Implementing Australia's Six Shields of Cybersecurity

A Guide for CISOs and IT Security Directors

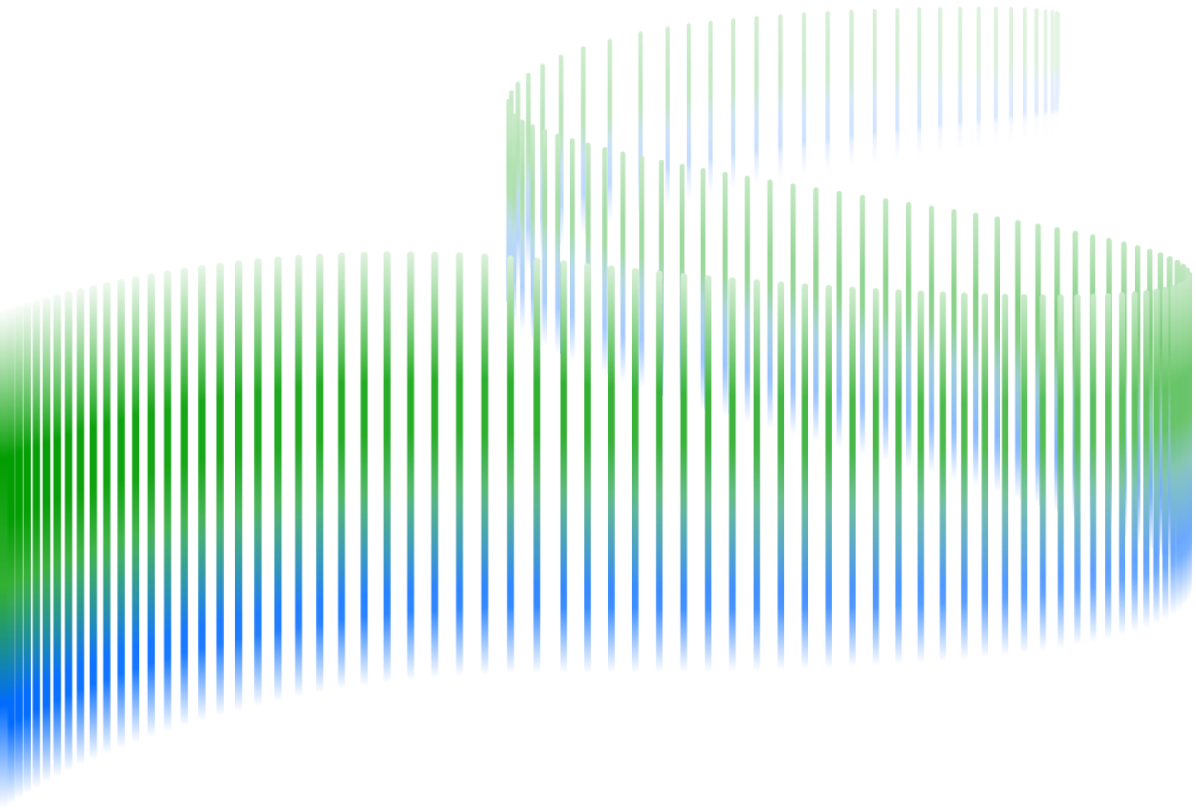

Table of Contents

Introduction

Cybercriminals aren't letting up. Whether they're using known exploits or new techniques, they're relentlessly testing the defenses of Australian businesses, governments, and critical infrastructure providers. When they succeed, the consequences are serious—compromised data, financial loss, legal headaches, and long-term damage to trust.

You've likely been doubling down on layered security for years, applying defence-in-depth strategies to protect what matters most. But as adversaries adapt, so must our understanding of what strong security looks like.

The Australian Government's new six cyber shields model is the latest framework guiding this evolution. It blends legislative, policy, and technology to define what's needed to build cyber resilience across the country.

While it's still early days, one thing is already clear: Visibility and threat detection are essential to meeting several shield requirements.

To adopt the model effectively, your organisation needs three things:

1. A deep understanding of every entry point attackers might target
2. The ability to quickly detect and respond to a wide range of threats using AI and machine learning (ML)—with fewer false positives
3. Clear, actionable intelligence that helps you continuously assess and improve your security posture

This white paper is for cybersecurity leaders ready to meet the initial requirements of the six cyber shields today and build a flexible foundation that can adapt to what's coming next.

Background

Since 2020, Australia has faced a surge in high-profile ransomware attacks, many targeting organisations that handle sensitive data. These aren't isolated incidents. They've triggered a national shift in how we think about cybersecurity policy and readiness.

The numbers tell the story. Over the past two financial years, the Australian Signals Directorate (ASD) was called in to help with more than 1,100 serious incidents. During FY24, Australians reported over 87,400 cybercrimes and two-thirds of the population were affected by a cyber incident or data breach in just 12 months.

This relentless wave of attacks has pushed cybersecurity to the top of the executive and Board agenda. We're seeing significant investments in operations, technology, and talent, but also a growing realisation that the nature of the threat has changed. It's no longer just about defending against individual attacks. It's about building lasting resilience across the entire organisation—and the country.

When a cyberattack hits, the impact can be devastating. You risk losing intellectual property, trade secrets, customer data, and the technologies that give you a competitive edge. Recovery isn't just technical; it's financial and reputational. Restoring systems can take weeks or even months, and cost millions. But regaining customer trust and market position is often the harder battle. Some organisations never recover fully. For them, a major incident does more than disrupt business; it ends it.

That's why every organisation, regardless of size or sector, needs a strong cybersecurity foundation—one that proactively detects threats, responds in real time, and adapts to emerging threats.

Clear guidance on cybersecurity standards isn't new, but until now, it's only applied selectively. Critical infrastructure operators have faced legislative requirements. Federal agencies follow the Protective Security Policy Framework (PSPF). And many private sector firms have acted to meet insurer demands just to maintain coverage.

The six cyber shields model changes the game. For the first time, Australia has a single, unified standard that applies to every organisation and defines the baseline for cybersecurity protections across the board.

History and Context for Australia's Six Cyber Shields Model

Australia is now developing its fourth national cybersecurity strategy. Building on earlier versions from 2009, 2016, and 2020, the latest strategy spans eight years—through to 2030—and is structured around three distinct time horizons.

Each strategy has shared common goals: stronger public-private collaboration, better threat intelligence sharing, and a focus on cyber skills and education. But what's changed over time is the urgency—and the scale—of action required.

That evolution reflects a hard truth: Today's cyberattacks are faster moving, more sophisticated, and harder to contain than ever. Attackers are moving faster. Incidents are more damaging. And defenders must break the cycle of reacting late and rebuilding slowly.

In response, the Australian Government has outlined a new vision: one where every organisation plays a part in lifting the nation's overall cybersecurity posture. If every business improves its capabilities, the collective result is a stronger, more resilient Australia.

To get there, organisations must first review their existing layers of defence. Then they must be ready to augment or modernise those layers to meet a new national baseline: the six cyber shields model.

This model outlines six key areas—or "shields"—that form a cumulative defence against today's threat activity:

1. Strong businesses and citizens
2. Safe technology
3. World-class threat sharing and blocking
4. Protected critical infrastructure
5. Sovereign capabilities
6. Resilient region and global leadership

Each shield is backed by targeted actions designed to strengthen it. Some of those actions are now legally required, thanks to Australia's first Cyber Security Act and recent amendments to the Security of Critical Infrastructure (SOCI) Act, passed in late 2024. But legislation alone doesn't build resilience. It's the actions that follow—at both government and organisational levels—that matter.

Other actions fall outside legal mandates. These represent best practices that reflect good cyber hygiene. You may already be doing some of them, but now is the time to assess whether your efforts meet or exceed the minimum standards set by the shields.

A third category of actions is still to come. The strategy runs through 2040 and is designed to adapt as cyber risks change. While the early focus is on ransomware and intelligence sharing, the Cyber Security Act is designed to expand, allowing future governments to tackle new threats as they emerge.

What does this mean for you? Two things:

1. You need full visibility into which actions—legislated or otherwise—apply to your organisation right now.
2. More importantly, you must build flexibility into your security infrastructure. It's not enough to meet today's requirements; you need to be ready for what's next.

Minimum Measures Regarding the Six Cyber Shields

Shield 1: Strong Businesses and Citizens

The first shield sets the foundation: Cybersecurity is everyone's responsibility. The goal is to raise the national baseline for cyber hygiene, making individuals and businesses harder targets and better prepared to recover quickly when incidents occur.

