KPMG

Threat hunting

Using advanced threat intelligence technologies and KPMG's cyber security expertise to identify previously unknown threats

kpmg.com/nz/cyber

Why?

The odds are stacked against the defenders

Traditional security tools such as firewalls and anti-virus software have relied upon signatures and pre-defined rules to detect and escalate cyber security incidents. Security frameworks also tout perimeter defences and defence-in-depth as the tried and tested approach to designing a secure IT environment.

However, advancements in attacker techniques and covert malware exploitation technologies, along with the evaporation of corporate boundaries, have reduced the effectiveness of these security axioms.

With the threat looming and ever evolving, KPMG's threat hunting helps you answer the critical question being asked by boards and senior management "has our organisation been breached?"

The threat hunting provides real-time, forward looking visibility and continuous monitoring for patterns of attacker activity. Malicious activities such as privilege escalation, lateral movement, malware deployment and credential dumping (among other areas) are actively monitored and hunted.

Through in-depth examination and monitoring of your systems, KPMG can identify, search and hunt for issues that affect you, and help you adopt an active stance towards cyber defence.

If you are maturing your security operations program, wanting to obtain higher levels of comfort, or just looking for visibility of existing threats and risks, KPMG's threat hunting service can provide significant value to your organisation.

Threat hunting

Cyber attacks have become increasingly complex and dynamic, and network defences are having trouble keeping up.

KPMG's threat hunting service can support your organisation gain an understanding of your current exposure and help identify previously invisible threats.

By combining the investigative experience of KPMG's cyber threat intelligence professionals with the multi-dimensional discovery capability of data science, we can help reveal threats and anomalies undetected by your current technologies.

The results can be the first step to an integrated approach to security operations, in a controlled and effective manner.

Identification of threats

KPMG services go beyond "point in time" monitoring, and emphasises both expert analysis, and real time threat detection and hunting. The data collection process provides historical forensic evidence, which enables hunting of threats both current and historical.

Knowing what has happened in the past, and what is happening now on your systems, is key to understanding how to defend your IT environment in the future.

Immediate triage of alerts and potential compromises, provide actionable intelligence to support decision making.

Actionable analysis and findings

In order to be successful, the findings and analysis reports must be actionable and appropriate for all the key stakeholders, including senior management, the IT team and risk management functions.

The outputs of the threat hunting include:

- Regular reports detailing the summary findings, whether evidence of an intrusion was discovered, areas of risk identification, and recommendations for improving your security posture.
- Plain English executive reporting detailing the most significant findings, conclusions and recommendations.
- Detailed technical analysis of the findings, designed to provide your IT and security teams with what they need to investigate, validate and remediate.
- Real time alerting, designed to provide your IT and security teams with the required intelligence, and actionable incident response/investigation to minimise impacts.

How does KPMG provide the service?

The threat hunting service consists of the following steps:

1 PREPARATION
Define the scope and the threat hunting techniques that will be used
We will work with you to define the scope of the threat hunting, including the threat hunting techniques that will be used, and determine where to deploy the sensors. This step is essential to help ensure you gain the maximum benefit possible from the threat hunting.

2 DEPLOYMENT
Deploy the threat hunting technologies and tailor the threat hunting rules.
We will guide and support your IT team with sensor deployment. During this phase, we will also set up the relevant policies for your environment, and tailor the threat hunting rules based on your environment, threats posed, specific threat hunting requirements and confirmation of what you will see as an outcome of this engagement.

3 DATA COLLECTION
Collect real time metadata from the systems and analyse in real time.
As an ongoing activity for the duration of the threat hunting metadata will be actively collected from your systems, analysed and monitored in real time.

4 MANAGED HUNTING
Undertake threat hunting, and investigate high risk and anomalous activities.
We will perform managed threat hunting throughout the course of the engagement, looking for malware and malware-free threats, exploits, indicators of attack (IoAs), advanced threat techniques, evidence of malicious content and other anomalous activities that may be indicative of a breach.

5 REPORTING
Perform reporting, alert on high risk findings, and identify root causes.
We will investigate the findings from the threat hunting and provide alerts in near real time for any high risk findings. The findings will be investigated in conjunction with you to quantify and qualify the threat posed. Reporting will be provided weekly, and at the end of the engagement.

What insights will you gain?

- 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.
- Visibility of privilege escalation and credential dumping.

Our experience shows

From past assessments, more than half of the organisations we analysed had already been compromised unknowingly, or were placed at a high risk of being compromised.

Our Threat Hunting service not only identified the threats, but also allowed the organisations to understand the root causes of the issues, and strengthen their cyber defences against future attacks.

About KPMG Cyber Security Services

KPMG Cyber Security Services is a large group of professionals specialising in various security fields including security risk assessments, security governance, security architecture, threat detection and response, penetration testing and read teaming, identity and access management, and cloud security. Within KPMG Cyber Security Services there is a dedicated incident response and threat hunting team. This team has assisted a multitude of organisations, active in almost all industries and sectors, with their security journey. Whether you are looking to mature your security, or transforming your security operations processes, KPMG Cyber Security Services is ready to help you to take the next step in a practical and effective manner, to increase your organisation's security through the use of advanced services.

Why KPMG?

KPMG can support your organisation identify and manage the cyber security risks faced, and aid you through the entire security maturity lifecycle. Our cyber security approach has been lauded by many clients varying from major international organisations to recognised local brands, in industries ranging from financial services and telecom providers to government and healthcare.

Our team of cyber security specialists have proven experience managing cyber security risks at a technical, policy, risk and organisational level. Partnering with KPMG ensures that you will get the KPMG quality with understandable presentations and reports, and effective assistance, helping your organisation to become future proof.

Contacts

For more information on KPMG's Threat Hunting service, or our wider Cyber Security Services, please contact us or visit us at www.kpmg.com/nz/cyber

Philip Whitmore
Partner, Cyber Security
T +64 9 367 5931
M +64 21 654846
E pwhitmore@kpmg.co.nz

Peter Benson
Director, Cyber Security
T +64 9 363 3484
M +64 27 571 0764
E peterbenson@kpmg.co.nz