MANAGED DETECTION AND RESPONSE SERVICE

CYBER SECURITY

Providing intrusion detection of malware and malicious activity in your network, and responding to suspicious activity and threats, proactively monitoring endpoints - on-premises, cloud or mobile.

HOW DOES THE SERVICE WORK?

The Managed Detection and Response (MDR) Service is delivered in the form of an agent that looks for points of compromise on endpoints, such as laptops, PCs and servers. Using the agent to make decisions based on detected activity, alerts are activated if a human response is required. A member of our dedicated team then takes appropriate action, such as quarantining, removing and/or remediating the problem device(s) away from the network to stop any further infection within your IT environments, or lateral movement.

Centrally managed and rolled out across Windows, Mac, Linux and Android operating systems, it offers out-of-the-box threat hunting and forensic data capabilities.

Catching security threats before they become full-scale incidents ensures your organisation continues running smoothly. Threat visibility strengthens your cyber resilience, and a human intervention reduces the impacts of incidents. Proactive monitoring ensures any points of compromise activate alerts and are checked out swiftly.

BENEFITS TO YOU

People

Our MDR Service is integrated into our SIEM (Security Information and Event Management) Service as well an Incident Response Service team. This means all teams can interact seamlessly when threats are identified to get you back to a point of operation as quickly as possible.

Technology

The service is compatible with any endpoint and any device and fully integrates with Office 365. This means you can detect threats within that environment and make decisions based on the users that are using that software. Our service provides the reassurance that your Office 365 setup is fully protected and secure.

Commercials

Endpoint Detection and Response (EDR) solutions require forensic expertise before decisions are made. With today's explosion of data and an increase in the number of incidents that require attention, this can lead to increased downtime and costs associated with employing the expertise required. It's important to ensure that when flags are raised, you have the capability you need to move forward – which is what our MDR Service provides.

SUITABLE FOR YOU IF...

- ✓ You need to reduce downtime and cost associated with security threats.
- ✓ You're looking for a managed service you can rely on to protect your organisation.
- ✓ You'd like peace of mind that your IT environment is proactively monitored.
- ✓ You need a solution that spans all endpoints across cloud, mobile devices and on-premises.
- ✓ You want a proactive approach to security monitoring.

WORKS WELL WITH

Incident Response Service

Mitigating security incidents 24 hours a day, helping contain threats and minimise financial and reputational loss, whilst reducing downtime.

Managed SIEM Service

Reducing cyber risk by monitoring for, and detecting, security threats – enabling you to respond quickly, with guidance from cyber analysts.

Cloud Essentials Service

Ongoing cloud governance support, visibility and financial operations.

WHAT'S INCLUDED

Swift action – Our team offers a 30-minute SLA for critical events, providing peace of mind that security threats will be swiftly dealt with.

The human touch – Intervention by real people ensures dedicated expertise to aid critical decision-making, 24/7/365.

Seamless integration – The MDR Service is compatible with any endpoint and device, covering all platforms. It integrates with Office 365, reassuring you that your setup is fully protected and secure.

Minimised downtime – As soon as flags are raised, swift action is taken by a combined force of forensic experts.

SERVICES THAT BRING YOUR TECHNOLOGY TO LIFE

Contact your Softcat Account Manager today.

DECEMBER 2022