CYBOTS

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

Cybots Cybersecurity Solutions

Case Study: Software Developer

Supply Chain Vulnerabilities and Intrusions

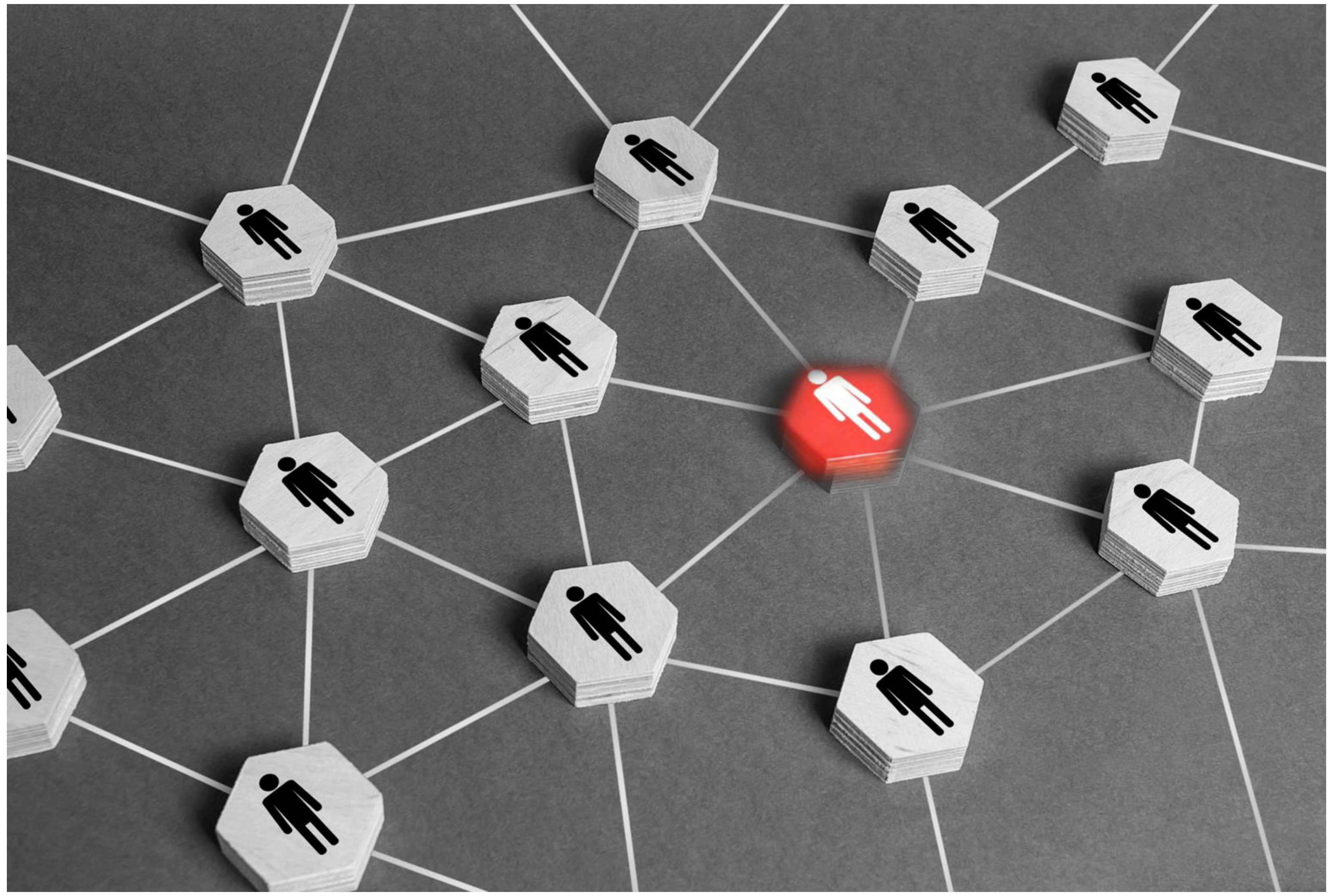
CYBOTS

INTRUSIONS

Software supply chain weaknesses have become pervasive. According to a global survey into third-party cyber risk management. 97% of firms have been negatively impacted by a supply chain cybersecurity breach.

Recent high profile supply chain beaches include Solarwinds and Kaseya.

