Simplifying your cybersecurity management

Anticipate, identify and resolve cyberthreats with Vocus Managed Detection and Response
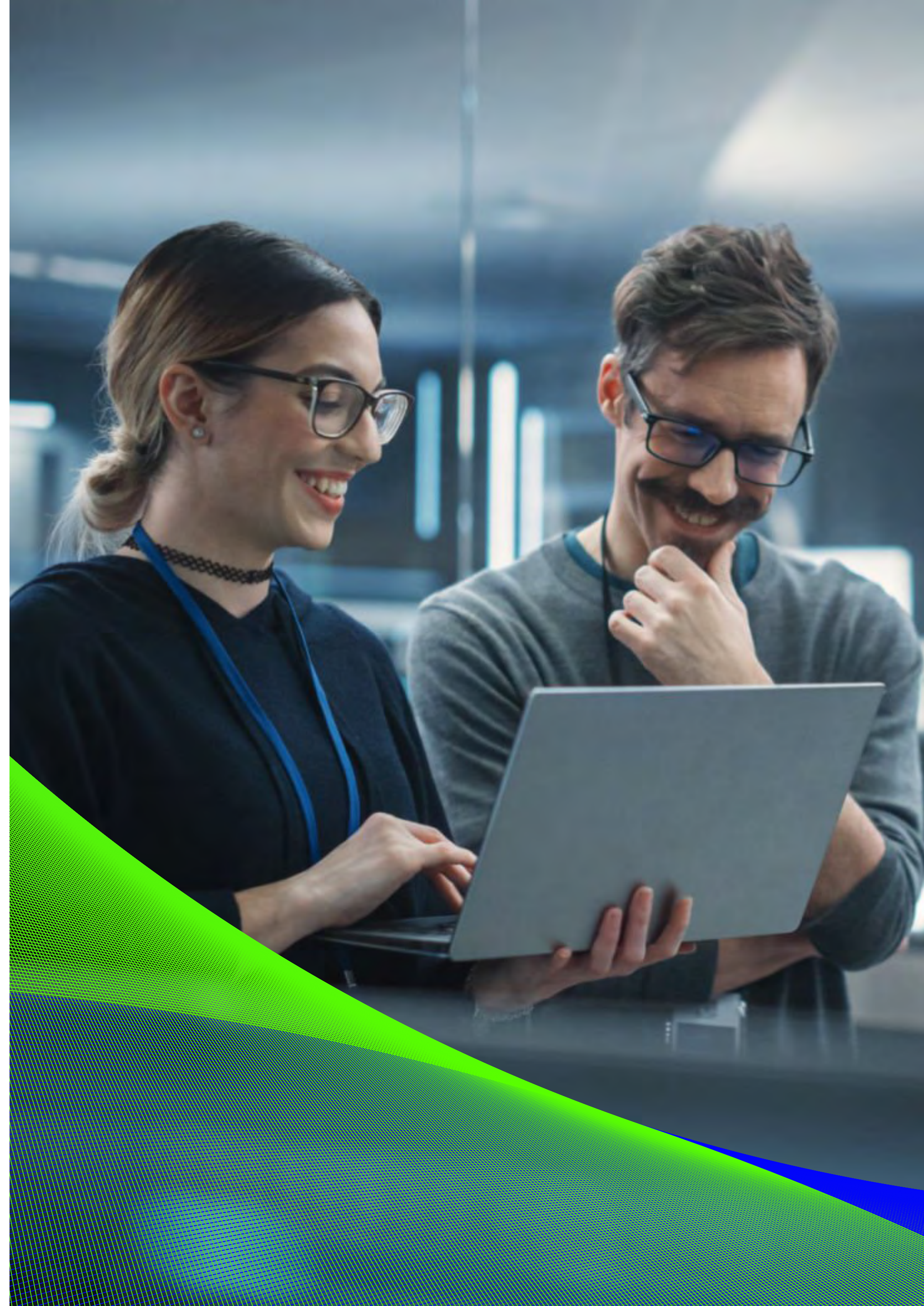
VOCUS

Protecting your business

As the risk of cyberattacks continues to grow, so does the need for fast, accurate threat detection and response to protect your company and customer data.

