kyndryl

Kyndryl Cybersecurity Incident Response and Forensics (CSIRF)

Whether you are a new or existing Kyndryl customer, there has never been a better time to review and realign your cyber incident response program. Kyndryl is a trusted global partner with extensive experience helping customers improve and respond to cyber incident readiness. Kyndryl Cybersecurity Incident Response and Forensics Service provides peace of mind, with cybersecurity experts who can help organizations reduce risk before and after a cyber incident.

Introduction

The operational, financial, and reputational impacts of cybersecurity incidents, such as ransomware, continue to grow. A survey of security professionals indicates that organizations have seen an increase in the volume of cyberattacks over recent years. To address this, businesses must adopt a mindset of assuming that a cyber incident could occur and be ready to mitigate its effects. Kyndryl's Cybersecurity Incident Response and Forensics specialists provide comprehensive support throughout the incident lifecycle, utilizing a prepare, respond, and improve model that includes digital forensics.

Kyndryl's CSIRF Cybersecurity Incident Response and Forensics offers proactive measures to safeguard organizations from the effects of cyber incidents. This service enhances an organization's cybersecurity posture and improves its ability to respond to such incidents. Incident response services are activated by events or requests, such as signs of attack activity or threats detected by an intrusion detection system.

Kyndryl's Point of View

Kyndryl Cybersecurity Incident Response and Forensics Service is designed to enable resilient models to mitigate risks and facilitate business continuity. Our cyber resilience best practices, advanced technologies, and expertise help you defend against those risks, protect your business-critical applications and data, and minimize impacts from breaches and disruptions. We offer experience helping thousands of customers anticipate, protect against, and recover from outages.

Highlights

Key Capabilities

- Proactive services to mitigate potential issues.
- Experts to support high-priority incidents.
- Intake process to understand client environment prior to an incident to respond effectively.
- Multi-year contract
- Broad view of threat landscape across multiple business sectors.
- Ability to serve customers in complex, highly regulated industries.

Available Services

- Flexibility The customer can purchase retainer hours based on the requirement, and has the flexibility to use remaining hours for proactive services.

Kyndryl Cybersecurity Incident Response and Forensics Services

The incident response service models offer flexible retainer hours for incident response and forensic scope. It provides a flexible global contract outlining a generic incident response engagement process and may support response during business hours, nights, or weekends.

The customer can purchase retainer hours ranging from 60 to 200, based on their requirements, and has the flexibility to use these hours for any proactive services. If the customer has fewer hours available to cover a required proactive service/ services, then they can purchase additional hours to cover it. The customer can take advantage of the following proactive services: Threat Assessment, Compromise Assessment, Tabletop Exercise, and Threat Intel Program Assessment

Kyndryl offers remote and best-efforts onsite support capabilities, with response times for invocation and triage.

- Uses forensics and investigation to identify indicators of compromise, confirm increased activity, intervene in an active attack, support post-incident, and conduct root cause analysis.
- Conducts threat intelligence, decreases the impact of incidents with a cyber environment sandbox, incident simulation, and incident response role training.
- Multi-country support

Kyndryl's Competitive Differentiators

Kyndryl Cybersecurity Incident Response and Forensics provides the ability to assess existing cyber resilience capabilities and run an on-demand incident response with forensics services remotely on notification of a cyber incident. This helps minimize the occurrence and impact of future cyber incidents. Kyndryl's service can help:

- Proactively strengthen your cyber incident recovery preparedness and plan for response
- Reduce the impact of cyber incidents
- Overcome skills shortage with on-demand availability of cybersecurity experts
- Expansion of CSIRF Support to Europe and Emerging Markets

For more information

To learn more, please contact your Kyndryl Representative or Kyndryl Business Partner, or visit www.kyndryl.com

Why Kyndryl?

At Kyndryl, we understand the pros and cons of various cyber resilience strategy options and can help you navigate and select a strategy that is most capable of meeting your requirements and assumptions.

Experience

Execute faster by leveraging the extensive skills and resources across Kyndryl and our broad partner ecosystem.

Technology

Securely integrate emerging technologies across hybrid environments, benefiting from our decades of experience and patterns of success.

Support

Manage the rapidly evolving operational risks, effectively protect business-critical infrastructure, and mitigate the business impact of security and resiliency incidents.