Know what matters.

Act first.

Recorded Future®

Generative AI: Use Cases for Attackers and Defenders

Agenda

AI Usage Today

Attacker Use Cases

Defender Use Cases

Outlook

TODAY

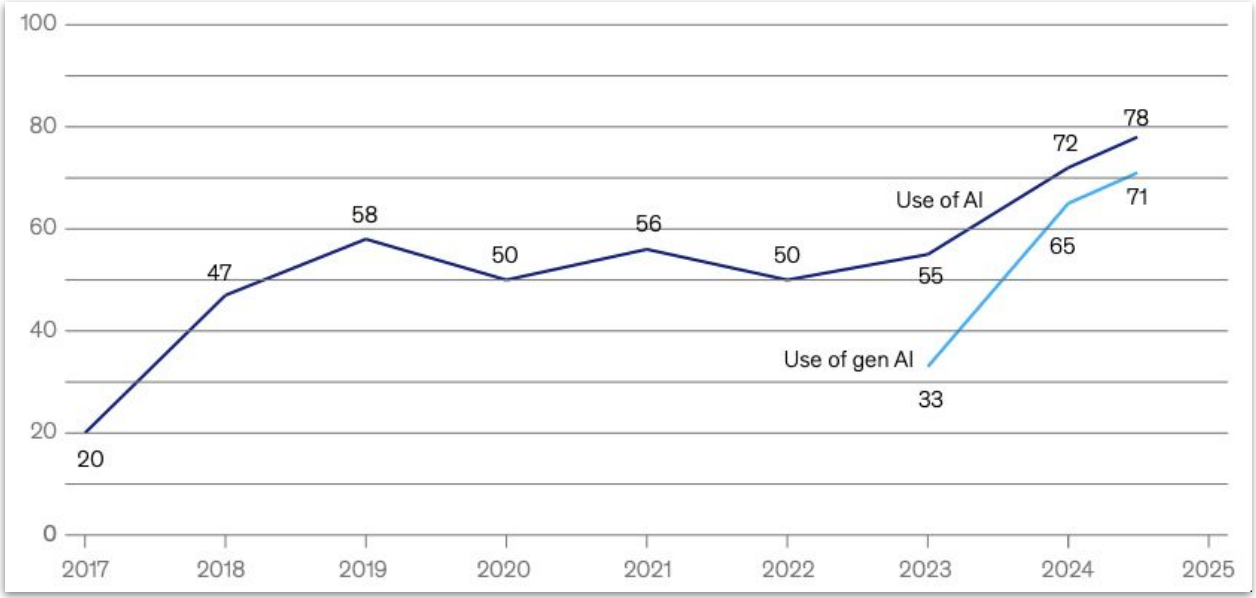
AI is enhancing, not yet replacing, human operators

