tdmgroup
we make IT possible

Advanced Security Intelligence

Innovative digital technologies are supposed to act as a business enabler, not open the back door to cybercriminals intent on compromising critical assets and confidential information.

Thankfully TDM Group has the key to keep them locked out. Our Advanced Security Intelligence is a specialist detection and response package that's designed to build cyber-resilience by inspecting your network, analysing the results and providing critical reporting.

Key Features

Internal and external vulnerability scan

An automated scan of internal and external computer networks, to identify and analyse technical security vulnerabilities that can expose your organisation to cyber-attacks.

TDM Group conducts two vital types of vulnerability scan:

Internal
Detects issues that potentially exist within the corporate firewall e.g. weak user credentials and unpatched software.

External
Detects potential vulnerabilities by focusing on externally-facing IP addresses e.g. open ports & application-level weaknesses.

Intrusion Detection System (IDS)

This valuable tool in the battle against cyber-attacks is designed to identify suspicious activity by monitoring network and host activity; enabling you to eradicate threats before they cause financial and/or reputational harm.

SIEM Service

The Security Information and Event Management (SIEM) service will collect events, audits and analyses different logs from a network, server, and applications to gain insight and detect any potential threats, unusual activities, policy violations, to lower the impact of an attack or a breach.

Key Features

Honeypot service

A honeypot is a computer system - internal or external - that's set up as a decoy to lure cybercriminals by mimicking likely targets. By monitoring incoming traffic, it's possible to learn where cybercriminals are coming from, the techniques they employ and what they want. Crucially, you can also determine which security measures are effective – and which ones may need improving or replacing.

On-site scan of your environment by an engineer

This manual network scan by an experienced engineer provides another layer of protection on top of the automated internal and external vulnerability scans. The primary objective is to identify vulnerabilities in networks, systems, hosts and network devices before cybercriminals can discover and exploit them.

Password checker

Passwords are often an organisation's weakest link. This bi-annual scan of your active directory protects your business data by identifying password related vulnerabilities, blocking weak passwords and securing user authentication.

Monthly KPI report to C-Level Executives

This custom report will detail all vulnerabilities observed during the engagement, assess the risk of any weaknesses identified and outline recommendations for further action.

Business Benefits

Identifies gaps in network security architecture, enabling proactive action to be taken to address vulnerabilities before they're exploited.

Reveals vulnerabilities that automated scans alone are unable to uncover.

Reduces the amount of time it takes to detect and respond to security threats.

Informs decision making around complex security vulnerabilities.

Enables C-level executives to prioritise the remediation of security weaknesses.

Provides data, recommendations and support designed to remedy and reduce risk exposure.

Contact us to advance your security detection and response

0808 129 22 99 | hello@tdmgroup.net | www.tdmgroup.net