Gold Team - Crisis Management Exercises

Full Spectrum Attack Simulation for the Cloud

Seize control of your cloud - Exploit future opportunities in a safe and secure way

Cloud computing is now as much a core business tool as it is a formidable threat surface.

While the pace of change is already transforming countless industries, every new opportunity presents new challenges and vulnerabilities.

So, if you're worried about your cloud security posture, NCC Group can help:

- Do you know your organization's cloud risk profile?
- How does that risk profile map to your budget?
- How does your budget map to your business risks?
- How has your risk profile changed in the last 28 days?

We can help you discover the answers.
Our consultants know exactly what it takes to assess, deploy and manage cloud strategies and technical services in a government context, to maximize your ability to innovate and minimize risk.

We combine world-leading technical cyber expertise with our advanced processes and thinking, creating a formidable service with a local touch and global reach that can assure your cloud environments and resolve your challenges head on. We provide full lifecycle Cloud Cyber security services from initial assessments to actively managing your system platforms, giving you the confidence you need to drive your business in the future.

A trusted partner, by your side. With the digital world moving so rapidly, we know every business and every cloud environment represents a very different challenge. That's why we work hand in hand with you, identifying your exact needs to create bespoke, tailored action plans. Armed with that plan, we mould a specialist team around your internal capability and trusted partners to ensure your cloud environment is safe, secure and fit for the future.

Expert Security Testing

Full Spectrum Attack Simulation (FSAS) for the Cloud by NCC Group is delivered by dedicated teams who focus solely on threat intelligence, real-world covert assessments and regulatory simulated attacks. NCC Group offers a suite of advanced assessment services and you can be confident your environment is reviewed by the very best using not only industry standard but internally developed and innovative techniques to identify your key issues.

Our extensive experience of assessing local government, central government and commercial organizations means we are able to assess the findings in the context of your organization's operations. NCC Group can therefore provide an accurate view of the likelihood of exposure and the threat posed of each vulnerability.

Key benefits of NCC Group's cloud software & application security assessment offerings include:

Bespoke: Every scenario is tailored to the organisation's specific concerns, team composition and previous experience.
Current: Addresses the need to move away from the classic network perimeter and to use identity based controls in the cloud.
Intelligence led: All attack scenarios are derived from the Threat Intelligence gathered on your organisation, mimicking the most realistic threats your organisation faces.
Safe: All activities are performed to pre-agreed rules of engagement, minimizing the risk of any adverse operational impact.
Comprehensive Reporting: Executive level summary of the business risks you face along with appropriate mitigation strategies, supported with remediation advice

NCC Group's cloud assessment experience and skills:

We have performed over 50 regulatory assessments and 100s of physical and cyber simulated attacks.

One of only a few organizations accredited to perform both threat intelligence and simulated attack assessments against all the international regulatory frameworks.

We have dedicated teams delivering nothing but FSAS engagements:

- Physical (Black) team
- Cyber (Red & Purple) team
- Board level assessment and advisory (Gold) team
- Phishing Simulation
- Threat Intelligence team
- Regulatory simulated attack team

Full Spectrum Attack Simulation for the Cloud

Cyber security and its associated risks is one of the largest threats to organisations worldwide. Traditionally cyber security has focused on applications and infrastructure. While this is extremely important, the vectors used by attackers are becoming increasingly sophisticated and varied.

Attackers are no longer limiting themselves to just cyber assets but including physical and human assets. The expansion to the cloud and the all too common loss of control associate with this only compounds the threat posed. As such, organisations need to defend and protect their business using more complex and skilled attack scenarios.

NCC Group has several service offerings to address your specific needs:

Physical assessments – we have both simulated attack and overt assessment offerings to identify threats to your staff and physical premises that may ultimately translate into a compromise of your cloud infrastructure.

Cyber assessments – we have both comprehensive custom Red Teams as well as two focused packaged offerings to address common concerns.

SOC improvement – our custom Purple Team sees NCC Group supporting your SOC team during a Red Team and is an ideal means of upskilling your staff and fine tuning your systems. If a lighter weight tool assisted approach is required, our adversary emulation platform, is the optimal solution.

Board level support – Our Gold Team is designed to assess your senior leadership in their ability to manage a crisis situation and the board level advisory and training services are designed to address any identified gaps.

Phising & Vishing Simulation – Our remote social engineering services range from basic to targeted assessments. This identifies vulnerabilities in policies and procedures and statistics on your susceptibility to such attacks.

Threat Intelligence – NCC Group have a number of threat intelligence solutions including a focused engagement designed to mimic the preparations of a skilled threat actor preparing for a concerted attack.

Regulatory Assessments – NCC Group can deliver the entire Full Spectrum Attack Simulation package of services in a manner that meets both UK and international regulatory requirements.

Whatever your need, whether it's a focused cyber assessment, assistance in improving your SOC or board level assessment and training, NCC Group has an offering to assist you in securing your cloud assets.

Our Approach to Securing Your Environment

Location of Testing

Traditionally the location of testing was a binary choice between remote and on-site, with remote testing conducted from across the Internet and on-site from within a trusted and protected network, typically a data centre or office location. The advent of cloud has blurred this distinction considerably, however the concept remains useful when considering the level of access a would be attacker or NCC Group consultant would have:

On-site Testing – the ability to assess the entire target unimpeded by network level security controls such as a firewall. Whilst firewalls and other mitigating controls are an essential component in a defence- in-depth strategy, many organisations wish to identify the true level of exposure of an individual target system should the network control fail or the attacker have trusted access behind the control. Software defined networks and virtual security appliances allow cloud environments to mimic traditional networks and as such the same considerations apply, albeit the controls are implemented differently, for example Conditional Access Policies within cloud environments.

Remote Testing – predominantly this testing takes place across the Internet and its intention is to mimic the level of access the majority of threat actors would have, be it a cybercriminal or hacktivist. Certain technologies may support remote testing across mediums other than the Internet, such as testing of wireless access points or remote access solutions over PSTN.

Firebase – an internally developed testing platform, Firebase is preconfigured to drop into your chosen network location, whether as a virtual machine or physical appliance. You have sole control of when the Firebase connects via a VPN using digital certificates to NCC Group's secure operations centre in the UK. All traffic is encrypted. Once connected, NCC Group consultants allocated to your project can conduct security testing as if they were physically in your office, data centre or cloud environment. Firebase allows for the level of testing associated with on-site engagements with the flexibility in scheduling and consultant support of remote engagements.

Black Team – Covert Physical Attack Simulation

A NCC Group Black Team assessment includes intelligence gathering, social engineering and physical security testing. The aim is to help you understand how easily an attacker can breach your physical security and access your networks.

A Black Team assessment will focus on the measures and processes you have in place to secure your environment against physical attacks. These attacks often rely on a lack of employee security awareness as well as social engineering attacks. Physical security weaknesses will normally be either procedural or cultural. Some organisations have excellent procedures, however, they may not be followed correctly due to a poor understanding of the need for appropriate security (cultural). In some cases the procedures themselves may be weak or absent (procedural).

During a Black Team assessment NCC Group will:

- Utilise Open Source Intelligence (OSINT) gathering techniques.
- Perform reconnaissance and surveillance.
- Assess the physical security.
- Attempt to circumvent technical controls and access sensitive areas of the organization or restricted locations.
- Manipulate staff to identify protected information, such as passwords, or allow access into their workspaces.
- Illustrate likely “post-breach” activities.
- Determine the level of response to threats.
- Determine likely threat actors for organization and target locations.

Key Activities:

Review the security policies and procedures in place for:

- Employees and Management
- Security Personnel
- Visitors and Contractors

Overtly assess the physical security controls:

- Physical protective controls
- Physical access routes or methods.
- Review monitored & unmonitored CCTV locations.
- Enumerate audible areas (Laser or Electronic Ear).
- Use of staff, visitor and contractor identification.
- Access card solution.

Red Team – Cyber Attack Simulation

Assessing individual applications and systems in isolation is no longer sufficient to protect your organisation. Instead, it is imperative that real-world adversarial behaviours and techniques are emulated to determine your ability to detect and respond to a cyber-attack.

Organisations must use more complex and skilled attack scenarios to better defend and protect their business

A Red Team assessment is a covert engagement designed to identify weaknesses in your cyber preventative controls, staff security awareness and to challenge your internal security team's detection and response capabilities. The ultimate objective of the engagement is to gain access to your critical assets.

