Security Information and Event Management

Contents

SIEM 2

SIEM Architecture 2

SIEM Log Management 2

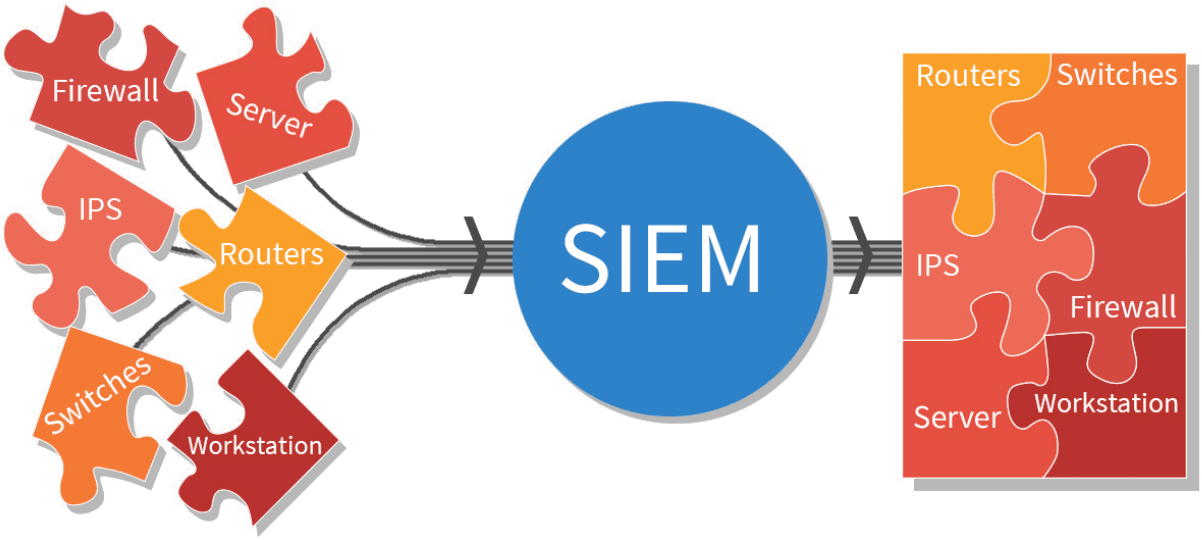
SIEM Components 3

SIEM Deployment Models 4

Common Attack Signatures 5

Command Line Log Analysis 7

Splunk 8



SIEM

A **SIEM** (Security Information and Event Management) is a system that helps collect, analyze, and respond to security-related data from different sources, like servers, applications, and devices in a network. In simple terms, it's like a security monitor that watches everything happening in a company's IT environment and alerts the team to see if it detects something suspicious or harmful.

SIEM Architecture

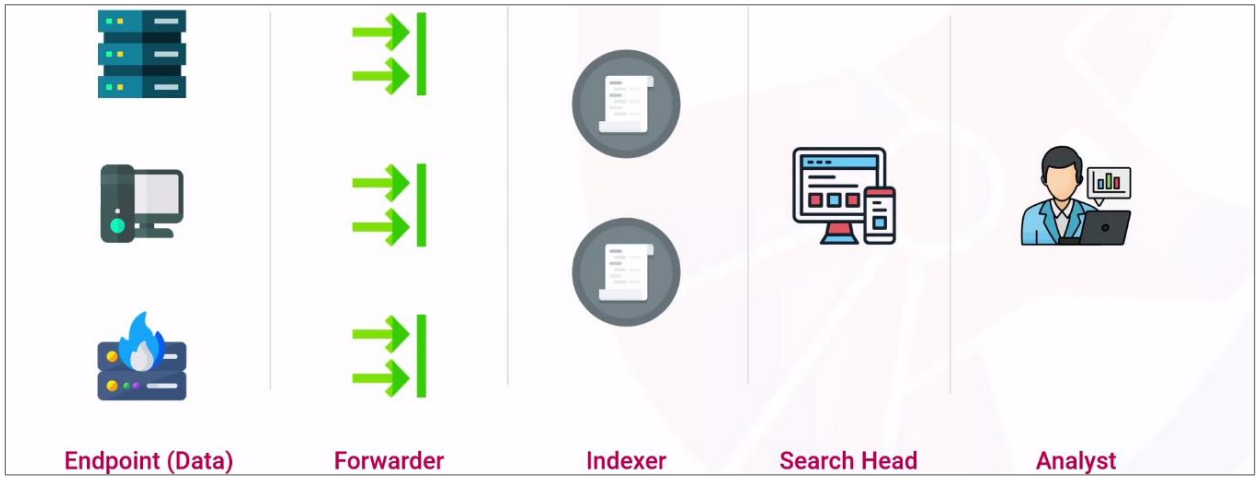
1. **Logs:**
   - These are records of activities happening on different devices (like servers, firewalls, or applications) in a network.
   - Logs contain information such as who accessed the system, what changes were made, and any errors or issues that occurred.
   - SIEM collects logs from various systems in one place for monitoring and analysis.
2. **Security Events:**
   - A security event is any activity detected in the logs that could have a potential impact on security, such as someone trying to access a restricted area of the system.
   - Not all security events are harmful, but they need to be checked to ensure the system is safe.
3. **Security Incidents:**
   - A security incident is when a security event is confirmed to be harmful or a threat, like a cyberattack, data breach, or malware infection.
   - The SIEM helps determine if an event is a real threat or just normal activity.
4. **Alerts:**
   - Alerts are warnings generated by the SIEM when it detects something unusual or dangerous in the system.
   - These alerts notify SOC analysts so they can take action to investigate and stop any threats before they cause damage.

