RAPID7

COMPLIANCE GUIDE

How to Proactively Manage Your Agency's Security Posture

Rapid7's approach to the ASD Essential Eight

TABLE OF CONTENTS

Introduction

Taking a proactive approach to your agency's security posture is a cost-effective way to reduce your cybersecurity exposure. Removing the attack vector through proactive measures is likely to stop many attacks in their tracks, and fixing a breach is far more costly than prevention. The average cost of a data breach in Australia is $2.13m according to the IBM Ponemon "Cost of a Data Breach" report, released in July 2019.

To help your agency mitigate cybersecurity incidents, the Australian Signals Directorate (ASD) published a cybersecurity baseline, 'The Strategies to Mitigate Cyber Security Incidents.' These are a list of prioritised initiatives to strengthen computer security. Of these, the Essential Eight are the most fundamental elements of that list, providing a baseline cybersecurity posture.

The Essential Eight strategies provide a solid baseline toward protecting your agency from security breaches, as well as damaging malware. The costs of implementing these strategies, along with the investment of staff training and upgrades, far outweigh the potential cost of a massive compromise.

We recommend you read the information provided by ASD beforehand to get a firm understanding of your requirements. In addition, we've outlined below the specific components of the ASD Essential Eight, and how Rapid7 can help you either measure against, or leverage our technology to help you further.

Our cyber-exposure measurement technologies help you follow the Essential Eight Guidelines. Above all, the Essential Eight promotes good security habits, and helps agencies better protect themselves against the plethora of attack vectors from unwelcome threat actors.

The table highlights how each of the components of the Essential Eight can be addressed with our solutions. Rapid7's full stack of platform-enabled solutions has you covered.

	InsightVM	InsightIDR	InsightAppSec	InisghtCloudSec	InsightConnect	Managed Detection and Response	Managed Vulnerability Management	Professional Services and Partners
Application control	★	★				★		★
Patch applications	★		★			★	★	★
Configure Microsoft	★	★		★				★
Macro Settings								
User application hardening	★		★			★	★	★
Restrict administrative privileges		★		★				★
Patch operating systems	★					★	★	★
Multi-factor authentication		★			★			★
Regular backups								★

The Australian Signals Directorate (ASD) has recently implemented an update (July 2021) to the Essential Eight, built around three core factors, namely:

- Redefining the number of maturity levels and what they represent.
- Moving to a stronger risk-based approach to implementation.
- Implementing the mitigation strategies as a package.

Outlined across four maturity levels, the strategies within each of these levels provide a solid baseline towards protecting your agency from security breaches, as well as damaging malware. The updates also see the reintroduction of maturity level zero. This provides a broader range of maturity level ratings for you to consider when evaluating Essential Eight implementations.

While there are a number of updates to consider across all eight strategies, and for each of the four maturity levels, some of the most significant address the identification of software and configuration vulnerabilities through the use of vulnerability scanners across your entire organisation, including workstations.

This is relevant to the 'Patch Applications' strategy, which is now updated. Further information regarding the updates can also be found here.

The Essential Eight Strategies

Outlined below are details of the Essential Eight mitigation strategies. We outline some of the basic requirements you need to know, why they're important, and how Rapid7 can help you.

Application Control

What you need to know

Application whitelisting is about only allowing approved and trusted programs or identified entities access to your network and thus, preventing the execution of unapproved/malicious programs e.g. .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA), and installers.

Why is it important?

This prevents malware and untrusted software from causing harm to systems in your environment.

How do we help?

We believe security is the responsibility of all technology users, manufacturers, and intermediaries, and that collaboration is the only way to achieve long-term change. That's why we're committed to openly sharing security information, helping our peers to learn, grow, and develop new capabilities, and supporting each other in raising and addressing issues that affect the cybersecurity community.

Whilst Rapid7 is not a provider of application control technologies, between the Metasploit Community, penetration testing, red teaming, and our 24/7 Managed Detection and Response service, we're investigating a constant stream of attacker behavior.

As part of the investigative process, our analysts directly contribute Attacker Behavior Analytics (ABA) detections into InsightIDR, our cloud-native SIEM, paired with recommendations and adversary context. These detections leverage the real-time user and endpoint data collected by InsightIDR. The result: the alert fidelity you want, filled with the context you need for when an adversary outsmarts application control technologies. When an application whitelisting tool is implemented, you can send logs to the InsightIDR instance for analysis and alerting upon (attempted) violations.

