Cyber Incident Response Services

G-Cloud (Cloud Support Services)

Service Definition Document

Leonardo UK Ltd
Registered Office: 1 Eagle Pl, St. James's, London SW1Y 6AF
Tel: +44 (0)117 988 0033 Fax: +44(0)117 988 0034

Table of Contents

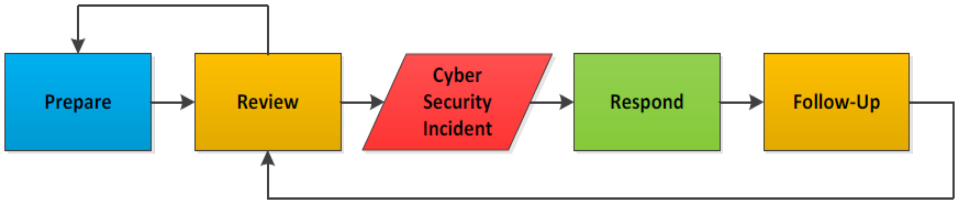
Leonardo UK Ltd
Registered Office: 1 Eagle Pl, St. James's, London SW1Y 6AF
Tel: +44 (0)117 988 0033 Fax: +44(0)117 988 0034

1. Introduction

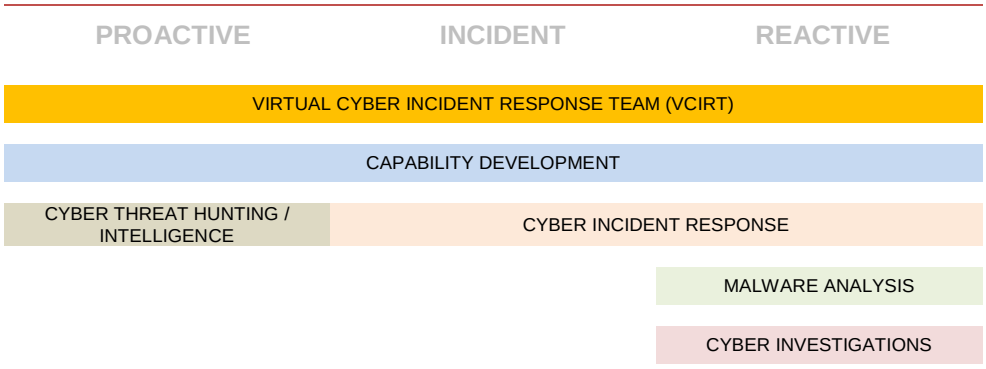
Leonardo MW (Leonardo) has a specialist Cyber Incident Response Team (CIRT) that provides a complete portfolio of services surrounding any cyber security breach or attack. The services assume that every organisation will experience an incident, with a combination of proactive and reactive services to help mitigate the impact effectively.

2. Service Overview

Our CIRT sits alongside the ARCHANGEL™ Protective Monitoring Service to provide advice and assistance to customers preparing for or dealing with a cyber security attack or breach. Our CIRT services cover each part of the three main frameworks and processes for cyber security incident response including those from SANS, NIST and CREST.



SANS Incident Response Process	Preparation		Identification	Containment	Eradication	Recovery	Lessons Learnt
NIST Cyber Security Framework	Identify	Protect	Detect	Respond		Recover	
CREST Cyber Security Incident Model	Prepare			Respond		Follow-Up	



Leonardo UK Ltd
Registered Office: 1 Eagle Pl, St. James's, London SW1Y 6AF
Tel: +44 (0)117 988 0033 Fax: +44(0)117 988 0034

3. Cyber Threat Hunting

Cyber Threat Hunting is our most proactive CIRT service which gives customers the opportunity to uncover evidence of their infrastructure having already been breached or attacked.

Cyber Threat Hunting takes a novel approach to ‘surveying’ an organisations infrastructure for indicators of compromise through analysis of forensic artefacts, security appliance logs and network-based anomalies. It focuses on all areas of an organisations digital estate, often finding evidence of compromise in areas deemed outside of the scope of other cyber security appliances or monitoring solutions.

Cyber Threat Hunting can be conducted either passively by ‘living off the land’ without deploying specialist tools, which is especially useful for sensitive networks, or actively with advanced tools for fast and more effective data collection and active monitoring.

As part of a complete cyber security strategy, Cyber Threat Hunting complements Cyber Vulnerability Investigations (CVI) and Penetration Testing.

Customers receive a report highlighting all identified threats and recommended remedial action, from both an organisational and technical perspective. A workshop is included as standard to go through either the technical or the managerial points made in the report.

