/ hackuity

# Comprendre et améliorer sa sécurité grâce à MITRE ATT&CK

Sylvain Cortes – VP Strategy @ hackuity

02.02.2023

# * sommaire *

_01_

>whoiam & sponsor

_02_

MITRE

_03_

MITRE ATT&CK

_04_

MITRE ATT&CK Enterprise

_05_

MITRE tools & data

_06_

MITRE ATT&CK Training

_07_

What's Next?

_08_

Questions

# _01_

## >whoiam
## &
## sponsor

# >whoiam

Sylvain Cortes

**Microsoft MVP 17x**

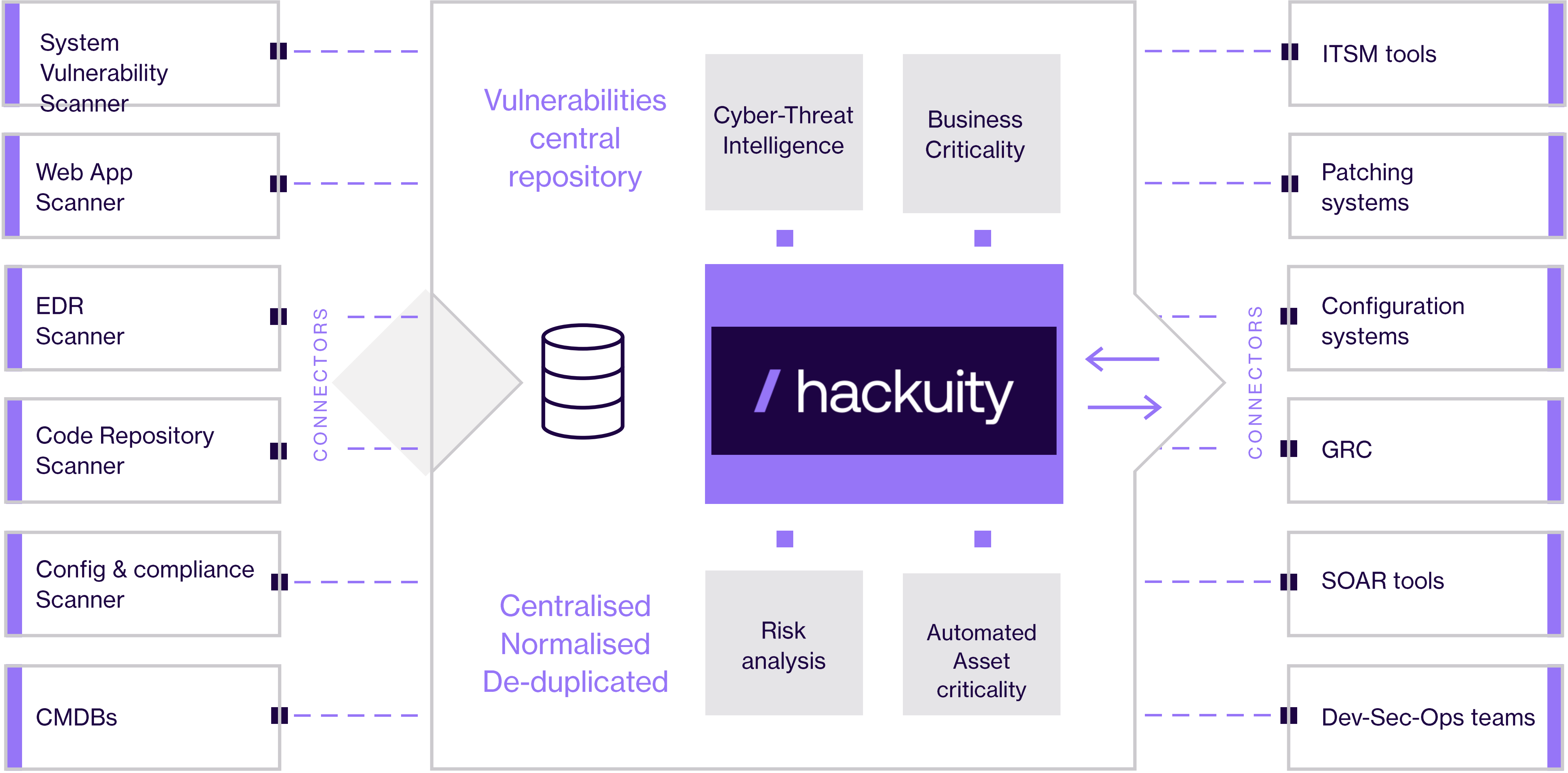
**CADIM: Communauté Active Directory & Identity Management**

**Identitydays**

**Alsid > tenable > hackuity**

**IAM / Directories / Directories Security / Cloud Identity**

**Cyber Security / Vulnerability Management**



Orchestrate detection arsenal

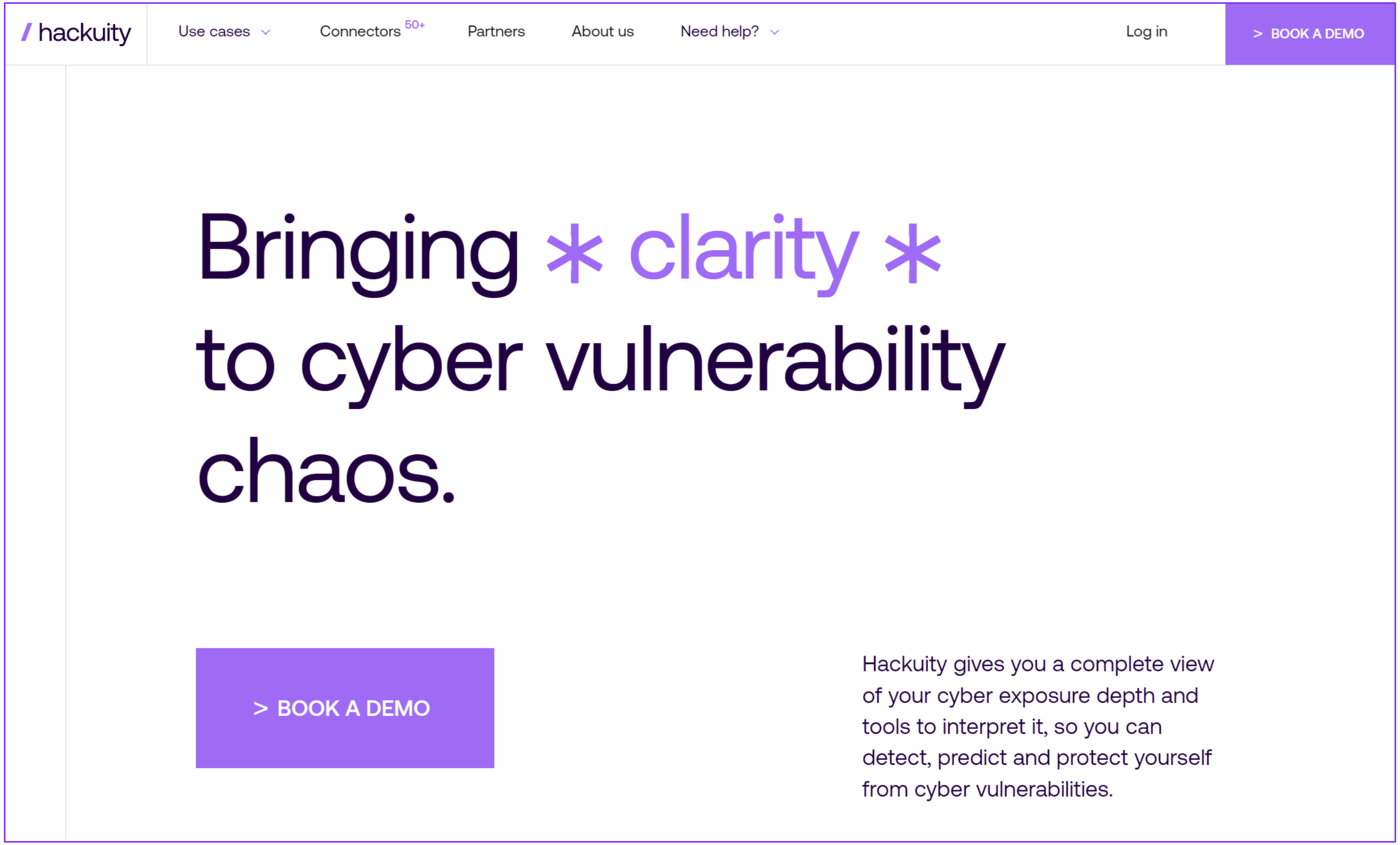
On prem Full cloud Hybrid

Automate remediation workflow

# Sponsor: hackuity

Comprendre et améliorer sa sécurité grâce à MITRE ATT&CK

Visit hackuity.io for additional information



Bringing * clarity * to cyber vulnerability chaos.

Hackuity gives you a complete view of your cyber exposure depth and tools to interpret it, so you can detect, predict and protect yourself from cyber vulnerabilities.

https://www.hackuity.io/

# _02_

# MITRE

Who is MITRE?

# 8 500 employees - Budget: US$ 2 billions

MITRE

As an independent, leading technology and research and development not-for-profit institution, MITRE serves as a trusted national resource. MITRE apply a cross-domain technical knowledge and expertise to deliver a data-driven, system-of-systems engineering approach with a single shared mission: solving problems for a safer world.

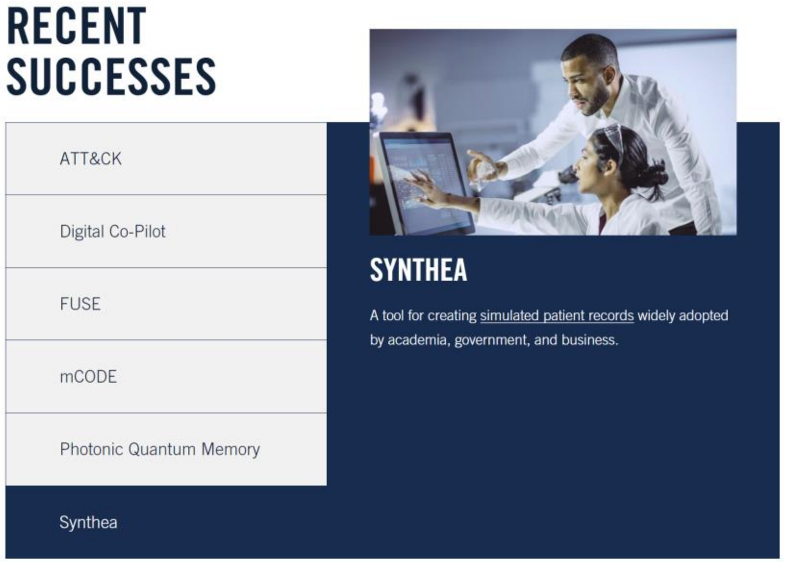
## MITRE operates six federally funded research and development centers (FFRDCs), sponsored by the following government agencies:

- **Department of Defense | National Security Engineering Center**
- **Federal Aviation Administration | Center for Advanced Aviation System Development**
- **Department of the Treasury and Internal Revenue Service, and co-sponsored by the Department of Veterans Affairs and Social Security Administration | Center for Enterprise Modernization**
- **Department of Homeland Security | Homeland Security Systems Engineering and Development Institute™**
- **Department of Health and Human Services | The Health FFRDC**
- **National Institute of Standards and Technology | National Cybersecurity FFRDC**

## Other partnerships

- **National Security Engineering Center (NSEC) is sponsored by the U.S. Department of Defense**
- **Center for Advanced Aviation System Development (CASSD) is sponsored by the Federal Aviation Administration**
- **Center for Enterprise Modernization (CEM) is sponsored by the Dept. of Treasury and the Internal Revenue Service, and co-sponsored by the Dept. of Veterans Affairs and Social Security Administration**
- **Homeland Security Systems Engineering and Development Institute™ (HSSEDI) is sponsored by the Department of Homeland Security**
- **Health FFRDC is sponsored by the Department of Health and Human Services**
- **National Cybersecurity FFRDC (NCF) is sponsored by the National Institute of Standards and Technology**

## Who is MITRE?

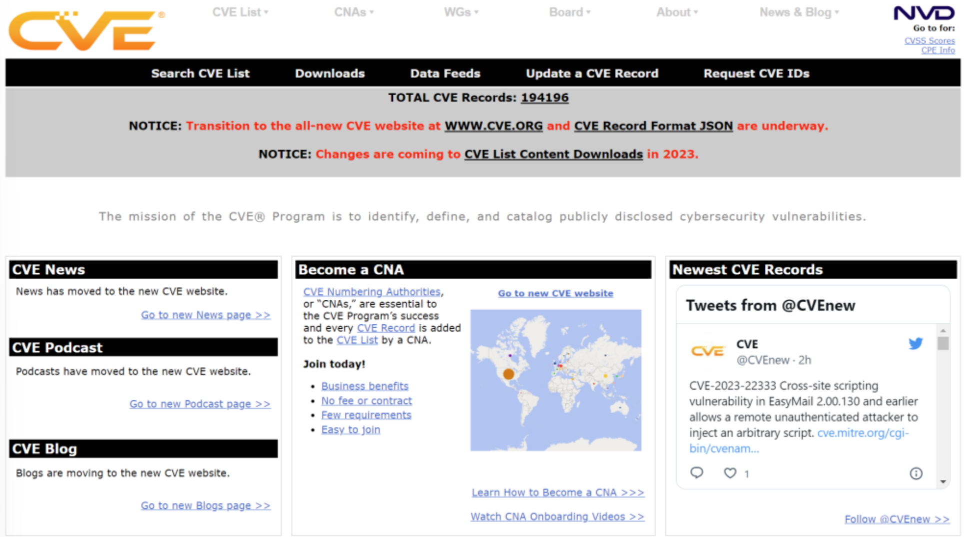


RECENT SUCCESSES

- ATT&CK
- Digital Co-Pilot
- FUSE
- mCODE
- Photonic Quantum Memory
- Synthea

SYNTHEA

A tool for creating simulated patient records widely adopted by academia, government, and business.



TOTAL CVE Records: 194196

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Changes are coming to CVE List Content Downloads in 2023.

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

**CVE News**

News has moved to the new CVE website.

Go to new News page >>

**CVE Podcast**

Podcasts have moved to the new CVE website.

Go to new Podcast page >>

**CVE Blog**

Blogs are moving to the new CVE website.

Go to new Blogs page >>

**Become a CNA**

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Go to new CVE website

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

**Newest CVE Records**

Tweets from @CVEnew

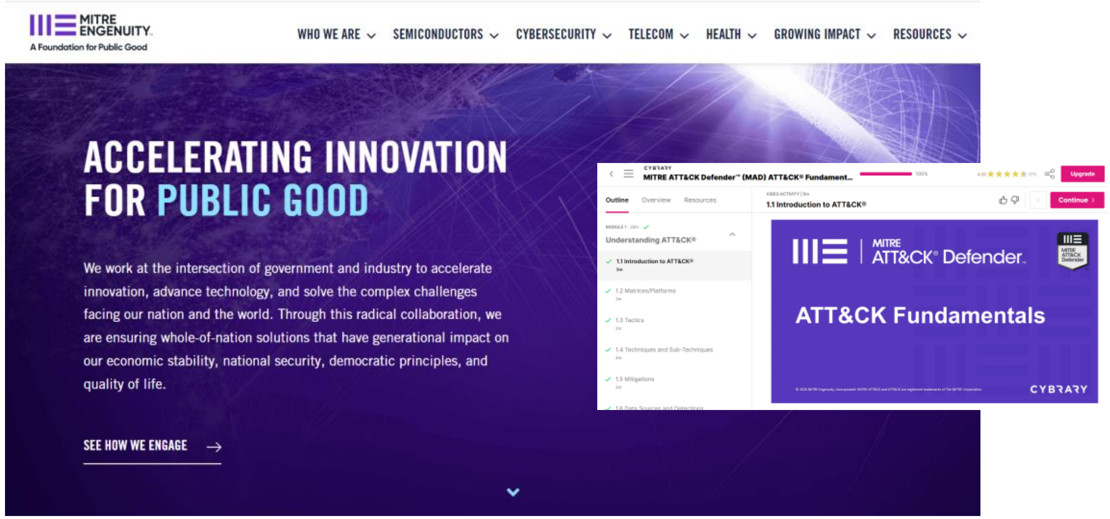
CVE @CVEnew · 2h

CVE-2023-22333 Cross-site scripting vulnerability in EasyMail 2.00.130 and earlier allows a remote unauthenticated attacker to inject an arbitrary script. cve.mitre.org/cgi-bin/cvenam...

1

Follow @CVEnew >>

**cve.mitre.org**

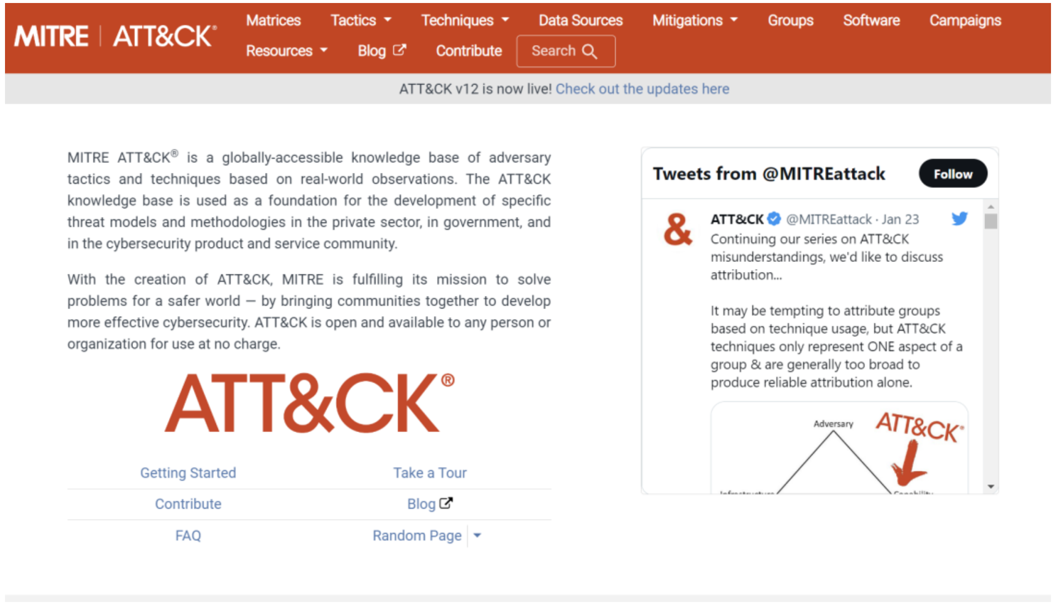


ACCELERATING INNOVATION FOR PUBLIC GOOD

We work at the intersection of government and industry to accelerate innovation, advance technology, and solve the complex challenges facing our nation and the world. Through this radical collaboration, we are ensuring whole-of-nation solutions that have generational impact on our economic stability, national security, democratic principles, and quality of life.

SEE HOW WE ENGAGE →

**mitre-engenuity.org**



ATT&CK v12 is now live! Check out the updates here

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

Tweets from @MITREattack Follow

ATT&CK @MITREattack · Jan 23

Continuing our series on ATT&CK misunderstandings, we'd like to discuss attribution...

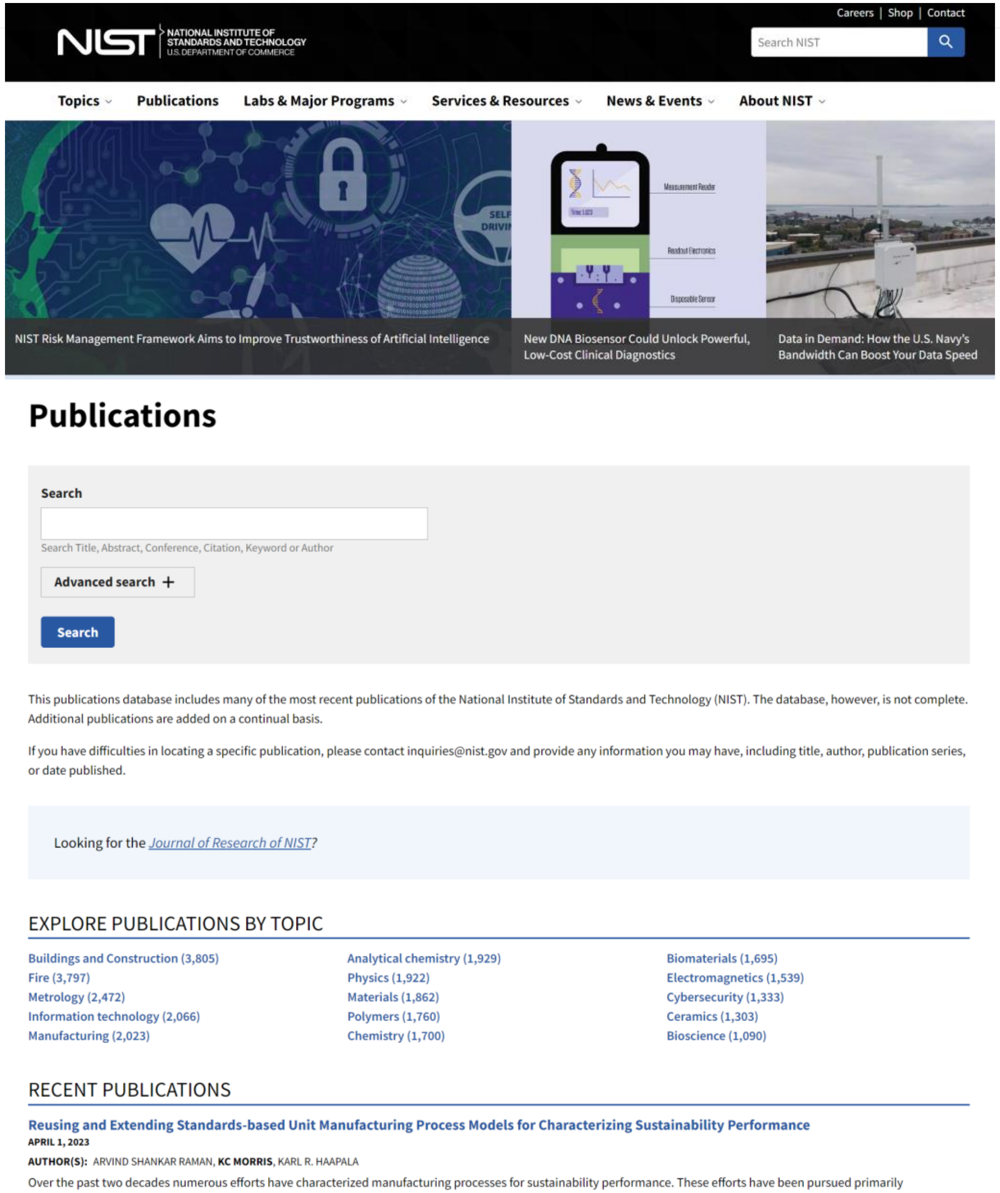
It may be tempting to attribute groups based on technique usage, but ATT&CK techniques only represent ONE aspect of a group & are generally too broad to produce reliable attribution alone.

**attack.mitre.org**

## Other agencies

**cisa.org**

**UScert**



NIST Risk Management Framework Aims to Improve Trustworthiness of Artificial Intelligence

New DNA Biosensor Could Unlock Powerful, Low-Cost Clinical Diagnostics

Data in Demand: How the U.S. Navy's Bandwidth Can Boost Your Data Speed

# Publications

Search

Search Title, Abstract, Conference, Citation, Keyword or Author

Advanced search +

Search

This publications database includes many of the most recent publications of the National Institute of Standards and Technology (NIST). The database, however, is not complete. Additional publications are added on a continual basis.

If you have difficulties in locating a specific publication, please contact inquiries@nist.gov and provide any information you may have, including title, author, publication series, or date published.

Looking for the *Journal of Research of NIST*?

## EXPLORE PUBLICATIONS BY TOPIC

- Buildings and Construction (3,805)
- Fire (3,797)
- Metrology (2,472)
- Information technology (2,066)
- Manufacturing (2,023)
- Analytical chemistry (1,929)
- Physics (1,922)
- Materials (1,862)
- Polymers (1,760)
- Chemistry (1,700)
- Biomaterials (1,695)
- Electromagnetics (1,539)
- Cybersecurity (1,333)
- Ceramics (1,303)
- Bioscience (1,090)

## RECENT PUBLICATIONS

**Reusing and Extending Standards-based Unit Manufacturing Process Models for Characterizing Sustainability Performance**

**APRIL 1, 2023**

**AUTHOR(S):** ARVIND SHANKAR RAMAN, **KC MORRIS**, KARL R. HAAPALA

Over the past two decades numerous efforts have characterized manufacturing processes for sustainability performance. These efforts have been pursued primarily

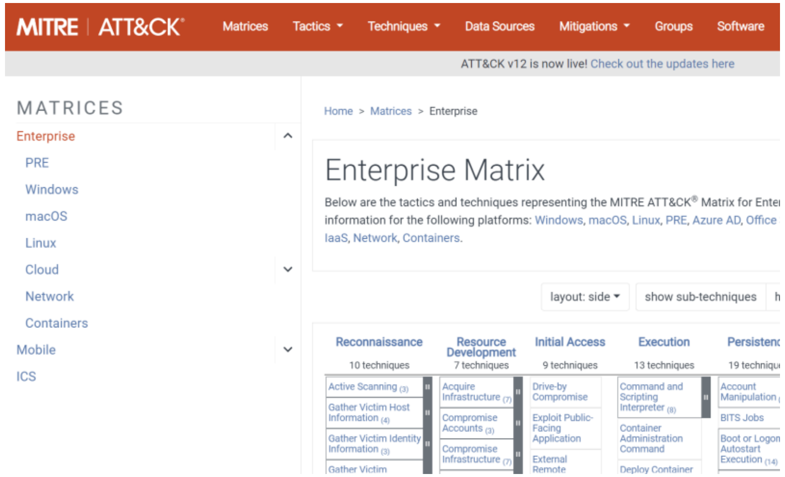
**nist.gov**

**standards & publications**

MITRE ATT&CK

MITRE ATT&CK®

**MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.**



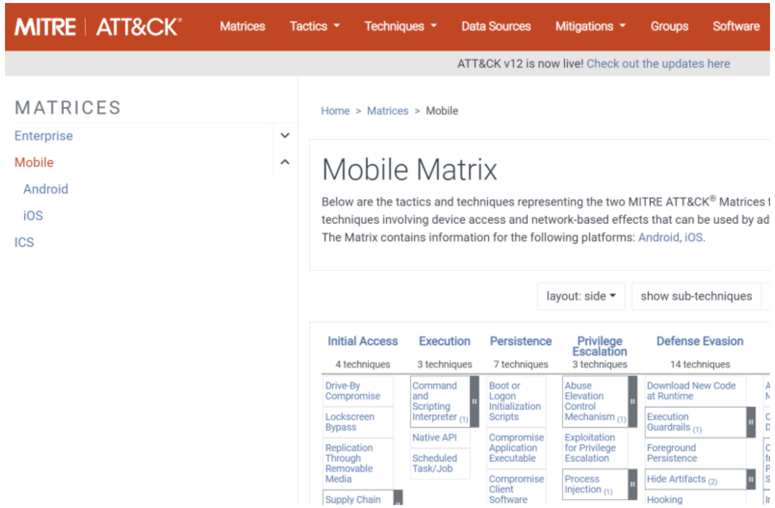
ATT&CK v12 is now live! Check out the updates here

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Ente information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office IaaS, Network, Containers.

| Reconnaissance | Resource Development | Initial Access | Execution | Persistenc |
|---|---|---|---|---|
| 10 techniques | 7 techniques | 9 techniques | 13 techniques | 19 techniqu |
| Active Scanning (3) | Acquire Infrastructure (7) | Drive-by Compromise | Command and Scripting Interpreter (8) | Account Manipulation |
| Gather Victim Host Information (4) | Compromise Accounts (3) | Exploit Public-Facing Application | Container Administration Command | BITS Jobs |
| Gather Victim Identity Information (3) | Compromise Infrastructure (7) | External Remote | Deploy Container | Boot or Logon Autostart Execution (14) |
| Gather Victim | | | | |

https://attack.mitre.org/matrices/enterprise/



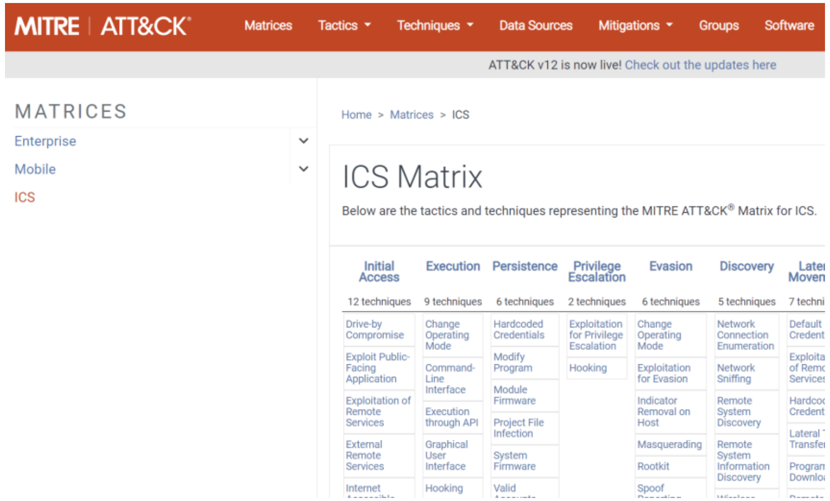
ATT&CK v12 is now live! Check out the updates here

Mobile Matrix

Below are the tactics and techniques representing the two MITRE ATT&CK® Matrices t techniques involving device access and network-based effects that can be used by ad The Matrix contains information for the following platforms: Android, iOS.

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion |
|---|---|---|---|---|
| 4 techniques | 3 techniques | 7 techniques | 3 techniques | 14 techniques |
| Drive-By Compromise | Command and Scripting Interpreter (1) | Boot or Logon Initialization Scripts | Abuse Elevation Control Mechanism (1) | Download New Code at Runtime |
| Lockscreen Bypass | Native API | Compromise Application Executable | Exploitation for Privilege Escalation | Execution Guardrails (1) |
| Replication Through Removable Media | Scheduled Task/Job | Compromise Client Software | Process Injection (1) | Foreground Persistence |
| Supply Chain | | | | Hide Artifacts (2) |
| | | | | Hooking |

https://attack.mitre.org/matrices/mobile/



ATT&CK v12 is now live! Check out the updates here

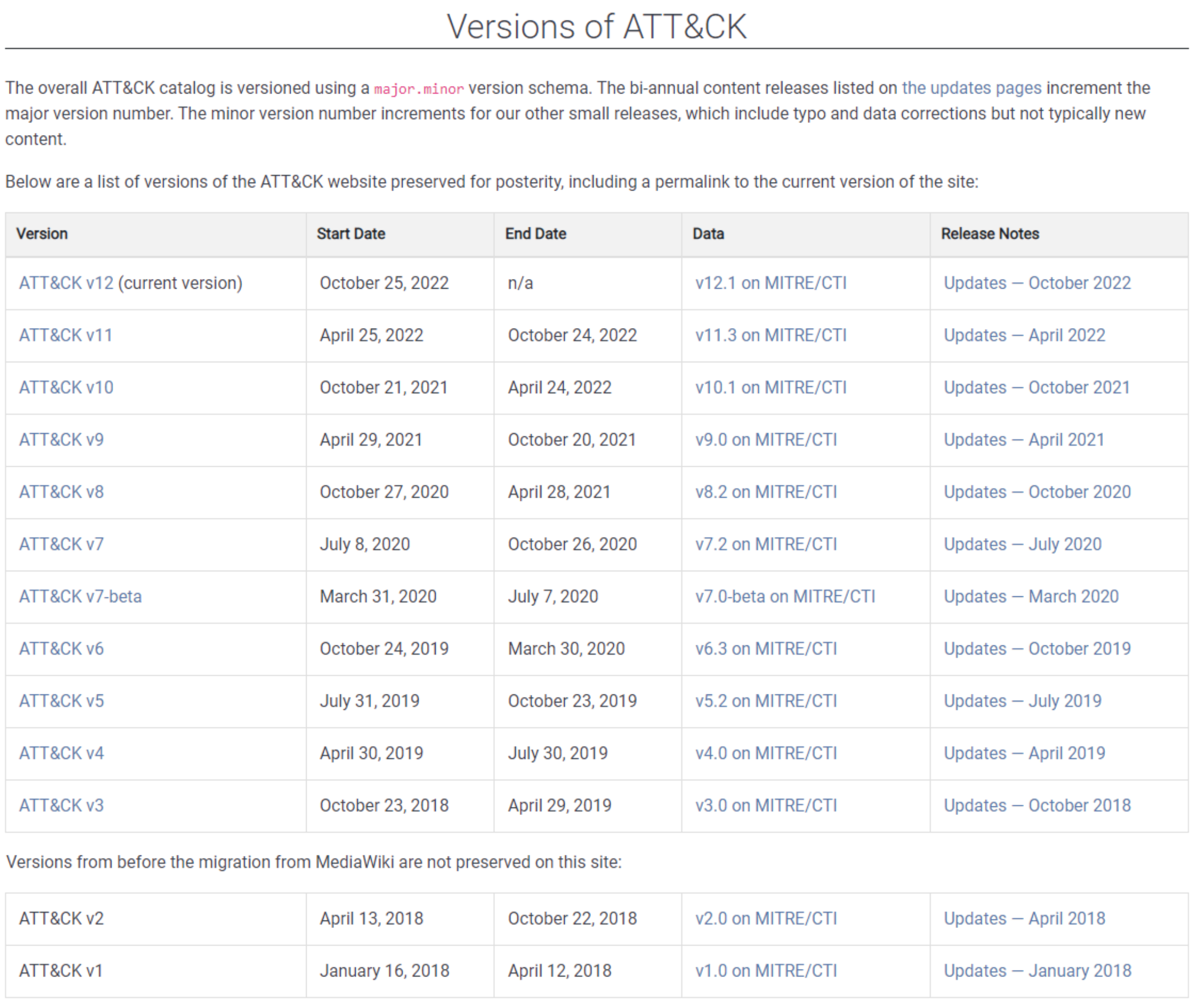
ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

| Initial Access | Execution | Persistence | Privilege Escalation | Evasion | Discovery | Later Moven |
|---|---|---|---|---|---|---|
| 12 techniques | 9 techniques | 6 techniques | 2 techniques | 6 techniques | 5 techniques | 7 techni |
| Drive-by Compromise | Change Operating Mode | Hardcoded Credentials | Exploitation for Privilege Escalation | Change Operating Mode | Network Connection Enumeration | Default Credent |
| Exploit Public-Facing Application | Command-Line Interface | Modify Program | Hooking | Exploitation for Evasion | Network Sniffing | Exploita of Remo Services |
| Exploitation of Remote Services | Execution through API | Module Firmware | | Indicator Removal on Host | Remote System Discovery | Hardcod Credent |
| External Remote Services | Graphical User Interface | Project File Infection | | Masquerading | Remote System Information Discovery | Lateral Transfe |
| Internet | Hooking | System Firmware | | Rootkit | | Program Downlo |
| | | Valid | | Spoof | | |

https://attack.mitre.org/matrices/ics/

## MITRE ATT&CK



## Versions of ATT&CK

The overall ATT&CK catalog is versioned using a `major.minor` version schema. The bi-annual content releases listed on the updates pages increment the major version number. The minor version number increments for our other small releases, which include typo and data corrections but not typically new content.

