COMPLIANCE GUIDE

How to Proactively Manage Your Business's Security Posture

Rapid7's approach to the New Zealand CERT Critical Controls

TABLE OF CONTENTS

Introduction

Taking a proactive approach to your organisation'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 business mitigate cybersecurity incidents, the CERT NZ publishes a list of Critical Controls. This is a list of 10 controls that, once implemented, strengthen any organisation's security posture. The Critical Controls strategies provide a solid baseline for protecting your business from security breaches, as well as damaging malware. The costs of implementing these controls, along with the investment of staff training and upgrades, far outweigh the potential cost of a massive compromise.

CERT NZ's Critical Controls are designed to help you decide where best to spend your time and money. They have been developed based on data and insights CERT NZ received from reports and international threat feeds. The top 10 list of critical controls for 2022 includes two additional controls and one modified control compared to the top 10 in 2021.

- Additional Controls:
- Asset lifecycle management
- Implement application control
- Modified Controls

Application allowlisting control (or application whitelisting control) has been remodelled to provide less restrictive advice and encourage a wider adoption of this control.

Many of these fundamental controls start by identifying the assets in use by the business, because it's difficult to protect systems and infrastructure if you don't know they exist. This is why CERT NZ has added asset lifecycle management to the top 10 critical controls this year. Additionally, in order for application allowlisting to be effective, it must be implemented in tandem with other controls. For example, if an application has a vulnerability and it's allowlisted, this creates an easy path for an attacker.

Although changes have been made, and some controls removed from the top 10, all of the previous controls are still relevant, and implementation guides can still be found and referenced on the CERT NZ website.

[1] https://www.cert.govt.nz/assets/Uploads/documents/cert-top-10-critical-controls-2021.pdf

CERT NZ Critical Controls Strategies 2022

Outlined below are details of the NZ CSS 2022 strategies. We outline some of the basic requirements you need to know, why they're important, and how Rapid7 can help you.

Control 1: Patch your software and systems

What you need to know

A common tactic for attackers is to exploit known unpatched vulnerabilities in software that an organisation has not yet updated. Modern IT environments are complex, with interconnected components and software. Attackers take advantage of this interconnectedness to join multiple vulnerabilities together to get into business systems. To combat this, patching is critical to reduce the number of issues and vulnerabilities that could be used against you. One of the best ways to find these vulnerabilities is by using a vulnerability scanning solution.

Why is it important?

Fully patched applications are an essential foundation on which other security controls can be augmented. Every IT environment is unique, so there is no one-size-fits-all approach when it comes to patching. This is why it is critical to first understand what you have in your environment and how your organisation operates before you can decide how you deploy patches.

How do we help?

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 the applications installed on them, or in the case of containers, perform assessments on the container images and builds. It prioritises which systems should be patched first by assigning the "Real Risk Score" to an asset. This score combines our threat intelligence, exploit information, the ease of which the vulnerability can be exploited, and how business-critical the asset is to your organisation. We also enable you to track remediation efforts and define Goals and SLAs, which are critical for monitoring and reporting of the program's success. Real-time metrics run on the platform and provide you with visibility of how you are tracking against those defined Goals and SLAs, allowing you to report on your organisation as a whole, as well as down to a team level.

InsightVM also automates the steps of aggregating key information, retrieving fixes for identified vulnerabilities, and ultimately, when appropriate or approved by a sysadmin, applying 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 and show how your real risk has been reduced.

Our Managed Vulnerability Management service takes the InsightVM technology and pairs it with expert guidance. Our experts' tailored recommendations help you manage, execute, and optimise your vulnerability management program. Not only does this allow you to offload day-to-day operations, but it 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. All that's left for your team to take care of is the actual execution of the remediation.

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. InsightAppSec allows users to automatically assess modern web apps and APIs with fewer false positives and missed vulnerabilities. Understanding these application layer risks should be part of your vulnerability and risk management program. InsightAppSec goes beyond just the OWASP Top Ten to test for over 95 attack types and best practices. Users can also create custom checks to address issues and risks custom to your environment.

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.

Control 2: Implement multi-factor authentication and verification

What you need to know

There are multiple options when it comes to MFA, and some might not fit with how you and your employees operate. You should review the methods available, as some are better than others. Universal 2nd Factor (U2F) using physical security keys is recommended as best practice, as methods using one-time passwords (OTP) through a mobile app are vulnerable to phishing or social engineering, and OTPs sent by SMS are now considered deprecated by the information security industry.

