ATLAS Matrix for AI Systems

Subtechniques

Expand All | Collapse All

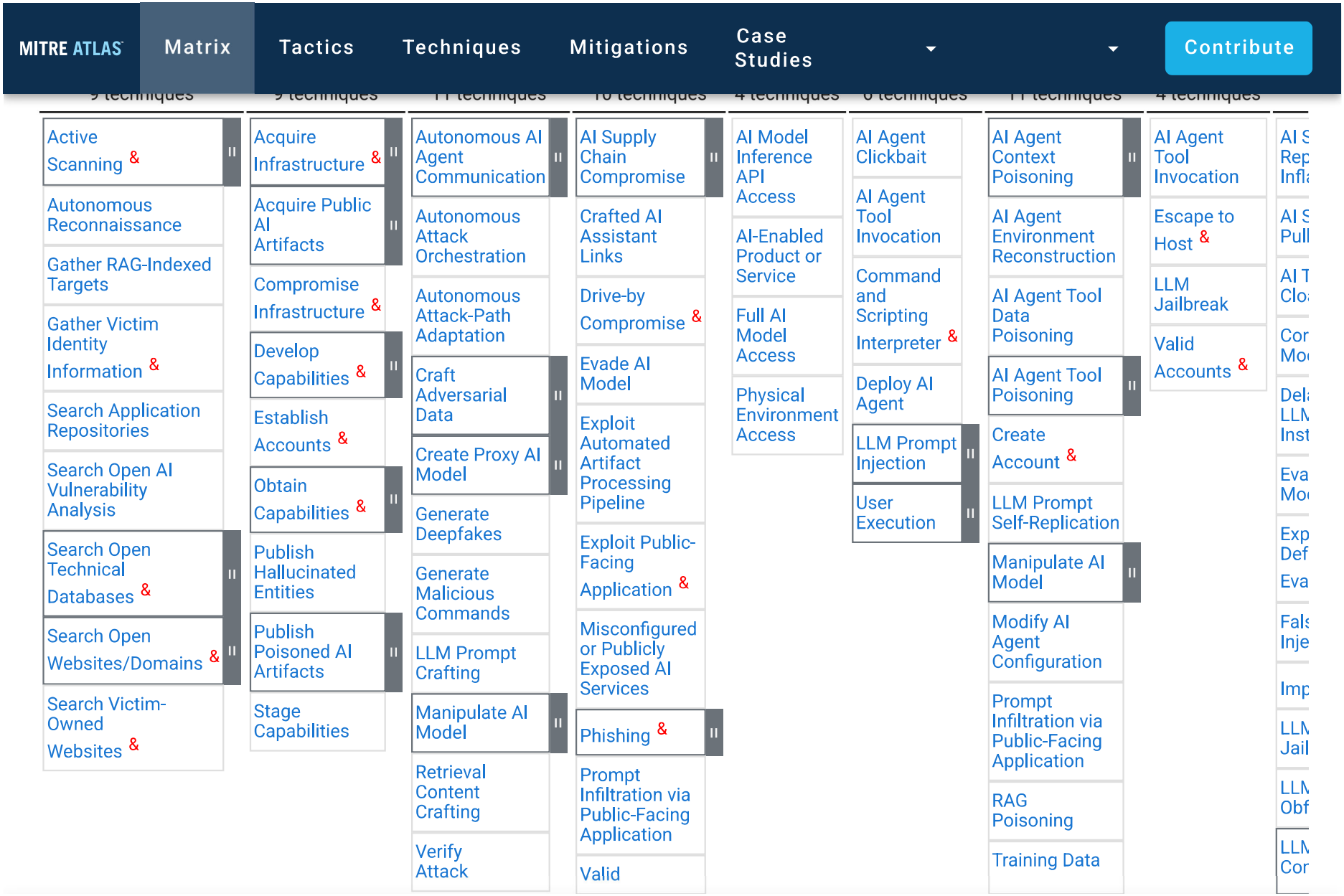
Filter by Platforms

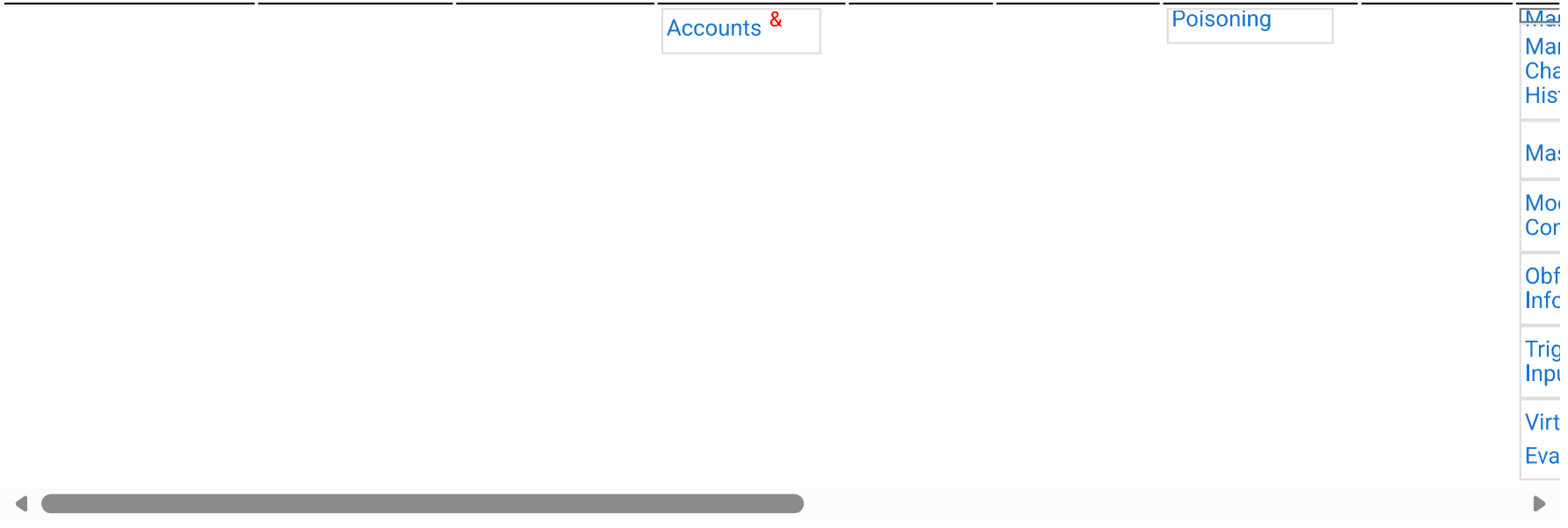
✓ Predictive AI ✓ Generative AI ✓ Agentic AI ✓ Enterprise

Filter by Maturity

Feasible — Demonstrated — Realized

Swipe horizontally to explore the matrix


MITRE ATLAS
Matrix
Tactics
Techniques
Mitigations
Case Studies
Contribute
Active Scanning &
Autonomous Reconnaissance
Gather RAG-Indexed Targets
Gather Victim Identity Information &
Search Application Repositories
Search Open AI Vulnerability Analysis
Search Open Technical Databases &
Search Open Websites/Domains &
Search Victim-Owned Websites &
Acquire Infrastructure &
Acquire Public AI Artifacts
Compromise Infrastructure &
Develop Capabilities &
Establish Accounts &
Obtain Capabilities &
Publish Hallucinated Entities
Publish Poisoned AI Artifacts
Stage Capabilities
Autonomous AI Agent Communication
Autonomous Attack Orchestration
Autonomous Attack-Path Adaptation
Craft Adversarial Data
Create Proxy AI Model
Generate Deepfakes
Generate Malicious Commands
LLM Prompt Crafting
Manipulate AI Model
Retrieval Content Crafting
Verify Attack
AI Supply Chain Compromise
Crafted AI Assistant Links
Drive-by Compromise &
Evade AI Model
Exploit Automated Artifact Processing Pipeline
Exploit Public-Facing Application &
Misconfigured or Publicly Exposed AI Services
Phishing &
Prompt Infiltration via Public-Facing Application
Valid
AI Model Inference API Access
AI-Enabled Product or Service
Full AI Model Access
Physical Environment Access
AI Agent Clickbait
AI Agent Tool Invocation
Command and Scripting Interpreter &
Deploy AI Agent
LLM Prompt Injection
User Execution
AI Agent Context Poisoning
AI Agent Environment Reconstruction
AI Agent Tool Data Poisoning
AI Agent Tool Poisoning
Create Account &
LLM Prompt Self-Replication
Manipulate AI Model
Modify AI Agent Configuration
Prompt Infiltration via Public-Facing Application
RAG Poisoning
Training Data
AI Agent Tool Invocation
Escape to Host &
LLM Jailbreak
Valid Accounts &



& indicates a tactic or technique is adapted from MITRE ATT&CK®

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 >



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.

