theta

SECURITY IMPROVEMENT SERVICE

A managed security solution:

Let us safeguard your organisation so that you can focus on your goals.

theta

CONTENTS

theta

WE WILL **HELP SECURE YOUR ORGANISATION**

Not every organisation has a team of security experts or a dedicated CISO.

You know you have a responsibility to secure your systems and protect your customers' data, but you are constantly fighting fires and have no time to be proactive.

Your Board is asking for your plan to mature your organisation's cyber security posture, but you don't really know where to start.

Theta's Cyber Security team is here to help.

theta

OUR SPECIALISTS

>> We are a consultant-led team of skilled and certified experts with experience in delivering security outcomes in a broad range of NZ public and private organisations.

>> We are familiar with delivering solutions aligned to appropriate security frameworks such as NIST, NZISM, ISO27001, Essential8, OPC Privacy Impact Assessment, CertNZ Top10 and the CIS controls.

>> Our team has a wide range of security, networking, and technology skillsets that can be leveraged to inform and deliver efficiently and effectively.

>> We are passionate about helping New Zealand companies of any size, small or large, to reduce risk and improve resiliency in the most cost-effective way that aligns with business priorities and budgets.

theta

KEY DETAILS

>> Our Security Improvement Service is the result of our Cyber Security team's collective knowledge and experience that we have gained from our interactions with customers over the years.

>> We have great insight into New Zealand businesses' security challenges and leverage this knowledge to deliver a practical service to help customers mature their cyber security processes and improve their cyber resilience in the face of an increasingly complex threat landscape.

>> With our help, your cyber security will be under control and constantly improving to meet modern threats. Your business will be supported by expert security leadership, and your team augmented by a large pool of skilled technical resources as you need them.

theta

Our service is designed to be adaptive to your needs through a

CONTINUOUS IMPROVEMENT FRAMEWORK

theta

1. IDENTIFY

Using established processes, we will work with you to understand your current state and identify gaps and areas that need to be addressed.

1. IDENTIFY

Critical System Review

Also known as a 'Crown Jewels' assessment.
Identify your key systems and build an operational view of everything you need to know – backups, dependencies, vendors, resilience, and continuity.

Risk Assessment

After identifying your 'Crown Jewels', we'll work with you to complete a risk assessment to determine the potential threats that could affect your operations and the impact of an event occurrence, as well as document opportunities for remediation and mitigation.

Privacy Impact Assessment

Leveraging the Office of the Privacy Commissioner's Privacy Impact Review process, our experts will look at any systems containing sensitive data and provide recommendations and actions required to ensure data protection that meets regulatory requirements and keeps your customers' information safe and secure.

Attack Simulation

Utilising advanced specialist tools, we will simulate real-world cyber threats by applying the latest techniques, tactics, and procedures (TTPs) used by adversaries. Our comprehensive approach identifies potential vulnerabilities within your systems and provides a detailed report outlining security gaps. We also offer actionable recommendations on implementing enhanced tools and processes to strengthen your defences and ensure robust protection.

Cloud Reviews

Whether it's AWS, Azure, or Google Cloud, everyone uses some cloud infrastructure to run their business today. Cloud computing is vast and can be complex to secure - we will review the configurations in place and recommend required configurations to make your cloud environments more secure.

External Attack Surface Monitoring

Leveraging Theta's Glasstrail product, we help you gain visibility of your external attack surface, encompassing internet-facing systems, web applications, network infrastructure, and public-facing services to identify potential vulnerabilities and weaknesses within the company's external-facing systems, applications, and infrastructure that malicious actors could exploit.

The assessment aims to enhance your organisation's understanding of its security posture from an external perspective and develop appropriate measures to mitigate potential risks, thereby enhancing the overall security of its external-facing assets.

Cyber Security Framework Assessments

Depending on your organisation, there may be a regulatory requirement to align to a security framework such as NZISM, ISO 27001 or the New Zealand Privacy Act. Our team will align your roadmap and plan to a set of framework controls that allow you to demonstrate compliance.

Networking Review

We find that customers invest in some great networking hardware but only use some of its capabilities. Our team can help you improve the security benefit of your current networking and firewall investment. Or maybe it's time for an upgrade, and you are ready to understand why your Wi-Fi generates too many support calls. We'll take a look and advise you on how to improve the user experience on your network.

Design and Architecture Review

Moving to the cloud, changing cloud providers, building landing zones, and changing existing infrastructure can all introduce new security risks. We can complete an external review of your plans to ensure they consider and mitigate risks as you plan the change.

Identity and Access Reviews

On-premise Active Directory user accounts are challenging to secure and monitor; however, with identity as the new security perimeter, they are critically important to protect. We can run an initial assessment to understand the risks and misconfigurations impacting your domain accounts and provide an ongoing monitoring service to identity potentially malicious changes as they happen.

