Version: 6.3

13 September 2021

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | **F:** +1.703.229.4489
www.ThreatConnect.com

Expanding the Platform

ThreatConnect is a software *platform*, which is a word we take very seriously. A platform is a very special kind of software application: one that you can build out by building other software on top of it. New applications, new interfaces, new aspects of the data. Facebook is a platform. Your smartphone is a platform. And ThreatConnect is a platform.

I talk to many customers who view this platform as a skeleton: the structural support (the bones) onto which they build out their entire security program. Part of our vision is to ensure that this skeleton can support whatever needs to be put on it. That's why our data model is flexible, why we have an API, why we have a software development framework, and why automation is a key component of every customer's workflow.

In 6.3, we're giving customers new ways to adapt that skeleton. We're adding Attribute support to Workflow, which means that SOAR customers can track whatever metadata they need to as part of a Case: business unit, impact types, geography, internal reference codes, etc. The beauty of the model is that it can be anything, but admins also have controls to keep things from going off the rails. We're also expanding our TIP data model to support half a dozen new Group types: from Attack Pattern to Vulnerability.

There are plenty of other features as well,like the ability for SOAR customers to track Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR), but ultimately this release is all about furthering ThreatConnect's goal of allowing our platform to adapt to your processes rather than the other way around.

As always, please feel free to reach out to me with any feedback!

Dan Cole

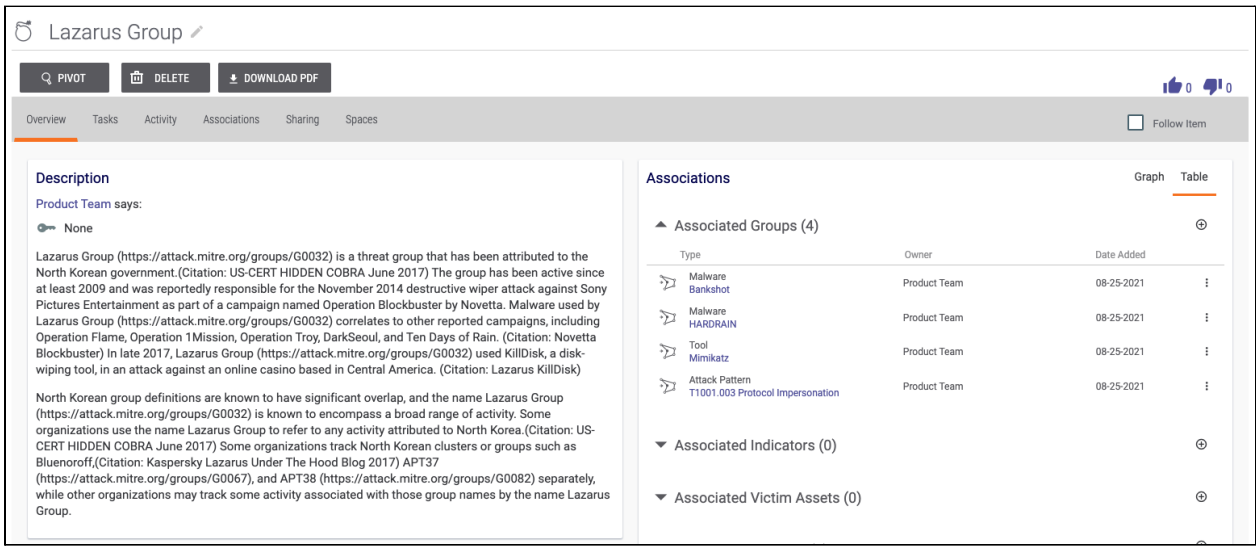
Senior Director of Product Management, ThreatConnect

dcole@threatconnect.com

New Features and Functionality

New Group Objects

With ThreatConnect 6.3, users gain access to six new Group types: Attack Pattern, Malware, Vulnerability, Tactic, Tool, and Course of Action. These new Group types function like existing Groups in ThreatConnect and allow users to map their data in a clearer, more intuitive way. For example, instead of mapping malware family information to Threat objects, users can now map malware family information directly to the Malware object, freeing up Threat objects to be used for Threat Actor Groups or other high-level threats.



Quickly discern if something is a Threat, a Malware Family, or an Attack Pattern.

