Today, it is an unavoidable fact that your business critical infrastructure and systems are at risk of attack.

The key to good security is a clear understanding of what is most critical to the business.

Where you do not have enough internal resources, time or skills to monitor and manage your IT environment 24/7, NCC Group can help, freeing up your skilled employees to focus on value-add activity.

NCC Group provides a range of managed and hosted services delivered from our 24/7 Security Operations Centre (SOC).

Benefits

- Reduces cost of managing IT security & data environments.
- Frees up your internal team to focus on value-add activity.
- Expert help in managing today’s complex infrastructures.
- Improves response times & reduces disruption.
- Single point of contact for all your managed security needs.
- Proactive monitoring & reporting.

Security Operations Centre (SOC)

- 24/7
- Over 5,000 devices under management
- Monitoring across 80 countries in 5 continents
- Over 130m events processed per day
- Approx. 200 actionable events analysed per day
- ISO 27001 certified
- ITIL service Framework aligned
Network Protection

Modern networks are complex and dynamic environments that are constantly changing and need careful management. Security strategies rely on multiple sophisticated solutions across every aspect of the network to create a capability based on defence in depth, in order to protect critical assets. These solutions need constant management and monitoring to ensure they remain effective and investments are not wasted.

NCC Group provides a range of managed services for security technologies to help organisations monitor and manage critical network components. By putting changes and health monitoring in the hands of our experts, we can ensure that your investment remains effective and your expensive resources can be deployed more efficiently.

Managed Firewall

With our Managed Firewall service, our dedicated firewall administrators will monitor, manage and maintain your firewalls, so you don’t have to. Our qualified engineers will help define and implement a security policy fit for your organisation and will monitor and manage your firewall investment all year round.

The service is also ideal for customers wanting to deploy next generation firewall technology to provide cost effective access to advanced protection features, without needing the skills in house to setup, manage and maintain a new technology.

Managed IPS

Managed IPS services ensure that your Intrusion Detection and Prevention systems are maintained with the very latest information, ensuring that your IDS/IPS ready to detect and block the latest attacks from doing harm to your network.

Typically a huge volume of false positive alarms are generated by this type of technology however our managed IPS service helps organisations to overcome this. Our analysts carry out inspection of alarms looking for any signs of a false alarm before working with our customers to help neutralise the threat.

Managed DDoS

Distributed Denial of Service (DDoS) attacks have the potential to affect every organisation connected to the internet. Our Managed Distributed Denial of Service (DDoS) services puts protective measures in front of your critical assets to prevent DDoS attacks from disrupting your online services. Our Security Operations Centre (SOC) monitors 24/7 for DDoS attacks and are able to take responsive action the moment an attack is launched.

Our Managed DDoS service utilises our in-house developed DDoS Secure technology to provide application-level DDoS protection. The service is monitored and managed by a team with extensive experience of the DDoS landscape and an understanding and ability to interpret the activity.

Managed DDI

Core network services such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) and IP Address Management (IPAM) - collectively known as DDI, are the core foundations of every network are critical to the reliable operation of your whole IT environment.

Our Managed DDI service is a unique offering, leading the way in advanced DNS, DHCP and IP Address management and monitoring, offering proactive monitoring for high severity availability and integrity issues with core network services. The service utilises our own unique in-house-developed monitoring framework to remotely analyse key indicators of your DDI systems, to monitor and alert on any indicators of potential problems.

Security Analytics

A massive amount of security insight is hidden in your machine data but unlocking it can be tricky without the right expertise. Our Security Analytics Managed Services not only unlock your data’s full potential but makes sure it is usable.

Advanced attacks are carefully planned, well executed and difficult to defend against. A well implemented security monitoring or SIEM solution can give you the early indicators that you need in order to provide an effective response to these attacks. However, even with the most advanced SIEM solutions, you can only react to indications of attack if someone is watching the SIEM and triaging the alarms.

