G-Cloud 15

Digital Forensic Incident Response and Cyber Investigations

CCL has a proven track record of delivering comprehensive Digital Forensic examinations as a core component of our Cyber Incident investigations, working seamlessly within our dedicated Incident Response team.

CCL's investigation services focus on reconstructing past events from artefacts such as the file system, memory, and log files. Operating as a unified force, we combine detailed forensic analysis with rapid response to determine the root cause of the incident, the scope of the breach, and the data that may have been impacted. This thorough examination allows us to gain a complete understanding of the incident to prevent its recurrence, support targeted isolation and remediation, and implement further improvements to an organisation's cyber resilience.

CCL's incident investigation teams offer a breadth of tailored investigative services including those detailed below:

Remote Forensic Collection

An incident may begin with the detection of abnormal behaviour on a single system but the scope of the incident often turns out be much bigger. Forensic work is focused on producing factual data to reconstruct past events or suspicious activities, which enables subsequent identification of the root cause of the incident. The days of capturing complete images of hard drives and volatile memory before commencing forensic analysis have long gone.

CCL's remote collection service can be used to access and triage a company's IT systems quickly and efficiently. This enables us to perform selective and targeted data collection from endpoints, with the option to collect forensic images of disks and memory as well if necessary. Our analysts can support clients through the whole process from start to finish to acquire data securely from a variety of endpoints and services, including from mobile devices and cloud-based systems.

G-Cloud 15

CCL SOLUTIONS GROUP

Insider Threat

Organisations of all types and sizes are vulnerable to insider threats. Current or former employees entrusted with access to a company's intellectual property or operational data represent a potential risk of this information being leaked. Potential threats to the business can be malicious or unintentional, and can include data loss, fraud, sabotage and theft. Loss of revenue and reputational damage can ensue as a result.

Effective communication between the organisation and a trusted digital forensic service provider is vital during the mitigation process after a breach. With a baseline established using techniques such as active monitoring, CCL's forensic investigators can help to identify abnormal behaviour indicative of insider threats.

Malware Identification and Analysis

Complex and targeted attacks are often the result of infection by malicious software (malware). Attackers can use malware to infiltrate systems, to perform reconnaissance, to gain access to further systems, to steal data and to sabotage systems. With malware being a root cause of many cyber incidents, the identification, analysis and remediation of malware is a vital part of the incident response process.

CCL's malware identification and analysis service provides incident responders with the information required to determine malware potential, perform damage assessment, and define the extent of incidents caused by malware. Detailed results from CCL's malware investigations provide actionable information that can help remediate vulnerabilities exploited by malware and mitigate potential recurrence of attacks.

Email Compromise

Compromise of business email is one of the most damaging attacks facing companies, potentially resulting in loss of funds, loss of sensitive information, breach of other computer systems and significant reputational damage. An attack often commences with a carefully crafted phishing email addressed to key personnel.

CCL's response to business email compromise incidents involves a fast forensic examination to identify the scale of the incident and its root cause. This process involves tracking back to the attacker's entry point ("patient Zero") to determine the original vector of the attack. By performing a targeted examination, CCL aims to reduce the time to resolve the compromise and provide recommendations to prevent similar attacks in the future.

CCL SOLUTIONS GROUP

G-Cloud 15

Open-Source Intelligence Investigations

There are a wide range of uses for Open-Source Intelligence (OSINT), including by government, law enforcement agencies and private companies. A large amount of information can be gathered from publicly available online sources and intelligence gained from such sources can be useful for many purposes. The online activities of an employee, press coverage about a cyber attack victim, listings of stolen data available for sale and leaked account credentials are some examples of important sources of intelligence.

CCL's analysts take an investigative approach to the planning, analysis and reporting required when conducting an OSINT investigation. A combination of our digital forensics pedigree and understanding of data landscapes allows for a thorough investigation to be conducted in line with the exact requirements scoped with the client. Following a comprehensive data gathering and investigation exercise, we produce a clear and detailed report that is suitable for use as evidence in court.

Dark Web Investigations

The Dark Web is a section of the Internet that cannot be accessed through standard means but instead requires the use of specialist tools. The Dark Web is home to many illicit marketplaces and forums which are used to trade illegal goods and services such as drugs and even data stolen by hackers who have infiltrated an organisation's network. The anonymity afforded by Dark Web technologies can make it very difficult for law enforcement agencies to trace services and transactions.

Once an organisation's network has been breached, the intruder can exploit the company by identifying and extracting valuable and sensitive information, such as customer account details, banking details and so on, and then threaten to publish it. CCL's Dark Web investigations can assist organisations to identify valuable or sensitive information that may have been released by an intruder.

G-Cloud 15

CCL SOLUTIONS GROUP

CCL Solutions Group is one of Europe's leading digital forensics, discovery and disclosure, and cyber security specialists.

Our range of services have been specially designed to help clients tackle their particular challenges efficiently and effectively. They provide a reliable, robust solution every time, with complete price certainty from the outset.

CCL Solutions Group in numbers

30+
year track record across public and private sector

8
of the UK's top 10 largest police forces supported

11,000+
cases handled over past five years

150+
forensic experts, investigators and analysts

1st
CCL-Forensics was one of the first to be ISO 17025 accredited

10
key quality standards achieved

1,500+
custom scripts developed by our R&D Centre of Excellence

4
continents with active operations

Our accreditations

CREST

Assured Service Provider — in association with National Cyber Security Centre — CHECK Penetration Testing

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

SGS UKAS MANAGEMENT SYSTEMS

SGS UKAS MANAGEMENT SYSTEMS

cclsolutionsgroup.com
+44 (0)1789 261 200

First for digital forensics and cyber security