CSG3309 – IT Security Management

Policy Compliance Dashboard Proposal

Student Name: Najath Najeem

Student Number: [redacted]

Campus: Sri Lanka

Lecturer: Mr. Kailanathan Mayuran

Unit Coordinator: Dr. Leah Shanley

Due Date: 30/05/2025

Contents

1. Introduction

Since Sutrefia works in a sensitive financial services field, it is required to adopt good measures to keep customers' and the company's information secure. Since cyber threats are spreading and attacks are becoming more complex, organizations must carefully observe their security policies related to access control and user accounts (*Verizon Business*, 2023).

This report shows how the Splunk dashboard was planned, created and deployed to check Sutrefia's Access Control & Multi Factor Authentication (MFA) policy compliance. Since this dashboard uses the BOTSv3 dataset, which is developed to mimic real world cybersecurity events, it can display important findings about login attempts, the success of authentication and how MFA is enforced. Using the dashboard, security teams and operations can easily spot when policies are not being followed and when someone tries to access systems without permission. This feature is necessary to keep systems secure and to follow the rules set by regulators.

The rest of the report explains the focus of the security policy, the design of the dashboard, each panel and their SPL queries and the main advantage this tool brings to Sutrefia's cybersecurity.

2. Security Policy Selected for Monitoring

Access Control & Multi-Factor Authentication (MFA)

The Access Control & MFA policy requires all systems (internal or external) to ask users to verify their identities using both MFA (something known and something possessed). MFA works as an important barrier, making credential theft and phishing attacks much less likely.

To ensure compliance login activities need to be continuously monitored for,

- Successful logins when MFA not enforced.
- Failed login attempts (which may indicate brute-force attacks).
- Trends in MFA adoption and identification of accounts bypassing MFA.

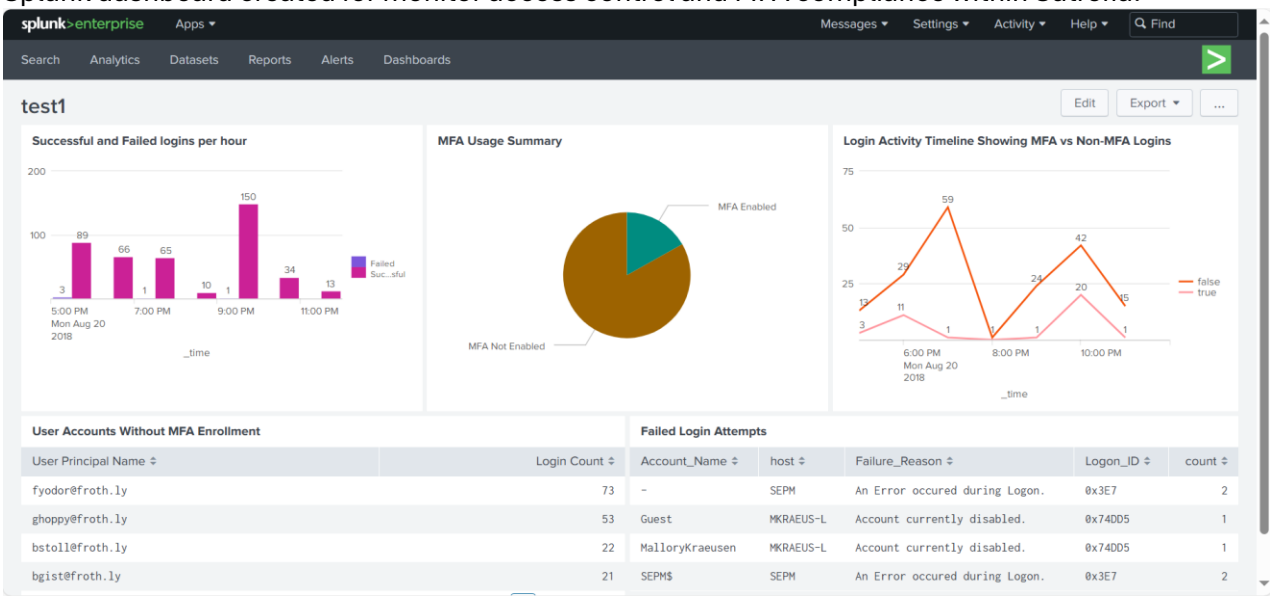
Tracking these metrics helps to ensure that the company meets its security goals and rules set by the industry. Regularly monitoring these login events, possible security breaches can be spotted early and dealt very quickly. This approach helps secure the network by making it less prone to unauthorized entry and MFA not being used (NIST, 2018).