Why is it important?

Stronger user authentication makes it harder for threat actors to access or compromise sensitive 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, our products support MFA for access. InsightIDR logs MFA activity and can detect compromised credentials by utilising User Behaviour Analytics (UBA) to differentiate your users' normal activity from the suspicious. Automated deception technology enables you to identify unwanted user behaviour, often revealing lateral movement behaviour, which would be highly unlikely for a legitimate user.

InsightCloudSec, our Cloud Security Posture Management solution, provides visibility into 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.

Control 3: Provide and use a password manager

What you need to know

Weak or reused passwords remain a common cause of incidents. A password manager is one of the few tools that can help your teams create unique passwords easily. It is a low-cost tool that can have a high impact and value when implemented well. Without a password manager staff typically don't use strong, unique passwords on all systems, which is why CERT NZ included this in the 2022 top 10 controls.

Why is it important?

Even with a password manager in place, strong, unique passwords are still important, and the tool needs to make this easy to increase the likelihood of your staff using strong passwords that are unique for each system. It also makes it easier to manage shared passwords such as your business's social media accounts.

How do we help?

Whilst Rapid7 is not a provider of password manager technologies, our products support password managers as well as MFA for access. InsightIDR can detect compromised credentials by utilising User Behaviour Analytics (UBA) to differentiate your users' normal activity from the suspicious. Automated deception technology enables you to identify unwanted user behaviour, often revealing lateral movement behaviour, which would be highly unlikely for a legitimate user.

Control 4: Configure Logging and Alerting

What you need to know

Often incidents reported to CERT NZ don't have enough detail to determine what happened, as important logs have not been retained. Storing and securing your logs in a central place is therefore an imperative. But enabling logs on everything may generate a lot of data and can become overwhelming. Trying to process this all by hand makes it hard to tell when there's a problem. Configuring central logging with built-in high fidelity alerts to notify you when key actions happen helps manage the noise, and ensures the detailed logs are still available when you need to look into them.

Why is it important?

Logs are a key part of understanding how an incident occurred and where the attacker gained entry. With that information, you can resolve incidents quicker, and get back to business as usual. Without logs enabled it can be harder to detect when an incident happens, or establish the full scope of the incident.

Having a central logging system which contains feeds from all your endpoints is the first step in having visibility into all activity in your environment. The second step is identifying key events that alert you to incidents, coupled with actionable alerts to let you know when something unexpected happens.

How do we help?

As a leading Security Operations Platform, Rapid7 provides central logging, built-in curated detections, and the ability to respond to identified alerts effectively, further enhanced with External Threat Intelligence capabilities.

InsightIDR

InsightIDR is our threat-focused Cloud SIEM, utilising Endpoint Detection and Response (EDR), User Behaviour Analytics (UBA), network traffic analysis (NTA), centralised log management, deception technology, and file integrity monitoring (FIM). It was listed by Gartner as a Leader in the 2021 Gartner Magic Quadrant for Security Information and Event Management. User Behaviour Analytics (UBA) is coupled with technologies like file and system honeypots to differentiate your users' normal activity from the suspicious, making identifying illegitimate users easier.

InsightIDR has been designed to enable organisations to rapidly detect and respond to cyber security incidents and breaches across physical, virtual, and cloud assets. Our agile, adaptable, cloud-native SIEM allows teams to get up and running quickly, while continuously improving their skills and capabilities as their maturity evolves. InsightIDR unifies critical security data in one place with lightweight data collection. It is powered by a robust library of curated out-of-the-box detections, infused with the expertise of our global managed SOC team and threat intelligence network unique to Rapid7. It learns from the environment so that it can quickly and confidently alert on abnormal behaviour and identify attacks early in the attack chain. InsightIDR's cloud benefits are impactful from the start. With a lightweight deployment of the Insight Agent, customers can deploy, baseline and reach a steady state in 1.5 months, compared to an average of 7 months with legacy SIEMs.

According to The Total Economic Impact™ Of Rapid7 InsightIDR, a 2020 commissioned study conducted by Forrester Consulting on behalf of Rapid7, customers experience increased visibility, decreased incident response time, and significant cost savings after switching to InsightIDR from their previous SIEM, translating to a 445% return on investment (ROI) over three years. (Read the full report here: https://www.rapid7.com/info/insightidr-roi/).

InsightIDR is priced by the total number of assets in your organisation. The standard subscription includes the storage of 13 months of logs, all of which are available for search, visualisation, and investigations. This is in deliberate contrast to data volume, events per second, or any other “consumption-based” pricing models. Our pricing is simple, transparent, and makes it easy for you to scale quickly with confidence.

Our Managed service (MDR) takes the InsightIDR technology and pairs it with expert guidance available 24/7/356. Not only does this allow you to offload day-to-day operations, but it 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.

InsightConnect

InsightConnect is our Security Orchestration, Automation, and Response (SOAR) solution. It increases the speed with which security professionals can identify risk and respond to incidents, and is used to connect disparate solutions to automate workflows. With a growing library of approximately 300 plugins to connect tools and easily customisable connect-and-go workflows, InsightConnect allows our customers to automate manual and tedious tasks while still leveraging their expertise when it is most critical, thereby saving time and improving efficiency.

IntSights

IntSights extends your threat landscape coverage by including external threat intelligence (ETI), providing additional business context that is laser-focused on your organisation’s digital footprint and the threat activity associated with it. As a result, ETI generates tangible value back to the business, and your security team, with actionable insights and security automation to neutralise the external threats that may be putting your organisation at risk. Similar to our SIEM vision, the IntSights vision is to make external intelligence instantly accessible for organisations of any type or size by synthesising complex signals captured from across the clear, deep, and dark web into contextualised, prioritised, and actionable intelligence.

With the IntSights Threat Intelligence Platform (TIP), you can proactively research malware, TTPs, and threat actors, and listen in on dark web chatter for up-to-the-minute details on what’s coming next for your organisation. Discover all the latest information on threat actors, campaigns, and MITRE ATT&CK Framework mapping from the cyber terms library and dark web search utility. This enables you to automate and streamline investigations via real-time visualisation into related malware, threat actors, and targeted campaigns.

InsightIDR leverages both internal and external threat intelligence. ETI is constantly being updated by our Threat Intelligence and Detections Engineering professionals and added to the platform in real time, including the latest threat actor activities. Their work is informed by Rapid7’s signature open-source projects, which improve security outcomes like no one else. Metasploit is the most impactful penetration testing solution on the planet, driven by a community of well over 200,000 users and contributors. Project Sonar regularly scans the public internet to gain insights into global exposure to common vulnerabilities, whilst Project Heisenberg has relationships with other internet-scale researchers and forums for collaboration and confirmation when new threats arise.

Detections are curated and constantly fine-tuned by our expert Threat Intelligence and Detections Engineering team. SaaS delivery means you always have access to the latest intel, with the knowledge that everything is vetted by our global MDR teams.

Control 5: Asset Lifecycle Management

What you need to know

You can’t properly implement security controls without first knowing what’s inside your environment and how it works.The intent of this control is for organisations to record, track, and maintain every system asset in the organisation. This includes software and hardware, as well as cloud-based systems that you use.

Why is it important?

Asset lifecycle management is a way to keep your view of your environment accurate and up to date. It tracks the software and hardware you have through each key stage - purchase or development, maintenance, and decommissioning. A critical part of this lifecycle is monitoring when a system goes from supported to legacy. Legacy systems are systems that a vendor no longer supports, or systems that an organisation no longer maintains, but still need for the business.

How do we help?

InsightVM uses a variety of asset discovery techniques to fingerprint the assets, including dynamic discovery, allowing you to discover and track assets without running a scan. The combination of these discovery techniques can often expose "Shadow IT." Dynamic discovery leverages technologies such as DHCP, Active Directory, VMware, AWS and Azure. It involves initiating a connection with a server or API that manages an asset's environment, such as the ones for virtual machines or containers. Once a system is verified as alive, or running, InsightVM scans the asset to collect information about services running on the asset.

InsightVM can identify unsupported operating systems or obsolete software in the environment, including newly vulnerable versions of applications like Log4Shell, by determining whether the JNDILookup class removal mitigation for Log4Shell has been applied to Log4j JAR files rather than just the version number.

InsightVM integrates with ServiceNow CMDB, enabling users to tag assets based on configuration items. It creates and updates CI data based on what was discovered, including risk metrics, and manages InsightVM site scopes based on CI data. You can find more information here: https://www.rapid7.com/partners/technology-partners/service-now/cmdb-insightvm/

Control 6: Implement and Test Backups

What you need to know

Backups have never been more important, as threat actors become increasingly sophisticated with ransomware tools. Restoration of your data is always preferable to paying the ransom. You should conduct regular backups of important new or changed data, software, and configuration settings and store these disconnectedly. Backups therefore need to be tested frequently and in different ways. During an incident is not the time to find out that your backups are not usable. You need to consider how long you want to retain your backups and whether there are any regulatory compliance mandates around them.

