CYBER INCIDENT RESPONSE SERVICE

Businesses are suffering from increasingly sophisticated cyber security incidents resulting in damaged reputation and the loss of critical business winning information and intellectual property. Many published surveys suggested 8 in 10 large UK companies have been breached, with almost 60 per cent expecting attacks to worsen.

After an intrusion, hackers can cause irrevocable damage within hours. Once a breach has been discovered it is vital that action is taken to understand the scope of the incident and limit its effect on the business.

Our Cyber Incident Response Team(CIRT) is responsible for rapidly responding to suspected security incidents and guiding customers through the next steps. We have developed a highly experienced security incident response team, equipped with industry-leading tools and intelligence to handle any cyber security incident whether it is large or small.

Supported by our Archangel™ 24/7/365 Incident Response Hotline we can rapidly deploy to suspected or confirmed cyber-attacks.

Our UK CIRT can be contracted for a single engagement; on a retainer basis; or as part of our larger Archangel™ protective monitoring offering. All engagements are tailored to the customer's requirements and will be delivered by experienced security professionals.

KEY POINTS

- Malware Reverse Engineering
- Forensic Investigations
- Readiness Planning and Attack Simulation
- Advisory Distribution
- Network Monitoring
- Immediate 24/7/365 CIRT Response call out.

INCIDENT RESPONSE

SERVICES

Malware Reverse Engineering
Using industry certified methods our UK CIRT will investigate all samples using a dedicated malware analysis laboratory containing commercial and bespoke analysis tools. The CIRT is able to analyse different sample types, from executables to word documents in order to extract indicators of compromise such as IP addresses, downloaded files and file hashes.

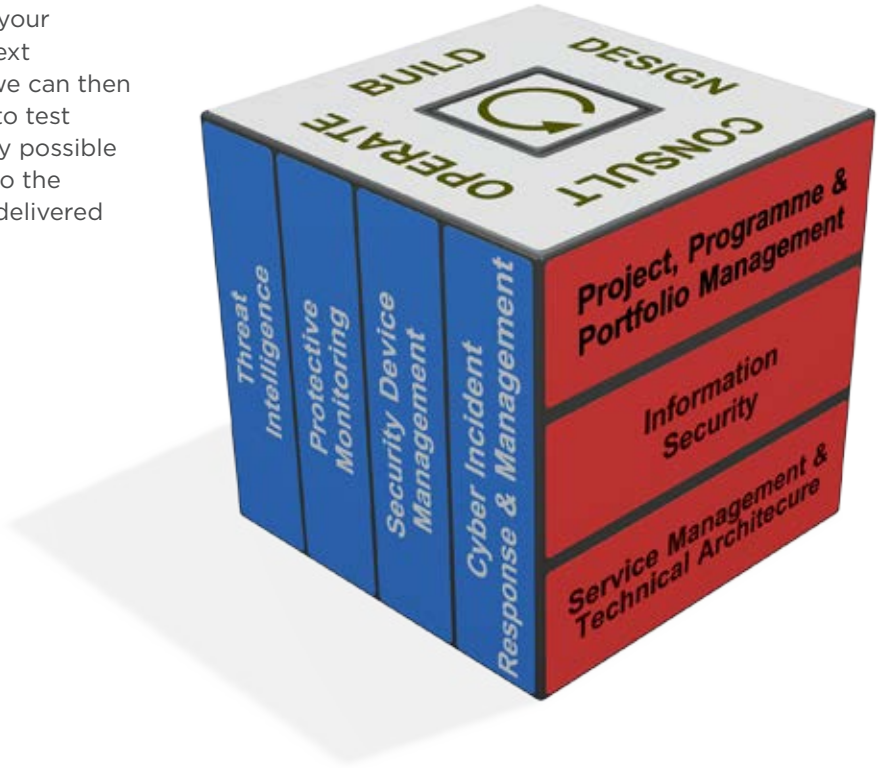
Forensic Investigations
Our UK Cyber Incident Responders are specifically trained in Intrusion Forensics, maintaining chains of evidence and the skills to identify unauthorised access. Our team members can deploy to your location quickly to collect forensic images of hard drives, volatile memory and network captures. These images will then be securely transported to the CIRT home site for forensic analysis using leading commercial tools and custom platforms.

Readiness Planning and Attack Simulation
Working with your in-house team, we can help you identify weaknesses in your systems, policies and procedures to maximize your resilience and preparedness for the next incident. Once planning is complete we can then construct security incident exercises to test your staff using known or theoretically possible attacks. Every simulation is bespoke to the customer's requirements and can be delivered on site or remotely by the CIRT.

Advisory Distribution
As your corporate network expands and the variety of internet connected devices increases the attack surface for malicious actors grows. Unless properly patched your devices can be used by the hacker to penetrate and disrupt your network. Everything from printers to cameras have their own unique vulnerabilities and flaws.

Using an in house advisory portal which combines multiple vulnerability feeds our UK CIRT is able to offer alerts on the newest vulnerabilities and threats as they happen. All alerts can be tailored to each customer's estate ensuring you receive alerts that are relevant to the devices within your network.

Network Monitoring
Using a custom built Incident Response platform containing remote forensics capabilities, a threat intelligence platform and elastic log search our UK CIRT can deploy a sensor into your estate. This allows us to detect previously unseen malicious activity within your network and respond to increase your resilience.



LEONARDO
SECURITY & INFORMATION SYSTEMS

For more information please email infomarketing@leonardocompany.com
Leonardo MW Ltd
430 Bristol Business Park - Coldharbour Lane - Bristol - BS16 1EJ - United Kingdom - Tel: +44 (0) 117 988 0033