



# ai circus

## The Greatest Risk on Earth

Hosted by: Cysec Bridge

In Partnership with: IAMSECURE & Cynet

Guest: Ryan van de Coolwijk (ITOO)



IAM SECURE

powered by  
cynet

Hosted by:



Powered by: 

In Partnership:

**IAM**

**SECURE**

powered by  
 **cynet**



**Claude Oosthuizen**

CEO  
CySec Bridge



**Ryan van de Coolwijk**

Managing Executive  
iTOO Special Risks



**Shane Visscher**

CEO  
IAMSECURE



**Ben Gold**

Security Engineer  
Cynet



ai circus  
Taming Lions  
Shadow AI



Powered by:  VNO

# There Are Giant Shifts Happening in Cybersecurity



Attackers Have  
Shifted Down  
Market.

43%

43% of all cyberattacks now target SMBs, and 88% of ransomware impacts small and mid-sized companies, not large enterprises.



Security Spend  
has Shifted to  
the SMB.

\$109B

SMBs will spend \$109 billion on cybersecurity by 2026, representing nearly 60% of total global security spend.



AI-Driven Attacks are  
Shifting the Threat  
Landscape

87%

AI-driven attacks now affect more than 87% of businesses. Reactive point tools are no longer enough to keep up with AI-driven threats.

# The Full Scope of Exposure

*Why protection needs to evolve*



# ai circus

## Send in the Clowns

### AI Threat Actors



# #1 AI Kill Chain

## Background

A regional financial services firm with ~250 employees relied on AI-powered tools to boost customer communications and internal productivity. Their lean security team ran **email filtering**, **MFA**, and **endpoint antivirus** as separate, disconnected controls, each managed on its own.

### Incident summary:

An AI-crafted **phishing email** slipped past filtering and lured an employee to an AI-generated **fake login page** that harvested their credentials. Using those credentials, the attacker's AI defeated MFA through **real-time session hijacking** and took over the identity. From that trusted account it quietly deployed AI-mutated, **signature-less malware** onto the user's endpoint, chaining email, identity, and endpoint into one seamless intrusion.

### Detection and response:

Each control saw only **a piece of the attack**: the email gateway logged a delivered message, the identity provider logged a valid login, and the endpoint tool logged an unknown but low-priority process. Because the email, identity, and endpoint alerts were **never correlated**, the full attack chain went unnoticed until data was already being exfiltrated.

## Lessons Learned



**AI now blends email, identity, and endpoint into a single, fast-moving attack chain. Siloed tools each see one harmless-looking step and miss the whole. Organizations need unified detection that correlates signals across email, identity, and endpoint in real time, not isolated point products.**

# #2 AI Cloud Phantom

## Background

A fast-scaling technology company ran most of its operations across **SaaS and cloud platforms, with a next-generation firewall** guarding the network perimeter and **antivirus** on every endpoint. Its lean security team watched cloud app logs, firewall logs, and endpoint alerts in three separate, disconnected consoles.

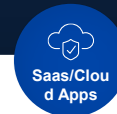
### Incident summary:

Attackers used AI to weaponize a **stolen OAuth token** and quietly sign into the company's SaaS and cloud environment, blending in with **normal user activity**. From a compromised cloud workload, AI-guided tooling probed the network and shaped its traffic to **mimic authorized services**, so the firewall logs recorded nothing out of the ordinary. It then pushed a lightweight, **AI-obfuscated payload** down to an endpoint to establish **persistence**, moving fluidly across SaaS/cloud, network, and endpoint.

### Detection and response:

Each layer held a clue in isolation: the SaaS logs showed an atypical login location, the firewall logs showed a faint spike in outbound traffic, and the endpoint flagged an unsigned process. None crossed a threshold on its own, and because cloud, network, and endpoint telemetry lived in separate tools, no one connected them until data was already leaving the cloud environment.

## Lessons Learned



AI lets attackers move quietly across SaaS & cloud, the network, and endpoints, keeping each footprint below the alert threshold. Reviewing cloud, firewall, and endpoint logs in isolation guarantees blind spots. Defenders need unified detection that correlates SaaS/cloud activity, network firewall logs, and endpoint signals into a single picture.



# ai circus

## High-wire no Net

### AI Evolution



Powered by:  VNO

# Use Case: Threat Actors + AI

Speed is the New Perimeter

1

## Reconnaissance & Credential Discovery *The AI Accelerator*

Attackers use LLMs and automated AI tools to scan public repositories, cloud buckets, and dark web dumps at scale to find exposed credentials or API keys instantly.

2

## Initial Access & Validation *The Velocity Trap*

High-velocity, automated botnets test validated credentials seconds after they are leaked. Traditional humans can't react in seconds.

