

ODA3 INSTITUTE

CROSSWALK

GAISSF™—MITRE ATT&CK Mapping

Threat-Informed AI Security Crosswalk — Enterprise ATT&CK v19.2

GAISSF-CRO-026 | Informative crosswalk | Draft for Publication

Version 1.0 | Updated 6 October 2026

© 2026 ODA3 Pvt Ltd

Field	Controlled value
Document ID	GAISSF-CRO-026
Version	1.0
Classification	Informative crosswalk / public
Status	Draft for Publication
Primary external baseline	MITRE ATT&CK v19 - Enterprise
Publication date	29 June 2026
Publisher	ODA3 Institute
GAISSF baseline	59 controls / 9 domains; Applicable-Control Baseline = 52 D1-D8 + applicable D9
ATT&CK baseline	Enterprise v19.2; 15 tactics; current as of 6 Oct 2026
Updated	6 October 2026

1. Executive Summary

GAISSF-CRO-026 documents defensive relationships between all 59 GAISSF™ v1.0 controls and a source-bounded priority set of 100 MITRE ATT&CK Enterprise techniques across the current 15 Enterprise tactics. The register contains 112 control-to-technique mapping records and a reverse tactic-level coverage view.

The crosswalk supports threat modelling, detection and telemetry planning, adversary-emulation scoping, evidence reuse, and assurance design. It does not convert ATT&CK into a compliance checklist and does not prove that any mapped technique is prevented, detected, or mitigated in operation.

2. Purpose and Intended Use

- Translate adversary behavior into GAISSF control and evidence requirements.
- Support SOC, threat-intelligence, red-team, purple-team, architecture, and assurance collaboration.
- Identify control, telemetry, detection, resilience, and testing gaps.
- Provide a repeatable source for GitHub, automation, and assessment tooling.

3. Scope

Primary scope: MITRE ATT&CK Enterprise v19.2, current as of 6 October 2026. Mobile and ICS are excluded from this edition because their matrices, operational consequences and evidence expectations require separate controlled profiles. The official ATT&CK dataset remains authoritative for the complete current technique, sub-technique, procedure, mitigation, Detection Strategy/Analytic, group, software and campaign inventory.

4. Source Baseline

Source	Version / status	Use in GAISSF-CRO-026
GAISSF Framework Standard	GAISSF-NOR-001 v1.0; published 1 Jul 2026; updated 4 Oct 2026	Normative framework architecture and conformance baseline
GAISSF Control Catalogue	GAISSF-NOR-004 v1.0; published 1 Jul 2026; updated 4 Oct 2026	Authoritative 59-control catalogue; D9 additional / conditional
MITRE ATT&CK	Enterprise v19.2; current as of 6 Oct 2026	Current Enterprise tactics and technique identifiers; v19 split Defense Evasion into Stealth and Defense Impairment
ATT&CK STIX Data	Official MITRE ATT&CK data / v19.2	Machine-readable source and future revalidation

5. Mapping Methodology

- Map substantive defensive outcomes, not labels.
- Use technique-level records; sub-technique and procedure analysis remains contextual.
- Separate relationship strength from confidence.
- Treat multiple GAISSF controls supporting one ATT&CK behavior as composite coverage.
- Record residual gaps for telemetry, procedure analysis, threat relevance, emulation, and operating effectiveness.
- Perform reverse tactic coverage to identify silent omissions.

6. Controlled Vocabulary

Code	Meaning
SP	Strong partial
P	Partial
S	Supporting

Code	Meaning
C	Contextual
N	No material mapping
O	Outside scope
U	Unable to determine

7. Enterprise Tactic Coverage

Tactic ID	Tactic	Mapped controls	Coverage	Confidence
TA0043	Reconnaissance	10	Substantially Addressed	Medium-High
TA0042	Resource Development	8	Substantially Addressed	Medium-High
TA0001	Initial Access	32	Substantially Addressed	Medium-High
TA0002	Execution	5	Partially Addressed	Medium
TA0003	Persistence	10	Substantially Addressed	Medium-High
TA0004	Privilege Escalation	1	Partially Addressed	Medium
TA0005	Stealth	8	Substantially Addressed	Medium-High
TA0112	Defense Impairment	1	Partially Addressed	Medium
TA0006	Credential Access	1	Partially Addressed	Medium
TA0007	Discovery	2	Partially Addressed	Medium
TA0008	Lateral Movement	2	Partially Addressed	Medium
TA0009	Collection	1	Partially Addressed	Medium
TA0011	Command and Control	0	Not Addressed	Not Rated
TA0010	Exfiltration	6	Partially Addressed	Medium
TA0040	Impact	12	Substantially Addressed	Medium-High

