MITRE ENGENUITY™ | Center for Threat Informed Defense

Mapping Platform Security Stacks to ATT&CK: Data Format, Rubric & Methodology

Nicholas Amon

June 2021

TLP:WHITE

Nicholas Amon

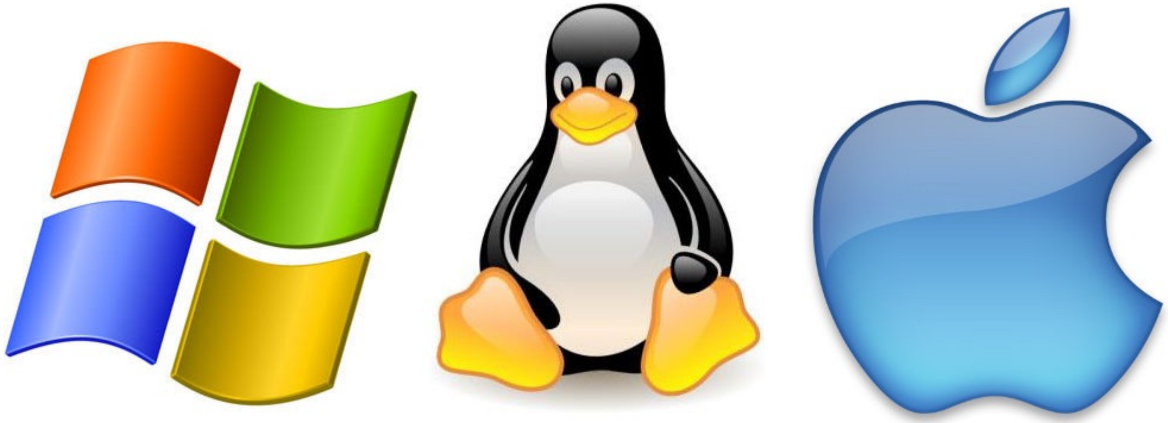
- Lead Cyber Security Engineer
- Cyber Threat Intel &
  Adversary Emulation @ MITRE
- Project Leader @
  Center for Threat-Informed Defense

Contact me at:
namon@mitre-engenuity.org

TLP:WHITE

What is Security Stack Mappings?

Empower defenders with independent data on which native security controls on a platform are most useful in defending against the ATT&CK TTPs which they care about.



