



TI Enriched, AI Empowered

Threat Detection and Response

Level Up Your Cyber Defenses

February 2025

ABOUT SECAI

SecAI is an innovative threat intelligence enriched, and AI-powered company aiming at cyber threat detection and response. We leverage deep research into adversary tactics, techniques and procedures, accelerate enterprise transformation from reactive defense to empowered SecOps. Our smarter, faster and more effective cybersecurity solutions deliver unprecedented efficiency in threat response, streamlining complexity and bolstering your overall security posture.

AI Empowered

Cutting Edge Generative AI for Security

We provide reliable actionable insights backed by a fine-tuned Gen-AI model and comprehensive global TI repositories to help SecOps team stay ahead of cyberattacks.

10k+

Data Sources

<20s

Threat Report Generating

70%*

Faster MTTI

TI Enriched

Industry Leading Threat Intelligence

We pioneer new approaches to deliver high-fidelity, efficient and actionable threat intelligence.

99.9%

CTI Accuracy

10B+

Threat Entities

200+

APT Groups Being Tracked

“ Elevate Your Security Operations with **TI** and **AI**. ”

* The result is based on extensive cases vs. traditional manual analysis.

SECAI PLATFORM

Threat Detection and Response

SecAI Investigator

Uplevel your SecOps team

SecAI Intelligence

Know your adversary

SecAI DRPS

Protect your brand against phishing

SecAI NDR

Discover real threats

“Intelligence” Will Make A Difference

Actionable Insights

Get comprehensive visibility and instant analysis from the perspectives of attacker to prioritize critical risks and threats with rich context.

Accurate Detection

Accurately identify compromised hosts and emerging threats from massive incident alerts, including zero-day exploits and APT attacks.

Efficient Operation

Simplify security investigation and streamline incident response to save time and boost ROI in security operations.

SecAI Investigator

Unleash the power of AI-driven security productivity

SecAI Investigator is a cybersecurity analysis assistant empower your security team to achieve breakthrough efficiency with cutting-edge AI. Leveraging a global threat intelligence repository, SecAI Investigator analyzes security data to deliver actionable insights, accelerating incident investigation and remediation. Automate routine tasks, freeing analysts to focus on strategic initiatives.



Key Capabilities

Pinpoint Threats with Precision



Gain clear verdicts and comprehensive context from our AI-powered threat intelligence analysis and attribution.

Actionable Insights from Logs & Scripts



Uncover hidden threat behavior and gain valuable insights to take decisive action.

Proactive Threat Actor Tracking



Track threat actors and CVEs across the web in real-time, allowing you to generate detailed threat reports and stay ahead of attacks.

Get Instant Cybersecurity Answers



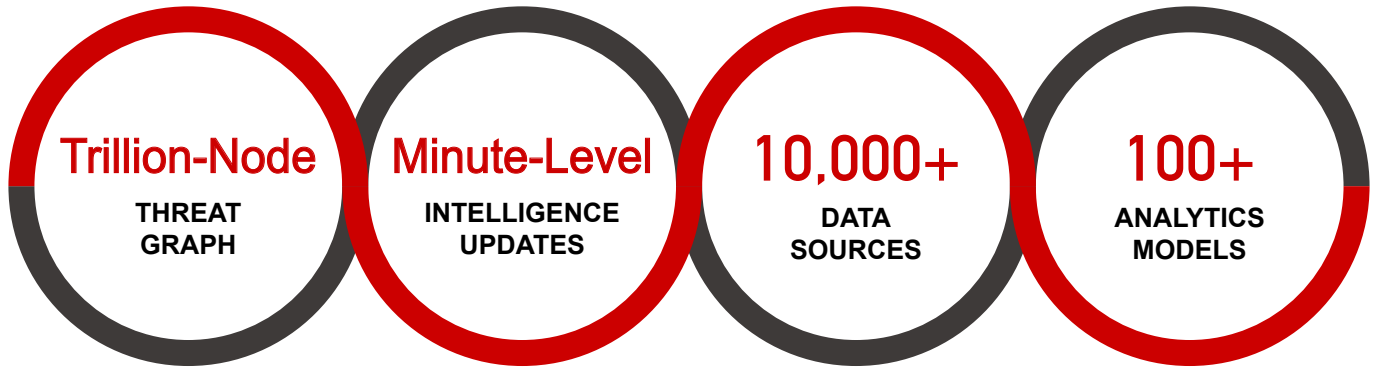
Engage with our AI for any cybersecurity-related questions and receive accurate, detailed answers.

