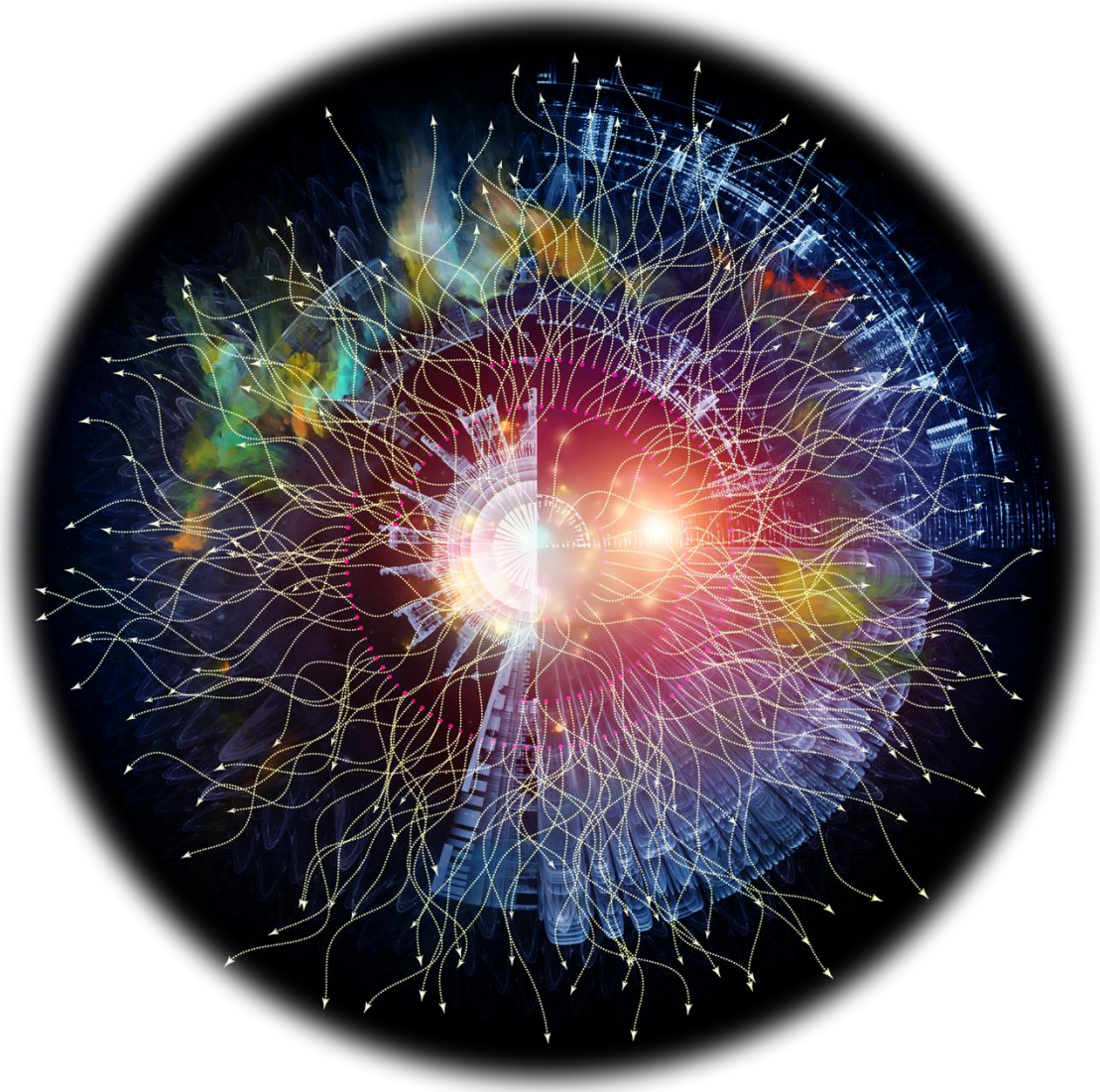
Deloitte.



