Decider User Guide

Version 3.0.0 - Loginless 'Kiosk'

(use version 2.x.y for content authoring)

Abstract

A web application that assists network defenders, analysts, and researchers in the process of mapping adversary behaviors to the MITRE ATT&CK® framework.

Prepared For
Department of Homeland Security

Product Of
Homeland Security Systems Engineering and Development Institute (HSSEDI™)

Code: Decider's GitHub Repo

Notice: This project makes use of MITRE ATT&CK® - ATT&CK Terms of Use

Contents

Introduction

About Decider

Decider is a web app that helps analysts map adversary behaviors to the MITRE ATT&CK Matrix.

What is the 'Kiosk'?

Decider Kiosk is a loginless version of Decider meant to be hosted as a publicly-accessible website.
User accounts, database-saved carts, and content authoring have all been removed from the application.
The frontend was also cleaned up - to improve accessibility and responsiveness.
The UI works on phones without issue.

Key Features

Decider has 3 key features:

- Question Tree
- Full Technique Search
- Shopping Cart

Question Tree *(structured progression through ATT&CK)*

Decider's homepage is the root of a question tree *(matrix level)*.
The answer cards on this page are Tactics *(adversary goals)*.
Clicking one progresses you along.

You descend down the hierarchy as such:
Matrix > Tactic > Technique > SubTechnique

Once you reach a (Sub)Technique, you can view a detailed page about it.
Should the description align with the adversary behavior you observed - you can add the Technique to your shopping cart.

Answer cards can be:

- filtered by relevant Platforms / Data Sources
  - knowing what systems a behavior occurred against / what data sources the behavior can be detected from reduces the amount of options to deal with
- re-ordered by a keyword search
  - providing key terms allows progressing through cards in a more optimal order

Full Technique Search *(ability to search and filter all Techniques at once)*

Search Technique IDs / names / descriptions using:

- prefix matching
- boolean expressions
- phrase matching

Filter Techniques by relevant:

- Tactics

- Platforms
- Data Sources

Shopping Cart *(a place to store your mappings, add context, and export to files)*

The 'CTI Shopping Cart' is a place where your mappings are stored.

- Cart entries have a text box where you can place mapping content / rationale / evidence
- Carts can be saved-to and loaded-from JSON files
- Carts can be exported to a(n)
  - ATT&CK Navigator layer
    - *(to visualize the attack heatmap in relation to defenses / existing adversary heatmaps)*
  - Microsoft Word Doc
    - *(creates a table of mapped Techniques + mapping context that can be embedded in a report)*

Support / Troubleshooting

Please create an issue / discussion on Decider's GitHub.

Does Decider Compete with the ATT&CK Website?

No, Decider complements the ATT&CK website.

Decider does not contain all of the information that is available on the ATT&CK website.
It primarily contains information on Tactics, Techniques, and the Platforms / Data Sources related to Techniques.

The goal of Decider is to aid in mapping threat reporting / adversary behaviors.
Once one has mappings - they can leverage the ATT&CK website for further insights / next steps (i.e. detections, mitigations).

Proposed Workflow

1. Go to the question tree homepage *(click **Decider** in the top left)*
2. Identify the goal of the adversary's actions *(Tactic)* - click this card
3. Identify what Platform(s) the adversary's actions occurred on/against and set these filters
   - *(optionally set Data Sources their behavior could be detected by)*
4. Follow the remaining prompts to end up on a (Sub)Technique Success Page
5. Read the Technique's description
   - **A. if it matches the observed behavior, then add it to your cart
   - B. if it does not, backtrack
     - a different SubTechnique may apply
     - **(or)** the 'Base' Technique may apply instead of one of its SubTechniques
     - **(or)** a different Technique may apply
     - **(or)** a different Tactic may apply even

** 5.A. Continued

- Before adding to your cart
  - If the **Mismappings** section is present
    - double check that the **Other Potential Technique(s)** do not apply instead
- After adding to your cart
  - If the **Frequently Appears With** section is present
    - skim the suggested Techniques, as the adversary *may* have leveraged them too

CISA Best Practices for MITRE ATT&CK Mapping

The mapping steps below follow those identified in CISA's ATT&CK Mapping Guide. Analysts may choose their own starting point based on their familiarity with ATT&CK and the technical details / context available in the report.

1. **Identify Tactics** – Comb through the report to identify the adversary's tactics and the flow of the attack. To identify the tactics (the adversary's goals), focus on what the adversary was trying to accomplish and why. Review the tactic definitions to determine how the identified behaviors might translate into a specific tactic. Each tactic includes a finite number of actions an adversary can take to implement their goal. Understanding the flow of the attack can help identify the techniques or sub-techniques that an adversary may have employed.

