THREATHUNTER.AI

Our Hunt Teams
Have the Watch

24/7/365 threat hunting by expert analysts powered by AI. We find the threats that automated tools miss—before attackers cause damage.

Trusted for

19+ Years

Certified

SDVOSB

6M+

Daily Investigation Targets

8.3TB+

Data Ingested Daily

1M+

Realtime Intel Artifacts

830M+

Events Analyzed, Zero False Positives

What We Do

We provide 24/7 threat hunting services powered by the ARGOS platform. Human experts + AI/ML technology—not just automation.

Expert Threat Hunters

Our analysts think like attackers. They actively hunt for threats—not just wait for alerts.

AI-Powered Detection

Custom AI/ML tools like MILBERT and Ptolemy process millions of events to surface real threats.

Real-Time Response

Direct communication via Slack, Teams, email, or phone. Mitigation steps, not just alerts.

Explore the ARGOS PlatformLearn About Our Services

Business Outcomes

Real results from our AI-powered threat hunting platform. Measurable security improvements for your organization.

47,000+

Threats Detected

12,800+

Attacks Prevented

<2.3 min

Mean Detection Time

0%

False Positive Rate

Service Tiers

Choose the level of protection that fits your organization. All tiers include unlimited data sources and storage.

Hunt

24/7 human threat hunting with AI-powered detection and unlimited data ingestion.

SLA: 30 min critical / 120 min high

- 24/7 human threat hunting
- ARGOS AI detection engine
- LogWarden data collection
- Customer portal and dashboards
- Slack, Teams, and email alerting
- Unlimited log sources and storage

Get Started

Popular

Hunt + Respond

Active containment, incident response, and forensic support on top of continuous hunting.

SLA: 15 min critical / 30 min high / 120 min medium

- Everything in Hunt
- Active threat containment and isolation
- Incident response and remediation
- Priority escalation
- Forensic investigation support
- Weekly threat briefings

Get Started

Hunt + Respond + Manage

Full managed security with vCISO, compliance, and dedicated account management.

SLA: Custom / Dedicated account team

- Everything in Hunt + Respond
- vCISO program

- Compliance support and reporting
- Purple team exercise coordination
- Dedicated account management
- Executive threat briefings
- Custom integration and engineering

Get Started

Add What You Need

Extend any tier with specialized tools for identity protection, vulnerability management, attack path analysis, and threat intelligence.

Free Trial

MILBERT

AI-powered identity threat detection and response. Stops AiTM phishing, session hijacking, and MFA bypass in real time.

Learn more

TACT-IO

Vulnerability management with Real Risk Scoring. Surface the 5% of vulnerabilities that pose 95% of your risk.

Learn more

GEIGER

Attack path management across AD, Azure, AWS, GCP, Okta, and Kubernetes in one unified graph.

Learn more

Ptolemy:TEMPEST

Zero-hour threat intelligence feed. Curated, hourly-updated active threat data with automatic stale IOC removal.

Learn more

Full Comparison

All tiers include access to the ARGOS platform and customer portal.

Feature	Hunt	Hu
Detection & Monitoring		
24/7 human threat hunting		
ARGOS AI detection engine		
LogWarden data collection		
Unlimited log sources and storage		
Customer portal and dashboards		
Response & Remediation		
Active threat containment and isolation		
Incident response and remediation		
Priority escalation		
Forensic investigation support		
Managed Services		
vCISO program		
Compliance support and reporting		
Purple team exercise coordination		
Dedicated account management		
Custom integration and engineering		
Communication		
Slack, Teams, and email alerting		
Weekly threat briefings		
Executive threat briefings		
SLA		

Feature	Hunt	Hu
Response SLA	30/120 min	15/

Compare All Features

Meet MILBERT

The first agentic AI that stops attacks before they happen.

MILBERT is the industry's most advanced Identity Threat Detection and Response platform. Processing 218,000 authentication events per second with zero false positives, MILBERT detects attacks that bypass MFA, steal sessions, and compromise identities - stopping them before damage occurs.

218K

Events/Sec

0%

False Positives

830M+

Events Analyzed

Learn More About MILBERT

Frequently Asked Questions

What is managed threat hunting?

Managed threat hunting is a proactive cybersecurity service where expert analysts actively search your environment for threats that automated tools miss. Unlike reactive SIEM alerts, threat hunters develop hypotheses and investigate suspicious activity 24/7/365.

How is ThreatHunter.ai different from a SIEM or MDR?

SIEMs and MDR providers rely on rules and alerts. ThreatHunter.ai combines human hunters with AI tools like MILBERT to actively seek threats. We process data from unlimited sources, deliver zero false positives, and have been protecting organizations since 2007.

Do I need to replace my existing security tools?

No. ThreatHunter.ai integrates with your existing firewalls, EDR, Active Directory, Office 365, and cloud infrastructure. We work alongside your current security stack, enhancing its effectiveness.

How quickly can I get started?

Most clients are fully onboarded within days. Our LogWarden data collector connects to your existing infrastructure with no network changes required. We begin active hunting as soon as data flows.

From the Hunt Desk

What our team is seeing, stopping, and thinking about right now.

NewThreat Hunter's Guide

How to Detect and Defeat Mimikatz: 17 Detections You Can Deploy Today

Working KQL + OpenSearch queries mapped to MITRE ATT&CK. Covers the full attack surface most teams miss.

Get the Free Guide

Threat Intel

Infostealers Are the Biggest Story in Cybersecurity Right Now. Your MFA Will Not Save You.

Infostealer malware is everywhere — in Chrome extensions, WhatsApp, fake AI tools, and GitHub repos. Attackers are not breaking your MFA. They steal what comes after it. The target is the session.

February 16, 202622 min read

Threat Intel

America's Cyber Defense Agency Is Burning Down and Nobody's Coming to Put It Out

CISA lost a third of its staff and its acting leader uploaded sensitive docs to public ChatGPT — while China sits inside U.S. critical infrastructure.

February 13, 202614 min read

Threat Intel

A Love Letter That Broke the Internet: The ILOVEYOU Worm, 26 Years Later

The ILOVEYOU worm infected 50 million machines in 10 days. Full technical breakdown and why the same attack pattern still works today.

February 10, 202615 min read

See All Field NotesTalk to a Threat Hunter

Ready to Secure Your Organization?

Talk to our team to see how ThreatHunter.ai can protect your business with 24/7 expert threat hunting and AI-powered detection.

Get Started TodayCall 1.888.674.9001

Or email us at sales@threathunter.ai