Cyber Incident Response

G-Cloud 14 Service Definition Document

May 2024

MAKING AN IMPACT THAT MATTERS since 1845

Contents

1 Deloitte Overview

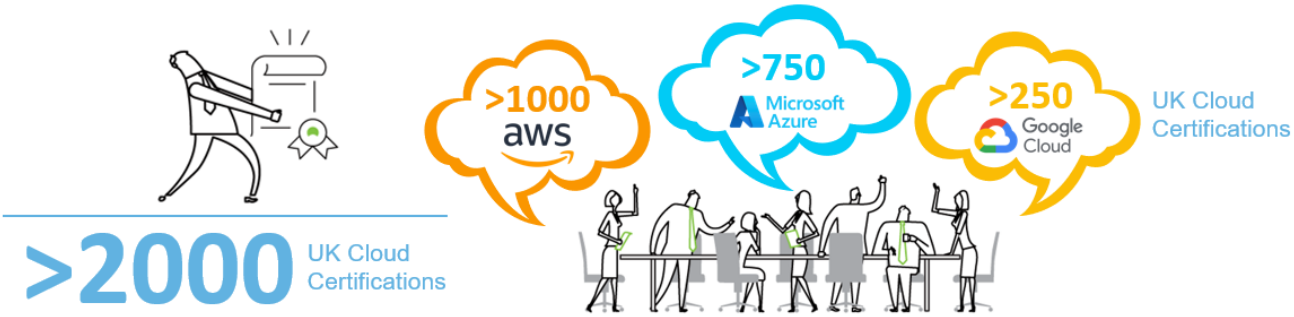
As a leader in professional services, Deloitte LLP is committed to making an impact to our clients, our people and for society. We have over 25,000 staff based across the UK providing audit, risk advisory, tax, consulting, financial advisory and legal services to public and private clients across multiple industries. We work together to build trust, support inclusive growth, and build capability, enabled by our **breadth and depth of expertise across advisory, delivery, engineering and managed services.**

Our **public sector practice** serves Central Government, Government Agencies, Local & Regional Government, Defence, Security and Justice, Health and Social Care, Transport, Education and Housing. We also provide services to the Northern Ireland Office, Scottish Government, Welsh Government and Crown Dependencies.

Our Cloud Capability

At Deloitte, we help our clients **Imagine, Deliver** and **Run** the businesses of the future through the power of **Cloud**. We have deep Cloud architecture, engineering, operational, commercial, and business transformation expertise delivered by a team of more than 26,000 Cloud Practitioners globally. We have delivered over 2,000 cloud implementations over the past 5 years and have 60+ cloud centres of excellence supporting the delivery of cloud services to our clients.

In the UK, we have a growing team of OCI specialists, over 100 Cloud managed service specialists plus the following certifications across AWS, Microsoft Azure and Google Cloud:



We help our clients with all aspects of their journey-to-cloud and optimisation of their cloud and cloud-services investments. Our Cloud practice can support you to optimise your client investments, and to navigate your organisations cloud journey, providing specialist cloud architecture, engineering, and operational skills at all stages, with a large proportion of our team holding the clearances required to meet your specific security requirements.

Our alliances & ecosystems

To bring full value to our clients, Deloitte is a premier consulting partner with all the leading hyper-scale cloud vendors in the market including AWS, Google, Microsoft[1], Google and SAP. A selection of our partners and alliances are presented below:

Azure MuleSoft salesforce servicenow workday.
aws 500 CERTIFIED AWS PARTNER NETWORK Google Cloud SAP Platinum Partner ORACLE PARTNERNETWORK snowflake

[1] As Microsoft's Independent Auditor, Deloitte cannot have a direct or material indirect business relationship with Microsoft, such as having an alliance or being a registered partner. Nonetheless, Deloitte can provide Microsoft-related technology services and invests heavily across its global business building technical skills and capabilities to develop world-class consulting and solution delivery capabilities.

What the analysts say

Don't just take our word for it. Deloitte is recognised by the analyst community as being **leaders in cloud transformation services.** This reflects the wealth of experience we have in delivering cloud services across the public sector and wider private sector combined with our out-of-the-box templates, tools and assets.

