Project

Splunk Project On Log Monitoring Documentation

Author

Adebayo Fijabi
Cybersecurity Analyst

Project Overview

This project focuses on deploying and configuring Splunk Enterprise as a Security Information and Event Management (SIEM) platform to centralize, monitor, and analyze security logs across multiple systems. The goal is to establish centralized visibility into system and security events, enabling effective threat detection, investigation, and response.

Splunk is used to aggregate logs from multiple client systems into a single, centralized dashboard, where events can be correlated, searched, and analyzed using detection rules and threat intelligence. This setup mirrors real-world SOC environments where visibility, monitoring, and log integrity are critical to cybersecurity operations.

NIST CSF Alignment→This project directly supports the NIST Cybersecurity Framework (CSF) core functions:

NIST CSF Function	Splunk Implementation
Identify (ID)	Log source identification, asset awareness, index creation
Protect (PR)	Firewall rule configuration, secure log forwarding
Detect (DE)	Centralized logging, dashboards, correlation and alerts
Respond (RS)	Investigation using indexed logs and search queries
Recover (RC)	Log retention, historical analysis, incident review

Architecture Overview

Splunk Enterprise (Host PC) → Acts as the centralized SIEM platform responsible for:

- Receiving logs
- Indexing events
- Hosting dashboards and searches

Splunk Universal Forwarder (Client PCs) → Installed on each client system (e.g., Windows Server) to securely forward logs to the Splunk Enterprise instance.

Implementation Steps

1.) Install Splunk Enterprise on the Host PC

NIST CSF: Identify (ID), Detect (DE)

- Deployed Splunk Enterprise on the host system to serve as the centralized log collection and analysis platform.
- This system functions as the **SIEM indexer and search head**, providing visibility into all ingested events.

2.) Install Splunk Universal Forwarder on Client Systems

NIST CSF: Identify (ID), Protect (PR)

- Installed the Splunk Universal Forwarder on Windows Server and client PCs.
- The forwarder securely collects local system and security logs and prepares them for transmission to the SIEM.

3.) Create Input Configuration on Client Devices

NIST CSF: Identify (ID), Detect (DE)

- Configured **inputs.conf** on each client to define:
    - Which log sources to collect
    - How logs are categorized and forwarded
- This ensures logs are indexed correctly and supports asset and log source identification.

4.) Configure Outbound Firewall Rules on Client PCs

NIST CSF: Protect (PR)

- Created outbound firewall rules on client systems to allow log traffic to be sent to the Splunk Enterprise host.
- Restricted outbound communication to specific ports and destinations to minimize exposure.

5.) Configure Indexes on Splunk Enterprise (Host)

NIST CSF: Identify (ID), Detect (DE)

- Created custom indexes on the Splunk Enterprise host to organize incoming logs.

- Indexing enables efficient searching, correlation, and long-term log retention.

6.) Configure Forwarding & Receiving Ports

NIST CSF: Detect (DE), Protect (PR)

- Enabled receiving on Splunk Enterprise using a designated TCP port.
- Ensured the port configured on client forwarders matched the listening port on the SIEM.
- This step establishes secure and reliable log ingestion.

7.) Configure Inbound Firewall Rules on Host PC

NIST CSF: Protect (PR)

- Configured inbound firewall rules on the host system to allow log traffic only from authorized client devices and specific ports.
- Prevents unauthorized systems from sending data to the SIEM.

8.) Search and Reporting on Splunk

DETAILED IMPLEMETATION PROCESS

1.) Downloading and Installing Splunk Components

1.1.) Downloading Splunk Enterprise and Splunk Universal Forwarder

The first step in this deployment is to download the required Splunk components:

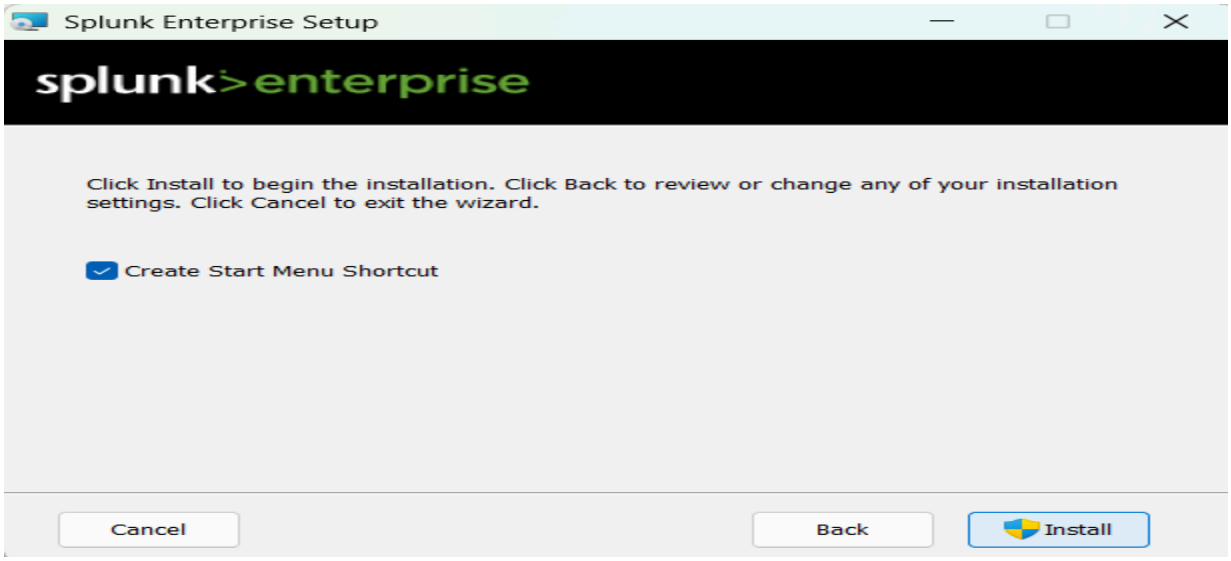
- **Splunk Enterprise (Host PC):**
  Used as the centralized SIEM platform for log ingestion, indexing, and analysis.
  Download link:
  https://drive.google.com/file/d/1sTzr2x4uw14Sc3Pq7xSelHn6T-Y4jjIL/view

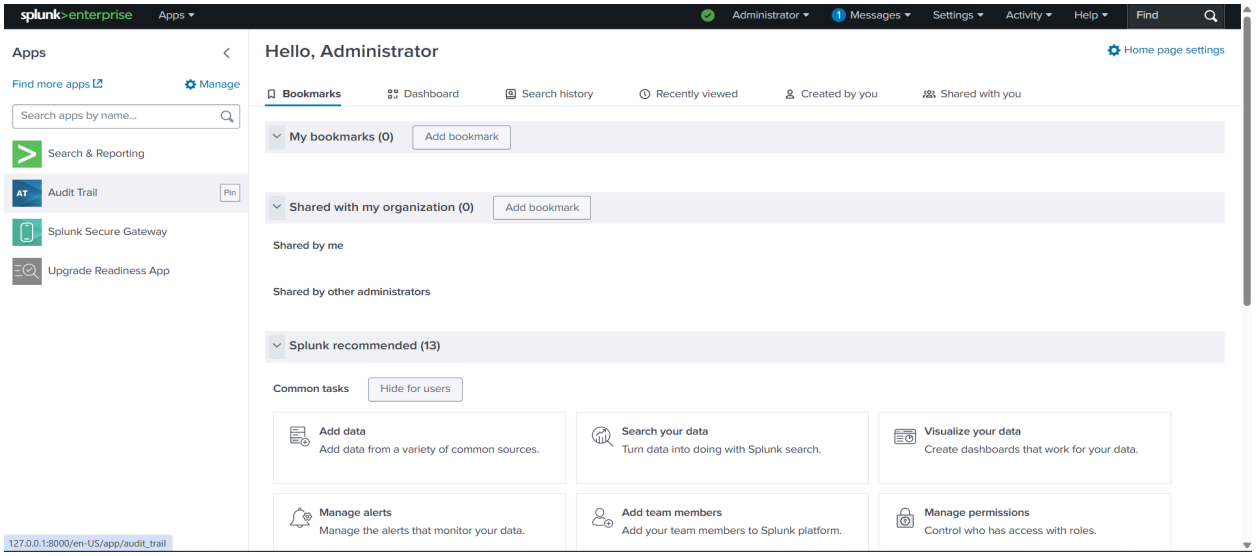
- **Splunk Universal Forwarder (Client PC):**
  Installed on client systems to securely collect and forward logs to Splunk Enterprise.
  Download link:
  https://drive.google.com/file/d/1LcpmikFiJvEHEIi6qcB-mmqVI4xukiRU/view

INSTALLATIONS

1.2.) Installing Splunk Enterprise on the Host PC

After downloading the Splunk Enterprise installer, it is installed directly on the **host machine**, which will function as the **SIEM server**. This system is responsible for receiving, indexing, and visualizing logs forwarded from client systems.



