Managed Detection & Response

www.zdlgroup.com

A Proactive Approach to Cyber Security

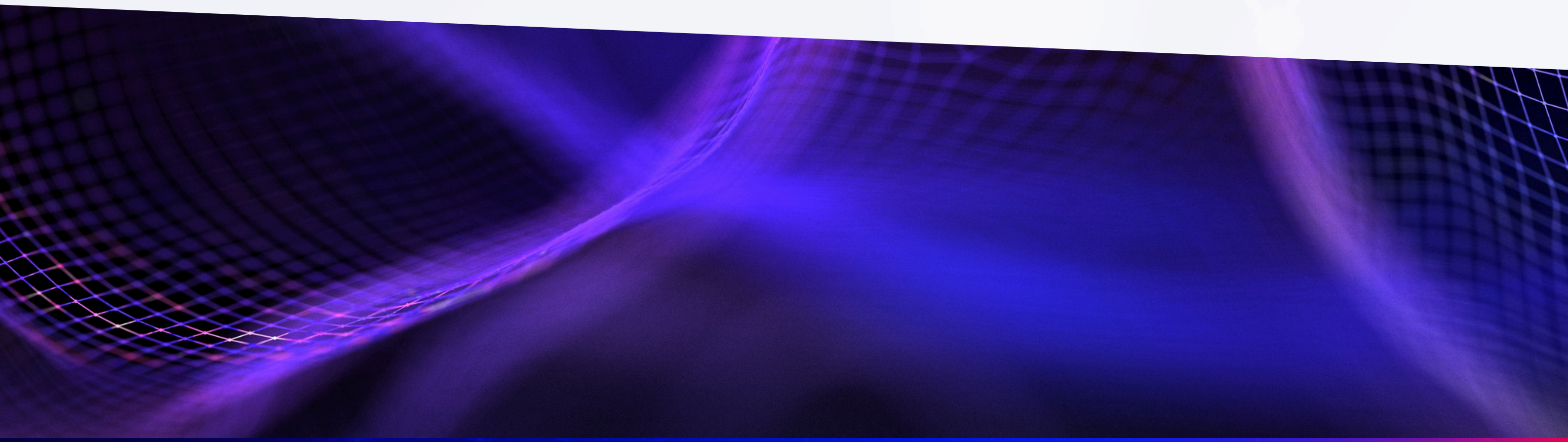
We live in an era where blind spots in detecting and reacting to early indicators of compromise can be punishing. Without a focus on detecting new and unseen attacks, organisations are left exposed and vulnerable to large scale breaches and the full spectrum of associated potential damage.

The best approach to proactive cyber security requires both technology that can identify potential attacks and skilled cyber security analysts who are armed and ready to investigate and mitigate these threats.

Round-the-clock monitoring and response

ZDL Groups Managed Detection and Response (MDR) powered by Wavenet CyberGuard is a proactive cybersecurity service that combines advanced threat detection, incident response, and continuous monitoring capabilities to defend against evolving cyber threats.

This combination of technology and human expertise perform threat hunting, monitoring, and response with the goal of rapidly identifying security incidents in real-time limiting the impact of threats.



This combination of technology and human expertise perform threat hunting, monitoring, and response with the goal of rapidly identifying security incidents in real-time limiting the impact of threats.

Our solution is designed to collect, monitor, and analyse information presented by the subscribed services, leveraging up-to-date threat intelligence feeds and data to enhance our detection capabilities and stay ahead of emerging threats. This proactive approach enables us to better protect a businesses or organisations critical assets.

In today's dynamic and evolving threat environment, we understand that busy IT teams don't have the time or resources to do threat analysis of emerging threats on their own. Our skilled security professionals possess in-depth knowledge and expertise in dealing with cyber threats. They actively monitor and analyse network traffic, system logs, and endpoint data, allowing for the early detection of potential threats and the rapid response to security incidents.

