G-Cloud 15 Lot 3 - Cloud Support
SOC Services Overview

Prism Infosec

Prism Infosec supports organisations globally to prepare for, respond to and manage cyber security threats.

Prism Infosec & Chorus SOC Services

Prism Infosec's partnership with Chorus will allow us to provide our clients Managed Cyber Security Operations Centre (CSOC) & Managed Detection and Response (MDR) services. Our comprehensive offerings include 24x7x365 threat detection powered by Microsoft's cloud-native MXDR, SIEM/SOAR technologies, Microsoft 365 Defender, and Microsoft Sentinel.

Chorus is one of the UK's leading Microsoft partners and are on a mission to build a more secure world of business, where you can thrive with modern Microsoft technology, in a new era of cyber threats. Being a leading Microsoft partner and proud members of the Microsoft Intelligent Security Association (MISA), makes Chorus one of the most reliable and trusted Microsoft-focused security companies across the globe. The Managed Security services have been awarded Microsoft-verified MXDR solution status, proving the calibre of the service.

Why Partner with Prism Infosec & Chorus

- Our people – We are a services company first and foremost. That means that we place our emphasis on our people delivering an excellent service. In comparison, many other MDR providers are a product/technology company first with services second. Our people are highly skilled and we place a great deal of importance on culture, as we know happy staff deliver great results. While we focus heavily on delivering innovative automations, you can rest assured that incidents are being analysed and responded by highly trained security analysts and you are working with real people that are available to speak to at any time.
- Built on Microsoft – Our CSOC has been built from the ground up using the latest cloud and machine learning innovations within Microsoft Security. By building our CSOC on Microsoft technologies, you benefit from advanced security technologies with unmatched telemetry, ability to use existing Microsoft licensing to remove third party costs, and the integrated remediation capabilities that come with having MDR services built upon the same stack as your Microsoft 365 productivity suite.
- Our impressive metrics – We have the statistics to prove what say. Our Mean Time to Acknowledge (MTTA) is under 3 minutes and our Mean Time to Respond (MTTR) is less than 17 minutes - far faster than industry standards. Everything we build – and continue to build through ongoing development – is focused on improving our detection and response times and reducing customer risk.
- Our team mentality – We don't want to just onboard you as a customer and stay silent. We focus on working together in partnership. We feed in security insights and continual security and service improvements to keep you evolving and staying ahead of threats – through our reports, service governance and reviews, as well as simply being at the end of the phone.
- Our reputation – We've got the badges and accreditations to validate what we do. We are proud members of the Microsoft Intelligent Security Association (MISA) and our services have been awarded Microsoft-verified MXDR status, which only a limited number of organisations hold globally, attesting to the calibre of our service.

Benefits and Outcomes

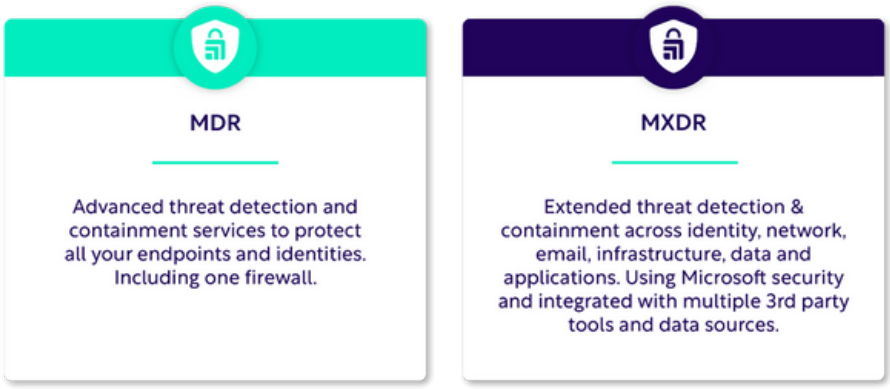
- Reduces your cyber risk – The core focus of what we do is reducing your cyber risk. Our services greatly reduce the risk of a breach and the potential impact of a successful breach.
- Assess to security experts 24x7 – Our CSOC operates 24x7x365, so you can contact our experts any time of day, giving you access to a team of highly skilled security staff.
- Delivers a cost-effective service – Our managed security services give you an advanced security service at a vastly lower cost to building an in-house security function.
- Peace of mind – With 24x7 protection, a one-hour response SLA and analysts available any time of the day, you can rest assured your estate is being continually monitored and protected.
- Keeps you continually improving – Our insights and recommendations feed into your security roadmap to keep your security strategy advancing and remaining ahead of evolving threats.

Managed Security Services (MDR & MXDR)

Our Cyber Security Operations Centre (CSOC) delivers 24x7x365 Managed Detection & Response (MDR) and Managed Extended Detection & Response (MXDR) services globally.

Powered by Microsoft Sentinel and Microsoft Defender XDR, our CSOC delivers services that quickly stop breaches and advanced threats, providing rapid response around-the-clock to keep you ahead of attackers.

