Claranet Cyber Security

Continuous Security Testing

Take a proactive stance and mitigate risk

claranet cyber security

sec-1

Continuously understand vulnerabilities, make the right decisions

Organisations must now deliver superior customer experience and innovation, and deliver it rapidly and meet customers' expectations to remain competitive. This new software driven world where speed of deployment is crucial creates even greater security challenges.

- **Increase in vulnerabilities** - The National Vulnerability Database discovered 3,744 new vulnerabilities during a three month period in 2019, with 50% being CRITICAL or HIGH.
- **Human error** - introduced by IT staff misconfiguring a network device or a developer inadvertently introducing vulnerable code into an application.

Being secure requires a new approach. Continuous Security Testing from Claranet Cyber Security combines industry-leading application scanning technology with the knowledge and expertise of experienced penetration testing consultants. Ensuring maximum coverage of your attack surface. Get faster insight into vulnerabilities than traditional point-in-time penetration testing with a continuous cycle of testing and remediation.

claranet cyber security

sec-1

Core benefits

Assurance - that your assets are constantly checked for vulnerabilities that could lead to network breach, data leakage or system unavailability if exploited

Confidence - that updates to production environments are checked for security flaws as change occurs

Assets - maintain an accurate register of all digitally facing assets and actively monitor for assets that are inadvertently exposed or published circumventing security checks

Secure - rapid alerts to new vulnerabilities allows you to address them with unprecedented response

times
Collaborative - gain a penetration testing team alongside your existing team

Awareness - as security practices improve organisations will benefit from effective and efficient development

claranet cyber security

sec-1

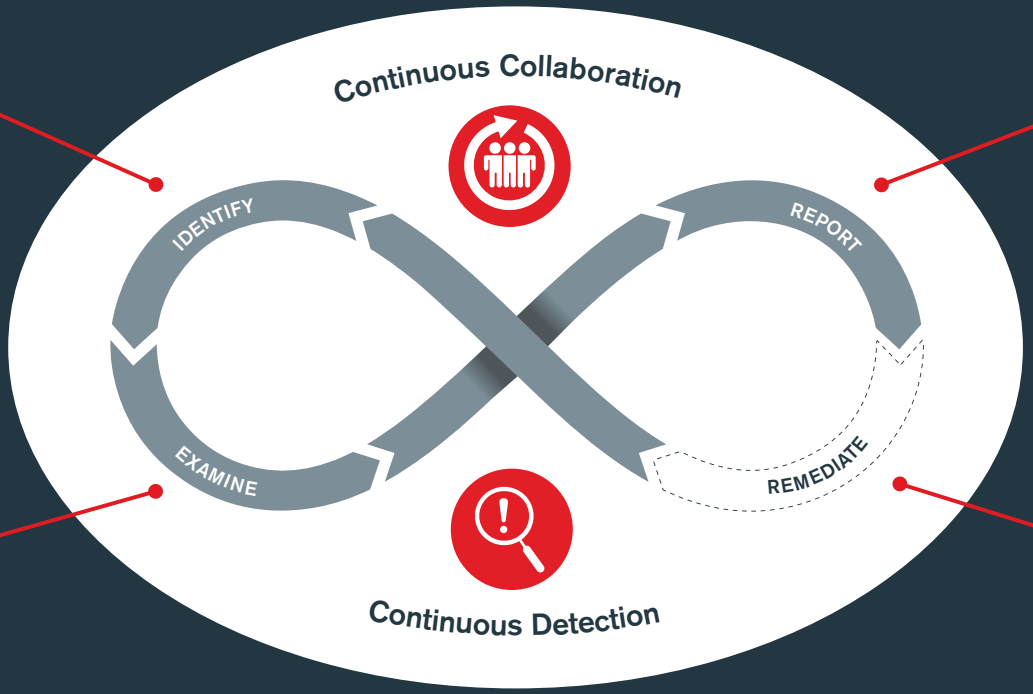
Continuous Security

Identify

- In-scope systems
- Testing windows
- Additional attack surface
- Changes to systems

Examine

- Infrastructure
- Applications
- Authenticated systems
- Assess for vulnerability
- Remove false-positives
- Exploitability of issues
- Impact of exploitation



Report

- Instant notifications for critical findings
- Scope alerts for discovered assets
- Remediation instructions
- Monthly security digest

Remediate

- Prioritise remediation by impact
- Ongoing technical advice
- Reconfigure insecure systems
- Reduce vulnerability time to live
- Reduce risk of breach

claranet cyber security

sec-1

Key features

- **Continuous assessment –** assets are tested 24x7x365 matching the approach an attacker would take
- **Continuous awareness –** we are constantly monitoring for newly introduced or changes to existing systems as well as looking for changes in the attacker's skillset and tools
- **Continuous detection –** of long term and newly discovered or introduced vulnerabilities
- **Complex flaws –** manual penetration testing finds vulnerabilities missed by automated tools
- **Attack surface monitoring –** Open Source Intelligence gathering checks for changes to your digital exposure
- **Vulnerability verification –** manual analysis of findings to confirm vulnerability existence
- **Simplified prioritisation –** prioritise your remediation efforts with contextual vulnerability impact
- **Rapid vulnerability notification –** elevated response times for critical issues
- **Monthly reporting –** summary reporting that includes all findings by asset, vulnerability class
- **Collaborative support –** fixes issues with support from the CST team

Increase monitoring, scope and the attack surface

Complex, dynamic estates with a high frequency of change can be a challenge to keep track of. These estates continually evolve over time with the introduction of new systems, upgrades to existing and the decommissioning of old, they must be managed correctly to assure security.

Continuous Security Testing enables faster insight into vulnerabilities allowing you to grow your business with security testing taking place at the pace of change.

Proactive attack surface monitoring

We proactively oversee the configuration and setup of the in-scope estate, as well as watch the Internet and Dark Web for assets, alerting you to exposed systems.

claranet cyber security

sec-1

Functions

- Analyse the predefined scope given by the client to determine omissions and system changes overtime, such as new systems, services and applications being added
- Test exposed applications, infrastructure, and cloud assets known vulnerabilities, missing patches and security misconfiguration
- Deep-dive into exposed applications to determine vulnerabilities introduced through bespoke systems such as those covered by the OWASP Top 10, which includes safe exploitation of complex issues such as SQL Injection and Cross-Site Scripting to eliminate false positive findings
- Keep your organisation informed through monthly digests of new vulnerabilities that highlight successful remediation work

Add-ons

- Additional scanning of the PCI scope for vulnerabilities and review of false positives
- Claranet Cyber Security is a PCI Approved Scanning Vendor (PCI ASV)

Our accreditations

Claranet Cyber Security continually invests in hiring the most experienced, highly trained teams in the industry. A core part of delivering the best service is our commitment to being fully accredited across all the major standards in IT security. These include:

claranet cyber security

sec-1

About Claranet

Quick facts

- Founded in 1996
- Owner managed
- £350m/€370m revenue
- Global reach with operations in nine countries
- Over 6,500 business customers
- Over 2,200 employees in 24 offices
- Long-term customer relationships
- Leader in Magic Quadrant for Managed Cloud Hosting, Europe

claranet cyber security

sec-1

claranet cyber security

sec-1

For more information about **Continuous Security Testing** please call:

01924 284 240

claranet cyber security

sec-1

claranet®
cyber security