SIEM Log Management

1. **Collection:**
   - SIEM gathers logs from different sources like servers, applications, firewalls, and network devices.
   - It collects data in real-time or at regular intervals to have up-to-date security information.
2. **Aggregation:**
   - SIEM combines all the collected logs from multiple sources into a single system.
   - This makes it easier to manage and analyze the data without having to look at each device separately.
3. **Parsing and Normalization:**
   - **Parsing:** SIEM breaks down the collected logs into specific fields (e.g., IP addresses, usernames, timestamps) for easy processing.
   - **Normalization:** It standardizes the log data from different sources into a common format so that all logs look similar and can be compared or analyzed consistently.

4. **Retention:**
   - SIEM stores the collected and processed logs for a set period (weeks, months, or even years).
   - This allows security teams to look back at historical data for investigations or compliance purposes.
5. **Indexing:**
   - SIEM creates an index or a catalog of the log data, making it easier to search and retrieve specific logs quickly.
   - Indexed data helps speed up investigations when analysts need to find logs related to an incident.
6. **Correlation and Analysis:**
   - **Correlation:** SIEM links together different log entries from multiple sources to identify patterns that may indicate security threats.
   - **Analysis:** It examines the correlated data to detect anomalies or suspicious behaviors that could be part of an attack.
7. **Alerting:**
   - When SIEM detects an issue or unusual pattern (based on predefined rules), it triggers an alert.
   - The alert notifies SOC analysts so they can investigate and respond to potential threats

SIEM Components



1. **Endpoint (Data):**
   - These are different systems or devices like servers, computers, or applications (shown on the left) where data originates. These systems generate logs (records of activities) such as user actions, system errors, or security events.
   - The endpoint devices provide raw log data to be collected by the SIEM system.
2. **Forwarder:**
   - A forwarder is a component responsible for gathering and sending log data from the endpoint devices to the next stage in the SIEM system.
   - It ensures that logs are forwarded to a central system for further processing. It's like a messenger that ensures the data reaches the right place.

3. Indexer:

- The indexer stores and organizes the log data received from the forwarder. It indexes the data, making it easy to search and retrieve when needed.
- The indexer helps with efficient searching and allows logs to be stored for future investigations or compliance checks.

