

ODA3 INSTITUTE

CROSSWALK

GAISSF™—MITRE ATLAS Mapping

AI Threat Alignment Crosswalk — MITRE ATLAS v2026.09

GAISSF-CRO-025 | Informative crosswalk | Draft for Publication

Version 1.0 | Updated 6 October 2026

© 2026 ODA3 Pvt Ltd

Field	Controlled value
Document ID	GAISSF-CRO-025
Status	Draft for Publication
Classification	Informative threat-alignment crosswalk / public
GAISSF baseline	GAISSF™ v1.0; 59 controls / 9 domains; Applicable-Control Baseline = 52 D1-D8 + applicable D9
ATLAS baseline	MITRE ATLAS content v2026.09; 16 tactics; 120 techniques + 88 sub-techniques
Publication date	29 June 2026
Publisher	ODA3 Institute
Version	1.0
Verification date	6 October 2026

The crosswalk does not demonstrate that a technique is prevented or detected. ATLAS describes adversary behavior; GAISSF establishes control and evidence expectations. Operating effectiveness must be tested in the relevant architecture and threat context.

2. Source baseline and scope

Source	Version / status	Role
GAISSF-NOR-001	v1.0 Corrected Final Publication Edition	Normative framework and conformance baseline
GAISSF-NOR-004	v1.0 Full Final	Authoritative 59-control catalogue
MITRE ATLAS	Content v2026.09; released 15 Sep 2026; current as of 6 Oct 2026	Primary external baseline: 16 tactics; 120 techniques; 88 sub-techniques; 40 mitigations; 73 case studies
ATLAS website	Content v2026.09; released 15 Sep 2026; current as of 6 Oct 2026	Primary external baseline: 16 tactics; 120 techniques; 88 sub-techniques; 40 mitigations; 73 case studies

The crosswalk maps all GAISSF controls to materially relevant ATLAS tactics and a deliberately bounded priority technique set. The priority set is not a substitute for the complete ATLAS v2026.09 knowledge base. ATLAS is a living knowledge base with monthly content releases; mappings must be revalidated when taxonomy, technique identity or scope changes.

3. Mapping method

1. Normalize each GAISSF control into its preventive, detective, corrective, governance, and evidence outcomes.
2. Compare those outcomes with the objective and operational effect of ATLAS tactics and techniques.
3. Classify the relationship as Strong Partial, Partial, or Supporting; do not infer equivalence from shared terminology.
4. Record residual detection, telemetry, adversary-emulation, and validation work.
5. Perform a reverse review at tactic level to identify thin or absent GAISSF coverage.

4. ATLAS tactic inventory

Tactic ID	Tactic
AML.TA0002	Reconnaissance
AML.TA0003	Resource Development
AML.TA0004	Initial Access
AML.TA0000	AI Model Access
AML.TA0005	Execution
AML.TA0006	Persistence
AML.TA0012	Privilege Escalation
AML.TA0007	Defense Evasion
AML.TA0013	Credential Access
AML.TA0008	Discovery
AML.TA0015	Lateral Movement
AML.TA0009	Collection
AML.TA0001	AI Attack Adaptation
AML.TA0014	Command and Control
AML.TA0010	Exfiltration
AML.TA0011	Impact

5. Priority technique inventory

Technique ID	Technique	Tactic
AML.T0064	Gather RAG-Indexed Targets	Reconnaissance
AML.T0087	Gather Victim Identity Information	Reconnaissance
AML.T0004	Search Application Repositories	Reconnaissance
AML.T0001	Search Open AI Vulnerability Analysis	Reconnaissance
AML.T0000	Search Open Technical Databases	Reconnaissance
AML.T0003	Search Victim-Owned Websites	Reconnaissance

