KPMG

KPMG Cyber Forensic and Response

CyFR

A fully integrated, AI-enhanced, rapid-response capability that unites digital forensics, fraud investigation, cyber security, and incident response into a single operational units.

CyFR

This integrated cyber incident response and Forensic service “CyFR” enables faster, more accurate investigations by combining our incident response expertise with forensic analysis, helping us quickly identify root causes, contain threats, and strengthen future resilience for our clients.

The *CyFR* service is designed for security, risk, and compliance leaders responsible for safeguarding digital assets and responding to technology-driven incidents. This includes heads of cybersecurity, IT operations managers, fraud teams, digital forensics specialists, and incident response coordinators who need rapid, reliable, and evidence-based support during and after a breach.

Technology and digital fraud

Enterprises are increasingly looking for integrated solutions that combine digital forensics, cyber investigation, and incident response. This creates strong market demand and significant opportunities for broad business growth.

The growing complexity of technology-related fraud and digital breaches demands rapid, expert assessment and remediation

Integrated Solution

KPMG Cyber Forensic and Response “CyFR”, our integrated solution delivers this through a seamless combination of forensic technology, incident response, and cyber investigation capabilities.

The CyFR difference

CyFR differs from traditional audit-firm forensic services by providing a fully integrated, AI-enhanced, rapid-response capability that unites digital forensics, fraud investigation, cyber security, and incident response into a single operational unit. Unlike the siloed and advisory-driven models used by other audit firms, CyFR delivers deep technical expertise, faster mobilisation, and seamless end-to-end investigations, offering a more agile, technically advanced, and comprehensive solution.

Cyber security – A board level risk

Everyone is affected by cyberattacks in our fast-changing, hyperconnected digital world. With more funds at hand, attackers are employing modern techniques such as machine learning and cloud computing to find novel ways to attack organisations. Keeping attackers at bay is becoming increasingly difficult.

In the KPMG Global CEO outlook survey 2022, cyber breaches were identified as the top concern of CEOs. As part of their digital transformation programs, CEOs are looking for stronger partnerships to maintain cyber resilience. With our incident response retainer program, we help organisations establish the partnerships they need to succeed in their transformation efforts.

Business resilience

It is evident that attackers will maintain an edge over your defences with the recent increase in zero-day vulnerabilities, so it is essential that you have a resilient approach to coping with cyber attacks, especially events that disrupt business services and force a company wide response.

Ransomware attacks

Computer malware can disrupt or shut down a company's operations when it encrypts critical business systems. Ransom demands can range from hundreds of thousands to millions of pounds.

Global economic and political situation

While the global pandemic pushed your capabilities for how you could use technology, cybercriminals and state sponsored attackers have also increased their activities, raising the associated risks in cyberspace. Due to the value you place on technology, cybercriminals and state-sponsored attackers are increasingly targeting systems.

Internal Threat

The breach of trust by employees and contractors can compromise competitive advantage. Every year, courts evaluate evidence of employee misconduct and theft of intellectual property. Companies require support from forensic investigators to address these cases.

'2023 Global CEO Outlook'

KPMG 2022 CEO Outlook - KPMG Global (home.kpmg)

You're in safe hands

With cyber security threats increasing in size, complexity and maturity, effective incident response is a critical business asset to an organisation. The client's experience during any one incident, regardless of how big or small, is not a comfortable situation. As part of KPMG's engagement process, our teams actively solicit feedback during every engagement. Client feedback is reviewed at all levels, including the lead client account team, in an effort to manage client expectations, satisfaction and build long standing relationships.

Global Coverage

Our cybersecurity consulting practice is among the largest in the world, with cyber response members located around the globe. Our 24/7 support service means that you'll have industry experts on hand no matter when or where an incident occurs.

Sector Insights

Our clients come from diverse industries and sectors, and we have gained a deep understanding of what's critical for them within their sectors - especially which data assets and processes create value for them, and which may hold value for threat actors.

Technical Prowess

It's critical to have expertise when it counts. The breadth of our team's expertise in all aspects of cyber security allows us to provide the highest quality of service. When needed, we can provide our own security tools or make the most of yours. Custom-developed tools, scripts, and licensed security products are part of our toolkit.

Our Alliances

Together with our digital partners, we provide services that give us a competitive advantage. KPMG leverages technology from a number of industry leaders.

