EKCO

24/7 Cyber Incident Response Service (CIR)

The cybersecurity threat landscape is constantly evolving, with cybercriminals becoming increasingly sophisticated in their tactics, techniques, and procedures. Organisations of all sizes face a myriad of challenges, including advanced persistent threats, ransomware attacks, insider threats, and targeted phishing campaigns. Attackers are leveraging emerging technologies such as artificial intelligence and machine learning to bypass traditional security measures, making threats more complex to deal with while they also grow in number.

In this dynamic environment, the need for 24/7 detection and response becomes crucial to ensure an organisation's cybersecurity resilience. Ekco's Cyber Incident Response (CIR) Service provides a **certified expert Ekco CIRT team on hand 24/7** as part of your team to support your business response to a cyber attack. With flexible annual IR retainer packages covering Basic, Standard, and Premium service levels, Ekco ensures that your organisation is **prepared for any incident**.

Ekco guarantees a rapid response SLA, understanding that a swift reaction is critical to containing and limiting the impact of a cyber incident. The service includes assisted onboarding and IR incident readiness planning, as well as annual tabletop simulations (TTX) tailored to your business needs. Ekco leverages leading industry technologies and the Ekco Threat Intelligence Platform (TIP) to assist in rapid response.

Additionally, 100% of retainer credits can be applied toward any Incident Response consulting service, including threat modelling, ransomware preparedness, compromise assessments, threat hunting, and malware reverse engineering.

By having Ekco's CIRT Service in place, your organisation can effectively mitigate risks and stay one step ahead of cyber adversaries in this increasingly hostile digital landscape.

"Every second counts. Expert response when you need it most."

24/7 Extended Expertise

Cybercriminals often exploit vulnerabilities outside regular business hours. Ekco's 24/7 Incident Response service ensures continuous security coverage, ensuring you have access to certified experts to ensure that your organisation is prepared for an attack and can respond against one. Ekco's CIRT Team act as part of your team to support your business response to a Cyber Attack.

Crisis Management

Designed to respond with your organisation during unexpected events, our expert team provide immediate and effective actions to manage and mitigate the impact of any crisis. We specialise in assessing the severity of the crisis and implementing tailored plans to stabilise the situation. We offer support and clear communication to all stakeholders.

Compliance Requirements

Organisations need to review and test in advance their capability to swiftly detect, contain, and mitigate cyber incidents, thereby minimizing the impact on their operations and reputation. This is crucial for maintaining compliance with NIS2, DORA, ISO (27001), GDPR, HIPAA, NIST and PCI. We provide and test your plans to ensure that a robust Cyber Incident Response plan is in place and works as intended.

»» Powered by

CROWDSTRIKE

CROWDSTRIKE CERTIFIED — CCFA — FALCON ADMINISTRATOR
CROWDSTRIKE CERTIFIED — CCFR — FALCON RESPONDER
CROWDSTRIKE CERTIFIED — CCFH — FALCON HUNTER

CREST | PEN TEST | SOC

Ekco - Beyond Detection

Ekco is a leading provider of Global Security Operations Center (SOC) services, with SOC operations in the UK, Ireland, the Netherlands and Malaysia. Our SOC services leverage the advanced features of our unified threat detection and response bolstered by the application of Threat Intelligence.

Our incident response team are equipped with sophisticated technologies and is staffed by highly experienced cybersecurity professionals who possess the knowledge and skills to proactively detect, analyse, and respond to potential threats. We have flexible annual IR Retainer packages covering Basic, Essential, Standard and Premium Service levels that align to SLA's as we understand that a rapid response is critical to containing, eradicating and limiting the impact of a Cyber Incident.
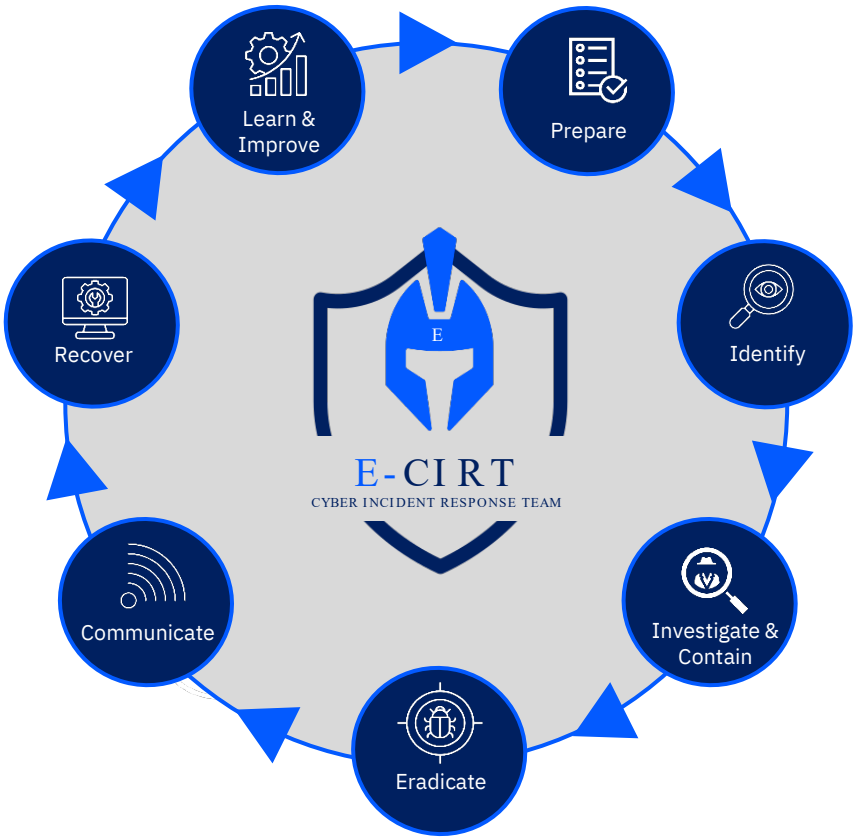
	BASIC	ESSENTIALS	STANDARD	PREMIUM
24/7 Hotline	✓	✓	✓	✓
SLA	4 Hrs	4 Hrs	2 Hrs	1 Hr
Retained	0 Hrs	22.5 Hrs	45 Hrs	75 Hrs
Plan Review	✗	✓	✓	✓
TTX	✗	✗	✓	✓