**WINDOWS EVENT LOG VISUALIZATION AND QUERY**

By

HAYAT ULLAH

Submitted to

**The University of Roehampton**

In partial fulfilment of the requirements

for the degree of

**MASTER OF SCIENCE IN COMPUTING**

**Abstract**

Windows Event Log use is essential for system monitoring, security, and performance enhancement, but it comes with several difficulties, such as log administration, analysis, and visualization. To effectively organize and prepare raw Windows Event Log data for analysis and visualization, this research project explores several approaches. It also aims to contrast the capacities of several Windows Event Log systems for interactive querying and visualization. The project's goals include investigating available technologies, creating an interactive artefact for log data, implementing the required architecture, and user testing. Additionally, the project shows real-world applications for Windows Event Logs in a Security Operations Centre (SOC) environment, illuminating how analysts may employ log analysis for monitoring of system health and security.

**Declaration**

I hereby certify that this report constitutes my own work, that where the language of others is used, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of others.

I declare that this report describes the original work that has not been previously presented for the award of any other degree of any other institution.

Signed (apply signature below)

**Hayat Ullah**

**Date:** SEP 06,20



**Acknowledgements**

I would like to express my sincere appreciation to everyone who contributed to the success of my dissertation. I would like to thank the entire School of Art and Digital Industries at the University of Roehampton for giving me the chance to pursue my graduate studies there. To contribute scientific knowledge was one of my most significant academic goals, and the opportunity to undertake a study allowed me to fulfil it. I would like to thank my supervisor Mr. Fakhreldin Saeed, for the knowledge, guidance, advice, and tireless support throughout the project. He also pushed me to be as professional as possible, not just in the project but also in my professional career. I was able to achieve my project goals because of his continuous assistance. This project's most significant source of motivation has been my family. They have been an inspiration in my life.

**TABLE OF CONTENTS**

[**CHAPTER 01: INTRODUCTION** 1](#_Toc144806825)

[1.1. RESEARCH QUESTIONS: 1](#_Toc144806826)

[1.2. PROBLEM STATEMENT 1](#_Toc144806827)

[1.3. AIMS 2](#_Toc144806828)

[1.4. OBJECTIVES 2](#_Toc144806829)

[1.5. BACKGROUND 2](#_Toc144806830)

[**CHAPTER 02: LITERATURE REVIEW** 7](#_Toc144806831)

[2.1. WINDOWS LOG EVENT DATA COLLECTION AND EXTRACTION 9](#_Toc144806834)

[2.2. DATA PREPROCESSING 10](#_Toc144806835)

[2.3. DATA FILTERING AND DEDUPLICATION 12](#_Toc144806836)

[2.4. CENTRALIZED LOG MANAGEMENT 13](#_Toc144806837)

[2.5. WINDOWS EVENT CORRELATION PROCESS 14](#_Toc144806838)

[**CHAPTER 03: TECHNOLOGY AND TOOLS** 16](#_Toc144806839)

[3.1. WINDOW EVENT VIEWER 16](#_Toc144806842)

[3.2. NIRSOFT 17](#_Toc144806843)

[3.3. SPLUNK 18](#_Toc144806844)

[**CHAPTER 04: ARTEFACT DESIGN METHODOLOGY** 19](#_Toc144806845)

[4.1. DEFINE TEST GOALS 19](#_Toc144806847)

[4.2. IDENTIFY TEST USERS 19](#_Toc144806848)

[4.3. PREPARE TEST DATA 19](#_Toc144806849)

[4.4. WINDOWS SECURITY LOG EVENT ANALYSIS ARTEFACT 21](#_Toc144806850)

[**CHAPTER 05: IMPLEMENTATION** 26](#_Toc144806851)

[5.1. ENVIRONMENT SETUP 26](#_Toc144806853)

[5.2. SPLUNK INSTALLATION 26](#_Toc144806854)

[5.3. CONFIGURE DATA INPUTS 29](#_Toc144806855)

[5.4. CREATE INDEXES 29](#_Toc144806856)

[5.5. CONFIGURE SOURCE TYPES 30](#_Toc144806857)

[5.6. WRITING SEARCH QUERIES 31](#_Toc144806858)

[5.7. BUILD VISUALIZATIONS 31](#_Toc144806859)

[5.8. CORRELATION SEARCHES 32](#_Toc144806860)

[5.9. SCHEDULED REPORTS 32](#_Toc144806861)

[5.10. ADVANCED QUERIES 33](#_Toc144806862)

[5.11. MAINTAIN AND OPTIMIZE 33](#_Toc144806863)

[5.12. TESTING 33](#_Toc144806864)

[5.13. DOCUMENTATION 33](#_Toc144806867)

[5.14. MONITORING AND MAINTENANCE 33](#_Toc144806868)

[**Chapter 06: RESULT** 34](#_Toc144806869)

[**CHAPTER 07: CONCLUSION** 42](#_Toc144806870)

[**REFERENCES** 44](#_Toc144806871)

**LIST OF FIGURES**

[Figure 1: Different sources of logs collecting in Winsyslog [1] 7](#_Toc144806873)

[Figure 2: Old method of analyzing windows logs 17](#_Toc144806874)

[Figure 3: Splunk Enterprise Installation 27](file:///C:\Users\User\Downloads\windows%20event%20complete%20thesis.docx#_Toc144806875)

[Figure 4: Splunk Enterprise Login 27](file:///C:\Users\User\Downloads\windows%20event%20complete%20thesis.docx#_Toc144806876)

[Figure 5: Splunk Enterprise Web view 28](#_Toc144806877)

[Figure 6: Upload data in Splunk 29](#_Toc144806878)

[Figure 7: Create Index in Splunk 30](#_Toc144806879)

[Figure 8: uploading Security Events csv file in Splunk 30](#_Toc144806880)

[Figure 9: Query to View All Events by Event ID 31](#_Toc144806881)

[Figure 10: Time chart to visualize the successful login events 32](#_Toc144806882)

[Figure 11: Column chart to visualize all events 32](#_Toc144806883)

[Figure 12: Initial Search for Successful Logins in Splunk 34](#_Toc144806884)

[Figure 13: Successful WIndow Login events 35](#_Toc144806885)

[Figure 14: Events for Privilege Escalation Attempts 35](#_Toc144806886)

[Figure 15: Detect Failed Logon Attempts in Splunk 36](#_Toc144806887)

[Figure 16: Monitoring Account Additions to Groups in Splunk 37](#_Toc144806888)

[Figure 17: Identify User or Group Creation in Splunk 37](#_Toc144806889)

[Figure 18: Track Changes to User Rights Assignment in Splunk 38](#_Toc144806890)

[Figure 19: Monitor Changes to Security Policies in Splunk 38](#_Toc144806891)

[Figure 20: Service and System Monitoring analysis in Splunk 39](#_Toc144806892)

[Figure 21: Detect Changes in Service Configuration 39](#_Toc144806893)

[Figure 22: Monitor System Shutdown Events 40](#_Toc144806894)

[Figure 23: Investigate System Startup Events 40](#_Toc144806895)

# **CHAPTER 01: INTRODUCTION**

Windows Event Logs, these are logs which has been developed by the Windows operating system to abduct notable activities and events. These logs hold key information about security-related events, applications, and system processes. Each log entry contains information and data like the source, event ID, time and date, and a narration of the event. Event Logs are vital for troubleshooting, monitoring system performance, and locating security issues or unauthorized access attempts. Administrators can use tools like Event Viewer to analyze and access these logs, helping them gain insights into identify potential issues and the system's health. Proper management of Event Logs, that includes regular monitoring, archiving and maintenance, that is essential for ensuring the stability, smooth operation of Windows-based systems and security.

These window event logs also enroll computer’s notification and alerts, Microsoft states about event as any type of occurrence in the system or device which requires users to be alerted to entry added to a log. Or furthermore Linux supports a lot of system logs that helps in administrating the Linux system. file */var/log/messages,* is the most important log, that records a wide range of events, that includes system startup, system error message and system shutdowns.

It makes categories of each event with the severity level that orders as information, verbose, warning, error as well as critical. The other tools to view window event logs are Sumo Logic log management and log analytics, Site24X7, Datadog, and SolarWinds Security Event Manager (SEM) [1].

## **RESEARCH QUESTIONS:**

1. What are the best ways to organize and prepare raw Windows Event Log data so that analysis and visualization can be done quickly and effectively?
2. How to compare the capabilities and usability of several Windows Event Log solutions for interactive querying and visualization?
3. What relationships and patterns may be found in datasets of Windows Event Logs, and how can these relationships be used to comprehend system behaviour and possible security incidents.

## **PROBLEM STATEMENT**

How can Windows Event log data be analyzed and visualized in a manner that is interactive and intuitive for system administrators?

## **AIMS**

The primary aims of this project are to work with a Windows Event Log data set and to create way for prospective system administrators to:

* Interactively query event logs
* Visualize event logs.
* Identify correlations in the event log dataset.

## **OBJECTIVES**

* Research existing windows event log tools for working with Windows Event Logs.
* Research techniques for preparing, structuring, managing Windows Event Log raw data.
* Design an artefact that can be used for interaction with Windows Event Log data.
* Acquire resources and deploy the architecture for the artefact.
* Implement the artefact.
* Test the artefact with users.
* Capture and interpret results from testing.

## **BACKGROUND**

The location of window event log is C:\WINDOWS\system32\config\ **folder**. Users can check event logs with the help of 'Event Viewer' to keep track of troubleshooting in the system [2]. The process to check is:

* Now press the **Windows key + R** on your keyboard, for the opening of the run window.
* Type in **eventvwr** and click OK.
* Expand the **Windows Logs** menu.
* Under the **Windows Logs** menu, you will notice different types of event logs—application, security, setup, system, and forwarded events.
  + 1. **Event Log Entry**

Each of every event suppress the following information:

* Time: the time when the event took place.
* Computer: name of the device.
* Date: the date whenever the event took place.
* User: the username of the user whenever the event took place.
* Type: type of event like warning, error, information, security failure audit, security success audit.
* Event ID: a window identification number that designates the event type.
* Source: the program or feature that caused the event.
  + 1. **Types of Event Messages**

The categories are:

1. Information event: it states the successful completion of the task, for example the installation of an app.
2. Error message: states the notable problem that causes the loss of functionality.
3. Warning event: notifies the authority of a possible problem, for example low disk space.
4. Failure audit: it states the failure of an audited security event, for example when a user ended up locking himself out by entering wrong password.
5. Success audit: it shows the completion of audited security events, for example logging in successfully.
   * 1. **Windows Log Event Categories**

The further categories of event logs are:

1. Application event log
2. System event log
3. Security event log
4. Setup log
5. Application and service log
6. **Application event logs**

The application event log [3], it is one of the most accepted event logs in the Windows operating system. It is an element of the Windows Event Logs; this element enrolls events that relate to programs and applications running on the system. When applications come across warnings, crashes, errors, or other notable events, they can develop entries in the application event log. Some general types of events enrolled in the application event log include:

* Application errors: This type of event happens when an application experiences an exception and error that causes it to crash or malfunction.
* Application warnings: Warnings can be logged, whenever an application encounters a non-fatal condition or issue that might crave attention.
* Informational events: App can log informational events to administrates data and information about their successful processes, normal operation, or other information which is relevant.

The application event log is an irreplaceable resource for system developers and administrators, as it assists them diagnose and identify issues with specific applications already installed on the system. Administrators can troubleshoot application-related problems as well as ensure smooth functioning of software on the Windows platform through analyzing the events in the system log.

1. **System event log**

The System Event Log [4], it is one of the ordinary event logs in the Windows operating system. System event log is accountable for record-keeping events that are related to the Windows operating system services and elements, furthermore it is one of the main components. The registered events in the System Event Log enables us vital information and data related to the system's hardware, functioning, and events that are related to driver, and as well as other system-level activities.

There are some standard types of events that were recorded in the System Event Log that includes:

1. Device driver installations and failures.
2. Service starts and stops events.
3. Hardware errors or malfunctions.
4. System critical errors and warnings.
5. System startup and stop events.

The System Event Log is significant for system support panel because it guides them to track wholesomeness and regularity of the window operating system and furthermore administrates them. Executives will be able to troubleshoot driver-related and hardware issues, analyze the problems that can affect the entire system, and identify system-level errors through analyzing the recorded events in the log.

1. **Device driver installation and failure**

This is a software program which enables communication between operating systems and hardware devices. Hardware devices which include graphic cards, printers, and network adapters. An event is recorded in the system event log whenever a device driver is updated or installed. This event generally notifies about the error occurred in installation or whether it is getting successful. In case of failure, it leads to system instability, hardware’s malfunctioning, and further compatibility issues.

1. **Service starts and stops event**

It is a background process that enables computing and running on the system. Start and stop events will be recorded in this system event log. They inform executives about the position of critical system services and their accessibility. This element is important for analyzing if the services are getting perfectly generated or not, as well as analyzing possible problem with the service dependencies.

1. **Hardware error and malfunction**

The system event log records the event whenever any element meets the malfunction or error. Some of the errors relates to hard drives failure, hardware related issue, RAM module malfunctioning, and overheating of processors. To analyzing faulty elements and then proceeds mind in one manner by repairing or replacing the hardware, all you need is to monitor to keep an eye on these errors.

1. **System critical errors and warning**

It indicates the possible problems and serious issues which require attention. Events like system crashing, critical issues which can affects the performance of the system and Kernel-level errors. Addressing these errors is important to maintain the health of the operating system.

1. **System startup and shutdown events**

These events are registered in the system event logs, that includes the details about the starting and stop times of the system as well as timestamps. These events are a handful for understanding system uptime and further issues which can occur while processing.

1. **Security event log**

This is a common event log in the window operating system and a main component of window event log which is responsible for the documenting of activities and security-related events. These events enable us to provide key information related to access control, user authentication, security-related activities, and changes in security policies [5].

Types of events which can be recorded in the security event logs are:

1. Object access: gain pursuit for accessing sensitive objects and resources on the system, for example folders, registry keys and files.
2. Audit policy changes: locate the changes in the security audit policies on the system.
3. Successful and failed logon attempts: it records events whenever an unauthorized login attempt fails and if the user log-in successfully.
4. Security group membership changes: it records the events during the modification of security group membership.
5. Account management: it records the changes whenever any user changes the password, while deleting the account and creating the account.

This event log is important for the maintenance and monitoring of the security of the window operating system, which helps system security when detecting any dubious activity, while helping the executives, examining security incidents, and identifying possible security breaches.

1. **Setup log**

It records the events while setup of software, installation, and device drivers on a window operating system. Window logs the installation procedure in the setup log whenever updating and installing the new software. It enables the important information for monitoring the installing of the process and troubleshooting and as well as it locates the outcome of the generating the software and traces the steps. This setup log is really a handful while facing the issues in driver updates and installing the software. The log will gather the details about description, details which is relevant, error codes and the files which is involved, in case if any problem occur in the setup.

User can access it by window event viewer, maneuver to "Applications and Services Logs" > "Microsoft" > "Windows" > "Setup," to find the setup events.

It will help to assist in troubleshooting while installing drivers and installing any program in the windows system.

1. **Application and service log**

It includes the custom event logs generated by services that are already installed in the window operating system and by wide range of applications. Third-party services and programs may generate the logs under application and service logs, non-identical or far from the standard event logs which are generated by the window itself. It enables a vision to operators to record information related to the service and application. These logs are a handful for diagnostics purposes, monitoring and troubleshooting, because they allow more control over the information and events they want to be achieved.

For accessing these logs, we need to follow these steps:

* Press window key + R to open the event viewer, type “eventvwr.msc” and hit Enter.
* Maneuver to “application and service log” on the left pane.
* Users can be able to see a list of custom logs which are created by different application and services. In the main pane on the right side, view the recorded event log.

They provide the important insights into activities of the service and application, and their behavior.

# **CHAPTER 02: LITERATURE REVIEW**

Forensic investigations involve log investigation because it tends to make investigation relatively easy and accelerates security. Logs provide important information about the intruder activities which could be involved in hacking of systems and website, DOS attack. Audit logs are very complicated log events and format is in binary form. Moreover, windows log events are decentralized in nature. To cope with these complexities and emphasize the importance over in this study [6], The author recommends a reasonable alternative for decentralized log storage which then seems to be using Win Syslog which is a central Syslog server and event reporter that can translate the data into syslog format from the binary format.

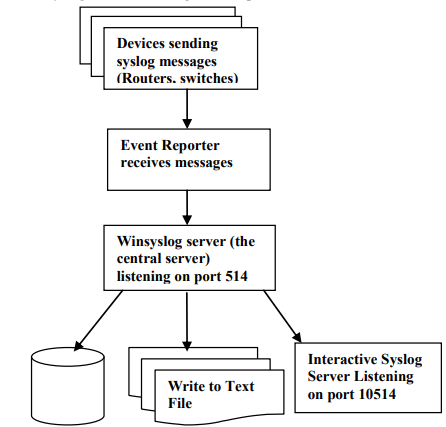


Figure 1: Different sources of logs collecting in Winsyslog [1]

Further study concludes that [7], Cybercrime is growing ever more relatively common, thereby further it needs to be evidence already when individuals may very well be accused of violating the law. Scientific proof, legal requirements, and Windows OS source materials as well as the Tracking system, slack space, and event log seem to be the major talking points of this research project. A VMware computer system was utilized to simulate cybercrime operational processes the same as computer-controlled password guessing and getting hacked on such a Windows operating system. Event information and data have been thoroughly investigated for weight and social acceptance by windows log investigation.

In this study the author concludes that [8], the Windows event log is a flawed tool used in digital forensic cases, often not being considered verifiable. This dissertation aims to develop a solution to address flaws in the Windows event logging service. Research found that disabling the service allowed for modification of important data and easy transplantation of event logs. A C# and Microsoft.NET-based event logging application was developed, using RSA and AES encryption and HMAC hash signatures to improve data integrity. The application consists of an event logger, an event viewer, and a symmetric and asymmetric encryption. The symmetric encryption was found to be 800% faster than asymmetric encryption, and the HMAC hash signatures were tested for brute force attacks.

In this approach [9], A Windows event forensic entire process is explained in this article (Win EFP) to try and understand the event log files with the Windows operating system. The Win EFP deals with forensics of logs of activities and occurrences that take place in Windows. As a consequence, it aims to provide guidance to forensic investigators on continuing to investigate digital forensics via Windows event logs. Including both business and home environments, Windows happens to be the most widely utilized operating system. The Windows event forensic service expects that the event logging service is not clear and unambiguously ended up turning off by a Windows user. Win EFP could be employed in almost any forensic official investigation. that included a computer windows XP. Many Windows event log items that used to be extremely important for forensics were catalogued and identified in process of WinEFP development.