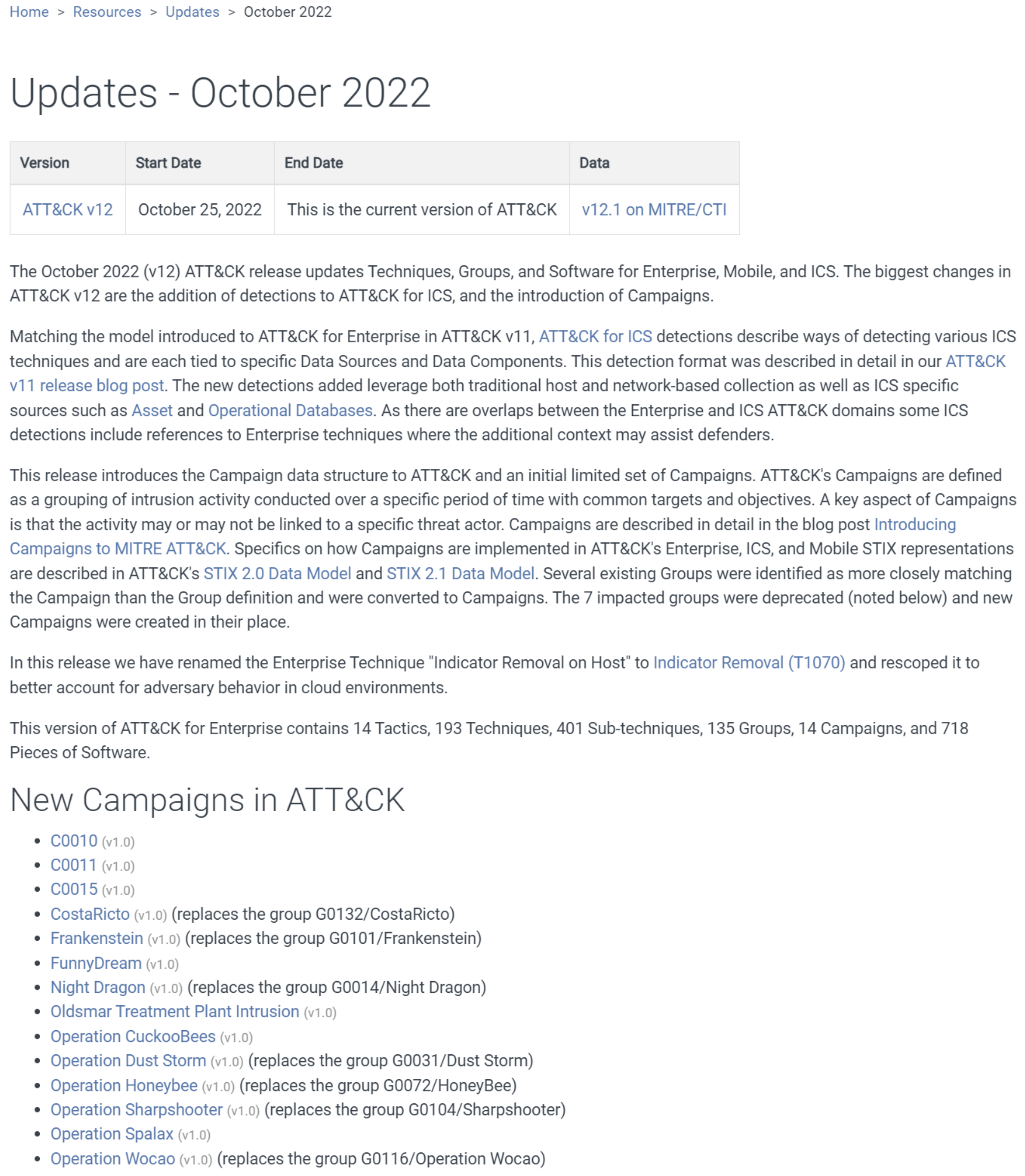
Below are a list of versions of the ATT&CK website preserved for posterity, including a permalink to the current version of the site:

| Version | Start Date | End Date | Data | Release Notes |
|---|---|---|---|---|
| ATT&CK v12 (current version) | October 25, 2022 | n/a | v12.1 on MITRE/CTI | Updates – October 2022 |
| ATT&CK v11 | April 25, 2022 | October 24, 2022 | v11.3 on MITRE/CTI | Updates – April 2022 |
| ATT&CK v10 | October 21, 2021 | April 24, 2022 | v10.1 on MITRE/CTI | Updates – October 2021 |
| ATT&CK v9 | April 29, 2021 | October 20, 2021 | v9.0 on MITRE/CTI | Updates – April 2021 |
| ATT&CK v8 | October 27, 2020 | April 28, 2021 | v8.2 on MITRE/CTI | Updates – October 2020 |
| ATT&CK v7 | July 8, 2020 | October 26, 2020 | v7.2 on MITRE/CTI | Updates – July 2020 |
| ATT&CK v7-beta | March 31, 2020 | July 7, 2020 | v7.0-beta on MITRE/CTI | Updates – March 2020 |
| ATT&CK v6 | October 24, 2019 | March 30, 2020 | v6.3 on MITRE/CTI | Updates – October 2019 |
| ATT&CK v5 | July 31, 2019 | October 23, 2019 | v5.2 on MITRE/CTI | Updates – July 2019 |
| ATT&CK v4 | April 30, 2019 | July 30, 2019 | v4.0 on MITRE/CTI | Updates – April 2019 |
| ATT&CK v3 | October 23, 2018 | April 29, 2019 | v3.0 on MITRE/CTI | Updates – October 2018 |

Versions from before the migration from MediaWiki are not preserved on this site:

| | | | | |
|---|---|---|---|---|
| ATT&CK v2 | April 13, 2018 | October 22, 2018 | v2.0 on MITRE/CTI | Updates – April 2018 |
| ATT&CK v1 | January 16, 2018 | April 12, 2018 | v1.0 on MITRE/CTI | Updates – January 2018 |

https://attack.mitre.org/resources/versions/



Home > Resources > Updates > October 2022

## Updates - October 2022

| Version | Start Date | End Date | Data |
|---|---|---|---|
| ATT&CK v12 | October 25, 2022 | This is the current version of ATT&CK | v12.1 on MITRE/CTI |

The October 2022 (v12) ATT&CK release updates Techniques, Groups, and Software for Enterprise, Mobile, and ICS. The biggest changes in ATT&CK v12 are the addition of detections to ATT&CK for ICS, and the introduction of Campaigns.

Matching the model introduced to ATT&CK for Enterprise in ATT&CK v11, ATT&CK for ICS detections describe ways of detecting various ICS techniques and are each tied to specific Data Sources and Data Components. This detection format was described in detail in our ATT&CK v11 release blog post. The new detections added leverage both traditional host and network-based collection as well as ICS specific sources such as Asset and Operational Databases. As there are overlaps between the Enterprise and ICS ATT&CK domains some ICS detections include references to Enterprise techniques where the additional context may assist defenders.

This release introduces the Campaign data structure to ATT&CK and an initial limited set of Campaigns. ATT&CK's Campaigns are defined as a grouping of intrusion activity conducted over a specific period of time with common targets and objectives. A key aspect of Campaigns is that the activity may or may not be linked to a specific threat actor. Campaigns are described in detail in the blog post Introducing Campaigns to MITRE ATT&CK. Specifics on how Campaigns are implemented in ATT&CK's Enterprise, ICS, and Mobile STIX representations are described in ATT&CK's STIX 2.0 Data Model and STIX 2.1 Data Model. Several existing Groups were identified as more closely matching the Campaign than the Group definition and were converted to Campaigns. The 7 impacted groups were deprecated (noted below) and new Campaigns were created in their place.

In this release we have renamed the Enterprise Technique "Indicator Removal on Host" to Indicator Removal (T1070) and rescoped it to better account for adversary behavior in cloud environments.

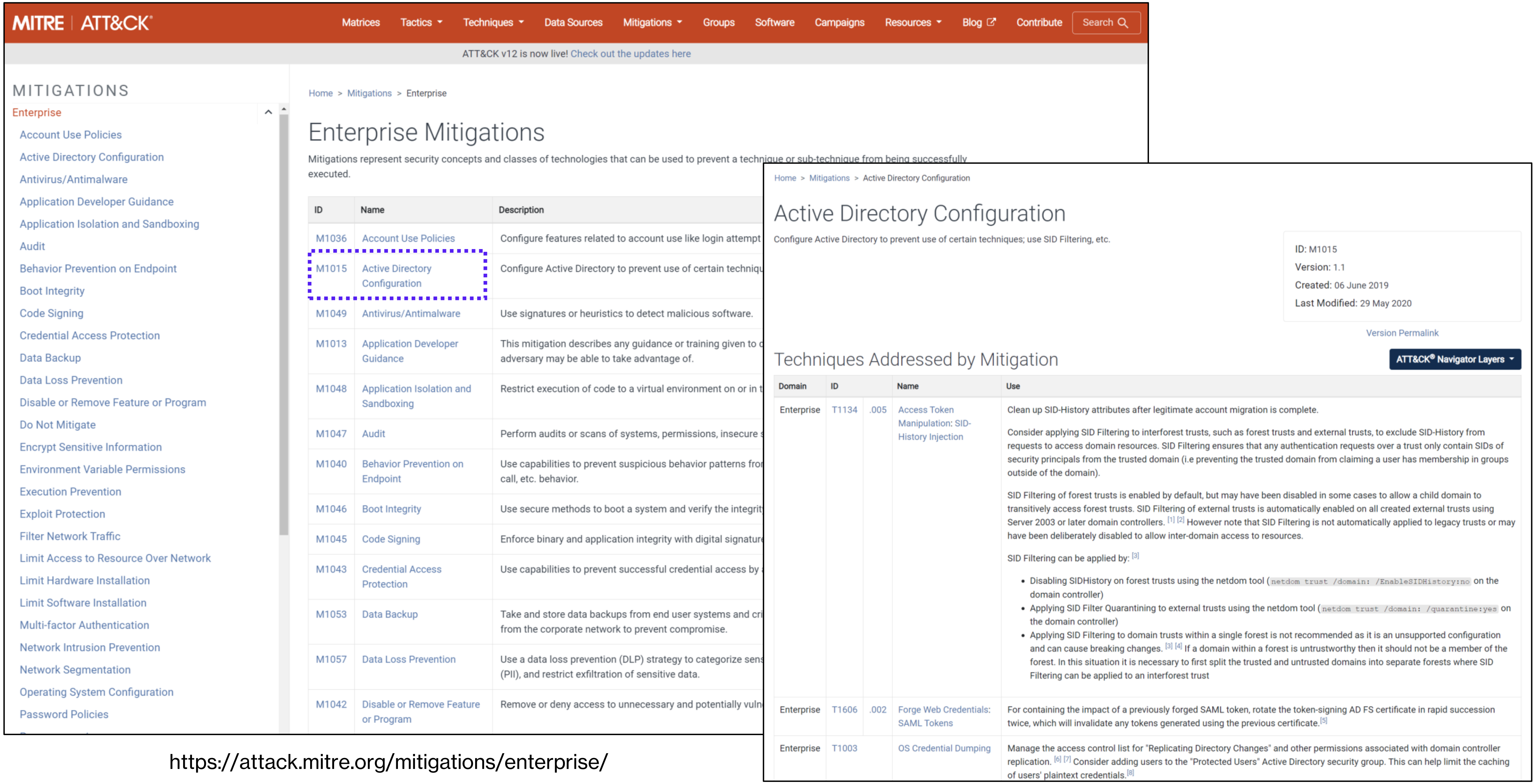
This version of ATT&CK for Enterprise contains 14 Tactics, 193 Techniques, 401 Sub-techniques, 135 Groups, 14 Campaigns, and 718 Pieces of Software.

### New Campaigns in ATT&CK

- C0010 (v1.0)
- C0011 (v1.0)
- C0015 (v1.0)
- CostaRicto (v1.0) (replaces the group G0132/CostaRicto)
- Frankenstein (v1.0) (replaces the group G0101/Frankenstein)
- FunnyDream (v1.0)
- Night Dragon (v1.0) (replaces the group G0014/Night Dragon)
- Oldsmar Treatment Plant Intrusion (v1.0)
- Operation CuckooBees (v1.0)
- Operation Dust Storm (v1.0) (replaces the group G0031/Dust Storm)
- Operation Honeybee (v1.0) (replaces the group G0072/HoneyBee)
- Operation Sharpshooter (v1.0) (replaces the group G0104/Sharpshooter)
- Operation Spalax (v1.0)
- Operation Wocao (v1.0) (replaces the group G0116/Operation Wocao)

MITRE ATT&CK

# MITRE ATT&CK® Mitigations



ATT&CK v12 is now live! Check out the updates here

MITIGATIONS

Enterprise

Account Use Policies
Active Directory Configuration
Antivirus/Antimalware
Application Developer Guidance
Application Isolation and Sandboxing
Audit
Behavior Prevention on Endpoint
Boot Integrity
Code Signing
Credential Access Protection
Data Backup
Data Loss Prevention
Disable or Remove Feature or Program
Do Not Mitigate
Encrypt Sensitive Information
Environment Variable Permissions
Execution Prevention
Exploit Protection
Filter Network Traffic
Limit Access to Resource Over Network
Limit Hardware Installation
Limit Software Installation
Multi-factor Authentication
Network Intrusion Prevention
Network Segmentation
Operating System Configuration
Password Policies

Home > Mitigations > Enterprise

## Enterprise Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

| ID | Name | Description |
|---|---|---|
| M1036 | Account Use Policies | Configure features related to account use like login attempt |
| M1015 | Active Directory Configuration | Configure Active Directory to prevent use of certain techniqu |
| M1049 | Antivirus/Antimalware | Use signatures or heuristics to detect malicious software. |
| M1013 | Application Developer Guidance | This mitigation describes any guidance or training given to d adversary may be able to take advantage of. |
| M1048 | Application Isolation and Sandboxing | Restrict execution of code to a virtual environment on or in t |
| M1047 | Audit | Perform audits or scans of systems, permissions, insecure s |
| M1040 | Behavior Prevention on Endpoint | Use capabilities to prevent suspicious behavior patterns fro call, etc. behavior. |
| M1046 | Boot Integrity | Use secure methods to boot a system and verify the integrit |
| M1045 | Code Signing | Enforce binary and application integrity with digital signatur |
| M1043 | Credential Access Protection | Use capabilities to prevent successful credential access by a |
| M1053 | Data Backup | Take and store data backups from end user systems and cri from the corporate network to prevent compromise. |
| M1057 | Data Loss Prevention | Use a data loss prevention (DLP) strategy to categorize sens (PII), and restrict exfiltration of sensitive data. |
| M1042 | Disable or Remove Feature or Program | Remove or deny access to unnecessary and potentially vuln |

Home > Mitigations > Active Directory Configuration

## Active Directory Configuration

Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.

ID: M1015
Version: 1.1
Created: 06 June 2019
Last Modified: 29 May 2020

Version Permalink

### Techniques Addressed by Mitigation

ATT&CK® Navigator Layers

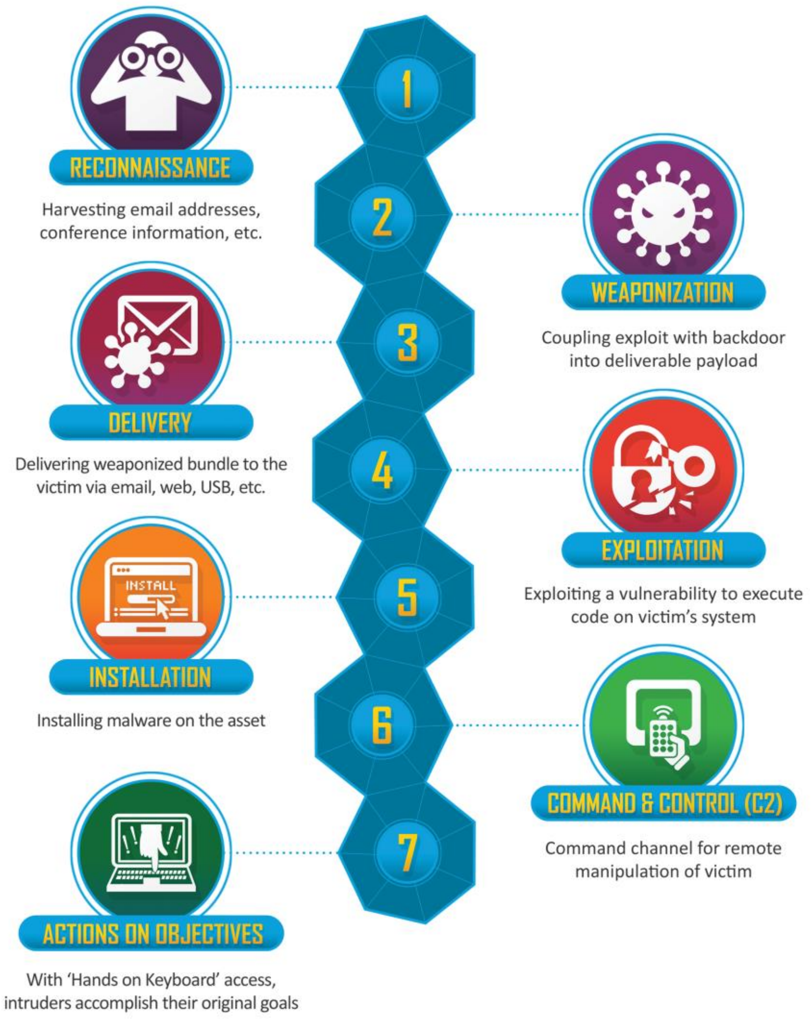
| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1134 | .005 | Access Token Manipulation: SID-History Injection | Clean up SID-History attributes after legitimate account migration is complete.<br>Consider applying SID Filtering to interforest trusts, such as forest trusts and external trusts, to exclude SID-History from requests to access domain resources. SID Filtering ensures that any authentication requests over a trust only contain SIDs of security principals from the trusted domain (i.e preventing the trusted domain from claiming a user has membership in groups outside of the domain).<br>SID Filtering of forest trusts is enabled by default, but may have been disabled in some cases to allow a child domain to transitively access forest trusts. SID Filtering of external trusts is automatically enabled on all created external trusts using Server 2003 or later domain controllers. [1] [2] However note that SID Filtering is not automatically applied to legacy trusts or may have been deliberately disabled to allow inter-domain access to resources.<br>SID Filtering can be applied by: [3]<br>• Disabling SIDHistory on forest trusts using the netdom tool (`netdom trust /domain: /EnableSIDHistory:no` on the domain controller)<br>• Applying SID Filter Quarantining to external trusts using the netdom tool (`netdom trust /domain: /quarantine:yes` on the domain controller)<br>• Applying SID Filtering to domain trusts within a single forest is not recommended as it is an unsupported configuration and can cause breaking changes. [3] [4] If a domain within a forest is untrustworthy then it should not be a member of the forest. In this situation it is necessary to first split the trusted and untrusted domains into separate forests where SID Filtering can be applied to an interforest trust |
| Enterprise | T1606 | .002 | Forge Web Credentials: SAML Tokens | For containing the impact of a previously forged SAML token, rotate the token-signing AD FS certificate in rapid succession twice, which will invalidate any tokens generated using the previous certificate.[5] |
| Enterprise | T1003 | | OS Credential Dumping | Manage the access control list for "Replicating Directory Changes" and other permissions associated with domain controller replication. [6] [7] Consider adding users to the "Protected Users" Active Directory security group. This can help limit the caching of users' plaintext credentials.[8] |

https://attack.mitre.org/mitigations/enterprise/

# _03_

# MITRE ATT&CK

### Yet Another Kill Chain


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

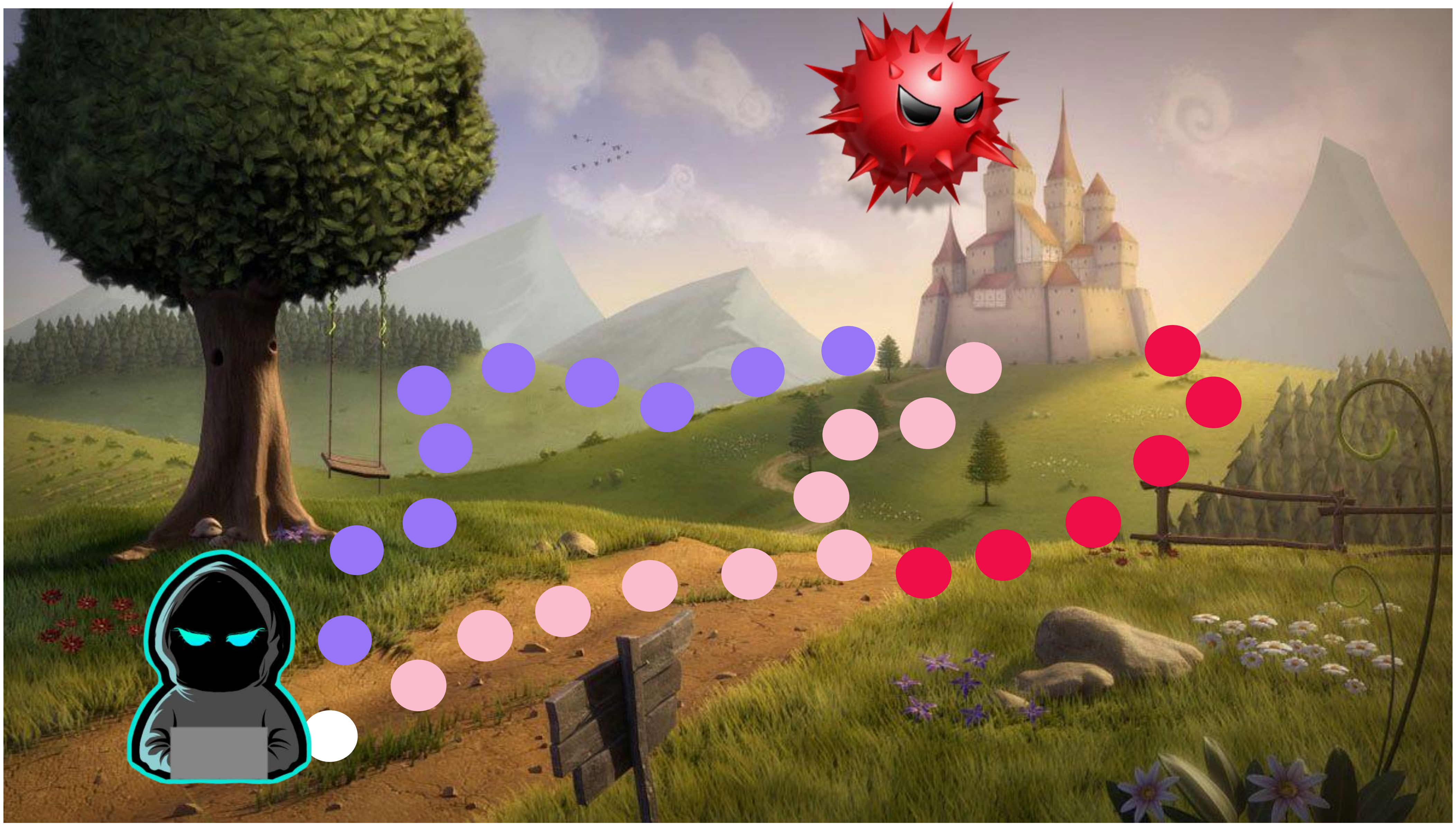
*Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*

Developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.

The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures. Developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.

The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.

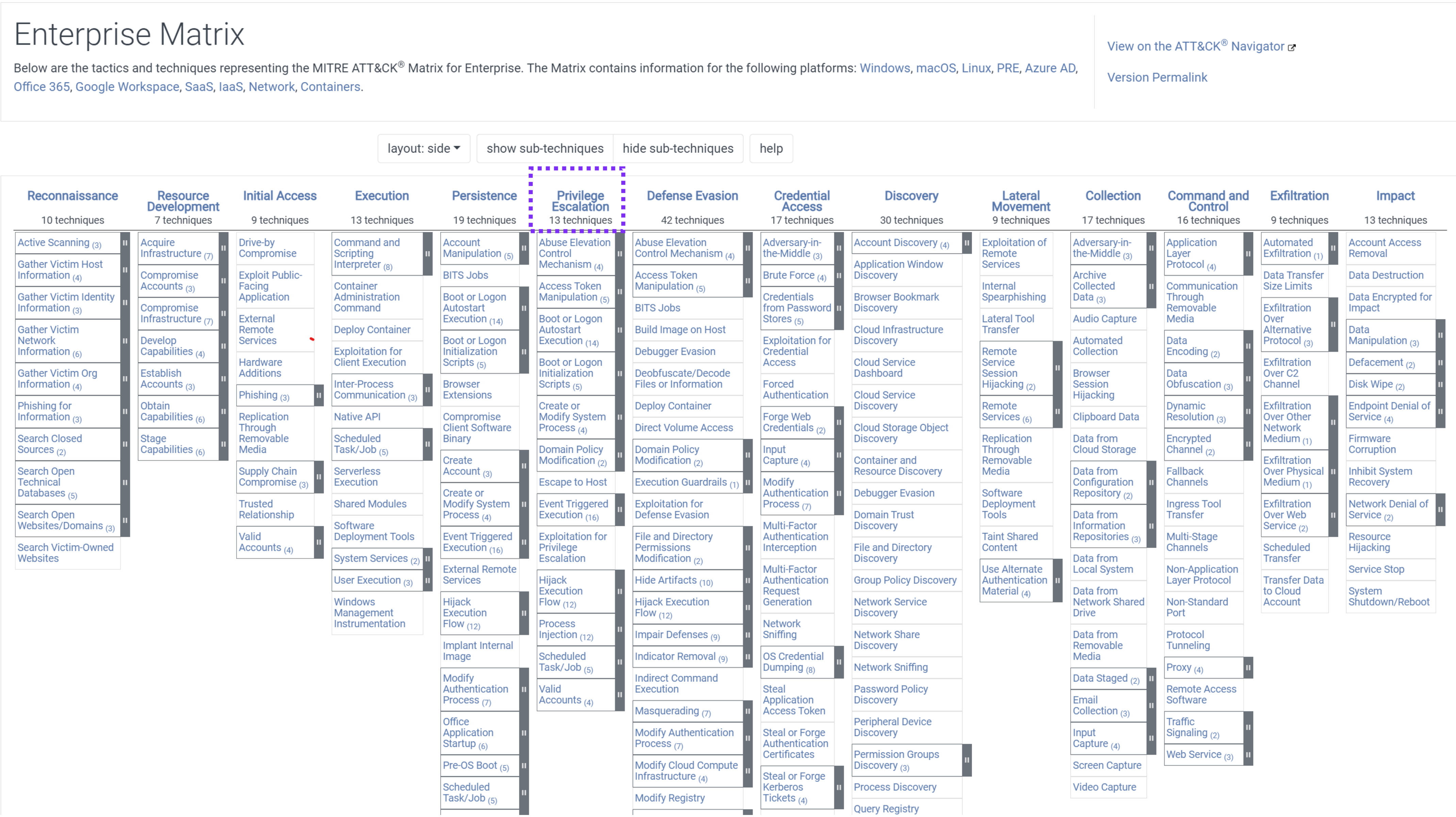
## Yet Another Kill Chain



# _04_

# MITRE ATT&CK Enterprise

Matrix: https://attack.mitre.org/matrices/enterprise/



# Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

View on the ATT&CK® Navigator

Version Permalink

**Reconnaissance** – 10 techniques
- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

**Resource Development** – 7 techniques
- Acquire Infrastructure (7)
- Compromise Accounts (3)
- Compromise Infrastructure (7)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (6)
- Stage Capabilities (6)

**Initial Access** – 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

**Execution** – 13 techniques
- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

**Persistence** – 19 techniques
- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (7)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)

**Privilege Escalation** – 13 techniques
- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

**Defense Evasion** – 42 techniques
- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (9)
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (7)
- Modify Authentication Process (7)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry

**Credential Access** – 17 techniques
- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (7)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (4)

**Discovery** – 30 techniques
- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry

**Lateral Movement** – 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

**Collection** – 17 techniques
- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

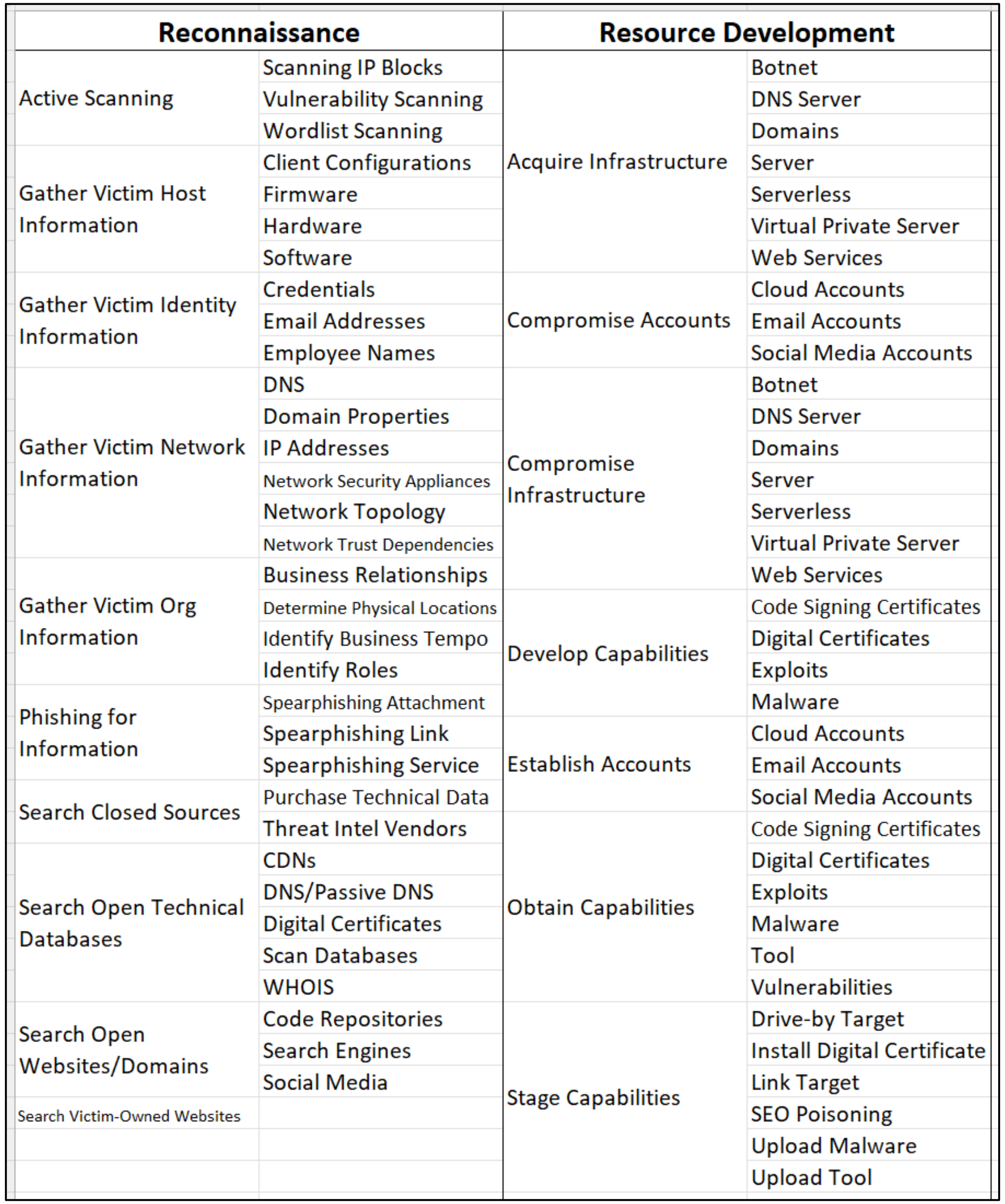
**Command and Control** – 16 techniques
- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (2)
- Web Service (3)

