Sutrefia Security Policy Compliance Dashboard Proposal

Prepared By : Bihanga Rathnayaka
Date : 2025.06.02

Contents

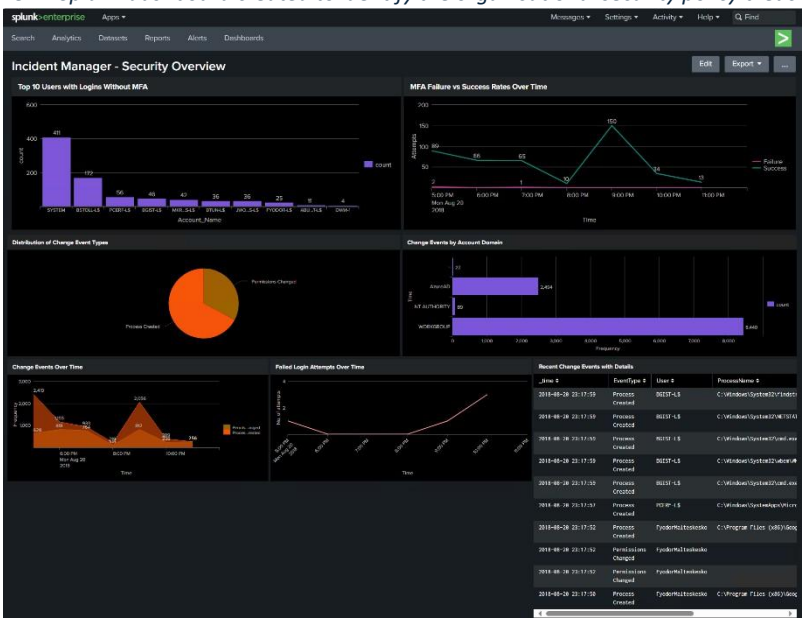
1. Introduction

Sutrefia, as a mid-to-large financial service firm, is in a very sensitive cyber environment requiring high security controls. Therefore, Sutrefia maintains strict adherence to security policies like Access Control & Multi-Factor Authentication (MFA) and Change Management.

This report is a sample Splunk security dashboard that utilizes the BOTSv3 data set to monitor compliance with these two policies. The dashboard is designed for higher management to easily recognize possible policy infractions with visual graphics and key security indicators (ASD, 2023; Chuvakin et al., 2012).

2. Dashboard Overview

Figure 1 - Splunk dashboard created to identify the organisational security policy breaches



Note: Screenshot captured from Splunk dashboard

The proposed security dashboard leverages the functionality of Splunk's Security Information and Event Management (SIEM) system to enable real-time monitoring and assessment of Sutrefia's information technology environment. SIEM-classified tools like Splunk integrate Security Information Management (SIM) with Security Event Management (SEM), thus enabling continuous threat monitoring, incident management, and comprehensive visibility taking place within networks and applications.

This dashboard consolidates various forms of log and event sources, such as user authentication history, activity by privileged accounts, and occurrences of system changes. This consolidation enables the swift identification of anomalies that may present security policy violations. The design of the dashboard adheres to accepted IT security frameworks and established best

practices like the NIST Cybersecurity Framework that emphasizes the critical security functions of identification, protection, detection, response, and recovery.

Specifically, the above dashboard offers Authentication and Access Control Insights such as Visualizations of user logins without multi-factor authentication, geographic login distributions, login failures over time, and privileged account usage. These helps enforce strong controls on access, blocking threats due to compromised credentials or insider attacks.

Also, Change Management Monitoring Dashboards show categories of system changes, responsible domains for changes, time patterns, detailed event logs, and software installation histories. These enable effective governance over changes in the IT infrastructure, reducing risks from unauthorized or unmonitored changes.

The combination of these components represents the tiered defense approach espoused in security management, coupling preventive, detective, and responsive countermeasures to protect the assets of the organization. The dashboard allows non-technical management to quickly comprehend the state of the organization's security and supports proactive counteractions against evolving threats or infractions of policy.

