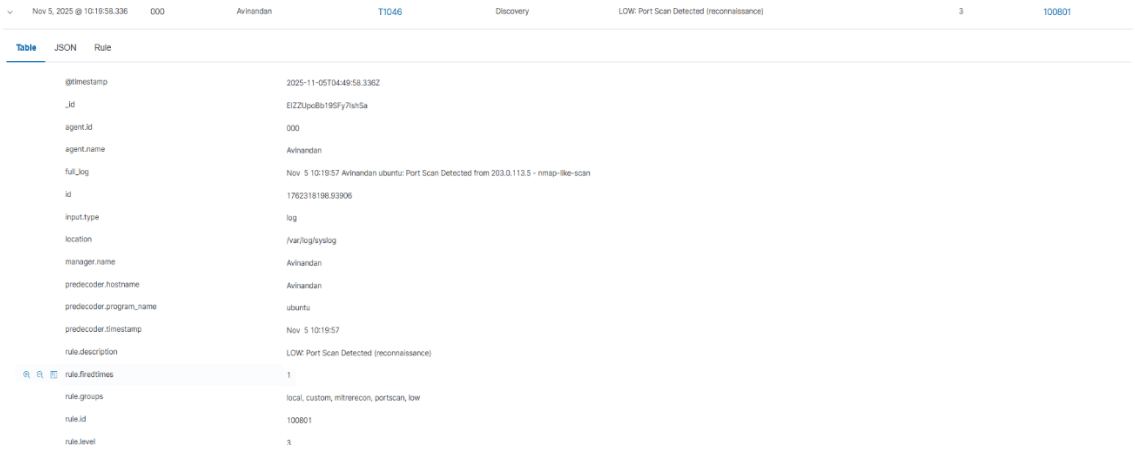
First, you drill down into the **"Phishing Email"** alert. This view shows the full log, the agent affected (Avinandan), and confirms it's a high-level alert (level 12, rule 100001).



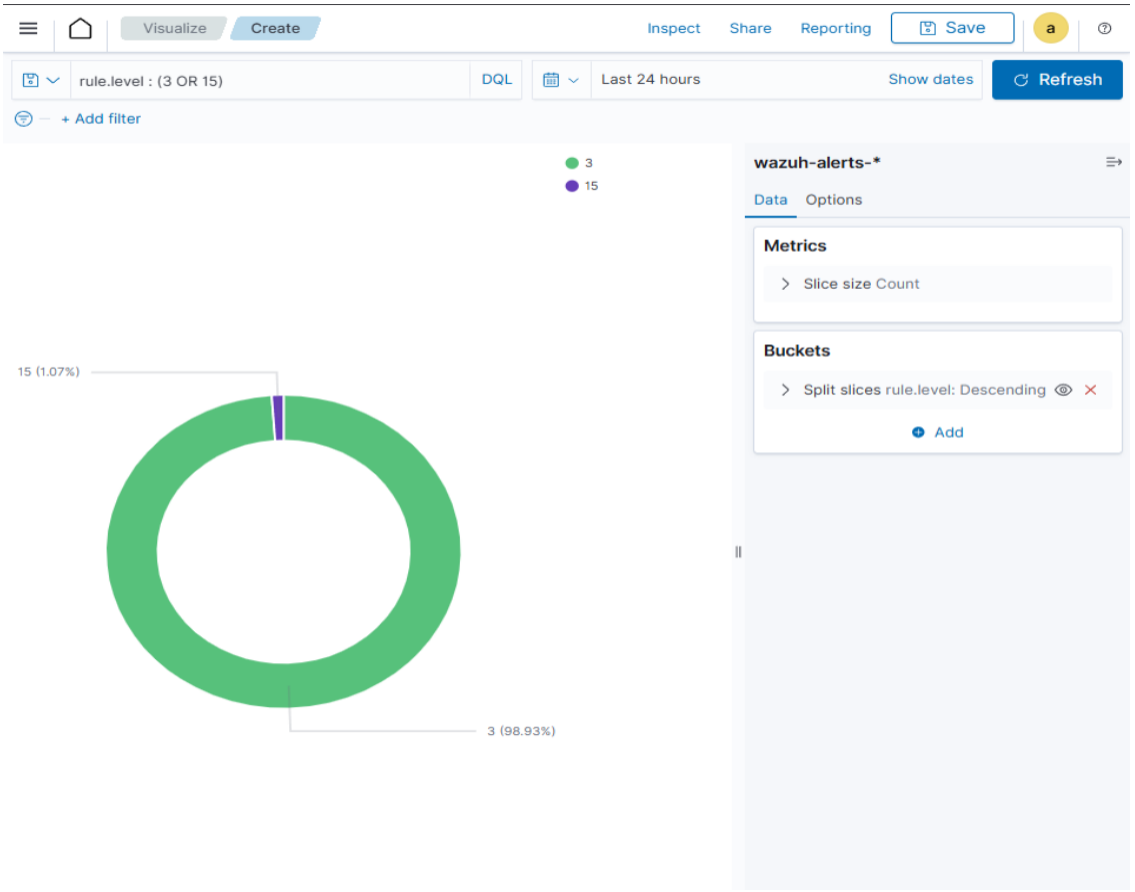
Next, you investigate the most critical event, the **"Log4Shell"** attempt. This shows the full details for this "CRITICAL" (level 15, rule 100800) alert.



