ManageEngine
Log360

ESSENTIAL EIGHT

EXPLAINED

- Explore the Essential Eight maturity model and its structure.
- Gauge the mindset of your adversary by mapping it with the MITRE ATT&CK framework.
- Learn how to comply with Essential Eight using SIEM.

TABLE OF **CONTENTS**

CHAPTER ONE

WHY THE ESSENTIAL EIGHT?

It's time for the cyberworld to face an inevitable truth: There is a tremendous amount of data being generated, and this amount is set to exceed 200ZB by 2025.[1]

This isn't a new crisis; we always knew there was going to be an infinite amount of data. But what's worrying is that new possibilities of misusing data keep popping up. A cybercriminal knows no rest, and this ever-increasing data pile gives them a goldmine of opportunities to create new problems. According to Cybersecurity Ventures, the annual damage caused by cybercrime worldwide will exceed $10.5 trillion by 2025. [2] Clearly, protecting data is going to be a global challenge for organizations. A good example of this is the cyberwar that occurred during the Russian-Ukraine crisis, which is evidence of how a data vulnerability could end up causing a big threat to nation states. While Russia's war on Ukraine began in February 2022, Ukraine had already been facing an onslaught of cyberattacks from 2014, when Russia had illegally annexed Crimea. Clearly, cyberattacks have become the new poison gas.

The governments of numerous countries, including Australia, have realized the importance of good cyberdefense policies and have recommended that organizations follow certain guidelines and safeguards. The Australian Cyber Security Center (ACSC) sent out a key alert on its official website urging all Australian organizations to prioritize cybersecurity and immediately improve their security posture. [3]

One of the key measures the ACSC suggests is implementing the Essential Eight cybersecurity controls, which can help organizations defend their systems and data more effectively.

Why should you implement the Essential Eight?

Before delving into the structure of the Essential Eight framework, let us first see why you should bother implementing it in the first place.

1. To make it difficult for adversaries to compromise your systems

Cybercrime is only going to increase, and it's time to lay out the battle plans. A framework like the Essential Eight was created with the intention of mitigating cybersecurity incidents faced by Australian organizations. Implementing it will ensure that any attacker trying to compromise your systems and sneak away with your data will face a hard time.

2. To follow a cost- and time-effective framework

A risk-based framework like the Essential Eight outlines a clear plan of action. It does so by classifying organizations into different maturity levels based on the extent of cyber risk they are exposed to. The principle behind this classification is that an organization that ranks higher in maturity will be exposed to lower levels of cyber risk. The framework goes on to give a customized plan of defense for each maturity level. This can save money and a significant amount of time that would otherwise be used to respond to cyberattacks. In this way, an organization's cybersecurity is more productive.

3. To avoid compliance penalties or fees

The Essential Eight was preceded by the Top Four. The Essential Eight retains the Top Four as its first four measures. While the Top Four was mandatory for all Australian federal government agencies, the Essential Eight is expected to be made mandatory for all 98 Commonwealth entities soon. This means, in the future, non-compliance could result in hefty penalties for non-corporate entities. It's better to be proactive by adopting the framework early on and putting the necessary controls in place. [4]

The objective of this e-book is to dive into the Essential Eight framework, its structure, and how you can ensure you comply with it in your organization using a SIEM solution. As a bonus, we also illustrate how to map the MITRE ATT&CK framework to the Essential Eight through an example.

Now that we've covered why any Australian organization should comply with the Essential Eight, let's get started with what this framework is all about.

CHAPTER TWO

WHAT IS THE ESSENTIAL EIGHT, AND HOW IS IT STRUCTURED?

Published in 2017, the Essential Eight is a cybersecurity framework created by the ACSC, and it cites eight security measures organizations can implement to mitigate cyberthreats and address security incidents. It is an upgrade from the Top Four, which consisted of four such measures.

The eight cybersecurity controls are listed here. We will take a deeper look at each one in chapter four.

1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening
5. Restrict administrative privileges
6. Patch operating systems
7. Multi-factor authentication
8. Regular backups

Three major objectives of the Essential Eight

1. Prevent attacks: The Essential Eight urges organizations to take a proactive approach to cybersecurity and adopt measures to mitigate attacks. These measures include:

- Application control.
- Patching applications.
- Configuring Microsoft Office macro settings.
- User application hardening.

2. Decrease attack impact: The framework wants organizations to implement measures that will reduce the impact of a cyberattack when the attacker has already entered the network, like in the case of lateral movement. These measures include:

- Restricting administrative privileges.
- Patching operating systems.
- Multi-factor authentication.