Patch Applications

What you need to know

Patching known security vulnerabilities in applications such as Flash, web browsers, Microsoft Office, Java, and PDF viewers is one of the most effective activities an organisation can do to ensure the security of their network and environment. The ASD Essential Eight July '21 update outlines specifically that:

- A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. (maturity level one, onwards)
- A vulnerability scanner is used at least fortnightly (maturity level one) or at least weekly (maturity levels two and three), to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
- Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release, or within 48 hours if an exploit exists.

A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications. (Maturity levels two and three).

Why is it important?

Security vulnerabilities in applications can be used to execute malicious code on systems or in your IT environment. Fully patched applications are also an essential foundation on which other security controls can be augmented.

How do we help?

Every network has assets more pivotal to the overall business than others, and no business—even one with an army of analysts—has the time (especially during an emergency) to determine where to start first.

Rapid7 can assist with this requirement from a few different perspectives, starting with vulnerability management. Our InsightVM solution can identify your assets' operating systems and applications installed on them and assist in remediation prioritisation based on our threat intelligence.

We also enable you to track remediation efforts and defined SLAs (as outlined in the new requirement) Additionally, you can expand your reach into dynamic application security testing (DAST) with InsightAppSec; This is significant if you are developing in-house applications or are having applications developed for you by a third party. Understanding these application layer risks should be part of your vulnerability and risk management program.

Our Managed Application Security (Managed AppSec) service takes a comprehensive approach, from configuring and scheduling scans to monitoring them and seeing them through to successful completion. Our experts will review findings, validate vulnerabilities, and remove false positives.

Configure Microsoft Office Macro Settings

What you need to know

Microsoft macros are a great productivity tool, helping you to automate tasks within Microsoft 365. You can configure Microsoft macro settings to block macros from the internet, allowing only vetted macros either in ‘trusted locations’ with limited write access, or digitally signed with a trusted certificate. Using group policy, you can enforce these settings and ensure end users can not revert them.

Why is it important?

Microsoft macros can be used to deliver and execute malicious code on systems, which can often result in unauthorised access to sensitive information or the manipulation of critical data.

How do we help?

At Rapid7, we see a constant stream of threats from Metasploit, our Managed Detection and Response customers, and our incident response and penetration testing engagements. During threat investigations, our expert analysts zero-in on these stealthy techniques, while researching the attacker’s targets and goals. This intelligence is crafted into Attacker Behavior Analytics (ABA) detections in InsightIDR, which can find malicious behaviors when they have been altered to evade policy configuration and prevention defenses.

InsightIDR includes containment capabilities, such as kill process, quarantine asset, and disable user, but does not include remediation capabilities such as remove file, change permissions, or adjust policies.

The InsightVM built-in Policy Manager allows configuration policy customization and a dashboard for drilling down into compliance by policy, asset group, asset, and individual policy element. Assessing for specific settings such as macro enforcement options is possible using the Policy Manager.

User Application Hardening

What you need to know

User application hardening concerns the configuration of web browsers to block (and ideally uninstall) Flash, ads, and Java on the internet. Web Browser settings should not be able to be modified, and Internet Explorer 11 should not be used to process content from the internet.

Why is it important?

In environments where web browsing is allowed, common attack vectors include malicious web pages, advertisements, and emails with infected attachments. Hardening user applications, such as hardening web browsers settings and removing an end users ability to change security settings can help reduce the risk associated with these vectors. Not using browsers known to be susceptible to internet-borne risks is also advised.

How do we help?

The InsightVM built-in Policy Manager allows configuration policy customization and a dashboard for drilling down into compliance by policy, asset group, asset, and individual policy element.

With the policy engine, your team has the ability to utilize best practices based on a multitude of built-in CIS benchmarks, and leverage a framework for creating complex vulnerability checks using a simple XML format. Additionally, InsightIDR's Attacker Behavior Analytics (ABA) can find malicious behaviors when they have been altered to evade policy configuration and prevention defenses.

Restrict Administrative Privileges

What you need to know

Administrator privileges should be restricted only to those who genuinely need them for privileged duties (for example, managing operating systems and applications, installing software, and implementing security patches). Additionally, they should be regularly revalidated and audited to ensure privileged accounts are not being used for activities like reading email and web browsing.

