
KPMG
Proactively manage cyber risk with our vulnerability management solutions

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.

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

A post-secondary education institution under the purview of Ministry of Education engaged KPMG to assist in meeting the government Instruction Manual (IM) requirements. The scope covered performing quarterly vulnerability assessments and penetration tests of the school's applications and systems.

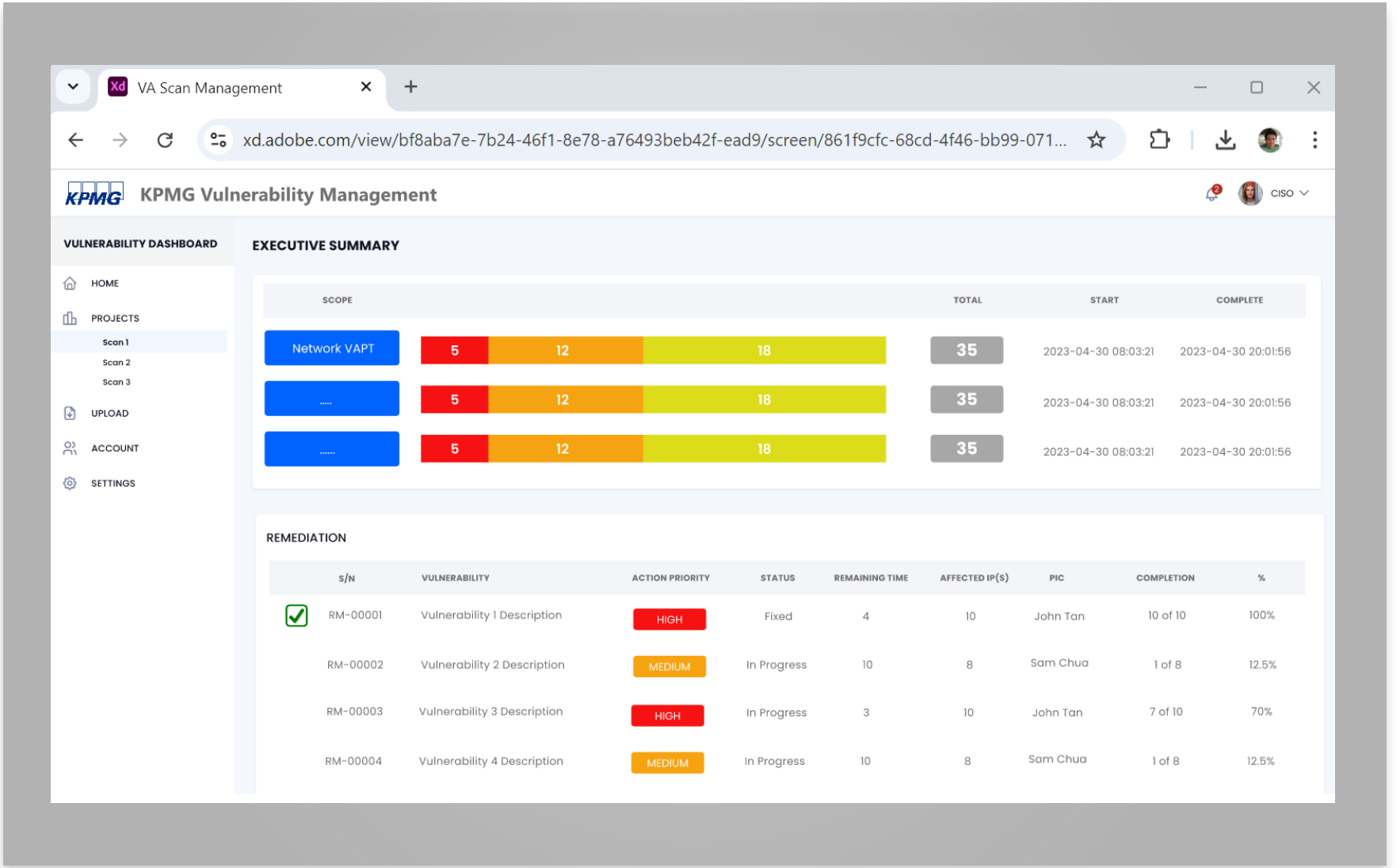
How KPMG Helped:

- Discovered live applications and servers of the school.
- Conducted quarterly vulnerability assessments and penetration tests of all applications and servers.
- Prioritised all security vulnerabilities identified and the remediation timelines against the classification of the systems.
- Worked closely with the respective system owners to remediate and ensure closure of the vulnerabilities.

