KPMG

KPMG Cyber Security Breach and Compromise Assessment and Investigation

A KPMG Service for G-Cloud 15

KPMG – About us

Our UK Cyber team

We've worked with countless organisations across multiple sectors, including financial services, life sciences, healthcare, government, telecommunications, energy and natural resources, and legal services. Our clients range in sizes, span across geographies and industries and are subjects to various regulatory requirements and obligations.

330+ professionals

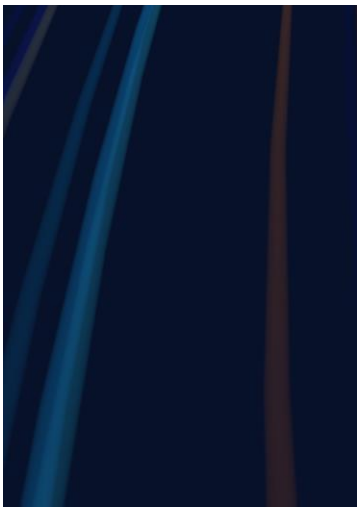
15 office locations

Part of a global team of 6200+ individuals

Our services

UK Cyber operates across 8 different service lines, catering to a wide range of governance and technical needs.

Cyber strategy	Cyber and enterprise resilience
Cyber tech transformation	Cyber defence services
Cyber risk	Privacy compliance
Identity and access management	Cyber incident response



Our Cyber team is complemented by our Connected Technology team.

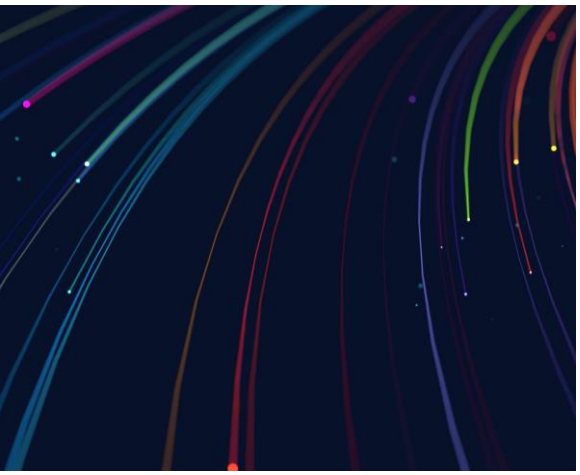
We have access to a 2000-strong team of client-facing technologists combined with alliance partners, with a diverse range of skills and experience. This enables us to bring to our clients the most suitable resources, expertise and insights when needed.

We apply a data and technology driven approach to drive change through our digital transformation services.

KPMG Cyber Security Breach and Compromise Assessment and Investigation

Service Description:

This service provides an independent review of organisation's cloud infrastructure, systems and applications to identify indicators of compromise, backdoors, unauthorised access and opportunities to further improve incident detection and response capabilities. This service assists our clients to identify, detect and respond to the latest and most advanced cyber threats.



What are the benefits of KPMG Cyber Security Breach and Compromise Assessment and Investigation service?

- Obtain an independent view of the risks organisation faces.
- Gain improved cost effective Cyber Response capabilities.
- Manage any Cyber Attacks that organisation may experience.
- Gain confidence in the state of breach protection capabilities.
- Improve insight into emerging issues and solutions to ever-increasing threats.

Our service features

- Scoping and identification of systems or applications of interest.
- Endpoint and / or network sensor deployment to monitor networks, systems and applications.
- Asset inventory, data discovery and classification.
- Assessment of security controls.
- Evaluation of detection and monitoring capabilities.
- Artefact Collection.
- Artefact analysis.
- Reporting.
- Training and awareness.

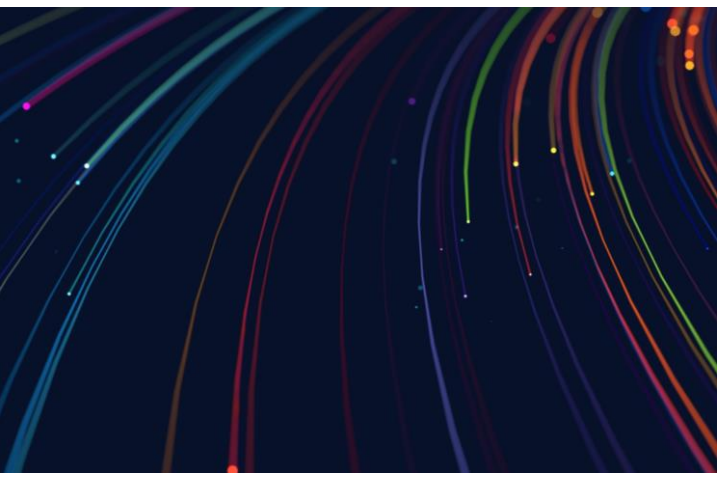
Our Approach

Overview

In an increasingly complex and dynamic threat landscape, now more than ever, organisations need to understand the effectiveness of their cyber defenses in proactively protecting, detecting and responding to threats. Recent cyber breaches at major corporations highlight the increasing sophistication, stealth, and persistence of cyber attacks that organisations are facing today. These breaches can result in fines, increased regulatory oversight, reputational damage and an overall negative business impact.

The loss of intellectual property, customer data, and other sensitive information can cause severe financial and reputational damage. KPMG can help organisations effectively and efficiently recognise, prevent and respond to potential attacks.

KPMG's breach assessment is a tailored, objective technical review of the organisation's network to find instances of compromise, backdoors, unauthorised access, and anomalous activity. This helps identify opportunities to further improve incident detection and response capabilities. We use our years of experience investigating security incidents paired with next generation malware detection to identify potential cyber security threats that may have already impacted the organisation. Ubiquitous, convenient, on demand, measured, pay as you go network access to a shared pool of configurable computing resources



Approach

Scope:

We work with our clients to identify sensitive and mission critical systems and applications that are high risk within their environment. We are able to take a sampling approach or, to gain a broader perspective on the state of the network, can include all applicable IT assets.

KPMG leverages our business knowledge, data discovery techniques, and threat intelligence to help identify systems or applications that should be the focus of the compromise assessment.

Deployment:

We deploy a simple, lightweight cloud based agent that seamlessly integrates into existing infrastructures, needing minimal resources to set up (usually within a few hours). Depending on scoping exercise performed at the onset, we have the ability to also deploy network egress sensors to monitor internet bound traffic. Deployments are temporary and generally last from 10 30 days. Similarly, we can deploy our installation free KPMG Digital Responder (details on next page) on specific high risk systems to conduct in depth forensic analysis.

Monitoring:

Over the course of the compromise/ breach assessment, KPMG cyber security professionals remotely monitor and review potential threats. As threats are identified, we provide recommendations for containment, remediation, and/or further investigation.

Reporting:

KPMG's compromise/ breach assessment provides a high level report card detailing the threats identified in the organisation and the risk classification of those threads. The detailed report provides the organisation greater insight into the distribution of malware or potentially unwanted programs by owner, device and frequency.

Our Approach

KPMG's breach assessment can be tailored to organisation's infrastructure and systems; some of the tools used include, but are not limited to the below:

Cylance:

Cylance PROTECT is a next-generation antivirus product that redefines what antivirus can and should do for organisations by leveraging artificial intelligence to detect and prevent malware from executing on every endpoint in real time. The fundamentals of malware detection have remained the same for more than three decades. In the face of constant innovation from attackers, traditional antivirus vendors continue to focus on aging technologies that use signatures and post attack behavior analysis to protect computers. A new approach is required. Algorithmic science and machine learning are fundamentally shifting the equation, offering new ways to effectively identify, diagnose, categorize and control the execution of every file. Cylance is leading this revolution with predictive and preventive products such as Cylance PROTECT.

Cylance PROTECT offers protection from system and memory based attacks, spear phishing, zero day malware, privilege escalations, scripts and malicious and potentially unwanted programs, all without the highfalse positive rates, operational overhead and management complexity of other solutions.

KPMG's Digital Responder:

KPMG Digital Responder ("KDR"), recently recognized by Frost & Sullivan with the Global New Product Innovation Award, allows us to automate forensic response from the point of collection to reporting – at a predictable fixed price. KDR allows us to conduct deep-dive forensics as part of a compromise assessment on any number of systems.

