CYBOTS

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

CASE STUDY

AFTER RANSOMWARE: BUILDING RESILIENCE BEYOND PREVENTION

Learning from a breach to strengthen the organisation's ability to detect, contain and recover.



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

BUILDING RESILIENCE BEYOND PREVENTION

Protected, But Still Breached: From Ransomware Incident to Operational Resilience

Client Background

A Singapore-based construction company manages large-scale infrastructure and development projects across multiple sites, coordinating contractors, project timelines, and critical documentation.

Operations rely heavily on digital systems for project management, file sharing, financial tracking, and communication between onsite and remote teams; making system availability essential to daily operations.

Industry Context: A Growing Target for Cyber Threats

The construction sector has increasingly become a target for cyberattacks due to:

- Decentralized operations across multiple project sites
- High reliance on shared documents and file systems
- Multiple third-party vendors and contractors
- Limited cybersecurity resources compared to other industries

Ransomware attacks in this sector are particularly disruptive, as they:

- Halt access to critical project files
- Delay construction timelines
- Impact financial flows and contractor coordination
- Create reputational and contractual risks

Unlike other industries, **cyber incidents in construction translate directly into physical and financial delays.**

The Operational Problem

The organization operated with:

- A single IT/SOC owner managing security
- No 24/7 monitoring capability
- Limited visibility across systems and endpoints

Despite having basic controls such as firewall and antivirus solutions, there was no centralized detection or response capability.

This created a critical gap: Threats could exist without being detected in time.



Moment of Truth: Ransomware Impact

The gap became real when a ransomware attack struck the organization.

- Critical servers were encrypted
- File access was disrupted across onsite and remote teams
- Project operations were impacted immediately

What initially appeared to be an IT issue quickly escalated into a **business disruption affecting project timelines and operations.**

Why Traditional Approaches Failed

Existing security measures were insufficient:

- Perimeter-based controls (firewall, antivirus) did not detect or stop the attack
- No real-time monitoring meant delayed response
- Lack of centralized visibility prevented early detection

This highlights a key reality:
Prevention alone is not enough. Organizations must be able to detect and respond in real time.

THE CYBOTS APPROACH:

From Containment to Transformation

Cybots initiated an immediate **Incident Response (IR)** engagement to contain and eradicate the threat.

Execution Timeline



Immediate Containment

- Isolated affected systems
- Prevented further spread of ransomware



Forensic Investigation

- Identified the root cause of the breach
- Analyzed attack vectors and system impact



Post-Incident Assesment

- Conducted a full Compromise Assessment
- Identified additional hidden threats and exposures



External Risk Visibility

- Deployed External Attack Surface Management (EASM)
- Identified exposed assets and vulnerabilities



Long Term Protection

- Implemented Advanced Managed Detection & Response (AMDR)
- Established 24/7 monitoring and rapid response capability

Outcome

Cybots successfully:

- Contained and eradicated the ransomware threat
- Identified and closed security gaps
- Restored operational stability

The organization gained full visibility into its environment, eliminating blind spots that previously existed.



Business Impact

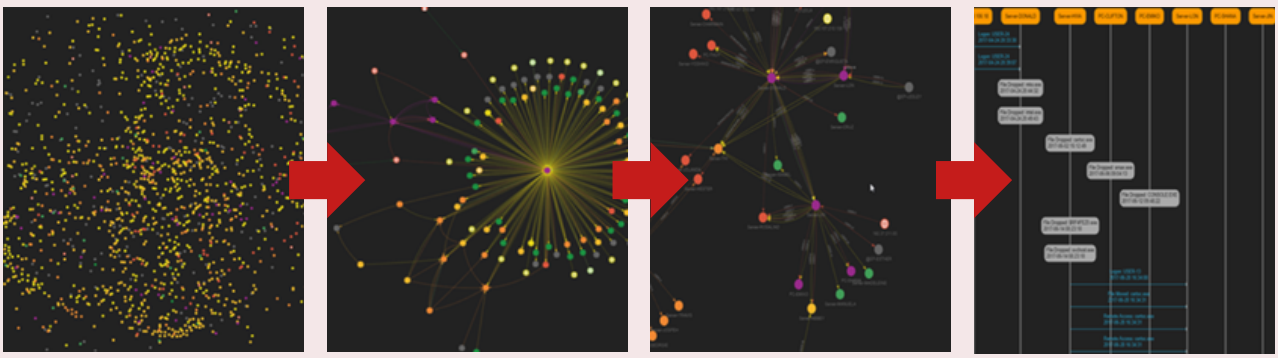
The engagement transformed the organization's cybersecurity posture:

- Minimized operational downtime and project disruption
- Improved resilience against future ransomware attacks
- Enabled continuous monitoring and faster response
- Reduced dependency on limited internal resources

Most importantly, the organization shifted from a reactive security posture to a proactive defense model.

The Power of Cybots AI Engine

Visualisation	Automation	Response
Visibility (5-in-one Sensors)	Corelation (More alerts)	Storyline (Impact/To-Do)



Time Savings From Months & Days to Minutes