Specific actions include:

- A free, tailored cyber health check program for small- and mid-sized businesses (SMBs)
- Mandatory, no-fault ransomware reporting to build threat visibility
- The Counter Ransomware Initiative, which discourages ransom payments (without prohibiting them)
- Expansion of the Digital ID program and the National Strategy for Identity Resilience to reduce how often people share sensitive personal information online

Practical Insight

This shield reflects a shift in how we think about security operations. Detecting a threat isn't the finish line; it's the first step in helping your organisation return to a secure, stable state after an incident.

How Exabeam Helps

Strengthening Cyber Resilience

Exabeam behaviour analytics uncovers threats traditional tools miss, like compromised insiders, ransomware, or unusual activity that signals an attack in progress. Using user and entity behaviour analytics (UEBA) to learn what normal looks like in your environment, Exabeam can quickly flag when something's wrong.

With automated, risk-based prioritisation, your team knows exactly where to focus—especially valuable for SMBs that may lack deep cyber expertise or resources.

Accelerating Incident Response

Exabeam uses ML and AI to automate threat detection, investigation, and response (TDIR) workflows. That means faster containment, fewer disruptions, and less time spent firefighting.

If ransomware or cyber extortion attacks strike, Exabeam helps your team map the full attack chain, isolate impacted systems, and take decisive action to contain the threat before the damage spreads.

Built-In Health Checks

Exabeam is the only vendor with an outcomes-based approach that includes automated health checks. You get clear visibility into how your defences stack up against frameworks like MITRE ATT&CK®, along with specific recommendations to improve configuration

These health checks reduce the burden on your team, so you can focus on meeting the shield's ransomware-related requirements and strengthening your security posture without guesswork.

Shield 2: Safe Technology

This shield sets the stage for a future where digital products are secure by design, not just secure by patch. Australian organisations are beginning to adopt secure-by-design principles across their engineering environments, building systems that are harder to exploit and better at protecting data from day one.

It's the early phase of a broader national mandate aimed at one goal: to "ensure Australians can trust their digital products and software" and the companies that build them.

Specific actions include:

- Legislating a mandatory cybersecurity standard for Internet of Things (IoT) devices
- Introducing a voluntary security labelling scheme for consumer-grade smart devices
- Reviewing data retention practices to reduce unnecessary risk from long-term data storage
- Investigating the data brokerage industry and its role in selling sensitive data to malicious actors

Practical Insight

Most organisations still deal with blind spots: unmonitored applications, insecure devices, or overlooked misconfigurations. This shield calls for a modern, proactive approach to vulnerability management, powered by automation and continuous visibility.

How Exabeam Helps

Securing Emerging Technologies

As you adopt IoT, AI, and hybrid cloud environments, Exabeam ensures these systems are monitored in real time for anomalies. Whether your infrastructure is on-premises, in the cloud, or both, Exabeam gives you the visibility to detect misconfigurations, unusual activity, and emerging threats before they become breaches

For IoT devices and connected devices, Exabeam spots abnormal patterns in device behaviour, reducing the risk of exploitation in environments often overlooked by traditional tools.

Turning Threat Intelligence Into Action

The Exabeam New-Scale and LogRhythm SIEM Platforms support the STIX/TAXII standard, allowing you to bring in any paid or open-source threat intelligence feed, whether from Information Sharing and Analysis Centers (ISACs), industry partners, or government sources. This flexibility gives your team access to the data it needs for high-fidelity threat detection across your environment.

But it doesn't stop at ingestion. Exabeam analyses and operationalises that intelligence in real time, helping your security team find poorly secured digital products, flag risky behaviours, and act before attackers can take advantage.

Enabling Secure-by-Design Practices

Exabeam helps developers and security teams identify vulnerabilities early by analysing system logs and software behaviour during development and deployment. This supports a true secure-by-design model and aligns directly with the shield's goals of protecting software and data from the inside out.

Shield 3: World-Class Threat Sharing and Blocking

Real-time, two-way threat intelligence sharing between government and industry has been a national priority for years. With the third shield, those efforts are being scaled up. Continuous streams of threat intelligence are essential for today's security teams. You need fast, actionable insights about threat actors and emerging risks to respond effectively.

Specific actions include:

- Forming a government-industry Executive Cyber Council to share strategic threat intelligence
- Expanding the ASD's threat-sharing platform through a dedicated Acceleration Fund
- Developing automated threat-blocking capabilities through the National Anti-Scam Centre

Practical Insight

Speed matters. The longer a threat stays undetected, the greater the damage. To act quickly, you need machine-readable intelligence that feeds directly into your security tools, where it can be analysed and blocked in real time, without relying on human intervention.

