JUMPSEC

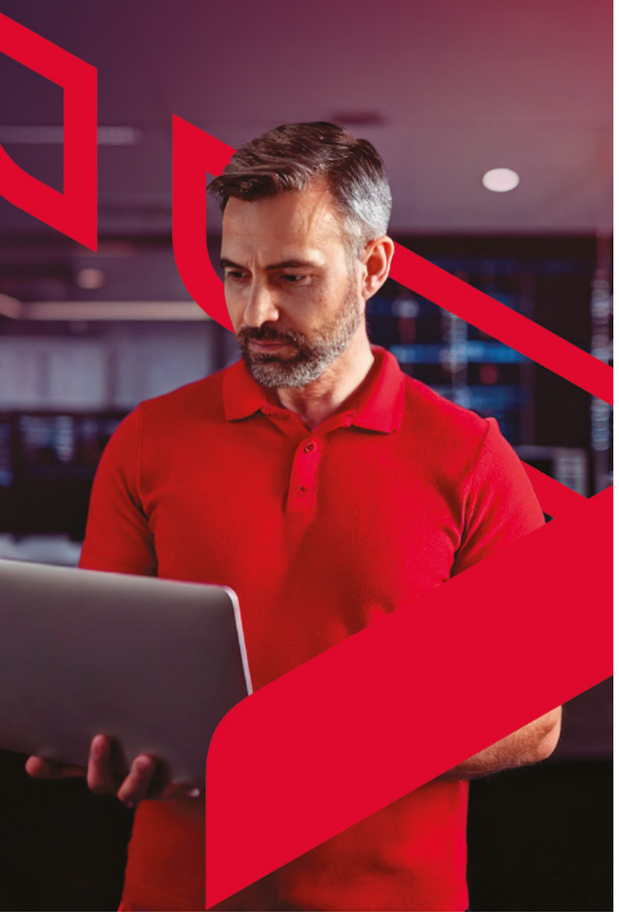
Managed Extended Detection and Response Service

MXDR (Managed Extended Detection and Response) is JUMPSEC's Microsoft-native threat detection and response service.

Built by experienced incident responders from the ground up, it delivers what traditional SOC services cannot: rapid triage, tailored containment, and meaningful protection against real-world threats.

jumpsec.com | 0333 939 8080 | hello@jumpsec.com

Built by Seasoned Incident Responders



First generation Security Operations Centre (SOC) and Managed Detection and Response (MDR) services are falling short. Traditional services are often developed by engineering teams focused on technical proficiency who lack an understanding of real-world attack scenarios.

Our MXDR service is built by seasoned Incident Responders with firsthand experience protecting organisation in critical cyber incidents, enabling them to contextualise threats, prioritise response activity, and fully attune your existing technology stack to ensure comprehensive detection and response coverage where you need it most.

Tailored, Threat-Led Detection

Unlike traditional SOCs, we understand that each client is unique, and we build custom detections aligned to what matters most to each client's risk profile, sector, and business operations – reducing noise and increasing precision. The result: a dynamic defensive posture that anticipates and mitigates emerging threats.

Active Cyber Defence

We proactively mitigate cyber threats by identifying high-risk attack scenarios and implementing countermeasures. Our threat-led methodology ensures a focus on critical security risks, from initial implementation to continuous MXDR service evolution. Combining automation with expert analysis, JUMPSEC enables rapid detection and response, distinguishing itself from other MDR providers that may lack advanced tools, incident response expertise, or operational maturity.

Core Service Pillars

Tailored Detection Engineering
We write, and tune detections based on your environment, not generic templates.

Active Threat Hunting
Ongoing analysis to identify stealthy or dormant threats.

Built on Microsoft Security Stack
Defender for Endpoint, Defender for Identity, Sentinel, and Purview.

Triage & Containment
We are IR Experts - Real-world decisions made by real-world responders.

Threat Actor Monitoring
Aligned to threats most likely to impact your sector or geography deployed technologies.

Service Management
Live dashboard, in-depth activity trend analysis, and threat landscape updates to drive continuous improvement.

