



## 1. Alert Priority Levels

### Theoretical Knowledge

#### Purpose:

In a Security Operations Center (SOC), alerts are generated continuously from multiple tools. To manage them efficiently, analysts must assign **priority levels** based on severity, impact, and urgency. This ensures that the most critical threats are handled first.

### Core Concepts

#### Priority Definitions:

**Critical:** Immediate attention required; may cause severe damage or data loss.

*Example:* Ransomware encryption on production servers.

**High:** Major security threat but not yet fully exploited.

*Example:* Unauthorized admin access detected.

**Medium:** Moderate threat that needs investigation.

*Example:* Suspicious PowerShell activity.

**Low:** Minor or informational events with limited impact.

*Example:* Regular port scans from external IPs.

#### Assignment Criteria:

**Asset Criticality:** Determine how important the asset is (e.g., database server vs. test VM).

**Exploit Likelihood:** Check if the vulnerability has a known exploit (e.g., public CVE).

**Business Impact:** Assess financial or operational damage if compromised.

*Example:*

CVSS Score 9.8 (Log4Shell – CVE-2021-44228) → **Critical**

CVSS Score 6.5 → **Medium**



## Scoring Systems:

### **CVSS (Common Vulnerability Scoring System):**

Used to calculate risk scores based on exploitability and impact.

### **SOC Risk Scoring Tools:**

Splunk Enterprise Security, Wazuh, and QRadar use internal scoring to highlight top-priority alerts.

### **Key Objective:**

Develop the ability to assess and prioritize alerts accurately to reduce response time and enhance SOC efficiency.

## Alert Priority Levels – Splunk Practical

### 1. Upload Sample Alert Data

I created a sample log file **sample\_alerts.log** containing 5 security alerts with fields: AlertID, Type, Priority, Description, MITRE. The file was uploaded to Splunk using **Settings → Add Data → Upload**.

### **Sample Events in the File:**

AlertID=001 Type=Phishing Priority=High Description='Suspicious link in email' MITRE=T1566

AlertID=002 Type=BruteForce Priority=Medium Description='Multiple SSH login failures' MITRE=T1110

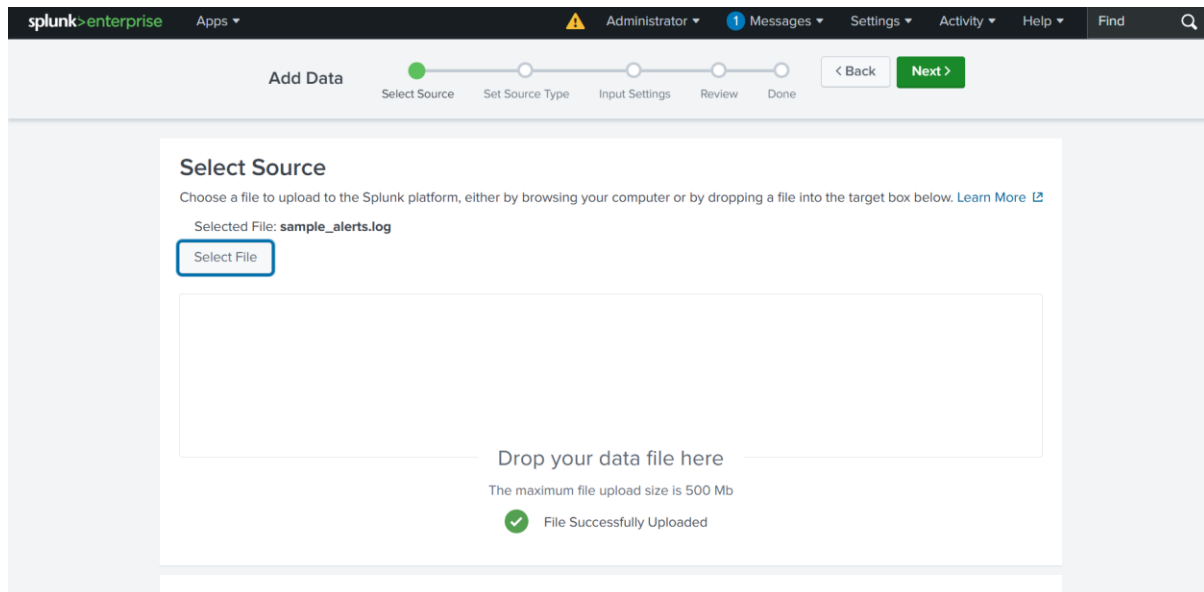
AlertID=003 Type=Ransomware Priority=Critical Description='Encryption activity detected on Server-X' MITRE=T1486

