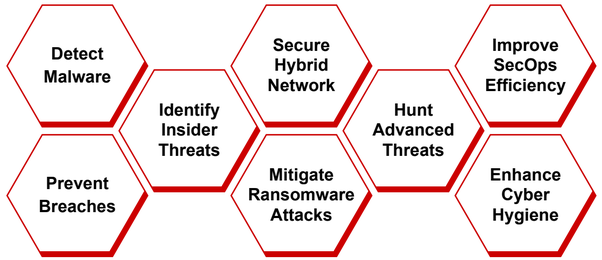
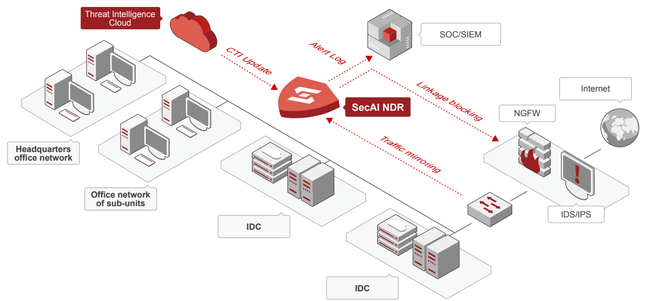
COMPREHENSIVE USE CASES

SecAI NDR enhances threat visibility, accelerates detection and response, and reduces SecOps burden across your entire hybrid attack surface.



EASE OF DEPLOYMENT

SecAI NDR can be deployed on-premises to meet specific compliance and data privacy needs.



WHY SECAI NDR

More Secure

- >81% Zero-day Detection
- >96% HTTP-based Cobalt Strike Attack Detection
- <3% Underreporting Rate

More Effective

- <0.03% False Positive Rate
- 85% Reduction in SecOps Workload
- 2.5x Faster SecOps Productivity

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

SecAI | INFOCOMM MEDIA DEVELOPMENT AUTHORITY | SPARK

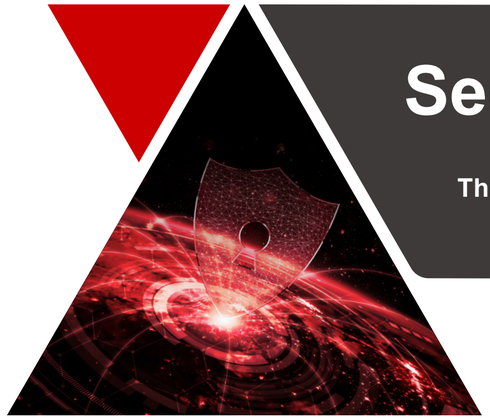
SecAI is an innovative threat intelligence-driven, and AI-powered company aiming at cyber threat detection and response. We leverage deep research into adversary tactics, techniques and procedures, accelerate enterprise transformation from reactive defense to empowered SecOps. Our smarter, faster and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

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

SecAI

SecAI NDR

See and Stop Threats that Matter Most with TI and AI



SecAI NDR provides the most effective network security capabilities with TI (threat intelligence) and AI to accurately detect sophisticated attacks and automate response actions.

KEY BENEFITS

- Mitigate Alert Fatigue
- Prevent Unknown Threats
- Reduce Attack Surface
- Speed Up Response

KEY CAPABILITIES

RISK PREVENTION

- **Asset Inventory**
  Automatically identify assets based on traffic monitoring, including domain and IP relationships, web applications and frameworks, etc.
- **Attack Surface Reduction**
  Identify critical risks across login portals, weak passwords, sensitive information, file downloads, API interface and upload interface, etc.
- **Custom Asset Risk Monitoring**
  Enable personalized monitoring of user-defined risk scenarios and unified alerts on a single dashboard.

ACCURATE DETECTION

- **Compromised Hosts Detection**
  Accurately identify compromised hosts by uniting rule based analytics with high-fidelity IOC intelligence.
- **Attack Result Determination**
  Automatically determine the success or failure of each attack and the severity level.
- **Zero-day Vulnerability Detection**
  Accurately detect high-risk zero-day vulnerabilities and provide a dedicated page for real-time zero-day threat visibility.

REAL-TIME ANALYSIS

- **Intelligent Aggregation**
  Aggregate scattered alerts into complete threat incidents from the perspective of the attacker over a timeline.
- **Multidimensional Investigation**
  Threat events are visually analyzed from the perspectives of alert hosts, external attacks and intranet incidents.
- **Attacker Analysis**
  Comprehensive analysis of attacker profiles through threat intelligence, historical attack behavior, and cloud-shared data for attack IPs.