Threat Intelligence

Rapid Response

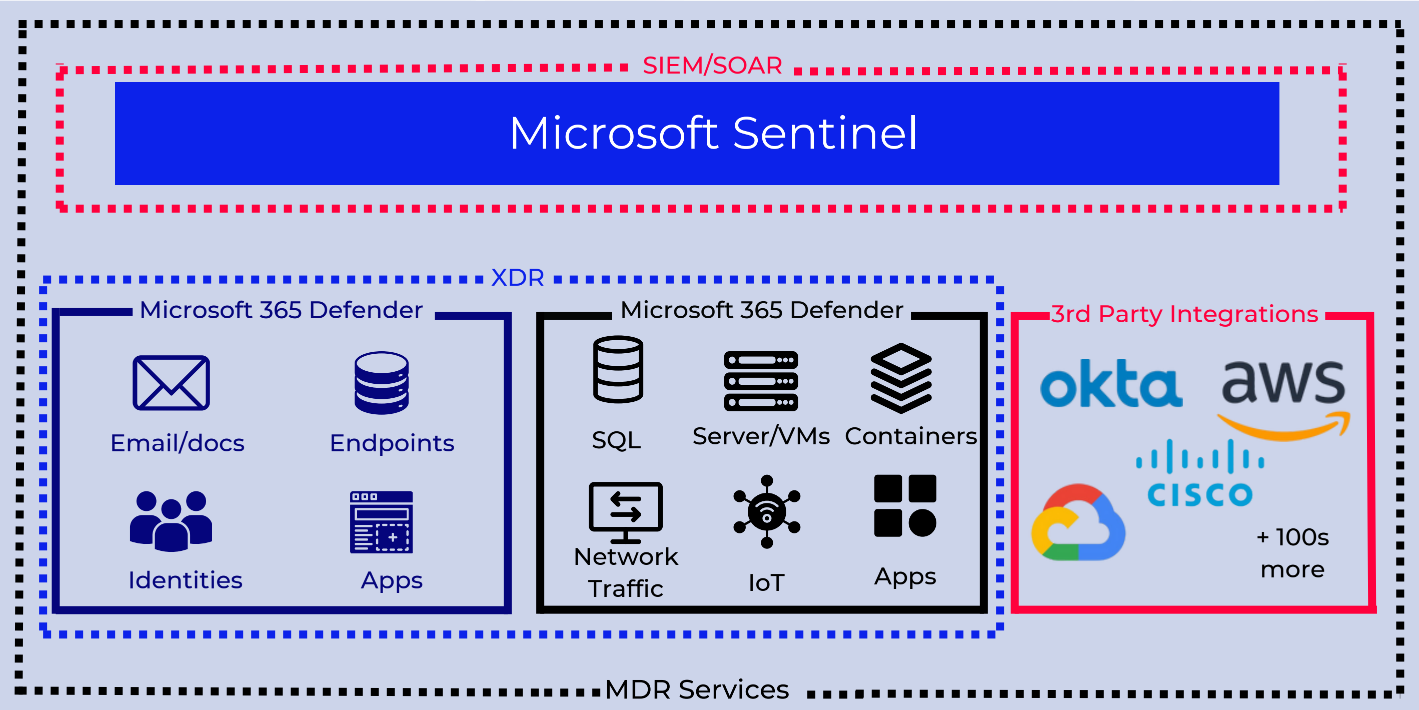
Accredited Professionals

24/7 Coverage

C-SOC Support

Product Customisation

Our MDR service enhances an organisation's security posture, minimises the risk of breaches, and provides peace of mind in an increasingly complex threat landscape. ZDL Group Ltd empowers organisations to strengthen their defences, and ensure the confidentiality, integrity, and availability of their critical data and systems.



Managed Security Operations Centre

At the heart of our cybersecurity efforts lies our UK-based Security Operations Centre (SOC), operational 24/7. This dedicated team comprises seasoned and accredited cybersecurity experts, diligently sifting through a multitude of alerts from various sources.

Choosing our SOC brings many advantages. Foremost among them is the capability to detect and counteract security threats in real-time, curtailing their potential to inflict substantive damage or result in financial losses. With vigilant eyes on networks, systems, and applications, our SOC ensures that deviations and questionable activities are swiftly detected and addressed.

Features and benefits

Threat Detection and Response

Incident Management

Proactive Threat Hunting

Enhanced Incident Response Time

Better Visibility

Reduced Costs

Our SOC delivers the following MDR Services

Managed SIEM

Our state-of-the-art SIEM solutions, powered by Microsoft Sentinel, ensures a comprehensive view of your security landscape. Through intelligent log analysis and event correlation, we spotlight unusual patterns and behaviours, facilitating quicker incident response and better threat visibility.

Managed EDR

We recognise the need for a layered defence strategy. By integrating industry leaders such as Microsoft Defender and CrowdStrike, our Endpoint Detection and Response (EDR) service offers unmatched precision in pinpointing and neutralising threats at the endpoint level, well before they can proliferate.

Managed XDR

Extended Detection and Response (XDR) is a unified defence against incidents that span endpoints, identities, email, collaboration tools and cloud applications. By monitoring diverse attack surfaces and analysing the overall threat landscape, XDR provides a higher level of protection against emerging and sophisticated threats.

Managed NDR

Network Detection and Response (NDR) platforms capture network metadata, enriches it with machine learning derived security intelligence, and applies it to your detection and response use-cases. NDR continuously analyses network traffic and behaviour, enabling security teams to respond quickly and prevent potential breaches or damage.

ZDL
GROUP

Delivering excellence in Cyber Security

At ZDL, we believe that effective risk management requires a holistic 360° approach. We take a comprehensive view of our clients' cyber security risks and provide quality services to address those risks.

Our approach to Total Security Management helps make our clients' infrastructure, applications and data more secure in the face of a continually evolving Threat Landscape. Our aim is to build a partnership with our clients, built on a mutual respect and understanding of each other's businesses.
We become a part of our clients' team, a valued partner; an intrinsic part of their business.

ZDL's 4 key service areas are designed to focus on our clients' cyber resilience journey. Our unique portfolio of services enables you to build an agile, responsive security infrastructure and strategy.

Our Services

Ethical Hacking

- Broad Security Review
- Red Teaming
- Security Audits
- Penetration Testing
- Cloud Security & Security Ops Testing
- Source Code Review/Coding Standards
- Social Engineering
- Physical Security

Training

- Security Awareness Programmes
- Secure Coding School for Developers
- Bespoke Senior Exec Security Training
- Runbook training/ Scenario Workshops
- Phishing & Resilience Programmes
- Physical Security Awareness
- Online Assessment / CBT Developer Training

Managed Services

- Supplier Evaluation Risk Management (VenDoor)
- Incident Response Preparedness
- Security Training for Developers - Annual Programme
- Managed Detection and Response (MDR)
- Virtual Information Security Manager
- OSINT/Threat Intelligence

Compliance

- Policy Review & Creation
- 360° Assessment
- PCI Remediation Support
- ISO/ NIST/EU GDPR Standards Agreement
- Business Continuity Management
- IR Management Review
- ISO Readiness Programmes
- Office365 Configuration Review

www.zdlgroup.com
London | Brighton | Manchester | USA

Contact Us ⟶