MITRE ENGENUITY™

A Foundation for Public Good

Insider Threat Knowledge Base Case Submission Portal User Guide

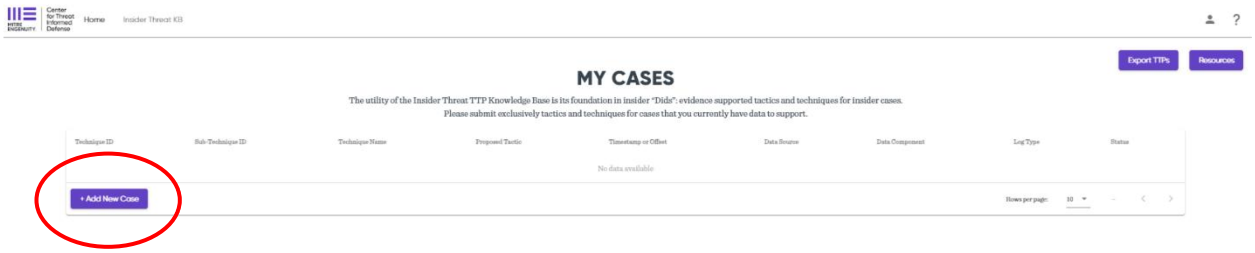
Contents

Public Release Disclaimer:

Unless otherwise stated, all information entered into the portal will be released to the public. Do not enter any information you or your organization are uncomfortable sharing, including PII, information that may point to your organization, or other highly sensitive or proprietary information.

Creating a Case

1. To enter a new case, select the purple + *Add New Case* button.



MY CASES

The utility of the Insider Threat TTP Knowledge Base is its foundation in insider "Dids": evidence supported tactics and techniques for insider cases.
Please submit exclusively tactics and techniques for cases that you currently have data to support.

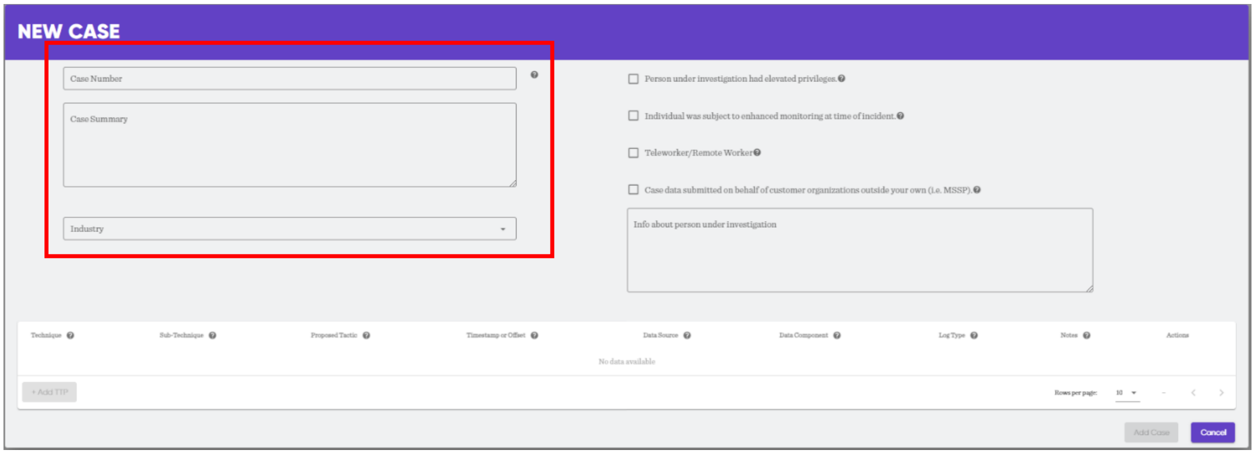
Technique ID	Sub-Technique ID	Technique Name	Proposed Tactic	Timestamp or Offset	Data Source	Data Component	Log Type	Status
No data available								

