

CAPABILITIES OVERVIEW

Assess

Protect

Monitor, Detect & React

Assure

EMAIL CYTHERA
sales@cythera.com.au

PHONE CYTHERA
1300 298 437



OVERVIEW

Cythera was founded by IT industry veterans in late 2018 to solve the real problem of protecting Australian businesses from cyber threats. Since inception, Cythera has built and delivered affordable, turnkey, managed security solutions that encompass the very best cloud delivered, or software-based security platforms bundled with expert, Australian based security analysts to monitor, detect and respond to common and emerging cyber-threats.

Cythera's cyber security solutions allow for the rapid deployment of **Assessment, Protection, Monitoring, Response** and **Assurance** services to protect Australian businesses.

Let's face it, cyber-security is a complex, highly specialised field. To protect any business against cyber threats you must have the right mix of protective technology, threat monitoring and proactive response capabilities to make sure the bad guys are kept away. All this takes plenty of technology, skilled resources, and money to make possible. To make this simpler, Cythera has built a business focused on delivering cyber security outcomes, using the very best security technology, proactive managed security services, all consumed on a month-by-month basis for an affordable price so our clients can focus on what they do best - running their businesses.

At Cythera, we call this **business-as-usual.**

TOP INDUSTRIES TO NOTIFY DATA BREACHES:

- HEALTH SERVICES
- FINANCE
- PROFESSIONAL SERVICES
- EDUCATION
- INDUSTRIAL
- MINING

71% OF DATA BREACHES AFFECTED BUSINESSES WITH LESS THAN 300 PEOPLE*



ASSESS

41% OF BREACHES CAUSED BY HUMAN ERROR*

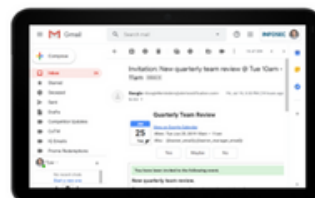
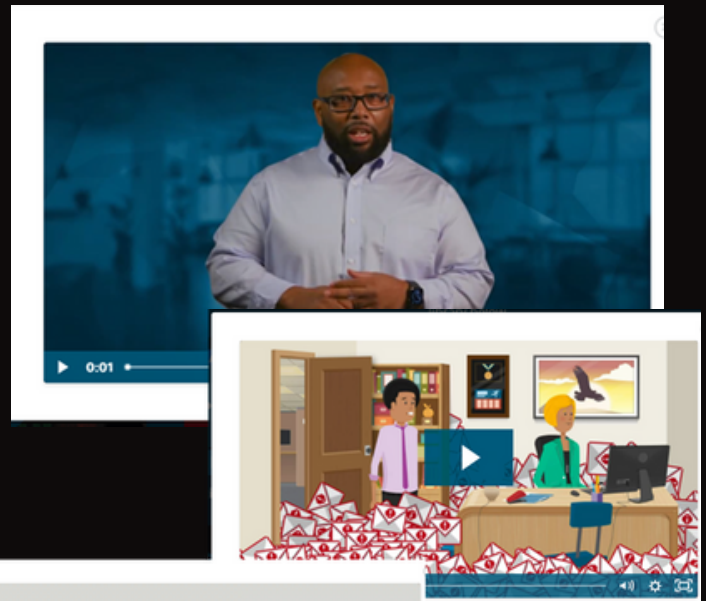
The Cythera Cyber Maturity Assessment is a business security posture assessment covering up to 37 security categories to determine the level of cyber risk across your business. This assessment service is underpinned by the Australian Cyber Security Centre and includes a report highlighting business risks and remediation strategies.

Cythera also provides an Cyber Awareness portal which delivers cyber security training to staff. This service also includes a phishing simulator to help businesses understand their current security posture and reduce cyber risk whilst improving user awareness.

Key Benefits:

- Understand your cyber risk
- Educate your staff
- Cyber Awareness training (2000+ courses)
- Phishing simulation (100+ pre-built Australian focused templates)
- Cyber Awareness posters