**Exfiltration** – 9 techniques
- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

**Impact** – 13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

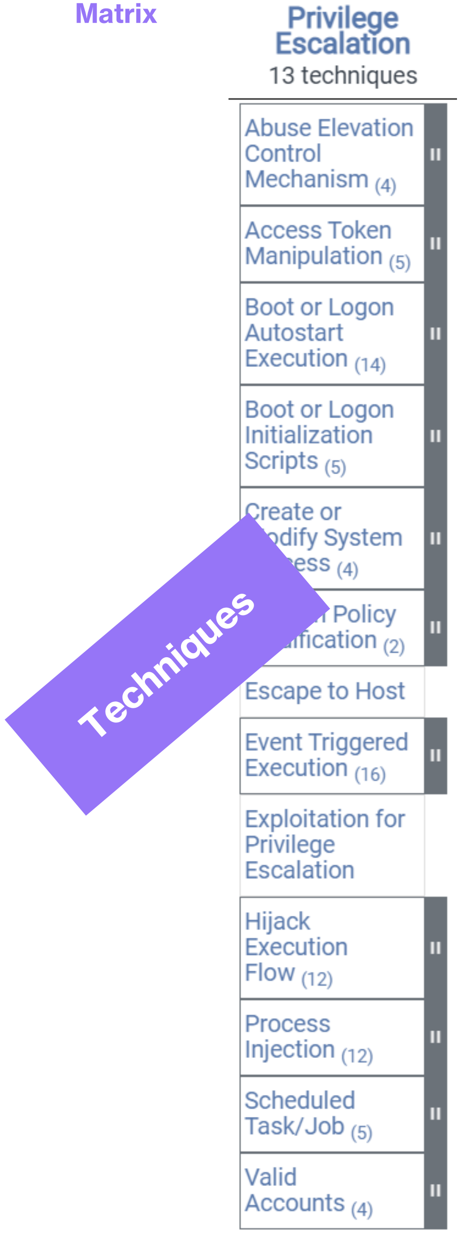
Tactics

## PRE Matrix



| Reconnaissance | | Resource Development | |
|---|---|---|---|
| Active Scanning | Scanning IP Blocks | Acquire Infrastructure | Botnet |
| | Vulnerability Scanning | | DNS Server |
| | Wordlist Scanning | | Domains |
| Gather Victim Host Information | Client Configurations | | Server |
| | Firmware | | Serverless |
| | Hardware | | Virtual Private Server |
| | Software | | Web Services |
| Gather Victim Identity Information | Credentials | Compromise Accounts | Cloud Accounts |
| | Email Addresses | | Email Accounts |
| | Employee Names | | Social Media Accounts |
| Gather Victim Network Information | DNS | Compromise Infrastructure | Botnet |
| | Domain Properties | | DNS Server |
| | IP Addresses | | Domains |
| | Network Security Appliances | | Server |
| | Network Topology | | Serverless |
| | Network Trust Dependencies | | Virtual Private Server |
| Gather Victim Org Information | Business Relationships | | Web Services |
| | Determine Physical Locations | Develop Capabilities | Code Signing Certificates |
| | Identify Business Tempo | | Digital Certificates |
| | Identify Roles | | Exploits |
| Phishing for Information | Spearphishing Attachment | | Malware |
| | Spearphishing Link | Establish Accounts | Cloud Accounts |
| | Spearphishing Service | | Email Accounts |
| Search Closed Sources | Purchase Technical Data | | Social Media Accounts |
| | Threat Intel Vendors | Obtain Capabilities | Code Signing Certificates |
| Search Open Technical Databases | CDNs | | Digital Certificates |
| | DNS/Passive DNS | | Exploits |
| | Digital Certificates | | Malware |
| | Scan Databases | | Tool |
| | WHOIS | | Vulnerabilities |
| Search Open Websites/Domains | Code Repositories | Stage Capabilities | Drive-by Target |
| | Search Engines | | Install Digital Certificate |
| | Social Media | | Link Target |
| Search Victim-Owned Websites | | | SEO Poisoning |
| | | | Upload Malware |
| | | | Upload Tool |

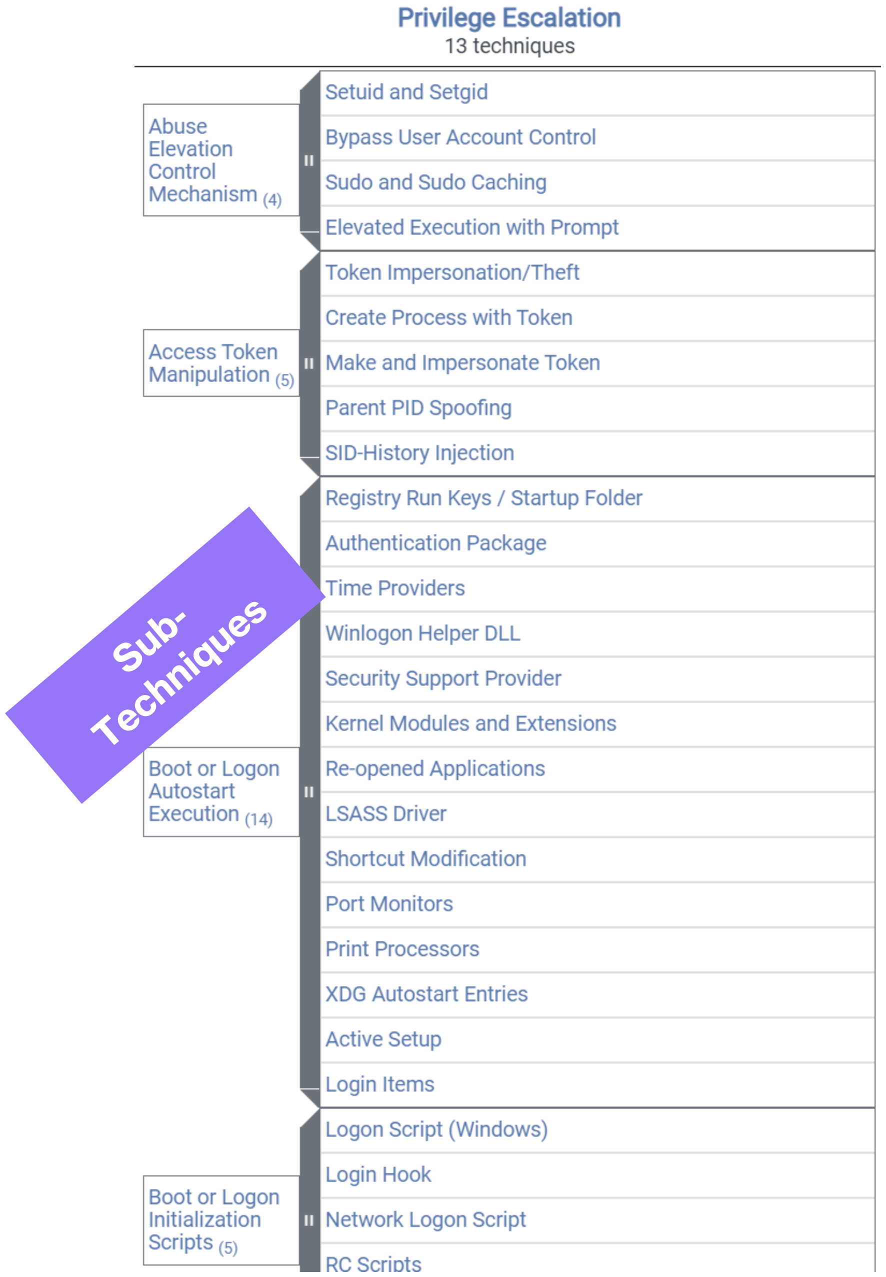
## Matrix



Privilege Escalation
13 techniques

Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or odify System ess (4)
r Policy ification (2)
Escape to Host
Event Triggered Execution (16)
Exploitation for Privilege Escalation
Hijack Execution Flow (12)
Process Injection (12)
Scheduled Task/Job (5)
Valid Accounts (4)

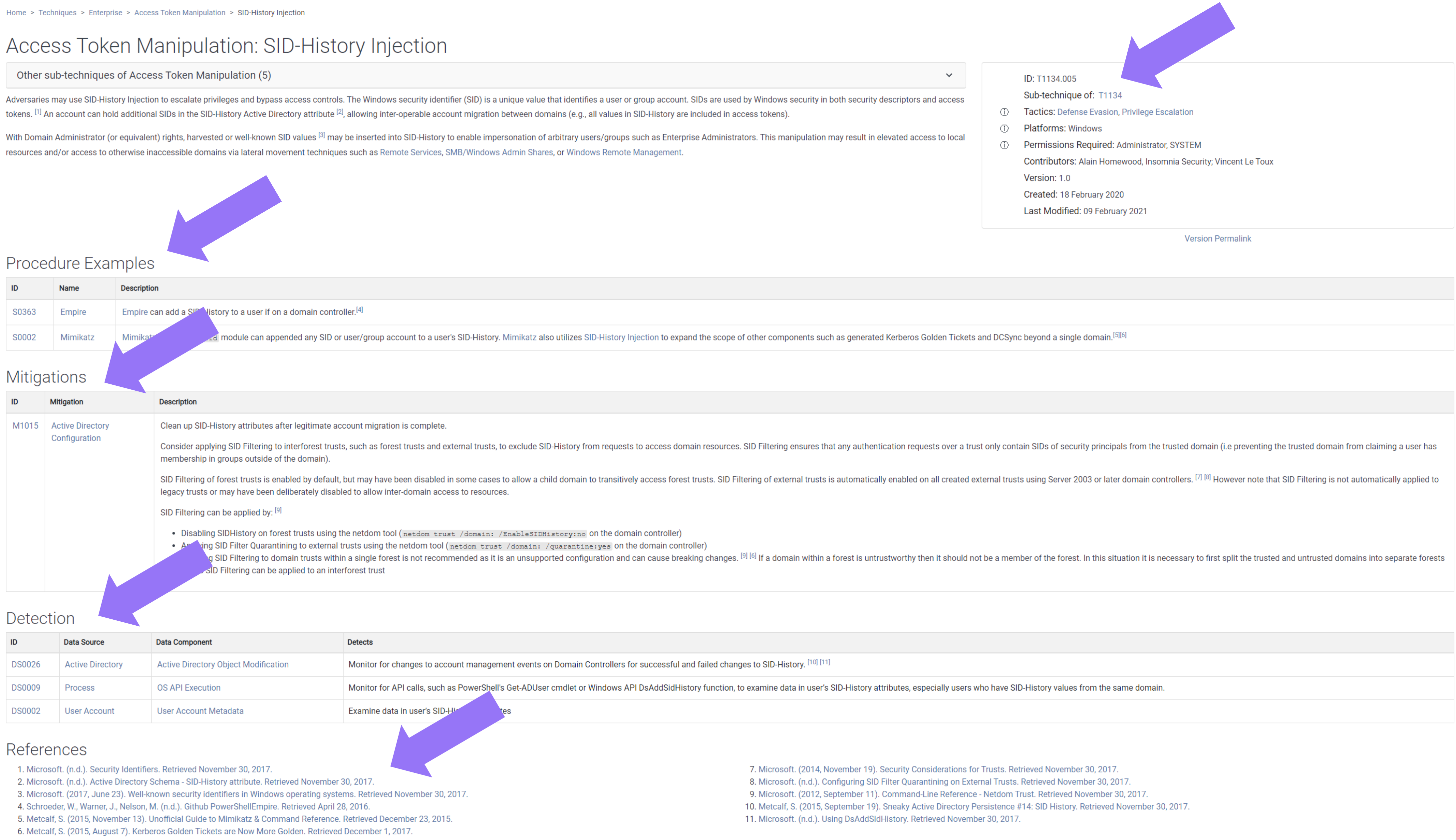
Techniques



Privilege Escalation
13 techniques

| | |
|---|---|
| Abuse Elevation Control Mechanism (4) | Setuid and Setgid<br>Bypass User Account Control<br>Sudo and Sudo Caching<br>Elevated Execution with Prompt |
| Access Token Manipulation (5) | Token Impersonation/Theft<br>Create Process with Token<br>Make and Impersonate Token<br>Parent PID Spoofing<br>SID-History Injection |
| Boot or Logon Autostart Execution (14) | Registry Run Keys / Startup Folder<br>Authentication Package<br>Time Providers<br>Winlogon Helper DLL<br>Security Support Provider<br>Kernel Modules and Extensions<br>Re-opened Applications<br>LSASS Driver<br>Shortcut Modification<br>Port Monitors<br>Print Processors<br>XDG Autostart Entries<br>Active Setup<br>Login Items |
| Boot or Logon Initialization Scripts (5) | Logon Script (Windows)<br>Login Hook<br>Network Logon Script<br>RC Scripts |

Sub-Techniques



Home > Techniques > Enterprise > Access Token Manipulation > SID-History Injection

# Access Token Manipulation: SID-History Injection

Other sub-techniques of Access Token Manipulation (5)

Adversaries may use SID-History Injection to escalate privileges and bypass access controls. The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. [1] An account can hold additional SIDs in the SID-History Active Directory attribute [2], allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).

With Domain Administrator (or equivalent) rights, harvested or well-known SID values [3] may be inserted into SID-History to enable impersonation of arbitrary users/groups such as Enterprise Administrators. This manipulation may result in elevated access to local resources and/or access to otherwise inaccessible domains via lateral movement techniques such as Remote Services, SMB/Windows Admin Shares, or Windows Remote Management.

ID: T1134.005

Sub-technique of: T1134

ⓘ Tactics: Defense Evasion, Privilege Escalation

ⓘ Platforms: Windows

ⓘ Permissions Required: Administrator, SYSTEM

Contributors: Alain Homewood, Insomnia Security; Vincent Le Toux

Version: 1.0

Created: 18 February 2020

Last Modified: 09 February 2021

Version Permalink

## Procedure Examples

| ID | Name | Description |
|---|---|---|
| S0363 | Empire | Empire can add a SID-History to a user if on a domain controller.[4] |
| S0002 | Mimikatz | Mimikat [illegible] module can appended any SID or user/group account to a user's SID-History. Mimikatz also utilizes SID-History Injection to expand the scope of other components such as generated Kerberos Golden Tickets and DCSync beyond a single domain.[5][6] |

## Mitigations

| ID | Mitigation | Description |
|---|---|---|
| M1015 | Active Directory Configuration | Clean up SID-History attributes after legitimate account migration is complete.<br>Consider applying SID Filtering to interforest trusts, such as forest trusts and external trusts, to exclude SID-History from requests to access domain resources. SID Filtering ensures that any authentication requests over a trust only contain SIDs of security principals from the trusted domain (i.e preventing the trusted domain from claiming a user has membership in groups outside of the domain).<br>SID Filtering of forest trusts is enabled by default, but may have been disabled in some cases to allow a child domain to transitively access forest trusts. SID Filtering of external trusts is automatically enabled on all created external trusts using Server 2003 or later domain controllers. [7] [8] However note that SID Filtering is not automatically applied to legacy trusts or may have been deliberately disabled to allow inter-domain access to resources.<br>SID Filtering can be applied by: [9]<br>• Disabling SIDHistory on forest trusts using the netdom tool (`netdom trust /domain: /EnableSIDHistory:no` on the domain controller)<br>• Applying SID Filter Quarantining to external trusts using the netdom tool (`netdom trust /domain: /quarantine:yes` on the domain controller)<br>• [illegible] SID Filtering to domain trusts within a single forest is not recommended as it is an unsupported configuration and can cause breaking changes. [9] [6] If a domain within a forest is untrustworthy then it should not be a member of the forest. In this situation it is necessary to first split the trusted and untrusted domains into separate forests [illegible] SID Filtering can be applied to an interforest trust |

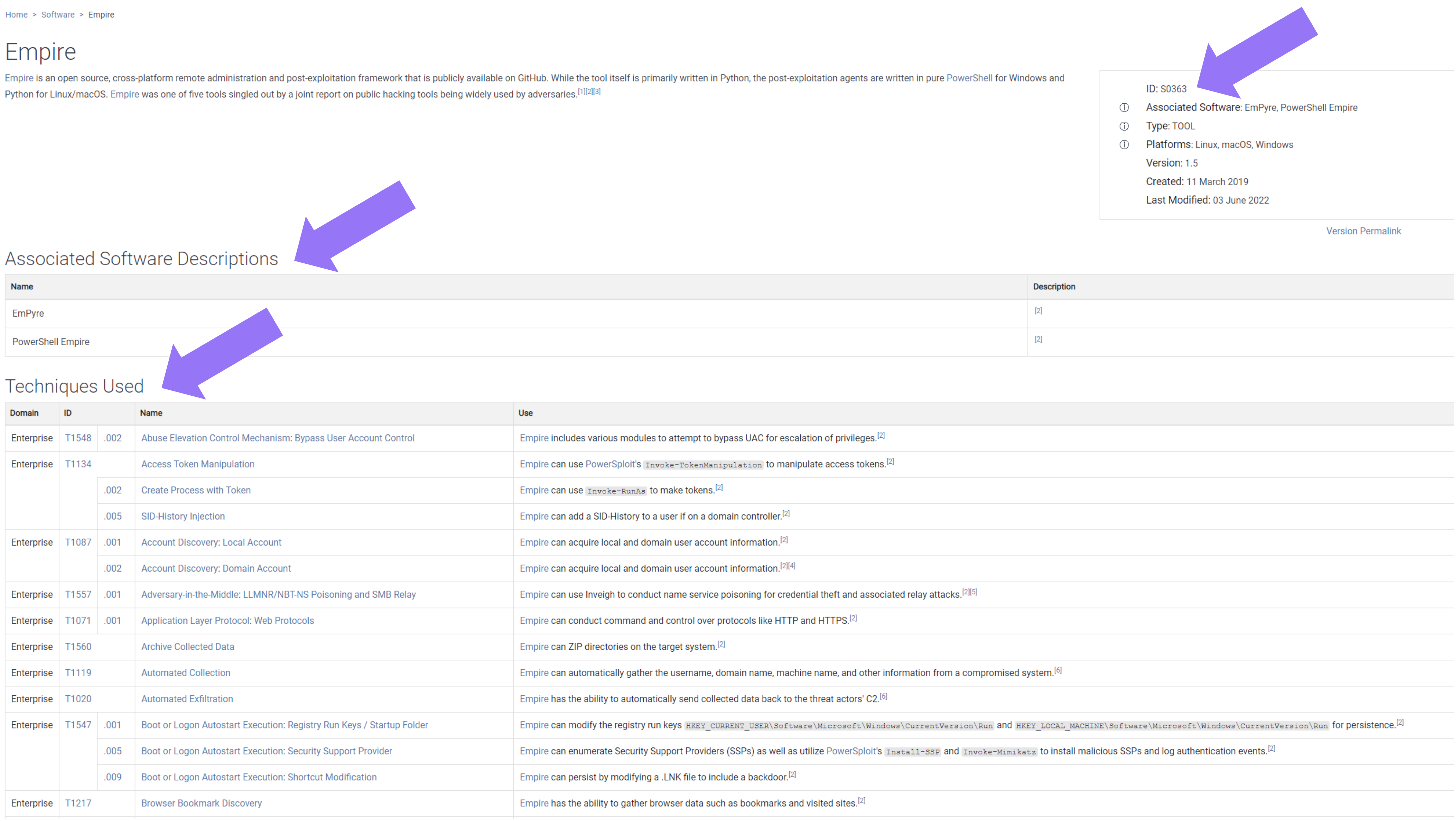
## Detection

| ID | Data Source | Data Component | Detects |
|---|---|---|---|
| DS0026 | Active Directory | Active Directory Object Modification | Monitor for changes to account management events on Domain Controllers for successful and failed changes to SID-History. [10] [11] |
| DS0009 | Process | OS API Execution | Monitor for API calls, such as PowerShell's Get-ADUser cmdlet or Windows API DsAddSidHistory function, to examine data in user's SID-History attributes, especially users who have SID-History values from the same domain. |
| DS0002 | User Account | User Account Metadata | Examine data in user's SID-History attributes |

## References

1. Microsoft. (n.d.). Security Identifiers. Retrieved November 30, 2017.
2. Microsoft. (n.d.). Active Directory Schema - SID-History attribute. Retrieved November 30, 2017.
3. Microsoft. (2017, June 23). Well-known security identifiers in Windows operating systems. Retrieved November 30, 2017.
4. Schroeder, W., Warner, J., Nelson, M. (n.d.). Github PowerShellEmpire. Retrieved April 28, 2016.
5. Metcalf, S. (2015, November 13). Unofficial Guide to Mimikatz & Command Reference. Retrieved December 23, 2015.
6. Metcalf, S. (2015, August 7). Kerberos Golden Tickets are Now More Golden. Retrieved December 1, 2017.
7. Microsoft. (2014, November 19). Security Considerations for Trusts. Retrieved November 30, 2017.
8. Microsoft. (n.d.). Configuring SID Filter Quarantining on External Trusts. Retrieved November 30, 2017.
9. Microsoft. (2012, September 11). Command-Line Reference - Netdom Trust. Retrieved November 30, 2017.
10. Metcalf, S. (2015, September 19). Sneaky Active Directory Persistence #14: SID History. Retrieved November 30, 2017.
11. Microsoft. (n.d.). Using DsAddSidHistory. Retrieved November 30, 2017.

## Matrix – Procedure [1/2]



Home > Software > Empire

# Empire

Empire is an open source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub. While the tool itself is primarily written in Python, the post-exploitation agents are written in pure PowerShell for Windows and Python for Linux/macOS. Empire was one of five tools singled out by a joint report on public hacking tools being widely used by adversaries.[1][2][3]

ID: S0363

ⓘ Associated Software: EmPyre, PowerShell Empire

ⓘ Type: TOOL

ⓘ Platforms: Linux, macOS, Windows

Version: 1.5

Created: 11 March 2019

Last Modified: 03 June 2022

Version Permalink

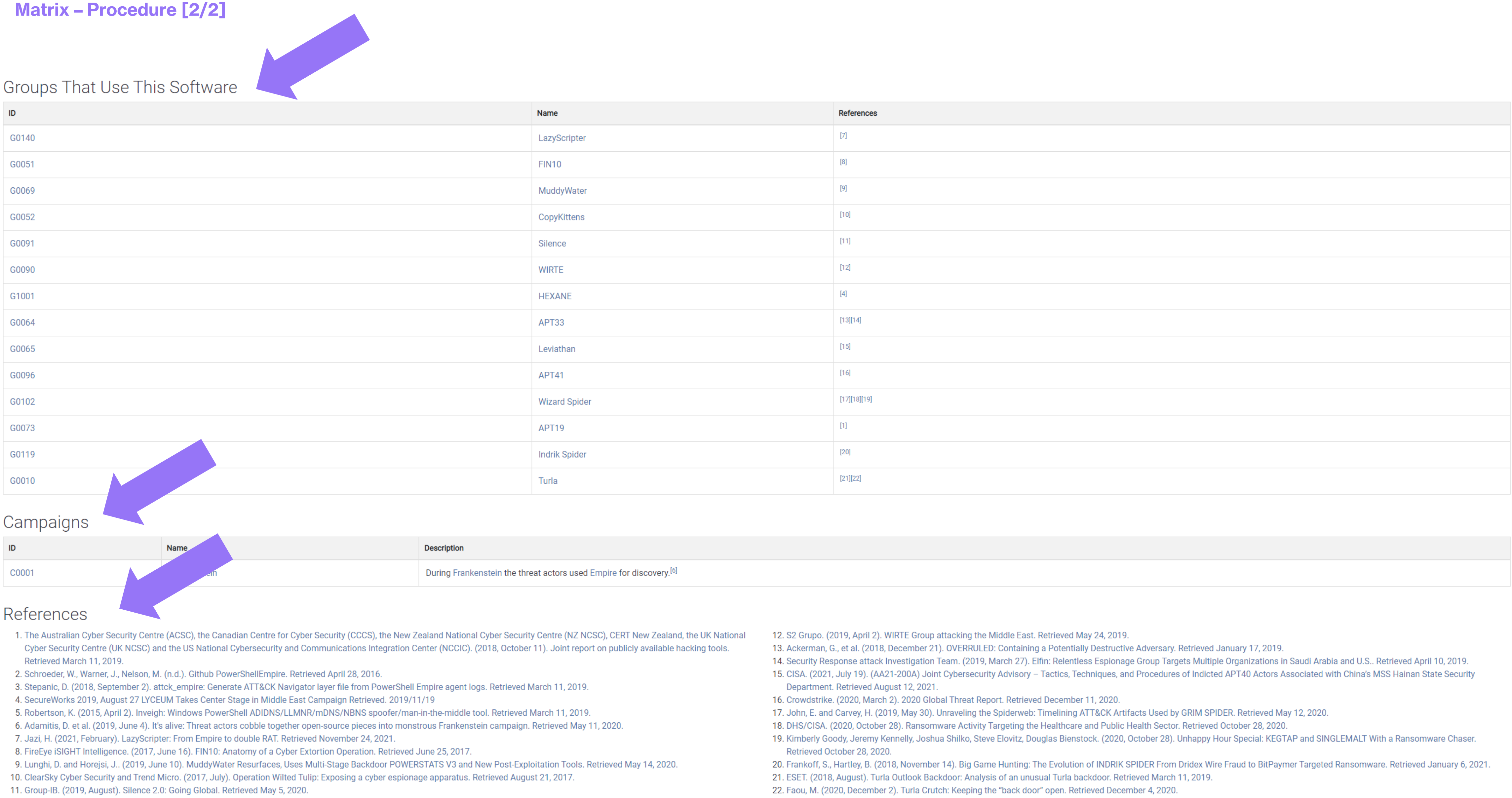
## Associated Software Descriptions

| Name | Description |
|---|---|
| EmPyre | [2] |
| PowerShell Empire | [2] |

## Techniques Used

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1548 | .002 | Abuse Elevation Control Mechanism: Bypass User Account Control | Empire includes various modules to attempt to bypass UAC for escalation of privileges.[2] |
| Enterprise | T1134 | | Access Token Manipulation | Empire can use PowerSploit's `Invoke-TokenManipulation` to manipulate access tokens.[2] |
| | | .002 | Create Process with Token | Empire can use `Invoke-RunAs` to make tokens.[2] |
| | | .005 | SID-History Injection | Empire can add a SID-History to a user if on a domain controller.[2] |
| Enterprise | T1087 | .001 | Account Discovery: Local Account | Empire can acquire local and domain user account information.[2] |
| | | .002 | Account Discovery: Domain Account | Empire can acquire local and domain user account information.[2][4] |
| Enterprise | T1557 | .001 | Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay | Empire can use Inveigh to conduct name service poisoning for credential theft and associated relay attacks.[2][5] |
| Enterprise | T1071 | .001 | Application Layer Protocol: Web Protocols | Empire can conduct command and control over protocols like HTTP and HTTPS.[2] |
| Enterprise | T1560 | | Archive Collected Data | Empire can ZIP directories on the target system.[2] |
| Enterprise | T1119 | | Automated Collection | Empire can automatically gather the username, domain name, machine name, and other information from a compromised system.[6] |
| Enterprise | T1020 | | Automated Exfiltration | Empire has the ability to automatically send collected data back to the threat actors' C2.[6] |
| Enterprise | T1547 | .001 | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder | Empire can modify the registry run keys `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` and `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` for persistence.[2] |
| | | .005 | Boot or Logon Autostart Execution: Security Support Provider | Empire can enumerate Security Support Providers (SSPs) as well as utilize PowerSploit's `Install-SSP` and `Invoke-Mimikatz` to install malicious SSPs and log authentication events.[2] |
| | | .009 | Boot or Logon Autostart Execution: Shortcut Modification | Empire can persist by modifying a .LNK file to include a backdoor.[2] |
| Enterprise | T1217 | | Browser Bookmark Discovery | Empire has the ability to gather browser data such as bookmarks and visited sites.[2] |

## Matrix – Procedure [2/2]



### Groups That Use This Software

| ID | Name | References |
|---|---|---|
| G0140 | LazyScripter | [7] |
| G0051 | FIN10 | [8] |
| G0069 | MuddyWater | [9] |
| G0052 | CopyKittens | [10] |
| G0091 | Silence | [11] |
| G0090 | WIRTE | [12] |
| G1001 | HEXANE | [4] |
| G0064 | APT33 | [13][14] |
| G0065 | Leviathan | [15] |
| G0096 | APT41 | [16] |
| G0102 | Wizard Spider | [17][18][19] |
| G0073 | APT19 | [1] |
| G0119 | Indrik Spider | [20] |
| G0010 | Turla | [21][22] |

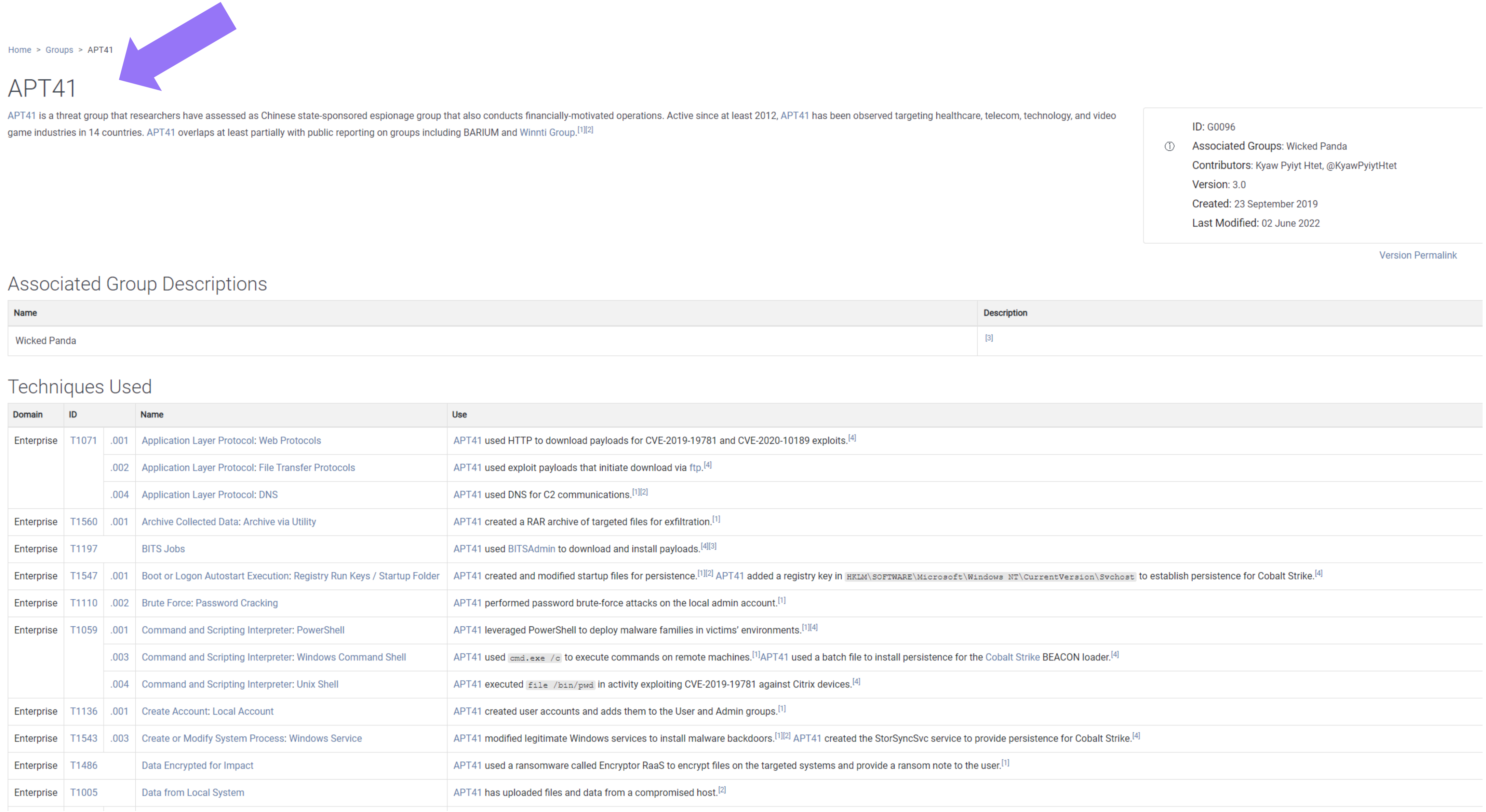
### Campaigns

| ID | Name | Description |
|---|---|---|
| C0001 | ein | During Frankenstein the threat actors used Empire for discovery.[6] |

### References

1. The Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NZ NCSC), CERT New Zealand, the UK National Cyber Security Centre (UK NCSC) and the US National Cybersecurity and Communications Integration Center (NCCIC). (2018, October 11). Joint report on publicly available hacking tools. Retrieved March 11, 2019.
2. Schroeder, W., Warner, J., Nelson, M. (n.d.). Github PowerShellEmpire. Retrieved April 28, 2016.
3. Stepanic, D. (2018, September 2). attck_empire: Generate ATT&CK Navigator layer file from PowerShell Empire agent logs. Retrieved March 11, 2019.
4. SecureWorks 2019, August 27 LYCEUM Takes Center Stage in Middle East Campaign Retrieved. 2019/11/19
5. Robertson, K. (2015, April 2). Inveigh: Windows PowerShell ADIDNS/LLMNR/mDNS/NBNS spoofer/man-in-the-middle tool. Retrieved March 11, 2019.
6. Adamitis, D. et al. (2019, June 4). It's alive: Threat actors cobble together open-source pieces into monstrous Frankenstein campaign. Retrieved May 11, 2020.
7. Jazi, H. (2021, February). LazyScripter: From Empire to double RAT. Retrieved November 24, 2021.
8. FireEye iSIGHT Intelligence. (2017, June 16). FIN10: Anatomy of a Cyber Extortion Operation. Retrieved June 25, 2017.
9. Lunghi, D. and Horejsi, J.. (2019, June 10). MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools. Retrieved May 14, 2020.
10. ClearSky Cyber Security and Trend Micro. (2017, July). Operation Wilted Tulip: Exposing a cyber espionage apparatus. Retrieved August 21, 2017.
11. Group-IB. (2019, August). Silence 2.0: Going Global. Retrieved May 5, 2020.
12. S2 Grupo. (2019, April 2). WIRTE Group attacking the Middle East. Retrieved May 24, 2019.
13. Ackerman, G., et al. (2018, December 21). OVERRULED: Containing a Potentially Destructive Adversary. Retrieved January 17, 2019.
14. Security Response attack Investigation Team. (2019, March 27). Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.. Retrieved April 10, 2019.
15. CISA. (2021, July 19). (AA21-200A) Joint Cybersecurity Advisory – Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department. Retrieved August 12, 2021.
16. Crowdstrike. (2020, March 2). 2020 Global Threat Report. Retrieved December 11, 2020.
17. John, E. and Carvey, H. (2019, May 30). Unraveling the Spiderweb: Timelining ATT&CK Artifacts Used by GRIM SPIDER. Retrieved May 12, 2020.
18. DHS/CISA. (2020, October 28). Ransomware Activity Targeting the Healthcare and Public Health Sector. Retrieved October 28, 2020.
19. Kimberly Goody, Jeremy Kennelly, Joshua Shilko, Steve Elovitz, Douglas Bienstock. (2020, October 28). Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser. Retrieved October 28, 2020.
20. Frankoff, S., Hartley, B. (2018, November 14). Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware. Retrieved January 6, 2021.
21. ESET. (2018, August). Turla Outlook Backdoor: Analysis of an unusual Turla backdoor. Retrieved March 11, 2019.
22. Faou, M. (2020, December 2). Turla Crutch: Keeping the "back door" open. Retrieved December 4, 2020.

