Advanced Log Analysis

Step 1: Log Ingestion and Setup

Objective:

The goal of this step is to upload and configure log files in **Splunk** for analysis. This process helps the SOC analyst to collect, store, and prepare data for correlation, alerting, and investigation.

1. Log File Used:

File Name: advanced_log_analysis.log
Content Type: Simulated security alerts containing information such as alert ID, type, priority, description, and MITRE ATT&CK technique.

Example log entries:

```
10/10/25 10:08:32.000 PM AlertID=005 Type=Malware Priority=High
Description='Malicious file hash detected' MITRE=T1204

10/10/25 10:08:32.000 PM AlertID=004 Type=PortScan Priority=Low
Description='Unusual port scanning from 192.168.1.100' MITRE=T1046

10/10/25 10:08:32.000 PM AlertID=003 Type=Ransomware Priority=Critical
Description='Encryption activity detected on Server-X' MITRE=T1486

10/10/25 10:08:32.000 PM AlertID=002 Type=BruteForce Priority=Medium
Description='Multiple SSH login failures' MITRE=T1110

10/10/25 10:08:32.000 PM AlertID=001 Type=Phishing Priority=High
Description='Suspicious link in email' MITRE=T1566
```

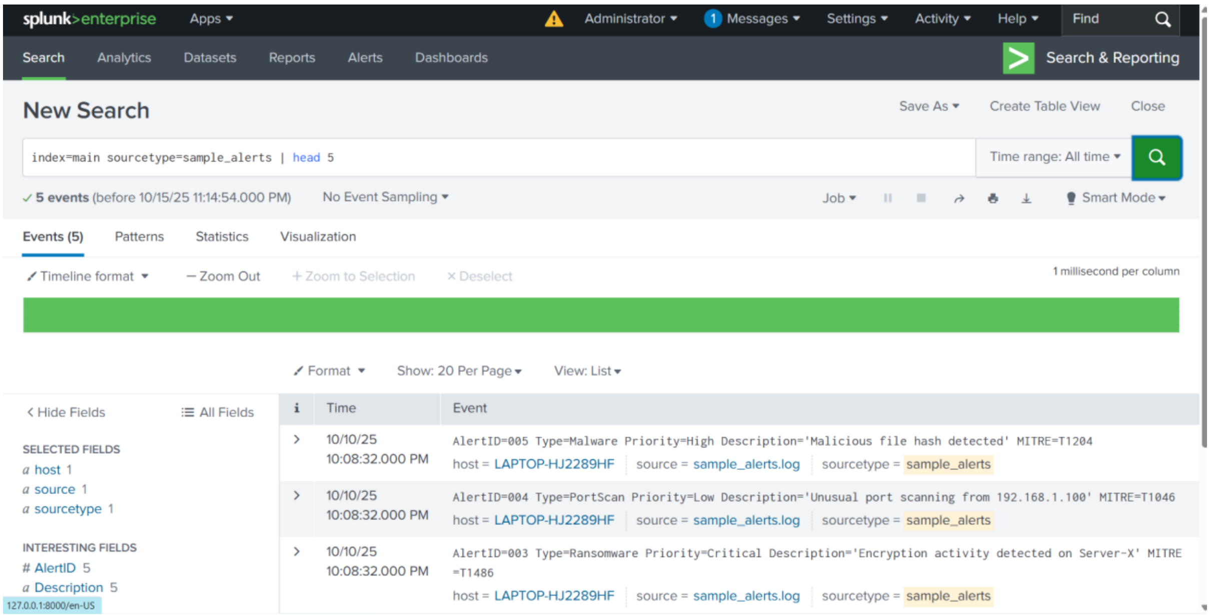
2. Steps to Upload Logs into Splunk:

Step 1.1 – Open Splunk Web Interface

Launch your browser and go to:
URL: http://localhost:8000

Login with your Splunk credentials.

Screenshot:



```
index=main sourcetype=sample_alerts | head 5
```

✓ 5 events (before 10/15/25 11:14:54.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
AlertID 5
a Description 5

i	Time	Event
>	10/10/25 10:08:32.000 PM	AlertID=005 Type=Malware Priority=High Description='Malicious file hash detected' MITRE=T1204 host = LAPTOP-HJ2289HF source = sample_alerts.log sourcetype = sample_alerts
>	10/10/25 10:08:32.000 PM	AlertID=004 Type=PortScan Priority=Low Description='Unusual port scanning from 192.168.1.100' MITRE=T1046 host = LAPTOP-HJ2289HF source = sample_alerts.log sourcetype = sample_alerts
>	10/10/25 10:08:32.000 PM	AlertID=003 Type=Ransomware Priority=Critical Description='Encryption activity detected on Server-X' MITRE =T1486 host = LAPTOP-HJ2289HF source = sample_alerts.log sourcetype = sample_alerts

