Updates from the Center for Threat-Informed Defense

Changing the game on the adversary

Jon Baker
Director, Center for Threat-Informed Defense
March 7, 2025

MITRE | Center for Threat Informed Defense™

FIVE

Center for Threat Informed Defense™

Changing the game on the adversary

© 2025 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE. DOCUMENT NUMBER CT0127

How do we scale MITRE ATT&CK?

7 years ago…

rapid community growth
tremendous passion
massive demand

… refine the model …
… expand the knowledge base …
… operationalize it …

© 2024 MITRE Engenuity, LLC. Approved for Public Release. Document number CT0129

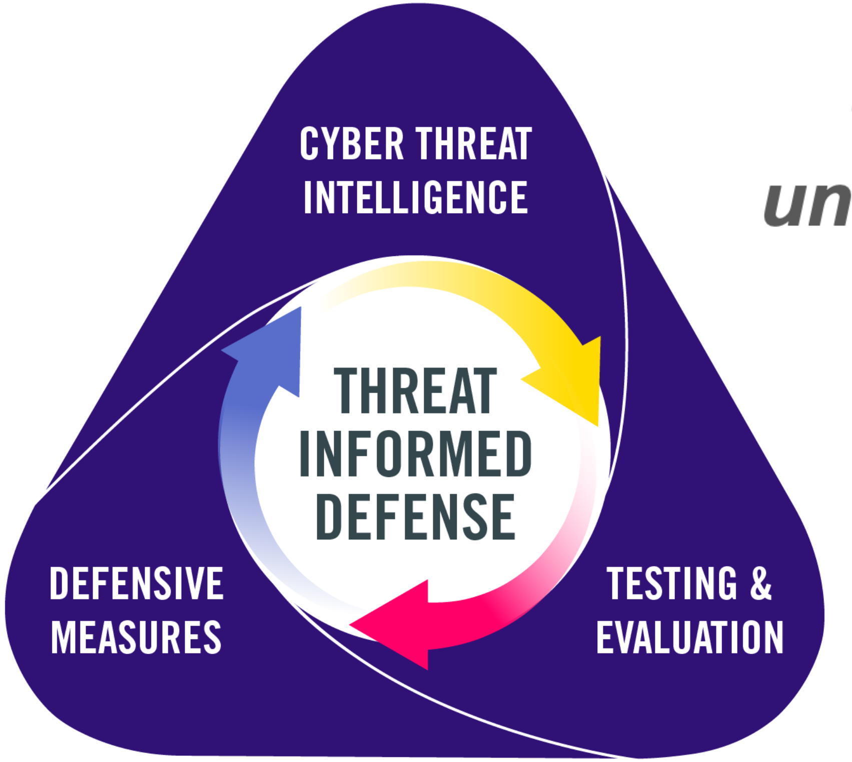
3 meetings demonstrated an opportunity

- Heavily using ATT&CK and invested in its success
- Wanted more ATT&CK faster and willing to help
- Saw MITRE as a connector to unite defenders in operationalizing ATT&CK

How do we harness this energy to improve cyber defense for all?

