RSA NETWITNESS® ORCHESTRATOR
BUILT ON THREATCONNECT™

Version: 6.0

9 March 2020

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

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

A Single Source of Truth for Action

Our users have always valued ThreatConnect as a “single source of truth” for threats. It’s where they put indicators, adversary data, and incident reports, all so that when someone or someSIEM asks, “what do we know about this threat?” the answers are all in one place. In our latest release, ThreatConnect becomes more than just a source of truth for threats: we’re now a source of truth for what to do about them.

Our new Workflow capability lets any team - SOC, IR, threat intel - memorialize their best processes while also providing a platform to take action. That includes case management, phishing triage, malware analysis: if you have a need to get work done in infosec, you can do it in ThreatConnect.

Our vision when we launched Playbooks a few years ago was always to, as psychologist and computer scientist J. C. R. Licklider put it: “**augment human intellect by freeing it from mundane tasks.**” With Workflow, we really bring the human element back into play, with powerful automation and analytics running behind the scenes to help the humans get valuable context when and where they need it to make efficient, accurate decisions.

As always, please reach out to me with any feedback on our new features.

Dan Cole

Senior Director of Product Management, ThreatConnect

dcole@threatconnect.com

New Features and Functionality

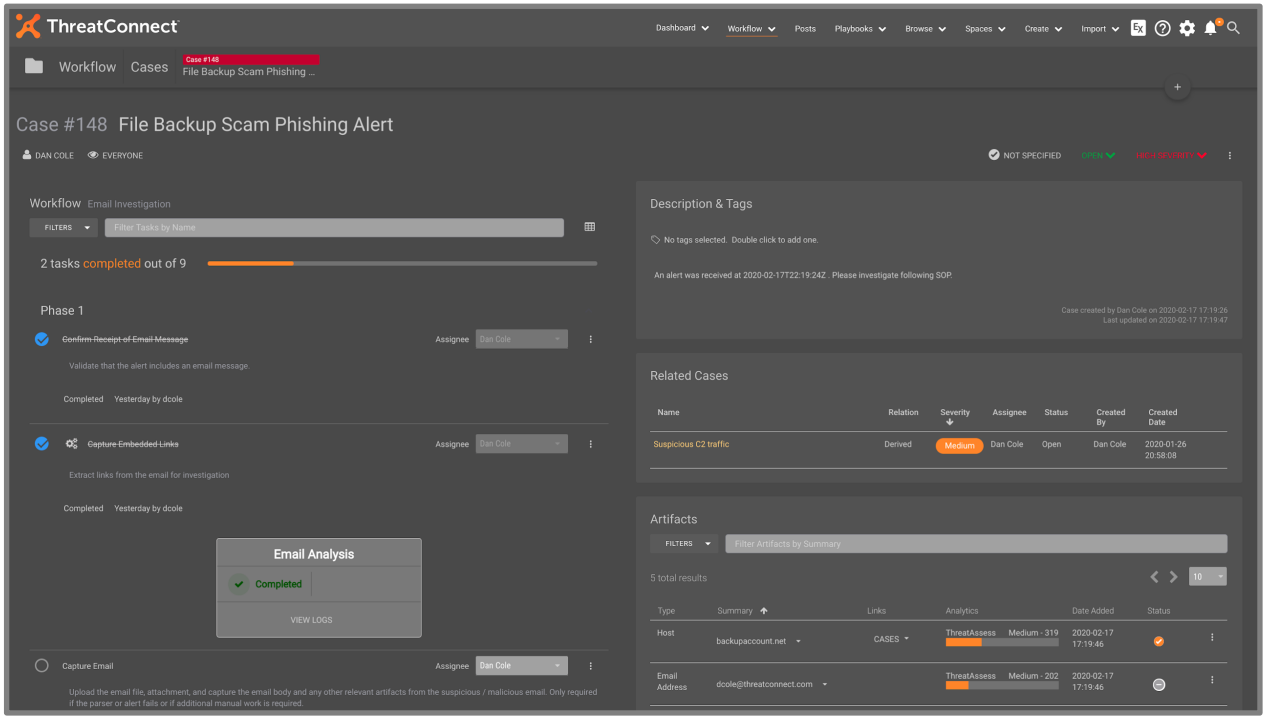
Workflow

The banner feature in 6.0 is Workflow. This new capability lets you combine manual and automated operations to define consistent and standardized processes for your security teams:

- Case management
- Malware analysis
- Phishing triage
- Alert triage
- Intel requirement development
- Escalation procedures
- Breach SOP
- And much more![1]

In other words, processes and procedures you've kept in binders (i.e., runbooks), case management tools, ticket systems, and in your brains can now all be captured in ThreatConnect and tied back to threat intel. In fact, we've designed Workflow explicitly to **reduce the time it takes to uncover relevant threat intel when working a case or investigation**.