## Matrix - Group



Home > Groups > APT41

# APT41

APT41 is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, APT41 has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. APT41 overlaps at least partially with public reporting on groups including BARIUM and Winnti Group.[1][2]

ID: G0096
ⓘ Associated Groups: Wicked Panda
Contributors: Kyaw Pyiyt Htet, @KyawPyiytHtet
Version: 3.0
Created: 23 September 2019
Last Modified: 02 June 2022

Version Permalink

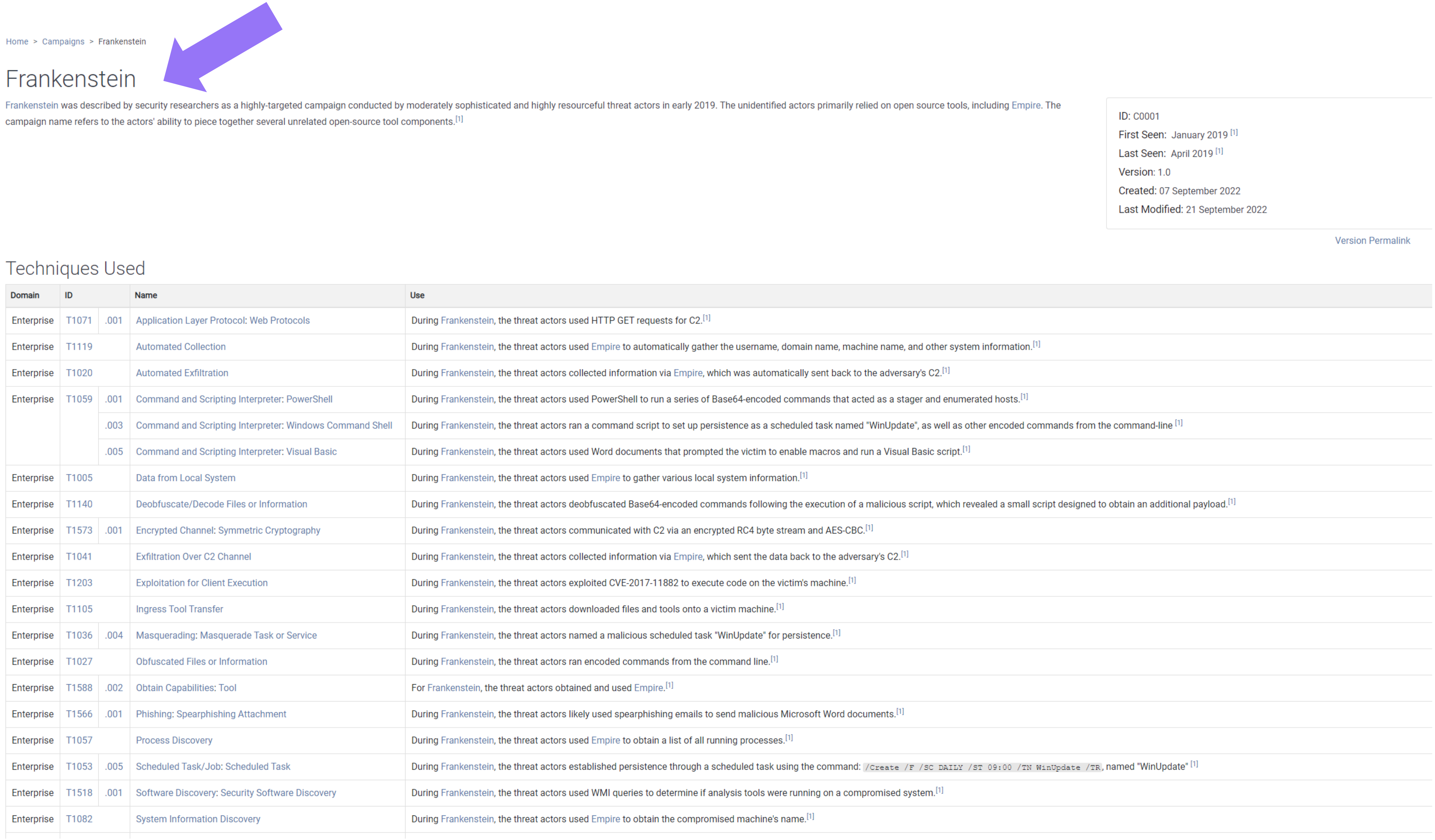
## Associated Group Descriptions

| Name | Description |
|---|---|
| Wicked Panda | [3] |

## Techniques Used

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1071 | .001 | Application Layer Protocol: Web Protocols | APT41 used HTTP to download payloads for CVE-2019-19781 and CVE-2020-10189 exploits.[4] |
| | | .002 | Application Layer Protocol: File Transfer Protocols | APT41 used exploit payloads that initiate download via ftp.[4] |
| | | .004 | Application Layer Protocol: DNS | APT41 used DNS for C2 communications.[1][2] |
| Enterprise | T1560 | .001 | Archive Collected Data: Archive via Utility | APT41 created a RAR archive of targeted files for exfiltration.[1] |
| Enterprise | T1197 | | BITS Jobs | APT41 used BITSAdmin to download and install payloads.[4][3] |
| Enterprise | T1547 | .001 | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder | APT41 created and modified startup files for persistence.[1][2] APT41 added a registry key in `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost` to establish persistence for Cobalt Strike.[4] |
| Enterprise | T1110 | .002 | Brute Force: Password Cracking | APT41 performed password brute-force attacks on the local admin account.[1] |
| Enterprise | T1059 | .001 | Command and Scripting Interpreter: PowerShell | APT41 leveraged PowerShell to deploy malware families in victims' environments.[1][4] |
| | | .003 | Command and Scripting Interpreter: Windows Command Shell | APT41 used `cmd.exe /c` to execute commands on remote machines.[1]APT41 used a batch file to install persistence for the Cobalt Strike BEACON loader.[4] |
| | | .004 | Command and Scripting Interpreter: Unix Shell | APT41 executed `file /bin/pwd` in activity exploiting CVE-2019-19781 against Citrix devices.[4] |
| Enterprise | T1136 | .001 | Create Account: Local Account | APT41 created user accounts and adds them to the User and Admin groups.[1] |
| Enterprise | T1543 | .003 | Create or Modify System Process: Windows Service | APT41 modified legitimate Windows services to install malware backdoors.[1][2] APT41 created the StorSyncSvc service to provide persistence for Cobalt Strike.[4] |
| Enterprise | T1486 | | Data Encrypted for Impact | APT41 used a ransomware called Encryptor RaaS to encrypt files on the targeted systems and provide a ransom note to the user.[1] |
| Enterprise | T1005 | | Data from Local System | APT41 has uploaded files and data from a compromised host.[2] |

## Matrix - Campaign



Home > Campaigns > Frankenstein

# Frankenstein

Frankenstein was described by security researchers as a highly-targeted campaign conducted by moderately sophisticated and highly resourceful threat actors in early 2019. The unidentified actors primarily relied on open source tools, including Empire. The campaign name refers to the actors' ability to piece together several unrelated open-source tool components.[1]

ID: C0001
First Seen: January 2019 [1]
Last Seen: April 2019 [1]
Version: 1.0
Created: 07 September 2022
Last Modified: 21 September 2022

Version Permalink

## Techniques Used

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1071 | .001 | Application Layer Protocol: Web Protocols | During Frankenstein, the threat actors used HTTP GET requests for C2.[1] |
| Enterprise | T1119 | | Automated Collection | During Frankenstein, the threat actors used Empire to automatically gather the username, domain name, machine name, and other system information.[1] |
| Enterprise | T1020 | | Automated Exfiltration | During Frankenstein, the threat actors collected information via Empire, which was automatically sent back to the adversary's C2.[1] |
| Enterprise | T1059 | .001 | Command and Scripting Interpreter: PowerShell | During Frankenstein, the threat actors used PowerShell to run a series of Base64-encoded commands that acted as a stager and enumerated hosts.[1] |
| | | .003 | Command and Scripting Interpreter: Windows Command Shell | During Frankenstein, the threat actors ran a command script to set up persistence as a scheduled task named "WinUpdate", as well as other encoded commands from the command-line [1] |
| | | .005 | Command and Scripting Interpreter: Visual Basic | During Frankenstein, the threat actors used Word documents that prompted the victim to enable macros and run a Visual Basic script.[1] |
| Enterprise | T1005 | | Data from Local System | During Frankenstein, the threat actors used Empire to gather various local system information.[1] |
| Enterprise | T1140 | | Deobfuscate/Decode Files or Information | During Frankenstein, the threat actors deobfuscated Base64-encoded commands following the execution of a malicious script, which revealed a small script designed to obtain an additional payload.[1] |
| Enterprise | T1573 | .001 | Encrypted Channel: Symmetric Cryptography | During Frankenstein, the threat actors communicated with C2 via an encrypted RC4 byte stream and AES-CBC.[1] |
| Enterprise | T1041 | | Exfiltration Over C2 Channel | During Frankenstein, the threat actors collected information via Empire, which sent the data back to the adversary's C2.[1] |
| Enterprise | T1203 | | Exploitation for Client Execution | During Frankenstein, the threat actors exploited CVE-2017-11882 to execute code on the victim's machine.[1] |
| Enterprise | T1105 | | Ingress Tool Transfer | During Frankenstein, the threat actors downloaded files and tools onto a victim machine.[1] |
| Enterprise | T1036 | .004 | Masquerading: Masquerade Task or Service | During Frankenstein, the threat actors named a malicious scheduled task "WinUpdate" for persistence.[1] |
| Enterprise | T1027 | | Obfuscated Files or Information | During Frankenstein, the threat actors ran encoded commands from the command line.[1] |
| Enterprise | T1588 | .002 | Obtain Capabilities: Tool | For Frankenstein, the threat actors obtained and used Empire.[1] |
| Enterprise | T1566 | .001 | Phishing: Spearphishing Attachment | During Frankenstein, the threat actors likely used spearphishing emails to send malicious Microsoft Word documents.[1] |
| Enterprise | T1057 | | Process Discovery | During Frankenstein, the threat actors used Empire to obtain a list of all running processes.[1] |
| Enterprise | T1053 | .005 | Scheduled Task/Job: Scheduled Task | During Frankenstein, the threat actors established persistence through a scheduled task using the command: `/Create /F /SC DAILY /ST 09:00 /TN WinUpdate /TR`, named "WinUpdate" [1] |
| Enterprise | T1518 | .001 | Software Discovery: Security Software Discovery | During Frankenstein, the threat actors used WMI queries to determine if analysis tools were running on a compromised system.[1] |
| Enterprise | T1082 | | System Information Discovery | During Frankenstein, the threat actors used Empire to obtain the compromised machine's name.[1] |

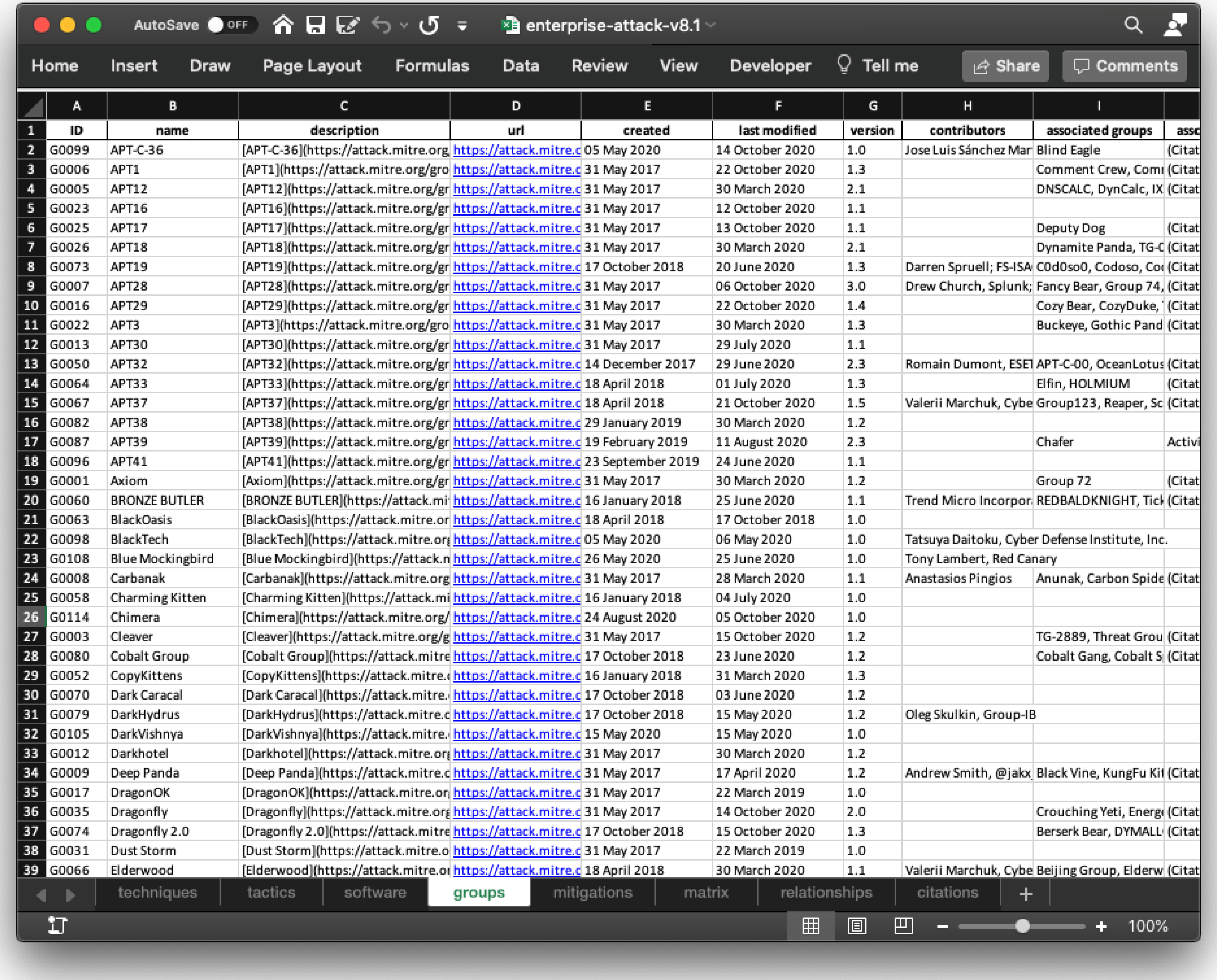
Comprendre et améliorer sa sécurité grâce à MITRE ATT&CK

# _05_

# MITRE
# Tools & data

# MITRE Tools & data

## ATT&CK in Excel

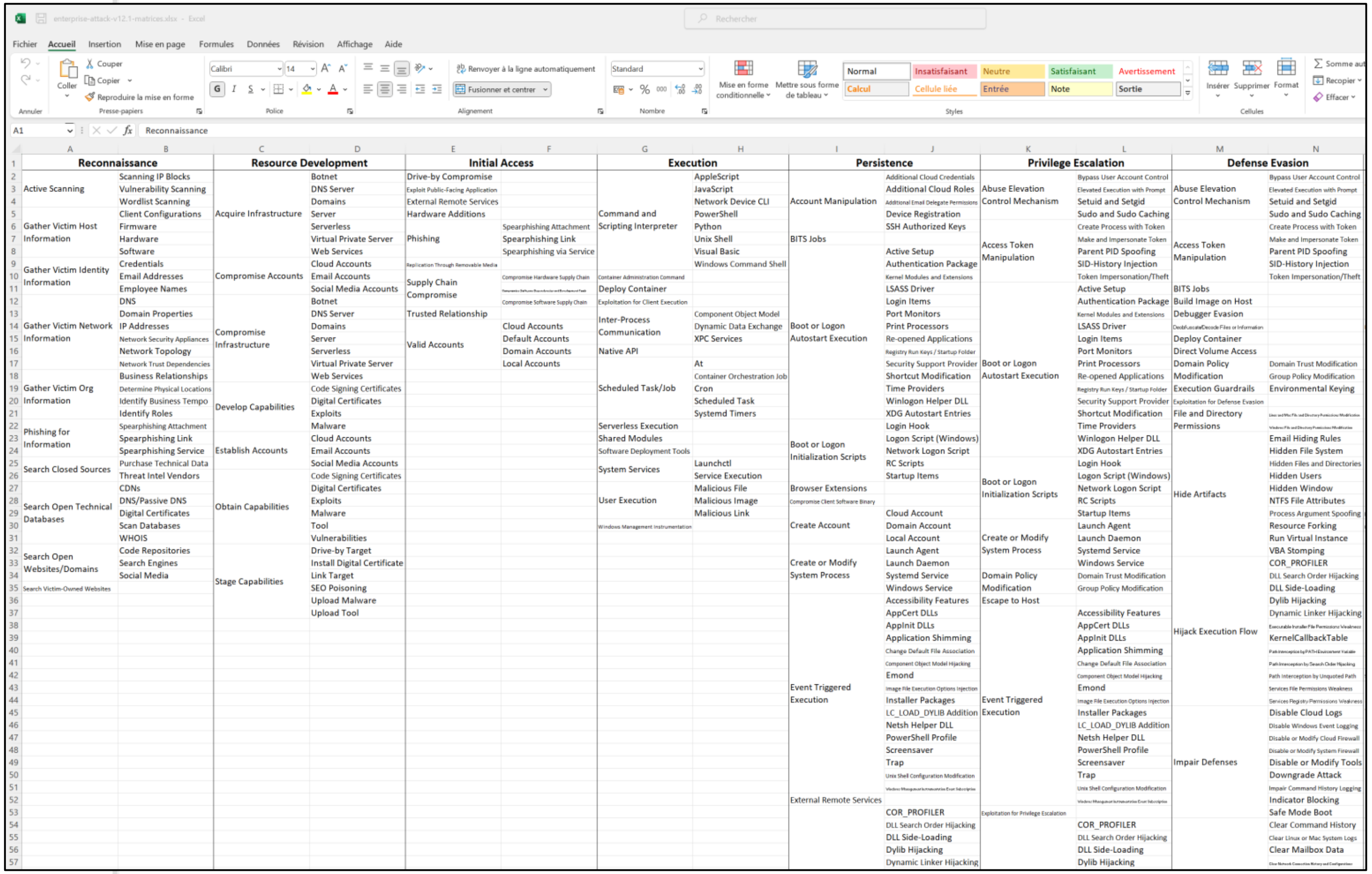


| | A | B | C | D | E | F | G | H | I | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ID | name | description | url | created | last modified | version | contributors | associated groups | assc |
| 2 | G0099 | APT-C-36 | [APT-C-36](https://attack.mitre.org | https://attack.mitre.c | 05 May 2020 | 14 October 2020 | 1.0 | Jose Luis Sánchez Mar | Blind Eagle | (Citat |
| 3 | G0006 | APT1 | [APT1](https://attack.mitre.org/gro | https://attack.mitre.c | 31 May 2017 | 22 October 2020 | 1.3 | | Comment Crew, Comı | (Citat |
| 4 | G0005 | APT12 | [APT12](https://attack.mitre.org/gr | https://attack.mitre.c | 31 May 2017 | 30 March 2020 | 2.1 | | DNSCALC, DynCalc, IX | (Citat |
| 5 | G0023 | APT16 | [APT16](https://attack.mitre.org/gr | https://attack.mitre.c | 31 May 2017 | 12 October 2020 | 1.1 | | | |
| 6 | G0025 | APT17 | [APT17](https://attack.mitre.org/gr | https://attack.mitre.c | 31 May 2017 | 13 October 2020 | 1.1 | | Deputy Dog | (Citat |
| 7 | G0026 | APT18 | [APT18](https://attack.mitre.org/gr | https://attack.mitre.c | 31 May 2017 | 30 March 2020 | 2.1 | | Dynamite Panda, TG-C | (Citat |
| 8 | G0073 | APT19 | [APT19](https://attack.mitre.org/gr | https://attack.mitre.c | 17 October 2018 | 20 June 2020 | 1.3 | Darren Spruell; FS-ISA | C0d0so0, Codoso, Co | (Citat |
| 9 | G0007 | APT28 | [APT28](https://attack.mitre.org/gr | https://attack.mitre.c | 31 May 2017 | 06 October 2020 | 3.0 | Drew Church, Splunk; | Fancy Bear, Group 74, | (Citat |
| 10 | G0016 | APT29 | [APT29](https://attack.mitre.org/gr | https://attack.mitre.c | 31 May 2017 | 22 October 2020 | 1.4 | | Cozy Bear, CozyDuke, | (Citat |
| 11 | G0022 | APT3 | [APT3](https://attack.mitre.org/gro | https://attack.mitre.c | 31 May 2017 | 30 March 2020 | 1.3 | | Buckeye, Gothic Pand | (Citat |
| 12 | G0013 | APT30 | [APT30](https://attack.mitre.org/gr | https://attack.mitre.c | 31 May 2017 | 29 July 2020 | 1.1 | | | |
| 13 | G0050 | APT32 | [APT32](https://attack.mitre.org/gr | https://attack.mitre.c | 14 December 2017 | 29 June 2020 | 2.3 | Romain Dumont, ESET | APT-C-00, OceanLotus | (Citat |
| 14 | G0064 | APT33 | [APT33](https://attack.mitre.org/gr | https://attack.mitre.c | 18 April 2018 | 01 July 2020 | 1.3 | | Elfin, HOLMIUM | (Citat |
| 15 | G0067 | APT37 | [APT37](https://attack.mitre.org/gr | https://attack.mitre.c | 18 April 2018 | 21 October 2020 | 1.5 | Valerii Marchuk, Cybe | Group123, Reaper, Sc | (Citat |
| 16 | G0082 | APT38 | [APT38](https://attack.mitre.org/gr | https://attack.mitre.c | 29 January 2019 | 30 March 2020 | 1.2 | | | |
| 17 | G0087 | APT39 | [APT39](https://attack.mitre.org/gr | https://attack.mitre.c | 19 February 2019 | 11 August 2020 | 2.3 | | Chafer | Activi |
| 18 | G0096 | APT41 | [APT41](https://attack.mitre.org/gr | https://attack.mitre.c | 23 September 2019 | 24 June 2020 | 1.1 | | | |
| 19 | G0001 | Axiom | [Axiom](https://attack.mitre.org/gr | https://attack.mitre.c | 31 May 2017 | 30 March 2020 | 1.2 | | Group 72 | (Citat |
| 20 | G0060 | BRONZE BUTLER | [BRONZE BUTLER](https://attack.mi | https://attack.mitre.c | 16 January 2018 | 25 June 2020 | 1.1 | Trend Micro Incorpor | REDBALDKNIGHT, Tick | (Citat |
| 21 | G0063 | BlackOasis | [BlackOasis](https://attack.mitre.or | https://attack.mitre.c | 18 April 2018 | 17 October 2018 | 1.0 | | | |
| 22 | G0098 | BlackTech | [BlackTech](https://attack.mitre.org | https://attack.mitre.c | 05 May 2020 | 06 May 2020 | 1.0 | Tatsuya Daitoku, Cyber Defense Institute, Inc. | | |
| 23 | G0108 | Blue Mockingbird | [Blue Mockingbird](https://attack.n | https://attack.mitre.c | 26 May 2020 | 25 June 2020 | 1.0 | Tony Lambert, Red Canary | | |
| 24 | G0008 | Carbanak | [Carbanak](https://attack.mitre.org | https://attack.mitre.c | 31 May 2017 | 28 March 2020 | 1.1 | Anastasios Pingios | Anunak, Carbon Spide | (Citat |
| 25 | G0058 | Charming Kitten | [Charming Kitten](https://attack.mi | https://attack.mitre.c | 16 January 2018 | 04 July 2020 | 1.0 | | | |
| 26 | G0114 | Chimera | [Chimera](https://attack.mitre.org/ | https://attack.mitre.c | 24 August 2020 | 05 October 2020 | 1.0 | | | |
| 27 | G0003 | Cleaver | [Cleaver](https://attack.mitre.org/g | https://attack.mitre.c | 31 May 2017 | 15 October 2020 | 1.2 | | TG-2889, Threat Grou | (Citat |
| 28 | G0080 | Cobalt Group | [Cobalt Group](https://attack.mitre | https://attack.mitre.c | 17 October 2018 | 23 June 2020 | 1.2 | | Cobalt Gang, Cobalt S | (Citat |
| 29 | G0052 | CopyKittens | [CopyKittens](https://attack.mitre. | https://attack.mitre.c | 16 January 2018 | 31 March 2020 | 1.3 | | | |
| 30 | G0070 | Dark Caracal | [Dark Caracal](https://attack.mitre. | https://attack.mitre.c | 17 October 2018 | 03 June 2020 | 1.2 | | | |
| 31 | G0079 | DarkHydrus | [DarkHydrus](https://attack.mitre.c | https://attack.mitre.c | 17 October 2018 | 15 May 2020 | 1.2 | Oleg Skulkin, Group-IB | | |
| 32 | G0105 | DarkVishnya | [DarkVishnya](https://attack.mitre. | https://attack.mitre.c | 15 May 2020 | 15 May 2020 | 1.0 | | | |
| 33 | G0012 | Darkhotel | [Darkhotel](https://attack.mitre.org | https://attack.mitre.c | 31 May 2017 | 30 March 2020 | 1.2 | | | |
| 34 | G0009 | Deep Panda | [Deep Panda](https://attack.mitre.c | https://attack.mitre.c | 31 May 2017 | 17 April 2020 | 1.2 | Andrew Smith, @jakx | Black Vine, KungFu Kit | (Citat |
| 35 | G0017 | DragonOK | [DragonOK](https://attack.mitre.or | https://attack.mitre.c | 31 May 2017 | 22 March 2019 | 1.0 | | | |
| 36 | G0035 | Dragonfly | [Dragonfly](https://attack.mitre.org | https://attack.mitre.c | 31 May 2017 | 14 October 2020 | 2.0 | | Crouching Yeti, Energ | (Citat |
| 37 | G0074 | Dragonfly 2.0 | [Dragonfly 2.0](https://attack.mitre | https://attack.mitre.c | 17 October 2018 | 15 October 2020 | 1.3 | | Berserk Bear, DYMALL | (Citat |
| 38 | G0031 | Dust Storm | [Dust Storm](https://attack.mitre.o | https://attack.mitre.c | 31 May 2017 | 22 March 2019 | 1.0 | | | |
| 39 | G0066 | Elderwood | [Elderwood](https://attack.mitre.o | https://attack.mitre.c | 18 April 2018 | 30 March 2020 | 1.1 | Valerii Marchuk, Cybe | Beijing Group, Elderw | (Citat |

Excel spreadsheets representing the ATT&CK dataset. These spreadsheets are built from the STIX dataset and provide a more human-accessible view into the knowledge base while also supporting rudimentary querying/filtering capabilities.

## ATT&CK in Excel

- enterprise-attack-v12.1.xlsx
  - enterprise-attack-v12.1-matrices.xlsx
  - enterprise-attack-v12.1-mitigations.xlsx
  - enterprise-attack-v12.1-relationships.xlsx
  - enterprise-attack-v12.1-software.xlsx
  - enterprise-attack-v12.1-groups.xlsx
  - enterprise-attack-v12.1-tactics.xlsx
  - enterprise-attack-v12.1-techniques.xlsx
  - enterprise-attack-v12.1-datasources.xlsx
  - enterprise-attack-v12.1-campaigns.xlsx
- mobile-attack-v12.1.xlsx
  - mobile-attack-v12.1-matrices.xlsx
  - mobile-attack-v12.1-mitigations.xlsx
  - mobile-attack-v12.1-relationships.xlsx
  - mobile-attack-v12.1-software.xlsx
  - mobile-attack-v12.1-groups.xlsx
  - mobile-attack-v12.1-tactics.xlsx
  - mobile-attack-v12.1-techniques.xlsx
  - mobile-attack-v12.1-campaigns.xlsx
- ics-attack-v12.1.xlsx
  - ics-attack-v12.1-matrices.xlsx
  - ics-attack-v12.1-mitigations.xlsx
  - ics-attack-v12.1-relationships.xlsx
  - ics-attack-v12.1-software.xlsx
  - ics-attack-v12.1-groups.xlsx
  - ics-attack-v12.1-tactics.xlsx
  - ics-attack-v12.1-techniques.xlsx
  - ics-attack-v12.1-campaigns.xlsx