Regulatory coverage

Our firm's comprehensive understanding of regulatory requirements in multiple jurisdictions allows us to assist our clients in clarifying their concerns regarding subject notification, liability, and business resilience.

KPMG Cyber – Global delivery capability

2,200+ Americas

3,400+ EMEA

3,100+ Asia Pacific

Americas:	US, Canada, Mexico, Brazil, Argentina
EMEA:	UK, Germany, Netherlands, France, Spain, Italy, Switzerland, Finland, the Nordics, Austria, Ireland, Nigeria, South Africa, Kenya, MESA
ASPAC:	China, India, Australia, Singapore, Japan, Malaysia, New Zealand

Global cyber delivery centres: India, Belfast, Sofia, Malta and Mexico

Our regional footprint

Our 3,400 EMEA consultants are steered by a team of 24 EMEA Cyber leaders and Sector Heads known as the EMEA Cyber SteerCo focusing on developing regional specific strategies and activities to address current threats, drive strategy transformation, foster innovation, and engage with the cybersecurity community in the EMEA region.

Virtual Overlay Structure

Our virtual overlays connect our clients to specialist resources across the globe (supported by remote delivery) allowing access to skills regardless of their geographic location.

- Scalable and on-demand resources with consistent pricing across different locations.
- Simplified contractual models.
- Quality assurance and consistency through streamlined onboarding processes and resource training.

Near Shore Location

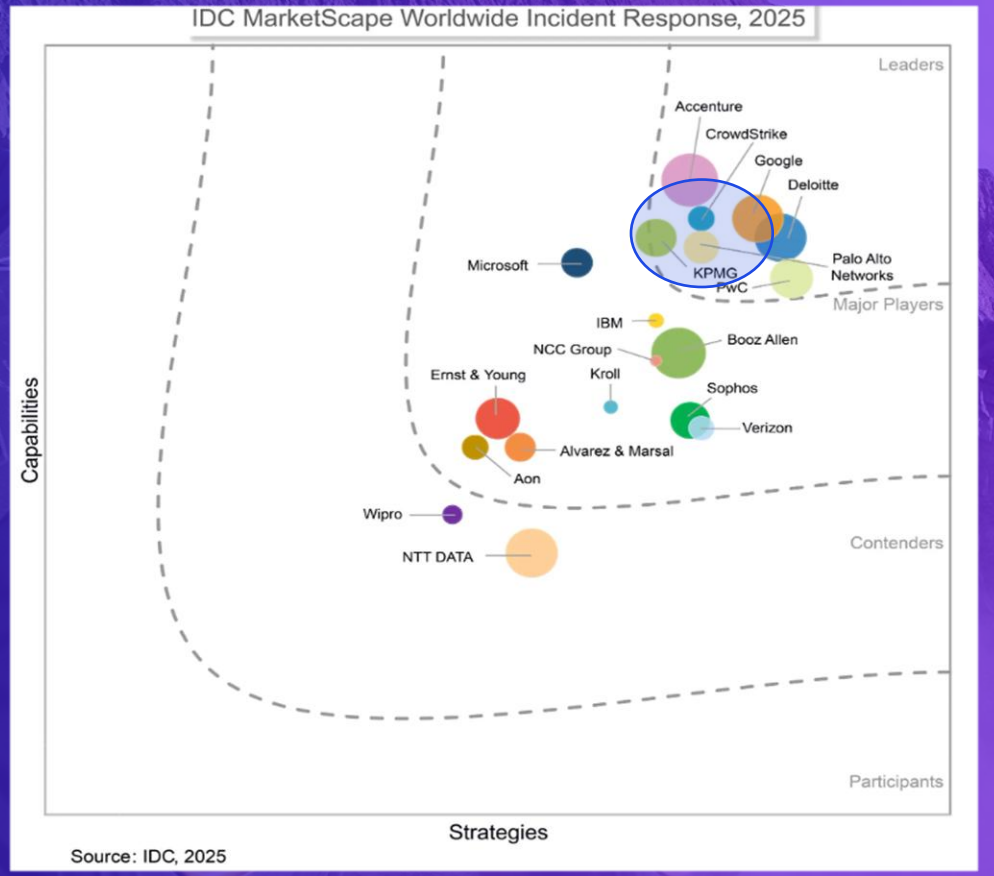
Near- and off-shore delivery is still a major focus area, with additional near-shore delivery centres being stood up in locations such as Belfast and Sofia.

