Digital responder

Managing spend for digital forensic and incident response services

May 2020

kpmg.com

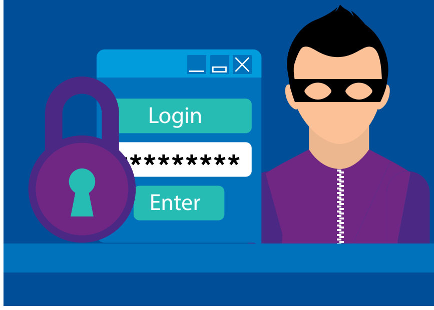
As the digital era continues to evolve, so must an organization's approaches when responding to cyber incidents. Whether it be responding to an insider threat or external adversary, one criterion across organizations that has remained dormant over the years is the traditional model of engaging vendors for Digital Forensic and Incident Response (DFIR) consulting services. When time is of the essence and actionable intelligence is paramount, not only should response techniques and tactics evolve to meet demands, but so should the consulting model.

This white paper will compare the traditional consulting model of delivering DFIR to a new solution, **KPMG Digital Responder**, and highlight cost savings and technical differentiators.

Examining the cost of DFIR

The economic cost associated with traditional DFIR may be unpredictable and inconsistent depending upon the complexity of each investigation. Generally, from a contracting standpoint, a common constant is a fixed hourly rate or hourly rate per level of employee. We can examine this impact across two example engagements:

Example engagements



Scope: Departing employee investigation related to suspected intellectual property theft requiring an examination of a user system.

Common tasks

- Hard disk collection
- Removable storage device analysis
- Link file analysis
- Jump list analysis
- Internet history review
- Registry analysis
- File deletion activity
- Software installed and usage
- Documentation of findings

Estimated total hours 50

Scope: Root cause analysis related to a security operations alert requiring a review of a server.

Common tasks

- Memory collection and analysis
- Hard disk collection
- Antivirus scan
- File execution analysis
- Timeline creation
- Malicious code analysis
- Remediation recommendations
- Documentation of findings

Estimated total hours 60

Ask yourself: Is it acceptable to wait three days or longer to determine whether an employee potentially left the organization stealing intellectual property, and also, to determine the origin of a security alert on a computer?

KPMG LLP (KPMG) estimates the average total "impact" cost to perform digital forensics on a single system can vary, and in many instances, could exceed *$10,000.*

It is important to keep in mind that the cost of an engagement can vary for investigation types. Further, it is important to note these estimated costs do not take into consideration the following:

- Potential need for expenses such as travel to collect data, shipping, and/or assets such as hard drives to store the data
- The time of key organizational stakeholders assisting throughout the investigative process
- Scope creep whether it is from new devices being identified or answering specific questions from other parties.
- Potentially more important is the number of hours (actually, days) that it takes on average until findings or recommendations can be provided back to an organization.

While not all cyber incidents are detrimental to the organization's sustainability, efforts cannot be wasted with the manual processes of data collection, artifact correlation, or subjective interpretation.

The speed with which organizations respond to a cyber incident may directly affect the organization's business and results of the investigation.

Other general noneconomic challenges that are observed include but are not limited to:

- Lack of consistency in reporting
- No standardized processes for triaging systems
- Results or triage process lack depth or specific organizational knowledge
- Capabilities of the investigation are limited based on the capability of a specific digital forensic solution or specific employee(s) knowledge.

Coupling the cost associated with traditional methods of triaging computer systems, the process is not only expensive, but inconsistent and ineffective.

How KPMG Digital Responder has changed the delivery of DFIR

KPMG knows first-hand from helping clients across the globe respond to many cyber incidents a year that there are similarities across investigation and organizational needs.

At the same time, KPMG understands the delivery of DFIR can be challenging, and therefore, the costs can become unpredictable.

This is why KPMG created a new solution drawing on KPMG's Cyber professionals' experience while addressing digital forensic challenges our clients face.

KPMG Digital Responder is a sophisticated software solution that can help information security, compliance, forensic, and legal groups reduce costs, maintain integrity, and increase the effectiveness of response to a cyber-incident.

Technically, KPMG Digital Responder allows for the targeted collection of forensic artifacts from a live computer or existing disk image, eliminating the need to capture a complete copy of a hard drive. Subsequently, the encrypted package is transferred over secure file transfer protocol or offline to KPMG's Forensic Operation Center, a center of excellence containing KPMG's leading Cyber specialists and technologies.

The data is automatically processed by KPMG, leveraging leading forensic data analytic techniques. KPMG's Cyber specialists review the output and deliver a tailored report, which can provide early insights to indicators of uncovering new incidents, who was responsible for an incident, what systems and people were impacted, who may still be at risk, and much more.

Throughout the process, KPMG in the U.S. uses industry-leading data collection and preservation methods. Evidence acquisitions are handled in accordance with digital evidence handling protocols, which include chain-of-custody procedures, authenticity of evidence, encryption, and tracking of physical and logical evidence using our Global Evidence Management Systems (GEMS).

