Enhancing Security Operations with Advanced SIEM Capabilities

Tirth Sharaf

DePaul University

CSEC 594: Security Capstone

Dr. Filipo Sharevski

03/18/2024

Enhancing Security Operations with Advanced SIEM Capabilities

Executive Sumaary

This capstone project explores the advanced capabilities of the Splunk Enterprise Security Information and Event Management (SIEM) solution to enhance organizational cybersecurity operations. Two use cases were examined:

Use Case 1: Custom Alerting and Incident Response (Practical Implementation)

Splunk's powerful data indexing and correlation enabled the creation of custom alerts to detect potential security incidents, such as malicious code execution on Windows clients. An alert management system streamlined incident triage, prioritization, and resolution. A practical implementation was conducted to validate this use case.

Use Case 2: Machine Learning for Advanced Threat Detection (Theoretical Exploration)

This section presents a research exploration of leveraging Splunk's Machine Learning Toolkit (MLSPL) for advanced threat detection, particularly against Advanced Persistent Threats (APTs). The research reviewed existing literature on machine learning techniques for threat detection within SIEM solutions, focusing on anomaly detection algorithms like Supervised and Unsupervised Learning for their effectiveness in identifying APT-related activity.

The project demonstrated Splunk's extensive functionality for enhancing security posture through advanced data analysis, customizable alerting, and machine learning-driven threat detection (theoretically), alert management, and risk quantification. By proactively detecting and responding to incidents, organizations can reduce risk exposure and maintain critical asset security, underscoring the importance of robust SIEM solutions against evolving cyber threats.

Enhancing Security Operations with Advanced SIEM Capabilities

1. Introduction

1.1. The Evolving Threat Landscape: Why Robust Security Solutions are Essential

The digital revolution has irrevocably transformed the way organizations operate. Businesses of all sizes leverage interconnected networks to foster collaboration, streamline operations, and drive innovation. However, this interconnectedness creates a double-edged sword. While it offers immense benefits, it also exposes organizations to a complex and ever-evolving security landscape.

The attack surface – the entirety of an organization's digital presence vulnerable to cyberattacks – has expanded exponentially. This enlarged landscape presents a constant barrage of cyber threats, ranging from common malware attacks exploiting system vulnerabilities to sophisticated Advanced Persistent Threats (APTs) targeting specific organizations and their valuable data. APTs are highly targeted attacks carried out by skilled adversaries who employ stealthy tactics to gain unauthorized access, establish persistence within a network, and exfiltrate sensitive information.

In this ever-changing threat environment, robust security solutions are no longer a luxury; they are a necessity. Organizations must possess the capability to safeguard critical assets, ensure business continuity, and protect sensitive data. Traditional security tools, while valuable, often operate in silos, hindering a holistic view of security activity across the network. This fragmented approach can lead to missed threats, delayed detection, and inefficient incident response.

1.2. SIEM: A necessity for Streamlining Security Operations in the Enterprise

Security Information and Event Management (SIEM) solutions act as the central nervous system for an organization's security posture. They function by collecting, aggregating, and analyzing security data (logs and events) generated from a multitude of security tools deployed across the IT infrastructure. This includes firewalls, intrusion detection/prevention systems (IDS/IPS), endpoint security solutions, applications, and even network devices.

Enhancing Security Operations with Advanced SIEM Capabilities

Traditionally, security teams faced the significant challenge of managing security logs from these siloed tools independently. Each security tool generates its own logs, often in varying formats and locations. This fragmented approach presented several difficulties:

- **Limited Visibility:** Security analysts would need to manually pivot between different consoles and log viewers to gain a comprehensive view of security activity across the network. This hindered the ability to identify potential threats that might span multiple security tools.
- **Inefficient Threat Detection**: Correlating security events from disparate sources was a time-consuming and laborious task. This could lead to missed threats or delayed detection, potentially allowing attackers to gain a foothold within the network.
- **Slow Incident Response:** Investigating security incidents required manually sifting through logs from various tools, hindering timely response and containment efforts.
- **Increased Workload for Security Teams:** Managing and analyzing logs from multiple security tools placed a significant burden on security teams, limiting their ability to focus on strategic security initiatives.

SIEMs address these challenges by consolidating security data into a central platform, offering a holistic view of security activity across the IT infrastructure. This centralized approach empowers security teams to overcome the limitations of traditional log management and significantly enhance their overall security posture.

1.3. The Power of SIEM: Benefits and Role in the Industry

Security Information and Event Management (SIEM) solutions have become an indispensable tool, acting as the central nervous system for security operations across various industries. They offer a multitude of benefits that empower security teams to significantly enhance their effectiveness. Here's how SIEMs transform security postures:

- **Proactive Threat Detection:** SIEMs consolidate security data from diverse tools into a single platform, providing a holistic view of activity across the entire IT infrastructure.

Enhancing Security Operations with Advanced SIEM Capabilities

This allows security teams to correlate events and identify subtle anomalies or indicators of compromise (IOCs) that might evade siloed monitoring. Imagine a SIEM correlating a failed login attempt with unusual access attempts from a geographically suspicious location, highlighting a potential attacker before a breach occurs.

- **Streamlined Incident Response:** In the face of a security incident, time is critical. SIEMs provide real-time alerts and comprehensive investigation tools, allowing security analysts to quickly pinpoint the source of the attack, understand the scope (affected systems and data), and take targeted actions to contain the threat, minimize damage, and eradicate the attacker's presence.
- **Enhanced Security Compliance:** Many regulations require organizations to collect and retain security data for audits. Traditionally, this was a manual and time-consuming process. SIEMs automate this process by collecting and storing relevant security data and generating reports that demonstrate compliance, streamlining the audit process and reducing workload for security teams.

In essence, SIEMs act as a force multiplier for security operations. They empower teams to proactively detect and respond to threats, ultimately safeguarding critical assets and ensuring business continuity.

1.4. Limitations of Traditional SIEMs and the Rise of Advanced Threats

While SIEM solutions offer significant benefits, it's crucial to acknowledge their limitations in the face of an ever-evolving threat landscape. Traditional SIEMs primarily rely on rule-based detection methods. These methods are effective for identifying known threats with well-defined signatures. However, advanced threats like Advanced Persistent Threats (APTs) often employ sophisticated techniques to evade signature-based detection.

APTs are targeted attacks carried out by skilled adversaries who employ stealthy tactics to gain unauthorized access to a network, establish persistence, and exfiltrate sensitive information. These attackers continuously adapt their tactics, making it difficult for traditional SIEMs to keep pace. Additionally, the sheer volume of security data generated by modern IT infrastructures can overwhelm traditional SIEMs, hindering their ability to identify critical security events amidst the noise.

1.5. Harnessing the Power of Advanced SIEM: Our Project Focus

This project, titled "Enhancing Security Operations with Advanced SIEM Capabilities," explores the potential of advanced SIEM functionalities to address these limitations and empower organizations to combat the evolving threat landscape. We place particular emphasis on investigating how these advanced capabilities can be leveraged to combat sophisticated threats like APTs.

The project will delve into two key use cases that showcase the potential of advanced SIEM features:

- **Use Case 1: Custom Alerting and Streamlined Incident Response (Practical Implementation):** This section showcases the practical implementation of custom alerts within a SIEM solution to detect specific security incidents. It demonstrates the effectiveness of leveraging advanced SIEM capabilities for streamlined incident response, enabling security teams to react faster and more effectively to potential threats.
- **Use Case 2: Machine Learning for Advanced Threat Detection (Research Exploration):** This section explores the theoretical application of a SIEM's Machine Learning Toolkit (MLSPL) for advanced threat detection. It examines the potential of machine learning algorithms to identify anomalous patterns indicative of sophisticated attacks like APTs. By leveraging machine learning, SIEMs can potentially detect previously unknown threats and improve the overall security posture of an organization.

By investigating these use cases, the project aims to demonstrate that advanced SIEM functionalities can significantly enhance security operations by enabling organizations to:

- Proactively detect and respond to advanced threats, including APTs.
- Improve threat visibility and situational awareness across the network.
- Streamline incident response processes for faster containment and mitigation.

Enhancing Security Operations with Advanced SIEM Capabilities

- Enhance the effectiveness of security teams through automation and advanced threat detection capabilities.

Ultimately, this project seeks to contribute valuable insights into how organizations can leverage advanced SIEM functionalities to stay ahead of the evolving threat landscape and safeguard their critical assets.

1.6. Purpose of This Report

This report serves a twofold purpose:

- **To inform:** This report aims to inform readers about the limitations of traditional SIEMs in the face of evolving cyber threats. It sheds light on the potential of advanced SIEM functionalities, specifically User Entity Behavior Analytics (UEBA) and Machine Learning (ML) for advanced threat detection.
- **To showcase our project:** This report delves into our project titled "Enhancing Security Operations with Advanced SIEM Capabilities." It details the two key use cases we will explore: practical implementation of custom alerting with UEBA and theoretical exploration of machine learning for advanced threat detection. Ultimately, the report seeks to demonstrate the value proposition of advanced SIEM functionalities in enhancing an organization's security posture.

By understanding the limitations of traditional SIEMs and the potential of advanced functionalities, organizations can make informed decisions about their security strategies. This report serves as a springboard for further discussion and exploration of how advanced SIEM capabilities can be leveraged to stay ahead of the ever-changing threat landscape.

2. Addressing Common Concerns Regarding the project

- Appropriateness for the Security Capstone: Undertaking the project "Enhancing Security Operations with Advanced SIEM Capabilities" for my master's capstone was a deliberate choice aimed at challenging myself and deepening my understanding of defensive security measures, particularly in the realm of Security Information and Event Management (SIEM). While I had prior exposure to offensive security techniques, this project provided me with a unique opportunity to explore the critical role of defensive security in safeguarding organizations against cyber threats. Through this project, I not only expanded my knowledge of SIEM technologies but also gained practical insights into the complexities of securing a company's digital assets in today's threat landscape. By grappling with real-world challenges and complexities, I honed my problem-solving skills and developed a deeper appreciation for the importance of proactive threat detection and incident response strategies in mitigating cyber risks.

- Advanced Aspects of the Project: The project showcased advanced capabilities of SIEM, particularly Splunk, in detecting and responding to cyber threats. While navigating through the investigation process, I leveraged various features and functionalities of Splunk, such as log aggregation, correlation searches, and visualization tools, to analyze vast amounts of security event data and identify potential indicators of compromise. Additionally, I explored advanced techniques such as threat hunting and the integration of threat intelligence feeds to enhance the effectiveness of the SIEM solution. Despite facing limitations due to resource constraints, particularly in terms of machine RAM, I attempted to implement a range of advanced use cases and methodologies within the scope of the project proposal. Although I couldn't execute every aspect as intended, I embraced the opportunity to learn and adapt, ultimately gaining valuable insights into the practical application of SIEM technologies in a real-world security environment. Through this hands-on experience, I not only expanded my technical skills but also cultivated a mindset of continuous learning and experimentation in the field of cybersecurity.

3. Literature Review.

Let's Security Information and Event Management (SIEM) solutions have been widely adopted by organizations as a critical component of their cybersecurity strategies. Numerous research studies and industry reports have explored the capabilities and benefits of SIEM solutions in enhancing security operations.

One of the key advantages of SIEM solutions highlighted in existing research is their ability to consolidate and analyze security-related data from diverse sources across an organization's infrastructure (Kotenko et al., 2019). By centralizing log data from endpoints, networks, applications, and security devices, SIEM solutions provide a comprehensive view of an organization's security posture, enabling effective threat detection and incident response.

Several studies have explored the use of SIEM solutions for detecting and responding to advanced persistent threats (APTs) and targeted attacks (Nichols et al., 2021; Lee et al., 2020). These research efforts have highlighted the importance of incorporating advanced analytics, such as correlation rules and machine learning algorithms, within SIEM solutions to identify subtle indicators of APT activity and anomalous behavior patterns.

The integration of machine learning capabilities into SIEM solutions has been a significant area of focus in recent years. Researchers have investigated the application of various machine learning techniques, including supervised and unsupervised learning algorithms, for anomaly detection, user behavior analytics, and threat hunting (Sillitti et al., 2022; Thakur et al., 2021). These studies have demonstrated the potential of machine learning to enhance the threat detection capabilities of SIEM solutions and improve their ability to identify previously unseen or evolving threats.

Despite the numerous benefits and advanced capabilities of SIEM solutions, existing research has also identified several gaps and limitations. One of the major challenges highlighted is the complexity of SIEM implementations and the need for skilled personnel to configure and maintain these solutions effectively (Jain et al., 2020). Additionally, the volume and variety of security data ingested by SIEM solutions can lead to performance and scalability issues, requiring robust infrastructure and efficient data management strategies (Chandola et al., 2019).

Another limitation identified in current approaches is the lack of standardized risk calculation methodologies and the subjective nature of risk assessment within SIEM solutions (Ramaki et al., 2021). Inconsistent risk quantification can hinder the prioritization of security incidents and lead to inefficient allocation of resources for incident response.

Furthermore, existing research has highlighted the need for improved integration and interoperability between SIEM solutions and other security tools and platforms within an organization's security ecosystem (Ghafir et al., 2021). Seamless integration and data sharing among various security components can enhance the overall effectiveness of security operations and provide a more comprehensive and holistic view of an organization's security posture.

This project aims to address some of the identified gaps and limitations by exploring advanced SIEM capabilities, such as custom alerting, machine learning-driven threat detection, and a standardized risk calculation methodology. By leveraging these advanced features, organizations can enhance their security operations, improve threat detection accuracy, and prioritize incident response efforts more effectively.

4. Project Implentation

4.1. Enhanced Project Implementation for Use Case 1: Custom Alerting and Streamlined Incident Response

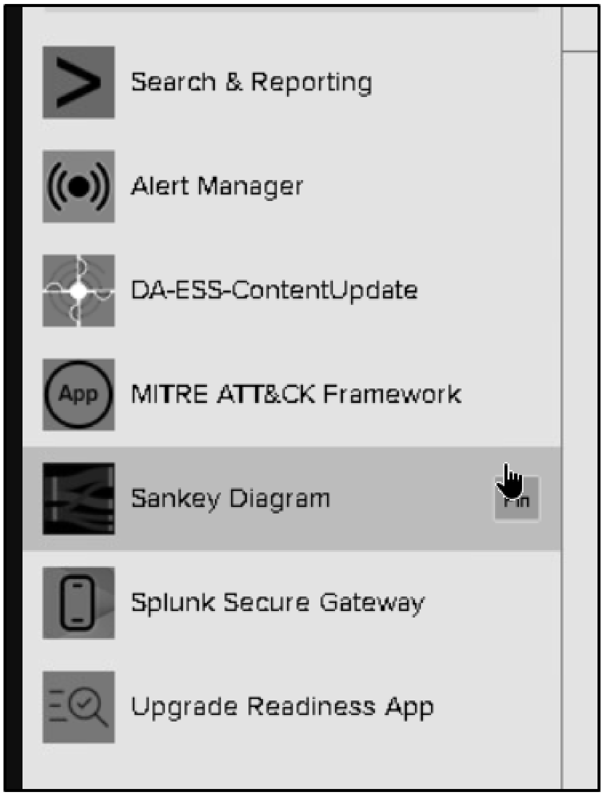
This section details the implementation approach for Use Case 1, which explores how custom alerts within a SIEM solution can be used to detect specific security incidents and expedite incident response.

The core tool for this project was Splunk Enterprise, a powerful SIEM platform renowned for its ability to collect, index, and analyze machine data from diverse sources. To further enhance Splunk's functionalities, several Splunk Apps were integrated:

- Alert Manager: This app empowers security teams with advanced alert management capabilities. It facilitates tasks like filtering alerts based on specific criteria, correlating related alerts, suppressing duplicate alerts to reduce noise, and routing alerts to appropriate teams or ticketing systems for efficient handling.

- MITRE ATT&CK Framework: This app integrates the MITRE ATT&CK knowledge base directly into Splunk. Security analysts can leverage this knowledge base to map detected security events to specific tactics and techniques employed by adversaries. This context is invaluable during incident response, allowing for a more targeted and efficient investigation.

- Splunk Secure Gateway: This app strengthens Splunk's communication security by encrypting data traffic between Splunk Universal Forwarders deployed on client machines and the central Splunk Enterprise server. This additional layer of encryption safeguards sensitive security data during transmission.



Installed necessary applications in splunk

To validate the effectiveness of the custom alerting functionality, a Trojan named **probablyBad.exe** was crafted using Kali Linux, a popular penetration testing platform. The Metasploit Framework's msfvenom utility within Kali Linux was used to generate the test payload.

The payload was designed to be particularly dangerous because it aimed to achieve persistence on the targeted Windows client machines by triggering the execution of both cmd.exe and PowerShell during system boot.

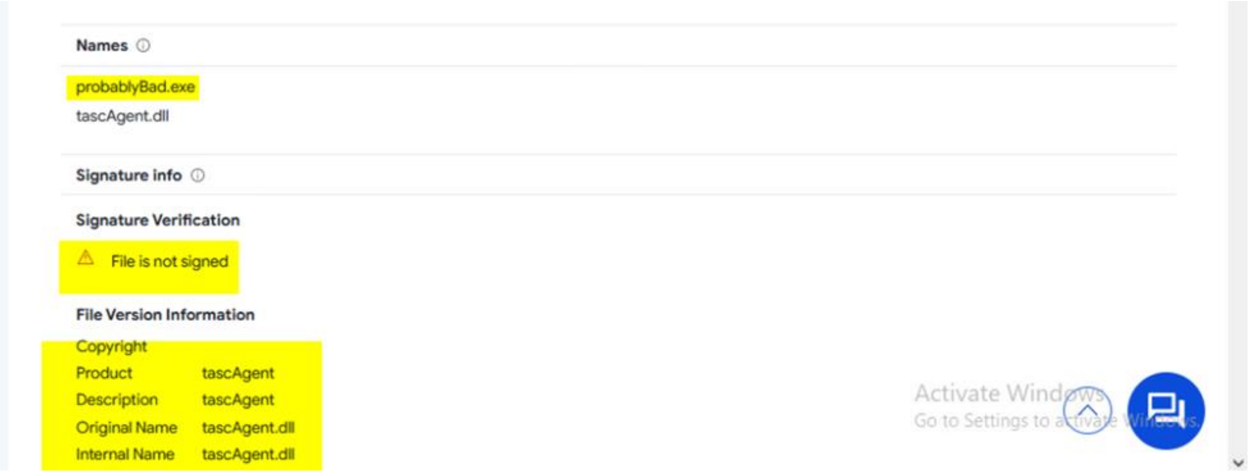
Here's why this scenario is dangerous:

- **Persistence:** By executing during system boot, the payload establishes persistence on the infected machine. This means the malicious code will run every time the system restarts, making it more difficult to detect and remove.
- **Privilege Escalation:** Both cmd.exe and PowerShell can be used to execute commands with administrative privileges on a Windows system. If exploited by a malicious payload,

this capability could allow attackers to gain control over critical system functions and install additional malware.

- **Lateral Movement:** Once a foothold is established on a machine, attackers can leverage tools like cmd.exe or PowerShell to move laterally across the network, potentially compromising additional devices and escalating the attack.

By simulating this type of Trojan attack, the testing process aimed to ensure that the custom alerting functionality could effectively detect such malicious activity and trigger appropriate alerts for prompt investigation and remediation.



Names ⓘ

probablyBad.exe
tascAgent.dll

Signature info ⓘ

Signature Verification

⚠ File is not signed

File Version Information

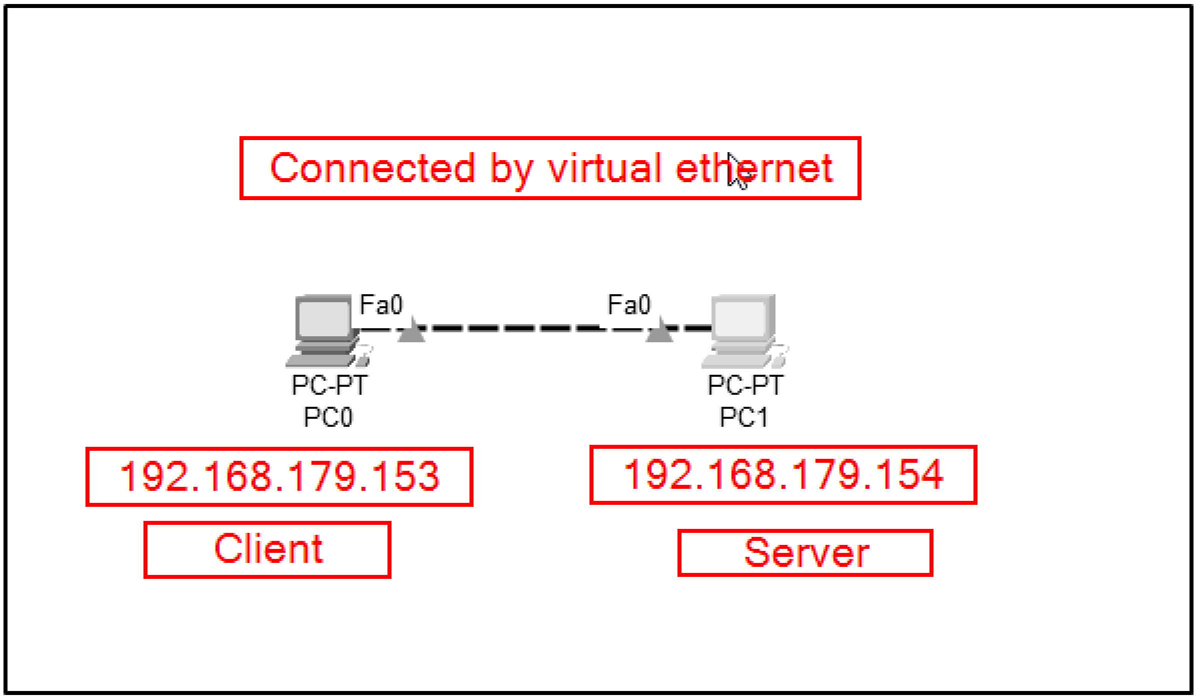
Copyright	
Product	tascAgent
Description	tascAgent
Original Name	tascAgent.dll
Internal Name	tascAgent.dll

probablyBad.exe-Trojan

A client-server architecture formed the foundation of the system design. Splunk Enterprise was deployed on a central server, acting as the core component for log collection, aggregation, analysis, and alert generation. Log data was collected from individual Windows client machines equipped with Splunk Universal Forwarders. These forwarders functioned as agents, responsible for gathering relevant log data from various sources on the client machines, including:

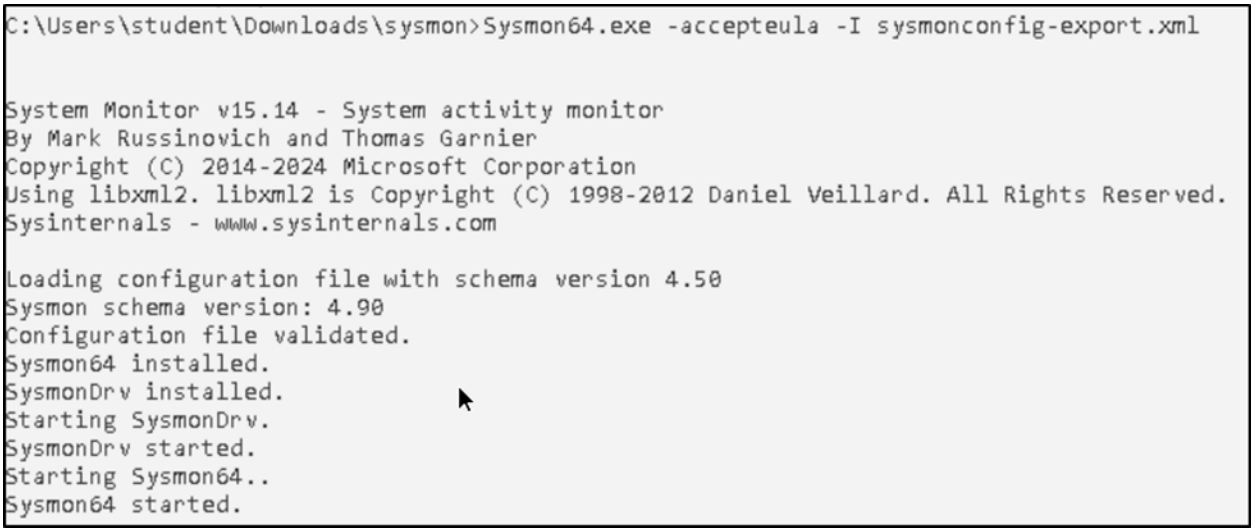
- Windows Event Logs: System-generated logs containing detailed information about system events and activities.

- Application Logs: Logs generated by specific applications running on the client machines, potentially containing security-relevant information.
- Network Traffic Data: Captured network traffic data can be valuable for identifying suspicious network activity or communication attempts.



Network Architecture of the Splunk environment

The Splunk instance was configured to ingest data from these diverse sources. To further enrich the detection of suspicious activity, Sysmon, a system monitoring tool, was additionally installed on the Windows client machines. Sysmon generates detailed logs of system activities, including process creation, network connections, and file changes, providing valuable insights for security analysis.

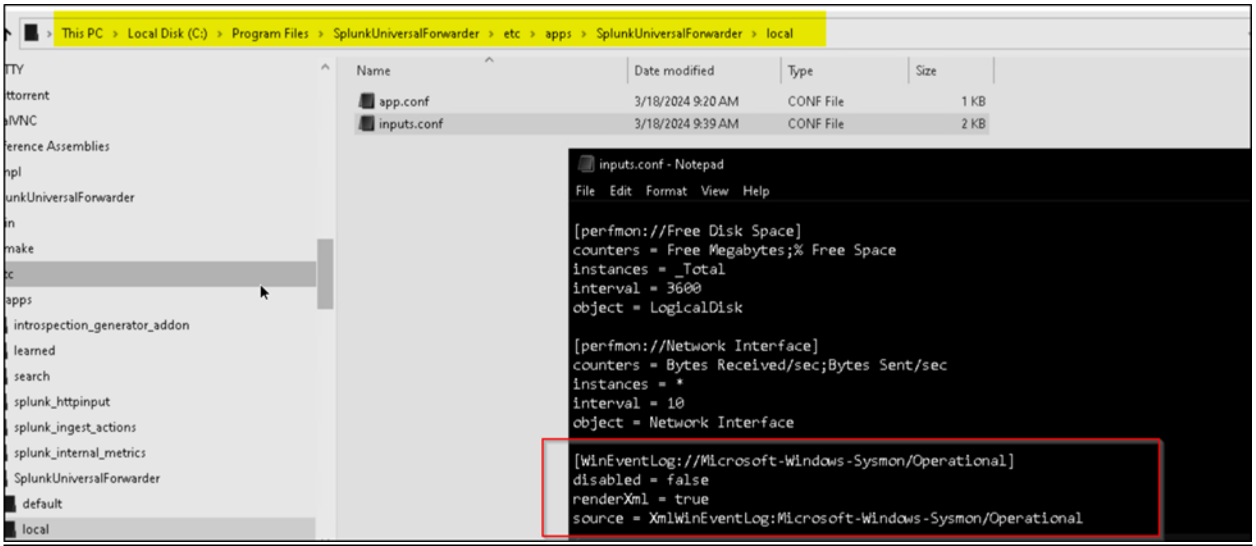


```
C:\Users\student\Downloads\sysmon>Sysmon64.exe -accepteula -I sysmonconfig-export.xml


System Monitor v15.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
```

Installing Sysmon



This PC > Local Disk (C:) > Program Files > SplunkUniversalForwarder > etc > apps > SplunkUniversalForwarder > local

Name	Date modified	Type	Size
app.conf	3/18/2024 9:20 AM	CONF File	1 KB
inputs.conf	3/18/2024 9:39 AM	CONF File	2 KB

