CYBER SECURITY MEETS BUSINESS STRATEGY

MDR XP360 - 24/7 threat detection, rapid incident response, and continuous security monitoring.

2-sec Limited, Tower 42, Old Broad Street, London EC1N 1HN
+44 (0) 207 877 0060
contact@2-sec.com

Why do I need MDR XP360?

Cyber threats are evolving rapidly, and organisations must stay ahead to prevent financial loss, reputational damage, and operational disruptions. MDR XP360 provides continuous monitoring, real-time threat detection, and rapid incident response, ensuring that your business is protected from cyberattacks before they cause harm. With proactive threat intelligence, automated security measures, and expert support, MDR XP360 helps you maintain compliance, secure critical assets, and focus on business growth without the burden of managing cybersecurity in-house.

Why trust 2-sec?

At 2-sec, we have over 14 years of experience helping more than 500 clients navigate complex security and compliance challenges. As a trusted Qualified Security Assessor Company (QSAC), we hold CREST and NCSC CHECK accreditations, demonstrating our commitment to excellence. Our MDR XP360 service combines advanced technology, expert threat intelligence, and a dedicated cybersecurity team to provide real-time threat detection, rapid incident response, and continuous monitoring. When you choose us, you gain proactive threat management, industry-leading expertise, cost-effective solutions, and the confidence that your cybersecurity is in the hands of experienced professionals.

MDR XP360 Benefits

- Proactive Threat Management: Stay ahead of cyber threats with proactive monitoring and response strategies.
- Expertise: Leverage the knowledge of seasoned cybersecurity professionals without the need for in-house resources.
- Cost-Effective: Reduce overhead costs associated with hiring and training a full-time security team.
- Peace of Mind: Focus on your core business operations while we handle your cybersecurity needs.
- Named point of contact: a dedicated named individual to engage with your organisation.

Underlying Technology Platform

The MDR XP360 service from 2-sec is built on a robust and sophisticated technology platform designed to deliver comprehensive threat detection, incident response, and continuous monitoring. Our platform integrates advanced tools and technologies to provide real-time visibility and proactive defence against cyber threats. Below are the key components of our technology stack:

Security Information and Event Management (SIEM)

- Centralised Log Management: Collects and aggregates logs from various sources including servers, network devices, endpoints, and cloud environments.
- Real-time Analytics: Using machine learning and behavioural analytics to detect anomalies and correlate events that indicate potential security incidents.
- Incident Response Automation: Facilitates automated responses to common threats, reducing response times and minimising damage.

Vulnerability Management Tools

- Continuous Scanning: Regularly scans IT assets for vulnerabilities, misconfigurations, and weaknesses in security controls.
- Risk Prioritisation: Classifies vulnerabilities based on severity and potential impact, allowing organisations to focus on the most critical issues first.
- Remediation Guidance: Provides actionable insights and recommendations for patching and mitigating identified vulnerabilities.
- Patching: Deploys system and security updates to endpoints quickly and without intervention to reduce exposure to known and unknown threats.

Cloud Security Solutions

- Cloud Workload Protection: Monitors and secures cloud environments (IaaS, PaaS, SaaS) against misconfigurations and threats.
- API Security: Protects APIs that are integral to cloud services from potential exploits.
- Compliance Monitoring: Ensures adherence to cloud security standards and regulations.

Orchestration and Automation

- Security Orchestration: Leverages Security Orchestration, Automation, and Response (SOAR) capabilities to streamline security operations.
- Automated Workflows: Implements automated playbooks for incident response, reducing the manual workload on security teams.
- Integration with Third-Party Tools: Seamlessly connects with existing security tools and platforms for enhanced operational efficiency.

User Behaviour Analytics (UBA)

- Insider Threat Detection: Monitors user behaviour patterns to identify anomalies that may indicate insider threats or compromised accounts.
- Behavioural Baselines: Establishes normal user behaviour baselines to detect deviations that could signify malicious activity.
- Risk Scoring: Assigns risk scores to user activities, enabling prioritisation of investigations.

Reporting and Dashboards

- Custom Dashboards: Provides real-time visibility of security posture through customisable dashboards tailored to organisational needs.
- Compliance Reporting: Generates reports that assist in meeting compliance requirements and demonstrating security effectiveness to stakeholders.
- Incident Reporting: Offers detailed incident reports that document actions taken and lessons learned during security events.

Our Packages

2-sec offer the following annual MDR XP360 service packages:

Bronze	Silver	Gold
Basic monitoring and alerting.	Comprehensive monitoring and response.	All features of Advanced MDR.
Monthly security reports.	Weekly threat intelligence updates.	Custom threat intelligence feeds.
Incident response assistance.	Vulnerability management and remediation guidance.	Full forensic investigation and compliance support.
	Annual pen test of perimeter	Endpoint Patching, Script Execution and Roll-back.
		Quarterly pen testing of three critical business applications or API.

Pricing is customised based on the size of the organisation, the complexity of the environment, and specific service requirements. Contact us for a personalised quote.

Get in touch today and let us walk you through the options.