KPMG

Keep tabs on evolving threats

Stay ahead in an expanding risk landscape with
Managed Threat Intelligence

At a glance: Key challenges

Emerging tech like AI and machine learning are revolutionising the way businesses operate and communicate with clients and customers. In the face of persistent and emerging cyber trends, business leaders are increasingly having to navigate new challenges in digital security. These include:

Demand for process excellence

As the global economy evolves, businesses are constantly looking for smart solutions to enhance their cyber posture while maximising productivity and efficiency.

Talent gap

Even as the demand for trained cybersecurity professionals grows, scarcity in talent supply is creating potential gaps in security.

Increased regulatory frameworks

The increasing frequency and sophistication of cyber threats is driving the demand in regulation and compliance.

Actionable intelligence at your fingertips

Stay ahead of emerging threats

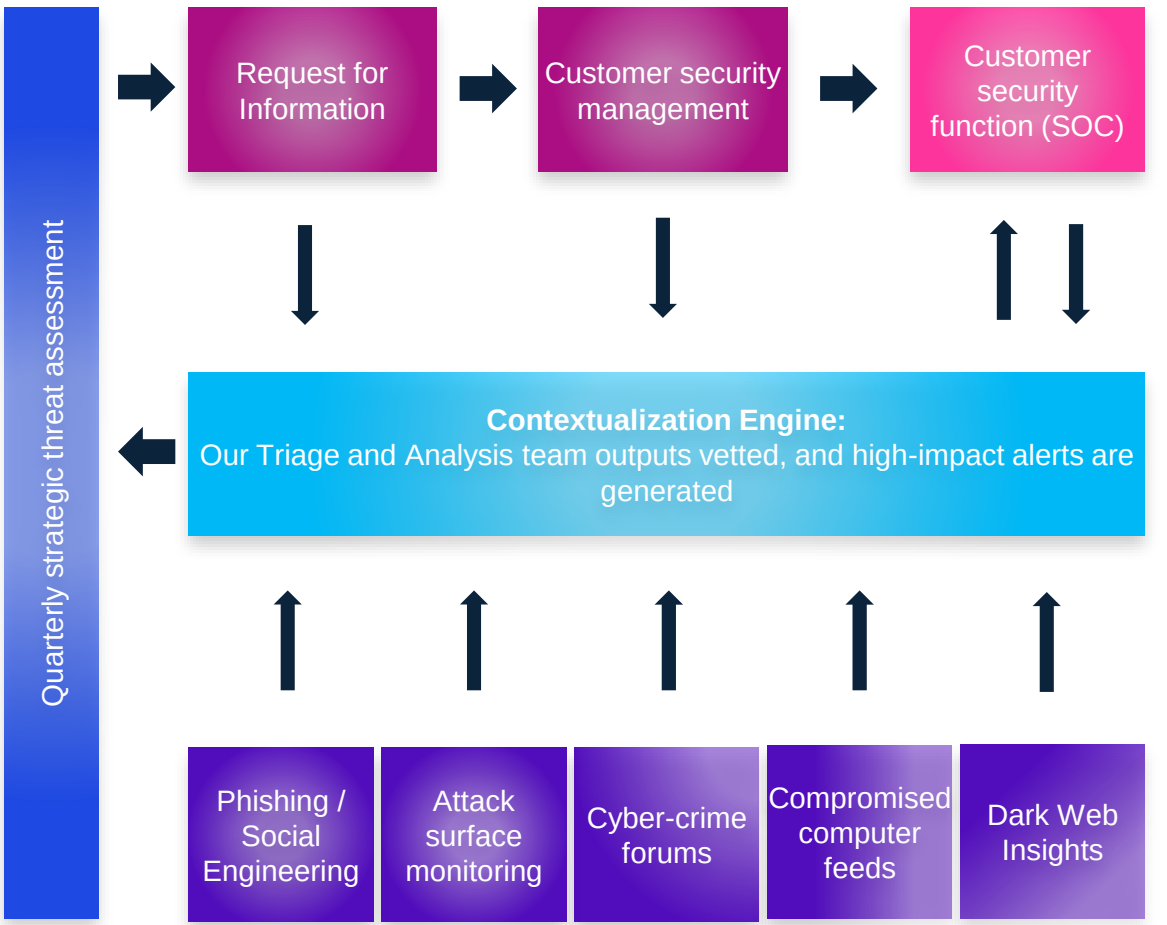
As digital transformation accelerates, so do new avenues of cyber-attacks.

The rise in volume and sophistication of threat actors' tactics can make it difficult for businesses to stay ahead of emerging threats.

KPMG in Singapore's **Managed Threat Intelligence** service provides the information and capabilities you need to continuously monitor risks, respond and refine your defences.

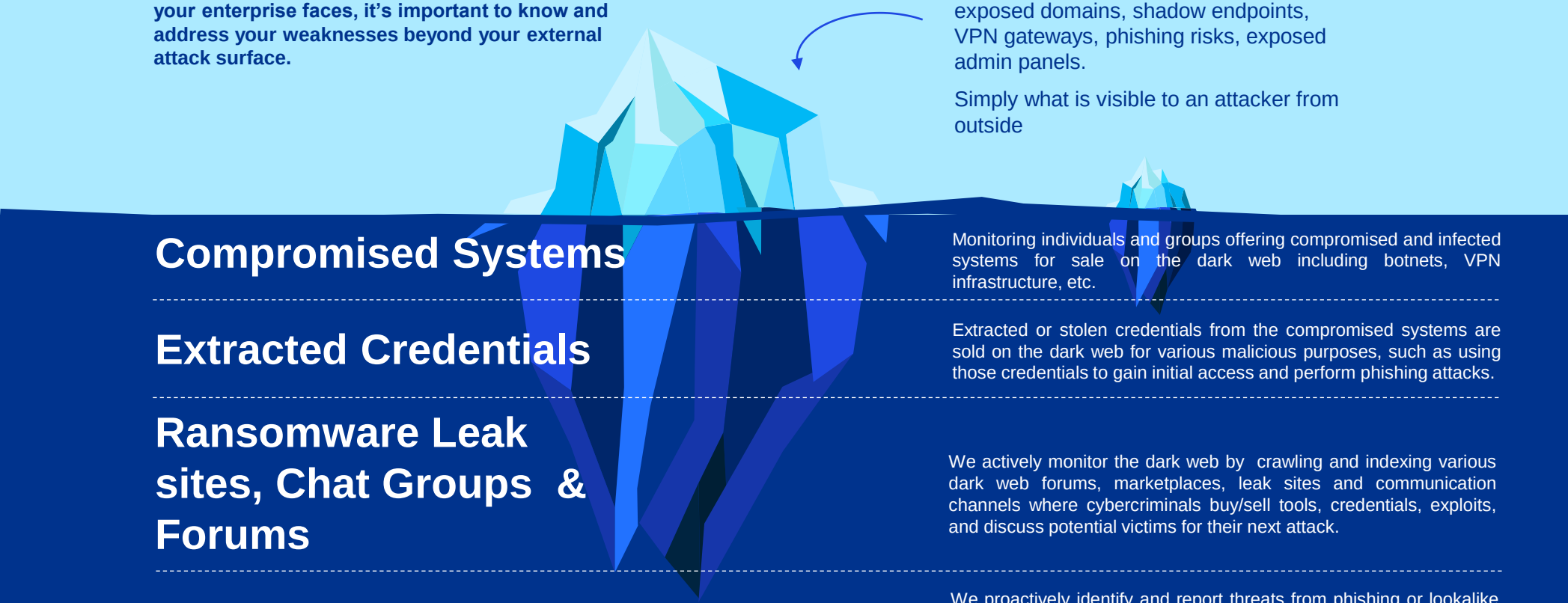
An intelligence-led approach to cyber risk management

We sift through raw data, conduct incident triage and report threats to your enterprise, so you are free to focus on what matters: your business.



