CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

SMB PACKAGE - CYBER ELITE

CISO OPERATION

DATASHEET

Microsoft
Cloud Solution Provider

ACSC Australian Cyber Security Centre
NETWORK PARTNER

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

WHO IS CISO ONLINE

CISO Online uplifts your cyber security posture through our cyber security uplift program, advanced professional services, and awareness training.

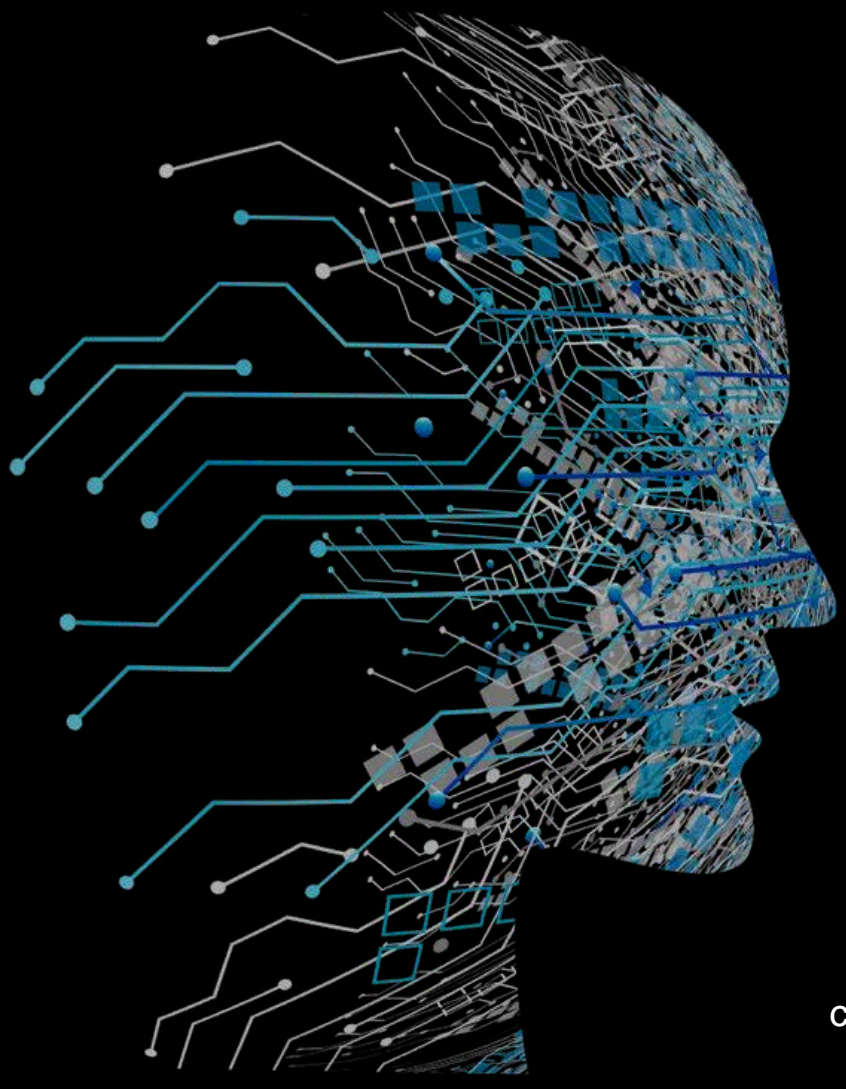
Whether you're an SME or a high-end Enterprise, with bad actors becoming increasingly smarter in their attack methods, safeguarding your business is more crucial than ever.

OUR VISION

Is to create a working and collaboration environment safe from cyberattacks and allowing enterprises to focus on their core business.

OUR MISSION

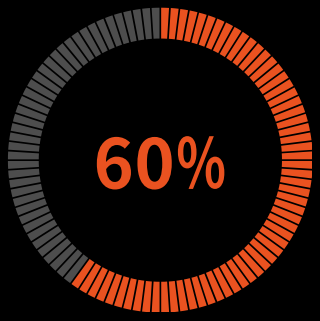
Is to protect businesses and uplift their cyber security posture and behaviour.