3. Data security: Organizations must ensure the data they generate is secure and is readily available through:

- Regular backups.

Why did it come to be?

In 2010, the ACSC, a part of the Australian Signals Directorate (ASD), released a document called Strategies to Mitigate Cyber Security Incidents, which cited 37 security controls. The controls were arranged in the order of effectiveness in addressing cyberattacks, and the top four were made mandatory for Australian federal organizations in 2014. In 2011, the ACSC claimed that implementing the Top Four helped organizations effectively address 85% of targeted cyberattacks. [6]

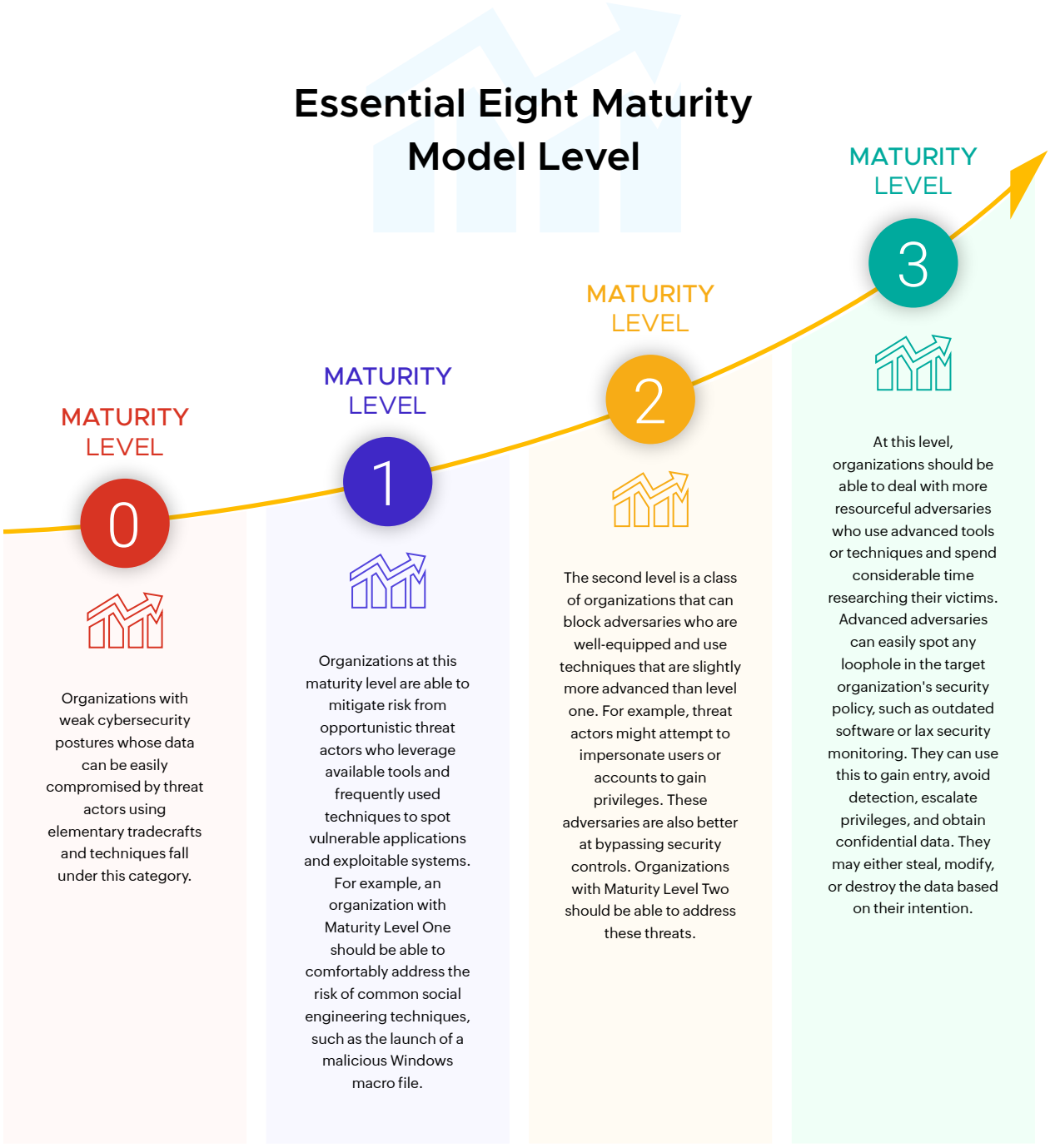
The ASD expanded the Top Four to the Essential Eight in its third update of Strategies to Mitigate Cyber Security Incidents in 2017. [7]

The ASD recently recommended that all Australian organizations implement the Essential Eight to improve their cybersecurity posture due to the increasing number of cyberattacks after Russia's war on Ukraine.

