



Incident Response.

Cyber-attacks are an unfortunate part of the digital landscape and need addressing alongside the essentials of getting your business to operate. New threats emerge daily, adding to the burden of cyber risk and non-compliance being handled by your cybersecurity team.

To be able to manage that cyber risk, you need an overall understanding of your company's cybersecurity posture across all areas of your attack surface – policies, on-premises technology, remote workers, cloud suppliers, other third-party services and their associated staff etc.

Understanding your security posture helps identify any weakness and provides the opportunity to address them and improve your risk posture to an acceptable level.

Through a combination of automated tools and consulting workshops and questionnaires, we examine your organisation's posture against the National Cyber Security Centre's Cyber Security Essentials and ISO27001, identifying risks and improvement areas and providing weighted recommendations in the form of a security improvement plan. Our services covers three critical points:

- Identifies what assets you have
- Shows how the assets are interconnected
- Determines which of these are truly at risk

Our approach ensures you can create a solid cybersecurity foundation to protect your digital assets and data from cyber risk and provide a safe environment for your customer and supplier interactions. The service can cover your entire digital estate or be tailored to specific Areas of Concern (AoC).

Features & Benefits

Features:

- Assesses your current governance and risk management framework effectiveness.
- Discovers the level of unmanaged devices on your network.
- Categorises your assets and data by sensitivity and criticality.
- Identifies which users are most vulnerable to social engineering.
- Finds weaknesses relevant to mobile and remote work force.
- Documents privilege users and their impact on security posture.
- Reviews third party service providers cybersecurity from context of your business.
- Assesses security configurations to best practice security guidelines.
- Highlights improvements within your existing incident response capabilities.

Benefits:

- Provides prioritised corrective actions to improve effectiveness.
- Allows a true understanding of the scope of your estate and associated risk.
- Identifies which assets and data require more controls.
- Allows training and education needs to be planned in line with highest risk.
- Enables development policies and secure configurations ensuring a secure baseline.
- Supports access management and identity planning.
- Highlights where third party providers security posture is miss-aligned to yours.
- Provides clarity on configurations to meet best practice.
- Identifies corrective action to strengthen response capability and reduce impact.

Service Delivery

- 1 The service is rapidly deployed and scalable, being delivered as a combination of on-site and remote discovery and collaboration and off-site analysis, report generation and recommendation.
- 2 Discovery agents are deployed at key points on your network/s (internal, cloud and hybrid) to identify network traffic meta data and identify digital assets. Metadata on assets is processed and analysed within our secure cloud centres and presented to our security consultants for validation and posture assessment. No payload data is sent outside your organisation.
- 3 Consultants work with your staff to correctly classify asset criticality, relative vulnerability and determine remediation action and priority.
- 4 During discovery, we will work with your staff to review various source materials related to each individual Area of Concern (AoC) and the wider business strategy. This will ensure we understand the systems in place and the context in which they operate including valuable user-centric context.
- 5 Our team will review and analyse the information gathered and provide you with a report of the activities undertaken and recommended improvement opportunities. The report will also contain details of our findings, the associated gap analysis and risk assessment undertaken.

Service Levels & Pricing

Delivery	Automated data discovery occurs 24x7 during the assessment. Consultants operate during our Normal Business Hours.
Data Retention	Data is retained for period of assessment and then securely deleted.
Pricing	P.O.A