4. Cyber Threat Intelligence

Digital technologies lie at the heart of nearly all industry today. The automation and inter-connectedness they afford have revolutionized the world’s economic and cultural institutions. However, they have also brought risk in the form of cyberattacks. Threat intelligence is knowledge that allows an organisation to prevent or mitigate those attacks. Rooted in data, threat intelligence provides context :-

- Who is attacking you?
- what is their motivation
- what are their capabilities
- what are the indicators of compromise in your systems to look for

That helps you make informed decisions about your security.

Our Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets.

5. Cyber Response Capability Development

Our Cyber Response Capability Development service is built on the need for organisations to develop capability across people, process and technology in order to effectively handle any cyber security incident.

All of our CIRT services can be used for development to build in-house capability with training, documentation and advise on staffing, skills and tools.

	People	Process	Technology
People	Professional development	Management and end-user skills training	Technical skills training
Process	Cyber Security Incident Response Plan Authoring	Cyber Security Incident Response Planning	Cyber Security Incident Response Plan Testing
Technology	Cyber Security Incident Response Teams	Security Operations Centres	Systems implementation and infrastructure improvement

Professional Development

The skills, competencies and awareness an organisation's people have are directly representative of their capability to effectively identify, respond to and recover from a cyber security incident. The professional development service delivers cyber skills training for end-users, technical staff or managers, including; technical training in incident response, malware analysis and digital forensics, managerial training in incident management and cyber threat awareness, and end-user awareness in phishing and social engineering.

End-user training can include phishing and social engineering assessments to measure the effectiveness of training.

Cyber Security Incident Response Planning

Planning for a cyber security incident is essential in effectively identifying, remediating and learning from it. Our incident response planning service helps customers author a tailored plan from scratch or rehearse and improve an existing one aligned to best-practice including CREST, SANS or NIST.

Systems Implementation and Infrastructure Improvement

Our systems implementation and infrastructure improvement service includes building or reviewing an organisations technical security monitoring or incident response capability, with a view to implementing improvements for a more effective capability.

6. Cyber Security Incident Response

Our retained or on-demand cyber security incident response (CSIR) service combines capability in incident management and investigation to deliver expert advice, comprehensive technical analysis and peace-of-mind in the face of any cyber security attack or breach. The service is underpinned by our capability development service to empower existing staff and help wider stakeholders comprehend the technicalities.

On-Demand

Organisations that do not have a service agreement with any provider for CSIR services will benefit from our on-demand service when they suspect or confirm a cyber security breach or attack.

Retained Service

Our retained CSIR service offers peace of mind and excellent value in the case of an incident or for any associated work in preparing for or following-up on an incident. The service is supported by a service level agreement.

7. Malware Analysis

Verifying a file is malicious by understanding how it conducts nefarious activity can deliver actionable insight into its wider purpose and motivations, sometimes extending to human factors. With this information, organisations can protect themselves better through derived cyber threat intelligence which can identify future attacks in monitoring systems or increase awareness in threat actor motivation.

Our malware analysis service is a natural follow-up to any CSIR or threat hunting engagement. The service complements our proactive threat hunting and reactive cyber security incident response services as a technical measure to assuring security after a breach or attack and assessing risk going forward.

8. Cyber Investigations

Investigating incidents or matters which are facilitated by or through digital means requires a capability to understand a range of technical subjects underpinned by investigative thinking. Customers can augment existing in-house capability long-term or call on investigatory services when required under our Cyber Investigations service.

Our digital forensics and cyber investigation specialists offer root cause analysis, internal investigation support, open-source cyber vulnerability investigation and data acquisition, discovery and presentation.

9. Virtual Cyber Incident Response Team (VCIRT)

Organisations need a capability for the identification, containment, eradication and recovery of cyber security attacks and breaches, but many do not have suitable capability due to cost and infrequent demand. This service allows your organisation to combine one or more of our incident response services to create a managed capability. This service allows your organisation to custom-build an Incident Response capability using an already experienced team with specialist services for comprehensive assurance that preparation for and dealing with incidents is done effectively. Experienced incident responders are available to support your technical capacity on-demand, integrate with existing your cyber security or IT teams to drive team development, or provide an entire capability independently as a service.

END OF DOCUMENT

Leonardo UK Ltd
Registered Office: 1 Eagle Pl, St. James's, London SW1Y 6AF
Tel: +44 (0)117 988 0033 Fax: +44(0)117 988 0034