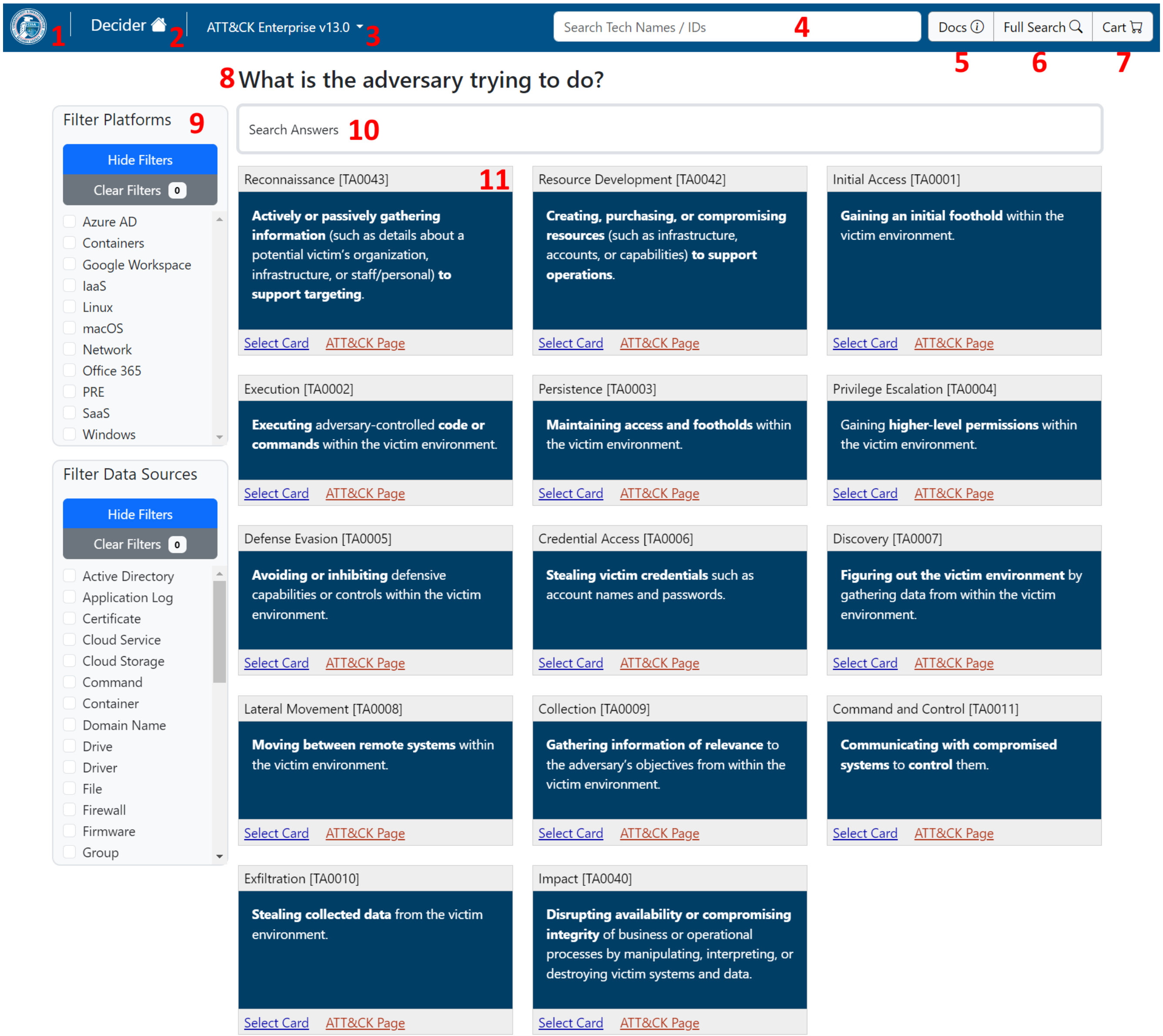
2. **Identify Techniques** – After identifying the tactics, review the technical details associated with how the adversary tried to achieve their goals. Note: if you have insufficient detail to identify an applicable technique, you will be limited to mapping to the tactic level, which alone is not actionable information for detection purposes. Compare the behavior in the report with the description of the ATT&CK techniques listed under the identified tactic. If one of them matches, then it may be an appropriate technique. Be aware that multiple techniques may apply concurrently to the same behavior.

3. **Identify Sub-Techniques** – Review sub-technique descriptions to see if they match the information in the report. A match here may be an appropriate sub-technique. Read sub-technique descriptions carefully to understand the differences between them. In cases where the parent of a sub-technique aligns to multiple tactics, make sure to choose the appropriate tactic. Note: map solely to the parent technique only if there is not enough context to identify a sub-technique.

Consider techniques and sub-techniques as elements of an adversary's playbook, rather than as isolated activities. Adversaries often use information they obtain from each activity in an operation to determine what additional techniques they will use next in the attack cycle. Because of this, techniques and sub-techniques are often linked in the attack chain.

Navigating Decider

Question Tree (Home) + Navbar



What is the adversary trying to do?

Reconnaissance [TA0043]
Actively or passively gathering information (such as details about a potential victim's organization, infrastructure, or staff/personal) **to support targeting**.
Select Card ATT&CK Page

Resource Development [TA0042]
Creating, purchasing, or compromising resources (such as infrastructure, accounts, or capabilities) **to support operations**.
Select Card ATT&CK Page

Initial Access [TA0001]
Gaining an initial foothold within the victim environment.
Select Card ATT&CK Page

Execution [TA0002]
Executing adversary-controlled **code or commands** within the victim environment.
Select Card ATT&CK Page

Persistence [TA0003]
Maintaining access and footholds within the victim environment.
Select Card ATT&CK Page

Privilege Escalation [TA0004]
Gaining **higher-level permissions** within the victim environment.
Select Card ATT&CK Page

Defense Evasion [TA0005]
Avoiding or inhibiting defensive capabilities or controls within the victim environment.
Select Card ATT&CK Page

Credential Access [TA0006]
Stealing victim credentials such as account names and passwords.
Select Card ATT&CK Page

Discovery [TA0007]
Figuring out the victim environment by gathering data from within the victim environment.
Select Card ATT&CK Page

Lateral Movement [TA0008]
Moving between remote systems within the victim environment.
Select Card ATT&CK Page

Collection [TA0009]
Gathering information of relevance to the adversary's objectives from within the victim environment.
Select Card ATT&CK Page

Command and Control [TA0011]
Communicating with compromised systems to **control** them.
Select Card ATT&CK Page

Exfiltration [TA0010]
Stealing collected data from the victim environment.
Select Card ATT&CK Page

Impact [TA0040]
Disrupting availability or compromising integrity of business or operational processes by manipulating, interpreting, or destroying victim systems and data.
Select Card ATT&CK Page

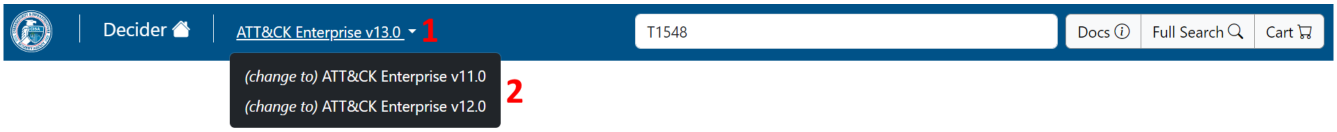
Usage

Answer the *Question* (8) by clicking one of the *Answer Cards* (11).
Optionally reduce the amount of cards to sift through by settings *Filters* (9).
Optionally order the answer cards by keyword relevance using *Search* (10).

