Managed XDR for Microsoft Sentinel

Combines the threat protection, security intelligence and automation of the Sentinel security platform and Defender product portfolio with expert monitoring and management by Softcat's 24x7x365 Security Operation Centre.

How does this service work?

Our Managed XDR (MXDR) service for Microsoft Sentinel can help you to proactively defend your organisation against threats and breaches.

The service will collect data from various sources such as cloud services, on-premises infrastructure and endpoints.

This data will then be analysed using machine learning and other techniques to detect and respond to potential security threats.

We combine this with the capabilities of Microsoft Defender XDR technologies to provide automated response actions across environments for endpoints. In addition to these automated playbooks and investigations, our 24x7x365 Security Operation Centre monitors and manages the service, providing expert guidance and support to our customers.

Additionally, the service includes features such as threat hunting and security orchestration, automation and response - all designed to help you locate and resolve any potential issues that might arise.

Benefits to you

People

Reduces your security teams' workloads by streamlining their operations with automated playbooks and investigations, freeing up time for them to focus on more important tasks and improve your organisation's overall security posture.

Our experts can help your security teams improve their knowledge and skills to stay ahead of evolving threats.

Technology

By integrating with other security tools and services, we can enhance the efficiency of your security operations and incident response, enabling your security team to work more effectively.

We use machine learning and other techniques to detect potential security threats, helping to protect your technology infrastructure from breaches and data loss.

Commercials

We'll manage your technical operations and ensure they are meeting compliance requirements, allowing you to focus on other priorities. Plus, through our technical workshops, we provide support with cost optimisation of the platform, to ensure you're getting the best out of your data and only utilising what you need.

We can also help you mitigate the risks associated with security incidents, thereby protecting your reputation and minimising the financial implications of a security incident.

Suitable for you if...

- You want endpoint response actions and expert guidance and support from a team of security professionals to help reduce the impact of incidents.
- You're looking for a fully managed security service to save time and money.
- You want to make improvements to your cyber security posture.
- You have limited resources (such as personnel or technology) to manage cyber risks.
- You are looking for a scalable solution that can grow with your organisation's security needs.

Works well with

Threat exposure management service

Providing a holistic and proactive approach to managing cyber security risks, helping you validate existing controls and stay ahead of emergency threats and vulnerabilities.

Managed firewall service

Taking on the day-to-day management of the firewall infrastructure, whether it's on-premises, or in a public or private cloud.

Managed Azure service

Work with a team of experts that can help you achieve all the benefits of Azure without the management burden. We provide round-the-clock availability, advanced techical support and secure management of your cloud resources.

What's included

Custom content

We create custom content for your needs, including detection rules and log onboarding.

Response actions

Leverages Defender's built-in response capabilities as part of our response plan.

Visibility

Gain access to our library of detection rules to ensure you make the right decisions for your organisation and insights into integrated threat intelligence feeds.

Response management

Major incident management, along with tickets and case management.

Accurate reporting

Regular reporting for peace of mind.

Reliability

Our security incident response team will be there to assist you if you face a potential threat.

Services that bring your technology to life

Contact your Softcat Account Manager today