3. Splunk Dashboard

The dashboard is designed to help Sutrefia's security management to see if Access Control & Multi-Factor Authentication (MFA) policy guidelines are followed in a quick and efficient manner.

Figure 1

Splunk dashboard created for monitor access control and MFA compliance within Sutrefia.



Note: Screenshot captured from Splunk Enterprise, used to illustrate dashboard panels monitoring security policy compliance.

All the panels on the dashboard combine to show a comprehensive picture of Access Control and Multi-Factor Authentication (MFA) policy compliance in Sutrefia. By monitoring both successful and failed login attempts, the dashboard can spot early warning signs of unauthorized access and possible weak MFA checks (Meyer et al., 2023; Wiefling et al., 2022).

The use of time-based panels allows detecting sudden changes or unusual behaviors that might suggest an active attack or when a business is not following policies. The MFA usage summary provides a broad overview of compliance, helping to measure how effective MFA is in the organization and the detailed account panel highlights users who may not be using MFA.

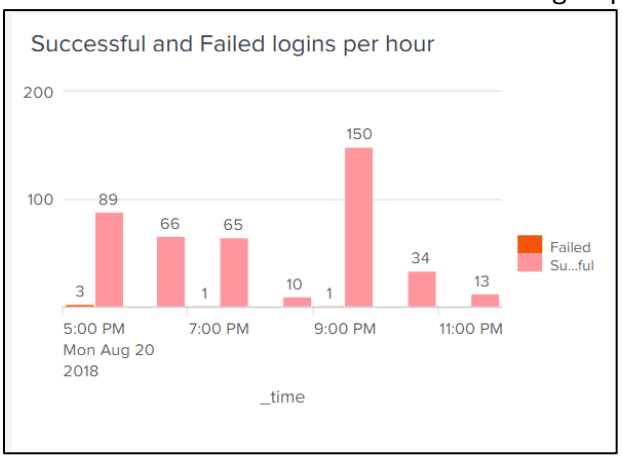
When combined, the panels work as a strong tool for monitoring that helps Sutrefia manage its security proactively by pointing out weaknesses, helping plan fixes and ensuring continued compliance with a key cybersecurity policy for the company's financial systems.

4. Panel details

4.1 Successful and Failed Logins Per Hour

This panel visualizes how many successful and failed logins attempts help in monitoring authentication activity. Tracking failed login attempts protects the Access Control & MFA policy by spotting suspicious actions or wrong configurations (*Verizon Business*, 2023).

Figure 2
Screenshot of the panel which shows Successful and Failed Logins per Hour (Bar chart)



By comparing failed and successful logins hourly, security teams can notice increases in failed logins, indicative of potential brute force or credential stuffing attacks. This insight help prioritize investigations and address these security threats immediately.

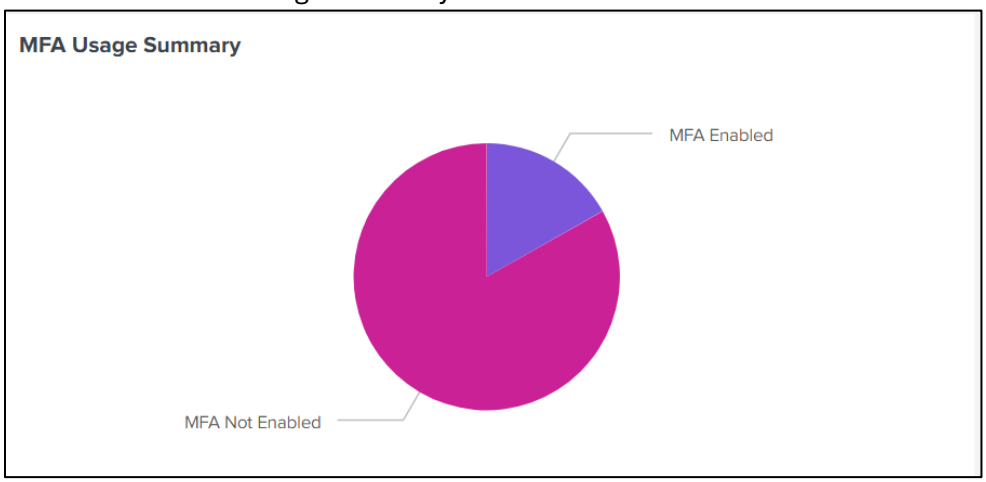
The SPL query searches through Windows event logs for events that indicate a successful (4624) or unsuccessful (4625) login attempt. It labels every event as “Successful” or “Failed” and counts up the totals by the hour. With this time-based aggregation, it becomes clear how login activity has changed which lets analysts find suspicious patterns and measure access control.