1. **CISA Seal** - Links to CISA.gov
2. **Decider Home** - Takes you to this page *(the question tree home)*
3. **Version Picker** - Lets you to change what version of ATT&CK data you're viewing
4. **Mini Technique Search** - Lets you quickly jump to a Technique's page by its name or ID
5. **Documentation** - Opens this user guide
6. **Full Technique Search** - Opens the Full Technique Search page, which supports searching/filtering all Techniques at once
7. **Shopping Cart** - Opens the CTI Shopping Cart, where your mappings can be viewed, edited, saved, or exported

8. **Question** - You select the *Answer Card* (11) that best answers this prompt
9. **Filters** - These allows hiding *Answer Cards* (11) that do not match the specified criteria
    - Filter Types
        - **Platforms** are the system types that the behavior occurred on/against
        - **Data Sources** are means by which behavior could have been detected
    - Filtering Advice
        - **Ignore on the homepage,** there are only 14 Tactics to pick from, no need to filter here
            - Also, Tactics have all Platforms / Data Sources of the Techniques under them. Setting a Platform filter + a Data Source filter may show a Tactic that has no Techniques under it fulfilling that filter combo
        - **Be generous,** an answer card is shown if it matches any of the filters *(of a given type)*
            - Accidentally hiding the correct answer card by mis-selecting would be detrimental
            - The goal of filters is to generally narrow how many answer card you need to look at *(Defense Evasion has 42 'Base' Techniques as of v13)*
10. **Search Answer Cards** - This re-orders the *Answer Cards* (11) by relevance to the keywords you've entered
    - Search Functionality
        - **On Matrix -> Tactics Homepage**
            - There are only 14 Tactics, this is a basic keyword search
        - **On Deeper Pages**
            - Advanced search functionality is supported here
            - Typed words are OR'd together by default
            - **&** requires both terms to be present
            - **|** requires either term to be present
            - **~** requires a term to be absent
            - **()** can be used to order AND/OR/NOT operators
            - ***** is used for prefix matching *(proc* -> proc, process, procedure)*
            - **""** specify that each word in a phrase must be present *(non a-z0-9 characters are stripped)*
11. **Answer Cards** - You pick the answer that best answers the *Question* (8).
    - These represent Tactics, the Techniques, and finally SubTechniques as you progress through the ATT&CK hierarchy structure.
    - Clicking the card progresses you through the tree (same as clicking 'Select Card').
    - Clicking 'ATT&CK Page' opens the ATT&CK page for the given Tactic/Technique

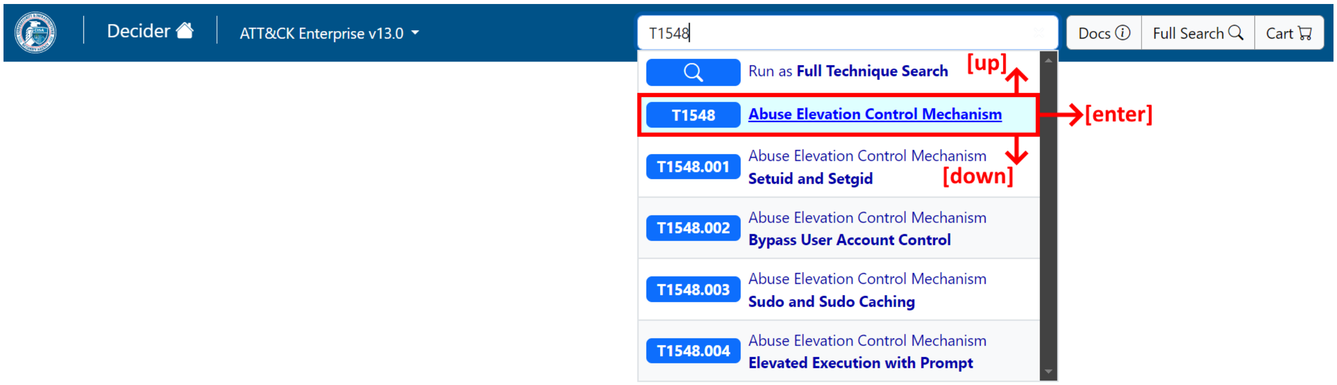
Navbar > Version Picker


Decider
ATT&CK Enterprise v13.0
1
Docs
Full Search
Cart
(change to) ATT&CK Enterprise v11.0
(change to) ATT&CK Enterprise v12.0
2

T1548

1. **Current Version** - This shows the current ATT&CK version the app is showing content for. Clicking this reveals *Other Versions* (2)
2. **Other Versions** - Clicking a version will make the app display content for it

