Managed Detection and Response

for Microsoft Sentinel

Secure your organisation against the latest threats **as fast as they evolve**

claranet cyber security®

Claranet Managed Detection and Response for Sentinel

Harness the full potential of Microsoft Sentinel to rapidly detect and manage threats in your estate. Reduce your setup and configuration time, plug into the latest threat intelligence, and create a single view of your threat detection and response, all managed by a team of CREST- and Microsoft-accredited threat hunters and cybersecurity analysts.

Your security information and event management (SIEM) is only as powerful as the deployment of the people, processes, and technology it requires to be effective. Our Managed Detection and Response (MDR) solution for Microsoft Sentinel takes care of all three to ensure your organisation is secured against the latest threats, **as fast as they evolve.**

Protect your business at the speed of the cloud

Grow your detection capability at cloud speed and scale with the latest threat intelligence, custom analytics, and 24/7/365 monitoring, containment, and threat management. All managed by a multiskilled security operations centre (SOC).

Streamline costs and resource

Develop a more cost-effective model by outsourcing your detection to a team of dedicated SOC specialists. Reduce alert fatigue, simplify setup, reduce noise and storage costs, and maximise your cost per alert.

Inform security investment

Learn from expert-led, in-depth investigations and the automated tracking of user and application behaviour. Understand where additional defensive measures are needed most to develop your cybersecurity posture over time.

A service built around real security challenges

Growing infrastructure, unmanaged and legacy systems, shadow IT, and data storage is creating an attack surface whose size and complexity works to the attacker's advantage.

People are essential for attack detection, but an in-house capability is expensive, and demands time and effort to become effective.

Cloud computing has changed the rulebook right across the cybersecurity lifecycle. The teams responsible for detection must now take control of the cloud control plane in addition to the network and its endpoints.

Attack detection doesn't rely on one tool, but rather a platform of technologies working together and being managed effectively.

22 the average number of security breaches faced by a company in 2022 [Accenture]

claranet cyber security®

The core elements

Our MDR is made up of 4 key components across people, process, and technology

Threat Intelligence (TI)

Our MDR uses world-leading threat intelligence to keep your detection capability in line with the latest threats, so they are identified and stopped before they can harm your business.

24/7/365 analysis

Our always-on, global SOC is dedicated to monitoring and analysing activity to identify and eliminate threats and provide actionable insights back to you and your team.

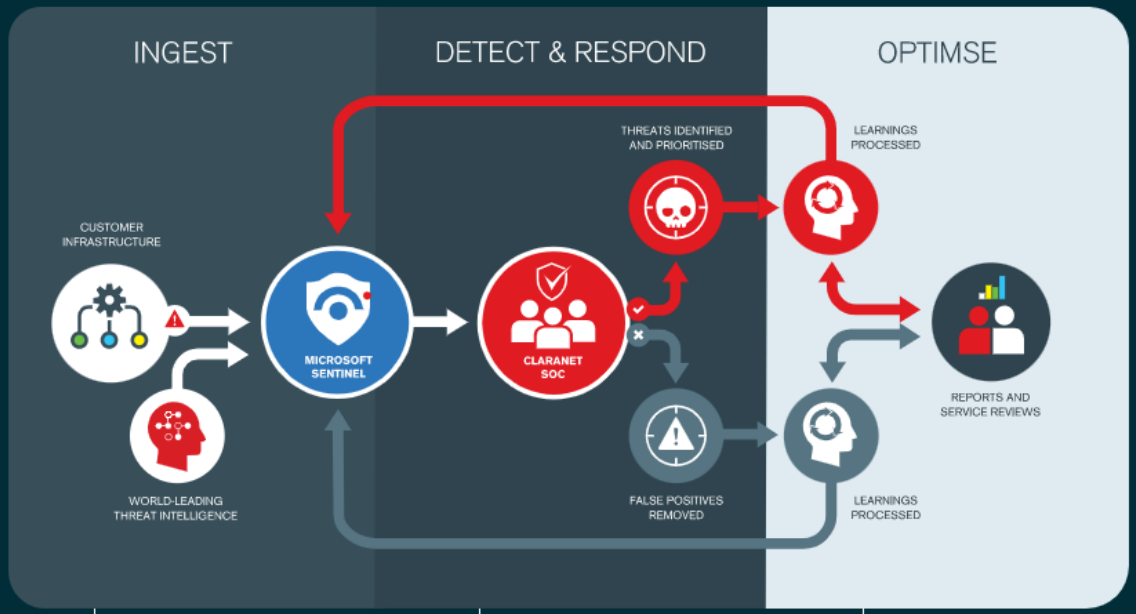
Continuous optimisation

Software is never fully effective “out of the box”. Our team will fine-tune your SIEM controls and develop custom rule sets that reduce false positives and prioritise detection where it’s needed most.

Proactive hunting

We supplement the power of Artificial-Intelligence-(AI)-led analysis with threat hunting to pre-empt and seek out complex threats that could go under the radar.