Technique ID	Technique	Tactic
AML.T0008	Acquire Infrastructure	Resource Development
AML.T0002	Acquire Public AI Artifacts	Resource Development
AML.T0017	Develop Capabilities	Resource Development
AML.T0021	Establish Accounts	Resource Development
AML.T0065	LLM Prompt Crafting	Resource Development
AML.T0016	Obtain Capabilities	Resource Development
AML.T0020	Training Data Poisoning	Resource Development
AML.T0060	Publish Hallucinated Entities	Resource Development
AML.T0104	Publish Poisoned AI Artifacts: AI Agent Tools	Resource Development
AML.T0019	Publish Poisoned AI Artifacts: Datasets	Resource Development
AML.T0058	Publish Poisoned AI Artifacts: Models	Resource Development
AML.T0066	Retrieval Content Crafting	Resource Development
AML.T0079	Stage Capabilities	Resource Development
AML.T0010	AI Supply Chain Compromise	Initial Access
AML.T0015	Evade AI Model	Initial Access
AML.T0049	Exploit Public-Facing Application	Initial Access
AML.T0052	Phishing	Initial Access
AML.T0093	Prompt Infiltration via Public-Facing Application	Initial Access
AML.T0012	Valid Accounts	Initial Access
AML.T0040	AI Model Inference API Access	AI Model Access
AML.T0047	AI-Enabled Product or Service	AI Model Access
AML.T0044	Full AI Model Access	AI Model Access
AML.T0041	Physical Environment Access	AI Model Access
AML.T0100	AI Agent Clickbait	Execution
AML.T0053	AI Agent Tool Invocation	Execution
AML.T0050	Command and Scripting Interpreter	Execution
AML.T0103	Deploy AI Agent	Execution
AML.T0051	LLM Prompt Injection	Execution
AML.T0011	User Execution	Execution
AML.T0110	AI Agent Context Poisoning	Persistence
AML.T0105	AI Agent Tool Data Poisoning	Persistence
AML.T0111	AI Agent Tool Poisoning	Persistence
AML.T0061	LLM Prompt Self-Replication	Persistence
AML.T0018	Manipulate AI Model	Persistence
AML.T0081	RAG Poisoning	Persistence
AML.T0070	Escape to Host	Privilege Escalation
AML.T0054	LLM Jailbreak	Privilege Escalation
AML.T0109	AI Supply Chain Reputation Inflation	Defense Evasion
AML.T0076	AI Supply Chain Rug Pull	Defense Evasion
AML.T0094	Corrupt AI Model	Defense Evasion
AML.T0107	Delay Execution of LLM Instructions	Defense Evasion
AML.T0071	False RAG Entry Injection	Defense Evasion
AML.T0073	LLM Prompt Obfuscation	Defense Evasion
AML.T0068	Manipulate User LLM Chat History	Defense Evasion
AML.T0092	Modify AI Agent Configuration	Defense Evasion
AML.T0097	AI Agent Tool Credential Harvesting	Credential Access
AML.T0098	Credentials from AI Agent Configuration	Credential Access
AML.T0083	RAG Credential Harvesting	Credential Access
AML.T0055	Unsecured Credentials	Credential Access
AML.T0106	Discover AI Agent Configuration	Discovery
AML.T0007	Discover AI Artifacts	Discovery
AML.T0014	Discover AI Model Family	Discovery
AML.T0013	Discover AI Model Ontology	Discovery
AML.T0063	Discover AI Model Outputs	Discovery
AML.T0062	Discover LLM Hallucinations	Discovery
AML.T0069	Discover LLM System Information	Discovery
AML.T0089	AI Artifact Collection	Collection
AML.T0091	Data from AI Services	Collection
AML.T0005	Create Proxy AI Model	AI Attack Adaptation
AML.T0043	Craft Adversarial Data	AI Attack Adaptation
AML.T0099	Generate Deepfakes	AI Attack Adaptation
AML.T0080	Generate Malicious Commands	AI Attack Adaptation
AML.T0042	Verify Attack	AI Attack Adaptation
AML.T0108	AI Agent	Command and Control
AML.T0102	AI Service API	Command and Control
AML.T0101	Exfiltration via AI Agent Tool Invocation	Exfiltration
AML.T0024	Exfiltration via AI Inference API	Exfiltration
AML.T0025	Exfiltration via Cyber Means	Exfiltration

Technique ID	Technique	Tactic
AML.T0056	Extract LLM System Prompt	Exfiltration
AML.T0057	LLM Data Leakage	Exfiltration
AML.T0090	LLM Response Rendering	Exfiltration
AML.T0029	Denial of AI Service	Impact
AML.T0031	Erode AI Model Integrity	Impact
AML.T0046	Spamming AI System with Chaff Data	Impact
AML.T0048	External Harms	Impact
AML.T0059	Erode Dataset Integrity	Impact

