Quality: Engineered. Tested. Assured.

Datasheet

Cyber Incident Response

Prepare, detect, contain, recover

Has your organisation suffered a cyber incident or data breach? For many, the impact of a serious incident can have far reaching and long-lasting consequences on your operations and reputation. Take action as soon as, or even before, an incident occurs.

The key challenge in the incident response process is accurately detecting and assessing possible cyber security incidents - determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.

The Solution

You need expert assistance to guarantee that associated evidence is not destroyed and your organisation can continue to operate with minimum disruption.

Our independent, investigative approach ensures that we find evidence of a data breach, discover the path used by the attacker and ultimately identify the security vulnerabilities that allowed the incident to happen.

Our team also give you the assurance that the attackers have left no artefacts behind on your systems that could allow them to gain access to your organisation or processes later.

The Resillion Advantage

Often, businesses believe they have correctly discovered the source of the breach. However, our independent investigation can bring new evidence to light, meaning that other parts of your existing security structure can be evaluated and, where applicable, improved upon. We use a stepwise approach to the analysis, shown right, to deliver robust results.

After the engagement, Resillion will deliver a report highlighting the investigator's findings. This report will also include an executive summary of the events, the timeline of the attack and remediation recommendations.

Additionally, we use a standard framework to describe the phases of an attack, measure progress in containing the attack and the damage caused. Findings and recommendations will be included at each stage, creating a visual representation.

We understand that cyber is not a 'one size fits all' approach, therefore offering different levels of CIR coverage, aligned to your organisation's needs. This will ensure that you will receive assistance from our team of experts exactly when you need it – preparation is key in managing an incident.

Resillion’s Four-Step Process

Step 1

Prior to forensic investigation, we first provide incident response assistance. This is critical in closing the window of opportunity of a breach.

Step 2

We will then work with your internal IT team and others to ensure the breach is contained, the attack eliminated, and that all evidence is securely collected and stored for future analysis.

Step 3

We also assist in liaising with your senior management team to manage communication internally and externally, including comms to customers, suppliers, the media, law enforcement, and any relevant regulatory bodies.

Step 4

All data that is extracted is securely sent back to our SOC for future analysis.

Why work with Resillion?

Work with our Digital Forensics & Incident Response team and you’ll get:

- End to end incident management by our team of trained experts
- 24/7 incident response hotline
- Guaranteed response times with retainer
- Return to BAU with minimal disruption, fast industry leading threat intelligence
- Dedicated forensic analysts who regularly work with UK law enforcement and deliver expert witness testimony in court
- Forensic analysis carried out by our ISO 17025 accredited lab
- Specialist teams for different aspects of the forensic investigations (such as mobile devices and computers)
- Post breach remediation support
- Flexible and scalable retainer schemes available - unused retainer days can go towards training and awareness

All methodologies and practices are in line with those set by the Forensic Science Regulator. We are an ISO 17025 accredited digital forensics laboratory. Discuss more about our accreditations by getting in touch with us today.