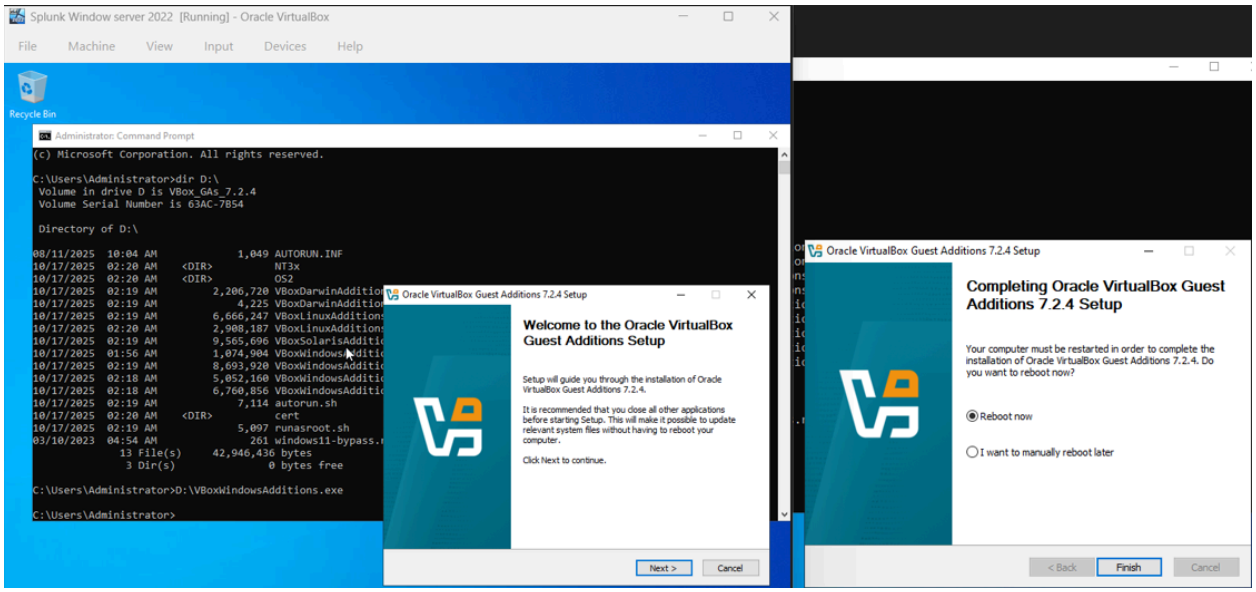


1.3) Mounting and Transferring Splunk Universal Forwarder to the Client VM

The Splunk Universal Forwarder is installed on the **client PC**, which in this lab environment is a **Windows Server virtual machine**. To transfer the installer from the host to the VM, VirtualBox Guest Additions and shared folders are used.

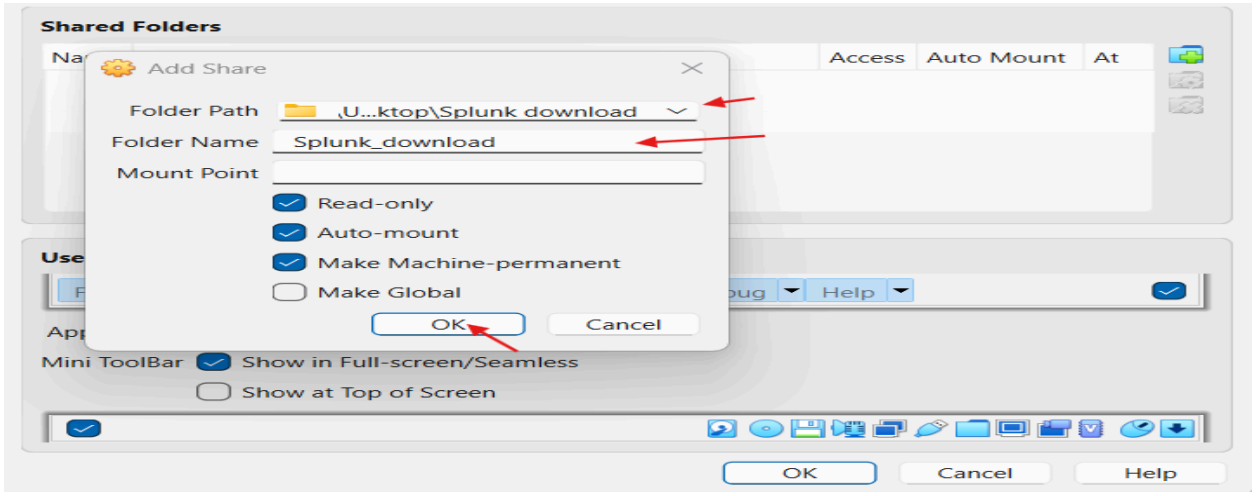
1.3.1.) Installing VirtualBox Guest Additions (Enables Drag & Drop and File Sharing)

1. Open Command Prompt on the client VM as Administrator.
2. Run the command: '**dir D:**' (This confirms the Guest Additions ISO is mounted)
3. Execute the installer: Type '**D:\VBoxWindowsAdditions.exe**'
4. Follow the Guest Additions installation wizard and reboot the VM if prompted.



1.3.2.) Configuring Shared Folders

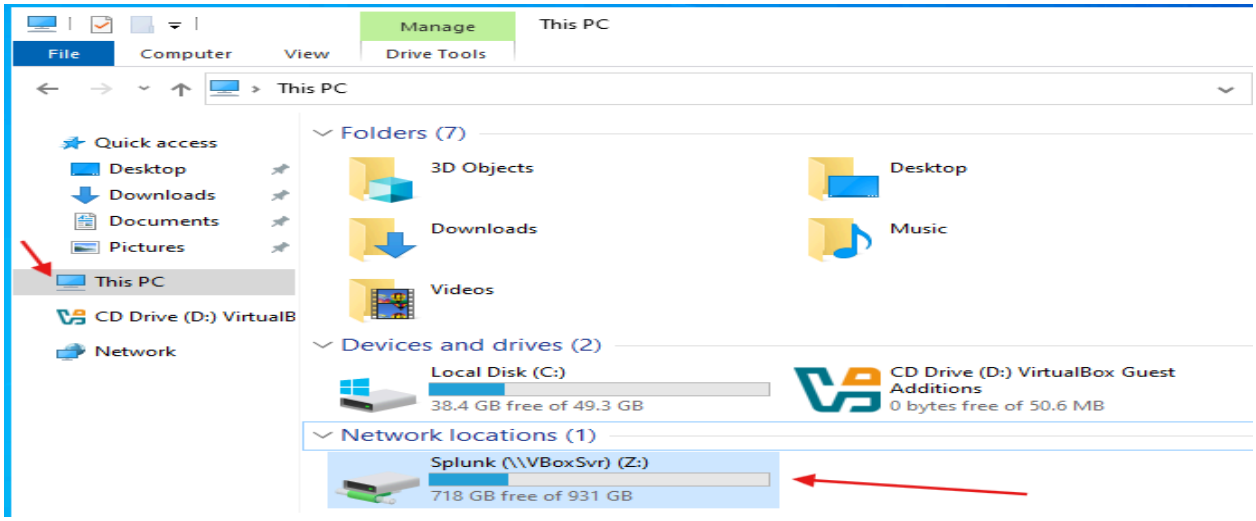
1. In VirtualBox, navigate to:
   Devices → Shared Folders → Shared Folder Settings
2. Select the intended host folder containing the Splunk Universal Forwarder installer.
3. Apply the settings and confirm access.



1.3.3.)Transferring the Installer to the Client VM

1. Open File Explorer on the client VM.
2. Navigate to ‘This PC and locate the shared folder.

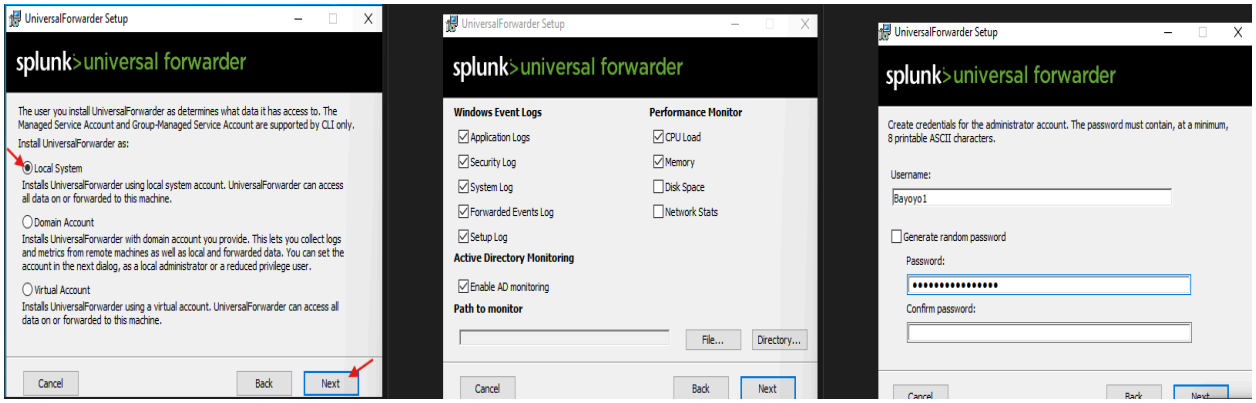
3. Copy or drag the Splunk Universal Forwarder installer to the client desktop

