Solution Brief

Insight's Managed Security Services

Business challenges

In today's rapidly evolving digital landscape, businesses face an array of complex challenges when it comes to cybersecurity. The constant barrage of cyber threats poses a significant risk to valuable assets and sensitive data. As cyber criminals become more cunning and innovative, it becomes increasingly difficult for organisations to detect and respond to these threats effectively.

Businesses struggle with tightening compliance regulations, the complexity of IT environments and the scarcity of skilled cybersecurity professionals. These challenges combined, creates the need to deliver comprehensive and proactive cybersecurity solutions to safeguard the businesses from the diverse and sophisticated threats they face daily.

Cybersecurity readiness and resilience is paramount to protecting the continuity and success of any modern business.

How Insight can help

Our Security Operations Centre (SOC) delivers two managed services offerings, providing advanced threat detection, investigation and response capabilities:

- **Managed Endpoint Detection and Response (MEDR)**
  Covering laptops, desktops and mobile devices.
- **Managed Extended Detection and Response (MXDR)**
  Bringing together logs and feeds from a wide range of sources, offering the most robust detection capability for your environment.

Combining technologies such as AI, threat intelligence and analytics, our team of expert security analysts are able to detect and respond to threats to your environment in real time.

We help you with:

- Comprehensive monitoring and real-time threat detection and response.
- Faster incident response and reduced downtime.
- Increased visibility into endpoint activity and potential threats.
- 24/7 service availability.
- Can aid compliance with some regulatory requirements and industry standards.
- Can be combined with other Insight services as part of an end-to-end security service.

Managed Endpoint Detection and Response Service

A managed service designed as an affordable and accessible detections and response capability for organisations with limited or no structured security programme. Our service is designed around Industry leading technology from the Microsoft security stack and utilises Microsoft Defender for Endpoint as the heart of its detection capabilities.

Key elements of our Managed EDR Service include:

- **Endpoint monitoring:** Using advanced tools and techniques to monitor endpoints 24/7 for signs of suspicious activity, including fileless attacks, advanced malware, ransomware, and insider threats.
- **Threat detection:** We use a combination of threat intelligence, behavioural analysis, and machine learning algorithms to detect advanced threats that may evade traditional security controls.
- **Investigation and response:** Our security analysts investigate and prioritise alerts and provide detailed incident reports to your team. We also work with you to develop and execute a response plan to mitigate the impact of any incidents.
- **Endpoint protection:** Our EDR solution includes advanced endpoint protection capabilities, including antivirus, anti-malware, and host-based intrusion prevention system (HIPS) features to help prevent and block attacks before they can do damage.
- **Threat hunting:** Proactive threat hunting capabilities, where our analysts search for and investigate potential threats that may have gone unnoticed by automated systems.

Managed Extended Detection and Response Services

A more robust detection capability that brings together all your security logs and feeds into a centralised SIEM platform based on Microsoft Sentinel technology.

Key elements of our Managed XDR Service include:

- **Monitoring:** Using advanced tools and techniques to monitor 24/7 for signs of suspicious activity, including fileless attacks, advanced malware, and insider threats.
- **Log collection and analysis:** Centralised collection and analysis of log data from various sources, including, endpoints, network devices, applications and cloud services.
- **Threat detection:** We use a combination of threat intelligence, behavioural analysis, and machine learning algorithms to detect advanced threats that may evade traditional security controls.
- **Investigation and response:** Our security analysts investigate and prioritise alerts and provide detailed incident reports to your team. We also work with you to develop and execute a response plan to mitigate the impact of any incidents.
- **Endpoint protection:** Our EDR solution includes advanced endpoint protection capabilities, including antivirus, anti-malware, and host-based intrusion prevention system (HIPS) features to help prevent and block attacks before they can do damage.
- **Threat hunting:** Proactive threat hunting capabilities, where our analysts search for and investigate potential threats that may have gone unnoticed by automated systems.

Outcomes of our Managed Security services

We will help you:

Advanced threat detection and response	24/7 monitoring and support	Cost-effectiveness	Compliance readiness
Helping prevent security breaches and minimising the impacts of potential attacks	Continuous protection and rapid incident response	A cost-effective alternative to building and maintaining an in-house team	Helping meet security standards and reporting requirements

For more information please contact your Insight Account Manager.

02 263 60 20 | be.insight.com

Insight