KPMG

Proactively manage risk and secure your digital future with our vulnerability management solutions

Resolve security vulnerabilities with real-time visibility and control

As cyber threats rise in volume and complexity, vulnerability management solutions can offer organisations flexible and scalable strategies to identify, evaluate and remediate security vulnerabilities across endpoints, workloads and systems.

KPMG in Singapore's vulnerability management solutions provide intelligent and optimised insights, giving you the clarity and confidence to gain an edge on emerging risks and strengthen your cybersecurity posture.

Our advanced attack surface monitoring capabilities empower you to seamlessly identify risks and mitigate cyber threats, whether they are planned, imminent or actively underway.

Our in-depth threat intelligence solutions can help you:

► Plan

Understand key risks to your business and monitor threats using our centralised dashboard.

► Prioritise

Assess and prioritise threat findings based on action priority (high, medium or low) against remediation timelines, ensuring that no findings exceed the benchmark/guideline frame for remediation.

► Prepare

Maintain endpoint compliance by tracking your vulnerability footprint, remediation action strategies, timelines and action parties.

Case study

Project scope

To ensure compliance of Critical Information Infrastructure under the Cybersecurity Code of Practice for Critical Information Infrastructure – Second Edition (CCoP2.0) regulations, we conducted a system vulnerability assessment for our client from 30 April 2023 to 30 May 2023.

Summary of findings

A total of 13 medium risks and 3 low risks findings were observed. For the host and network security assessments, the medium risks findings were due to missing patches and misconfigurations. However, there was no immediate need to install these missing patches and updates. These patches and updates should be tested and approved by the respective plant vendors prior to the roll-out in the next scheduled patching interval or next planned downtime.

Other key findings include the use of insecure Server Message Block (SMB) version 1 service and end-of-life (EOL) Windows operating systems. The need for SMB version 1 service should be reviewed during the on-going replacement of the EOL Windows operating systems. In addition, XXX_DC1 should be reviewed periodically to resolve any user account management issues. The stored web credentials should also be removed.

For the architecture security review, it was noted that the architecture features in the system had been implemented by design and hence, could not be configured easily. To address the threat of the ease of lateral movement in the plant network, it is important to strengthen the detection and respond/recover to possible cyber-attacks capability.

Overview of findings

Assessment	No. of Findings			
	Low	Medium	High	Very High
Host and Network Security Assessment	3	12	0	0
Architecture Security Review	0	1	0	0

Host and network security assessment findings

Reference/ Section	Findings	Risk
3.1	Missing patches from Field Control Station (FCS) and Safety Control Station (SCS)	Medium
3.2	Missing patches from Centum VP application	Medium
3.3	Missing patches from Vulnerabilities in 3rd party applications	Medium
3.4	Missing Windows Operating System and Microsoft-related Applications Security Updates	Medium
3.5	Ghost Assets	Low
3.6	Assets discovered not in authorised list	Low
3.7	Security configurations not compliant with basline	Medium
3.8	Use of Server Message Block version 1	Medium
3.9	End-of-life Windows Operating Systems	Medium
3.10	Host-based firewall turned off	Medium
3.11	Writable Startup Applications	Medium
3.12	Limited audit log buffer size	Low
3.13	User account management issues	Medium
3.14	Unnecessary services or firewall rules enabled	Medium
3.15	Credentials stored in Web Credentials	Medium

Architecture security review findings

Reference/ Section	Findings	Risk
4.1	Ease of lateral movement within the plant network	Medium

Safeguard your digital future with the CII Assurance Tracker (CAT)

KPMG's CII Assurance Tracker (CAT) can help deliver integrated compliance management solutions and sustain value for your organisation, tailored to your business needs and objectives.

CAT can empower you to streamline and automate your compliance management tools. Our platform can assist you in aligning your cyber security framework with existing compliance and regulations, allowing you to identify, report, and remediate security risks in real-time.

Explore new business frontiers with us, sign up for our CAT pilot programme

Join us as a pilot participant for our CAT programme and enhance your organisation's cyber posture today.

- Pilot participants will co-fund the development of a Beta version and might receive incentives for it. The pilot can be conducted together with participants based on their requirements and preferences with regards to what information is useful for them. This includes options like interface design and workflow processes.
- A typical timeline for a pilot trial is 3 months.
- Subsequent clients who come onboard after the pilot trial will be charged on a subscription basis.

Inspiring stakeholder trust with KPMG managed services

Business transformation can pave the way for sustained advantage. But transformation is more than a destination — it is a continuous journey. How can you evolve your business while keeping up with everchanging goals?

KPMG Managed Services can help you realise your dreams. We combine advanced tech with functional sector expertise to handle knowledge-intensive processes across your enterprise — both on a subscription and a as-a-service basis. In addition to maximising your costs, we can help deliver other outcomes like resilience, customer retention, stakeholder trust and an added competitive edge. Let us help you operationalise your growth ambitions as you can accelerate your transformation journey amid disruptions and risks.

Contact us

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

Wong Loke Yeow
Partner
Cyber,
Advisory
KPMG in Singapore
T: +65 6213 3053
E: lokeyeowwong@kpmg.com.sg

Edmund Goh
Director
Cyber,
Risk Consulting
KPMG in Singapore
T: +65 9724 3454
E: edmundgoh@kpmg.com.sg

kpmg.com.sg