3. Policy 1 - Access Control & MFA Policy Monitoring

Policy Summary

This policy requires all access to systems to use multi-factor authentication (MFA), including internal systems, to prevent unauthorized access via compromised credentials. It also requires strict monitoring of privileged account activities (ASD, 2023; Ibrokhimov et al., 2019).

Key Indicators and Panel Selection

In order to measure adherence to the Access Control and Multi-Factor Authentication (MFA) policy, the dashboard calls out key indicators that include reports of the following incidents.

1. User logins without MFA authentication
2. Suspicious or geographically anomalous login locations
3. Elevated failed login attempts suggesting attack attempts
4. Privileged account activity that might be unauthorized
5. Execution of privileged commands (via sudo) without oversight

These indicators collectively detect potential security threats, including credential compromise, insider threat, or breakdowns in appropriately applying authentication controls. Panels displaying these indicators allow management to quickly identify accounts or patterns of risk, enabling targeted remediation and access control tightening (Nelson et al., 2025).

1.1 Top 10 User Logins Without MFA

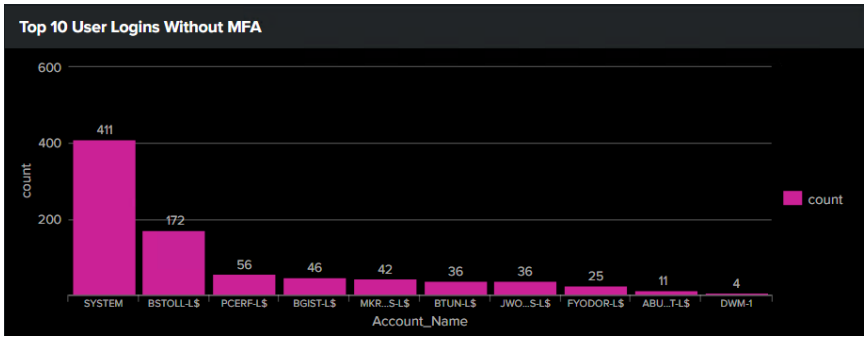
Purpose:
This dashboard provides the top ten users who have the highest number of successful logon attempts where MFA was not enforced. This shows potential anomalies or breakdowns in the enforcement of MFA, which is essential in blocking unauthorized access.

Rationale:
Management requires real-time insights into which accounts could be bypassing the MFA requirement. Elevated numbers could point to incorrectly configured systems or users circumventing security measures, a direct and obvious risk to system integrity and data confidentiality (ASD, 2023).

SPL Query:

```
index=botsv3 sourcetype=WinEventLog:Security EventCode=4624
| eval MFA=if(searchmatch("MFA"), "Yes", "No")
| search MFA="No"
| stats count by Account_Name
| sort - count
| head 10
```

Figure 2 - Top 10 User Logins Without MFA Panel Screenshot



Note: Screenshot captured from Splunk dashboard

1.2 Login Locations by IP (Top 20 Countries)

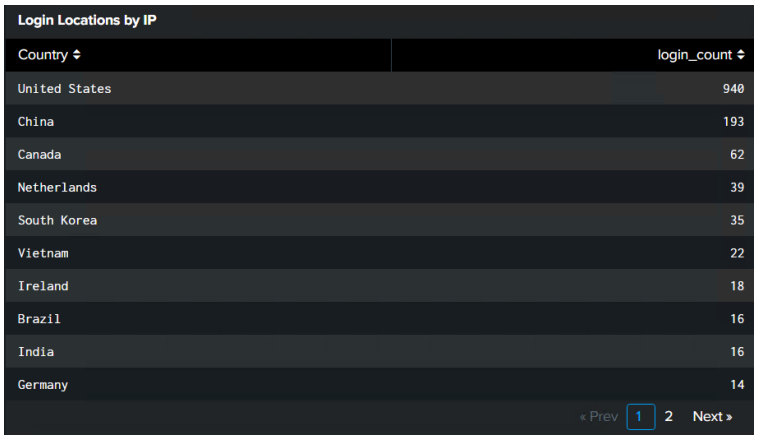
Purpose:
This geographical mapping consolidates login activity by nation and displays the top 20 nations from which system access is originating. It detects anomalous geographic login activity that could be a sign of compromised credentials or unauthorized remote access.