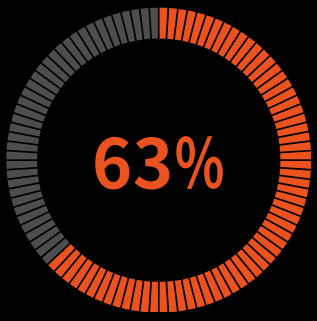
cisoonline.com.au

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

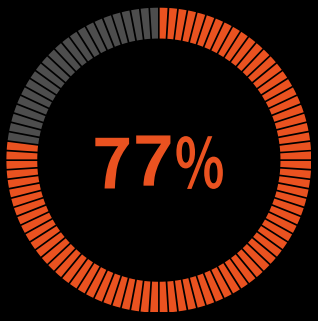
CYBER SECURITY STATICS FOR SMB



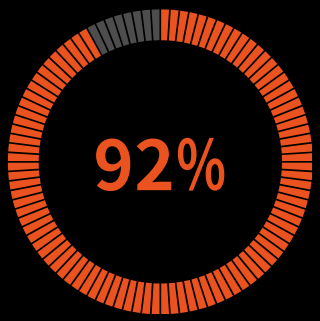
of **SMB's** have experience at least one data breach



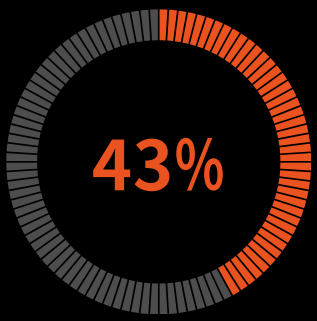
of **SMB's** have faced ransomware



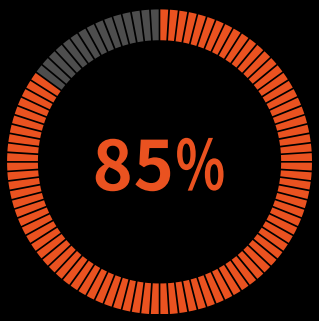
of attacks happen after hours or the weekend



of all cybercrime reports were made by **SMB's**



of cyberattacks specifically target **SMB's**



of data breaches are the result of **human error**

IT'S NOT IF YOU FACE A CYBER ATTACK! IT'S WHEN!

$46,000

Is the average cost of data breach for **small businesses**

$97,200

Is the average cost of data breach for **medium businesses**

33,000

Cyber incidents are reported to the ACSC hotline in last FY

10 minutes

An SMB reports a cyber attacks

309,000

Australian SMB say they've been targeted by cyberattacks

every 6 minutes

A cybercrime is reported

cisoonline.com.au

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

NOTIFIABLE DATA BREACHES (NDB) SCHEME

Australian Government

Australian Government
Office of the Australian Information Commissioner

Updated Privacy ACT

Australian organisations are required to notify any individuals likely to be at risk of serious harm by a data breach.

[Directors liability]

CRIMINAL RECORD

Examples of a data breach:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

For more information visit https://oaic.gov.au

cisoonline.com.au

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

OUR PURPOSE: CYBER SOLUTIONS FOR SMB

The Australian Cyber Security Centre (ACSC) reports a 23% increase in cybercrime last year, including identity fraud, online banking fraud, and business email compromise. Despite the increase in cyber incidents, nearly half of Australian Small and Medium-sized Businesses (SMBs) allocate less than $500 annually to cyber security.

Recognising the budget constraints faced by SMBs, Our partnership with Microsoft as a Cloud Solution Provider (CSP), enables us to offer advanced and scalable cloud-based cyber security solutions and ongoing operations, so SMBs can focus on their core business rather than cyber security challenges.

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

OUR TRUSTED PARTNERS for SMB PACKAGES

Microsoft

ACSC Australian Cyber Security Centre — NETWORK PARTNER

KnowBe4
Human error. Conquered.