What is the Essential Eight Maturity Model?

The Essential Eight Maturity Model defines four maturity levels for organizations based on their ability to address the risk caused by threat actors and the tradecraft or techniques used by them. The four maturity levels help organizations identify their exposure to cyber risk and focus on mitigating it.[8]

Before implementing the Essential Eight Maturity Model, organizations should decide on a target maturity level and then try to achieve it across all eight controls before moving on to the next maturity level.



How do the eight security measures fit in with the maturity model?

The ACSC also details how organizations can mitigate threats at each level across all eight security controls, and reach their target maturity level. For example, implementing multi-factor authentication (MFA), the seventh measure in the model, differs across organizations according to their maturity levels:

Level one	Level two	Level Three
If users (both organizational and non-organizational) have to be authenticated before they can use internet-facing services that might store, process, or pass on sensitive enterprise information, the organization must implement MFA.	Along with the requirements of level one, organizations must also implement MFA to authenticate privileged users when they log on to their systems. They also have to use a combination of the three authentication factors: 1. Something the user has (e.g., a phone or tablet) 2. Something they know (password) 3. Something they are (eyes or thumbprint for biometric scanning)	Along with the requirements of level two, level three organizations have to implement an MFA- impersonation-resistant protocol. This means the authentication protocol used should stop attackers from carrying out a phishing attack, for example, and fooling users into revealing credentials.

While achieving Maturity Level Three means that an organization has implemented the necessary controls described by the ACSC to mitigate threats of a higher level, it does not mean that they are not at risk of attacks. The ACSC suggests that, apart from achieving Maturity Level Three, it's essential that organizations put into place the controls listed in the Information Security Manual, the ACSC's cybersecurity framework, and Strategies to Mitigate Cyber Security Incidents.[9]

Requirements for implementing an Essential Eight control at each level

Taking the example of the fourth mitigation measure, user application hardening, we will now explore the different requirements organizations across all three maturity levels have to fulfill. A similar process can be applied to all security measures to determine requirements at each maturity level.

User application hardening:
In general, application hardening is a best practice used by organizations to make it harder for criminals to hack into an app. While this should be implemented from the development stages, application hardening is an external measure which consists of plugging loopholes and possible vulnerabilities. The Essential Eight framework recommends that organizations implement this according to their cyber risk exposure.

Maturity Level ONE

Level one organizations must implement the following requirements to fulfill the fourth security measure of user application hardening.

- Web browsers are restricted from processing Java or web advertisements from the internet
- Browser settings cannot be modified by users
- Internet Explorer 11, which is now deprecated, cannot process internet content

Maturity Level TWO

Level two organizations must implement the following requirements to fulfill the fourth security measure of user application hardening.

- All of level one's requirements must be in place
- Creation of child processes through Microsoft Office or PDF applications is blocked
- MS Office is stopped from creating executable content or injecting code into other processes, and is configured to prevent activation of OLE packages
- Application hardening guidelines are implemented for browsers, MS Office, and PDF software; users cannot change their security settings
- There is a logging mechanism in place to keep track of blocked PowerShell script executions

Maturity Level

THREE

Level three organizations must implement the following requirements to fulfill the fourth mitigation strategy of user application hardening.

- All of level two's requirements must be in place
- Internet Explorer 11, which is now deprecated, must either be disabled or removed
- .NET framework 3.5 and PowerShell 2.0 should be removed to avoid remote code execution vulnerabilities
- The existing PowerShell version should be used only in Constrained Language mode
- Most importantly, the ACSC recommends that there is a central logging mechanism in place which records all blocked PowerShell script executions, monitors for signs of compromise or unauthorized modification or deletion, and triggers appropriate responses or actions when security events are detected

In this e-book, we have focused on one of the eight strategies, user application hardening, to understand how organizations across all three maturity levels have to implement the eight controls. For a more detailed description of how to implement all eight measures across the three maturity levels, you can refer to the ACSC's official document on the maturity model.[10]

How to implement user application hardening across all three levels with a SIEM solution

Taking the example of user application hardening, let us now see how a SIEM solution can help meet the requirements of this measure across all three levels.