Rationale:
Banks typically limit or track access by familiar geographic user groups. Unanticipated logins from atypical or high-risk nations can be an indicator of account takeover or malicious insider behavior. This panel allows management to launch investigations or alter access policy as necessary (ASD, 2023).

SPL Query:

```
index=botsv3 sourcetype=stream:ip
| iplocation src_ip
| stats count as login_count by Country
| where Country!="" AND login_count > 0
| sort -login_count
| head 20
```

Figure 3 - Login Locations by IP Panel Screenshot



Note: Screenshot captured from Splunk dashboard

1.3 Failed Logins Over Time (Hourly)

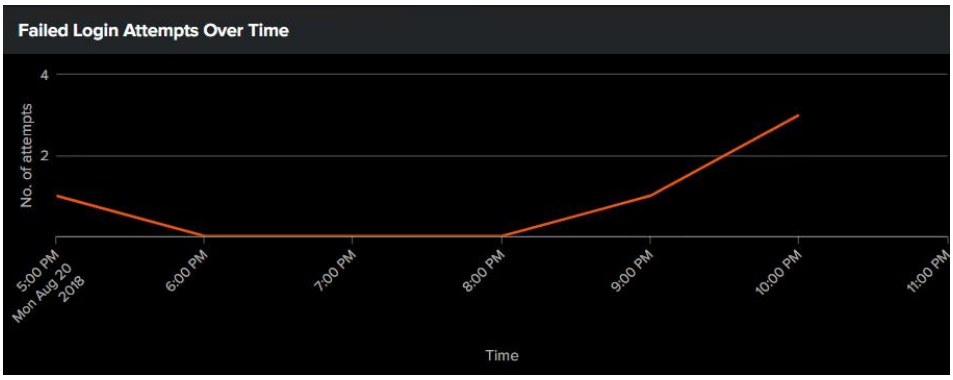
Purpose:
This is a time-series chart of failed login attempts per user per hour. It shows trends in failed logins that may indicate brute force attacks, credential stuffing, or user access problems.

Rationale:
Spiking or repeated failed login attempts are a common indicator of malicious use. Management can use monitoring of this panel to see if such activities are occurring frequently or against specific users, so that early response to incidents and risk mitigation can be achieved (Nelson et al., 2025).

SPL Query:

```
index=botsv3 sourcetype=linux_secure OR sourcetype=auth
| search "failed" OR "failure" OR "authentication failure"
| timechart span=1h count by user
```

Figure 4 - Failed Logins Over Time Panel Screenshot



Note: Screenshot captured from Splunk dashboard

1.4 Privileged Account Logins Over Time

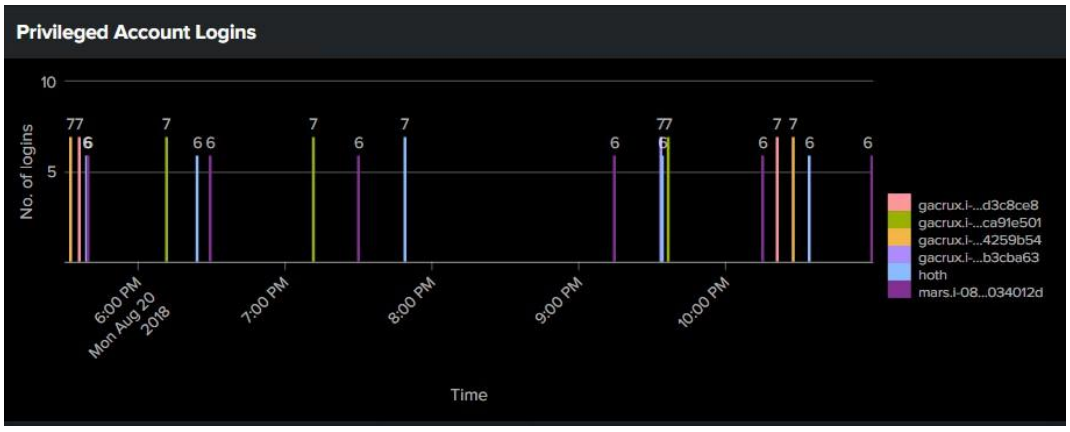
Purpose:
This chart displays the number of login events over time for privileged users, i.e., `root` and `admin` accounts, per host. It offers privileged account activity monitoring.

