MITRE ATLAS | Protected-action mapping

AML.T0053 · AI Agent Tool Invocation

A credentialed agent calls a privileged tool. Check the exact requested operation, target and current authority; refuse or escalate. Limit: Only protected execution routes are checked.

AML.T0012 · Valid Accounts

Legitimate account access is used for an unauthorized change. Separate authentication and tool access from permission for the exact action. Limit: Not credential theft prevention.

AML.T0051 · LLM Prompt Injection

Injected instructions propose a changed payment or record. Check proposed parameters against trusted authority rather than prompt claims. Limit: Not universal prompt injection detection.

AML.T0080 · AI Agent Context Poisoning

Manipulated context attempts to change the basis for a tool action. Use trusted current context; refuse or escalate missing or altered required authority. Limit: Does not establish truth of all context.

AML.T0101 · Data Destruction via AI Agent Tool Invocation

An agent requests destructive changes through an available tool. Require exact authorization and executor verification for the protected operation. Limit: Unintegrated delete routes are outside scope.

AML.T0086 · Exfiltration via AI Agent Tool Invocation

An agent requests a sensitive export to an unauthorized destination. Check covered export destination, scope and authority. Limit: Not universal DLP or network monitoring.

AML.T0083 · Credentials from AI Agent Configuration

Stolen credentials are used to propose a privileged operation. Require trusted current authority for the specific protected action. Limit: Does not prevent credential extraction.

Scope

ATLAS mappings describe where OntoGuard can act; they are not a certification or a guarantee of detection. Individual technique and mitigation associations require confirmation against MITRE source records.

Public evidence covers reviewed integrations and controlled reference tests, not customer deployments. No guarantee of ROI, universal enforcement or semantic correctness.

Evidence hub · OEM integration kit