https://cybotsai.com/what-is-kaseya-attack/



VULNERABILITIES

Unintentional insider failures/vulnerabilities

Supply Chain

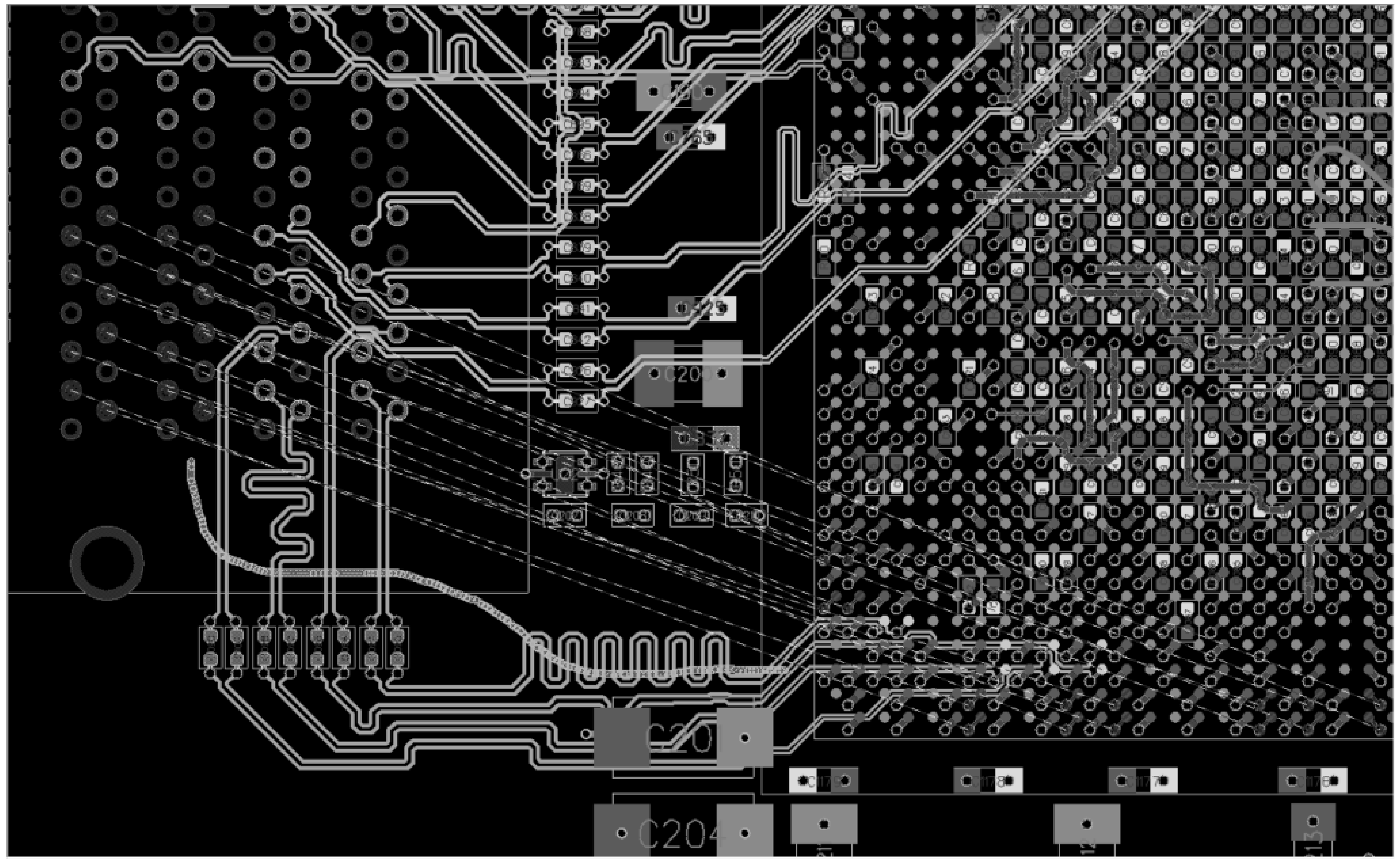
Gaps in technology

Gaps in Expertise

Why are Software Developers Targeted?

- Huge database of sensitive customer data.
- Compromised software can be used as a backdoor to spread attacks to the company's clients and penetrate unsuspecting victims.

Case Study – Software Developer in Asia



A Malaysian Software Developer was hit by Ransomware and wanted to use Cybots Solutions to generate an Incident Response.
The Customer was looking for an Incident Response Plan for identification and eradication.

Deployment across 1500+ machines in 8 days

AI-Powered investigation produced a thorough Incident Response Plan.