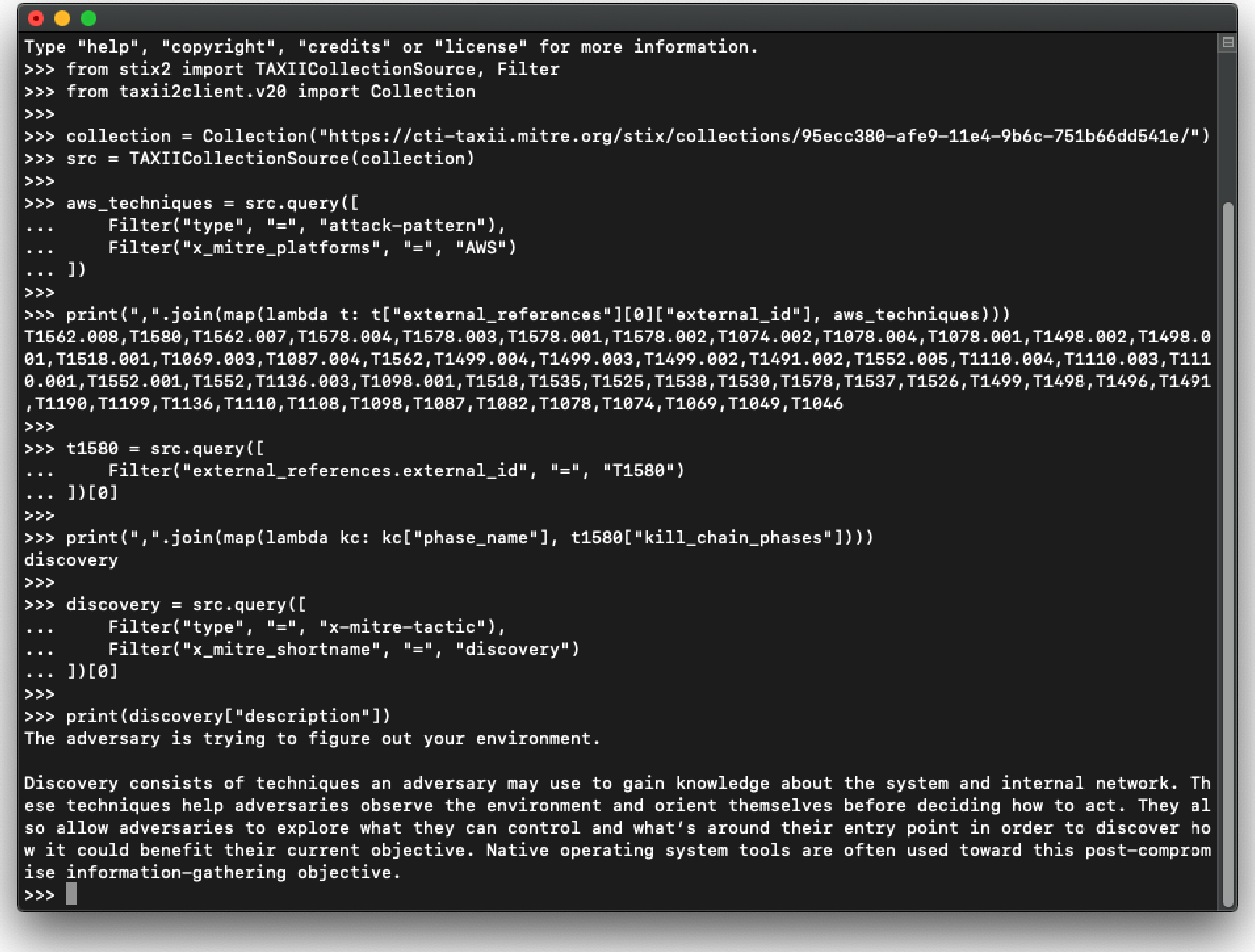


A1 Reconnaissance

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Reconnaissance | | Resource Development | | Initial Access | | Execution | | Persistence | | Privilege Escalation | | Defense Evasion | |
| 2 | Active Scanning | Scanning IP Blocks | Acquire Infrastructure | Botnet | Drive-by Compromise | | Command and Scripting Interpreter | AppleScript | Account Manipulation | Additional Cloud Credentials | Abuse Elevation Control Mechanism | Bypass User Account Control | Abuse Elevation Control Mechanism | Bypass User Account Control |
| 3 | | Vulnerability Scanning | | DNS Server | Exploit Public-Facing Application | | | JavaScript | | Additional Cloud Roles | | Elevated Execution with Prompt | | Elevated Execution with Prompt |
| 4 | | Wordlist Scanning | | Domains | External Remote Services | | | Network Device CLI | | Additional Email Delegate Permissions | | Setuid and Setgid | | Setuid and Setgid |
| 5 | Gather Victim Host Information | Client Configurations | | Server | Hardware Additions | | | PowerShell | | Device Registration | | Sudo and Sudo Caching | | Sudo and Sudo Caching |
| 6 | | Firmware | | Serverless | Phishing | Spearphishing Attachment | | Python | | SSH Authorized Keys | Access Token Manipulation | Create Process with Token | Access Token Manipulation | Create Process with Token |
| 7 | | Hardware | | Virtual Private Server | | Spearphishing Link | | Unix Shell | BITS Jobs | | | Make and Impersonate Token | | Make and Impersonate Token |
| 8 | | Software | | Web Services | | Spearphishing via Service | | Visual Basic | Boot or Logon Autostart Execution | Active Setup | | Parent PID Spoofing | | Parent PID Spoofing |
| 9 | Gather Victim Identity Information | Credentials | Compromise Accounts | Cloud Accounts | Replication Through Removable Media | | | Windows Command Shell | | Authentication Package | | SID-History Injection | | SID-History Injection |
| 10 | | Email Addresses | | Email Accounts | Supply Chain Compromise | Compromise Hardware Supply Chain | Container Administration Command | | | Kernel Modules and Extensions | | Token Impersonation/Theft | | Token Impersonation/Theft |
| 11 | | Employee Names | | Social Media Accounts | | Compromise Software Dependencies and Development Tools | Deploy Container | | | LSASS Driver | Boot or Logon Autostart Execution | Active Setup | BITS Jobs | |
| 12 | Gather Victim Network Information | DNS | Compromise Infrastructure | Botnet | | Compromise Software Supply Chain | Exploitation for Client Execution | | | Login Items | | Authentication Package | Build Image on Host | |
| 13 | | Domain Properties | | DNS Server | Trusted Relationship | | Inter-Process Communication | Component Object Model | | Port Monitors | | Kernel Modules and Extensions | Debugger Evasion | |
| 14 | | IP Addresses | | Domains | Valid Accounts | Cloud Accounts | | Dynamic Data Exchange | | Print Processors | | LSASS Driver | Deobfuscate/Decode Files or Information | |
| 15 | | Network Security Appliances | | Server | | Default Accounts | | XPC Services | | Re-opened Applications | | Login Items | Deploy Container | |
| 16 | | Network Topology | | Serverless | | Domain Accounts | Native API | | | Registry Run Keys / Startup Folder | | Port Monitors | Direct Volume Access | |
| 17 | | Network Trust Dependencies | | Virtual Private Server | | Local Accounts | Scheduled Task/Job | At | | Security Support Provider | | Print Processors | Domain Policy Modification | Domain Trust Modification |
| 18 | Gather Victim Org Information | Business Relationships | | Web Services | | | | Container Orchestration Job | | Shortcut Modification | | Re-opened Applications | | Group Policy Modification |
| 19 | | Determine Physical Locations | Develop Capabilities | Code Signing Certificates | | | | Cron | | Time Providers | | Registry Run Keys / Startup Folder | Execution Guardrails | Environmental Keying |
| 20 | | Identify Business Tempo | | Digital Certificates | | | | Scheduled Task | | Winlogon Helper DLL | | Security Support Provider | Exploitation for Defense Evasion | |
| 21 | | Identify Roles | | Exploits | | | | Systemd Timers | | XDG Autostart Entries | | Shortcut Modification | File and Directory Permissions | Linux and Mac File and Directory Permissions Modification |
| 22 | Phishing for Information | Spearphishing Attachment | | Malware | | | Serverless Execution | | Boot or Logon Initialization Scripts | Login Hook | | Time Providers | | Windows File and Directory Permissions Modification |
| 23 | | Spearphishing Link | Establish Accounts | Cloud Accounts | | | Shared Modules | | | Logon Script (Windows) | | Winlogon Helper DLL | Hide Artifacts | Email Hiding Rules |
| 24 | | Spearphishing Service | | Email Accounts | | | Software Deployment Tools | | | Network Logon Script | | XDG Autostart Entries | | Hidden File System |
| 25 | Search Closed Sources | Purchase Technical Data | | Social Media Accounts | | | System Services | Launchctl | | RC Scripts | Boot or Logon Initialization Scripts | Login Hook | | Hidden Files and Directories |
| 26 | | Threat Intel Vendors | Obtain Capabilities | Code Signing Certificates | | | | Service Execution | | Startup Items | | Logon Script (Windows) | | Hidden Users |
| 27 | Search Open Technical Databases | CDNs | | Digital Certificates | | | User Execution | Malicious File | Browser Extensions | | | Network Logon Script | | Hidden Window |
| 28 | | DNS/Passive DNS | | Exploits | | | | Malicious Image | Compromise Client Software Binary | | | RC Scripts | | NTFS File Attributes |
| 29 | | Digital Certificates | | Malware | | | | Malicious Link | Create Account | Cloud Account | | Startup Items | | Process Argument Spoofing |
| 30 | | Scan Databases | | Tool | | | Windows Management Instrumentation | | | Domain Account | Create or Modify System Process | Launch Agent | | Resource Forking |
| 31 | | WHOIS | | Vulnerabilities | | | | | | Local Account | | Launch Daemon | | Run Virtual Instance |
| 32 | Search Open Websites/Domains | Code Repositories | Stage Capabilities | Drive-by Target | | | | | Create or Modify System Process | Launch Agent | | Systemd Service | | VBA Stomping |
| 33 | | Search Engines | | Install Digital Certificate | | | | | | Launch Daemon | | Windows Service | Hijack Execution Flow | COR_PROFILER |
| 34 | | Social Media | | Link Target | | | | | | Systemd Service | Domain Policy Modification | Domain Trust Modification | | DLL Search Order Hijacking |
| 35 | Search Victim-Owned Websites | | | SEO Poisoning | | | | | | Windows Service | | Group Policy Modification | | DLL Side-Loading |
| 36 | | | | Upload Malware | | | | | Event Triggered Execution | Accessibility Features | Escape to Host | | | Dylib Hijacking |
| 37 | | | | Upload Tool | | | | | | AppCert DLLs | Event Triggered Execution | Accessibility Features | | Dynamic Linker Hijacking |
| 38 | | | | | | | | | | AppInit DLLs | | AppCert DLLs | | Executable Installer File Permissions Weakness |
| 39 | | | | | | | | | | Application Shimming | | AppInit DLLs | | KernelCallbackTable |
| 40 | | | | | | | | | | Change Default File Association | | Application Shimming | | Path Interception by PATH Environment Variable |
| 41 | | | | | | | | | | Component Object Model Hijacking | | Change Default File Association | | Path Interception by Search Order Hijacking |
| 42 | | | | | | | | | | Emond | | Component Object Model Hijacking | | Path Interception by Unquoted Path |
| 43 | | | | | | | | | | Image File Execution Options Injection | | Emond | | Services File Permissions Weakness |
| 44 | | | | | | | | | | Installer Packages | | Image File Execution Options Injection | | Services Registry Permissions Weakness |
| 45 | | | | | | | | | | LC_LOAD_DYLIB Addition | | Installer Packages | Impair Defenses | Disable Cloud Logs |
| 46 | | | | | | | | | | Netsh Helper DLL | | LC_LOAD_DYLIB Addition | | Disable Windows Event Logging |
| 47 | | | | | | | | | | PowerShell Profile | | Netsh Helper DLL | | Disable or Modify Cloud Firewall |
| 48 | | | | | | | | | | Screensaver | | PowerShell Profile | | Disable or Modify System Firewall |
| 49 | | | | | | | | | | Trap | | Screensaver | | Disable or Modify Tools |
| 50 | | | | | | | | | | Unix Shell Configuration Modification | | Trap | | Downgrade Attack |
| 51 | | | | | | | | | | Windows Management Instrumentation Event Subscription | | Unix Shell Configuration Modification | | Impair Command History Logging |
| 52 | | | | | | | | | External Remote Services | | | Windows Management Instrumentation Event Subscription | | Indicator Blocking |
| 53 | | | | | | | | | | COR_PROFILER | Exploitation for Privilege Escalation | | | Safe Mode Boot |
| 54 | | | | | | | | | | DLL Search Order Hijacking | | COR_PROFILER | | Clear Command History |
| 55 | | | | | | | | | | DLL Side-Loading | | DLL Search Order Hijacking | | Clear Linux or Mac System Logs |
| 56 | | | | | | | | | | Dylib Hijacking | | DLL Side-Loading | | Clear Mailbox Data |
| 57 | | | | | | | | | | Dynamic Linker Hijacking | | Dylib Hijacking | | Clear Network Connection History and Configurations |

https://attack.mitre.org/resources/working-with-attack/

## ATT&CK in STIX

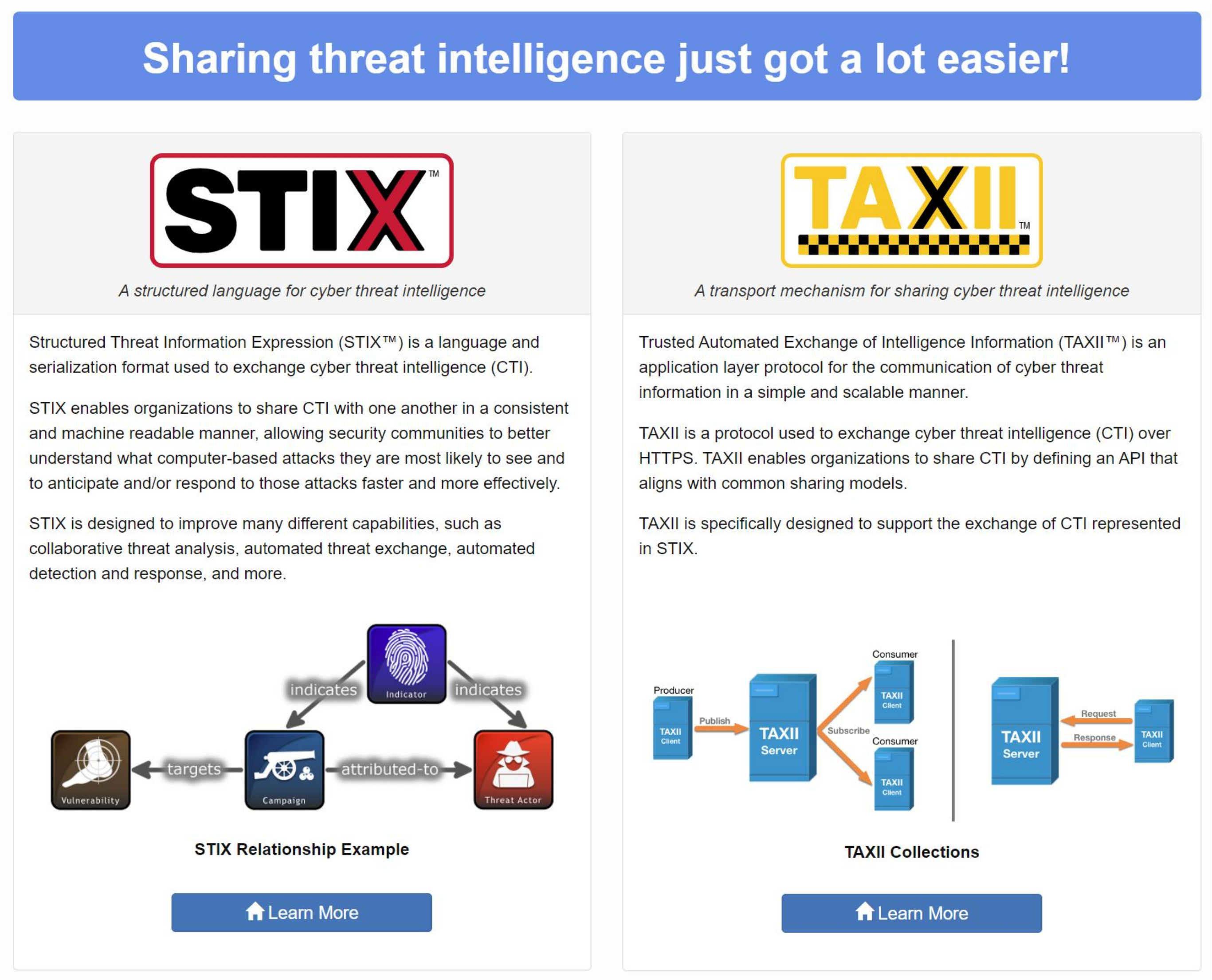


```
Type "help", "copyright", "credits" or "license" for more information.
>>> from stix2 import TAXIICollectionSource, Filter
>>> from taxii2client.v20 import Collection
>>>
>>> collection = Collection("https://cti-taxii.mitre.org/stix/collections/95ecc380-afe9-11e4-9b6c-751b66dd541e/")
>>> src = TAXIICollectionSource(collection)
>>>
>>> aws_techniques = src.query([
...     Filter("type", "=", "attack-pattern"),
...     Filter("x_mitre_platforms", "=", "AWS")
... ])
>>>
>>> print(",".join(map(lambda t: t["external_references"][0]["external_id"], aws_techniques)))
T1562.008,T1580,T1562.007,T1578.004,T1578.003,T1578.001,T1578.002,T1074.002,T1078.004,T1078.001,T1498.002,T1498.0
01,T1518.001,T1069.003,T1087.004,T1562,T1499.004,T1499.003,T1499.002,T1491.002,T1552.005,T1110.004,T1110.003,T111
0.001,T1552.001,T1552,T1136.003,T1098.001,T1518,T1535,T1525,T1538,T1530,T1578,T1537,T1526,T1499,T1498,T1496,T1491
,T1190,T1199,T1136,T1110,T1108,T1098,T1087,T1082,T1078,T1074,T1069,T1049,T1046
>>>
>>> t1580 = src.query([
...     Filter("external_references.external_id", "=", "T1580")
... ])[0]
>>>
>>> print(",".join(map(lambda kc: kc["phase_name"], t1580["kill_chain_phases"])))
discovery
>>>
>>> discovery = src.query([
...     Filter("type", "=", "x-mitre-tactic"),
...     Filter("x_mitre_shortname", "=", "discovery")
... ])[0]
>>>
>>> print(discovery["description"])
The adversary is trying to figure out your environment.

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. Th
ese techniques help adversaries observe the environment and orient themselves before deciding how to act. They al
so allow adversaries to explore what they can control and what's around their entry point in order to discover ho
w it could benefit their current objective. Native operating system tools are often used toward this post-comprom
ise information-gathering objective.
>>> 
```

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI). The ATT&CK dataset is available in STIX 2.0 and STIX 2.1.

# MITRE Tools & data

## ATT&CK in STIX



Sharing threat intelligence just got a lot easier!

STIX™

*A structured language for cyber threat intelligence*

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).

STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively.

STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

STIX Relationship Example

Learn More

TAXII™

*A transport mechanism for sharing cyber threat intelligence*

Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner.

TAXII is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models.

TAXII is specifically designed to support the exchange of CTI represented in STIX.

TAXII Collections

Learn More

*Source: https://oasis-open.github.io/cti-documentation/*

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

**CERT-US**

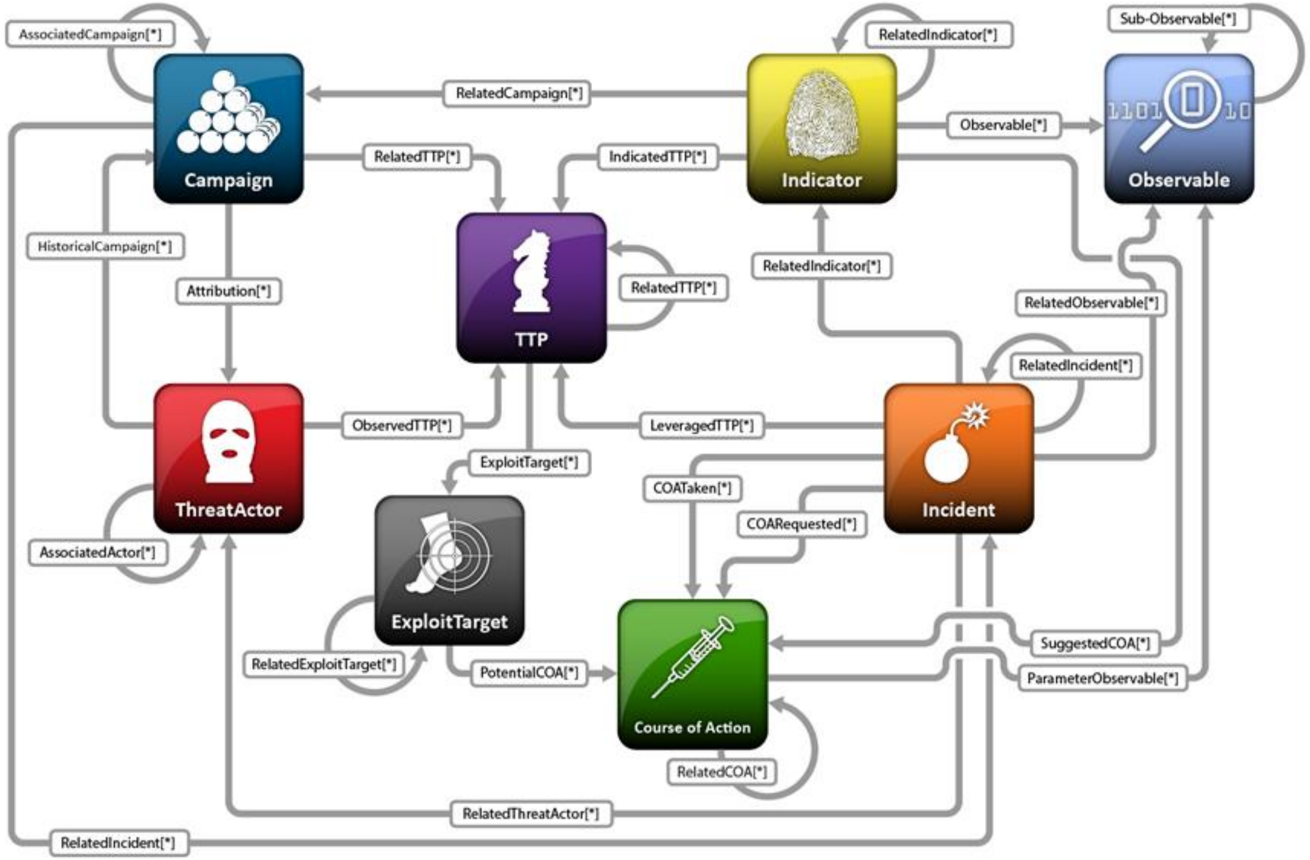
**(Department of Homeland Security)**

MITRE

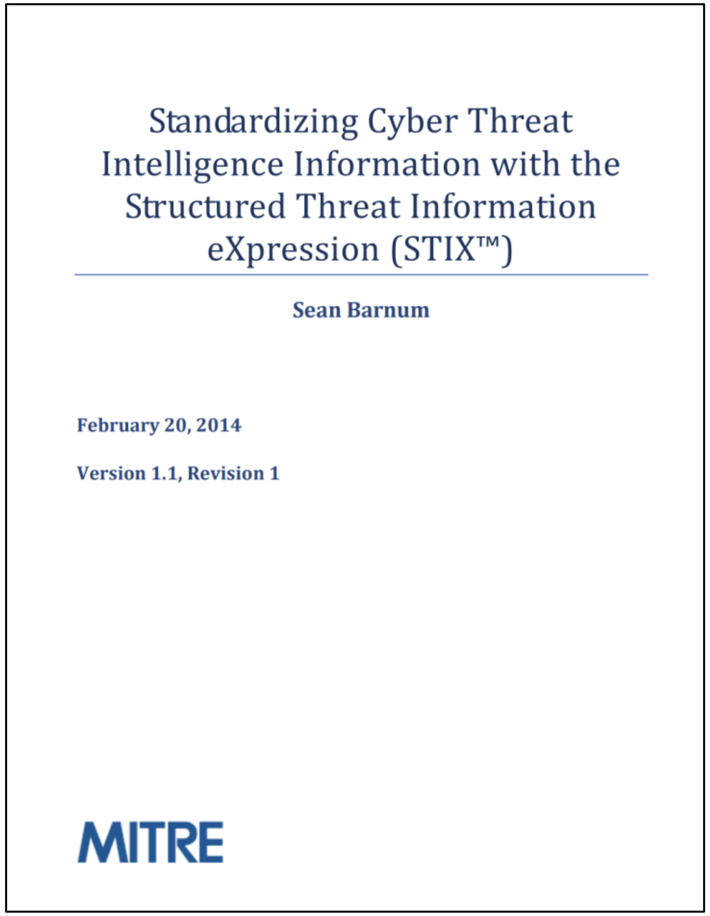
OASIS OPEN

# MITRE Tools & data

## ATT&CK in STIX



*Source: https://stixproject.github.io/about/*



Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)

**Sean Barnum**

**February 20, 2014**

**Version 1.1, Revision 1**

MITRE

https://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf

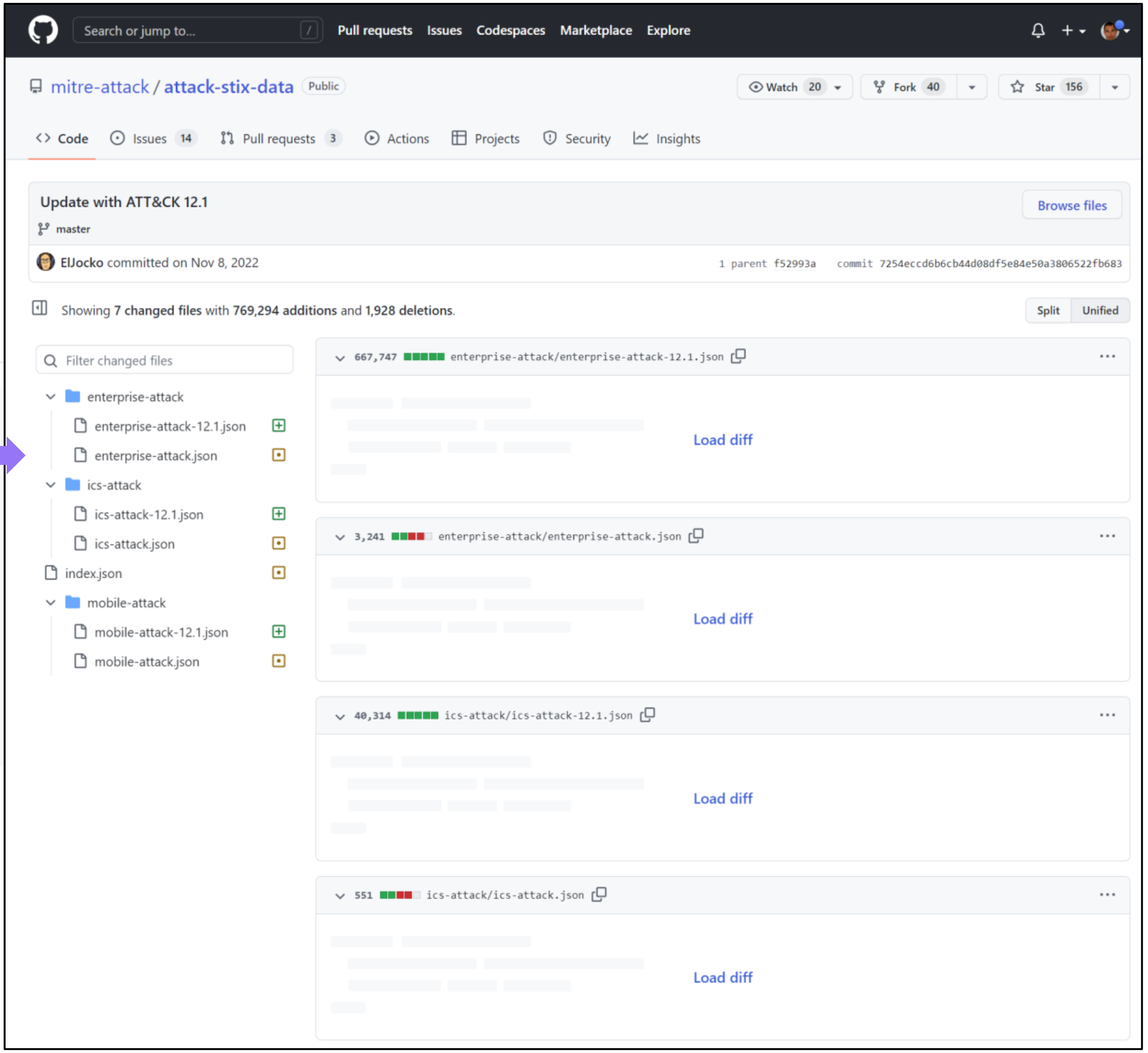
# MITRE Tools & data

## ATT&CK in STIX

### Repository Structure

```
.
├─ enterprise-attack ························ [1] Collection folder for Enterprise
│  ├─ enterprise-attack.json ·············· [2] Most recent Enterprise release
│  ├─ enterprise-attack-9.0.json ·········· [3] Enterprise ATT&CK v9.0 collection
│  └─ [other releases of Enterprise ATT&CK]
├─ mobile-attack
│  └─ [Mobile ATT&CK releases]
├─ ics-attack
│  └─ [ATT&CK for ICS releases]
├─ index.json ····························· [4] Collection index JSON
└─ index.md ······························· [5] Collection index markdown
```

https://github.com/mitre-attack/attack-stix-data



mitre-attack / attack-stix-data Public

Update with ATT&CK 12.1

master

ElJocko committed on Nov 8, 2022    1 parent f52993a    commit 7254eccd6b6cb44d08df5e84e50a3806522fb683

Showing 7 changed files with 769,294 additions and 1,928 deletions.

- enterprise-attack
  - enterprise-attack-12.1.json
  - enterprise-attack.json
- ics-attack
  - ics-attack-12.1.json
  - ics-attack.json
- index.json
- mobile-attack
  - mobile-attack-12.1.json
  - mobile-attack.json

667,747 enterprise-attack/enterprise-attack-12.1.json

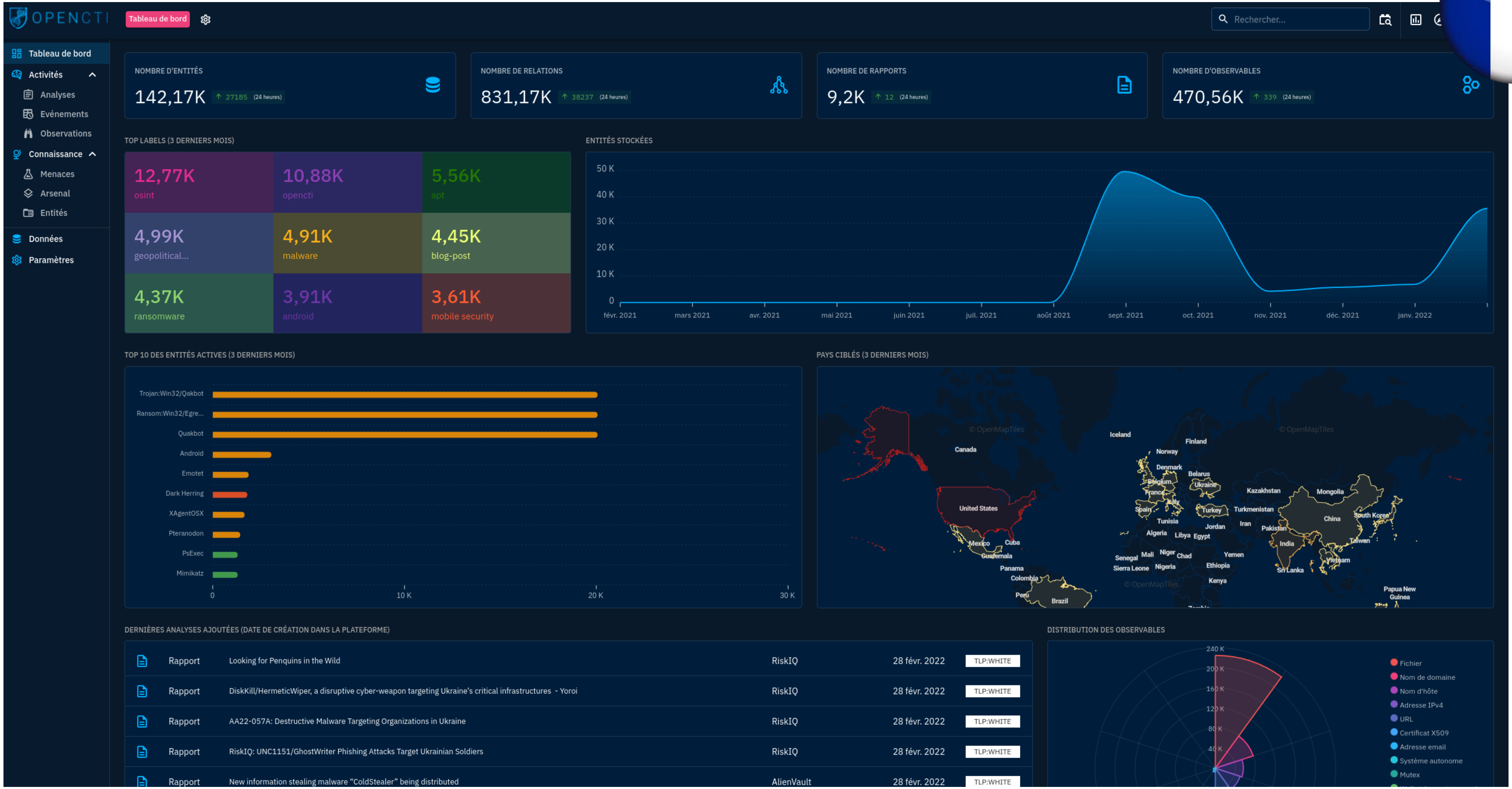
3,241 enterprise-attack/enterprise-attack.json

40,314 ics-attack/ics-attack-12.1.json

551 ics-attack/ics-attack.json

# MITRE Tools & data

## ATT&CK in STIX - OpenCTI



NOMBRE D'ENTITÉS 142,17K ↑ 27185 (24 heures)

NOMBRE DE RELATIONS 831,17K ↑ 38237 (24 heures)

NOMBRE DE RAPPORTS 9,2K ↑ 12 (24 heures)

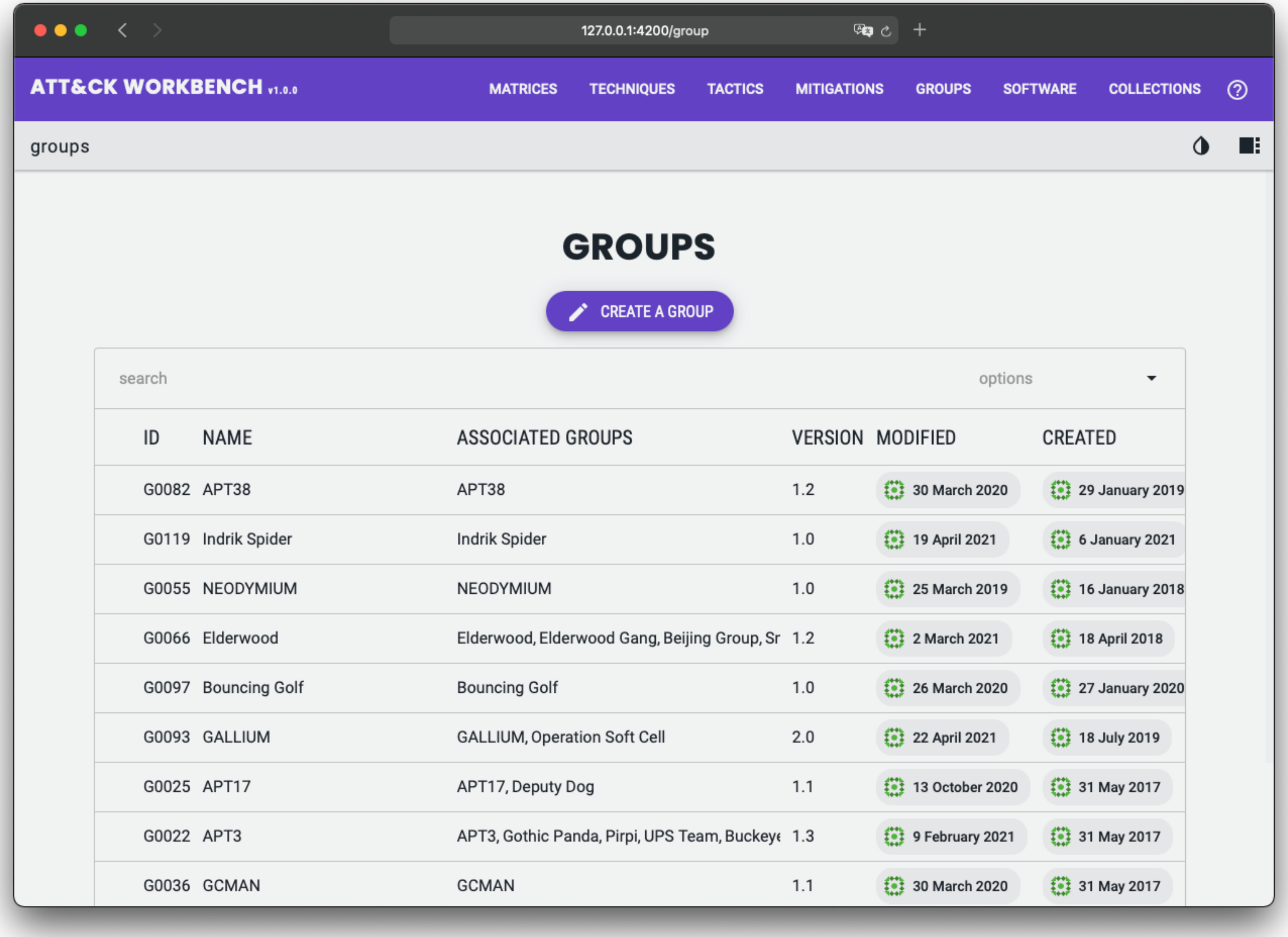
NOMBRE D'OBSERVABLES 470,56K ↑ 339 (24 heures)

DERNIÈRES ANALYSES AJOUTÉES (DATE DE CRÉATION DANS LA PLATEFORME)

| | | | | |
|---|---|---|---|---|
| Rapport | Looking for Penquins in the Wild | RiskIQ | 28 févr. 2022 | TLP:WHITE |
| Rapport | DiskKill/HermeticWiper, a disruptive cyber-weapon targeting Ukraine's critical infrastructures - Yoroi | RiskIQ | 28 févr. 2022 | TLP:WHITE |
| Rapport | AA22-057A: Destructive Malware Targeting Organizations in Ukraine | RiskIQ | 28 févr. 2022 | TLP:WHITE |
| Rapport | RiskIQ: UNC1151/GhostWriter Phishing Attacks Target Ukrainian Soldiers | RiskIQ | 28 févr. 2022 | TLP:WHITE |
| Rapport | New information stealing malware "ColdStealer" being distributed | AlienVault | 28 févr. 2022 | TLP:WHITE |

*Source: https://github.com/OpenCTI-Platform/opencti*

## ATT&CK Workbench



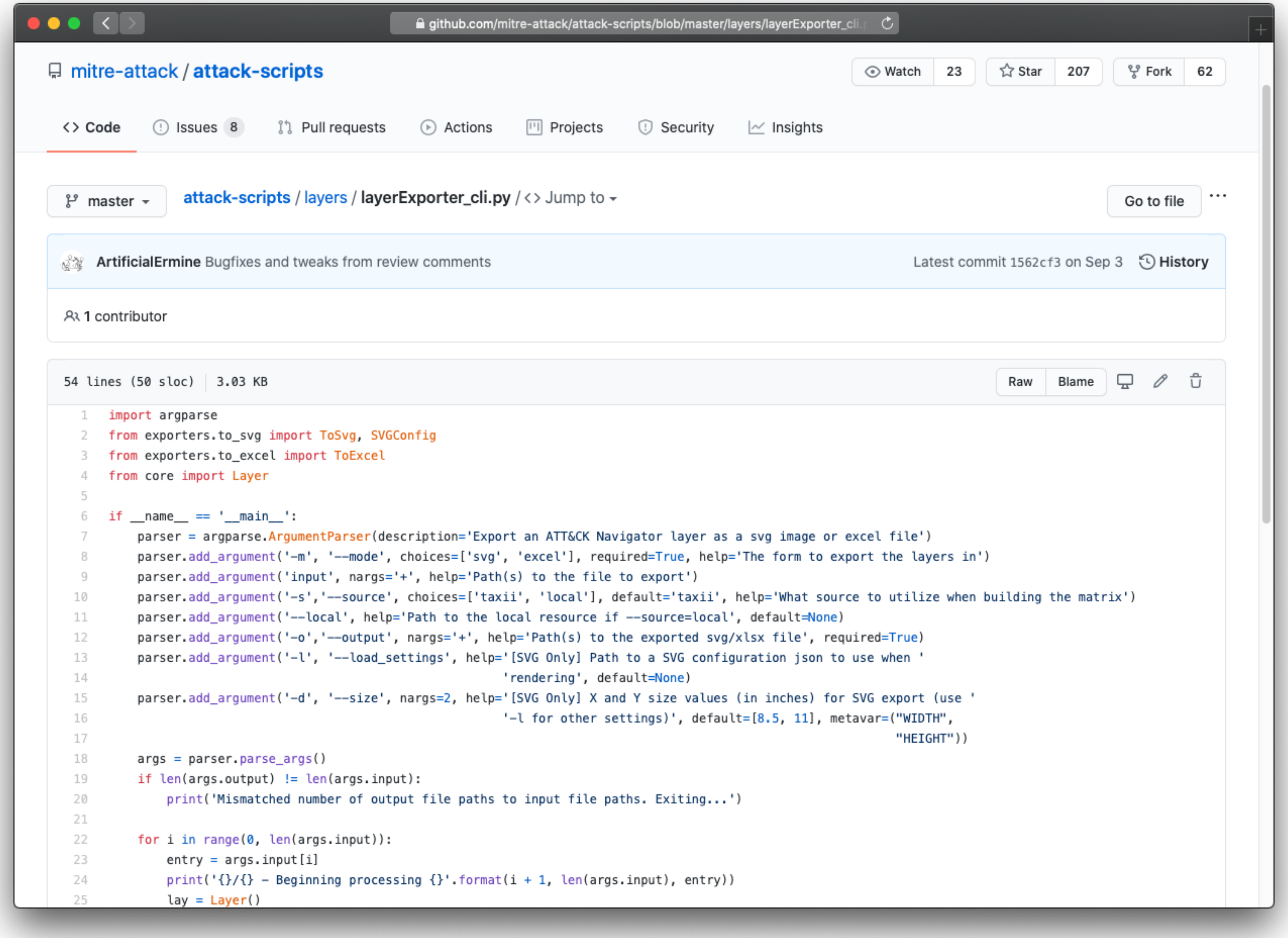
GROUPS

| ID | NAME | ASSOCIATED GROUPS | VERSION | MODIFIED | CREATED |
|---|---|---|---|---|---|
| G0082 | APT38 | APT38 | 1.2 | 30 March 2020 | 29 January 2019 |
| G0119 | Indrik Spider | Indrik Spider | 1.0 | 19 April 2021 | 6 January 2021 |
| G0055 | NEODYMIUM | NEODYMIUM | 1.0 | 25 March 2019 | 16 January 2018 |
| G0066 | Elderwood | Elderwood, Elderwood Gang, Beijing Group, Sr | 1.2 | 2 March 2021 | 18 April 2018 |
| G0097 | Bouncing Golf | Bouncing Golf | 1.0 | 26 March 2020 | 27 January 2020 |
| G0093 | GALLIUM | GALLIUM, Operation Soft Cell | 2.0 | 22 April 2021 | 18 July 2019 |
| G0025 | APT17 | APT17, Deputy Dog | 1.1 | 13 October 2020 | 31 May 2017 |
| G0022 | APT3 | APT3, Gothic Panda, Pirpi, UPS Team, Buckeye | 1.3 | 9 February 2021 | 31 May 2017 |
| G0036 | GCMAN | GCMAN | 1.1 | 30 March 2020 | 31 May 2017 |

The ATT&CK Workbench is an application allowing users to explore, create, annotate, and share extensions of the ATT&CK knowledge base.