Generative AI: Current Usage

Adoption of Generative AI is increasing

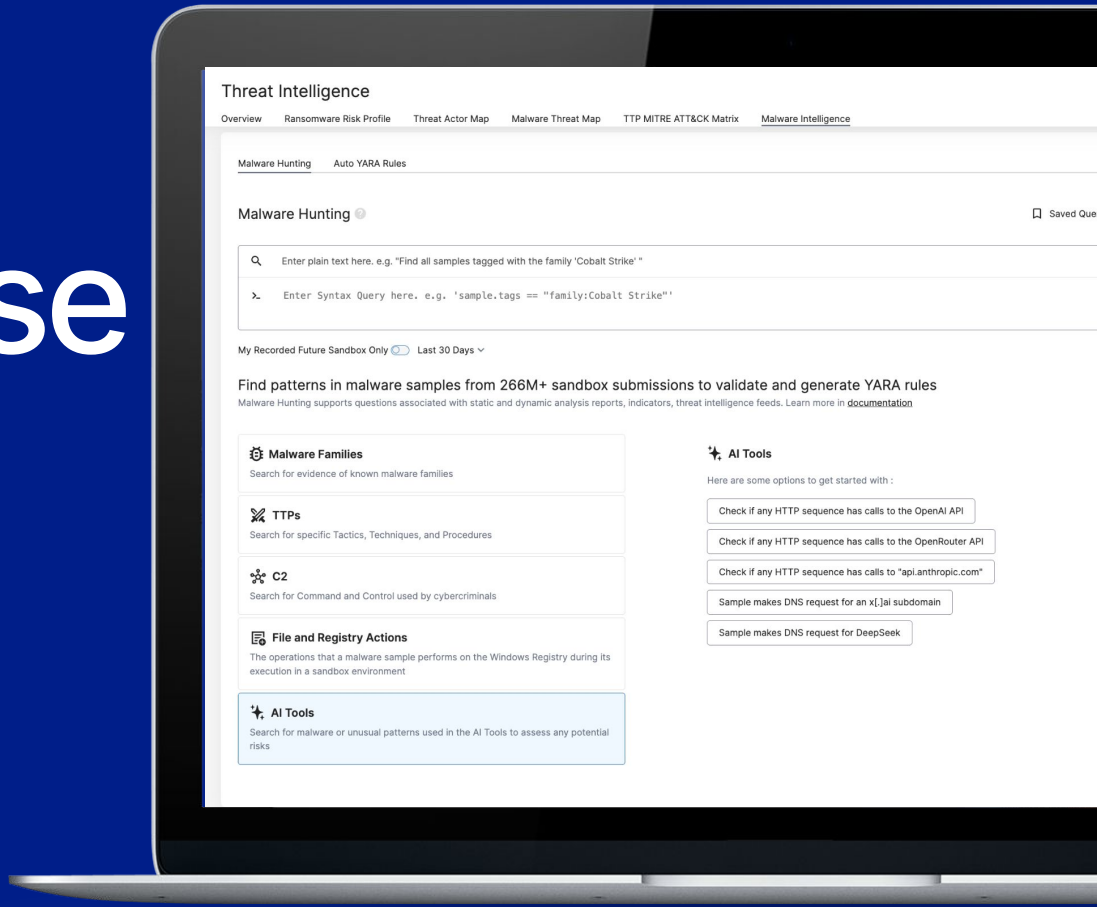
2026 = 80% expected overall adoption

GenAI completes tasks
40% faster
18% higher quality



Organizations that have adopted GenAI to support at least one business function, % of respondents (McKinsey, The State Of AI, March 2025)

Attacker Use Cases

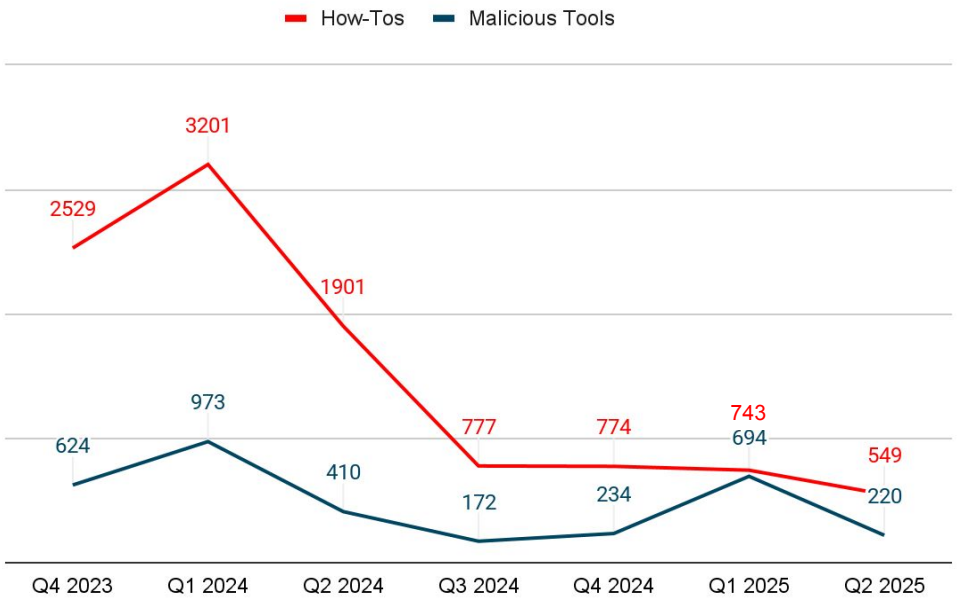


Where do criminals get malicious AI tools?