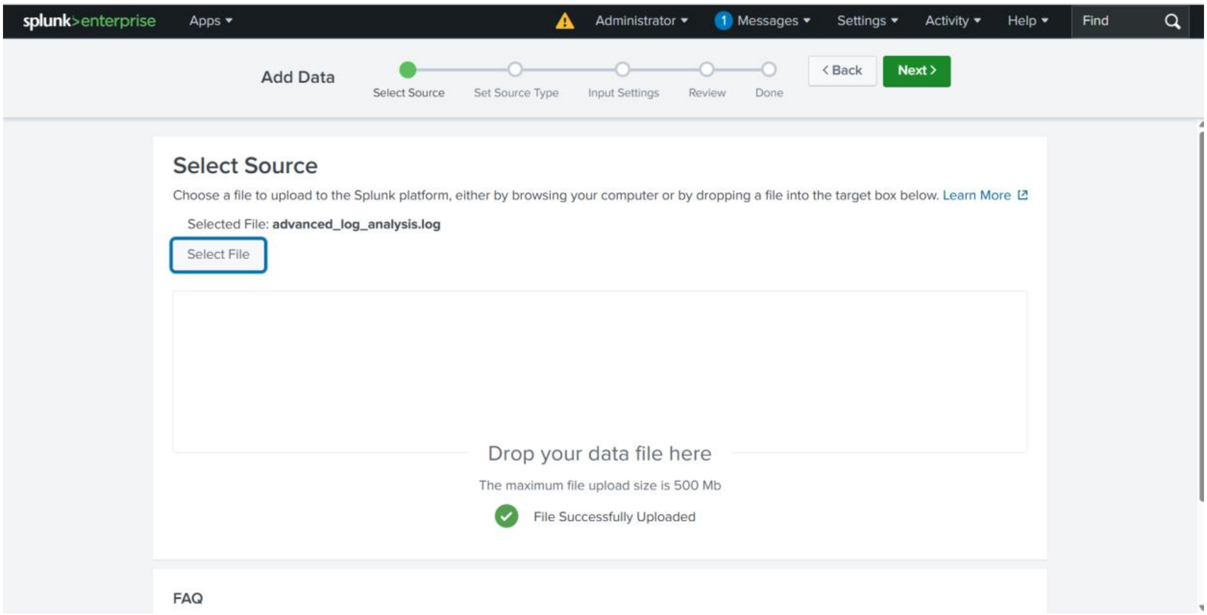
Step 1.2 – Upload the Log File

From the home page, click on **"Add Data"**.

Select **"Upload"** and choose the file advanced_log_analysis.log from your system.

Click **Next** to continue.

Screenshot:



Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Selected File: **advanced_log_analysis.log**

Drop your data file here

The maximum file upload size is 500 Mb

✓ File Successfully Uploaded

Step 1.3 – Define Source Type and Index

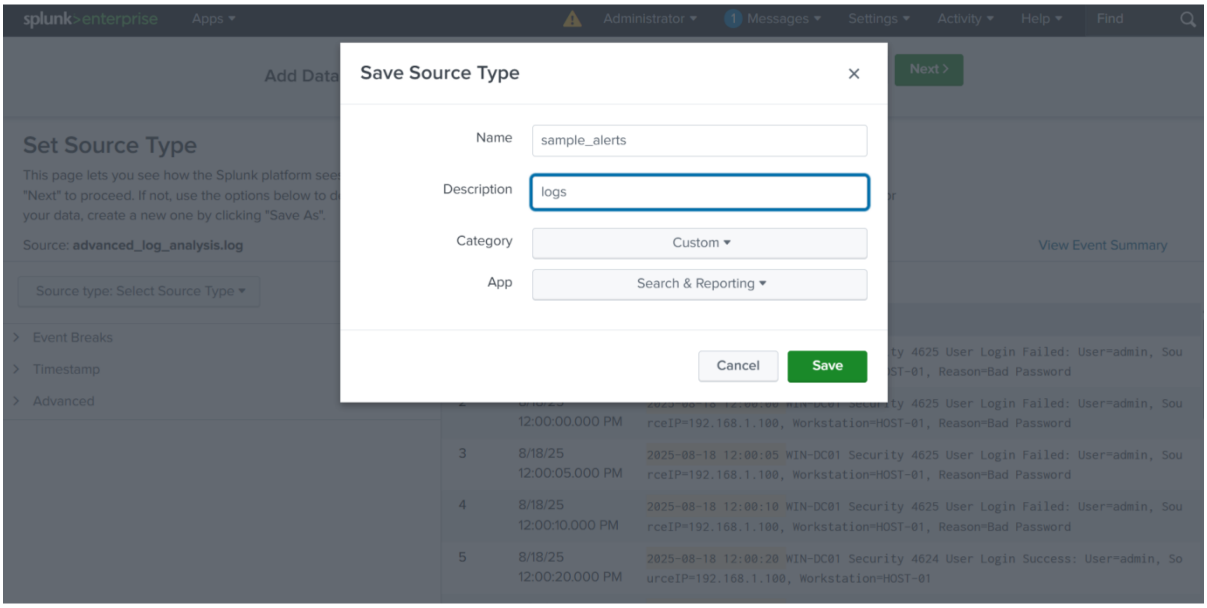
Source Type: sample_alerts

Host: LAPTOP-xxxxx

Index: main

Click **Review** → **Submit** to finalize data ingestion.

Screenshot:



Set Source Type

This page lets you see how the Splunk platform sees "Next" to proceed. If not, use the options below to d your data, create a new one by clicking "Save As".