2. On the New Case page, enter the following on the left side.
   a. **Case Number**: this is any combination of numbers and letters and can be unique to your organization. **Case Numbers will not be released to the public.** It is intended to help organizations track which cases have been entered into the portal.

   b. **Case Summary**: This summary should be detailed enough to give researchers an understanding of what happened in the case, but vague enough that it does not give away information that can lead back to your organization or the individual involved. Again, this information will eventually be published. Do not include information you do not want to be made public.
      i. **Good Example**: Subject placed roughly 230 documents, many of which were proprietary or sensitive, into a new folder on their desktop in three separate batches over the course of 16 days. Three days later they started uploading the documents to their personal cloud storage account. He performed this task over the course of the 3 days, placing between 15 and 20 documents in his account at a time.

      ii. **Bad Example**: John Smith placed roughly 230 documents into a new folder on his desktop, many of which were related to the NeuralNails and SynapseScrews which is proprietary technology being developed within Acme Corporation's AI-powered Construction and Building Materials Division. He collected these documents over the course of 16 days. Three days later they started uploading the documents to their personal cloud storage account under the username TakeTheDataAndRun. He performed this task over the course of the 3 days, placing between 15 and 20 documents in his account at a time.

c. **Industry**: this is the industry your organization belongs to, or if submitting on behalf of a customer organization outside of your own, their industry.



NEW CASE

Case Number

Case Summary

Industry

□ Person under investigation had elevated privileges.

□ Individual was subject to enhanced monitoring at time of incident.

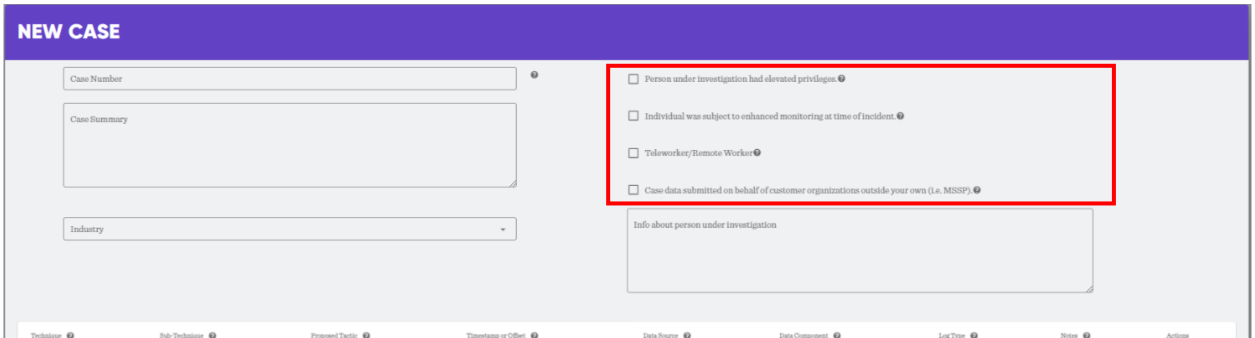
□ Teleworker/Remote Worker

□ Case data submitted on behalf of customer organizations outside your own (i.e. MSSP).

Info about person under investigation

Technique	Sub-Technique	Proposed Tactic	Timestamp or Offset	Data Source	Data Component	Log Type	Notes	Actions
No data available								

3. Select any of the boxes on the right side that apply. If unsure, hover over the question mark to see an additional explanation and example.
   a. **Person Under Elevated Privileges**: "elevated privileges" refer to the heightened level of access and control granted to certain users or accounts within a system or network. These privileged users are able to perform tasks and operations that regular users cannot, such as creating or modifying user accounts, modifying system settings, or installing software.
   b. **Individual was subject to enhanced monitoring at the time of incident**: was this person flagged for heightened monitoring for any reason, except that they are leaving the organization. This will be captured in another section. This may be due to previous user behavior, their role within the company, that they have access to highly sensitive data, or some other reason the organization has deemed necessary.
   c. **Teleworker/Remote Worker:** an employee who works from a location outside the traditional office. If the employee is a hybrid worker who splits their time between an office and non-office location, please mark them as a teleworker if most of the actions within the case were performed while outside the office.
   d. **Case Data was submitted on behalf of customer organizations outside your own:** if you are submitting for some other organization, please indicate this in each case,



NEW CASE

Case Number

Case Summary

Industry

□ Person under investigation had elevated privileges.