The proposed theory states that [10] logs contain a great deal of runtime information; logs are essential to the design and administration of software development system. As the complexity and size of software are increasing, the volume of logs are also increasing. As there is a shortage of openly accessible data sets and standardization, so only a small proportion of AI-powered log analytics techniques have already been successfully implemented in the sector over the past several years. Log hub had also managed to gather 17 real-world log datasets from those of a wide range of technologies, which include supercomputers, distributed systems, mobile systems, operating systems, server applications, and dedicated software. The paper also provides a situational analysis on intrusion detection system, describes the data, and introduces real-world usage specific cases. Including around 77 GB of data, Log hub is a 17-log dataset enabling log analytics that uses artificial intelligence. It supports the log activities of the organization and continues to act as a discussion board for performance monitoring, datasets, and comments from business and the academic community. Log hub has indeed been downloaded by over 380 organizations, and the platform is planning on keeping trying to gather clearly labelled datasets and planning to release open-source log analysis toolkits.



## **WINDOWS LOG EVENT DATA COLLECTION AND EXTRACTION**

Event log entries in Windows systems are generated and obtained as components of the Windows Event Log collection, analysis, and processing conditions for management, observation, troubleshooting, and multifactor authentication.

The steps in this process are organized as follows:

* + 1. **Event Log Types and Channels**

Windows Event Logs are split into different groups, each of which represents general and especially channel-specific attributes of security events. Although there are three basic categories [11]:

* **Application:** Framework logs and Operating system.
* **Security:** Document security-related incidents include login attempts that appear to be trying to authenticate legislative alterations and human rights abuses.
* **System:** Manages to capture startup and shutdown events, driver limitations and hardware, and network configuration.
  + 1. **Identifying Relevant Channels**

Must use the event log channels that have been influential in their intellectual aims and observation. Choose another channel that directly relates to their key targets because they're all going to accumulate a broad spectrum of activities.

* + 1. **Accessing Event Viewer**

Windows' Event Viewer program offers a GUI for retrieving information and representing event log goods and services. It's either a platform one that's helpful for detailed analysis or that's already readily accessible.

* + 1. **Using PowerShell for Extraction**

The procedure for gathering information can be accomplished and organized via PowerShell test scripts. Like using 'Get-WINEVENTT' and perhaps other PowerShell cmdlets to remove unwanted event usernames and passwords. For example, in the article:

Get-WinEvent "Application" -LogName (Get-Date).

AddDays(-7)

* + 1. **Filtering Events**

Events may very well be categorized employing PowerShell; obviously, it depends on several different parameters, which would include the designated period, event ID, keywords, and sources. The personal information users retrieve is diminished through detection to include only valuable data.

* + 1. **Exporting Data**

Event log data that has been managed to gather and allowed to settle may be produced and sold in a broad range of formats, which would include XML, CSV, and even a personalized database. In-depth interrogation has now become entirely feasible using advanced and powerful software or technological devices.

* + 1. **Using Third-Party Tools**

There are third-party alternatives that are already considered experts at gathering and evaluating event log data from various websites throughout the whole network, including SIEM (Security Information and Event Management) systems.

* + 1. **Remote Event Log Collection**

With a portable event log personal library, users might very well gather up event data from some of the other computer systems connected to the identical network, as long as ownership permits. The portable functionality of PowerShell allows this to be accomplished.

* + 1. **Automated Collection and Scheduled Tasks**

With Task Scheduler, PowerShell practices may very well be originally planned to be organized at predetermined time intervals. By continuing to support commonly performed fully automated intelligence gathering, you can ensure users have a consistent stream of event information that can be analyzed.

* + 1. **Data Analysis and Visualization**

Until the event log data is assessed, it may very well be explored using a variety of instruments that range from simple and effective scripts to artificial intelligence and machine learning systems. Data interpretation may be aided by analytical techniques such as Power BI, Splunk, or ELK Stack.

## **DATA PREPROCESSING**

Data parsing is the manner of subdividing extremely complex and poorly structured log data [12], including event log entries, in and out of surrounding nature or character traits that have been simple to handle, draw conclusions from, and process. Raw log data more and more often manages to combine chronological data alongside event IDs, event sources, characterizations, and some other relevant information. In the interests of creating and implementing the ideas of the log entry, data parsing essentially involves indexing and trying to extract certain sources. Data parsing in either the frame of reference of the paper might also necessarily imply:

* + 1. **Log Entry Segmentation**

Demographic segmentation of log entries into several more different components, such as sequence numbers, event sources, event IDs, and event descriptions, is the first step.

* + 1. **Field Extraction**

Attempting to create relational database variables by removing the unwanted unique characteristics from either the log or the individual product Attempting to take the timestamp, user ID, and resource that would have been allowed access from a security event log entry, for example, in this case.

* + 1. **Contextual Information**

Summarizing additional semantic information, such as IP addresses, machine names, or user roles, that places particular emphasis on the frame of reference of something like the event

* + 1. **Handling Variability**

Trying to handle points of difference in log formats because they might appear to come from many sources of information and systems and seem to have different characteristics.

* + 1. **Data Normalization**

The procedure known as data normalization attempts to put the interpreted log data into something like a reliable, consistent, and symmetric version. By guaranteeing that all of the information is racially homogenous, this strategy reduces the effort needed to observe differences, and consumers are attracted to the numerous different log entries. Data normalization throughout the general framework of the paper would have to include:

1. **Timestamp Alignment:** Working to create a universal timestamp configuration from several different formats with the purpose of providing consistent quality for time-based characterization.
2. **Standardization of Event IDs and Sources:** To make the distinction and assessment of Events relatively easy, ensure consistent Event IDs as well as Sources.
3. **Data Unit Conversion:** For concentration to be measured, transmit data units (which include bytes, or rather kilobytes) into something like a dependable unit.
4. **Value Mapping:** To reduce manual analysis and diminish complexity, measurements are segmented into a previously agreed collection of subcategories or bar codes.
5. **Managing Missing Data:** Had used unsupported assertions and perhaps other suited sorting to come to grips with insufficient or absent data sets.
6. **Encoding Categorical Data:** Attempting to create graphical representations of discrete variables (including certain produced content and user roles) that computers can process.
7. **Data Transformation:** Working to improve the statistical distribution of information through the implementation of conceptual modifications (such as logarithmic transformations)

To construct an adequate dataset that can be used as a foundation for further observation and optimization techniques, comprehensive data manufacturing and normalization are extremely important [12].

## **DATA FILTERING AND DEDUPLICATION**

The publications will more assuredly help in providing cutting-edge techniques or instrumentation for querying the database and data compression for event log administrators, including the setting of their investigation [13]. These technologies contribute to enhancing the caliber of the data that can be utilized for analysis, or something that contributes to the effectiveness of observing analysis and planning treatment plans. The "Event Log Filter" network, which would also be implied in the introduction, could very well incorporate various stages or individual components that work collaboratively to provide good quality and sensor information in an effective manner during immediate and almost specific circumstances.

* + 1. **Data Filtering**

The organized method by which to select specific desired log entries that satisfy specific criteria when resisting others is commonly referred to as data filtering. This technique allows for the elimination of unimportant, redundant, duplicated, and irrelevant features, focusing the analysis exclusively on directly relevant and the most important occurrences. In the historical context of the research, the words Event Log Filter likely represent a program or a power structure that employs advanced and complex techniques and algorithms on event log information to successfully purify and organize the information for further investigation. The manuscript could cover an extensive and broad range of information filtering aspects, like:

1. **Criteria Selection:** Establishing the standards on the core principle of which events are to be incorporated or effectively removed Filtering by data, event source, perceived severity, time window, and so many other standards may have an impact on this.
2. **Redundancy Removal:** Attempting to remove irrelevant information that would save cutting and pasting diagnostic initiatives.
3. **Noise Reduction:** Focusing on identifying and limiting progressively explicit or completely meaningless events that sometimes adversely influence explanatory survey results or cause incorrect strong points.
4. **Online filtering:** Promoting filtering in everyday or almost real-time to reduce computation flexibility interruptions and activate a comprehensive response to future events or situations.
5. **Data Transformation:** The method used to transform raw data event log information into an organized form that encourages individual filtering based on an array of minimum standards.
   * 1. **Deduplication**

The mechanism of deduplicating tends to involve efforts to delete and find unused event log entries from something like a dataset. Network problems, system bugs, and many other contributing factors could perhaps cause duplicate events, which can sometimes lead to research results, incorrect analysis, and budget overruns. the above implementation of traditional topics might be comprehensively addressed in the research article:

1. **Duplicate Detection:** An approach for trying to locate event data that has been exactly equal or way too like the original data.
2. **Scalability:** Working to make sure deduplication security measures are valuable and cost effective, and even more so in present conditions with large event log archives.
3. **timestamp consideration:** Failure to manage duplicates that have the exact timestamp, especially when managing frequently occurring events, seems to be another component to keep in mind.
4. **Duplicate removal:** The techniques of reducing the number of duplicates when managing to keep the data and information.

## **CENTRALIZED LOG MANAGEMENT**

To improve the efficacy of data presentation, log information gathering, and problem resolution, a central management organization describes the methods of stockpiling, information accumulation, and summarizing log information from numerous sources in a centralized location. The ELK Stack (Elasticsearch, Logstash, and Kibana) is utilized in the present study [14] to either provide cost-effective centralized log management or by providing a complete representation of the software's functioning and state of health, centralized log management should make troubleshooting simple and easy. Decision-makers are capable of immediately narrowing down reasonable explanations for problems and responding in a timely manner.

Considerable amounts of log information gathered from various places might also be accommodated using central management storage advancement alternatives like the ELK Stack without removal.

The article basically outlines why centralized log management is executed through ELK Stack, more so than Elasticsearch, Logstash, and Kibana. This would try to explain methodologies for establishing and operating such a system, the potential benefits of central control, deployment layouts limitations, and operational configurations.

Further Explanation of this concept:

1. **Logstash:** Logstash seems to be a powerhouse for consuming information into an automated data optimization procedure. It needs to gather, refine, and integrate log information into an appropriate layout for use in storage and analysis.
2. **Kibana:** Users can communicate with the categorized log data while using visual representations and dashboarding access control Kibana. It appears to offer a graphicuser interface for designing visualizations, operating concerns, and collecting information. Kibana enables users to construct personal dashboards that showcase developments, errors, and structures in log data. Dashboards that integrate significant information should provide immediate knowledge and statements.
3. **Elasticsearch:** Both structured and unstructured information can be organized and tracked down t using Elasticsearch, a reliable and consistent listing and data management generator. It functions as the primary archive for log cloud services in the context of centralized log management. The customized log data is listed by Elasticsearch, which ultimately results in a searchable database offering immediate and adaptable data gathering. The speed and reliability of log data retrieval are strengthened by filtering.
4. **Data Normalization and Transformation:** Logstash directly converts supervised or unsupervised log data into something like a required format that has been adapted for efficient browsing and indexing in Elasticsearch. It might just require extracting essential data, extracting timestamps, and making the necessary arrangements. With efficient log management, management will monitor behaviors and developments in real time. Users can set up alerts to warn them of situations that need to be fixed quickly and should be addressed to their consideration.

## **WINDOWS EVENT CORRELATION PROCESS**

Windows Event Correlation has been the technique for characterizing and finding links and correlations within and between running on windows events to notice advanced and complex attacks or cybercriminals. This strategic approach tends to strengthen the ability to define advanced and powerful attacks that may imply a cycle of associated mishaps rather than solo attacks. Here's a brief representation of the possibility [15].

1. **Gathering Event Data:** The method involves organizing event information from different Windows environment sources. Windows Event Logs monitor the performance of several different occurrences, which would include web applications, application behaviors, and operating systems.
2. **. Event Correlation rules:** Implementing guidelines for event correlation involves understanding correlations between incidences that might indicate malicious or unauthorized behavior. These regulations were created using information about normal network threats and attack procedures.
3. **Event Sources and Types:** Events in several categories, which would include joining materials, wireless routers, user usernames and passwords, and authority changes, offer insights on security events. Many aspects, including the operating system, applications, and security systems, provide events.
4. **Temporal and Logical Correlation:** Correlation among events is primarily focused on both rational and reasonable and empirical (time-related) aspects. Because even though logical similarity appears in the associations among both actions in terms of cause and effect, dynamical connection validates the timing and breakdown of occurrences.
5. **Recognition of patterns:** To find established patterns that correspond to well-known attack scenarios, correlation engines scan event data. These trends may also include predefined cycles of flexion and extension, password cracking, or security breaches.
6. **Event Chains and Sequences:** Optimized cyberattacks often contain a range of situations recognized as malicious code chains. Event effect is provided because of certain event structures that could also refer to a multi-stage assault.
7. **Alert generation:** A signal is managed to be produced if a linkage rule discovers a behavior or collection of occurrences that correspond to the description of a cyberattack context. The security team will observe and adapt more thoroughly as a side effect of this alert.
8. **Incident investigation:** Correlated factors have helped security personnel identify the nature and severity of an event occurring by presenting a better understanding of attack patterns and deadlines.
9. **Contextual Evaluation:** The circumstances of an event that occurs are addressed when relating events. Regarding making properly rational choices concerning the potential of an attack, this involves details regarding the user, the system, and the environment.
10. **Reducing False Positives:** Cutting Down on False Positives By analyzing many changes in practice, effective linkage rules tend to eliminate random errors. This guarantees that alarms are only increased when a clear and present danger is more probable.

The researchers behind the research [15] go through how hack establishments sequence of events together, something that accounts for a lengthy malicious activity spotted that uses reporting and control technologies on Windows event data. Developers would perhaps be processing information algorithms, highlight the consistent and accurate investigation procedures, or processes they were using to optimize cybersecurity in Windows systems.

# **CHAPTER 03: TECHNOLOGY AND TOOLS**



## **WINDOW EVENT VIEWER**

The Windows Event Viewer is a dynamic tool which administers query log events and visualization for event logs in the Windows operating system. Furthermore, it also grants users the opportunity to analyze and view numerous event logs, as well as authorize advanced querying to refine and search for events that are based on numerous criteria.

To employ the Windows Event Viewer for log visualization and querying:

* Firstly, open Event Viewer: Press the Windows key + R, for the opening of the Run dialog box, type "EVENTVWR.MSC", and press Enter. This will open the Event Viewer application.
* operate to Event Logs: In the Event Viewer window, you will be able to find wide range of event log folders on the left-hand side, that includes security, application, System, and others. Click on the significant log folder to view its recorded events.
* View Events: Clicking on a log folder will display the recorded events in the main pane on the right. You can scroll through the events to examine their details.
* Filter Events: To perform a basic filter, click "Filter Current Log" in the Actions pane on the right. You will be able to filter events by different parameters like keywords, event IDs, event source, as well as date ranges.
* Create Custom Queries: For more up-to-date querying, use the "Create Custom View" option in the Actions pane. This will grant you the ability to build complex queries that are based on specific criteria, such as keywords, event IDs, event sources, event levels, and others.
* Save Queries: user can save custom queries for the future use and easy access.

Through employing the query capabilities and log visualization of the Windows Event Viewer, operators will be efficiently analyzing event logs, monitor system performance, troubleshoot issues, further investigate security incidents, ultimately helping to maintain the security and health of the Windows environment.

[8] it is necessary to have “security information and event management” (SIEM), this solution not only aggregate the logs rather they also provide user to efficiently visualize the data and gather evaluative perception. The old method of analyzing the logs is:

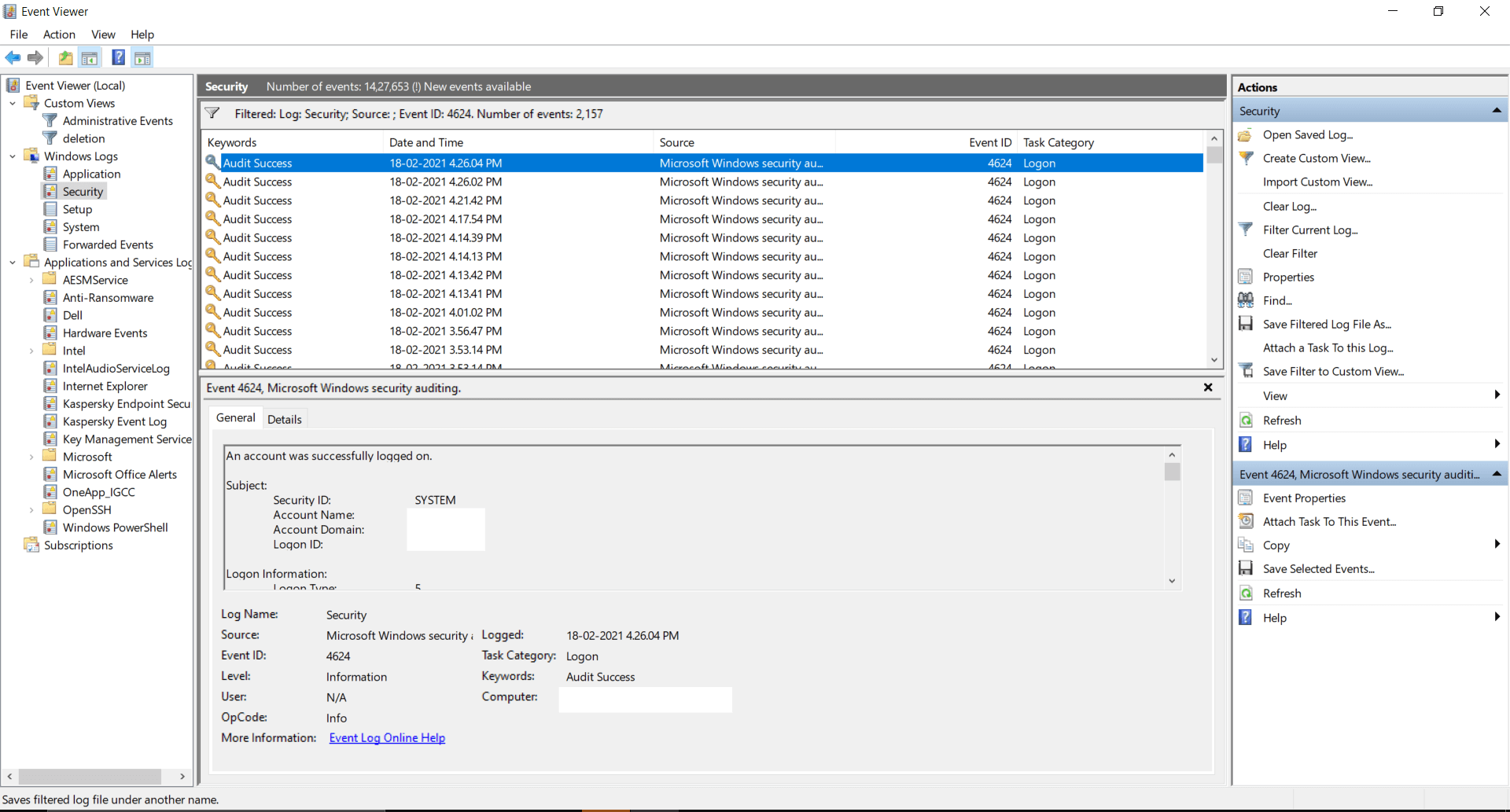


Figure 2: Old method of analyzing windows logs

Features of event log analyzer:

* SEIM
* IT compliance management
* Reporting console
* Log management
* File integrity monitoring
* Log forensic analysis.

## **NIRSOFT**

NirSoft provides several tools for system troubleshooting, security, and maintenance. They would not provide a specific tool allocated entirely to querying and log visualization like Windows Event Viewer**.** Nevertheless, NirSoft's assemblage of services includes diverse tools that can be helpful for accessing and analyzing defined types of logs on Windows systems. For example:

* Nir-Soft's "Event Log Sources View" service allows the user to view a list of all event log sources equipped on your system, that also provides data and information related to each source as well as their associated event logs.
* "My Event Viewer" is another Nir-Soft tool. This tool presents a more user-friendly terminal than the default Event Viewer, authorizing the user to view event logs in an uncultured manner.
* "Last Activity View" presents an inclusive report on various system activities, such as user login, system shutdowns, and application installations. which can be handful for monitoring system troubleshooting and usage.

On other hand, While NirSoft activities offer beneficial performance for system analysis, they might not be able to cover the entire range of characteristics enabled by the local Windows Event Viewer. In case the user needs more up-to-date log visualization capabilities and querying, it is better to count on the local Event Viewer tool or investigate other functional log analysis tools that are available in the market.

## **SPLUNK**

Splunk is the most powerful log management system and analysis platform and an internationally well-known system, which can be utilized for querying and log visualization and includes window log data. It proposes indexing, application logs, hefty abilities for ingesting, system logs, examining log data from different sources, security logs, and window event logs and more.

* **Advanced querying**: Splunk’s search processing language (SPL), offers the user the chance to search on the log data and perform complex queries. Users can correspond and filtrate, and analyze the time range, event types and as well as keywords.
* **Data visualization:** Splunk enables a user-friendly affiliate to generate interactive visualization and dashboards. Through log data, users can generate tables, maps, graphs, and charts to gather insights.
* **Indexing and parsing**: Splunk indexes and parses the log data to make it easy to search for the user as well as enabling efficient and fast querying after ingestion.
* **Data ingestion:** By using different methods like window event log monitoring, Splunk universal forwarder, or HTTP event collector, Splunk allows the users to ingest the data from the window machines.
* **Reporting and analytics:** to initialize the analytic based on log data and custom reports, Splunk proposes the reporting characteristic. These can be scheduled for distribution and automatic generation.
* **Alerting and monitoring:** based on the custom searches and already defined conditions, Splunk allows users to set up notification and alerts.

# **CHAPTER 04: ARTEFACT DESIGN METHODOLOGY**

It would be important to examine the artifact with consumers to determine if it meets their goals and requirements. This is the flow for verifying the artifact:



## **DEFINE TEST GOALS**

Consider making the testing phase's targets more obvious. Plan on which basic characteristics of the artifact, such as cloud computing, toolbar user friendliness, alert outcomes, and overall brand wellbeing, users want to conduct an assessment on.

## **IDENTIFY TEST USERS**

A diverse and interesting set of users representing the different internal management tasks and duties should have been utilized. These should be necessary for market analysts, IT administration staff, SOC analyst and other key stakeholders.

## **PREPARE TEST DATA**

Users may require that you generate test data that closely resembles personal characteristics and specify the conditions based on the characteristics of a particular artifact. For instance, try to ensure the test data accurately describes absolute log entries since you're interacting with Windows Event Log data in a CSV format.

Generate some induction training for the test users before and during the verification process. Illustrate to them how to identify the artifact, perform results, engage in conversation with visualization techniques, customize alerting, and move throughout reports.  
Provide us with a variety of hypothetical test situations that users could employ to characterize key characteristics of the artifact. Neither ordinary user applications nor hypothetical edge occurrences are required to be encompassed by these models. For example, there could be different scenarios that can be used to design artefact:

**Scenario 1:** Evaluate any rejected login attempts and perform a line graph to establish.

**Scenario 2:** Produce an inquiry to be updated when a definite event code begins to happen.

**Scenario 3:** Consider specialized security events by examining relevant and important outbreaks.

Monitor the performance of whatever significant issues or omissions that users have throughout testing. Provide further appropriate information, which includes the routines to utilize the dilemma and therefore any syntax errors.  
Using the information provided, justify making any necessary adjustments and corrections that were already desired. Test the alteration again with consumers to ensure that they've dealt with the issues they'd recognized and continued to improve the experience for customers.

Launch the managed-to-finish artifact for routine overuse after testing and performance improvements are accomplished.  
Sometimes after installation and configuration, continue to gather user feedback. Use individual-specific recommendations to continually boost the artwork.  
Considering how certain their artifact is performing as well as identifying key opportunities for enhancement based on the results helps maximize and validate testing statistics. Following are certain techniques for yielding promising results and observing research findings:

1. Each test case that users helped create for the validation process should already be cataloged. Summarize the desirable output, the operations for transcription, as well as any other innovative key performance indicators.
2. Manage a comprehensive and detailed log of any concerns, glitches, or malfunctions that users encounter while testing. Continue to offer relevant information about both the initial problem character, the events that may occur encompassing its appearance, and any error messages.
3. Start examining the comfortability through which users might sometimes run queries, communicate directly with visualization techniques, and set up alerts to identify the artifact's usability. Pay attention to trends in misunderstandings or usability conflicts. This essentially allows you to capitalize throughout the development of the conceptual framework on different characteristics.
4. Choose whether an area should be improved first based on the importance and potential consequences of the problems. Put your attention on fixing important problems that have a big impact on the functional or user experience.
5. Should be doing a root cause analysis on each error user experiences to accurately predict how everything caused the problem.
6. As a starting point for iterative improvement, use the findings and comments that were recorded. Make the required adjustments, then run further tests to confirm the effectiveness of the modifications.
7. Monitor the testing procedure, the observational studies, and the issues that were resolved. This documentary evidence is beneficial to use as a comparison and can suggest recommendations for investments that are significant.
8. To properly comprehend test findings and get an accurate analysis of your artifact's performance and user experience, you must analyze tangible and intangible qualitative and quantitative information. It helps you decide on significant improvements and upgrades, which might certainly result in an improved, beneficial, and straightforward artifact.

## **WINDOWS SECURITY LOG EVENT ANALYSIS ARTEFACT**

Emily's day as a Security Operations Center (SOC) analyst initiate with either a hot cup of coffee or a rapid analysis of the immediately preceding day's events. Her actual main research interests include evaluating the banking services the company provides and user authentication events from the inside of the Windows environment.  
A rising trend in successful logins quickly captures Emily's eye (Event ID 4624). By studying logon types and authentication packages, she designs a Splunk query to determine the specifications of these logins and guarantee that only authorized users have access. Several entries stand out for her as a consequence of their unique login times and uncommon logon types. She identifies these for further analysis.

Emily switches her efforts at this point in the morning to take full responsibility for policy and oversight upgrades. She notices the incorporation of an additional user into a complicated security group (Event ID 4907). Using Splunk, she efficiently tries to grab relevant and important information before taking note of the target account and gaining a detailed understanding. She makes use of this information to work with the identity management coaching staff to audit the design changes and helpdecide their moral authority.  
Emily reports a fundamental change in the user rights assigned tasks on the same day that appears to be going on (Event ID 4904). Just a few changes in policies have occurred. She detects the design changes by tryingto compare individuals to the organizational development documentary evidence. A possible isolated incident where only a semi-user partially or completely managed to acquire significantly greater access permission has now become plainly obvious on further closer observation. With the accusation of a possible risky endeavor in network access, Emily tends to raise that one with her program manager for management approval.  
Emily needs to shift her priority to system health throughout lunch. She discovers an unusual demographic shift toward frequent service at the beginning of the story (Event ID 7024). She tries to search for either of these events in Splunk and focuses on the users and conditions of the solution-based solutions. She eventually finds a few circumstances where non-standard systems were conceived, regardless of whether a significant proportion are appropriate. To make sure these operations are authorized, she tends to work with the network engineers in synchronization. Emily considers system shutdown and startup events before considering them throughout the day (Event IDs 1100 and 1101). She needs to recognize a shutdown event that seems to have occurred without any of the appropriate alerts and initiate additional data analysis. She helps to verify that the shutdown was a component of a recurring upgrade after interacting with the IT professionals. She verifies the event that occurred for the link and the terror attack report shortly afterward.  
Emily considers her requests for information and behavior as the day expires. The SOC seems to have been competent in maintaining a secure environment, even though her detailed exploration generated Splunk's positive request. She is certain that her efforts have allowed her to investigate possible dangers, crack down on significant illegal exposure, and reestablish the system's wellbeing.

The SOC data scientist, Emily, seems to be using the obtained Splunk results in this given set of circumstances to investigate several different types of security-related tasks, including other user authentication, customer support, and system monitoring. Her behaviors demonstrate her dedication to maintaining a dependable and effective IT environment.  
Primarily intended for a Security Operations Center (SOC) auditor using Splunk, the comprehensive configurations associated with each of the four distinct use case scenarios are available in the following table.

**Use Case 1: User Authentication Analysis**

**Scenario:** Trying to uncover a skeptical user authentication interaction scenario **Background**: In the interest of identifying appropriate privacy concerns and security breaches, the SOC analyst oversees continuously keeping tabs on rather than analyzing user authentication operations taking place within the Windows operating system.