inputs.conf - Notepad

```
[perfmon://Free Disk Space]
counters = Free Megabytes;% Free Space
instances = _Total
interval = 3600
object = LogicalDisk

[perfmon://Network Interface]
counters = Bytes Received/sec;Bytes Sent/sec
instances = *
interval = 10
object = Network Interface

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

Editing the inputs.conf file for windows log

Collected log data was then indexed and stored within Splunk's distributed data repositories. This indexing process facilitates efficient search and analysis of the collected security data. Splunk's Search Processing Language (SPL) was leveraged to create custom search queries and correlation rules. These queries and rules were designed to identify specific security events based on patterns within the collected log data. In this use case, the focus was on detecting the execution of cmd.exe or PowerShell on Windows client machines during system boot, potentially indicating a malicious attempt.

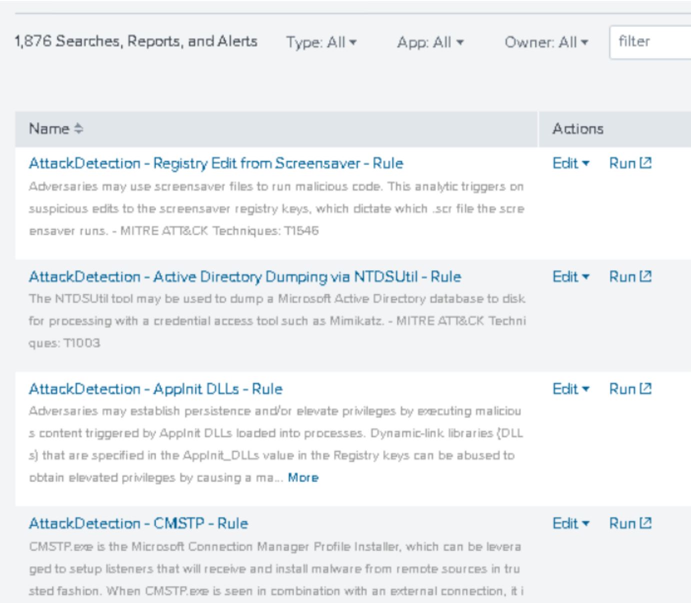
Enhancing Security Operations with Advanced SIEM Capabilities

Index=”main” sourcetype=xmlwineventlog EventCode=1 (cmd.exe OR powershell.exe) AND CommandLine != *Splunk

Here's a breakdown of what this search is looking for:

- **Index="main":** This specifies that the search should look in the "main" index for log data.
- **sourcetype=xmlwineventlog**: This filters the log data to events with a sourcetype of "xmlwineventlog," which typically corresponds to Windows Event Log data.
- **EventCode=1:** EventCode 1 in Windows Event Logs typically represents a system startup event.
- **(cmd.exe OR powershell.exe):** This part of the query is looking for events where the "cmd.exe" or "powershell.exe" processes were involved. It uses the logical OR operator to find events related to either of these processes.
- **AND CommandLine != *Splunk**: This part of the query excludes events where the "CommandLine" field contains the word "Splunk." It filters out events related to Splunk commands or operations, which can be useful to avoid self-referencing logs.

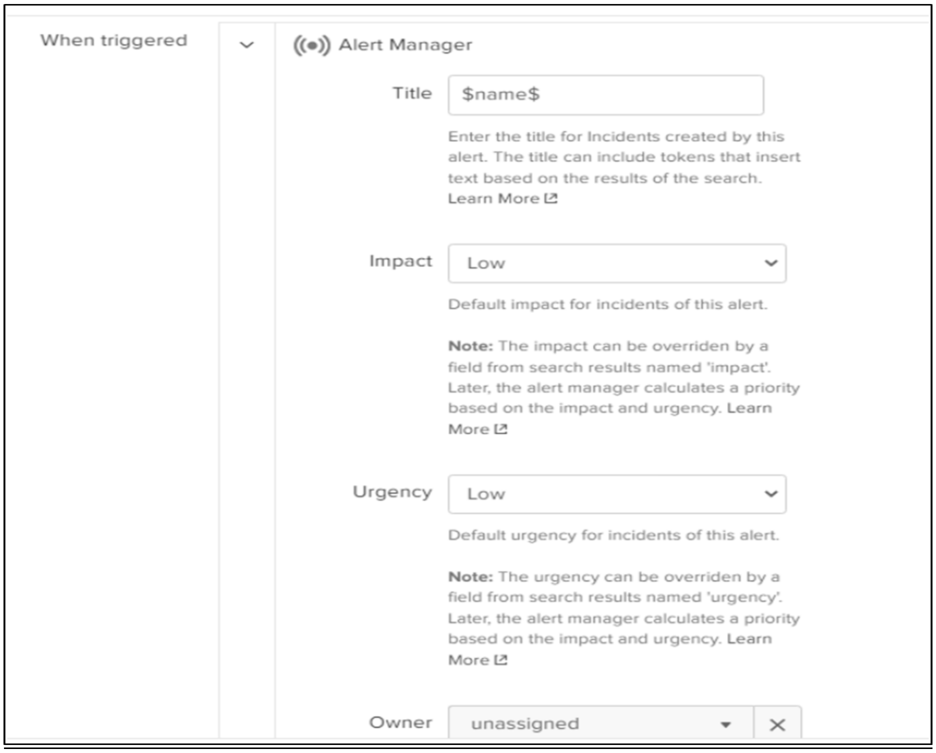
Once this search query was created, it was integrated with the Splunk Alert Manager app. This integration allows the system to automatically trigger alerts whenever the search query identifies a matching event in the log data. These alerts would then be routed and prioritized based on the severity and potential risk associated with the detected activity, enabling security teams to take swift action for investigation and remediation.



1,876 Searches, Reports, and Alerts   Type: All ▾   App: All ▾   Owner: All ▾   filter

Name ≑	Actions
AttackDetection - Registry Edit from Screensaver - Rule Adversaries may use screensaver files to run malicious code. This analytic triggers on suspicious edits to the screensaver registry keys, which dictate which .scr file the screensaver runs. - MITRE ATT&CK Techniques: T1546	Edit ▾ Run
AttackDetection - Active Directory Dumping via NTDSUtil - Rule The NTDSUtil tool may be used to dump a Microsoft Active Directory database to disk for processing with a credential access tool such as Mimikatz. - MITRE ATT&CK Techniques: T1003	Edit ▾ Run
AttackDetection - AppInit DLLs - Rule Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppInit DLLs loaded into processes. Dynamic-link libraries (DLLs) that are specified in the AppInit_DLLs value in the Registry keys can be abused to obtain elevated privileges by causing a ma... More	Edit ▾ Run
AttackDetection - CMSTP - Rule CMSTP.exe is the Microsoft Connection Manager Profile Installer, which can be leveraged to setup listeners that will receive and install malware from remote sources in trusted fashion. When CMSTP.exe is seen in combination with an external connection, it i	Edit ▾ Run

Created the custom rule



When triggered

Alert Manager

Title: $name$

Enter the title for Incidents created by this alert. The title can include tokens that insert text based on the results of the search. Learn More

Impact: Low

Default impact for incidents of this alert.

Note: The impact can be overriden by a field from search results named 'impact'. Later, the alert manager calculates a priority based on the impact and urgency. Learn More

Urgency: Low

Default urgency for incidents of this alert.

Note: The urgency can be overriden by a field from search results named 'urgency'. Later, the alert manager calculates a priority based on the impact and urgency. Learn More

Owner: unassigned

Set the alert as critical

The testing and evaluation procedures involved deploying the malicious payload crafted using msfvenom on one of the Windows client machines to simulate a real-world attack scenario. The

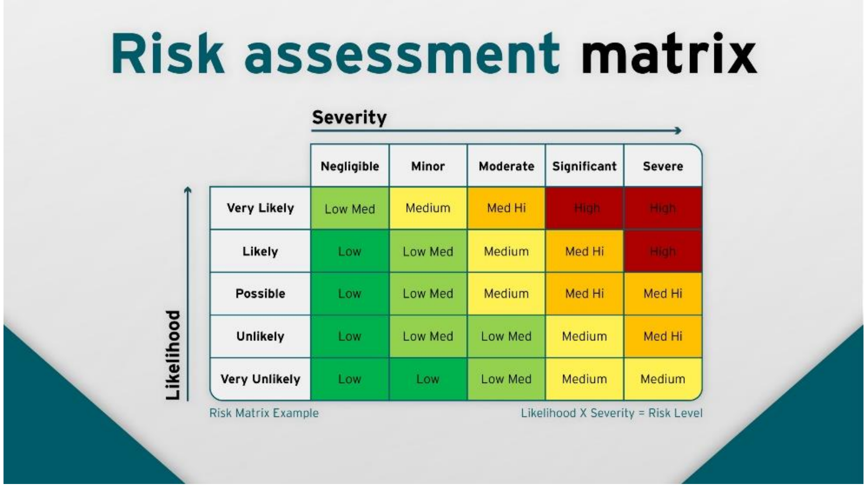
Splunk instance was then closely monitored to observe if the custom search queries and correlation rules successfully triggered corresponding alerts based on the payload execution.

The effectiveness of the alert management system was assessed by simulating various incident scenarios. This evaluation involved testing the triage process (categorization of alerts based on severity), prioritization (determining the order in which alerts are addressed), and assignment processes (assigning alerts to appropriate security personnel for investigation). The Alert Manager app likely played a significant role in streamlining these processes.

An essential aspect of this use case involved evaluating the effectiveness of the implemented risk calculation methodology. This methodology likely utilized a standard risk assessment matrix, a well-established framework for evaluating security risks. The matrix typically considers two key factors:

- **Impact:** This factor assesses the potential severity of the consequences if a security threat materializes. In this context, a critical alert might be triggered for scenarios with high potential impact, such as unauthorized access to sensitive data, disruption of critical systems, or compromise of a large number of devices.
- **Likelihood:** This factor assesses the probability of a security threat occurring. Here, the custom search query played a crucial role by identifying specific events associated with a high likelihood of malicious activity (e.g., execution of cmd.exe or PowerShell during system boot).