Azure Security Stack Mappings

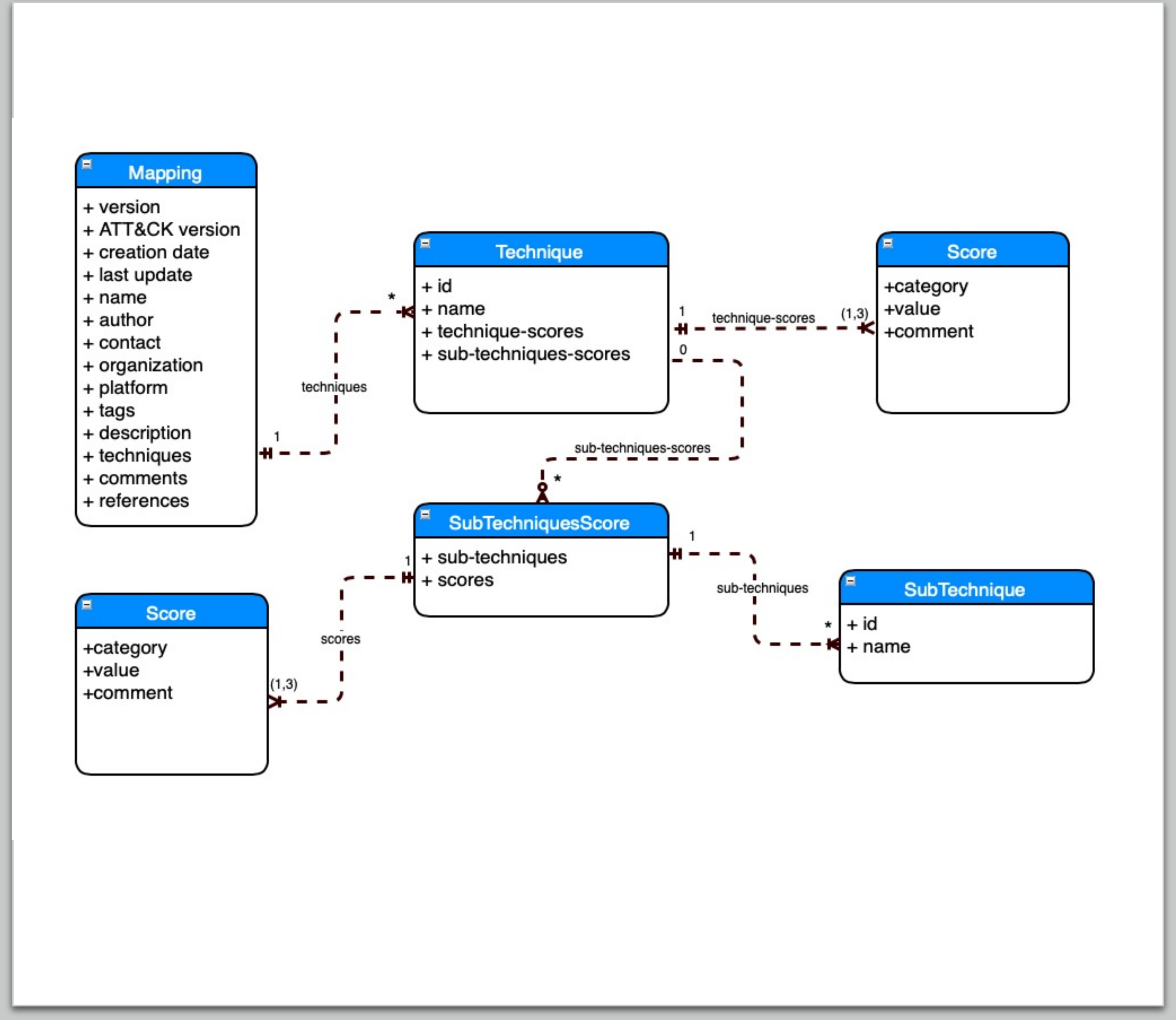
Problem: Users of Azure lack a comprehensive view of how security controls native to the platform can help defend against real-world adversary TTPs.

Solution: Build a methodology and scoring rubric and use it to create mappings showing how effective native Azure security controls are in defending against specific ATT&CK techniques.

Impact: Empowers defenders with independent data on which Azure controls are most useful in defending against the adversary TTPs they care about.

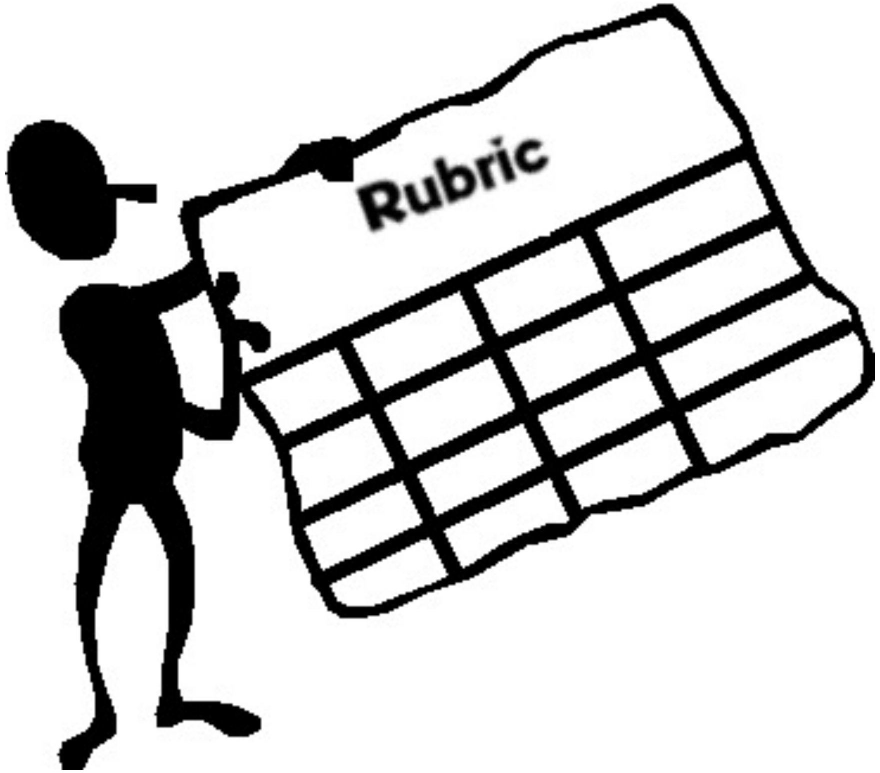
YAML Mapping Data Format

- Describes the mapping of a native control to ATT&CK (sub-)techniques.
- Score at technique level and sub-techniques level.
- Score sub-techniques as a group.
- Support commenting at multiple levels.



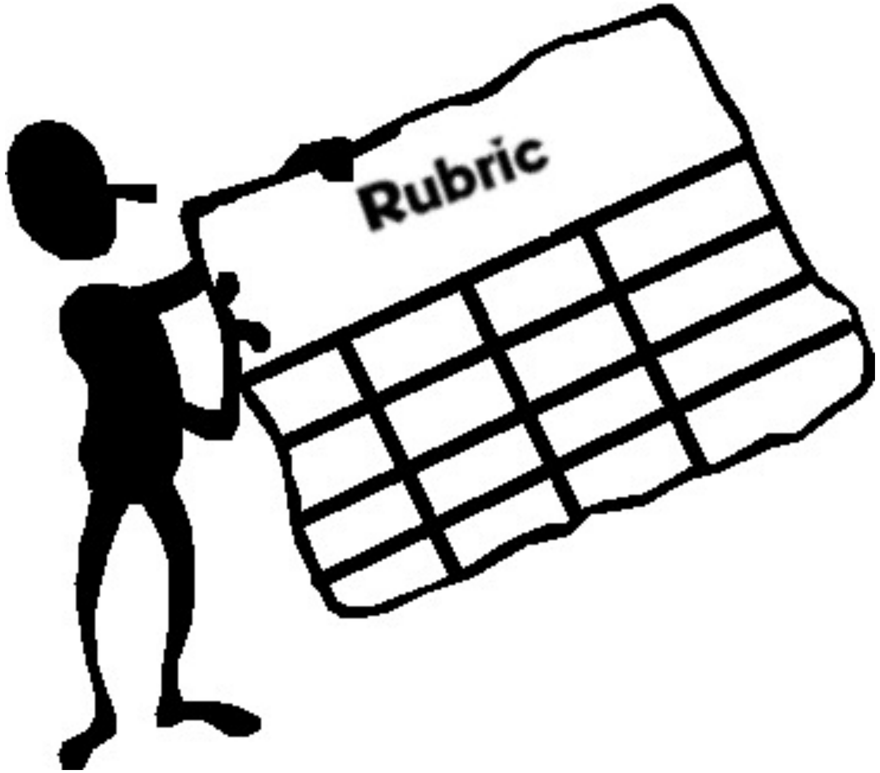
Scoring Rubric

- **Categories**:
  - **Protect**: prevents the execution of an ATT&CK TTP.
  - **Detect:** detects the execution of an ATT&CK TTP.
  - **Respond:** responds to the execution of an ATT&CK TTP.
- **Scores:**
  - **Minimal**
  - **Partial**
  - **Significant**