[1] Please forgive the cliche, but it's true!



Everything an analyst needs to investigate a case on a single screen.

Here are some terms to keep in mind when working with Workflow:

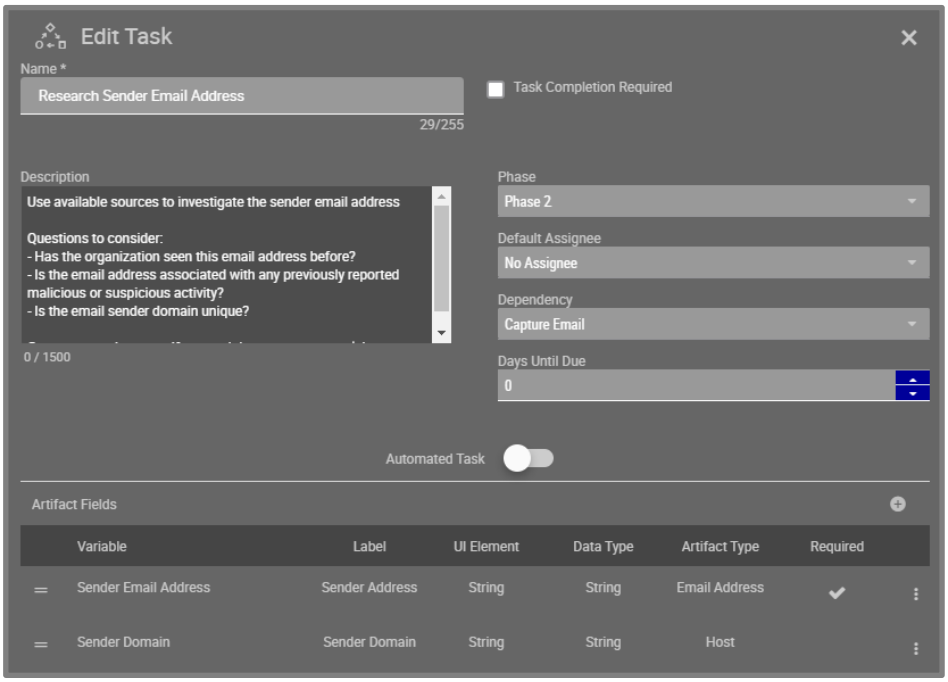
1. Workflow Template - A codified process, typically created by an experienced team member or leader, that's designed to walk a user through that process.
    a. *Examples*: Email Triage Template | Breach Escalation Template | File Hash Enrichment Process Template
2. Case - A single instance of a case or investigation. Users can create Cases on the fly or create a Case from a Workflow Template (recommended).
    a. *Examples*: Case 12345 - Bank Password Reset Phishing Investigation | Case 11111 - Bank Password Reset Phishing Escalation to IR | Case 99999 - Enrichment of File Hash RFI
3. Task - Cases are divided up into individual Tasks a user must perform. Tasks can be Manual (a human user must complete them) or Automated (a Playbook[2] completes the task).
    a. *Examples*: Analyze Packet Capture Data I Review Malware Sandbox Results | Contact Business Stakeholders.
4. Phase - A Phase is simply a logical grouping of Tasks.
    a. *Examples*: Phase 1 includes Tasks to gather email forensic data, Phase 2 includes analyzing that data, Phase 3 includes distributing a report on the analyzed data.

[2] In a future release, you'll also be able to have Apps (ours and yours!) complete Tasks and even take direct action on Artifacts.

5. Note - Users can take freeform notes as part of a Case or even notes that are related to a Task or Artifact.
    a. Examples: “There’s something wonky about this network traffic, I can feel it.” | “Alice, I’m not sure what to do here. Please help.” | “Sure thing, Bob. I added a new Task for you to complete that should help guide you along.”
6. Artifacts - An Artifact is any piece of data not captured in a freeform Note as part of a Case. All Artifacts are saved to the Case.
    a. *Examples*: Email MSG File | Screenshot | PCAP | IP Addresses | File Hashes | Malicious File Attachment

Workflow Templates

Workflow in ThreatConnect starts with the creation of a Workflow Template. These Templates represent the processes you want to define for your team. For example you might have one Template for Phishing Analysis, one for Alert Triage, and maybe several different ones for handling Breaches. By codifying these processes in a Template, you can **reduce the risk of users missing critical steps or artifacts during an investigation**.