Why is it important?

Most organisations these days are reliant on their systems and the data they hold. Significant disruption to the availability of this data can be devastating, whether it was caused by a cybersecurity incident or a simple accident. In these situations, being able to restore from backup quickly makes all the difference. Ransomware attacks are often highlighted in CERT NZ's quarterly reports, because they happen regularly and have significant impacts to an organisation. Backups can reduce those impacts and allow your organisation to restore the lost data in the most cost-effective way.

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 centres 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 centres have disaster recovery plans and their own risk assessments.

Control 7: Implement 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 preventing the execution of unapproved/malicious programs or installers, including .exe, .dll, and scripts like Windows Script Host, PowerShell, and HTA.

Why is it important?

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

How do we help?

Whilst Rapid7 is not a provider of application control technologies, when an application whitelisting tool is implemented, you can send its logs to the InsightIDR platform for analysis and alerting. 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.

InsightVM has a custom policy builder. For example, it can check to ensure that the systems are set up to prevent users from changing installation options that may bypass security features, search for the presence of software such as application whitelisting tools, and examine and report on system configurations.

Additionally, we investigate a constant stream of attacker behaviour through the Metasploit Community, penetration testing, red teaming, and our 24/7 Managed Detection and Response service. As part of the investigative process, our analysts directly contribute Attacker Behaviour Analytics (ABA) detections into InsightIDR, paired with recommendations and adversary context.

Control 8: Enforce the principle of least privilege

What you need to know

The principle of least privilege means only granting users the minimum level of access they need to perform their job. This reduces the ability of an attacker to move laterally across the organisation, even if they manage to steal a user's account credentials. Additionally, all administrative actions need to be logged to identify any suspicious or abnormal behaviour.

Be especially critical of giving out administrative access. It's OK to ask these users why they may need those permissions and what tasks they need to perform. Instead of giving your CIO administrator access to keep an eye on things, configure alerts and reports so they can monitor use of administrative actions.

Why is it important?

Administrative 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, but 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, regardless of whether the assets are on-premises or in the cloud.

Authentication and auditing of user and administrative accounts is a large component of our User Behaviour Analytics (UBA) in InsightIDR. UBA connects activity on the network to a specific user, as opposed to an IP address or an asset, and by querying LDAP will determine privileged users, allowing their actions to be more closely monitored. This means that if a user starts to behave in a way that's unusual or unlikely, you'll be able to spot the behaviour quickly, determine whether it's anomalous, and start an investigation if needed. InsightIDR can also inject fake honey credentials on your endpoints to deceive attackers and quickly identify if these credentials are being used anywhere, such as in a pass-the-hash exploit. Whenever you get an alert in InsightIDR, notable user and asset behaviour 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.

Control 9: Implement network segmentation

What you need to know

Network segmentation involves breaking down your network into smaller segments and implementing access controls to manage the connections between them. It only works if network traffic is blocked by default and allowed as necessary.

Why is it important?

Without effective network segmentation, attackers can move around your network and gain access to additional systems. Implementing network controls limits an attacker's access once they enter your network.

How do we help?

InsightIDR detections leverage the real-time user and endpoint data collected by the agent on a host and sent directly to our InsightCloud platform, regardless of the assets network location. InsightIDR also understands your network zones and can create a zone violation alert if a user accesses a network they do not normally access, or are not meant to access. This gives your organisation the alert fidelity you want, filled with the context you need if an adversary outsmarts your network segmentation implementation.

Control 10: Set Secure Defaults for Macros

What you need to know

Macros are small programs that can be run in office productivity software, like Microsoft Office.

If your business uses Microsoft macros, you can configure the settings to be more secure by default by blocking macros from the internet and allowing only vetted macros, either from trusted locations with limited write access, or digitally signed with a trusted certificate. Forcing macros to run in a sandbox will reduce their impact and reach within your network.

If your business does not use Microsoft macros, disabling them entirely can protect you from this type of attack.

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?

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.

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 Behaviour Analytics (ABA) detections in InsightIDR, which can find malicious behaviours such as malicious macro execution and perform containment actions, such as kill process, quarantine asset, and disable users.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight platform. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behaviour, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organisations. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.