Figure 3
Splunk query for displaying successful and failed login counts per hour using timechart and eval to classify status.

```
index=botsv3 sourcetype=wineventlog* (EventCode=4625 OR EventCode=4624)
| eval status=if(EventCode=4625, "Failed", "Successful")
| timechart span=1h count by status
```

4.2 MFA Usage Summary

Figure 4
Screenshot of MFA Usage Summary Pie chart



The panel clearly displays the proportion of successful logins that involved Multi-Factor Authentication (MFA) by the pie chart. It lets management know how many logins use MFA and how many do not, so the organization's Access Control & MFA security policy is clear. Through a visual comparison, the panel points out areas where MFA is not used, so administrators can quickly find security holes and fix them by enforcing MFA. This clear view helps spot where MFA is still lacking among applications or users which is essential for reducing the dangers of unauthorized access (Bonneau et al., 2012). This panel turns detailed authentication data into understandable information for even non-technical stakeholders.

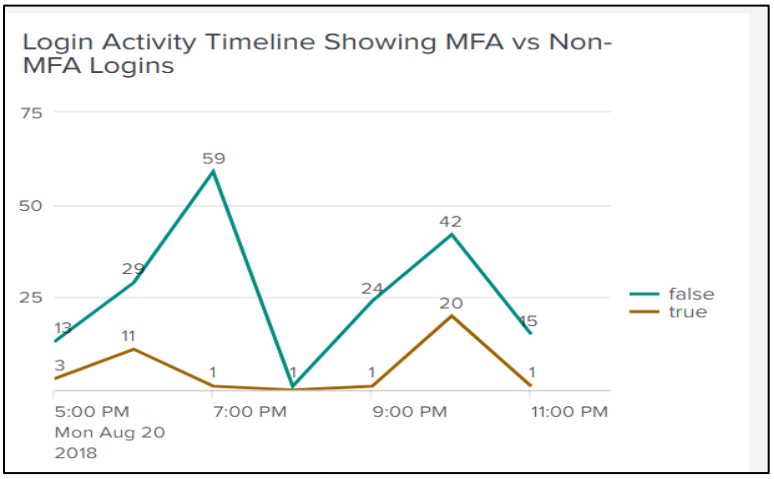
Figure 5
Splunk query for displaying MFA Usage Summary.

```
index=botsv3 sourcetype= "ms:aad:signin"
| eval MFA_Status=if(mfaRequired=="true", "MFA Enabled", "MFA Not Enabled")
| stats count by MFA_Status
| rename MFA_Status as "Multi Factor Authentication Status"
```

This SPL query examines the sign-in logs ("ms:aad:sihnin") to check if MFA was needed for every successful login. Next, it adds up the login counts separated by MFA status ("Enabled" or "Not Enabled") and then it adjusts the name of the field to reflect the Multi-Factor Authentication status, so the graph becomes easier to read and understand. The simplicity of this query enables easy customization to include more filters or dimensions as organizational needs grow.

4.3 Login Activity Timeline Showing MFA vs Non-MFA Logins

Figure 6
Screenshot of time-series chart showing Login Activity Timeline Showing MFA vs Non-MFA Logins



This panel graphically represents the login events, showing which required MFA and which did not. It contributes to the Access Control & MFA policy by displaying how many successful logins occurred and when, depending on whether MFA was used or not. By using a line graph, one can clearly see how login activity changes over time and find situations where too many logins were managed without MFA which may suggest suspicious behavior. Reviewing the difference between MFA-enabled logins and non-MFA logins hourly allows security teams and management to monitor how well MFA is implemented in the organization's systems (Meyer et al., 2023). This approach can reveal when MFA is not being used enough, so important security issues can be tackled more directly. In general, this panel helps supervise MFA policies and can verify compliance in real time, decreasing the probability of malicious activity and breaches.