Account authorisation and access should also be controlled, with unprivileged accounts unable to login to privileged operating environments, as well as privileged accounts (excluding local administrator accounts) unable to login to unprivileged operating environments. Privileged accounts should also be prevented from accessing Internet email and web services. Controls should also be put in place to address organisational changes, such as staff turnover or movements in the organisation.

Why is it important?

Admin accounts are essentially the ‘keys to the kingdom.’ Threat actors will use these accounts to gain full access to company information and systems if accessed.

How do we help?

Managing user permissions is a critical process all organizations should be able to do quickly and effectively in order to respond to a variety of security threats. However, the reality is that most companies struggle with this process. InsightConnect, our security orchestration and automation solution, can eliminate the burden of manually managing user accounts in a variety of use cases, from provisioning and deprovisioning users to responding in the event of an incident.

Furthermore, InsightIDR not only provides real-time endpoint detection, but also injects fake honey credentials on your endpoints to deceive attackers. If this credential is used anywhere else on the network, such as with pass-the-hash, you'll be automatically alerted. Whenever you get an alert in InsightIDR, notable user and asset behavior is shown on a visual investigation timeline. Not only do you have the necessary context to make a decision regarding a user account, but you can take action directly from an investigation to contain the threat.

Authentication and auditing of user and administrative accounts is a large component of our User Behavior Analytics (UBA) in InsightIDR. These capabilities enable you to more easily determine whether a potential threat is an outside party pretending to be an employee, or an actual employee who presents some kind of risk. UBA connects activity on the network to a specific user, as opposed to an IP address or an asset. This means that if a user starts to behave in a way that's unusual or unlikely, even if it isn't flagged by traditional perimeter monitoring tools, you'll be able to spot the behavior quickly, determine whether it's anomalous, and start an investigation if needed.

For example, stolen credentials are a common attack vector used by penetration testers and real-world criminals alike. Whether the criminal obtains credentials via phishing attacks, malware, key logging, or even a third-party data breach, all they need is one correct username and password combination to work; once they're able to log in, they can silently move within a network undetected.

However, once an attacker is in, they usually start to act in ways unlike a normal user, such as by moving laterally between assets. The intruder moves from step to step in what's often called the "attack" or "kill chain," looking for increasingly interesting targets to raid and data to exfiltrate. The ability to baseline what kind of user behavior is normal on a network and what isn't is critical.

User Behavior Analytics provides you with the data to identify trends and easily spot outliers, so you can more easily and quickly identify and investigate potential threats and break the attack chain.

Patch Operating Systems

What you need to know

Operating systems are forever in need of patches to update and treat security vulnerabilities. Always look to patch and mitigate devices, including network devices, with known exploitable vulnerabilities within defined timeframes. Internet-facing services with exploitable vulnerabilities should be patched within 48 hours.

All other patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices should be applied within one month of release.

Never use unsupported versions, and aim to use the latest operating system version. To achieve this, vulnerability scanners should be used at least daily for public-facing assets, and at least fortnightly for all other workstations, servers and network devices.

Why is it important?

Security vulnerabilities in operating systems can be used to further the compromise of systems. Internet-facing devices with exploitable vulnerabilities are at a higher risk. Applying patches quickly is critical to ensuring the security of a system and the security of data that resides on the system.

How do we help?

Every network has assets more pivotal to the overall business than others and no business, even one with an army of analysts, has the time, especially during an emergency to determine where to start first. You just need to know now!

Rapid7 can assist with this requirement from a few different perspectives, starting with vulnerability management. Our InsightVM solution can identify your assets' operating systems and applications installed on them. Additionally, you can expand your reach into dynamic application security testing (DAST) with InsightAppSec; This is significant if you are developing in-house applications or are having applications developed for you by a third party.

Let us take deeper a look at how InsightVM and InsightAppSec can assist.

First, the robust tagging system in InsightVM lets you assign criticality tags to important systems, such as those that host PII or sensitive corporate data.

Second, our Real Risk score provides an actionable scale based on the exploitability and likeliness of an attacker exploiting the vulnerability in a real attack.

Third, our researchers' insights into the threat landscape and recent attacker methods are applied via Threat Feeds within InsightVM. This dynamic view shows you the threats that are most relevant to your environment.

InsightVM also automates the steps of aggregating key information, retrieving fixes for identified vulnerabilities, and ultimately, when appropriate or approved by a sysadmin, applies the patches via integration with your existing patch management systems. Upon completion, you can have InsightVM automatically re-assess impacted assets to verify successful patching.

The combination of business context via rich asset tagging, meaningful risk scoring, and integrated threat feeds from the perspective of an adversary enable you to better prioritise and protect against current, impending threats and react quickly to critical, named vulnerabilities in the application and operating system space.

Thirdly, Remediation Projects combined with Goals and SLAs assist in accelerating remediation tasks required to be performed, against what assets and by what team. This provides all of the required remediation information in a succinct spot and avoids timely manual analysis.

Goals and SLAs are defined based on criteria such that any exploitable vulnerability on an internet-facing host must be fully remediated within 48 hours of discovery. Real-time metrics will run on the platform and provide you with visibility of how you are tracking against those defined SLAs, allowing you to report against your organisation as a whole, as well as down to a team level.

Our Managed Vulnerability Management service takes the InsightVM technology and pairs it with expert guidance. Our experts' tailored recommendations help you manage, execute, and optimize your vulnerability management program. Not only does this allow you to offload day-to-day operations, but also lets you allocate people, time, and resources to other areas of security so you can reduce your risk exposure and strengthen your overall security posture.

Along with your dedicated Security Advisor, our team will handle the configuration, scanning, and reporting for you so that your team doesn't have to spend extra time getting trained or offloading other important initiatives. They act as an extension of your team, and your top priorities are theirs. All that's left for your team to take care of is the actual execution of remediation.

Multi-Factor Authentication

What you need to know

Multi-factor authentication requirements were updated (July 2021) to focus on the use of different types of authentication factors (e.g., something you know, something you have and something you are) rather than specific authentication factors (e.g., password, smartcard and fingerprint).

Why is it important?

Stronger user authentication makes it harder for threat actors to access or compromise sensitive government information and systems, even if the threat actor has a password.

How do we help?

Whilst Rapid7 is not a provider of multi-factor authentication technologies, we know a thing or two about detecting compromised credentials. InsightIDR includes User Behavior Analytics (UBA) to differentiate your users' normal activity from the suspicious, automated deception technology to identify unwanted user behavior missing from logs, and endpoint visibility to reveal lateral movement behavior which would be highly unlikely for a legitimate user.

InsightCloudSec, our Cloud-Native Security Platform, provides visibility of configuration elements for Public Cloud (AWS, Azure, GCP and more), including whether MFA is enabled for accounts accessing the cloud platforms, and in some instances whether MFA is configured for users accessing PaaS components.

Regular Backups

What you need to know

You should conduct regular backups of important new or changed data and software and configuration settings, stored disconnectedly. This has never been more important as threat actors become increasingly sophisticated with ransomware tools.

Backup requirements were updated (July 2021) to focus on performing and retaining backups in accordance with your organisation's own business continuity requirements, as opposed to specifying backup frequencies and backup retention timeframes. Emphasis should be placed on performing and retaining backups in a coordinated and resilient manner. Additional emphasis should be placed on the restoration of systems, software and important data from backups being regularly tested in a coordinated manner as part of disaster recovery exercises.

Why is it important?

To minimise the threat from ransomware and to ensure information can be accessed following a cybersecurity incident (e.g. a ransomware incident), backups are absolutely crucial.

How do we help?

The Insight cloud platform stores files using a secure, multi-tenant, and stateless microservices architecture within Amazon Web Services (AWS). This enables a secure, scalable cloud computing platform with high availability, offering flexibility for us to build a wide range of additional layers of security for data at rest, in transit, and in use.

On the Rapid7 side, our network infrastructure has redundancy, backup, and recovery capabilities. Our data centers have disaster recovery plans and their own risk assessments.

We take advantage of the automatic backup, redundancy, and high availability provided by AWS. On the Rapid7 side, we also do the same—our data centers have disaster recovery plans and their own risk assessments.

About Rapid7

With Rapid7 (NASDAQ: RPD), security and IT professionals gain the clarity and confi- dence they need to protect against risk and drive innovation Rapid7 analytics transform data into answers, eliminating blind spots and giving customers the insight they need to securely develop and operate today's sophisticated IT infrastructures, networks, and applications, Rapid7 solutions include vulnerability management, penetration testing, application security, incident detection and response, SIEM and log management, and offers managed and consulting services across its portfolio. To learn more about Rapid7 or get involved in our threat research, www.rapid7.com.