AlertID=004 Type=PortScan Priority=Low Description='Unusual port scanning from 192.168.1.100' MITRE=T1046

AlertID=005 Type=Malware Priority=High Description='Malicious file hash detected' MITRE=T1204



## Screenshot :



## 2. Field Extraction :

We extracted fields from the `_raw` log to create separate columns: AlertID, Type, Priority, Description, MITRE.

### Regular Expression Used:

`AlertID=(?<AlertID>\S+)\s+Type=(?<Type>\S+)\s+Priority=(?<Priority>\S+)\s+Description='(?<Description>[^\s]+)\s+MITRE=(?<MITRE>\S+)`

### Steps:

Run a search on the uploaded logs:

```
index="main" sourcetype="sample_alerts"
```

- Click **Extract New Fields** → choose “I prefer to write the regular expression myself”.
- Paste the regex and preview extracted fields.
- Save the extraction with name `alert_fields_extraction`



## Screenshot :

The screenshot shows the 'Extract Fields' workflow in Splunk Enterprise. The top navigation bar includes 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. The workflow progress bar shows four steps: 'Select Sample' (active), 'Select Method', 'Select Fields', and 'Save'. A 'Next >' button is visible. The main content area is titled 'Select Sample Event' and includes instructions: 'Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. [Learn more](#)'. Below this, there is a link 'I prefer to write the regular expression myself >'. The 'Source type' is set to 'sample\_alerts'. The 'Time Range' is set to 'Last 90 days'. A list of sample events is displayed in a light blue box:

```
AlertID=001 Type=Phishing Priority=High Description='Suspicious link in email' MITRE=T1566
AlertID=002 Type=BruteForce Priority=Medium Description='Multiple SSH login failures' MITRE=T1110
AlertID=003 Type=Ransomware Priority=Critical Description='Encryption activity detected on Server-X' MITRE=T1486
AlertID=004 Type=PortScan Priority=Low Description='Unusual port scanning from 192.168.1.100' MITRE=T1046
AlertID=005 Type=Malware Priority=High Description='Malicious file hash detected' MITRE=T1204
```

At the bottom, there is an 'Events' tab.

The screenshot shows the 'Extract Fields' workflow in Splunk Enterprise, Step 2: Regular Expression. The top navigation bar is the same as the previous screenshot. The workflow progress bar shows 'Select Sample' and 'Select Method' completed, with 'Select Fields' (active) and 'Save' remaining. A '< Back' button is on the left, and an 'Existing fields >' button is on the right. The main content area includes a warning icon and text: 'If you manually edit and then preview the regular expression below, you cannot return to the automatic field extraction workflow.' Below this, it says 'Use the event listing below to validate the field extractions produced by your regular expression.' The 'Regular Expression' section has a text input field containing the regex: `AlertID=(?<AlertID>\S+)\s+Type=(?<Type>\S+)\s+Priority=(?<Priority>\S+)\s+Description='(?<Description>[^\s]+)'\s+MITRE=(?<MITRE>\S+]`. To the right of the input field are links for 'Regular Expression Reference' and 'View in Search'. Below the input field are 'Preview' and 'Save' buttons. At the bottom, there is an 'Events' tab showing '✓ 1 event (7/12/25 12:00:00.000 AM to 10/10/25 5:14:36.000 PM)' and a '20 per page' dropdown. A 'filter' input field with an 'Apply' button and a 'Sample: 1,000 events' dropdown are also present.