AUTOMATED RESPONSE

- **TCP Reset Blocking**
  Disrupt network connections between compromised hosts and attackers by using TCP protocol without altering network topology.
- **Firewall Integration**
  Integrate seamlessly with third-party firewall devices to block network threats instantly.

High Accuracy and Comprehensiveness

By seamlessly integrating three detection engines, SecAI NDR can filter out noise, identify high-risk behaviors, and provide in-depth contextual analysis for suspected attacks, enabling you to focus on real threats.

Real-time Engine	Asynchronous Engine	AI Engine
Instant alerts on high-risk behaviors	Correlation analysis across contexts	Efficient analysis by over 200 AI models

Threat Intelligence

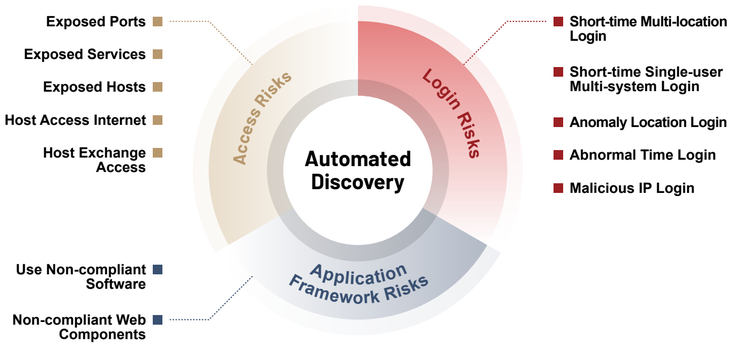
Identify Advanced Threats Faster

Leveraging high-quality threat intelligence, machine learning models, rule-based feature recognition, and dynamic file analysis engines, SecAI NDR offers comprehensive detection capabilities that cover all phases of the kill chain and most of the MITRE ATT&CK techniques that are relevant to network traffic.

Reconnaissance	Weaponization	Exploitation	Installation	Command & Control	Exfiltration	Impact
Goby Scans	Email Sending	WebLogic Deserialization Vulnerability	Behinder Webshell	Webshell Trojan	FRP	Data Theft
Email Addresses Collection					Windows Vulnerabilities	
Spear Phishing Emails		Office Vulnerabilities	PowerShell	C&C: ***.windows update.top	Over Pass the Hash	Ransomware

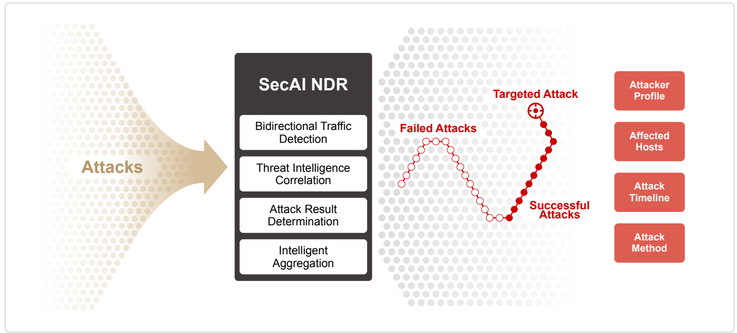
Prevent Asset Risks One Step Ahead

Unlike other NDR providers that simply identify assets, SecAI NDR goes a step further by mapping the entire attack surface. This unique capability allows SecAI NDR to proactively detect risks in login portals, upload interfaces, and APIs, providing unparalleled protection.



Prioritize the Most Severe Threats

SecAI NDR can accurately analyze attack intent, identify targeted threats and automatically determine the success or failure of each attack and adjust the severity level. By aggregating scattered alerts into complete threat incidents, SecAI NDR provides a visual overview of the overall attack landscape. The SecOps team can concentrate their efforts on the highest priority threats.



Stop the Threats Instantly

SecAI NDR can disrupt malicious connections by using TCP reset blocking or seamlessly integrating with leading firewalls, XDR, and SIEM/SOAR solutions.

TCP Reset Blocking

99%

BLOCKING RATE

Firewall Integration

paloalto NETWORKS · CROWDSTRIKE · CHECK POINT · SONICWALL · CISCO · FORTINET