□ Individual was subject to enhanced monitoring at time of incident.

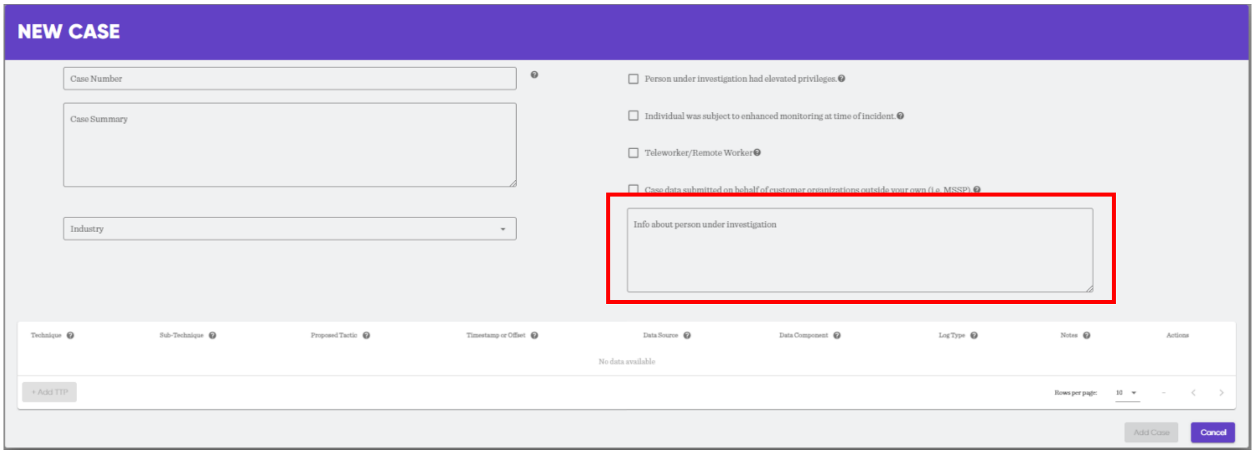
□ Teleworker/Remote Worker

□ Case data submitted on behalf of customer organizations outside your own (i.e. MSSP).

Info about person under investigation

Technique	Sub-Technique	Proposed Tactic	Timestamp or Offset	Data Source	Data Component	Log Type	Notes	Actions

4. Put any additional information about the person under investigation in the text box on the right. This can be anything that can possibly help the research.
    a. **Good Example**: Subject worked at the company for 16 years and was a team lead on a project related to the documents they exfiltrated. Prior to the time of their data collection activity, they were seen looking for new employment outside the organization. Subject has a background in Artificial Intelligence and Machine Learning.
    b. **Bad Example**: John Smith worked at Acme Co. for 16 years and was an AI subject matter expert on the NeuralNails project. Prior to the time of his data collection activity, he was seen looking for new employment outside the organization on his work computer. John has a background in Artificial Intelligence and Machine Learning.



NEW CASE

□ Person under investigation had elevated privileges.

□ Individual was subject to enhanced monitoring at time of incident.

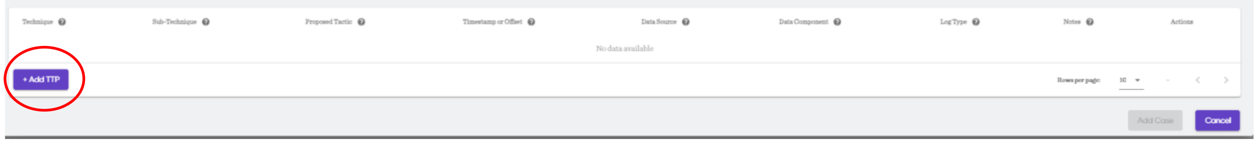
□ Teleworker/Remote Worker

□ Case data submitted on behalf of customer organizations outside your own (i.e. MSSP)

Entering TTPs

Once all the case information is filled out, it is time to enter the TTPs used by the person under investigation.

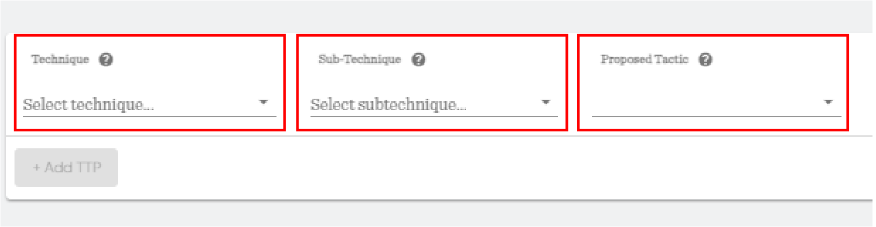
1. Select the purple + *Add TTP* button.



2. Select the Technique and sub-Technique (if available and known) from the drop-down menus. These are the tactics and techniques that best describe the action taken by the insider. Some actions by the Subject may not fit *perfectly* into the definition within the

MITRE ATT&CK® framework. If the action *mostly* fits a current technique, use the existing options. We have included an option to submit a New Technique which this guide will get into later.

3. **Proposed Tactic:** Techniques within the MITRE ATT&CK® framework are already placed under one or more Tactics. We want to understand how people are using these techniques, regardless of whether their actions were intentional or malicious, or their actions were accidental or due to complacency. This information will help us understand where insider threats act similar to APTs and where they might differ.

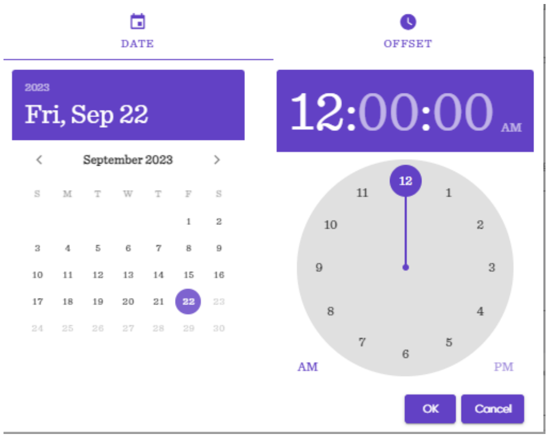


4. **Timestamp or Time Offset:** We want to understand the timeframe and sequencing of each action, as well as the interval between each action. We have included two options for submitting this data.
    a. **Timestamp:** This is the *time* and *date* that each technique was performed based on log data. Time should be normalized to the time zone the actions occurred as opposed to server time, should they be different.
    b. **Time Offset:** Insider threat cases occasionally make news. In order to further obfuscate the organization and subject involved in the case from the information being submitted into the portal, we included an option for a time offset. Calculator.net has a *Time Between Two Dates* calculator that can help with these conversions.
        i. For the first technique, leave the 'Days', 'Hours', 'Minutes', and 'Seconds' to 00.
        ii. For each subsequent technique, set the fields to the amount of time each technique happened *relative to the **first***. For example, if the timestamp of the techniques read:
            1. Technique 1: 2023-09-05 T 13:26:39
            2. Technique 2: 2023-09-05 T 13:33:15
            3. Technique 3: 2023-09-08 T 09:54:06
            4. Technique 4: 2023-09-08 T 10:02:26