Define Tasks for users to follow, including detailed instructions and required data elements.

When creating these Templates, team leaders can:

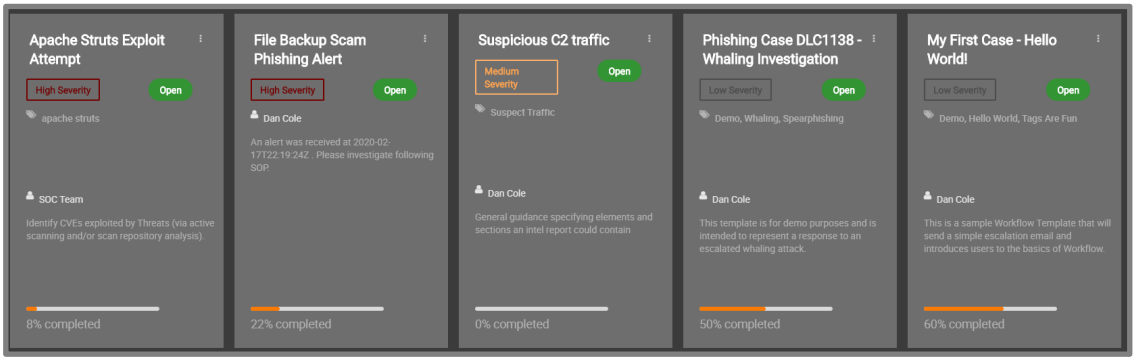
- Create the specific Tasks their users need to complete
- Manage dependencies
- Define the information needed to be collected at each Task

- Incorporate Playbooks that help users get their their Tasks more efficiently

We also provide example Templates through TC Exchange that you can use as educational aids. Templates can also be imported and exported as needed.

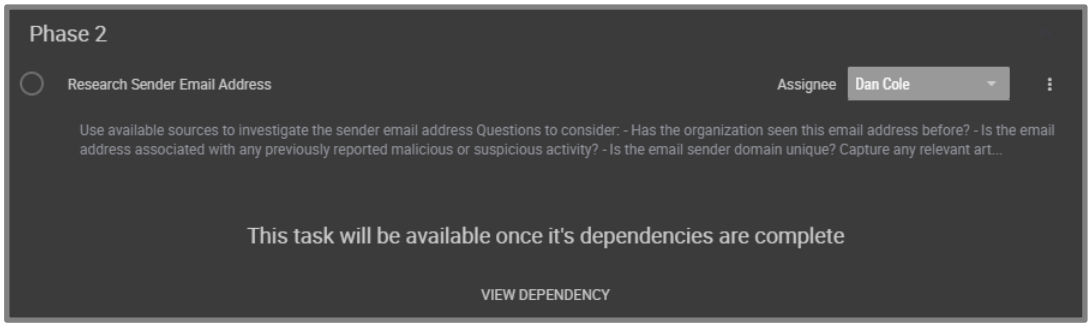
Cases and Tasks

A Workflow Template is the process defined. A Case is an instance of (optionally) using one of those Templates. Your SIEM triggers an alert. Phishing activity is detected. You receive a request for an investigation. An analyst has a hunch. All of these are things that can automatically or manually kick off the creation of a Case.



View Cases assigned to you or the team in Grid or Table View.

Within each Case, users are able to address the specific Tasks assigned to them, run Playbooks, collect Artifacts, and collaborate with their team.

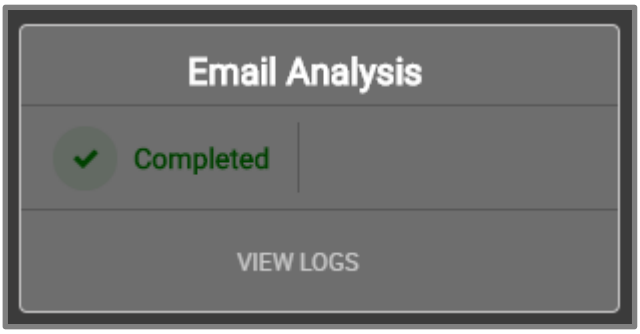


Dependencies defined by team leaders help keep Cases on rails, but enterprising users can also go "off book" and collect additional Artifacts and Notes as they see fit.

Users can manage the assignment of individual Tasks or entire Cases, as well as track status, resolution, and severity.

Automated Tasks (Workflow Playbooks)

Not all Tasks are manual. In fact, the workhorse of your Workflows is likely to be our newly introduced "Workflow Playbooks." These are special Playbooks that can take data from a Case, run it through a series of Apps, and return data back to the Case. For example, an analyst might collect a malicious file and add it to a Case as an Artifact. A Workflow Playbook can take the file, detonate it in a malware analysis tool, and return the results back to the Case as new Artifacts. Alternatively, Automated Tasks can be used to sync important data to other systems, for example separate case or ticketing tools used by other teams.