To implement user application hardening, organizations are required to have a mechanism in place that sends out notifications for the following events:

- When a web browser processes Java files or web advertisements
- When a user modifies browser, MS Office, or PDF application settings
- Any remote execution through .NET 3.5 or PowerShell 2.0
- When a child process is created by any MS Office or PDF applications
- Execution of any blocked PowerShell scripts or any suspicious processes or indicators of compromise that could lead to a security event

A unified SIEM solution like Log360 comes equipped with advanced log collection and archival capabilities, real-time security analytics, and an automated incident management system.

Using Log360's prebuilt reporting module, you can track:

- Changes made to any application or security settings.
  Irregular software installations done via browsers.
- Execution of any suspicious child processes, or PowerShell scripts done remotely or on-premises.

Apart from this, because Log360 correlates network events with known adversary behavior identified in the MITRE ATT&CK framework, you can spot suspicious activity, understand which part of the kill chain it could belong to, and identify what attack it might eventually lead to. You can also set up alerts and automated response workflows for each of these activities.

If you're new to the MITRE ATT&CK framework, fear not! We will cover that in detail in the next chapter. We will also explore how to map the Essential Eight strategies with the MITRE ATT&CK framework. How is this beneficial to you, you ask? Turn the page to find out!

CHAPTER THREE

MAPPING THE ESSENTIAL EIGHT MATURITY MODEL WITH MITRE ATT&CK

As explored in the earlier chapters, organizations can classify themselves into various maturity levels based on the risks posed by cyberattackers and the techniques or tradecraft used by them to carry out an attack.

Here, we'll attempt to map the MITRE ATT&CK framework to the ACSC's Essential Eight maturity level framework. This will help organizations:

1. Recognize which attack techniques to focus on first.
2. Prioritize their resources for cyberdefense.
3. Get into the mindset of the adversary, and come up with a better defense strategy.

Before getting to the mapping, let's first brush up on what the MITRE ATT&CK framework is and how it's structured.

What is the MITRE ATT&CK framework?

ATT&CK (which stands for adversarial tactics, techniques, and common knowledge) was created in 2013 by MITRE, an American not-for-profit research organization. Designed to gauge adversary behavior in the post-compromise stages of an attack, it is a matrix consisting of various tactics and techniques. [11]

Tactics are a list of possible reasons or adversarial goals for an attack. Tactics are divided into three types based on the environment in which attacks are carried out: enterprise, mobile, and industrial control systems (ICSs). In 2017, MITRE released a PRE-ATT&CK framework with the intention of providing more insights into the pre-compromise stages of attacks. This included reconnaissance and resource development as pre-compromise tactics.

Techniques listed under each tactic are possible ways adversaries can carry out the attack. These are further divided into sub-techniques.

Mapping the Essential Eight with MITRE ATT&CK using the example of lateral movement

Lateral movement is a critical tactic employed by adversaries to pivot and move across an organization's network as part of their kill chain. Lateral movement also involves the malicious access and control of remote systems in a network. We've chosen this technique because it is challenging to detect and prevent. Once a deeper level of access is gained, differentiating between usual network traffic and a malicious actor moving through the network becomes nearly impossible. We will map this tactic of the MITRE ATT&CK to the Essential Eight just as an example. In a similar fashion, other tactics of ATT&CK can also be mapped to the Essential Eight.

In order to effectively map lateral movement to the Essential Eight maturity level framework, we'll first pick a characteristic trait of adversaries and then assess the extent to which an organization has the wherewithal to withstand this trait. The ability to withstand this trait can be ranked across three levels: low, medium and high. In our mapping model, a rank of "low" would be associated with level one of the Essential Eight framework. Similarly, a rank of "medium" and "high" would be associated with level two and level three respectively.

The characteristic trait of adversaries we have picked to map the frameworks is:

Reliance on public tools and effectiveness of techniques

Organizations are classified into three maturity levels based on how well they can address adversaries who rely on public tools and techniques to various degrees and sophistication. By this, we mean how well organizations can mitigate risk from adversaries that opt for free, open-source software like Mimikatz (level one) instead of paid options, like purchasing malcode written in Golang off the dark web (level two or three), for example. Golang is a programming language that has been increasingly used to create malware since 2017. [12]

In most cases, level one organizations are only able to address non-sophisticated attackers who use amateur techniques like mass phishing emails, while level three organizations are more likely to be adept at addressing advanced techniques.

Level one	Level two	Level Three
Can only defend against the use of public tools, e.g. script kiddies.	Can defend against attackers that customize publicly available tools.	Can defend against attackers that rarely or do rely on publicly available tools.