What's covered in our Threat Intelligence

When assessing the potential threats and risks that your enterprise faces, it's important to know and address your weaknesses beyond your external attack surface.



External attack surface monitoring – exposed domains, shadow endpoints, VPN gateways, phishing risks, exposed admin panels.

Simply what is visible to an attacker from outside

Compromised Systems

Monitoring individuals and groups offering compromised and infected systems for sale on the dark web including botnets, VPN infrastructure, etc.

Extracted Credentials

Extracted or stolen credentials from the compromised systems are sold on the dark web for various malicious purposes, such as using those credentials to gain initial access and perform phishing attacks.

Ransomware Leak sites, Chat Groups & Forums

We actively monitor the dark web by crawling and indexing various dark web forums, marketplaces, leak sites and communication channels where cybercriminals buy/sell tools, credentials, exploits, and discuss potential victims for their next attack.

Phishing Domains

We proactively identify and report threats from phishing or lookalike domains that closely resemble your legitimate ones. These domains are often used by attackers to deceive users, leading to credential theft, financial loss, or other serious consequences

What's covered in our Threat Intelligence

01

External Attack Surface Monitoring

Our External Attack Surface Scanning and Monitoring service continuously identifies and monitors exposed assets, vulnerabilities, and entry points across your organization's digital footprint. By detecting misconfigurations, open ports, and unprotected systems before attackers exploit them, we help reduce the risk of cyberattacks and ensure your security posture remains strong.

02

Ransomware Leak sites, Chat Groups & Forums

We actively monitor the dark web by crawling and indexing various dark web forums, marketplaces, leak sites and communication channels where cybercriminals buy/sell tools, credentials, exploits, and discuss potential victims for their next attack.

03

Compromised Systems

Monitoring individuals and groups offering compromised and infected systems for sale on the dark web including botnets, VPN infrastructure, etc.

04

Open-Source Intelligence

Our Open-Source Intelligence (OSINT) service collects and analyses publicly available information from a wide range of sources, including social media, forums, websites, and news outlets. By uncovering potential threats, data leaks, or mentions of your organization in risky contexts, we provide actionable intelligence to enhance your security and help you stay ahead of emerging risks.

05

Phishing Domains

We proactively identify and report threats from phishing or lookalike domains that closely resemble your legitimate ones. These domains are often used by attackers to deceive users, leading to credential theft, financial loss, or other serious consequences

