claranet® cyber security

SEC-1 | NOT SO SECURE

Stay secure and compliant

The pressure is on to be agile, to move fast, while always staying secure. Today's security challenges fall into 3 main areas:

The ever-increasing pace of innovation driving rapid application development

To be compliant and the need to meet required regulations

The necessity to protect your complete IT environment from cyber-attacks

Don't wait until an attack is successful. Claranet Cyber Security provides managed detection and response capabilities in addition to security testing and training. As well as providing the visibility needed to make the decisions that protect your business, we will teach your staff to better defend key assets and give you the right consultancy to meet your compliance and legal responsibilities.

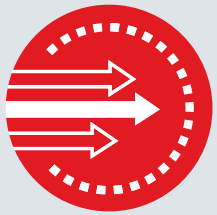
claranet cyber security

World leading security experts

Claranet Cyber Security has 17 years' experience in delivering and training cybersecurity services and techniques, for the biggest brands across the globe. With over 60 penetration testers and a world-renowned security training team, Claranet Cyber Security combines the deep expertise of Sec-1 and NotSoSecure.

We hack. We teach.

We are trusted for our research and understanding of the very latest security threats and this insight continually informs all our cybersecurity work. What we learn from penetration testing in the field, feeds into our training courses and vice versa. It's mutually beneficial.



Penetration Testing

Continuous Security Testing

Hacking Training

Audit and Compliance

Employee Cybersecurity Awareness

Managed Detection and Response

Red Teaming

claranet cyber security

Cyber attacks : the numbers

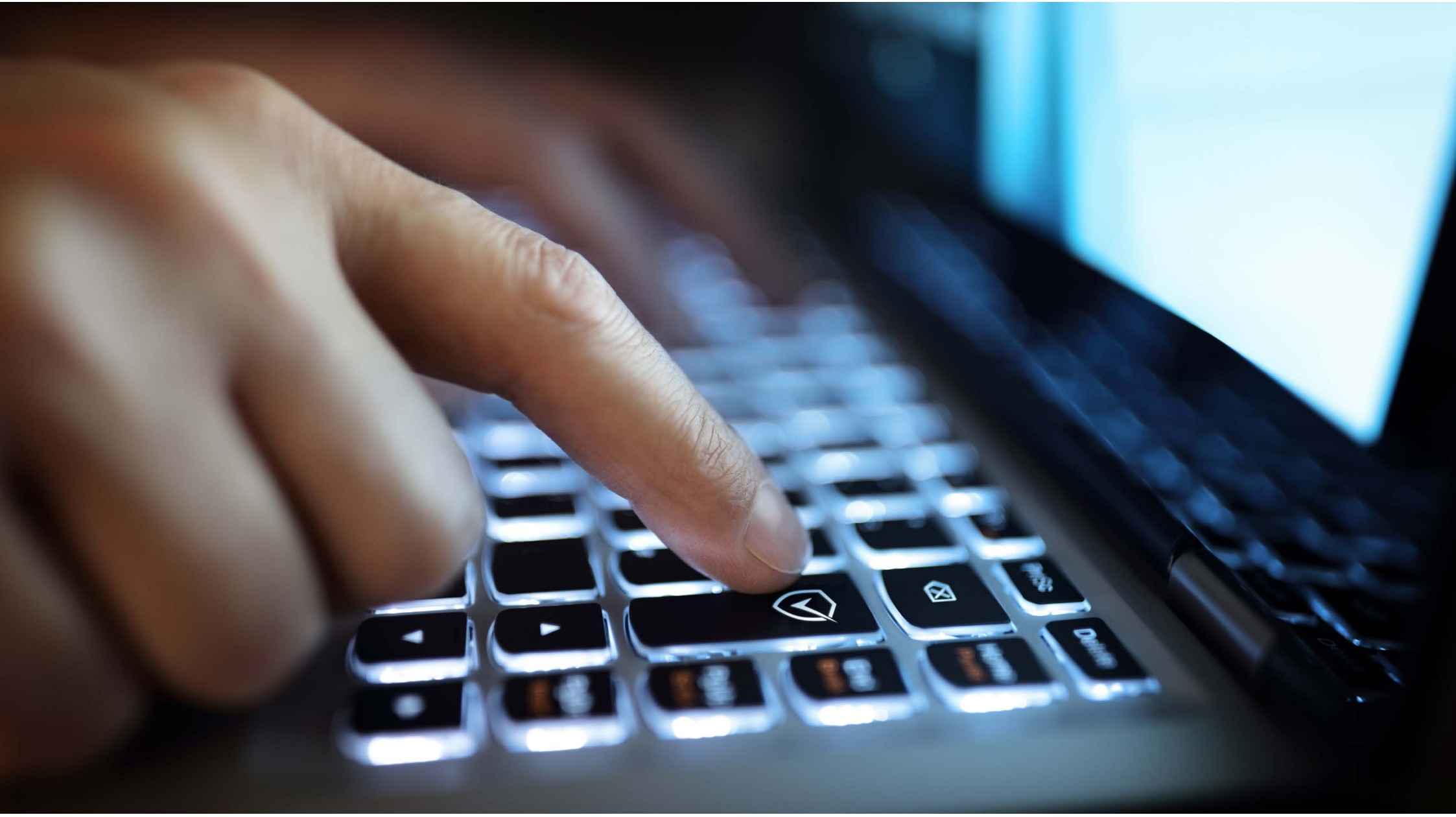
According to the government's recent Cyber Security Breaches Survey 2018, just under half (43%) of all UK businesses identified at least one cyber security breach or attack in the last 12 months. This rises to nearly three quarters (72%) among large organisations. To remain secure and protect your intellectual property, customer data, and brand reputation, it's now essential that security is a priority for your business. Based on those facts forward-thinking businesses now choose a proactive partner to help them understand IT vulnerability and develop a plan to keep them one step ahead of any threats.

Do you understand the costly impact of a breach?

According to a recent study by Juniper Research cyber-crime will cost businesses, globally, eight trillion dollars by 2022*. With cyber security threats continuing to increase, understanding the financial implications of a breach, and how secure your infrastructure, networks, applications and data are, is essential. Talk to us to discuss the true cost to your business and help you mitigate the risk of a breach before it happens.

*https://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats-2018

claranet cyber security

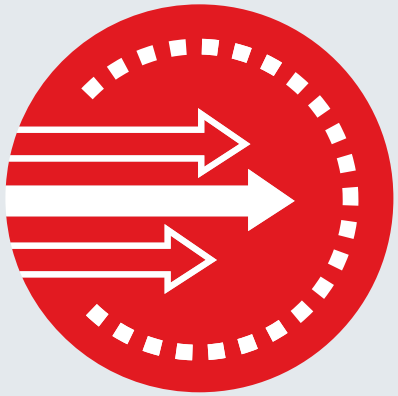


claranet cyber security

Penetration Testing

A clear and logical strategy of security testing against key targets within your organisation can provide the threat visibility needed in order to make changes, deploy defensive technology and train staff in a way that will make the job of an attacker harder and reduce the chances of a security breach.

Selecting the right type of attack simulation and targets to bring into the scope of the exercise requires experience and knowledge. With 17 years' experience in security testing, we will work closely with you to ensure that every risk to your organisation's data and systems is fully considered. Most attacks use a combination of powerful hacking tools alongside manual techniques, our attack simulations use the same blended approach to give you a realistic view of what could be achieved.



Testing Services include:

- Web and mobile application testing
- Internal, external & wireless network infrastructure testing
- Firewall, router and endpoint device assessment
- Cloud configuration assessment
- Phishing, vishing and smishing campaigns
- Open Source Intelligence gathering
- Physical Access Assessment
- Red Team Exercises

claranet cyber security

Continuous Security Testing

Whilst Penetration Testing is a proven method to discover vulnerabilities within an organisation's external systems, it is limited to a snapshot in time. A system that may be considered secure today may be found to be vulnerable to a critical security issue tomorrow. Continuous Security Testing is designed to ensure security vulnerabilities don't go unchecked between engagements.

Continuous Security Testing combines manual penetration testing activities with automated security testing. Delivered by qualified penetration testers, this ensures that online assets are continuously assessed for vulnerabilities and alerts raised when issues are detected. The service alerts you when changes are detected within your environment. Continuous Security Testing successfully addresses these security challenges by detecting new vulnerabilities, monitoring your attack surface and using the evolving tools and techniques built by hackers.

Business benefits:

- **Continuous scope monitoring: We look at your total attack surface**
- **Reduce internal security overhead: We identify, rank and report**
- **Get faster insight into vulnerabilities and mean time to fix**
- **Make security testing a continuous process to enable on-going security**
- **Meet compliance requirements which call for regular security testing**

claranet cyber security

Hacking Training

Hands-on, lab-based hacking, taught globally.