Navbar > Mini Technique Search

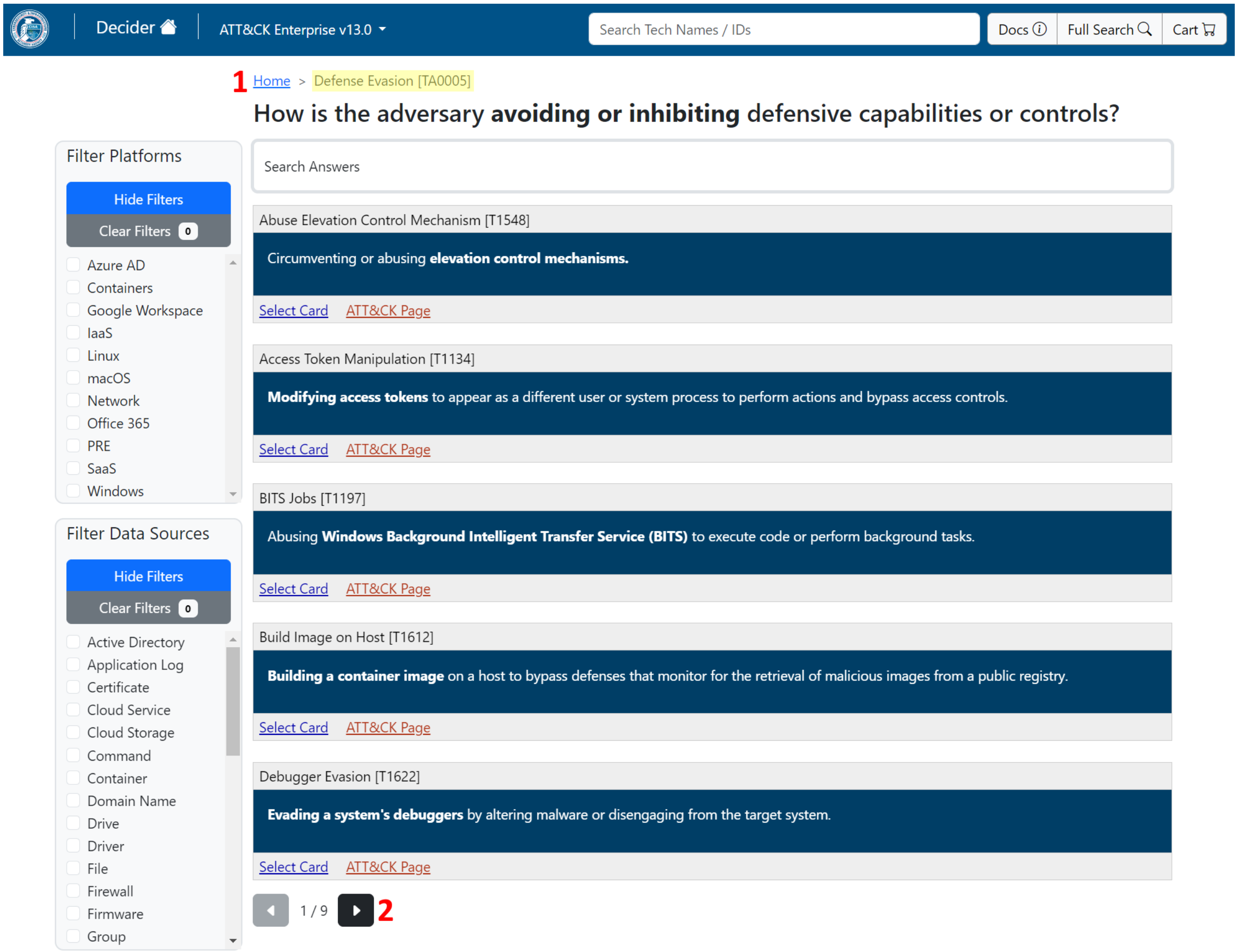

Decider
ATT&CK Enterprise v13.0
T1548
Docs
Full Search
Cart
Run as Full Technique Search
[up]
T1548 Abuse Elevation Control Mechanism
[enter]
T1548.001 Abuse Elevation Control Mechanism Setuid and Setgid
[down]
T1548.002 Abuse Elevation Control Mechanism Bypass User Account Control
T1548.003 Abuse Elevation Control Mechanism Sudo and Sudo Caching
T1548.004 Abuse Elevation Control Mechanism Elevated Execution with Prompt

Usage

Use to quickly jump to a Technique's Success Page.
Or to start a Full Technique Search.

- **Searching -** Techniques can be searched by Name or ID here
- **Keyboard Navigation** is supported as well *(in addition to mouse, touchscreen, etc)*
  - [**up**] and [**down**] to select options
  - [**enter**] to open the selected entry
    - If a selection has not yet been made, a Full Technique Search is performed by default

Question Tree > Tactic



How is the adversary **avoiding or inhibiting** defensive capabilities or controls?

Abuse Elevation Control Mechanism [T1548]

Circumventing or abusing **elevation control mechanisms.**

Select Card ATT&CK Page

Access Token Manipulation [T1134]

Modifying access tokens to appear as a different user or system process to perform actions and bypass access controls.

Select Card ATT&CK Page

BITS Jobs [T1197]

Abusing **Windows Background Intelligent Transfer Service (BITS)** to execute code or perform background tasks.

Select Card ATT&CK Page

Build Image on Host [T1612]

Building a container image on a host to bypass defenses that monitor for the retrieval of malicious images from a public registry.