8. Function-by-Function Analysis

TA0043 - Reconnaissance

Coverage assessment: Substantially Addressed (Medium-High confidence). Mapped GAISSF controls: D2-CTL-04, D3-CTL-05, D7-CTL-H01, D7-CTL-H02, D7-CTL-H04, D8-CTL-01, D8-CTL-02, D8-CTL-03, D8-CTL-04, D8-CTL-05. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0042 - Resource Development

Coverage assessment: Substantially Addressed (Medium-High confidence). Mapped GAISSF controls: D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-07, D6-CTL-06, D8-CTL-05. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0001 - Initial Access

Coverage assessment: Substantially Addressed (Medium-High confidence). Mapped GAISSF controls: D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-06, D1-CTL-07, D1-CTL-08, D1-CTL-09, D2-CTL-01, D2-CTL-03, D2-CTL-05, D3-CTL-01, D3-CTL-02, D3-CTL-03, D3-CTL-06, D3-CTL-07, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07, D6-CTL-03, D6-CTL-05, D6-CTL-06, D7-CTL-H01, D7-CTL-H05, D9-CTL-03, D9-CTL-04, D9-CTL-05. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0002 - Execution

Coverage assessment: Partially Addressed (Medium confidence). Mapped GAISSF controls: D2-CTL-04, D2-CTL-05, D2-CTL-06, D3-CTL-04, D7-CTL-H02. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0003 - Persistence

Coverage assessment: Substantially Addressed (Medium-High confidence). Mapped GAISSF controls: D1-CTL-01, D1-CTL-02, D1-CTL-03, D1-CTL-04, D1-CTL-05, D1-CTL-07, D1-CTL-08, D1-CTL-09, D6-CTL-01, D6-CTL-04. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0004 - Privilege Escalation

Coverage assessment: Partially Addressed (Medium confidence). Mapped GAISSF controls: D7-CTL-H03. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0005 - Stealth

Coverage assessment: Substantially Addressed (Medium-High confidence). Mapped GAISSF controls: D2-CTL-01, D2-CTL-06, D3-CTL-02, D3-CTL-03, D3-CTL-05, D3-CTL-07, D6-CTL-02, D9-CTL-06. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0112 - Defense Impairment

Coverage assessment: Partially Addressed (Medium confidence). Mapped GAISSF controls: D3-CTL-04. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0006 - Credential Access

Coverage assessment: Partially Addressed (Medium confidence). Mapped GAISSF controls: D7-CTL-H03. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0007 - Discovery

Coverage assessment: Partially Addressed (Medium confidence). Mapped GAISSF controls: D4-CTL-06, D6-CTL-02. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0008 - Lateral Movement

Coverage assessment: Partially Addressed (Medium confidence). Mapped GAISSF controls: D3-CTL-01, D3-CTL-06. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0009 - Collection

Coverage assessment: Partially Addressed (Medium confidence). Mapped GAISSF controls: D2-CTL-03. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0011 - Command and Control

Coverage assessment: Not Addressed (Not Rated confidence). Mapped GAISSF controls: None. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0010 - Exfiltration

Coverage assessment: Partially Addressed (Medium confidence). Mapped GAISSF controls: D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-06. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

TA0040 - Impact

Coverage assessment: Substantially Addressed (Medium-High confidence). Mapped GAISSF controls: D2-CTL-02, D5-CTL-01, D5-CTL-02, D5-CTL-03, D5-CTL-04, D5-CTL-05, D5-CTL-06, D6-CTL-07, D8-CTL-04, D9-CTL-01, D9-CTL-02, D9-CTL-07. Priority-set tactic coverage does not establish complete ATT&CK Enterprise technique/sub-technique coverage, procedure coverage, platform-specific detection coverage, validated telemetry, evidence sufficiency or operating effectiveness.