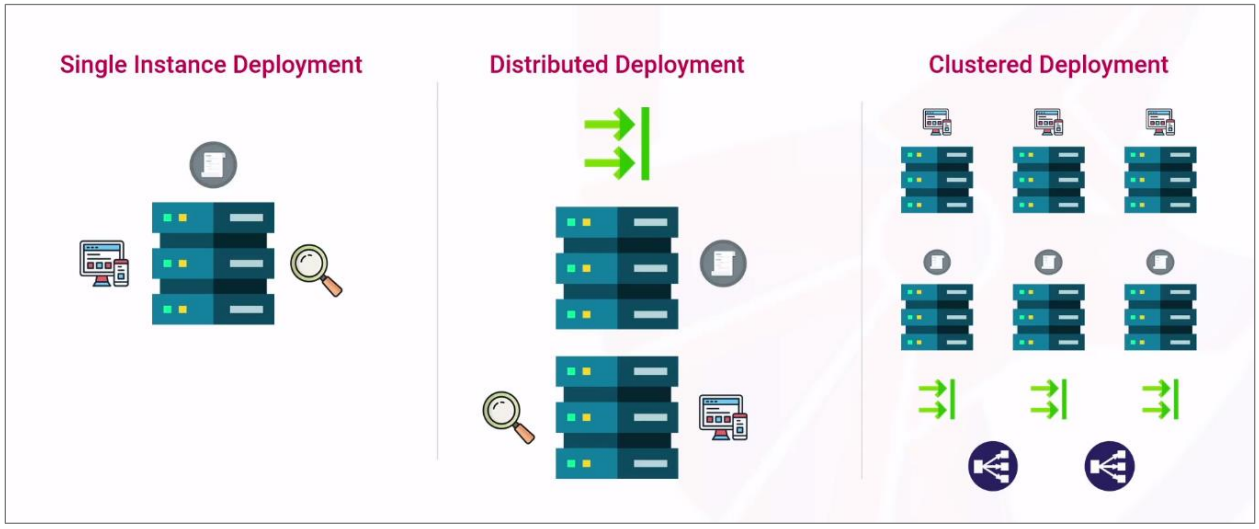
4. Search Head:

- The search head is the interface or tool that allows analysts to search and query the indexed logs.
- It provides the SOC analysts with the ability to perform searches on the log data, run reports, and look for specific security events or patterns.

5. Analyst:

- The security analyst (on the far right) is the person who uses the search head to investigate and respond to any security incidents detected in the log data.
- The analyst investigates alerts, responds to incidents, and ensures that potential threats are addressed.

SIEM Deployment Models



1. Single Instance Deployment:

- In a single instance deployment, everything (data collection, processing, indexing, searching) happens on one server.
- The logs are collected and processed in a single system. Analysts use this system to search, analyze, and monitor security events.
- This is suitable for smaller organizations with lower data volume or fewer security monitoring needs.

2. Distributed Deployment:

- In a distributed deployment, the tasks are split across multiple servers or components.
  - Data collection (forwarders) happens on one set of servers.
  - Data indexing and storage happen on another set of servers.
  - Analysts use a separate system to search and analyze the data.
- This is useful for larger organizations where different parts of the process need to be handled by separate systems for better performance.

3. Clustered Deployment:

- A clustered deployment involves multiple servers working together at every step to handle data collection, processing, and analysis.
  - Multiple forwarders collect data and send it to multiple indexing systems.
  - Data is stored across different servers, and multiple search heads allow analysts to access and analyze the logs simultaneously.
  - Load balancers help distribute the workload evenly across all the systems.
- This deployment is ideal for very large organizations or those with high data volumes. It provides redundancy and ensures that no single system is overloaded, improving performance and reliability.

Common Attack Signatures

1. **SQL Injection:**
   SQL Injection is a type of attack where malicious SQL code is inserted into a query to manipulate or exploit a database. It takes advantage of vulnerable applications that fail to properly validate user input.

   How Hackers Use SQL Injection to Retrieve Data

- **Find Vulnerable Input:** Identify input fields that directly interact with SQL queries.
- **Inject Malicious Query:** Insert SQL code (e.g., "' OR '1'='1"), manipulating the query to retrieve unintended data.
- **Extract Data:** Alter SELECT statements to fetch sensitive information, bypass authentication, or access unauthorized tables.

SQL Injection Characters

Character	Normal Character	URL-Encoded Character
Single Quote	'	%27
Double Quote	"	%22
Space		%20
Semicolon	;	%3B
Dash	-	%2D

2. **Cross Site Scripting (XSS):**
   A vulnerability where attackers inject malicious JavaScript into a webpage, which is then executed in the browser of users visiting that page.

   How XSS is Used by Attackers

- **Inject JavaScript:** Attackers insert malicious code to execute in user's browsers.
- **Hijack Sessions & Steal Cookies:** Gain unauthorized access and impersonate users.
- **Deface Websites:** Modify content to mislead or disrupt users.

3. **Command Injection:**
   An attack where malicious commands are inserted into an application to execute on the server, exploiting insufficient input validation.

   How Attackers Use Command Injection

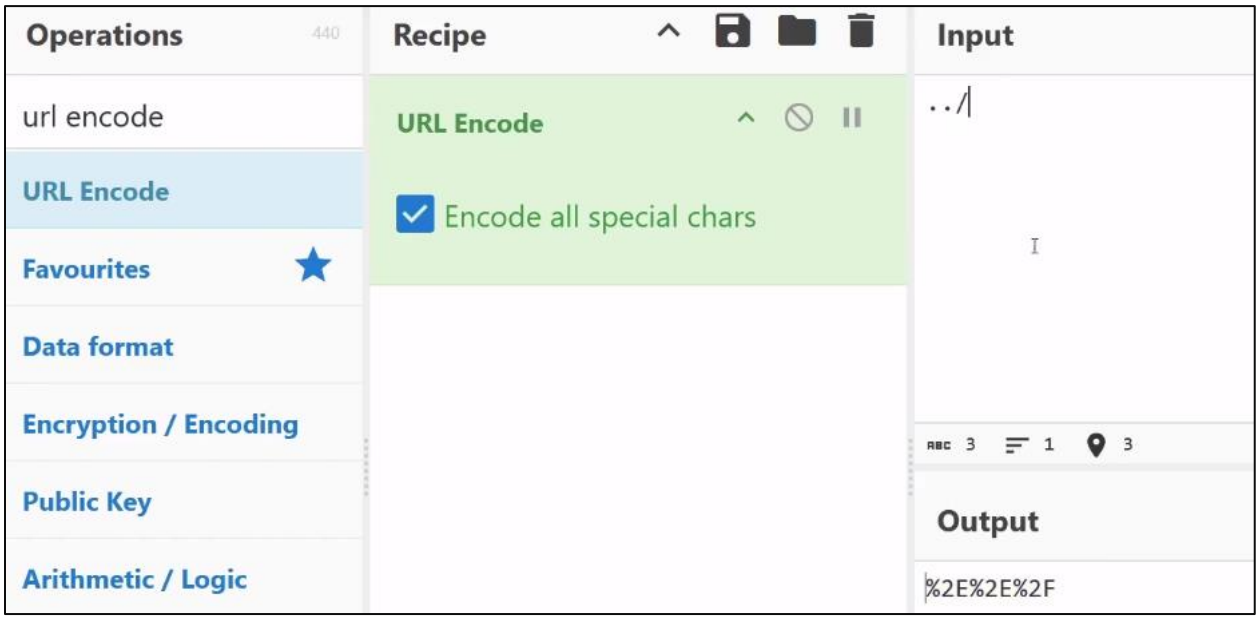
   - **Inject Malicious Commands:** Attackers input OS commands instead of expected data, making the server execute them.
   - **Execute System Commands:** Attackers can run commands like ls, cat, or ping to retrieve information, alter files, or monitor network connections.
   - **Escalate Privileges:** By chaining commands, attackers may gain unauthorized access, allowing them to control or alter the system.
   - **Use Special Characters:** Characters like ;, &&, |, && are used to separate or chain commands, bypassing input restrictions.

4. **Path Traversal**

   An attack where an attacker manipulates file paths to access restricted directories and files outside the intended directory structure.

   How Attackers Use Path Traversal

   - **Manipulate File Paths**: Attackers use ../ sequences (known as "directory traversal") to navigate up the directory hierarchy.
   - **Access Sensitive Files**: By crafting file paths, they can access sensitive files like /etc/passwd (on Linux) or C:\Windows\System32\config\SAM (on Windows).
   - **View or Modify Data**: Path traversal may allow attackers to read confidential data, alter configuration files, or even execute unauthorized code if the server interprets file contents.
   - **Use Special Characters**: Characters like ../, ..%2f (URL encoded) help bypass filters and gain access to restricted directories.



Command Line Log Analysis

Commands used for log analysis

1. **head access.log -n 1**

Displays the first line of access.log. This is useful to quickly check the format or structure of the log file, ensuring you know how to parse it.

2. **cut access.log -d " " -f 1 | sort | uniq**

Extracts the first field (typically the IP address) from access.log, sorts it, and displays unique IPs. This provides a quick list of all unique visitors or sources accessing the server.

3. **cut access.log -d " " -f 1 | sort | uniq -c**

Extracts the IP addresses, sorts them, and counts occurrences of each. This is helpful to see the frequency of visits per IP, identifying patterns or potential high-volume users.

4. **cut access.log -d " " -f 1 | sort | uniq -c | grep -v " 1 " | sort -nr**

Shows IPs that appear more than once, sorted by frequency in descending order. This helps to spot repeated access from the same IP, which may indicate suspicious behavior like brute-force attempts.

5. **grep "Mozilla/5.0 (Hydra)" access.log | awk '{print $1}' | sort | uniq -c**

Finds lines with the "Hydra" user agent in access.log, extracts the IPs, and counts them. This is helpful to detect IPs associated with Hydra, a tool often used in automated attacks.

6. **grep "Mozilla/5.0 (Hydra)" access.log | awk '$9 > 200'**

Filters logs with the "Hydra" user agent where the HTTP status code is greater than 200. This is useful to pinpoint failed or suspicious requests made by the Hydra tool, which could indicate probing attempts.
Here's a concise explanation of each `grep` command in the context of log analysis:

7. **grep "404" access.log**

Searches for all occurrences of "404" in the `access.log`, indicating requests for non-existent pages. Useful for identifying broken links and user behavior.

8. **grep -c "404" access.log**

Counts the number of lines with "404" in the `access.log`. This provides a quick metric of how many 404 errors occurred, helping assess the impact on user experience.

9. **grep -E '%3C|%3E|>|<' access.log`**

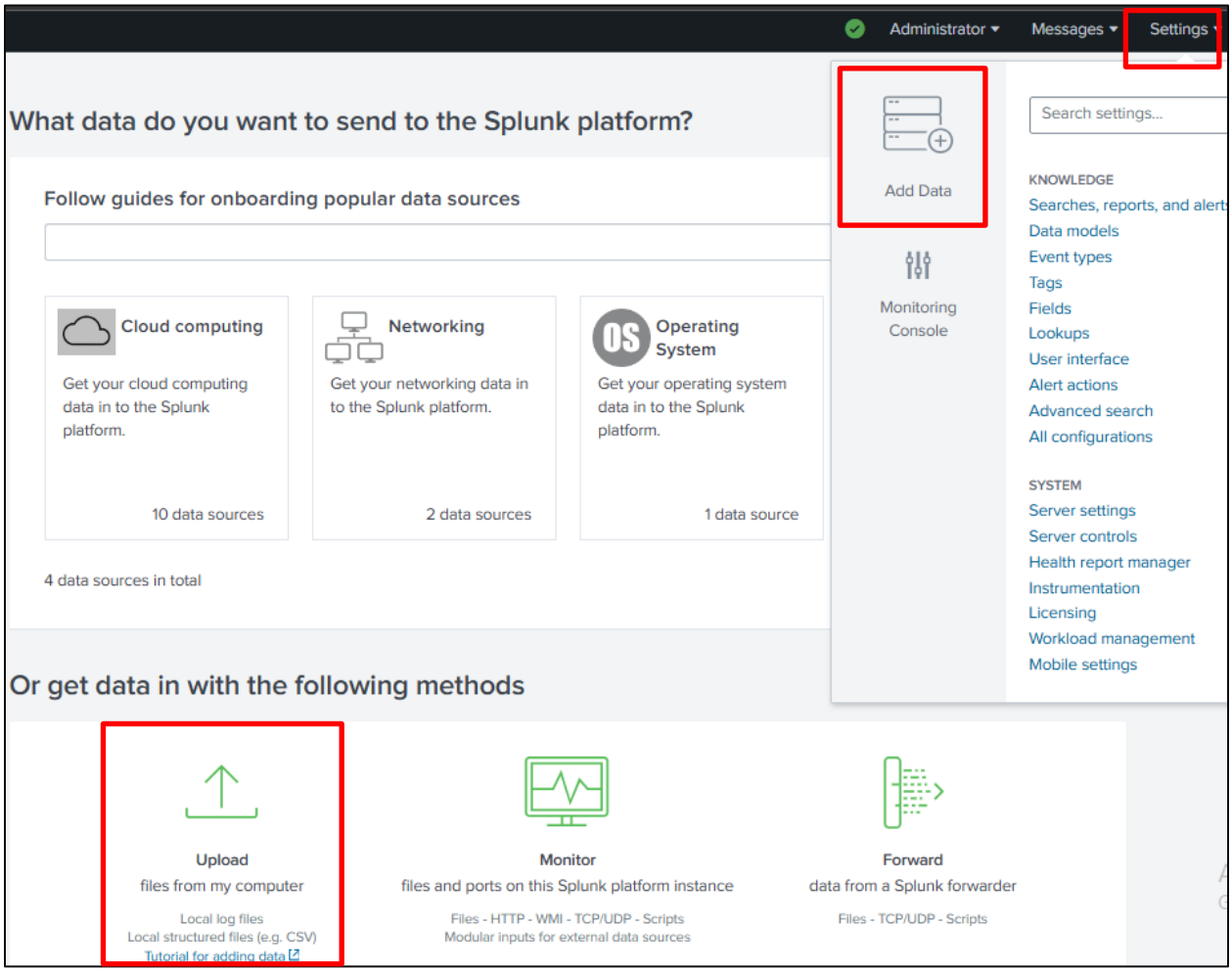
Uses extended regex to find instances of URL encoded `<` and `>` characters, which can indicate attempts at HTML injection or XSS attacks. Helps identify potential security threats.