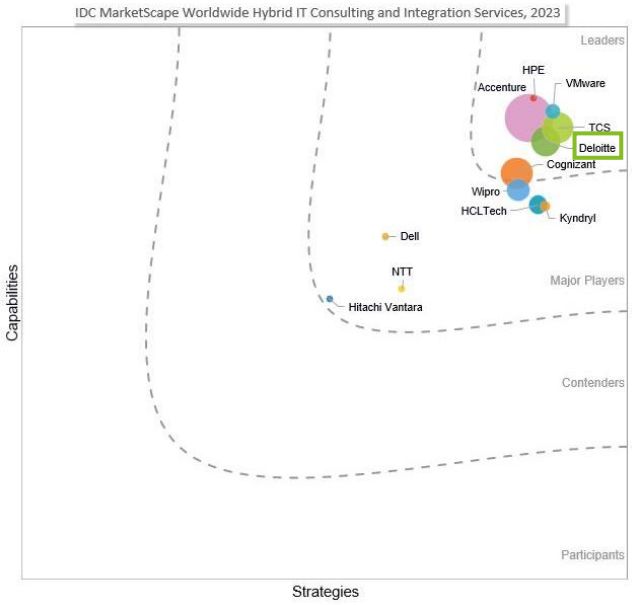
Gartner

Originating in 2021, Deloitte has been recognised as a Leader in this category for three years in a row. Deloitte was also positioned as a Leader in the **Gartner Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide** in 2021, 2020 and 2019.

Gartner: Magic Quadrant for Public Cloud IT Transformation Services. **© Gartner inc. 2023**

IDC

Deloitte has been awarded Leader status in the **IDC MarketScape: Worldwide Hybrid IT Consulting and Integration Services 2023** Vendor Assessment. In 2023, we were also recognised as Leaders in **Hybrid IT Consulting & Integration Services** and **Software Engineering Services**.



IDC MarketScape: Worldwide Hybrid IT Consulting and Integration Services 2023 Vendor Assessment **© IDC inc. 2023**

Deloitte scored highest in 4 of 5 Use Cases in **Gartner® Critical Capabilities for Public Cloud IT Transformation Services 2023** report:

"Deloitte approaches all aspects of cloud adoption, including migration, with transformation as an objective."

2 Service Overview

Deloitte's Cyber Incident Response service provides a readily available response capability to support clients suffering from **cloud attacks** or **breaches** from either **internal or external threats** and limits their impact by recovering faster, with the aim of **emerging stronger**.

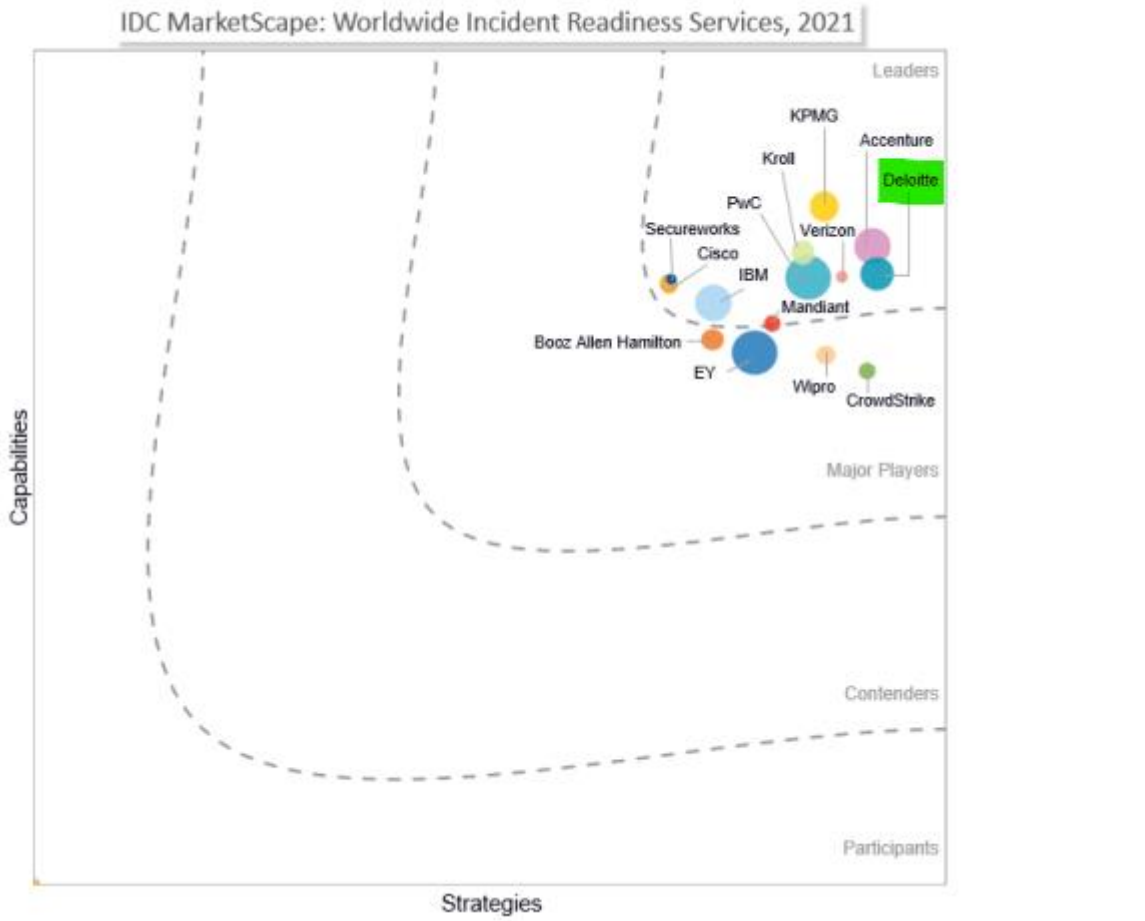
Features

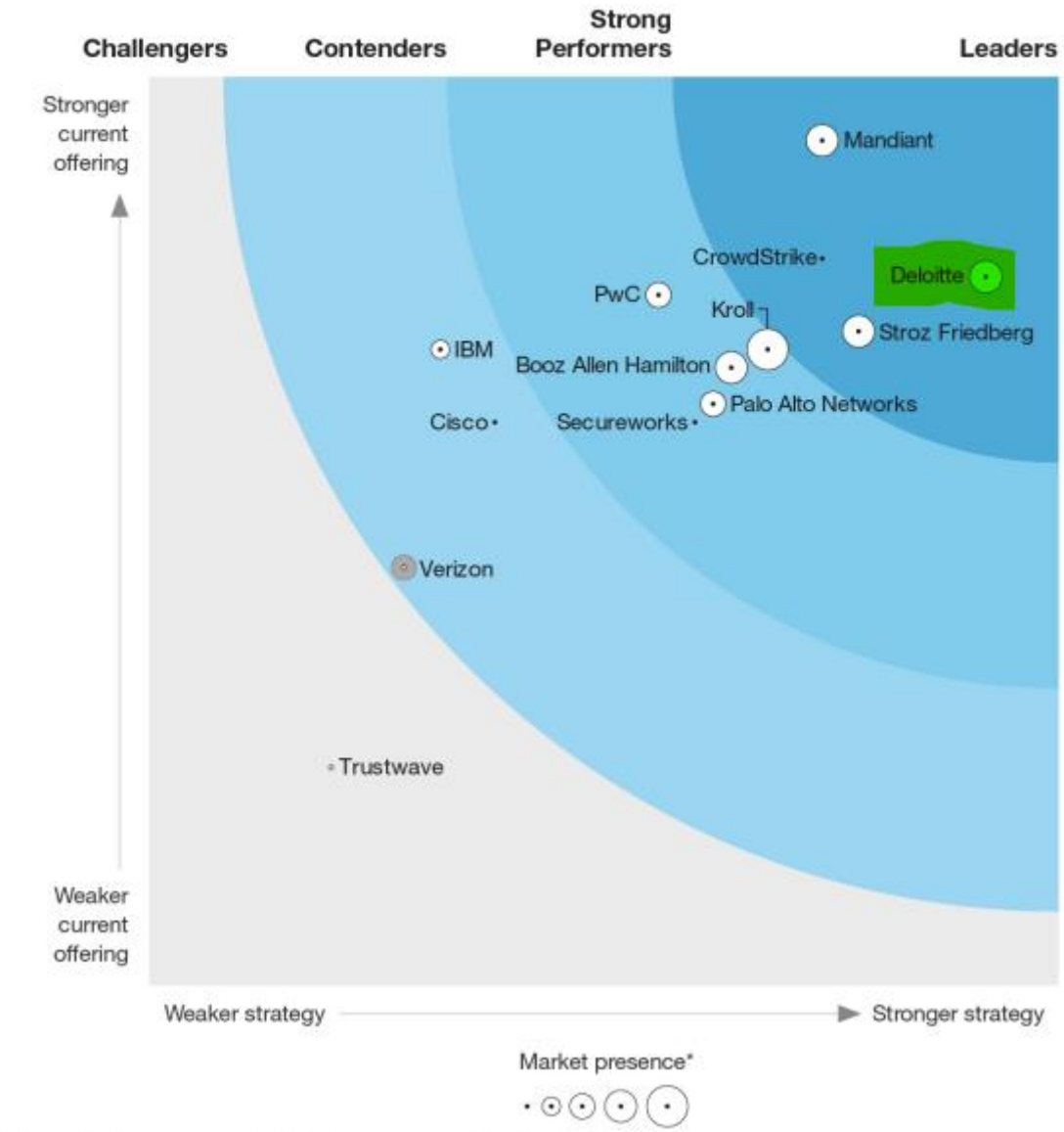
- Cyber Incident Response Retainer
- Cyber Incident Response Emergency Technical Support
- Cyber Incident Recovery

