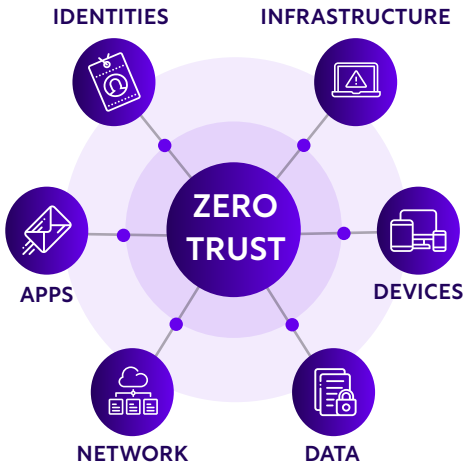
# Microsoft SOC Services

Advanced Managed Detection & Response (MDR) and Managed Extended Detection & Response (MXDR) services, delivered via the Chorus Cyber **24×7×365 Cyber Security Operations Centre** (CSOC) and powered by Microsoft Defender XDR and Microsoft Sentinel.

## Staying ahead of evolving cyber threats

Cyber security attacks are increasing in frequency and sophistication, which is why cyber security is a key business priority. Today, organisations need to reduce the likelihood of an attack, proactively detect threats, and rapidly respond to reduce potential business impact. To achieve this, organisations need the right processes and technology in place with a team of highly skilled security experts, however for many, this is uneconomical to build and maintain internally.

Delivered via the Chorus Cyber 24×7×365 CSOC, our managed security services help organisations stay protected in today's rapidly evolving threat landscape. Combining a highly qualified SecOps team, advanced automation and processes and underpinned by powerful Microsoft security technologies, we bring affordable enterprise-level security to organisations of any size.




## Microsoft MDR & MXDR Services

Our managed security services leverage Microsoft technologies to help organisations detect, investigate, hunt and respond to cyber security threats. We provide flexible managed security services, allowing organisations to choose the right level of protection to meet their security requirements.

### MDR

Advanced threat detection and containment services to protect all of your identities and endpoints including 1x firewall.

(Defender for Endpoints & Sentinel)

### MXDR

Extended threat detection and containment across your entire Microsoft E5 security tooling + various third party sources.

(Defender Stack & Sentinel)

# Microsoft MDR & MXDR Security Services

## Service Benefits

**24×7×365 Advanced CSOC** – Our 24×7 CSOC makes best use of technical innovations and cutting-edge security technologies to deliver an advanced service. Underpinned by a team of highly skilled and experienced CSOC analysts, we will protect your organisation around-the-clock.

**Leading technical architecture** – Built on Microsoft Defender XDR and Microsoft Sentinel, our CSOC architecture is built to best-practice benefiting from advanced automation, machine learning and AI to reduce alert noise and accelerate threat detection and response speed and accuracy.

**Rapid threat detection and response** – Through our skilled SecOps team and use of automation, we ensure cyber threats are quickly identified, investigated and remediated – reducing the likelihood and potential impact of successful attacks, to keep your organisation ahead of evolving threats.

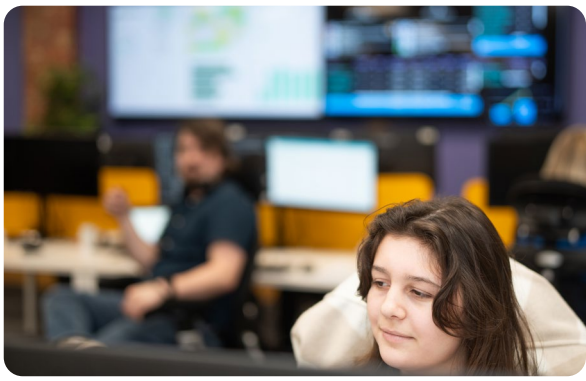
**Maximise the value of your Microsoft licensing** - With most organisations already using Microsoft 365, we use the powerful security features available to maximise the value of your licensing, removing third party costs and consolidating technologies to reduce complexity.