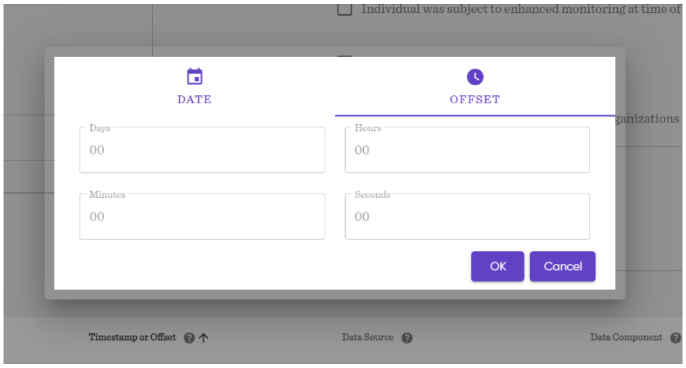
            The Time Offset would be entered as:

            1. Technique 1: Days 00; Hours 00; Minutes 00; Seconds 00
            2. Technique 2: Days 00; Hours 00; Minutes 06; Seconds 36
            3. Technique 3: Days 02; Hours 20; Minutes 27; Seconds 27
            4. Technique 4: Days 02; Hours 20; Minutes 35; Seconds 47

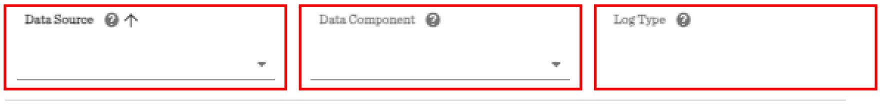
Time and Date



Time Offset

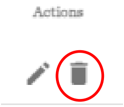


5. Select the data source, data component (optional) and type in additional information about the log type (optional) that corresponds to where the insiders' action was identified. This information can help other Insider Threat Programs better understand how to identify the use of these techniques.

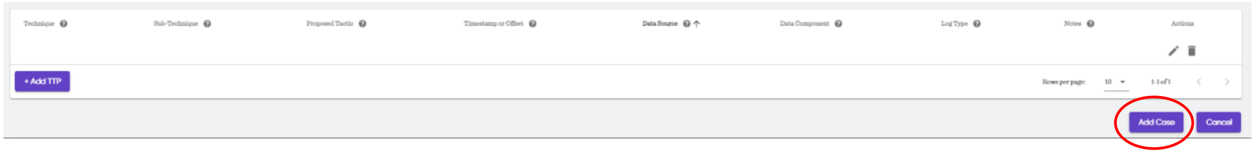


6. Add in any additional notes or details about the insiders' action in the notes box. NOTE: **These notes will not be released to the public and can be seen ONLY by the submitter and the researchers within MITRE.**

7. Add as many TTPs as necessary within each case to give a full picture of the Subjects actions.
8. TTPs can be deleted by clicking on the trash can button.