Instead of wondering if a Group is a Malware family name, a Tool, MITRE ATT&CK Technique, Vulnerability, or Threat Actor Group, users can now quickly see and understand what exactly they are viewing. The release of these new Groups enables ThreatConnect to map to STIX objects more effectively and lays the groundwork needed to expose more data from the ThreatConnect Collective Analytics Layer (CAL™) in the future.

Ultimately, this helps ensure that the threat library you build with ThreatConnect is approachable, organized, and equipped to help your security teams when they need it most.

Workflow Case Metrics

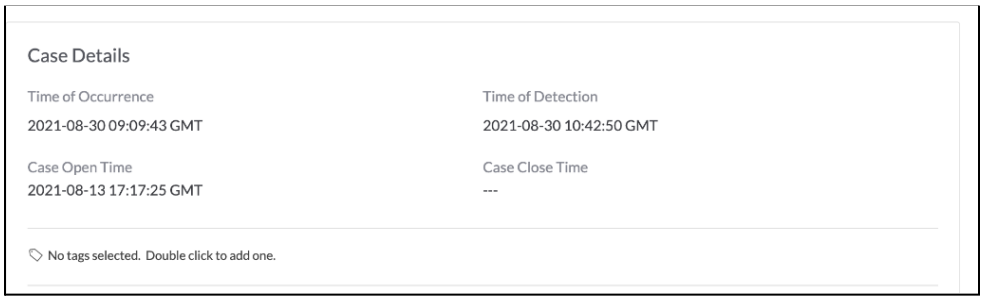
Users can now create dashboard cards on three key performance indicators (KPI):

- **Mean Time to Detect (MTTD)**: The average time it takes to discover a security threat or incident.
- **Mean Time to Respond (MTTR)**: The average time it takes to control and remediate a threat.
- **False Positive Ratio**: The percentage of alerts that upon investigation are revealed to be not valid threats.

Team leads and managers need more granular information about the tools, processes, and people in their environment to define clear and realistic short-term and long-term strategies. These metrics will help users identify whether tools, processes, and automations in place are helping the organization identify and remediate threats faster.

Mean Time to Detect (MTTD)

MTTD measures the elapsed time between the first occurrence of the threat and the time it was detected. Cases now have the option to record the **Time of Occurrence** and **Time of Detection** of the threat for each Case in the **Case Details** section.



Relevant timestamps are displayed at the top of each Case.

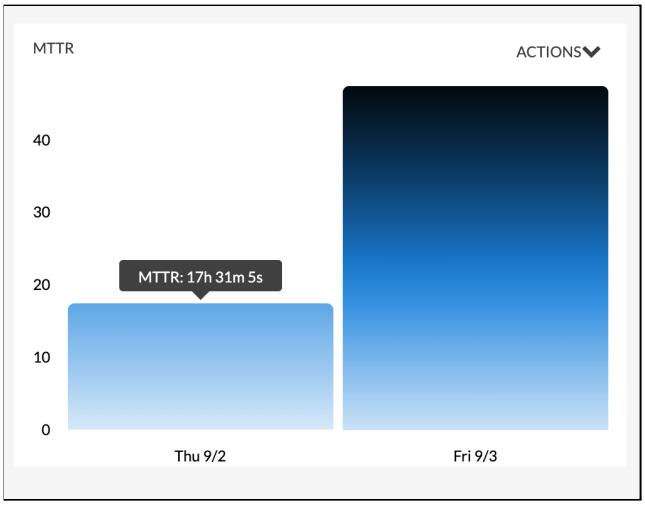
The primary reason behind measuring MTTD is to bring down the lurking threats sooner. MTTD also serves as a way to measure how effective an organization's already adopted tools and processes are at overall defense.

Mean Time to Respond (MTTR)

MTTR measures the elapsed time between when a Case is opened and when it is closed, which shows how quickly a security operations team was able to respond to and remediate a threat. Workflow records the

time a Case is opened and closed and stores it in the **Case Open Time** and **Case Close Time** elements for each Case in the **Case Details** section.

The primary reason behind measuring MTTR is to maximize staff efficiency and optimize the security tools and automation used by a security operations team. This also serves as a metric for how security operations teams utilize their processes and procedures in automated ways to significantly reduce the MTTR within their organizations.