**Step:**

**1. Initial Search for Successful Logins:**

Start executing the service request to obtain a collection of successful logins, paying proper attention to the user, user account type, and identity verification component elements.  
**2. Analyze Successful Logins:**

Start examining the quickly and effectively logged-in relevant information to determine whether it represents what else was originally planned. Divert attention to any slightly odd authentication packages or login patterns.

**3. Identify Privilege Escalation Attempts:**

Operate the search queries to determine possible efforts to try authentication and authorization. Pay attention to target users, disturbing methodologies, and login IDs.

**4. Detect Failed Logon Attempts:**

Operate the query to determine unproductive authentication attempts. Research factors that cause malfunctions and determine whether they indicate any feasible security breaches.

**5. Investigation and Response:**

Analyze much further and have used additional authentication skills and knowledge and intra- and inter-additional sources for every kind of unauthorized or unscientific operation.

Revealed that the implementation actions that are consistent with both the association's detection and response programs, or depending on the degree of severity, generate higher-level observers.

**Use Case 2: Account Management and Policy Changes**

**Scenario**: Detect Anti-Trafficking in Persons Username and Policy Rearrangements Scenario **Background:** To continue ensuring security policies are highly regarded and major unauthorized access changes are explored, the SOC observer should indeed maintain oversight on account management system and policy changes.

**Steps:**

**1. Monitoring Account Additions to Groups:**

Perform the query to preserve records of any modifications to local security groups. Start concentrating on the target accounts and individuals in the organization.

**2. Identify User or Group Creation:**

Complete the request to explore the creation of new users or community organizations. Suggest paying a great deal of attention to the input field, type, and topic user.

**3. Track Changes to User Rights Assignment:**

Operate the query to keep track of design changes to user rights dissemination. Examine out because of customized policy keys and reconfigured values.

**4. Monitor Changes to Security Policies:**

Utilize the query to check the status of changes to security policies. Start examining the goals of sustainable development, the identification number, and improvements.

**5. Investigation and Response:**

To verify whether such changes are authorized, correlate the processes occurring to authorized project changes or policies.  
Execute the association's vulnerability management policies and standards to capture, completely remove, and recover from the occurrence if unauthorized access updates are considered.

**Use Case 3: Service and System Monitoring**

**Scenario:** Supporting System Health and Service Authenticity  
**Background:** To help maintain data consistency and effectively analyze possible concerns, the SOC analyst is accountable for keeping track of the software system and data.

**Steps:**

**1. Identify Windows Service Starts:**

Perform the query to identify when a Windows service starts. Pay close enough attention to the name and functionality of the service.

**2. Detect Changes in Service Configuration:**

Operate the query to look for improvements in the effects of strategic Look into modifications to the configuration and service name.

**3. Monitor System Shutdown Events:**

Run the inquiry to track events connected to the system shutdown. Examine shutdown patterns and any attendant recommendations.

**4. Investigate System Startup Events:**

Conduct the query to inspect the occurrences that took place based on the learning. Investigate boot rates and boot protocols.

**5. Investigation and Response:**

* To check whether some odd service initiations, alterations, or system incidents are valid, review the system documentation and necessary teams.
* If malicious activity is discovered, assess its impact, and execute the necessary measures in a manner consistent with vulnerability management regulatory requirements.

The SOC analyst ends up going through some kind of process of operations at every simulation to analyze, investigate, examine, and manage any serious security events and instabilities capable of connecting to the predefined Windows event IDs. Recognize that the scenarios may very well be customized to fit the distinctive systems, sources of information, and security standard operating procedures of a particular organization.

# **CHAPTER 05: IMPLEMENTATION**



## **ENVIRONMENT SETUP**

Take steps to ensure that you are equipped with both beneficial resources for software and hardware. Users may not need Windows hosts or Universal Forwarder even though you're negotiating with a CSV dataset. To host a Splunk implementation, you'll need a server or virtual machine. Investigate Splunk's hardware specifications in consideration of the existing quantity of data and forecast uses.

**Hardware Resources:**

|  |  |
| --- | --- |
| **Property** | **Description** |
| ***Manufacturer*** | **HP** |
| ***Model*** | **Pavilion** |
| ***Architecture*** | **x64 based** |
| ***Operating System*** | **Windows 11** |
| ***Processor*** | **Intel(R) Core (TM) i7-8550U CPU @ 1.80GHz 1.99 GH GHz** |
| ***RAM*** | **8 GB** |
| ***Storage*** | **1 TB** |

## **SPLUNK INSTALLATION**

* On the cloud service or virtual servers of one's preference, install Splunk Enterprise. Execute the following steps:  
  From the Splunk website, obtain the Splunk Enterprise installation package necessary for one’s computer system. Generate a Splunk Cloud account, start the installation, and execute the on-screen recommendations. Choose a configuration for installation.
* Whenever the completion of the installation has occurred, launch Splunk. Have a web browser to activate the Splunk Web interface by going to <http://localhost:8000>.

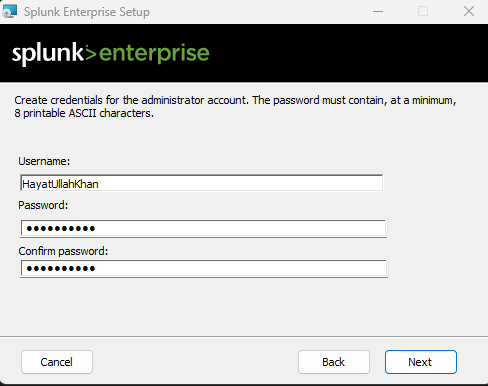


Figure 3: Splunk Enterprise Installation

A screenshot of a computer

Description automatically generated

Figure 4: Splunk Enterprise Login

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Figure 5: Splunk Enterprise Web view

**Add data:** Without including a reason to suspect, the preceding gives a comprehensive summary of each step for trying to carry out even the artifacts that use Windows Event Log data extracted from a CSV dataset.

## **CONFIGURE DATA INPUTS**

Users shall immediately disclose their CSV dataset into Splunk because they currently have one. Execute the following steps:

* Add the default usernames and passwords (admin/admin) to navigate the Splunk Web interface.
* Click " "Settings" and then "Data inputs."
* Tap "Files & Directories" once hitting "New."
* Choose your CSV dataset, after which select the appropriate source type

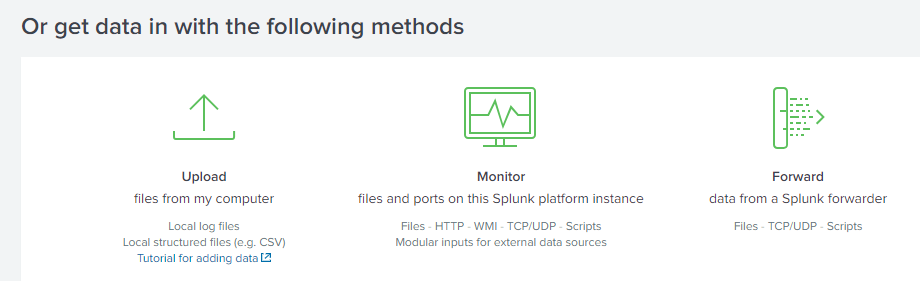


Figure 6: Upload data in Splunk

## **CREATE INDEXES**

To preserve the CSV data, users could very well generate an index:  
Pick "Settings" and thereafter "Indexes." Use the "Create Index" and give the index a name, including certain "windows event logs." Rearrange maintenance preferences and other details as desired.

A screenshot of a computer

Description automatically generated

Figure 7: Create Index in Splunk

## **CONFIGURE SOURCE TYPES**

Designed one's CSV data's source type:

Select "Settings" and thereafter "Source Types." Pick "Add new" and specify a name, also including "csv windows event." Describe the timestamp format, field extractions, and other configurations.

A screenshot of a computer

Description automatically generated

Figure 8: uploading Security Events csv file in Splunk

## **WRITING SEARCH QUERIES**

Construct search queries to either get significant information from the Windows Event Log or the Data processing, altering, and summarizing data are almost all entirely feasible through Splunk's Search Processing Language (SPL). Develop search queries to conduct a survey from your CSV files:  
Execute queries that use the Splunk Search & Reports app.

To collect all events, for example, in the case:

'sourcetype=csv windows event' index="windows event logs"

Take into consideration the following specific instances of queries:

View All Events by Event ID:

source="security.csv" host="WINDOWS" sourcetype="csv"| stats count by "Event ID", "Task Category"