NINJIO

OUR CERFITCATES

Microsoft CERTIFIED EXPERT

Microsoft CERTIFIED SPECIALTY

Microsoft CERTIFIED CYBERSECURITY ARCHITECT EXPERT

aws certified Security SPECIALTY

OFFENSIVE SECURITY OSCP

CISCO CERTIFIED CCIE SECURITY

vmware NSX

CERTIFIED juniper JNCIE-SEC EXPERT

CERTIFIED SOLUTION EXPERT f5 SECURITY

INTERNATIONAL QUALITY SERVICES ISO 27001:2005 INFORMATION SECURITY IQS

CompTIA Security+ CERTIFIED·CE

pcnse

EC-Council C|EH CERTIFIED ETHICAL HACKING

SABSA Enterprise Security Architecture

iRAP

TOGAF® TOGAF® 9.1 Certified

PROFESSIONAL CERTIFICATION IBM Cloud Solutions V3 IBM Certified Architect IBM CLOUD

PMP

ITIL®

CCSP

CISSP®

IPv6 FORUM CERTIFIED CERTIFICATION

MICROSOFT CERTIFIED PROFESSIONAL Microsoft MCSE Core Infrastructure Certified 2021

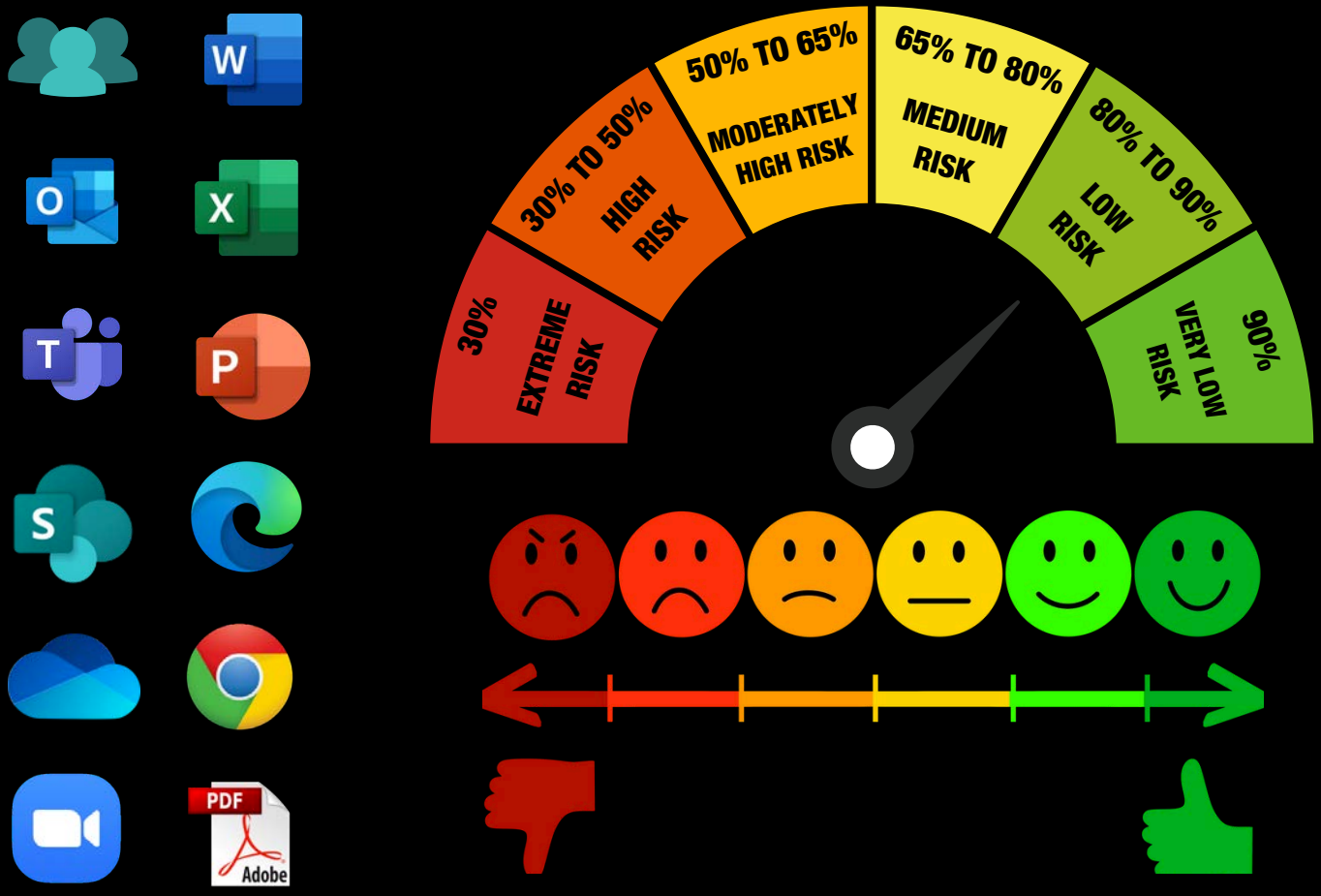
CISA Certified Information Systems Auditor An ISACA® Certification