How to Make AI Malicious Through Prompt Engineering

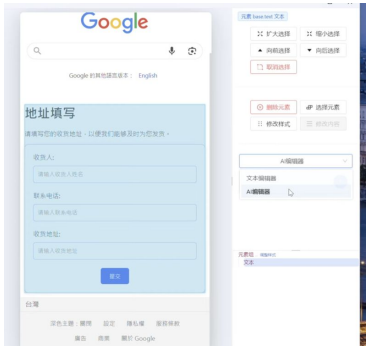
- Role playing
- Multi-step prompting
- Logic attacks
- Policy puppetry attacks

References to AI How-Tos and Malicious Tools on Criminal Forums



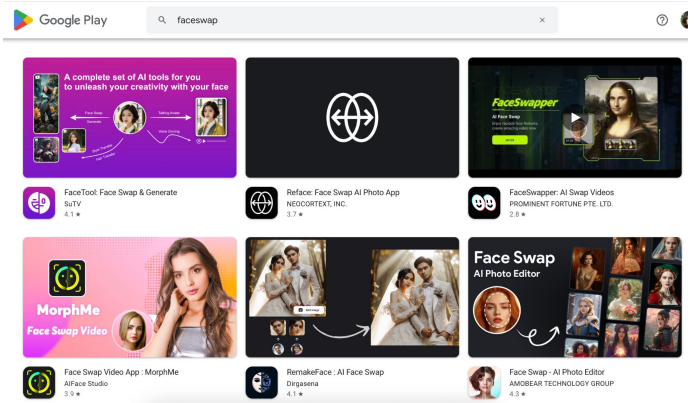
AI makes social engineering easier and more effective

AI-Enhanced Phishing-as-a-Service



Screenshot from Darcula demo video showing how AI helps generate phishing lures. (Source: The Register)

Real Time DeepFakes



Searching "Faceswap" on Google Play reveals dozens of apps for download.

AI enhances existing cyber operations and TTPs

Iranian state-sponsored Sophisticated social engineering

Generate convincing translations in non-native languages.

Chinese state-sponsored "Living off the land"

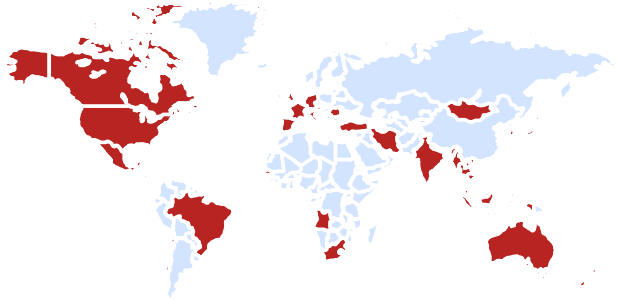
Troubleshoot native tools and functions.

Hello,
On behalf of the Dr. Mohammed Al-Sulami, Head of the International Institute for Iranian Studies (RASANAH), I am cordially inviting you to be our resource speaker for a webinar on the topic **"Saudi Arabia and Iran and the future of KSA and Israel relation"** on October 20 at International Institute for Iranian Studies.
Your expertise and invaluable knowledge on the subject will be of great help to our institute as well as other attendees from other think tanks.

The webinar will be organized through Zoom and the keynote speakers are:
1. Abdullah bin Saud Al-Enezi, Saudi Arabia's ambassador to Iran,
2. Michael A. Ratney, U.S. Ambassador to Saudi Arabia,
3. Amos Yadlin, president and founder of MIND Israel.

Till now some experts include:

Quality of Iranian phishing lures are reportedly improving to contain fewer errors and more fluent text.



Impacket and other tools observed in global espionage campaigns.

How AI enhances steps along the cyber kill chain

Incorporating AI throughout cyber operations

Reconnaissance

Criminals discuss using ChatGPT to identify card fraud targets

Discovery

Incorporate LLMs to generate commands to tailor execution based on victim environment

