How ThreatConnect Leverages AI

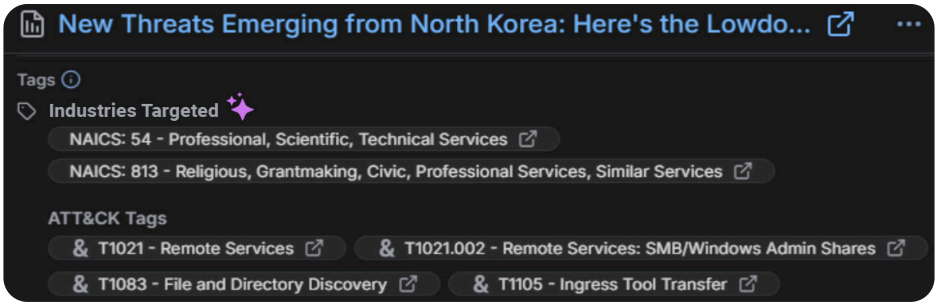
ThreatConnect.

Augmenting Cyber Defenders with Intelligence-Driven AI & Analytics

Practical AI for Cyber Defenders

AI is not a one-size-fits-all solution, especially in cybersecurity. Many vendors rush to market with AI branding but fail to deliver real, applicable value. Cyber defenders need AI solutions that enhance—not replace—their expertise, enabling them to make faster, smarter, and more informed decisions.

ThreatConnect takes a dynamic, use case-driven approach that fuses our dual, deep expertise in artificial intelligence (AI) and cyber threat intelligence (CTI). This powerful combination empowers solutions that optimize human effectiveness rather than seeking to replace skilled professionals. Our AI technology is deeply integrated into the ThreatConnect Ecosystem, supporting intelligence operations with automated decision support, classification, correlation, scoring, and summarization.



New Threats Emerging from North Korea: Here's the Lowdo...

Tags

Industries Targeted

- NAICS: 54 - Professional, Scientific, Technical Services
- NAICS: 813 - Religious, Grantmaking, Civic, Professional Services, Similar Services

ATT&CK Tags

- T1021 - Remote Services
- T1021.002 - Remote Services: SMB/Windows Admin Shares
- T1083 - File and Directory Discovery
- T1105 - Ingress Tool Transfer

Our AI read through this intelligence report and identified key insights on industries and TTPs. Now the information can be queried, summarized for reports, and cleanly aligned to intelligence requirements.

Built On: Big Data, Model Transparency, and Workflow Integration

- **2.5 billion** intelligence insights classified via AI combined with **one quarter trillion** data points help contextualize analyst workflows
- **4X** more ATT&CK Tactics and Techniques identified compared to traditional methods: more than any other vendor
- Natively embedded into security workflows, integrating with SIEMs, SOAR platforms, and analyst-driven intelligence operations

AI CREDIBILITY: NO BLACK BOXES

Built on transparent, explainable AI models with visibility into training data lineage, decision logic, and model accuracy.

ThreatConnect.

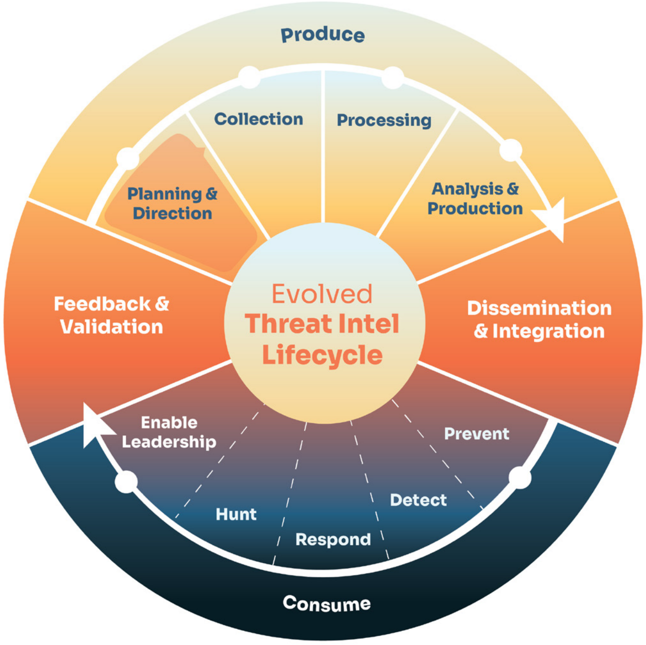
ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

AI-Driven Use Cases Aligned to the Evolved Threat Intelligence Lifecycle

ThreatConnect's AI solutions are built around three core AI capabilities:

- **Correlate:** Uncover meaningful relationships across vast datasets and CTI frameworks to improve prioritization, context, and decision-making
- **Classify:** Automatically tag, categorize, and contextualize threat intelligence to align with frameworks like MITRE ATT&CK.
- **Accelerate:** Reduce technical barriers to action through customizable automation and by distilling large volumes of intelligence, enabling teams to act faster



Those three capabilities are mapped to the **Evolved Threat Intelligence Lifecycle,** ensuring intelligence is relevant, actionable, and continuously refined.