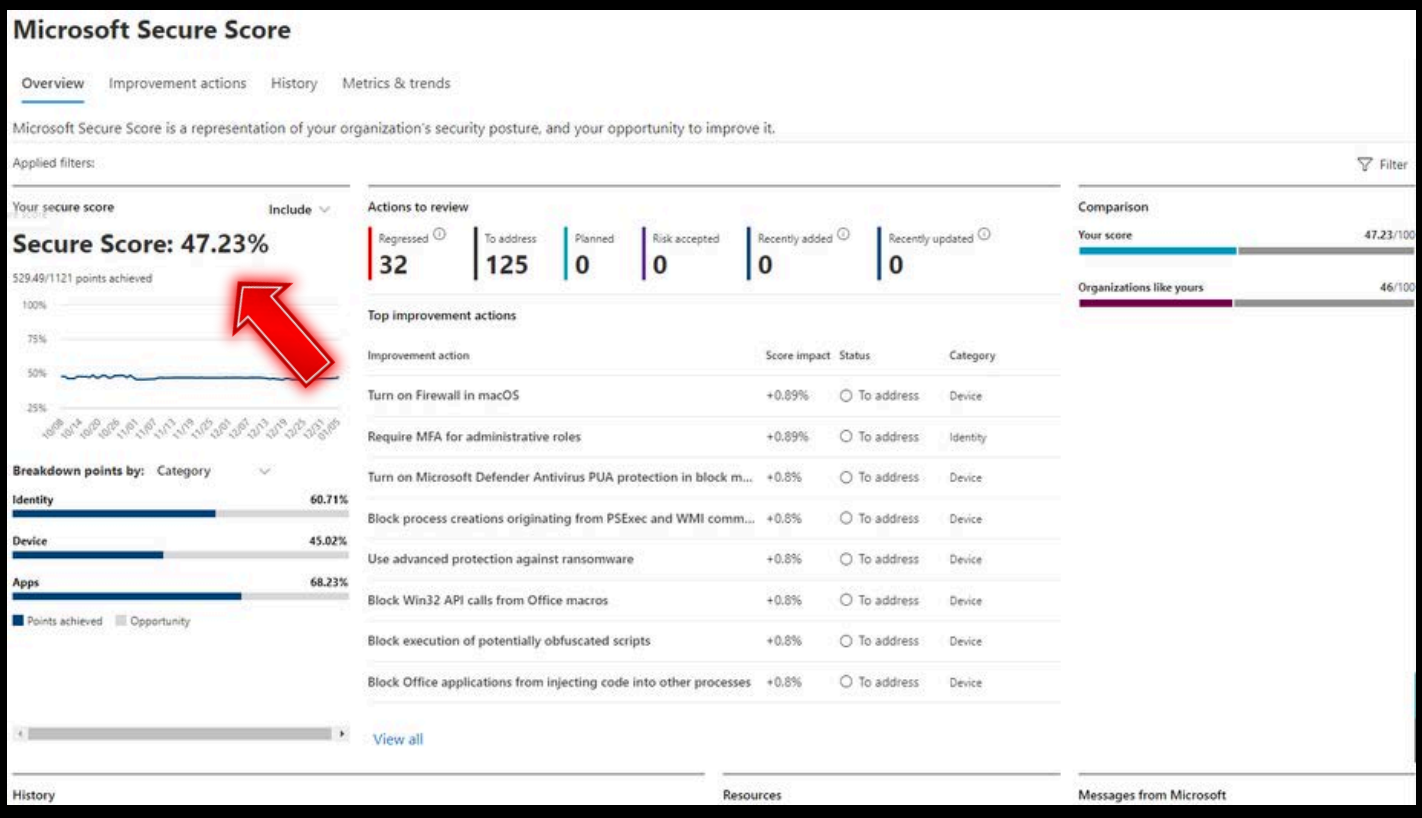
cisoonline.com.au

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft
Cloud Solution Provider

How Secure is your collaboration / working environment?