© 2024 MITRE Engenuity, LLC. Approved for Public Release. Document number CT0129

It was broader than ATT&CK



Threat-Informed Defense

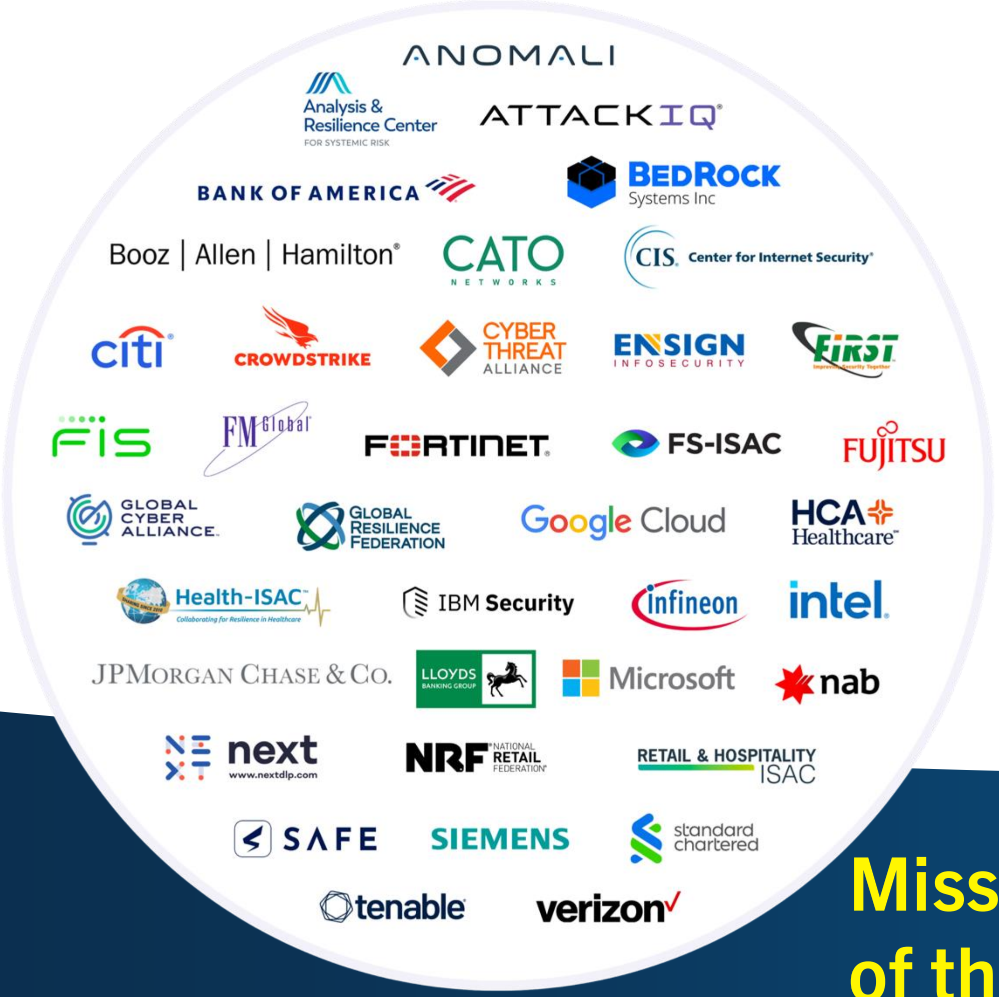
"The systematic application of a deep understanding of adversary tradecraft and technology to improve defenses."

ATT&CK® is at the core of threat-informed defense

How Do We Scale Threat-Informed Defense?

The Center for Threat-Informed Defense conducts collaborative R&D projects that

improve cyber defense at scale



+ MITRE

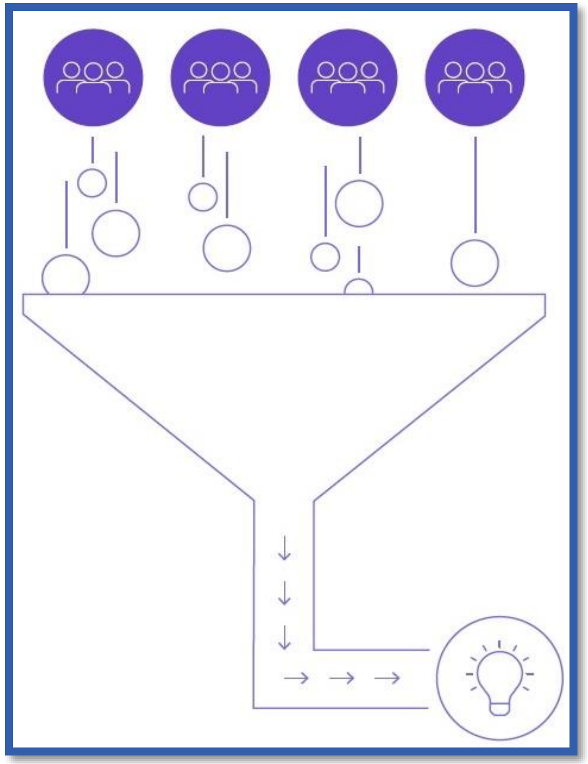
Membership is:

- ✓ Global & cross-sector
- ✓ Non-governmental
- ✓ Committed to collaborative R&D in the public interest

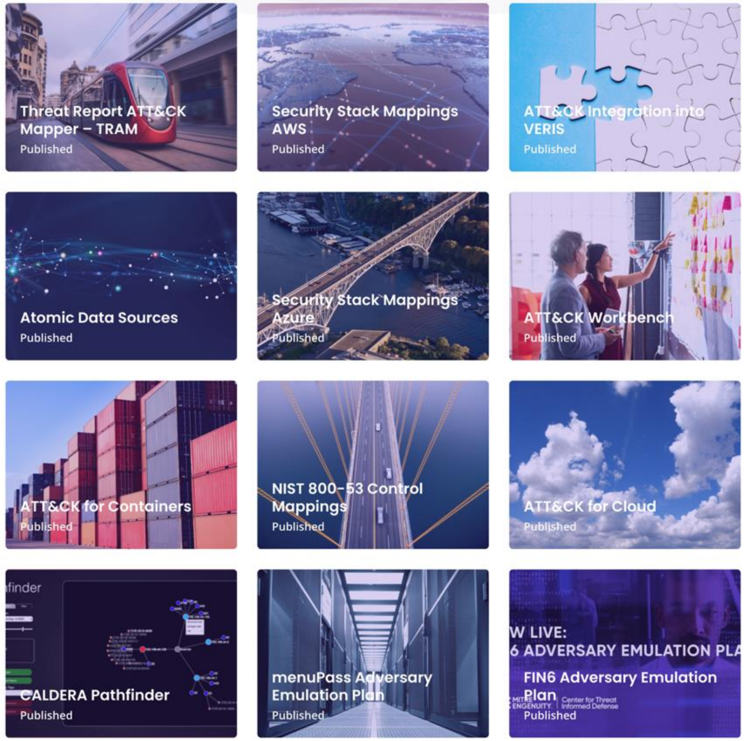
Mission: Advance the state of the art and the state of the practice in threat-informed defense globally.

