Introduction

Cybersecurity is a critical concern for organizations worldwide, particularly in the face of escalating cyber threats. The Buildings Cybersecurity Framework (BCF) offers a structured approach to enhance cybersecurity practices in various types of buildings, including residential, small commercial, large commercial, and federal buildings. Based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the BCF focuses on five key operations: Identify, Protect, Detect, Respond, and Recover. These operations are designed to mitigate cybersecurity risks by identifying threats and vulnerabilities, implementing protection measures, detecting anomalies and attacks, responding effectively to cybersecurity events, and recovering normal operations post-incident. By adopting the BCF guidelines, organizations can assess their cybersecurity state, prioritize improvements, track progress, and communicate risks to stakeholders, ultimately strengthening their cybersecurity posture and resilience against evolving threats in the digital landscape.

Literature review

The Buildings Cybersecurity Framework (BCF) outlined in the document is designed to enhance cybersecurity practices in various types of buildings, including residential, small commercial, large commercial, and federal buildings. Based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the BCF focuses on five key operations: Identify, Protect, Detect, Respond, and Recover. These operations aim to mitigate cybersecurity risks by identifying threats and vulnerabilities, implementing protection measures, detecting anomalies and attacks, responding effectively to cybersecurity events, and recovering normal operations post-incident. The BCF provides structured methodologies for organizations to assess their cybersecurity state, prioritize improvements, track progress, and communicate risks to stakeholders. By following the BCF guidelines, organizations can strengthen their cybersecurity posture and adapt to evolving threats in the digital landscape.

Cyber Security Metrics and Measures emphasizes the importance of context in interpreting security measures. It highlights that qualitative measures lack significance without context, such as the frequency of attacks relative to total connections. The document stresses the need for analyzing measures in conjunction with trends, control changes, and external data to derive meaningful insights. It discusses the challenges of measure accuracy and the value of aggregating data into metrics for better analysis. Additionally, it references workshops on security metrics and suggests the necessity of research to determine effective security metrics and analytical methods. The paper also mentions resources like the National Vulnerability Database for further information. Overall, the document underscores the critical role of context, analysis, and continuous monitoring in utilizing security metrics effectively to enhance cybersecurity practices.

Methodologies

To implement cyber metrics within the context of the Buildings Cybersecurity Framework (BCF), organizations can follow these steps:

I. **Identify Key Performance Indicators (KPIs):** Determine the specific metrics that align with the core functions of the BCF - Identify, Protect, Detect, Respond, and Recover. For example, KPIs could include the number of cybersecurity vulnerabilities identified, response time to cyber incidents, or recovery time after a cyber attack.

II. **Establish Baselines:** Set baseline measurements for each KPI to understand the current cybersecurity posture of the organization. This will provide a reference point for future assessments and improvements.

III. **Implement Monitoring Tools:** Utilize cybersecurity monitoring tools to track and measure the identified KPIs. These tools can help in collecting data, analyzing trends, and generating reports on cybersecurity performance.

IV. Regular Assessment and Reporting: Conduct regular assessments to evaluate the effectiveness of cybersecurity measures based on the established metrics. Generate reports to communicate the findings to relevant stakeholders.

V. Continuous Improvement: Use the metrics data to identify areas for improvement and adjust cybersecurity strategies accordingly. Implement best practices recommended in the BCF to enhance cybersecurity posture.

By integrating cyber metrics into the BCF framework, organizations can effectively measure, monitor, and improve their cybersecurity efforts to mitigate risks and enhance overall security resilience.

To implement cyber metrics focusing on a specific framework like the Common Vulnerability Scoring System (CVSS):

I. Understand the Framework: Familiarize yourself with the CVSS framework, its scoring system, and how vulnerabilities are assessed.

II. Identify Key Metrics: Determine which metrics within the CVSS framework are relevant to your organization's security needs. Focus on metrics that align with your security goals and priorities.

III. Collect Data: Gather data on vulnerabilities, their severity, and impact on systems. Ensure data accuracy and consistency to derive meaningful metrics.

IV. Calculate Scores: Use the CVSS formulas and guidelines to calculate scores for each vulnerability. Consider factors like exploitability, impact, and complexity in scoring.

V. Analyze and Interpret Results: Analyze the CVSS scores to prioritize vulnerabilities based on severity. Interpret the results to understand the potential risks and implications for your organization.

VI. Implement Mitigation Strategies: Develop mitigation strategies based on the prioritized vulnerabilities. Allocate resources to address high-risk vulnerabilities first.

VII. Monitor and Review: Continuously monitor the effectiveness of your mitigation efforts. Regularly review and update your metrics based on new vulnerabilities and changes in the threat landscape.

By following these steps and focusing on the CVSS framework, we can effectively implement cyber metrics to enhance your organization's security posture and prioritize vulnerability mitigation efforts.

Metrics for cyber security derived from the Deakin Threat Mirror.

Here is a proposed framework for cyber metrics that align with the objectives of the Deakin Threat Mirror project:

1. Identify Key Performance Indicators (KPIs)

- Number of cyber threats identified per month
- Percentage of vulnerabilities mitigated within a specified time frame
- Average response time to cyber incidents

- Number of successful cyber attacks prevented
- Percentage of systems recovered after a cyber incident

2. Establish Baselines

- Determine baseline measurements for each KPI to assess the current cybersecurity posture of the organization.

