CYBOTS

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

CASE STUDY

FROM ASSUMPTION TO CERTAINTY

Validating Security in a High-Stakes Environment for a Southeast-Asian Financial Services Institution



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

TURNING SECURITY UNCERTAINTY INTO CERTAINTY

A proactive assessment to uncover weaknesses across a critical financial environment.

Client Background

A leading financial technology provider in Southeast Asia delivers core banking solutions and digital financial platforms to banks and financial institutions across the region.

Operating at the heart of the financial ecosystem, the organization supports mission-critical systems that process high volumes of transactions and sensitive financial data daily. Ensuring the integrity, availability, and security of these systems is essential; not just for its own operations, but for the institutions and customers that depend on them.

Industry Context: Financial Services Under Constant Threat

The financial services sector remains one of the most targeted industries globally due to:

- Direct financial gain opportunities for attackers
- High-value transaction and customer data
- Interconnected systems across banks, partners, and platforms
- Increasing regulatory scrutiny and compliance requirements

Modern threats in this sector are increasingly sophisticated:

- Attackers bypass perimeter defenses and remain undetected for extended periods
- Compromises often occur silently within trusted systems
- Traditional controls provide visibility into activity; but not certainty of compromise

In this environment, not knowing is the biggest risk.



The Operational Problem

Despite existing security controls, the organization faced a critical question:

"Are we already compromised?"

This uncertainty was driven by:

- Lack of definitive visibility into potential hidden threats
- Increasing pressure to comply with evolving cybersecurity regulations
- The need to validate security posture quickly and accurately

Without clear answers, the organization risked operating under false confidence, where threats could exist undetected within critical systems.

Why Traditional Approaches Failed

Conventional security approaches were insufficient to answer this question:

- Compliance-based assessments confirmed controls, but not compromise
- Alert-driven monitoring lacked deep investigation capability
- Point-in-time reviews missed ongoing or dormant threats

These methods focused on potential risk, not actual compromise, leaving leadership without the clarity needed to act decisively.

THE CYBOTS APPROACH:

Investigation-First Security Validation

Cybots deployed a **Compromise Assessment (CA)** designed to deliver definitive answers, not assumptions.

The approach was grounded in:

- Assume-breach methodology
- AI-driven forensic analysis across endpoints
- Expert-led investigation and validation

Execution Timeline

Within 9 days, Cybots completed the full lifecycle:

RAPID DEPLOYMENT AND INSTALLATION → **DEEP TELEMETRY ANALYSIS** → **CORRELATION ACROSS ENDPOINTS** → **CLEAR REPORTING WITH ACTIONABLE REMEDIATION STEPS**



Outcome

The Compromise Assessment gave the organisation a **clear, evidence-based understanding of its security posture**, replacing uncertainty with verified findings.

The organisation was able to:

- Establish greater confidence in its environment by validating whether signs of compromise were present across monitored endpoints.
- Identify and prioritise genuine security risks based on severity, potential impact, and observed attacker behaviours.
- Reduce investigation noise by filtering false positives and focusing security teams on findings that required attention.
- Accelerate remediation through clear, actionable recommendations that enabled teams to respond to identified risks quickly.
- Strengthen security decision-making by providing leadership with forensic evidence rather than assumptions or incomplete alerts.
- Improve visibility beyond traditional controls by investigating endpoint activity and potential attacker techniques that may otherwise remain undetected.

