OneCollab

CYBER SECURITY SERVICES

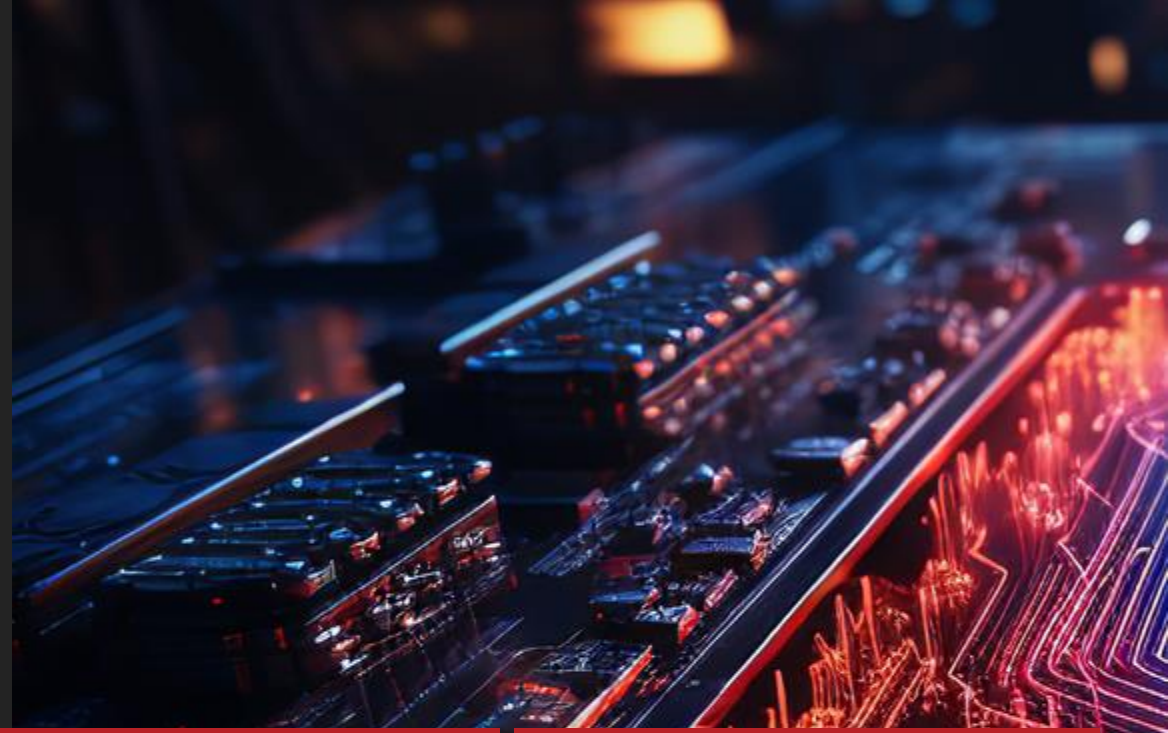
Cyber Security is complex

Our purpose is to make it simple

OUR SUPPORT MODEL

We understand that your business is one-of-a-kind

Our model offers you **flexibility** in how you utilise our cyber security services, ensuring they seamlessly align with your business needs.



KEY BENEFITS FOR YOUR BUSINESS:

- 24/7 cyber security protection, monitoring and support
- Maintenance and upgrades of all security tools
- Swift identification and remediation of any issues
- Regular insights (MI) and production of dashboards/ board reports

24/7 Cyber Monitoring and Support

Our technology is monitoring your environment 24/7. We also undertake regular preventative maintenance required to maintain the basic operation of your devices, including:

- Windows Patch Management
- 3rd Party Patch Management
- Device Performance Reviews
- Clean Windows Update Cache
- Windows Firewall Management

Threat Prevention & Detection

A unified Anti-Virus solution to actively monitor and manage devices, ensuring that your business is protected and secure.

Standard Anti-Virus includes:
- Anti-malware protection
- Scheduled scans
- Software updates
- Remediation of issues

Premium Next Gen Anti-Virus also includes Advanced Threat Security, Anti-Ransomware Protection, Email Security & Web Protection & Content Filtering

Safeguarding Your People

Cyber criminals are diligent in finding new, sophisticated methods to trick unsuspecting individuals into putting themselves at risk. Having a proactive approach is key in a robust security culture.

We can help you to safeguard your people through:

- Dark Web Monitoring
- Routine Simulation Phishing Campaigns
- Continuous Education

Additional Services

Additional Services include:

- BYOD Management
- Back Ups
- Ethical Hacking
- Penetration Tests
- Website Security
- Cyber Governance
- Virtual CISO
- Cyber Regulation Compliance

OneCollab

CYBER SECURITY IS COMPLEX... OUR PURPOSE IS TO MAKE IT SIMPLE

Have you ever been involved in a conversation with your IT department and thought, "What does that even mean?" Well, you are not alone. Understanding the myriad of security terms and how they relate to you can be a daunting task.

Here are six frequently used security terms and the definitions associated with each to help you become your organisation's cyber security thesaurus.

Patching

Security patches are software and operating system updates that aim to fix a security vulnerability in a programme or product. The updates literally "patch" a hole in your defence, preventing a hacker from exploiting a way into your network.

Anti-Virus

A computer virus is a type of malicious software that spreads between computers and causes damage to data and software.

Antivirus software is designed to evaluate data to help find and eradicate this malicious code as quickly as possible.

Malware

Malware, short for "malicious software," is a blanket term that refers to a wide variety of software programs designed to do damage or do other unwanted actions to a computer, server or computer network.

"Signatures" refers to the regular updates made by antivirus software to the database of known malware signatures.

Web Content Control

Web content filtering is a technique that blocks and screens access to inappropriate or unsafe web content.

Dark Web Monitoring

The dark web refers to sites that are not indexed and only accessible via specialised web browsers, often linked to criminal intent and the purchase of "illicit' goods and services, including your personal data.

Dark Web Monitoring continuously monitors the dark web for compromised data providing a detailed view of what has been compromised, including any available breached passwords.

Virtual CISO

A virtual chief information security officer is a specialist information security professional that you can call on for support with planning and executing an effective cyber security strategy.

OneCollab