9. Priority Technique Inventory

Technique ID	Technique	Tactic
T1595	Active Scanning	Reconnaissance
T1592	Gather Victim Host Information	Reconnaissance
T1589	Gather Victim Identity Information	Reconnaissance
T1590	Gather Victim Network Information	Reconnaissance
T1591	Gather Victim Org Information	Reconnaissance
T1593	Search Open Websites/Domains	Reconnaissance
T1594	Search Victim-Owned Websites	Reconnaissance
T1596	Search Open Technical Databases	Reconnaissance

Technique ID	Technique	Tactic
T1583	Acquire Infrastructure	Resource Development
T1584	Compromise Infrastructure	Resource Development
T1585	Establish Accounts	Resource Development
T1586	Compromise Accounts	Resource Development
T1587	Develop Capabilities	Resource Development
T1588	Obtain Capabilities	Resource Development
T1608	Stage Capabilities	Resource Development
T1189	Drive-by Compromise	Initial Access
T1190	Exploit Public-Facing Application	Initial Access
T1133	External Remote Services	Initial Access
T1566	Phishing	Initial Access
T1195	Supply Chain Compromise	Initial Access
T1078	Valid Accounts	Initial Access
T1059	Command and Scripting Interpreter	Execution
T1203	Exploitation for Client Execution	Execution
T1204	User Execution	Execution
T1047	Windows Management Instrumentation	Execution
T1129	Shared Modules	Execution
T1106	Native API	Execution
T1053	Scheduled Task/Job	Execution
T1127	Trusted Developer Utilities Proxy Execution	Execution
T1098	Account Manipulation	Persistence
T1547	Boot or Logon Autostart Execution	Persistence
T1136	Create Account	Persistence
T1505	Server Software Component	Persistence
T1525	Implant Internal Image	Persistence
T1554	Compromise Host Software Binary	Persistence
T1053.003	Scheduled Task/Job: Cron	Persistence
T1068	Exploitation for Privilege Escalation	Privilege Escalation
T1548	Abuse Elevation Control Mechanism	Privilege Escalation
T1134	Access Token Manipulation	Privilege Escalation
T1484	Domain or Tenant Policy Modification	Privilege Escalation
T1027	Obfuscated Files or Information	Stealth
T1070	Indicator Removal	Stealth
T1036	Masquerading	Stealth
T1685	Disable or Modify Tools	Defense Impairment
T1553	Subvert Trust Controls	Defense Impairment
T1218	System Binary Proxy Execution	Stealth
T1222	File and Directory Permissions Modification	Defense Impairment
T1497	Virtualization/Sandbox Evasion	Stealth
T1574	Hijack Execution Flow	Stealth
T1110	Brute Force	Credential Access
T1555	Credentials from Password Stores	Credential Access
T1552	Unsecured Credentials	Credential Access
T1003	OS Credential Dumping	Credential Access
T1528	Steal Application Access Token	Credential Access
T1539	Steal Web Session Cookie	Credential Access
T1649	Steal or Forge Authentication Certificates	Credential Access
T1621	Multi-Factor Authentication Request Generation	Credential Access
T1087	Account Discovery	Discovery
T1580	Cloud Infrastructure Discovery	Discovery
T1613	Container and Resource Discovery	Discovery
T1526	Cloud Service Discovery	Discovery
T1083	File and Directory Discovery	Discovery
T1049	System Network Connections Discovery	Discovery
T1018	Remote System Discovery	Discovery
T1518	Software Discovery	Discovery
T1482	Domain Trust Discovery	Discovery
T1614	System Location Discovery	Discovery
T1021	Remote Services	Lateral Movement
T1570	Lateral Tool Transfer	Lateral Movement
T1210	Exploitation of Remote Services	Lateral Movement
T1550	Use Alternate Authentication Material	Lateral Movement
T1119	Automated Collection	Collection
T1213	Data from Information Repositories	Collection
T1530	Data from Cloud Storage	Collection