Why the 'X' in MDR is Key

The "X" in MXDR represents the extended capabilities beyond traditional MDR services, encompassing various facets.

'X'tended capabilities

Core MDR service

Let's show you how we build the right detections within your estate:

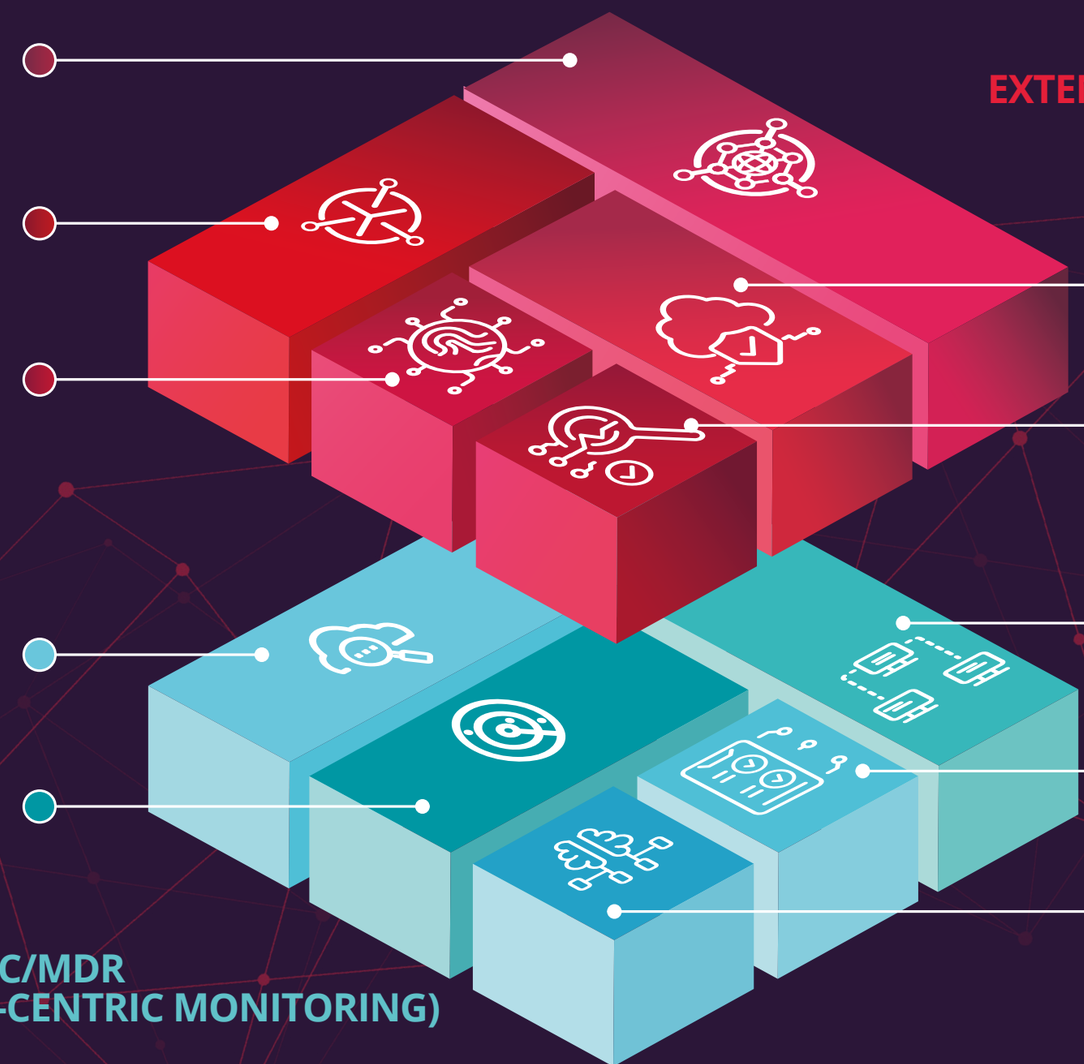
Where MXDR Has You Covered

Stop Relying on Default Rules. Start Detecting What Matters to You.