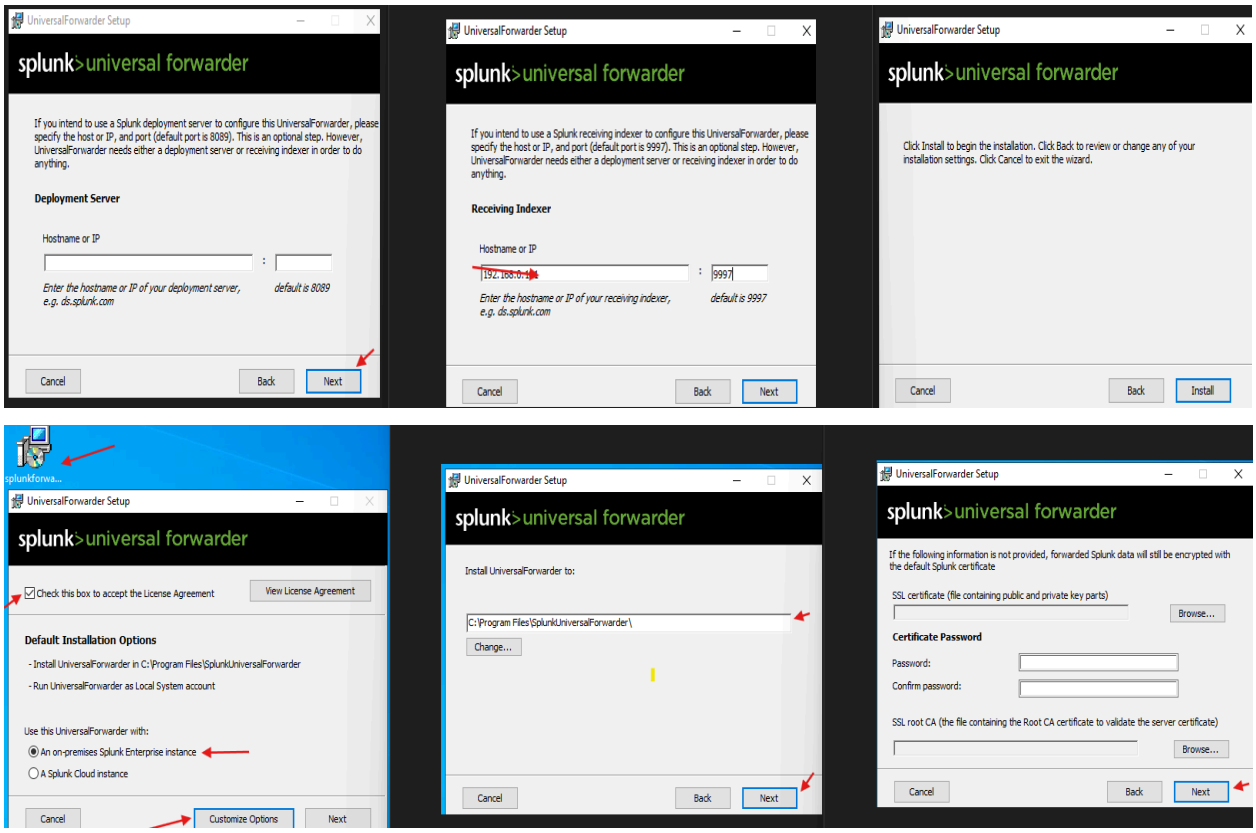


2.) Installing Splunk Universal Forwarder on the Client PC

- Once transferred, the Splunk Universal Forwarder installer is executed on the Windows Server client. This prepares the system to securely collect local logs and forward them to the Splunk Enterprise host for centralized monitoring and analysis.
- The Splunk Universal Forwarder is installed on the **client server (Windows Server VM)** to **collect and forward local system and security logs** to the centralized **Splunk Enterprise instance**.
- This client system **does not function as a log collector or indexer**—its sole role is to securely transmit logs to the SIEM host for analysis and monitoring.

Below are screenshots of the Installation Steps





Once installation is complete:

- The client server begins forwarding logs to the Splunk Enterprise host
- Logs are ingested into the configured index
- Events become visible in the Splunk dashboard for search, correlation, and analysis

This implementation establishes a secure and centralized logging capability that enhances organizational visibility into system activity, supports proactive threat detection, and provides a scalable SIEM foundation aligned with enterprise Security Operations Center (SOC) monitoring, governance and incident response objectives.

3.) Create Input Configuration on Client Devices

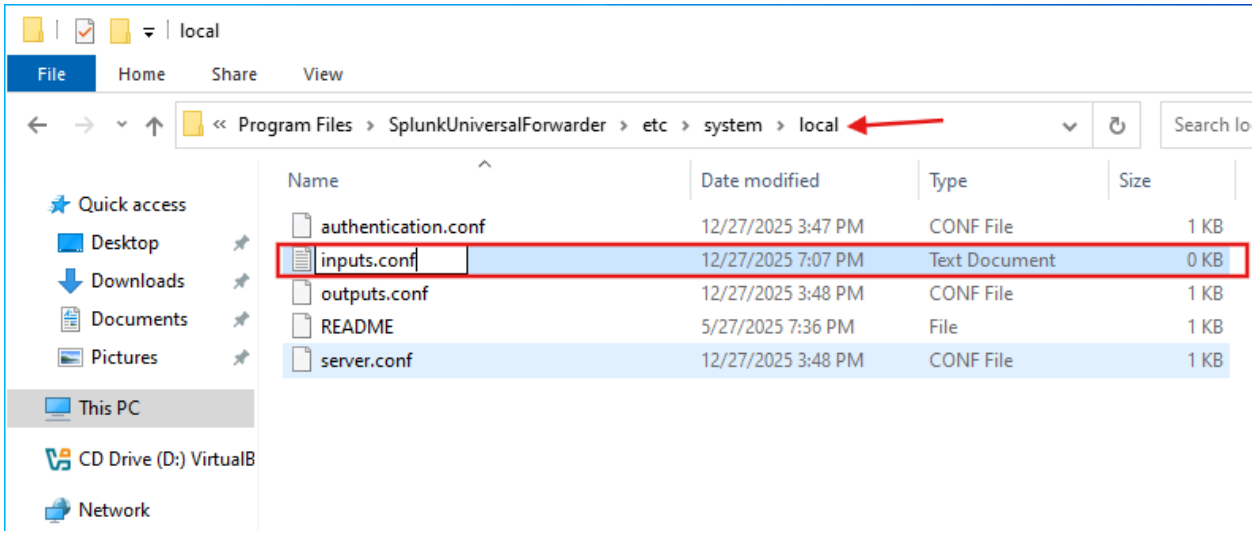
The input configuration defines which logs are collected on the client system and how they are forwarded to the centralized Splunk Enterprise instance. This ensures that only

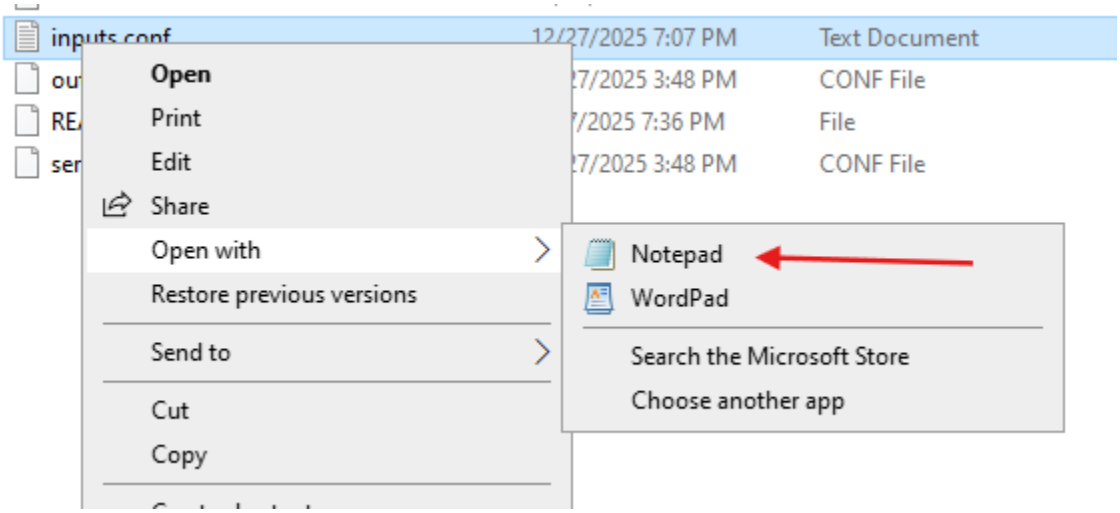
relevant security, system, and application logs are ingested, enabling effective monitoring, detection, and investigation.