The process starts by providing you a sophisticated, yet simple installation-free, tool that you can self-collect targeted forensic artifacts from an endpoint (live or disk image). Subsequently, collected data is packaged into an encrypted container and sent back to KPMG securely for processing. Upon receipt, we automatically parse the collected data, and normalize it in order to perform thousands of analysis and correlations procedures. In result, this can be used to identify and report on system vulnerabilities, previous infections, suspicious file execution activity, suspicious user activity, lateral movement, and other indicators of compromise.

KDR example workflow

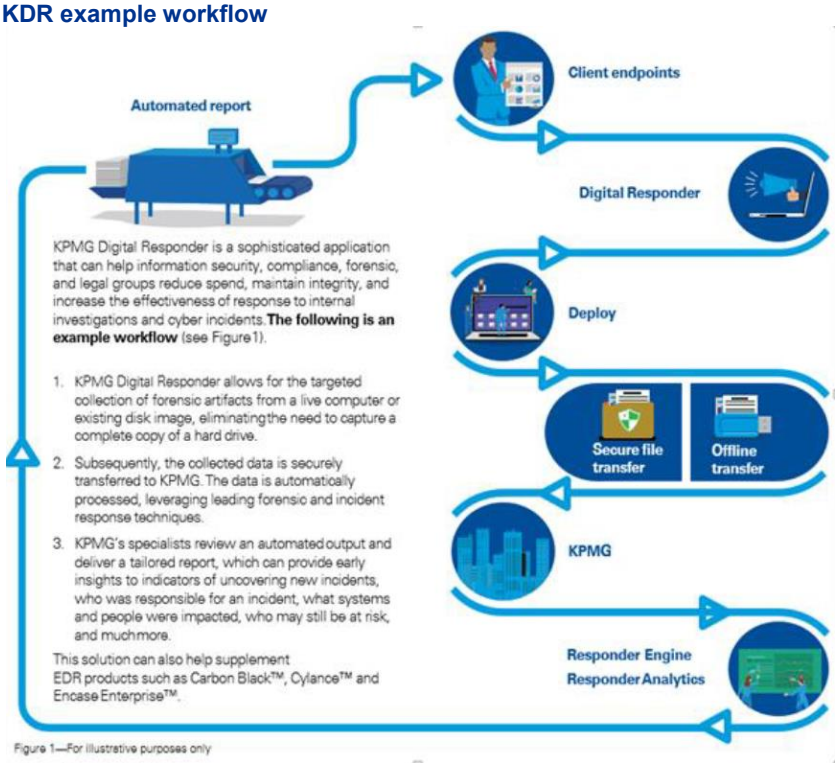
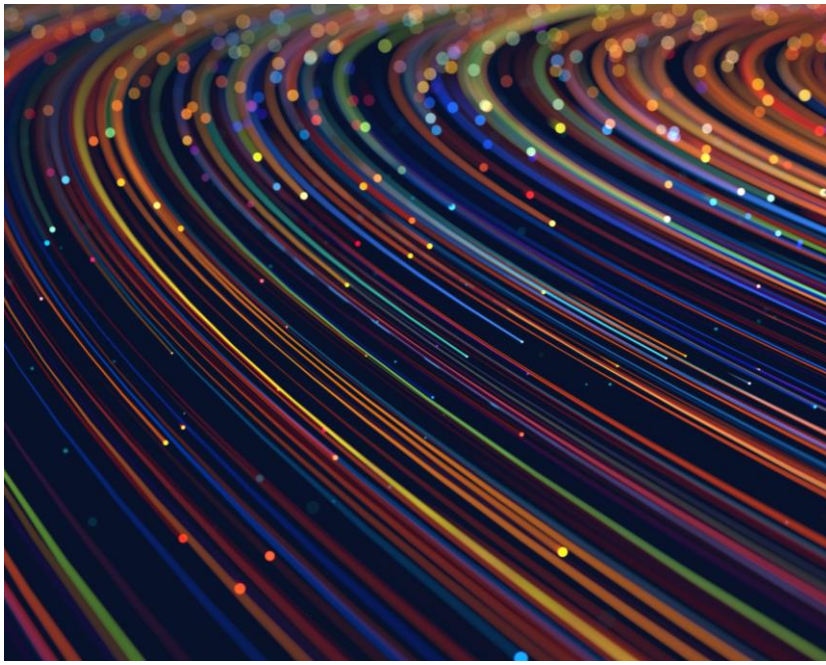


