Updates

All Updates

Sep 2026

Aug 2026

Jul 2026

Jun 2026

May 2026

Apr 2026

Feb 2026
Jan 2026
Dec 2025
Nov 2025
Oct 2025
Sep 2025
Aug 2025
Apr 2025
Mar 2025
Oct 2024
Mar 2024
Jan 2024

Apr 2023
Feb 2023
Jan 2023
Oct 2022
Jul 2022
Mar 2022
Oct 2021
Jul 2021
Jun 2021

September 2026

Website v5.4.0

- Updated ATLAS data to version 2026.09

Data v2026.09

This version of ATLAS data contains 1 matrix, 16 tactics, 120 techniques, 88 sub-techniques, 40 mitigations, and 73 case studies.

Techniques

- Added new techniques
  - Triggers in Multimodal Inputs
  - AI Agent Response Biasing
  - Crafted AI Assistant Links
  - Misconfigured or Publicly Exposed AI Services
  - Discover AI Agent Runtime Capabilities
  - AI Targeted Cloaking
  - Search Open Technical Databases: Scan Databases
  - Active Scanning: Enumerate Hosted AI Resources
  - Active Scanning: Query Platform Metadata APIs
  - Active Scanning: Scan for Exposed AI Infrastructure
  - Active Scanning: Probe AI Agent Trigger Channels

- Search Open Website/Domains
- Active Scanning
- LLM Prompt Obfuscation
- LLM Prompt Injection: Indirect
- LLM Jailbreak
- LLM Response Rendering
- AI Agent Clickbait

Mitigations

- Added new mitigations
  - AI Honeypots
- Updated existing mitigations
  - Generative AI Guardrails

Case Studies

- Added new case studies
  - AI Recommendation Poisoning via Crafted AI Assistant Links
- Updated existing case studies

- Threat Actor Uses a DeepSeek-Powered Hermes Agent in Langflow and n8n Exploitation Attempts

Join our collaborative community to shape future tool and framework developments in threat mitigation, robustness, privacy and other critical aspects of AI security.

Connect with us >

MITRE

Pioneering For A
Better Future
www.mitre.org

© 2021-2026 The MITRE Corporation. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. Case Number 21-2363.