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

## ATT&CK Python Utilities

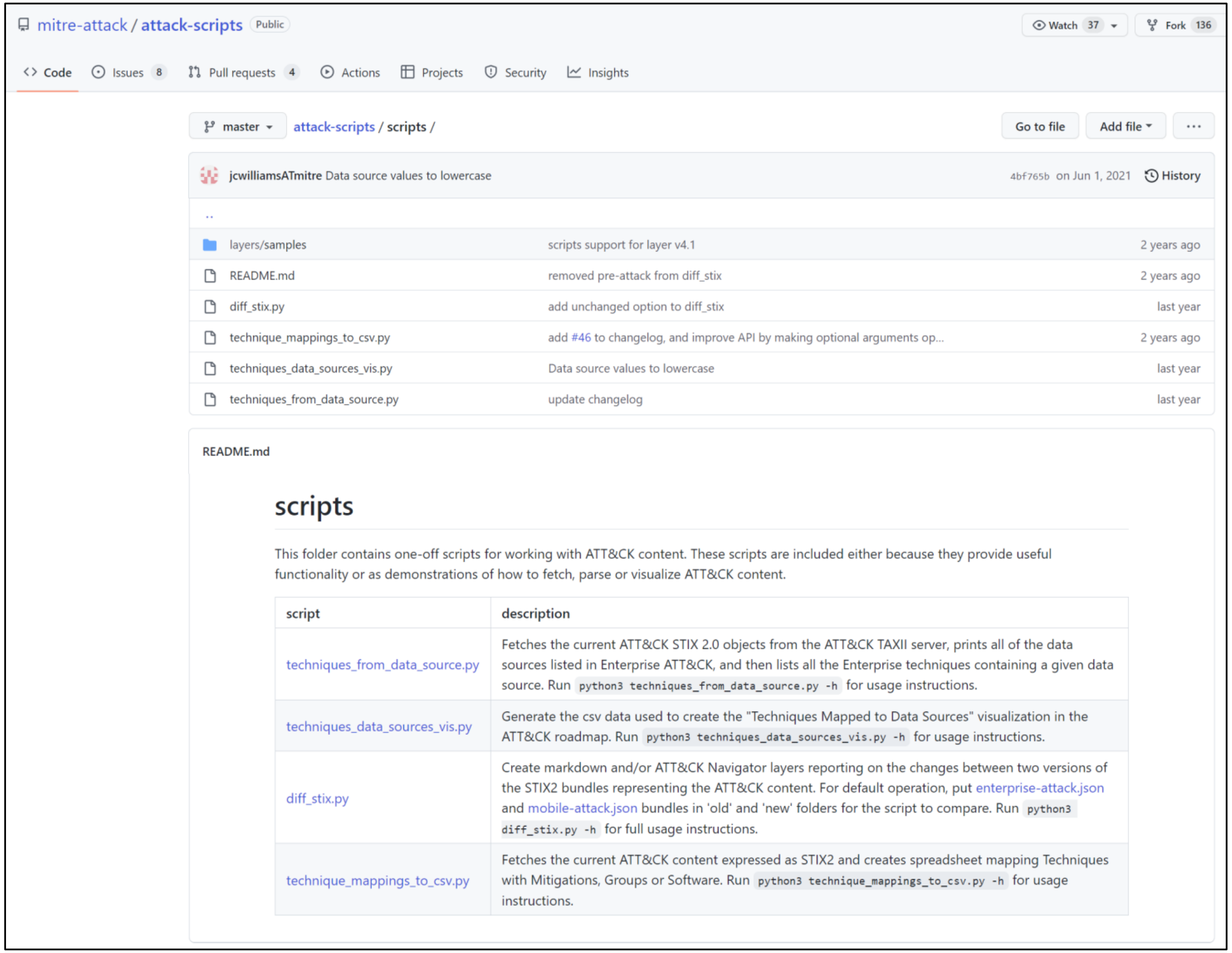

github.com/mitre-attack/attack-scripts/blob/master/layers/layerExporter_cli.
mitre-attack / attack-scripts
Watch 23
Star 207
Fork 62
Code
Issues 8
Pull requests
Actions
Projects
Security
Insights
master
attack-scripts / layers / layerExporter_cli.py / <> Jump to
Go to file
ArtificialErmine Bugfixes and tweaks from review comments
Latest commit 1562cf3 on Sep 3
History
1 contributor
54 lines (50 sloc) | 3.03 KB
Raw
Blame

```python
import argparse
from exporters.to_svg import ToSvg, SVGConfig
from exporters.to_excel import ToExcel
from core import Layer

if __name__ == '__main__':
    parser = argparse.ArgumentParser(description='Export an ATT&CK Navigator layer as a svg image or excel file')
    parser.add_argument('-m', '--mode', choices=['svg', 'excel'], required=True, help='The form to export the layers in')
    parser.add_argument('input', nargs='+', help='Path(s) to the file to export')
    parser.add_argument('-s','--source', choices=['taxii', 'local'], default='taxii', help='What source to utilize when building the matrix')
    parser.add_argument('--local', help='Path to the local resource if --source=local', default=None)
    parser.add_argument('-o','--output', nargs='+', help='Path(s) to the exported svg/xlsx file', required=True)
    parser.add_argument('-l', '--load_settings', help='[SVG Only] Path to a SVG configuration json to use when '
                                                      'rendering', default=None)
    parser.add_argument('-d', '--size', nargs=2, help='[SVG Only] X and Y size values (in inches) for SVG export (use '
                                                      '-l for other settings)', default=[8.5, 11], metavar=("WIDTH",
                                                                                                            "HEIGHT"))

    args = parser.parse_args()
    if len(args.output) != len(args.input):
        print('Mismatched number of output file paths to input file paths. Exiting...')

    for i in range(0, len(args.input)):
        entry = args.input[i]
        print('{}/{} - Beginning processing {}'.format(i + 1, len(args.input), entry))
        lay = Layer()
```

ATT&CK provides a variety of Python tools for accessing, querying, and processing the ATT&CK dataset. These scripts can be useful utilities or serve as examples for how to work with ATT&CK programmatically.

# MITRE Tools & data

## ATT&CK Python Utilities



jcwilliamsATmitre Data source values to lowercase 4bf765b on Jun 1, 2021

| | | |
|---|---|---|
| .. | | |
| layers/samples | scripts support for layer v4.1 | 2 years ago |
| README.md | removed pre-attack from diff_stix | 2 years ago |
| diff_stix.py | add unchanged option to diff_stix | last year |
| technique_mappings_to_csv.py | add #46 to changelog, and improve API by making optional arguments op... | 2 years ago |
| techniques_data_sources_vis.py | Data source values to lowercase | last year |
| techniques_from_data_source.py | update changelog | last year |

README.md

### scripts

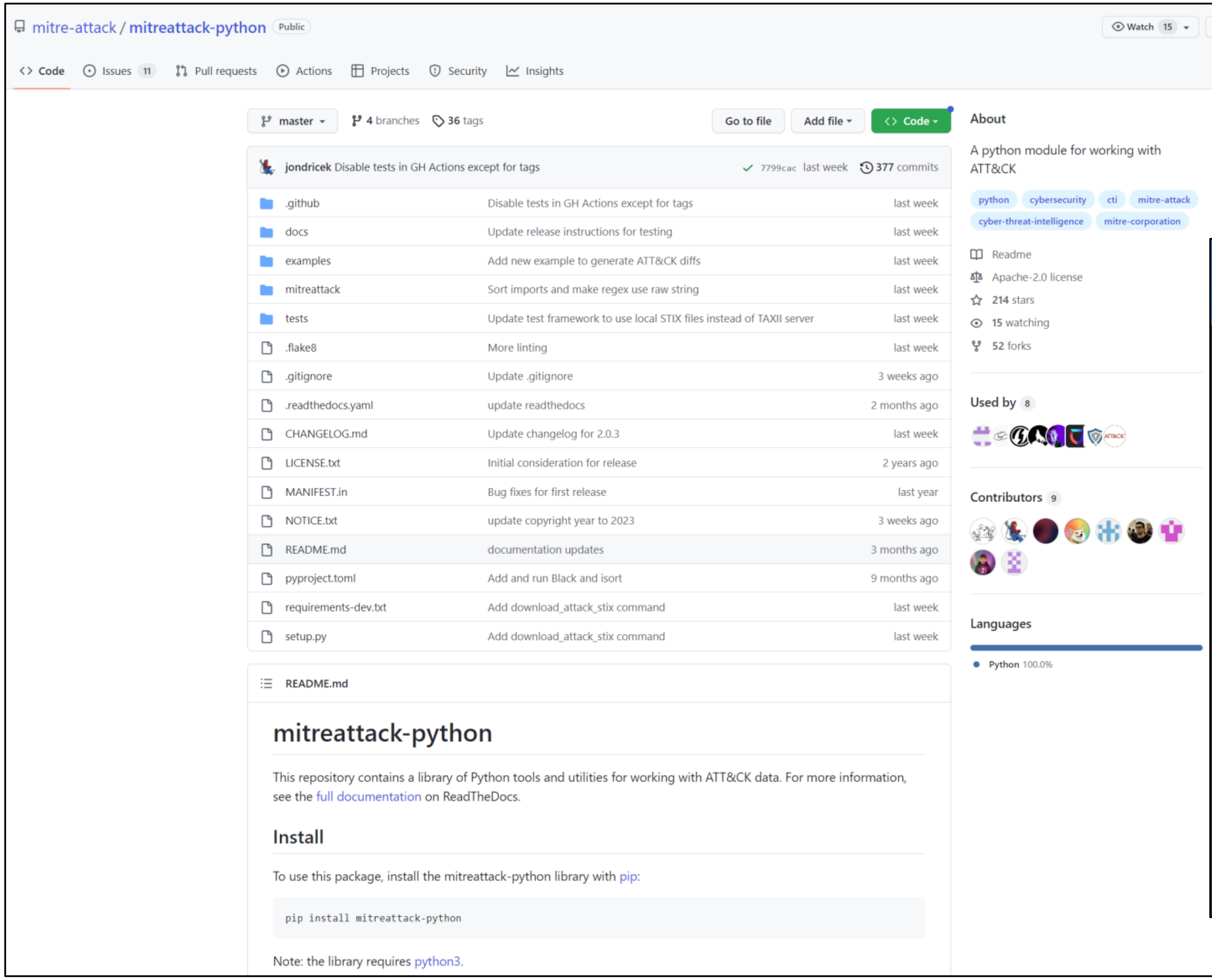
This folder contains one-off scripts for working with ATT&CK content. These scripts are included either because they provide useful functionality or as demonstrations of how to fetch, parse or visualize ATT&CK content.

| script | description |
|---|---|
| techniques_from_data_source.py | Fetches the current ATT&CK STIX 2.0 objects from the ATT&CK TAXII server, prints all of the data sources listed in Enterprise ATT&CK, and then lists all the Enterprise techniques containing a given data source. Run `python3 techniques_from_data_source.py -h` for usage instructions. |
| techniques_data_sources_vis.py | Generate the csv data used to create the "Techniques Mapped to Data Sources" visualization in the ATT&CK roadmap. Run `python3 techniques_data_sources_vis.py -h` for usage instructions. |
| diff_stix.py | Create markdown and/or ATT&CK Navigator layers reporting on the changes between two versions of the STIX2 bundles representing the ATT&CK content. For default operation, put enterprise-attack.json and mobile-attack.json bundles in 'old' and 'new' folders for the script to compare. Run `python3 diff_stix.py -h` for full usage instructions. |
| technique_mappings_to_csv.py | Fetches the current ATT&CK content expressed as STIX2 and creates spreadsheet mapping Techniques with Mitigations, Groups or Software. Run `python3 technique_mappings_to_csv.py -h` for usage instructions. |

https://github.com/mitre-attack/attack-scripts/tree/master/scripts

This project seems to be slow, no regular updates

## ATT&CK Python Utilities



jondricek Disable tests in GH Actions except for tags ✓ 7799cac last week 377 commits

| | | |
|---|---|---|
| .github | Disable tests in GH Actions except for tags | last week |
| docs | Update release instructions for testing | last week |
| examples | Add new example to generate ATT&CK diffs | last week |
| mitreattack | Sort imports and make regex use raw string | last week |
| tests | Update test framework to use local STIX files instead of TAXII server | last week |
| .flake8 | More linting | last week |
| .gitignore | Update .gitignore | 3 weeks ago |
| .readthedocs.yaml | update readthedocs | 2 months ago |
| CHANGELOG.md | Update changelog for 2.0.3 | last week |
| LICENSE.txt | Initial consideration for release | 2 years ago |
| MANIFEST.in | Bug fixes for first release | last year |
| NOTICE.txt | update copyright year to 2023 | 3 weeks ago |
| README.md | documentation updates | 3 months ago |
| pyproject.toml | Add and run Black and isort | 9 months ago |
| requirements-dev.txt | Add download_attack_stix command | last week |
| setup.py | Add download_attack_stix command | last week |

About

A python module for working with ATT&CK

python · cybersecurity · cti · mitre-attack · cyber-threat-intelligence · mitre-corporation

Readme

Apache-2.0 license

214 stars

15 watching

52 forks

Used by 8

Contributors 9

Languages

Python 100.0%

README.md

# mitreattack-python

This repository contains a library of Python tools and utilities for working with ATT&CK data. For more information, see the full documentation on ReadTheDocs.

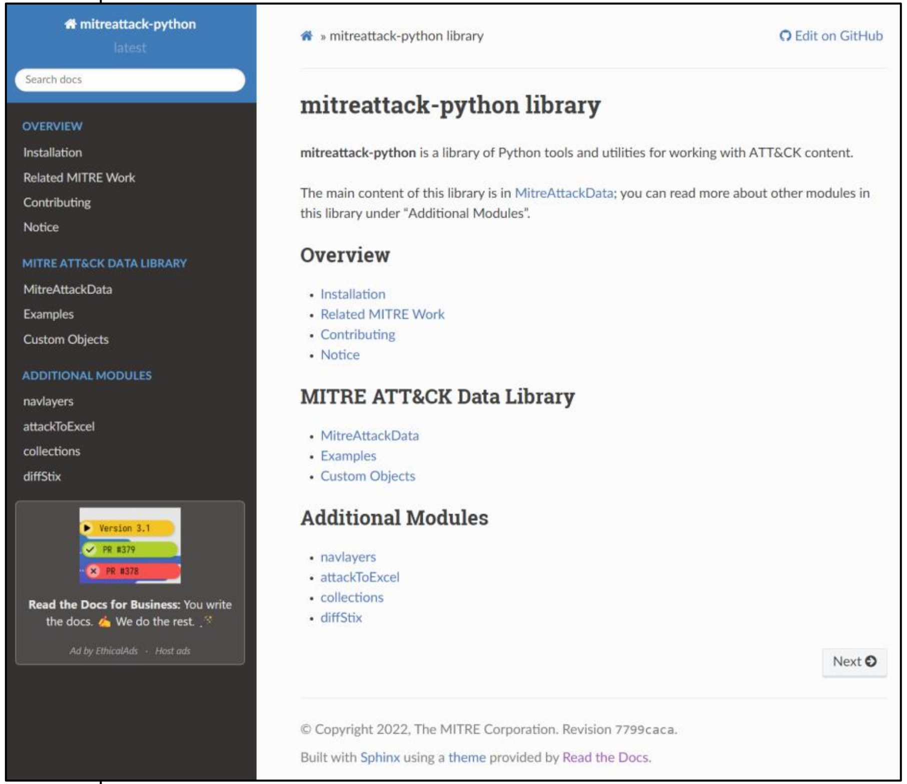
## Install

To use this package, install the mitreattack-python library with pip:

```
pip install mitreattack-python
```

Note: the library requires python3.

https://github.com/mitre-attack/mitreattack-python



# mitreattack-python library

**mitreattack-python** is a library of Python tools and utilities for working with ATT&CK content.

The main content of this library is in MitreAttackData; you can read more about other modules in this library under "Additional Modules".

## Overview

- Installation
- Related MITRE Work
- Contributing
- Notice

## MITRE ATT&CK Data Library

- MitreAttackData
- Examples
- Custom Objects

## Additional Modules

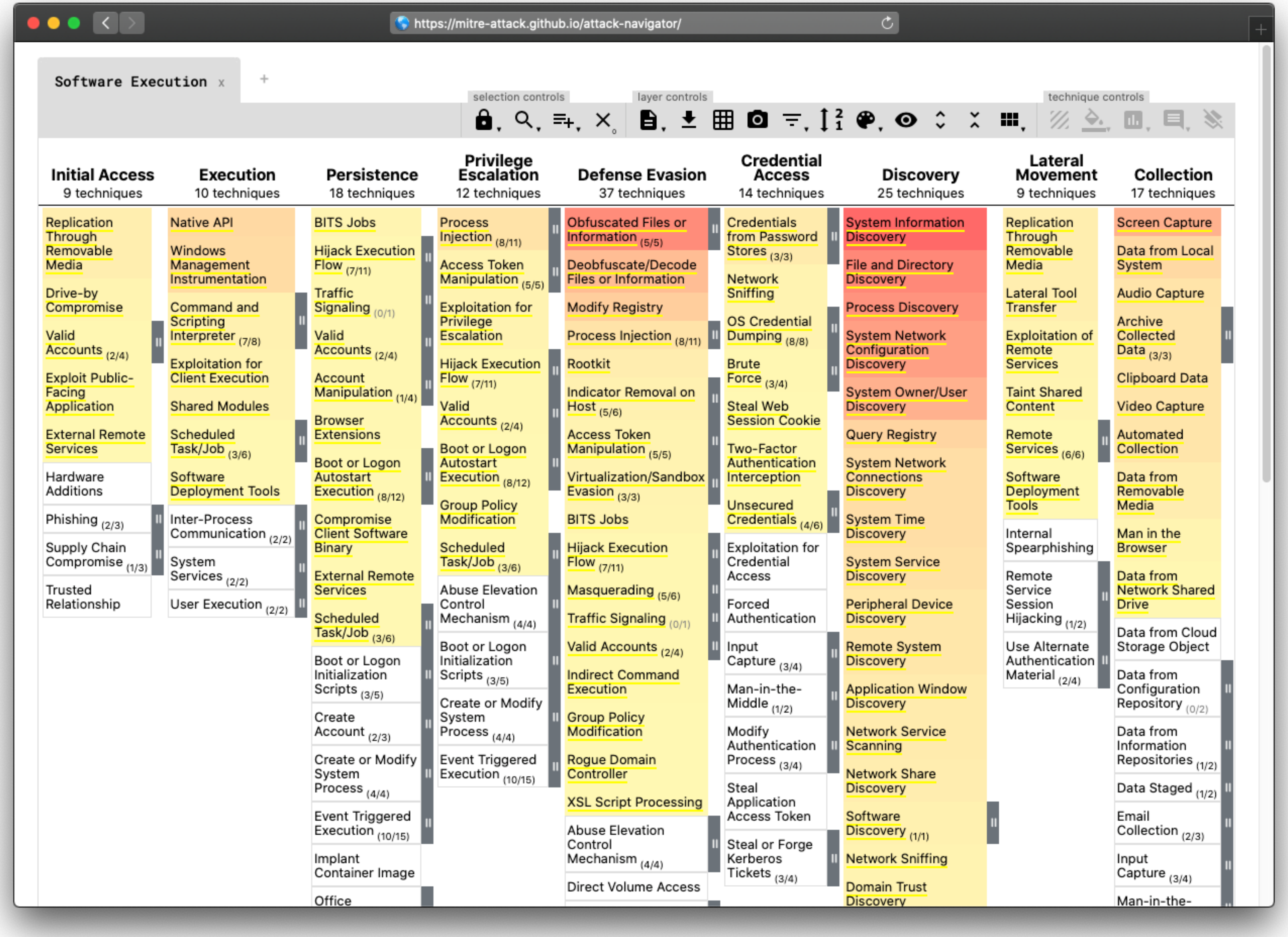
- navlayers
- attackToExcel
- collections
- diffStix

© Copyright 2022, The MITRE Corporation. Revision 7799caca.

Built with Sphinx using a theme provided by Read the Docs.

https://mitreattack-python.readthedocs.io/en/latest/

## ATT&CK Navigator



| Initial Access<br>9 techniques | Execution<br>10 techniques | Persistence<br>18 techniques | Privilege Escalation<br>12 techniques | Defense Evasion<br>37 techniques | Credential Access<br>14 techniques | Discovery<br>25 techniques | Lateral Movement<br>9 techniques | Collection<br>17 techniques |
|---|---|---|---|---|---|---|---|---|
| Replication Through Removable Media | Native API | BITS Jobs | Process Injection (8/11) | Obfuscated Files or Information (5/5) | Credentials from Password Stores (3/3) | System Information Discovery | Replication Through Removable Media | Screen Capture |
| Drive-by Compromise | Windows Management Instrumentation | Hijack Execution Flow (7/11) | Access Token Manipulation (5/5) | Deobfuscate/Decode Files or Information | Network Sniffing | File and Directory Discovery | Lateral Tool Transfer | Data from Local System |
| Valid Accounts (2/4) | Command and Scripting Interpreter (7/8) | Traffic Signaling (0/1) | Exploitation for Privilege Escalation | Modify Registry | OS Credential Dumping (8/8) | Process Discovery | Exploitation of Remote Services | Audio Capture |
| Exploit Public-Facing Application | Exploitation for Client Execution | Valid Accounts (2/4) | Hijack Execution Flow (7/11) | Process Injection (8/11) | Brute Force (3/4) | System Network Configuration Discovery | Taint Shared Content | Archive Collected Data (3/3) |
| External Remote Services | Shared Modules | Account Manipulation (1/4) | Valid Accounts (2/4) | Rootkit | Steal Web Session Cookie | System Owner/User Discovery | Remote Services (6/6) | Clipboard Data |
| Hardware Additions | Scheduled Task/Job (3/6) | Browser Extensions | Boot or Logon Autostart Execution (8/12) | Indicator Removal on Host (5/6) | Two-Factor Authentication Interception | Query Registry | Software Deployment Tools | Video Capture |
| Phishing (2/3) | Software Deployment Tools | Boot or Logon Autostart Execution (8/12) | Group Policy Modification | Access Token Manipulation (5/5) | Unsecured Credentials (4/6) | System Network Connections Discovery | Internal Spearphishing | Automated Collection |
| Supply Chain Compromise (1/3) | Inter-Process Communication (2/2) | Compromise Client Software Binary | Scheduled Task/Job (3/6) | Virtualization/Sandbox Evasion (3/3) | Exploitation for Credential Access | System Time Discovery | Remote Service Session Hijacking (1/2) | Data from Removable Media |
| Trusted Relationship | System Services (2/2) | External Remote Services | Abuse Elevation Control Mechanism (4/4) | BITS Jobs | Forced Authentication | System Service Discovery | Use Alternate Authentication Material (2/4) | Man in the Browser |
| | User Execution (2/2) | Scheduled Task/Job (3/6) | Boot or Logon Initialization Scripts (3/5) | Hijack Execution Flow (7/11) | Input Capture (3/4) | Peripheral Device Discovery | | Data from Network Shared Drive |
| | | Boot or Logon Initialization Scripts (3/5) | Create or Modify System Process (4/4) | Masquerading (5/6) | Man-in-the-Middle (1/2) | Remote System Discovery | | Data from Cloud Storage Object |
| | | Create Account (2/3) | Event Triggered Execution (10/15) | Traffic Signaling (0/1) | Modify Authentication Process (3/4) | Application Window Discovery | | Data from Configuration Repository (0/2) |
| | | Create or Modify System Process (4/4) | | Valid Accounts (2/4) | Steal Application Access Token | Network Service Scanning | | Data from Information Repositories (1/2) |
| | | Event Triggered Execution (10/15) | | Indirect Command Execution | Steal or Forge Kerberos Tickets (3/4) | Network Share Discovery | | Data Staged (1/2) |
| | | Implant Container Image | | Group Policy Modification | | Software Discovery (1/1) | | Email Collection (2/3) |
| | | Office | | Rogue Domain Controller | | Network Sniffing | | Input Capture (3/4) |
| | | | | XSL Script Processing | | Domain Trust Discovery | | Man-in-the- |
| | | | | Abuse Elevation Control Mechanism (4/4) | | | | |
| | | | | Direct Volume Access | | | | |

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

## MITRE Tools & data

### ATT&CK Navigator

Run it locally

(https://github.com/mitre-attack/attack-navigator/)

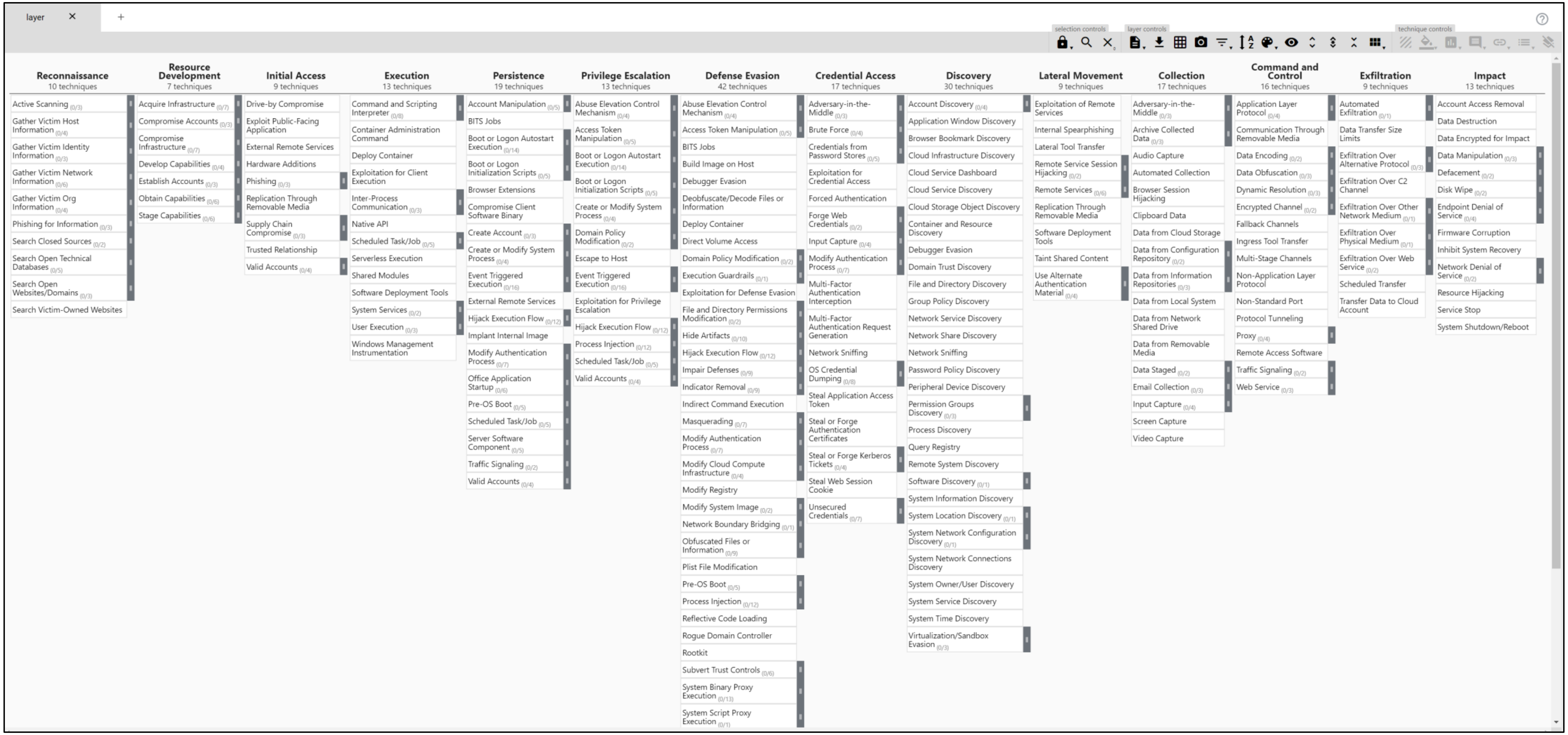
OR

Use the ATT&CK Navigator online App

(https://mitre-attack.github.io/attack-navigator/)

# MITRE Tools & data

## ATT&CK Navigator



**Reconnaissance**
10 techniques

- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Victim-Owned Websites

**Resource Development**
7 techniques

- Acquire Infrastructure (0/7)
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/6)

**Initial Access**
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

**Execution**
13 techniques

- Command and Scripting Interpreter (0/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/3)
- Windows Management Instrumentation

**Persistence**
19 techniques

- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/16)
- External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (0/7)
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/5)
- Server Software Component (0/5)
- Traffic Signaling (0/2)
- Valid Accounts (0/4)

**Privilege Escalation**
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- Valid Accounts (0/4)

**Defense Evasion**
42 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/10)
- Hijack Execution Flow (0/12)
- Impair Defenses (0/9)
- Indicator Removal (0/9)
- Indirect Command Execution
- Masquerading (0/7)
- Modify Authentication Process (0/7)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (0/9)
- Plist File Modification
- Pre-OS Boot (0/5)
- Process Injection (0/12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls (0/6)
- System Binary Proxy Execution (0/13)
- System Script Proxy Execution (0/1)

**Credential Access**
17 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/7)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Unsecured Credentials (0/7)

**Discovery**
30 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery (0/1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (0/3)

**Lateral Movement**
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

**Collection**
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Screen Capture
- Video Capture

**Command and Control**
16 techniques

- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/2)
- Web Service (0/3)