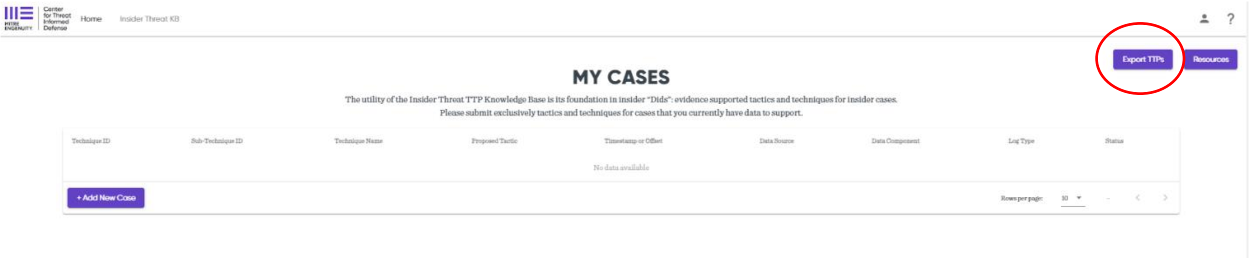


9. Once all case information is entered, select the *Add Case* button to submit the case to the portal.



Exporting TTPs

1. To export TTPs from submitted cases, select the *Export TTPs* button on the right side of the portal.

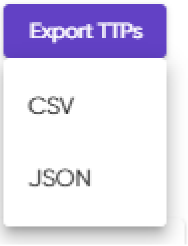


MY CASES

The utility of the Insider Threat TTP Knowledge Base is its foundation in insider "Dids": evidence supported tactics and techniques for insider cases. Please submit exclusively tactics and techniques for cases that you currently have data to support.

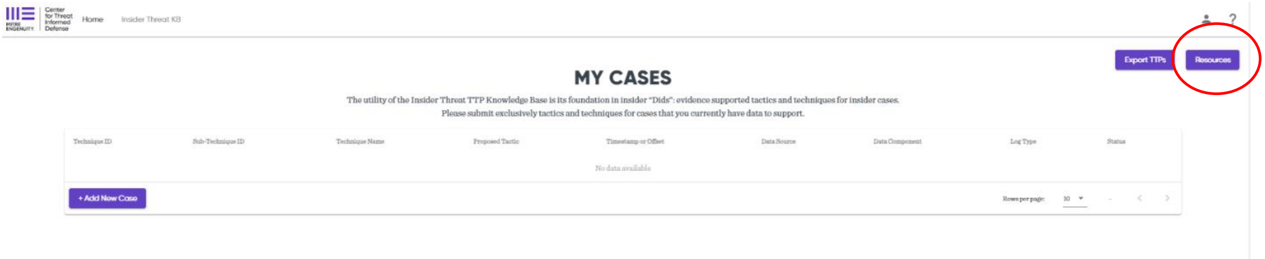
Technique ID	Sub-Technique ID	Technique Name	Proposed Tactic	Timestamp or Offset	Data Source	Data Component	Log Type	Status
				No data available				

2. Choose to download as either CSV or JSON.



Additional Resources

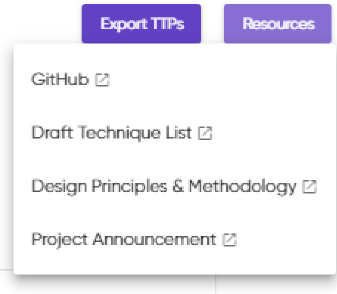
1. To see additional resources, select the *Resources* button to see options for the Knowledge Base GitHub Repository, a Draft Technique List, the Design principles and Methodology paper, and the Project Announcement.



MY CASES

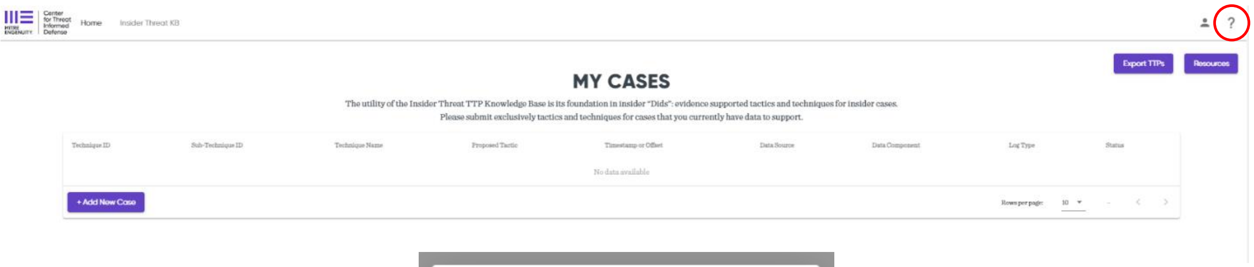
The utility of the Insider Threat TTP Knowledge Base is its foundation in insider "Dids": evidence supported tactics and techniques for insider cases. Please submit exclusively tactics and techniques for cases that you currently have data to support.