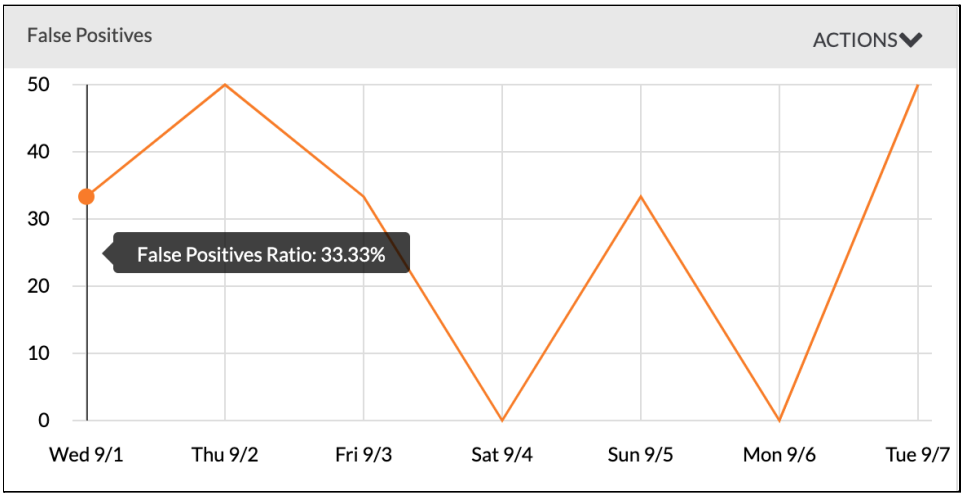


There was a significant difference in MTTR in the Cases closed on the 2nd and 3rd.

False Positive Ratio

While MTTR and MTTD are considered “industry standard” metrics, False Positive Ratio is something unique to ThreatConnect that we hope will help drive teams to optimize and respect their analysts’ time.

The False Positive Ratio is the percentage of the number of Cases created that turned out to be false positives versus those that were true positives. The primary reason behind measuring False Positive Ratios is to know whetherd

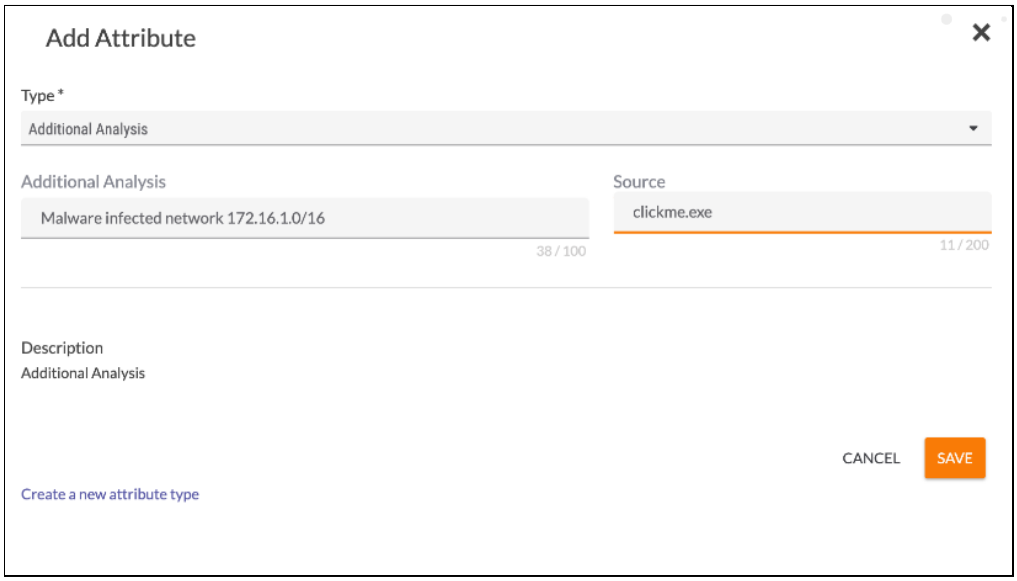


One-third of Cases on Wednesday were false positives.

Workflow Case Attributes

Users now have the ability to create Attributes for Cases. Case Attributes are key/value data sets that can be added to a Case, and they provide an excellent way to organize and categorize Case metadata. Users can add anything of value to a Case, such as relevant research and analysis associated with Cases, the source that triggered an alert, affected network or business units, and recommended courses of action. The sky's the limit. New Case Attributes and their values can be created and managed in the **Organization Config** screen under the **Attributes Types** and **Attributes Validation Rules** tabs. Relevant Attributes for the Cases can be selected and added to a Case by clicking on the "+" icon in the Case's **Attributes** Card.

Template creators can also include Attributes in Workflow Templates. This allows team leaders to ensure that the most important elements needed on a Case are captured.



Personalize Workflow to your needs with Case Attributes.

Improvements

In addition to the new features listed above, we've made a number of improvements to the features users already know and love.

Playbooks

- **Longer App and Operator Titles** - Playbook App and Operator titles will now wrap onto multiple lines allowing users to provide more context as to what each part of a Playbook does without it being truncated in the Playbook Designer.
- **Editable Choice Input** - Playbook Apps now support a new input type: Editable Choice. This new input type enables app developers to provide dropdown selections while simultaneously allowing users to enter values or variables that are not part of the select list, which greatly reduces complexity and increases the user experience for certain Playbook Apps.

Workflow

- Users now have the flexibility to uncomplete a Task in Cases in the event that a Task is inadvertently marked as complete.
- Users can now search for, sort, and filter Cases by Case ID.
- The Case list can now be sorted by Case Closed Date.
- Users can now sort Artifacts by data added when viewing a Case.
- Filtering or sorting options applied to the **Cases**, **Tasks**, and **Templates** screens are now persistent.

Miscellaneous

- System Attributes have been updated to include Attributes supporting the six new Group types.
- Trailing white space will now be trimmed from email addresses when logging in.
- Users can now choose **Select All** when copying data from one Owner to another.
- Users can now delete items via the **Browse** screen even if they have multiple owners selected under the **MY INTEL SOURCES** selector.
- When an Admin user types a value into the **Account Setting** search box and presses the Enter key, the search will now execute.
- On the Threat Intelligence side of the platform, users can now click once and convert a Potential Association into a Direct Association. This improvement establishes consistency between the TI

side of ThreatConnect and functionality that exists in Workflow for converting Potential Associations into Direct Associations.

- The **File Create** window will no longer automatically trim values pasted into the fields to fit the expected hash length.
- ThreatConnect will now maintain consistency with any server keystore file changes and the keystore file persisted in doc storage. This change prevents the Environment Server keystore file from becoming stale, which can cause connectivity issues between the Environment Server and the ThreatConnect instance.

Bug Fixes

API & Under the Hood

- Tags with special characters can now be deleted and/or viewed via the API.
- Fixed an issue that was causing deprecation rules on instances with large data sets to skip Indicators.

Groups and Indicators

- Fixed an issue that was not allowing users to Pivot on Attributes when the Attribute values contained an "&" symbol.
- Addressed an issue that was causing an application error when interacting with the Associations Graph.
- Fixed an issue in the UI that was causing the ThreatAssess Indicator impact information on an Indicator's **Details** screen to be distorted and improperly aligned.
- Corrected a bug that caused the Description and Source attributes of a Custom Indicator to be duplicated anytime the user edited the Indicator.
- Addressed an issue impacting the sort by **Type** column in the **Indicator Association** window accessed via the **Associations** card on the **Details** screen.
- Fixed a bug that forced users to cancel out of the **Group Association** window accessed via the **Associations** card on the **Details** screen when they selected a specific Group type. Users can now go back and view a list of all Group types without having to cancel out of the **Group Association** window.
- Addressed an issue impacting the sort by **Type** column in the **Group Association** window accessed via the **Associations** card on the **Details** screen.
- Users are now able to upload files larger than 5GB via the ThreatConnect API.

Tags

- Users will now be able to delete tags that have "\n" in the name.

Workflow

- Formatting issues in Workflow Notes are now fixed.
- Potential Associated Cases now display properly in Workflow.

- Users were experiencing issues with “My Cases” in Workflow. This has been fixed.
- Fixed an error when sorting Workflow Tasks by Type.

Dependencies & Library Changes

- None.

Maintenance Releases Changelog

There have been no patch releases at this time. 6.3 is the latest version.

Browser Extension 1.1 (Latest)

Version 1.1 is an incremental update for Browser Extension v1. This version works with ThreatConnect version 6.2 or later. Here is a list of minor changes included in this update:

- Users now have the option to **Select All** or **Deselect All** when choosing Indicators to import into ThreatConnect from the Known and/or Unknown lists presented in the Browser Extension.
- The CAL message in the **Settings** menu has been updated for clarity and to look less like an error message.
- Users no longer have the option to view **Threat Rating** and **Confidence Rating** in the Browser Extension. These ratings were coming from an outdated API endpoint and causing confusion because they often did not match the ratings displayed on an object's **Details** drawer or **Details** screen.