KPMG

Incident Response Service

October 2021

Content

01 Incident Response Service Overview

02 Local Presence

04 Comprehensive Incident Response Services

05 IR Expertise

06 IR Toolset & Partners

08 Overview of IR Services

11 Team

Incident Response Service Overview

KPMG's approach to cyber incident response investigations is based on industry standards such as the NIST framework, ISO and other industry best practices. Our Methodology includes the collection and investigation of digital forensic artifacts and a comprehensive review of host-based and network-based events, while managing regulatory obligations. Specifically, KPMG's methodology is base on five primary concepts:

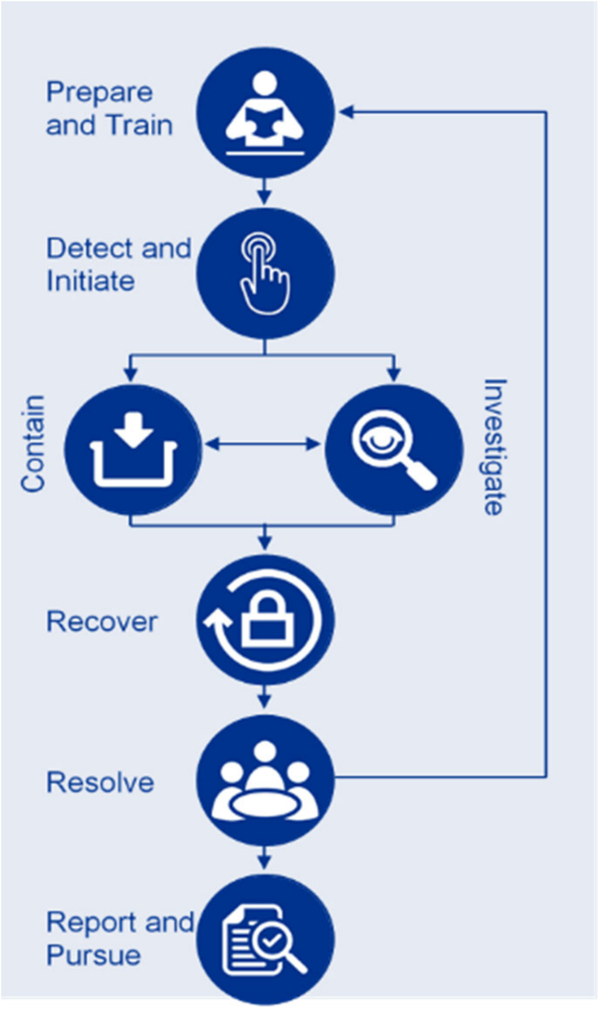
Prepare and Train: KPMG's Cyber Response team will work with you to prepare for an incident. This phase typically includes understanding your technology stack, security architecture and incident response plan and procedures. Once a security event occurs, KPMG's incident responders will assess the event, deploy technology solutions to monitor attacker activity and perform a review of the network environment to identify any indicators of compromise.

Detect and Initiate: KPMG's Cyber Response will initiate the incident response process, collect and review network and host-based artifacts, while initiating digital forensic investigations on affected systems. Our team will leverage threat intelligence to aid the incident investigation.

Contain and Investigate: The goal of KPMG's Cyber Response team is to contain the threat and reduce reputational damage. In doing so, KPMG will collaborate with your business leaders and support personnel to contain the threat. Specifically, KPMG will complete an in-depth analysis on the actions taken by the attacker in an attempt to identify the tactics, techniques and procedures used by the attacker.