By applying this risk assessment matrix to different alert scenarios, the testing process aimed to assess how effectively the assigned risk scores influenced alert prioritization within the Splunk Alert Manager app. Ideally, scenarios with a high impact and high likelihood, such as the one identified by the search query, would trigger critical alerts. These critical alerts would be routed first to security personnel for immediate investigation and response, ensuring that the most impactful threats receive the highest level of attention.



Risk assessment matrix

Severity

Likelihood

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Risk Matrix Example

Likelihood X Severity = Risk Level

Following the standard risk matrix

This evaluation process helps to ensure that the risk calculation methodology effectively translates into actionable prioritization of alerts. By focusing on high-risk scenarios first, security teams can optimize their response efforts and mitigate potential security incidents with the greatest potential for harm.

By following these steps and leveraging the capabilities of Splunk Enterprise and the additional Splunk Apps, this use case demonstrates the practical application of custom alerting functionalities within a SIEM solution. This approach empowers security teams to proactively detect potential security incidents, streamline incident response processes, and ultimately improve overall security posture.

4.2. Project Implementation for Use Case 2: Leveraging Splunk Investigation Findings (Hypothetical Approach)

While a full-scale implementation wasn't feasible due to limitations in technical resources, particularly the processing power required to handle vast amounts of network data, the insights gleaned from the Splunk Boss of the SOC investigation remain valuable. This section outlines a hypothetical approach detailing key steps that could be taken within these resource constraints:

Enhancing Security Operations with Advanced SIEM Capabilities

1. Evaluating Existing Security Landscape (Always Relevant):

Regardless of resource limitations, a thorough assessment of the current security infrastructure is crucial. This evaluation would focus on identifying any potential gaps or weaknesses within the security architecture that could leave the organization, particularly a financial institution, vulnerable to sophisticated attacks employed by APT groups targeting sensitive financial data.

2. Optimizing SIEM Configuration (Prioritization):

Ideally, the SIEM system would undergo configuration changes to strengthen its ability to detect APT activities. However, with resource limitations, prioritizing critical changes is essential. This might involve fine-tuning alerting mechanisms to minimize false positives and prioritize alerts related to potential APT threats, such as execution of suspicious processes during system startup.

3. Enhancing Incident Response Procedures (Focus on APT-Specific Actions):

Incident response procedures would be updated to encompass specific measures for detecting, analyzing, and effectively responding to APT incidents. Given resource limitations, prioritizing the development and training for procedures specifically addressing APT threats would be essential. This could include incorporating steps for identifying suspicious lateral movement within the network, a common tactic employed by APTs.

4. Deploying Additional Security Controls (Phased Approach):

To further enhance the capabilities of the SIEM system and fortify the overall security posture, the organization might consider deploying additional security controls. A staged or phased approach to implementing these controls would be most practical. This could involve prioritizing endpoint detection and response (EDR) solutions, which can provide valuable insights into suspicious activity on user devices within the financial institution.

5. Patching and System Updates (Risk-Based):

A critical step involves identifying and patching vulnerabilities in critical systems, applications, and services. This focus would likely target vulnerabilities specifically exploited by APT groups during the investigation. A risk-based approach to prioritization would be necessary to ensure the most critical systems, such as those handling financial transactions, are patched first.

6. Monitoring Threat Intelligence Feeds (Streamlined Approach):

While continuous monitoring of threat intelligence sources is ideal, a more streamlined approach might be necessary due to resource limitations. This could involve focusing on monitoring high-priority threat intelligence feeds associated with known APT groups targeting the finance sector. Integrating these feeds with the SIEM system would still be beneficial for enriching security event data and identifying potential attack patterns.

7. Regular Security Audits and Assessments (Risk-Based):

Regular security audits and assessments are essential for evaluating the effectiveness of implemented security measures and identifying areas for further improvement. Given resource constraints, a risk-based approach focusing on critical systems and assets within the financial institution would likely be most practical.

8. Collaboration with External Partners (Leveraging Existing Relationships):

Building strong partnerships with external cybersecurity organizations, industry groups, and government agencies is crucial. However, leveraging existing relationships and participating in relevant information sharing initiatives (ISACs) specific to the finance sector might be a more realistic approach due to resource limitations. Collaboration allows for sharing threat intelligence and best practices for defending against APTs.

Benefits of Implementation in the Finance Sector

By implementing the strategies outlined above, even with resource constraints, a financial institution can significantly improve its security posture. Early detection and response to APT activities can prevent substantial financial losses, reputational damage, and regulatory violations. Prioritizing critical security measures and leveraging threat intelligence specific to the finance sector would enable security teams to focus their efforts on the most high-risk threats.

In conclusion, while resource limitations may have prevented a full-scale implementation, the insights gained from the Splunk investigation remain valuable. This hypothetical approach demonstrates that even with limited resources, financial institutions can take significant steps towards enhancing their security posture and mitigating the risks posed by Advanced Persistent Threats.

5. Report & Finidings

5.1. Use Case 1: Custom Rule Implementation and Alert Generation - Findings Report

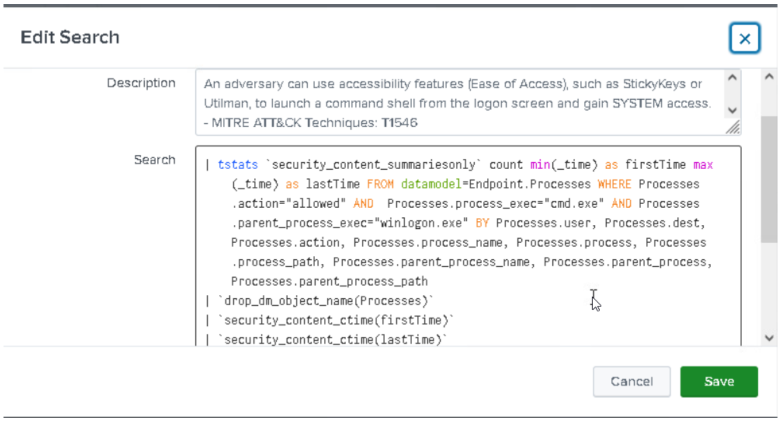
This section details the findings associated with Use Case 1, which focused on validating the effectiveness of the custom alerting functionality within Splunk. To achieve this, a test payload mimicking a Trojan attack was crafted and utilized to trigger a critical alert.

Custom Rule Implementation and Log Monitoring

A custom search query was implemented within Splunk to identify suspicious activity potentially indicative of malicious attempts to execute unauthorized programs during system startup. This query leveraged the following criteria:

- **Index:** "main" - This specifies that the search should focus on log data stored within the "main" index, where security-related events are likely to be located.
- **Sourcetype:** "xmlwineventlog" - This filters the log data to events with a sourcetype of "xmlwineventlog," typically corresponding to Windows Event Log data.
- **EventCode:** "1" - This targets events associated with system startup, a prime time for malicious actors to inject code for persistence.
- **Processes:** "(cmd.exe OR powershell.exe)" - This part of the query focuses on events involving either "cmd.exe" or "powershell.exe" processes, commonly used by attackers for various malicious activities.
- **CommandLine Exclusion:** " *Splunk" - This clause excludes events where the "CommandLine" field contains the term "Splunk." This helps to filter out noise generated by Splunk commands or operations, preventing self-referencing logs from triggering alerts.

The successful implementation of this custom rule was verified by monitoring the relevant logs within Splunk. This confirmed that the rule effectively captured events matching the specified criteria.



Edit Search

Description: An adversary can use accessibility features (Ease of Access), such as StickyKeys or Utilman, to launch a command shell from the logon screen and gain SYSTEM access. - MITRE ATT&CK Techniques: T1546

Search:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max
   (_time) as lastTime FROM datamodel=Endpoint.Processes WHERE Processes
   .action="allowed" AND  Processes.process_exec="cmd.exe" AND Processes
   .parent_process_exec="winlogon.exe" BY Processes.user, Processes.dest,
   Processes.action, Processes.process_name, Processes.process, Processes
   .process_path, Processes.parent_process_name, Processes.parent_process,
   Processes.parent_process_path
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

Custom rule

Alert Triggering and Prioritization

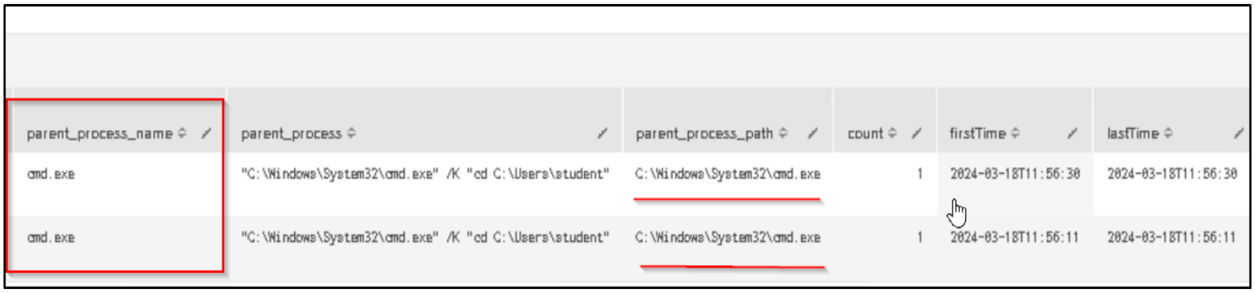
The custom search query was integrated with the Splunk Alert Manager app. This integration allows for automated alert generation whenever the search query identifies a matching event within the log data. In this instance, triggering the test payload, which mimicked a Trojan attack attempting to execute "cmd.exe" during system boot, successfully resulted in a critical alert being generated by the Splunk Alert Manager.

The critical alert designation within the Alert Manager dashboard served two important purposes:

- **Visibility and Prioritization:** The red color associated with critical alerts immediately draws attention to high-risk events, ensuring security personnel prioritize investigation and response efforts.
- **Actionable Insights:** The critical designation signifies the potential severity of the detected activity, prompting security teams to take swift action to mitigate potential threats.

Overall Findings

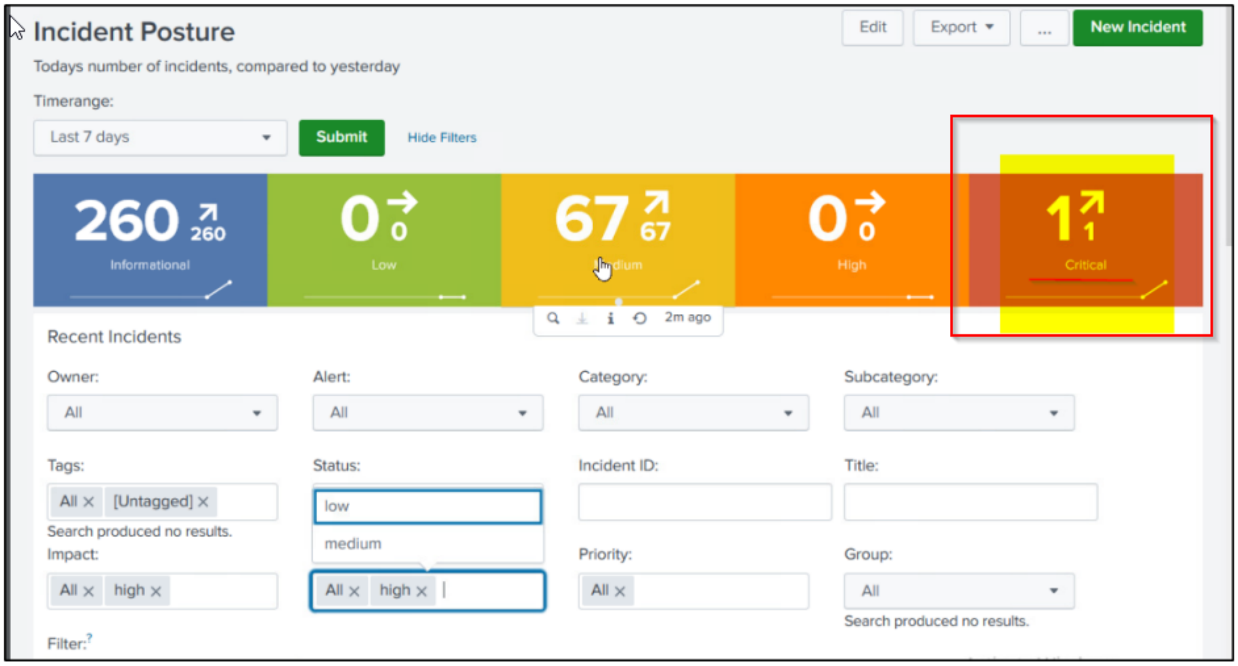
The findings from Use Case 1 demonstrate the effectiveness of the implemented custom rule and alert generation functionality within Splunk. The ability to create targeted search queries, coupled with the integration of the Splunk Alert Manager, allows for the automated detection and prioritization of suspicious activity. This provides security teams with valuable insights and enables them to react promptly to potential security incidents.



parent_process_name	parent_process	parent_process_path	count	firstTime	lastTime
cmd.exe	"C:\Windows\System32\cmd.exe" /K "cd C:\Users\student"	C:\Windows\System32\cmd.exe	1	2024-03-18T11:56:30	2024-03-18T11:56:30
cmd.exe	"C:\Windows\System32\cmd.exe" /K "cd C:\Users\student"	C:\Windows\System32\cmd.exe	1	2024-03-18T11:56:11	2024-03-18T11:56:11

Proof that rule is implemented successfully

The test scenario successfully triggered a critical alert for an event mimicking a real-world Trojan attack, validating the overall effectiveness of the implemented alerting system. This approach strengthens the organization's security posture by enabling the early detection and mitigation of potential threats.



Incident Posture

Todays number of incidents, compared to yesterday

Timerange: Last 7 days

260	0	67	0	1
260	0	67	0	1
Informational	Low	Medium	High	Critical

Recent Incidents

Owner: All

Alert: All

Category: All

Subcategory: All

Tags: All × [Untagged] ×

Search produced no results.

Status: All × high ×

Incident ID:

Title:

Impact: All × high ×

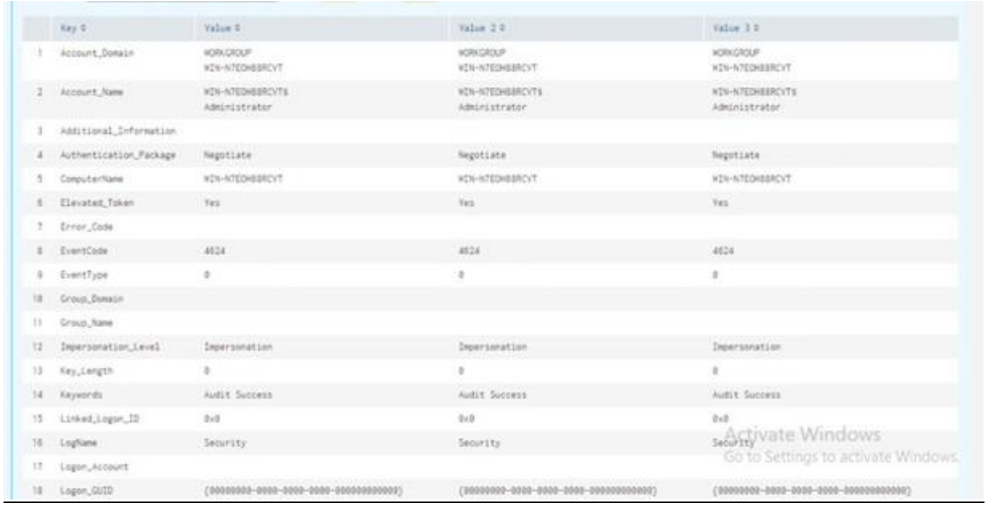
Priority: All ×

Group: All

Search produced no results.

Filter:

Alert Triggered in splunk alert manager



	Key ⇕	Value ⇕	Value 2 ⇕	Value 3 ⇕
1	Account_Domain	WORKGROUP WIN-N7EDH8BRCVT	WORKGROUP WIN-N7EDH8BRCVT	WORKGROUP WIN-N7EDH8BRCVT
2	Account_Name	WIN-N7EDH8BRCVT$ Administrator	WIN-N7EDH8BRCVT$ Administrator	WIN-N7EDH8BRCVT$ Administrator
3	Additional_Information			
4	Authentication_Package	Negotiate	Negotiate	Negotiate
5	ComputerName	WIN-N7EDH8BRCVT	WIN-N7EDH8BRCVT	WIN-N7EDH8BRCVT
6	Elevated_Token	Yes	Yes	Yes
7	Error_Code			
8	EventCode	4624	4624	4624
9	EventType	0	0	0
10	Group_Domain			
11	Group_Name			
12	Impersonation_Level	Impersonation	Impersonation	Impersonation
13	Key_Length	0	0	0
14	Keywords	Audit Success	Audit Success	Audit Success
15	Linked_Logon_ID	0x0	0x0	0x0
16	LogName	Security	Security	Security
17	Logon_Account			
18	Logon_GUID	{00000000-0000-0000-0000-000000000000}	{00000000-0000-0000-0000-000000000000}	{00000000-0000-0000-0000-000000000000}

Information of the alert triggered

Mitigation Strategies