Managed SIEM

Our SIEM service leads the industry in delivering comprehensive and robust Security Analytics capabilities that help detect the modern multifaceted internet borne attacks, as well as threats that may come from within such as rogue admins and malicious insiders. We use a case-based approach to ensure that outputs delivered are of high value.

Our Managed SIEM service leverages our specialist expertise and includes professional services hours with SIEM experts, 24/7 monitoring of your infrastructure and continual review of customers’ systems identifying new ways to tune, improve and implement new detection logic so you don't have to.
Hosted SIEM

The NCC Group Hosted SIEM Service provides customers with comprehensive, highly resilient SIEM capabilities, using our hosted multi-tenancy LogRhythm SIEM platform, installed in our UK based data centre.

We use a use-case based approach to ensure that outputs delivered are of high value. The service provides advanced correlation, analysis and reporting capabilities on the log information collected from the customer’s sources. This service extends visibility beyond the network perimeter to the application layer to help businesses achieve more effective identification and mitigation of security threats and compliance validation with numerous regulatory standards.

With the Managed SIEM service, NCC Group SIEM experts will deploy an new full managed on premise SIEM solution or take over management and monitoring of an existing ArcSight, Splunk or LogRhythm platform, ensuring that you retain ownership of your critical security data, while we provide a true managed service to manage and maintain the platform as well as provide 24/7 monitoring.

Managed Performance Analytics

In a modern technology driven world carefully leveraging valuable system and performance data for business advantage can make all the difference. We provide a human triage and escalation of performance analytics alarms, not just relying on technology to send out alerts.

Cyber Threat Detection

Advanced network monitoring and threat detection is a necessity in order to keep organisations defended against the security risks posed by today’s adversaries. Network intrusions are an unfortunate but increasingly growing reality in today’s interconnected world. Organisations are now facing the harsh reality that if they haven’t already been breached, they probably will be in the future.

Managed Network Intruder Alarm

Our Managed Network Intruder Alarm (MNIA) is designed to detect attackers that have gained access to internal networks, using emulated services that form traps for attackers to trigger. MNIA triggers an emergency alarm back to our 24/7 SOC the moment they are touched. With a very low false positive rate, this early warning provides clear and concise evidence that someone is inside your network and you need to take action. Presenting themselves as genuine network components they wait silently for uninvited connection attempts before raising the alarm to our SOC.

Vulnerability Management and Detection

Our portfolio of vulnerability detection and management services delivers rapid detection, monitoring and remediation of deep-seated vulnerabilities within external and internal systems as well as proprietary and bespoke applications. Tens of thousands of endpoints, multiple networks, custom written applications, billions of lines of code and blurred lines between public and private access all have the ability to introduce unknown vulnerabilities into a network.

It’s these that cause the biggest risk as they can leave you with a false sense of security and an attacker with a powerful foothold into the very heart of an organisations sensitive data. Our Vulnerability Management services provide organisations with powerful capabilities to help identify unknown vulnerabilities in internal and external systems.

Web App Scanning

Our web application scanning services provide you with a fully managed, automated service that is designed to significantly reduce the risk of an external or internal breach. Our automated web application scanning services enable you to assess, track and remediate your web application vulnerabilities on a continual basis. Whilst penetration testing is necessary to give you an in-depth understanding of your weaknesses, our web application scanning managed service notifies you of new vulnerabilities on a much more frequent basis.

Security Monitoring

Our Managed Security Monitoring service provides an effective means to manage and monitor vulnerability risks on a more regular basis than standard penetration testing. Our service is intended to supplement the comprehensive penetration testing you are already receiving, and consists of daily infrastructure delta scanning coupled with monthly, quarterly or adhoc automated vulnerability assessments.

Types of scan include:

- Daily Delta scanning: Provides you with an initial baseline of your external infrastructure to highlight which services are visible.
- Automated Vulnerability Assessments: Provides you with the assurance that your infrastructure is being scanned at regular intervals.