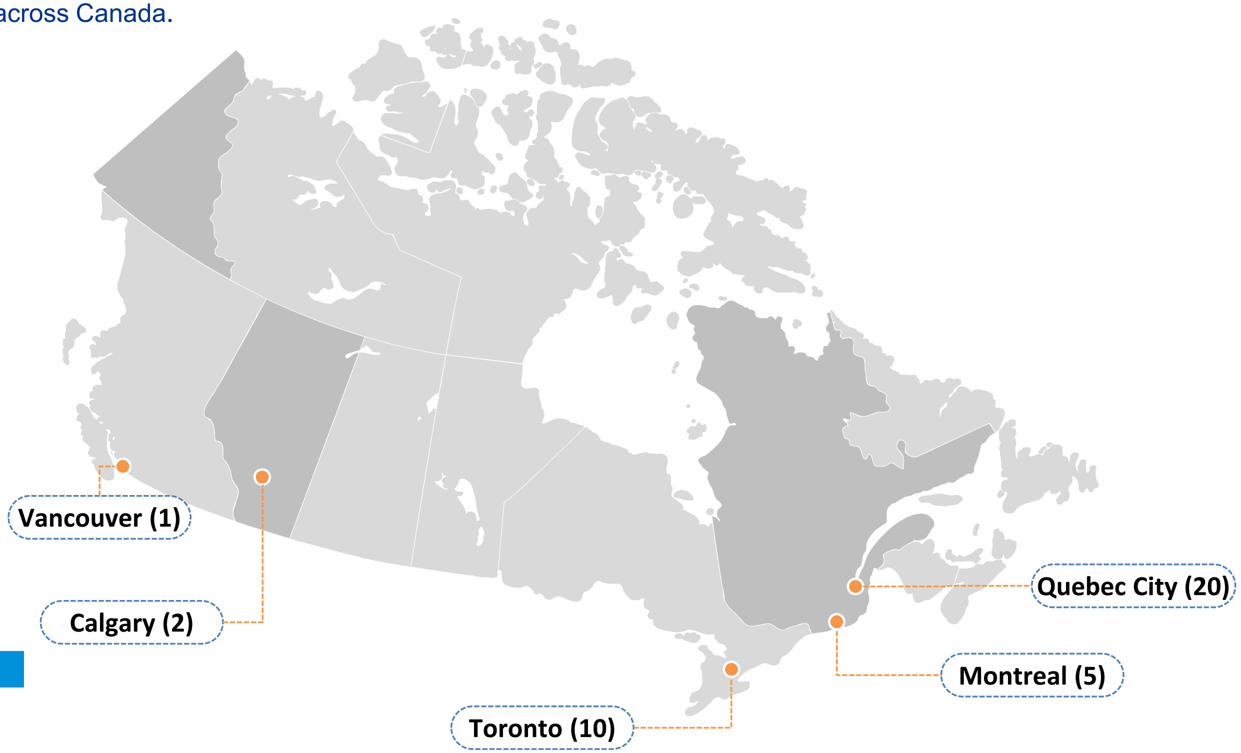
Recover and Resolve: KPMG Cyber Response team will work with you to identify impacted systems, assist in remediation activities and identify necessary steps to prevent recurrence of the incident in the future.

Report and Pursue: Our reporting may include executive and technical reports on the incident investigation, timeline of attacker activity, root cause and lessons learnt. KPMG Cyber Response Team will work with you to provide on-the-job training and share knowledge gained during the investigation.



Local Presence...

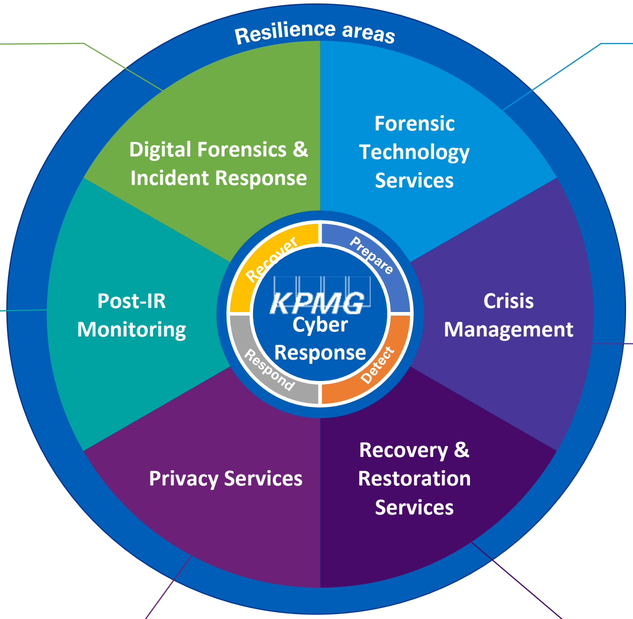
KPMG's Incident Response services are being delivered through the IR Centre or Competencies located in Quebec City, QC and Toronto, ON with supporting resources located in various locations across Canada.



Comprehensive Incident Response Services

Digital Forensic & Incident Response
Scoping, containment, root cause and investigation into cyber breaches
Cyber Incident Response Management
Evidence preservation
Malicious code analysis
Threat hunting and cyber threat intelligence

Forensic Technology Services
Measurement impact by consolidating with other sources (i.e., PII exposure, Financial Losses).
eDiscovery Services to accelerate PII and other data review.
Digital evidence collection and processing
Incident Response/Forensic lab environments (cloud, on-prem)



Post-IR Monitoring
SOAR Automation and Implementation
CTI Dark Web Monitoring
SIEM configuration, use case development, monitoring and alerting
Cyber Security toolset optimization, monitoring and alerting

Crisis management
Integration of organizational stakeholders to monitor and directly respond to major incidents
Incident management processes
Indicator tracking and correlation
Reporting, metrics, KPIs, etc.

Privacy Services
Remediation Roadmap and implementation towards compliance with legislation, standards and best practices
Privacy Training to create a "privacy culture"
Ad-hoc Privacy Advisory Services
Implications of privacy during the breach
Regulatory privacy considerations

Recovery & Restoration Services
System and Application rebuild
Hands on Keyboard/Boots on ground recovery
Domain/Network/Cloud infrastructure rebuild
Post-Breach cyber maturity initiatives

IR Expertise

KPMG is committed to providing quality service by leveraging its proven track record, skillsets and experience in delivering similar cyber security and incident response engagements. In the last three years, KPMG has been involved in over **100** incident response and digital forensic engagements. In Appendix 3 we have provided a sample selection of anonymized client incident response engagement profiles. Due to client confidentiality, we are unable to provide client names in this document. However, KPMG would be happy to meet with you to further discuss the details of each engagement as needed. KPMG IR Team partnered with various industry leading organizations to provide comprehensive incident response services.