The techniques used to carry out lateral movement

The MITRE ATT&CK framework lists the following techniques used by an adversary to carry out lateral movement in a network.

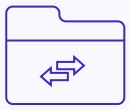
Exploitation of remote services

Once a bad actor gains access to a network, one of the techniques they execute is exploiting remote services to move laterally or escalate privileges. This happens in a sequence of two events:

1. The adversary looks for vulnerabilities in various devices across the network
2. The adversary uses the vulnerability to gain access to remote services and move laterally

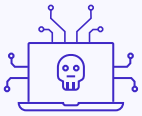
Internal spear phishing

The bad actor first hacks into the user's account through compromised credentials or through previously installed malware. Then, they gain the email account access of not just one but eventually several users through phishing emails. This is one of the ways cybercriminals carry out lateral movement.



Lateral tool transfer

Once they enter the compromised network, bad actors can transfer malicious tools between victim systems through internal file sharing protocols or RDP. Transferring files internally between two systems in a network could either pave the way for lateral movement or support an attacker that has already compromised the receiving system.



Remote service session hijacking

When a user establishes and logs in to a remote service session by using their credentials, the attacker uses this connection to move laterally from one system to another.

Remote services

Several applications use remote services that use different protocols to connect to other systems in a network—adversaries exploit this by logging in to victim systems using valid accounts and using these protocols for lateral movement.

Replication through removable media

When a user inserts removable media into the system, the adversary copies malicious software onto it. When the same media is inserted into another system, the malicious software runs due to the auto-run feature in the other system, enabling infiltration and lateral movement.

Software deployment tools

Sometimes adversaries exploit existing third-party applications or software to move laterally across systems. For example, if a bad actor gains access to enterprise-wide used software, they could use this to move laterally.

Taint shared content

Once they gain access to shared files or documents, bad actors can deliver malicious software to remote systems by adding it to this shared content repository.

Use alternate authentication material

Systems generate alternate authentication credentials, which are stored in a cache and used to verify a user's identity. They act as substitutes to real credentials. Once adversaries gain access to this cache, they can log in to accounts without actual passwords or authentication information.

Now that we've explored each of the techniques used by attackers to carry out lateral movement, we will rank each of them according to the chosen trait, reliance on public tools and effectiveness of techniques.

1. Non-sophisticated techniques that are mostly based on publicly available tools will be ranked as "low."
2. Slightly more sophisticated techniques that require adversaries to customize publicly available tools will be ranked as "medium."
3. Techniques that are more sophisticated will be ranked as "high."

Please note that there is a level of subjectivity that is involved in this ranking.

This ranking will then be used as an indicator of the maturity level of an organization. Organizations that belong to Maturity Level One will be able to defend against lateral movement techniques that are ranked "low." Likewise, organizations that belong to Maturity Levels Two and Three will be able to defend against lateral movement techniques that are ranked "medium" and "high" respectively.

Level one (Low)	**Level two** (Medium)	**Level Three** (High)
• Internal spear phishing • Replication through removable media • Taint shared content	• Lateral tool transfer • Remote service session hijacking • Software deployment tools	• Exploitation of remote services • Remote services Use alternate authentication • method

Level one (Low)

The techniques classified under level one include:

- Internal spear phishing.
- Replication through removable media.
- Taint shared content.

These techniques don't require a lot of coding knowledge or expertise, and they don't need specific resources. For example, to move laterally through a corrupt file in removable media, an attacker either has to manipulate the media, the firmware, or the system where the media has been inserted. None of these options require substantial knowledge of code or hardware to execute, so we can classify these under "low."

Level two (Medium)

The techniques classified under level two include:

- Lateral tool transfer.
- Remote service session hijacking.
- Software deployment tools.

When it comes to medium level techniques, attackers must have knowledge of third-party applications and how to hack into them to gain access and move laterally. At the same time, they do not need to be proficient in developing their own malcode. To hijack remote service sessions, the attacker needs valid credentials to accept remote connections. Once they gain access to third-party software, they need to know how they can use and manipulate them to enter other systems in the enterprise network that use this software.

Level one (High)

The techniques classified under level three include:

- Exploitation of remote services.
- Remote services.
- Use alternate authentication method.

These techniques are ranked "high" because they require additional coding knowledge and hacking expertise. In order to exploit a remote service or connection, the attacker must be able to identify vulnerabilities in the program, service, or operating system, and take advantage of them to execute malicious code. This requires good knowledge of malcode development and execution.

