# 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**


## 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

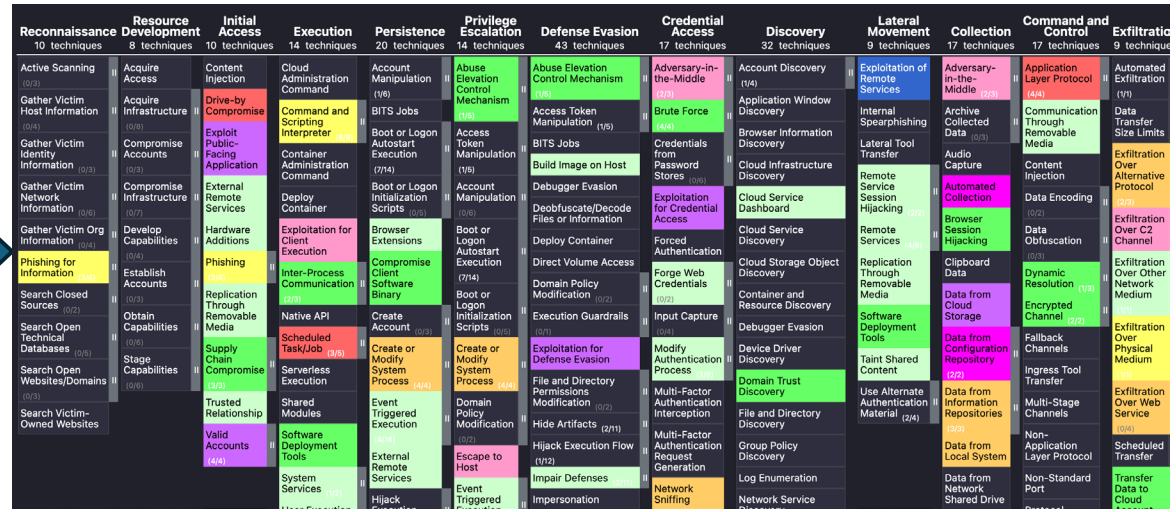
Research with DARPA & PSU Applied Research Laboratory for the intelligence community

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) |




DISA Security Technical Implementation Guides

MITRE ATT&CK™

# 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.

Target Users

- Cybersecurity Auditors
- Network/Host Analysts
- Security Administrators

CORA

Cyber Operational Readiness Assessment

DISA STIG

DATA SOURCES

## PARSING

pandas

Raw Data → Parsed Data

## MAPPING

NIST SP 800-53

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

→ JSON

ASSESSMENT

ATT&CK® MITRE

JSON Navigator

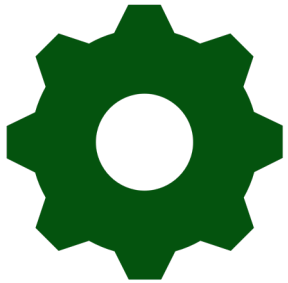
CSV Mapping

THREAT ACTORS

CSV XLSX Match Overlap % Heatmap

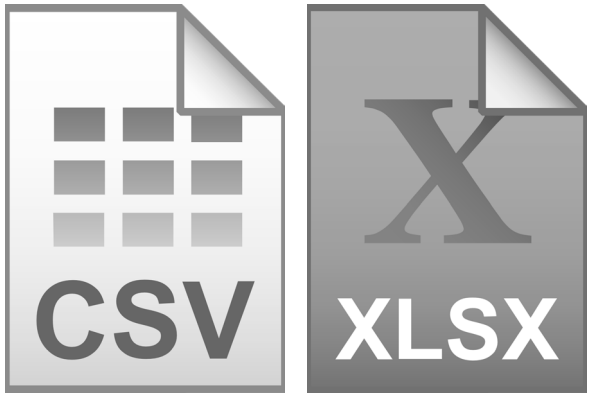
OUTPUT

# Features



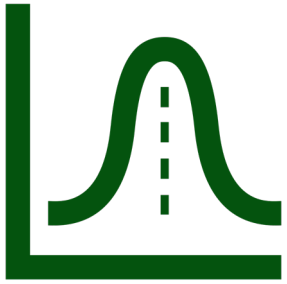
**Simple Customization**

**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.

<u>Target Users</u>
- Analytic Support Officers
- Network/Host Analysts
- Cyber Threat Intelligence Analysts

### CORA
Cyber Operational Readiness Assessment

DISA STIG

### IONIC
Zeek EVTX TYCHON CVEs

**DATA SOURCES**

### PARSING
pandas

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
ATT&CK Tech IDs + Scores → JSON

**ASSESSMENT**

### MITRE
ATT&CK

JSON Navigator

CSV Mapping

### THREAT ACTORS
CSV XLSX Match Overlap % Heatmap

**OUTPUT**