6. Reverse tactic coverage

Tactic	Mapped GAISSF controls	Priority techniques represented	Coverage	Residual limitation
AML.TA0002 Reconnaissance	D5-CTL-05, D5-CTL-06, D6-CTL-01, D6-CTL-02, D6-CTL-04, D7-CTL-H01, D7-CTL-H03, D8-CTL-01, D8-CTL-02, D8-CTL-03, D8-CTL-05	AML.T0087 Gather Victim Identity Information; AML.T0064 Gather RAG-Indexed Targets; AML.T0001 Search Open AI Vulnerability Analysis; AML.T0000 Search Open Technical Databases	Substantially Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0003 Resource Development	D1-CTL-01, D1-CTL-04, D2-CTL-02, D2-CTL-06, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-04, D3-CTL-05, D3-CTL-06, D3-CTL-07, D7-CTL-H01, D7-CTL-H02, D8-CTL-03, D8-CTL-05	AML.T0020 Training Data Poisoning; AML.T0058 Publish Poisoned AI Artifacts: Models; AML.T0065 LLM Prompt Crafting; AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools; AML.T0017 Develop Capabilities	Substantially Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0004 Initial Access	D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D2-CTL-04, D2-CTL-05, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D6-CTL-06, D7-CTL-H05	AML.T0015 Evade AI Model; AML.T0010 AI Supply Chain Compromise; AML.T0052 Phishing	Substantially Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0000 AI Model Access	D3-CTL-01, D3-CTL-04, D4-CTL-04, D5-CTL-02, D6-CTL-03, D6-CTL-05, D9-CTL-02, D9-CTL-03, D9-CTL-05, D9-CTL-06	AML.T0040 AI Model Inference API Access; AML.T0041 Physical Environment Access; AML.T0044 Full AI Model Access	Substantially Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0005 Execution	D2-CTL-01, D2-CTL-02, D3-CTL-02, D3-CTL-05, D3-CTL-07	AML.T0051 LLM Prompt Injection; AML.T0100 AI Agent Clickbait	Partially Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0006 Persistence	D9-CTL-02	AML.T0110 AI Agent Context Poisoning	Partially Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0012 Privilege Escalation			Not Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0007 Defense Evasion	D1-CTL-06, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-05, D4-CTL-06, D4-CTL-07, D6-CTL-06	AML.T0109 AI Supply Chain Reputation Inflation	Substantially Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0013 Credential Access			Not Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0008 Discovery	D5-CTL-01, D5-CTL-03, D5-CTL-04, D5-CTL-05, D8-CTL-04, D9-CTL-01, D9-CTL-05, D9-CTL-07	AML.T0062 Discover LLM Hallucinations; AML.T0106 Discover AI Agent Configuration; AML.T0007 Discover AI Artifacts; AML.T0069 Discover LLM System Information	Substantially Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0015 Lateral Movement			Not Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0009 Collection			Not Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0001 AI Attack Adaptation	D1-CTL-02, D1-CTL-03, D1-CTL-05, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-03, D2-CTL-04, D2-CTL-05, D5-CTL-01, D5-CTL-03, D5-CTL-04, D7-CTL-H02, D7-CTL-H04, D9-CTL-01	AML.T0042 Verify Attack; AML.T0005 Create Proxy AI Model; AML.T0043 Craft Adversarial Data; AML.T0099 Generate Deepfakes	Substantially Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0014 Command and Control			Not Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.
AML.TA0010 Exfiltration	D2-CTL-01, D2-CTL-06, D3-CTL-03, D3-CTL-06, D5-CTL-06, D6-CTL-04, D7-CTL-H04	AML.T0056 Extract LLM System Prompt; AML.T0101 Exfiltration via AI Agent Tool Invocation; AML.T0024 Exfiltration via AI	Partially Addressed	ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience

Tactic	Mapped GAISSF controls	Priority techniques represented	Coverage	Residual limitation
AML.TA0011 Impact	D1-CTL-01, D6-CTL-07, D7-CTL-H03, D7-CTL-H05	AML.T0059 Erode Dataset Integrity; AML.T0046 Spamming AI System with Chaff Data; AML.T0029 Denial of AI Service; AML.T0048 External Harms	Partially Addressed	against every procedure under the tactic. ATLAS is an adversary-behavior knowledge base; control mapping does not establish detection coverage, prevention, or resilience against every procedure under the tactic.

7. Implementation and evidence reuse

- AI-system and model threat models linked to ATLAS tactic and technique IDs
- Adversary-emulation plans and red-team test cases
- Model, dataset, agent-tool, RAG, and supply-chain inventories
- Prompt-injection, poisoning, evasion, extraction, and jailbreak test results
- IAM, secrets, least-privilege, tool-authorization, and human-approval records
- Telemetry design, detection logic, alerts, investigations, and incident records
- Model integrity, provenance, signing, and deployment-gate evidence
- Residual-risk decisions and management approvals

D9 mappings are additional/conditional. Where Physical AI or cyber-physical actuation is in scope, PAI-SF™ v1.0 may be used alongside GAISSF; CSX-PAISF-004 is mapping only and does not establish equivalence, evidence sufficiency, operating effectiveness, or automatic conformance.

8. Limitations

- Mapping is not MITRE endorsement, certification, equivalence, evidence sufficiency, verified prevention/detection coverage, or proof of defensive operating effectiveness.
- ATLAS describes adversary behavior and AI-security threat knowledge; GAISSF defines control and evidence expectations. A mapping relationship does not prove prevention, detection, mitigation, completeness, or operating effectiveness.
- The priority technique register is deliberately focused on techniques and sub-techniques with direct AI-system relevance to the source GAISSF mappings. The current ATLAS v2026.09 data contains 120 techniques and 88 sub-techniques; the official ATLAS dataset remains authoritative.
- Environment-specific threat modelling, telemetry, detection engineering, adversary emulation, and validation remain necessary.
- ATLAS publishes monthly content releases. Revalidate this crosswalk against the current ATLAS content version before publication, reuse or material assurance decisions.

9. Notably absent

- No MITRE certification, approval, endorsement, or conformance declaration is established.
- No claim is made that GAISSF implementation prevents or detects every ATLAS technique.
- No universal technique-coverage percentage or maturity score is asserted.
- No assumption is made that control documentation proves operating effectiveness.
- No claim is made that ATLAS replaces ATT&CK, application threat modelling, or environment-specific incident intelligence.