We have two service offerings so that you can choose the right service to suit your organisations requirements. The key difference between the services are the levels of coverage.



MDR

Our MDR service is delivered by our 24x7x365 CSOC. The service helps you rapidly identify, investigate, proactively hunt, and remediate cyber security threats across your endpoints.

MXDR

Our MXDR service ensures 24x7 threat detection and response to keep your data secure across cloud and on-premises environments.
The service provides integrated protection across your endpoints, identities, Microsoft 365, SaaS apps, and email. We rapidly detect and respond to threats, making best use of automated response capabilities to support long-term success in the cloud.

CSOC Statistics

With our focus on rapid threat detection and response, our service statistics are far higher than industry standards. Our ability to detect a threat in under 5 minutes and then respond and close in under 20 minutes shows the speed of our service and the reduction in your cyber risk.

Service Comparison

SERVICE COMPARISON		MDR	MXDR
24×7×365 UK-based 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			✓

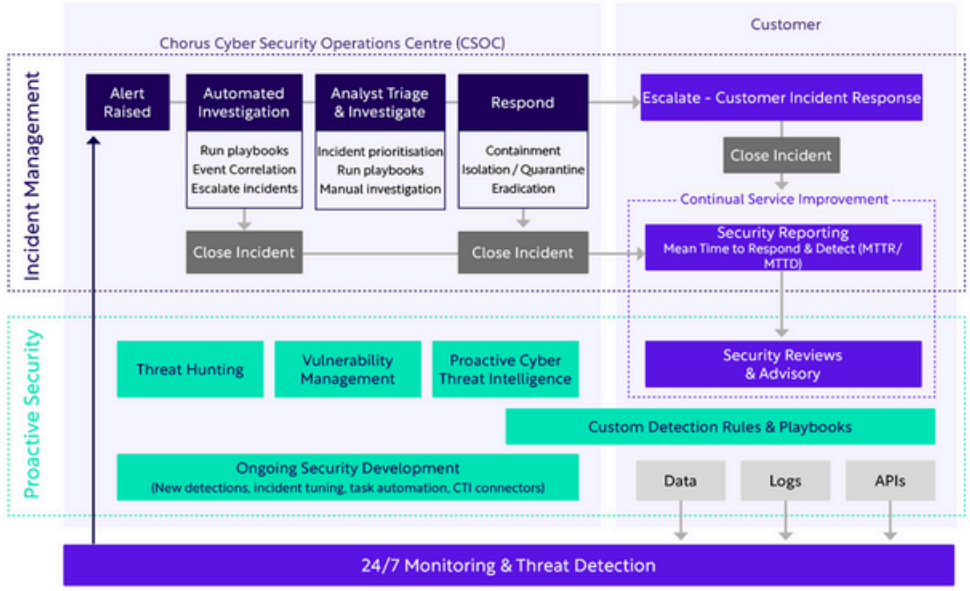
Service Overview

Service processes

During the service, the Chorus CSOC will be responsible for the initial triage, investigation, and response to any security incident. We will contact you directly if we need your action or input (an escalation). We will also inform you of any actions we take in response to an alert.

All responses and escalations are clearly agreed during the onboarding process, so we follow a standardised and agreed process with you. You will also get emails from us about new emerging threats, with details about the threat, our approach, and how we will protect your environment.

Across Microsoft 365, security incidents will be raised in several places, but Microsoft Sentinel will be the authoritative source for any SecOps incident. The division of customer and Chorus CSOC responsibilities is presented in the diagram below.



Prism Infosec

prisminfosec.com

Prepare

Prepare your organisation for cyber security threats.

Prepare your organisation for cyber security threats. Understand your current posture and strengthen your defences. We can help you get ahead of the risks with tailored testing, preparedness services and red teaming.

- Cyber Security Assessments & Penetration Testing
- Cloud Security
- Red Teaming & Simulated Attack
- Regulated Testing Schemes

Respond

Respond effectively to cyber security incidents.

Take control when incidents strike and recover with the confidence to move forward. Specialist support to help you respond to cyber threats and restore operations quickly.

- Remediation Services
- Incident Response
- Digital Forensics

Manage

Manage your ongoing cyber security resilience.

Build long-term resilience with ongoing support and consultancy. From strategic governance to fully managed SOC services and incident response retainers.

- Managed Security Services
- GRC & Security Consulting
- Compliance Services
- vCISO

About Prism Infosec

Prism Infosec is an Information Security company based in Cheltenham and Liverpool and was founded in 2006. The Company has delivered information security consultancy and assessment services to some of the world's largest organisations including private enterpise, public sector, government, defence and healthcare. Uniquely, Prism Infosec's consultants possess both a business and management focus, but also a diverse range of technical skills. Whether delivering advice on cutting edge information security architectural solutions, conducting management controls audits, or in-depth technical penetration testing, our consultants always deliver a quality end-to-end service.

To book an assessment call:
+44 (0) 1242 652100

Send us an enquiry email:
contact@prisminfosec.com