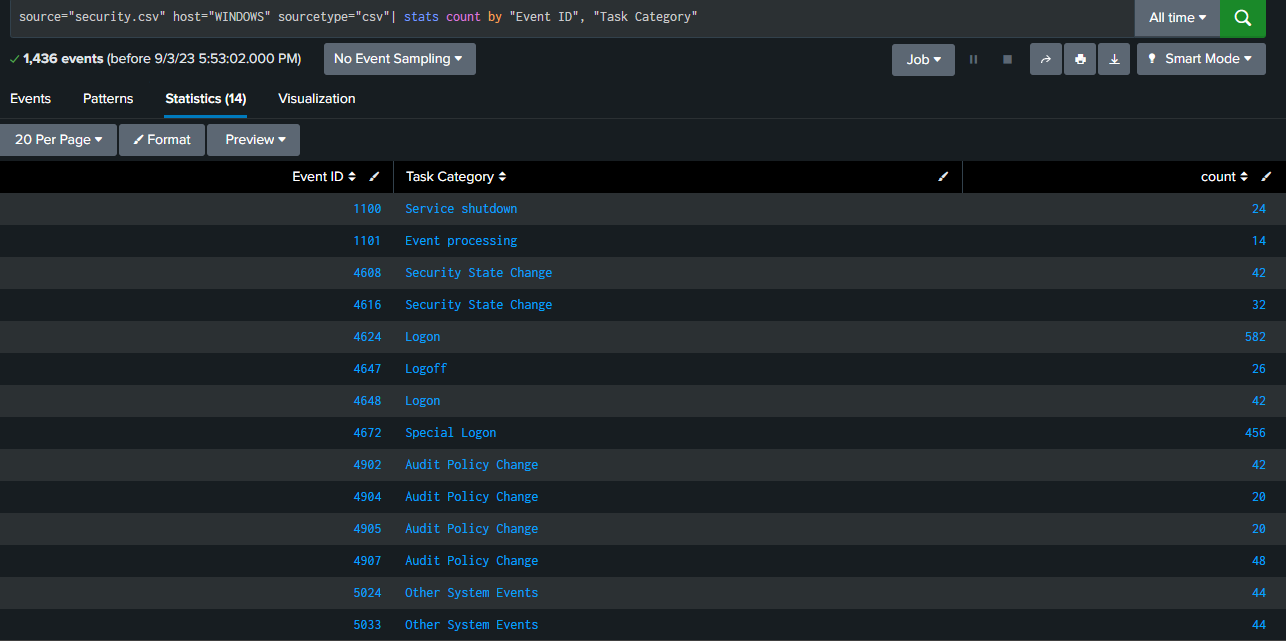


Figure 9: Query to View All Events by Event ID

## **BUILD VISUALIZATIONS**

To effectively characterize the CSV file, design visuals. Charts, tables, and dashboards seem to be just a few of the numerous visualization alternatives that Splunk enables. Using the search queries as an example, create visualizations:  
Select "Search & Reports" > "Visualizations" from the menu.  
In accordance with the outcomes of your query, choose a visualization type (such as "line chart," "table," or "pie chart") and configure configuration information.

**Time Chart Visualization:**

Create a time chart to visualize the trend of successful login events over time.

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=4624 | timechart count

A graph on a computer screen

Description automatically generated

Figure 10: Time chart to visualize the successful login events

source="security.csv" host="WINDOWS" sourcetype="csv" | timechart count by "Event ID"

A screen shot of a computer

Description automatically generated

Figure 11: Column chart to visualize all events

## **CORRELATION SEARCHES**

Initiate correlation searches to investigate for trends or errors throughout several data sources. This could also aid in the monitoring of operational or security issues.

## **SCHEDULED REPORTS**

Establishing and disseminating reports automatically depends on the organic listings. Sharing data with those involved is essential.

## **ADVANCED QUERIES**

Suppose you have high-dimensional data that has been analyzed using Splunk's statistical analysis, anomaly detection, and machine learning tools.

* 1. **MAINTAIN AND OPTIMIZE**Maintaining validity and performance as your data and requirements change requires periodic examination and modification of your results, indexes, and dashboards.
  2. **TESTING**

Verify their architectural features and configuration in depth. Guarantee that your alarms, visualizations, and search queries function as planned. To verify that the system can accommodate patterns, analyze multiple scenarios.



## **DOCUMENTATION**

Include every single one of their modifications, configuration settings, search terms, and installation methodology. This documentation will then be essential for attempting to maintain, be complete and accurate, and troubleshoot.

## **MONITORING AND MAINTENANCE**

Use monitoring tools to monitor and report on your Splunk instance's efficiency as well as its general wellness. Evaluation and enhancement of your user preferences, indexes, and visualizations on a continuous basis. Implement scheduled maintenance procedures, such as security patches and performance enhancements.

The accompanying is a typical, narrative illustration of the way a SOC analyst might implement the specified queries to inquire into potential security occurrences.

# **Chapter 06: RESULT**

Investigation based on designed artefact:

1. Initial Search for Successful Logins:

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=4624

A screenshot of a computer

Description automatically generated

Figure 12: Initial Search for Successful Logins in Splunk

2. Analyze Successful Logins:

*source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=4624 | table \_time, Level, extracted\_Source, "Task Category"*

A screenshot of a computer

Description automatically generated

Figure 13: Successful WIndow Login events

3. Identify Privilege Escalation Attempts:

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=4648

A screenshot of a computer

Description automatically generated

Figure 14: Events for Privilege Escalation Attempts

Detect Failed Logon Attempts:

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=4647

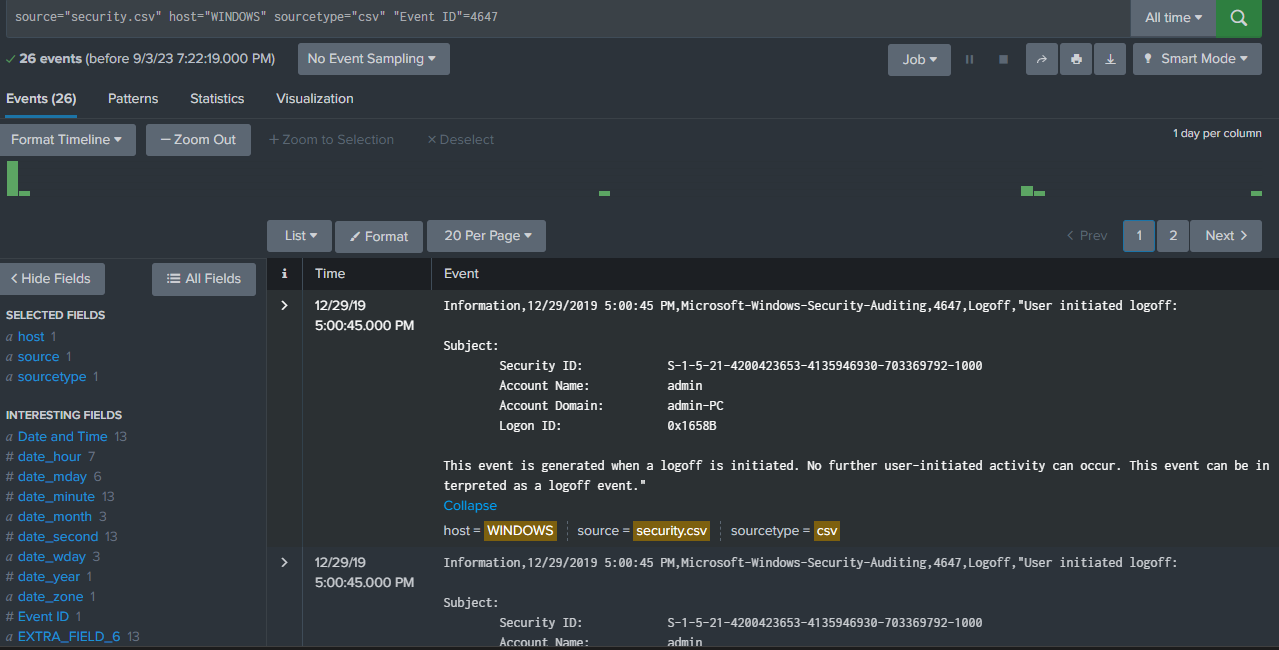


Figure 15: Detect Failed Logon Attempts in Splunk

Use Case 2: Account Management and Policy Changes

1. Monitoring Account Additions to Groups:

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=4907

A screenshot of a computer program

Description automatically generated

Figure 16: Monitoring Account Additions to Groups in Splunk

1. Identify User or Group Creation:

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=4902

A screenshot of a computer

Description automatically generated

Figure 17: Identify User or Group Creation in Splunk

1. Track Changes to User Rights Assignment:

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=4904

A screenshot of a computer

Description automatically generated

Figure 18: Track Changes to User Rights Assignment in Splunk

1. Monitor Changes to Security Policies:

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=4905

A screenshot of a computer

Description automatically generated

Figure 19: Monitor Changes to Security Policies in Splunk

Use Case 3: Service and System Monitoring

A screenshot of a computer

Description automatically generated

Figure 20: Service and System Monitoring analysis in Splunk

1. Detect Changes in Service Configuration:

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=5033

A screenshot of a computer

Description automatically generated

Figure 21: Detect Changes in Service Configuration

2. Monitor System Shutdown Events:

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=1100

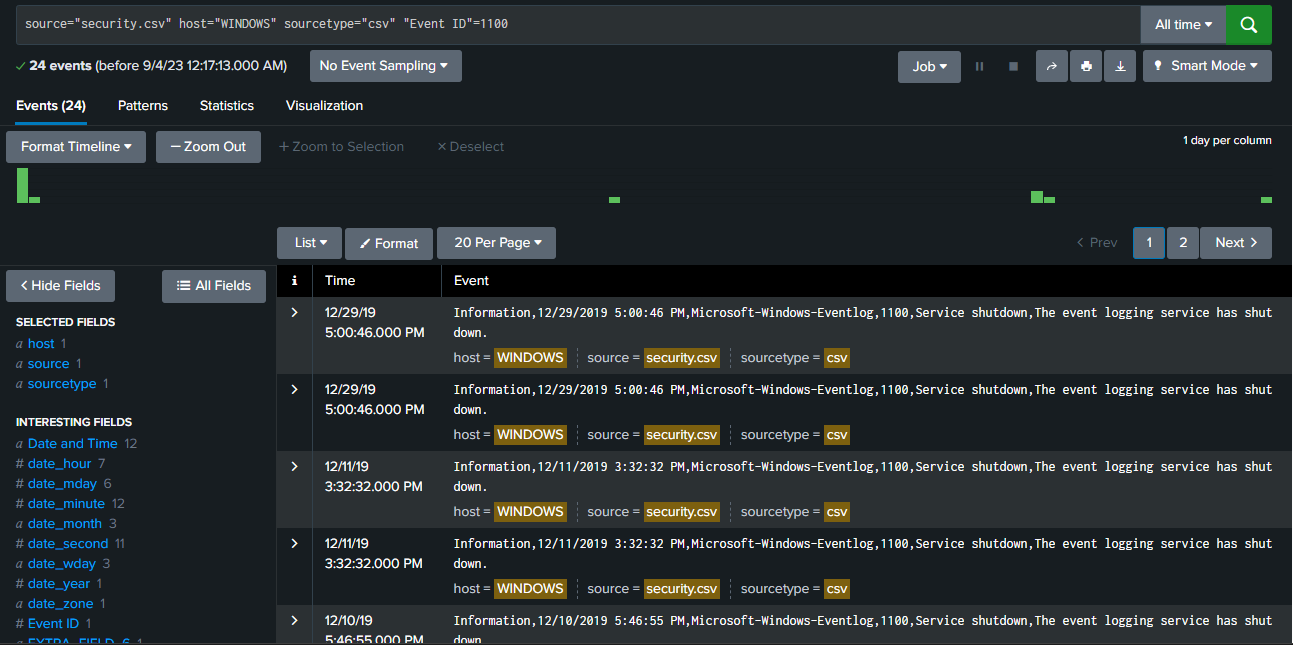


Figure 22: Monitor System Shutdown Events

3.Investigate System Startup Events:

source="security.csv" host="WINDOWS" sourcetype="csv" "Event ID"=1101

A screenshot of a computer

Description automatically generated

Figure 23: Investigate System Startup Events

**DISCUSSION**

In the cases mentioned, we really need a quick overview from the inside of the skilled SOC expert Emily's day and when she has been using Splunk queries to monitor and watch out for cybersecurity issues in a Windows system and respond immediately. The article illustrates the significant role SOC analysts play in maintaining a corporation's cryptographic certificates and trying to secure open-source operations.  
The concept of real-time observation in uncovering unwanted access to the computer system has been demonstrated by Emily's fast and accurate skills in identifying unexpected login actions (Event ID 4624) and critically evaluating issues. Her proactive approach to customer support administration and regulation variations (Event IDs 4902, 4904, 4905, and 4907) further emphasizes both the significance of development policy ideological commitment and the intensity of collaborating with illicit changes. Especially over the past, but really not least, her dedication to accuracy in tracking the movement of the security of the system (Event IDs 5024, 5033, 1100, 1101) characterizes how crucial it is to be continuing to keep IT operations balanced.  
A surprisingly common characteristic in this type of situation is the economic growth of Splunk queries as a means of evaluating information and ongoing investigations. Emily tends to make use of Splunk's skills and knowledge to understand massive volumes of security event data, designed to allow her to see potential complications, take immediate action, and maintain robust cybersecurity core strength quickly better.

# **CHAPTER 07: CONCLUSION**

As a result, the formation of an artifact towards using Splunk to communicate directly with Windows Event Log data seems to be a complex and difficult undertaking that has the objective of continuing to give system administrators effective toolkits for real-time monitoring, considering, and protecting complex public systems. This artifact offers an easily understood graphical interface, significant steps that can be taken, and comprehensive query and modeling possibilities to resolve the disconnect between the complexity of log data and the demands of users. This artifact switches into a significant instrument for security professionals by comprehensively constructing both web service and server components and connecting with Splunk's high-end specifications, actively encouraging data-driven decision-making and a proactive interactionist perspective. The artifact must undergo regular management, user input, and upgrades to continue to be usable and comply with the constantly evolving specifications of system administrators in their endeavor to control systems.

The example demonstrates how crucial SOC analysts and material removal vulnerability management tools like Splunk are to an effective cybersecurity ecosystem. The contribution and technical expertise Emily illustrated all through her interrogations emphasize the market pressure for key professionals who could also skillfully properly assess security event information and engage in effective and timely steps towards safeguarding organizations information.

Emily is competent enough to successfully explore some kind of broad spectrum of privacy event attribute values, ranging from username and password to guideline alterations and system health monitoring, by incorporating Splunk's skills and abilities. Her behavior and attitude provide an excellent explanation of the monetary worth of a complete and accurate security plan, which includes real-time monitoring, prompt reaction, and open communication with other IT and security teams.

 The opportunities that are available act as an illustration of the ongoing difficulties in the subject of cybersecurity. Businesses should indeed purchase through both skilled candidates and material removal innovations to maintain a competitive edge in terms of potential consequences and preserve the anonymity, validity, and accessibility of their data and systems as attackers keep on developing.

**Limitations:**

Although the sequence of events does provide a comprehensive description of a SOC analyst's collecting and measuring data and displays some potentially beneficial aspects associated with using Splunk for analysis, it's important to take into account predefined advantages and disadvantages:

**1.Simplified Representation:**

The various utilitarian aspects of a densely packed portrayal of a SOC analyst's day in practice, SOC operations can turn out to be more complex and difficult; systems require a higher level of knowledge, a wider-ranging partnership approach, and advanced analytics.

**2. Resource Requirements:**

Staff members, teaching, and infrastructural facilities were only a few of the essential resources needed for efficient security monitoring and incident response. Multinational corporations with constrained resources could experience challenges putting such strategies into effect.

**3.Scenario Specificity:**

The scenario only addresses a relatively small number of Windows event IDs, simply trying to take into consideration the broad spectrum of prospective security tools and events that could be useful depending on different system preferences.

**4. Real-Time Challenges:**

Because of the immense amount of information captured and the legal obligation to control both false positives and false negatives, locating and responding to security vulnerabilities in real-time can be hard and expensive in the virtual world.

**5. Legal and Compliance Considerations:**

Trying to investigate known vulnerabilities more and more often usually involves legal as well as administrative issues, such as data privacy laws and the management of custody for evidence, which are not attempted to address in this context.

Considering the advantages and disadvantages, the set of circumstances continues to offer interesting information on the task of SOC analysts and the possible applications of how to use technologies like Splunk for security monitoring and vulnerability management. It looks and behaves as a point of departure for interactions on ideal approaches to carrying out cybersecurity initiatives.

# **REFERENCES**

[1] SearchWindowsServer. (n.d.). What is Windows event log? - Definition from WhatIs.com. [online] Available at: https://www.techtarget.com/searchwindowsserver/definition/Windows-event-log.

[2] What Is a Windows Event Log? - IT Glossary | SolarWinds. (n.d.). [Www.solarwinds.com](http://Www.solarwinds.com) Retrieved July 28, 2023, from <https://www.solarwinds.com/resources/it-glossary/windows-event-log>.

[3] crowdstrike.com. (n.d.). *What is an Application Log? Definition and Types - CrowdStrike*. [online] Available at: <https://www.crowdstrike.com/cybersecurity-101/observability/application-log/>.

[4] www.solarwinds.com. (n.d.). *What Is a Windows Event Log? - IT Glossary | SolarWinds*. [online] Available at: <https://www.solarwinds.com/resources/it-glossary/windows-event-log>.

[5] www.manageengine.com. (n.d.). *Log Visualization and Analysis Tool - Read and Analyze your Logs Online | EventLog Analyzer*. [online] Available at: https://www.manageengine.com/products/eventlog/log-visualization-tool.html [Accessed 28 Jul. 2023].

[6] Sahoo, P.K., Chottray, R.K. and Pattnaiak, S., 2012. Research issues on windows event log. *International Journal of Computer Applications*, *41*(19).

[7] Ibrahim, N.M., Al-Nemrat, A., Jahankhani, H. and Bashroush, R., 2011, August. Sufficiency of windows event log as evidence in digital forensics. In *International Conference on e-Democracy* (pp. 253-262). Berlin, Heidelberg: Springer Berlin Heidelberg.

[8] Codona, B., 2007. Analysis and Evaluation of the Windows Event Log for Forensic Purposes. In *Honour Project, Edinburgh Napier Univ.*

[9] Do, Q., Martini, B., Looi, J., Wang, Y. and Choo, K.K., 2014. Windows event forensic process. In *Advances in Digital Forensics X: 10th IFIP WG 11.9 International Conference, Vienna, Austria, January 8-10, 2014, Revised Selected Papers 10* (pp. 87-100). Springer Berlin Heidelberg.

[10] He, S., Zhu, J., He, P. and Lyu, M.R., 2020. Loghub: A large collection of system log datasets towards automated log analytics. *arXiv preprint arXiv:2008.06448*.

[11] Schauland, D., Jacobs, D., Schauland, D. and Jacobs, D., 2016. Managing the windows event log. *Troubleshooting Windows Server with PowerShell*, pp.17-33.

[12] J. Dwyer and T. M. Truta, "Finding anomalies in windows event logs using standard deviation," 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, Austin, TX, USA, 2013, pp. 563-570, doi: 10.4108/icst.collaboratecom.2013.254136.

[13] Rozinat, A., De Jong, I.S.M., Günther, C.W. and van der Aalst, W.M., 2007. Process mining of test processes: A case study.

[14] Ahmed, F., Jahangir, U., Rahim, H. and Ali, K., 2020, February. Centralized Log Management Using Elasticsearch, Logstash and Kibana. In *2020 International Conference on Information Science and Communication Technology (ICISCT)* (pp. 1-7). IEEE.

[15] Yamiun, M.M., Katt, B. and Gkioulos, V., 2020. Detecting windows-based exploit chains by means of event correlation and process monitoring. In *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 2* (pp. 1079-1094). Springer International Publishing.

‌

‌

‌