**Proactive and preventative protection** – We take our managed security services a step further by building in pre-emptive protection through advanced threat hunting and cyber threat intelligence to proactively block emerging and unknown threats before they occur.

**Cyber risk reduction** – With proactive threat detection, investigation, hunting and response, your organisation is better protected and cyber risk is greatly reduced. This helps you to reduce cyber insurance premiums, meet compliance regulations and benefit from peace of mind against increasingly costly attacks.

## CSOC Metrics

| | |
|---|---|
| <5 mins | Mean Time to Acknowledge (MTTA) |
| <20 mins | Mean Time to Close (MTTC) |
| 50% | Incidents closed by automation |



## WHAT'S INCLUDED?

- 24×7×365 CSOC
- Flexible Coverage
- 24×7 Monitoring
- Proactive Cyber Threat Intelligence (CTI)
- Threat Detection
- Threat Triage & Investigation
- Rapid Threat Response & Containment
- Proactive Threat Hunting
- Service Governance & Reporting
- Security Reviews & Recommendations
- Streamlined Service Transition
- Microsoft Security Guidance

# Services Compared

## Which level of service is right for you?

| SERVICE COMPARISON | | MDR | MXDR |
|---|---|---|---|
| 24×7×365 CSOC | | ✓ | ✓ |
| Analysts available by phone 24×7 | | ✓ | ✓ |
| 30 minute high severity SLA | | ✓ | ✓ |
| Containment and response actions | | ✓ | ✓ |
| Chorus proprietary analytic rules | | ✓ | ✓ |
| Microsoft Security suite coverage | Defender for Endpoint | ✓ | ✓ |
| | Defender for Identity | | ✓ |
| | Defender for Cloud Apps | | ✓ |
| | Defender for Office | | ✓ |
| | Defender for Cloud | | ✓ |
| | Azure services | | ✓ |
| Microsoft Sentinel custom integration | | | ✓ |
| Threat Detection & Response Coverage | Endpoints | ✓ | ✓ |
| | Entra ID Identities | ✓ | ✓ |
| | Servers | ✓ | ✓ |
| | Active Directory Identities | | ✓ |
| | Non-Azure cloud services | | ✓ |
| | Networking log sources (Firewalls/Switching/APs) | | ✓ |
| | 3rd Party APIs/Logs | | ✓ |
| Weekly security service reports | | ✓ | ✓ |
| Cyber Essentials aligned TVM report | | ✓ | ✓ |
| Endpoint threat hunting | | ✓ | ✓ |
| Cyber Threat Intelligence | | ✓ | ✓ |
| Standard security playbooks | | ✓ | ✓ |
| Security recommendations & guidance | | ✓ | ✓ |
| Service governance | | ✓ | ✓ |
| MITRE ATT&CK framework mapping | | ✓ | ✓ |
| Custom security playbooks | | | ✓ |
| Extended threat hunting | | | ✓ |
| External attack surface monitoring | | | ✓ |

## MDR & MXDR

**Two flexible 24×7 managed security services, allowing organisations to choose the right level of protection.**

## Microsoft-verified MXDR

Our MDR & MXDR services are delivered through our partner, Chorus Cyber and their 24×7×365 CSOC. Chorus are members of the Microsoft Security Intelligent Association (MISA) and awarded Microsoft-verified MXDR solution status.

Member of
Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

# MDR

**Our MDR service delivered by our 24×7 CSOC, helps organisations rapidly identify, investigate, proactively hunt, and remediate cyber security threats across their endpoints.**

With an estimated 70% of cyber security threats starting on endpoints and the continuing rise of remote working and BYOD, devices are a common attack surface that need to be actively monitored and protected. We leverage the power of advanced automation, AI and proactive cyber threat intelligence, using Microsoft Defender for Endpoint and Microsoft Sentinel to rapidly detect and remediate threats across your devices.