© 2024 MITRE Engenuity. Approved for public release. Document number CT0112

A repeatable, scalable, approach to R&D built on member-powered collaboration



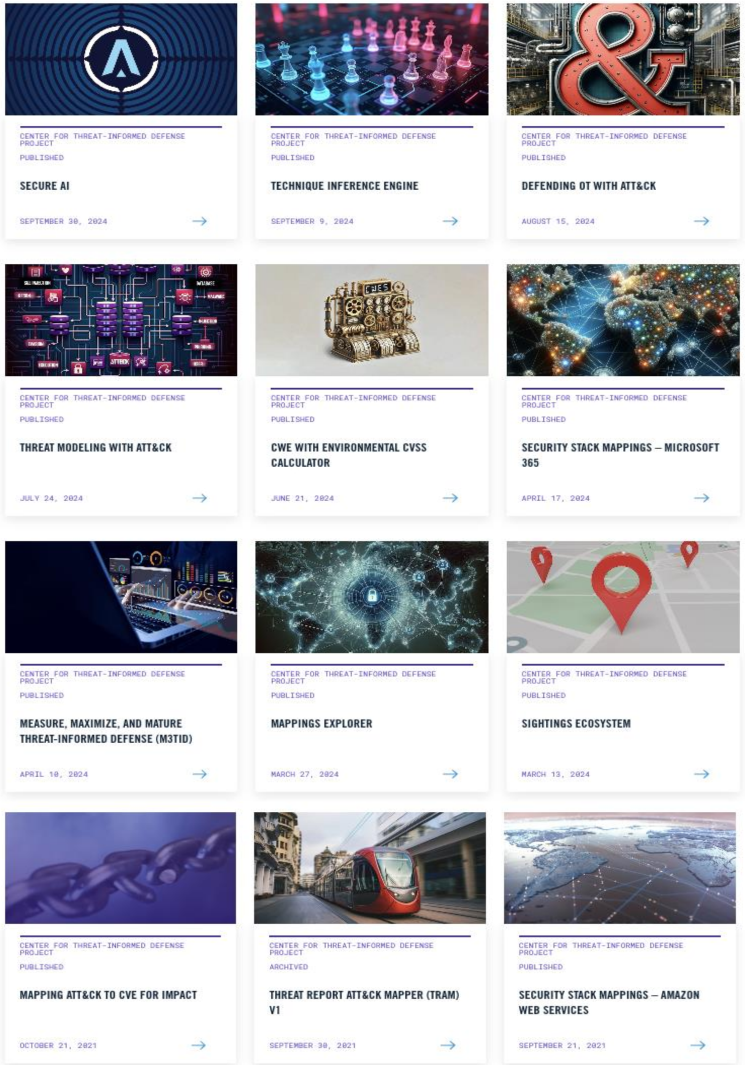
Systematically identify challenges


Threat Report ATT&CK Mapper – TRAM
Published
Security Stack Mappings AWS
Published
ATT&CK Integration into VERIS
Published
Atomic Data Sources
Published
Security Stack Mappings Azure
Published
ATT&CK Workbench
Published
ATT&CK for Containers
Published
NIST 800-53 Control Mappings
Published
ATT&CK for Cloud
Published
finder
CALDERA Pathfinder
Published
menuPass Adversary Emulation Plan
Published
W LIVE:
6 ADVERSARY EMULATION PLA
FIN6 Adversary Emulation Plan
MITRE ENGENUITY | Center for Threat Informed Defense
Published

Develop solutions together

© 2025 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE. DOCUMENT NUMBER CT0127

5 years later



CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
SECURE AI
SEPTEMBER 30, 2024

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
TECHNIQUE INFERENCE ENGINE
SEPTEMBER 9, 2024

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
DEFENDING OT WITH ATT&CK
AUGUST 15, 2024

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
THREAT MODELING WITH ATT&CK
JULY 24, 2024

