KONTEX

Incident Response

Is your organisation ready to respond to the ever-growing risk of cyber related incidents?

Our dedicated team of Cyber Security Professionals, highly specialised in incident detection and response, including industry leaders in the Digital Forensics space, can provide expert remediation advise as part of a formal incident response service and framework.

Our Services

IR – Readiness

The key to effective incident response risk mitigation is to ensure you have to ability and knowledge to respond to any cyber related incident in a swift, decisive and informed manner. Kontex can assist via our specialised Ransomware Assessment Framework, Adversary Emulation and Cyber Crisis Simulation Training, Incident Response Policy/Plan preparation and on-going Security Awareness Training.

IR – Response

Kontex offer both Proactive/Reactive response services to organisations, which are specifically tailored to match client requirements to an agreed upon service level with the ability to have an Incident Responder engaged in a matter of hours.

IR - Recovery

Our experts can assist with the implementation of industry best practices for incident response and can provide investigative, consultancy, engineering and managed services to respond to an incident, assist with business recovery and provide on-going support and maintenance based around our zero-trust methodology.

Currently Under Attack?

If you are currently experiencing a cyber security incident and wish to speak with a member of our dedicated Incident Response Team, please call: **+353(0)1 22 39 456**

Available 24 hours per day, 7 days per week.

Preparation

Conduct a baseline assessment, establish policies, procedures and tooling for effective Incident Management, train personnel and regularly test ability to respond to cyber related incidents.

Detection & Analysis

Collection of data from IT systems, security tools, publicly available information, along side people inside and outside the organisation, to identify signs that an incident may be imminent and indicators showing that an attack has occurred or is actively in progress.

Containment, Eradication & Recovery

Stop the attack before it overwhelms resources or causes irreputable damage, identify the attack vector, isolate infected endpoints and act to remove all elements of the incident from the environment taking steps to ensure that assets are not attacked again in a similar manner.

Post-Incident Activity

Learn from previous incidents to improve the process, adjust your incident response policies, plans and procedures, in order to feed the new data into the preparation stage of your incident response process.

SERVICES	SERVICE LEVEL AGREEMENTS	BENEFITS
• Agreed Terms & Conditions for Incident Response Services. • Onboarding and Quarterly Technological Business Reviews. • Access to a **24/7** Service Hotline. • Incident Response Preparedness Assessment (One day). • Access to Cyber Threat Intelligence Indicators, Deep Web Reporting and Endpoint Telemetry. • Incident Report and Lessons Learned. • Architectural Review for improved IT posturing. • Update on incident activities on a **Daily basis**. • Direct channel (**War room**) with local IT.	• Maximum of **30 minutes** for contact after Incident Response request is received. • First-responder assigned to case within a maximum of **4 hours**.	• Guaranteed SLA & Rapid Response. • Negotiated terms and conditions to expedite engagement. • Proven retainer service with clients who proactively engage on retainer service prioritised. • Incident Response Preparedness Assessment. • Full client environment awareness. • Benefits of accessing industry leaders in the Information Security field with specialists in the Incident Response and Digital Forensics Space. • Latest up to date Industry knowledge across the threat landscape.

OPTION 1	OPTION 2	OPTION 3
• Core Retainer Service Offering • Block of **40 pre-paid** support hours per annum. • First-responder assigned to case within a maximum of **4 hours**.	• Core Retainer Service Offering • Block of **80 pre-paid** support hours per annum. • First-responder assigned to case within a maximum of **4 hours**.	• Core Retainer Service Offering • Block of **120 pre-paid** support hours per annum. • First-responder assigned to case within a maximum of **2 hours**.

About Kontex: where security meets quality

Formed in Ireland, Kontex has grown to become a leading supplier of cyber technologies and services to the financial services industry and enterprises around the world. Our team can help organisations with a range of cyber governance, strategy, technical controls, risk management and technical implementation and management.

Kontex has a wealth of experience founded on advising, implementing and embedding industry proven security principles into enterprise organisations. Our Security Advisory team have decades of experience across Information Security, Governance, Risk & Compliance and Technical Architecture.

CREST GCFA GCIH GCIA GCTI Microsoft Partner Gold Security Gold Cloud Platform Gold Data Analytics CISSP CISSP ISSAP

CISA CISM CRISC CIPP/E CIPM AWS certified Solutions Architect Professional AWS certified Security Specialty PMP CDPSE CPSA OSCP TOGAF 9 Certified