Rationale:
Privileged accounts represent high-risk targets. Unauthorized or unusual access patterns could signal insider threats or compromised accounts. Monitoring this panel helps management ensure privileged access adheres to security policies and investigate anomalies quickly (ASD, 2023).

SPL Query:

```
index=botsv3 (user=root OR user=admin)
| timechart count by host
```

Figure 5 - Privileged Account Logins Over Time Panel Screenshot



Note: Screenshot captured from Splunk dashboard

1.5 Privileged Commands Executed (via sudo)

Purpose:
This panel displays the number of privileged commands run through `sudo` by host and user, sorted by frequency. It monitors significant command runs that need authorization.

Rationale:
`sudo` usage increases privileges and can modify system settings or disclose sensitive information. Unauthorized or unintended use is a critical policy violation. This panel allows management to track privileged command usage, account for users, and catch misuse in time (Nelson et al., 2025).

SPL Query:

```
index=botsv3 sourcetype=linux_secure "sudo"
| stats count by USER, host, COMMAND
| sort -count
```

Figure 6 - Privileged Commands Executed Panel Screenshot

Privileged Commands Executed (via sudo)

USER	host	COMMAND	count
root	gacrux.i-06fea586f3d3c8ce8	/opt/splunkforwarder/bin/splunk	1
root	gacrux.i-06fea586f3d3c8ce8	/usr/bin/tee	1
root	gacrux.i-09cbc261e84259b54	/opt/splunkforwarder/bin/splunk	1
root	gacrux.i-09cbc261e84259b54	/usr/bin/tee	1
root	gacrux.i-0cc93bade2b3cba63	/opt/splunkforwarder/bin/splunk	1
root	gacrux.i-0cc93bade2b3cba63	/usr/bin/tee	1
root	mars.i-08e52f8b5a034012d	/usr/bin/pip	1

Note: Screenshot captured from Splunk dashboard

3. Policy 2 - Change Management Policy Monitoring

Policy Summary

Any device or network changes, including new devices, software installations, or permission changes, need to be approved by IT or Security Operations and documented in order to maintain system integrity and security (ASD, 2023; Ramluckan et al., 2020).

Key Indicators and Panel Selection

For Change Management policy, the most significant measures are the frequency and nature of system changes, such as process creation and permission modifications, initiating domains, change event timing patterns, complete histories of recent changes, and software installation activity. Monitoring these metrics enables the detection of unapproved or unmonitored alterations to the IT environment that can destabilize systems and compromise security. The

panels chosen give the management the extent and type of changes so that they can ensure all changes are authorized, recorded, and align with organizational policies (Nelson et al., 2025; Scarfone & Mell, 2007).

2.1 Change Event Type Distribution

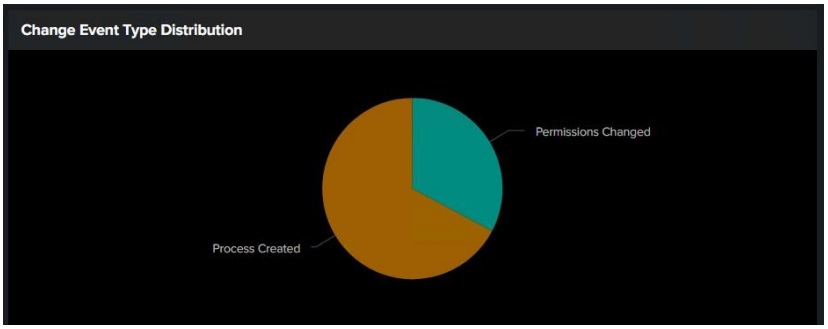
Purpose:
The bar chart displays occurrence allocation related to changes, distinguishing between process initiation and permissions modifications, thus providing an insight into the characteristics and scope of activities related to modifications.

Rationale:
A rise or pattern of irregularity in change activity could indicate illicit behavior or policy breaches. This dashboard can be used by the management team to effectively assess overall change activity and compliance adherence (ASD, 2023).

