SPLUNK

Optimizing Data Insights and Security Monitoring

Ahmad Abdullah – i22-1609

Abdul Sami Qasim – i22-1725

Muhammad Talha – i22-1577

NETWORKS & CYBER - II

NOVEMBER 15, 2024

Contents

Executive Summary

This report outlines a project focused on utilizing Splunk, a powerful data analytics platform, to enhance network security and threat detection through real-time monitoring and analysis. The project covers key Splunk components, including the Indexer, Forwarder, and Search Processing Language (SPL), and demonstrates how these elements are used to detect and mitigate security threats. The primary objectives include monitoring network traffic for anomalies, tracking suspicious file activities across endpoints, and detecting potential data exfiltration by analyzing outbound traffic. The implementation plan involves configuring data collection from network devices, setting up detection policies, and using SPL to analyze and visualize suspicious activities, generating alerts for proactive response. By focusing on critical areas such as data exfiltration, file monitoring, and network traffic analysis, the project will strengthen security infrastructure, improve threat detection capabilities, and reduce the risk of unauthorized access or data breaches. Ultimately, this project will help ensure that the organization can respond swiftly and effectively to security incidents, improving the overall security posture and compliance with standards.

Introduction

Splunk is a data analytics platform designed to index, analyse, and visualise machine-generated data. It is used for real-time monitoring, advanced data analytics, and security intelligence. In cybersecurity and network monitoring, Splunk offers capabilities to detect, prevent, and respond to security incidents through log aggregation and analytics. Splunk is versatile software that allows organizations to integrate Intrusion Detection Systems and Intrusion Prevention Systems.

How Splunk is Used

Splunk has three main components which it utilizes to perform as a product i.e. Data Forwarder, Indexer and Search Processing Language.

- ## Indexer

The Splunk Indexer processes and indexes incoming data, transforming raw data into searchable events. It stores this data in indexes for efficient searching and retrieval. The Indexer is responsible for parsing data, applying timestamps, and creating searchable fields. It also responds to search queries by retrieving the relevant data quickly for analysis.

- ## Forwarder

The Splunk Forwarder is a lightweight agent installed on data source systems to collect and forward data to a Splunk Indexer. It ensures secure, real-time data transmission with minimal impact on the source system's performance. Forwarders can be either universal (lightweight) or heavy (with parsing capabilities). This allows for centralized data collection and monitoring across multiple systems.

- ## SPL (Search Processing Language)

SPL is Splunk's query language for searching, analyzing, and transforming data within Splunk. It allows users to perform complex searches, create alerts, visualize data, and build dashboards. SPL supports various commands, functions, and operators for extracting meaningful insights from indexed data. Examples include filtering, statistical aggregation, data formatting, and visualization creation.

- ## Data Ingestion

Splunk ingests data from sources like files, syslogs, applications, and network devices using forwarders or connectors. It indexes data in real-time for searching and analysis, parsing fields for easy querying. Forwarders send data to indexers for organization and storage. Splunk supports diverse data formats and can use REST APIs or scheduled inputs for flexible, centralized monitoring.

- ### Data Indexing and Storage

Splunk indexes incoming data by transforming raw data into searchable events, and organizing it into logical indexes for efficient access. Data is parsed and stored in buckets, categorized by time for quick retrieval. The indexing process includes metadata tagging, field extraction, and compression for optimized storage. Splunk ensures data is readily available for searches, reports, and analytics.

- ### Search, Alerts, and Dashboards

Splunk allows users to search indexed data using its Search Processing Language (SPL) for detailed analysis. Searches can be saved as alerts, triggering notifications or actions when specific conditions are met. Dashboards provide visual representations of search results, enabling real-time monitoring, data insights, and customizable views. Together, these features offer powerful data exploration, automated responses, and interactive reporting capabilities.

Scope of Project

Purpose: To use Splunk in a project, demonstrating its network security and threat detection capabilities.