> **In the case of a departing employee investigation, this may be the difference of whether the employee leaves the organization with a removable storage device containing intellectual property – or knowing prior to the exit interview exactly what was connected to the employee's computer, therefore having an expectation of what should be returned.**
>
> *– Ed Goings, Principal, KPMG Cyber Security Services*

Let's take a closer look at the two previous examples using KPMG Digital Responder.

First example: Departing employee

In advance of a human resources exit interview, your organization's information technology team can run KPMG Digital Responder on a departing employee's computer. This data can then be securely transferred to KPMG to analyze automatically for artifacts, including, but not limited to, removable storage device connections, Internet history, nonapproved installed applications, mass deletion of files, and recent user activity.

In totality, this can produce a standardized report that can be used in the exit interview to formulate questions, such as, "Why did you transfer 200 confidential files to a non-company removable storage device asset?" "Why did you search how to securely delete files last week?" or "What do you use third-party file sharing Web services for?"

Less time and effort is focused on the need for technical complication associated with forensics tools and more time can be spent mitigating potential harm to your organization.

Second example: Malware root cause

The traditional response to a suspected malware investigation typically focuses on the computer in a live state.

With the use of the KPMG Digital Responder, the collected data will be securely transferred to KPMG to analyze automatically for artifacts including, but not limited to, infection vector, file execution, malware analysis, lateral movement, and indicators of compromise. In parallel, there is an option to leverage artificial intelligence to statically analyze files on the computer system and identify even "undetectable" malware from traditional antivirus analysis.

In totality, this produces a standardized report that can be used for mitigation, further monitoring, and other remediation activities.

The technical functionalities of KPMG Digital Responder are entirely driven by KPMG clients' and Cyber professionals' needs, making this solution technically distinct in many ways:

- Lightweight stand-alone executable (that does not require install) and can be run from removable storage device
- Targeted collection of artifacts from live system or disk image
- Includes workflows so anyone can use the tool consistently
- Dictionary of common artifacts so no need to remember file names or locations
- Includes collection of files from Alternate Data Stream (ADS) and Volume Shadow Copies (VSC)
- Option to leverage artificial intelligence to statically analyze files on the computer system and identify "undetectable" malware from antivirus
- Extensive audit logging
- Output consists of an encrypted and compressed container
- Extensive reporting including data, data enrichment, artifact normalization, correlation, and intuitive presentation

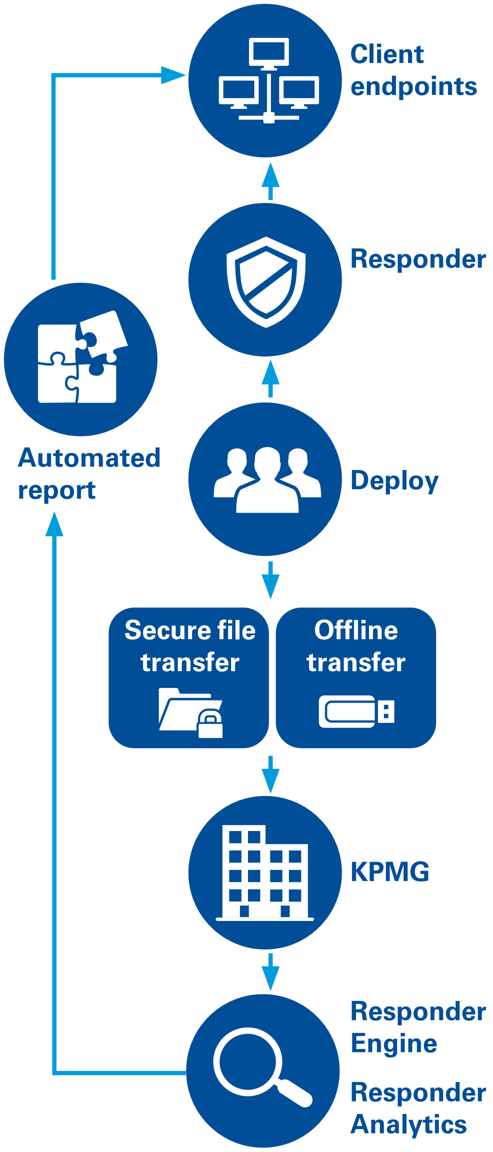


Figure 1 – For illustrative purposes only

Example Reporting

Reporting from Digital Responder is customizable to clients, audiences (technical and non), and data types. Most importantly, all reporting is scrutinized to leading practices. Default reporting options include workbooks for the following areas:

- Departing employee investigations
- Security Operation Center (SOC) alert triage
- Detailed removable storage service analysis
- Volume Shadow copy analysis
- Timeline review
- Advanced analyst detailed report

Below is a sample of types of information Digital Responder automatically report on for a Departing employee investigation.