SPL Query:

```
index=botsv3 sourcetype="WinEventLog:Security" (EventCode=4688 OR
EventCode=4670)
| stats count by EventCode
| eval EventCode=case(
    EventCode=="4688", "Process Created",
    EventCode=="4670", "Permissions Changed",
    true(), tostring(EventCode))
| rename count as "Total Events", EventCode as "Change Event Type"
```

Figure 7 - Change Event Type Distribution Panel Screenshot



Note: Screenshot captured from Splunk dashboard

2.2 Change Events by Account Domain

Purpose:
This panel aggregates change events by account domains to determine which organizational domains or units are causing these changes.

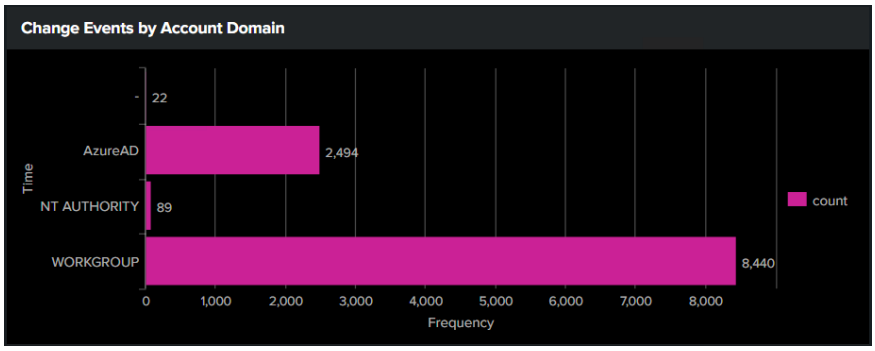
Rationale:
Changes from non-sanctioned or unintended sources could indicate malicious behavior or

organizational dangers. The committee helps management ensure that modifications originate from authorized arenas only (Nelson et al., 2025).

SPL Query:

```
index=botsv3 sourcetype="WinEventLog:Security" (EventCode=4688 OR
EventCode=4670)
| rex field=_raw "Account Domain:\s+(?<AccountDomain>[^
]+)"
| stats count by AccountDomain
```

Figure 8 - Change Events by Account Domain Panel Screenshot



Note: Screenshot captured from Splunk dashboard

2.3 Change Events Over Time (Hourly)

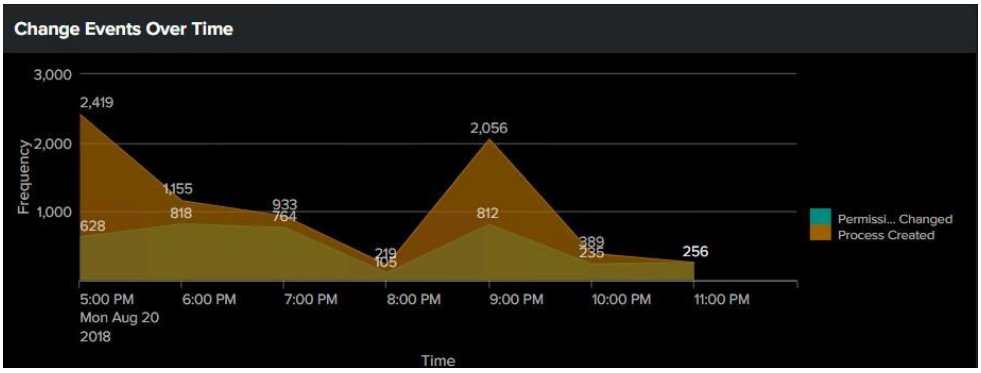
Purpose:
Provides hour-by-hour tallies of modification events by type of event, making it possible to identify anomalous spikes or temporal patterns.

Rationale:
Management can detect irregular change activity timing, possibly indicating automated attacks or insider actions outside normal business hours (ASD, 2023).

