MITRE ENGENUITY | Center for Threat Informed Defense

New Resources from the Center

Richard Struse

EU ATT&CK Community Workshop: June 1, 2021

TLP:WHITE

Together, we are changing
the rules of the game

Members as of April 2021

All Center R&D project outputs are made freely-available to the world

+

MITRE

SOLVING PROBLEMS FOR A SAFER WORLD™

The center
by the numbers

Advancing the state of the art and the state of the practice in threat-informed defense globally

Mission:
1

Months old:
18

Members:
25

Sponsors per project (average):
4

Ideas in pipeline:
35

Projects underway:
8

Published projects:
6

Completed Project Highlights

Adversary Emulation Plans

FIN6, menuPass

Problem: Understanding defenses from the adversary perspective is critical, but teams often lack the resources to conduct effective adversary emulation

Solution: Establish a library of standardized intelligence-driven adversary emulation plans that can be easily leveraged by defenders

Impact: Greatly reduce time & cost for defenders to test their defenses against real-world adversary TTPs

Published: Sep 2020, Feb 2021

Center R&D outputs available at:

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

Security Control Mappings

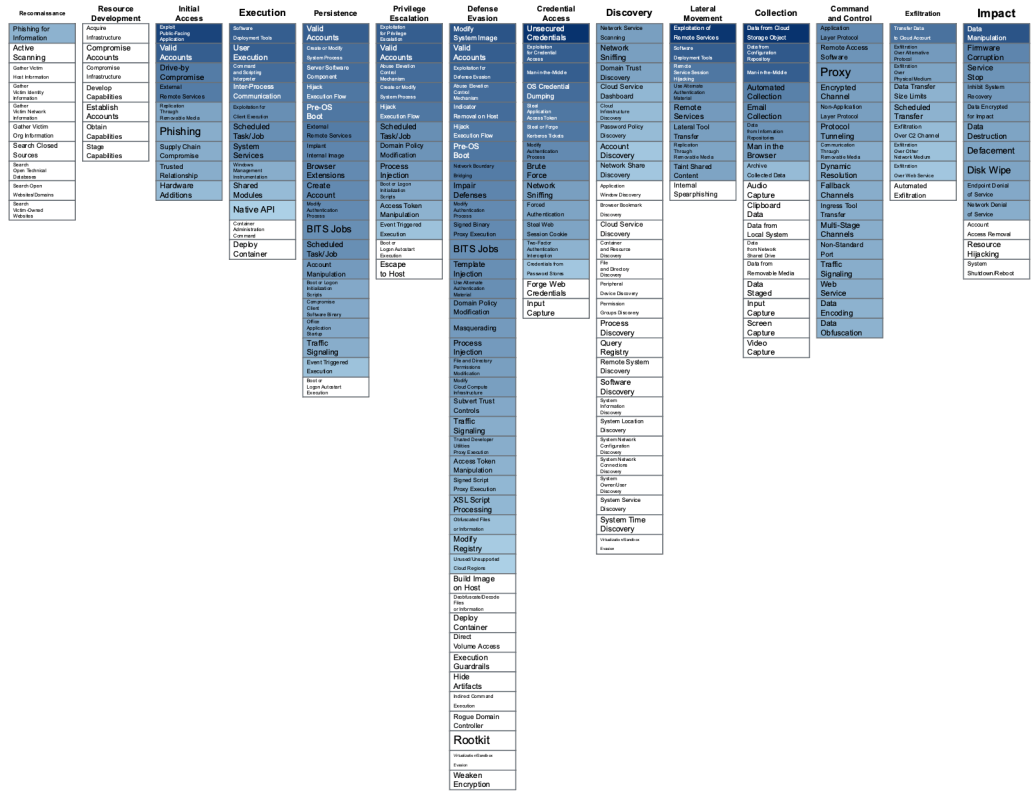
Controls Mappings

Problem: Defenders struggle to relate large and unwieldy security control frameworks such as NIST 800-53 to TTPs in ATT&CK

Solution: Create a comprehensive and open, curated set of mappings between 800-53 controls and ATT&CK techniques

Impact: Defenders can quickly and easily focus on understanding how the controls in use in their environment relate to adversary TTPs of interest to them

Published: Dec 2020



MITRE ENGENUITY | Center for Threat Informed Defense

Container Techniques

Container Techniques

Problem: Defenders lack visibility into adversary behaviors in and against container technologies leaving their organizations exposed to emerging threats

Solution: Expand MITRE ATT&CK to describe adversary behaviors in and against container technologies including Docker and Kubernetes