## SERVICE FEATURES

- **24×7×365 CSOC** - Our highly skilled SecOps team are available 24×7 to offer round the clock protection and support.
- **Endpoint Threat Detection & Investigation** – Our MDR service proactively monitors, identifies and responds to threats across your endpoint environment by using Microsoft Defender for Endpoint to analyse, contain and remediate threats.
- **Automated Response** – We provide automated threat containment and remediation through agreed security playbooks and SOAR capabilities to rapidly isolate devices, contain threats and reduce their impact.
- **Cyber Threat Intelligence (CTI)** – We continually integrate threat intelligence from external sources, as well as CTI from our CSOC team. Taking this a step further, we automatically feed emerging Indicators of Compromise (IOC) into our playbooks to block malicious content, so that you stay ahead of continually evolving adversarial tactics and techniques.
- **Proactive Threat Hunting** – Through manual and automated threat hunting we identify early indicators of emerging threats, tactics or procedures (TTPs), to stay ahead of emerging cyber threats.
- **Reporting & Analytics** – Weekly digestible email reports that highlight security metrics so you have a frequent, high-level overview.
- **Service Governance** – Through quarterly operational security reviews and annual security reviews, we evaluate key service metrics, review security trends and discuss strategic goals.
- **Security Recommendations** – We share recommended security improvements as part of our continual service improvement, to eliminate risks and reduce your attack surface.

70%

An estimated 70% of successful breaches start on endpoint devices

Source: IDC Research

## SERVICE BENEFITS

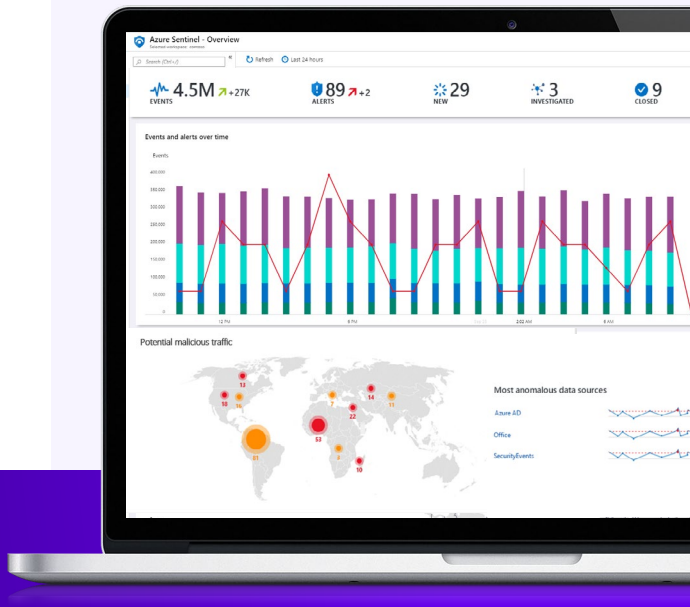
Protect your most vulnerable attack surface with 24×7 monitoring, detection and response to reduce your endpoint security risk.

Advanced threat detection using Defender for Endpoint, enhanced with AI analysis, machine learning and automated investigation to detect advanced and sophisticated attacks.

Rapid response and threat containment through automated responses, manual investigation and security playbooks to quickly contain threats and isolate devices to remove or reduce their impact.

Microsoft security expertise ensures skilled investigation and remediation as well as guidance on best practice implementation so you get the most from your Microsoft licensing.

Proactive threat reduction to reduce the likelihood of future attacks through threat hunting, proactive CTI to block emerging threats and ongoing security recommendations.