Monitoring, analysing and responding to cyberthreats can be time consuming and expensive for IT teams, especially when existing security tools produce an array of false positives. Addressing every alert can be overwhelming and, in some cases, genuine threats can be overlooked amongst the deluge of information.

In a recent report*, only 1/3 of companies discovered a breach using their own security teams. All of this points to overwhelmed cyber teams needing help in detecting and responding to cyber events, whilst trying to also support the wider business objectives.

* Source: Cost of a Data Breach Report 2023, IBM

How Vocus can support your business

Vocus Managed Detection and Response (MDR) is a smart, end-to-end solution which identifies and alerts threats across your organisation's endpoint devices, infrastructure, applications and cloud-based services.

As part of our service offering, security analysts from Vocus' Australian-based Security Operations Centre (SOC) will augment your cyber security team to accelerate threat detection – freeing up your team to focus on other responsibilities, without the distraction of constantly monitoring incidents and potential threats.

How it works

Vocus MDR closes the loop on security detection and remediation.
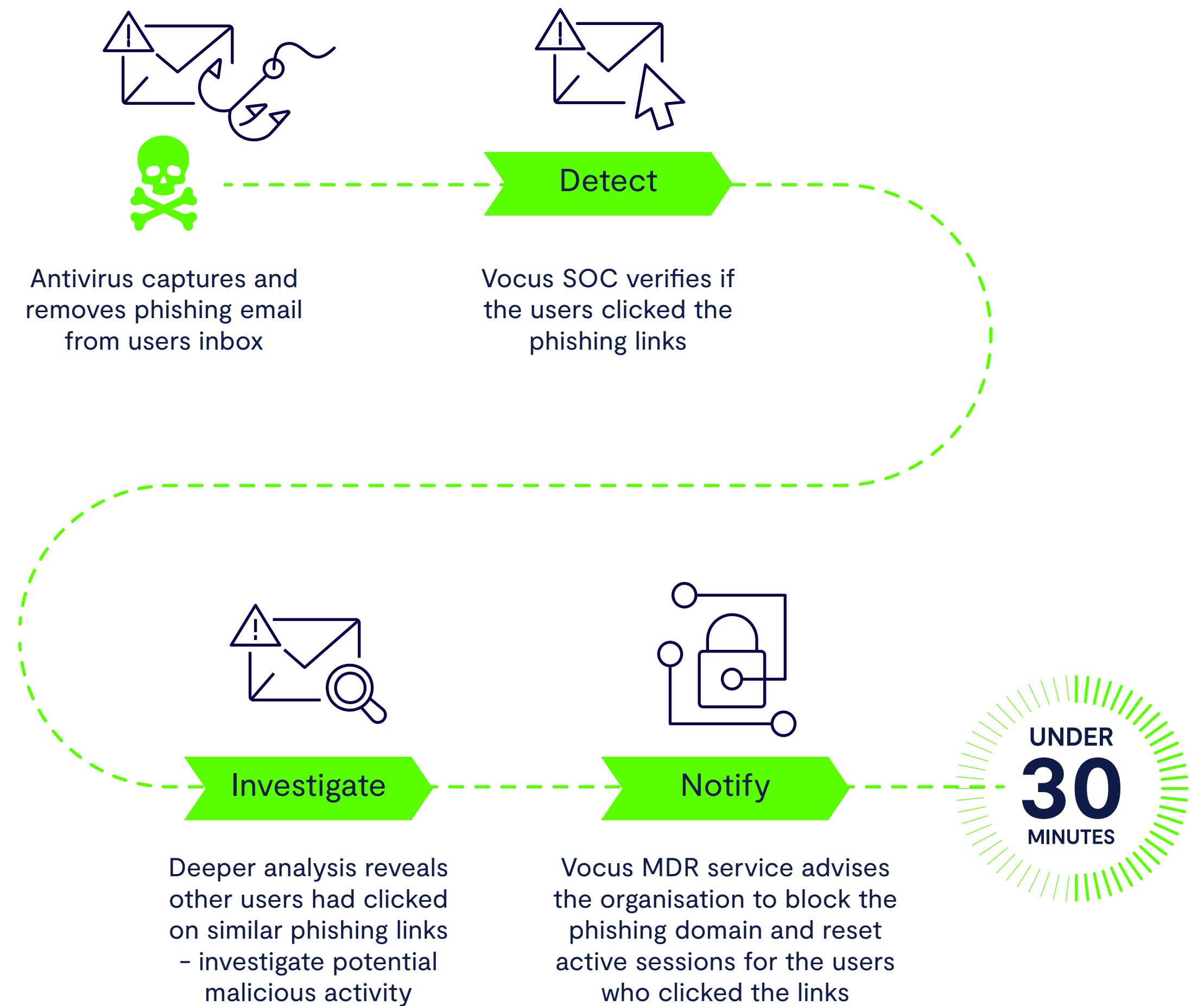
Our fully sovereign SOC collects your cyber log files for analysis through our cyber security specialists. These logs may come from existing cyber tools such as end point protection, firewalls, network infrastructure, identity management, cloud and applications. There's no need to replace your existing investments in cybersecurity tools.