Source: **advanced_log_analysis.log**

Source type: Select Source Type ▾

› Event Breaks
› Timestamp
› Advanced

View Event Summary

Save Source Type ×

Name: sample_alerts

Description: logs

Category: Custom ▾

App: Search & Reporting ▾

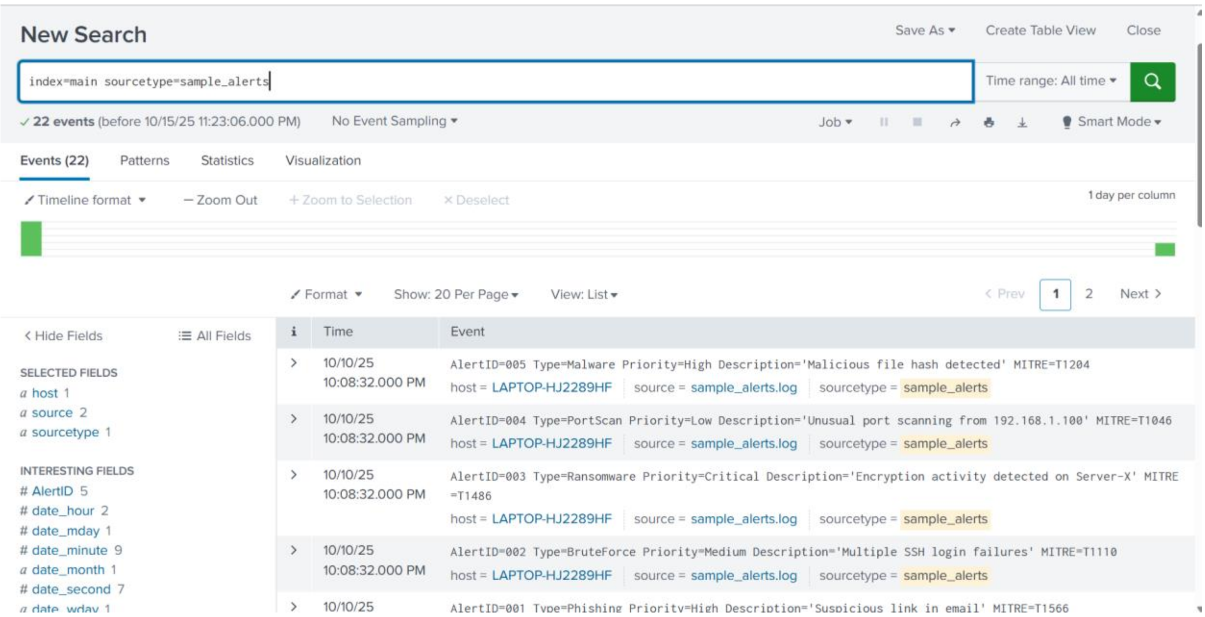
Cancel | Save

```
   ty 4625 User Login Failed: User=admin, Sou
   ST-01, Reason=Bad Password
2  12:00:00.000 PM   ty 4625 User Login Failed: User=admin, Sou
                     rceIP=192.168.1.100, Workstation=HOST-01, Reason=Bad Password
3  8/18/25           2025-08-18 12:00:05 WIN-DC01 Security 4625 User Login Failed: User=admin, Sou
   12:00:05.000 PM   rceIP=192.168.1.100, Workstation=HOST-01, Reason=Bad Password
4  8/18/25           2025-08-18 12:00:10 WIN-DC01 Security 4625 User Login Failed: User=admin, Sou
   12:00:10.000 PM   rceIP=192.168.1.100, Workstation=HOST-01, Reason=Bad Password
5  8/18/25           2025-08-18 12:00:20 WIN-DC01 Security 4624 User Login Success: User=admin, So
   12:00:20.000 PM   urceIP=192.168.1.100, Workstation=HOST-01
```

Step 1.4 – Verify Data Ingestion

After uploading, verify if Splunk successfully indexed your data by running this simple search:

Search head = index=main sourcetype=sample_alerts



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

✓ 22 events (before 10/15/25 11:23:06.000 PM)   No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 2
- a sourcetype 1

INTERESTING FIELDS
- # AlertID 5
- # date_hour 2
- # date_mday 1
- # date_minute 9
- a date_month 1
- # date_second 7
- a date_wday 1

i	Time	Event
›	10/10/25 10:08:32.000 PM	AlertID=005 Type=Malware Priority=High Description='Malicious file hash detected' MITRE=T1204 host = LAPTOP-HJ2289HF | source = sample_alerts.log | sourcetype = sample_alerts
›	10/10/25 10:08:32.000 PM	AlertID=004 Type=PortScan Priority=Low Description='Unusual port scanning from 192.168.1.100' MITRE=T1046 host = LAPTOP-HJ2289HF | source = sample_alerts.log | sourcetype = sample_alerts
›	10/10/25 10:08:32.000 PM	AlertID=003 Type=Ransomware Priority=Critical Description='Encryption activity detected on Server-X' MITRE=T1486 host = LAPTOP-HJ2289HF | source = sample_alerts.log | sourcetype = sample_alerts

›	10/10/25
	10:08:32.000 PM
		AlertID=002 Type=BruteForce Priority=Medium Description='Multiple SSH login failures' MITRE=T1110
		host = LAPTOP-HJ2289HF | source = sample_alerts.log | sourcetype = sample_alerts

›	10/10/25	AlertID=001 Type=Phishing Priority=High Description='Suspicious link in email' MITRE=T1566

Log Correlation — Detect Suspicious Behavior

This will correlate **failed logins** with **outbound connections** from the same source IP.

Run this SPL query:

index=main sourcetype=sample_alerts ("4625" OR "Firewall Allowed Connection")

| rex "SourceIP=(?<src_ip>\S+)"

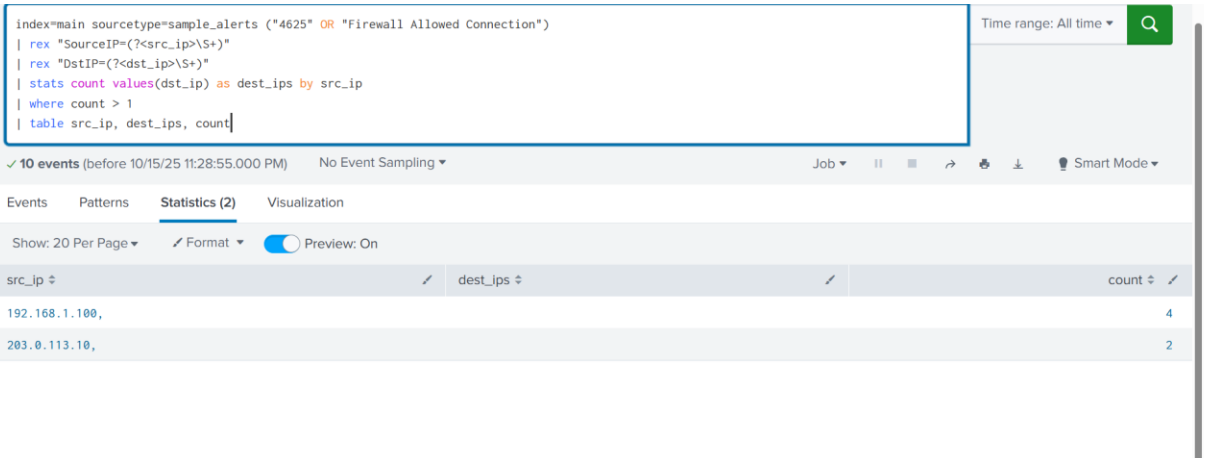
| rex "DstIP=(?<dst_ip>\S+)"

| stats count values(dst_ip) as dest_ips by src_ip

| where count > 1

| table src_ip, dest_ips, count

Screenshot :



```
index=main sourcetype=sample_alerts ("4625" OR "Firewall Allowed Connection")
| rex "SourceIP=(?<src_ip>\S+)"
| rex "DstIP=(?<dst_ip>\S+)"
| stats count values(dst_ip) as dest_ips by src_ip
| where count > 1
| table src_ip, dest_ips, count
```

✓ 10 events (before 10/15/25 11:28:55.000 PM)

src_ip	dest_ips	count
192.168.1.100,		4
203.0.113.10,		2

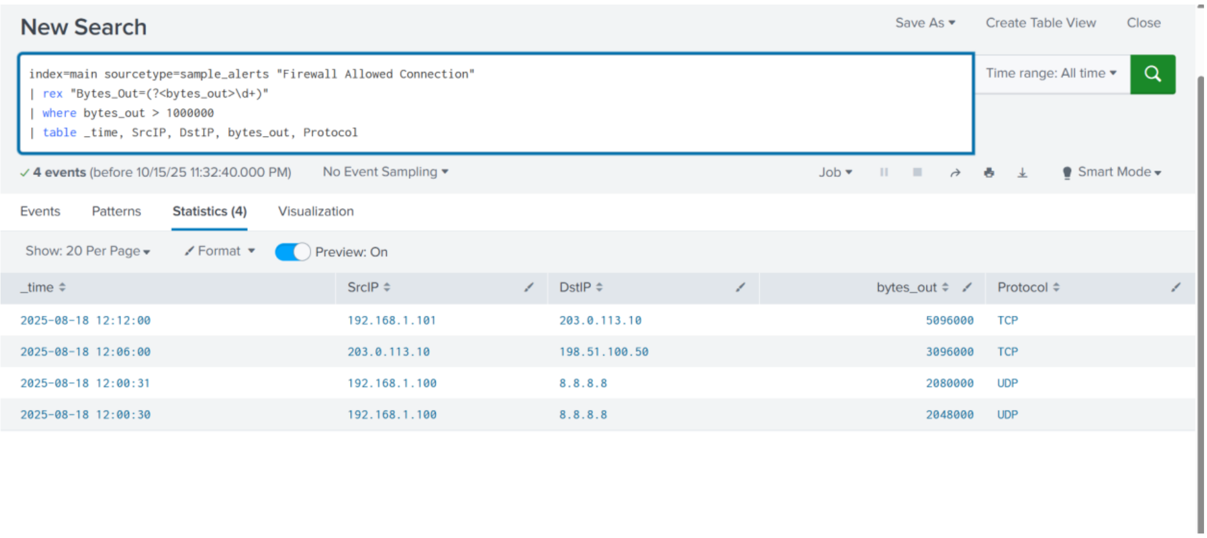
Anomaly Detection — High Data Transfers

Detect unusual outbound connections (large byte transfers).