Valid Credentials

Use Claude to assist in parsing combo lists for valid credentials

Actions on Objectives

Improve encryption and support ransomware negotiations

Defense Evasion

Detect and block AI tools to prevent reverse engineering

Skilled humans are still required to complete operations

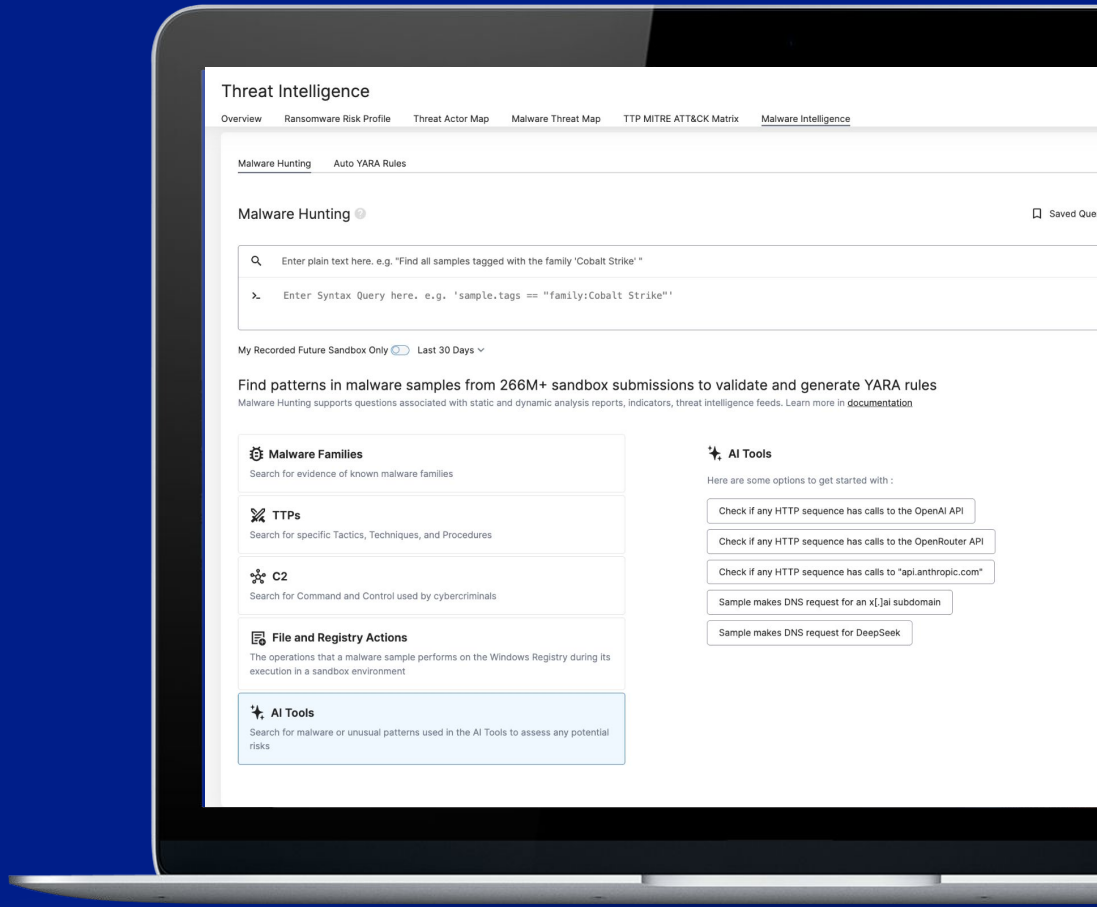
AI Attempt: *Use Cosmic Forge App to Write Malicious Scripts*

Outcome: Could not effectively encrypt or wipe files

AI Attempt: *Use Grok to Develop DDOS Capabilities*

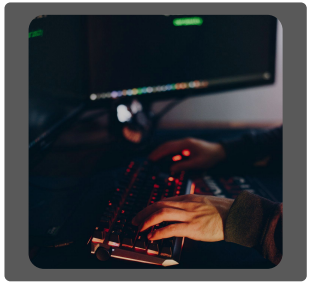
Outcome: Provided hallucinated list of botnet vendors

Defender Use Cases



Too much data

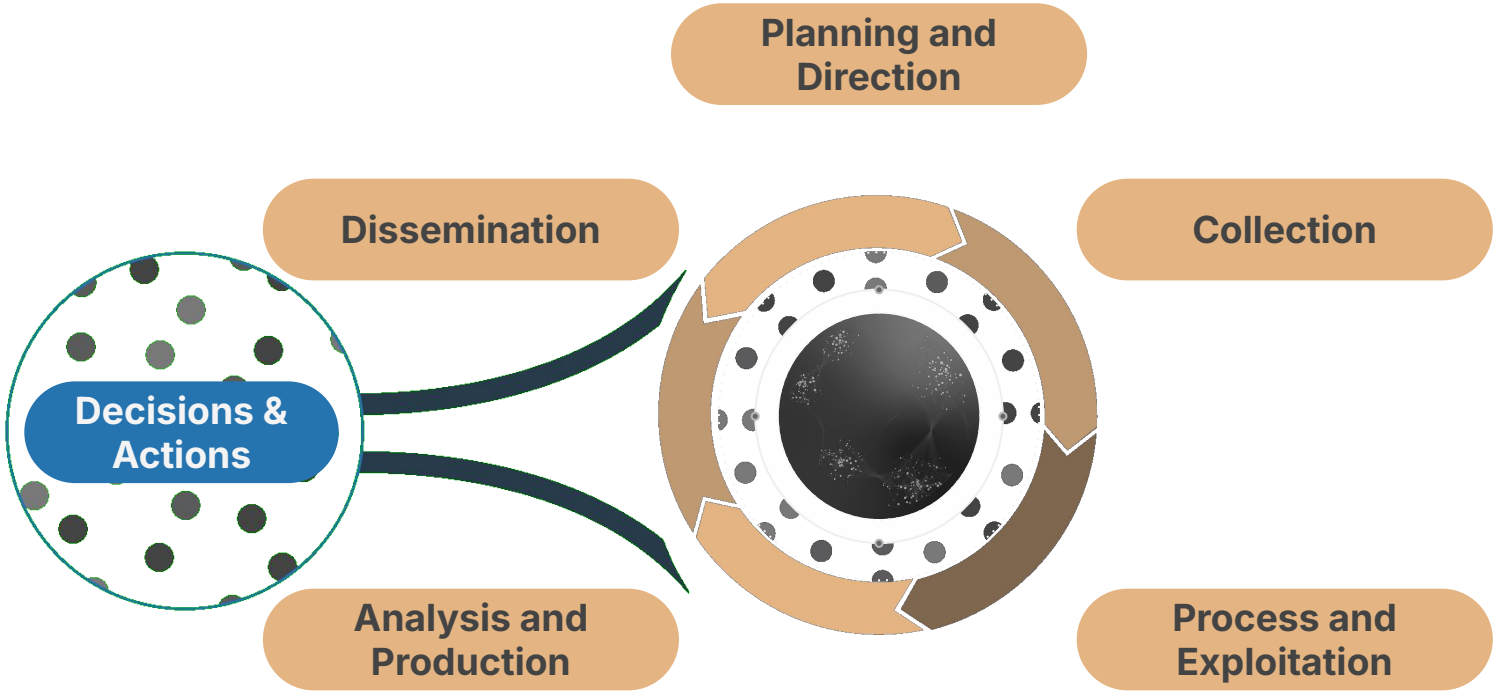
Too few people



Motivated Threat Actors using AI

AI for Threat Intelligence

Automate the intelligence cycle



Defensive applications of Generative AI

Threat Detection & Response

- ➔ Anomaly Detection
- ➔ Behavioural Analysis
- ➔ Automated Incident Response

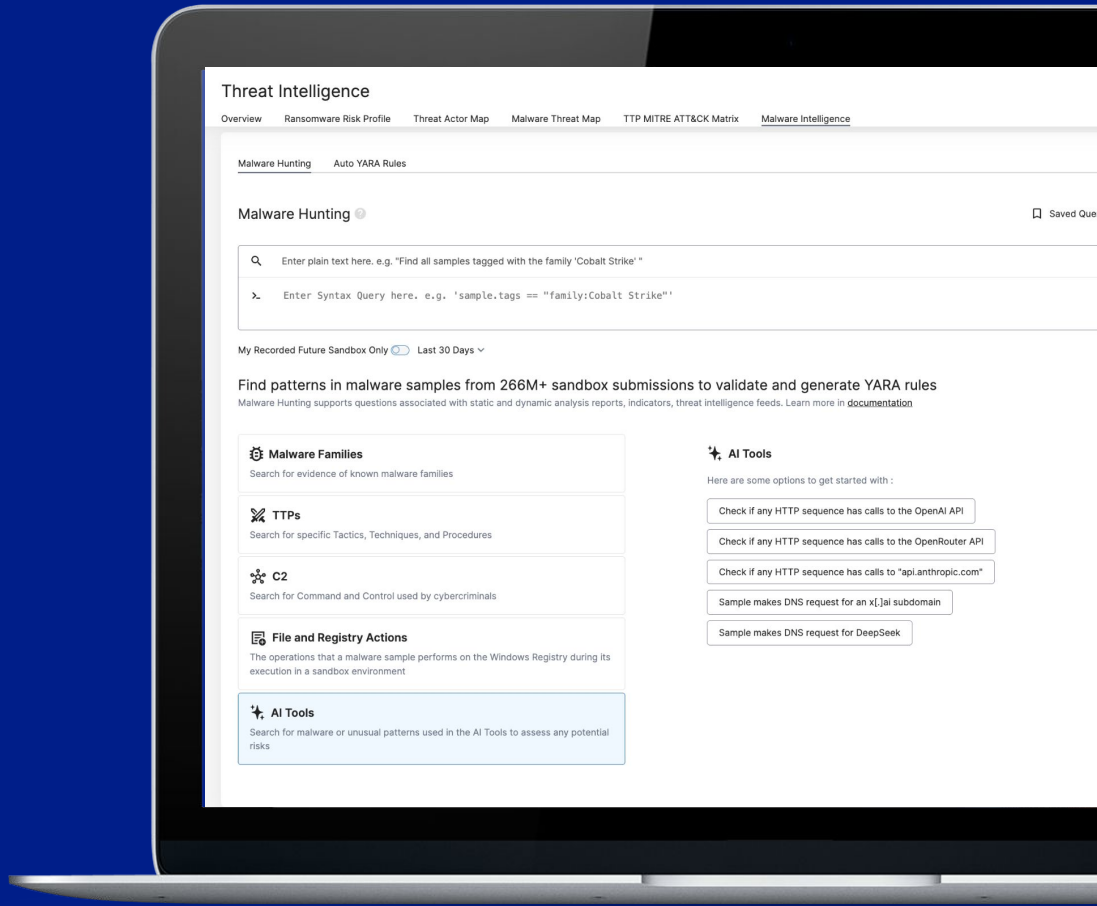
Penetration Testing & Red Teaming

- ➔ Vulnerability Discovery
- ➔ Reconnaissance
- ➔ Attack Simulation
- ➔ Analysis and Reporting

Threat Intelligence & Analysis

- ➔ Insights
- ➔ Productivity
- ➔ Knowledge Sharing
- ➔ Prediction

Outlook


Threat Intelligence
Overview
Ransomware Risk Profile
Threat Actor Map
Malware Threat Map
TTP MITRE ATT&CK Matrix
Malware Intelligence
Malware Hunting
Auto YARA Rules
Malware Hunting
Saved Que
Enter plain text here. e.g. "Find all samples tagged with the family 'Cobalt Strike' "
Enter Syntax Query here. e.g. 'sample.tags == "family:Cobalt Strike"'
My Recorded Future Sandbox Only
Last 30 Days
Find patterns in malware samples from 266M+ sandbox submissions to validate and generate YARA rules
Malware Hunting supports questions associated with static and dynamic analysis reports, indicators, threat intelligence feeds. Learn more in documentation