The SPL query (Figure 7) searches the BOTSv3 dataset for Azure AD sign-in events ("ms:aad:sihnin") and then uses "timechart" to show how many logins took place every hour. It separates logins by the "mfaRequired" field, showing which were logged in with MFA and which were not. By doing this, we can see the way MFA has been enforced and easily spots any unexpected changes from the security policy.

Figure 7
Splunk query for Login Activity Timeline Showing MFA vs Non-MFA Logins

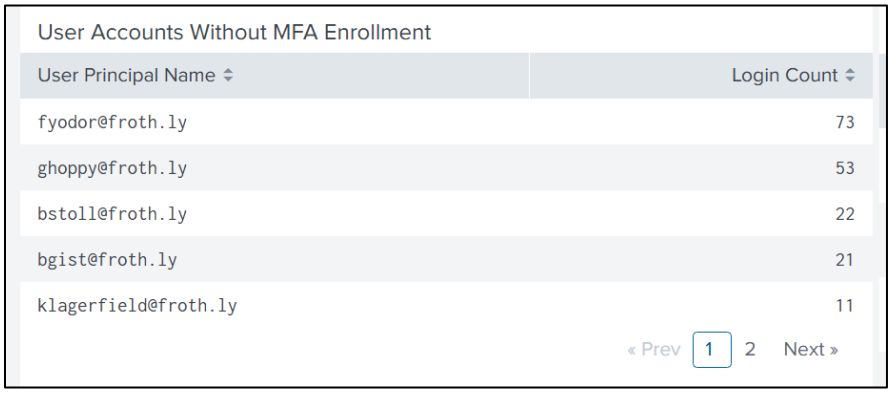
```
index=botsv3 sourcetype="ms:aad:signin"
| timechart span=1h count by mfaRequired
```

4.4 User Accounts Without MFA Enrollment

The panel points out user accounts that have logged in without Multi-Factor Authentication (MFA) which is a significant security policy violation according to the organization's Access Control & MFA policy. Adding this panel helps make it easy to check accounts that could be at risk because MFA is not required. Because MFA is not used, these accounts may be compromised through weak or stolen passwords which make data breaches or threats from within more likely (Bonneau et al., 2012).

Since this panel includes the "User Principal Name" and "Login Count," security managers can quickly tell which accounts are used regularly without MFA and address these issues first. By prioritizing, it is possible to secure high-risk users first, which improves the security level for the entire organization. The panel aids compliance auditing by highlighting non-compliant accounts and keeping track of logins which helps spot trends. In general, the panel helps with risk management by catching MFA policy violations early and helping identify the most serious risks.

Figure 8
Screenshot User Accounts without MFA table



The SPL query filters BOTSv3 events for Azure AD sign-ins ("ms:aad:signin") where "mfaRequired = False". It uses "stats count" to group login counts by "userPrincipalName", sorts the results by highest frequency first and changes the field names for clarity. It lists users who have successfully logged in most times without using MFA.

Figure 9
SPL query for User Accounts without MFA

```
index=botsv3 sourcetype="ms:aad:signin" mfaRequired=false
| stats count as "Login Count" by userPrincipalName
| sort -"Login Count"
| rename userPrincipalName as "User Principal Name"
| table "User Principal Name" "Login Count"
```

4.5 Failed Login Attempts Overview

The Failed Login Attempts panel is necessary to see and stop unauthorized attempts to access the network. With this panel, you can spot user accounts and hosts that fail to authenticate which could signal problems like brute force attacks, somebody trying to log in to disabled accounts or configuration errors (NIST, 2018).

Figure 10
Screenshot of Failed Login Attempts Table

Failed Login Attempts

Account_Name	host	Failure_Reason	Logon_ID	count
-	SEPM	An Error occured during Logon.	0x3E7	2
Guest	MKRAEUS-L	Account currently disabled.	0x74DD5	1
MalloryKraeusen	MKRAEUS-L	Account currently disabled.	0x74DD5	1
SEPM$	SEPM	An Error occured during Logon.	0x3E7	2

The panel shows the reasons for login failures and relates them to the unique account, host and logon IDs. Because of this, security teams can handle suspicious activity faster, make needed changes and upgrade access control policies. It also supports compliance with the organization's Access Control & MFA policy by noticing any unusual attempts to log in.