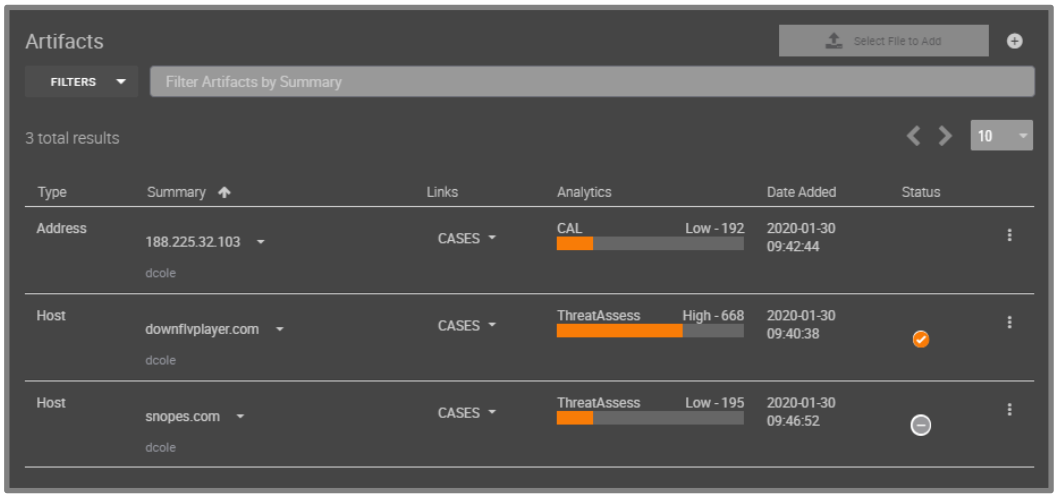
We don't like black boxes, so users working a Case can see what an Automated Task is doing as well as dive deep into logs if they need to, all directly from the Case itself.

Workflow Playbooks can be incorporated into the Workflow Template or added on the fly by the Analyst.

Artifact Management

The Artifact pane gives you a central view of all of the information captured in a Case: emails, files, observables, analysis, forensic data, PCAP files; whatever you want to collect, it's here.

Artifacts that have related threat intel will automatically populate with analytics and the ability to load additional context, including globally crowdsourced context from our Collective Analytics Layer (CAL):



*Embedded analytics reduce the time it takes to **uncover relevant threat intelligence** during an investigation, as well as reduces the risk of spending time on **false positives** and wild goose chases.*

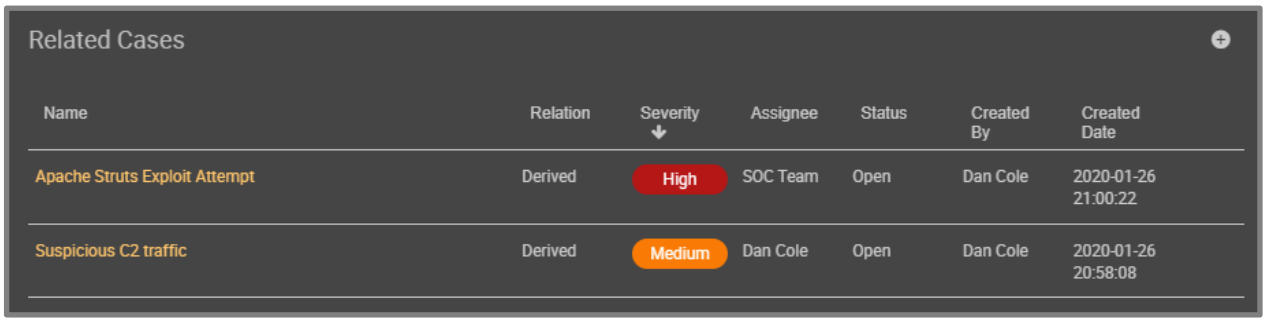
Artifacts can be added as part of a Task, required as part of a Template, or added on the fly. Users can also filter and sort the Artifacts in a Case.

Certain Artifacts can be added directly to ThreatConnect as Indicators so you can leverage them as threat intel in future investigations, which helps you maximize the amount of threat intelligence squeezed from day-to-day operations.

Related Cases

There's a lot of interrelated information in infosec, so to help you out Workflow includes two methods for linking Cases together:

- **Defined** - Users can define that two Cases are related.
- **Derived** - Cases are automatically linked based on having common Artifacts.