Select Card ATT&CK Page

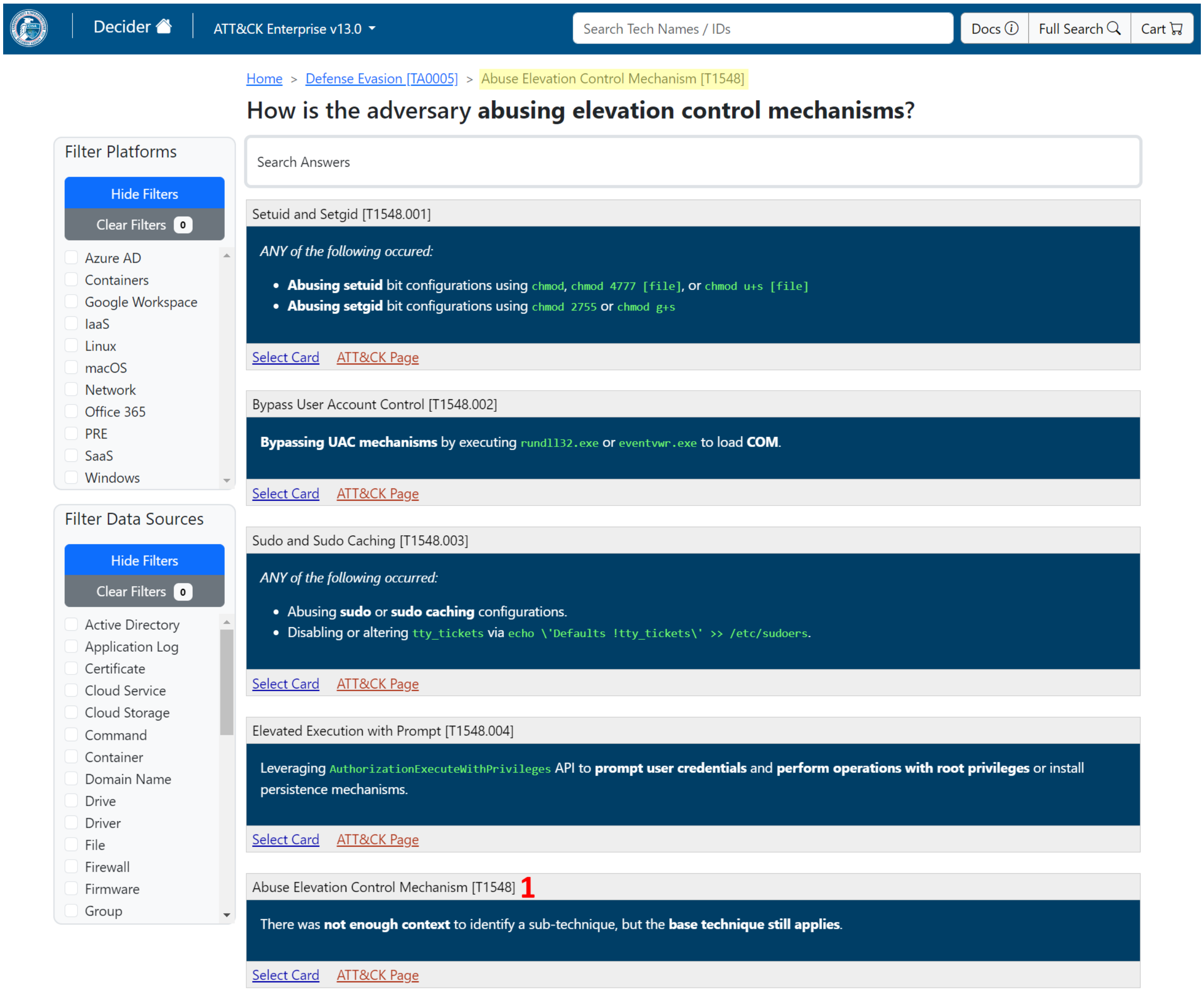
Debugger Evasion [T1622]

Evading a system's debuggers by altering malware or disengaging from the target system.

Select Card ATT&CK Page

1. **Crumbs Bar -** This shows your progress through the question tree
   - You can click crumbs to navigate back up the tree
2. **Answer Card Page Navigation -** These buttons allow you to flip through the available answer cards
   - 5 answer cards are shows per page

Question Tree > Technique



Home > Defense Evasion [TA0005] > Abuse Elevation Control Mechanism [T1548]

How is the adversary **abusing elevation control mechanisms?**

Filter Platforms

Hide Filters

Clear Filters 0

□ Azure AD
□ Containers
□ Google Workspace
□ IaaS
□ Linux
□ macOS
□ Network
□ Office 365
□ PRE
□ SaaS
□ Windows

Filter Data Sources

Hide Filters

Clear Filters 0

□ Active Directory
□ Application Log
□ Certificate
□ Cloud Service
□ Cloud Storage
□ Command
□ Container
□ Domain Name
□ Drive
□ Driver
□ File
□ Firewall
□ Firmware
□ Group

Search Answers

Setuid and Setgid [T1548.001]

ANY of the following occured:

- **Abusing setuid** bit configurations using `chmod`, `chmod 4777 [file]`, or `chmod u+s [file]`
- **Abusing setgid** bit configurations using `chmod 2755` or `chmod g+s`

Select Card ATT&CK Page

Bypass User Account Control [T1548.002]

Bypassing UAC mechanisms by executing `rundll32.exe` or `eventvwr.exe` to load **COM**.

Select Card ATT&CK Page

Sudo and Sudo Caching [T1548.003]

ANY of the following occurred:

- Abusing **sudo** or **sudo caching** configurations.
- Disabling or altering `tty_tickets` via `echo \'Defaults !tty_tickets\' >> /etc/sudoers`.

Select Card ATT&CK Page

Elevated Execution with Prompt [T1548.004]

Leveraging `AuthorizationExecuteWithPrivileges` API to **prompt user credentials** and **perform operations with root privileges** or install persistence mechanisms.

