CYBOTS

CYBER THREATS DON'T SLEEP. **NEITHER DO WE.**

CASE STUDY

BUILT FOR DIGITAL. READY FOR THREATS.

Protecting a digital-first banking environment as technology, users and risk continue to scale.



CASE STUDY | **DIGITAL BANK**

CYBOTS
CYBER THREATS DON'T SLEEP. NEITHER DO WE.

SECURING BANKING AT DIGITAL SPEED

Strengthening security visibility and resilience across a rapidly scaling digital banking environment.

Client Background

A licensed digital bank in Malaysia operates a fully cloud-native financial ecosystem, delivering seamless banking experiences across mobile and web platforms.

With no physical branches, the organization relies entirely on its digital infrastructure to manage customer onboarding, transactions, and financial services; making cybersecurity not just a function, but a core pillar of business continuity and customer trust.

Industry Context: The New Risk Landscape for Digital Banks

Digital banks operate in one of the most targeted and regulated environments globally. Unlike traditional banks, their attack surface is:

- Fully digital and always exposed
- Heavily reliant on APIs and third-party integrations
- Driven by identity and access systems
- Continuously evolving with rapid product releases

Threat actors increasingly exploit:

- API vulnerabilities
- Identity and authentication weaknesses
- Misconfigurations in cloud environments
- Gaps between development and security teams

In this environment, **a single vulnerability can directly translate into financial loss, regulatory penalties, and erosion of customer trust.**



The Operational Problem

The bank needed to validate the security of a large and complex digital environment under strict regulatory requirements.
This included:

- Multiple customer-facing applications
- Backend financial systems
- Network and infrastructure layers
- Continuous deployment pipelines

The challenge was not just identifying vulnerabilities, but doing so at scale, depth, and speed, while ensuring alignment with regulatory frameworks.

Why Traditional Approaches Failed

Conventional security testing methods were insufficient for a digital-first bank:

- **Point-in-time testing** could not keep pace with rapid development cycles
- **Siloed assessments** failed to provide a complete view of risk
- **Limited scalability** restricted coverage across the full environment

This created gaps between what was tested and what was actually exposed, leaving potential vulnerabilities unaddressed.

THE CYBOTS APPROACH:

Continuous, Scalable Security Validation

Cybots approached the engagement as a long-term security validation program, designed to scale with the bank's digital growth.

A team of specialized consultants worked in parallel to ensure comprehensive coverage across all layers of the environment.

Execution Timeline

Over a 12-month engagement, Cybots delivered:



Full-Scope Security Testing

- Web applications
- Mobile applications
- APIs
- Network infrastructure



Parallel Assessment Model

- Up to 7 consultants deployed simultaneously
- Continuous testing aligned with development cycles



Risk-Based Prioritization

- Identification of high-impact vulnerabilities
- Clear mapping of attack paths across systems



Regulatory Alignment

- Testing aligned with Bank Negara Malaysia (BNM) requirements
- Support for audit and compliance readiness

Business Impact

The engagement strengthened the bank's ability to operate securely at scale:

- **Enhanced protection of customer data and financial transactions**
- **Improved resilience against API and identity-based attacks**
- **Accelerated compliance with regulatory requirements**
- **Increased confidence at leadership level in security readiness**

Most importantly, the bank was able to scale its digital services without scaling its risk exposure.

Outcome

The bank achieved end-to-end visibility across its digital ecosystem, enabling:

- Identification of critical vulnerabilities across applications and infrastructure
- Continuous validation of security posture as the environment evolved
- Clear prioritization of remediation based on real-world risk

