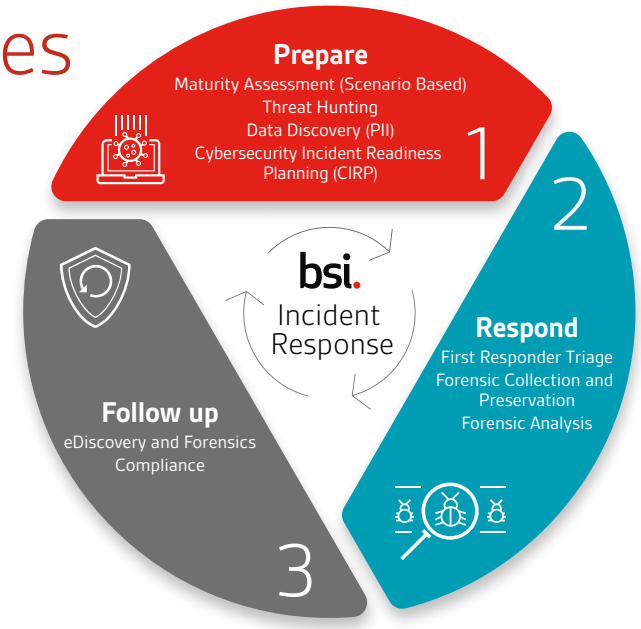
Incident response services



Implementing a robust incident response programme means an organization has the ability to quickly react to a security incident to limit the damage and impact. Planning proactively and reacting quickly are necessary to minimize business impact, as every organization is different, our team can utilize the following services to provide a tailored approach.

Prepare

We plan and implement disaster and incident dry-runs to give you the assurance that your systems work. We leverage the SANS, NIST and ISO/IEC 27001 based methodologies to consistently and effectively implement information security incident response programmes.

When implementing an incident response plan in an organization, our tailored approach ensures that:

- Staff are trained on how to respond to a security incident in a methodical manner using a defined framework
- Roles and responsibilities are allocated and defined
- Incident scenarios are drilled, and the response is effective
- Legal, regulatory and contractual obligations for incident response and notifications are defined and documented

Maturity Assessment

We are a member of CREST. CREST has developed a maturity model to enable assessment of the status of an organization's cybersecurity incident response capability. The tool is powerful yet easy to use and consists of two different spreadsheets, enabling assessments to be made at either a summary or detailed level.

Threat Hunting

Is the activity of performing proactive "hunts" through networks for indications of malicious activity and software. It goes beyond the traditional signature and rule-based detection and instead uses proactive and iterative data searching techniques to identify threats that evade traditional security solutions.

Our threat hunting service has two elements:

- **Host Triage** allows an organization to perform a threat hunting exercise across an entire enterprise quickly without the need of an experienced internal team nor the requirement to have software installed locally on the targeted host
- **Threat Hunter** is designed to provide a longer assessment of an organization. The software is deployed across the targeted hosts, each host logs data such as process creation and new network connections to a central server

Cybersecurity Incident Readiness Planning (CIRP):

The CIRP service aims to review the customer's' existing operating procedures and environment to ensure that in the event of an incident there is sufficient information and processes in place to contain the incident in a timely manner, minimizing the impact, damage, cost and reduce any potential reputational damage.

Data Discovery (PII)

We combine our experience with the latest technologies to set up and run challenging local and multi-jurisdictional eDiscovery projects.

Respond

In addition to developing an Incident Response policy in an organization, we can also provide real-time first responder services to support you in the midst of an attack.

Our methodology for incident response provides a systematic and structured approach to respond to a security incident, broken down into the below stages

First responder triage – Our first responders will be able to determine whether any specialist resources – including third parties will be required.

Forensic collection and preservation – It is critical in the preliminary stages of an incident or event that all potentially relevant evidence is correctly captured and preserved in a forensically sound manner.

Forensic analysis – We've extensive experience conducting forensic analysis activities to uncover the true cause of an incident, its scale, and its impact. BSI maintains numerous ISO 27001 certified laboratories equipped with the most up to date and sophisticated forensic technology. Our consultants are highly qualified with extensive experience and follow strict procedures including those of the CREST CSIR Scheme.

Follow up

We use our eDiscovery experts and technology to fully support organizations in facilitating an efficient review of electronic evidence to meet the scope of a regulatory or court order request. We apply world class project management techniques and leading technology to collect and analyze large volumes of data quickly and accurately.

To find out more

Call UK: **+44 345 222 1711**
Call IE: **+353 1 210 1711**
Visit: **bsigroup.com**

BSI Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:

Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services

Security awareness

Phishing and user awareness training, online solutions, social engineering and simulation testing

Information management and privacy

Information risk management, privacy, data protection, eDiscovery and forensics

Compliance and testing

PCI DSS services, Cyber Lab testing and product and software assessments (CC, CAS-T/CPA)

Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CREST STAR

CHECK IT Health Check Service

Find out more

UK

Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com

IE/International

+353 1 210 1711
cyber.ie@bsigroup.com
bsigroup.com

bsi.