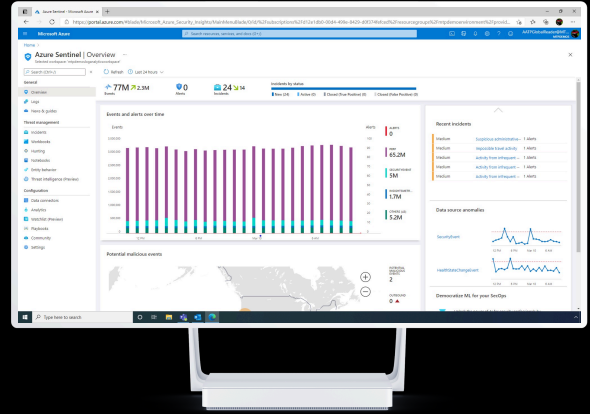





Microsoft Sentinel Accelerator

A two-month Microsoft Sentinel deployment service




Key Benefits

 **Maximise Security Capabilities:** Fully leverage the game-changing features of Microsoft Sentinel from day one.

 **Accelerate Deployment:** Achieve optimal efficiency in just two months.

 **Reduce Alert Fatigue:** Filter out noisy alerts, enabling you to focus on genuine threats.

 **Seamless Transition:** Easily migrate from your previous SIEM, integrating across all clouds and third-party products.

Navigating Today's Threat Landscape

In today's digital world, the threat landscape is more complex and volatile than ever. With cybercriminals leveraging increasingly sophisticated techniques to exploit network, application and device vulnerabilities the need for a robust, proactive and comprehensive security solution has never been greater.

Why Microsoft Sentinel?

Microsoft Sentinel's cloud-native SIEM capabilities are designed to provide market-leading security analytics and threat intelligence.

But it's not just about having the tools, it's ensuring they are configured and optimised to your unique needs to take advantage of its advanced capabilities enabling swift detection, investigation and response to threats, keeping your business secure.

Why CyberOne?

We understand that an effective security solution is only the result of a thorough setup, achieved through close collaboration. Our Microsoft Sentinel Accelerator program is designed to ensure that your security operations are not just powered by technology, but perfected through our expertise.

Microsoft Sentinel Accelerator Key Features

The Microsoft Sentinel Accelerator includes the essential features needed to optimise your security operations:

Comprehensive Scoping Session

Understand your specific business needs and infrastructure.

A Fully Integrated Setup

Connect your Microsoft estate, third-party solutions and cloud environments.

Optimal Log Source Configuration

Ensure maximum fidelity, visibility and value from your log data.

Threat Intelligence & Hunting

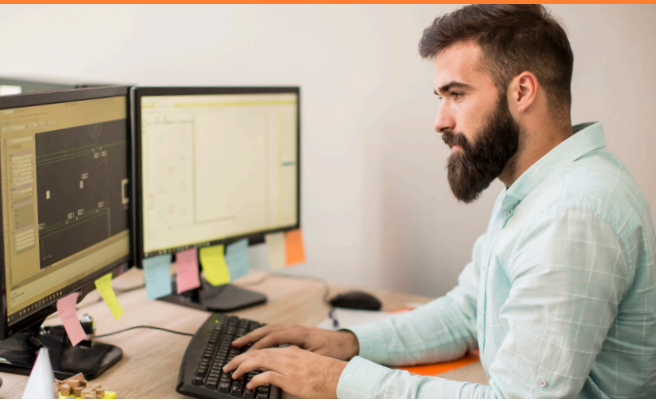
Configure intelligence sources and hunting capabilities for proactive security.

Custom Alert Rules & Playbooks

Develop tailored alert rules and automation workflows.

The Initial 5-Day Deployment

- Scoping session to understand your business requirements and infrastructure
- Integration with your Microsoft estate, 3rd party solutions and across multiple clouds
- Set-up of all log sources for optimal fidelity, visibility and value
- Configuration of threat intelligence sources and hunting capability
- Set-up of alert rules and playbooks
- Integration with your MISP threat intelligence environment



The 2-Month Microsoft Sentinel Accelerator

- Dedicated level 1 support and level 2 escalation
- Continual tuning and refinement of log sources
- Implementation of MDR use cases identified during deployment
- Continual categorisation and prioritisation of alerts
- Optimisation of data enrichment tools
- Configuration of watchlists
- Development of custom automation workflows
- Development of bespoke and dynamic playbooks
- 24x7x365 MDR and SOC option with triage and ticket resolution
- Creation of custom reports and dashboards within Sentinel
- Weekly 2-hour reviews and a final service review and summary report
- Easy transition to a fully managed service should you wish to continue with CyberOne after the Accelerator period

About CyberOne

Trusted by some of the world's most respected brands and organisations, CyberOne specialises in delivering end-to-end Microsoft Security solutions to secure mission-critical services.

From conducting Microsoft 365 security reviews and remediation to deploying integrated security services and Assure 365 our proactive managed detection and response solutions defending your operations against the most sophisticated threats.

Since 2005, CyberOne's mission has been to make the digital world a safer place, in close partnership with Microsoft. We measure our impact by our ability to reduce business risk and IT downtime. Cyber security is not just about providing a service; it's about being a strategic partner in our clients' success. Securing today, safeguarding tomorrow.

Take the First Step

Connect with our team today to understand how our Microsoft Sentinel Accelerator can maximise security performance and optimise costs with a comprehensive analysis.



+44 (0) 3452 757575

enquiries@cyberone.security

cyberone.security

