Retained Cyber Incident Response

During a cyber security incident, it is essential to have a partner you can trust to help.

NCC Group's Cyber Incident Response Retainer establishes an SLA and commercial terms, around our Emergency Cyber Incident Response Services, allowing NCC Group to respond faster when you need the service most.

Public Sector Investigations underpinned by an intelligence led methodology

Our Digital Forensics and Incident Response (DFIR) consultants have good experience of the public sector and have previously worked to support incidents of all sizes. NCC Group's threat intelligence, support incident response to help you react to changes in the attacker's Tactics, Techniques and Procedures (TTP). This enables the DFIR team to close the intelligence loop, understand the attack and quickly bring the incident under control.

Service Level Agreement (SLA) backed rapid incident support options

The Retained Cyber Incident Response service adds the assurance of service level agreements, with response times as little as one hour, to support your mission critical requirements.

Certified by NCSC Cyber Incident Response (CIR) and CREST Cyber Security Incident Response (CSIR) schemes

NCC Group's Cyber Incident Response service is recognised under both NCSC's Cyber Incident Response (CIR Standard & Enhanced) and CREST's Cyber Security Incident Response (CSIR) scheme. NCC Group is constantly engaged with these bodies and others to support our services with the latest available advice and threat intelligence.

Access to a 24x7 telephone service from our UK Secure Operations Centre (SOC)

The Retained Cyber Incident Response service provides a 'phone a friend' option that clients can use to confirm whether concerns are warranted, providing support and expertise to determine whether a security event should be handled as an incident.

The retainer service is a strategic service for clients opting for a proactive Incident Management stance.

Clients wishing to enhance this can (at additional cost) take out additional services as below which are designed to support your Incident Response Readiness.

- Compromise Assessment (subject to scoping)
- Incident Simulation
- External Attack Surface Management Scan

Benefits

- Public Sector Investigations underpinned by an intelligence led methodology
- Service Level Agreement (SLA) backed rapid incident support options
- Certified NCSC Cyber Incident Response (CIR) Standard & Enhanced
- CREST Cyber Security Incident Response (CSIR) schemes
- Access to a 24x7 telephone service, from our UK SOC
- Includes access to Specialists for Legal and/or Crisis Management support.

During the highly charged, dynamic environment of a live attack, it is comforting to have the support of trusted experts who can respond to the event with a calm, methodical approach.

The Retained Cyber Emergency Incident Response service from NCC Group provides you with all the components you need to effectively handle and respond to a breach. This offers you the assurance that should you require assistance, it is on hand 24 hours a day, 365 days a year.

Our DFIR team has the experience and technical capability to deal with any cyber emergency incident, from state sponsored attacks through to less sophisticated attacks that still bypass traditional network defences. With one of the largest incident response (IR) teams in the world, we are equipped to minimise the impact of an incident.

Retainer Phases:

1. **Scoping**

   A brief questionnaire on your controls and network, so we can understand options in the event of an incident.

2. **On-boarding**

   An understanding of organisation supports our investigation to address the incident effectively and swiftly. Understanding your response needs allows us to adopt your way of working, to support as seamlessly as possible.

3. **Business as Usual**

   The steady state phase. Our triage service is available to you, providing advice/triggering the incident response service.

4. **Incident Response**

   When you trigger, a scoping call will identify the business priorities and we will advise on initial containment and forensic acquisition actions. As the investigation begins, you will receive regular updates via email and calls as required. We will work with you throughout the incident, developing a joint understanding of the attack, and providing you with a full report afterwards.

5. **Close down**

   As the retained contract comes to a close, your account manager will discuss options around renewal, and options around any unused retained days against our other services.

Summary

Incidents will happen. Proactive efforts significantly reduce how often, yet do not prevent everything. The Retained Cyber Incident Response service from NCC Group takes our well regarded incident response services and provides extra assurance with established SLA's and a series of additional features, intended to reduce how often incidents occur.

A Retainer provides clients with the ability, and confidence, that NCC Group will leverage its resources in a timely manner to support you when you need it most.

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