In an increasingly complex and dynamic threat landscape, are you confident that your organization has not fallen victim to a compromise that you don’t yet know about?

Compromise Assessment

Be in a defensible position.
Be cyber resilient.

Animal species such as the thorny devil have adapted to ward off threats in the most challenging environments. Organizations also need to protect, detect and respond to threats in an ever-changing landscape.

Has your organization maintained the visibility and controls needed to detect a compromise?

In today’s cyber realm, threats from petty criminals, hacktivists, organized crime syndicates and nation states often leverage 0-day vulnerabilities, custom malware and specially crafted attack tools that can infiltrate systems while evading detection.

More than ever, organizations looking to establish a cyber defensible position need to understand the evolving threat landscape, assess and determine response capabilities.

How do you know if your current security controls and processes are sufficient? Is your organization looking in the right areas to find compromised systems and network devices? Do you have the ability to stop threats before they have covertly penetrated your environment?

KPMG’s Compromise Assessment can help you answer these questions and close any resulting gaps.

What is a compromise assessment?

KPMG’s Compromise Assessment is an independent review of your organization’s infrastructure, systems and applications to identify indicators of compromise, back-doors, unauthorized access and opportunities to further improve incident detection and response capabilities.

Harnessing our global experience in cyber threat intelligence and threat detection, investigation and response, we assess your processes, infrastructure, systems and applications to not only identify gaps that can hinder your ability to detect a compromise, we identify historical and active incidents that may have already infiltrated your environment undetected.

KPMG’s Compromise Assessment will help your organization:
- Identify the unique cyber threats and adversaries that threaten it
- Pinpoint Indicators of Compromise (IoC) and Indicators of Attack (IoA) which signify a possible active or past incident
- Detect back doors and misconfigurations within your environment that can be used by attackers to access your systems and data
- Determine where in the Cyber Kill Chain® your organization can detect and eradicate an attack to limit impact

The Cyber Kill Chain methodology, used by cyber adversaries to covertly penetrate environments and steal data:

Reconnaissance
Infiltrate
Exploit
Remote access
Persistence
Lateral access
Aggregate
Exfiltrate
Clean up

Containing and eradicating compromises is key to managing risk during an incident. To do this efficiently, measures must address the way in which an attack progresses. KPMG’s cyber team uses the cyber kill chain analysis for this. Kill chains detail the steps of an attack and, during the containment and eradication stages, KPMG helps ensure that the chain is broken with multiple controls aiming to remove the threat to the organization.

Our approach to compromise assessment

1. Scoping and identifying systems of interest

Identify sensitive and mission-critical systems and applications that are high-risk of attack within your environment. KPMG will leverage threat intelligence to identify systems, and applications within your organization that have been or are future targets by actual cyber criminals.
2. Artifact Collection
KPMG will use industry leading tools and practices to gather artifacts from networks, systems and applications. Artifact collection will follow court-approved forensic practices to ensure artifacts are acquired and preserved in a manner that is acceptable in a court of law in event of future legal proceedings.

3. Artifact Analysis
KPMG will analyze collected data and identify instances of present and historical indicators of compromise which signify an attack. KPMG will leverage threat intelligence for situational awareness and investigate detected instances of interest, working with your organization to qualify malicious and suspicious traffic and activity.

4. Response and Recovery
The sooner you can recognize and remediate an incident, the smaller the impact you will have to manage. In addition to identifying and qualifying incidents, KPMG’s Cyber team can assist you to efficiently and effectively respond to the compromise, severing unauthorized access, eradicating backdoors and recovering affected business operations.

5. Reporting
Proactively identifying existing gaps and limitations that will hinder an actual breach investigation is a critical component of building a cyber defensible position. KPMG’s cyber team will document review findings and recommendations to improve incident readiness and response—for example, inadequate logging of levels of data retention.

By helping your organization better understand your cyber defensible position, KPMG’s Compromise Assessment will help you identify, detect and respond with optimal effectiveness to the latest and most advanced cyber threats.

Why choose KPMG’s cyber team?
Our global cyber team leverages the skills, experience and capabilities of 2,700 accredited practitioners to deliver security and forensic services spanning multiple geographies.

Using the same tools and techniques that professional hackers use for ethical hacking and offensive security, we have tested the layers of security for a large number of clients and organizations across multiple industries.

To complete our team, we include not only advisors to local, regional and federal law enforcement agencies across North America, but cyber thought leaders and authors of multiple security and forensics books that are shaping the industry.

We believe cyber security should be about what you can do – not what you can’t.

Awards winning
KPMG International has been named a Leader in the Forrester Research Inc. report, The Forrester Wave™: Information Security Consulting Services, Q1 2016.

The KPMG cyber team won the Information Security Consultancy award in 2011 and 2012. The team also won the MCA award in 2011 and 2012.

Independent
Our recommendations and technical strategies are based solely on what is fit and appropriate for your business.

KPMG in Canada is not tied to any technology or software vendor.

Collaborative
We facilitate and work with collaborative forums to bring together many of the best minds in the industry to collectively solve shared challenges and emerging threats.

KPMG’s I-4 forum brings together over 50 of the world’s leading organizations to talk about how to effectively deal with Cyber challenges.

Trusted
KPMG member firms have a long list of certifications and permits to work on engagements for many of the world’s leading organizations.

Global, local
KPMG is a global network of member firms with over 174,000 professionals in 155 countries with over 2,700 security practitioners globally. KPMG’s regional practices can service your local needs from information security strategy and change programs, to low level technical assessments, forensic investigations, incident response, training and ISO27001 certification.

KPMG’s Cyber Team works with organizations to prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

Contact us

Kevvie Fowler
Partner, National
Cyber Response Leader
T: 416 777 3742
E: kevviefowler@kpmg.ca

Paul Hanley
Partner, National
Cyber Security Leader
T: 416 777 8501
E: pwhanley@kpmg.ca

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.