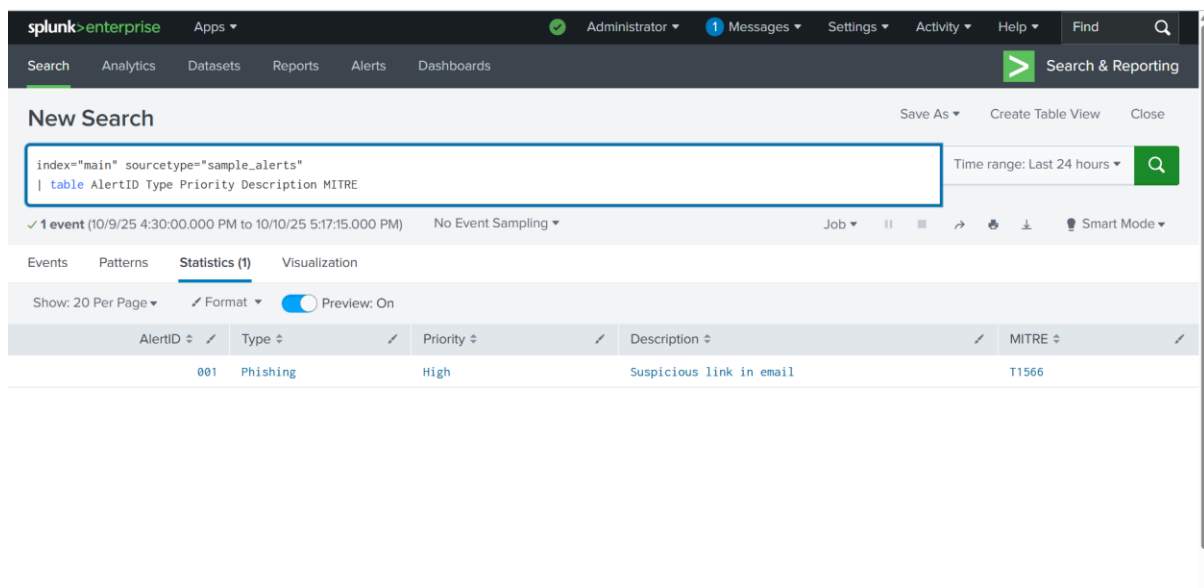


### 3. Table View of Alerts

**I tested the extraction using a table view:**

index="main" sourcetype="sample\_alerts"

| table AlertID Type Priority Description MITRE



### 3. Visualization – Alert Priority Pie Chart

**I visualized the alert priorities using a pie chart:**

**Query Used:**

index="main" sourcetype="sample\_alerts"

| stats count by Priority



## Steps:

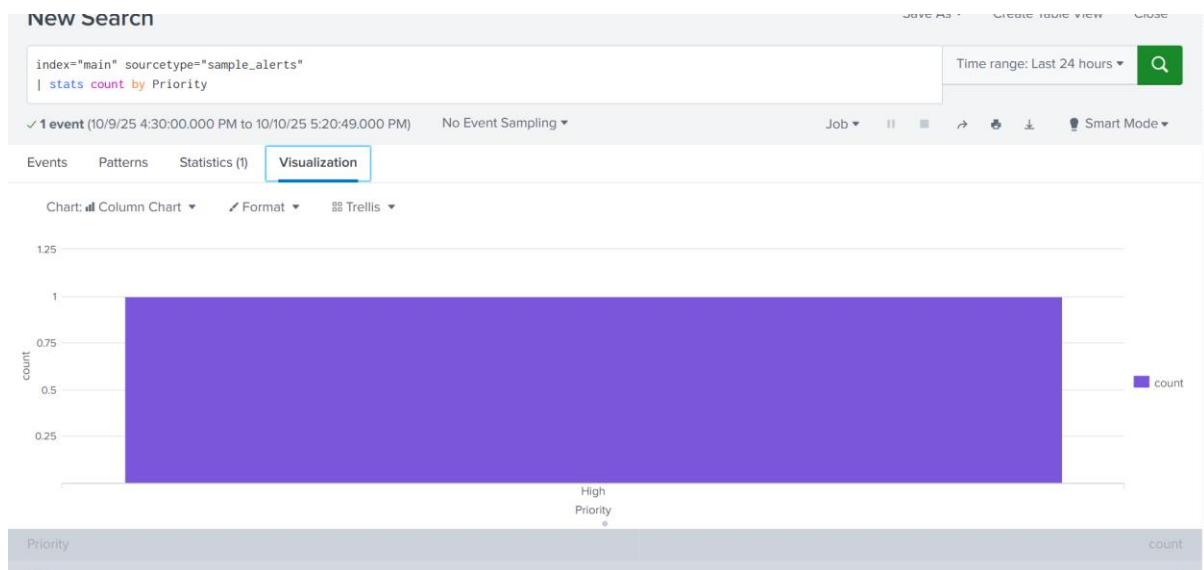
Click **Visualization** → **Pie Chart**.