3

## Lateral Movement & Execution *The Behavior Blindspot*

Compromised AI agents or service accounts carry out dynamic, context-dependent actions. Because they are designed to act autonomously, their malicious behavior is incredibly difficult to baseline or catch with legacy, rule-based systems.

**Key Takeaway:** AI isn't just inventing entirely new attacks; it is radically accelerating execution speeds across the existing attack chain. The window from vulnerability disclosure or credential leak to full exploitation has dramatically shrunk.

# Our AI SOC Method

## AI + HUMANS IN THE LOOP

Humans & AI make each other better. Years of our SOC insights power AI. AI amplifies human expertise.

Agentic SOC's miss the human element, most AI SOC's never close the loop.

**Speed + Efficacy:**

AI handles the **volume**.

Humans add the **value**.

The loop drives the **velocity**.



# Proven Performance

## Loved by Customers, Validated by Analysts.

*Technical, Real-World + Customer Feedback*

**GIGAOM**

**GigaOm**

*XDR Radar v5,  
2026*

Leader  
Outperformer

**MITRE**

**MITRE ATT&CK**

*2023 / 2024 /  
2025*

100% Detection, Protection,  
and Technique-Level  
coverage and **zero false  
positives** for  
3 Consecutive Years

**Gartner**  
Peer Insights™

**Gartner Peer Insights**

*XDR + EPP,  
2025-2026*

Strong Performer  
4.7/5 | 95% Recommend



**G2**

*Among highest in customer  
satisfaction - 2026*

Leader in UEBA, Incident  
Response, XDR, MDR,  
SIEM, EDR, System  
Security, Cloud Security

*Our platform is powered by Cynet who is independently recognized across major evaluation frameworks.*

# ai circus

## Balancing Act

### CapEx v OpEx



Powered by:  VNO

# IAM SECURE Managed Security

*Every Threat Vector, Covered.*



## Endpoint

- NextGen Antivirus (AI)
- Ransomware Protection
- Exploit Protection
- Malware Protection
- Credential, Files, Documents Protection
- Device Control
- Endpoint Detection & Response
- Full Endpoint Visibility
- Endpoint Security Posture Management
- Windows Event Visibility
- Secure Remote Shell



## Network

- Network Visibility
- Domain & Phishing Filtering
- Network Scan Detection
- Web Threat Protection
- Web Content Filtering
- DNS Attack Protection
- Tunneling & Exfiltration Detection
- External Attack Surface Management
- Network Anomaly Detection



## Identity & User

- Identity Threat Detection and Response (ITDR)
- Credential Theft Protection
- User Activity Visibility
- Lateral Movement Detection
- User Behavior Anomaly Detection
- Deceptive Users



## SaaS & Cloud Apps

- Security Misconfiguration Detection & Remediation
- Compliance Management
- Reports & Notifications
- Cloud Users & Resource Inventory
- SaaS & Cloud User Behavior Anomaly Detection



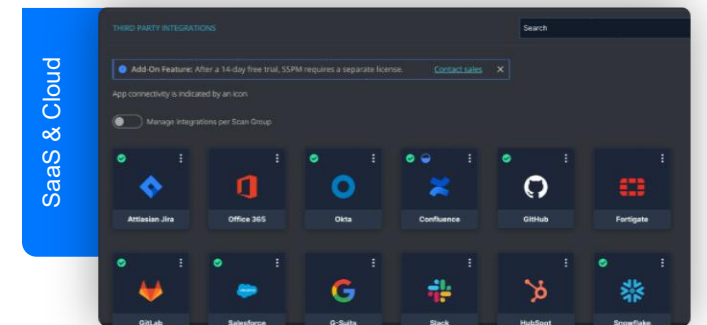
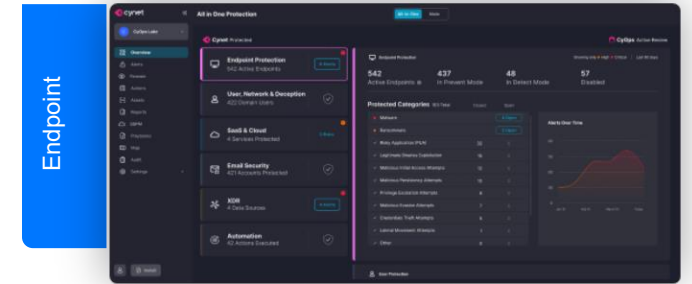
## Mobile

- Device, Network, App & Phishing Threat Detection
- On-Device Remediation
- Mobile App Risk Detection & Mitigation
- iOS, Android & Chrome OS Devices



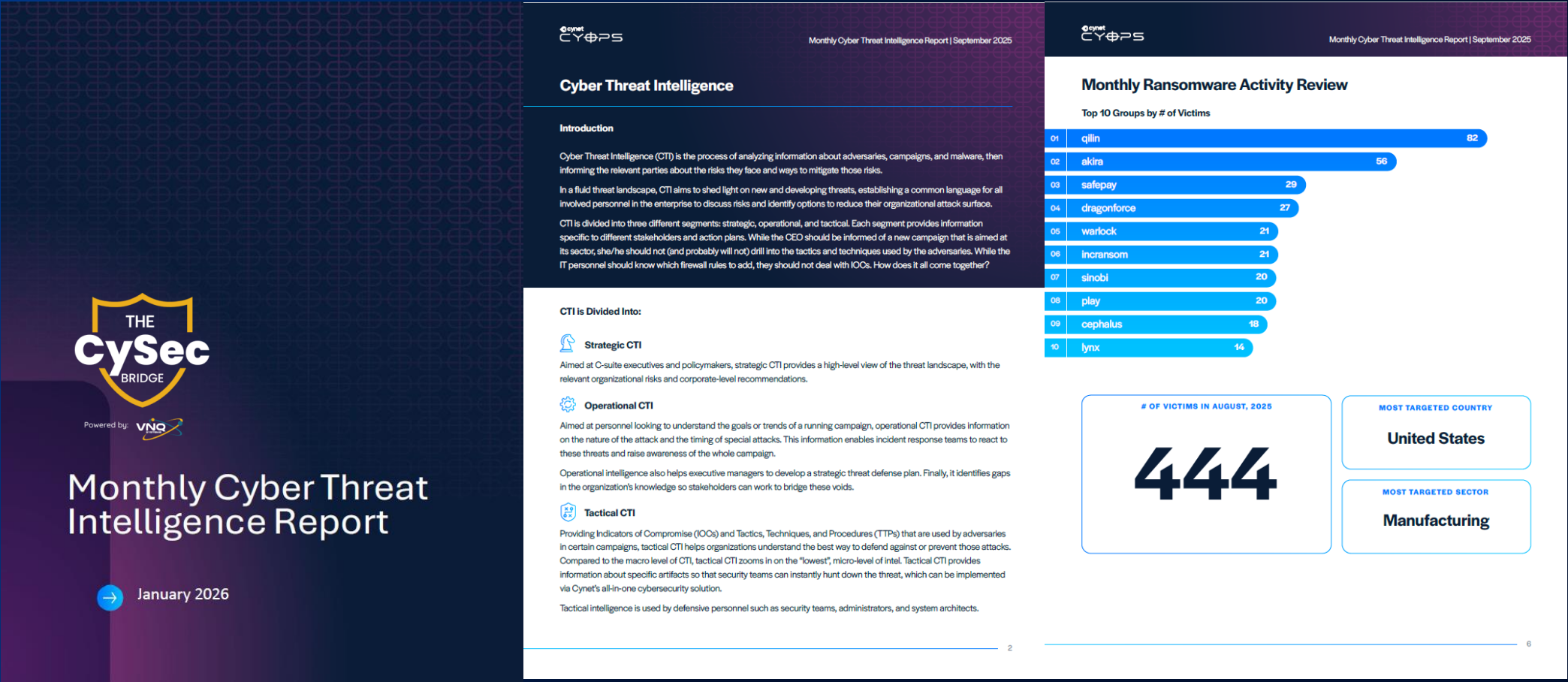
## Email

- Integration with Office 365 + Google
- Phishing Prevention
- Malware Prevention
- Exploit Prevention
- Unauthorized Senders Management
- Block Malicious File Extensions
- Safe URLs



# Threat Intel Report

Learn more about the latest cyber threats impacting organizations of all sizes



# AI Handles the **Volume**

## STOPPING THREATS AT SCALE

Advanced  
Threats

**97%**

Of threats  
identified  
autonomously by  
our SOC &  
behavioral analysis

Automatic  
Remediation

**90%**

Of threats  
remediated  
automatically. No  
human intervention  
required

Detection to full  
Containment

**<1s**

Milliseconds –  
seconds from  
detection to full  
containment

**500,000+ events analyzed daily** across global customer environments.

# Humans Bring the **Value**

EXPERT HUMAN OVERSIGHT, CONSISTENT FEEDBACK LOOP

Analyst Force  
Multiplier

**1:100K**

our SOC security experts combined with autonomous detection drives industry-best 1:100K analyst-to-endpoint efficiency.

AI Speed, Human  
Assurance

**9000**

# of confirmed incidents our SOC handles monthly.

Faster than the  
Adversary

**<5m** **<10m**  
MTTD MTTR

Sub-5 minute detection, sub-10 minute response, that's accelerated by our AI and our SOC.

**500,000+ events analyzed daily** across global customer environments

# Q&A

**IAM** **SECURE**



# THANK YOU

**IAM** **SECURE**