Select Card ATT&CK Page

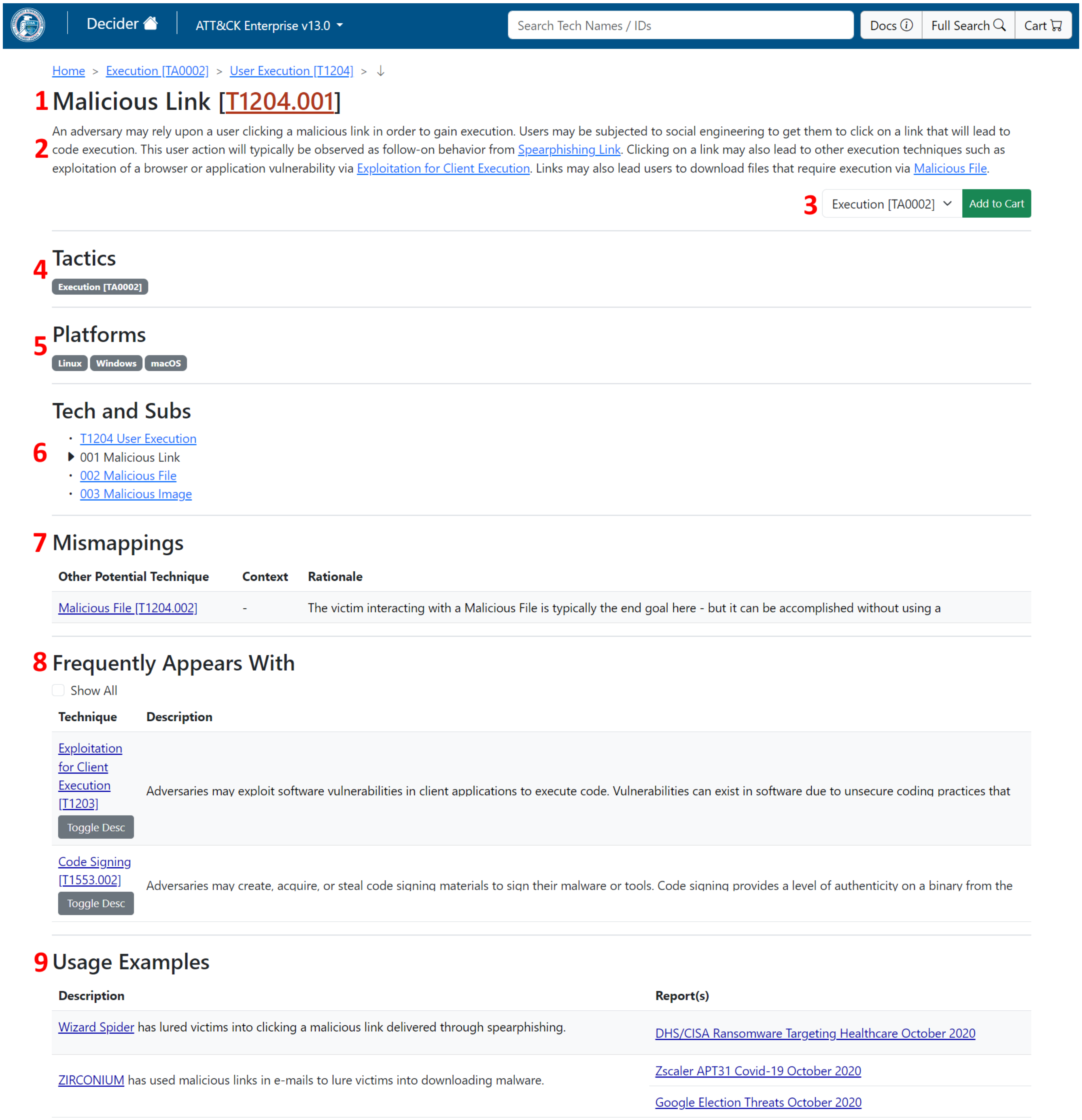
Abuse Elevation Control Mechanism [T1548]

There was **not enough context** to identify a sub-technique, but the **base technique still applies**.

Select Card ATT&CK Page

1. **Base Technique Card -** Notice that this answer card has the same ID as the question page we're on. This is because the 'Base' Technique still applies even if we did not find behavior specific to any of the SubTechniques

Question Tree > Technique Success Page



Home > Execution [TA0002] > User Execution [T1204] > ↓

Malicious Link [T1204.001]

An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Link. Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via Exploitation for Client Execution. Links may also lead users to download files that require execution via Malicious File.

Tactics

Execution [TA0002]

Platforms

Linux Windows macOS

Tech and Subs

- T1204 User Execution
- ▶ 001 Malicious Link
- 002 Malicious File
- 003 Malicious Image

Mismappings

Other Potential Technique	Context	Rationale
Malicious File [T1204.002]	-	The victim interacting with a Malicious File is typically the end goal here - but it can be accomplished without using a

Frequently Appears With

Technique	Description
Exploitation for Client Execution [T1203]	Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that
Code Signing [T1553.002]	Adversaries may create, acquire, or steal code signing materials to sign their malware or tools. Code signing provides a level of authenticity on a binary from the

Usage Examples

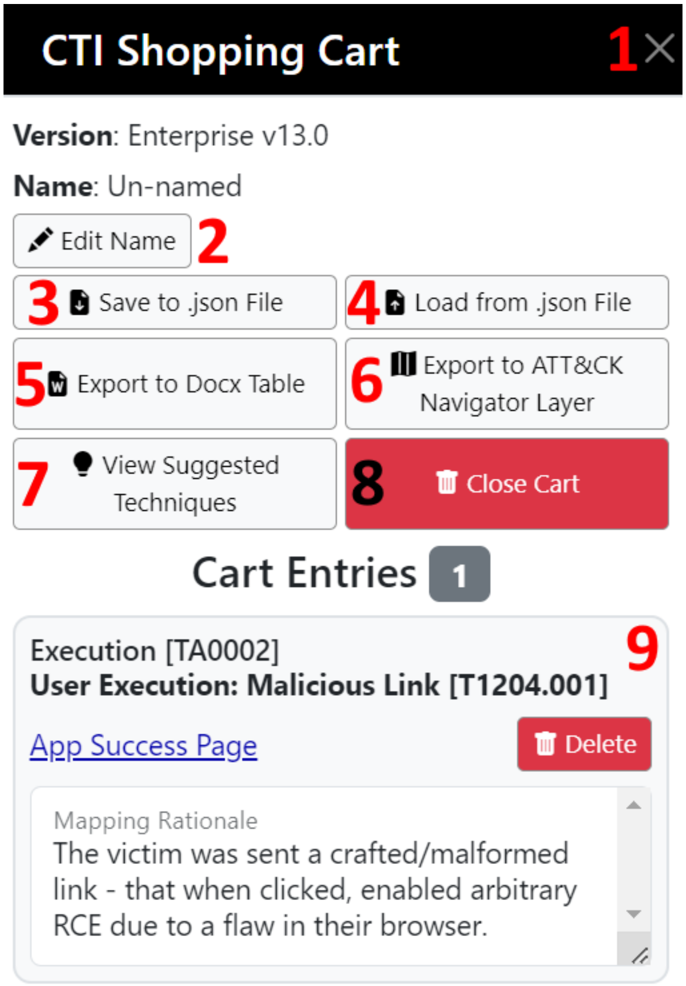
Description	Report(s)
Wizard Spider has lured victims into clicking a malicious link delivered through spearphishing.	DHS/CISA Ransomware Targeting Healthcare October 2020
ZIRCONIUM has used malicious links in e-mails to lure victims into downloading malware.	Zscaler APT31 Covid-19 October 2020 Google Election Threats October 2020