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
CWE WITH ENVIRONMENTAL CVSS CALCULATOR
JUNE 21, 2024

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
SECURITY STACK MAPPINGS – MICROSOFT 365
APRIL 17, 2024

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
MEASURE, MAXIMIZE, AND MATURE THREAT-INFORMED DEFENSE (M3TID)
APRIL 10, 2024

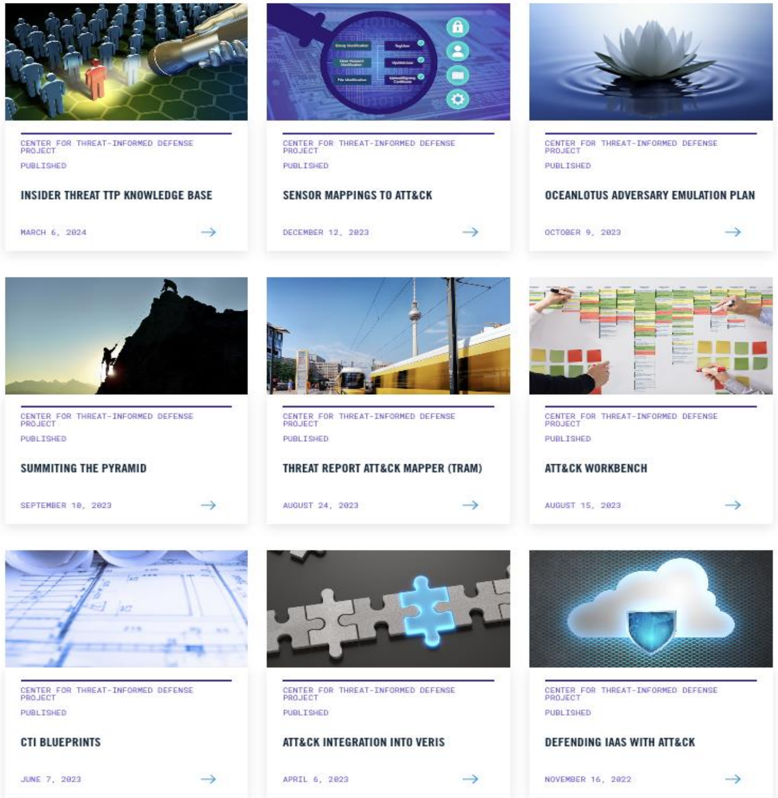
CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
MAPPINGS EXPLORER
MARCH 27, 2024

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
SIGHTINGS ECOSYSTEM
MARCH 13, 2024

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
MAPPING ATT&CK TO CVE FOR IMPACT
OCTOBER 21, 2021

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
ARCHIVED
THREAT REPORT ATT&CK MAPPER (TRAM) V1
SEPTEMBER 30, 2021

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
SECURITY STACK MAPPINGS – AMAZON WEB SERVICES
SEPTEMBER 21, 2021



CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
INSIDER THREAT TTP KNOWLEDGE BASE
MARCH 6, 2024

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
SENSOR MAPPINGS TO ATT&CK
DECEMBER 12, 2023

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
OCEANLOTUS ADVERSARY EMULATION PLAN
OCTOBER 9, 2023

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
SUMMITING THE PYRAMID
SEPTEMBER 18, 2023

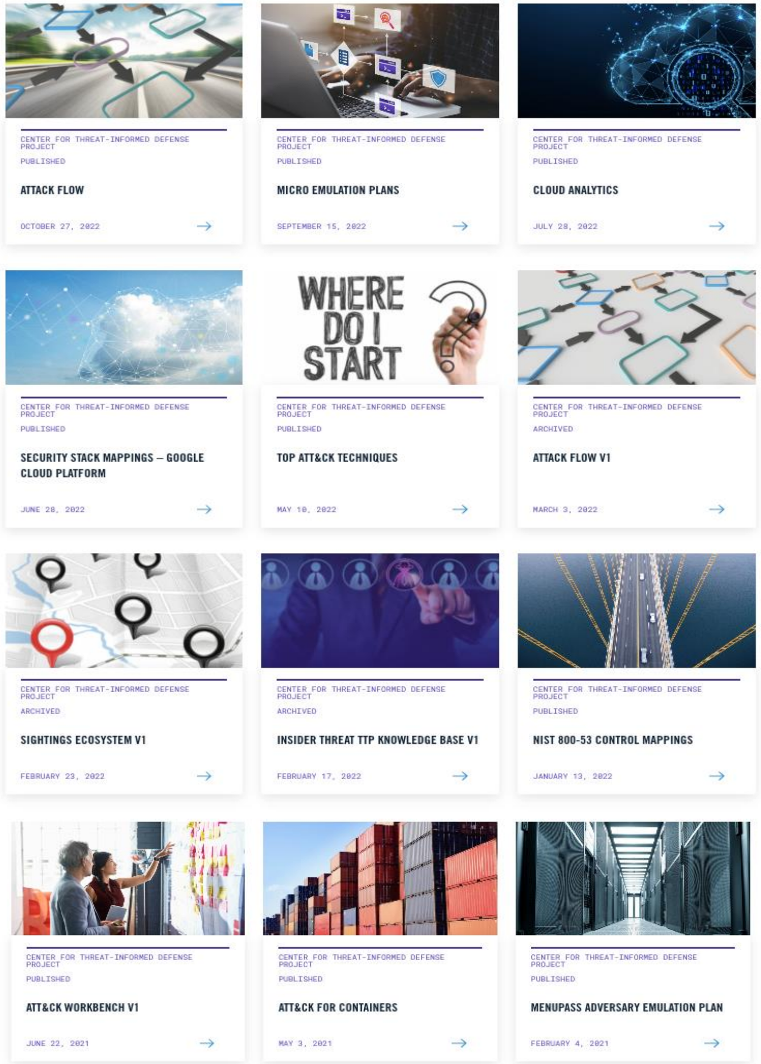
CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
THREAT REPORT ATT&CK MAPPER (TRAM)
AUGUST 24, 2023

