Abstract –This document provides an analysis of the Essential Eight Maturity Model, a strategic framework developed by the Australian Cyber Security Centre to enhance cybersecurity defenses within organizations. The analysis will cover various aspects of the model, including its structure, implementation challenges, and the benefits of achieving different maturity levels.

The analysis offers valuable insights into its application and effectiveness. This analysis is particularly useful for security professionals, IT managers, and decision-makers across various industries, helping them to understand how to better protect their organizations from cyber threats and enhance their cybersecurity measures.

I. Introduction

The Essential Eight Maturity Model provides detailed guidance and information for businesses and government entities on implementing and assessing cybersecurity practices.

- **Purpose and Audience**: designed to assist small and medium businesses, large organizations, and government entities in enhancing their cybersecurity posture. It serves as a resource to understand and apply the Essential Eight strategies effectively.
- **Content Updates**: was first published on July 16, 2021, and has been regularly updated, with the latest update on April 23, 2024. This ensures that the information remains relevant and reflects the latest cybersecurity practices and threats.
- **Resource Availability**: available as a downloadable, titled "PROTECT - Essential Eight Maturity Model," making it accessible for offline use and easy distribution within organizations.
- **Feedback Mechanism**: users are encouraged to provide feedback on the usefulness of the information, which indicates an ongoing effort to improve the resource based on user input.
- **Additional Services**: page cyber.gov.au also offers links to report cyber security incidents, especially for critical infrastructure, and to sign up for alerts on new threats, highlighting a proactive approach to cybersecurity.

II. Specifics

The Essential Eight Maturity Model FAQ provides comprehensive guidance on implementing and understanding the Essential Eight strategies. It emphasizes a proactive, risk-based approach to cybersecurity, reflecting the evolving nature of cyber threats and the importance of maintaining a balanced and comprehensive cybersecurity posture

A. General Questions

- **Essential Eight Overview**: The Essential Eight consists of eight mitigation strategies recommended for organizations to implement as a baseline to protect against cyber threats. These strategies are application control, patch applications, configure Microsoft Office macro settings, user application hardening, restrict administrative privileges, patch operating systems, multi-factor authentication, and regular backups.
- **Purpose of Implementing the Essential Eight**: Implementing the Essential Eight is seen as a proactive measure that is more cost-effective in terms of time, money, and effort compared to responding to a large-scale cyber security incident.
- **Essential Eight Maturity Model (E8MM)**: The E8MM assists organizations in implementing the Essential Eight in a graduated manner based on different levels of tradecraft and targeting.

B. Updates to the Essential Eight Maturity Model

- **Reason for Updates**: The Australian Signals Directorate (ASD) updates the E8MM to ensure the advice remains contemporary, fit for purpose, and practical. Updates are based on evolving malicious tradecraft, cyber threat intelligence, and feedback from Essential Eight assessment and uplift activities.
- **Recent Updates**: Recent updates include recommendations for using an automated method of asset discovery at least fortnightly and ensuring vulnerability scanners use an up-to-date vulnerability database.

C. Maturity Model Updates and Implementation

- **Redefinition of Maturity Levels**: The July 2021 update redefined the number of maturity levels and moved to a stronger risk-based approach to implementation. It also reintroduced Maturity Level Zero to provide a broader range of maturity level ratings.
- **Risk-Based Approach**: The model now emphasizes a risk-based approach, where circumstances like legacy systems and technical debt are considered. Choosing not to implement entire mitigation strategies where technically feasible is generally considered Maturity Level Zero.

- **Implementation as a Package**: Organizations are advised to achieve a consistent maturity level across all eight mitigation strategies before moving to a higher maturity level. This approach aims to provide a more secure baseline than achieving higher maturity levels in a few strategies to the detriment of others.

D. *Specific Strategy Updates*

- **Application Control Changes**: Additional executable content types were introduced for all maturity levels, and Maturity Level One was updated to focus on using file system access permissions to prevent malware execution

III. Approach to Cybersecurity

These strategies are designed to work in concert to provide a robust defense against a variety of cyber threats. While the Essential Eight focuses on these core strategies, organizations are encouraged to implement these in a manner that aligns with their specific needs and risks, potentially incorporating other security measures as part of a broader cybersecurity framework

- **Application Control**: Restricting the execution of unapproved applications to prevent malware and unauthorized software.
- **Patch Applications**: Regularly updating applications to close security vulnerabilities.
- **Configure Microsoft Office Macro Settings**: Restricting the use of macros to prevent malware delivery via Office documents.
- **User Application Hardening**: Reducing the attack surface by disabling features that are commonly exploited, such as Java, Flash, and web ads.
- **Restrict Administrative Privileges**: Limiting administrative rights to reduce the potential for misuse and limit the scope of damage from an attack.
- **Patch Operating Systems**: Regularly updating operating systems to mitigate vulnerabilities.
- **Multi-factor Authentication (MFA)**: Requiring additional verification methods to strengthen access controls.
- **Regular Backups**: Ensuring data is regularly backed up and that backups are tested to ensure they can be restored.

IV. Maturity Levels

Organizations are advised to achieve a consistent maturity level across all eight mitigation strategies before considering moving to a higher level. This ensures a balanced approach to cybersecurity, minimizing weak points that could be exploited by attackers.