NCC Group will assess your organisation through the emulation of adversarial behaviours and techniques that are used by real world threat actors, including hacktivists, cyber criminals, cyber spies, state sponsored actors as well as the ever present insider threat.

Throughout the simulated attack, a number of different attack scenarios will be planned and attempted in order of likely success.

NCC Group will highlight weaknesses in your systems, processes and security architecture. This will be tailored to different audiences from providing technical signatures and heuristics to Blue Teamers and threat hunters making strategic recommendations for the board and improving the state of security in both the short and long term.

Approach:

Red Teams follow dynamic attack paths that attempt to reach the agreed objectives.

Activities may include:

- Targeting your publically accessible services such as email and web servers, VPNs, Virtual Desktop Environments and Office 365 instances.
- Targeting your staff via their web and email clients to assess their level of cyber security awareness and the effectiveness of your security controls around communications.
- Determining if your endpoint protection can appropriately react to an advanced intrusion that attempts.
- Assessing if your workstation and server lockdowns are effectively restricting access to sensitive data and preventing unauthorised application usage.
- Establishing covert egress channels to enable command and control, persistent access and a means of collecting and exfiltrating data.
- Determining to what extent lateral movement is possible within your network.

Red Team – External Threat

A NCC Group External Threat assessment is a focused limited Red Team engagement with the goal of simulating an internet based threat actor attempting to gain Domain Administrator control of your internal network.

The goal of the engagement is to understand the threats facing you from a remote unauthenticated attacker who is attempting to breach the perimeter and gain privileged access to the internal network.

The prime objective is to gain domain admin access on your internal network

Typical Activities:

- Limited OSINT
- Targeted assessment of your externally facing systems
- Targeted phishing against internal users
- Activities necessary to elevate access to domain admin

Red Team – Internal Threat

A NCC Group Internal Threat assessment is a focused limited Red Team engagement with goal of simulating a malicious insider or an external threat actor who has gained a foothold on your network

The goal of the engagement is to understand the threats facing you from an attacker who already has a presence on the network. This will mimic both insider threat and successful remote attacks.

In addition to gaining domain administrator rights, we attempt to achieve three selective objectives.

Selective Objectives:

- Access Financial System
- Access R&D environment
- Exfill data from key system
- Access sensitive mailbox
- Access door controller(s)
- Access CCTV infrastructure

Purple Team – Upskilling Your SOC

Organisations are increasingly finding that vulnerability mitigation strategies alone are no longer sufficient to defend their business. The need to understand the attacker mind-set, interpret ongoing malicious activities and actively defend are becoming increasingly important components of an appropriate defence in depth strategy.

Organisations must ensure their security operations teams are appropriately skilled to detect and respond to the real-world adversarial behaviours they face.

A Purple Team engagement combines the Red and Blue Team activity, and sees NCC Group attack simulation experts embedded within your internal security operations (Blue Team) during the simulation of a real world attack.

A Purple Team can be delivered in a number of modes with either a focus on education or benchmarking.

In all cases full details of attack timelines, techniques used and an analysis of any detection and response capabilities will be provided.

The key differences between the differing approaches being at what point elements of this analysis is presented and to what degree we assist your Blue Team in their response to the attack.

Defensive Maturity Model

NCC Group will assess your defensive capability against the key phases of the attack methodology:

- Reconnaissance
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

Furthermore, each phase will be mapped to the MITRE ATT&CK framework and further analysed against your ability to perform the following actions against threat actor activities:

- Detect
- Deny
- Disrupt
- Degrade
- Deceive

The results will be presented in a manner that facilitates the easy comparison of a given environment over time or the comparison of differing environments.

Gold Team – Crisis Management Exercises

The ability of an organisation to detect, respond to and recover from an attack is a mark of resilience

However, to truly test that the people, policies, plans and procedures in place actually work, a realistic exercise is required. NCC Group's Gold Team exercises are designed to test your most senior crisis management team (CMT).

Business continuity exercises traditionally focus on an organisation's response to fire, terrorism or natural disasters. However, the response to a cyber-incident requires an organisation's most senior CMT, or Gold Team, to manage a situation with high levels of ambiguity and often greater interest from the public, media, regulators and other stakeholders.