Run:

index=main sourcetype=sample_alerts "Firewall Allowed Connection"
| rex "Bytes_Out=(?<bytes_out>\d+)"
| where bytes_out > 1000000
| table _time, SrcIP, DstIP, bytes_out, Protocol

Screenshot :



```
index=main sourcetype=sample_alerts "Firewall Allowed Connection"
| rex "Bytes_Out=(?<bytes_out>\d+)"
| where bytes_out > 1000000
| table _time, SrcIP, DstIP, bytes_out, Protocol
```

✓ **4 events** (before 10/15/25 11:32:40.000 PM) No Event Sampling ▾

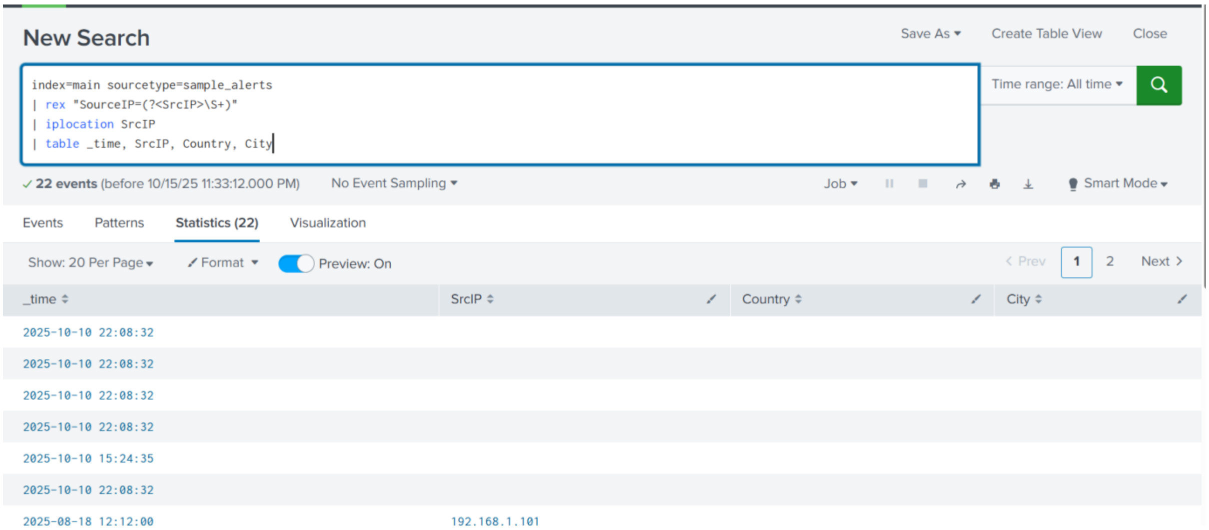
_time	SrcIP	DstIP	bytes_out	Protocol
2025-08-18 12:12:00	192.168.1.101	203.0.113.10	5096000	TCP
2025-08-18 12:06:00	203.0.113.10	198.51.100.50	3096000	TCP
2025-08-18 12:00:31	192.168.1.100	8.8.8.8	2080000	UDP
2025-08-18 12:00:30	192.168.1.100	8.8.8.8	2048000	UDP

Log Enrichment

Run:

```
index=main sourcetype=sample_alerts
| rex "SourceIP=(?<SrcIP>\S+)"
| iplocation SrcIP
| table _time, SrcIP, Country, City
```

Screenshot:



```
index=main sourcetype=sample_alerts
| rex "SourceIP=(?<SrcIP>\S+)"
| iplocation SrcIP
| table _time, SrcIP, Country, City
```

✓ **22 events** (before 10/15/25 11:33:12.000 PM) No Event Sampling ▾

_time	SrcIP	Country	City
2025-10-10 22:08:32			
2025-10-10 22:08:32			
2025-10-10 22:08:32			
2025-10-10 22:08:32			
2025-10-10 15:24:35			
2025-10-10 22:08:32			
2025-08-18 12:12:00	192.168.1.101		

Threat Intelligence Integration – Practical Application

Objective

To integrate external threat-intelligence feeds into a SOC workflow using Splunk and other tools.
This enhances alert enrichment, detection accuracy, and proactive threat hunting.

1. Tools Used

Splunk Enterprise – for log ingestion and correlation

AlienVault OTX – for real-world threat feeds (IOCs)

VirusTotal – for IP and hash reputation lookup

Google Sheets / Notes – to document matches and observations

2. Tasks Performed

2.1 Import Threat Feed (IOCs)

Simulated the import of a threat feed from **AlienVault OTX** containing known malicious IP addresses.

Step 1 — Create the IOC lookup file (CSV)

Open Notepad.

Copy the exact CSV content below and save it as otx_iocs.csv (CSV, UTF-8)

- IP,IndicatorType,Reputation,Category,Source
- 8.8.8.8,ip,High,Botnet,OTX
- 192.168.1.100,ip,Critical,C2,OTX
- 198.51.100.50,ip,High,MaliciousHost,OTX
- 203.0.113.10,ip,Medium,Suspicious,OTX

Save the file where you can easily upload it.

Step 2 — Upload the CSV into Splunk as a lookup table

Log into Splunk Web (http://localhost:8000).

Go to **Settings** → **Lookups** → **Lookup table files**.

Click **Add new** → choose your app (use search or default) → **Upload** → select otx_iocs.csv → Submit.