Splunk

Splunk is a SIEM platform that collects, analyzes, and visualizes data from IT systems, helping in defensive security by enabling real-time threat detection and rapid response. It centralizes logs from various sources, making it easier to monitor and investigate suspicious activities across an organization's infrastructure. Splunk's ability to correlate events allows security teams to identify complex attack patterns, enhancing incident detection and investigation efforts.

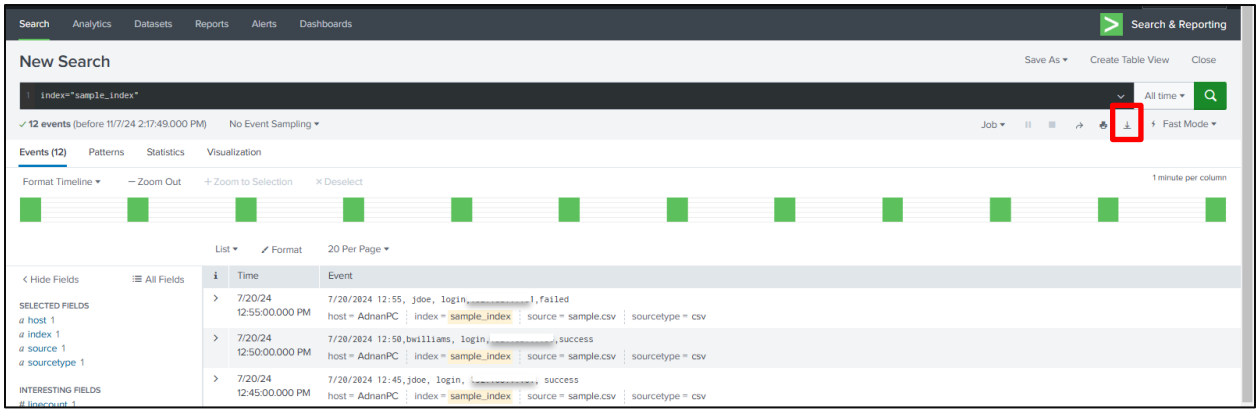
Importing data to Splunk

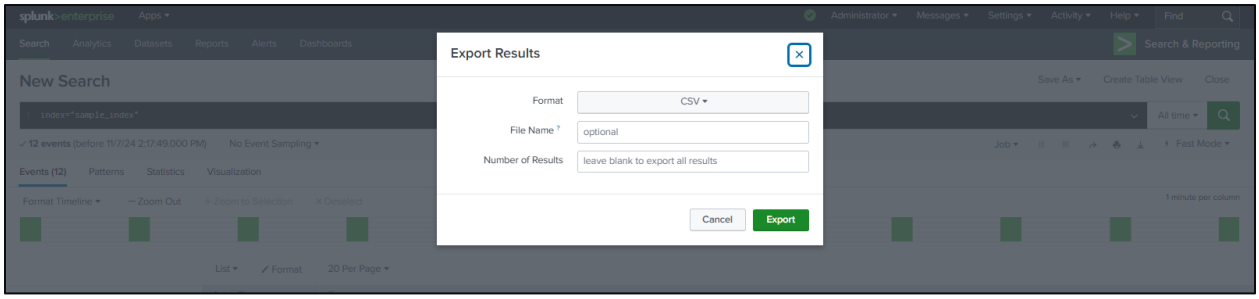
- Settings > Add Data > Upload



Exporting data from Splunk

- Run a search to retrieve the data you want to export.
- Once the search is completed, click on download icon (usually found at the top right of the results area).
- Choose your preferred file format (CSV, JSON, XML, or raw events).





https://www.linkedin.com/in/adnan-musa-b62879319/