https://security.microsoft.com/securescore

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft
Cloud Solution Provider

YOUR JOURNEY

Phase 1

Improve your Secure Score

Phase 2

Maintain your Secure Score

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft
Cloud Solution Provider

CISO OPERATION

ONGOING OPERATION & DEFENCE

CYBER ELITE PACKAGE

cisoonline.com.au

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft
Cloud Solution Provider

RECOMMENDED

CISO OPERATION CYBER ELITE

- **Ongoing user Behaviour Analysis by AI**
  - Next-gen protection with adaptive AI security
- **Reactive Response to Security Events**
  - Ongoing vulnerability remediation and monthly response to security events (threat hunting) - Advanced
- **Ongoing Security Report - monthly**
  - Ongoing Secure Score monitoring and improvement with adaptive AI security
  - Advanced Log Collection and monthly security report
- **CISO as a Service advisory**
  - CISOaaS advisory and ongoing review of the policies - Fortnighly
- **Fine-Tuning Identity Protection Policies**
  - Ongoing support for provisioning new users/licenses and updating user credentials
  - Providing seamless login for new users using single sign-on
- **Fine-Tuning Email Protection Policies**
  - Fine-tuning advanced Email Protection policies against the latest threat tactics
  - Assessing and Releasing Quarantined Emails
- **Fine-Tuning Device Protection Policies**
  - Fine-tuning advanced computer and laptop protection policies
  - Updating device protection policies for new compnay-issued and BYOD devices
- **Fine-Tuning Data Protection Policies**
  - Ongoing review of data loss and leakage protection policies
- **Fine-Tuning Internet Protection Policies**
  - Ongoing review of website filtering - Standard
  - Ongoing Shadow IT report (Cloud Apss visibility)
- **Security Awareness Training**
  - Updating security awareness training plans

INVESTMENT: ONGOING MONTHLY FEE

cisoonline.com.au

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft
Cloud Solution Provider

Bulletproof your environment with CYBER ELITE

Microsoft Entra

Microsoft Defender

Microsoft Intune

Microsoft Purview

Microsoft Sentinel

Microsoft AI

cisoonline.com.au

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft
Cloud Solution Provider

CISO OPERATION - CYBER ELITE

Ongoing User Behaviour Analysis and Protection by AI

Next-gen protection with adaptive AI security

Next-generation operation leveraging AI to catch and block all types of emerging threats. This rapid evolution underscores the need for agile and innovative security operations using AI and machine learning models, behavior analysis, and heuristics.

How is this achieved?

- Behavior-based and real-time protection, which includes always-on scanning using file and process behavior monitoring and real-time protection.
- Detecting and blocking apps that are deemed unsafe, but might not be detected as malware.

Reactive Response to Security Events

Ongoing vulnerability remediation and monthly response to security events (threat hunting) - Advanced

Ongoing vulnerability remediation and reactive response to security events (monthly response) is a critical process, involving the identification and resolution of security vulnerabilities within your M365 environment.

How is this achieved?

- Identify, assess, remediate, and track all your biggest vulnerabilities across your most critical M365 assets, all in a single solution.
- Monthly reactive response and report to security events
- Ongoing Secure Score monitoring and improvement with adaptive AI security

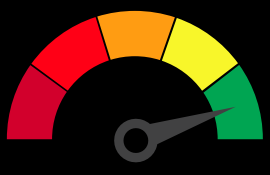
Ongoing Security Report - monthly

Ongoing Secure Score monitoring and improvement with adaptive AI security

Ongoing operation leveraging M365 portal capabilities to maintain and improve your secure score. In addition, a monthly Ongoing Security Report is essential for continuous monitoring of emerging threats, proactive risk management, and ensuring regulatory compliance.

How is this achieved?

- Ongoing Secure Score monitoring and improvement with adaptive AI security
- Monthly security report Leveraging M365 portal capabilities to maintain and improve your security posture.



CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft
Cloud Solution Provider

CISO OPERATION - CYBER ELITE

Ongoing Security Report - monthly

Advanced log collection

Ongoing log collection and providing monthly advanced security reports is required to detect and mitigate security incidents, enhancing overall cybersecurity resilience.

How is this achieved?

- M365 unified log collection and centeralised management of audit logs, which includes collecting and processing logs from various sources.
- Logs essential for threat detection, compliance, and security incident management.
- Archive logs for compliance purposes

CISO as a Service Advisory

CISOaaS advisory and ongoing review of the policies - Monthly

Cyber security policies defined in your M365 environment are safeguarding your data and systems from cyber threats. They provide a strategic framework for protecting sensitive information, ensuring operational continuity, maintaining trust, and complying with legal standards. Updating M365 policies is critical for your security posture and overall success.