We then combine these logs with cyberthreat intelligence feeds and insights from across our customer base to provide you with timely, accurate and actionable cyberthreat information.
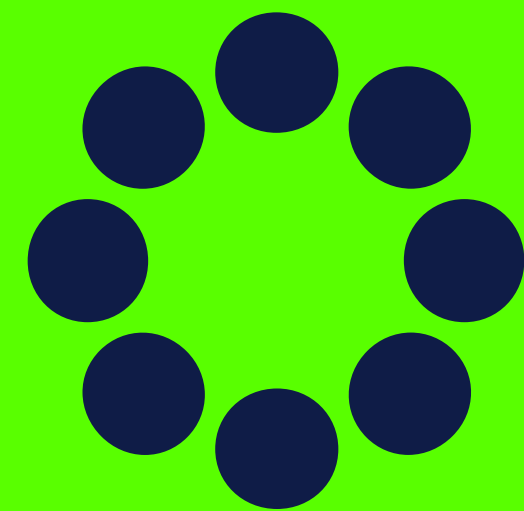
Vocus can detect, investigate and notify a cyberthreat in **under 30 minutes**

This real life example showcases the SOC's pivotal role in detecting, investigating, and mitigating cyberthreats

Detect

Antivirus captures and removes phishing email from users inbox

Vocus SOC verifies if the users clicked the phishing links

Investigate

Notify

Deeper analysis reveals other users had clicked on similar phishing links – investigate potential malicious activity

Vocus MDR service advises the organisation to block the phishing domain and reset active sessions for the users who clicked the links

UNDER **30** MINUTES

Business benefits of Vocus MDR

In today's digital landscape it is paramount businesses are being protected from potential cyberthreats as well as being empowered with the agility and insights needed to thrive.

Vocus MDR provides key business benefits with simplified management and rapid response times, ensuring cybersecurity threats are monitored and resolved swiftly.

The service offers deep integration for comprehensive visibility and is 100% Australian-owned, guaranteeing data sovereignty. Additionally, Vocus MDR's trusted partner network and open platform integration optimise security investment.

Better business outcomes

- Increased staff retention & acquisition
- Improved governance & complicance
- Reduced business risk
- Increased operational resilience
- Enhanced customer experience

Optimised security

- MPLS
- SD-WAN
- MDR
- SASE

Get in touch

Vocus builds outcome-based cybersecurity strategies—empowering organisations to streamline their cybersecurity efforts, mitigate risk, and accelerate business objectives.

Visit our website to learn more or get in touch with your Vocus Account Manager today.