evolution SYSTEMS

ESSENTIAL EIGHT GUIDE: WHY + WHAT + HOW

Find out how to strengthen your cyber security resilience

INTRODUCTION

Since the start of 2022, there has been a heightened cyber threat environment on a global scale, and the risk of cyber attacks on Australian networks has significantly increased.

That's why the Australian Cyber Security Centre (ACSC) is recommending that organisations urgently adopt an enhanced cyber security posture and improve their cyber security resilience. Australian businesses are strongly encouraged to implement the Essential Eight mitigation strategies which make it much more difficult for adversaries to compromise their systems.

In this guide, we are providing an overview of all the critical things you need to know about the Essential Eight, including:

WHY implementing the Essential Eight is so important

WHAT exactly is included in the Essential Eight

HOW the Essential Eight can help improve your security resilience

WHY | CYBER CRIME ON THE RISE

Over the last few years, the ACSC has observed ransomware continuing to target Australian organisations of all sizes. Recent industry reports mention a wide range of malicious cyber activity, in particular destructive malware and threats to both common enterprise solutions and specific sectors.

Some of the most widespread criminal behaviours and trends include:

- **Phishing emails, RDP exploitation, and exploitation of software vulnerabilities**
- **Targeting the cloud**
- **Targeting managed service providers**
- **Attacking industrial processes**
- **Attacking the software supply chain**

WHAT | ABOUT ESSENTIAL EIGHT

The ACSC has developed prioritised mitigation strategies meant to help organisations protect themselves against various cyber threats. The most effective of these strategies are known as the Essential Eight.

The Essential Eight include:

Prevent Attacks

1 Application Control

BACKGROUND:
Non-approved applications increase the risk of executing, including malicious code.

STRATEGY:
Whitelist all approved and trusted programs to prevent the execution of unapproved or malicious programs, including DLL, .exe, installers, and scripts (e.g. PowerShell, HTA, or Windows Script Host).

2 Patching Application

BACKGROUND:
Adversaries can use security vulnerabilities in your applications (e.g. Flash, web browsers, Microsoft Office, Java, and pdf viewers) to execute malicious code on systems.

STRATEGY:
Apply patches/mitigate computers with 'extreme risk' vulnerabilities as soon as possible and always within 48 hours or less. Make sure to use the latest application version.

3 Configuring Microsoft Office macro settings

BACKGROUND:

Microsoft Office macros can be used as entry points to executing malicious codes on your systems.

STRATEGY:

Update your Microsoft Office settings to make sure the macros are blocked from the internet and only allow trustworthy macros in Trusted locations with limited write access or ones that are digitally signed with a trusted certificate.

4 User Application Hardening

BACKGROUND:

Some of the most common ways to deliver and execute malicious code on systems and devices include Flash, ads and Java.

STRATEGY:

Configure web browsers to uninstall or at least block Flash, ads, and Java. And make sure to disable any unnecessary features in your Microsoft Office, web browsers and pdf viewers.

Limit The Extent of Attacks

5 Restricting Administrative Privileges

BACKGROUND:
Adversaries use admin accounts to gain full access to your company's information and systems.

STRATEGY:
Limit administrative privileges to your operating systems and applications to only users that require them to perform their duties and regularly review and update who needs admin access. Ensure these users know they are not to use their accounts for nonessential activities like, e.g. checking their email or browsing the web.

6 Patching Operation Systems

BACKGROUND:
Adversaries can use security vulnerabilities across your operating systems to compromise your systems.

STRATEGY:
Apply patches/mitigate computers with 'extreme risk' vulnerabilities as soon as possible and always within 48 hours or less. Make sure to use the latest operating system version and never use unsupported versions.

7 Multi Factor Authentication

BACKGROUND:
Adversaries are less likely to gain access to sensitive information and systems if strong user authentication is prevalent.

STRATEGY:
Introduce multi-factor authentication (VPN, RDP, SSH, etc.) as a requirement for all users every time they need to access an important or sensitive data repository or execute a privileged action.