Secure Coding Review

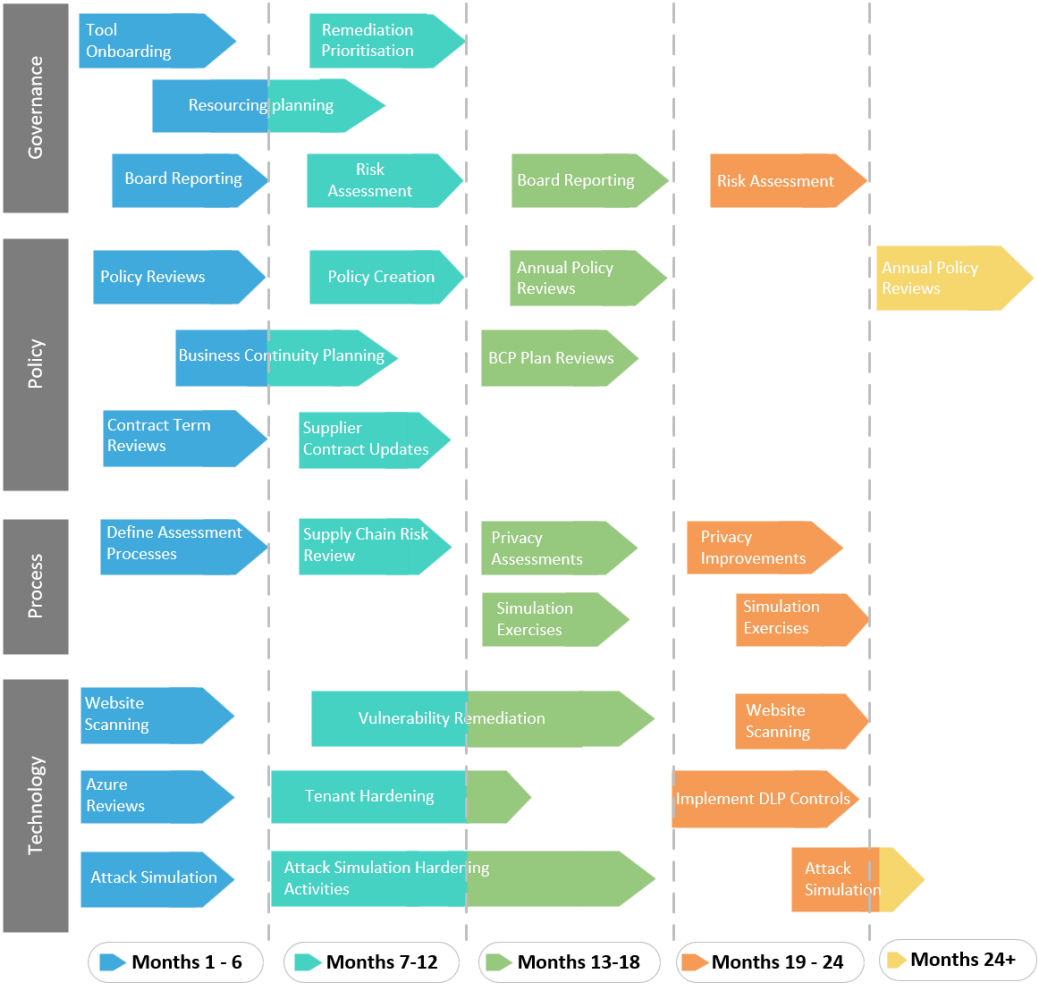
We'll spend time with your development team, understanding how they follow secure coding standards and guidelines. We'll also review the software architecture and design process, check how security considerations are integrated into the design phase, and review your lifecycle management processes, including version control systems, testing procedures, deployment, software updates and patching. The goal of this review is to identify potential security risks in the software development lifecycle and to recommend improvements to enhance the security of the software development process in a collaborative and constructive manner.

theta

2. PLAN

Whether you have immediate needs based on customer requirements or regulatory obligations or are looking to align with a security standard, we will work with your team to build a cyber security roadmap to strengthen, remediate, and mature your security posture.

EXAMPLE CYBER SECURITY
STRATEGIC ROADMAP



theta

3. EXECUTE

Once the plan is agreed upon, we are ready for action! Our team can deliver on a wide range of activities to build resilience as required through the defined and agreed-upon roadmap.

theta

3. EXECUTE

Our team will work with you to extract the greatest possible benefit from your current technology by maximising the efficiency of your tools and improving your security processes.

Technical subject matter experts from the wider Theta business can be consulted as needed to provide guidance on architecture, design, and specialist systems.

3. EXECUTE

Policy Development

Influencing change can be challenging without the right policies in place. Policy development will need consultation with the right stakeholders to achieve successful adoption throughout your business. Through a collaborative and iterative process, we will help you build practical security policies tailored to align with your regulatory requirements and workforce.

Supply Chain Vetting

We will work with you to implement tools and processes so that you have better visibility of the risks in your supply chain. We can also help develop a vendor vetting process, ensuring that applications, systems, and integrations are reviewed, vetted, and approved for use in your environment.

Contract Reviews

It's important that all vendor contracts are reviewed and updated to clearly communicate their contractual requirements to protect sensitive data in their systems so you can meet the stipulations of the New Zealand Privacy Act and the New Zealand Health Information Act 2020. We will help guide you through the changes required.

Security Awareness Building

Building your employees' skills and awareness is an instrumental part of protecting your business and building resilience. Our team is passionate about sharing their knowledge—we can provide customised, in-person training or automated training tools to meet your needs.

Business Continuity Planning

Putting together a practical BCP plan and Incident Response Plans can be daunting. We'll help you get started and ensure the important elements of an effective business continuity plan are captured and documented – just in case. We will then run through simulations with your team regularly and update your plans with the learnings.

Business Continuity Testing

We will design and run through tabletop exercises with you to get a good feel for what needs tuning for your Business Continuity plan to be effective. Each simulation exercise will cover a different scenario, e.g., a security breach or a ransomware scenario, and involve various aspects of your business. After each test, post-incident reviews will be completed, and an improvement plan will be developed.

Cyber Security Board Reporting

When it comes to cyber security, an informed and engaged Board is critical. We can help develop an effective communication plan for ongoing updates to your executive team and Board, so they know the risks currently impacting your business and can track remediation.

theta

4. REVIEW

Security work is never done.

It is important to regularly review whether the controls you have in place are effective, whether your tools and processes are still relevant, and whether you are adapting against ever-evolving threats.

theta

4. REVIEW

We will track progress and re-assess your risks to identify and plan the next phase of continued improvement.

Let’s get your cyber security sorted.

theta

For more information, get in touch.

enquiries@theta.co.nz
0800 4 THETA