SPL Query:

```
index=botsv3 sourcetype="WinEventLog:Security" (EventCode=4688 OR
EventCode=4670)
| eval EventType=case(
    EventCode=="4688", "Process Created",
    EventCode=="4670", "Permissions Changed",
    true(), "Other" )
| timechart span=1h count by EventType
```

Figure 9 - Change Events Over Time Panel Screenshot



Note: Screenshot captured from Splunk dashboard

2.4 Recent Change Events with Details

Purpose:
The above table outlines recent change events, including timestamps, user IDs, event types, and related processes, thus making it feasible to analyze recent alterations holistically.

Rationale:
Management is competent to monitor and check regularly recent alterations to ensure their approval and proper implementation, hence enabling effective control (Nelson et al., 2025).

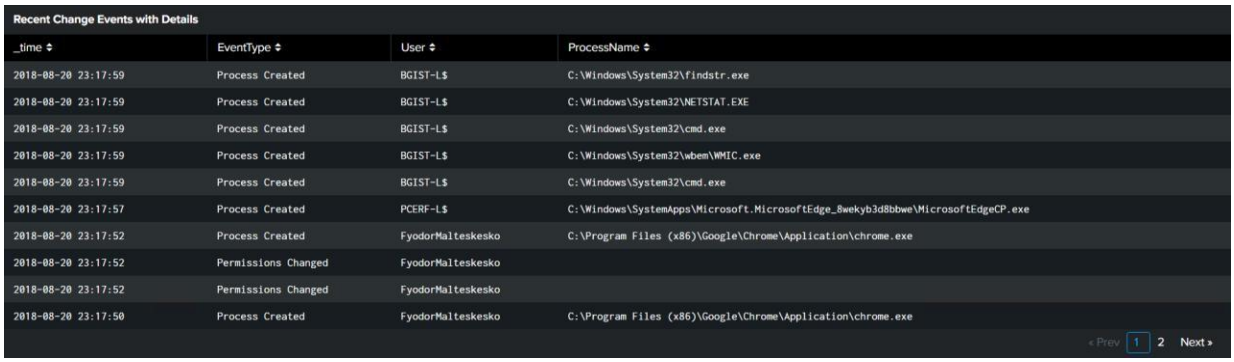
SPL Query:

```
index=botsv3 sourcetype="WinEventLog:Security" (EventCode=4688 OR
EventCode=4670)
| eval EventType=case(
    EventCode=="4688", "Process Created",
    EventCode=="4670", "Permissions Changed",
    true(), "Other"  )
| where EventType!="Other"
| rex field=_raw "Account Name:\s+(?<User>[^

]+)"
| rex field=_raw "New Process Name:\s+(?<ProcessName>[^

]+)"
| table _time EventType User ProcessName
| sort -_time
| head 20
```

Figure 10 - Recent Change Events with Details Panel Screenshot



Recent Change Events with Details

_time	EventType	User	ProcessName
2018-08-20 23:17:59	Process Created	BGIST-L$	C:\Windows\System32\findstr.exe
2018-08-20 23:17:59	Process Created	BGIST-L$	C:\Windows\System32\NETSTAT.EXE
2018-08-20 23:17:59	Process Created	BGIST-L$	C:\Windows\System32\cmd.exe
2018-08-20 23:17:59	Process Created	BGIST-L$	C:\Windows\System32\wbem\WMIC.exe
2018-08-20 23:17:59	Process Created	BGIST-L$	C:\Windows\System32\cmd.exe
2018-08-20 23:17:57	Process Created	PCERF-L$	C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdgeCP.exe
2018-08-20 23:17:52	Process Created	FyodorMalteskesko	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
2018-08-20 23:17:52	Permissions Changed	FyodorMalteskesko	
2018-08-20 23:17:52	Permissions Changed	FyodorMalteskesko	
2018-08-20 23:17:50	Process Created	FyodorMalteskesko	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