Key investments & focus areas

- Managed Detection & Response
- Cyber Threat Management
- Cyber Breach Recovery
- Risk Quantification
- Digital Identity & Zero Trust
- AI Security & AI for Cyber
- Quantum Security
- IOT/OT security

KPMG's Cyber & Incident response sector Leadership

Organisations trust KPMG to deliver resilience when it matters most. Our position as a Leader in both the Forrester Wave™ and IDC MarketScape for Cybersecurity and Incident Response Services underscores our ability to combine rapid technical response with strategic business continuity. These recognitions validate our global reach, multidisciplinary expertise, and commitment to safeguarding organisations against evolving cyber threats. By partnering with KPMG, you gain a trusted advisor recognised by the world's most influential analysts for excellence in incident response and cyber resilience.



Key Cyber Response Capabilities

INCIDENT RESPONSE / MONITORING & THREAT HUNTING	FORENSIC INVESTIGATION	SECURING & HARDENING EXISTING ENVIRONMENT	SERVICE RECOVERY SUPPORT
We apply a structured response process from detection and communication to containment and remediation. Our teams also carry out focused threat hunting to uncover active or hidden threats.	KPMG conducts forensic analysis on servers, workstations and network infrastructure. We identify indicators of compromise, analyse malware behaviour and deliver reports that support internal and regulatory follow-up.	We secure affected systems by hardening identity infrastructure, network perimeter and endpoints. This includes restoring clean assets and preventing re-entry.	We help restore critical services, manage third-party involvement when needed and align recovery efforts to business priorities.
Key Outcomes			
• **Eradicate "Threat Actors"** • **Prevent Re-infection** • **Facilitate Recovery Plans**	• **Determine Activity** • **Set of IOC's** • **Post Incident Forensic Reports**	• **Increased confidence that operational environment reinfection likelihood is minimised**	• **Operational Services aligned to business priority**

KPMG delivers a complete, end-to-end incident response capability, from threat detection and containment to forensic investigation, service recovery, and hardening, all integrated and aligned to business priorities.

Typical Incident Response Flow

Notification

Client notifies KPMG using the 24/7/365 Hotline or Incident Response Email.

24/7/365 available staff to support

Triage Call

KPMG will arrange a triage call within 1 hour to understand the scope of the incident, advise first steps and assign appropriate resources.

Initial recommendation and data requests

Investigation, Containment and Recovery

Where needed, KPMG will deploy resources on site within 24 to 36 hours and begin containment and response activities.

Containment and response strategies, daily investigation updates

Monitoring and Reporting

KPMG will monitor the network to ensure no further malicious activity has occurred. Upon completion of the forensic investigation, KPMG will produce a report of our findings to support compliance efforts and inform decision making.

Full or summarised investigation report

Crisis Management Support

KPMG will set up and coordinate crisis management committees.

Tailored crisis management support with daily meetings

KPMG Incident Response Approach

KPMG IR capability that would provide 24/7 services on all cyber incidents.

01

Detect and initiate

The trigger for this phase is a technical alert, an indication of fraud or other communications from an outside entity such as law enforcement or an internet service provider to an organisation. KPMG cyber response professionals help execute plans created during the preparation phase and provide answers to pressing questions, such as: Have we been breached? Is the activity continuing? What are the potential damages? Do we need to begin notification and self-reporting?

02

Contain and Investigate

During this phase, KPMG help determine the source, method and impact of the breach event, while attempting to limit ongoing damage. These efforts are typically a balancing act between investigating and eradicating the threat. Responses can range from allowing the malicious actions to continue to facilitate evidence-gathering to immediately suppressing malicious actions to limit damage.

03

Incident Response Recovery

This phase consists of removal efforts that could not occur during the previous phases because of the potential impact on investigative efforts or prioritisation of other activities. The focus of this stage is to return the environment to normal operations.

04

Resolve and Review

A significant work stream during this phase is vulnerability assessment and penetration testing. This work may occur throughout the cyber response process to support tactical efforts and is followed by a more thorough process during this phase to determine the root causes of the malicious activity. This enables KPMG to produce prioritised recommendations for improving the technical and governance environments, which can help prevent similar events from occurring in the future.

