Tactics

ATLAS-matrix

Reconnaissance

Resource Development

AI Attack Adaptation

Initial Access

AI Model Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery



# Tactics

Tactics are tactical adversary goals during an attack. They represent the “why” of a technique: the reason for performing an action. Tactics serve as useful contextual categories for individual techniques and cover standard notations for things adversaries do during an operation. [1]

MITRE ATLAS™ tactics represent new adversary goals particular to artificial intelligence systems, as well as tactics adapted from the MITRE ATT&CK® Enterprise Matrix. In those cases, ATT&CK tactic definitions are stretched to include ML concepts.

The table below lists tactics from MITRE ATLAS™. Scroll through the table or use the filter to narrow down the information.

Search for Keywords

Tactics

ATLAS-matrix

Reconnaissance

Resource Development

AI Attack Adaptation

Initial Access

AI Model Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

| | | |
|---|---|---|
| AML.TA0002 | Reconnaissance & | The adversary is trying to gather information about the AI system they can use to plan future operations. |
| AML.TA0003 | Resource Development & | The adversary is trying to establish resources they can use to support operations. |
| AML.TA0001 | AI Attack Adaptation | The adversary is adapting capabilities, methods, knowledge, or objectives into attack-ready outputs for a target or current operational conditions. |
| AML.TA0004 | Initial Access & | The adversary is trying to gain access to the AI system. |
| AML.TA0000 | AI Model Access | The adversary is attempting to gain some level of access to an AI model. |
| AML.TA0005 | Execution & | The adversary is trying to run malicious code embedded in AI artifacts or software. |
| AML.TA0006 | Persistence & | The adversary is trying to maintain their foothold via AI artifacts or software. |
| AML.TA0012 | Privilege Escalation & | The adversary is trying to gain higher-level permissions. |

Tactics

ATLAS-matrix

Reconnaissance

Resource Development

AI Attack Adaptation

Initial Access

AI Model Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

| | | |
|---|---|---|
| AML.TA0007 | Defense Evasion & | The adversary is trying to avoid being detected by AI-enabled security software. |
| AML.TA0013 | Credential Access & | The adversary is trying to steal account names and passwords. |
| AML.TA0008 | Discovery & | The adversary is trying to figure out your AI environment. |
| AML.TA0015 | Lateral Movement & | The adversary is trying to move through your AI environment. |
| AML.TA0009 | Collection & | The adversary is trying to gather AI artifacts and other related information relevant to their goal. |
| AML.TA0014 | Command and Control & | The adversary is trying to communicate with compromised AI systems to control them. |
| AML.TA0010 | Exfiltration & | The adversary is trying to steal AI artifacts or other information about the AI system. |
| AML.TA0011 | Impact & | The adversary is trying to manipulate, interrupt, erode confidence in, or destroy your AI systems and data. |

robustness, privacy and other critical aspects of AI security.

Connect with us >

MITRE

Pioneering For A
Better Future
www.mitre.org

## Tactics

- ATLAS-matrix
  - Reconnaissance
  - Resource Development
  - AI Attack Adaptation
  - Initial Access
  - AI Model Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery

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

Privacy Policy | Terms of Use | Manage Cookies

# Tactics

ATLAS-matrix
- Reconnaissance
- Resource Development
- AI Attack Adaptation
- Initial Access
- AI Model Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery