Deloitte.

Cyber Incident Response

Deloitte has been named a leader in Cyber Incident Response Services in Forrester's recent report entitled The Forrester Wave™: Cybersecurity Incident Response Services, Q1 2019

An ever changing threat

The cyber landscape is always changing. Advancements like robotics, IoT, and artificial intelligence, although positive, can mean greater cyber threats for organisations. Cyber threats can't always be detected by conventional cyber protection methods, and whilst these conventional methods do offer some protection, organisations must develop their cyber response capability to be able to respond quickly and effectively when incidents occur.

What risks are you taking?

If your organisation works online, you are at risk. Cyber threats can strike at any time and can impact organisations of any size, based anywhere in the world. Although the upfront cost of a contingency service such as Cyber Incident Response may initially be hard to justify, the impacts of a cyber attack can be far more serious. Not only are you at risk of *financial* damage through loss of service or remediation action, you also risk *reputational* damage, especially when considered alongside the potential fines that can be levied as a result of a data breach under GDPR.

What can you do to protect your organisation?

Deloitte believe that preparation and continuous monitoring are the best ways to maintain cyber security. We know that developing and maintaining in-house capability to undertake this task can be too time and resource heavy. That's where Deloitte can help. Our Cyber Incident Response team work with you to develop processes and strategies to enable you to respond effectively during an incident and exercise these processes using realistic cyber simulations. This alongside our Global network of technical responders enables you to be confident that when the worst happens, you have the capability and support to effectively deal with the problem in an efficient manner.

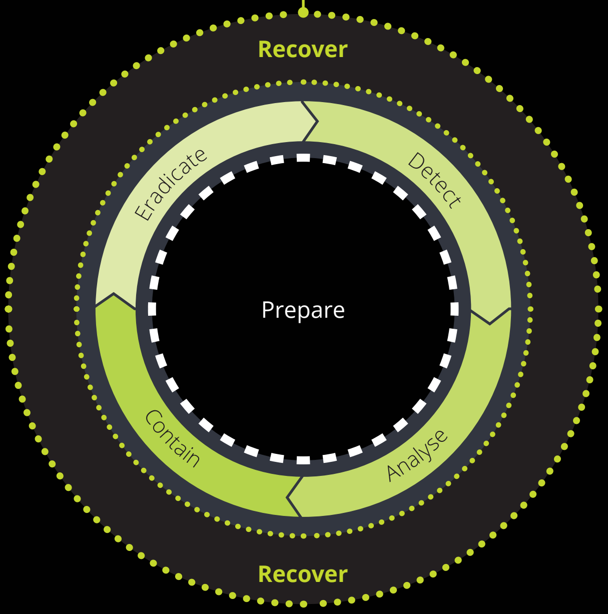
CYBER INTELLIGENCE centre

What's different about Deloitte?

At Deloitte, we understand that no matter how prepared you are, an attack can still happen. Deloitte's Cyber Incident Response specialists are here to help you before, during, and after a cyber incident.

As soon as an attack happens, our responders and specialist teams, including Forensics, Communications Support, Crisis Management, Customer Breach Support and Technology Recovery can rapidly deploy into your environment using an accredited methodology and state of the art technology to identify what has happened, how it occurred, and what's at risk. Once we've established key facts about the attack, our teams work with you to restore your services, protect you from further attack, and get you back to business as usual as quickly as possible.

Our Cyber Incident Response doesn't end there. Our teams continue to work with you after an attack, to assist you in implementing robust security measures and procedures to enhance your posture against any future attacks.



Cyber Incident Response services

- Incident Management
- Malware Analysis
- Network & Endpoint analysis
- Forensic Services
- Threat Intelligence
- Crisis Monitoring
- Crisis Management
- Communications Support
- Technology Recovery
- Customer Breach Support

Cyber Incident Response Proactive services

Our range of proactive Cyber Incident Response Services help your organisation improve its preparedness and ability to respond to major cyber incidents. Our services deliver an orchestrated and proactive approach to managing cyber incidents through bespoke frameworks aligned to our Deloitte methodology.

Our services include:

- Breach Readiness Assessments to baseline and benchmark your current readiness to respond, identifying weakness and providing recommendations for improvement.
- Process and playbook development to embed bespoke processes at the people, process and technology layers.
- Cyber Simulations and war gaming exercises to rehearse and test all layers of your response capability.
- Threat hunting activities allow you to identify and remediate events before they become incidents.
- CSIRT transformation to develop or transform current capability.

Breach Readiness Assessment
Threat Hunting
Cyber Incident Response
Process and Playbook Development
Cyber Simulations / War gaming
CSIRT Transformation

Contact

IE Cyber Incident Response Team
iecir@deloitte.ie