1. **Technique Name / ID** - The ID is also a link to the Technique's ATT&CK page
2. **Technique Description** - This is the same description as on the Technique's ATT&CK page
3. **Confirm Tactic + Add to Cart**
   - 'Technique Success Pages' can be reached through the Question Tree or through the Full Technique Search
     - The Question Tree already gives you the Tactic context you're working with (dropdown is pre-selected)
     - Whereas getting to a Success Page via Search will require you to select a Tactic before the Add-to-Cart button works
   - Clicking Add-to-Cart places an entry for the selected Technique+Tactic combo in your mapping cart
4. **Tactics** - Goals this behavior can achieve
5. **Platforms** - Systems this Technique can be leveraged against/on

6. **Tech and Subs** - Success Page links for the Base Technique and its Sub Techniques
7. ****Mismappings** - Techniques listed here may have occurred instead of the Technique on this page
   - That is, this table records knowledge of previously incorrectly mapped Techniques *(user editable)*
   - Decider does not provide any mismappings out of the box
   - Mismappings can be added via JSON during the build process
     - **(or)** a Decider 2.x.y instance can be pointed at the same database used by Kiosk (Decider 3.x.y) in order to edit these
8. ****Frequently Appears With** - Techniques here are likely to have occurred with the current Technique being viewed
   - Skim the Technique descriptions to see if any match the observed adversary behaviors
   - The table shows a slightly randomized subset of suggested Techniques - this is to help prevent availability bias in mapping
     - Checking **Show All** will list all suggestions
   - This dataset comes from Andy Applebaum's work - Medium Article
     - In short: Techniques that frequently appear together in CTI reports, *may* appear together in future adversary behavior too
9. ****Usage Examples** - These are examples of the Technique being used by Campaigns, Groups, Software, and Tools.
   - Reports covering / mapping the observation are linked too

** *(Section hidden if no data for this Technique)*

CTI Shopping Cart



Version: Enterprise v13.0

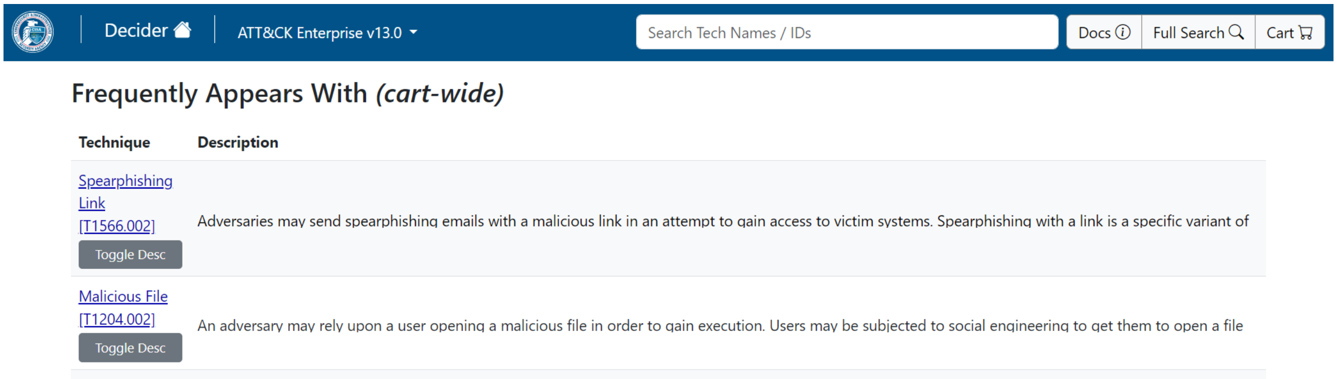
Name: Un-named

Execution [TA0002]
User Execution: Malicious Link [T1204.001]

Mapping Rationale
The victim was sent a crafted/malformed link - that when clicked, enabled arbitrary RCE due to a flaw in their browser.

1. **Close Cart** - Closes the cart
2. **Edit Name** - Allows naming the cart *(changes name of exported files + saved / loaded cart)*
3. **Save Cart to .json** - Saves the contents of the cart as a JSON file
4. **Load Cart from .json** - Loads a prior-saved JSON cart file
5. **Export to Docx Table** - Creates a Microsoft Word DOCX file containing a table of the Tactics / Techniques mapped and their mapping rationales
6. **Export to ATT&CK Navigator** - Creates a MITRE ATT&CK® Navigator layer with cart entries highlighted. The mapping rationales are also added to the Navigator layer in the form of comments
7. **View Suggested Techniques** - A cart-wide variant of the Technique Success Page > *Frequently Appears With* listing
8. **Close Cart** *(has confirmation screen)* - Deletes / closes the cart. Make sure you saved to a JSON before clicking this - otherwise the cart is irrecoverable
9. **Cart Entry** - A mapped Technique + Tactic combo
   - **App Success Page** - Takes you to the Technique Success Page for this entry
   - **Delete** - Removes this entry from your cart
   - **Mapping Rationale** - An area for you to record context / rationale / evidence as to why this entry was mapped. A good place for notes too