How it works



Security logs and Microsoft threat protection alerts generated across your infrastructure are ingested by Microsoft Sentinel providing a "single pane of glass" across your data.

World-leading threat intelligence (TI) is also fed into inform detection with confirmed malicious indicators of compromise (IoCs).

IoCs trigger alerts and feed into the Claranet SOC. False positives are removed.

Confirmed malicious behaviours are prioritised by severity and escalated for removal or deeper response.

Threat hunting is conducted to identify undetected threats and optimise detections.

Learnings are used to optimise alerts and train Microsoft Sentinel to focus on the most high-priority threats.

Reports and service reviews take place regularly to improve performance futher

Service deep dive, how we detect threats

Always-on detection and triage

We don't stop looking

Claranet's SOC layers the automation power of our detection technology stack with proactive, human-led threat hunting and alert triage. This triple-edged approach gives us maximum visibility, so attackers can't persist un-detected. It also ensures threats are accurately prioritised before being escalated to the customer, ready for response.

- Continuous log collection and event correlation
- Ingestion of all logs from any data source across your on-premise and cloud infrastructure
- Malware analysis in line with the latest strains
- Comprehensive triage, including false-positive removal and threat prioritisation
- Direct escalation of high-priority security events

Threat intelligence and analysis

We seek out attackers before they execute an attack

We continually ingest threat intelligence data so we can identify new threats and attacker tradecraft the moment they appear on a customer's estate. We also use Microsoft security tools, automated and manual data analysis, and our proactive threat hunting to predict attacks by:

- Listening to hacker channels
- Mining the dark web for malicious activity
- Manually analysing threat intelligence feeds
- Investigation of your network for advance persistent threats
- Carrying out in-house offensive and defensive research

Accelerate your response

MDR to enable containment and eradication

Effective attack detection helps engineer the first response to an incident. With Claranet's MDR for Microsoft Sentinel, incidents are reported through our threat and incident management portal, Claranet Online, with the added context of business priority and potential impact. This single pane of glass empowers your team with sustained visibility and control of your Azure-based detection controls and creates a holistic and inclusive view of your cybersecurity programme across different services and platforms so you can streamline all activity.

Full support to contain the event will ensure that the breach timeline is shortened from months to just hours. Claranet Cyber Security respond to you within defined SLA's with contextual classification of the impact of an event allowing you to focus on critical issues.

Tickets include detailed information regarding:

- The origin, location, and severity of the incident
- Recommended containment actions
- Recommended future prevention measures

The impact of our approach

Claranet's offering

Core correlation rules
Our correlation rules are written so that Microsoft Sentinel can identify genuine malicious activity without delay. They are constantly optimised around the most high-impact threats.

Intelligent workbooks
Claranet's custom workbooks dynamically analyse data, so it can be used to produce detailed, visual reports that help you understand you measure metrics like Analytics Efficiency, Incident Overview, and Cybersecurity Maturity Model Certification (CMMC).

Certified 24/7/365 SOC
Our global SOC is made up of CREST-accredited, SC-200-certified analysts and threat hunters with a breadth of experience. They work with the tried and tested methodologies to ensure detection happens fast.

Threat Intelligence
Claranet is plugged into world-leading threat intelligence streams, which are ingested by Microsoft Sentinel to help it identify authentic indicators of compromise (IoCs) and alert against the latest attacker behaviours and tradecraft.

Security, Orchestration, Automation and Response (SOAR)
Integrate Microsoft Sentinel with your incident response (IR) products and services via a suite of playbooks and connectors for security orchestration, automation, and response (SOAR).

Cloud practice
Whether you have an established cloud strategy or you're just beginning your journey, tap into the expertise of our dedicated Cloud Practice. This team works across all areas of cloud, from operations and optimisation, to migration and governance.

Claranet Online
A single pane of glass across your security activities. Our portal, Claranet Online, empowers you and your team with visibility and control of your Azure-based detection controls, whilst helping create a joined-up view of your cybersecurity programme across different services and platforms.

Threat hunting
Proactive threat hunting from Claranet's SOC team helps identify complex attacks and potential advanced persistent threats (APTs) across the kill chain, stopping attackers from going under the radar.

Getting started

Service build

We will work with you to choose the right service for your organisation and your team depending on resources and capabilities.

Fully managed setup

Deployment, and setup of optimised software, usually within days or weeks.

