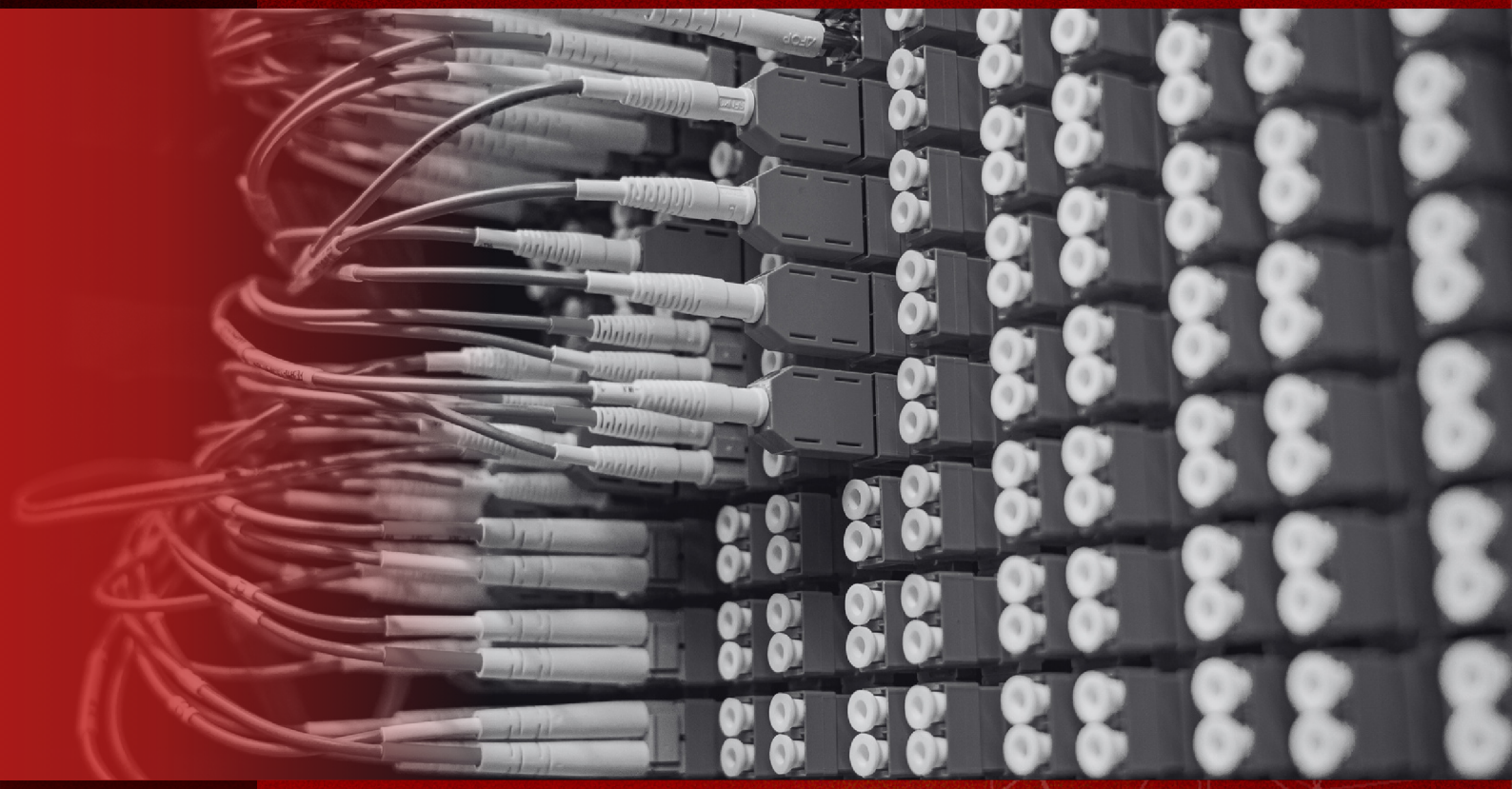
CYBOTS

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

CASE STUDY

SECURITY CERTAINTY UNDER REGULATORY PRESSURE

Validating security controls across a critical telecommunications environment when there is no room for uncertainty.



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

FROM REGULATORY PRESSURE TO SECURITY CONFIDENCE

Identifying and addressing security gaps before they become operational or compliance concerns.

Client Background

A major mobile network operator in Malaysia provides critical telecommunications infrastructure supporting millions of subscribers, enterprise customers, and national connectivity services.

As a backbone of digital communication, the organization plays a vital role in enabling mobile connectivity, data services, and digital ecosystems; making operational resilience and security non-negotiable.

Industry Context: Telecommunications as Critical Infrastructure

Telecommunications providers are among the most targeted sectors globally due to:

- High-value network access (entry point into broader digital ecosystems)
- Massive volumes of user data and metadata
- Interconnected infrastructure across regions and partners
- Dependency from governments, enterprises, and consumers

Threat actors, including nation-state groups, often target telecom providers to:

- Conduct surveillance and data exfiltration
- Disrupt critical communications
- Use telecom networks as a gateway for broader attacks

In this environment, even a small undetected compromise can scale into a large-scale operational or national risk.



The Operational Problem

The organization faced a time-critical regulatory requirement, needing to validate its security posture and submit findings within a strict 3-week deadline.

Key challenges included:

- Limited time for comprehensive assessment
- Need for accurate, defensible results for regulatory submission
- Lack of full visibility into potential hidden threats
- Risk of operational disruption if threats remained undetected

The challenge was not just speed; it was delivering certainty under pressure.

Why Traditional Approaches Failed

Conventional security assessments were not built for this scenario:

- Manual processes could not meet compressed timelines
- Fragmented tools limited visibility across systems
- Point-in-time testing failed to identify existing compromises

This created a gap between what was reported and what actually existed in the environment, increasing regulatory and operational risk.

THE CYBOTS APPROACH:

Rapid, AI-Driven Security Validation

Cybots deployed a **high-speed, AI-driven Compromise Assessment**, designed to **deliver both depth and speed without compromising accuracy.**

The approach focused on:

- Identifying existing compromises, not just vulnerabilities
- Leveraging AI-powered forensic analysis
- Validating findings with expert investigation

Execution Timeline

Cybots executed a tightly coordinated assessment:

RAPID DEPLOYMENT AND INSTALLATION

- Agents deployed across 140+ machines within days

DEEP ENVIRONMENT ANALYSIS

- AI-driven analysis of system behaviors and anomalies
- Correlation across endpoints to detect hidden threats

ACCELERATED REPORTING

- Full analysis completed within 2 days
- Comprehensive report delivered within 24 hours



Outcome

The organization achieved clear, evidence-based visibility into its environment within an extremely compressed timeframe.

Key outcomes included:

- Rapid validation of security posture
- Identification of potential risks and exposures
- Delivery of actionable remediation insights



Business Impact

Cybots enabled the organization to move from uncertainty to control:

- Successfully met regulatory submission requirements within deadline
- Reduced risk of undetected threats impacting operations
- Strengthened confidence among leadership and stakeholders
- Ensured continuity of critical telecommunications services