Cyber Insurance Providers

cfc

AIG

beazley

RIDGE CANADA

HUB

CHUBB

Legal Firms

BLG

FASKEN

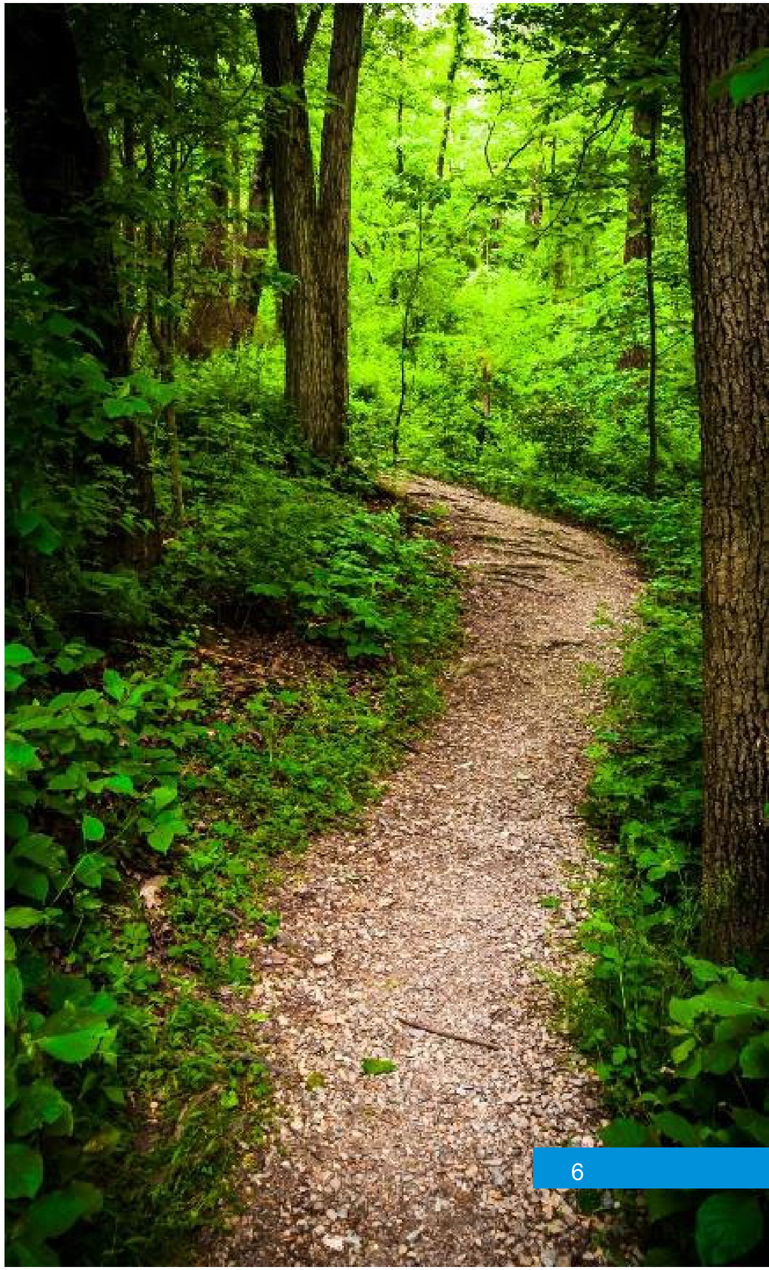
NORTON ROSE FULBRIGHT

OSLER

Blakes

GOWLING WLG

DOLDEN WALLACE FOLICK LLP

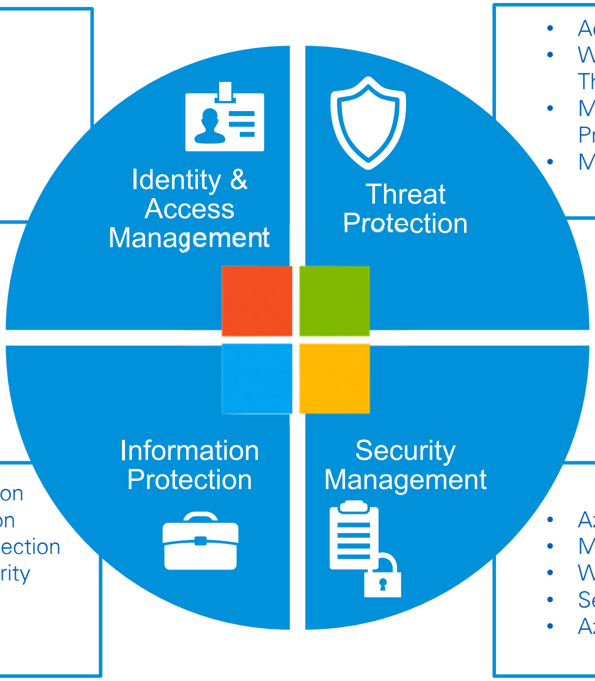


Microsoft Centric Response Approach

KPMG's Incident Response service for Microsoft client's evolves around and utilizes Microsoft's security tool stack and eco system. KPMG's incident responders are trained and have experience with various Microsoft technologies in the cloud or on-premise with Microsoft endpoints.

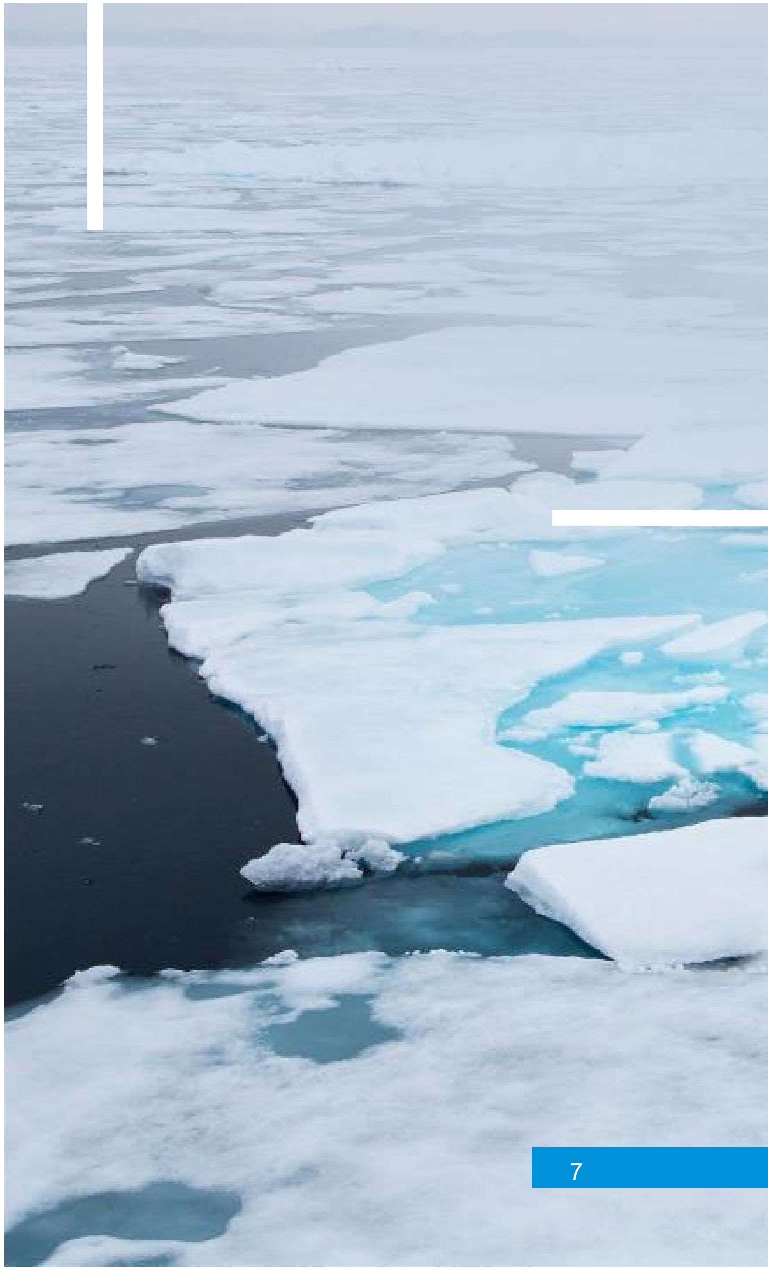
- Azure Active Directory
- Conditional Access
- Windows Credential Guard