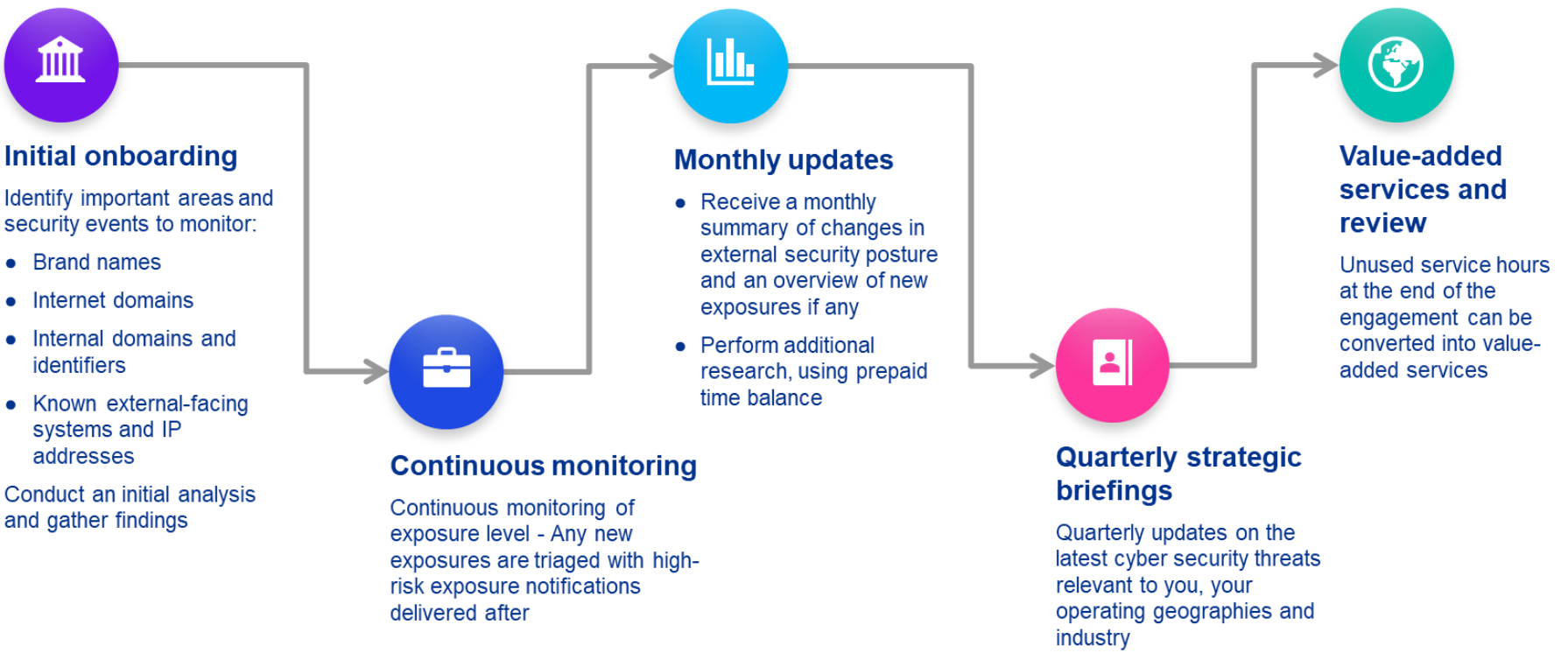
06

Extracted Credentials

Extracted or stolen credentials from the compromised systems are sold on the dark web for various malicious purposes, such as using those credentials to gain initial access and perform phishing attacks.

How our threat intelligence journey works

Our Managed Threat Intelligence journey proactively identifies and addresses evolving cyber threats, keeping your organization secure through continuous monitoring, real-time insights, and strategic updates. This ensures your defences stay strong as the threat landscape evolves.



Threat Intelligence Process Example – Leaked Credentials

The leaked credentials monitoring of the threat intelligence process monitors the dark web for leaked credentials associated with the organization, enabling proactive risk mitigation and prioritization of responses to protect sensitive information and enhance overall security posture.

Identify leaked Credentials

We search the dark web using the client's public and internal domains, public IP addresses, and other relevant keywords to find any potentially leaked credentials.

Filter and Contextualize

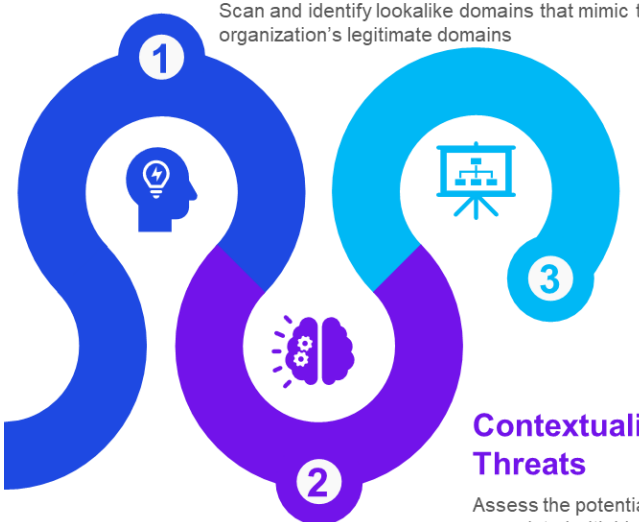
After identifying the leaked credentials, we add context by distinguishing between personal and corporate credentials. We also identify whether the credentials belong to office systems, VPN gateways, or SaaS applications and categorize them by priority.

