Managed Detection and Response

Stay focused on your business. You are protected.

claranet cyber security

sec-1

Stay secure and compliant

Continually hunt, detect, analyse and report on threats

Attackers are increasingly finding new ways to breach systems and evade detection, whilst organisations are challenged with a lack of investment and skilled staff to asses' these new threats. Many organisations are not aware of data or systems compromise until well after the event, typically weeks or months. You need the ability to proactively predict an impending attack or detect one that's happening. Meeting strict breach detection and reporting requirements is necessary to ensure regulatory compliance.

claranet cyber security

sec-1

Managed Detection and Response

Cyber-attacks are increasing in volume and sophistication on a daily basis and even organisations with strong defensives are falling victim. Most organisations are not aware of data or system compromise until well after the event, typically weeks or months. You need the ability to predict an impending attack or detect one that's happening.

Managed Detection and Response from Claranet Cyber Security allows you to quickly identify threats and attacks to your business systems and data, allowing you to rapidly respond, manage and contain the threat.

Our dedicated Managed Detection and Response team work as an extension of your business and remove the resource pressure of proactive research analysis required to accurately identify and prioritise security incidents on your network.

claranet cyber security

sec-1

A comprehensive approach

Claranet Cyber Security provide a comprehensive approach with three essential components:

People

Experienced security analysts who monitor and investigate all indicators of compromise from threat intelligence or log sources to identify an attack and help you prevent or resolve an incident.

Technology

Our Security Incident and Event Management (SIEM) enables collection of any log message from any log source, PCI compliant Cloud storage ensures retention of information ready for exhaustive investigation.

Knowledge

Research and hunt for potential attacks, scouring threat intelligence feeds, the dark web and hacker channels for indicators that new attacks are just around the corner.

claranet cyber security

sec-1

Security tailored to your needs

The right options for you now and for the future

Manage Detection Response solution from Claranet Cyber Security enables the right level of security based on your business and risk management needs, you select from a spectrum of threat protection capabilities which include:

Asset Discovery

Continuously monitor infrastructure to identify all hardware and software enabling you to spot changes and address potential security issues.

Threat intelligence

Threat hunting across multiple threat intelligence feeds, hacker channels and the dark web to get ahead of threats.

Vulnerability scanning

Check for vulnerabilities in all systems to identify where weakness exists in unpatched or misconfigured systems.

Intrusion prevention

Host based (HIPS), network based (NIDS) and cloud ready (AWS and Microsoft Azure) detection of threats.

File integrity monitoring

Monitor changes in critical system files, configuration files, sensitive data files, and files that attackers change to hide their tracks.

Compliant storage and monitoring

We use AlienVault USM Anywhere to collect, store and monitor your logs. AlienVault is compliant to PCI DSS, HIPAA, and SOC 2.

claranet cyber security

sec-1

Comprehensive Detection

Put yourself on the front foot

Working as an extension of your team, we proactively identify and predict security breaches around the clock. Using comprehensive practices that detect malicious activity, so attackers are unable to persist un-noticed in your network for substantial amounts of time.

Activity can be tracked within network devices, systems, endpoints, and data whether stored on-premise or in the Cloud.

- **Every log. any source**
- **Expert analysis of security events**
- **Malware analysis**
- **Continuous log collection and event correlation**

claranet cyber security

sec-1

Threat hunting and intelligence

Seek out adversaries before they execute an attack

Early warning of a potential attack allows you to take proactive measures in anticipation of these new types of attacks, addressing them as a priority.

Claranet Cyber Security use proactive techniques that combines security tools, analytics, and threat intelligence with human analysis and instincts to hunt and predict attacks by:

- **Listening to hacker channels**
- **Mining the dark web for nefarious activity**
- **Analysing threat intelligence feeds**
- **Investigation of your network for advance persistent threats**

Rapid and collaborative incident response

Accelerate your incident response and containment

Incidents are reported via an incident management portal, including priority business context and potential impact. Full support to contain the events will ensure that the breach timeline is shortened from months to 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:

- **How the event started and what has been breached**
- **What actions should be taken to contain the threat**
- **What changes should be implemented to mitigate it in the future**

claranet cyber security

sec-1

Features:

- **Every Log – Any Source -** Collection and storage of events from any log source on any network
- **Incident Validation -** In depth analysis of malware, identifying indicators of compromise
- **Fully Managed Setup -** deployment and setup of optimised and highly tuned software usually within days or weeks
- **Resource & expertise -** address monitoring, detection and response gaps with best of breed technology and a team of security specialists
- **Managed Threat Hunting -** Discovery of advanced threats through manual network investigation and threat intelligence analysis
- **Comprehensive Security -** Asset Discovery, Intrusion Detection, Vulnerability Assessment, Event Correlation
- **Rapid Incident Response -** remote incident response validating potential incidents, applying business context, and investigating thoroughly to provide actionable advice about the threat
- **Incident management portal -** access to Claranet Online for full incident management and reporting
- **Compliance driven -** Fully PCI/ISO27001 compliant data storage and reporting
- **Always-on -** Service flexibility to suit your needs with Business Hours or 24x7x365 coverage

claranet cyber security

sec-1

Benefits:

- Enhance stakeholder confidence by reducing you information security risk
- Provide rapid incident response by proactively detecting threats and breaches
- Fully address identified threats through rapid remediation support and guidance
- Detects and responds to advanced attacks that bypass traditional controls
- Acts as a virtual extension of an organisation's in-house team
- Enables staff to focus on fixing rather than discovering threats
- Leverage new and existing security technologies and stay ahead of the curve
- Provide (up to 24x7) monitoring aligned to your business need
- Delivers weekly and monthly security reports
- Avoids capital expenditure by supplying all resources as a subscription

claranet cyber security

sec-1

Our accreditations

Claranet Cyber Security continually invest in hiring the most experienced, highly trained teams in the industry. This means irrespective of the IT security issue you face, we have the people who can help. A core part of delivering the best service is our continued commitment to being fully accredited across all the major security and comliance standards. These include:

CREST

CHECK IT Health Check Service

CYBER ESSENTIALS

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

PCI Security Standards Council APPROVED SCANNING VENDOR

ISO27001:2013 UKAS MANAGEMENT SYSTEMS

C|CISO Certified Chief Information Security Officer

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP

CRISC Certified in Risk and Information Systems Control An ISACA Certification

OFFENSIVE security OSCE

OFFENSIVE security OSCP

C|EH CERTIFIED ETHICAL HACKER

claranet cyber security

sec-1

For more information about **Managed Detection and Response,** call us today:

01924 284 240

www.claranet/cybersecurity

claranet cyber security

sec-1

claranet®
cyber security