




A JOURNEY FROM **CRISP** TO **ATLAS**

Points of Contact:

- Eric Kaden (eric.j.kaden.mil@army.mil)

As of: 21 MAY 25

whoami

 [linkedin.com/in/eric-kaden](https://www.linkedin.com/in/eric-kaden)

Eric Kaden

AI/ML COMPUTER SCIENTIST | DATA SCIENTIST | CYBERSECURITY | LEADER

Accomplished data scientist with 15+ years leading data science teams for data-driven decision-making through actionable insights.



Formerly

Chief Data Scientist

Cyber Protection Brigade, Army Cyber Command

Currently

Analytic Support Officer / Data Scientist

Task Force Morpheus, Army Reserves Cyber Protection Brigade



Lead Data Scientist

Data Machines

Research with DARPA & PSU Applied Research Laboratory for the intelligence community

 Data Science + Cybersecurity =

Introducing CRISP

Cyber Readiness Inspection Statistics Platform (CRISP) converts STIG-based Cyber Operational Readiness Assessment (CORA) data to MITRE ATT&CK® Navigator JSON layers with comprehensive statistical processing in just a few steps. It generates a heatmap of the overlap between CORA and threat groups, making it easy to identify gaps in security to harden the system.



TechnologyArea	Vuln ID	Severity	STIG ID	Status	NIST SP 800-53 Rev 4
UNIX OS	V-230221	high	RHEL-08-010000	Not A Finding	CM-6 b
UNIX OS	V-230222	medium	RHEL-08-010010	Not A Finding	CM-6 b
UNIX OS	V-230223	high	RHEL-08-010020	Not A Finding	AC-17 (2)
UNIX OS	V-230224	medium	RHEL-08-010030	Open	SC-28
UNIX OS	V-230225	medium	RHEL-08-010040	Not A Finding	AC-8 a
UNIX OS	V-230226	medium	RHEL-08-010050	Not Applicable	AC-8 a
UNIX OS	V-230227	medium	RHEL-08-010060	Not A Finding	AC-8 a
UNIX OS	V-230228	medium	RHEL-08-010070	Not A Finding	AC-17 (1)
UNIX OS	V-230229	medium	RHEL-08-010090	Open	IA-5 (2) (a)
UNIX OS	V-230230	medium	RHEL-08-010100	Not A Finding	IA-5 (2)
UNIX OS	V-230231	medium	RHEL-08-010110	Not A Finding	IA-5 (1) (c)
UNIX OS	V-230232	medium	RHEL-08-010120	Not A Finding	IA-5 (1) (c)
UNIX OS	V-230233	medium	RHEL-08-010130	Not A Finding	IA-5 (1) (c)



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques
Active Scanning (0/2)	Acquire Access (0/8)	Content Injection (0/10)	Cloud Administration Command (0/14)	Account Manipulation (1/8)	Abuse Elevation Control Mechanism (1/14)	Abuse Elevation Control Mechanism (1/43)	Adversary-in-the-Middle (1/17)	Account Discovery (1/32)	Exploitation of Remote Services (1/9)	Adversary-in-the-Middle (2/17)	Application Layer Protocol (1/17)	Automated Exfiltration (1/9)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise (0/10)	Command and Scripting Interpreter (1/14)	BITS Jobs (0/20)	Access Token Manipulation (1/14)	Access Token Manipulation (1/43)	Brute Force (1/17)	Application Window Discovery (1/32)	Internal Spearphishing (1/9)	Archive Collected Data (0/17)	Communication Through Removable Media (1/17)	Data Transfer Size Limits (1/9)
Gather Victim Identity Information (0/2)	Compromise Accounts (0/8)	Exploit Public-Facing Application (0/10)	Container Administration Command (0/14)	Boot or Logon Autostart Execution (7/14)	Account Manipulation (1/14)	BITS Jobs (1/43)	Credentials from Password Stores (1/17)	Browser Information Discovery (1/32)	Lateral Tool Transfer (1/9)	Audio Capture (1/17)	Content Injection (1/17)	Exfiltration Over Alternative Protocol (1/9)
Gather Victim Network Information (0/2)	Compromise Infrastructure (0/8)	External Remote Services (0/10)	Deploy Container (0/14)	Boot or Logon Initialization Scripts (0/20)	Account Manipulation (1/14)	Debugger Evasion (1/43)	Exploitation for Credential Access (1/17)	Cloud Service Dashboard (1/32)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Data Encoding (1/17)	Exfiltration Over C2 Channel (1/9)
Gather Victim Org Information (0/2)	Develop Capabilities (0/8)	Hardware Additions (0/10)	Exploitation for Client Execution (0/14)	Browser Extensions (0/20)	Deobfuscate/Decode Files or Information (1/14)	Deobfuscate/Decode Files or Information (1/43)	Exploitation for Credential Access (1/17)	Cloud Service Discovery (1/32)	Remote Services (1/9)	Browser Session Hijacking (1/17)	Data Obfuscation (1/17)	Exfiltration Over Network Medium (1/9)
Phishing for Information (0/2)	Establish Accounts (0/8)	Phishing (1/10)	Inter-Process Communication (0/14)	Compromise Software Binary (0/20)	Boot or Logon Autostart Execution (7/14)	Direct Volume Access (1/43)	Forge Web Credentials (1/17)	Cloud Storage Object Discovery (1/32)	Replication Through Removable Media (1/9)	Clipboard Data (1/17)	Dynamic Resolution (1/17)	Exfiltration Over Other Network Medium (1/9)
Search Closed Sources (0/2)	Obtain Capabilities (0/8)	Replication Through Removable Media (0/10)	Native API (0/14)	Create Account (0/20)	Boot or Logon Initialization Scripts (0/20)	Domain Policy Modification (0/43)	Input Capture (1/17)	Container and Resource Discovery (1/32)	Software Deployment Tools (1/9)	Data from Cloud Storage (1/17)	Encrypted Channel (1/17)	Exfiltration Over Physical Medium (1/9)
Search Open Technical Databases (0/2)	Stage Capabilities (0/8)	Supply Chain Compromise (0/10)	Scheduled Task/Job (1/14)	Create or Modify System Process (1/20)	Create or Modify System Process (1/20)	Exploitation for Defense Evasion (1/43)	Modify Authentication Process (1/17)	Device Driver Discovery (1/32)	Taint Shared Content (1/9)	Data from Configuration (1/17)	Fallback Channels (1/17)	Exfiltration Over Web Service (1/9)
Search Open Websites/Domains (0/2)	Trusted Relationship (0/8)	Valid Accounts (1/10)	Shared Modules (0/14)	Event Triggered Execution (1/20)	Domain Policy Modification (1/20)	File and Directory Permissions Modification (0/43)	Multi-Factor Authentication Interception (1/17)	Domain Trust Discovery (1/32)	Use Alternate Authentication Material (1/9)	Data from Information Repositories (1/17)	Multi-Stage Channels (1/17)	Exfiltration Over Web Service (1/9)
Search Victim-Owned Websites (0/2)			Software Deployment Tools (0/14)	External Remote Services (1/20)	Escape to Host (1/20)	Hide Artifacts (2/11)	Multi-Factor Authentication Request Generation (1/17)	File and Directory Discovery (1/32)		Data from Local System (1/17)	Non-Application Layer Protocol (1/17)	Scheduled Transfer (1/9)
			System Services (1/14)	Hijack (1/20)	Impersonation (1/20)	Impersonation (1/43)	Network Sniffing (1/17)	Log Enumeration (1/32)		Data from Network Shared Drive (1/17)	Non-Standard Port (1/17)	Transfer Data to Cloud (1/9)



Security Technical Implementation Guides



CRISP converts STIG-based Cyber Operational Readiness Assessment (CORA) data to MITRE ATT&CK® Navigator JSON layers with comprehensive statistical processing in just a few steps. It generates a heatmap of the overlap between CORA and threat groups, making it easy to identify gaps in security to harden the system.

Target Users

- Cybersecurity Auditors
- Network/Host Analysts
- Security Administrators



CORA

Cyber Operational Readiness Assessment

DISA

STIG

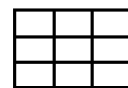
DATA SOURCES



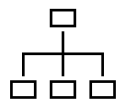
PARSING



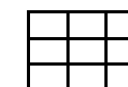
Raw Data



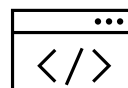
Parsed Data



MAPPING



Parsed Data



ATT&CK

DATA ENGINEERING



ANALYSIS

- Statistics
- Score Normalization
 - Values between 1 and 10
- Threat Actor Matching
 - Compares Source Techniques to Threat Actor Techniques
 - Identifies Top Matches
 - Generates Heatmaps



VISUALIZATION

ATT&CK
Tech
IDs

Scores



ASSESSMENT



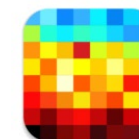
Navigator



Mapping

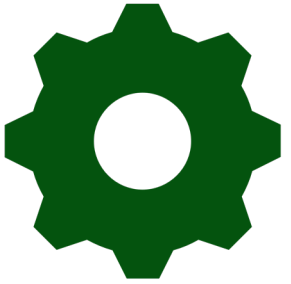


THREAT ACTORS



Match Overlap
% Heatmap

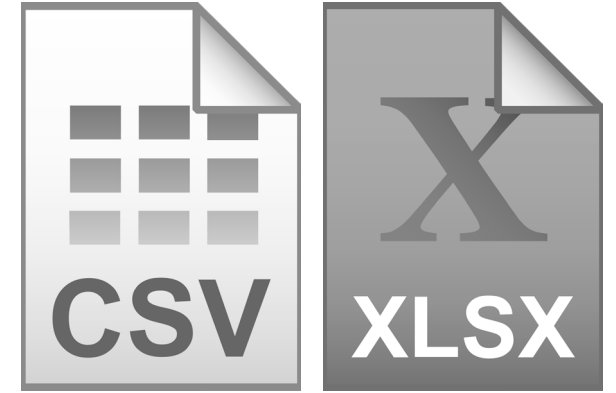
OUTPUT



Simple Customization



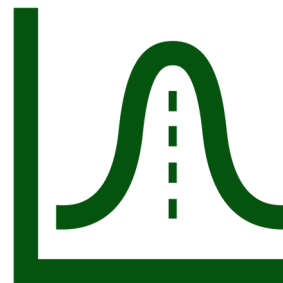
Automatic Data Updates



Versatile Output for Reporting



Easy to Use



Sophisticated Statistics



Overlap Heatmaps



ATLAS

Automated Threat Landscape Assessment System

ATLAS transforms complex cybersecurity data into visually digestible threat landscapes and actionable insights through MITRE ATT&CK Navigator heatmaps. By mapping data sources to MITRE ATT&CK for enhanced clarity, ATLAS provides organization's security posture at a glance that enables informed prioritization of resources and proactive mitigation strategies while facilitating data-driven decision-making.

Target Users

- Analytic Support Officers
- Network/Host Analysts
- Cyber Threat Intelligence Analysts



CORA

Cyber Operational Readiness Assessment



STIG



IONIC



Zeek



EVTX



TYCHON



CVEs

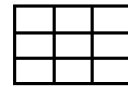
DATA SOURCES



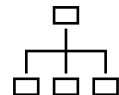
PARSING



Raw Data



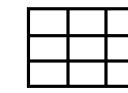
Parsed Data



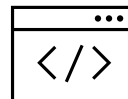
MAPPING



References



Parsed Data



ATT&CK

DATA ENGINEERING

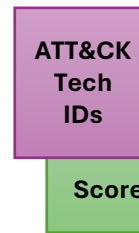


ANALYSIS

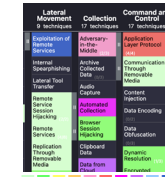
- Statistics
- Score Normalization
 - Values between 1 and 10
- Threat Actor Matching
 - Compares Source Techniques to Threat Actor Techniques
 - Identifies Top Matches
 - Generates Heatmaps



VISUALIZATION



ASSESSMENT



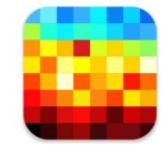
Navigator



Mapping



THREAT ACTORS



Match Overlap %
Heatmap

OUTPUT