Technique ID	Technique	Tactic
T1114	Email Collection	Collection
T1005	Data from Local System	Collection
T1074	Data Staged	Collection
T1560	Archive Collected Data	Collection
T1056	Input Capture	Collection
T1071	Application Layer Protocol	Command and Control
T1105	Ingress Tool Transfer	Command and Control
T1090	Proxy	Command and Control
T1219	Remote Access Software	Command and Control
T1572	Protocol Tunneling	Command and Control
T1102	Web Service	Command and Control
T1048	Exfiltration Over Alternative Protocol	Exfiltration
T1567	Exfiltration Over Web Service	Exfiltration
T1537	Transfer Data to Cloud Account	Exfiltration
T1020	Automated Exfiltration	Exfiltration
T1041	Exfiltration Over C2 Channel	Exfiltration
T1052	Exfiltration Over Physical Medium	Exfiltration
T1486	Data Encrypted for Impact	Impact
T1485	Data Destruction	Impact
T1490	Inhibit System Recovery	Impact
T1498	Network Denial of Service	Impact
T1499	Endpoint Denial of Service	Impact
T1565	Data Manipulation	Impact
T1531	Account Access Removal	Impact
T1529	System Shutdown/Reboot	Impact
T1657	Financial Theft	Impact

10. Detailed Mapping Register

Record	GAISSF control	ATT&CK technique	Tactic	Rel.	Conf.
GAISSF-CRO-026-MAP-0001	D1-CTL-01 Dataset Provenance & Poisoning Prevention	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0002	D1-CTL-01 Dataset Provenance & Poisoning Prevention	T1554 Compromise Host Software Binary	Persistence	S	Low
GAISSF-CRO-026-MAP-0003	D1-CTL-02 Model Extraction Resistance	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0004	D1-CTL-02 Model Extraction Resistance	T1554 Compromise Host Software Binary	Persistence	S	Low
GAISSF-CRO-026-MAP-0005	D1-CTL-03 Behavioral Drift Detection	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0006	D1-CTL-03 Behavioral Drift Detection	T1554 Compromise Host Software Binary	Persistence	S	Low
GAISSF-CRO-026-MAP-0007	D1-CTL-04 Federated Learning Poisoning Prevention	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0008	D1-CTL-04 Federated Learning Poisoning Prevention	T1554 Compromise Host Software Binary	Persistence	S	Low
GAISSF-CRO-026-MAP-0009	D1-CTL-05 Embedding Space Robustness	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0010	D1-CTL-05 Embedding Space Robustness	T1554 Compromise Host Software Binary	Persistence	S	Low
GAISSF-	D1-CTL-06 Post-	T1195 Supply	Initial Access	P	Medium

Record	GAISSF control	ATT&CK technique	Tactic	Rel.	Conf.
CRO-026-MAP-0011	Quantum Model Signing & Crypto Hardening	Chain Compromise			
GAISSF-CRO-026-MAP-0012	D1-CTL-07 Lora/Adapter Integrity Verification	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0013	D1-CTL-07 Lora/Adapter Integrity Verification	T1554 Compromise Host Software Binary	Persistence	S	Low
GAISSF-CRO-026-MAP-0014	D1-CTL-08 Model Merge Attack Detection	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0015	D1-CTL-08 Model Merge Attack Detection	T1554 Compromise Host Software Binary	Persistence	S	Low
GAISSF-CRO-026-MAP-0016	D1-CTL-09 Quantization Backdoor Screening	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0017	D1-CTL-09 Quantization Backdoor Screening	T1554 Compromise Host Software Binary	Persistence	S	Low
GAISSF-CRO-026-MAP-0018	D2-CTL-01 Direct Prompt Injection Prevention	T1078 Valid Accounts	Initial Access	S	Low
GAISSF-CRO-026-MAP-0019	D2-CTL-01 Direct Prompt Injection Prevention	T1218 System Binary Proxy Execution	Stealth	S	Low
GAISSF-CRO-026-MAP-0020	D2-CTL-02 Indirect Prompt Injection Prevention	T1485 Data Destruction	Impact	S	Low
GAISSF-CRO-026-MAP-0021	D2-CTL-02 Indirect Prompt Injection Prevention	T1565 Data Manipulation	Impact	S	Low
GAISSF-CRO-026-MAP-0022	D2-CTL-03 Jailbreak Resistance Testing	T1078 Valid Accounts	Initial Access	S	Low
GAISSF-CRO-026-MAP-0023	D2-CTL-03 Jailbreak Resistance Testing	T1119 Automated Collection	Collection	S	Low
GAISSF-CRO-026-MAP-0024	D2-CTL-04 Multi-Modal Injection Defense	T1595 Active Scanning	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0025	D2-CTL-04 Multi-Modal Injection Defense	T1059 Command and Scripting Interpreter	Execution	S	Low
GAISSF-CRO-026-MAP-0026	D2-CTL-05 Function Call/Tool Call Injection Prevention	T1078 Valid Accounts	Initial Access	S	Low
GAISSF-CRO-026-MAP-0027	D2-CTL-05 Function Call/Tool Call Injection Prevention	T1203 Exploitation for Client Execution	Execution	S	Low
GAISSF-CRO-026-MAP-0028	D2-CTL-06 Cross-Context Hijacking Mitigation	T1047 Windows Management Instrumentation	Execution	S	Low
GAISSF-CRO-026-MAP-0029	D2-CTL-06 Cross-Context Hijacking Mitigation	T1218 System Binary Proxy Execution	Stealth	S	Low
GAISSF-CRO-026-MAP-0030	D3-CTL-01 Least Agency Enforcement	T1133 External Remote Services	Initial Access	P	Medium
GAISSF-	D3-CTL-01 Least	T1021 Remote	Lateral Movement	P	Medium