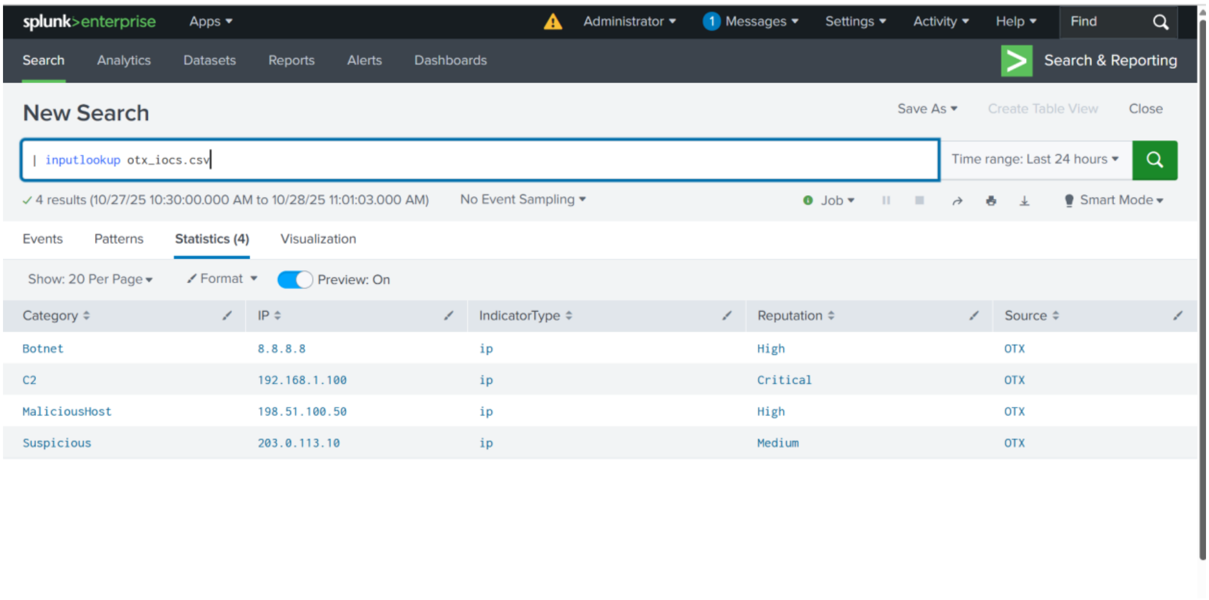
After upload, go to **Lookup definitions** → **Add new** → Give it a name (e.g., otx_lookup) → select the uploaded file otx_iocs.csv → Save.

Step 3 — Verify the lookup file exists

Run this SPL to preview the lookup content:

| inputlookup otx_iocs.csv

Screenshot:



```
| inputlookup otx_iocs.csv
```

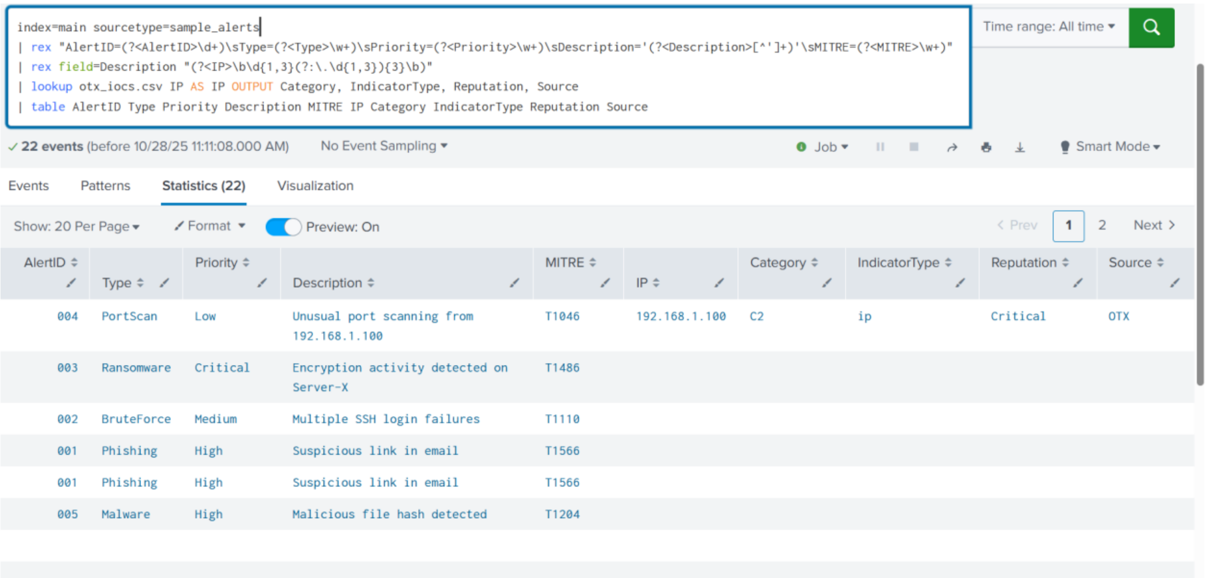
✓ 4 results (10/27/25 10:30:00.000 AM to 10/28/25 11:01:03.000 AM)

Category	IP	IndicatorType	Reputation	Source
Botnet	8.8.8.8	ip	High	OTX
C2	192.168.1.100	ip	Critical	OTX
MaliciousHost	198.51.100.50	ip	High	OTX
Suspicious	203.0.113.10	ip	Medium	OTX