Then, you examine the **"Port Scan"** alert, confirming it was an "nmap-like-scan" and noting its low priority (level 3, rule 100801).

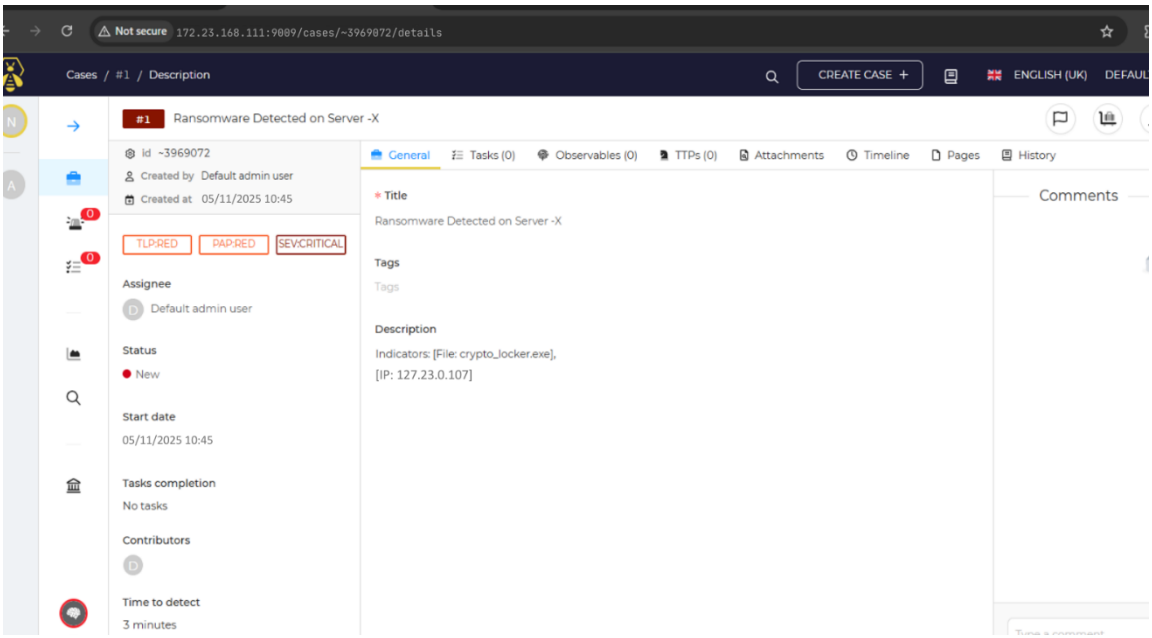


Create a New Visualization: After analyzing the different types of alerts, you move to the "Visualize" section to create a new dashboard panel. Here, you are building a pie chart to compare the *volume* of different rule levels. By filtering for rule.level : (3 OR 15), you can see that the low-level port scans (98.93%) are far more common than the critical Log4Shell attempts (1.07%).



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 occurs when an attack is classified as critical and demands immediate action. In such cases, the Tier-1 analyst forwards the incident to the Tier-2 team with a brief summary and relevant IOCs.
The email below demonstrates how a critical incident is escalated to the Tier-2 team.
Escalating a critical incident to the tire 2 team

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

Body:

Tier 2 Team,

A **critical ransomware incident** has been identified on **Server-X (172.23.0.107)** and requires immediate escalation.

The initial alert indicates the presence of a malicious executable **crypto_locker.exe**, with the suspected attacker's source IP logged as **172.23.0.107**.

Action Taken: Server-X has been isolated from the network to contain encryption activity and prevent lateral spread.

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,
Avinanadan Roy
Tier-1 SOC Analyst