As part of our comprehensive cyber incident response offering, we provide a highly immersive training exercise that puts your Gold Team at the heart of a major incident. This allows them to develop and practise their skills while mastering an ambiguous and challenging crisis situation in a safe environment.

Our bespoke and highly interactive exercise enables organisations to test their existing crisis knowledge, processes and protocols. The demands of internal and external stakeholder management will challenge them and allow both creative thinking and the examination of internal processes.

The Process:

As well as running and evaluating the exercise, we go through an in-depth planning and preparation process to ensure the exercise is realistic and reflects how your organisation operates.

The stages for a Gold Team exercise as are follows:

Diagnosis: A fact finding stage to understand existing processes, identify relevant personnel and define the objectives of the exercise.

Development: Content creation of the agreed scenario(s) for the multi-channel simulation.

Simulation: Delivery of the exercise itself.

Evaluation: Summary of key learnings and clear next step recommendations.

Board Advisory & Training Services

Cyber security risks come in many forms and Board and Executive directors are responsible for setting the strategy to ensure the organisation's resilience to support operations and growth.

NCC Group's Senior Advisers are experienced in providing, in non-technical language, appropriate advice and guidance to ensure that at a high level the essential cyber issues are sufficiently understood. They can equip the directors with the knowledge and skills to effectively manage cyber risk as part of their legally required governance and oversight responsibilities.

We provide a bespoke service to your executive and non-executive leadership team to assist and equip them to understand cyber issues throughout the year and business lifecycles.

Our engagement often starts with ensuring that they are aware of and understand the specific threats to their organisation.

Further engagements take the form of individual or group workshops, regular briefings, attending Board or Risk committee meetings, annual exercises, individual or organisation threat assessments, and personal cyber resilience reviews for Board members and key staff.

We regularly work as 'quasi non-executive directors' using our specialism in cyber risk to help the Board come to the right decisions on all cyber related issues.

Support to your business as usual activities

Senior Advisers provide specific support during both normal operations and when unforeseen challenges arise.

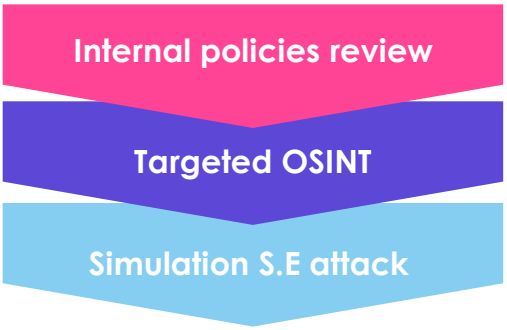
We offer advice, training and support on:

- Digital footprint reviews
- Essential cyber skills for members
- Cyber strategy development
- Secure migration to and within the cloud
- Cyber and privacy risks associated with mergers and acquisitions, or divestiture.
- Candidate assessment for C-level security roles
- Board roles in handling cyber related incidents

Phishing & Vishing Simulation

Phishing is used by fraudsters to trick email recipients into revealing valuable personal details such as usernames and passwords. Criminals send bogus communications and often embed links that will direct those who click on the link to a hoax website where login or personal details may be requested. It can also involve sending malicious attachments or website links in an effort to infect computers or mobile devices.

S.E attack simulation



It can take as little as 1 minute 29 seconds for an organisation to be breached by a phishing attack, with over 22 per cent of employees falling victim. But can you tell the difference between a legitimate email and a phishing email? What about your employees? Do you think they would be able to spot a phishing attack? Knowing how to spot the signs is vital.

The hoax websites used by cyber criminals are a lot more sophisticated than in previous years, so it is not surprising that more people are getting caught out.

Furthermore, our own research suggests that such websites are becoming a lot harder to spot with some 70% of employees at large organisations unable to tell a legitimate website from a phishing site.

The consequences of a successful attack could be catastrophic if information is leaked. And it won't be just your bottom line that suffers - it will also be your reputation.

But how can you help raise awareness within your organisation? In order to mitigate the risk, you need to understand your susceptibility.

Phishing and vishing attacks, OSINT and policy reviews, from NCC Group, helps to identify where weaknesses lie within your organisation and how you can improve your defences in a layered approach.

Standard Service:

One time service that determines your staffs' and organisation's current susceptibility to basic social engineering attacks. This can be carried out as telephone based (vishing) or email based (phishing) attack.

- Custom, targeted social engineering campaigns
- Create and send bespoke phishing emails, attachments and "landing pages" to your internal staff.
- Target an unlimited number of emails, sites and regions.
- Analyse your results with in-depth results via easy to digest graphs and charts.
- Optional education microsite to upskill users.
- Spoof internal phone numbers when making calls

S.E Attack Simulation:

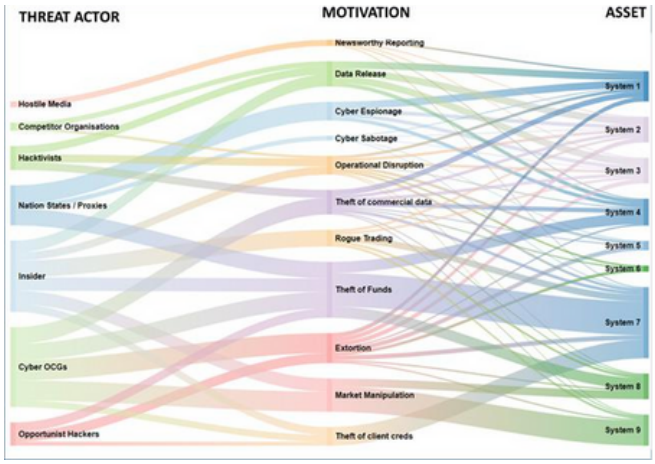
A "white box" simulated S.E attack based on a review of your security policies and open source intelligence (OSINT) gathering techniques. Attacks are targeted rather than "mass targeting" :

- Recommendations to improve associated security policies.
- Details of which users and information based on policy review was identified using open source intelligence, how they were profiled and recommendations to minimise exposure.
- Combination of vishing and phishing attacks.
- Targeted objectives linking the policy reviews, OSINT and S.E together for a proof of concept.

Targeted Threat Intelligence

Our expert threat intelligence services provide information on which threat actors are out there, what their intent is and which tactics, techniques and procedures they use to execute attacks. Through both human and technical information gathering we take raw data and information from a variety of sources and turn it into strategically, tactically or operationally valuable information for your organisation. NCC group can help you build confidence and develop an understanding of your current capabilities, along with the threats and vulnerabilities you face with the goal of developing a cyber-resilient organisation.

Mapping of threat actor, motivation and systems



NCC Group are accredited to perform CBEST (UK), iCAST (Hong Kong), AASE (Singapore) and TIBER-EU (other EU Regions). We are therefore highly experienced in bringing such programmes together to ensure you realise the commercial and operational benefits of this activity

Delivery of a Targeted Threat Intelligence (TTI) Report:

- The TTI report is a synopsis of the most significant, publicly available information, which is available about your organisation, which would facilitate the conduct of an attack by a threat actor.
- This information is collected passively in accordance with regulators guidance i.e., collection is limited to information which is in existence – NCC Group will not phish, socially engineer or otherwise 'hack' your organisation in order to obtain information.
- The TTI report cumulates in the creation of a number of attack scenarios which subsequently form the basis of any follow-on penetration test. These scenarios are designed to be credible, realistic scenarios which reflect the TTPs of relevant threat actors and where possible take in to consideration the findings of the General Threat Landscape (GTL) phase.

Benefits of Threat Intelligence:

The ability to consume threat intelligence can bring many benefits:

- Insight into of threats and associated risk faced by the enterprise
- General threat landscape and horizon understanding
- Internet exposure understanding
- Breach identification
- Breach prevention
- Fraud and theft minimisation
- Personnel/asset protection and risk minimisation

Our Experience:

NCC Group has conducted over 25 different regulator driven, intelligence-led threat intelligence assessments, including GBEST, TIBER-EU, CBEST and iCAST assessments and has been involved in over 50 engagements.

Targeted Threat Intelligence

Regulated testing and CREST STAR improves and organisation's understanding of real world threats, exploitable security weaknesses and detection and response capabilities. They provide evidence to the board and help formulate remediation plans to focus security spend for the greatest impact

These engagements are conducted without the knowledge or the organisation's defence teams over an extended period. The purposes of these tests is to evaluate weaknesses in people, technology and processes, providing an assessment of the detection and response capabilities of the defence teams.

