CYSIAM

"When seconds count, expertise matters. When expertise matters, choose CYSIAM."

Managed Detection and Response (MDR)

Cyber threats don't respect information overload, and neither should your defences. With your security teams facing thousands of daily alerts, how can you be sure that you don't end up chasing false positives, while genuine attacks go unnoticed until it's too late?

CYSIAM's intelligence-led MDR service transforms your CrowdStrike and Microsoft investments from alert generators into a precision defence system. Our UK-based and CREST-accredited Security Operations Centre doesn't just monitor - we investigate, respond, and neutralise threats before they impact your business. 24/7/365 threat detection that actually works.

What is Managed Detection and Response?

CYSIAM MDR is what happens when advanced security technology meets genuine human expertise. While others might opt for alternatives such as SentinelOne, Sophos, or Rapid7, we choose CrowdStrike and Microsoft because they offer the deepest integration capabilities and most comprehensive threat intelligence ecosystems.

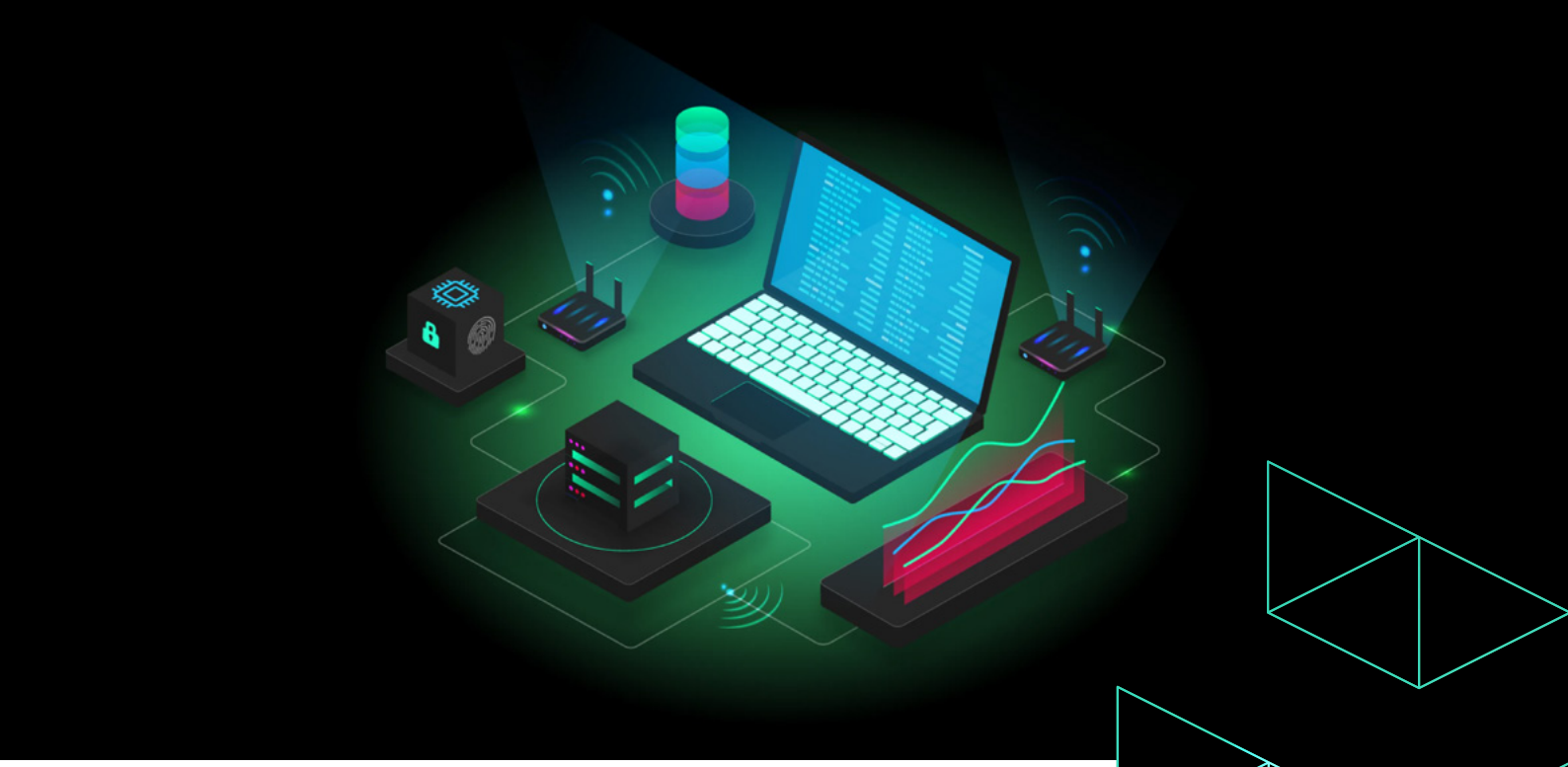
Our security analysts integrate seamlessly with your existing Microsoft Sentinel, Defender for Endpoint, and CrowdStrike Falcon platforms, applying threat intelligence from multiple closed and proprietary sources to identify genuine security incidents.

Assured Service Provider – in association with National Cyber Security Centre – Cyber Incident Response (Level 2)

Assured Service Provider – in association with National Cyber Security Centre – Cyber Incident Exercising

CREST – VA – PEN TEST – CSIR – SOC

Armed Forces Covenant – Employer Recognition Scheme – Gold Award 2022 – Proudly supporting those who serve



What's covered?

Intelligence-Led Security Operations

- **FIRST accredited CERT**
  With intelligence sharing from 782 incident response teams across 111 countries, to keep you ahead of emerging threats before they reach your organisation
- **Microsoft security stack optimisation**
  To make your Sentinel, Defender and M365 investments work harder by reducing false positives to let your team focus on genuine threats
- **CrowdStrike Falcon platform mastery**
  Advanced endpoint protection that doesn't just detect - it responds before attacks spread
- **Proactive threat hunting**
  Proven TaHiTI methodology that identifies hidden threats before they can cause significant damage

24/7/365 UK-Based SOC Operations

- **Multi-tier operational model**
  For the right expert response at the right moment. Level 1 triage, Level 2 investigation, Level 3 threat hunting - when situations demand it
- **Layered technology architecture**
  Provides complete visibility across your environment, so no attack goes undetected
- **Guaranteed response times**
  Our 1-hour critical response prevents small incidents turning into major breaches

Advanced Detection and Response Capabilities

- **Custom detection engineering**
  With tailored rules that focus on threats relevant to your business environment, to reduce false positive noise
- **Automated remediation**
  For rapid response to known threats and expert analysis for complex incidents
- **Remote endpoint isolation**
  Stops lateral movement before one compromised device affects your wider network

Comprehensive Service Management

- **Executive reporting**
  That shows leadership exactly what their security investment is delivering
- **Regulatory compliance support**
  That helps you stay compliant without the compliance headache - we handle the documentation whilst you focus on business
- **Emergency response services**
  That provide immediate access to world-class expertise when every minute counts

EVERY organisation using CrowdStrike and Microsoft security tools deserves expert analysis that transforms raw alerts into actionable intelligence. CYSIAM MDR services deliver exactly that. Maximum protection and rapid response capabilities that quickly detect and neutralise modern cyber threats.