As the Black Hat conferences' most popular training provider, featuring the renowned "Art of Hacking" course, our ethical hacking credentials are unmatched. From old-school misconfiguration issues to the very latest cutting-edge techniques and exploits against the modern network platforms, we've got it all covered.

We hack. We teach

All our trainers are hands-on penetration testers, their experience in field feeds into the training.
This knowledge continually informs course content, giving you the latest most up to date information.

1 - Introductory classes

- Hacking Training 101

2 - Intermediate classes

- Art of hacking
- Infrastructure Hacking Training
- Web Hacking Training

3 - Specialist offensive classes

- Advanced Infrastructure Hacking Training
- Advanced Web Hacking Training
- Hacking and Securing Cloud Infrastructure

4 - Specialist defensive classes

- AppSec for Developers
- DevSecOps training

claranet cyber security

Managed Detection and Response

There is growing acceptance that being hacked is a matter of when and not if. Being prepared to detect the breach, stopping it as it is happening, and containing the breach if the worst happens, is essential.

The need to detect and respond to sophisticated cyber attacks continues to increase. A successful attack can result in network downtime, financial loss and reputational damage. Investing in an in-house Security Operations Centre (SOC) requires considerable setup and running costs. Claranet Cyber Security provides all the benefits of a fully managed SOC without breaking your IT budget.

Why use Claranet Cyber Security for Managed Detection and response?

- **Threat detection, lightweight incident response, and 24/7 monitoring capabilities**
- **Expert threat intelligence, working with complex networks and environments**
- **Reduce the time to know about an attack, from months to minutes and seconds**
- **Constant validation and rapid human lead verification**
- **Event collection from any system anywhere**
- **PCI compliant log storage and retention**

claranet cyber security

Audit and Compliance

The need to manage an overwhelming amount of data while achieving and maintaining security compliance is increasingly challenging. An active security program is important as non-compliance and security breaches can result in expensive fines, lost revenue and a damaged brand. Wherever you are on your journey, we can help.

PCI DSS Compliance

Complete end-to-end consultancy partner for all your PCI compliance needs. PCI Qualified Security Assessors on hand to help you through the entire process.

Cyber Essentials and Cyber Essentials Plus

As a CREST Certification Body, we can help you achieve or renew your Cyber Essentials and Cyber Essentials Plus accreditation.

IT Health Check for PSN

We demystify and support PSN compliance with our specialist penetration testing for public sector organisations.

claranet cyber security

PCI DSS Compliance Services

Store, transmit, process and protect your customer card data securely

Meeting regulatory compliance can be a complex minefield without the right level of knowledge or technical support. Secure your business and cardholder data, mitigate risk and meet your PCI DSS compliance requirements with Claranet Cyber Security. In addition to our accreditations as Payment Card Industry Qualified Security Assessors and a PCI Approved Scanning Vendor we provide a complete end-to-end service for all your PCI needs. From gap analysis to risk assessments, from milestone assessments to onsite resources, we can help.

5 stage approach to meeting PCI DSS

We have developed a 5-stage approach designed to follow an organisation's journey from the start of a PCI DSS project towards becoming PCI DSS compliant and then maintaining compliance on an ongoing basis. Claranet Cyber Security can also assist if you are part way through a PCI DSS project.

claranet cyber security

Employee Cybersecurity Awareness

Your best defensive strategy against sophisticated attacks is to raise employee awareness and provide education on good cybersecurity practices. To increase protection further, businesses are educating and motivating staff to understand and be vigilant in the face of these ever-increasing threats.

Claranet Cyber Security has developed a security cybersecurity awareness programme to demonstrate the latest techniques hackers are using, how the boundary between private and corporate communication has become increasingly blurred and how prudent security precautions can prevent hackers causing corporate, as well as personal, damage.

Social Engineering Assessment

Allows you to see how susceptible your staff might be when presented with an attempt by an attacker to trick them.

Security Awareness Training

We support IT departments in demonstrating to employees the importance of cybersecurity awareness. Engaging and easily understood, these sessions provide users insight into to how to defend themselves and their business against cyber attacks.

claranet cyber security

Our accreditations

Claranet Cyber Security continually invests in hiring and developing 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

About Claranet

Quick facts

- Founded in 1996
- $450m / £350m / €400m annualised revenues
- Over 6,500 business customers
- Operations in nine countries
- Over 2,200 staff in 24 offices
- CREST and CHECK accredited providers

claranet cyber security

For more information about our services:

01924 284 240

claranet.co.uk/cybersecurity

claranet cyber security

claranet®
cyber security

sec-1 | NOT SO SECURE