Record	GAISSF control	ATT&CK technique	Tactic	Rel.	Conf.
CRO-026-MAP-0031	Agency Enforcement	Services			
GAISSF-CRO-026-MAP-0032	D3-CTL-01 Least Agency Enforcement	T1210 Exploitation of Remote Services	Lateral Movement	P	Medium
GAISSF-CRO-026-MAP-0033	D3-CTL-02 Inter-Agent Communication Security	T1218 System Binary Proxy Execution	Stealth	S	Low
GAISSF-CRO-026-MAP-0034	D3-CTL-02 Inter-Agent Communication Security	T1133 External Remote Services	Initial Access	S	Low
GAISSF-CRO-026-MAP-0035	D3-CTL-03 Agentic Prompt Chaining Detection	T1218 System Binary Proxy Execution	Stealth	S	Low
GAISSF-CRO-026-MAP-0036	D3-CTL-03 Agentic Prompt Chaining Detection	T1133 External Remote Services	Initial Access	S	Low
GAISSF-CRO-026-MAP-0037	D3-CTL-04 Embodied Ai Safety Controls	T1059 Command and Scripting Interpreter	Execution	S	Low
GAISSF-CRO-026-MAP-0038	D3-CTL-04 Embodied Ai Safety Controls	T1553 Subvert Trust Controls	Defense Impairment	S	Low
GAISSF-CRO-026-MAP-0039	D3-CTL-05 Multi-Agent Trust Chain Attestation	T1589 Gather Victim Identity Information	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0040	D3-CTL-05 Multi-Agent Trust Chain Attestation	T1218 System Binary Proxy Execution	Stealth	S	Low
GAISSF-CRO-026-MAP-0041	D3-CTL-06 Persistent Memory Exfiltration Prevention	T1133 External Remote Services	Initial Access	P	Medium
GAISSF-CRO-026-MAP-0042	D3-CTL-06 Persistent Memory Exfiltration Prevention	T1021 Remote Services	Lateral Movement	P	Medium
GAISSF-CRO-026-MAP-0043	D3-CTL-06 Persistent Memory Exfiltration Prevention	T1210 Exploitation of Remote Services	Lateral Movement	P	Medium
GAISSF-CRO-026-MAP-0044	D3-CTL-07 Secure Memory Lifecycle Management	T1218 System Binary Proxy Execution	Stealth	S	Low
GAISSF-CRO-026-MAP-0045	D3-CTL-07 Secure Memory Lifecycle Management	T1133 External Remote Services	Initial Access	S	Low
GAISSF-CRO-026-MAP-0046	D4-CTL-01 Ai Bill Of Materials (Ai Bom) Maintenance	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0047	D4-CTL-01 Ai Bill Of Materials (Ai Bom) Maintenance	T1584 Compromise Infrastructure	Resource Development	S	Low
GAISSF-CRO-026-MAP-0048	D4-CTL-02 Model File & Artifact Scanning	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0049	D4-CTL-02 Model File & Artifact Scanning	T1584 Compromise Infrastructure	Resource Development	S	Low
GAISSF-CRO-026-MAP-0050	D4-CTL-03 Model Hub & Registry Vetting	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0051	D4-CTL-03 Model Hub & Registry Vetting	T1584 Compromise Infrastructure	Resource Development	S	Low
GAISSF-CRO-026-	D4-CTL-04 Mcp Server Behavioral	T1195 Supply Chain	Initial Access	S	Low