Cart-Wide Frequently Appears With



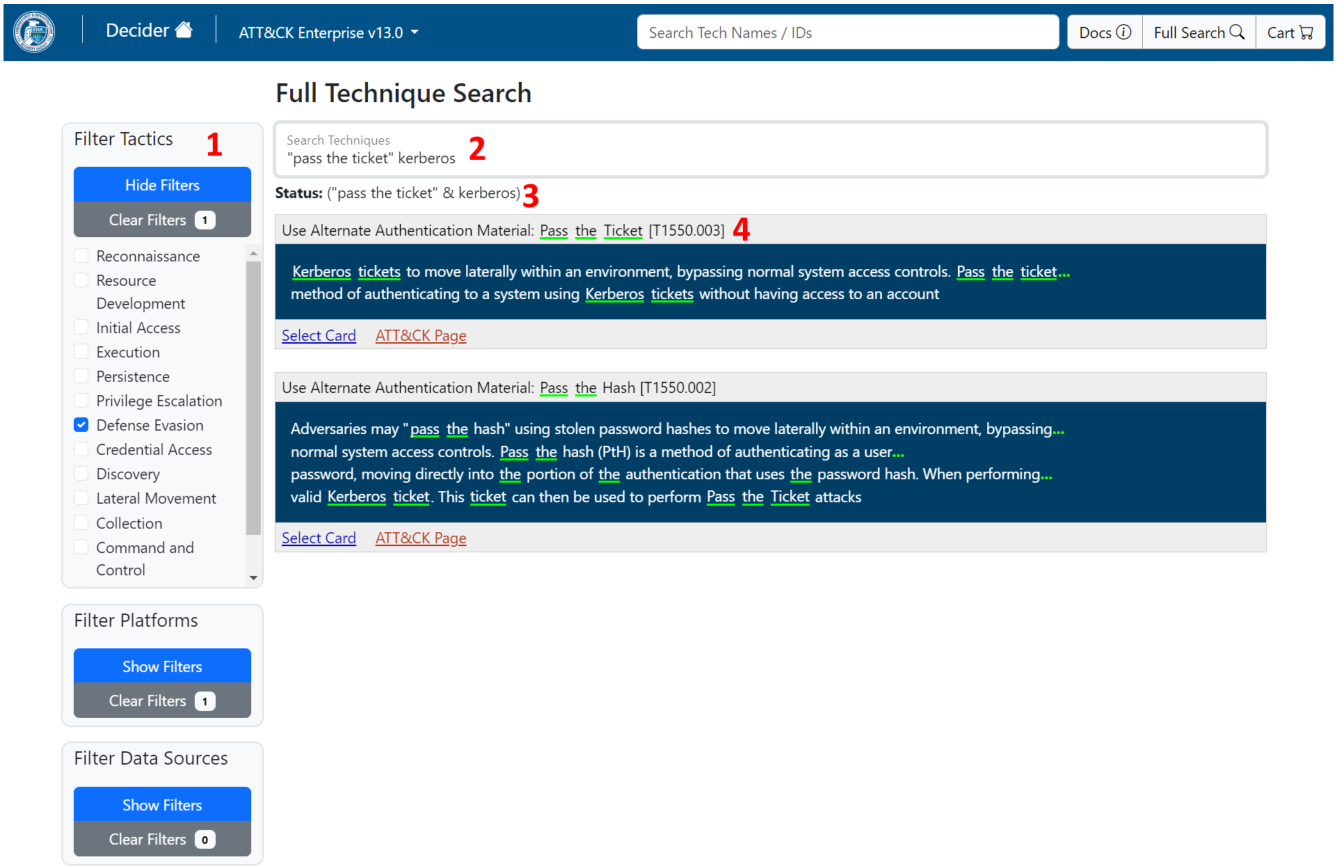
Frequently Appears With *(cart-wide)*

Technique	Description
Spearphishing Link [T1566.002] Toggle Desc	Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of
Malicious File [T1204.002] Toggle Desc	An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file

- A cart-wide variant of Technique Success Page > *Frequently Appears With*
- Suggests Techniques that *may* have occurred based upon the contents of your cart

Skim the Technique descriptions to see if any match the observed adversary behaviors.
Read the full description to confirm a mapping before adding it to your cart.

Full Technique Search



Search Techniques
"pass the ticket" kerberos

Status: ("pass the ticket" & kerberos)

Use Alternate Authentication Material: Pass the Ticket [T1550.003]

Kerberos tickets to move laterally within an environment, bypassing normal system access controls. Pass the ticket...
method of authenticating to a system using Kerberos tickets without having access to an account

Use Alternate Authentication Material: Pass the Hash [T1550.002]

Adversaries may "pass the hash" using stolen password hashes to move laterally within an environment, bypassing...
normal system access controls. Pass the hash (PtH) is a method of authenticating as a user...
password, moving directly into the portion of the authentication that uses the password hash. When performing...
valid Kerberos ticket. This ticket can then be used to perform Pass the Ticket attacks

1. **Filters** - Only Techniques that match at least 1 filter *(per each type)* are shown. *(a filter is ignored if 0 are set)*
   - Filter Types
     - **Tactics:** goals of the adversary's behaviors
     - **Platforms:** systems that the Technique was performed on/against
     - **Data Sources:** sources that can be used to detect the behavior
   - Filtering Advice
     - **Be generous,** it's better to accidentally include slightly more results than to miss the correct Technique by over-constraining
2. **Search** - Your search goes here
   - Searched Fields
     - IDs
     - Names
     - Descriptions
   - Usage
     - **Basic Search**
       - By default, terms are AND'd together here
       - So, typing more terms will constrain further
       - You can use | between terms to OR them together for a simple keyword search
     - **Advanced Search**
       - Advanced search functionality is supported here
       - Typed words are AND'd together by default
       - **&** requires both terms to be present
       - **|** requires either term to be present
       - **~** requires a term to be absent
       - **()** can be used to order AND/OR/NOT operators
       - ***** is used for prefix matching *(proc* -> proc, process, procedure)*

        - **""** specify that each word in a phrase must be present *(non a-z0-9 characters are stripped)*

3. **Search Status -** Provides feedback on your search
    - Warns if the search query is malformed / invalid
    - **(otherwise)** Indicates how the search query was interpreted
4. **Technique Cards -** The Technique results from your search
    - Clicking a card opens its Technique Success Page *(same as clicking ‘Select Card’)*
    - Clicking ‘ATT&CK Page’ opens the Technique’s ATT&CK Page