Planning & Direction

- AI-powered insights guide **Intelligence Requirements** by ensuring that unstructured intelligence can be mapped to key priorities, such as industry and adversary tactics.

Collection

- Automated ingestion and classification of open-source, commercial, and community threat intelligence.

Processing

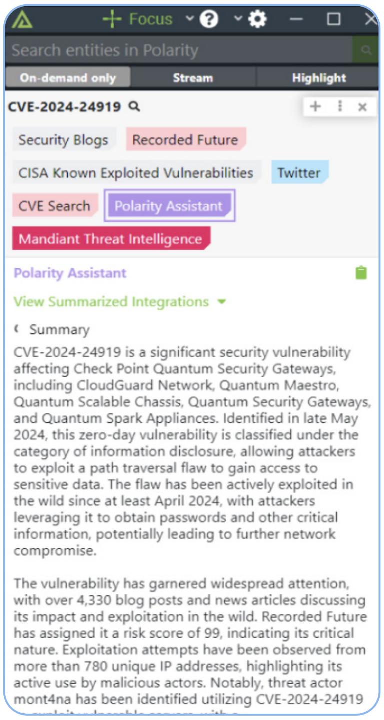
- AI-enabled **Indicator Classification** uses advanced ML models to distinguish suspected malicious from benign IOCs, improving prioritization and reducing false positives.
- AI-driven MITRE ATT&CK classification that performs X4 better than traditional methods at identifying TTPs.
- DGA Detection leverages deep learning models to classify domains, flagging those generated for malicious campaigns.
- AI-built on well-established taxonomies like MITRE ATT&CK, NAICS, and the ThreatConnect Data Model provide more actionable outputs based on industry best practices.

Analysis & Production

- **AI-driven Threat Library Summarization** automatically condenses intel reports into digestible insights.
- Finely tuned generative AI turns simple, plain-language inputs into complex queries so you can ask **deep, meaningful questions** of your data without needing to learn complicated query syntax

Dissemination & Integration

- Automated AI tagging structures intelligence for seamless integration into security workflows.



CVE-2024-24919 is a significant security vulnerability affecting Check Point Quantum Security Gateways, including CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, and Quantum Spark Appliances. Identified in late May 2024, this zero-day vulnerability is classified under the category of information disclosure, allowing attackers to exploit a path traversal flaw to gain access to sensitive data. The flaw has been actively exploited in the wild since at least April 2024, with attackers leveraging it to obtain passwords and other critical information, potentially leading to further network compromise.

The vulnerability has garnered widespread attention, with over 4,330 blog posts and news articles discussing its impact and exploitation in the wild. Recorded Future has assigned it a risk score of 99, indicating its critical nature. Exploitation attempts have been observed from more than 780 unique IP addresses, highlighting its active use by malicious actors. Notably, threat actor mont4na has been identified utilizing CVE-2024-24919

AI-generated summaries optimize reporting for leadership and operational teams in real time in any tool at the moment of decision and action

Prevention, Detection Response, and Executive Enablement

- AI-enhanced threat scoring ensures focus on the most impactful threats.
- AI-powered entity correlation connects seemingly unrelated events to detect emerging threats.
- We use Natural Language Processing (NLP) and various classifiers to gather and enrich data for risk modeling in order to help CISOs and other leaders make risk-informed prioritization decisions

Feedback & Validation

- AI, Supervised by Experts – Our AI team actively monitors AI models to ensure they deliver high-quality, relevant intelligence, adjusting them based on real-world threat trends and user feedback.
- We also know that - just like human-product intelligence - AI can make mistakes. That's why many of our AI features include built-in feedback mechanisms so we can listen to our users and align our accuracy more to your needs over time.

Why ThreatConnect AI?

ThreatConnect's AI capabilities are battle-tested and trusted by over 250 enterprises worldwide. Our AI solutions seamlessly integrate into existing security workflows, enhancing efficiency without disrupting operational processes. Whether it's classifying vast amounts of intelligence, filtering false positives, or providing actionable summaries, ThreatConnect AI ensures cybersecurity teams stay ahead of adversaries.

Learn More

Discover how ThreatConnect AI can transform your cyberdefense, please connect with us via chat on threatconnect.com, request a demo at threatconnect.com/request-a-demo, or email sales@threatconnect.com.

ABOUT THREATCONNECT

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. More than 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240