Record	GAISSF control	ATT&CK technique	Tactic	Rel.	Conf.
MAP-0052	Monitoring	Compromise			
GAISSF-CRO-026-MAP-0053	D4-CTL-04 Mcp Server Behavioral Monitoring	T1584 Compromise Infrastructure	Resource Development	S	Low
GAISSF-CRO-026-MAP-0054	D4-CTL-05 Third-Party Ai Api Security Assessment	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0055	D4-CTL-05 Third-Party Ai Api Security Assessment	T1584 Compromise Infrastructure	Resource Development	S	Low
GAISSF-CRO-026-MAP-0056	D4-CTL-06 Shadow Ai Discovery & Governance	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0057	D4-CTL-06 Shadow Ai Discovery & Governance	T1049 System Network Connections Discovery	Discovery	S	Low
GAISSF-CRO-026-MAP-0058	D4-CTL-07 Ai Software Composition Analysis (Sca)	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0059	D4-CTL-07 Ai Software Composition Analysis (Sca)	T1584 Compromise Infrastructure	Resource Development	S	Low
GAISSF-CRO-026-MAP-0060	D5-CTL-01 Harmful Content Blocking	T1565 Data Manipulation	Impact	P	Medium
GAISSF-CRO-026-MAP-0061	D5-CTL-02 Pii Leakage Prevention	T1565 Data Manipulation	Impact	P	Medium
GAISSF-CRO-026-MAP-0062	D5-CTL-03 Copyright Detection	T1565 Data Manipulation	Impact	P	Medium
GAISSF-CRO-026-MAP-0063	D5-CTL-04 Ai Watermarking Robustness	T1565 Data Manipulation	Impact	P	Medium
GAISSF-CRO-026-MAP-0064	D5-CTL-05 Privacy-By-Design Verification	T1565 Data Manipulation	Impact	P	Medium
GAISSF-CRO-026-MAP-0065	D5-CTL-06 Privacy-Preserving Ml Validation	T1565 Data Manipulation	Impact	P	Medium
GAISSF-CRO-026-MAP-0066	D6-CTL-01 Human-In-The-Loop For High-Risk Actions	T1098 Account Manipulation	Persistence	S	Low
GAISSF-CRO-026-MAP-0067	D6-CTL-01 Human-In-The-Loop For High-Risk Actions	T1136 Create Account	Persistence	S	Low
GAISSF-CRO-026-MAP-0068	D6-CTL-02 Audit Trail Completeness	T1087 Account Discovery	Discovery	S	Low
GAISSF-CRO-026-MAP-0069	D6-CTL-02 Audit Trail Completeness	T1070 Indicator Removal	Stealth	S	Low
GAISSF-CRO-026-MAP-0070	D6-CTL-03 Ai Model Card Completeness	T1190 Exploit Public-Facing Application	Initial Access	S	Low
GAISSF-CRO-026-MAP-0071	D6-CTL-03 Ai Model Card Completeness	T1133 External Remote Services	Initial Access	S	Low
GAISSF-CRO-026-MAP-0072	D6-CTL-04 Ai Incident Response Readiness	T1098 Account Manipulation	Persistence	S	Low
GAISSF-CRO-026-	D6-CTL-04 Ai Incident Response	T1136 Create Account	Persistence	S	Low

Record	GAISSF control	ATT&CK technique	Tactic	Rel.	Conf.
MAP-0073	Readiness				
GAISSF-CRO-026-MAP-0074	D6-CTL-05 Model Deprecation & Decommissioning	T1190 Exploit Public-Facing Application	Initial Access	S	Low
GAISSF-CRO-026-MAP-0075	D6-CTL-05 Model Deprecation & Decommissioning	T1133 External Remote Services	Initial Access	S	Low
GAISSF-CRO-026-MAP-0076	D6-CTL-06 Third-Party Ai Vendor Governance	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0077	D6-CTL-06 Third-Party Ai Vendor Governance	T1584 Compromise Infrastructure	Resource Development	S	Low
GAISSF-CRO-026-MAP-0078	D6-CTL-07 Ai Resilience & Business Continuity	T1490 Inhibit System Recovery	Impact	S	Low
GAISSF-CRO-026-MAP-0079	D6-CTL-07 Ai Resilience & Business Continuity	T1529 System Shutdown/Reboot	Impact	S	Low
GAISSF-CRO-026-MAP-0080	D7-CTL-H01 Ai-Generated Phishing Simulation	T1566 Phishing	Initial Access	S	Low
GAISSF-CRO-026-MAP-0081	D7-CTL-H01 Ai-Generated Phishing Simulation	T1595 Active Scanning	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0082	D7-CTL-H02 Deepfake Detection Training	T1129 Shared Modules	Execution	S	Low
GAISSF-CRO-026-MAP-0083	D7-CTL-H02 Deepfake Detection Training	T1595 Active Scanning	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0084	D7-CTL-H03 Out-Of-Band Authentication	T1484 Domain or Tenant Policy Modification	Privilege Escalation	S	Low
GAISSF-CRO-026-MAP-0085	D7-CTL-H03 Out-Of-Band Authentication	T1110 Brute Force	Credential Access	S	Low
GAISSF-CRO-026-MAP-0086	D7-CTL-H04 Ai Social Engineering Ir	T1595 Active Scanning	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0087	D7-CTL-H04 Ai Social Engineering Ir	T1592 Gather Victim Host Information	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0088	D7-CTL-H05 Ai-Enhanced External Attack Defense	T1133 External Remote Services	Initial Access	S	Low
GAISSF-CRO-026-MAP-0089	D7-CTL-H05 Ai-Enhanced External Attack Defense	T1566 Phishing	Initial Access	S	Low
GAISSF-CRO-026-MAP-0090	D8-CTL-01 Eu Ai Act Risk Tier Mapping	T1595 Active Scanning	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0091	D8-CTL-01 Eu Ai Act Risk Tier Mapping	T1592 Gather Victim Host Information	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0092	D8-CTL-02 Iso 42001 Gap Analysis	T1595 Active Scanning	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0093	D8-CTL-02 Iso 42001 Gap Analysis	T1592 Gather Victim Host Information	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0094	D8-CTL-03 Gpai Technical Documentation Verification	T1596 Search Open Technical Databases	Reconnaissance	S	Low

