GROUP-IB



CRITICAL INFRASTRUCTURE

GROUP-IB × K-ELECTRIC

Solidifying Cyber Resilience Through Ransomware Response Simulation

About this case study

Client	K-Electric, a vertically integrated power utility serving Karachi, Pakistan
Sector	Energy and Critical Infrastructure
Services	Incident Response Retainer, Incident Response Readiness Assessment, Incident Response Drill
Scope	IT Environment
Timeline	Retainer since 2023; Readiness Assessment in late 2025; Incident Response Drill in May 2026
Delivery Team	Group-IB Digital Forensics and Incident Response (DFIR), Middle East and Africa

The Incident Response Drill described in this case study was a planned, controlled simulation, not a live cyberattack. It was designed to test K-Electric's response capabilities in a safe environment. No customer services, operational systems, or customer data were impacted during the exercise.

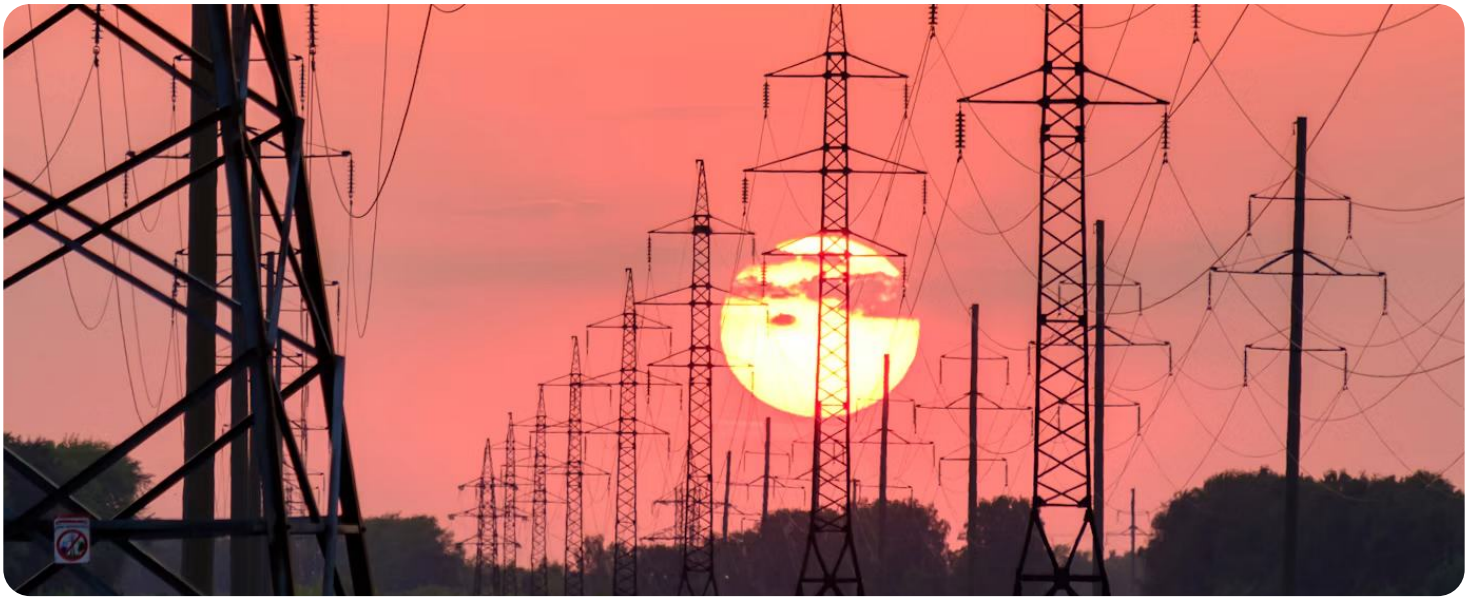
The Challenge

For K-Electric, incident response readiness is more than a cybersecurity concern: it is an operational necessity. K-Electric supplies power to Karachi and its surrounding regions, so its incident response strategy must be capable of defending against and responding to cyber threats effectively.

While the organisation had invested in security controls and built a capable team, the leadership wanted an answer for a more difficult question: could the organization respond effectively under pressure during a serious cyber incident?

That question matters more every year for energy operators. Group-IB's High-Tech Crime Trends 2026 report **describes ransomware as an industrialised supply chain, with initial access brokers and ransomware operators working as coordinated partners, and it flags operational technology in energy and water as an increasingly targeted surface.**

K-Electric wanted to know where it stood before an attacker decided to find out first.