Report and Recommendations

Based on the findings and their priority levels, we provide specific recommendations for each one. We also integrate results from external attack surface scanning to adjust the priority and give precise, actionable steps to address the issue and prevent it from happening again.

Threat Intelligence Process Example – Phishing Domain Analysis

The Phishing Domain Analysis process focuses on detecting and assessing lookalike domains to protect against phishing threats. By proactively identifying these domains, we can provide actionable recommendations to enhance user awareness and security measures.



Identify Phishing Domains

Scan and identify lookalike domains that mimic the organization's legitimate domains

Actionable Recommendations

Provide specific actions to mitigate phishing threats and enhance security awareness

Contextualize Threats

Assess the potential risks associated with identified phishing domains

Identify Phishing Domains

We monitor and analyse domain registrations to identify any lookalike phishing domains that closely resemble the organization's legitimate domains.

Contextualize Threats

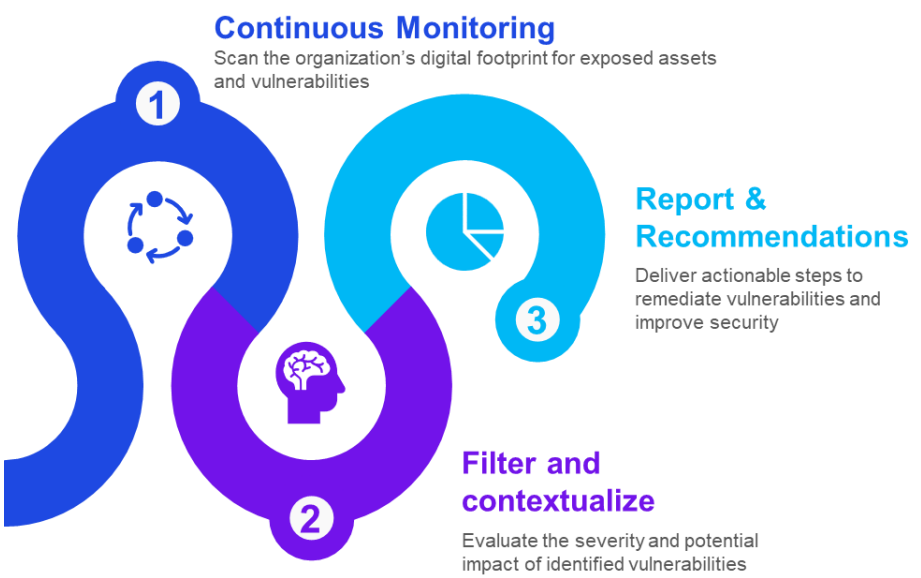
Once identified, we assess the potential threat posed by these phishing domains by analysing their usage, reputation, ASN and registration history, target audience, and methods of attack.

Actionable Recommendations

Based on the analysis, we provide actionable recommendations, including network defences, domain blockings, and user awareness campaigns to mitigate the risks associated with phishing attacks.

Threat Intelligence Process Example – External Attack Surface Scanning

The External Attack Surface Scanning process aims to continuously monitor the organization's digital presence for vulnerabilities and misconfigurations. By evaluating risks and delivering targeted remediation strategies, this process strengthens the organization's security posture against potential attacks.



Continuous Monitoring

We conduct ongoing scans of the organization's digital footprint to detect exposed assets, Shadow IT, vulnerabilities, and misconfigurations across public-facing systems.

Risk Assessment

After identifying vulnerabilities, we validate the findings and evaluate their severity and potential impact on the organization, prioritizing them based on asset criticality and exploitability.

Remediation Strategies

We deliver actionable remediation strategies, including patching vulnerabilities, updating security configurations, and implementing additional safeguards to strengthen the organization's security posture.

Contact us

Eddie Toh
Partner
Cyber, Advisory
KPMG in Singapore
T: +65 6213 3028
E: eddietoh@kpmg.com.sg

kpmg.com.sg