There you have it, mapping of one of the tactics of ATT&CK—lateral movement—with the Essential Eight maturity model. Organizations can similarly map any tactic they are likely to be targeted for. Using this methodology will not only help security teams identify the various attacks and techniques used by cybercriminals, it will also help them:

- Get an idea of their cyber risk levels, and carry out an appropriate cybersecurity plan.
- Identify possible loopholes in their network and address them beforehand.
- Identify the indicators of compromise they need to watch out for.
- Put out alerts for indicators of compromise, and implement appropriate incident response measures.

CHAPTER FOUR

COMPLYING WITH ESSENTIAL EIGHT MITIGATION STRATEGIES USING SIEM

Let's take a deeper look at the eight cybersecurity measures of the Essential Eight and how you can implement each one using an efficient SIEM solution.

1 MITIGATION STRATEGY

Application control

Application control is the practice of regulating the execution of unauthorized applications or malicious code. Organizations usually do this either through application whitelisting or blacklisting. To implement this measure, organizations need to gain visibility into all the applications run by users in the network. Also necessary is tracking unusual activity and taking immediate action if required.

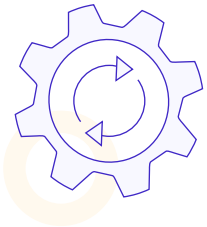
The Essential Eight framework suggests using three rule conditions that are also commonly used in AppLocker, Microsoft's app whitelisting software:

- **Cryptographic hash rules:** This rule or algorithm converts passwords into enciphered hash values (or just hashes). These are stored instead of passwords and used for verification.
- **Publisher certificate rules:** A publisher certificate is used to verify the software publisher. A publisher certificate rule in Applocker can only be made for digitally signed files and helps identify whitelisted apps from others.
- **Path rules:** A path helps identify where a file is located. A path rule prevents access to all files within a folder or a location.
- **Event logs:** Apart from the three rules, event logs generated by applications must also be tracked to analyze allowed and blocked executions. This will help spot adversaries taking over applications to execute malicious code as a precursor to a bigger attack.

How Log360 can help you with this: Controlling which applications are allowed or blocked can be made easy through Log360's CASB feature, which helps define authorized, banned, and shadow applications. Log360 also blocks banned applications when users attempt to access them.

2 MITIGATION STRATEGY

Patch applications



Patching happens when a flaw is identified in an application after its release. It is the process of installing a new "patch," or a change in code, to fix the vulnerability. If applications are not patched promptly, there is every chance of an attacker using the vulnerability to infiltrate systems. To execute this control effectively, organizations must find a way to analyze the data obtained from different vulnerability scanners and generate actionable analytical insights. When a threat is detected, action should be taken to mitigate it immediately and automatically.

The ACSC recommends the following time frames for applying patches and conducting vulnerability scans for missing patches, according to the level of cyberthreat posed.

Level of cyberthreat	Type of application	Time frame to apply patches	Time frame for conducting vulnerability scans for missing patches
Basic	Internet-facing application	Within two weeks, or within 48 hours if an exploit exists	Daily
	Commonly targeted application	Within one month	Fortnightly
	Other applications	-	As required
Intermediate	Internet-facing application	Within two weeks, or within 48 hours if an exploit exists	Daily
	Commonly targeted application	Within Two month	Weekly
	Other applications	Within one month	Fortnightly
Advanced	Internet-facing application	Within two weeks, or within 48 hours if an exploit exists	Daily
	Commonly targeted application	Within two weeks, or within 48 hours if an exploit exists	Weekly
	Other applications	Within one month	Fortnightly

For critical infrastructures like those found in ICSs, organizations might prefer manual patching measures instead of automated processes. For these, the framework suggests taking up procedures that are more suitable for their specific business needs and risk profile, like network monitoring or segmentation.

How Log360 can help you with this: Log360 can collect, ingest, and analyze logs generated by various vulnerability scanners. It also comes with over 50 preconfigured reports to monitor traffic that help you stay on top of any new vulnerabilities in your systems. This way, whenever a new vulnerability pops up, security analysts can check for the release of a relevant patch and install it.

3 MITIGATION STRATEGY

Configure Microsoft Office macro settings

While using macros helps increase productivity and automate repetitive tasks, it can also lead to cyberattacks. For example, a cybercriminal could deploy a file with a malicious macro in it, and this could be triggered when the file is downloaded by a user. It is advised to have certain configuration settings in place to avoid such threats. The Essential Eight lists a set of measures organizations can take to mitigate the threat of malicious macros.