Technique ID	Sub-Technique ID	Technique Name	Proposed Tactic	Timestamp or Offset	Data Source	Data Component	Log Type	Status
				No data available				



Getting Help

To get assistance with either submitting cases or portal administration, select the question mark button on the top right of the screen.

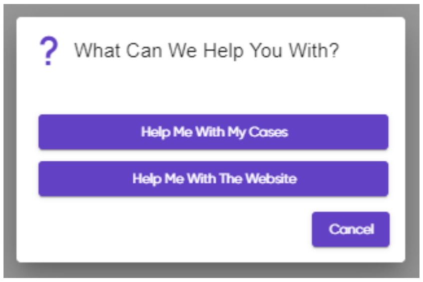


MY CASES

The utility of the Insider Threat TTP Knowledge Base is its foundation in insider "Dids": evidence supported tactics and techniques for insider cases. Please submit exclusively tactics and techniques for cases that you currently have data to support.

Technique ID	Sub-Technique ID	Technique Name	Proposed Tactic	Timestamp or Offset	Data Source	Data Component	Log Type	Status

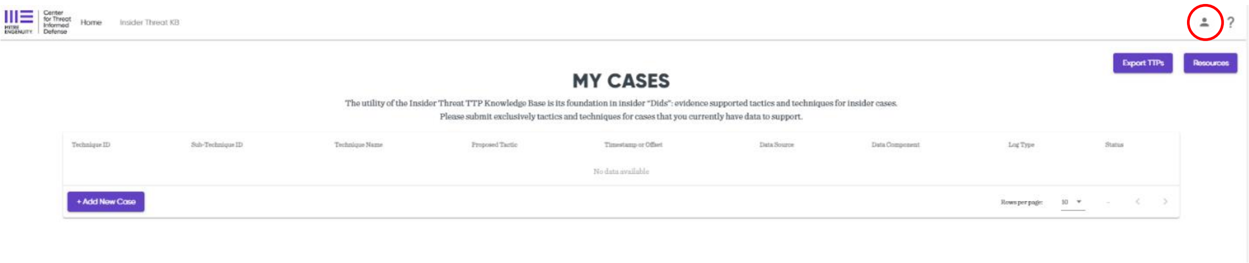
No data available



What Can We Help You With?

Password Changes

1. To change a password if the current password is known, select the profile button on the top right of the screen. This will bring you to your profile.



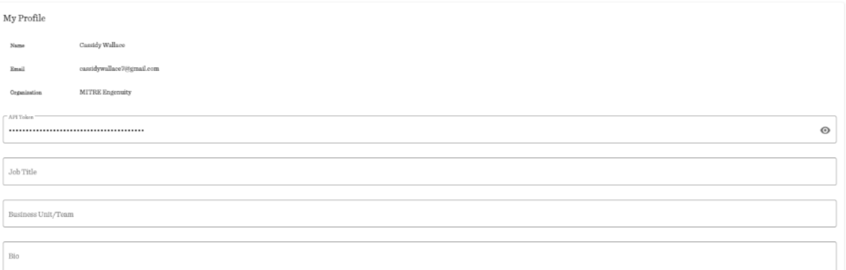
MY CASES

The utility of the Insider Threat TTP Knowledge Base is its foundation in insider "Dids": evidence supported tactics and techniques for insider cases. Please submit exclusively tactics and techniques for cases that you currently have data to support.

Technique ID	Sub-Technique ID	Technique Name	Proposed Tactic	Timestamp or Offset	Data Source	Data Component	Log Type	Status

No data available

2. Click on Change Password to change the account password.



My Profile

Name	Cassidy Wallace
Email	cassidywallace7@gmail.com
Organization	MITRE Engenuity

API Token: ••

Job Title

Business Unit/Team

Bio

Thank you for submitting your case and supporting our research!