Figure 11
SPL query for Failed Login Attempts

```
index=botsv3 sourcetype="wineventlog:security" EventCode=4625
| rex field=_raw "Failure Reason:\s*(?P<Failure_Reason>.+?)\s*Status"
| rex field=_raw "Logon ID:\s*(?P<Logon_ID>\S+)"
| stats count by Account_Name, host, Failure_Reason, Logon_ID
```

This SPL query search in the Windows security logs (wineventlog:security) for EventCode 4625 which means a failed login attempt. It makes use of rex commands to find out failure reasons and the IDs of people who logged in from the raw events. The stats group the total number of authentication failures by account, host, reason and logon ID, helping with close observation of authentication errors for security purposes. This helps security teams quickly identify and respond to suspicious login activities.

5. Final Argument and Conclusion

The Splunk dashboard developed for Sutrefia is a key and efficient tool for overseeing the company's compliance with its Access Control and MFA security policies. By bringing together visual representations of login attempts, MFA usage rates, bypasses and suspicious activities, the dashboard combines important indicators of both security and compliance. With this approach, security teams and management can detect policy violations and suspicious activities in real time and address them before they become major breaches. With the help of the designed panels and SPL queries, all users, regardless of their technical knowledge, can easily assess and ensure that the organization's security posture continuously evaluated and strengthened (NIST,2018).

The rationale for selecting these panels is that they align with the main requirements for good access control, ensuring MFA is set for all users, spotting attempts to access data without permission and regularly checking risky user accounts. For example, in "Successful and Failed Logins Per Hour panel", it is noticeable that any unusual login activity that may suggest brute-force or credential stuffing attacks, while the panel on "User Accounts Without MFA Enrollment" will show which accounts can be made more secure. The use of time-series charts and detailed summaries of activities helps protect systems by following policies and reducing the risk of attacks. Furthermore, the BOTSv3 dataset ensures that the dashboard's metrics and alerts respond to real-world cases, enhancing their practical relevance.

In conclusion, this Splunk dashboard allows the organization for effective management to protect from cybersecurity threats. It links security details with daily workflows which makes it simpler to apply Access Control and MFA policies. Regular tracking of important compliance indicators on the dashboard reduces threats, aids in following regulations and encourages everyone at Sutrefia to focus on security. The implementation of this solution enables the company to fend off new forms of cyber threats, secure customers' financial data and maintain their trust. With this dashboard, the company can spot policy violations and be prepared for new threats, making sure the long-term protection of its vital assets.

References

I acknowledge the use of QuillBot's citation generator to format references in accordance with APA 7th edition guidelines.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The Quest to Replace Passwords: A framework for Comparative Evaluation of web Authentication Schemes. *IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/sp.2012.44

Boustead, A. E., & Kugler, M. B. (2023). Juror interpretations of metadata and content information: implications for the going dark debate. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad002

Duo Security. (n.d.). *Download Duo Cisco's Multi-Factor Authentication EVAL Guide*. Cisco Duo. Retrieved June 1, 2025, from https://duo.com/resources/ebooks/the-multi-factor-authentication-evaluation-guide

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (2018). https://doi.org/10.6028/nist.cswp.04162018

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines: revision 3*. https://doi.org/10.6028/nist.sp.800-63-3

Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Ferres, J. L. (2023). How effective is multifactor authentication at deterring cyberattacks? *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2305.00945

National Institute of Standards and Technology. (2018). Framework for improving Critical Infrastructure Cybersecurity. In *National Institute of Standards and Technology*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Verizon Business. (2023). Verizon Business. Retrieved June 1, 2025, from https://www.verizon.com/business/resources/reports/dbir/

Wiefling, S., Jørgensen, P. R., Thunem, S., & Lo Iacono, L. (2022). Pump Up Password Security! Evaluating and enhancing Risk-Based authentication on a Real-World Large-Scale online service. *ACM Transactions on Privacy and Security*, *26*(1), 1–36. https://doi.org/10.1145/3546069