Project Goals:

- Learning to set up Splunk e.g. Indexer, Forwarder and SPL.
- Setting up different Detection Policies on the Indexer as well as the Forwarder.
- Integrating extra tools where necessary.
- Writing required policies to generate alerts for suspicious entries
- Utilizing SPL to filter out those alerts

Requirements:

- Splunk Enterprise
- Data Sources (e.g., Syslog data, firewall logs, Windows event logs)
- Hardware or virtual environment for setup (VMs running Splunk, networked devices, etc.)

• Potential Implementations Using Splunk

1. **Network Traffic Analysis and Anomaly Detection**
   Involves monitoring and analyzing network traffic to identify unusual patterns or anomalies that could indicate potential security issues.
2. **Log Analysis for Incident Response**
   Gather and analyze logs from different sources to reconstruct a security incident and identify the root cause.
3. **Data Exfiltration Monitoring**
   Alerts for common suspiciously large files whether going upstream or downstream.
4. **Suspicious File Monitoring System and Analysis**
   Implement basic security automation to generate alerts on Executables, scripts and unusual extensions.
5. **Compliance and Audit Reporting**
   Develop dashboards to demonstrate compliance with security standards (e.g., PCI-DSS, ISO 27001) by analyzing relevant logs.

• Implementation Plan for this Project

From all the above-stated potential scope, we chose three of the most common threat-vulnerable

I. Data Exfiltration

This project will focus on building a system to detect potential data exfiltration activities by monitoring high-volume outbound traffic or unusual data transfers. The scope will include analyzing network traffic for indicators of exfiltration, such as large file transfers, suspicious data destinations, or high data transfer volumes originating from sensitive sources. The project will set up monitoring to track these data flows continuously, providing alerts on any suspicious data transfers and generating visualizations of potential exfiltration activities. The outcome will be an enhanced ability to proactively detect and respond to unauthorized data movements, strengthening the network's data security posture.

II. Suspicious File Monitoring and Analysis

This project will aim to identify suspicious files, such as executables or scripts, that may be introduced to networked systems. The scope will include monitoring file creation and modification activities across endpoints and analyzing patterns that might indicate malware introduction. By leveraging Splunk's capabilities, the project will set

up monitoring to track file activities continuously, providing alerts on suspicious file changes and generating dashboards that visualize potentially malicious file activities. The outcome will be a robust system that proactively detects and flags unusual file behavior, enhancing network security and reducing the risk of unauthorized access or compromise.

III. Network Traffic Analysis

This project will involve monitoring and analyzing network traffic to identify unusual patterns or anomalies that could indicate potential security issues. Splunk's capability to ingest network logs and other data sources directly will simplify the setup of data inputs and the creation of queries for visualizing traffic patterns and detecting anomalies. Key steps will include configuring data collection from network devices, such as firewalls and routers, to gather real-time traffic data. The project will focus on creating dashboards to visualize data trends and setting up alerts to signal any traffic anomalies. This approach will enable proactive detection and response to security threats, strengthening the network's overall security and operational reliability.

Conclusion

In conclusion, this project demonstrates the powerful capabilities of Splunk as a comprehensive data analytics platform for network security and threat detection. By focusing on areas such as data exfiltration monitoring, suspicious file analysis, and network traffic anomaly detection, the project aims to implement effective solutions for identifying and responding to potential security threats in real-time. Through the use of Splunk's indexing, data ingestion, and SPL functionalities, the project will enable continuous monitoring, efficient data analysis, and automated alerts, enhancing the overall security posture of the network.

The successful implementation of these key security use cases will not only provide valuable insights into suspicious activities but will also empower organizations to detect and mitigate potential threats proactively. As organizations continue to rely on digital infrastructures, leveraging tools like Splunk will become essential in maintaining robust network security, ensuring compliance, and protecting sensitive data from unauthorized access. The knowledge gained from this project will serve as a foundation for future work in network security and data monitoring, allowing for the continuous improvement of threat detection systems.

References

Splunk Basics 101 TryHackMe Walkthrough - YouTube
https://chatgpt.com/share/67337ea5-c4f4-8012-942d-739ca6436340

Splunk | The Key to Enterprise Resilience