The choice of a target maturity level should be informed by a risk-based approach, taking into account the organization's specific circumstances and the evolving nature of cyber threats. This approach helps organizations prioritize their cybersecurity efforts effectively.

- **Maturity Level Zero**: Indicates significant weaknesses in an organization's cybersecurity posture, making it easy for adversaries to exploit.
- **Maturity Level One**: Targets basic cyber hygiene to protect against adversaries using widely available tools and techniques. This level is suitable for organizations looking to protect themselves from general, non-targeted cyber threats.
- **Maturity Level Two**: Provides a more advanced defense against adversaries who are willing to invest more effort and resources to target a specific organization. This level involves tighter controls and quicker response actions.
- **Maturity Level Three**: Represents the highest standard of cybersecurity within the model, aimed at protecting against highly capable adversaries who target specific organizations with advanced tactics.

V. Benefits of Achieving the Target Maturity Level

Reaching the target maturity level in the Essential Eight Maturity Model not only fortifies an organization's defenses against cyber threats but also enhances its operational efficiency, compliance, and strategic positioning in the market

A. *Enhanced Cybersecurity Defense*

- **Reduced Vulnerability to Attacks**: By adhering to the Essential Eight strategies at the target maturity level, organizations can significantly reduce their vulnerability to a wide range of cyber-attacks, including malware, ransomware, and phishing.
- **Prevention of Data Breaches**: Implementing the Essential Eight effectively helps prevent unauthorized access to sensitive information, thereby protecting against data breaches that can have severe financial and reputational consequences.

B. *Improved Compliance and Risk Management*

- **Compliance with Standards**: For Australian government agencies, compliance with the Essential Eight is mandated, and achieving the target maturity level ensures adherence to these standards. For other organizations, it aligns with best practices and can meet or exceed industry standards, which may become more regulated over time.
- **Enhanced Risk Management**: Achieving the target maturity level allows organizations to manage risks more effectively, aligning cybersecurity measures with their risk appetite and threat landscape.

C. *Operational Benefits*

- **Cost-Effective Security**: Implementing the Essential Eight strategies to the required maturity level is generally more cost-effective compared to dealing with the aftermath of security breaches. It provides a good return on investment by mitigating potential losses from cyber incidents.
- **Streamlined IT Management**: Organizations that reach their target maturity level have well-defined processes and systems for managing cybersecurity,

which can lead to more efficient IT operations and reduced downtime.

D. Strategic Advantages

- **Reputation and Trust**: Organizations that demonstrate a high level of cybersecurity maturity can build greater trust with customers, partners, and stakeholders, enhancing their market reputation.
- **Competitive Edge**: By achieving and maintaining a high maturity level, organizations can gain a competitive advantage, particularly if cybersecurity is a critical aspect of their business or sector.

E. Long-Term Sustainability

- **Future-Proofing**: The Essential Eight Maturity Model is designed to be adaptive to changes in the threat landscape. Achieving the target maturity level prepares organizations to quickly adapt to new threats and technologies, ensuring long-term cybersecurity resilience

VI. LAST CHANGES

The last update Essential Eight Maturity Model introduced several significant changes aimed at enhancing cybersecurity measures across various maturity levels.

A. Patch Applications and Operating Systems

- **Increased Priority on Patching**: Organizations are now urged to patch critical vulnerabilities within 48 hours. The focus has also been placed on patching applications that interact with untrusted content within a two-week timeframe.
- **Regular Vulnerability Scanning**: The frequency of scanning systems for critical vulnerabilities has been increased from at least fortnightly to at least weekly.

B. Multi-Factor Authentication (MFA)

- **Enhanced MFA Requirements**: The update introduced stricter MFA requirements, including the use of 'something users have' in addition to 'something users know' starting from Maturity Level One. MFA is now mandatory for web portals storing sensitive data and for staff logging onto business systems at higher maturity levels.
- **Phishing-Resistant MFA**: There is a new emphasis on implementing phishing-resistant MFA to enhance security further.

C. Restrict Administrative Privileges

- **Governance of Privileged Access**: Enhanced processes for managing privileged access, including the need for secure admin workstations and break glass accounts. Privileged accounts accessing the internet must be explicitly identified and their access strictly limited.

D. Application Control

- **Annual Reviews and Blocklists**: Organizations are required to conduct annual reviews of application control rule sets and implement Microsoft's recommended application blocklist at Maturity Level Two.

E. User Application Hardening

- **Discontinuation of Internet Explorer 11**: Organizations must disable or remove Internet Explorer 11 following its support discontinuation. There is also a focus on implementing stringent vendor and ASD hardening guidance, including PowerShell logging and command-line process creation events at higher maturity levels.

F. Regular Backups

- **Data Criticality Consideration**: While there are no significant changes to the backup requirements, organizations are encouraged to consider the business criticality of data when prioritizing backups.

G. Logging

- **Centralized Logging Requirements**: The requirement for centralized logging has been moved from Maturity Level 3 to Maturity Level 2, which will substantially increase the size of log repositories.

H. Cloud Service Management and Incident Detection and Response

- **New Focus Areas**: These have been added as new focus areas in the update, reflecting the need to manage cloud services more effectively and respond to incidents more robustly.

I. General Enhancements

- **Consistency with Information Security Manual (ISM)**: The update has adopted language from mapped controls within the ISM to ensure consistency between the two frameworks and facilitate the automatic ingestion of Essential Eight tracking and reporting by governance, compliance, and reporting tools