Red Team+

Ensuring your business has a strong cyber defensible position is essential for managing today's cyber security risks.

What is your defensible position?

KPMG's cyber team will evaluate and test your organizations' defences using real world attack scenarios to more accurately gauge and address your cyber risk. KPMG's Red Team+ service can help you understand the adversaries and tactics that criminals will use to penetrate your organization's defences.

What is Red Team+?

The KPMG Red Team+ approach is an industry leading, intelligence based capability for hands-on security assessment to help identify and provide greater visibility into cyber operational threats. Red Team+ will help ensure your business processes and systems meet their mission objectives when challenged by Advanced Persistent Threats (APTs).

Red Team+ is intelligence-led.

Red Team+ is a multi-disciplinary team that utilizes "all- source" intelligence capabilities to support an exhaustive testing strategy. Red Team+ leverages this approach in evaluating the specific business model and operations of your organization.

Once profiled, attack vectors are identified and strategies devised to implement sophisticated attacks including: spear phishing, watering hole, malware and social engineering. This is delivered through simulated war-gaming activities, within a controlled testing framework.

Red Team+ is customized for your organization.

Based on the threat intelligence, a threat profile is then developed. This identifies the potential attackers and their most likely and most dangerous forms of potential attack.

This tailor-made approach of combining threat intelligence with specific testing aims to provide a more realistic picture of your organizations' security posture, allowing you to make informed risk decisions on areas requiring remediation.

We will work with you to identify the Red Team+ activities that best meet your requirements; the flexible, tailored approach means that all services could be used, or an appropriate subset.

Red Team+ adapts to the reality of changing threats.

The current cyber threat landscape is highly irregular and can range from state sponsored actors to highly sophisticated criminal organizations. Red Team+ is a fluid and dynamic process that adapts to these asymmetric threats and learns from their tactics, techniques and practices.

Red Team+ goes beyond penetration testing

Range of services	Penetration testing	Red Team+
Vulnerability scanning	✓	✓
Customized scripts & applied intelligence	✓	✓
Social engineering	✗	✓
Cyber scenario testing (tabletop & hands-on)	✗	✓
Breach via third party analysis	✗	✓
Metadata scan, sensitive data web search	✗	✓
Dark web search	✗	✓
Insider threat simulation	✓	✓
VOIP / Telephony attack	✗	✓
Identity & access management exploitation exercise	✗	✓
Targeted attack review (e.g. carbanak)	✗	✓
Physical penetration testing	✗	✓

Typical cyber security questions:

- Will my firm's existing combination of security controls protect against a sophisticated cyber attack in practice?
- Do the existing risk assessments, budgets and IT initiatives appropriately reflect the cyber security risks facing my firm?
- Can my firm be breached due to security issues at foreign subsidiaries?
- What information can office visitors, contractors and employees find on the corporate network?

KPMG's Red Team+ help answer these, and assists by providing an objective security assessment of your IT systems and business processes against specific cyber risks.

The Red Team + difference:

KPMG's Cyber Team has an established framework for threat intelligence and Red Team+ assessments. The KPMG Red Team+ framework offers the following:

- Provides the ability to test the effectiveness of your digital forensics and incident response capability.
- Measures the resilience of your organization's defensive posture.
- Provides access to good quality threat intelligence on your organization that has been vetted by our professionals.
- Provides visibility into your organization's exposure to information harvesting by examining its digital footprint.
- Provides knowledge and early warning signs to help your organization harden its business systems so that they better resist an active attack.
- Provides a practical training opportunity for your cyber defense team.
- Simulates a more realistic threat environment to better tune your Security Information Event Management (SIEM) and Intrusion Detection/Prevention System (IDS / IPS) solutions.
- Identifies the attack vectors that would be employed by criminals to exfiltration private information or corporate secrets from your organization.
- Qualifies the effectiveness of your organization's security awareness program.
- Gives a clear view of your cyber security risks and their impacts, allowing you to prioritize improvement activities.

Cyber Emergency?

Please contact our 24/7 Cyber response hotline

1-844-KPMG-911

1 (844) 576-4911

Red Team + key services:

Cyber attack simulation

This service helps you to understand your incident response capabilities. KPMG's security and information protection team designs, develops and facilitates a Cyber Incident Simulation, allowing you to make any necessary improvements to your response policies and procedures. This exercise is an effective, low-cost initial step for preparing for cyber incidents and provides a platform to build a proactive capability to manage and respond to real threats.

Social engineering

This testing capability can use persuasion and deception to gain access to your information and systems. Such persuasion and deception is typically implemented through human interaction. The basic goals are to typically gain unauthorized access to systems or information that may result in system or network intrusion or disruption. The common attack vectors include malicious emails, phone calls, removable media and physical penetration testing.

Penetration testing

External and internal penetration testing involves a suite of security services including reconnaissance, network testing, host testing, web application testing and scenario testing. The advanced KPMG Penetration testing capabilities complement the Red Team+ activities.

Remediation efforts

KPMG's cyber team provides post-assessment advice and implementation, with a team of professionals covering all areas of cyber security disciplines, including, but not limited to: Security strategy, Transformation and Governance, Secure Architecture and Design, SDLC, Cyber Maturity Assessments and Identity and Access Management (IAM).

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

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

Francis Beaudoin
National Leader,
Technology Risk Consulting
T: 514-840-2247
E: fbeaudoin@kpmg.ca

Jean-Francois Allard
Partner
T: 514 840 2645
E: jeanfrancoisallard@kpmg.ca

Yassir Bellout
Partner
T: 514-840-2546
E: ybellout@kpmg.ca

Erik Berg
Partner
T: 604-691-3245
E: erikberg@kpmg.ca

John Heaton
Partner
T: 416-476-2758
E: johnheaton@kpmg.ca

Adil Palsetia
Partner
T: 416-777-8958
E: apalsetia@kpmg.ca

Jeff Thomas
Partner
T: 403-691-8012
E: jwthomas@kpmg.ca

kpmg.ca/cyber