

Stellar Cyber MITRE ATT&CK Aligned Coverage Analyzer

Turn Visibility into Strategy. Map, Measure, and Maximize Your Detection Coverage.

Overview

The MITRE ATT&CK Aligned Coverage Analyzer from Stellar Cyber is a purpose-built, web-based solution that helps organizations measure and optimize how well their detection strategies align with the MITRE ATT&CK framework. Designed for cybersecurity teams, CISOs, MSSPs, and compliance officers, this tool brings transparency and actionable insights into detection posture across all data sources—giving users a clear view of how well their defenses perform against real-world adversary tactics and techniques.

As cybersecurity professionals face pressure to justify technology spend, reduce risk exposure, and ensure regulatory alignment, this analyzer provides the evidence needed to make smart, confident decisions. It transforms abstract framework coverage into tangible metrics that can inform SOC planning, support cyber insurance reviews, and strengthen client trust.

Why It Matters

In today's evolving threat landscape, it's not enough to simply have tools in place—you need to know how effective those tools really are. The Coverage Analyzer helps security teams move beyond gut feeling and toward precision measurement. Whether you're defending a smart factory, scaling an MSSP offering, or validating SOC investments, this tool empowers you to quantify and communicate your detection effectiveness—clearly, credibly, and continuously.



MITRE ATT&CK ID	MITRE ATT&CK Name	MITRE ATT&CK Category	MITRE ATT&CK Subcategory	MITRE ATT&CK Description	MITRE ATT&CK Coverage Status	MITRE ATT&CK Coverage Score	MITRE ATT&CK Coverage Details
T1001	Initial Access	Initial Access	Initial Access	Initial Access	Not Covered	0	
T1002	Execution	Initial Access	Initial Access	Execution	Not Covered	0	
T1003	Persistence	Initial Access	Initial Access	Persistence	Not Covered	0	
T1004	Privilege Escalation	Initial Access	Initial Access	Privilege Escalation	Not Covered	0	
T1005	Defense Evasion	Initial Access	Initial Access	Defense Evasion	Not Covered	0	
T1006	Credential Access	Initial Access	Initial Access	Credential Access	Not Covered	0	
T1007	Discovery	Initial Access	Initial Access	Discovery	Not Covered	0	
T1008	Lateral Movement	Initial Access	Initial Access	Lateral Movement	Not Covered	0	
T1009	Collection	Initial Access	Initial Access	Collection	Not Covered	0	
T1010	Exfiltration of Confidential Information	Initial Access	Initial Access	Exfiltration of Confidential Information	Not Covered	0	
T1011	Exfiltration of Information	Initial Access	Initial Access	Exfiltration of Information	Not Covered	0	
T1012	Exfiltration of Data	Initial Access	Initial Access	Exfiltration of Data	Not Covered	0	
T1013	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1014	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1015	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1016	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1017	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1018	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1019	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1020	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1021	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1022	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1023	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1024	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1025	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1026	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1027	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1028	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1029	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1030	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1031	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1032	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1033	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1034	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1035	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1036	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1037	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1038	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1039	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1040	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1041	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1042	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1043	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1044	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1045	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1046	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1047	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1048	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1049	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1050	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1051	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1052	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1053	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1054	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1055	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1056	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1057	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1058	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1059	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1060	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1061	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1062	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1063	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1064	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1065	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1066	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1067	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1068	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1069	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1070	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1071	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1072	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1073	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1074	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1075	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1076	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1077	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1078	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1079	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1080	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1081	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1082	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1083	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1084	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1085	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1086	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1087	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1088	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1089	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1090	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1091	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1092	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1093	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1094	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1095	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1096	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1097	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1098	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1099	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	
T1100	Exfiltration of Data to Cloud	Initial Access	Initial Access	Exfiltration of Data to Cloud	Not Covered	0	

Use Cases



Coverage Validation and Gap Identification

Pinpoint gaps in your threat detection capability across MITRE ATT&CK tactics and techniques, broken down by data source and alert type. Visualize areas where coverage is strong, weak, or entirely missing.



Optimizing Telemetry Strategy

Model how adding or removing data sources—such as EDR, NDR, identity logs, or SIEM inputs—affects overall detection coverage. Simulate the return on investment of each new sensor, tool, or platform before committing resources.



Cyber Insurance and Risk Reporting

Create clear, defensible documentation of your detection program's strength and maturity. Useful for policy underwriting, security questionnaires, and board-level risk reporting.



Multi-Tenant MSSP Management

For MSSPs, analyze ATT&CK-aligned detection metrics across your client base in a single dashboard. Quickly identify which clients need enrichment, triage improvement, or rebalanced coverage.

Deployment



Flexible Deployment Options

Includes a fully contained Docker Compose version for customers operating in restricted environments, enabling localized installation and use behind VPNs or proxies.



Multi-Tenant Aware

Supports selection and analysis of different tenants or clients from a shared MSSP instance, with configurable alert time windows and scope.

Core Capabilities



Real-Time Detection Coverage Mapping

Dynamically maps alerts and data sources to specific MITRE ATT&CK tactics and techniques. Delivers instant visual feedback on your coverage footprint.



Simulated Architecture Changes

Add or remove specific data sources to model how your detection posture improves or weakens. Helps SOC leaders and architects prioritize next investments.



Custom and System Alert Inclusion

Tracks both native Stellar detections and user-created or custom alerts, helping teams understand how well their tuning efforts align with adversary techniques.



Quantitative Metrics for Decision-Making

Provides detailed, percent-based breakdowns of coverage—by tactic, technique, and category—so teams can make data-driven improvements.



Built-in Recommendations Engine

Intelligent suggestions show which additional data sources or alert types will yield the greatest coverage improvement per cost or complexity added.



Reporting & Export



Comprehensive Multi-Format Reporting

Download detailed ZIP reports with multiple export types:

- MITRE Navigator layer files (JSON)
- Excel spreadsheets
- CSV tables with metrics and recommendations



Rich Metadata for Analysis or Integration

Reports include detailed breakdowns of tactics, techniques, alert types, data source mappings, and coverage deltas—ideal for importing into other tools or visualizations.



Board and Compliance Ready

Exportable summaries are suitable for CISO-level reporting, vendor security questionnaires, or evidence for compliance with frameworks like NIST CSF, IEC 62443, or ISO 27001.

Visual Interface & Navigation



ATT&CK Navigator Visualization

Integration with the MITRE ATT&CK Navigator for interactive visual exploration of detection coverage and deep analysis.



Interactive Tables and Filters

Includes sortable, filterable tables showing each tactic, technique, and detection source. Enables teams to drill down into exactly what's covered, by whom, and how.



Color-Coded Differentiation

Distinguishes between coverage already achieved and coverage added through simulation. Clearly shows how each data source contributes to overall coverage.



Toggle Between Views

Switch between Stellar Cyber-specific coverage (alerts from within the platform) and a generalized MITRE ATT&CK view to see full theoretical potential.

Performance & Enhancements



High-Performance Architecture

Fully reengineered for enhanced speed and responsiveness. Handles larger datasets and broader analysis windows with ease.



Backward-Compatible Experience

Maintains a familiar user experience from previous versions while introducing expanded functionality and improved UI performance.



Scales with You

Equally effective for enterprises managing a single environment or MSSPs managing dozens of tenants. Built to support dynamic environments and hybrid deployments.

By shining a bright light on the darkest corners of security operations, Stellar Cyber empowers organizations to see incoming attacks, know how to fight them, and act decisively – protecting what matters most. Stellar Cyber's award-winning open security operations platform includes NG SIEM, NDR, Open XDR, and Multi-Layer AI™ under one license. With almost 1/3 of the top 250 MSSPs and over 14,000 customers worldwide, Stellar Cyber is one of the most trusted leaders in security operations. Learn more at <https://stellarcyber.ai/>.