Annex A - GAISSF-to-ATLAS mapping register

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-025-MAP-0001	D1-CTL-01 Dataset Provenance & Poisoning Prevention	Resource Development AML.T0020 Training Data Poisoning	S	Low	GAISSF D1-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0020 Training Data Poisoning. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0002	D1-CTL-01 Dataset Provenance & Poisoning Prevention	Impact AML.T0059 Erode Dataset	S	Low	GAISSF D1-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0059 Erode	Threat modelling, architecture-

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
		Integrity			Dataset Integrity. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0003	D1-CTL-02 Model Extraction Resistance	AI Attack Adaptation AML.T0042 Verify Attack	P	Medium	GAISSF D1-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0042 Verify Attack. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0004	D1-CTL-03 Behavioral Drift Detection	AI Attack Adaptation AML.T0042 Verify Attack	P	Medium	GAISSF D1-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0042 Verify Attack. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0005	D1-CTL-04 Federated Learning Poisoning Prevention	Resource Development AML.T0020 Training Data Poisoning	S	Low	GAISSF D1-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0020 Training Data Poisoning. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0006	D1-CTL-04 Federated Learning Poisoning Prevention	Resource Development AML.T0058 Publish Poisoned AI Artifacts: Models	S	Low	GAISSF D1-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0058 Publish Poisoned AI Artifacts: Models. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation,

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0007	D1-CTL-05 Embedding Space Robustness	Initial Access AML.T0015 Evade AI Model	S	Low	GAISSF D1-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0015 Evade AI Model. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0008	D1-CTL-05 Embedding Space Robustness	AI Attack Adaptation AML.T0005 Create Proxy AI Model	S	Low	GAISSF D1-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0005 Create Proxy AI Model. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0009	D1-CTL-06 Post-Quantum Model Signing & Crypto Hardening	Initial Access AML.T0010 AI Supply Chain Compromise	S	Low	GAISSF D1-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0010 AI Supply Chain Compromise. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0010	D1-CTL-06 Post-Quantum Model Signing & Crypto Hardening	Defense Evasion AML.T0109 AI Supply Chain Reputation Inflation	S	Low	GAISSF D1-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0109 AI Supply Chain Reputation Inflation. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency,

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0011	D1-CTL-07 Lora/Adapter Integrity Verification	Initial Access AML.T0015 Evade AI Model	S	Low	GAISSF D1-CTL-07 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0015 Evade AI Model. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0012	D1-CTL-07 Lora/Adapter Integrity Verification	AI Attack Adaptation AML.T0005 Create Proxy AI Model	S	Low	GAISSF D1-CTL-07 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0005 Create Proxy AI Model. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0013	D1-CTL-08 Model Merge Attack Detection	Initial Access AML.T0015 Evade AI Model	S	Low	GAISSF D1-CTL-08 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0015 Evade AI Model. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0014	D1-CTL-08 Model Merge Attack Detection	AI Attack Adaptation AML.T0005 Create Proxy AI Model	S	Low	GAISSF D1-CTL-08 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0005 Create Proxy AI Model. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						testing remain necessary.
GAISSF-CRO-025-MAP-0015	D1-CTL-09 Quantization Backdoor Screening	AI Attack Adaptation AML.T0042 Verify Attack	P	Medium	GAISSF D1-CTL-09 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0042 Verify Attack. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0016	D2-CTL-01 Direct Prompt Injection Prevention	Execution AML.T0051 LLM Prompt Injection	S	Low	GAISSF D2-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0051 LLM Prompt Injection. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0017	D2-CTL-01 Direct Prompt Injection Prevention	Exfiltration AML.T0056 Extract LLM System Prompt	S	Low	GAISSF D2-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0056 Extract LLM System Prompt. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0018	D2-CTL-02 Indirect Prompt Injection Prevention	Execution AML.T0051 LLM Prompt Injection	S	Low	GAISSF D2-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0051 LLM Prompt Injection. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-	D2-CTL-02 Indirect Prompt Injection Prevention	Resource Development	S	Low	GAISSF D2-CTL-02 provides preventive, detective, governance, or assurance measures	Threat modelling,