Strategy No.	Relative Security Effectiveness Rating	Mitigation Strategy	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost	Level of Implementation	Risks
1	Excellent	Application whitelisting of approved programs to prevent execution of unapproved programs including .exe, .dll, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	M	H	M	Low	Users broadly block applications to users and often users. Pats Also NDR client can block malicious applications. Knowledge configuration is costly. No application whitelisting solution deployed on endpoints.
2	Excellent	Patch applications (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patched desktops with software not security vulnerabilities within 48 hours. Use the latest version of applications.	L	H	H	None	Applications are not patched. OS level patching happens in ManageEngine which deploys critical and security updates from Microsoft. No app specific patching of non MS products.
3	Excellent	Configure Microsoft Office macro settings to block macros from the Internet, and only allow macro settings in trusted locations, with locked with access or digitally signed with a trusted certificate.	M	M	M	None	No controls around Macro use in place within the business.
4	Excellent	Over application hardening. Configure and restricts to block Flash (already uninstalled), Java and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. DLLs) with browsers and PDF viewers.	M	M	M	None	OS is deployed with vendor application settings. Users cannot deploy third party apps. Runs on workstations and servers to further network segmentation, however is deployed in monitoring mode only.
9	Excellent	Operating system generic exploit mitigation (e.g. Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) and Control Flow Integrity (CFI)).	L	L	L	Low	Control flow integrity coverage for many of these exploits. Nothing covered into the OS.
13	Very Good	Control removable storage media and connected devices. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth (BT) devices.	H	H	M	None	No removable media controls in place. No monitoring of use and no policy for best practice. Capability is available within ManageEngine but not presently deployed.
16	Good	User education. Avoid phishing emails (e.g. with links to login to fake websites), weak passwords, password reuse, as well as unapproved removable storage media, connected devices and cloud services.	M	H	M	None	None in place today. Have used the ProSight cyber awareness platform for some time in the past.
20	Excellent	Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.	M	H	M	Low	Multiple instances of MFA used for various purposes. General access to O365 is not behind MFA (internal and external), but administrators are MFA enabled on ManageEngine. MFA enabled on all management tools.
21	Excellent	Disable local administrator accounts or assign passwords that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials.	L	M	L	Low	Server local admin account is locked and disabled. Domain admin accounts used to access servers. Workstations local admin account (C:\admin) with a generic password across the fleet and local admin on workstations is active.
23	Excellent	Protect authentication credentials. Remove O/Password values (Auto-Cache). Configure Windows (WSST) and Use Credential Guard. Change default passwords. Regularly change passwords.	M	M	L	None	Not deployed.
30	Very Good	Endpoint detection and response software on all computers to centrally log system behaviour and facilitate incident response. Microsoft's first Defender tool is an early tool.	L	M	M	None	Pats Cortex NDR agent exists but EDR license is not subscribed to at present.
31	Very Good	Plan to discover incidents based on knowledge of adversary tactics. Leverage threat intelligence consisting of analysed threat data with content enabling mitigating action, not just indicators of compromise.	L	UH	UH	Low	Proactive hunting appears to be available within the MDR. Cortex tool is not used if it is used to allow Cortex Health or Pats. DarkTrace monitors for threats and incidents but this is not always integrated into the MDR service or any (existing) alerting systems.
35	Very Good	Business continuity and disaster recovery plans which are tested, documented and placed in harmony with a strategic threat plan. Focus on the highest priority systems and data to recover.	L	H	M	None	No formal or informal BCP/DR plans. Highly available architecture. PaaS is redundant with workload enabled by vendor. RDS has high redundancy. M1/H2 are mirrored for several services. Redundant documentation as a result.



Choose from 1,000+ realistic phishing templates

Build simulated phishing campaigns from our library of over 1,000 templates to teach employees how to avoid the most dangerous phishing threats they face.

New templates are added weekly to simulate ongoing attacks, leverage recent news and keep employees ahead of new threats. Build your own phishing simulation campaign or select template categories to run automatically.

[Get Started](#)

PROTECT

The Protect portfolio includes a comprehensive range of security protection technology for your users, applications, IT assets and infrastructure, including: malware protection, endpoint protection, DNS firewall functionality, web content filtering, email filtering, ransomware protection, botnet protection and scheduled cyber-drills for a low, monthly, per user cost. Each security service can be implemented individually or interwoven into a complete personalised security offering to protect your business from the unique and ever evolving threats it faces.

The Protect portfolio is underpinned by strong partnerships with market leading technology providers such as CrowdStrike, Proofpoint, Netskope, and Automox.

Key Benefits:

- Cloud delivered solutions
- Low cost subscription basis
- Personalised approach
- Multi-layered security
- Managed service available incl. 24x7 or 12x5 Monitoring, Fault and Security Management and Phone Support

MAIN CAUSES OF BREACHES 2021*:

55% CRIMINAL ATTACK
41% HUMAN ERROR
4% SYSTEM FAULTS



DNSProtect

Monitor and block sophisticated attacks by enforcing security policies at the application, port and protocol levels.