These engagements are conducted without the knowledge or the organisation's defence teams over an extended period. The purposes of these tests is to evaluate weaknesses in people, technology and processes, providing an assessment of the detection and response capabilities of the defence teams.

Two key assessment phases include:

- **Targeted Threat Intelligence:** the identification of the likely threat actors targeting your key assets and techniques they will commonly use.
- **Scenario based testing;** covert Red Teams and potentially Black teams will attempt to enact the scenarios detailed within the Threat Intelligence report.

It is common for organisations to follow up a regulated assessment with phases of Purple and Gold team activity to address identified deficiencies.

As detailed to the right, NCC Group are able to deliver to a number of national and international standards. Reports generated from CREST STAR are not circulated amongst the regulatory authorities, as in the other schemes. This can make a CREST STAR an ideal preparation engagement. However the various regulators have access to government and sector specific cyber threat intelligence that is only available when conducting a regulated test.

Frameworks:

NCC Group has been approved to conduct both Threat Intelligence and simulated attacks against a number of frameworks:

- **CREST STAR:** Can be used by any organisation, in any sector and any country to evaluate their resilience to real work attacks
- **CBEST:** Is based on CREST STAR but requires specific accreditation of the provider by the Bank of England (BoE). Organisations are invited by BoE to conduct a CBEST and the regulators (FCA, PRA) will have oversight of all activities and reports.
- **GBEST:** GBEST is based on CBEST and is being rolled out across Government Departments. The scheme aims to be similar to CBEST but with some minor changes and is expected to take slightly longer than an average CBEST. The aim is for a GBEST exercise to take place in every major department at least once every five years. NCSC will provide validation and technical assurance of each exercise.
- **TIBER-EU:** Is the European framework for threat intelligence-based ethical red-teaming. It is an EU-wide guide on how authorities, entities and threat intelligence and red-team providers should work together to test and improve the cyber resilience of entities by carrying out a controlled cyberattack.
- **iCAST:** Is a framework introduced by the Hong Kong Monetary Authority (HKMA). It is not only a regulatory requirement, intelligence-led simulating testing uses real-world scenarios tailored to the target organization which can demonstrate an organisation's cyber defence capability to the board.

Our Experience:

NCC Group has conducted over 25 different regulator driven, intelligence-led threat intelligence assessments, including GBEST, TIBER-EU, CBEST and iCAST assessments and has been involved in over 50 engagements.

Reporting and Deliverables

NCC Group's consultative engagements support a number of vulnerability scoring systems including:

- Risk (default) – Issues are assigned a criticality rating of Critical, High, Medium, Low or Info
- CVSSv2/CVSSv3 – The Common Vulnerability Scoring System is a vendor-independent industry open standard,
- CWSS - The Common Weakness Scoring System (CWSS) provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner.
- MS BugBar – Microsoft SDL Security BugBar.
- DREAD - Classification scheme for quantifying, comparing and prioritizing the amount of risk presented by each evaluated threat

Symbol	Risk	CVSSv2	Explanation
	CRITICAL	9.0 - 10	This vulnerability requires resolution as quickly as possible.
	HIGH	7.0 - 8.9	This vulnerability requires resolution in the short term.
	MEDIUM	4.0 - 6.9	This vulnerability should be resolved as part of the ongoing security maintenance of the system.
	LOW	1.0 - 3.9	This vulnerability should be addressed as part of routine maintenance tasks.
	INFO	0 - 0.9	This finding should be addressed in order to meet leading practice.
	N/A	N/A	Good security practices were being followed or an audit item was found to be present and correct.

Optional information channels:

Daily wash-up meetings – an opportunity to discuss progress, any issues and findings to date. Any high or critical issues are always reported as they are identified.

End of engagement presentation – A post assessment briefing can be provided to give you an opportunity to discuss the engagement's findings and recommended next steps.

Findings in CSV format – to allow for the importing of findings into any GRC and issue tracking systems you utilised.

About NCC Group

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

With our knowledge, experience and global footprint, we are well placed to help organisations identify, assess, mitigate and 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.

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com