**Behind the Dashboard: How I Built a Custom Security Monitoring System with Splunk**

**1. Overview**

The Splunk Enterprise research was part of a larger security monitoring action that focused on real-time analysis of Windows Security Event Logs. The objective was to examine Splunk’s capabilities for collecting, analyzing, and displaying system events to detect abnormal activity and potential security concerns. Splunk was the primary SIEM (Security Information and Event Management) technology, providing extensive search, indexing, and dashboard capabilities for rapid incident detection.

**2. Key Findings**

After Splunk has been installed and configured properly, the system may use the log data from Windows Event Viewer. To set up appropriate monitoring parameters, security logs were acquired. Important security events for preventative threat management were shown on a particular security dashboard.

**Project Goals**

This project aimed to emulate a typical business security environment in which constant monitoring of system activity is required for threat detection. The primary goal was to utilize Splunk to examine the frequency and kinds of system security events after log clearing and to evaluate the usefulness of visual dashboards for security insights.

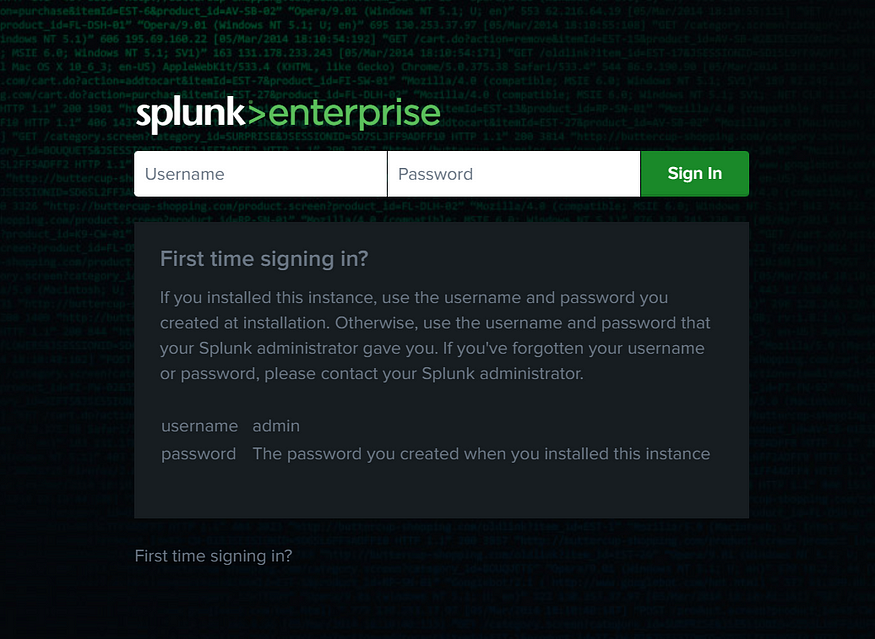
**3. METHODOLOGY**

**Downloading Splunk:**

* Visit your browser
* Visit the Splunk official website: [https://www.splunk.com](https://www.splunk.com/)
* Click on the first link
* Click on free trial and download
* Click on get my free trial on Splunk Enterprise

**Installing Splunk:**

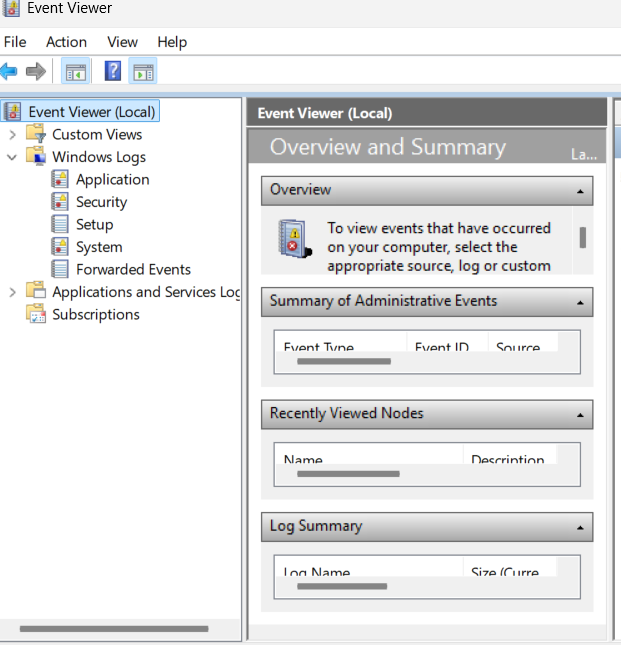
* Run the installation (splunk-x.x.x-x-win64.exe).
* Accept the licensing agreement.
* Select Local System Account
* Set an administrator username and password.
* Select the installation directory (default: C:\Program Files\Splunk).
* Click Install and wait for the installation to complete**.**