EndpointProtect

Continuous monitoring and response to advanced threats, malware and viruses targeting endpoint devices



WebProtect

Proactively protect important HTTP applications from fraud, data theft and intentional misuse.



CloudProtect

Defend your cloud from advanced threats and data theft



EmailProtect

Defends against known and emerging email-borne threats before they reach your network.



EmployeeProtect

Actively teaches employees about cybersecurity, IT best practices and regulatory compliance.



EndpointPatch

Automated, prioritised vulnerability patching for desktops, servers and laptops.



MONITOR, DETECT & REACT

Cythera has developed a powerful security monitoring and incident response platform powered by Rapid7's InsightIDR technology. The Cythera Managed Detection and Response (MDR) platform is a cloud delivered service, powered by Australian-based human-led specialists, offering incident detection and response capabilities that combines user behaviour analytics, SIEM, Security Orchestration / Automation and endpoint detection capabilities all in one place.

Cythera provides customers with 24x7 monitoring of all IT Infrastructure and endpoint assets and proactive threat hunting with integrated rapid incident response services upon a threat being detected.

If there is an incident, such as an attempted breach, the team is ready 24x7 to switch from detection mode to respond and act. The remediation plan will be tailored to your organisation and created upon commencement of the service. You will also be provided with reporting containing an executive summary as well as in-depth analysis of the issue to help fuel threat intelligence to increase speed in detection and response in the future and to make sure your organisation understands the incident.



Key Benefits:

- Australian based
- 24x7 Monitoring, Threat Detection & Response
- Proactive threat hunting
- User behaviour monitoring
- Playbooks and workflow automation
- Cloud delivered managed SIEM
- Named Security Operations Analyst
- One uncapped incident response p.a

Featured	Cythera Managed SOC - Essentials	Cythera Managed SOC - Advanced	Cythera Managed SOC - Elite
Cloud based log and event management (SIEM)	✓	✓	✓
User Behaviour Analytics	✓	✓	✓
Attacker Behaviour Analytics	✓	✓	✓
Endpoint Detection and Visibility Monitoring incl. Investigation Timeline	✓	✓	✓
Centralised Log Management	✓	✓	✓
Deception Technology (Intruder Traps)	✓	✓	✓
Canaries (Enhanced Detection)	Optional	✓	✓
24x7 Managed Monitoring and Alerting	✓	✓	✓
Incident Triage, Investigation and Guided Response	7am-7pm (AEST) Monday to Friday (2 hr SLA)	7am-7pm (AEST) Monday to Friday (2 hr SLA)	24x7 (2 hr SLA)
Incident Response	T&M	T&M	1 x Uncapped (BH)
Threat Hunting	Quarterly	Monthly	Monthly
Customer Advisor	✓	✓	✓
Incident Playbooks and Automated Response	Optional	Optional	Unlimited
Real-time Online Reporting and Threat Assessments	✓	✓	✓

ASSURE

Cythera also provides a range of complimentary cyber security services to assist you in assessing your risk, security posture, and exposure. Along with assessment services we can also provide assistance with incident response, education and training.

Breach/Compromise Assessment:

- Malware Analysis & Threat Hunting
- Endpoint Digital Forensics
- Root Cause Analysis
- Development of Security Requirements

Incident Response:

- Rapid response to ongoing incidents
- Breach assessment
- Incident Response Plan

Penetration Testing & Vulnerability

Assessment:

- Vulnerability scanning of applications, network and devices
- Prioritise critical vulnerabilities
- Assist with remediation and patching strategy
- Assessment Report

Education, Training & Strategy

- Training employees on information security
- Developing programs to train staff to identify attacker tactics and techniques
- Assistance in designing security programmes

"WE SUFFERED A CYBER INCIDENT. THE TEAM AT CYTHERA PERFORMED A COMPROMISE ASSESSMENT AND HELPED US PUT A PLAN IN PLACE TO REMEDIATE SOME OF OUR ISSUES. WE HAVE NOW DEPLOYED THE CYTHERA PROTECTION PLATFORM WHICH HAS NOT ONLY PREVENTED CYBER SECURITY ISSUES, IT'S IMPROVED THE AWARENESS AND PREPAREDNESS OF OUR STAFF GIVING US GREAT PEACE OF MIND."

IT MANAGER - AUSTRALIAN CONSULTING FIRM





CONTACT

Level 22, 120 Spencer St
Melbourne VIC 3000

123 Eagle St
Brisbane QLD 4000

152 St Georges Terrace
Perth WA 6000

EMAIL

sales@cythera.com.au

PHONE

1300 298 437