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
ATT&CK WORKBENCH
AUGUST 15, 2023

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
CTI BLUEPRINTS
JUNE 7, 2023

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
ATT&CK INTEGRATION INTO VERIS
APRIL 6, 2023

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
DEFENDING IAAS WITH ATT&CK
NOVEMBER 16, 2022



CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
ATTACK FLOW
OCTOBER 27, 2022

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
MICRO EMULATION PLANS
SEPTEMBER 15, 2022

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
CLOUD ANALYTICS
JULY 28, 2022

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
SECURITY STACK MAPPINGS – GOOGLE CLOUD PLATFORM
JUNE 28, 2022

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
TOP ATT&CK TECHNIQUES
MAY 18, 2022

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
ARCHIVED
ATTACK FLOW V1
MARCH 3, 2022

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
ARCHIVED
SIGHTINGS ECOSYSTEM V1
FEBRUARY 23, 2022

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
ARCHIVED
INSIDER THREAT TTP KNOWLEDGE BASE V1
FEBRUARY 17, 2022

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
NIST 800-53 CONTROL MAPPINGS
JANUARY 13, 2022

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
ATT&CK WORKBENCH V1
JUNE 22, 2021

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
ATT&CK FOR CONTAINERS
MAY 3, 2021

CENTER FOR THREAT-INFORMED DEFENSE PROJECT
PUBLISHED
MENUPASS ADVERSARY EMULATION PLAN
FEBRUARY 4, 2021

We learn together

FUJITSU

“We learn a lot throughout the collaborative process gaining valuable insights that help our teams and our customers.”

HCA Healthcare℠

“Being in the same room with some of the world’s most regarded cybersecurity teams has been a true learning experience for our researchers and our business.”

standard chartered

“The biggest advantage is learning from others. From their ideas and problems, we understand adversarial perspectives we may not have thought of before.”

A Year in Threat-Informed R&D

MITRE | Center for Threat Informed Defense™

It's been a busy year

April 2024	Security Stack Mappings – M365
June 2024	CWE with Environmental CVSS Calculator
July 2024	Threat Modeling with ATT&CK
Aug 2024	Defending OT with ATT&CK
Sept 2024	Technique Inference Engine
Oct 2024	Secure AI
Dec 2024	Summiting the Pyramid II
Jan 2025	Security Stack Mappings – Hardware Enabled Defense
Feb 2025	Prioritize Known Exploited Vulnerabilities

- **Launched Secure AI Program**
  MITRE ATLAS is now in sync with ATT&CK!
- **Expanded ATT&CK Mappings**
  Simplified & expanded our mappings to ATT&CK
- **TID Training**
  Driven by your feedback, creating more training
- **Detection Engineering Innovation**
  Make detections more robust to changes in adversary behavior