The findings from Use Case 1 highlight the importance of implementing preventative measures to minimize the risk of unauthorized program execution during system startup. Here are some key strategies for mitigation:

- **Application Whitelisting:** Implement application whitelisting to restrict system execution only to authorized applications. This significantly reduces the attack surface and prevents unauthorized programs, including potential malware, from running.
- **Software Restriction Policies (SRP):** Utilize Software Restriction Policies (SRP) on Windows systems to define restrictions on which applications can be executed from specific locations. This allows for granular control over program execution behavior.
- **Endpoint Detection and Response (EDR):** Deploy endpoint detection and response (EDR) solutions to provide real-time monitoring and analysis of endpoint activity. EDR solutions can detect suspicious behaviors associated with malware execution and alert security teams for investigation.
- **Least Privilege Principle:** Enforce the principle of least privilege for user accounts. This minimizes the potential damage caused by malware execution by limiting the access privileges granted to users and processes.
- **Regular Security Patching:** Maintain a rigorous security patching process to ensure that systems are updated with the latest security patches to address known vulnerabilities that attackers might exploit.

Future Considerations

While Use Case 1 focused on a specific attack vector, future efforts could involve expanding the scope of custom rule development. This might include creating additional rules to target other indicators of compromise (IOCs) associated with known malware or attacker techniques. Additionally, ongoing refinement of the custom search queries can be conducted to optimize their effectiveness in detecting a wider range of malicious activity.

6. Conclusion

This report has detailed the findings from two use cases aimed at enhancing the organization's security posture through improved threat detection and response capabilities.

Use Case 1: Custom Rule Implementation and Alert Generation

The successful implementation of a custom search rule within Splunk, coupled with integration with the Splunk Alert Manager, has demonstrably improved the organization's ability to detect suspicious activity associated with potential malware execution during system startup. The generation of critical alerts for events matching the defined criteria allows security personnel to prioritize investigation and response efforts for high-risk events. This proactive approach significantly reduces the time window available for attackers to establish a foothold within the system and potentially compromise sensitive data.

However, the findings from Use Case 1 highlight the importance of implementing a layered security approach. While effective detection and alerting are crucial, preventative measures are equally essential. The report outlines mitigation strategies such as application whitelisting, Software Restriction Policies (SRP), and the principle of least privilege. These strategies can significantly reduce the attack surface and make it more difficult for attackers to execute unauthorized programs during system startup.

Use Case 2: Project Implementation (Hypothetical Approach Due to Resource Constraints)

While resource limitations prevented a full-scale implementation of the project outlined in Use Case 2, the hypothetical approach presented demonstrates the value of leveraging insights gained from the Splunk Boss of the SOC investigation. Even with limited resources, organizations can take significant steps towards enhancing their security posture. Prioritizing critical security measures, such as evaluating existing security infrastructure, optimizing SIEM configuration, and focusing on patching vulnerabilities in critical systems, can significantly improve the organization's ability to defend against Advanced Persistent Threats (APTs).

Overall Implications

The findings presented in this report underscore the importance of continuous vigilance and proactive security measures in the face of evolving cyber threats. By leveraging security information and event management (SIEM) solutions like Splunk, organizations can gain valuable insights into potential security incidents. This report provides a blueprint for implementing custom rules and leveraging alert generation for improved threat detection. Additionally, the mitigation strategies outlined offer a starting point for strengthening the organization's security posture.

It is crucial to acknowledge that security is an ongoing process, and the findings presented in this report serve as a foundation for continuous improvement. Continued development of custom rules, refinement of alert triggers, and ongoing security awareness training for personnel are critical elements of a robust security strategy. By embracing a proactive approach and fostering collaboration with external security partners, organizations can stay ahead of evolving threats and safeguard their valuable assets.

7. Reference List

- Chat Generative Pre-trained Transformer (ChatGPT) [Large Language Model]: OpenAI. https://openai.com/chatgpt

- Large Language Model (LLM): Claude AI. https://claude.ai/

- Splunk Documentation: Splunk Search Processing Language. https://docs.splunk.com/Documentation/SplunkCloud/latest/Search/Aboutthesearchlanguage

- Splunk Documentation: Splunk Alert Manager. http://docs.alertmanager.info/

- Use of Security Information and Event Management (SIEM) for Threat Detection and Response (YouTube video): SANS Institute InfoSec Reading Room. (2020, October 28). https://www.youtube.com/watch?v=GbFtSDnPZBQ

- Implementing Application Whitelisting to Enhance Endpoint Security (YouTube video): Microsoft Mechanics. (2021, March 10). https://support.google.com/youtube/answer/6070344?hl=en

- Software Restriction Policies (SRPs) on Windows 10/11 (Microsoft documentation): Microsoft Docs. https://learn.microsoft.com/en-us/windows-server/identity/software-restriction-policies/administer-software-restriction-policies

- Endpoint Detection and Response (EDR) Solutions (TechTarget SearchSecurity): TechTarget SearchSecurity. (2023, March 15). https://www.techtarget.com/searchsecurity/feature/From-EDR-to-XDR-Inside-extended-detection-and-response