05

Report and Pursue

The final phase includes detailed engagement reporting and may involve providing sustained support for legal or civil proceedings involving individuals or groups. All reports are classified as highly privileged and confidential.

Tooling and Integration (1/2)

Skills and tools available to assist you in the event of an incident

01

Digital Evidence Preservation

KPMG utilises industry-leading collection and preservation methods for electronic media. Evidence acquisitions are handled in accordance with KPMG's digital evidence handling protocols, which include chain of custody procedures, authenticity of evidence, encryption, and tracking of evidence.

02

Security Tooling Monitoring

KPMG has experience working with the Microsoft Threat Protection Suite, including Defender for Endpoint, and other major security tools such as SentinelOne, Carbon Black and CrowdStrike to monitor for further compromise. Moreover, KPMG has an alliance with Vectra AI for AI based Network Detection and Response.

03

Network Forensics

KPMG has experience with live monitoring capture and analysis of network traffic for the purposes of information gathering, intrusion detection, or response. KPMG's experience spans from isolated network segments to global enterprise networks.

04

Host and Mobile Forensics

Need to tell a story of what happened? KPMG's team of professionals can help you get the facts quickly. KPMG employs leading investigation and analysis techniques including imaging and dead disk forensics to gather evidence from on-premise and cloud computing systems (AWS, Azure, GCP) and devices in a way suitable for presentation in a court of law.

05

Memory Forensics

Memory content typically holds evidence of user actions, as well as non-legitimate processes and furtive behaviours implemented by malicious code. KPMG's professionals have the critical skills necessary to successfully perform live system memory triage and analysis.

06

Malicious Code Analysis

KPMG has automated and manual experience in statically breaking down the components of malicious code, reverse engineering and binary code analysis, dynamically studying malware behaviour in a sandbox, and reporting capabilities or indicators of compromise.

Tooling and Integration (2/2)

Skills and tools available to assist you in the event of an incident

07

Database and Log Analysis

Whether a single file or terabytes, structured or unstructured, KPMG professionals have leading experience applying investigative and data analytic techniques to contents and metadata of databases and logs.

08

Threat Management

Processes, procedures, roles and responsibilities regarding the identification, detection and treatment of threats to your organisation's network and systems are defined, documented and implemented.

09

Vulnerability Management

Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to vulnerabilities is evaluated by performing vulnerability scans. Found vulnerabilities are documented in a defined way.

10

AI Security

Cranium, developed by KPMG, is an advanced AI Security and Trust platform designed to protect organisations as they adopt artificial intelligence. It provides end-to-end visibility across AI ecosystems, mapping models and pipelines to identify vulnerabilities and mitigate adversarial threats.

Post Incident Services | Remediation

The remediation phase occurs after containment and focuses on removing the root cause of the incident, restoring systems securely, and preventing recurrence.

The process typically spans Eradication → Recovery → Hardening.

Eradication:

Eliminate all traces of the threat and vulnerabilities that were exploited.

Key Actions:

- Remove malicious artifacts: Delete malware, scripts, and persistence mechanisms from endpoints and servers.
- Patch vulnerabilities: Apply security patches and fix misconfigurations that enabled the breach.
- Credential hygiene: Reset passwords for compromised accounts, enforce MFA, and review privileged access.
- Threat hunting: Use EDR/SIEM to confirm no hidden backdoors or lateral movement paths remain.
- Forensic validation: Ensure evidence collection is complete before wiping systems.

Recovery:

Restore business operations safely and validate system integrity.

Key Actions:

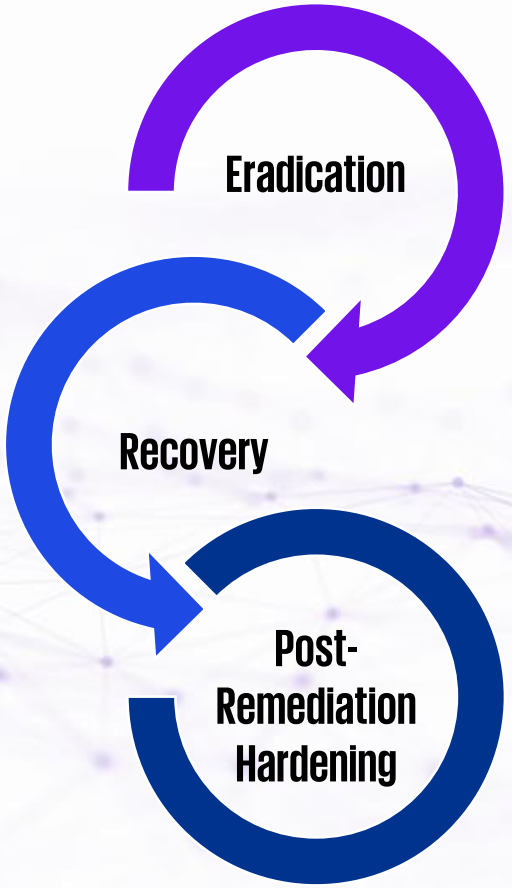
- Restore from clean backups: Verify backups are uncompromised before restoration.
- System hardening: Update antivirus, EDR, IDS/IPS signatures; disable unnecessary services.
- Controlled reintegration: Bring systems online gradually, monitor for anomalies.
- Business continuity alignment: Follow BCP/DRP plans to minimise downtime.
- Testing & validation: Conduct functional and security testing before full production rollout.

Post-Remediation Hardening:

Prevent recurrence and strengthen resilience.

Key Actions:

- Update detection rules: Add new IoCs to SIEM and EDR.
- Improve overall defences: Implement compensating controls, network segmentation, and Zero Trust principles.
- Conduct lessons-learned review: Update IR playbooks and security policies.
- Awareness training: Educate staff on phishing and social engineering tactics.
- Continuous monitoring: Enhance logging and anomaly detection.



Post Incident Services | Post Incident Review

KPMG's Post-Incident Response Review service goes beyond traditional incident response, offering organisations and their board of directors a comprehensive and tailored approach to navigating the complexities of cyberattacks.
We have a global team of more than 1000 Digital forensic and incident responders, with deep multi-industry knowledge, who provide unparalleled support in the aftermath of an incident, helping you understand the technical intricacies, mitigate risks, and ensure legal compliance for your clients.

We provide opinions for:

Incident response effectiveness

As an NCSC-assured, enhanced level cyber incident response provider, KPMG has a proven track record of handling the entire lifecycle of cyber security incidents and can provide an expert opinion to confirm the accuracy of earlier forensic investigations.

Root cause analysis

Our team's extensive experience in handling thousands of cyber incidents provides deep understanding of attacker tactics, enabling us to deliver factual and targeted feedback on control failures.

Post Incident Lessons Learned

Our team's extensive experience in handling thousands of cyber incidents provides deep understanding of attacker tactics, enabling us to deliver factual and targeted feedback on control failures.

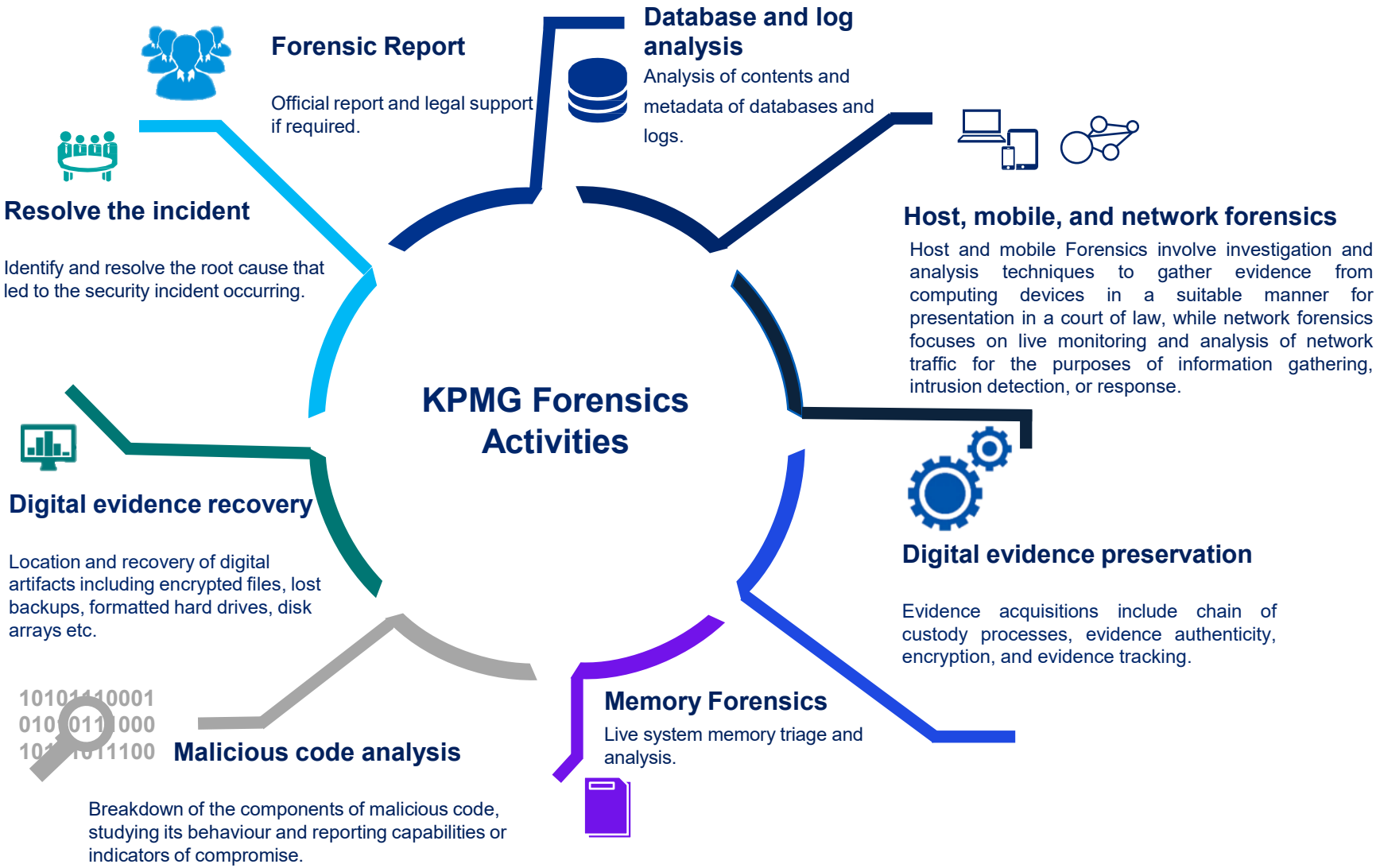
This allows us to support your organisation in navigating the post-incident landscape with confidence and achieve peace of mind.

Forensics

On the right you can see activities that KPMG will perform as a part of our greater forensics methodology.

As part of this methodology we:

- **Collect data and metadata** from sources such as databases, logs, desktops, mobile devices and networks.
- **Recover digital artifacts** such as encrypted files, disk arrays, backups, etc.
- **Analyse data and metadata** using techniques such as malicious code analysis to uncover the threat actor's actions.
- **Preserve evidence** through tracking, chain of custody process, encryption, etc.
- **Provide an official forensic report.**



Post Incident Services | Digital Forensic Services

KPMG can provide digital forensic services in addition to incident response and management support.

As part of this methodology we:

- **Collect data and metadata** from sources such as databases, logs, desktops, mobile devices and networks.
- **Recover digital artifacts** such as encrypted files, disk arrays, backups, etc.
- **Analyse data and metadata** using techniques such as malicious code analysis to uncover the threat actor's actions.
- **Preserve evidence** through tracking, chain of custody process, encryption, etc.
- **Provide an official forensic report.**

Database and log analysis

Analysis of contents and metadata of databases and logs.

Host, mobile, and network forensics

Host and Mobile Forensics involve investigation and analysis techniques to gather evidence from computing devices in a suitable manner for presentation in a court of law, while Network Forensics focuses on live monitoring and analysis of network traffic for the purposes of information gathering, intrusion detection, or response.

Forensic Report

Official Report and legal support if required.

Resolve the incident

Identify and resolve the root cause that led to security incident occurring.

Digital evidence preservation

Evidence acquisitions include chain of custody processes, evidence authenticity, encryption, and evidence tracking.

Digital evidence recovery

Location and recovery of digital artifacts including encrypted files, lost backups, formatted hard drives, disk arrays etc.

Memory Forensics

Live system memory triage and analysis.

Malicious code analysis

Breakdown of the components of malicious code, studying its behaviour and reporting capabilities or indicators of compromise.