**Exfiltration**
9 techniques

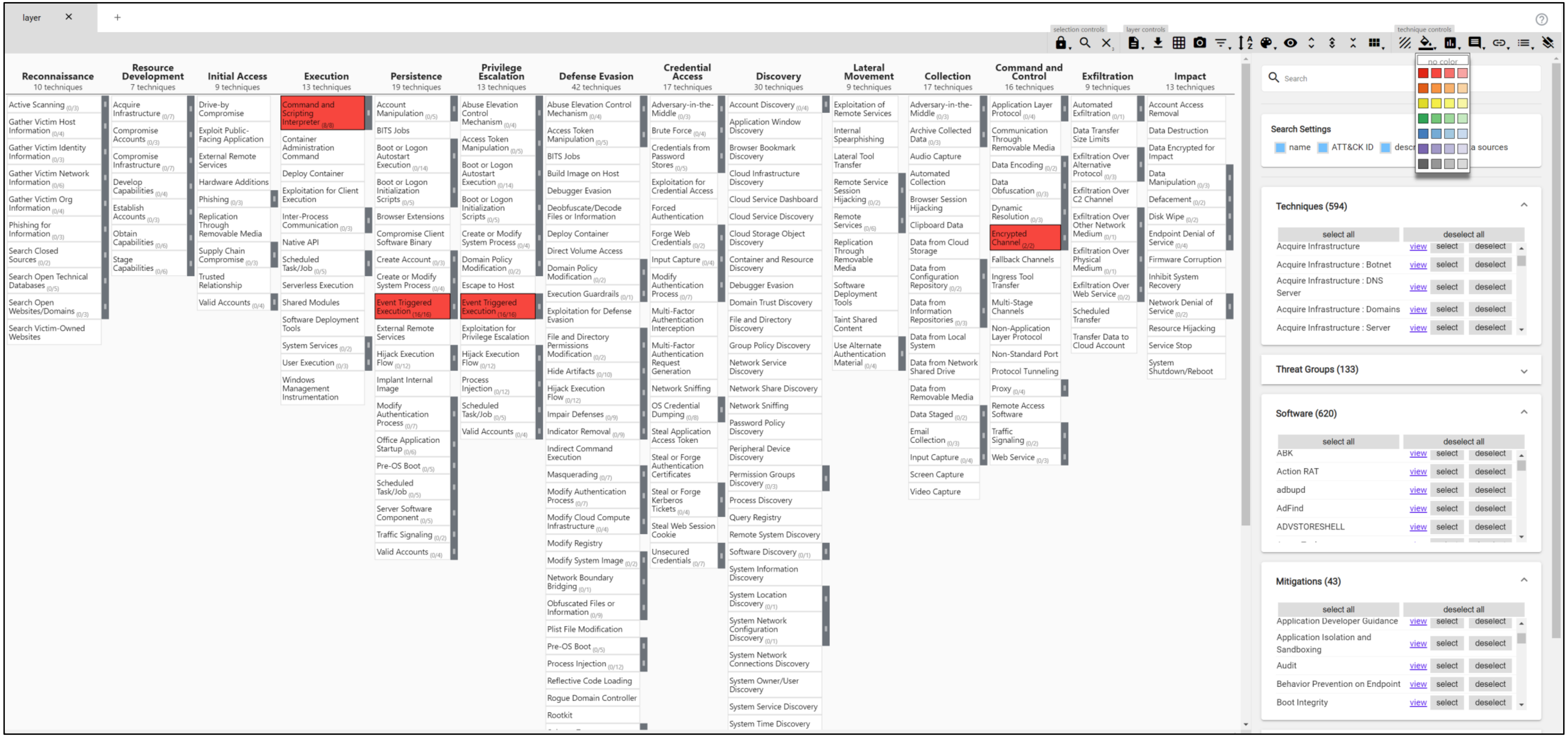
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

**Impact**
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

# MITRE Tools & data

## ATT&CK Navigator



**Reconnaissance** 10 techniques
- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Victim-Owned Websites

**Resource Development** 7 techniques
- Acquire Infrastructure (0/7)
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/6)

**Initial Access** 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

**Execution** 13 techniques
- Command and Scripting Interpreter (8/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/3)
- Windows Management Instrumentation

**Persistence** 19 techniques
- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (16/16)
- External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (0/7)
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/5)
- Server Software Component (0/5)
- Traffic Signaling (0/2)
- Valid Accounts (0/4)

**Privilege Escalation** 13 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (16/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- Valid Accounts (0/4)

**Defense Evasion** 42 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/10)
- Hijack Execution Flow (0/12)
- Impair Defenses (0/9)
- Indicator Removal (0/9)
- Indirect Command Execution
- Masquerading (0/7)
- Modify Authentication Process (0/7)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (0/9)
- Plist File Modification
- Pre-OS Boot (0/5)
- Process Injection (0/12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit

**Credential Access** 17 techniques
- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/7)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Unsecured Credentials (0/7)

**Discovery** 30 techniques
- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery (0/1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery

**Lateral Movement** 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

**Collection** 17 techniques
- Adversary-in-the-Middle (0/3)
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Screen Capture
- Video Capture

**Command and Control** 16 techniques
- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (2/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/2)
- Web Service (0/3)

**Exfiltration** 9 techniques
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

**Impact** 13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Search

**Search Settings**
☑ name ☑ ATT&CK ID ☑ descr... ...a sources

**Techniques (594)**

select all | deselect all
- Acquire Infrastructure view select deselect
- Acquire Infrastructure : Botnet view select deselect
- Acquire Infrastructure : DNS Server view select deselect
- Acquire Infrastructure : Domains view select deselect
- Acquire Infrastructure : Server view select deselect

**Threat Groups (133)**

**Software (620)**

select all | deselect all
- ABK view select deselect
- Action RAT view select deselect
- adbupd view select deselect
- AdFind view select deselect
- ADVSTORESHELL view select deselect

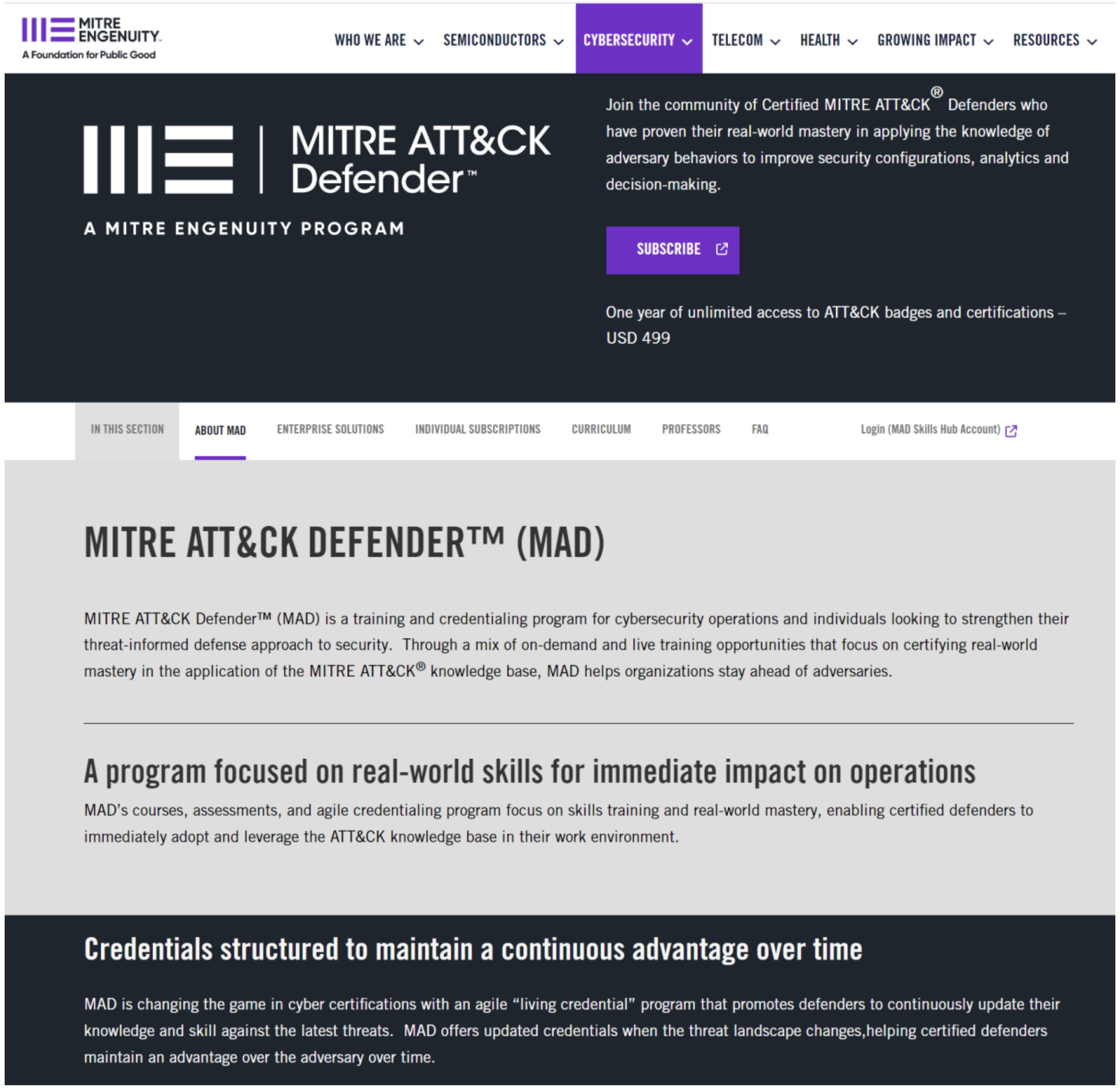
**Mitigations (43)**

select all | deselect all
- Application Developer Guidance view select deselect
- Application Isolation and Sandboxing view select deselect
- Audit view select deselect
- Behavior Prevention on Endpoint view select deselect
- Boot Integrity view select deselect

# _06_

# MITRE ATT&CK Training

## MITRE ATT&CK Defender



Join the community of Certified MITRE ATT&CK® Defenders who have proven their real-world mastery in applying the knowledge of adversary behaviors to improve security configurations, analytics and decision-making.

One year of unlimited access to ATT&CK badges and certifications – USD 499

### MITRE ATT&CK DEFENDER™ (MAD)

MITRE ATT&CK Defender™ (MAD) is a training and credentialing program for cybersecurity operations and individuals looking to strengthen their threat-informed defense approach to security. Through a mix of on-demand and live training opportunities that focus on certifying real-world mastery in the application of the MITRE ATT&CK® knowledge base, MAD helps organizations stay ahead of adversaries.

### A program focused on real-world skills for immediate impact on operations

MAD's courses, assessments, and agile credentialing program focus on skills training and real-world mastery, enabling certified defenders to immediately adopt and leverage the ATT&CK knowledge base in their work environment.

### Credentials structured to maintain a continuous advantage over time

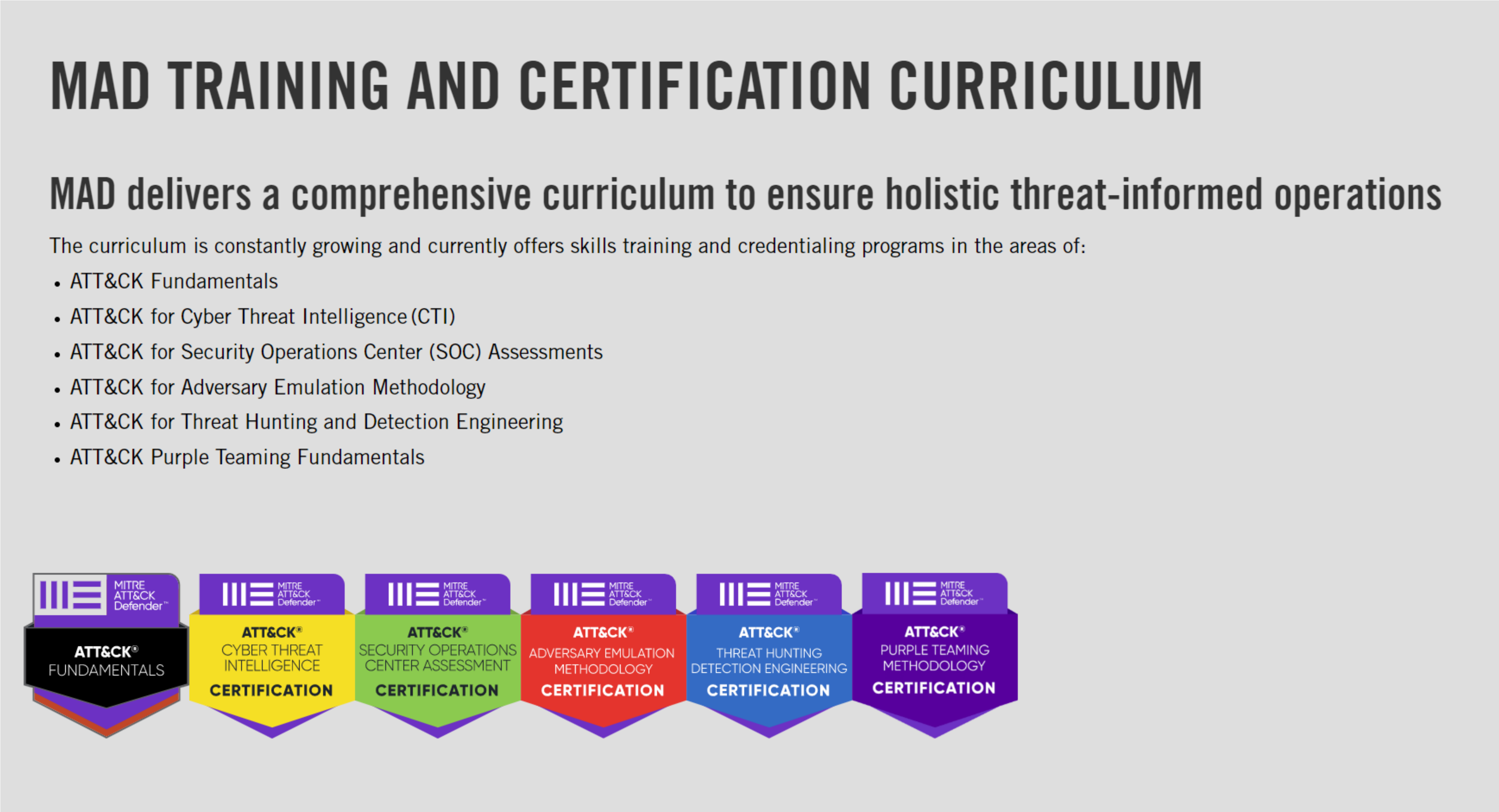
MAD is changing the game in cyber certifications with an agile "living credential" program that promotes defenders to continuously update their knowledge and skill against the latest threats. MAD offers updated credentials when the threat landscape changes,helping certified defenders maintain an advantage over the adversary over time.

https://mitre-engenuity.org/cybersecurity/mad/

MITRE ATT&CK Defender™ (MAD) is a training and credentialing program for cybersecurity operations and individuals looking to strengthen their threat-informed defense approach to security. Through a mix of on-demand and live training opportunities that focus on certifying real-world mastery in the application of the MITRE ATT&CK® knowledge base, MAD helps organizations stay ahead of adversaries.

Comprendre et améliorer sa sécurité grâce à MITRE ATT&CK

## MITRE ATT&CK Defender



# MAD TRAINING AND CERTIFICATION CURRICULUM

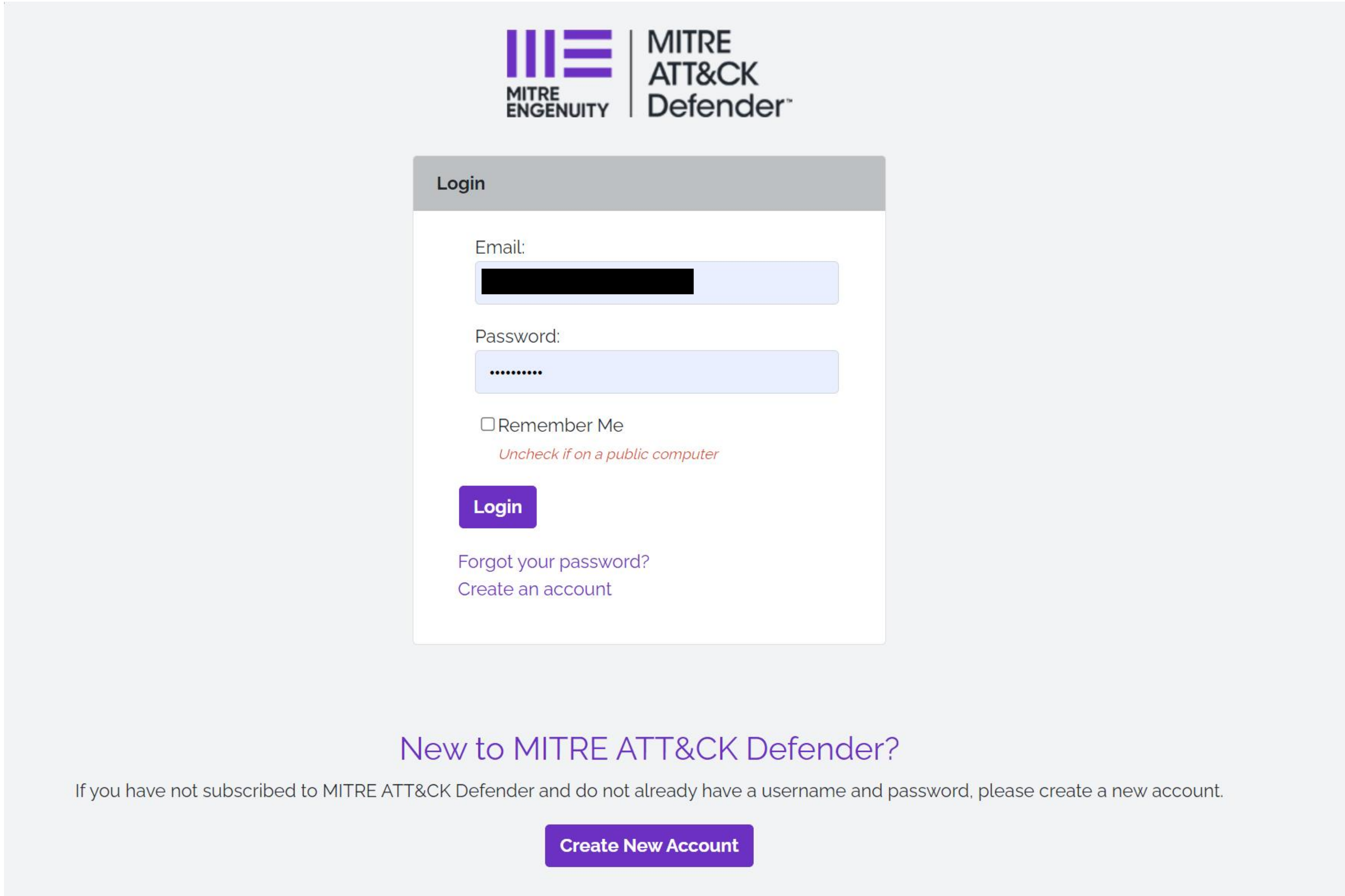
## MAD delivers a comprehensive curriculum to ensure holistic threat-informed operations

The curriculum is constantly growing and currently offers skills training and credentialing programs in the areas of:

- ATT&CK Fundamentals
- ATT&CK for Cyber Threat Intelligence (CTI)
- ATT&CK for Security Operations Center (SOC) Assessments
- ATT&CK for Adversary Emulation Methodology
- ATT&CK for Threat Hunting and Detection Engineering
- ATT&CK Purple Teaming Fundamentals

MITRE ATT&CK Defender™
ATT&CK® FUNDAMENTALS
MITRE ATT&CK Defender™
ATT&CK® CYBER THREAT INTELLIGENCE CERTIFICATION
MITRE ATT&CK Defender™
ATT&CK® SECURITY OPERATIONS CENTER ASSESSMENT CERTIFICATION
MITRE ATT&CK Defender™
ATT&CK® ADVERSARY EMULATION METHODOLOGY CERTIFICATION
MITRE ATT&CK Defender™
ATT&CK® THREAT HUNTING DETECTION ENGINEERING CERTIFICATION
MITRE ATT&CK Defender™
ATT&CK® PURPLE TEAMING METHODOLOGY CERTIFICATION

## MITRE ATT&CK Defender



Login

Email:

[redacted]

Password:

••••••••••

□ Remember Me

*Uncheck if on a public computer*

Forgot your password?

Create an account

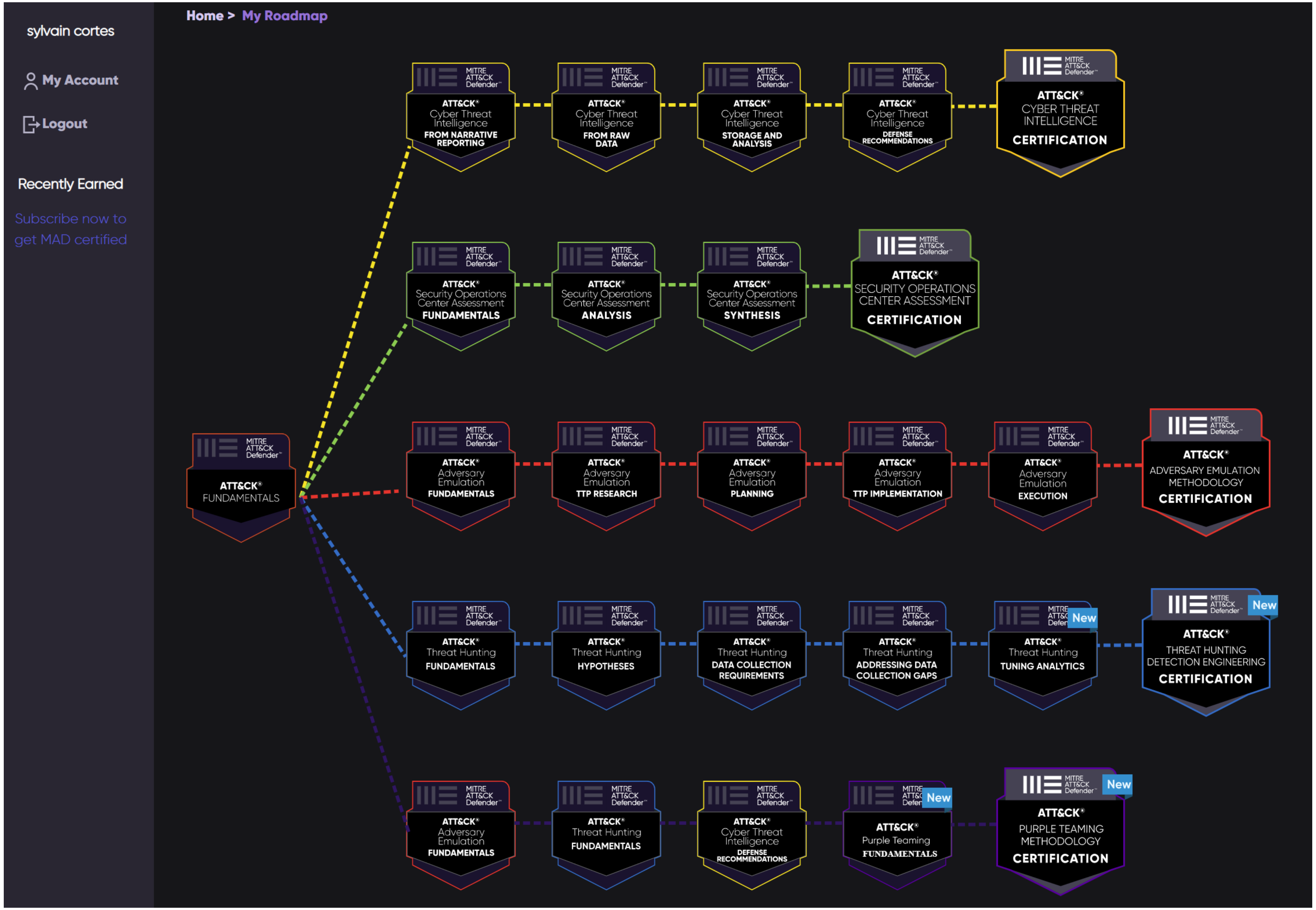
New to MITRE ATT&CK Defender?

If you have not subscribed to MITRE ATT&CK Defender and do not already have a username and password, please create a new account.

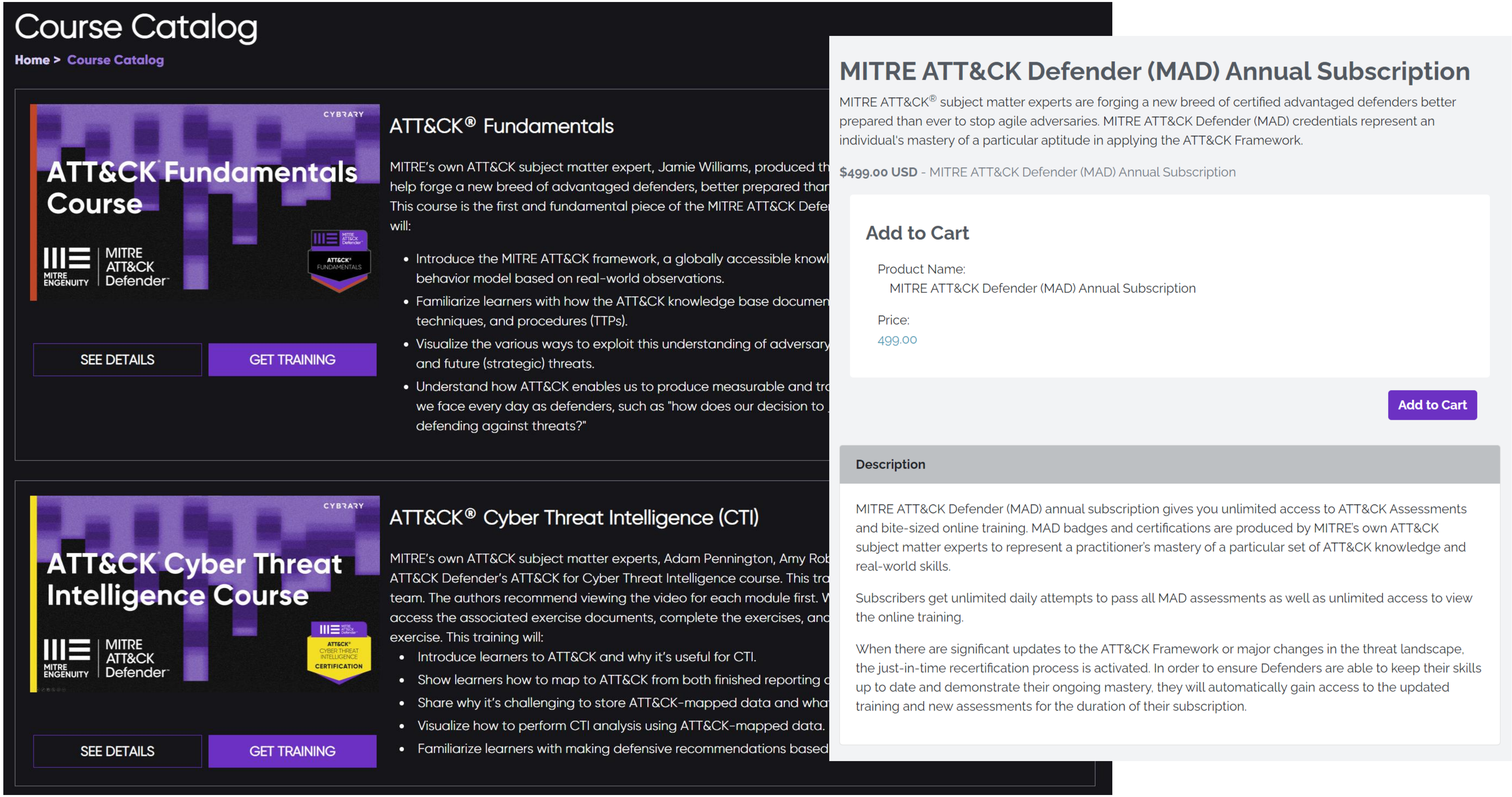
https://mad.mitre-engenuity.org/

Comprendre et améliorer sa sécurité grâce à MITRE ATT&CK

## MITRE ATT&CK Defender


sylvain cortes
My Account
Logout
Recently Earned
Subscribe now to get MAD certified
Home > My Roadmap
ATT&CK® FUNDAMENTALS
ATT&CK® Cyber Threat Intelligence FROM NARRATIVE REPORTING
ATT&CK® Cyber Threat Intelligence FROM RAW DATA
ATT&CK® Cyber Threat Intelligence STORAGE AND ANALYSIS
ATT&CK® Cyber Threat Intelligence DEFENSE RECOMMENDATIONS
ATT&CK® CYBER THREAT INTELLIGENCE CERTIFICATION
ATT&CK® Security Operations Center Assessment FUNDAMENTALS
ATT&CK® Security Operations Center Assessment ANALYSIS
ATT&CK® Security Operations Center Assessment SYNTHESIS
ATT&CK® SECURITY OPERATIONS CENTER ASSESSMENT CERTIFICATION
ATT&CK® Adversary Emulation FUNDAMENTALS
ATT&CK® Adversary Emulation TTP RESEARCH
ATT&CK® Adversary Emulation PLANNING
ATT&CK® Adversary Emulation TTP IMPLEMENTATION
ATT&CK® Adversary Emulation EXECUTION
ATT&CK® ADVERSARY EMULATION METHODOLOGY CERTIFICATION
ATT&CK® Threat Hunting FUNDAMENTALS
ATT&CK® Threat Hunting HYPOTHESES
ATT&CK® Threat Hunting DATA COLLECTION REQUIREMENTS
ATT&CK® Threat Hunting ADDRESSING DATA COLLECTION GAPS
New ATT&CK® Threat Hunting TUNING ANALYTICS
New ATT&CK® THREAT HUNTING DETECTION ENGINEERING CERTIFICATION
ATT&CK® Adversary Emulation FUNDAMENTALS
ATT&CK® Threat Hunting FUNDAMENTALS
ATT&CK® Cyber Threat Intelligence DEFENSE RECOMMENDATIONS
New ATT&CK® Purple Teaming FUNDAMENTALS
New ATT&CK® PURPLE TEAMING METHODOLOGY CERTIFICATION

## MITRE ATT&CK Defender



# Course Catalog

Home > Course Catalog

### ATT&CK® Fundamentals

MITRE's own ATT&CK subject matter expert, Jamie Williams, produced th
help forge a new breed of advantaged defenders, better prepared thar
This course is the first and fundamental piece of the MITRE ATT&CK Defe
will:

- Introduce the MITRE ATT&CK framework, a globally accessible knowl behavior model based on real-world observations.
- Familiarize learners with how the ATT&CK knowledge base documen techniques, and procedures (TTPs).
- Visualize the various ways to exploit this understanding of adversary and future (strategic) threats.
- Understand how ATT&CK enables us to produce measurable and tra we face every day as defenders, such as "how does our decision to defending against threats?"

CYBRARY
ATT&CK Cyber Threat Intelligence Course
MITRE ENGENUITY
MITRE ATT&CK Defender
ATT&CK CYBER THREAT INTELLIGENCE CERTIFICATION
SEE DETAILS
GET TRAINING

### ATT&CK® Cyber Threat Intelligence (CTI)

MITRE's own ATT&CK subject matter experts, Adam Pennington, Amy Rob
ATT&CK Defender's ATT&CK for Cyber Threat Intelligence course. This tra
team. The authors recommend viewing the video for each module first. W
access the associated exercise documents, complete the exercises, and
exercise. This training will:

- Introduce learners to ATT&CK and why it's useful for CTI.
- Show learners how to map to ATT&CK from both finished reporting a
- Share why it's challenging to store ATT&CK-mapped data and wha
- Visualize how to perform CTI analysis using ATT&CK-mapped data.
- Familiarize learners with making defensive recommendations based

## MITRE ATT&CK Defender (MAD) Annual Subscription

MITRE ATT&CK® subject matter experts are forging a new breed of certified advantaged defenders better prepared than ever to stop agile adversaries. MITRE ATT&CK Defender (MAD) credentials represent an individual's mastery of a particular aptitude in applying the ATT&CK Framework.

**$499.00 USD** - MITRE ATT&CK Defender (MAD) Annual Subscription

### Add to Cart

Product Name:
MITRE ATT&CK Defender (MAD) Annual Subscription

Price:
499.00

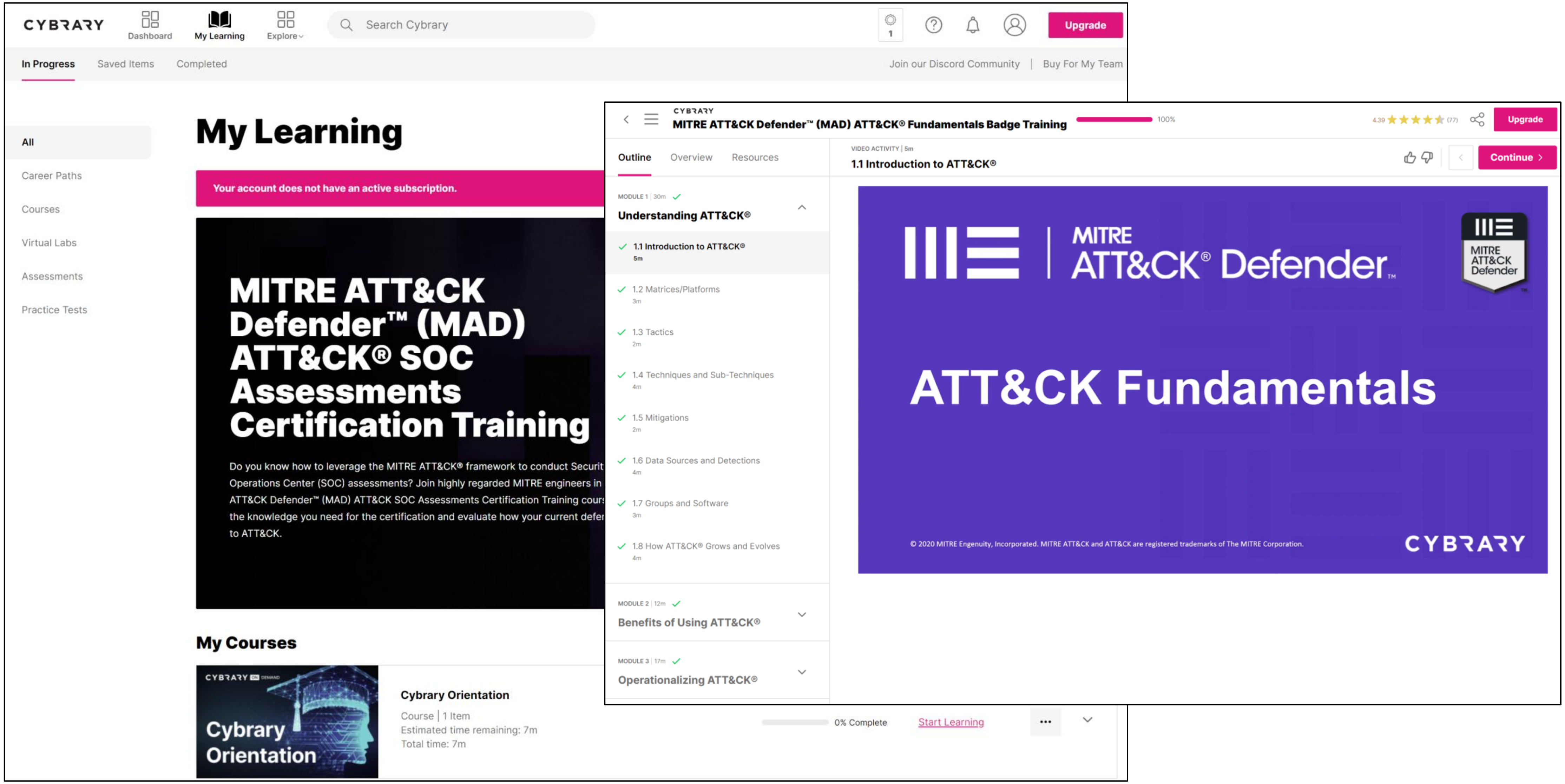
**Description**

MITRE ATT&CK Defender (MAD) annual subscription gives you unlimited access to ATT&CK Assessments and bite-sized online training. MAD badges and certifications are produced by MITRE's own ATT&CK subject matter experts to represent a practitioner's mastery of a particular set of ATT&CK knowledge and real-world skills.