Figure 1—For illustrative purposes only

Why KPMG



Our Experience:

KPMG has a team with deep experience in performing these types of services. An important hallmark of our offering is that we do not seek to merely identify issues, but rather we will provide actionable remediation guidance to address any identified deviations from better practices, as well as identify any underlying root causes of the identified issues.

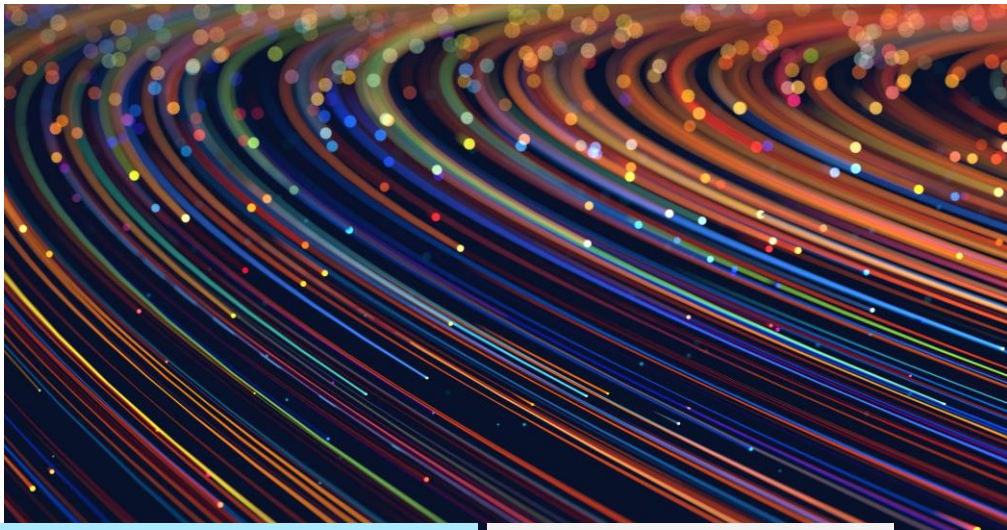
We are proud of our professionals, who provide deep technical expertise combined with a business oriented approach and focus. Although it is difficult to capture all the tools, technologies and expertise we have at our disposal at KPMG, the following list will attempt to highlight some of our capabilities:

- Our team has multiple years of experience, industry insight and the support of the KPMG Global Network of professionals.
- Our world-wide connected KPMG professional network allows collaboration around the globe, where we have the capability to continuously test a network 24 hours a day from various points of the globe.
- Our professionals regularly attend security events, trainings, conferences, develop tools and work closely with vendors to positively impact the security community
- Our professionals have experience working on a variety of cybercrimes, including insider threats, data breaches, hacktivism, and advanced persistent threat-style intrusions by highly motivated adversaries. Our services include a variety of strategy and investigation offerings to support your needs.
- We use modern attack platforms, commercial and open-source tools, such as Kali Linux, Nessus Professional, AcunetixWeb Vulnerability Scanner, IBM Security AppScan, Burp Suite Professional, Metasploit Framework, various scripts included in Kali, Nikto, Webscarab, ArachniFramework, w3af and similar software.
- Our in-house developed security testing tools, scripts, custom testing labs and devices may also be used during our testing.

In addition, Certifications and credentials carried by this team include the following, amongst others:

- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Information Privacy Professional (CIPP)
- Microsoft Certified Systems Engineer (MSCE)
- Various SANS GIAC Certifications (GSNA, GCFA, GWAPT, GCED, GPEN, GCUX, etc.)
- Professionals that have presented at international conferences, both technical and industry-focused, on security-related matters (DefCon, DerbyCon, SchmooCon, HackNet, ISSA, ISACA)
- Strong experience in n-Tier application architectures (including J2EE, .NET, and Legacy systems design and development)
- Code-level review and evaluation experience for protocol, operating system, and application processing (C++, LISP, AWK, SED, Java, VB, PERL, COBOL)
- Database and RDBMS design and evaluation experience (Oracle, MS SQL, Informix, Sybase/JDBC, ODBC, SQL-Connect)

Service Details



Implementation Plan

Timescales are driven by a number of variables including the scale and complexity of each Customer's scope together with quality of data and availability of resources.We would agree the implementation plan, resource requirements and project milestones as part of the process of procuring our services.