Impact: Brings focus to adversary behaviors in an emergent domain leveraging the well-understood and widely adopted ATT&CK methodology

Published: April 2021

This project's outputs have been directly incorporated into ATT&CK

Running Project Preview

Upcoming Mapping Projects

Security Mapping: Other Platforms

Problem: Users of various platforms lack a comprehensive view of how native security controls can help defend against real-world adversary TTPs

Solution: Build a scoring methodology and use it to create mappings showing how effective each security control is in defending against specific ATT&CK techniques

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

Release Date: Beginning June 2021

- Look for the Center to release mappings for various cloud service providers and operating systems
- Will be released on GitHub

Sightings Ecosystem

Sightings Ecosystem

Problem: Defenders lack visibility into which adversary behaviors they should focus their attention on first

Solution: Build and operate a way for organizations to safely contribute sightings of specific ATT&CK TTPs powering analytics that give defenders a picture of what TTPs are used where and when

Impact: Injects real-world data and insights from that data into the decision-making process of defenders, allowing them to focus their resources on the highest-priority problems

Release Date: Dec 2021

A notional, data driven technique prioritization based on last 30 days. Red techniques are most frequently seen. Unmarked techniques were not seen.

- Looking for data contributors
- https://medium.com/mitre-engenuity/tracking-adversary-footprints-e37668a0d665
- For more information, email ctid@mitre-engenuity.org

ATT&CK Workbench

ATT&CK Workbench

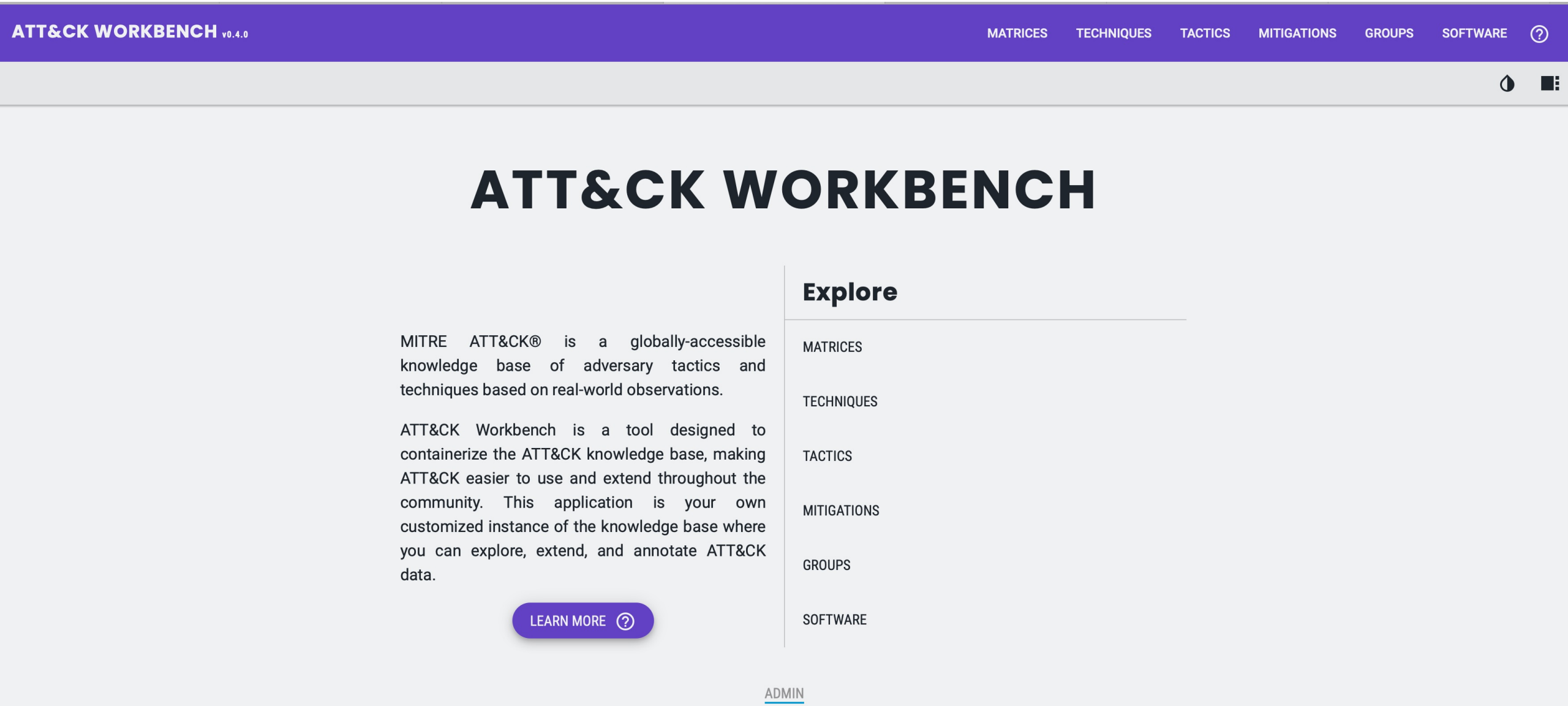
Problem: Defenders struggle to integrate their organization's local knowledge of adversaries and their TTPs with the public ATT&CK knowledge base