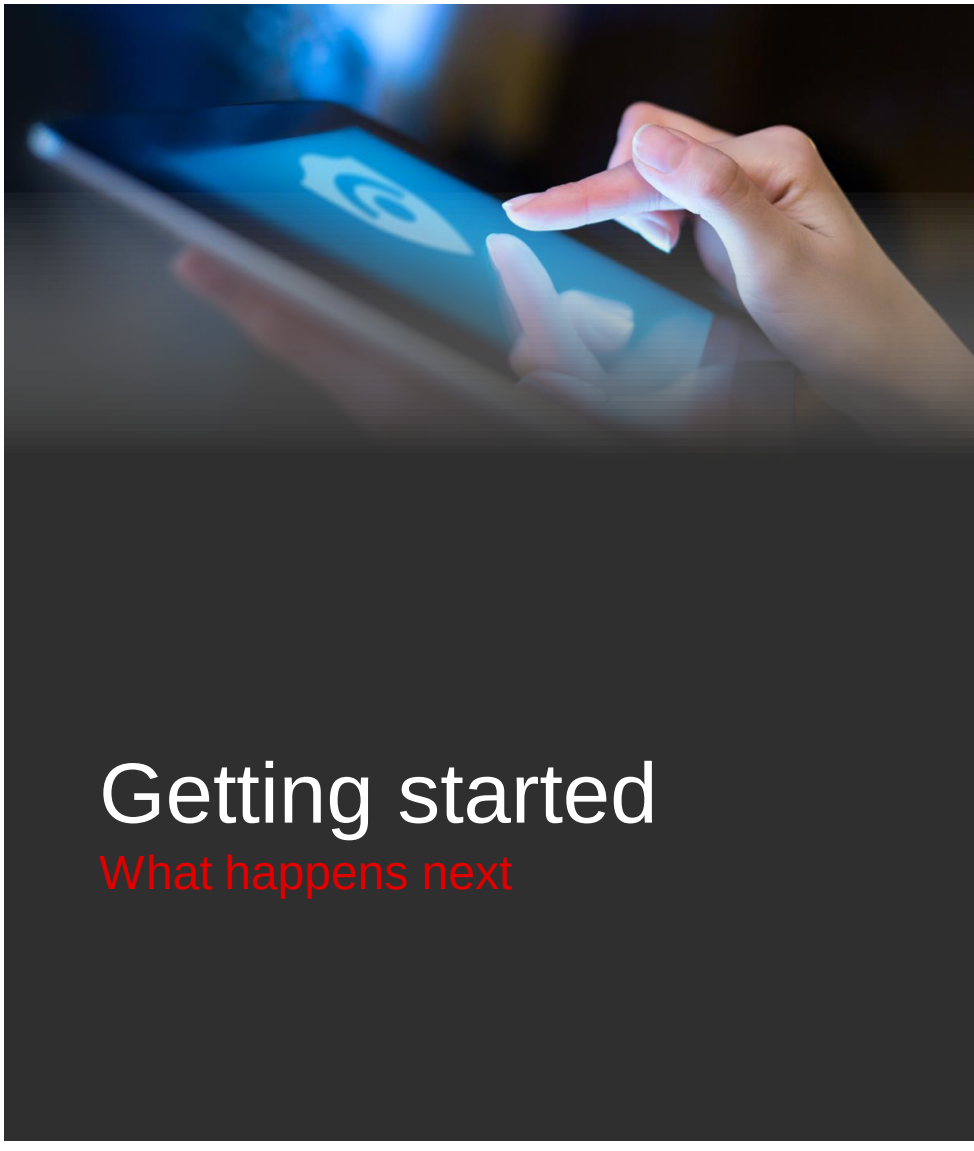
Claranet Online

Full control for you and your team within our threat management and reporting portal* from day one.

Reports and service reviews

Monthly reporting and quarterly face-to-face calls.

**Claranet is ISO 27001 compliant for data storage and reporting functionality.*



Claranet Cyber Security

Claranet Cyber Security is the global cybersecurity services division within Claranet Group. Claranet has an annual revenue of over £440m, more than 10,000 business customers, and 2,500 staff across the world.

The cybersecurity technical team brings together 1,500 technical experts and 75 pentesters under a 25+ year legacy that includes work with FTSE250 Fortune 500 global customers.

Claranet Cyber Security is a leader in ISG's Provider Lens™ for both "Cybersecurity – Solutions & Services" and "Public Cloud – Solutions and Services".*

Claranet is one of only a few MSPs to achieve the highest partner accreditation status with Microsoft, AWS, and Google. The organisation is recognised as a leader in Gartner's Magic Quadrant and a market leader in cybersecurity

Our service portfolio covers Managed Detection and Response, Endpoint Detection and Response (EDR), penetration testing, Continuous Security Testing, and cybersecurity training.

We are one of the leading training providers at Black Hat around the world and we have training partnerships with Check Point , Nano, Rapid7,and QA.

Gold Microsoft Partner | Azure Expert MSP

aws partner network – Premier Consulting Partner – MSP Partner

ISO 9001 · ISO 14001 · ISO 22301 · ISO 27001 · ISO 27017

Cyber Essentials Plus · PCI DSS Compliant · CHECK IT Health Check Service · CREST · Qualys

Get in touch to find out more

www.claranet.co.uk/services/cybersecurity

info@claranetcybersecurity.com

0330 390 0504 (UK)

claranet cyber security®

we hack | we teach | we protect