Secure Internal Scanning

Cyber-attacks won’t stop at your external perimeter, so why should your security testing? Our internal security scanning services bring our comprehensive approach and enterprise grade scanning technologies to your networks. By becoming your internal security partner via our secure Firebase scanning appliance we can carry out assessments without needing to visit your site - improving both responsiveness and efficiency.

PCI ASV Scanning

Any company that has to comply with the PCI Data Security Standards has to perform quarterly external vulnerability scans (performed by an Approved Scanning Vendor (ASV)) as outlined by requirement 11.2. As one of the longest running members of the PCI ASV program our service gives you the confidence of a tried and tested scanning partner. Our accredited PCI ASV service uses enterprise grade scanning technology, experienced professionals and knowledge from across NCC Group's Assurance teams to help you secure your infrastructure against breach and maintain your compliance.
Our scanning service is flexible, scaling to any size engagement. It’s designed to be your partner – to help you to gain and maintain compliance by finding vulnerabilities and assisting your remediation efforts.

**Cyber Essentials**

The Cyber Essentials scheme is a Government certification to help businesses understand the basics of cyber security. As a Cyber Essentials accredited assessor, NCC Group can help guide organisations through the certification process, for both Cyber Essentials (Stage 1) and Cyber Essentials Plus (Stage 2). Stage 1 involves a self-assessment questionnaire which evaluates some of the basic controls that an organisation has in place to protect against cyber attacks along with an external vulnerability assessment. Stage 2 is based on an internal vulnerability scan of the system(s) in scope and, once again, this directly tests that the individual controls have been implemented correctly or recreates various attack scenarios to see whether a compromise with commodity capabilities can be achieved.

**Domain Assured**

Domain abuse such as spam, typosquatting, hosting of malicious code and phishing can all damage the reputation of an internet domain, resulting in lost revenues and trust as confidence from end users disappears. Domain Assured from NCC Group uses expert threat intelligence capabilities to deliver a complete picture of a domain's threat landscape with continual monitoring of the major domain abuse types to provide rapid notifications of any attacks. It monitors a domain's health and reputation and supports ICANN requirements by enabling registrars and registries to take a proactive approach to seeking out abuse.

**User Driven Vulnerability Scanning**

xStorm is a highly secure, centrally managed vulnerability assessment service hosted on a global network of NCC Group data centre locations. Customers in any part of the world can simply schedule scans, producing an automated security assessment report after each scan. Designed to enable network managers to run scheduled or on demand perimeter scans, the xStorm service can be configured for unlimited numbers of scans on any number of external IP addresses visible from outside the network.

**Two-Factor Authentication**

Through our Signify services we offer a scalable, cloud based solution, delivering market leading strong authentication services. We help organisations to secure their computer networks with a secure alternative to passwords that safely enables remote access to systems and information by delivering two-factor authentication as an on-demand hosted authentication service.

The successful deployment of two-factor authentication takes more than just technology; you also need to implement a framework of policies, procedures, logistics and user support.

**Signify token based authentication**

Signify delivers the market leading token based two-factor authentication system, using RSA SecurID tokens which have been the market leading two-factor authentication solution for the last 20+ years.

**Tokenless authentication - Signify software tokens**

The Signify Software Tokens deliver market leading RSA two-factor authentication by turning an Apple iPhone, iPad or iPod Touch, BlackBerry or Android smartphone and laptops into a strong authentication token, which work just like RSA's market leading SecurID keyfob tokens.

**Tokenless authentication - Passcode on-demand**

Signify Passcode On-Demand delivers tokenless two-factor authentication by turning any mobile phone or BlackBerry into an authentication device. When they wish to log in, a one-time passcode is sent to the user's mobile device in an SMS text or email message.

**Web Single Sign-On**

Web Single Sign-On (SSO) builds on our trusted two-factor authentication service by acting as a common single portal from which users can securely authenticate to Office 365, Salesforce.com and Mimecast cloud services, with a unified strong authentication service.

---

**About NCC Group**

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

---

+44 (0) 161 209 5200  
response@nccgroup.trust  
www.nccgroup.trust