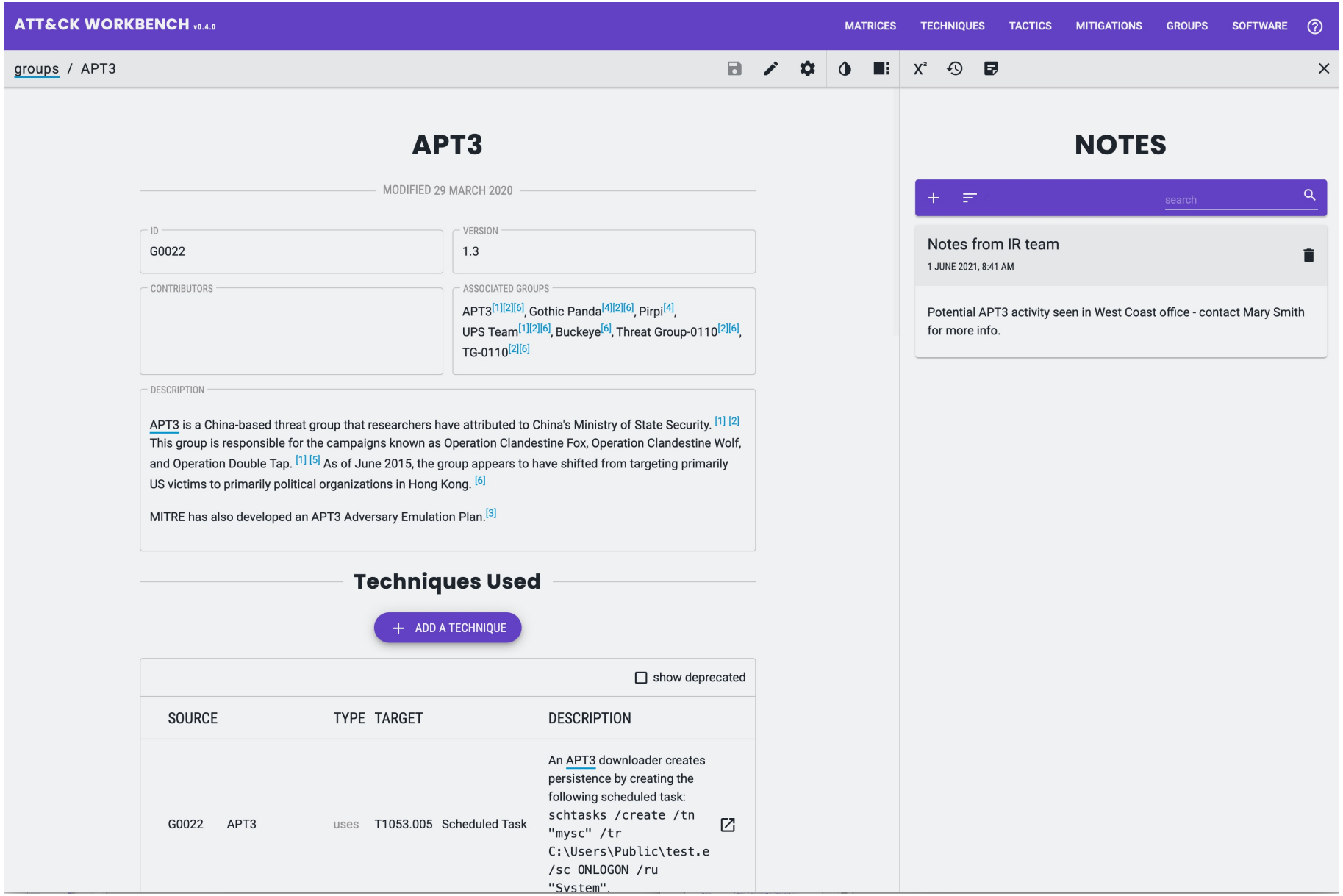
Solution: Build an easy-to-use open-source software tool that allows organizations to manage and extend their own local version of ATT&CK and keep it in sync with MITRE's knowledge base

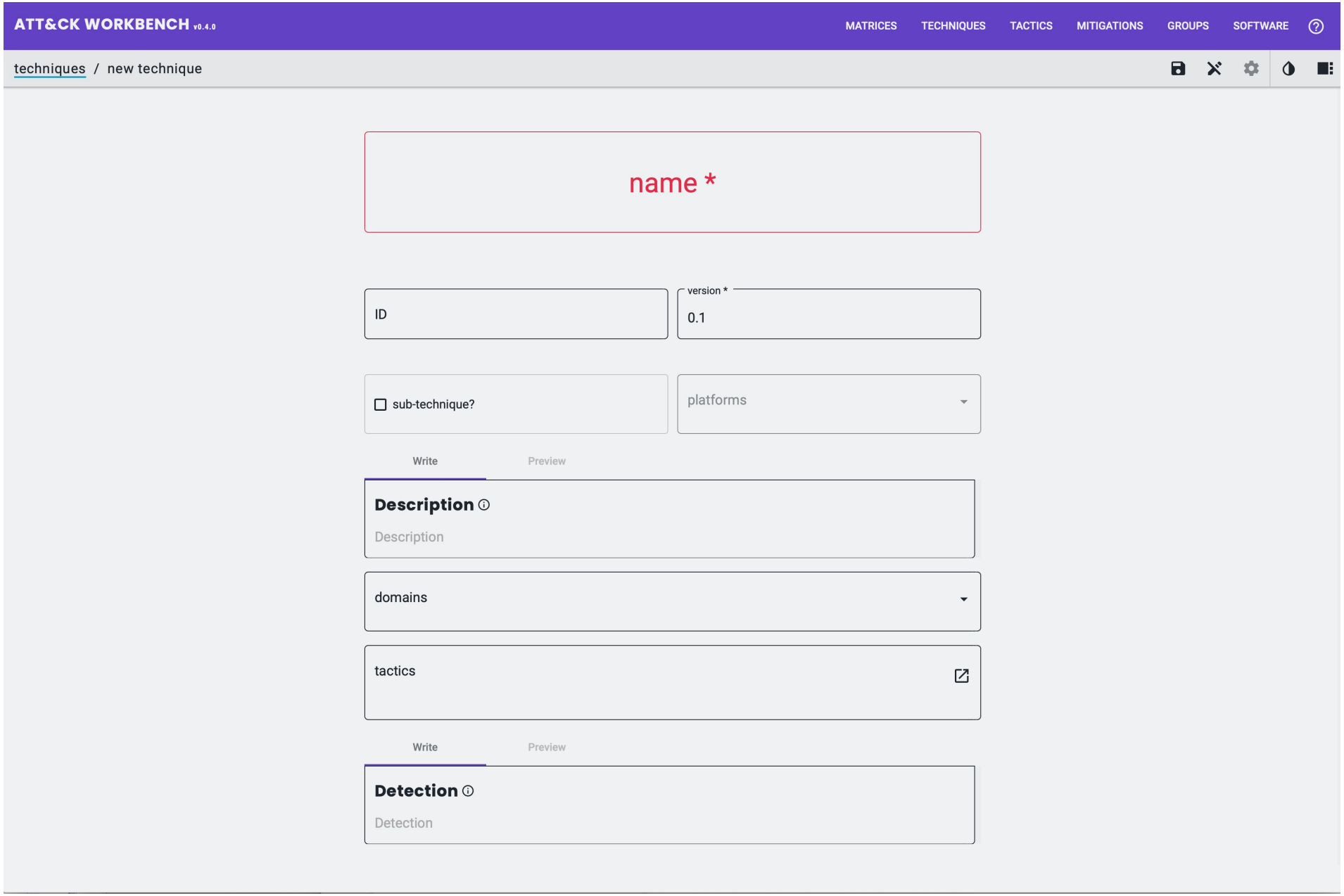
Impact: Drastically reduces the barriers for defenders to ensure that their threat intelligence is aligned with the public ATT&CK knowledge base

Release Date: June 2021

- Scheduled to be released on GitHub later this month!







To sign up for updates from the Center, visit:
https://share.hsforms.com/1fBf6rPTLT8-ROom3UUCG5w4m7ji

Thank you!

www.mitre-engenuity.org/ctid