Log in to our website to experience cutting-edge cybersecurity AI for free!

Web: <https://i.secai.ai> >>

SecAI Investigator

Unleash the power of AI-driven security productivity



Real-Time Data

Leverage real-time data and built-in intelligence to provide the most up-to-date threat information.

Open Platform

No vendor lock-in and supports open data standards.

Free to Use

SecAI Investigator is currently free to all users.

**Accelerate
Analysis**

**Enhance
SecOps**

**Boost
Productivity**

“ Saving up to 70% of the time needed for investigation. ”

SecAI Intelligence

Focusing on what is essential to achieve more

SecAI Intelligence provides full-coverage, high-fidelity, rich context and up-to-date threat intelligence API services dedicated to helping SecOps teams to work more efficiently on compromise detection and alert noise reduction.

Key Capabilities

Threat Analysis Enhancement

Detect suspicious events by extracting domains or IP addresses from logs collected by SOC or SIEM for analysis, enhancing the capabilities of threat detection, discovery, and analysis.



IP Reputation Identification

Not only provide the capability to accurately identify whether the suspicious IP is a risk of scanning, vulnerability exploitation, botnet, etc., but also further attribute itself, such as gateway, IDC, CDN, etc., better conforming with your business to respond to threats.



Malware Analysis

The Cloud Sandbox analysis makes it easier to detect trojans and identify malicious behaviors from the office terminals, Web/FTP/email attachments, and URLs.



Compromised Assets Detection

Accurately detect the threats of office terminals and servers in production network or DMZ that may have been compromised due to coin mining, ransomware, backdoor, and APT attacks, and offer sample forensic information and response suggestions, helping enterprises to quickly respond to threats.



Enterprise Assets Discovery

Quickly discover hidden assets and monitor their changes with the extension of domains and IP addresses, help to reduce attack surface and minimize risks of data leakage and service exposure.

SecAI Intelligence

Focusing on what is essential to achieve more

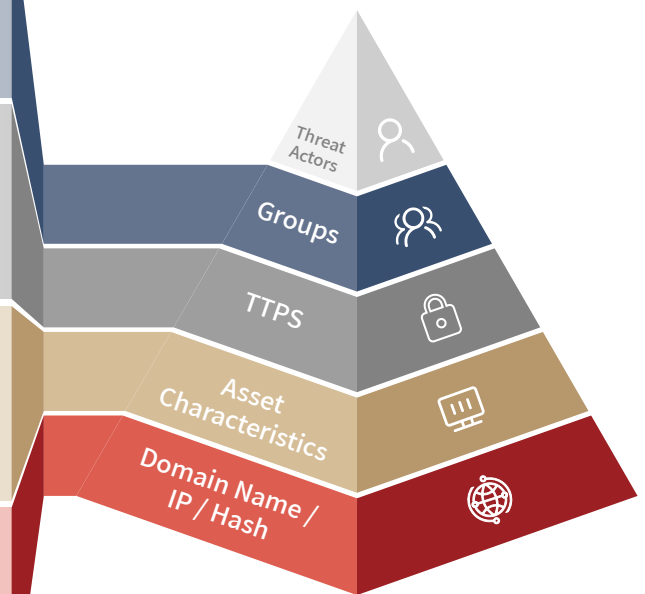
Advantages

- **APT Groups:** 200+ APT groups are being tracked.
- **Threat Profiles:** Collection of tens of millions of threat profiles related to IP attacks and vulnerabilities.

- **Attack Events:** Analysis of tens of thousands of attack events.
- **Attack Tools:** Analysis of more than 1000+ tools used by attackers.

- **IOA:** Tens of thousands IOA intelligence.
- **Yara:** Collection of thousands of Yara rules.
- **C2:** Millions of high credible C2 intelligence.