The Partnership: A Retainer Treated as Active, Not Standby

Most incident response retainers bill against reactive hours that sit unused when a year is quiet. K-Electric had exactly that kind of year: a stable subscription period with no incidents to escalate. The value of the retainer was at risk of going unrealised, so the client raised that question with its Subscription Manager.

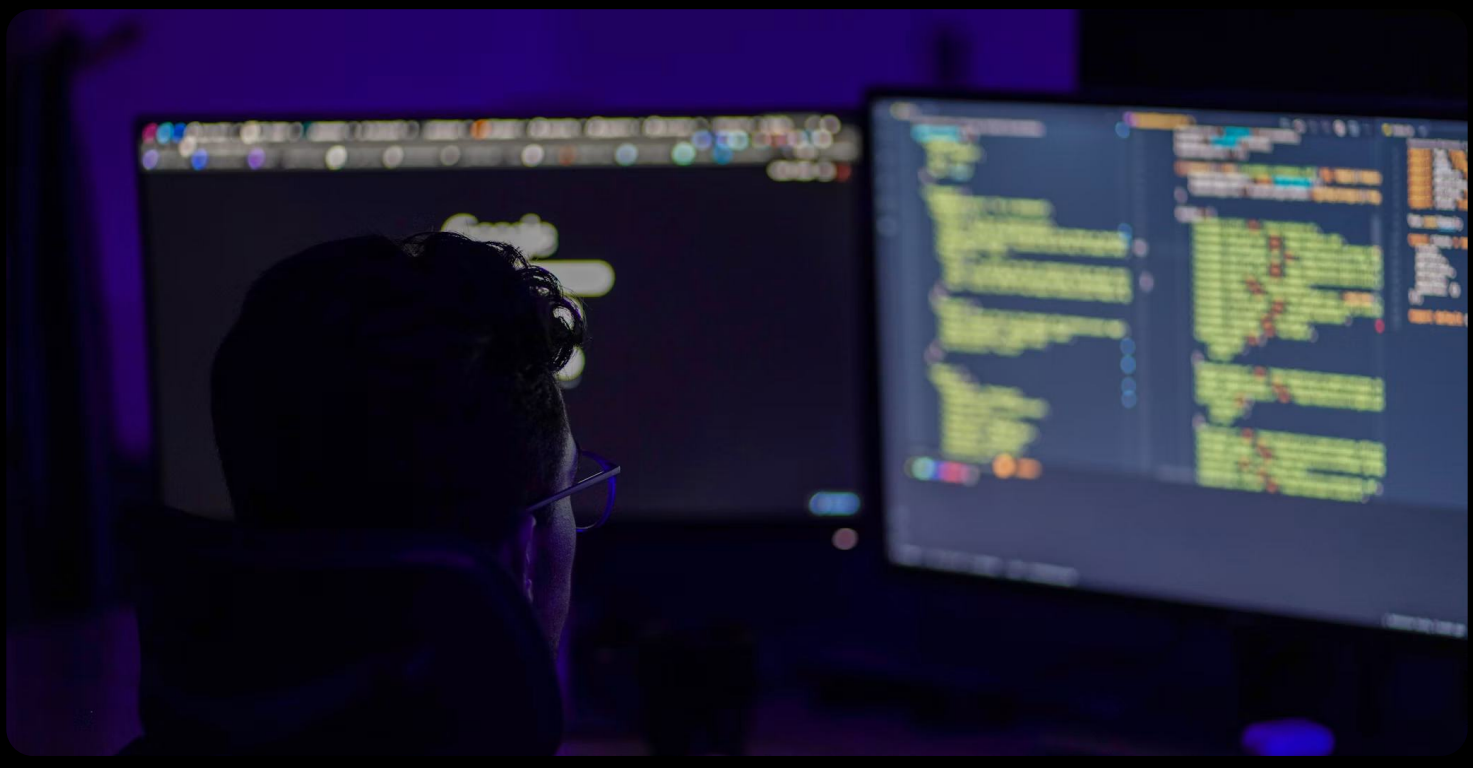
Every Group-IB Incident Response Retainer ships with a named Subscription Manager: an industry-recognised cybersecurity expert with a decade or more in the field. The Subscription Manager guides the client through their cybersecurity programme, helping them use their subscription to strengthen their security posture and stay resilient to emerging threats. **They draw on a portfolio of more than 25 industry-standard services across Cyber Defense Consulting, Red Teaming, Digital Forensics and Incident Response, and Education.**

For K-Electric, that meant starting from the client's own situation, not a standard offer. Working from the question the client had raised, Group-IB built a project around K-Electric's specific need rather than a generic upsell, funded from the subscription capacity the quiet year had left unused. The project had two parts, sequenced so each fed the next: an Incident Response Readiness Assessment to map where the response needed to grow, and an Incident Response Drill to test that response against a realistic ransomware scenario.