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
MAP-0019		AML.T0065 LLM Prompt Crafting			relevant to adversary use of AML.T0065 LLM Prompt Crafting. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0020	D2-CTL-03 Jailbreak Resistance Testing	AI Attack Adaptation AML.T0042 Verify Attack	P	Medium	GAISSF D2-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0042 Verify Attack. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0021	D2-CTL-04 Multi-Modal Injection Defense	AI Attack Adaptation AML.T0043 Craft Adversarial Data	S	Low	GAISSF D2-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0043 Craft Adversarial Data. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0022	D2-CTL-04 Multi-Modal Injection Defense	Initial Access AML.T0015 Evade AI Model	S	Low	GAISSF D2-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0015 Evade AI Model. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0023	D2-CTL-05 Function Call/Tool Call Injection Prevention	AI Attack Adaptation AML.T0043 Craft Adversarial Data	S	Low	GAISSF D2-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0043 Craft Adversarial Data. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
					effectiveness.	emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0024	D2-CTL-05 Function Call/Tool Call Injection Prevention	Initial Access AML.T0015 Evade AI Model	S	Low	GAISSF D2-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0015 Evade AI Model. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0025	D2-CTL-06 Cross-Context Hijacking Mitigation	Exfiltration AML.T0056 Extract LLM System Prompt	S	Low	GAISSF D2-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0056 Extract LLM System Prompt. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0026	D2-CTL-06 Cross-Context Hijacking Mitigation	Resource Development AML.T0065 LLM Prompt Crafting	S	Low	GAISSF D2-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0065 LLM Prompt Crafting. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0027	D3-CTL-01 Least Agency Enforcement	Resource Development AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools	S	Low	GAISSF D3-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0028	D3-CTL-01 Least Agency Enforcement	AI Model Access AML.T0040 AI Model Inference API Access	S	Low	GAISSF D3-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0040 AI Model Inference API Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0029	D3-CTL-02 Inter-Agent Communication Security	Resource Development AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools	S	Low	GAISSF D3-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0030	D3-CTL-02 Inter-Agent Communication Security	Execution AML.T0100 AI Agent Clickbait	S	Low	GAISSF D3-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0100 AI Agent Clickbait. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0031	D3-CTL-03 Agentic Prompt Chaining Detection	Exfiltration AML.T0056 Extract LLM System Prompt	S	Low	GAISSF D3-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0056 Extract LLM System Prompt. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0032	D3-CTL-03 Agentic Prompt Chaining Detection	Resource Development AML.T0065 LLM Prompt Crafting	S	Low	GAISSF D3-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0065 LLM Prompt Crafting. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0033	D3-CTL-04 Embodied AI Safety Controls	Resource Development AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools	S	Low	GAISSF D3-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0034	D3-CTL-04 Embodied AI Safety Controls	AI Model Access AML.T0041 Physical Environment Access	S	Low	GAISSF D3-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0041 Physical Environment Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0035	D3-CTL-05 Multi-Agent Trust Chain Attestation	Resource Development AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools	S	Low	GAISSF D3-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-	D3-CTL-05 Multi-Agent Trust Chain Attestation	Execution	S	Low	GAISSF D3-CTL-05 provides preventive, detective, governance, or	Threat

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
CRO-025-MAP-0036		AML.T0100 AI Agent Clickbait			assurance measures relevant to adversary use of AML.T0100 AI Agent Clickbait. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0037	D3-CTL-06 Persistent Memory Exfiltration Prevention	Exfiltration AML.T0101 Exfiltration via AI Agent Tool Invocation	S	Low	GAISSF D3-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0101 Exfiltration via AI Agent Tool Invocation. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0038	D3-CTL-06 Persistent Memory Exfiltration Prevention	Resource Development AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools	S	Low	GAISSF D3-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0039	D3-CTL-07 Secure Memory Lifecycle Management	Resource Development AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools	S	Low	GAISSF D3-CTL-07 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0104 Publish Poisoned AI Artifacts: AI Agent Tools. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0040	D3-CTL-07 Secure Memory Lifecycle Management	Execution AML.T0100 AI Agent Clickbait	S	Low	GAISSF D3-CTL-07 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0100 AI Agent Clickbait. The mapping records defensive relevance, not technique	Threat modelling, architecture-specific telemetry,

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
					elimination or verified operating effectiveness.	adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0041	D4-CTL-01 Ai Bill Of Materials (Ai Bom) Maintenance	Initial Access AML.T0010 AI Supply Chain Compromise	S	Low	GAISSF D4-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0010 AI Supply Chain Compromise. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0042	D4-CTL-01 Ai Bill Of Materials (Ai Bom) Maintenance	Defense Evasion AML.T0109 AI Supply Chain Reputation Inflation	S	Low	GAISSF D4-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0109 AI Supply Chain Reputation Inflation. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0043	D4-CTL-02 Model File & Artifact Scanning	Initial Access AML.T0010 AI Supply Chain Compromise	S	Low	GAISSF D4-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0010 AI Supply Chain Compromise. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0044	D4-CTL-02 Model File & Artifact Scanning	Defense Evasion AML.T0109 AI Supply Chain Reputation Inflation	S	Low	GAISSF D4-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0109 AI Supply Chain Reputation Inflation. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering,