Onboarding and offboarding support:

The range of on boarding activity required for clients adopting a KPMG Powered service would be agreed as part of the procurement of the service. As part of the service we build and agree a plan covering all relevant activities, planned times, durations, responsibilities, accountabilities and outputs.Typical elements comprise:

Onboarding:

- Development of the project charter, if needed, and associated project guiding principles
- Assistance to develop / articulate the case for change
- Change management and communications strategy to aid who needs to be communicated with, how and when in relation to the changes the project is planning to implement

Provision of orientation sessions in the Methodology Execution Suite tools to prepare clients teams for the program, including workshop execution

- Engagement with client teams to understand the 'as is', to take into account in change impact assessment during workshops
- Definition of collective roles and responsibilities including that for outputs
- Execution of a Project kick off event and associated materials to formally launch the project and to aid new joiners in orientation

The migration of client data is often a critical path item on the on boarding plan. We work with our clients to assist them to transition data to the new Platform. As part of this we would provide standard templates and knowledge transfer to allow the client and/or their existing service provider to extract and provide data in the correct format.

Pricing overview, including volume discounts or data extraction costs

Consulting Prices are as per the G Cloud 14 rate structure.

Projects can be charged using either Fixed Price and Time and Materials approaches, according to the situation, and can be delivered on site and/or remotely.

Volume discounts would be considered on a case by case basis.

Service constraints like maintenance windows or the level of customisation allowed

Maintenance:

This is not applicable for this service.

Customisation:

This is not applicable for this service.

Offboarding:

Each implementation has a post go live ("Evolve phase") in which KPMG will provide post go live support working with each Clients Business as Usual (BAU) team to fully transition on going service delivery to the Clients' BAU support team according to the agreed plan.

Service Details

Service levels like performance, availability and support hours

This is not relevant as KPMG's Breach Assessment Service does not involve a standard software solution.

Service levels like performance, availability and support hours

Not applicable.

How you'll repay or compensate buyers if you do not meet service levels

Any service credit regime for Cloud software vendors are per the relevant authority's direct agreement with that vendor.

KPMG can discuss specific service credit requirements on a case by case basis.

The ordering and invoicing process

The ordering process for G Cloud services is laid out in the 'G Cloud buyers' guide on the www.gov.uk website.

Invoicing arrangements will be as per the agreed G Cloud order form and will vary from engagement to engagement.

How buyers or suppliers can terminate a contract:

Our terms provide for a range of scenarios where both Buyer and Supplier are able to terminate contracts, to defined notice periods, for:

- convenience,
- failure to remedy a material breach and
- insolvency.

In addition, Supplier has the right to terminate if: (a) circumstances arise or have arisen which KPMG reasonably considers does or may impair its impartiality, objectivity or independence in respect of the provision of the Services; or (b) for legal, regulatory or other justified ethical reasons.

After sales support

KPMG can provide a range of services to assist users of this service post implementation ranging from managed services, staff secondment, impact assessments on the implementation due to cloud software vendor upgrade / major patches and associated regression testing.

Any technical requirements

Each Cloud software vendor provides details directly of their supported web browsers and personal computer and related requirements. These are not onerous and typically do not present an issue for the majority of organisations.

KPMG also uses a range of collaboration tools, as appropriate, to assist in the delivery of the Services. Microsoft Office 365 & Teams are used by all colleagues within the firm, with other tools such as Jira and Confluence being used if required for the project. KPMG is also able to use other collaboration tools if used on client provided laptops.

Project team members will need to be provided with a software VPN and virtual machine or client laptop.

kpmg.com/uk

Document Classification: KPMG Confidential

CREATE. | CRT164925A January 2026