© 2024 MITRE Engenuity. Approved for public release. Document Number CT0112

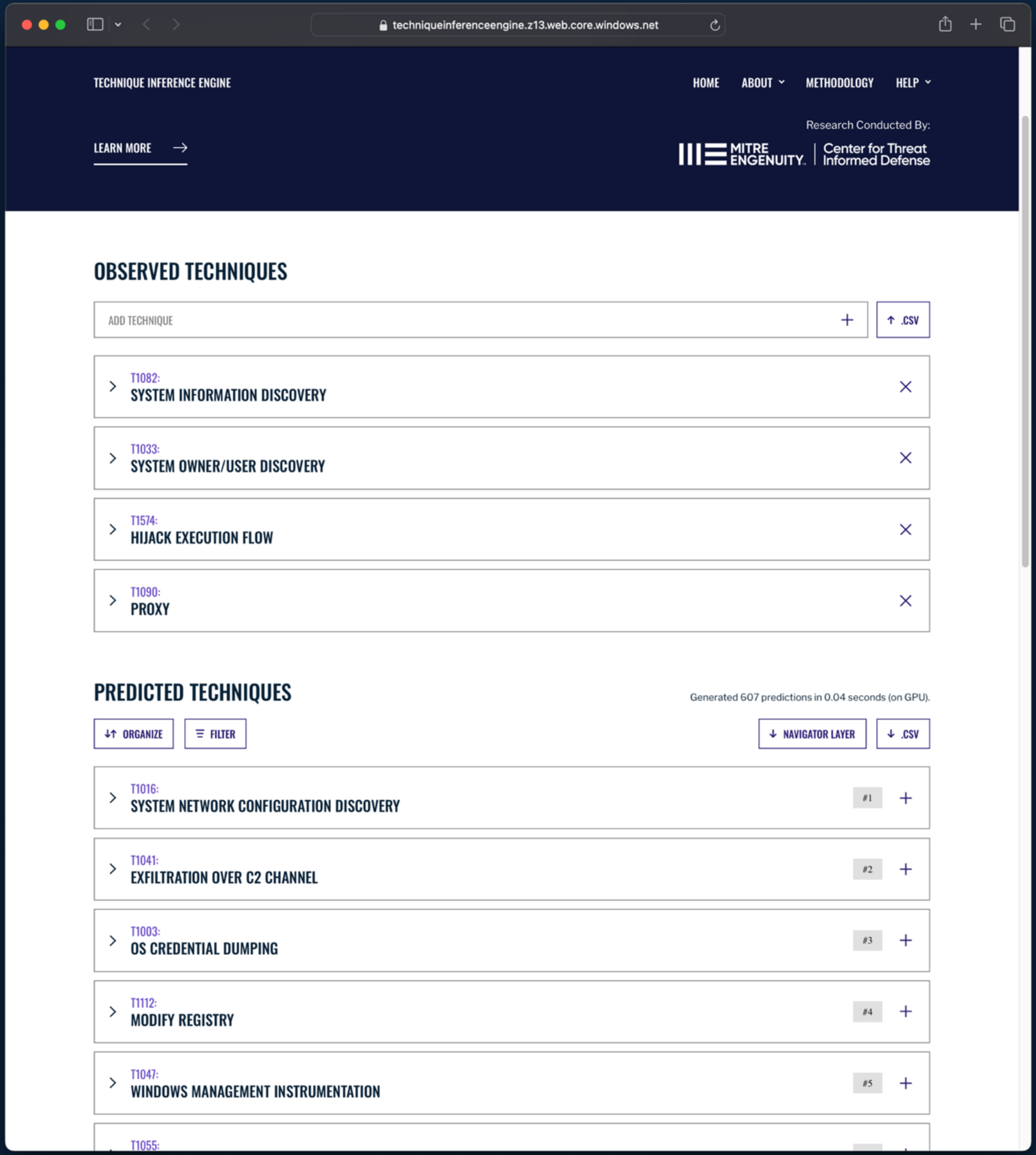
MITRE | Center for Threat Informed Defense

Technique Inference Engine

MITRE | Center for Threat Informed Defense™

Predict TTPs with Threat Intelligence

- **Threat hunting:** what should I look for next?
- **Cyber Threat Intel:** what else may have happened?
- **Threat Modeling:** what might we expect in this scenario?
- **Detection Engineering:** how can I reduce false positives by looking beyond an individual TTP?
- **Threat Emulation:** how can I build realistic scenarios with alternate courses of actions based on what adversaries really do?



techniqueinferenceengine.z13.web.core.windows.net
TECHNIQUE INFERENCE ENGINE
HOME
ABOUT
METHODOLOGY
HELP
LEARN MORE →
Research Conducted By:
MITRE ENGENUITY
Center for Threat Informed Defense