Save as a **Dashboard Panel**:

Dashboard Name: Alert Priority Overview

Panel Name: Alert Priority Distribution

## Screenshot :





## Practical: Incident Ticket & Escalation Email

### Tools Required

Splunk Enterprise (for alert detection)

TheHive

Google Docs / Email client (for escalation email)

### Step 1: Identify Critical Alert in Splunk

Open **Search & Reporting** app in Splunk.

Run the table query:

```
index="main" sourcetype="sample_alerts"
```

```
| table AlertID Type Priority Description MITRE
```

Identified **Critical priority alert**

### Screenshot :

The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query `index="main" sourcetype="sample_alerts"` and the table view is selected. The results show a single event with the following details:

AlertID	Type	Priority	Description	MITRE
001	Phishing	High	Suspicious link in email	T1566



## Step 2: Create Incident Ticket

- Open **TheHive** .
- Click **New Case / New Ticket**.
- Fill in the ticket fields:

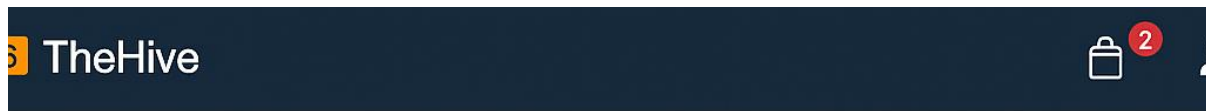
Field	Value
Title	[Critical] Ransomware Detected on Server-X
Description	Indicators: <ul style="list-style-type: none"><li>• File: crypto_locker.exe</li><li>• IP: 192.168.1.50</li></ul>
Priority	Critical
Assignee	SOC Analyst
Status	Open

- Click **Submit**.





## Screenshot:



Dashboard

Cases

## [Critical] Ransomware Detected on Server-X

### DESCRIPTION

#### Indicators:

- File: cryppoto\_locker.exe
- IP: 192.168.1.50

### PRIORITY

**CRITICAL**

### ASSIGNEE

SOC Analyst

### STATUS

OPEN



## Step 3: Draft Escalation Email

Open **Email client** or **Google Docs**.

Draft an escalation email to Tier 2 analyst:

Case: [Critical] Ransomware Detected on Server-X

### 1. Introduction

On October 10, 2025, a critical alert was triggered in our SIEM tool (Splunk) indicating potential ransomware activity on Server-X. The alert included indicators such as the presence of a suspicious executable file named `crypto\_locker.exe` and network traffic from IP address `192.168.1.50`. Given the severity and potential impact, I initiated an immediate investigation.

### 2. How I Investigated

To assess the situation, I followed these steps:

1. Validated the alert to confirm it wasn't a false positive.
2. Queried Splunk for file execution logs and process creation events on Server-X.
3. Checked the hash of `crypto\_locker.exe` against threat intelligence databases (e.g., VirusTotal, MISP).
4. Reviewed network logs to trace outbound connections from `192.168.1.50`.
5. Inspected system changes, including registry modifications and file encryption patterns.
6. Verified whether the ransomware had spread laterally or impacted other systems.

### 3. What I Found

Splunk logs confirmed that `crypto\_locker.exe` was executed on Server-X at approximately 02:47 AM IST. Shortly after, multiple files on the server were renamed with a `.locked` extension, and a ransom note was dropped in several directories.



The IP `192.168.1.50` showed unusual outbound traffic to known command-and-control (C2) servers. The file hash matched known ransomware signatures in VirusTotal, confirming it was a variant of CryptoLocker.

No signs of lateral movement were detected within the first two hours, and containment measures were promptly initiated.

## 4. My Analysis

This was a confirmed ransomware infection. The attacker likely gained access through a vulnerable service or phishing vector and deployed the payload during off-hours to avoid detection. The encryption behavior, ransom note, and C2 communication all point to a targeted attack using a known ransomware strain.