Data Recovery & System Availability

8

Regular Backups

BACKGROUND:

If a cyber security incident takes place, your IT team needs to be able to access, recover, and restore data.

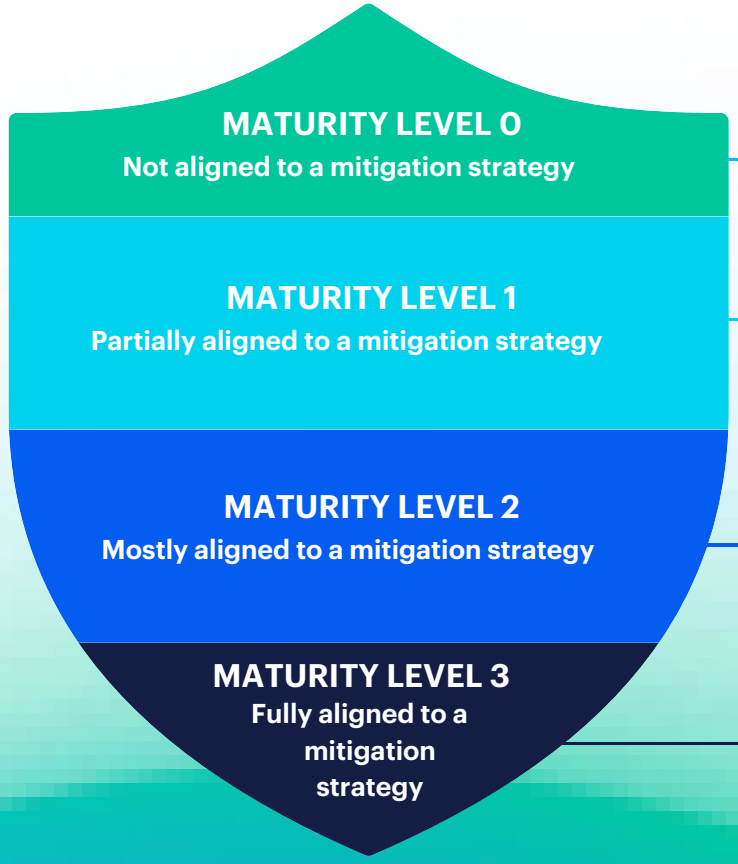
STRATEGY:

Ensure regular, daily backups of important data, software, and configuration settings that are safely stored and retained for at least three months.

There has never been a more critical time to strengthen your company's defences against cyber threats. By implementing the recommended Essential Eight requirements you can reduce cyber security risks by up to **85%.**

HOW | MATURITY LEVEL BREAKDOWN

To help organisations implement the Essential Eight, the ACSC has defined four maturity levels based on mitigating increasing levels of adversary tradecraft (including tactics, tools, techniques, and procedures) and targeting.



Organisations at this level have weaknesses in their overall cyber security posture that, if exploited, could lead to compromising the confidentiality, integrity, and availability of their systems and data, as described below for Maturity Level 1.

Focuses on adversaries that might leverage widely available commodities to gain access to a target's systems.

Focuses on adversaries with slightly higher capability than Maturity Level 1 that are prepared to invest more time in a target and the effectiveness of their tools.

Focuses on adversaries that are more adaptive and less reliant on public tools and techniques who are capable of exploiting the weaknesses in their target's cyber security posture, like, in particular older software or insufficient logging and monitoring.

?

How do you get started on improving your Maturity Level?

Engage security experts

Identify and work on addressing your cyber security weaknesses

Create a Roadmap to maturity

WE CAN SUPPORT YOUR ESSENTIAL EIGHT JOURNEY

evolution SYSTEMS

Our purpose is to improve lives through technology.

For over 25 years, Evolution Systems has been a trusted IT services provider, delivering tailored business solutions and comprehensive cyber security and cloud services to help organisations evolve, innovate, and succeed.

While we work with organisations of all sizes, the majority of our clients are Australian mid-market companies, where we combine deep expertise with flexible, scalable solutions designed to meet their unique operational, cyber security and growth challenges.

What are your cyber security needs?

Let's Talk

www.evolutionsystems.com.au