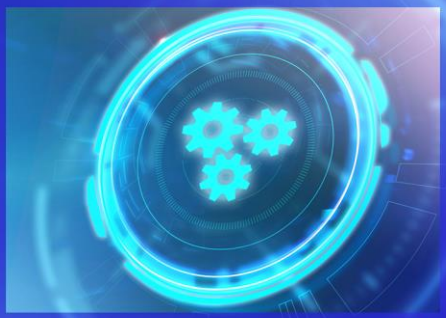
KPMG

KPMG Threat Hunting Solution

Identify previously unknown cyber threats before they create significant problems for your business

July 2023



Unfair odds stacked against defenders

Cyber attacks have become increasingly complex and dynamic, and network defences are having trouble keeping up. While organisations are aware of this and are making use of solutions to mitigate cyber risks, advancements in attacker techniques, delays in patch availability and increasing use of covert malware exploitation technologies, along with the evaporation of corporate boundaries, have reduced the effectiveness of existing security axioms.

As cyber threats continue to evolve, can you answer the critical question being asked by boards and senior management: “Has our organisation been breached?”

With cyber threats looming and ever evolving, there is an urgency for all organisations to adopt an active stance towards cyber defense and to understand that systems can be compromised. Actively hunting for cyber threats before they become an issue is one way to do this.

The KPMG Cyber Threat Hunting Solution is an end-to-end solution that combines the investigative experience of forensic professionals with the multi-dimensional discovery capability of data science to identify otherwise undetected threats and anomalies. It collects, analyses and reports threats and anomalies from both past and current system activities, so that you can take the action necessary to better protect your organisation.

THE KPMG CYBER THREAT HUNTING SOLUTION

1 Minimal footprint in data collection and analysis

KPMG’s unique approach does not require any prior software installation. This ensures operational secrecy and thwarts reconnaissance attempts by attackers. This low-profile, installation-free approach is essential for effective insider threat investigations.

2 Early detection of data breaches

Detecting and stopping a cyber attack in its early stages allows an organisation to eradicate threats before catastrophic damages are incurred. An attacker’s goal is often an organisation’s crown jewel, which is usually protected by multiple layers of defenses. Your goal should be detecting them before they get close to their target.

3 Enhancing critical cyber defenses

Cyber threat hunting also allows you to maximize the returns on existing security defense investments, and brings improvements to current security appliances. KPMG also provides recommendations to improve your security system's performance and reduce operating costs.

4 Advanced visualisation

Our advanced visualisation tools allow analysts to view large amounts of data in a way that is easy to understand and spot patterns or anomalies that may indicate a cyber threat.

Cyber criminals are notoriously difficult to apprehend as they often operate out of regions where cyber regulations are weak or non-existent. The ability to leverage on anonymisation technology to cover their tracks makes these cyber criminals even bolder.

THE KPMG CYBER THREAT HUNTING SOLUTION: Five steps to taking down cyber threats in your system

Scope and identify

- Identify sensitive and critical networks and systems, and prepare cyber threat hypotheses such as impact due to recent vulnerability, input from penetration test report, prolonged exposed services, threat intelligence driven feedback.

Collect and gather

- Gather artefacts from networks, systems and applications using KPMG's agentless approach or using existing EDR/ XDR/ SIEM

Analyse collected artefacts

- Identify possible instances of present and historical indicators of compromise
- Detect misconfigurations of networks, systems and/or applications
- Detect procedural gaps relating to existing technologies and/or processes which can hinder ability to detect and respond to cyber incidents

Respond and recover

- Behaviour based cyber threat identification
- Identification and analysis of previously unseen threats, including full kill chain (infection vector) analysis where possible
- Identification of anomalies, such as suspicious patterns of process execution.
- Track and trace evidence of lateral movement and suspicious user behaviour

Report

- Document identified cyber threats, including internal threats
- Provide recommendations to improve current cyber security posture such as active defense, threat detection, incident readiness and response capabilities

Shifting the odds in your favour

By applying the KPMG Cyber Threat Hunting Solution, you will have enhanced visibility and gain cyber situational awareness of what is happening within your IT environment and how you can better secure your system moving forward.

Our experienced investigators will work hand-in-hand with your IT security teams. Over time, we will also empower them to conduct their own cyber threat hunts. Our depth of knowledge, actionable inputs from cyber threat intelligence, proficient skill sets and the experience of thinking like an attacker add a competitive edge to your cyber threat hunt.

Contact us

Chad Olsen
Partner and Head of Forensics – Hong Kong
Hong Kong
KPMG China
T: +852 3927 5576
E: chad.olsen@kpmg.com

Mohit Kumar
Director, Cyber Incident Management
Hong Kong
KPMG China
T: +852 2685 7428
E: mohit.kumar@kpmg.com

kpmg.com/cn/socialmedia