- **IOC:** Millions of high-fidelity IOC intelligence.
- **Domain Data:** Millions of domain names daily updated.
- **IP Reputation:** 4.2 billion IPv4 and tens of thousands of IPv6 reputation.



High-Fidelity

Full-Coverage

Rich Context

“ Mitigate cybersecurity alert fatigue, accurately. ”

SecAI DRPS

Protect your brand against phishing and impersonation

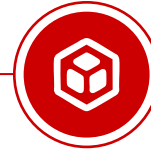
SecAI Digital Risk Protection Service (DRPS) offers anti-phishing and anti-fraud solutions powered by big data and AI, proactively detect and mitigate potential brand threats across digital channels.

Key Capabilities



Domain Monitoring

Proactively detect and mitigate typo squatting, suspicious domains, and phishing attacks.



Application Protection

Detect and take down fake applications to remove any brand infringements instantly.



Social Media Protection

Monitor and protect against impersonation and scam attempts across all major social media platforms.



Counterfeit Hotline Detection

Protect your customers from fraudulent customer service hotlines through timely detection and removal.

SecAI DRPS

Protect your brand against phishing and impersonation

Advantages

Highly Reliable Service With A Strong SLA

SecAI DRPS delivers comprehensive services backed by robust Service Level Agreements (SLAs). Our expert team provides real-time monitoring and rapid response, protecting your brand reputation against phishing and fraud.



SLA:

- Monitoring Services: **24/7**
- Emergency Services: **24/7**
- Routine Services: **10/7**
- Initial response within **2 hours** of phishing detection
- Action initiated within **30 minutes** after customer confirmation

Average Takedown Time:

- Phishing websites and apps: **48 hours** globally
- Phishing accounts and calls: **72 hours** globally

Detect and Stop Phishing Scams Instantly

Advanced Technology

Our AI-powered platform utilizes advanced algorithms, including search-based discovery and reverse lookup, to proactively detect and prevent phishing, impersonation and scams.

Dedicated Team

Our in-house team has established strong partnerships with domain registrars, DNS providers, hosting companies, app stores, and cloud storage providers, ensuring swift and effective remediation.

Unparalleled ROI

We provide the most competitive takedown quotas within your budget, tailored to address the high volume of phishing attacks and providing exceptional value.

SecAI NDR

Be confident above the rising cyberattacks

SecAI NDR provides the most effective network security capabilities with high-fidelity detection on sophisticated attacks and automated response with a low false positive rate of less than 0.03% and a high zero-day detection rate of over 81%.

Key Capabilities

Risk Prevention

- **Comprehensive Visibility**
Get real-time visibility into the network, including ports, services, applications and domains.
- **Attack Surface Reduction**
Identify critical risks across newly launched applications, public entries, login portals, cloud services and APIs.
- **Customizable Asset Risk Monitoring**
Achieve flexible and centralized risk management based on the specific needs of the SecOps teams.

Accurate Detection

- **Zero-day Threats Detection**
Accurately detect generic zero-day exploits as well as file-based zero-day vulnerabilities.
- **Compromised Hosts Detection**
Accurately identify compromised hosts by uniting rule based analytics with high-fidelity IOC intelligence.
- **Alert Noise Reduction**
Reveal the most critical threats with powerful analytics of in-progress attacks.

Real-time Analysis

- **Attack Path Analysis**
Aggregate events in a timeline intelligently to clearly sort out hacker attack paths.
- **Multidimensional Analysis**
Conduct a comprehensive analysis of threats from attacker's and defender's perspective.
- **Attacker Profiling**
Analyze and extract patterns of attack behavior automatically to build attacker profiles.

Automated Response

- **TCP Reset Blocking**
Realize high TCP reset blocking rate by using the TCP session mechanism.
- **Firewall Blocking**
Integrate seamlessly with firewall, configure the firewall blocking policy through SecAI NDR in real-time.

<0.03%*

FALSE POSITIVE
RATE

>81%*

ZERO-DAY
DETECTION RATE

<3%*

UNDERREPORTING
RATE

99%*

TCP RESET
BLOCKING RATE

* Results are based on statistical analysis of SecAI customer use cases in 2024.