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0045	D4-CTL-03 Model Hub & Registry Vetting	Initial Access AML.T0010 AI Supply Chain Compromise	S	Low	GAISSF D4-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0010 AI Supply Chain Compromise. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0046	D4-CTL-03 Model Hub & Registry Vetting	Defense Evasion AML.T0109 AI Supply Chain Reputation Inflation	S	Low	GAISSF D4-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0109 AI Supply Chain Reputation Inflation. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0047	D4-CTL-04 Mcp Server Behavioral Monitoring	Initial Access AML.T0010 AI Supply Chain Compromise	S	Low	GAISSF D4-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0010 AI Supply Chain Compromise. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0048	D4-CTL-04 Mcp Server Behavioral Monitoring	AI Model Access AML.T0040 AI Model Inference API Access	S	Low	GAISSF D4-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0040 AI Model Inference API Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0049	D4-CTL-05 Third-Party Ai Api Security Assessment	Initial Access AML.T0010 Ai Supply Chain Compromise	S	Low	GAISSF D4-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0010 Ai Supply Chain Compromise. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0050	D4-CTL-05 Third-Party Ai Api Security Assessment	Defense Evasion AML.T0109 Ai Supply Chain Reputation Inflation	S	Low	GAISSF D4-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0109 Ai Supply Chain Reputation Inflation. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0051	D4-CTL-06 Shadow Ai Discovery & Governance	Initial Access AML.T0010 Ai Supply Chain Compromise	S	Low	GAISSF D4-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0010 Ai Supply Chain Compromise. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0052	D4-CTL-06 Shadow Ai Discovery & Governance	Defense Evasion AML.T0109 Ai Supply Chain Reputation Inflation	S	Low	GAISSF D4-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0109 Ai Supply Chain Reputation Inflation. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-025-MAP-0053	D4-CTL-07 Ai Software Composition Analysis (Sca)	Initial Access AML.T0010 AI Supply Chain Compromise	S	Low	GAISSF D4-CTL-07 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0010 AI Supply Chain Compromise. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0054	D4-CTL-07 Ai Software Composition Analysis (Sca)	Defense Evasion AML.T0109 AI Supply Chain Reputation Inflation	S	Low	GAISSF D4-CTL-07 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0109 AI Supply Chain Reputation Inflation. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0055	D5-CTL-01 Harmful Content Blocking	Discovery AML.T0062 Discover LLM Hallucinations	S	Low	GAISSF D5-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0062 Discover LLM Hallucinations. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0056	D5-CTL-01 Harmful Content Blocking	AI Attack Adaptation AML.T0099 Generate Deepfakes	S	Low	GAISSF D5-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0099 Generate Deepfakes. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0057	D5-CTL-02 Pii Leakage Prevention	AI Model Access AML.T0040 AI Model	S	Low	GAISSF D5-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0040 AI Model Inference API Access. The mapping records	Threat modelling, architecture-specific

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
		Inference API Access			defensive relevance, not technique elimination or verified operating effectiveness.	telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0058	D5-CTL-02 Pii Leakage Prevention	AI Model Access AML.T0044 Full AI Model Access	S	Low	GAISSF D5-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0044 Full AI Model Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0059	D5-CTL-03 Copyright Detection	Discovery AML.T0062 Discover LLM Hallucinations	S	Low	GAISSF D5-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0062 Discover LLM Hallucinations. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0060	D5-CTL-03 Copyright Detection	AI Attack Adaptation AML.T0099 Generate Deepfakes	S	Low	GAISSF D5-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0099 Generate Deepfakes. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0061	D5-CTL-04 Ai Watermarking Robustness	Discovery AML.T0062 Discover LLM Hallucinations	S	Low	GAISSF D5-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0062 Discover LLM Hallucinations. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0062	D5-CTL-04 Ai Watermarking Robustness	AI Attack Adaptation AML.T0099 Generate Deepfakes	S	Low	GAISSF D5-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0099 Generate Deepfakes. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0063	D5-CTL-05 Privacy-By-Design Verification	Reconnaissance AML.T0087 Gather Victim Identity Information	S	Low	GAISSF D5-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0087 Gather Victim Identity Information. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0064	D5-CTL-05 Privacy-By-Design Verification	Discovery AML.T0062 Discover LLM Hallucinations	S	Low	GAISSF D5-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0062 Discover LLM Hallucinations. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0065	D5-CTL-06 Privacy-Preserving ML Validation	Exfiltration AML.T0024 Exfiltration via AI Inference API	S	Low	GAISSF D5-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0024 Exfiltration via AI Inference API. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0066	D5-CTL-06 Privacy-Preserving MI Validation	Reconnaissance AML.T0087 Gather Victim Identity Information	S	Low	GAISSF D5-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0087 Gather Victim Identity Information. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0067	D6-CTL-01 Human-In-The-Loop For High-Risk Actions	Reconnaissance AML.T0064 Gather RAG-Indexed Targets	S	Low	GAISSF D6-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0064 Gather RAG-Indexed Targets. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0068	D6-CTL-01 Human-In-The-Loop For High-Risk Actions	Reconnaissance AML.T0087 Gather Victim Identity Information	S	Low	GAISSF D6-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0087 Gather Victim Identity Information. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0069	D6-CTL-02 Audit Trail Completeness	Reconnaissance AML.T0064 Gather RAG-Indexed Targets	S	Low	GAISSF D6-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0064 Gather RAG-Indexed Targets. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
GAISSF-CRO-025-MAP-0070	D6-CTL-02 Audit Trail Completeness	Reconnaissance AML.T0087 Gather Victim Identity Information	S	Low	GAISSF D6-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0087 Gather Victim Identity Information. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	necessary. Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0071	D6-CTL-03 AI Model Card Completeness	AI Model Access AML.T0040 AI Model Inference API Access	S	Low	GAISSF D6-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0040 AI Model Inference API Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0072	D6-CTL-03 AI Model Card Completeness	AI Model Access AML.T0044 Full AI Model Access	S	Low	GAISSF D6-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0044 Full AI Model Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0073	D6-CTL-04 AI Incident Response Readiness	Exfiltration AML.T0090 LLM Response Rendering	S	Low	GAISSF D6-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0090 LLM Response Rendering. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0074	D6-CTL-04 AI Incident Response Readiness	Reconnaissance AML.T0064 Gather RAG-	S	Low	GAISSF D6-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0064 Gather	Threat modelling, architecture-