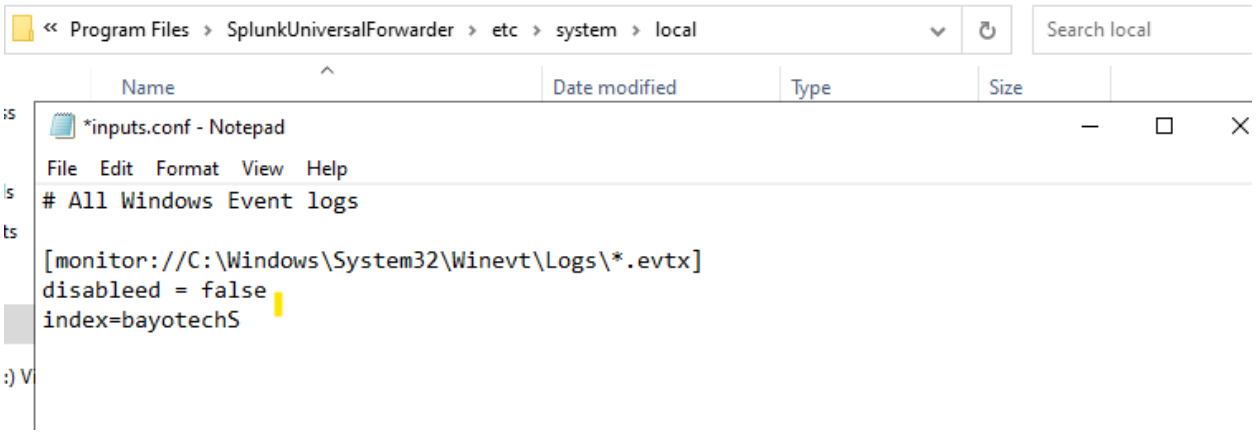
On Splunk Universal Forwarder, this configuration is managed through the **inputs.conf** file.

Path to Locate Input configuration file →

- 'C:\Program Files\SplunkUniversalForwarder\etc\system\local'
- Create a new text file name → 'inputs.conf' → Open the file using Notepad(Run as Administrator).
- Input Configuration







This configuration was able to ;

- Centralizes Windows system and security logs for real-time monitoring and investigation.
- Sends endpoint events to a dedicated Splunk index to support correlation, alerting, and threat detection.
- Maintains original event formatting to improve visibility and reduce parsing errors.
- Preserves native event structure using **XML rendering**, ensuring accurate field extraction and reliable detection logic.

4.) Configure Outbound Firewall Rules on Client PCs

Purpose of Firewall Rules

Firewalls are security controls that regulate **inbound and outbound network traffic** based on predefined rules. These rules can be applied to **programs, ports, services, or custom traffic patterns**, allowing organizations to enforce strict communication policies and reduce attack surface.

Firewall rules are generally categorized into:

- **Inbound Rules:** Control traffic entering a system
- **Outbound Rules:** Control traffic leaving a system

Why an Outbound Rule Is Required

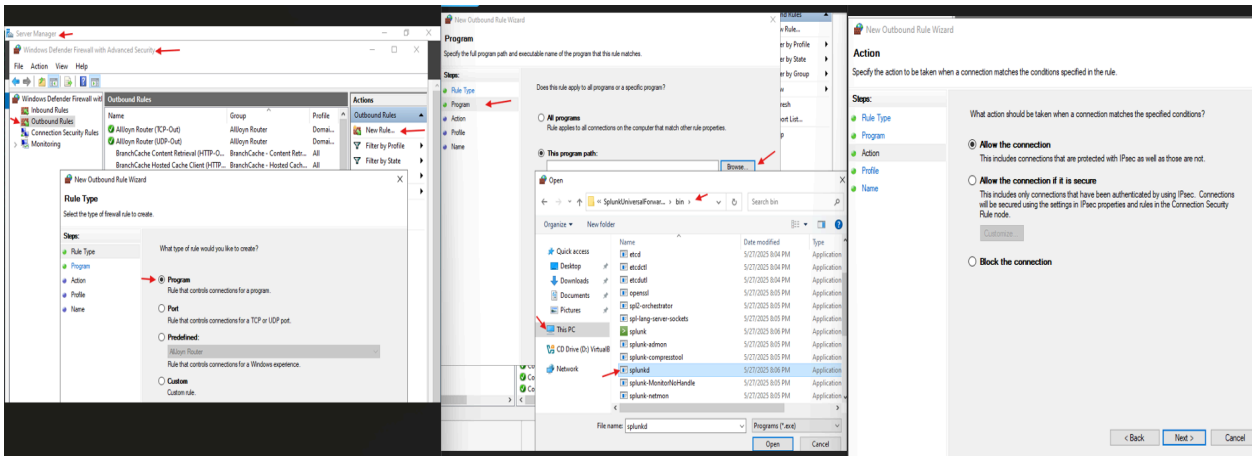
In this SIEM deployment, client systems (log sources) must be able to **send log data to a centralized Splunk Enterprise server**.
To support this, an **outbound firewall rule** is required on each client device to explicitly allow the Splunk Universal Forwarder service to transmit logs.

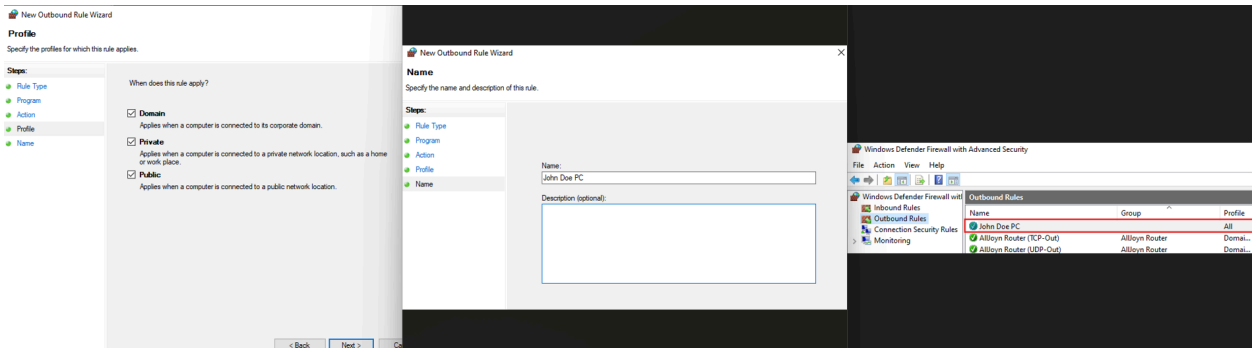
Steps to Configure an Outbound Firewall Rule (Client PC)

1. Open **Server Manager** (or Control Panel on non-server systems).
2. Navigate to:
   Windows Defender Firewall with Advanced Security
3. Select **Outbound Rules**.
4. From the **Actions** pane, click **New Rule**.

Rule Configuration

- Select **Program** as the rule type.(This allows traffic based on a specific executable rather than an open port).
- Specify the program path for the Splunk Universal Forwarder daemon:(C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe)
- Select **Allow the connection**.
- Apply the rule to the appropriate profiles:
  - Domain
  - Private
  - Public (as required by the environment)
- Assign a descriptive name to the rule (e.g.,Splunk Outbound Rule.
- Click **Finish** to apply the rule.





Security Impact→

Once configured:

- The client system is permitted to forward logs to the SIEM
- Only the authorized Splunk forwarder process is allowed outbound communication
- Unnecessary outbound traffic remains restricted

This approach supports **secure, controlled log forwarding** while maintaining firewall enforcement.

5.) Configure Indexes on Splunk Enterprise (Host)

Purpose of Indexing

Indexes in Splunk define where incoming log data is stored and organized. Proper index configuration is essential for efficient searching, correlation, retention, and security monitoring within a SIEM environment.
In this setup, custom indexes are created on the Splunk Enterprise host to receive and store logs forwarded from client systems.

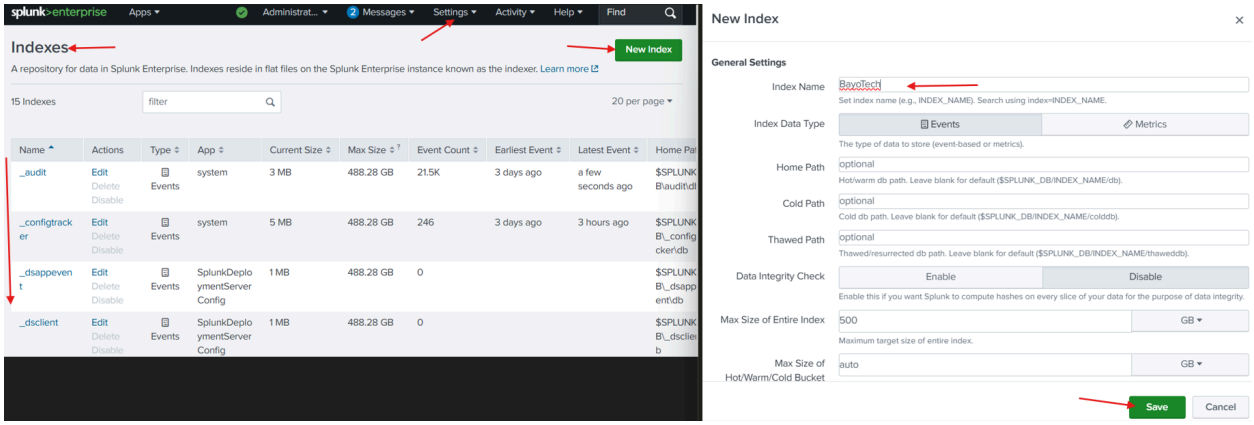
Steps to Create a New Index

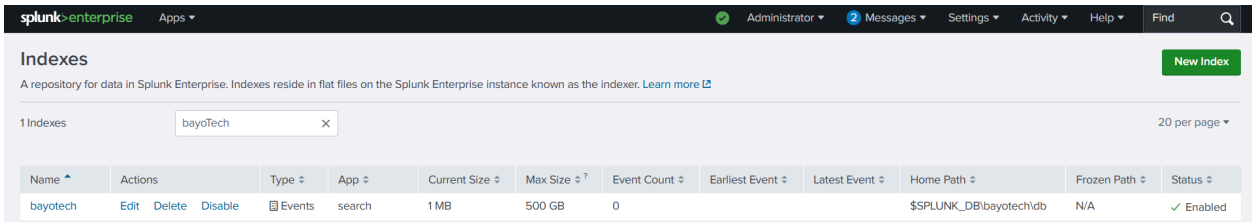
1. Log in to the **Splunk Enterprise Web Interface** on the host PC.