How is this achieved?

- Ongoing review of M365 policies by leveraging our CISO as a Service (CISOaaS) capabilities and experience - Monthly

Fine-Tuning Identity Protection Policies

Ongoing support for provisioning new users/licenses and updating user credentials

Cyber Security starts with protecting your identity. Ongoing protection of your business identity by provisioning new users/licenses and updating user credentials

How is this achieved?

- Ongoing Multi-Factor Authentication (MFA) support
- Updating Conditional Access Policies
- Ongoing Biometric Sign in support
- Self Service Password Reset support
- New users and licenses provisioning

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft
Cloud Solution Provider

CISO OPERATION - CYBER ELITE

Fine-Tuning Identity Protection Policies

Providing seamless login for new users using single sign-on (SSO)

Providing seamless login for new users using single sign-on (SSO). New and current users will be using your protected M365 login across your business applications such as your accounting or CRM.

How is this achieved?

- Implementing Seamless Single Sign-On (SSO) for new users
- Leverage strong Microsoft 365 authentication methods for business applications, such as multi-factor authentication (MFA).

Fine-Tuning Email Protection Policies

Fine-tuning advanced email protection policies against the latest threat tactics

Fine-tuning advanced email protection policies against the latest threat tactics such as phishing attacks, malware threats, Business Email Compromise (BEC) scams is crucial for maintaining business continuity, and preserving reputation and trust in today's digital environment.

How is this achieved?

- Updating and fine-tuning Anti-malware, Anti-spam, Anti-phishing policies, Safe attachments and Safe links
- Ongoing assessment and release of quarantined email as per user request

Fine-Tuning Device Protection Policies

Fine-tuning advanced computer & laptop protection policies

Fine-tuning advanced computer & laptop protection policies are required for ongoing protection of computers and laptops are essential for protecting data, defending against viruses & malware threats, ensuring business continuity in both personal and organisational contexts.

How is this achieved?

- Fine-tuning Defender for Endpoint policies and Windows Security,
- Fine-tuning windows Firewall rules

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft
Cloud Solution Provider

CISO OPERATION - CYBER ELITE

Fine-Tuning Device Protection Policies

Updating device protection policies for new company-issued and BYOD devices (Laptops, Smartphones, Tablets)

Updating device protection policies for new company-issued and BYOD devices such as laptops, smartphones and tablets is essential for safeguarding Apps and protection for company data on any device preserving privacy, preventing identity theft, enabling remote device management.

How is this achieved?

- Fine-tuning and updating Mobile Device Management (MDM) policies
- Fine-tuning and updating Mobile Application Management (MAM) policies
- Remotely wipe lost or stolen devices
- Fine-tuning policies and managing M365 apps (Outlook, OneDrive, Word, Excel, PowerPoint) on any devices
- Managing Mobile Defender and Antivirus for Android and iOS devices

Fine-Tuning Data Protection Policies

Ongoing review of Advanced data loss & leakage protection policies

Ongoing review of data loss & leakage protection policies is crucial for safeguarding sensitive information and preventing unauthorised access. By updating data loss prevention (DLP) policies, you can reduce the risk of data breaches, regulatory fines, and reputational damage.

How is this achieved?

- Ongoing review and update of DLP policies to control access to sensitive information and prevent unauthorised access and unauthorised change.
- Tracks the movement of sensitive information within the organisation.
- Ongoing support of bring your own encryption

Fine-Tuning Internet Protection Policies

Ongoing review of Advanced website filtering

Ongoing review of website filtering is crucial to prevent access to malicious or inappropriate websites, enhancing network security whilst maintaining a more productive work environment

How is this achieved?

- Ongoing review and update of website filtering categories - Advanced

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft
Cloud Solution Provider

CISO OPERATION - CYBER ELITE

Fine-Tuning Internet Protection Policies

Ongoing Shadow IT Repoprt (Cloud Apss visibility)

Shadow IT refers to the use of software, applications, and services available on the Internet without explicit approval or oversight from the IT department.

How is this achieved?