# MXDR

**Our MXDR service ensures 24×7 threat detection and response to keep your cloud environments secure. We provide integrated protection across your endpoints, identities, Microsoft 365, SaaS apps and email to rapidly detect and respond to threats, making best use of automated response capabilities to support long-term success in the cloud.**

| | |
|---|---|
| 187 days | On average to detect a security breach |
| £720,000 | Saved if breach contained within 30 days |

Source: IBM, Cost of a Data Breach Report 2021

## SERVICE FEATURES

- **24×7 CSOC and skilled analysts** – Our Security Analysts are available 24×7×365 offering continuous monitoring and protection.
- **Extended Threat Detection & Investigation** – 24×7 threat detection across your entire estate using advanced XDR, including endpoints, network, infrastructure (on-premise and cloud) and the ability to ingest events from any API or source for complete coverage.
- **Proactive Threat Intelligence** – Continuous cyber threat intelligence (CTI) integration from wide-ranging sources is used to take proactive action and block emerging threats to better defend your organisation.
- **Custom Threat Detection Rules** - Creation and management of bespoke threat detection rules above out-of-the-box and Chorus detection rules to meet your unique cyber security requirements.
- **Rapid Threat Response** – Automated security playbooks instantly respond to common tasks and threats, while sophisticated attacks are rapidly investigated and mitigated by our CSOC analysts, reducing time to detect and respond to threats and their potential impact.
- **Custom Security Playbooks** – We expand upon our library of built-in and Chorus security playbooks with custom playbooks to automate investigation or response actions in-line with your security policies.
- **Extended Threat Hunting** – Advanced threat hunting and vulnerability management across your entire estate to proactively identify and protect against new and emerging threats.
- **Service Governance and Reporting** – Regular service governance, account management and reporting ensure optimal service delivery and drive continuous service and security improvement.
- **Security Advisory** – We continuously feed security recommendations and guidance into your teams and security strategy based on the metrics we gather so you benefit from a proactive and forward-thinking roadmap.
- **Service Transition** – Through our standardised service transition and a rapid technical onboarding using Azure Lighthouse, we ensure all key information is captured and you can be up and running quickly.

## SERVICE BENEFITS

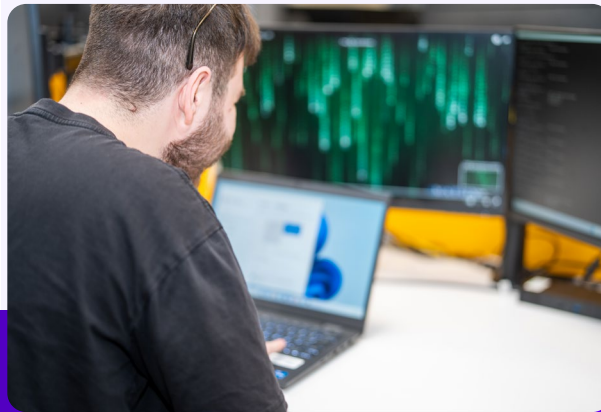
Extensive threat visibility across your estate, covering endpoints, networks, infrastructure (on-premise and cloud) and any other sources to ensure fewer blind spots and reduce gaps in threat detection visibility.

Automatically detect sophisticated threats across any source with integrated threat detection, AI-based analysis and custom detection rules.

Better leverage advanced automation, AI and machine learning capabilities to automatically investigate and respond to threats across your estate against agreed security playbooks.

Enrich events with holistic contextual information to reduce alerts and prioritise those that matter, increasing CSOC efficiency and reducing alert noise and fatigue.

Faster detection and response times by eliminating common threats through automation whilst advanced attacks are prioritised by our CSOC team.



# Service Transition

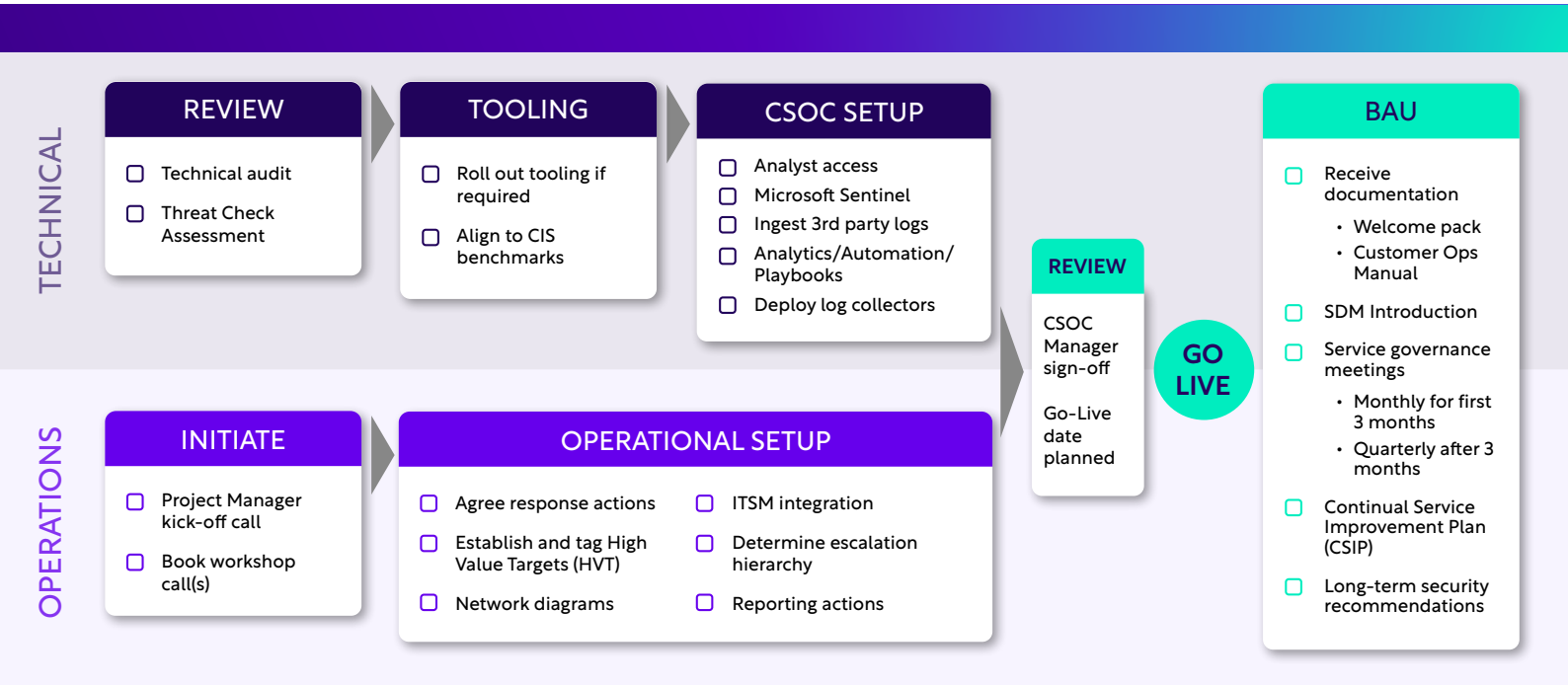
**Our standardised service transition model means that we can get you onboarded quickly and efficiently. Following a consistent and proven approach, we work closely with you to gain a detailed understanding of your organisation and ensure everything is setup, so you can experience great service from day one.**

## TRANSITION PROCESS

Our transition model is split into two key streams: service and technical onboarding. Working with a dedicated project manager and technical contact, we will guide you through the transition process to gain an in-depth understanding of your environment, processes and capabilities to ensure that our service meets your requirements and all key information is captured.

As part of our technical onboarding we carry out a Cyber Threat Assessment to feed recommendations into your ongoing security strategy and help further strengthen your security posture. Using Azure Lighthouse, we enable rapid technical onboarding whilst ensuring you retain precise control and visibility over the delegated services.

Once live, we actively monitor threats and alerts being raised and use this telemetry to fine tune any rules and playbooks before going into operational service. With regular service governance reviews, account management and reporting, we continue to work closely with you for ongoing security posture enhancements and continual service improvement.




## Contact us

partners@choruscyber.com | www.choruscyber.com

chorus cyber