Incident Response

The rate and volume of cyber-attacks grows by the day.

Cyber criminals are continuously reinventing their code and their methods of operation, hoping to stay one step ahead of the cyber security tactics that businesses use to protect their digital infrastructure.

Incident response has earned its right in any board-level discussion on cyber security. It's importance is also tied to the simple fact that businesses must be able to respond to a cyber-attack if they want to avoid suffering its three negative impacts: reputational risk, legal risk and financial risk.

At Integrity360, we understand that every business is unique, which is why we work closely with you to create a customised plan that meets your specific needs. We pride ourselves on our responsiveness, transparency, and commitment to client satisfaction.

Why use Integrity360 for Incident Response?

Integrity360 is one of Europe's leading cyber security specialists operating from office locations in Ireland, UK, Bulgaria, Italy, Sweden, Spain, Lithuania, and Ukraine with Four Security Operation Centres (SOC) located in Dublin, Sofia, Stockholm and Naples.

Integrity360 is a trusted partner for businesses of all sizes when it comes to incident response. Our team of experts is equipped with the knowledge and tools to handle any cyber-attack, from malware and phishing scams to ransomware and more. We offer a range of services to help you respond to and recover from cyber incidents quickly and effectively.

Our cyber incident process involves:

- Preparation: Integrity360 incident response specialists meet with you to discuss the scope of the incident and establish a communication matrix for escalation.

- Detection and Analysis: Assist in the deployment of assessment tools. Conduct log analysis from your systems and environment in an effort to determine the root cause of the incident.

- Containment and Eradication: Collaborate with you in containing the incident, and restoring the business to normal operational standard.

- Post-incident recovery: Our incident response team produces a technical report detailing the incident while a briefing of management, board and any other key personnel takes place.

- Timeliness- Guaranteed availability of an experienced incident response management expert in the event of a compromise or suspected breach.

- Experience- Skilled specialists from a variety of disciplines paired with a communication matrix allow for enhanced visibility and clearer decision-making.

- Productivity- Speed up investigations to contain them within days and reduce response times while still clearing tasks and objectives.

- Our incident response management gives organisations more resources, specialised services and managerial skills to deal with security incidents – not to mention the in-depth perspective on how to remediate them.

- Clients gain access to malware experts who can add the decision-making perspective, proprietary tools and proven methodologies to respond more quickly.

Find out more

integrity360.com