- Visibility into all cloud applications to obtain a comprehensive picture of cloud apps activity and enact security measures accordingly

Updating Security Awareness training plans and ongoing simulated phishing campaigns

Human error is how most organisations get compromised and hackers are always looking for new ways to exploit vulnerabilities and this include humans! Updating Security Awareness training plans and ongoing simulated phishing campaigns are required to keep your employees educated on the latest tactics.

How is this achieved?

- Ongoing quarterly Security Awareness training plans and ongoing simulated phishing campaigns

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

SMB PACKAGES

Microsoft
Cloud Solution Provider

Secure Cloud Services CISO Operation & Defence	CYBER ESSENTIALS	RECOMMENDED CYBER PREMIUM	CYBER ELITE
Ongoing User Behaviour Analysis and Protection by AI	✗	✓ Advanced	✓ Advanced
Reactive Response to Security Events Monthly vulnerability Remediation & threat hunting	✓ Standard	✓ Advanced	✓ Advanced
Ongoing Security Report - monthly	✓ Standard	✓ Advanced	✓ Advanced
CISO as a Service Advisory	✓ Quarterly	✓ Monthly	✓ Fortnightly
Fine-Tuning Identity Protection Policies Login details, passwords and new users	✓ Standard	✓ Advanced	✓ Advanced
Fine-Tuning Email Protection Policies	✓ Standard	✓ Advanced	✓ Advanced
Fine-Tuning Device Protection Policies Computers, Laptops, Smartphones and tablets	✓ Standard	✓ Advanced	✓ Advanced
Fine-Tuning Data Protection Policies Data Loss and Leakage	✗	✓ Standard	✓ Advanced
Fine-Tuning Internet Protection Policies	✗	✓ Standard	✓ Advanced
Security Awareness Training	✓ Standard	✓ Advanced	✓ Advanced
Suitable for but not subject to	Micro Businesses with 1 to 10 users	Small Businesses with 1 to 250 users	Medium Sized Businesses with 250 to 500 users

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Microsoft Surface
Authorized Reseller

ULTIMATE ENDPOINT SECURITY WITH MICROSOFT SURFACE

When you purchase a Microsoft Surface laptop from CISO Online, you have the opportunity to natively integrate your laptops with Cyber Premium security features for the ultimate security.

SECURITY OUT OF THE BOX

Our SMB cyber packages are crafted to offer comprehensive protection tailored specifically for small and medium-sized businesses. By integrating these packages with Microsoft's industry-leading, built-in security features, Surface devices safeguard you and your data, no matter where you work.

Hardware
Easily encrypt and protect your data in a sandboxed environment that stores passwords, PIN numbers and certificates with Trusted Platform Module 2.0. (TPM 2.0)

Firmware
Automated updates to Microsoft firmware make start up faster and more secure, while DFCI enables remote management of hardware components. (camera, Bluetooth)

AI-enabled
Ultrathin laptop designed for enhanced AI experiences, with industry leading AI acceleration to unlock powerful new features.

Cloud
Get peace of mind with always-on security features to keep data, devices and identities more secure than ever.

cisoonline.com.au

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

OUR SERVICES

CISO Uplift
SMB Packages

CISO Operation
SMB Packages

CISO Defence
SMB Packages

Cyber Security Uplift
Risk Based Approach

CISOaaS
CISO on Demand

Secure Laptops

Essential 8

Penetration Testing

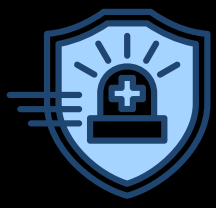
Security Risk
Assessment

Security Solution
Architecture

Security Implementation

Business Continuity &
Disaster Recovery
(BCDR)

Digital Forensics



Incident Response

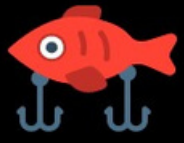
ISO27001/ISMS
Consultancy

IRAP Assessment

Governance, Risk,
Compliance (GRC)

Security Operation
Centre (SOC)

Cybersecurity
Awareness Training



Simulated Phishing
Attack & Phish Alert

cisoonline.com.au

CISO ONLINE
CYBER SECURITY UPLIFT & AWARENESS

Contact us:

cisoonline.com.au
info@cisoonline.com.au

1300 710 677

Three International Towers, Level 24,
300 Barangaroo Ave, Sydney, NSW 2000, Australia

AUG 2024