SecAI NDR

Be confident above the rising cyberattacks

Advantages

Ease of Deployment

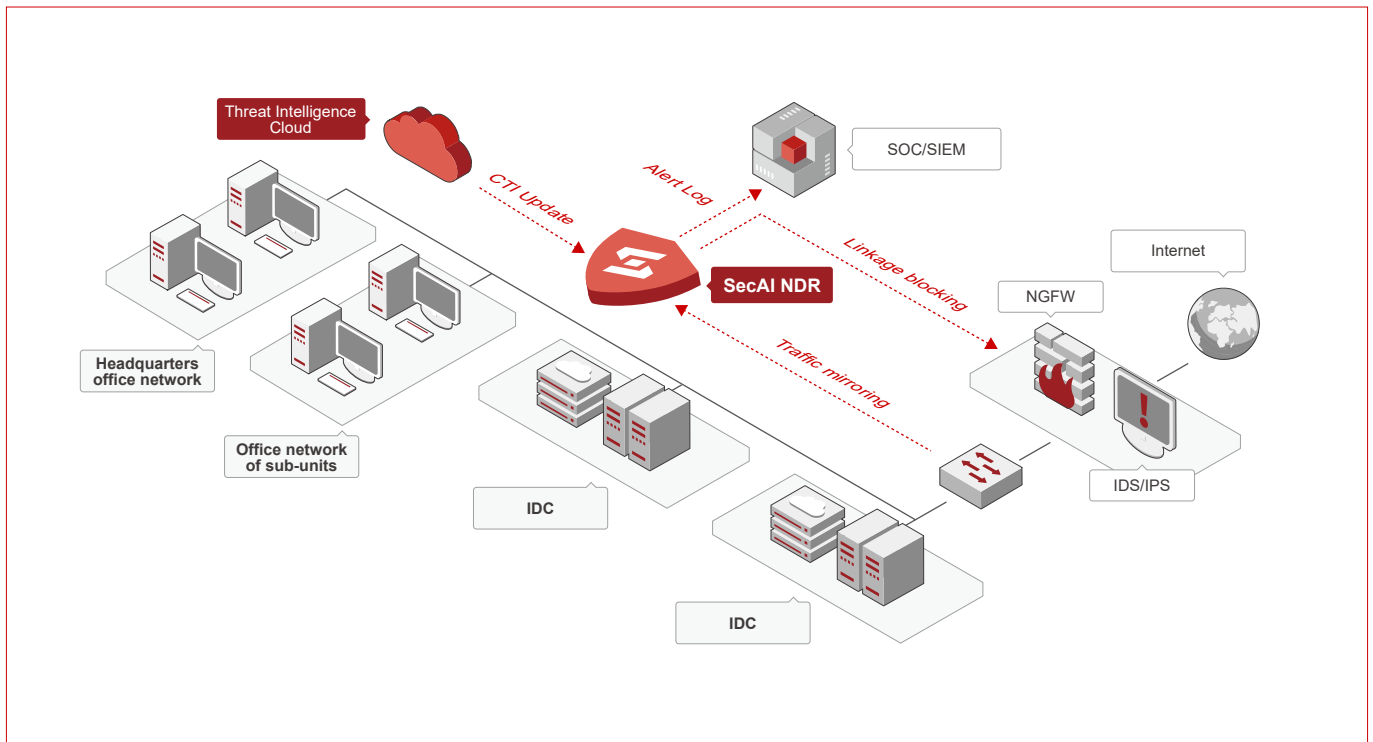
Can be deployed on your own infrastructure and comply with any compliance and data privacy requirements.

High Accuracy of Detection

Achieve high detection accuracy by leveraging high-fidelity threat intelligence combined with AI detection models to reduce alert noise efficiently.

Response Instantly

Integrate seamlessly with firewall, XDR and SIEM/SOAR of major international solutions including Palo Alto, CrowdStrike, CISCO, Check Point, FortiGate, etc.



“ See and stop advanced cyber attacks faster. ”



12 Marina View, Asia Square Tower 2 #11-01, Singapore 018961
contactus@secai.ai
<https://www.secai.ai>