2. Navigate to:
   Settings → Indexes
3. Click **New Index** to create a custom index.
4. Under **General Settings**:
   - Enter a descriptive **Index Name** (BayoTech)
   - Leave other settings at default unless retention or storage customization is required
5. Click **Save** to create the index.

Verifying Index Creation

- Once saved, the newly created index will appear in the index list.
- Use the Filter by Name option to quickly locate and confirm the index.
- The index is now ready to receive incoming logs from Splunk Universal Forwarders.





Proper indexing:

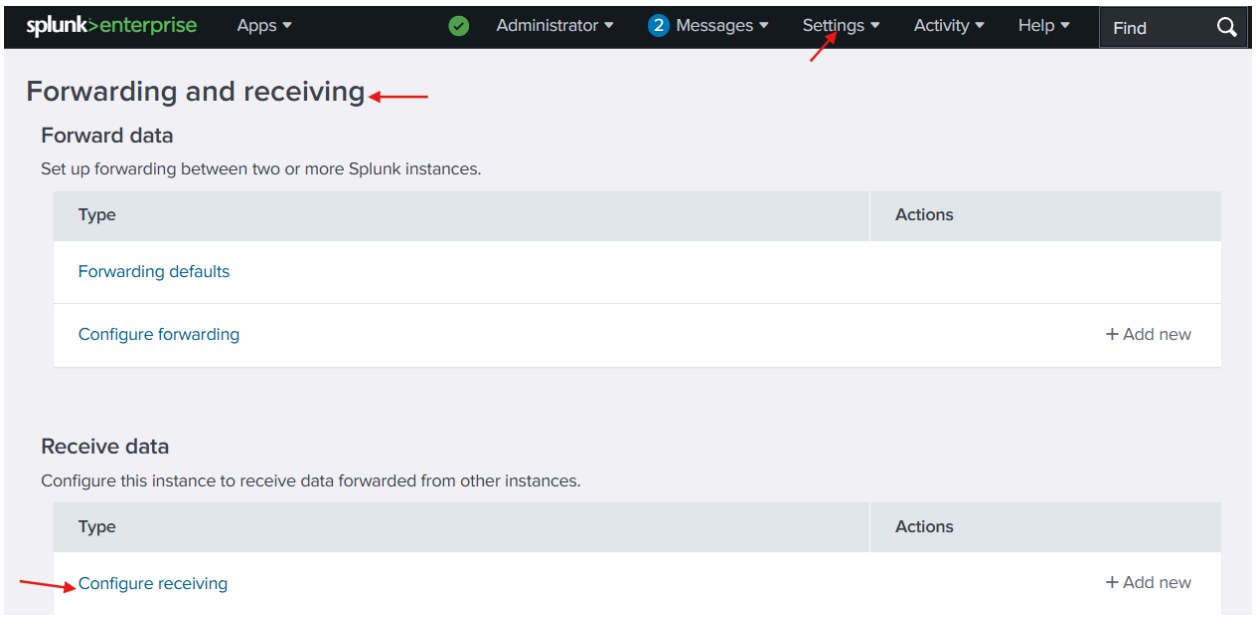
- Ensures log data is logically separated and organized
- Improves search performance and incident investigation
- Supports compliance and retention requirements
- Enables effective correlation across multiple log sources

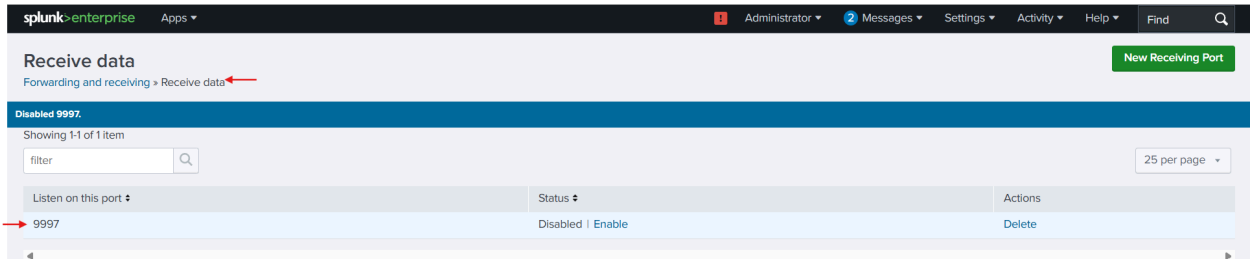
6.) Configure Forwarding & Receiving Ports

Purpose of Forwarding and Receiving Configuration

Splunk Enterprise must be explicitly configured to listen for incoming data from Splunk Universal Forwarders. This is accomplished by enabling a receiving port, which allows the SIEM to securely accept log data from authorized client systems.

In this environment, TCP port **9997** is used, which is the **default and recommended Splunk receiving port.**





Result and Validation

- Splunk Enterprise is now actively listening on TCP port 9997.
- This port allows incoming logs and indexed data from Splunk Universal Forwarders.
- Client systems configured with the same port can successfully forward events to the SIEM.

7.) Configure Inbound Firewall Rules on Host PC

Purpose of Inbound Firewall Rules

Inbound firewall rules control which external systems are allowed to send traffic into the Splunk Enterprise host. In a SIEM environment, this is critical to ensure that only authorized log sources (Splunk Universal Forwarders) can transmit data to the SIEM.
In this setup, the Splunk host must allow inbound traffic on TCP port 9997, which is the designated receiving port for Splunk log ingestion.

This Is Required;

- Client systems forward logs to the SIEM over TCP
- Without an inbound rule, the Splunk host would block incoming log data
- Restricting inbound access reduces attack surface and enforces least privilege

Steps to Configure Inbound Firewall Rules (Splunk Host)

1. On the Splunk Enterprise host PC, open:
   'Windows Defender Firewall with Advanced Security'
2. Select **Inbound Rules** from the left panel.
3. In the Actions pane, click New Rule.
4. Select **Port** as the rule type and click **Next**.
5. Choose:**TCP , Specific local ports:9997**
6. Click **Next**, then select **Allow the connection**.
7. Apply the rule to the appropriate profiles:
- Domain
- Private (Public profile should only be selected if required by the environment)
8. Assign a descriptive name, such as:
    - **Splunk-Receiving-Port-9997**

- **SIEM-Inbound-Log-Ingestion**

Click **Finish** to enable the rule.

This configuration:

- Enforces least-privilege network access
- Prevents unauthorized systems from sending data to the SIEM
- Supports secure log ingestion and centralized monitoring
- Aligns with enterprise SOC and SIEM security standards

8.) Search and Reporting on Splunk

Purpose of Search and Reporting

Splunk's Search & Reporting capability allows security analysts to efficiently query, filter, and analyze large volumes of log data collected from multiple sources. This functionality enables analysts to isolate relevant events, investigate suspicious activity, and support detection and incident response workflows.
Rather than reviewing raw logs manually, analysts can apply targeted search criteria to quickly identify events relevant to their investigative or monitoring objectives.

Accessing Search & Reporting

1. From the Splunk Enterprise dashboard, navigate to Apps.
2. Select Search & Reporting to open the primary search interface.

Performing Searches

- Use the **search bar** to enter specific criteria such as:
    - Index names
    - Hostnames
    - Event types
    - Keywords related to security activity

Interpreting Search Results

- The Events tab displays the total number of matching events returned by the search.
- Events may originate from multiple devices and log sources.
- The left-hand panel provides summarized metadata, including:
    - Hosts
    - Source types
    - Event severity indicators
    - Field value counts

This summary view helps analysts quickly identify patterns and anomalies.

Viewing and Analyzing Event Details

- Select specific fields to drill down into individual event logs.
- Expand events to review:
    - Timestamps
    - Source IP addresses
    - User accounts
    - Event messages and codes

This granular visibility supports deeper investigation and root cause analysis.

9.) Analyzing Events in Splunk (Investigation Workflow)

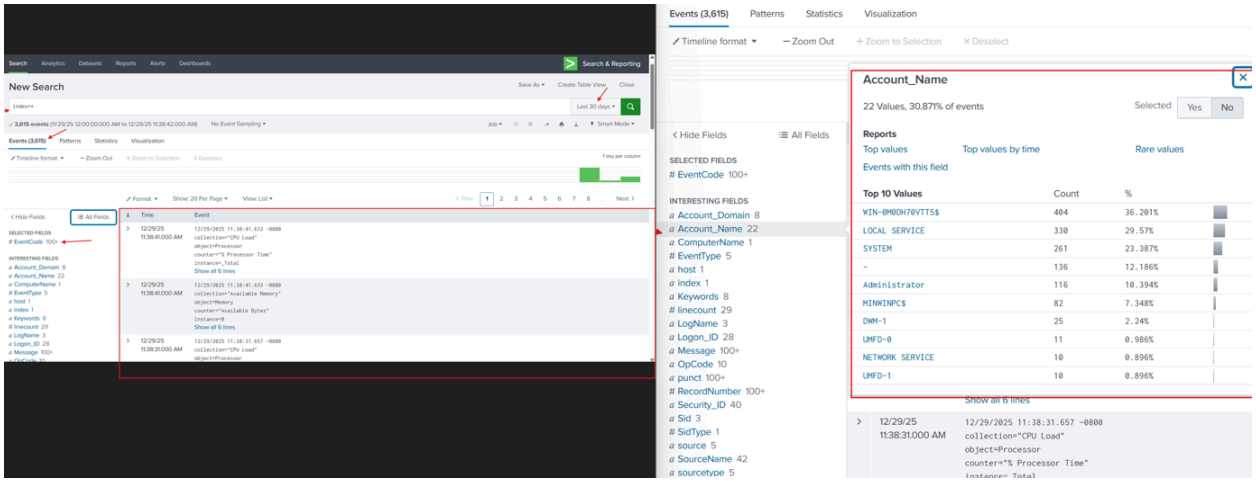
Purpose

Event analysis in Splunk allows analysts to **pivot from a single event to a broader investigation**, enabling identification of related activity across hosts, time ranges, and event categories. This process is critical for incident triage, root cause analysis, and threat hunting.

STEPS→

Step 1: Identify the Host from an Event

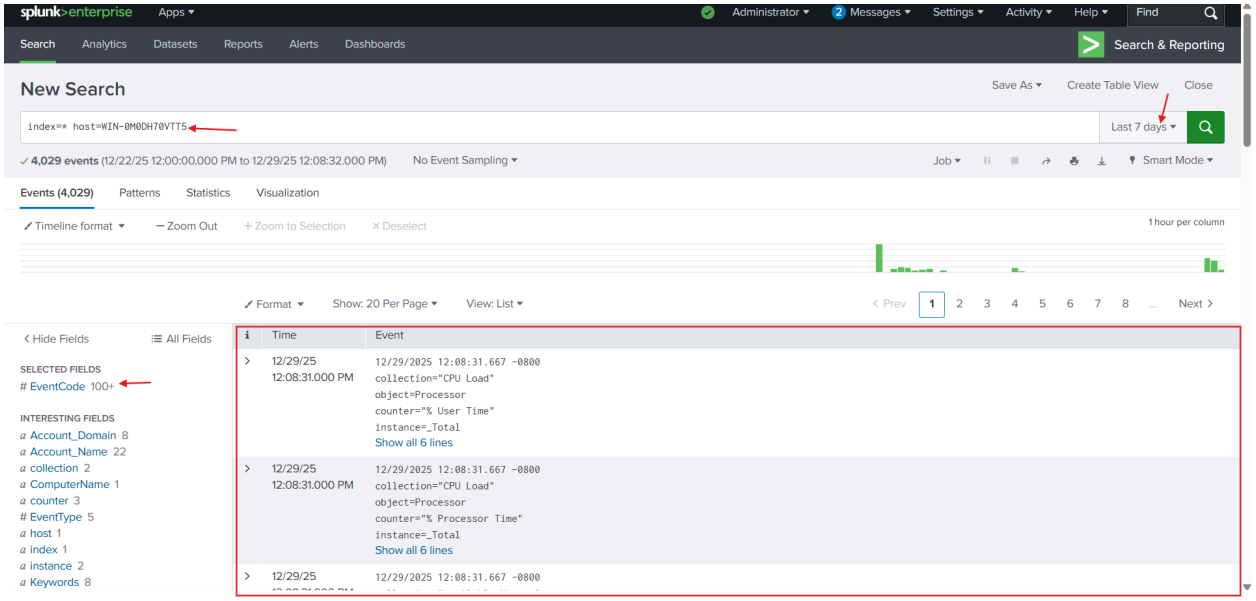
1. Expand a relevant event in the **Events** view.
2. Locate the Host field and copy the value.
   Example host in this project: WIN-0M0DH70VTT5



Step 2: Search All Events for the Host

Use the host value to retrieve all related logs: index=* host=WIN-0M0DH70VTT5

- Set the **time range** to **Last 7 days** to provide investigation context.
- This search aggregates events from all indexes associated with the host

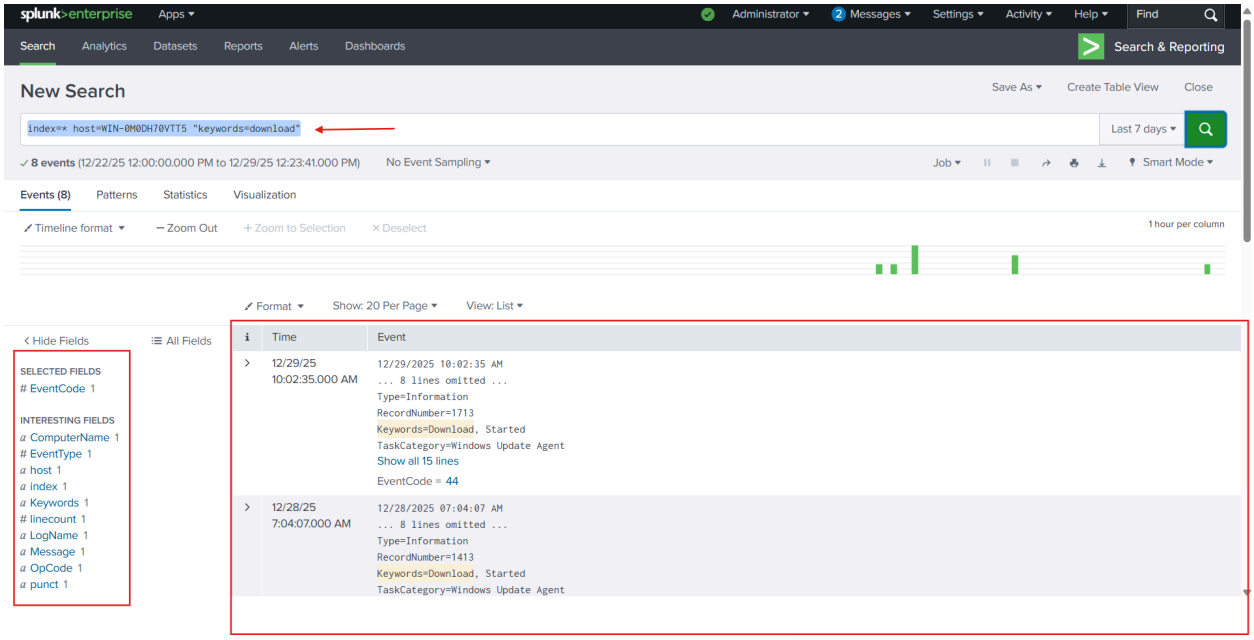


Step 3: Keyword-Based Event Filtering

Search for Download-Related Activity index=* host=WIN-0M0DH70VTT5 "download"

This query identifies events related to file downloads or update activity.

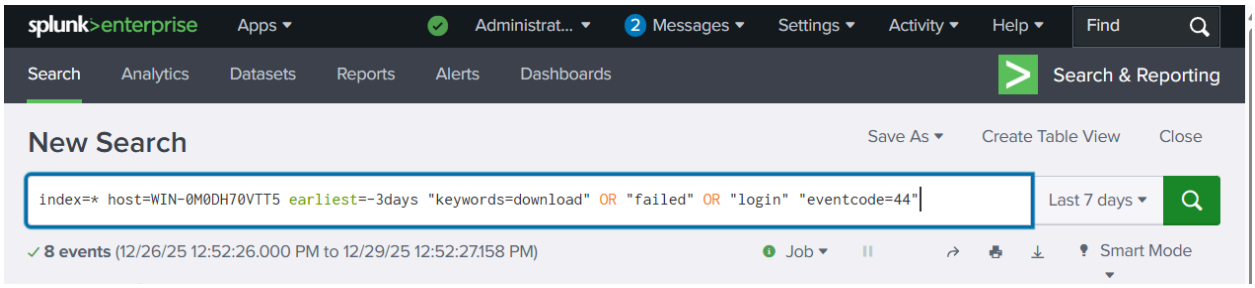
Example observation: (TaskCategory=Windows Update Agent indicating legitimate system update behavior)



Search for Multiple Keywords

Download OR Failed Events → index=* host=WIN-0M0DH70VTT5 ("download" OR "failed")

Download, Failed, OR Login Events → index=* host=WIN-0M0DH70VTT5 ("download" OR "failed" OR "login" “eventcode=44”