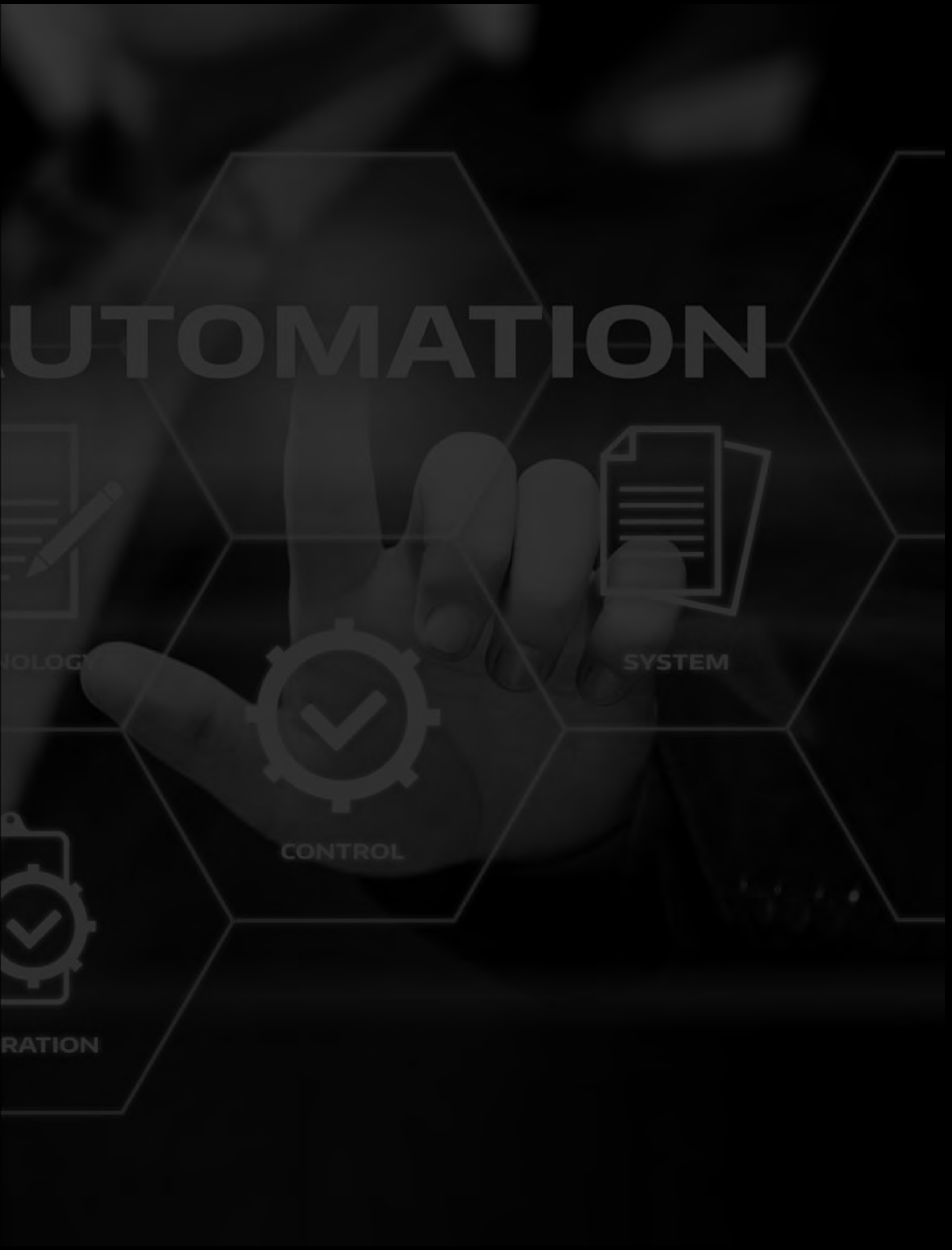
AI-Powered Forensics is fast, efficient and produces accurate actionable insights.

Noteworthy points

Cybots generated an Incident Response Plan and provided MDR services for 30 days.

- Cybots deployed AI-enabled agents across 1,500+ machines in 8 days.
- AI identified 7 infected machines including 2 machines which were not installed with our AI agents.
- The AI-enabled Incident Response Plan was generated in 1 day.

Implementation and Conclusion



OUR ROLE

Cybots was engaged to provide an Incident Response to a Ransomware intrusion. The environment included approximately 1,900 endpoints. Cybots was also engaged to provide MDR services for 30 days.

The identification of infected machines from a pool of 1,500 endpoints was completed within 8 days. Thereafter, the Incident Report Plan was generated in 1 day. This was only possible with AI-enabled systems. The deployment of AI-enabled Cybots Solutions reduced the time this task would normally take to 9 days from 6 to 8 weeks.

This highlights the speed and accuracy with which Cybots AI-driven solutions are able to pinpoint infected machines.

OUR RESULT

The engagement of Cybots yielded the desired outcome by:

- completing the identification of infected machines from a pool of 1,900 endpoints in a timely manner.
- providing MDR services for the stipulated amount of time.
- completing the engagement within stipulated budget.

CYBOTS

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

OUR SUITE OF SOLUTIONS

- Advanced Managed Detection and Response (AMDR) Services
- Compromise Assessment Services
- Incident Response and Fast Forensic Services
- Threat Intelligence
- RiskInt

TURNKEY CYBERSECURITY SERVICES (ON REQUEST)

- Next-Generation SOC
- 24x7 Managed Security Services
- Security Consulting Services
- Security Testing Services
- Security Device Maintenance

OUR AWARDS

Gold Winner - Advanced Persistent Threat (APT) Protection
Gold Winner - Endpoint Detection and Response (EDR) **Gold Winner** - AWS Cloud Security
Gold Winner - Artificial Intelligence Security **Gold Winner** - Cyber Threat Intelligence (CTI) **Gold Winner** - Critical Infrastructure (CI) Security **Gold Winner** - Cybersecurity Audit

CONTACT US

The Cybots team is here to be your cybersecurity partner throughout your cyber defense journey.

CYBOTS PTE LTD (Headquarters)
60 Paya Lebar Road, Paya Lebar Square,
#13-08, Singapore 409051

cybotsAI.com   contactus@cybotsAI.com

CYBOTS Powered By CYCRAFT