NCSC Certified Cyber Incident Response

CIR Standard and Enhanced

NCC Group's Digital Forensics and Incident Response provides Emergency Cyber Incident Response services to give rapid access to experts following a cyber breach. NCC Group will provide support or manage the incident entirely, reacting to the incident and altering the response as necessary.

From deep threat intelligence and technical expertise to legal & regulatory support, our integrated offering helps you recover with confidence from a cyber incident.

Incident Response is made up of a number of activities which take place during and immediately after an incident, including:

- Determining the extent of an incident against an organisation's datasets, systems, and networks
- Managing the immediate impact and assisting in containment activities
- Providing advice and assistance to rectify the compromise of that system
- Reviewing security posture improvement and suggesting takeaway improvements
- Providing security Improvement & Remediation activity longer term to increase security across the network

Incident management is conducted by qualified and experienced individuals, and certified by NCSC Cyber Incident Response (CIR Standard & Enhanced) 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. We are constantly engaged with these bodies, and others, to support our services with the latest available advice and threat intelligence.

Investigations underpinned by an intelligence led methodology

NCC Group provides Threat Intelligence across all sectors. Investigators are engaged internally with these services and refine external intelligence sources to rapidly understand changes to the threat environment. This enables the Incident Response team to close the loop, and quickly bring incidents under control.

Comprehensive technical analysis including forensics, network investigation & malware analysis

Our Incident Response team draws on a wide and varied skill set to deliver our incident response services. They are supported by specialists in the team and can draw on the wider skillset of the NCC Group consultants if needed for specific technologies.

Supported by a global technical security consulting team

NCC Group has a widely respected team of specialists. This provides an extended pool of talent that can support larger incidents in parallel. Working behind the scenes, our response to recent large-scale incidents, supports continued service delivery in times of need.

Benefits

- Incident Response conducted by qualified and experienced individuals
- Investigations underpinned by an intelligence led methodology
- Comprehensive technical analysis including forensics and network investigation
- Certified NCSC Cyber Incident Response (CIR) Standard and Enhanced
- CREST Cyber Security Incident Response (CSIR) schemes
- Supported by a large global technical security consulting team

Digital Forensics and Incident Response Team

Our Digital Forensics and Incident Response Team offers expert support when you need it most. The team are armed with the expertise and experience needed to triage, investigate, contain and remediate any threats. Our team of experts leverages its experience directly to understand the crucial aspects of the incident and coordinate an appropriate team.

Incidents take many forms, and clients can have varying degrees of preparedness. We can engage at all levels including Executive Board Support, Crisis Management and Incident Response Lead and Incident Response Analysts as desired and required by the incident.

The assigned team scales with the incident, and may include multiple incident responders, incident managers, malware analysts and gold command support. Reaching across NCC Group, we bring in SMEs as required to support you and address the incident with minimum disruption.
Incidents often blend NCC Group services, commonly leveraging;

- Host analysis (including memory and disk forensics)
- Log analysis
- Open Source Threat Intelligence (OSINT)
- Compromise Assessments
- GDPR support

Retained Cyber Incident Response service

For clients desiring a service level agreement or a faster deployment, our Retained Cyber Incident Response service adds a management wrapper, access to a 24x7 telephone service, First Responder training, Incident Response Readiness review and access to specialists for legal advice/crisis communications support, and other features around the Emergency Incident Response service.

Technical details

The Digital Forensics and Incident Response Team leverages specialist software to assist our work. An aspect that always helps is having access to good log information, from a SIEM source. Ideally this should retain logs for a lengthy time period, from before the incident started, and scoped to include key assets, such as authentication system, domain controllers, perimeter security controls, email and web filtering, and any hosts involved in the incident. As this is impossible retrospectively, proactive log and audit controls are always encouraged, along with patching, privilege management and strong anti-malware controls.

A typical incident engagement will see several stages, aligned to the NIST 800-61 framework;

1. Triage & Scoping
2. Authorisation
3. Deployment and travel to site where necessary
4. Forensic evidence capture and analysis
5. Containment
6. Eradication and Recovery
7. Post Incident Reporting and Remedial activities

Summary

The most proactive cyber security control framework will dramatically reduce the rate of incidents yet comes with significant financial and agility penalties. Deploying a team of incident specialists to manage incidents is neither desirable nor cost effective.

NCC Group's Cyber Emergency Incident Response service provides you with access to trained, qualified specialists when you need them most, and can facilitate a prompt return to service.

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