OBSERVED TECHNIQUES

ADD TECHNIQUE +   ↑ .CSV

- T1082: SYSTEM INFORMATION DISCOVERY
- T1033: SYSTEM OWNER/USER DISCOVERY
- T1574: HIJACK EXECUTION FLOW
- T1090: PROXY

PREDICTED TECHNIQUES

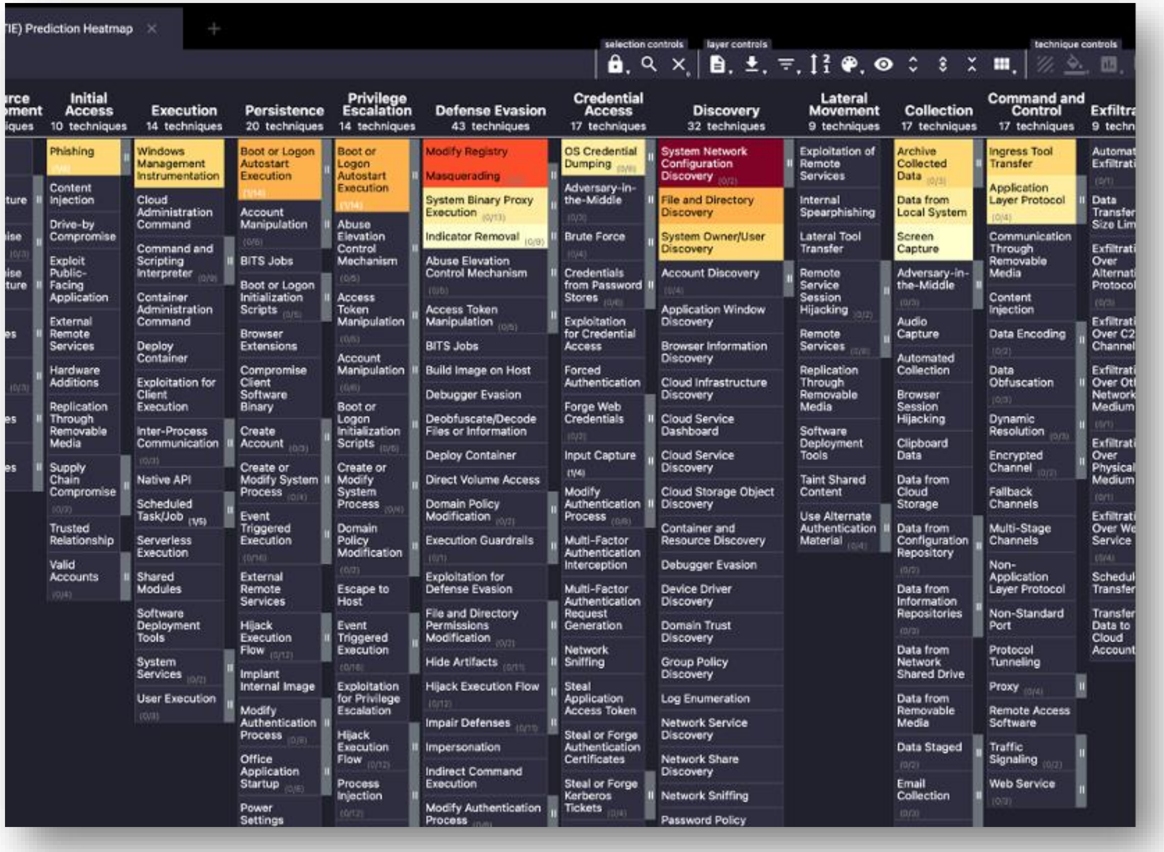
Generated 607 predictions in 0.04 seconds (on GPU).

↓↑ ORGANIZE   FILTER   ↓ NAVIGATOR LAYER   ↓ .CSV

- T1016: SYSTEM NETWORK CONFIGURATION DISCOVERY #1
- T1041: EXFILTRATION OVER C2 CHANNEL #2
- T1003: OS CREDENTIAL DUMPING #3
- T1112: MODIFY REGISTRY #4
- T1047: WINDOWS MANAGEMENT INSTRUMENTATION #5
- T1055:

© 2025 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE. DOCUMENT NUMBER CT0127

Gain a Complete Picture of an Adversary



Initial Access 10 techniques
- Phishing
- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution 14 techniques
- Windows Management Instrumentation
- Cloud Administration Command
- Command and Scripting Interpreter
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job (1/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution

Persistence 20 techniques
- Boot or Logon Autostart Execution
- Account Manipulation
- BITS Jobs
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- External Remote Services
- Hijack Execution Flow
- Implant Internal Image
- Modify Authentication Process
- Office Application Startup
- Power Settings

Privilege Escalation 14 techniques
- Boot or Logon Autostart Execution
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Account Manipulation
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain Policy Modification
- Escape to Host
- Event Triggered Execution
- Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection

Defense Evasion 43 techniques
- Modify Registry
- Masquerading
- System Binary Proxy Execution
- Indicator Removal
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Impersonation
- Indirect Command Execution
- Modify Authentication Process

Credential Access 17 techniques
- OS Credential Dumping
- Adversary-in-the-Middle
- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture (1/4)
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets

Discovery 32 techniques
- System Network Configuration Discovery
- File and Directory Discovery
- System Owner/User Discovery
- Account Discovery
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- Group Policy Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy

Lateral Movement 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

Collection 17 techniques
- Archive Collected Data
- Data from Local System
- Screen Capture
- Adversary-in-the-Middle
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository
- Data from Information Repositories
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection

Command and Control 17 techniques
- Ingress Tool Transfer
- Application Layer Protocol
- Communication Through Removable Media
- Content Injection
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service

Exfiltra 9 techn
- Automat Exfiltrati
- Data Transfer Size Lim
- Exfiltrati Over Alternati Protocol
- Exfiltrati Over C2 Channel
- Exfiltrati Over Ot Network Medium
- Exfiltrati Over Physical Medium
- Exfiltrati Over We Service
- Schedul Transfer
- Transfer Data to Cloud Account

- TIE is easy to use from a web-based interface; all data is stored locally and *inference is done on-device*.
- Predicted Techniques can be grouped, filtered, sorted, and exported.
- We published our training data and our code.
- Launch our code in a Jupyter notebook to adjust model parameters, retrain the model with a custom data set, and more.

© 2025 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE. DOCUMENT NUMBER CT0127

Innovation Roadmap

MITRE | Center for Threat Informed Defense™

What’s up next?

- ATT&CK Mappings
  - NIST CSF Financial Sector Profile, NIST 800-53, GCP
- Secure AI
  - More ATLAS, more red teaming, more mitigations
  - Ongoing AI Incident sharing
- Ambiguous Techniques
  - Identify adversary use of living-off-the-land techniques
- Visualize Attacks
  - Expand upon Attack Flow with new tools and visualizations
  - Enable more effective communications about attacks and defense in-depth strategies
- M3TID
  - Survey capability, recommendations, progress tracking

© 2025 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE. DOCUMENT NUMBER CT0127

What’s on the Horizon?

Our mission: advance the state of the art and the state if the practice in threat-informed defense globally.

An R&D organization

- Explore new areas like Financial Fraud, Intersection Risk & Operations, AI enabling analysts…
- With a threat-informed approach

Focused on impact

- Publish foundational resources, more training to scale our impact
- Increase accessibility of R&D products

Building a global community

- EU ATT&CK Community Workshop – May 2025
- ATT&CKcon 6.0 - October 14 & 15, 2025 at MITRE's McLean, VA campus

© 2025 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE. DOCUMENT NUMBER CT0127

How Do We Scale Threat-Informed Defense?

© 2025 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE. DOCUMENT NUMBER CT0127

It Takes Community

Participants

ANOMALI

Analysis & Resilience Center FOR SYSTEMIC RISK

ATTACKIQ

BANK OF AMERICA

Booz | Allen | Hamilton

CIS. Center for Internet Security

citi

CROWDSTRIKE

CYBER THREAT ALLIANCE

ENSIGN INFOSECURITY

FIRST

FM Global

FORTINET

FS-ISAC

FUJITSU

GLOBAL CYBER ALLIANCE

Google Cloud

HCA Healthcare

Health-ISAC

IBM Security

infineon

JPMORGAN CHASE & CO.

LLOYDS BANKING GROUP

Microsoft

nab

NRF NATIONAL RETAIL FEDERATION

RETAIL & HOSPITALITY ISAC

SAFE

SIEMENS

standard chartered

tenable

verizon

Participants drive the R&D program with active engagement and funding

Benefactors

Enable the global community to advance public interest cybersecurity programs through charitable giving. Benefactors are globally recognized for supporting independent research in the public interest.

ACALVIO

COALFIRE

nviso

SOC PRIME

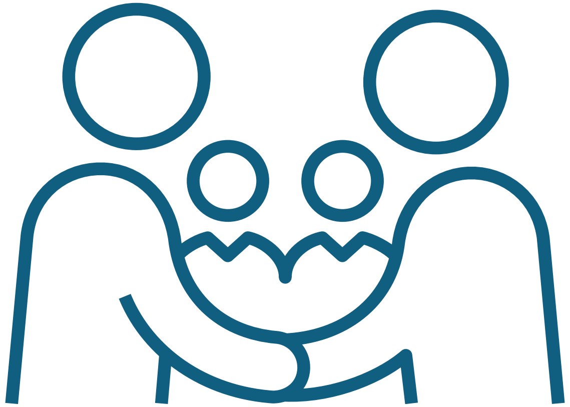
TIDAL CYBER

ZIMPERIUM

LIMBER SECURITY

Benefactors support independent research in the public interest

Community



Global adoption leads to impact. Your use cases enable improvement

© 2025 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE. DOCUMENT NUMBER CT0127

Join us and change the game!

Changing the game
on the adversary requires a
community-wide approach.

https://ctid.io/get-involved

© 2025 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE. DOCUMENT NUMBER CT0127