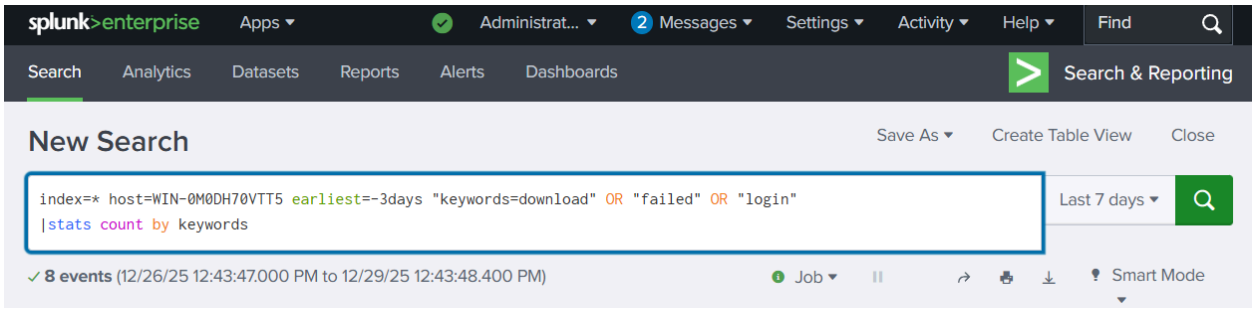


Step 4: Time-Bound Analysis with Statistics

To limit results to a specific time window and summarize findings:

index=* host=WIN-0M0DH70VTT5 earliest=-3d ("download" OR "failed" OR "login")
| stats count by _raw

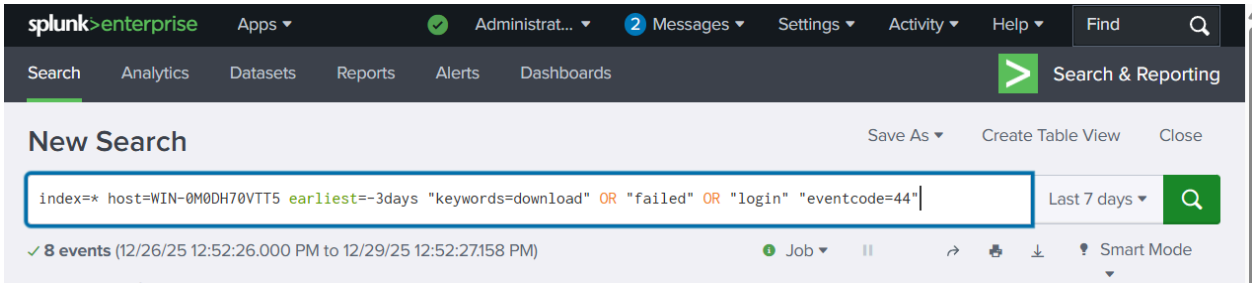
This reduces noise and focuses on recent activity.



Step 5: Filtering by Event Code

To isolate specific event types using an event code (example: EventCode 44):

index=* host=WIN-0M0DH70VTT5 earliest=-3d ("download" OR "failed" OR "login") EventCode=44



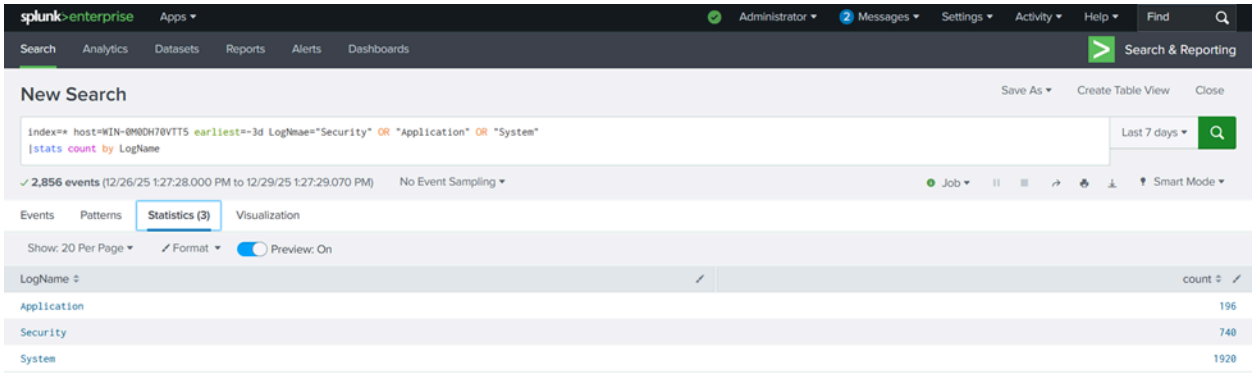
This is useful when investigating known error codes, failures, or security-relevant events.

Step 6: Scanning Security, Application, and System Logs

To analyze core Windows log categories over the last three days:

index=* host=WIN-0M0DH70VTT5 earliest=-3d (LogName="Security" OR LogName="Application" OR LogName="System")

| stats count by LogName



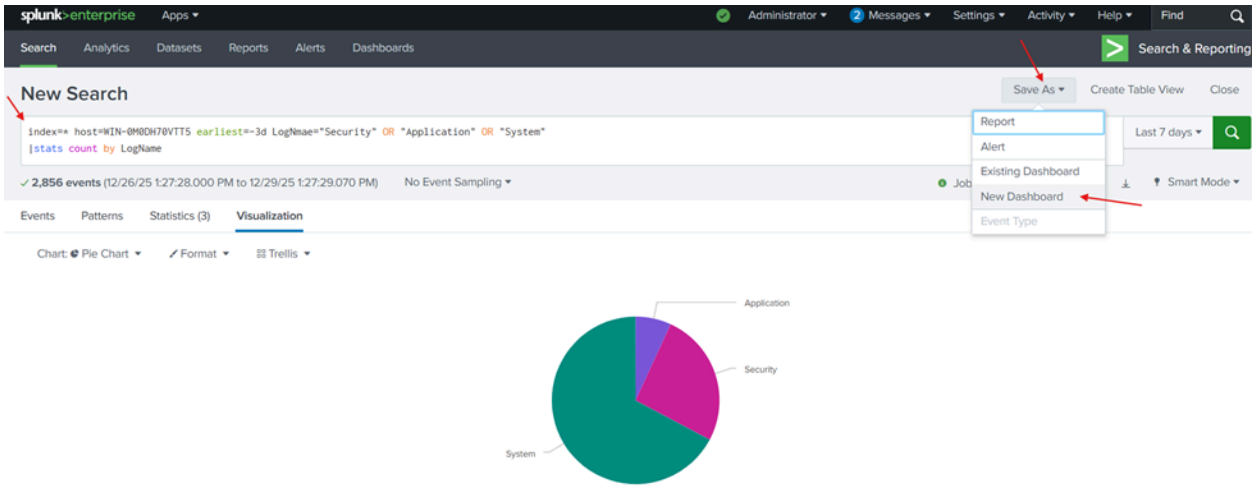
This provides a high-level breakdown of activity across key log sources.

Visualizing and Saving Results as a Dashboard

Search results and analysis performed in Splunk can be **visualized and saved as a custom dashboard**. This allows analysts to transform raw event data into clear visual insights such as tables, charts, and time-series graphs.

By saving searches as dashboard panels, recurring investigations and monitoring use cases can be quickly accessed without re-running manual queries. Dashboards also provide real-time visibility into trends, anomalies, and security-relevant activity across hosts and log sources.

This capability supports continuous monitoring, operational reporting, and SOC workflows by presenting actionable intelligence in an easily consumable format.



Use of Splunk for Security Investigation

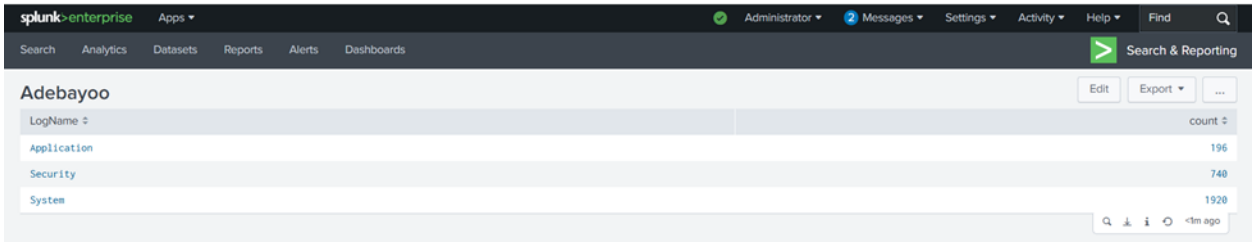
Splunk can be used for a wide range of operational and analytical purposes; however, in this project, it is primarily leveraged as a **security investigation and monitoring platform**.

Splunk enables analysts to investigate key security questions such as:

- Who logged in and logged out of a system
- When authentication events occurred
- Whether a user logged in from an unusual or unexpected location
- Whether login behavior deviates from established baselines and appears suspicious

By correlating authentication, system, and application logs, Splunk provides visibility into user activity and potential security incidents.

To support continuous monitoring and repeatable analysis, these investigations are translated into **custom dashboards**. Dashboards present authentication trends, anomalous activity, and security-relevant events in a visual format, enabling faster detection, triage, and response.



Using Splunk for Alerting and Detection

Purpose of Alerts in Splunk

In addition to log collection and investigation, Splunk can be used to **create automated security alerts**. Alerts enable proactive detection by notifying analysts when specific events, patterns, or Indicators of Compromise (IOCs) are observed in log data.