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
		Indexed Targets			RAG-Indexed Targets. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0075	D6-CTL-05 Model Deprecation & Decommissioning	AI Model Access AML.T0040 AI Model Inference API Access	S	Low	GAISSF D6-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0040 AI Model Inference API Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0076	D6-CTL-05 Model Deprecation & Decommissioning	AI Model Access AML.T0044 Full AI Model Access	S	Low	GAISSF D6-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0044 Full AI Model Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0077	D6-CTL-06 Third-Party AI Vendor Governance	Initial Access AML.T0010 AI Supply Chain Compromise	S	Low	GAISSF D6-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0010 AI Supply Chain Compromise. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0078	D6-CTL-06 Third-Party AI Vendor Governance	Defense Evasion AML.T0109 AI Supply Chain Reputation Inflation	S	Low	GAISSF D6-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0109 AI Supply Chain Reputation Inflation. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation,

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0079	D6-CTL-07 Ai Resilience & Business Continuity	Impact AML.T0046 Spamming AI System with Chaff Data	S	Low	GAISSF D6-CTL-07 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0046 Spamming AI System with Chaff Data. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0080	D6-CTL-07 Ai Resilience & Business Continuity	Impact AML.T0029 Denial of AI Service	S	Low	GAISSF D6-CTL-07 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0029 Denial of AI Service. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0081	D7-CTL-H01 Ai-Generated Phishing Simulation	Reconnaissance AML.T0001 Search Open AI Vulnerability Analysis	S	Low	GAISSF D7-CTL-H01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0001 Search Open AI Vulnerability Analysis. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0082	D7-CTL-H01 Ai-Generated Phishing Simulation	Resource Development AML.T0020 Training Data Poisoning	S	Low	GAISSF D7-CTL-H01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0020 Training Data Poisoning. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency,

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0083	D7-CTL-H02 Deepfake Detection Training	Resource Development AML.T0020 Training Data Poisoning	S	Low	GAISSF D7-CTL-H02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0020 Training Data Poisoning. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0084	D7-CTL-H02 Deepfake Detection Training	AI Attack Adaptation AML.T0042 Verify Attack	S	Low	GAISSF D7-CTL-H02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0042 Verify Attack. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0085	D7-CTL-H03 Out-Of-Band Authentication	Impact AML.T0048 External Harms	S	Low	GAISSF D7-CTL-H03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0048 External Harms. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0086	D7-CTL-H03 Out-Of-Band Authentication	Reconnaissance AML.T0064 Gather RAG-Indexed Targets	S	Low	GAISSF D7-CTL-H03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0064 Gather RAG-Indexed Targets. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						testing remain necessary.
GAISSF-CRO-025-MAP-0087	D7-CTL-H04 Ai Social Engineering Ir	AI Attack Adaptation AML.T0042 Verify Attack	S	Low	GAISSF D7-CTL-H04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0042 Verify Attack. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0088	D7-CTL-H04 Ai Social Engineering Ir	Exfiltration AML.T0090 LLM Response Rendering	S	Low	GAISSF D7-CTL-H04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0090 LLM Response Rendering. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0089	D7-CTL-H05 Ai-Enhanced External Attack Defense	Impact AML.T0048 External Harms	S	Low	GAISSF D7-CTL-H05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0048 External Harms. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0090	D7-CTL-H05 Ai-Enhanced External Attack Defense	Initial Access AML.T0052 Phishing	S	Low	GAISSF D7-CTL-H05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0052 Phishing. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-	D8-CTL-01 Eu Ai Act Risk Tier Mapping	Reconnaissance AML.T0064	S	Low	GAISSF D8-CTL-01 provides preventive, detective, governance, or assurance measures	Threat modelling,