Malware Families
Search for evidence of known malware families
TTPs
Search for specific Tactics, Techniques, and Procedures
C2
Search for Command and Control used by cybercriminals
File and Registry Actions
The operations that a malware sample performs on the Windows Registry during its execution in a sandbox environment
AI Tools
Search for malware or unusual patterns used in the AI Tools to assess any potential risks
AI Tools
Here are some options to get started with :
Check if any HTTP sequence has calls to the OpenAI API
Check if any HTTP sequence has calls to the OpenRouter API
Check if any HTTP sequence has calls to "api.anthropic.com"
Sample makes DNS request for an x[.]ai subdomain
Sample makes DNS request for DeepSeek

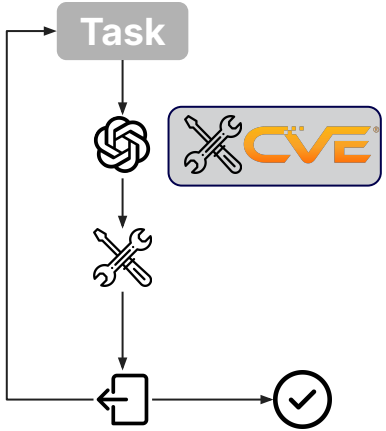
TOMORROW

Evolving technology will enable more automated attacks

What's coming next?

Polymorphic malware

Automated exploitation with malicious agents



Data poisoning via automated propagation

Key Takeaways

- AI acts as a force multiplier, for both unskilled and sophisticated actors
- Generative AI facilitates proactive cybersecurity stance
- Future threats: fully automated operations and targeting of AI ecosystem

Thank you