aztech

Extended Detection & Response (XDR)

Revolutionise Your Cyber Security with Integrated Detection and Response.

Cyber Security Services

The Challenge

Modern businesses face an increasingly complex threat landscape, with attackers exploiting weaknesses across cloud, on-premises and hybrid infrastructures. Remote working, expanding attack surfaces and advanced threats demand a unified and scalable security approach. Traditional tools often lack the integration and speed needed to respond effectively and, without a comprehensive detection and response solution, businesses may struggle to combat zero-day vulnerabilities and multi-vector attacks that bypass traditional defences.

Aztech IT's XDR service provides a unified approach to security, designed to bridge gaps between siloed systems and deliver faster, smarter threat detection and response. Our platform integrates data from endpoints, cloud environments and network traffic into a central hub, leveraging AI-driven insights to deliver real-time protection.

Key Business Outcomes:

Comprehensive Protection:
Shield your organisation from sophisticated attacks with proactive and automated threat response.

Optimised Resources:
Streamline security operations by reducing false positives and automating repetitive tasks.

Automation-First Approach:
Reduces reliance on manual processes, enabling faster responses to emerging threats.

Faster Containment:
Act on threats immediately, reducing the time to detect and remediate incidents.

Why Choose Us?

Expert Guidance: Our experienced team ensures seamless implementation and ongoing support, tailored to your organisation's security needs.

Proven Results: Clients rely on us to strengthen their threat detection and response capabilities while minimising operational disruption.

Customised Support: We adapt our solutions to your unique environment, providing enhanced protection against advanced threats.

"Aztech are an extremely responsive, capable and flexible company. They understand the demands placed on a retail business. They provide solutions that deliver ongoing value and mitigate business risk. We have developed a strong partnership with them and wouldn't hesitate to recommend them."

Paul Walker, Managing Director (Fitness Superstore)

aztechit.co.uk
0330 0949 420 | info@aztechit.co.uk

Service Overview

Unlike a Security Operations Centre, which focuses on live monitoring, XDR automates data correlation and threat response, empowering teams to act decisively and efficiently. Our XDR service provides a unified approach to security, designed to bridge gaps between siloed systems and deliver faster, smarter threat detection and response, with features including:

Expanded Visibility: Covers endpoints, network traffic, cloud services, and identity management systems to detect threats across all vectors.

Automated Threat Correlation: Consolidates alerts and prioritises based on risk, reducing noise and enabling focused responses.

Real-Time Analysis: Employs machine learning to uncover patterns and anomalies indicative of complex attacks.

Integrated Remediation: Automatically blocks or contains threats with predefined rules, ensuring minimal disruption.

Unified Platform: Provides a single interface for investigating, responding to, and managing security incidents.

Example Use Cases

Detect and respond to ransomware attacks in real time: Isolate infected systems and neutralise threats to prevent business disruptions.

Mitigate the impact of phishing campaigns through rapid containment: Identify and secure compromised accounts to block unauthorised access.

Identify and address suspicious activities in cloud environments: Monitor for anomalies and implement controls to secure sensitive data.

How It Works:

Multi-Vector Monitoring:
Tracks activity across endpoints, cloud platforms and networks to identify threats from all sources.

AI-Driven Insights:
Uses behavioural baselines to detect anomalies and predict potential risks.

Incident Correlation:
Connects related events to build a comprehensive view of attacks, reducing investigation time.

Immediate Action:
Automates responses like isolating endpoints or blocking malicious IPs to

Continuous Improvement:
Integrates threat intelligence and feedback to strengthen defences over time.

What's Next?

Transform your security operations with Aztech IT's XDR service.
Book a consultation call today to discover how we can deliver integrated protection and faster response capabilities for your organisation.