Record	GAISSF control	ATT&CK technique	Tactic	Rel.	Conf.
GAISSF-CRO-026-MAP-0095	D8-CTL-03 Gpai Technical Documentation Verification	T1595 Active Scanning	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0096	D8-CTL-04 Dora lct Incident Reporting (Financial Sector)	T1657 Financial Theft	Impact	S	Low
GAISSF-CRO-026-MAP-0097	D8-CTL-04 Dora lct Incident Reporting (Financial Sector)	T1595 Active Scanning	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0098	D8-CTL-05 Nist Sp 800-218A Compliance Check	T1587 Develop Capabilities	Resource Development	S	Low
GAISSF-CRO-026-MAP-0099	D8-CTL-05 Nist Sp 800-218A Compliance Check	T1595 Active Scanning	Reconnaissance	S	Low
GAISSF-CRO-026-MAP-0100	D9-CTL-01 Physical Harm Boundary Enforcement	T1052 Exfiltration Over Physical Medium	Exfiltration	S	Low
GAISSF-CRO-026-MAP-0101	D9-CTL-01 Physical Harm Boundary Enforcement	T1565 Data Manipulation	Impact	S	Low
GAISSF-CRO-026-MAP-0102	D9-CTL-02 Safe State And Graceful Degradation	T1052 Exfiltration Over Physical Medium	Exfiltration	S	Low
GAISSF-CRO-026-MAP-0103	D9-CTL-02 Safe State And Graceful Degradation	T1490 Inhibit System Recovery	Impact	S	Low
GAISSF-CRO-026-MAP-0104	D9-CTL-03 Human Override And Emergency Stop	T1052 Exfiltration Over Physical Medium	Exfiltration	S	Low
GAISSF-CRO-026-MAP-0105	D9-CTL-03 Human Override And Emergency Stop	T1190 Exploit Public-Facing Application	Initial Access	S	Low
GAISSF-CRO-026-MAP-0106	D9-CTL-04 Cyber-Physical Attack Detection	T1052 Exfiltration Over Physical Medium	Exfiltration	S	Low
GAISSF-CRO-026-MAP-0107	D9-CTL-04 Cyber-Physical Attack Detection	T1078 Valid Accounts	Initial Access	S	Low
GAISSF-CRO-026-MAP-0108	D9-CTL-05 Physical Environment Integrity Monitoring	T1052 Exfiltration Over Physical Medium	Exfiltration	S	Low
GAISSF-CRO-026-MAP-0109	D9-CTL-05 Physical Environment Integrity Monitoring	T1195 Supply Chain Compromise	Initial Access	S	Low
GAISSF-CRO-026-MAP-0110	D9-CTL-06 Actuator Command Verification	T1052 Exfiltration Over Physical Medium	Exfiltration	S	Low
GAISSF-CRO-026-MAP-0111	D9-CTL-06 Actuator Command Verification	T1218 System Binary Proxy Execution	Stealth	S	Low
GAISSF-CRO-026-MAP-0112	D9-CTL-07 Physical Incident Evidence Preservation	T1565 Data Manipulation	Impact	P	Medium

11. Evidence Reuse Guidance

- Threat models, attack-path models, architecture diagrams and trust-boundary records.
- Identity, access, secrets, privileged-access and service-account evidence.
- Secure development, dependency, build, image and supplier assurance records.
- Logging, telemetry, detection, alert triage and incident-response evidence.
- Backup, restoration, resilience, denial-of-service and recovery test records.
- Red-team, purple-team, penetration-test and adversary-emulation evidence.

ATT&CK v19 changed the Enterprise tactic model: TA0005 is now Stealth and TA0112 is Defense Impairment. The source package used the pre-v19 Defense Evasion label and a legacy T1562 Impair Defenses priority entry; this revision reconciles the taxonomy and substitutes T1685 Disable or Modify Tools only for the bounded priority-inventory context. No broader successor equivalence is asserted.

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.

12. Limitations

- ATT&CK describes adversary behavior and is not a prescriptive control or compliance framework.
- A mapping does not prove prevention, detection, mitigation effectiveness, or test coverage.
- The priority technique inventory is a selected Enterprise subset and does not replace the complete official ATT&CK v19.2 dataset. ATT&CK v19 split the former Defense Evasion tactic into Stealth and Defense Impairment; this edition reconciles the source package to that current taxonomy.
- Sub-techniques and procedures require environment-specific analysis.
- Mobile and ICS domains are excluded from this edition and require separate controlled profiles.
- ATT&CK major, minor and agile content releases require impact-based source revalidation.

13. Notably Absent

- No MITRE endorsement, approval, certification, or recognition.
- No claim of complete prevention or detection of an ATT&CK technique.
- No universal ATT&CK coverage score or compliance percentage.
- No substitution for current threat intelligence, procedure analysis, detection engineering, or adversary emulation.
- No Mobile or ICS mapping in this edition.
- No claim that ATT&CK is a control framework or regulatory standard.

14. Maintenance and Revalidation

GAISSF-CRO-026 shall be reviewed after every ATT&CK major, minor or agile content release, any material GAISSF control change, new platform scope, significant threat-intelligence change, or evidence that a mapping is ambiguous or no longer operationally useful.

Annex A - Quality Assurance Record

QA check	Result
GAISSF controls inventoried	59
Enterprise tactics inventoried	15
Priority techniques in bounded inventory	100
Forward mapping records	112
Reverse tactic records	15
ATT&CK v19.2 taxonomy applied	Yes
Legacy Defense Evasion split reconciled	Yes
Legacy T1562 parent removed from current inventory	Yes
D9 additional / conditional	Yes
Automatic prevention/detection/equivalence claim prohibited	Yes
Independent crosswalk review required before publication approval	Yes