Once an event code, keyword, or behavior is identified as suspicious during analysis, an alert can be configured to trigger whenever that condition is detected in the future.

Creating an Alert from a Search

1. Perform a search that identifies the event of interest.
   index=windows EventCode=4625 (this detect failed login attempts)
2. Validate that the search reliably returns relevant events and minimizes false positives.
3. Click **Save As** at the top of the search window.
4. Select **Alert**.

Alert Configuration

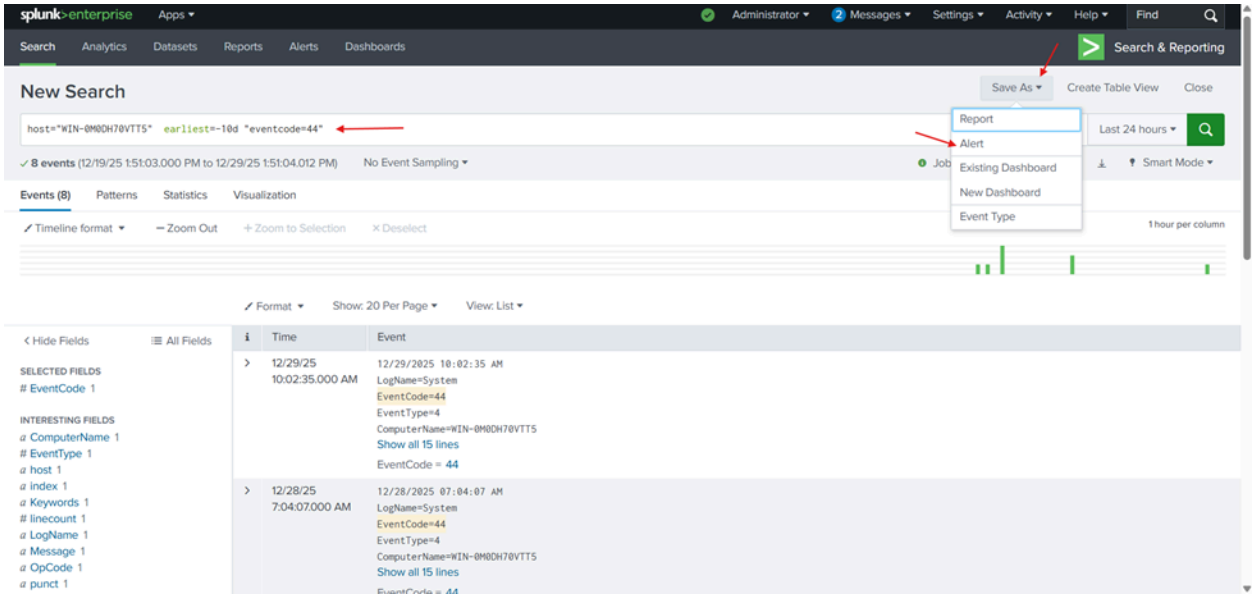
When creating the alert:

- **Alert Type:**
  - Scheduled (recommended for security use cases)

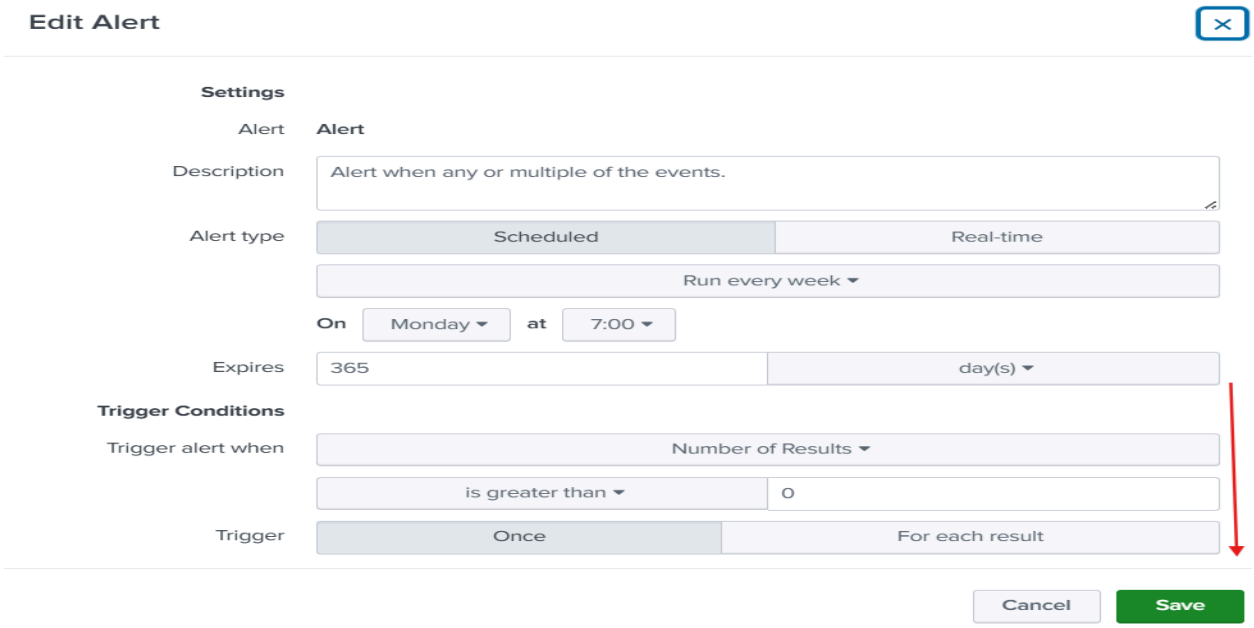
- **Trigger Condition:**
  - Trigger when the number of results is greater than a defined threshold

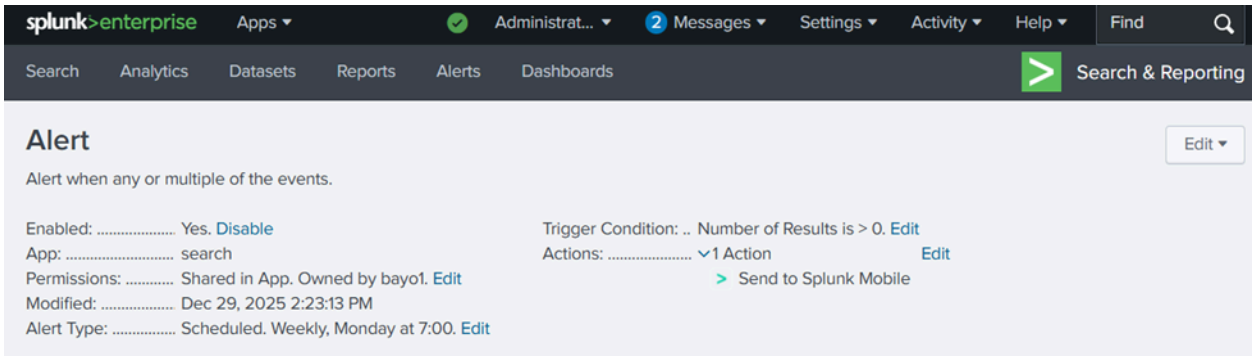
- **Time Range:**
  - Example: Last 5 minutes, Last 15 minutes

- **Trigger Actions:**
  - Send email
  - Create notable event
  - Log event for SOC review



splunk>enterprise
Apps
Administrat...
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
host="WIN-0M0DH70VTT5" earliest=-10d "eventcode=44" OR "4625"
Last 24 hours
9 events (12/19/25 2:12:14.000 PM to 12/29/25 2:12:15.586 PM)
No Event Sampling
Job
Smart Mode
Events (9)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
EventCode 2
INTERESTING FIELDS
a ComputerName 1
EventType 1
a host 1
a index 1
a Keywords 2
linecount 2
a LogName 2
a Message 2
12/29/25
10:02:35.000 AM
12/29/2025 10:02:35 AM
LogName=System
EventCode=44
EventType=4
ComputerName=WIN-0M0DH70VTT5
Show all 15 lines
EventCode = 44
12/28/25
7:04:07.000 AM
12/28/2025 07:04:07 AM
LogName=System
EventCode=44
EventType=4
ComputerName=WIN-0M0DH70VTT5





Conclusion

This Splunk SIEM project demonstrates the end-to-end deployment and use of a centralized security monitoring platform aligned with real-world SOC operations. By installing and configuring Splunk Enterprise and Splunk Universal Forwarders, implementing secure log forwarding, creating custom indexes, and enforcing firewall rules, this project establishes a solid foundation for centralized visibility and threat detection.

Through structured search and reporting, event investigation, and alert creation, the project showcases how raw log data can be transformed into actionable security intelligence. The ability to pivot from individual events to host-wide investigations,

visualize findings through dashboards, and configure automated alerts reflects practical incident detection and response workflows.

Overall, this project illustrates a strong understanding of SIEM architecture, log management, detection logic, and SOC investigation techniques, while aligning monitoring capabilities with the **NIST Cybersecurity Framework (Identify, Protect, Detect, Respond)**. The lab environment closely mirrors enterprise SOC practices and provides hands-on experience applicable to real operational security roles.