Removable Storage Device Activity

- Total unique removable storage device connected
- Removable storage device connections
- DVD/CDRom read/write capabilities

File Activity

- Items accessed from potential external sources
- Printed files
- Items accessed from Network Share Drives
- Archive-Encrypted containers created
- User files created
- User files modified
- User files deleted
- Word Wheel Query
- Accessed items
- Recycle bin items
- Overview of File Activity

Internet Activity

- Downloaded files
- Cloud storage Websites visited
- Personal e-mail Websites visited
- Internet history

Program Activity

- Virtual machine files in the system
- Programs uninstalled
- File sharing software installed
- Encryption software installed
- Remote access software installed
- Instant messaging communication software installed
- Program development software installed
- Cloud storage software installed
- File compression software installed
- Anti-Forensics software installed
- Virtualization software installed
- Installed browsers

Email Activity

- Email containers

Mobile Activity

- Mobile backups created

Other Activity

- **Associated networks**
- **User accounts in the system**
- **Volume Shadows in the collection**

Tailoring the needs

KPMG recognizes “one size does not fit all”—each organization’s needs and requirements differ. To help our clients understand and prepare for response needs, KPMG offers an on-boarding process. This service provides the opportunity for KPMG Cyber professionals to meet with the organization’s team members to discuss their environments, standard builds, and expectation of the services provided.

As a result, KPMG can tailor deliverables based on the organization’s needs while integrating into existing processes/workflows.

For example, items that can be taken into consideration when discussing reporting requirements are:

- Custom Microsoft Event Log querying based specific application logs or security settings
- Custom correlation of artifacts
- Collection of proprietary logs or other artifacts unique to the environment
- Disregarding of certain applications to reduce false positives (e.g., OK for “ABC” computers to have “xyz” software installed)
- Building known file hash lists
- Align with business needs such as departing employee questionnaires
- Apply logic and risk rankings to certain result criteria.

The ability to proactively tailor a response in a repeatable and consistent manner is what we believe sets KPMG Digital Responder apart.

The cost and result difference

By innovating and automating common parts of DFIR, KPMG Digital Responder is able to eliminate the unpredictable spend associated with traditional DFIR approaches.

> **The best way to put this solution into perspective is to think about how you might triage malware. Generally, you submit a file to a sandbox, and in return get a report summarizing what is known about the file, such as how it interacts with the operating system, file system changes, network connections established, and other indicators. It’s an effective method for answering generally 90% of your questions. KPMG Digital Responder applies the sandbox methodology to computer system triage and forensics response.**
>
> *– David Nides, Principal, KPMG Cyber Security Services*

As noted earlier, the total impact cost of a single analysis can vary and often exceed $10,000. With KPMG Digital Responder, KPMG is transforming the delivery of DFIR services by charging fixed fees on a per analysis basis.

So instead of a standard rate card for estimated hourly fees, there is one price per single system analysis (report delivered).

Only if additional analysis is required (e.g., you would like more information on something mentioned in the report, etc.) would hourly consulting rates apply.

For large organizations that have many DFIR needs a year, pricing for KPMG Digital Responder is tiered based on usage levels and can also be negotiated for unlimited usage.

The potential benefits

KPMG Digital Responder provides a versatile and critical answer to a growing business need. The demand is accelerating for a cost-efficient solution to provide effective and accurate information in a consistent format. Your organization does not need to spend precious resources on tasks that can be completed in an automated manner with a set of tested and reliable processes.

Your organization can move forward with confidence and do so in an efficient and economical manner with the KPMG Digital Responder solution.

About KPMG's Cyber Response Services

KPMG member firms employ over 2,500 cyber professionals globally who are available to help you with your cyber needs. Many of these professionals are leaders in the cyber community, helping to develop the tools and methodologies used to combat cybercrime on a daily basis.

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.

KPMG is also heavily involved in the information security community. This involvement provides us with early insight into emerging issues, which we share with our clients and our project support teams, as a component of our advisory role. The pragmatic advice and the services we can offer your organization are shaped from the experience we have gained and relationships we have developed serving clients of various size, scope, and complexity.

KPMG Cyber Security Services

Keep it simple—the right balance of information protection and accessibility.

The KPMG Cyber Security Services approach is designed to be simple and effective, and most importantly, aligned with the business needs of our clients. KPMG Cyber assists global organizations in transforming their security, privacy, and continuity controls into business-enabling platforms, while maintaining the confidentiality, integrity, and availability of critical business functions.

Contact us

Edward Goings
Principal, KPMG Cyber Security Services
T: 312-665-2551
E: egoings@kpmg.com

James Arnold
Principal, KPMG Cyber
T: 314-740-2626
E: jarnold@kpmg.com

David Nides
Principal, KPMG Cyber Security Services
T: 312-665-3760
E: dnides@kpmg.com

☎ KPMG's Cyber Emergency Hotline at 855-444-0087
kpmg.com
www.kpmg.com/us/cyber

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia