Tenable and the ACSC Essential 8 – June 21 Revision

ACSC ESSENTIAL 8

Overview

The Australian Cyber Security Centre (ACSC) provides a wealth of resources and experience to the Australian cyber security landscape. One such resource that has arguably had the largest impact on government departments, critical infrastructure and enterprises alike is the Essential 8 (E8).

The Essential 8 Strategies

The E8 are the eight most effective security risk mitigation strategies from a prioritised list of strategies in the parent document "Strategies to Mitigate Cyber Security Incidents". They are focused on Microsoft Windows networks but are equally applicable to Linux, Cloud and the networks and infrastructure that support them.

The E8 strategies are a distillation of risk-based security and vulnerability management practices into simplified strategies that are prioritized based on effectiveness. It could be said that this simplification strays from the industry recognized best practice of true risk-based security, but it should be treated as a way of understanding the importance of mitigation strategies in supporting a risk-based program. The E8 shouldn't detract from an organisation's goals of reducing cyber risk as it relates to them and their organisation (Gartner Risk-Based Vulnerability Management[1]).

The E8 is comprised of:

- Application control
- Patch applications
- Configure Microsoft Office macro settings
- User application hardening
- Restrict administrative privileges
- Patch operating systems
- Multi-factor authentication
- Regular backups

[1] https://www.gartner.com/smarterwithgartner/how-to-set-practical-time-frames-to-remedy-security-vulnerabilities/

The implementation of the E8 strategies is designed to be self-assessed and/or externally assessed against a maturity model. The model consists of four maturity levels, Maturity Level 0 to Maturity Level 3, that are clearly articulated for each of the E8 strategies. They are designed to identify an organisation's maturity in mitigating increasing levels of adversary threats.

A complete implementation of the E8 at the highest maturity level does not stop adversaries that are willing to invest significant time, money and effort to compromise a target. As such, the E8 should not be an all-consuming part of an organisation's risk mitigation strategy. At the very least, this demonstrates the importance of an organisation's responsibility in understanding the entire threat landscape and specifically as it pertains to their organisation.

TENABLE AND THE ESSENTIAL 8

Tenable provides risk measurement and communication tools that are suited to consistently measuring an organisation's maturity and risk posture. While Tenable can assist with measuring risk in many of the E8 strategies, there are two strategies that Tenable directly assists an organisation's E8 maturity level; Patch Applications and Patch Operating Systems. Tenable does; however, have the ability to audit the implementation of other E8 strategies, as well as other security strategies more widely, to assist in measuring and reporting an overall maturity level.

Patching Applications and Operating Systems

Applying patches to applications and operating systems is critical to ensuring the security of systems. As such, patching

forms part of the E8 from the Strategies to Mitigate Cyber Security Incidents. In addition to patching, the identification of missing patches forms part of the strategy. Specifically, timeframes for conducting "vulnerability scans" are articulated for varying classes of assets. This is the foundation of most risk-based vulnerability management programs and can be leveraged by organisations adhering to the E8 principles.

Tenable has the platform and an array of scan sensors to ensure the efficient conduct of vulnerability scans regardless of network topology and/or complexities. Tenable provides thorough vulnerability scanning of traditional IT assets, work-from-home assets, cloud assets including ephemeral workloads, and supporting infrastructure. Additionally, the E8 specifies an asset class as "internet-facing services", highlighting the importance of web application scanning and IoT/OT scanning should the assets be accessible from public sources.

Talk to your Tenable representative about:

tenable.sc or tenable.io

Auditing the Essential 8 implementation

Implementing an E8 mitigation strategy is likely to directly improve the security posture of an organisation. Auditing the implementation does not improve the maturity level of the mitigation, but rather, confirms the quality, consistency and expected state of that implementation.

Tenable's risk-based vulnerability management capabilities include extensive auditing capabilities. The auditing capabilities empower you to confirm the state of just about any such implementation such as:

- E8 Application control (The application control agent is installed, its version, it's log file exist, the application allow-list file exists) – see tenable.sc
- Configure Microsoft Office macro settings (GPOs are in place to control Microsoft Office functions) – see tenable.sc
- User application hardening (policies are in place as expected to control application function) – see tenable.sc
- Restrict administrative privileges (Numbers of admins, admin lists, policies for controlling access, expiry of passwords, GPOs controlling passwords, complexities and MFA) – see tenable.sc and tenable.ad
- Multi-factor authentication (policies are in place to control authentication processes) – see tenable.sc and tenable.ad
- Regular backups (software installed, processes running, logs being written, policy in place) – see tenable.sc

The listed auditing items are examples only. Implementation of mitigation strategies is likely to be different for every organization. Where deviations to a mitigation are identified, they can be measured, reported and fixed in accordance with the RBVM lifecycle.

COMMUNICATING THE ESSENTIAL 8 STATUS

While the communication component of cyber security programs can be easily overlooked, it continues to be fundamental in describing program efficacy. In order to consistently measure risk and the resultant effectiveness of risk mitigation strategies, Tenable adopts a continuous risk-based vulnerability management lifecycle.

The RBVM Lifecycle

Tenable conducts rich data collection throughout the lifecycle of all assets in a Risk-based Vulnerability Management lifecycle. This is not a point-in-time activity but continues as the assets evolve in order to better describe the threat surface and efficacy of the cyber security program. Tenable adopts a "See. Predict. Act" model that encapsulates this asset lifecycle to ensure continuity.

"See. Predict. Act." is the risk-based vulnerability management lifecycle adopted by Tenable.

See: Discovery and Scanning

Asset discovery is the process of mapping the threat surface and forms the foundation of scanning operations. It is done continuously and frequently through Tenable passive and active sensors to ensure complete coverage as the environment evolves.

Scanning and auditing are the processes of collecting vulnerability data and compliance data. This data directly informs the risk posture and directly increases an organisation's maturity level by meeting the E8 Patch Operating Systems and Patch Applications scan components

Predict: Risk-based or compliance

With a thorough understanding of the threat surface and the corresponding risk posture of assets, Tenable provides detailed insights based on the stakeholders needs. The rich vulnerability data is frequently used to assess patching SLAs in accordance with the E8 strategies. As part of Tenable platforms, Tenable uses threat intelligence sources to **predict** the most significant vulnerabilities (Vulnerability Priority Rating - VPR). This results in a highly prioritised actionable list of remediation activities that focuses risk-based vulnerability management programs on activities that directly reduce the organisation's threat surface.

Act: Treat risk

The final part of the lifecycle is to communicate the outcomes that matter to stakeholders, treat risk and measure the effectiveness of the treatment. While stakeholders actively treat risks, Tenable continues to measure their implementations and responses to ensure your ability to communicate and report the efficacy of the program and the overall maturity level of the organisation.

SUMMARY

The ACSC Essential 8 are a subset of risk mitigation strategies designed to assist organisations reduce cyber risk. Tenable provides the best tools in its class designed to measure and communicate cyber risk whether it be for elements of the Essential 8 or for a robust risk-based cyber security program.

Tenable capabilities are trusted across all levels of federal, state and local governments; the financial sector; the commercial sector; and the education sector to name a few. Whether for Essential 8 maturity or for a robust risk-based security program, Tenable can assist you.

For further information, get in contact with a Tenable representative - anz-sales@tenable.com

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

COPYRIGHT

111 Pacific Hwy

12th Floor

North Sydney, NSW, 2060

www.tenable.com