Fortunately, the infection was isolated to Server-X, and no further compromise was observed in adjacent systems.

## 5. Conclusion

This was a legitimate and critical security incident. Server-X was compromised by ransomware, resulting in file encryption and potential data loss. The infection was contained before it could spread further.

## 6. Recommendations

- Immediately isolate Server-X from the network.
- Initiate forensic imaging and preserve logs for deeper analysis.
- Restore affected files from clean backups.
- Patch any vulnerabilities and review access controls.
- Notify stakeholders and initiate incident response protocols.
- Implement endpoint protection and network segmentation.
- Conduct a post-incident review and update the playbook accordingly.



## Step 4: Update Ticket After Escalation

Once email is sent, go back to TheHive.

Update ticket status to **Escalated**.

Add **comments**: "Email sent to Tier 2 team, awaiting further analysis."



## Practical 3: Alert Triage & Threat Intelligence Validation

### Objective:

To investigate a **Critical alert** from Splunk and validate if it's a real threat or a false positive using threat intelligence.

### Step 1: Identify the Critical Alert

In Splunk's **Search & Reporting**, run:

```
index="main" sourcetype="sample_alerts" Priority="Critical"
```

```
| table AlertID Type Priority Description MITRE
```

This filters only **Critical** priority alerts.

### Screenshot:

The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query: `index="main" sourcetype="sample_alerts" | table AlertID Type Priority Description MITRE`. The results are displayed in a table with 6 events. The table has columns: AlertID, Type, Priority, Description, and MITRE. The results are sorted by Priority, with Critical alerts at the top.

AlertID	Type	Priority	Description	MITRE
004	PortScan	Low	Unusual port scanning from 192.168.1.100	T1046
003	Ransomware	Critical	Encryption activity detected on Server-X	T1486
002	BruteForce	Medium	Multiple SSH login failures	T1110
001	Phishing	High	Suspicious link in email	T1566
001	Phishing	High	Suspicious link in email	T1566
005	Malware	High	Malicious file hash detected	T1204



## Step 2: Check Alert Details

Double-click the **Critical Ransomware alert** event to view raw log data.  
Review fields like:

**AlertID** → 003

**Type** → Ransomware

**Priority** → Critical

**Description** → Encryption activity detected on Server-X

**MITRE Technique** → T1486 (Data Encrypted for Impact)

## Screenshot :



## Step 3: Validate the Threat

Use public threat intelligence sites such as:

**VirusTotal** (<https://www.virustotal.com>)

**AlienVault OTX** (<https://otx.alienvault.com>)

**MITRE ATT&CK** (<https://attack.mitre.org/techniques/T1486/>)

### Screenshot :

The screenshot displays the MITRE ATT&CK website interface. The top navigation bar includes links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and a Blog. A search bar is located on the right. Below the navigation bar, a banner for 'ATT&CKcon 6.0' is visible. The main content area is titled 'Data Encrypted for Impact' (ID: T1486). The left sidebar lists various techniques under the 'TECHNIQUES' heading, with 'Data Encrypted for Impact' selected. The main text describes the technique: 'Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.' It also mentions that in the case of ransomware, common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted. The right sidebar provides additional details: 'Sub-techniques: No sub-techniques', 'Tactic: Impact', 'Platforms: ESXi, IaaS, Linux, Windows, macOS', 'Impact Type: Availability', 'Contributors: ExtraHop; Harshal Tupsamudre, Qualys; Mayuresh Dani, Qualys; Oleg Kolesnikov, Securonix; Travis Smith, Qualys', 'Version: 1.5', 'Created: 15 March 2019', and 'Last Modified: 15 April 2025'. A 'Version Permalink' link is also present.

## Step 4: Analyst Action

If the alert is confirmed as real:

Escalate to the **Incident Response team** (Tier 2).

Document findings and timestamp of detection.

Recommend isolating **Server-X** from the network.

If it's a false positive:

Close the alert and update the alert rule to reduce noise.



## **Step 5: Documentation**

Record the following in your SOC report:

Alert ID: 003

Source: Splunk

Analyst: Syed Sameer Hussain

Validation Source: MITRE ATT&CK

Final Decision: Escalated to Tier 2