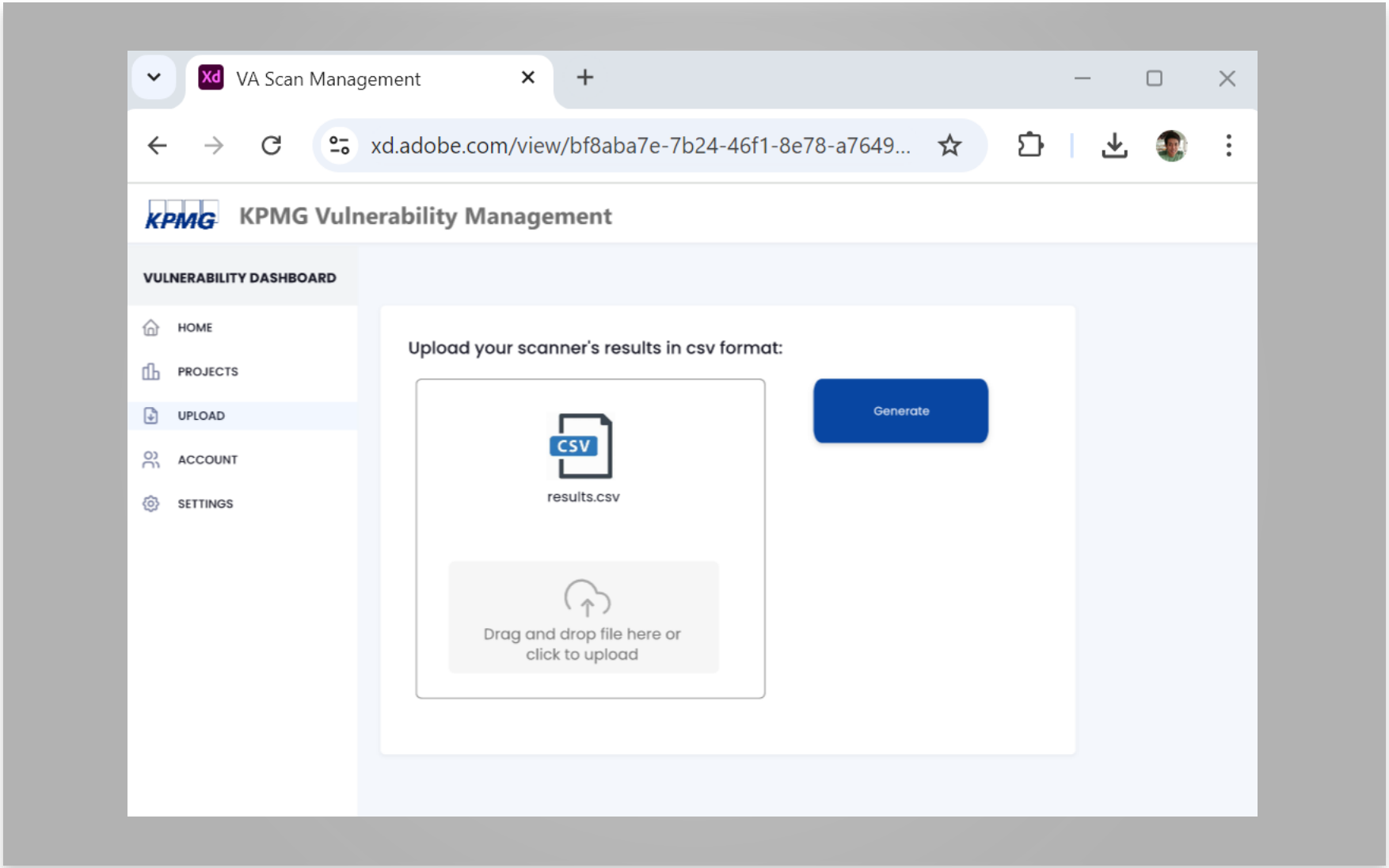
Outcomes delivered for our client:

- KPMG identified critical security vulnerabilities, and rapidly reduce overall risks to the school.
- Client has a more confident view of the cyber risks for its applications and systems, and its ability to manage them.
- Client was able to meet the regulatory requirements.

Dashboard View (1/2)



Dashboard View (2/2)



Key takeaway

1. Dashboard visibility and control to resolve security vulnerabilities with the system owners

2. Reduce the overall threat exposure

KPMG

Contact us

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

Carl Hunt
Principal Advisor
Cyber, Advisory
KPMG in Singapore
T: +65 6212 3388
E: carlhunt@kpmg.com.sg

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

kpmg.com.sg