These include:

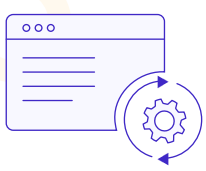
- Disabling macros for users that do not require them.
- Only enabling macros from trusted sources.
- Checking macros for digital signatures before use.

Organizations should also be able to track activities like processes, services, or applications launched unbeknownst to the user due to the execution of a macro.

How Log360 can help you with this: Log360's log management feature continuously keeps track of all activity including the launch of processes, services, and applications.

4 MITIGATION STRATEGY

User application hardening



In general, application hardening is a best practice to make it harder for criminals to hack into an application. While this should be implemented from the development stages, app hardening is an external measure which consists of plugging loopholes and possible vulnerabilities. The Essential Eight framework recommends that organizations implement this according to their cyber risk exposure. Some measures organizations can take include blocking Flash and advertisements on web browsers, or blocking JavaScript on certain websites.

How Log360 can help you with this: Log360 comes equipped with a CASB feature that can help organizations recognize banned applications used by employees and curb their access. It can detect shadow IT activity and help IT administrators address it immediately through real-time alerts sent via SMS and email.

5 MITIGATION STRATEGY

Restrict administrative privileges

Privileged users have access to confidential enterprise data, and this poses a risk of both insider attacks and account compromise. The ACSC lists restricting these privileges and putting security measures in place as necessary guidelines to be followed.

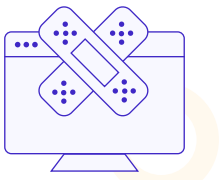
To effectively implement this control, the ACSC suggests implementing measures like:

- Identifying tasks that require privileged access.
- Creating separate attributable accounts for members who carry them out.
- Restricting administrative privileges to a select few to limit the escalation of critical activities.
- Periodically re-verifying the requirement for privileged accounts based on changes in employee responsibilities and designations or in case of exposure to security incidents.

How Log360 can help you with this: Log360's real-time security monitoring feature helps track changes made by privileged users and trace suspicious activities like unusual logon attempts or modifications made to important files. Its incident management module enables the customization of a set of workflows to be executed for each security alert, and facilitates building a proper incident response mechanism.

6 MITIGATION STRATEGY

Patch operating systems



Similar to patching applications, patching operating systems involves regularly checking for newly released patches (like keeping an eye out for Patch Tuesday if you are a Microsoft user) and analyzing data from vulnerability management systems to take timely action. Those involved in this process must take the initiative to check if the patch is necessary and safe, and test it before deployment.

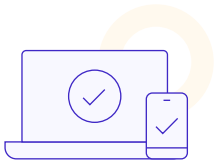
The ACSC recommends the following time frames for applying patches and conducting vulnerability scans for missing patches, according to the level of cyberthreat posed.

Level of cyberthreat	Type of application	Time frame to apply patches	Time frame for conducting vulnerability scans for missing patches
Basic	Internet-facing services	Within two weeks, or within 48 hours if an exploit exists	Daily
	Workstations, servers, network devices, and other network-connected devices	Within one month	Fortnightly
Internet-facing services	Internet-facing services	Within two weeks, or within 48 hours if an exploit exists	Daily
	Workstations, servers, network devices, and other network-connected devices	Within two weeks	Weekly
Advanced	Internet-facing application	Within two weeks, or within 48 hours if an exploit exists	Daily
	Workstations, servers, network devices, and other network-connected devices	Within two weeks, or within 48 hours if an exploit exists	Weekly

How Log360 can help you with this: The laundry list of Log360's 750 types of log sources includes vulnerability scanners. It comes with over 50 preconfigured reports to monitor traffic that help you stay on top of any new vulnerabilities in your systems. This way, whenever a new vulnerability pops up, security analysts can check for the release of a relevant patch and install it.

7 MITIGATION STRATEGY

Multi-factor authentication



MFA is an identity verification method that uses a combination of the following three factors to authenticate your credentials:

- Something you know (knowledge), like your password
- Something you have (possession), like your phone
- Something you are (inherence), like your fingerprint

Common measures used to implement MFA include the following:

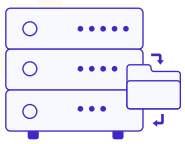
- U2F security cards
- Physical one-time PIN tokens
- Biometrics
- Smart cards
- Mobile authentication apps
- SMS messages or voice calls
- Software certifications

The ACSC also recommends measures like hardening devices to the maximum extent, ensuring a visual notification appears for every authentication request, and storing software certificates in the devices' trusted platform module. Specific requirements for each measure are also recommended.

ManageEngine's AD360, an integrated IAM tool, comes equipped with customized solutions to help you easily implement effective MFA protocols tailored for your organization's tool.

8 MITIGATION STRATEGY

Regular backups



Regular offline and online backups are highly recommended. These should also provide measures to alert users or indicate a breach as well as specify proper incident response actions.

How Log360 can help you with this: A comprehensive SIEM solution like Log360 comes equipped with the ability to monitor constantly and detect malicious attempts to access, delete, or modify privileged data stored in backup folders.

Implementing the ESSENTIAL EIGHT with Log360

MITIGATION STRATEGY

1 Application control

Identify banned applications used by employees and curb their access with a cloud access security broker. Detect shadow IT activity and alert administrators in real time via SMS and email.

MITIGATION STRATEGY

2 Patch applications

Detect vulnerabilities by examining data from the most popular vulnerability scanners to generate actionable insights

MITIGATION STRATEGY

3 Configure Microsoft Office macro settings

Eliminate possible attacks through malicious macros by continuously tracking processes, services, or applications launched unbeknownst to the user through the event correlation engine and the behavioral analysis module.

MITIGATION STRATEGY

4 User application hardening

Keep tabs on access to both in-house and third-party applications by using built-in analytics and the custom log parser. You can set up notifications for indicators of compromise.

MITIGATION STRATEGY

5 Restrict administrative privileges

Track all administrative user actions and trace suspicious activities like modifications made to important files or access permissions through real-time security monitoring.

MITIGATION STRATEGY

6 Patch operating systems

Get visibility on the vulnerabilities in your network to learn which areas require prompt patching.

MITIGATION STRATEGY

7 Multi-factor authentication (MFA)

Identify security gaps in your network and track whether authentication protocols like MFA are being efficiently deployed where required.

MITIGATION STRATEGY

8 Regular backups

Monitor accesses and any modifications made to all backup files or folders.

ABOUT THE AUTHOR

Anupama
Product Marketing Associate

Anupama is a product marketing associate at ManageEngine, the enterprise IT management division of Zoho Corporation. In her current role, she keeps track of the latest trends in the cybersecurity space, especially those related to SIEM. A keen writer, she contributes to organizational cybersecurity awareness through her research-led insights.

REFERENCES

1. Morgan, S., 2022. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. [online] Cybersecurity Ventures. Available at: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> [Accessed 23 August 2022].

2.Morgan, S., 2022. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. [online] Cybersecurity Ventures. Available at: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> [Accessed 23 August 2022].

3. Official website of the ACSC. 2022. Australian organisations encouraged to urgently adopt an enhanced cyber security posture. [online] Available at: <https://www.cyber.gov.au/acsc/view-all-content/alerts/australian-organisations-encouraged-urgently-adopt-enhanced-cyber-security-posture> [Accessed 23 August 2022].

4. ACSC. "PGPA Act Flipchart and List." PGPA Act Flipchart and List | Department of Finance. Accessed September 5, 2022. https://www.finance.gov.au/government/managing-commonwealth-resources/structure-australian-government-public-sector/pgpa-act-flipchart-and-list.

5. Official ACSC website. 2022. Essential Eight. [online] Available at: <https://www.cyber.gov.au/acsc/view-all-content/essential-eight> [Accessed 23 August 2022].

6. A, Anupama. "ManageEngine - IT Management: Network Management Software." ManageEngine Log360. Accessed September 5, 2022. https://www.manageengine.com/log-management/cyber-security/essential-eight-explanied.html.

7. Official ACSC website. 2022. Strategies to Mitigate Cyber Security Incidents. [online] Available at: <https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents> [Accessed 23 August 2022].

8. 2022. Protect- Essential Eight Maturity Model (October 2021. [ebook] ACSC, p.17. Available at: <https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20(October%202021).pdf> [Accessed 23 August 2022].

9.ACSC, Essential eight maturity model - cyber. Essential Eight Maturity Model . Available at: https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20%28October%202021%29.pdf [Accessed September 7, 2022].

10. 2022. Information security manual (ISM). [online] Available at: <https://www.cyber.gov.au/acsc/view-all-content/ism> [Accessed 5 September 2022].

11. Attack.mitre.org. 2022. MITRE ATT&CK®. [online] Available at: <https://attack.mitre.org/> [Accessed 23 August 2022].

12. Singh, M., 2022. The Trend of Golang in Cyber Security - CyberFrat. [online] CyberFrat. Available at: <https://cyberfrat.com/the-trend-of-golang-in-cyber-security/> [Accessed 5 September 2022].