- Advanced Threat Analytics
- Windows Defender Advanced Threat Protection
- M365 Advanced Threat Protection
- M365 Threat Intelligence



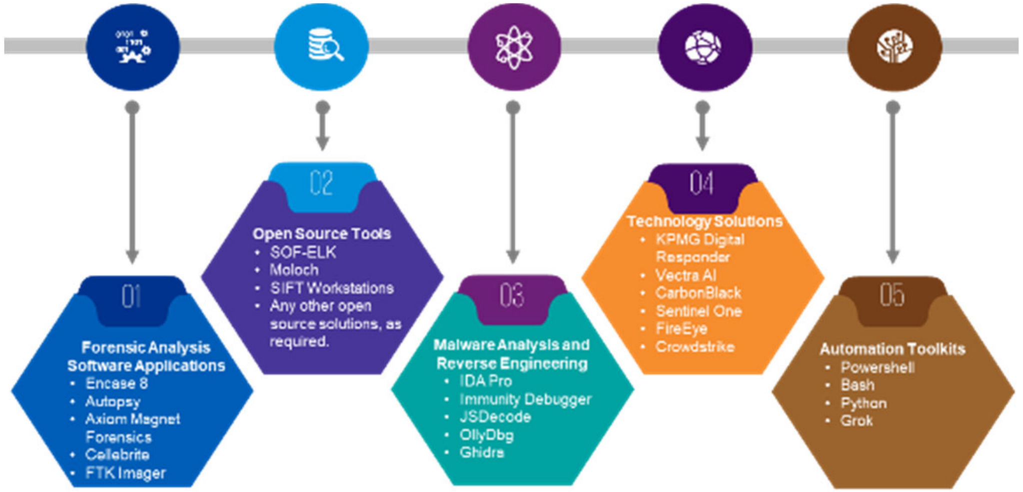
- Azure Information Protection
- M365 Data Loss Prevention
- Windows Information Protection
- Microsoft Cloud App Security
- M365 Advanced Security Management
- Microsoft Intune

- Azure Security Centre
- M365 Security Centre
- Windows Defender
- Security Center
- Azure Sentinel



Augmentative IR Toolset & Partners

KPMG'S Microsoft centric incident response approach is driven by our experience in dealing with complex cyber security incidents. Below are some additional tools that we typically use in an incident response investigation. In addition, KPMG can leverage other enterprise solution(s) for investigating and responding to incidents, depending on the client's environment.



01

Forensic Analysis Software Applications

- Encase 8
- Autopsy
- Axiom Magnet Forensics
- Cellebrite
- FTK Imager

02

Open Source Tools

- SOF-ELK
- Moloch
- SIFT Workstations
- Any other open source solutions, as required.

03

Malware Analysis and Reverse Engineering

- IDA Pro
- Immunity Debugger
- JSDecode
- OllyDbg
- Ghidra

04

Technology Solutions

- KPMG Digital Responder
- Vectra AI
- CarbonBlack
- Sentinel One
- FireEye
- Crowdstrike

05

Automation Toolkits

- Powershell
- Bash
- Python
- Grok

Additional IR Technology Partners

CROWDSTRIKE SentinelOne

FIREEYE VECTRA vmware Carbon Black.

Cyber Threat Intelligence (CTI) Services

KPMG's CTI services provide clients with ongoing monitoring services specific to cyber incidents with respect to activity on the Dark Web (including but not limited to credential leaks and communication regarding the incident) to further enhance response activities and strategic planning.

KPMG's post-incident response CTI services will be provided at additional costs and include:

Credential leak monitoring

Leveraging KPMG's up-to-the-moment knowledge of the cyber threat landscape, we will monitor post sites, underground forums, and social media for evidence of credential leaks to help determine where and how cyber attackers received the information (e.g., logins, passwords, etc.) to execute their attack. More importantly, we look to see if credential information is still out there for the taking.

Deep and dark web monitoring

We scour criminal underground forums and marketplaces for evidence or "chatter" regarding the breach. This includes monitoring suspected online channels for communications with details of the attack or postings of leaked/exfiltrated company data.

VIP account monitoring

Scanning underground forums, social media, and other known cybercriminal "hot spots" for chatter regarding leaked credentials belonging to key organization leaders and privileged users (e.g., C-suite executives, the board of directors, managers, etc.)

Appendix A: Overview of Services

Document Classification: KPMG Confidential

KPMG Cyber Incident Response Services

Cyber Incident Response Services

KPMG has developed a comprehensive approach to digital forensics and cyber incident response that minimizes the impact to ongoing business operations in the event of a cyber incident. Our framework is based on NIST cyber security framework and industry best practice for handling and responding to security incidents and performing digital forensics. This framework helps to ensure that critical business operations are safeguarded and impacts from cyber threat/attacks are minimized

KPMG's investigations include host, network and event based analysis for comprehensive, holistic assessment of the environment. Our response actions are tailored to help you respond and recover from an incident. Our incident responders are able to scope the incident, perform in-depth analysis including digital forensics, leveraging a variety of tools and techniques, perform damage assessment, and effectively identify solutions that will remediate and prevent recurrence of the threat. KPMG also has extensive experience in developing incident related crisis response plans including executive communications, public relations and disclosure requirements.

Sample Cyber Response Investigations	
Financial Fraud	Payment card theft, unauthorized cash transfers and invoice fraud
Financial Crime	Ransomware and extortion, ATM jackpotting.
Data Disclosure	Misconfigurations that expose system information
Data Exfiltration & Insider Threats	Unauthorized activity performed by employees, other insiders or by former employees.
Destructive Attacks	Attacks including DDOS, bot attacks or credential attacks that make systems unavailable for customers.
Cloud	Attacks against cloud infrastructure and/or misconfigurations.

KPMG's approach to cyber incident response is tool agnostic and vendor neutral. Our approach is entirely driven by our experience in dealing with complex incident cases.

On-Demand Cyber Response Services. We are here, when you need us. KPMG's on-demand cyber response model is a tailored service to collectively address many of KPMG's cyber services in one package. Our on-call agreement enables KPMG to engage services with you without a retainer, have guaranteed response times remotely and in-person. In addition

Cyber Training Exercises. KPMG can host, guide or develop a threat or incident scenario that includes involvement from senior leadership and the incident management team. These exercises are designed to simulate real-life complex threat scenarios and to assess the readiness of an organization, both in terms of technical response capabilities and the executive decision making processes.

KPMG Cyber Incident Response Services

KPMG’s Digital Investigation Services

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

Digital Evidence Recovery. Critical files get deleted or lost on a regular basis. KPMG’s professionals have the experience to locate and recover digital artifacts including, but not limited to, encrypted files, lost backups, formatted hard drives, disk arrays, and more.

Network Forensics. KPMG has experience with live monitoring 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.

Malicious Code Analysis. KPMG has automated and manual experience statically breaking down the components of malicious code, studying its behavior, and reporting capabilities or indicators of compromise.

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.

Host and Mobile Forensics. Need to tell the story of what happened? Whether theft of intellectual property, a ‘he said/she said’ human resources matter, inappropriate use of resources, root cause analysis, or a data exfiltration incident, KPMG’s team of professionals can help get to the facts quickly. KPMG employs leading investigation and analysis techniques to gather evidence from computing devices in a way that is suitable for presentation in a court of law.

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

eDiscovery. KPMG’s eDiscovery platforms enable the processing, filtering and hosting of preserved data, including email, electronic documents, chat, social media and audio/video data.

Our data processing team has created customized solutions to automate and deal with the processing of different types of data. The team is also able to configure workflows for review and create bespoke dashboards to allow clients to monitor review progress, manage costs and identify risk.

We deploy Technology Assisted Review technology and innovative products, including machine learning programs, with the aim of ensuring the investigation is fast and exhaustive.

Forensic Data Analytics. KPMG’s Forensic professionals use the latest data analysis tools and techniques to help clients identify fraud indicators. Through tailored, advanced analytics and visualization techniques, we can identify opportunities to help to prevent and detect fraud, waste and misappropriation of resources that can have an immediate impact on the bottom line.

KPMG Cyber Security Services Overview

KPMG brings an uncommon combination of vast technological expertise, deep business and industry knowledge, and creative professionals who are passionate about defending and securing your business.

Summarized below are the various cyber security services that KPMG provides in addition to incident response.

Strategy & Insights

Developing a future-ready Cyber strategy tailored to business risk and Board priorities.

Information Governance & Privacy

Enabling organizations to leverage data securely, while also meeting consumer and regulatory privacy expectations.

Identity & Access Management (Customer/Enterprise)

Creating frictionless security experiences, with intelligent decision making about who can access which information assets, when, and in what context.

Third Party Security

Insights driven third party security monitoring, instilling confidence around data sharing within increasingly integrated digital ecosystems.

Cloud Security

Providing a strategic approach to governing, architecting, and securing solutions for cloud platforms.

Security Operations

Enabling organizations to predict, prevent, detect, and respond to security incidents while increasing efficiency of security tool orchestration.

Threat Management & AI

Assisting clients by leveraging analytics and automation to respond to sophisticated internal and external cyber threats with advanced correlation techniques.

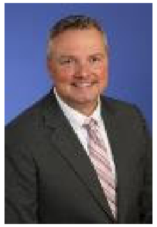
Cyber Response

Assisting organizations detect and respond to cyber breaches, by providing immediate response services.

Appendix B: Engagement Team

IR Leadership Team

The KPMG team brings a multidisciplinary range of skills, deep insight, and hands-on experience performing incident response and digital forensic engagements. Our approach is to work collaboratively with you to ensure we are aligned with your objectives. See the following short biographies of a sample of our Cyber Response team members with relevant experiences:



Alexander Rau, Partner - Engagement Lead
Alexander leads KPMG's national Cyber Response practice and will be responsible for stakeholder communication, engagement oversight and ensuring timely delivery of services. He has extensive experience in incident management and executive incident response communication and coordination. He has been involved in incident response activities with clients in numerous sectors.

Christopher Walker (ACEDS), Engagement Senior Manager – Lead Incident Responder
Chris will be responsible for managing the overall engagements, addressing any issues that may arise with respect to resourcing and resolve any issues. Chris will also be the first point of escalation if there are any challenges during the engagement. Chris has extensive experience leading numerous digital forensic and incident response engagements, involving ransomware, data exfiltration and wire transfer fraud. With his forensic and incident response experience, Chris will assist you in maturing their overall cyber response capabilities.

Ganesh Ramakrishnan (CISSP, GCFA, GNFA), Engagement Manager – Lead Incident Responder
Ganesh will be responsible for managing day-to-day activities, supervising the delivery team, helping lead the delivery of incident response and investigation tasks. Ganesh will be leading the discussions and incident response investigations with your respective teams. Ganesh has extensive experience leading numerous incident response and digital forensic cases, he was previously a cyber security incident response team (CSIRT) manager at one of the largest Canadian Banks, where he led complex incident investigations, assisted law enforcement agencies and matured the bank's incident response capabilities. His specialties include threat intelligence, malware reverse engineering, incident response, digital forensics (Host and network) amongst other security domains.

Contact us

Alexander Rau
KPMG Partner
Cyber Response
alexanderrau@kpmg.ca
(416) 777-3450

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Designed by CREATE. | CRT130713 | November 2020