‹ Prev 1 2 Next ›

Note: Screenshot captured from Splunk dashboard

2.5 Software Installation Logs

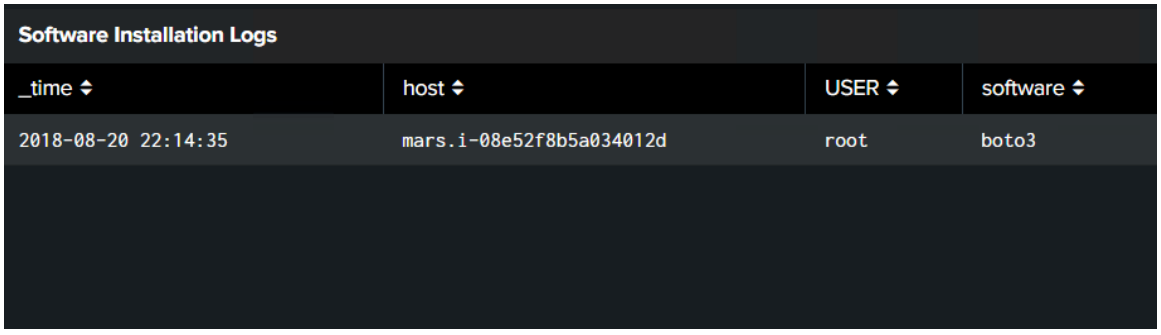
Purpose:
Lists recent software installation events detected on Linux systems, detailing time, host, user, and software name.

Rationale:
Unapproved installations of software are critical security risks and could indicate breaches of applicable compliance regulations. This panel allows management to ensure all installations of software have been authorized through proper change management processes (ASD, 2023).

SPL Query:

```
index=botsv3 sourcetype=linux_secure OR sourcetype=linux_audit
| search "install"
| rex field=_raw "pip\s+install\s+(?<software>[^\s]+)"
| table _time host USER software
| sort -_time
```

Figure 11 - Software Installation Logs Panel Screenshot



Software Installation Logs

_time	host	USER	software
2018-08-20 22:14:35	mars.i-08e52f8b5a034012d	root	boto3

Note 1 - Note: Screenshot captured from Splunk dashboard

4. Final Argument for Dashboard Effectiveness

The dashboard gives a clear and understandable overview of two critical policies that are central to Sutrefia's cybersecurity framework. The transformation of complex logs of events into graphical representations and structured statistical information gives management

- Direct recognition of policy compliance and examples of non-compliances without expecting technical competence.

The identified findings focused primarily on the most critical areas, such as bypassing multifactor authentication, privilege access vulnerabilities, and unauthorized changes.

- Temporal and contextual understanding of security events to differentiate between normal and suspicious activity.

Actionable information enables quick decision-making, accurate questioning, and improved implementation of security measures.

In short, such a dashboard allows management of Sutrefia to maintain a strong defensive posture, increase funds invested in security activities, and effectively minimize vulnerabilities to cyberattacks (ASD, 2023; Chuvakin et al., 2012; Solms & Niekerk, 2013).

References

I acknowledge the use of the ChatGPT free version and the Grammarly free version to correct the grammar of the report.

ASD. (2023). *Information security manual (ISM)*. Australian Cyber Security Centre. https://www.cyber.gov.au/acsc/view-all-content/ism

Chuvakin, A., Schmidt, K., & Phillips, C. (2012). *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*. https://www.researchgate.net/publication/294592364_Logging_and_Log_Management_The_Authoritative_Guide_to_Understanding_the_Concepts_Surrounding_Logging_and_Log_Management

Ibrokhimov, S., Hui, K. L., Al-Absi, A. A., lee, h. j., & Sain, M. (2019). Multi-Factor Authentication in Cyber Physical System: A State of Art Survey. *2019 21st International Conference on Advanced Communication Technology (ICACT)*, 279-284. https://doi.org/https://doi.org/10.23919/ICACT.2019.8701960

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management *NIST Special Publication 800* https://doi.org/https://doi.org/10.6028/NIST.SP.800-61r3

Ramluckan, T., Niekerk, B. v., & Martins, I. (2020). A Change Management Perspective to Implementing a Cyber Security Culture. *19th European Conference on Cyber Warfare and Security*. https://www.researchgate.net/publication/342501668_A_Change_Management_Perspective_to_Implementing_a_Cyber_Security_Culture

Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) *NIST Special Publication 800-94* https://doi.org/https://doi.org/10.6028/NIST.SP.800-94

Solms, R. v., & Niekerk, J. v. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/https://doi.org/10.1016/j.cose.2013.04.004