KPMG

Threat Analytics Assessment

Be in a defensible position.
Be cyber resilient.

High Definition Threat Analytics | See what your security monitoring and threat intelligence have been missing.

Species such as the mimic octopus have adapted to ward off threats in the most challenging environments. Organizations must do the same to protect, detect and respond to ever-changing threats.

Confidence and effectiveness in security data, intelligence and analysis equals High Definition Threat Analytics.

The cyber threat landscape is ever-changing, as the sophistication of attacks increases. State and non-state actors possess the means, motives and resources to create complex attacks that evade conventional security.

Continuous threat monitoring is integral to your security foundation, but they also generate a lot of noise. Organizations can become quickly overwhelmed trying to identify the needle in the haystack amongst millions of security events and divergent types of information, structured and unstructured, that come both internally and externally.

The best offense is a strong defense in depth. You need to look beyond reliance on the same trusted techniques for adequate protections. Integrating threat intelligence into your existing program through analytics and proactive threat hunting will increase your ability to isolate and respond to the threats that matter.

Many organizations ask themselves the following questions:

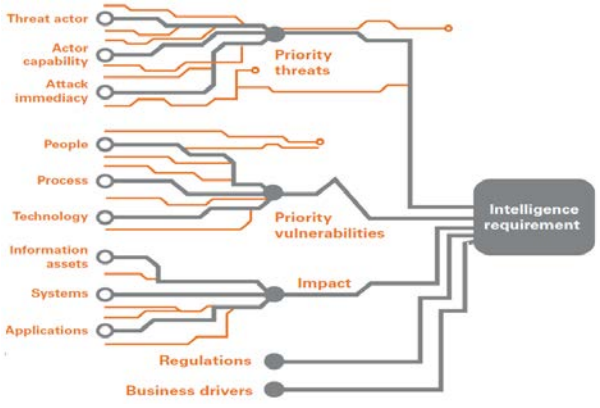
- Are we receiving the right security data and intelligence?
- Can we prioritize what really needs attention?
- Have we found ways to automate and optimize?
- Are we effectively using existing data to drive our security decisions?

What is a Threat Analytics Assessment?

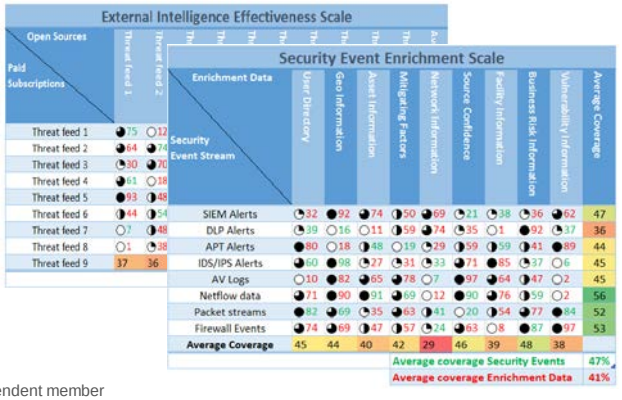
KPMG's Threat Analytics Assessment reviews your level of security monitoring, intelligence and analysis maturity to ensure you are collecting the right security data and enriching it with the right intelligence to get a wider scope and a sharper image of threats.

Threats adapt and evolve – so too must security. A mature threat analytics program ensures you have the information you need when you need it the most. Our assessment is executed in three steps:

1. Identify your intelligence requirements, From tracking cyber adversaries across the clear and dark web or addressing regulatory requirements, KPMG will identify the unique intelligence requirements of your organization.



2. Assess the coverage and accuracy of your security data and intelligence, KPMG will review the sources of security data across your organization, event logging levels and the accuracy of threat intelligence data needed to enrich analysis.



3. Assess your analytical ability to identify threats through hunting and analytics

A Hunting Team is charged with the task of looking at all those data feeds, enriching the data with outside information, and doing what no level of automation can do. They will strategically assess the Threat Intelligence to look beyond what you, your IDS/IPS, and any third party sources typically evaluate against. They can then take their findings and interpret them in terms of use cases specific to your business environment that can be pushed across all levels to create awareness and change patterns.

Harnessing our global experience in cyber analytics, threat detection and intelligence, we will review and assess your ability to normalize, ingest and analyze security data and leverage it for effective response. This assessment will leverage KPMG's Cyber Analytics Maturity Model (CAM^2).

Benefits of a Threat Intelligence Assessment

We understand the need to connect all the dots in order to generate the big picture for a comprehensive security framework. The following assessment deliverables will improve threat detection and response times, limiting impact to your organization:

- Recommendations that will allow you to better leverage your security investments for improved cyber threat visibility and analytics maturity via a defined target operating state and roadmap
- Confidence in the value of your threat intelligence feeds and the ability to reduce costs by eliminating unneeded feeds
- Current maturity index for the existing security environment
- Process enhancement techniques such as use cases to innovate and disrupt security and effect continuous improvement across all layers

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

Cyber Emergency?

Please contact our 24/7 Cyber response hotline

1-844-KPMG-911

1 (844) 576-4911

We believe cyber security should be about what you CAN DO – not what you can't.

Award winning

KPMG International has been named a Leader in the Forrester Research Inc. report, The Forrester Wave™: Information Security Consulting Services, Q1 2016 achieving the highest score for current offering and strategy.

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 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.

Trusted

KPMG member firms have a long list of certifications and permits to work on engagements for 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, giving member firms the ability to orchestrate and deliver to consistently high standards worldwide. 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 Services Leader
T: 416 777 8501
E: pwhanley@kpmg.ca