25+

services available across the subscription portfolio

> " An incident response retainer earns its value in the quiet years. With K-Electric we started from their own question and built a project around it, using a year without incidents to find the gaps and rehearse the response, so that if an attacker ever did come, the team had already run the play.
>
> **ANATOLY TYKUSHIN**
>
> Director, Unified Cybersecurity Services, Global, Group-IB



The Assessment: Mapping Readiness with the Ready-Steady-Go Framework

The Incident Response Readiness Assessment evaluates an organisation across 27 incident types, scoring against more than 400 criteria in 13 domains using the ready-steady-go framework: infrastructure, process, and team. The methodology draws on 23 years of hands-on digital forensics and incident response.

For K-Electric, the assessment delivered a prioritized view of response readiness and highlighted opportunities to strengthen:

01

Incident Monitoring and forensic visibility

02

Investigation-grade log retention

03

Evidence preservation procedure

04

Incident response playbooks

05

Infrastructure manipulation for incident containment, eradication and recovery

06

Vulnerability and patch management

The assessment also provided

- A readiness maturity score
- Security controls analysis
- Incident response playbooks
- A phased remediation roadmap

Rather than simply identifying issues, the engagement translated findings into actionable recommendations aligned to short-, medium-, and long-term improvement horizons. For a critical infrastructure operator, these findings were not abstract controls. They directly influence how quickly teams can investigate activity, establish root cause, coordinate stakeholders, and recover from an incident.

From Assessment to Validation

The purpose of the readiness assessment was not simply to score preparedness. It was to identify where response capabilities could be strengthened and establish a roadmap for improvement. The next step was validation.

To test those capabilities in practice, K-Electric and Group-IB designed an Incident Response Drill built around a realistic ransomware scenario, allowing the team to exercise detection, investigation, coordination, and response processes in a controlled environment.

The Drill: Testing Response Against a Life-like Ransomware Scenario

K-Electric conducted an Incident Response Drill built around a realistic ransomware attack simulation. The drill was a planned scenario conducted in a controlled environment, not a live incident. It **was designed to test K-Electric's ability to detect, investigate, and coordinate a response to a realistic threat scenario, with no impact on operational systems or services.**

The scenario included:

01. A simulated phishing attack targeting an administrator account
02. Credential theft
03. Lateral network movement
04. Disabling of endpoint protection
05. Simulated ransomware deployment

K-Electric's security team detected and reported suspicious activity on the same day, then engaged Group-IB through the Incident Response Retainer.

Group-IB's Digital Forensics and Incident Response (DFIR) specialists reconstructed the complete attack chain using the MITRE ATT&CK framework and traced the root cause to the original phishing email. Malware analysts reverse-engineered the simulated ransomware sample, recovered the embedded encryption key, and extracted indicators of compromise for broader investigation activities.

For K-Electric, the value was not only the speed of analysis, but the ability to validate how detection, escalation, investigation, malware analysis, and IOC extraction would work together before facing a live ransomware scenario.

The complete analysis of the simulated scenario was delivered within three business days.

The drill was intentionally conducted under controlled conditions rather than during a live incident. Its purpose was to validate readiness, decision-making, and coordination before a real adversary could test them.

K-Electric and Group-IB Strengthened Cyber Resilience Through Ransomware Response Simulation

The assessment identified gaps in readiness, and the drill tested the response built to address them. Together, they turn readiness from an assumption into evidence.

About Group-IB

Group-IB is a global leader in predictive cybersecurity technologies that investigate, prevent, and fight digital crime. Headquartered in Singapore, the company operates Digital Crime Resistance Centers across the Middle East and Africa, Europe, Central Asia, Latin America, and Asia-Pacific.

Group-IB is a trusted partner of international law enforcement organizations including Interpol, Europol, and Afripol, and has been recognized by Gartner, Forrester, KuppingerCole, and Datos Insights.

Its incident response practice is built on experience from more than 1,600 high-tech cybercrime investigations across over 60 countries. Group-IB is also recognized as a Representative Vendor in the 2026 Gartner Market Guide for Cybersecurity Incident Response Retainer Services.

To learn more, visit: www.group-ib.com

GROUP-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,600+
Successful investigations of high-tech crime cases

600+
Employees

60
Countries

$1 bln+
Saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

*According to Cybersecurity Excellence Awards

11
Unique Digital Crime Resistance Centers

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- Forrester®
- datos INSIGHTS
- kuppingercole ANALYSTS
- Gartner®
- IDC
- FROST & SULLIVAN

Fight against cybercrime



GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785