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
MAP-0091		Gather RAG-Indexed Targets			relevant to adversary use of AML.T0064 Gather RAG-Indexed Targets. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0092	D8-CTL-01 Eu Ai Act Risk Tier Mapping	Reconnaissance AML.T0087 Gather Victim Identity Information	S	Low	GAISSF D8-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0087 Gather Victim Identity Information. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0093	D8-CTL-02 Iso 42001 Gap Analysis	Reconnaissance AML.T0001 Search Open AI Vulnerability Analysis	S	Low	GAISSF D8-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0001 Search Open AI Vulnerability Analysis. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0094	D8-CTL-02 Iso 42001 Gap Analysis	Reconnaissance AML.T0064 Gather RAG-Indexed Targets	S	Low	GAISSF D8-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0064 Gather RAG-Indexed Targets. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0095	D8-CTL-03 Gpai Technical Documentation Verification	Reconnaissance AML.T0000 Search Open Technical Databases	S	Low	GAISSF D8-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0000 Search Open Technical Databases. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
					operating effectiveness.	emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0096	D8-CTL-03 Gpai Technical Documentation Verification	Resource Development AML.T0020 Training Data Poisoning	S	Low	GAISSF D8-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0020 Training Data Poisoning. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0097	D8-CTL-04 Dora Ict Incident Reporting (Financial Sector)	Discovery AML.T0106 Discover AI Agent Configuration	S	Low	GAISSF D8-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0106 Discover AI Agent Configuration. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0098	D8-CTL-04 Dora Ict Incident Reporting (Financial Sector)	Discovery AML.T0007 Discover AI Artifacts	S	Low	GAISSF D8-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0007 Discover AI Artifacts. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0099	D8-CTL-05 Nist Sp 800-218A Compliance Check	Resource Development AML.T0017 Develop Capabilities	S	Low	GAISSF D8-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0017 Develop Capabilities. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0100	D8-CTL-05 Nist Sp 800-218A Compliance Check	Reconnaissance AML.T0064 Gather RAG-Indexed Targets	S	Low	GAISSF D8-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0064 Gather RAG-Indexed Targets. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0101	D9-CTL-01 Physical Harm Boundary Enforcement	Discovery AML.T0062 Discover LLM Hallucinations	P	Medium	GAISSF D9-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0062 Discover LLM Hallucinations. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0102	D9-CTL-01 Physical Harm Boundary Enforcement	AI Attack Adaptation AML.T0042 Verify Attack	P	Medium	GAISSF D9-CTL-01 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0042 Verify Attack. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0103	D9-CTL-02 Safe State And Graceful Degradation	AI Model Access AML.T0041 Physical Environment Access	S	Low	GAISSF D9-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0041 Physical Environment Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
						effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0104	D9-CTL-02 Safe State And Graceful Degradation	Persistence AML.T0110 AI Agent Context Poisoning	S	Low	GAISSF D9-CTL-02 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0110 AI Agent Context Poisoning. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0105	D9-CTL-03 Human Override And Emergency Stop	AI Model Access AML.T0040 AI Model Inference API Access	S	Low	GAISSF D9-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0040 AI Model Inference API Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0106	D9-CTL-03 Human Override And Emergency Stop	AI Model Access AML.T0044 Full AI Model Access	S	Low	GAISSF D9-CTL-03 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0044 Full AI Model Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0107	D9-CTL-04 Cyber-Physical Attack Detection	AI Attack Adaptation AML.T0042 Verify Attack	P	Medium	GAISSF D9-CTL-04 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0042 Verify Attack. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-	D9-CTL-05 Physical Environment Integrity Monitoring	AI Model	S	Low	GAISSF D9-CTL-05 provides preventive, detective, governance, or	Threat

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
CRO-025-MAP-0108		Access AML.T0041 Physical Environment Access			assurance measures relevant to adversary use of AML.T0041 Physical Environment Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0109	D9-CTL-05 Physical Environment Integrity Monitoring	Discovery AML.T0069 Discover LLM System Information	S	Low	GAISSF D9-CTL-05 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0069 Discover LLM System Information. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0110	D9-CTL-06 Actuator Command Verification	Initial Access AML.T0015 Evade AI Model	S	Low	GAISSF D9-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0015 Evade AI Model. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0111	D9-CTL-06 Actuator Command Verification	AI Model Access AML.T0041 Physical Environment Access	S	Low	GAISSF D9-CTL-06 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0041 Physical Environment Access. The mapping records defensive relevance, not technique elimination or verified operating effectiveness.	Threat modelling, architecture-specific telemetry, adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.
GAISSF-CRO-025-MAP-0112	D9-CTL-07 Physical Incident Evidence Preservation	Discovery AML.T0062 Discover LLM Hallucinations	P	Medium	GAISSF D9-CTL-07 provides preventive, detective, governance, or assurance measures relevant to adversary use of AML.T0062 Discover LLM Hallucinations. The mapping records defensive relevance, not	Threat modelling, architecture-specific telemetry,

Record	GAISSF control	ATLAS tactic / technique	Rel.	Confidence	Rationale	Residual gap
					technique elimination or verified operating effectiveness.	adversary emulation, detection engineering, technique currency, evidence sufficiency and operating-effectiveness testing remain necessary.

Annex B - QA and change record

Check	Result
GAISSF controls inventoried	59
ATLAS tactics inventoried	16
Official ATLAS reported technique count	208 technique objects = 120 techniques + 88 sub-techniques
Priority techniques mapped	82
Forward mapping records	112
Monthly source revalidation required	Yes
Independent threat-informed-defense review	Required before publication approval