3. Implement Monitoring Tools

- Utilize cybersecurity monitoring tools to track and measure the identified KPIs. These tools can help in collecting data, analyzing trends, and generating reports on cybersecurity performance.

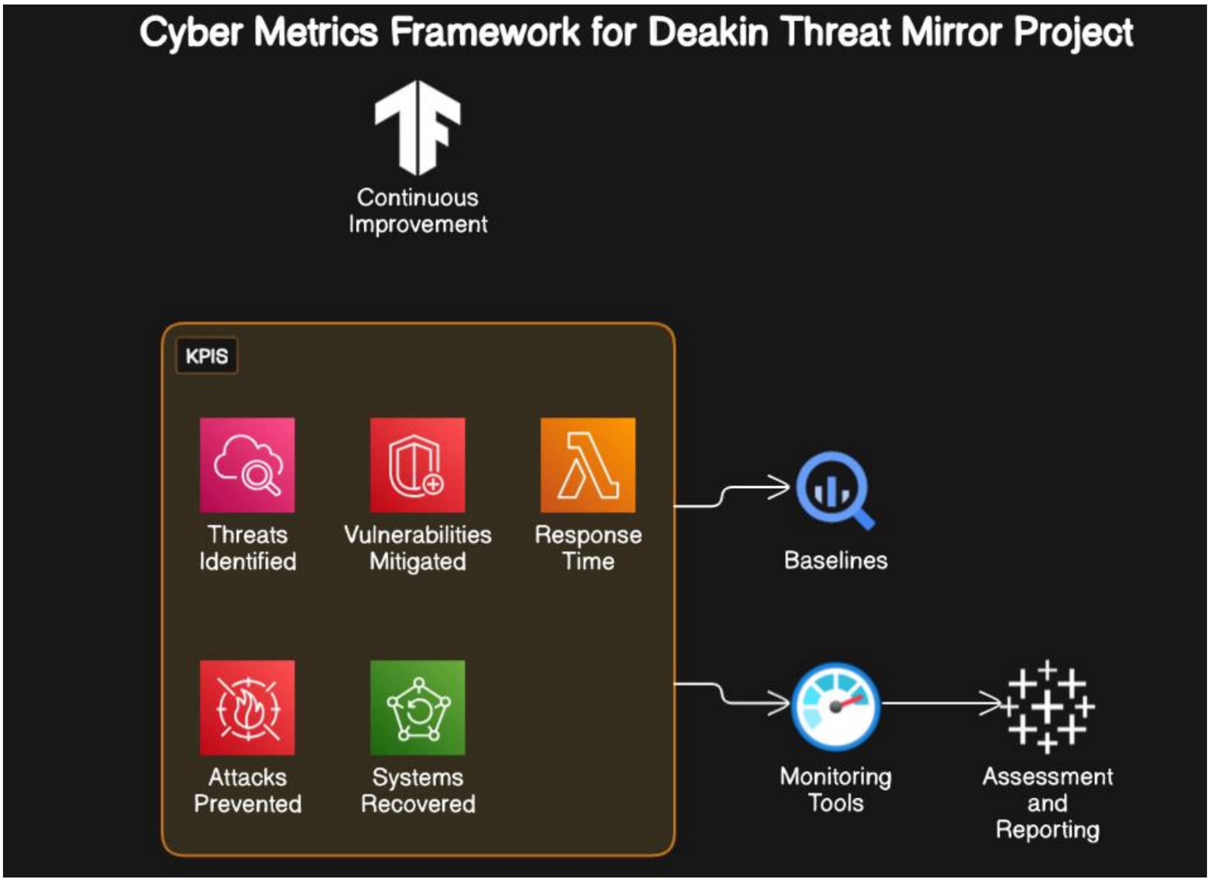
4. Regular Assessment and Reporting

- Conduct regular assessments to evaluate the effectiveness of cybersecurity measures based on the established metrics. Generate reports to communicate the findings to relevant stakeholders.

5. Continuous Improvement

- Use the metrics data to identify areas for improvement and adjust cybersecurity strategies accordingly. Implement best practices recommended in the Deakin Threat Mirror project to enhance cybersecurity posture.

By integrating these cyber metrics into the Deakin Threat Mirror project, organizations can effectively measure, monitor, and improve their cybersecurity efforts to mitigate risks and enhance overall security resilience.



Conclusion

In conclusion, the Buildings Cybersecurity Framework (BCF) provides a comprehensive framework for organizations to enhance their cybersecurity practices in various types of buildings. By focusing on key operations such as Identify, Protect, Detect, Respond, and Recover, organizations can effectively mitigate cybersecurity risks and strengthen their overall security posture. The BCF's structured approach enables organizations to assess their cybersecurity state, prioritize improvements, track progress, and communicate risks to stakeholders. Additionally, the framework emphasizes the importance of context in interpreting security measures and highlights the need for continuous monitoring and analysis of security metrics. By implementing the BCF guidelines, organizations can adapt to the evolving threat landscape and enhance their resilience against cyber threats.

References

[1] Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2007). "Incident Management Capability Metrics." Software Engineering Institute/CERT, Version 0.1. Retrieved from http://www.cert.org/archive/pdf/07tr008.pdf

[2] M. Mylrea, S. N. Gourisetti, and A. Nicholls, "An introduction to buildings cybersecurity framework," in Proceedings of the IEEE Symposium Series on Computational Intelligence, November 2017, doi: 10.1109/SSCI.2017.8285228.