Managed Detection and Response

For those that don't have a dedicated security operations centre (SOC)

The Threat Landscape

Around 50% of UK organisations experience monthly cyberattacks according to UK government statistics.

The challenge for many organisations is, ***'do they have the right levels of defence'*** and ***'can they effectively mitigate threats with the intelligence that their systems provide them?'*** For many the honest answer is no.

In 2022 the National Cyber Security Centre (NCSC), sent 34 million alerts to 7,500 members to inform them of potential threats, risks, vulnerabilities or open ports in their networks. It's unlikey their members could act upon all these alerts as it's estimated that it takes a person around 20 minutes to investigate one. For many organisations alerts generated from their systems can overwhelm an IT team, leading to them dealing with only the most obvious ones, but potentially still leaving vulnerabilities that threat actors can exploit.

The Maintel Detection and Response (MDR)

Our MDR service provides a remotely delivered security operations centre (SOC) function. These functions allow your organisation to rapidly detect, analyse, investigate and actively respond through threat mitigation and containment.

The service utilises a predefined technology stack (covering areas such as endpoint, network and cloud services) to collect relevant logs, data and contextual information. This telemetry is analysed within our platform using a range of techniques. This process allows for investigation by experts skilled in threat hunting and incident management, who deliver actionable outcomes.

Benefits

Expert resource 24/7
Our security experts are there for you 24/7. We're an extension of your security team, aligning our service to your risk and goals.

A detailed understanding of your environment
Our experts provide tailored advice based on the nuances of your individual environment to help ensure you are continuously protected.

Predictable costs
We agree the commercial model with you at the start, which is for an agreed period with defined SLAs.

Extensive experience in security technologies as a service
Delivering you combined value through playbooks, integrations and enrichments. Our expertise include Windows and Linux, SSO/MFA, and a variety of network monitoring and cloud systems.

Increased Security ROI
Our service helps improve your security technology and tooling investments. It's likely you'll have technologies that can perform comparable functions - we'll identify these and make recommendations.

The smart utilisation of automation
We use this to add capacity, bandwidth and speed to repetitive tasks. It means our experts can focus on those significant events that require human intervention.

A mature and robust threat intelligence (TI) capability
Our experts combine market leading TI feeds, personalised to you, with a deep understanding of the threat landscape and attacker behaviours to protect your systems and identify potential threat actors.

Reduce alert fatigue
Our analysts will investigate and triage incoming alerts for you. We provide you with all the information you need and assist you where required in focusing your resource on mitigating the right threats.

Find out how MDR would work for your organisation

Tel: *03448711122*
Email: *Info@maintel.co.uk*
maintel.co.uk