Subscribers get unlimited daily attempts to pass all MAD assessments as well as unlimited access to view the online training.

When there are significant updates to the ATT&CK Framework or major changes in the threat landscape, the just-in-time recertification process is activated. In order to ensure Defenders are able to keep their skills up to date and demonstrate their ongoing mastery, they will automatically gain access to the updated training and new assessments for the duration of their subscription.

## MITRE ATT&CK Defender



# My Learning

Your account does not have an active subscription.

**MITRE ATT&CK Defender™ (MAD) ATT&CK® SOC Assessments Certification Training**

Do you know how to leverage the MITRE ATT&CK® framework to conduct Securit Operations Center (SOC) assessments? Join highly regarded MITRE engineers in ATT&CK Defender™ (MAD) ATT&CK SOC Assessments Certification Training cours the knowledge you need for the certification and evaluate how your current defer to ATT&CK.

**My Courses**

Cybrary Orientation

Cybrary Orientation

Course | 1 Item
Estimated time remaining: 7m
Total time: 7m

**MITRE ATT&CK Defender™ (MAD) ATT&CK® Fundamentals Badge Training**

VIDEO ACTIVITY | 5m

1.1 Introduction to ATT&CK®

MODULE 1 | 30m ✓

**Understanding ATT&CK®**

- ✓ 1.1 Introduction to ATT&CK® 5m
- ✓ 1.2 Matrices/Platforms 3m
- ✓ 1.3 Tactics 2m
- ✓ 1.4 Techniques and Sub-Techniques 4m
- ✓ 1.5 Mitigations 2m
- ✓ 1.6 Data Sources and Detections 4m
- ✓ 1.7 Groups and Software 3m
- ✓ 1.8 How ATT&CK® Grows and Evolves 4m

MODULE 2 | 12m ✓

**Benefits of Using ATT&CK®**

MODULE 3 | 17m ✓

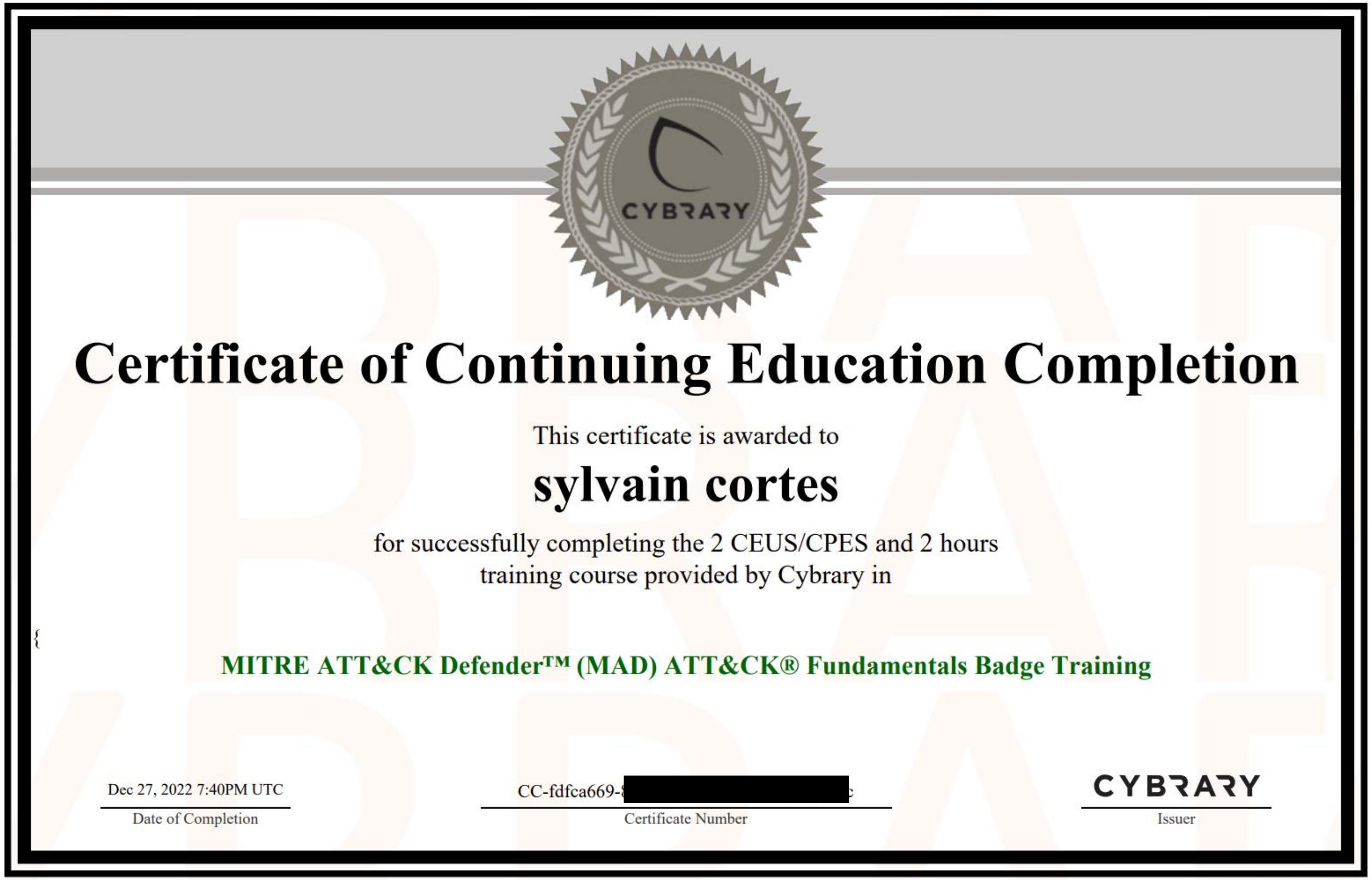
**Operationalizing ATT&CK®**

ATT&CK Fundamentals

© 2020 MITRE Engenuity, Incorporated. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

https://app.cybrary.it/my-learning

## MITRE ATT&CK Defender



CYBRARY

# Certificate of Continuing Education Completion

This certificate is awarded to

**sylvain cortes**

for successfully completing the 2 CEUS/CPES and 2 hours training course provided by Cybrary in

{

**MITRE ATT&CK Defender™ (MAD) ATT&CK® Fundamentals Badge Training**

| | | |
|---|---|---|
| Dec 27, 2022 7:40PM UTC | CC-fdfca669-[redacted] | CYBRARY |
| Date of Completion | Certificate Number | Issuer |

# _07_

# What’s next?

# The best conclusion about MITRE ATT&CK you could imagine 😊

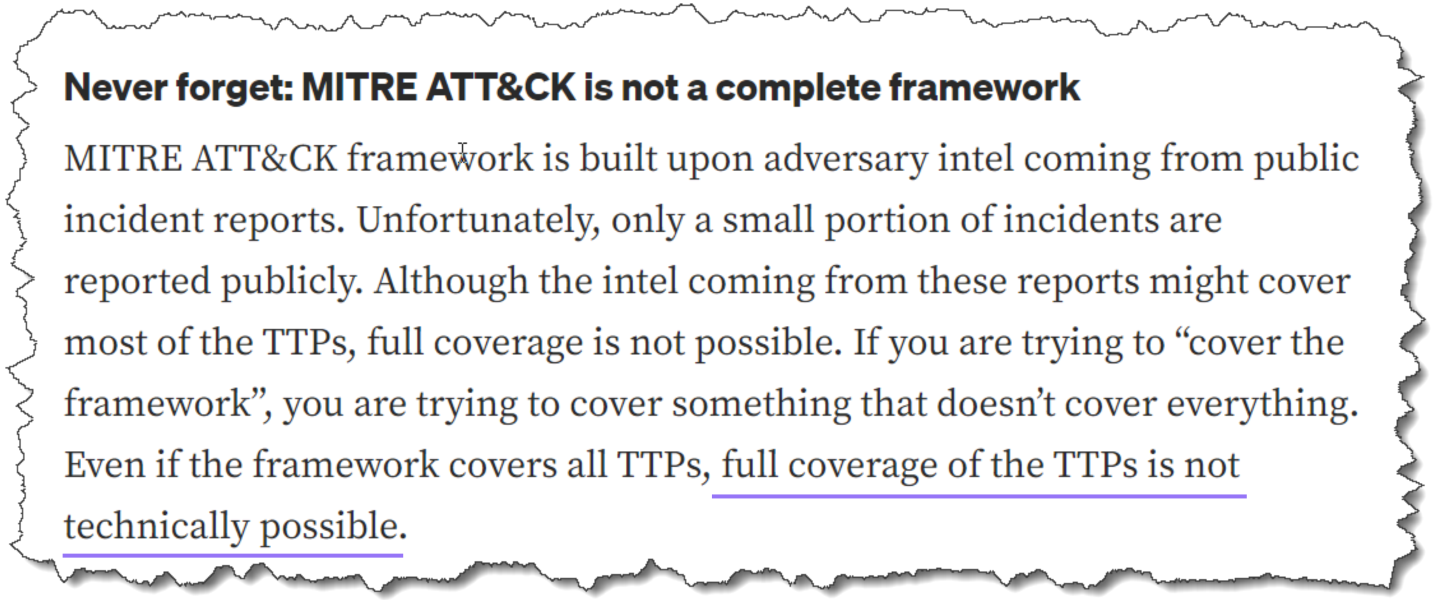
Medium

Mehmet Ergene

1K Followers

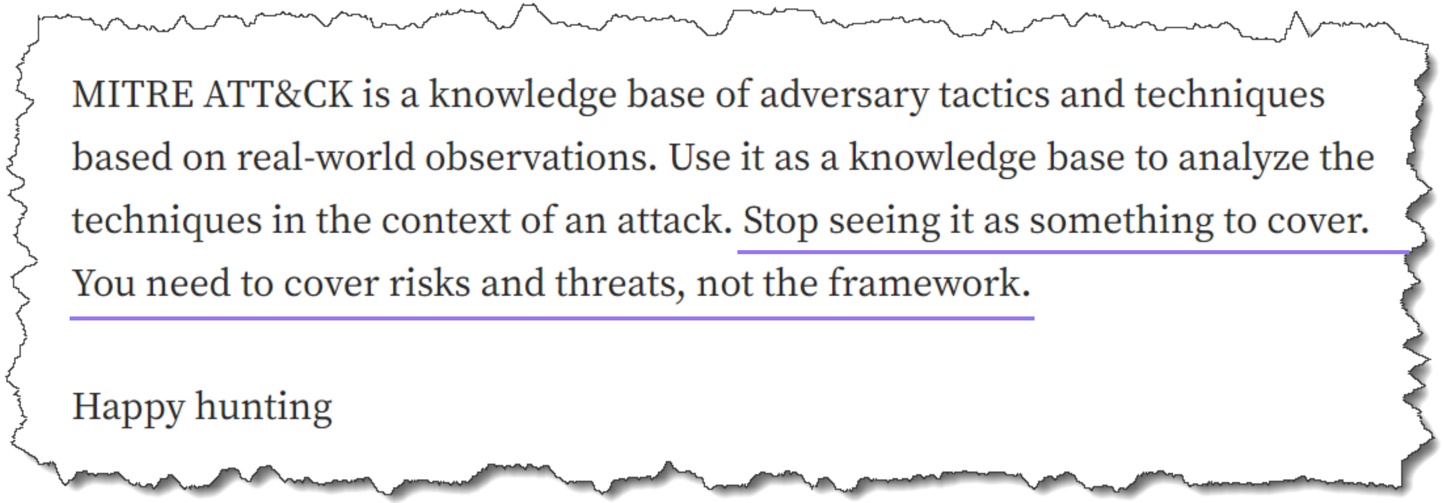
Cyber Defense Professional | Threat Research | Threat Hunting | DFIR | Detection Engineering | SOC | SIEM | @Cyb3rMonk

https://medium.com/@mergene/an-alternative-way-of-using-mitre-att-ck-for-threat-hunting-and-detection-be55739dc7aa



**Never forget: MITRE ATT&CK is not a complete framework**

MITRE ATT&CK framework is built upon adversary intel coming from public incident reports. Unfortunately, only a small portion of incidents are reported publicly. Although the intel coming from these reports might cover most of the TTPs, full coverage is not possible. If you are trying to "cover the framework", you are trying to cover something that doesn't cover everything. Even if the framework covers all TTPs, full coverage of the TTPs is not technically possible.

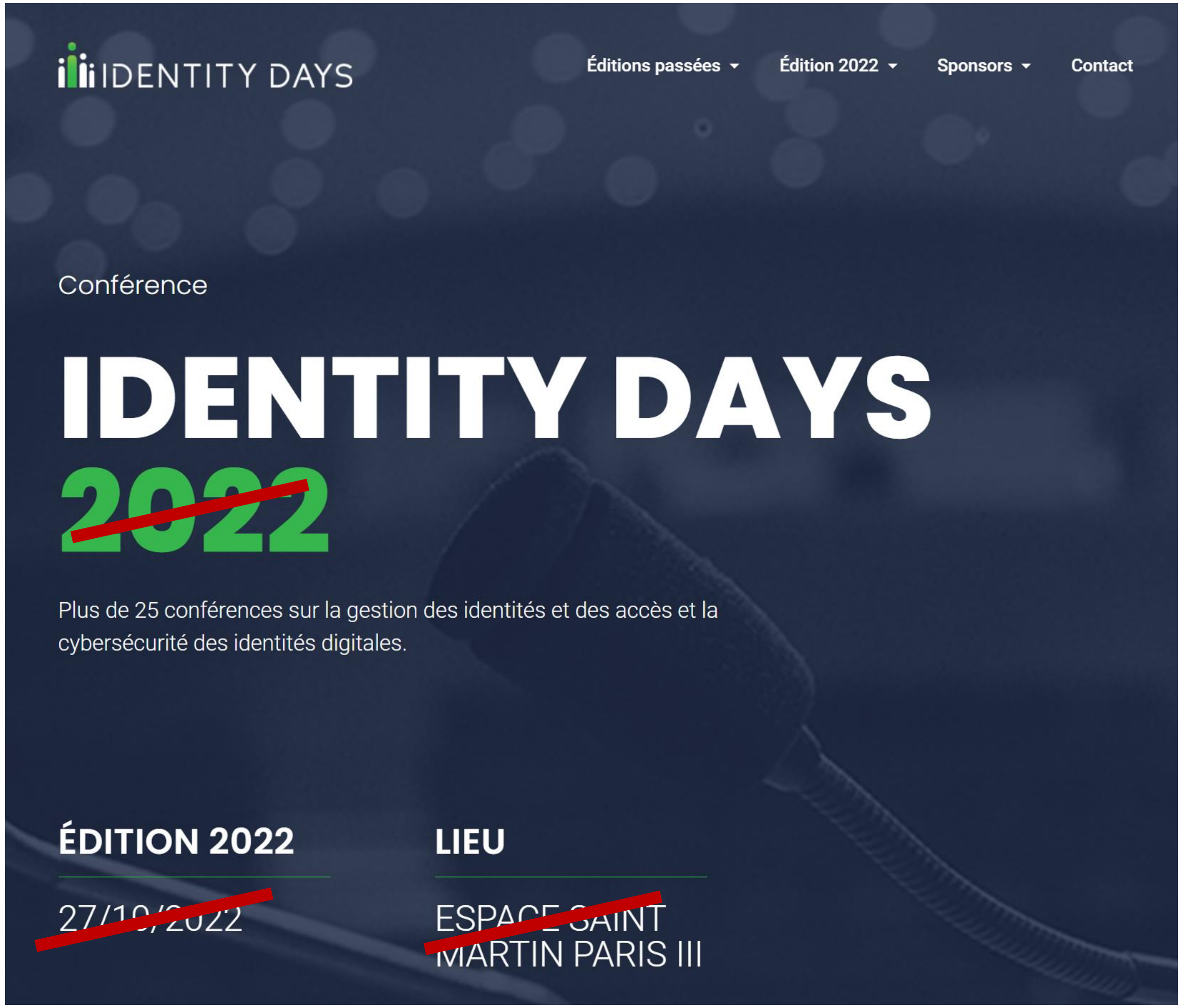


MITRE ATT&CK is a knowledge base of adversary tactics and techniques based on real-world observations. Use it as a knowledge base to analyze the techniques in the context of an attack. Stop seeing it as something to cover. You need to cover risks and threats, not the framework.

Happy hunting

Comprendre et améliorer sa sécurité grâce à MITRE ATT&CK

# What’s next?



Conférence

IDENTITY DAYS ~~2022~~

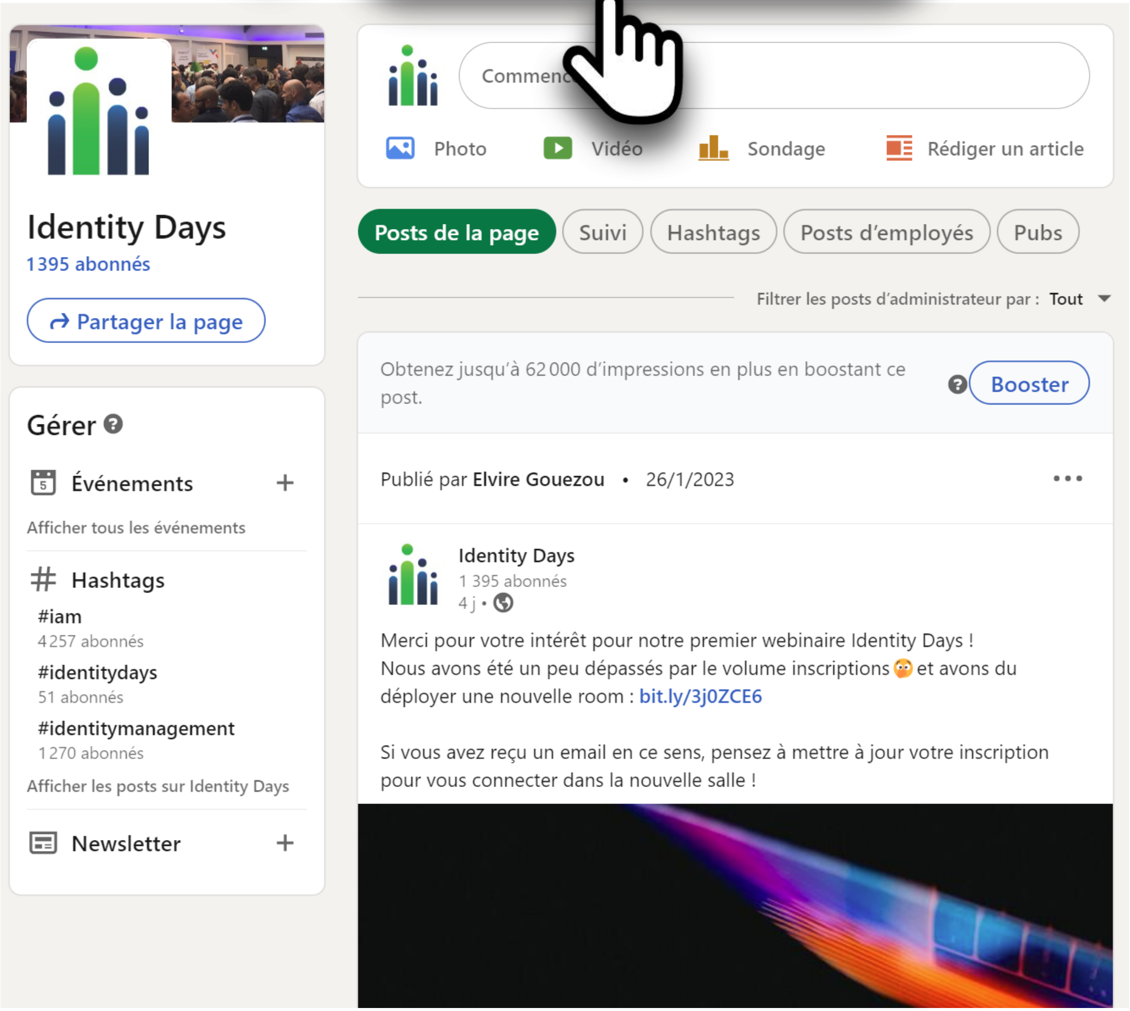
Plus de 25 conférences sur la gestion des identités et des accès et la cybersécurité des identités digitales.

ÉDITION 2022

~~27/10/2022~~

LIEU

~~ESPACE SAINT MARTIN PARIS III~~



Identity Days
1395 abonnés

#iam
4 257 abonnés

#identitydays
51 abonnés

#identitymanagement
1 270 abonnés

Obtenez jusqu’à 62 000 d’impressions en plus en boostant ce post.

Publié par Elvire Gouezou • 26/1/2023

Identity Days
1 395 abonnés
4 j •

Merci pour votre intérêt pour notre premier webinaire Identity Days !
Nous avons été un peu dépassés par le volume inscriptions 😳 et avons du déployer une nouvelle room : bit.ly/3j0ZCE6

Si vous avez reçu un email en ce sens, pensez à mettre à jour votre inscription pour vous connecter dans la nouvelle salle !

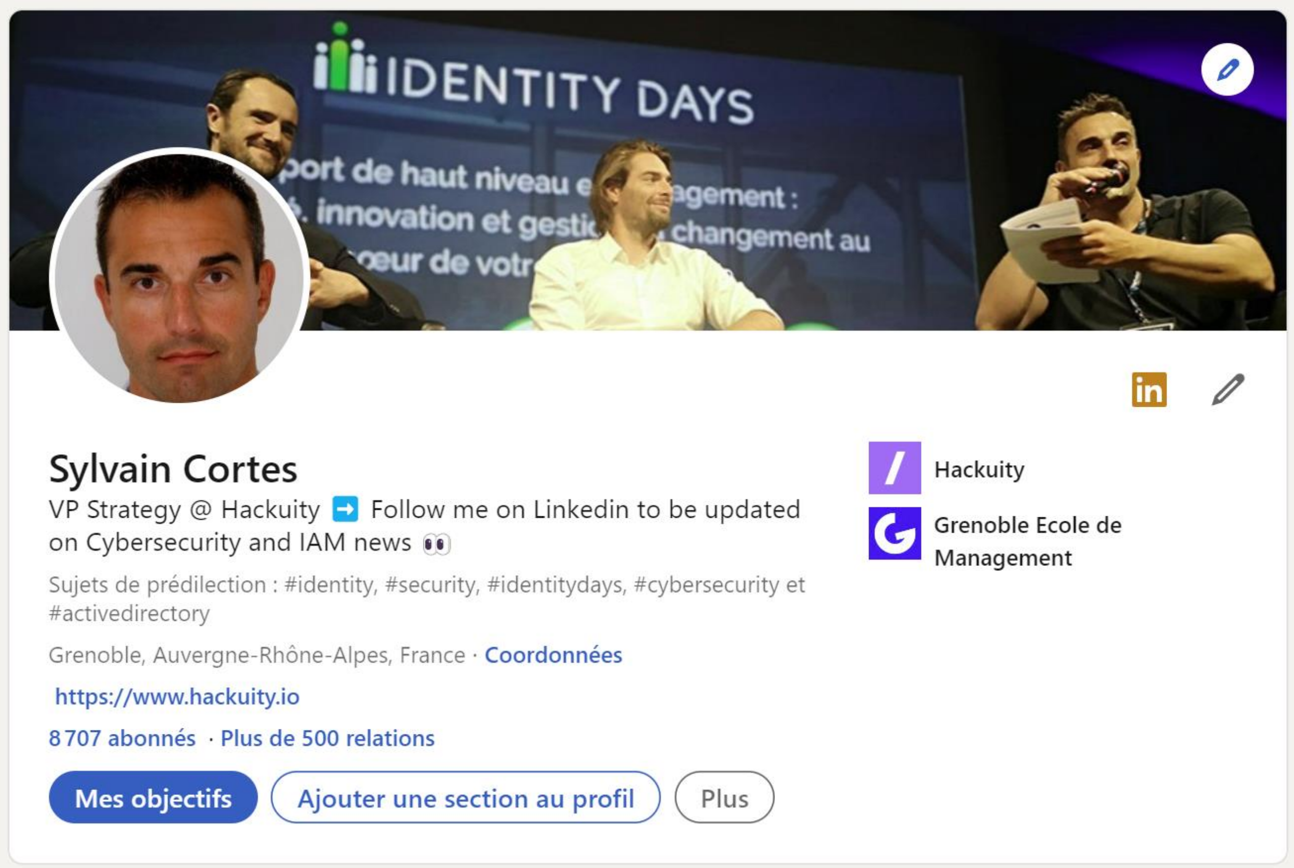
https://identitydays.com/

https://www.linkedin.com/company/identity-days/

Comprendre et améliorer sa sécurité grâce à MITRE ATT&CK

# What's next?

Subscribe



IDENTITY DAYS
port de haut niveau e... agement :
. innovation et gestic... changement au
œur de votr

Sylvain Cortes

VP Strategy @ Hackuity ➡️ Follow me on Linkedin to be updated on Cybersecurity and IAM news 👀

Sujets de prédilection : #identity, #security, #identitydays, #cybersecurity et #activedirectory

Grenoble, Auvergne-Rhône-Alpes, France · Coordonnées

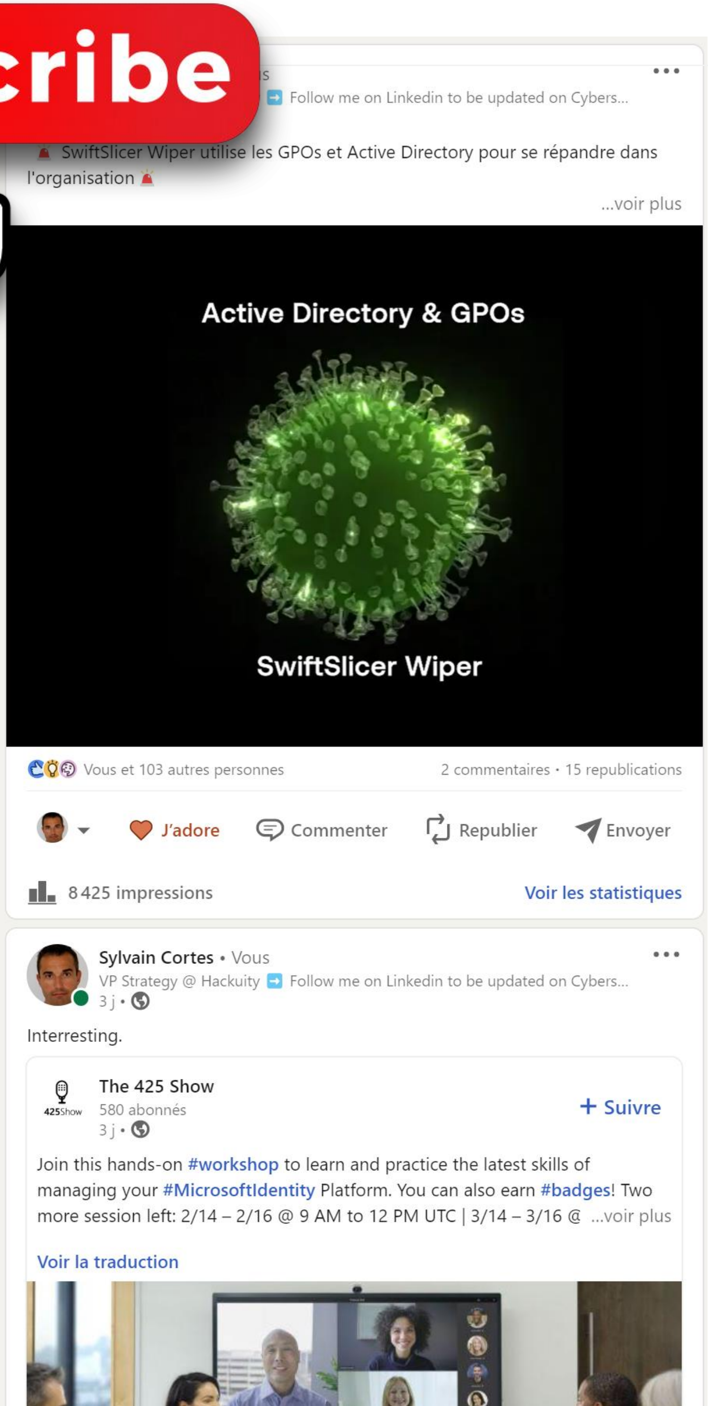
https://www.hackuity.io

8 707 abonnés · Plus de 500 relations

Hackuity

Grenoble Ecole de Management

Mes objectifs
Ajouter une section au profil
Plus



➡️ Follow me on Linkedin to be updated on Cybers...

🚨 SwiftSlicer Wiper utilise les GPOs et Active Directory pour se répandre dans l'organisation 🚨

...voir plus

Vous et 103 autres personnes · 2 commentaires · 15 republications

8 425 impressions · Voir les statistiques

Sylvain Cortes • Vous

VP Strategy @ Hackuity ➡️ Follow me on Linkedin to be updated on Cybers...

3 j •

Interesting.

The 425 Show

580 abonnés

3 j •

Join this hands-on #workshop to learn and practice the latest skills of managing your #MicrosoftIdentity Platform. You can also earn #badges! Two more session left: 2/14 – 2/16 @ 9 AM to 12 PM UTC | 3/14 – 3/16 @ ...voir plus

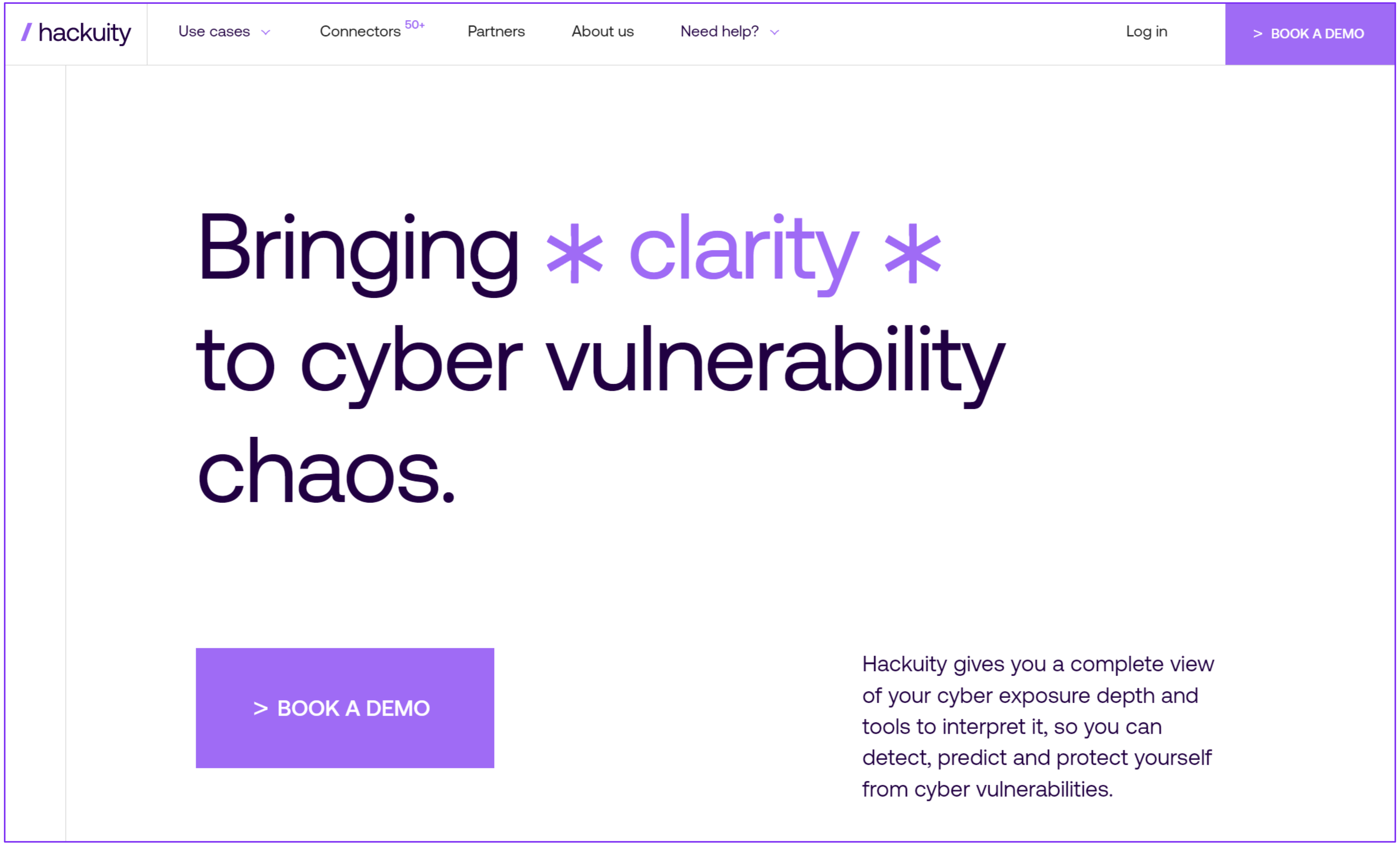
Voir la traduction

https://www.linkedin.com/in/sylvaincortes/

https://twitter.com/sylvaincortes

## What’s next?

Visit hackuity.io for additional information



/ hackuity

Use cases ⌄ Connectors 50+ Partners About us Need help? ⌄ Log in > BOOK A DEMO

Bringing * clarity * to cyber vulnerability chaos.

> BOOK A DEMO

Hackuity gives you a complete view of your cyber exposure depth and tools to interpret it, so you can detect, predict and protect yourself from cyber vulnerabilities.

https://www.hackuity.io/

# _08_

# Questions

/ hackuity

# Thank you

https://www.hackuity.io →