Scoring Rubric

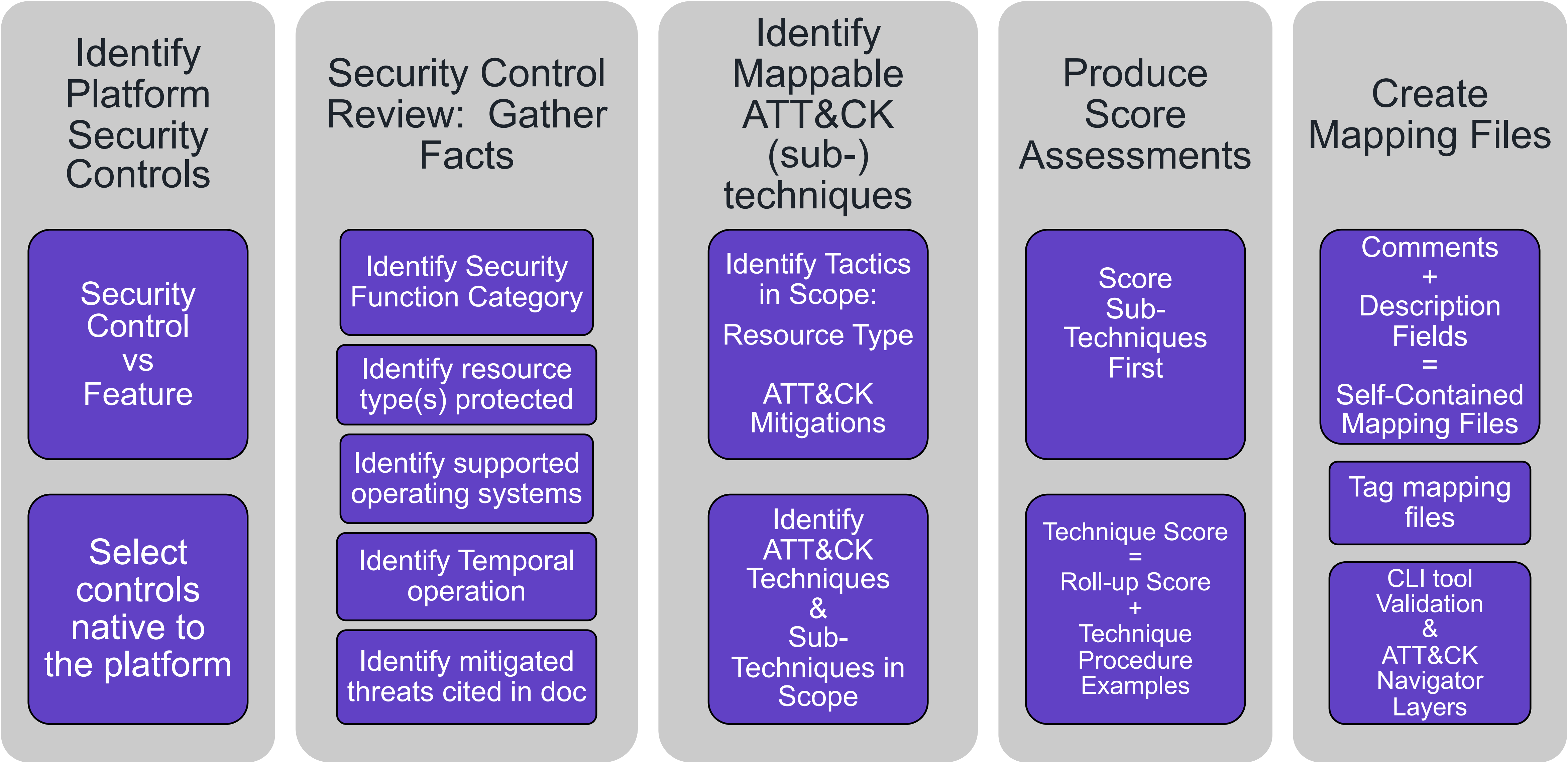
- **Categories**:
  - **Protect**: prevents the execution of an ATT&CK TTP.
  - **Detect**: detects the execution of an ATT&CK TTP.
  - **Respond**: responds to the execution of an ATT&CK TTP.
- **Scores:**
  - **Minimal**
  - **Partial**
  - **Significant**



Scoring Rubric: Scoring Factors

- **Protect & Detect Scoring Factors:**
  - Coverage
  - Accuracy
  - Temporal
- **Respond Scoring Factors:**
  - Coverage
  - Type of Response:
    - Enrichment (Minimal)
    - Containment (Partial)
    - Eradication (Significant)

Mapping Methodology



Identify Platform Security Controls

Security Control vs Feature

Select controls native to the platform

Security Control Review: Gather Facts

Identify Security Function Category

Identify resource type(s) protected

Identify supported operating systems

Identify Temporal operation

Identify mitigated threats cited in doc

Identify Mappable ATT&CK (sub-) techniques

Identify Tactics in Scope:

Resource Type

ATT&CK Mitigations

Identify ATT&CK Techniques & Sub-Techniques in Scope

Produce Score Assessments

Score Sub-Techniques First

Technique Score = Roll-up Score + Technique Procedure Examples

Create Mapping Files

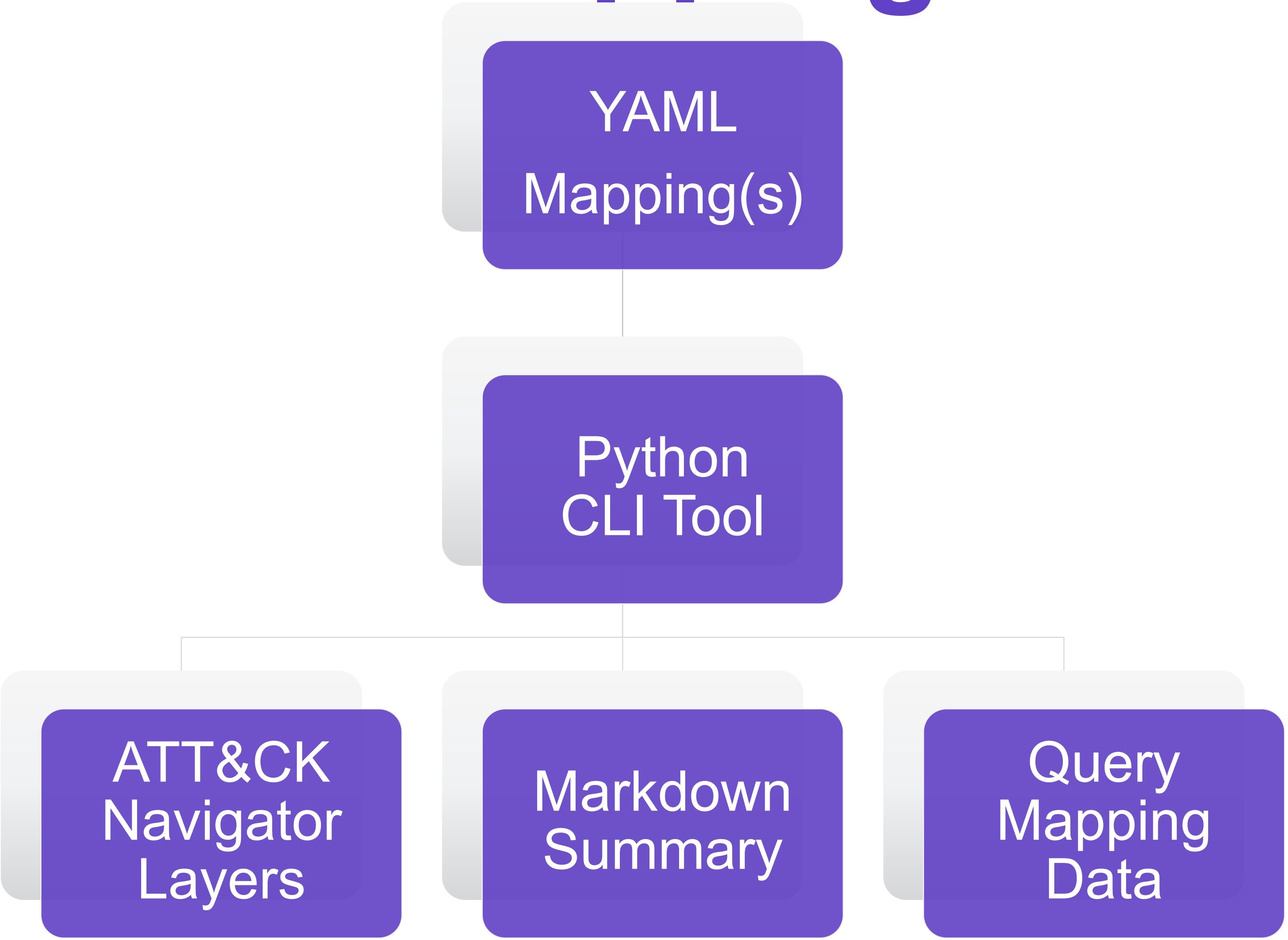
Comments + Description Fields = Self-Contained Mapping Files

Tag mapping files

CLI tool Validation & ATT&CK Navigator Layers

TLP:WHITE

CLI Mapping Tool



- Inputs:
  - YAML mapping(s)
- Functionality:
  - Validate YAML
  - Convert to visualization formats
  - Query mapping data by score, tactic, control, (sub-)technique, etc.
- Output
  - ATT&CK Navigator layers
  - Markdown Summary

Example Use Cases

- Determine the ATT&CK (sub-)technique coverage of a platform security control.
- Better understand what security controls to select/implement in order to mitigate a specific set of ATT&CK (sub-)techniques.

June 2021

CTID GitHub
https://github.com/center-for-threat-informed-defense

TLP:WHITE