IOC Match – High or Critical Reputation

```
index=main sourcetype=sample_alerts

| rex "AlertID=(?<AlertID>\d+)\sType=(?<Type>\w+)\sPriority=(?<Priority>\w+)\sDescription='(?<Description>[^']+)'\sMITRE=(?<MITRE>\w+)"

| rex field=Description "(?<IP>\b\d{1,3}(?:\.\d{1,3}){3}\b)"

| lookup otx_iocs.csv IP AS IP OUTPUT Category, IndicatorType, Reputation, Source

| table AlertID Type Priority Description MITRE IP Category IndicatorType Reputation Source
```

Screenshot:



```
index=main sourcetype=sample_alerts
| rex "AlertID=(?<AlertID>\d+)\sType=(?<Type>\w+)\sPriority=(?<Priority>\w+)\sDescription='(?<Description>[^']+)'\sMITRE=(?<MITRE>\w+)"
| rex field=Description "(?<IP>\b\d{1,3}(?:\.\d{1,3}){3}\b)"
| lookup otx_iocs.csv IP AS IP OUTPUT Category, IndicatorType, Reputation, Source
| table AlertID Type Priority Description MITRE IP Category IndicatorType Reputation Source
```

Time range: All time

✓ 22 events (before 10/28/25 11:11:08.000 AM)

No Event Sampling

Preview: On

Show: 20 Per Page

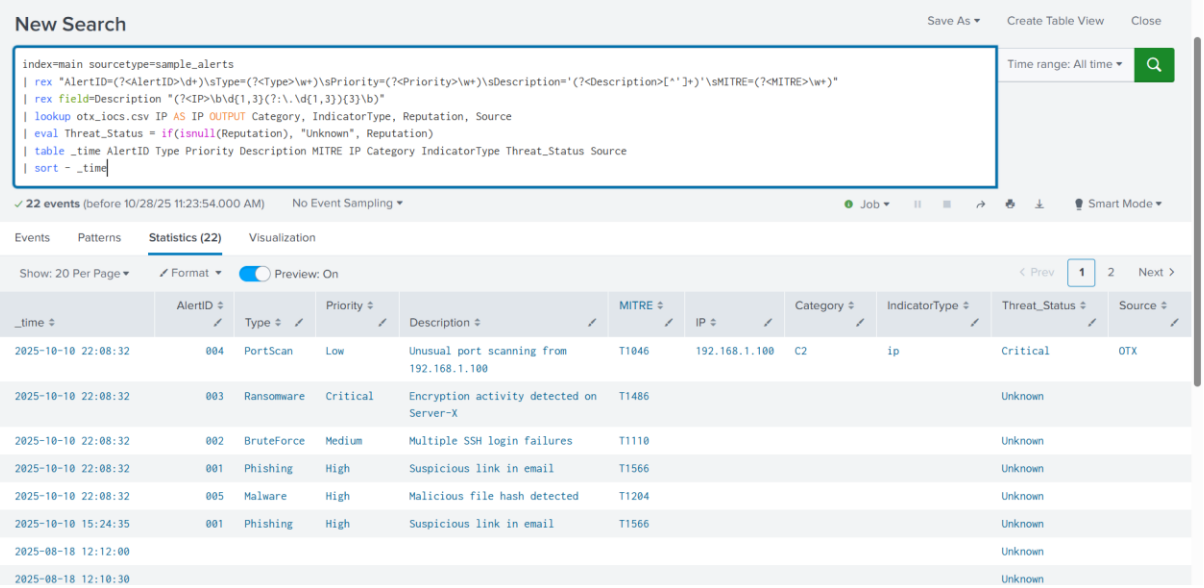
AlertID	Type	Priority	Description	MITRE	IP	Category	IndicatorType	Reputation	Source
004	PortScan	Low	Unusual port scanning from 192.168.1.100	T1046	192.168.1.100	C2	ip	Critical	OTX
003	Ransomware	Critical	Encryption activity detected on Server-X	T1486					
002	BruteForce	Medium	Multiple SSH login failures	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					

Threat Intelligence Integration

Query:

```
index=main sourcetype=sample_alerts

| rex "AlertID=(?<AlertID>\d+)\sType=(?<Type>\w+)\sPriority=(?<Priority>\w+)\sDescription='(?<Description>[^']+)'\sMITRE=(?<MITRE>\w+)"

| rex field=Description "(?<IP>\b\d{1,3}(?:\.\d{1,3}){3}\b)"

| lookup otx_iocs.csv IP AS IP OUTPUT Category, IndicatorType, Reputation, Source

| eval Threat_Status = if(isnull(Reputation), "Unknown", Reputation)

| table _time AlertID Type Priority Description MITRE IP Category IndicatorType Threat_Status Source

| sort - _time
```

Screenshot:



```
index=main sourcetype=sample_alerts
| rex "AlertID=(?<AlertID>\d+)\sType=(?<Type>\w+)\sPriority=(?<Priority>\w+)\sDescription='(?<Description>[^']+)'\sMITRE=(?<MITRE>\w+)"
| rex field=Description "(?<IP>\b\d{1,3}(?:\.\d{1,3}){3}\b)"
| lookup otx_iocs.csv IP AS IP OUTPUT Category, IndicatorType, Reputation, Source
| eval Threat_Status = if(isnull(Reputation), "Unknown", Reputation)
| table _time AlertID Type Priority Description MITRE IP Category IndicatorType Threat_Status Source
| sort - _time
```