Benefits

- Cyber Incident Response Retainer and response SLAs
- Access to skilled crisis management experts when an incident occurs
- Support with technical analysis, containment and post-incident recovery
- End-to-end incident lifecycle coverage from preparation to incident management
- Analysis of root causes, response effectiveness, and adequacy of remediation
- Leader in the 2022 Forrester Wave for Cybersecurity Incident Response Services
- Deloitte named a worldwide leader in the 2021 IDC MarketScape vendor assessment for Incident Readiness Services.

IDC MarketScape Worldwide Incident Readiness Services Vendor Assessment





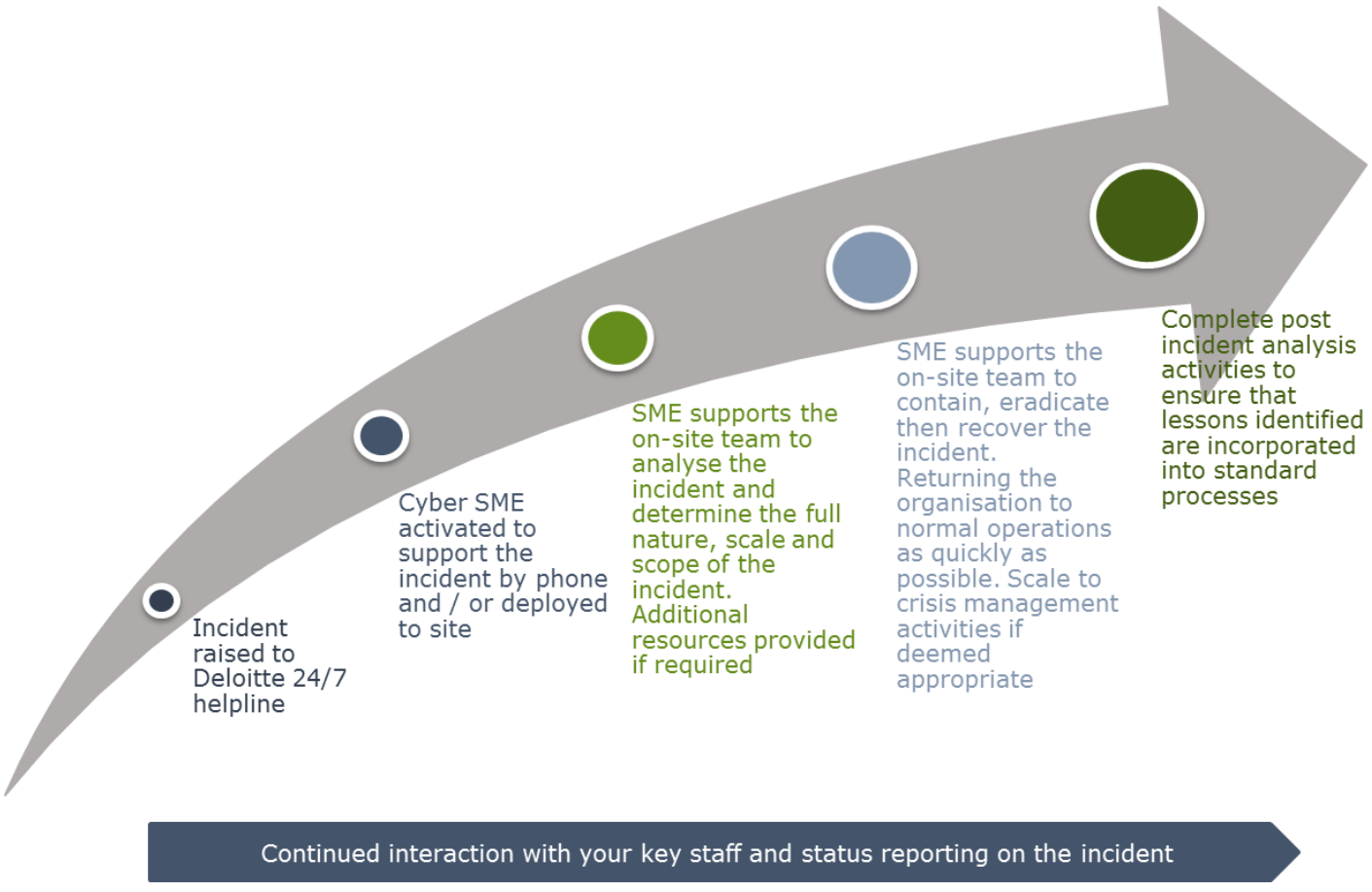
3 Detailed Service Description

Our Cyber Incident Response (CIR) service assists security teams with the effective management of a security incident, breach or attack. Our assistance may be requested due to a lack of resource, technology or expertise in the organisation to resolve the incident effectively.

Our goal is to limit the impact of an incident so that the business can resume normal operations as soon as possible. The range of CIR capabilities offered to assist with the management of a cyber incident is shown below, this list is not exhaustive:

- **Incident management** – managing and prioritising multiple work streams, limiting disruption to the business and liaising with the key stakeholders during an incident, to limit an incidents impact on the business.
- **Incident Recovery** – Managing the recovery process and the safe restoration of services
- **Network forensics** – monitoring and analysing network traffic for information gathering or intrusion detection.
- **Endpoint forensics** – collecting, preserving and analysing information gathered from operating systems.
- **Malware analysis** – detecting and analysing pieces of advanced malicious malware, that may threaten client infrastructure.
- **Log file analysis** – collecting and analysing large volumes of log data from various systems using automated and manual techniques.

Our adopted incident management approach allows our responders to determine the most appropriate resource(s) for supporting the incident, ensuring effective and timely remediation.



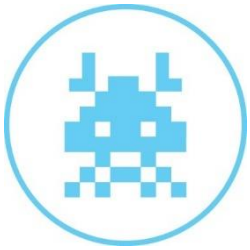
We maintain a focused and systematic Cyber Incident Response approach in accordance with the National Institute of Standards and Technology (NIST) Computer Security Incident Handling guidelines.

The service is assured by the NCSC.

Our specialist team is able to deal with the full spectrum of incidents that can affect client organisations:

Advanced persistent threat

A targeted attack from an individual or other credible organisation with an intention to exfiltrate corporate data. These attacks can use any form of delivery mechanism but are hard to detect and even harder to effectively remediate.



Malicious code

Successful installation of malicious software that infects an operating system or application.
An attack executed via an email message, external device or web-based application

Unauthorised access

An individual gains logical or physical access without permission to a network, system, application, data, or other resource.
This attack could originate from within or from outside the network.

Improper usage

Any incident resulting from violation of an organisation's acceptable usage policies by an authorised user.
This could be accidental or on purpose but should be reviewed to ensure suitable action is taken.

Data Breach

The loss or theft of a computing device or media used by the organisation.
A damage limitation exercise must be undertaken to ensure that relevant bodies are notified if necessary and the data is recovered where possible.

Post-incident Activities

Learning and fixing what went wrong in an incident is key to improving maturity.
Root-cause analysis, detailed forensic analysis, strategic assistance and lessons learned workshops are all services that can help organisations to learn and improve.

Investigation Review

An investigation review is the validation of activity that has already been carried out across any of the incident domains identified above. The investigation review will allow for an independent and objective view of the steps taken and suggest recommendations for improvement.

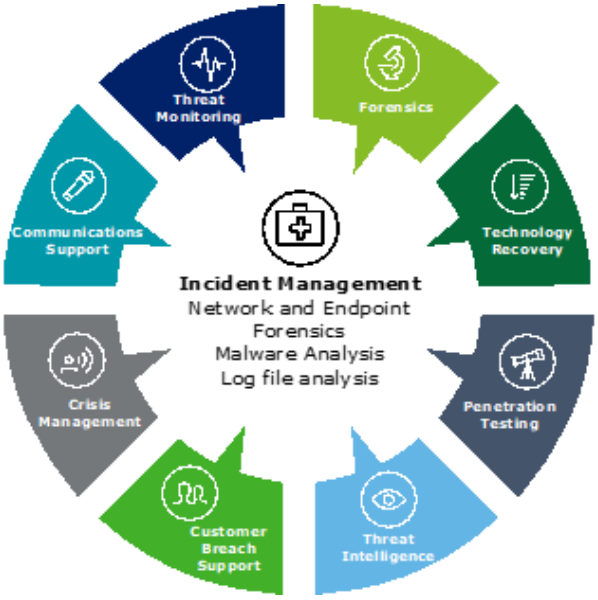
Integrated support to a variety of incident types

While the ability to detect attacks on your information is key, being able to respond effectively is often the real differentiator between an incident being a line item on a management report and potentially being front page news.

We can provide you with rapid and on-demand access to a pool of highly skilled and experienced incident response professionals to help you when your cyber security is breached.

Our specialist responders will provide the immediate technical support needed by your team to help with the initial triage and containment of the incident. The team are specialists in general incident management and the related technical activities to help contain and reduce the impact of the incident, they will also help the leadership team determine the most appropriate course of action quickly.

Our team will then help determine if any of the range of specialist support services (shown to the right) may also be required during the course of an incident. Services such as Crisis Management as well as the communication of messages to key stakeholders and customers may be required. These supporting services are fully integrated into our response capability to enable us to provide a single point of contact for the services when they are urgently required.



Retained Service

Our retained service includes the pre-purchase of days (credit) that establish SLAs which commit us to responding within pre-agreed response times. If these pre-purchased days are not used for incident support within 12 months of signing, they can be allocated for other CIR related activities such as maturity assessments, training and CIR process improvement. On agreement, our retainer agreements can support organisations that have a presence outside of the UK (EMEA and/or Global).

Service Components
• Designated CIR engagement manager
• On-boarding workshop
• Dedicated phone number
• Pre-agreed response times (SLA)
• Pre-purchased incident response days

Levels of support

As part of the CIR retainer service, we offer three different levels of support to help an organisation at the time of an incident. From the initial discussions, we will be able to provide the appropriate recommendation of which level should be adopted and when.

Level	Description	Maximum Response time
1	On-call CIR staff are available to offer technical support and advice to an organisation 24/7. This can be provided in parallel to a responder travelling to site.	2 Hours
2	CIR staff can provide on-site or remote support to conduct incident triage, analysis and containment activities.	24 Hours (In transit)
3	Specialist support teams can provide support for major incidents including forensics, eDiscovery and crisis management.	3 days

Value Delivered

The CIR capability helps you plan for, respond to, and manage/recover from high-consequence cyber incidents in the cloud environment which have the potential to seriously disrupt operations, damage reputation, and destroy shareholder value. Forensic and malware analysis services help to protect your brand and reputation by proactively advising on your exposure to fraud, corruption, and other business risk issues.

4 Contact Details

Please send your requirement to publicsectorbidteam@deloitte.co.uk. Alternatively, if you wish to discuss your requirements in more detail, please send us the following information and we will be happy to contact you:

- Your organisation name
- The name of this service
- Your name and contact details
- A brief description of your business situation
- Your preferred timescales for starting the work.

Deloitte.