CYBOTS

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

CASE STUDY

BEYOND COMPLIANCE: FINDING THE RISK THAT MATTERS

Turning a regulatory requirement into actionable insight across the bank's security environment.



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

FINDING THE RISK THAT MATTERS

Using security assessment to uncover risks that traditional compliance checks can miss.

Client Background

A major financial institution in Malaysia provides a wide range of banking services, supporting millions of customers across retail and business segments.

As part of a highly regulated industry, the organization operates complex systems handling transactions, customer data, and financial operations that requires continuous assurance of security, integrity, and compliance.

Industry Context: Compliance Is Not Security

The banking sector faces constant pressure from both regulators and evolving threat actors.

While regulatory frameworks such as technology risk management guidelines enforce strong controls, they do not guarantee that systems are free from compromise.

Modern threats in banking environments are increasingly:

- Stealthy and persistent, bypassing traditional controls
- Identity-driven, using legitimate credentials to avoid detection
- Embedded within systems, remaining undetected for extended periods

This creates a critical gap:
Organizations may be compliant but still compromised.



The Operational Problem

The organization was required to meet regulatory compliance within a strict 6-week timeline, driving the need for a comprehensive assessment of its security posture.

However, the real challenge extended beyond compliance:

- Limited visibility into existing compromises
- High dependency on alert-based monitoring
- Uncertainty around the true state of security across thousands of systems

The organization needed more than a checklist; it needed certainty.

Why Traditional Approaches Failed

Conventional methods were insufficient in this scenario:

- Compliance-driven assessments validated controls, not compromise
- Manual reviews could not scale across thousands of machines
- Siloed tools failed to correlate activity across the environment

As a result, risks could remain hidden even as compliance requirements were technically met.

THE CYBOTS APPROACH:

AI-Driven, Large-Scale Compromise Assessment

Cybots deployed a large-scale **Compromise Assessment** across more than 5,000 machines using AI-driven analysis and expert validation.

Execution Timeline

FULL ENVIRONMENT SCANNED WITHIN 6 WEEKS → **AI-DRIVEN ANALYSIS IDENTIFIED ANOMALIES** → **EXPERT INVESTIGATION VALIDATED FINDINGS**

Moment of Truth

The assessment revealed that over 10% of machines were already compromised. An exposure that would have remained undetected under conventional approaches.

Outcome

An AI-enabled Incident Response Plan was generated within one day, enabling rapid containment and remediation.

The organization achieved compliance within timeline and budget while significantly reducing risk exposure.