✓ 22 events (before 10/28/25 11:23:54.000 AM) No Event Sampling ▾

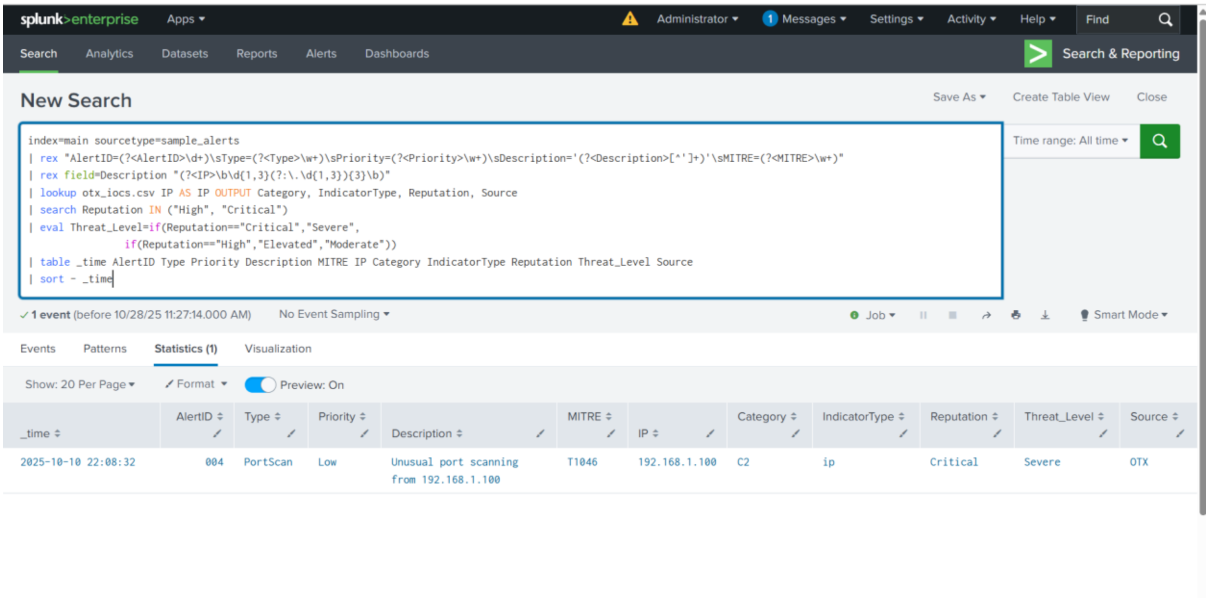
_time	AlertID	Type	Priority	Description	MITRE	IP	Category	IndicatorType	Threat_Status	Source
2025-10-10 22:08:32	004	PortScan	Low	Unusual port scanning from 192.168.1.100	T1046	192.168.1.100	C2	ip	Critical	OTX
2025-10-10 22:08:32	003	Ransomware	Critical	Encryption activity detected on Server-X	T1486				Unknown	
2025-10-10 22:08:32	002	BruteForce	Medium	Multiple SSH login failures	T1110				Unknown	
2025-10-10 22:08:32	001	Phishing	High	Suspicious link in email	T1566				Unknown	
2025-10-10 22:08:32	005	Malware	High	Malicious file hash detected	T1204				Unknown	
2025-10-10 15:24:35	001	Phishing	High	Suspicious link in email	T1566				Unknown	
2025-08-18 12:12:00									Unknown	
2025-08-18 12:10:30									Unknown	

Saved Search & Alert for IOC Matches:

Query:

```
index=main sourcetype=sample_alerts

| rex "AlertID=(?<AlertID>\d+)\sType=(?<Type>\w+)\sPriority=(?<Priority>\w+)\sDescription='(?<Description>[^']+)'\sMITRE=(?<MITRE>\w+)"

| rex field=Description "(?<IP>\b\d{1,3}(?:\.\d{1,3}){3}\b)"

| lookup otx_iocs.csv IP AS IP OUTPUT Category, IndicatorType, Reputation, Source

| search Reputation IN ("High", "Critical")

| eval Threat_Level=if(Reputation=="Critical","Severe",

                     if(Reputation=="High","Elevated","Moderate"))

| table _time AlertID Type Priority Description MITRE IP Category IndicatorType Reputation Threat_Level Source

| sort - _time
```

Screenshot:



New Search

```
index=main sourcetype=sample_alerts
| rex "AlertID=(?<AlertID>\d+)\sType=(?<Type>\w+)\sPriority=(?<Priority>\w+)\sDescription='(?<Description>[^']+)'\sMITRE=(?<MITRE>\w+)"
| rex field=Description "(?<IP>\b\d{1,3}(?:\.\d{1,3}){3}\b)"
| lookup otx_iocs.csv IP AS IP OUTPUT Category, IndicatorType, Reputation, Source
| search Reputation IN ("High", "Critical")
| eval Threat_Level=if(Reputation=="Critical","Severe",
              if(Reputation=="High","Elevated","Moderate"))
| table _time AlertID Type Priority Description MITRE IP Category IndicatorType Reputation Threat_Level Source
| sort - _time
```

Time range: All time ▾

✓ 1 event (before 10/28/25 11:27:14.000 AM) No Event Sampling ▾

_time	AlertID	Type	Priority	Description	MITRE	IP	Category	IndicatorType	Reputation	Threat_Level	Source
2025-10-10 22:08:32	004	PortScan	Low	Unusual port scanning from 192.168.1.100	T1046	192.168.1.100	C2	ip	Critical	Severe	OTX