How Exabeam Helps

Exabeam uses behaviour analytics to distinguish between normal and suspicious activity in your environment. This gives you a powerful, automated way to spot threats early and block them before they escalate, especially when combined with ML, AI, and generative AI (GenAI) to reduce manual effort and improve accuracy.

Exabeam delivers real-time threat sharing and blocking in three key ways:

Automated Threat Intelligence Sharing

The New-Scale and LogRhythm SIEM Platforms support the STIX/TAXII standard, enabling you to ingest any paid or open-source intelligence feed—from government sources, ISACs, or commercial providers.

Once ingested, Exabeam processes and correlates that data in real time, delivering high-fidelity threat detection and helping you align with key regulatory frameworks.

Government and Industry Collaboration:

Exabeam supports a Common Information Model (CIM), developed with global cybersecurity partners, to transform logs into normalised, actionable security events. This structure helps teams ingest threat data faster, analyse it more effectively, and take action at machine speed.

The New-Scale Security Operations Platform—sold as Exabeam Fusion—automates TDIR workflows, turning shared threat intelligence into tangible results.

Exabeam also contributes to the ATT&CK framework, sharing insights into attacker tactics and techniques seen in real-world scenarios. That contribution strengthens global threat awareness and keeps your team aligned with emerging best practices.

Threat Blocking at Scale

Exabeam integrates with your existing security investments, including firewalls, endpoint detection and response (EDR) tools, and network gateways, to automatically block known bad IPs, domains, and file hashes.

With built-in security orchestration, automation, and response (SOAR) capabilities, both the New-Scale and LogRhythm Platforms can execute playbooks and block malicious actions in real time, cutting off attacks before they can spread.

Shield 4: Protected Critical Infrastructure

Planning, preparation, and practice are essential to effective incident response. After a series of high-profile attacks targeting critical infrastructure, Australia has taken steps to strengthen its national cyber resilience, starting with clearer definitions of critical sectors and new obligations for the organisations that operate within them.

The government is also investing in real-world readiness through sector-specific tabletop and operational exercises. These simulations help industry and government improve coordination, identify gaps, and refine joint responses before a real crisis unfolds.

Specific actions include:

- Shifting telecommunications security regulation from the Telecommunications Act 1997 to the Security of Critical Infrastructure Act 2018
- Pressure-testing critical infrastructure through a National Exercise Program
- Developing standardised incident response playbooks

Practical insight

If your organisation plays a role in delivering essential services, you need more than good tools; you need muscle memory. Tested plans, real-time visibility, and coordinated response playbooks are now baseline requirements. These playbooks guide fast, consistent action during an incident and help you maintain regulatory compliance by ensuring your responses are properly executed and documented.

When integrated with SOAR tools, playbooks can go even further, enabling fully automated responses with minimal human intervention. Exercises, simulations, and automation should be core parts of your ongoing response readiness strategy.

How Exabeam Helps

Monitoring Critical Systems

Exabeam delivers continuous monitoring across critical infrastructure networks, flagging abnormal behaviour—whether caused by insider threats, supply chain compromises, or unknown actors—before it can disrupt operations.

Using UEBA, Exabeam establishes behaviour baselines across users, devices, and applications. When activity strays from the norm, your team gets alerted quickly.

Incident Response Readiness

Exabeam includes prebuilt incident response playbooks aligned with the Australia's national strategy. These playbooks support rapid, consistent action during incidents and are ready to be tested to evaluate and improve your preparedness.

For systems designated as Systems of National Significance (SoNS), Exabeam also helps you meet mandatory reporting and cyber risk management requirements with precision and speed.

Threat Hunting for Resilience

Exabeam empowers your team to hunt down threats before they escalate. You can investigate anomalies, validate risks, and act on indicators of compromise (IoCs) early, building true resilience into your core infrastructure.

Shield 5: Sovereign Capabilities

Australia's cybersecurity workforce has long faced two major challenges: a shortage of skilled professionals and the high cost of attracting and retaining talent. With sectors competing for limited expertise, the gap continues to widen.

To close it, the government is investing in education, professional development, and local industry innovation, ensuring Australia can build and sustain its own cybersecurity capabilities well into the future.