**4. Clearing window logs**

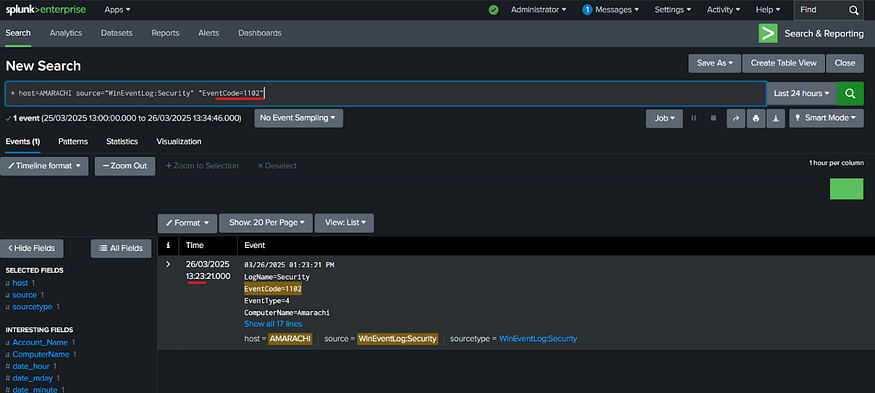
**Open Event Viewer:**

* Press the Window button, search event viewer, and click Enter.
* Navigate to *Windows Logs > Security.*
* Right-click Security and select Clear Log.
* Confirm to clear all events.
* Navigate to *window log -> Application, system, security*and setup
* Click on security and select clear log



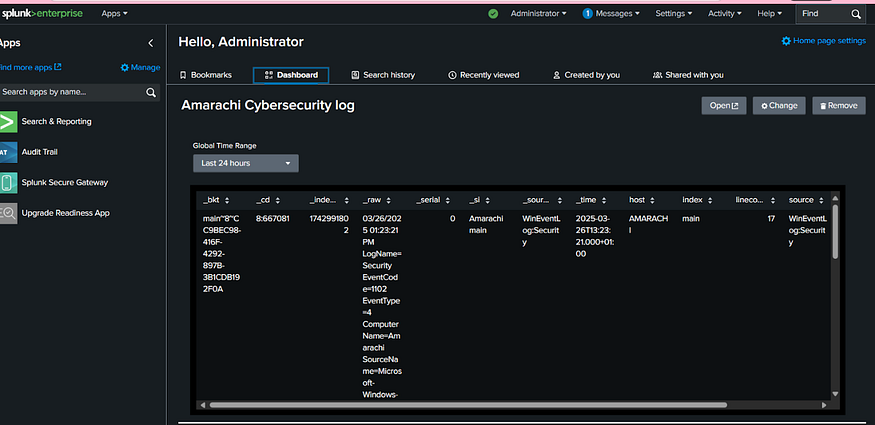
**5. Using Splunk for Monitoring**

* I accessed Splunk’s **Search & Reporting** feature on Splunk
* I also ran custom search queries, such as:**\* host=AMARACHI source=”WinEventLog:Security” “EventCode=1102”**



**6. Create a dashboard on splunk**

* Click on dashboard
* Click on Create dashboard
* Fill in the dashboard title, click on Dashboard studio, Grid layout mode and click on create
* Create a Table
* Copy the command and click on create search and input the command on the SQL query
* Click on Apply and close



**7. Potential Impact:**

The poor administration of security logs may delay the discovery of malicious activities which may considerably increase system exposure to breaches as well as compromise. Through its Splunk dashboard operators gain information that allow risk reduction. Security log monitoring alongside its analysis gives early alerts about occurrences that reduce attack implications.

**8. Recommendations**

**Immediate Remediation Actions**

* Regular examination of the Splunk dashboard should be carried out to discover any unusual security incidents.
* Set up Splunk for real-time scenario tracking by activating notifications for important security events like aggressive attacks.
* The configuration settings of Splunk should be adjusted to extract all security-related log data.

**CONCLUSION**

Splunk Enterprise was successfully installed and effectively configured to monitor and analyze Windows Event Viewer security data. By clearing the initial records, a clean baseline was established, enabling more accurate tracking of future security incidents. A custom dashboard was developed to highlight key security activities, providing a clear and user-friendly view of system events.

Overall, Splunk’s real-time monitoring capabilities proved highly effective in identifying critical risk indicators within the Windows Event Logs, demonstrating its value as a powerful tool for proactive security management.