MITRE ATLAS — Adversarial ML

Contents

1 MITRE ATLAS — Adversarial ML

Field	Value
Reference key	`mitre-atlas`
Availability	AVAILABLE
Capture method	`github_yaml_mirror`
Source type	remote_url
URL / path	https://atlas.mitre.org/
Captured (UTC)	2026-06-23T03:30:32Z
Content type	text/plain; charset=utf-8
HTTP status	200

1.1 Boardroom Citation Context

Adversarial ML threat mapping; P2 red-team scenarios.

1.2 Source Location

https://atlas.mitre.org/

1.3 Capture Provenance

Field	Value
Capture method	`github_yaml_mirror`
Primary URL	https://atlas.mitre.org/

Field	Value
Primary result	partial
Fallback URL	https://raw.githubusercontent.com/mitre-atlas/atlas-data/main/dist/v6/ATLAS-2026.05.yaml

Primary https://atlas.mitre.org/ is a JavaScript SPA with no static HTML body. MITRE publishes canonical ATLAS matrix data in the public mitre-atlas/atlas-data repository.

Primary failure: HTML retrieved but yielded minimal extractable text (JavaScript-rendered or paywall shell).

1.4 Captured Content

```
MITRE ATLAS canonical data export (YAML mirror from mitre-atlas/atlas-data).
Description: Adversarial Threat Landscape for AI Systems
Version: 2026.05
Modified: 2026-05-27
Tactics indexed: 16
Techniques indexed: 101

Sample tactics:
- AI Model Access
- AI Attack Staging
- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Defense Evasion
- Discovery
- Collection
- Exfiltration
- Impact
- Privilege Escalation
- Credential Access
- Command and Control

Sample techniques:
- Search Open Technical Databases
- Search Open AI Vulnerability Analysis
- Acquire Public AI Artifacts
- Search Victim-Owned Websites
- Search Application Repositories
- Create Proxy AI Model
```

- Active Scanning
- Discover AI Artifacts
- Acquire Infrastructure
- AI Supply Chain Compromise
- User Execution
- Valid Accounts
- Discover AI Model Ontology
- Discover AI Model Family
- Evade AI Model
- Obtain Capabilities
- Develop Capabilities
- Manipulate AI Model
- Publish Poisoned Datasets
- Poison Training Data
- Establish Accounts
- Exfiltration via AI Inference API
- Exfiltration via Cyber Means
- Denial of AI Service
- Erode AI Model Integrity

Archived reference article for AICSR-STUDY-2026-001 footnote corpus.