IoT and OT Coverage & Expertise
Protecting operational technology, industrial control systems, and unmanaged devices.

Edge Access & Device Coverage
Securing external-facing infrastructure like routers, VPNs, and remote access points.

Identity & Access Management (IAM) Logs
Monitoring authentication, privileged access misuse, and MFA bypass.



Cloud Security Monitoring (Basic)
Limited monitoring of major cloud services (M365, AWS, Azure).

24/7 SOC Alert Monitoring & Incident
Handling Responding to security events.

TRADITIONAL SOC/MDR (CORE NETWORK-CENTRIC MONITORING)

EXTENDED MXDR (ADVANCED THREAT VISIBILITY – EXTENDING BEYOND THE PERIMETER)

Cloud Security Logs (Deep Visibility)
Advanced analytics for SaaS applications, containers, and hybrid environments.

Cutting-Edge Threat Intelligence
Leveraging TTP-driven insights, custom YARA rules, and real-time threat feeds.

Endpoint Detection & Response (EDR/XDR Agents)
Traditional endpoint monitoring.

SIEM Log Aggregation & Correlation
Collecting logs from core security tools.

Basic Network Traffic Analysis (NDR/NTA)
Detecting lateral movement inside the network.

How JUMPSEC MXDR Differs From Traditional SOCs

	Traditional SOC	JUMPSEC MXDR
Detection Approach	Static alert rules	Tailored threat-led detections
Response Speed	Alert triage in hours/days	Triage + containment in real time
Built For	Compliance + monitoring	Incident response
False Positives	High	Tuned to reduce noise and increase precision
Value to Client	Reactive visibility	Active risk reduction
Alignment to Business Risk	Generic	Mapped to business priorities
Ownership	Outsourced alerting	Embedded extension of the client team

Built by Responders, Not Monitors

This isn't just another alerting platform – it's an incident response-ready managed service designed by professionals who have lived through high-stakes breaches. It's fast, decisive, and tailored.

Real-Time Triage and Containment

We don't just raise tickets – we take action. Our MXDR service provides rapid triage and containment, drastically reducing the time to respond and limit business impact. In fact, whilst JUMPSEC responds to the associated incidents almost constantly, none has developed into a major compromise or breach – None of JUMPSEC's clients have had a breach on our watch.

Maximises Microsoft Security Investment

Many organisations have the Microsoft stack but aren't leveraging it effectively. We activate and operationalise it – turning underused tools into a powerful, cost-effective defence capability. We also can spot opportunities to reduce unnecessary cost.

More Than a SOC - We're a Partner

JUMPSEC MXDR integrates with your team, regularly reviews and improves posture, and provides access to CIR-accredited IR support when it matters most.

Highly Accredited Experts

Including CREST and NCSC-certified teams, deliver top-tier security services.

T: 0333 939 8080 **E:** hello@jumpsec.com

What Our Clients Say

For over a decade we have been building strong relationships with our clients.

Find out how we have enabled them to future proof their cyber defences:

"It has been a pleasure working with JUMPSEC, the team are extremely talented, professional, and it was an easy decision to renew the service."

Toob Ltd

"They are a true partner in every sense of the word and effectively are an extension of our team. This close relationship means we are able to offer a truly excellent security service"

Head of Cyber Security, Groupe Atlantic

"The level of service is unparalleled from JUMPSEC. Never standing still they undersatnd our business completely. We are a team and our business is safer by working with JUMPSEC"

IT Director, London Borough of Ealing

JUMPSEC

JUMPSEC offers a comprehensive suite of services, to cater to your unique needs and risk profiles. By working in partnership with you we improve your cyber resilience. Tailoring our services to your organisation's needs, budget and desired security posture.

To Learn more about JUMPSEC's services please feel free to get in touch:

Call us on	**0333 939 8080**
Send us an Email	**hello@jumpsec.com**
Visit us at	**jumpsec.com**