Specific actions include:

- Improving education and training systems in partnership with Jobs and Skills Australia and the Jobs and Skills Council
- Promoting cybersecurity careers across primary, secondary and tertiary levels
- Accelerating investment in domestic cyber industry and research programs

Practical Insight

CISOs and security leaders have a unique opportunity—and responsibility—to build teams that can grow with the pace and complexity of modern cyberthreats. That means cultivating a culture of continuous learning, giving analysts access to the right data and tools, and empowering them to act with context and confidence. When you align training, automation, and collaboration, you create defender-first security operations built to last.

How Exabeam Helps

Cyber Workforce Uplift

Exabeam simplifies TDIR with automated workflows, making it easier for newer team members to hit the ground running. Built-in GenAI capabilities accelerate insights, offer recommended next steps, and guide junior analysts toward the thinking of more experienced team members.

With intuitive dashboards and hands-on tools, Exabeam supports the development of foundational TDIR skills across Australia's emerging cyber workforce, aligning directly with the national strategy's focus on professionalisation.

Supporting Australia's Cyber Industry

Exabeam partners with local cybersecurity, developers, integrators, and service providers to support sovereign innovation and enable the creation of home-grown solutions.

Our platforms also play a role in training and education. Exabeam supports learning environments with realistic TDIR workflows and hands-on simulations, including a Capture the Flag (CTF) experience where participants face real-world scenarios in red team/blue team exercises. These exercises teach the concepts, but they also highlight the simplicity and effectiveness of the Exabeam user experience.

Shield 6: Resilient Region and Global Leadership

Australia can't go it alone. Cybersecurity is a shared global responsibility, and while national resilience is the priority, regional cooperation is critical. Through the six shields model, Australia is stepping up as both a leader and model nation, using this framework to strengthen domestic defences, lift cyber capabilities across its neighbours, and deepen international partnerships.

Specific actions include:

- Establishing a regional cyber crisis response team across the Pacific and Southeast Asia
- Using private sector innovation to improve regional cybersecurity
- Deploying all arms of statecraft to deter and respond to malicious actors

Practical Insight

Leadership in cybersecurity doesn't come from policy alone. It's earned through sustained action and adaptability. As a CISO or security leader, your strategy must evolve with changing threats, technologies, and regulations. AI is already reshaping how organisations detect and respond to threats. That trend will accelerate, but so will adversaries. Staying ahead means investing in tools, partnerships, and intelligence that extend beyond your own network.

How Exabeam Helps

Global Threat Coverage

Exabeam integrates threat intelligence from international sources, helping Australian organisations detect and respond to international cyberthreats with global origins. This visibility is essential for staying ahead of rapidly evolving tactics used by well-funded, globally dispersed adversaries.

Exabeam also supports alignment with global security frameworks and regulatory mandates, positioning your organization—and Australia—as a trusted partner in international cyber cooperation.

Building Regional Resilience

The Exabeam Platforms can be deployed across regional partners and neighbouring countries, strengthening joint threat detection and response capabilities. This aligns directly with Australia's goal of improving cybersecurity across the Indo-Pacific and reducing vulnerabilities that adversaries could exploit across borders.

By enabling threat intelligence sharing and collaborative response workflows, Exabeam helps disrupt transnational cybercrime and improve collective resilience.

Upholding International Standards

Exabeam solutions have successfully completed the Information Security Registered Assessors Program (IRAP) assessment at the Protected level. They also align with global cybersecurity standards, ensuring your organisation meets both national compliance expectations and international benchmarks.

Conclusion

The six cyber shields model introduces a clear, national cybersecurity standard: one that every Australian organisation is now expected to work toward. Meeting these requirements is about compliance, but it's also a critical step toward helping Australia become more resilient to cyberthreats by 2030.

You don't need to overhaul your entire security environment to align with the model. But you do need to make smart, deliberate choices about the tools you use, especially around TDIR. With the right capabilities in place, you can meet today's obligations and stay ready for tomorrow's evolving requirements.

The Exabeam New-Scale and LogRhythm SIEM Platforms align with all six shields in the 2023–2030 Australian Cyber Security Strategy. They provide prepackaged support for a wide range of cybersecurity use cases, enabling compliance with today's ransomware-focused mandates and preparing you for future government priorities.

By strengthening threat detection, automating incident response, and fostering collaboration across government, industry, and the region, Exabeam helps forward-thinking organisations do more than meet the standard—it helps them lead.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam™

Learn more at
www.exabeam.com →