G-Cloud 15 Lot 3 - Cloud Support
Incident Response Services Overview

Prism Infosec supports organisations globally to prepare for, respond to and manage cyber security threats.

Incident Response

Incident Response is a co-ordinated response to an incident to include the triage, analysis, containment and recovery from a cyber incident. Prism Infosec's service will provide a team of experts to guide you through the process of responding to, managing and recovering from a cyber incident, and this can involve technical support as well as legal and PR advice.

Incident Life Cycle

Service Offering

Prism Infosec has provided the following service offerings to our clients:

- Up to 24/7/365 availability via telephone, email or any other pre-agreed communications channel.
- Two sales mechanisms:
  - Annual Retainer
  - Emergency Incident Response Consulting Days
- Three tiers of service for retainer customers.
- Full incident handling, management and forensics support where required.
- The client will invoke an Incident Response service if:
  - they have spotted suspicious activity or indicators of compromise on their network;
  - a serious incident has been reported by employees or a third-party, such as a data breach or business email compromise.

Delivery of Services Retainer

Prism Infosec's Incident Response Service Retainer offers a variety of elements to help organisations prepare, respond and successfully navigate security and privacy incidents in a way that limits the extent and impact of a data incident and assists with recovery.

Incident Response Services can be purchased in half day units when incidents occur or can be pre-purchased as an annually renewable reactive support plan with defined response Service Level Agreements (SLA's) and all our offerings include a number of inclusive response hours to ensure that support is available at the point of an incident occurring without the need to go through a statement of work process.

Approach To An Incident

- Prism Infosec's Incident Response consultants will help the client respond and support recovery from a cyber incident.
- The following services can be consumed by the client for the consultancy support:
- Establish team communication channels;
- Mobilise technical and incident forensics teams to identify cause, assess threats, determine severity level, initiate response and initiate containment and minimisation plan;
- Direct internal and external response and guide teams through response process;
- Ensure regulatory or contractual reporting obligations are managed;
- Liaise with external agencies (ICO, payment partners, media etc) as required;
- Navigate incident and adjust approach as required;
- Lead a post incident lesson learned exercise that includes as a minimum:
  - A root cause analysis;
  - An assessment of network, system and software vulnerabilities;
  - A review of how the response team performed and how their actions limited operational, reputational and financial risk.

Service name	Description
Cyber Incident Exercise	A Cyber Incident Exercise is a structured, scenario-based activity designed to test an organisation's ability to respond effectively to a significant cyber security incident. The exercise typically simulates realistic threats such as ransomware, data breaches, or supply-chain compromise, and is tailored to the organisation's sector, threat landscape, and risk profile. Exercises involve key stakeholders across technical, operational, legal, communications, and executive teams, ensuring decision-making processes are tested under pressure. Scenarios evolve in real time, introducing injects such as media interest, regulatory notifications, or operational disruption to assess coordination and escalation procedures. Outcomes include a clear understanding of roles and responsibilities, validation of incident response plans, identification of capability gaps, and actionable recommendations to improve readiness. Cyber Incident Exercises help organisations build confidence, improve cross-team communication, and demonstrate preparedness to regulators, customers, and insurers.
Cyber Incident Response	Cyber Incident Response provides rapid, expert support to help organisations contain, investigate, and recover from cyber security incidents such as ransomware attacks, data breaches, insider threats, or advanced persistent threats. The service focuses on minimising operational disruption, limiting data loss, and restoring services safely and efficiently. Incident response activities include incident triage, threat containment, forensic investigation, root cause analysis, and eradication of malicious activity. Specialists work alongside internal teams to preserve evidence, assess impact, and guide technical recovery actions while supporting regulatory, legal, and stakeholder obligations. The service also includes post-incident reporting and lessons-learned reviews, helping organisations strengthen controls and prevent recurrence. Cyber Incident Response services may be delivered on a reactive basis or as part of a retainer, providing assurance that expert support is available when it is needed most.
Cyber Maturity Assessment	A Cyber Maturity Assessment evaluates an organisation's current cyber security capabilities against recognised frameworks, best practices, and regulatory expectations. The assessment provides a holistic view of how well people, processes, and technology work together to manage cyber risk. The service typically reviews governance structures, risk management practices, policies, technical controls, incident response capability, and security awareness. Findings are mapped to maturity levels, enabling organisations to clearly understand strengths, weaknesses, and gaps relative to peers and industry standards. Outputs include a prioritised roadmap for improvement, aligned to business objectives and risk appetite. Cyber Maturity Assessments support strategic planning, investment decisions, and assurance reporting, helping organisations demonstrate progress towards a resilient and sustainable security posture.
Ransomware Readiness Assessment	A Ransomware Readiness Assessment is a targeted evaluation of an organisation's ability to prevent, detect, respond to, and recover from ransomware attacks. The assessment focuses on the controls and processes most critical to limiting the impact of ransomware incidents. The service reviews areas such as backup and recovery capabilities, endpoint protection, network segmentation, identity and access management, incident response planning, and staff awareness. It also assesses the organisation's ability to make informed decisions during an attack, including containment, recovery, and communication. Deliverables include a clear assessment of current readiness, identification of high-risk gaps, and practical recommendations to strengthen defences and recovery capabilities. Ransomware Readiness Assessments help organisations reduce downtime, protect critical data, and demonstrate preparedness to boards, insurers, and regulators.

Prepare

Prepare your organisation for cyber security threats.

Prepare your organisation for cyber security threats. Understand your current posture and strengthen your defences. We can help you get ahead of the risks with tailored testing, preparedness services and red teaming.

- Cyber Security Assessments & Penetration Testing
- Cloud Security
- Red Teaming & Simulated Attack
- Regulated Testing Schemes

Respond

Respond effectively to cyber security incidents.

Take control when incidents strike and recover with the confidence to move forward. Specialist support to help you respond to cyber threats and restore operations quickly.

- Remediation Services
- Incident Response
- Digital Forensics

Manage

Manage your ongoing cyber security resilience.

Build long-term resilience with ongoing support and consultancy. From strategic governance to fully managed SOC services and incident response retainers.

- Managed Security Services
- GRC & Security Consulting
- Compliance Services
- vCISO

About Prism Infosec

Prism Infosec is an Information Security company based in Cheltenham and Liverpool and was founded in 2006. The Company has delivered information security consultancy and assessment services to some of the world's largest organisations including private enterpise, public sector, government, defence and healthcare. Uniquely, Prism Infosec's consultants possess both a business and management focus, but also a diverse range of technical skills. Whether delivering advice on cutting edge information security architectural solutions, conducting management controls audits, or in-depth technical penetration testing, our consultants always deliver a quality end-to-end service.

To book an assessment call:
+44 (0) 1242 652100

Send us an enquiry email:
contact@prisminfosec.com