We should probably check this out.

Derived links in particular can significantly reduce the time it takes to correlate Cases to historic data and patterns.

Notes

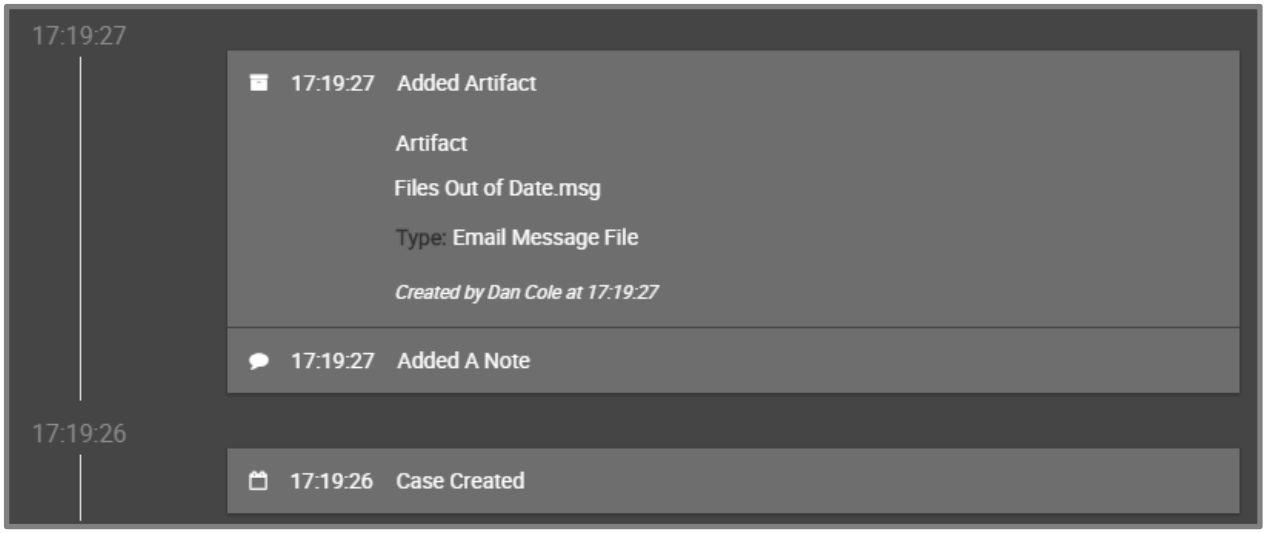
Compared to some of the other features in Workflow it might seem basic, but the ability to take Notes on Cases, and in particular use Notes as a vehicle to collaborate with other team members, is one of the key activities for successful infosec teams.

Notes can be used to collaborate within or across teams.

Users can take notes on Cases, Tasks, or individual Artifacts, as well as @tag other users.

Timeline

The Timeline is a record of everything that happens in a Case.



The Timeline even tracks actions taken as part of an Automated Task.

The Timeline can be searched, filtered, and grouped by time (second, minute, etc.). In addition to the Timeline tracking activity automatically, users can also manually add events to the Timeline.

Workflow API

Workflow introduces the first elements of our new v3 API.

The v3 API was designed in an attempt to leverage a few "lessons learned" identified within the design and deployment of the v2 API. Of particular note, the number of calls needed to make relatively complex setting/getting operations has been greatly reduced and simplified. **TQL filtering** is also now supported, allowing

the user to format, filter, and sort data in a nearly infinite number of ways. The path structure has been simplified as well, having eliminated the need for many levels of nested paths within a given primary endpoint. Finally, error messaging has also been improved in order to better assist the user in identifying and repairing malformed requests.

Additional details, including a breakdown of the new endpoints, are available in our documentation.

Workflow Playbook Apps

In addition to the robust controls provided by the API, we're also including a series of Playbook Apps for managing Cases. We have dedicated Apps for Artifacts, Notes, Tags, Tasks, Timeline Events, and Cases themselves. This makes it easy to tie Workflow into other tools. Creating a Case from another system might be as simple as tying it to an HTTPlink Trigger and then passing information to the ThreatConnect Cases App to create and assign a new Case.

App Services

One of the main use cases of ThreatConnect is the ability to increase collaboration of your tools, i.e. get more software talking to each other. 6.0 extends this use case with a new feature called App Services, which is an always on micro-service that can process requests from an integration, enabling the creation of services like:

Custom Playbook Triggers - Receive push type events over a custom protocol, raw port access, or poll on a configured schedule (e.g.. Syslog UDP listener, Microsoft Graph API, Twitter Stream Subscriber, etc.)

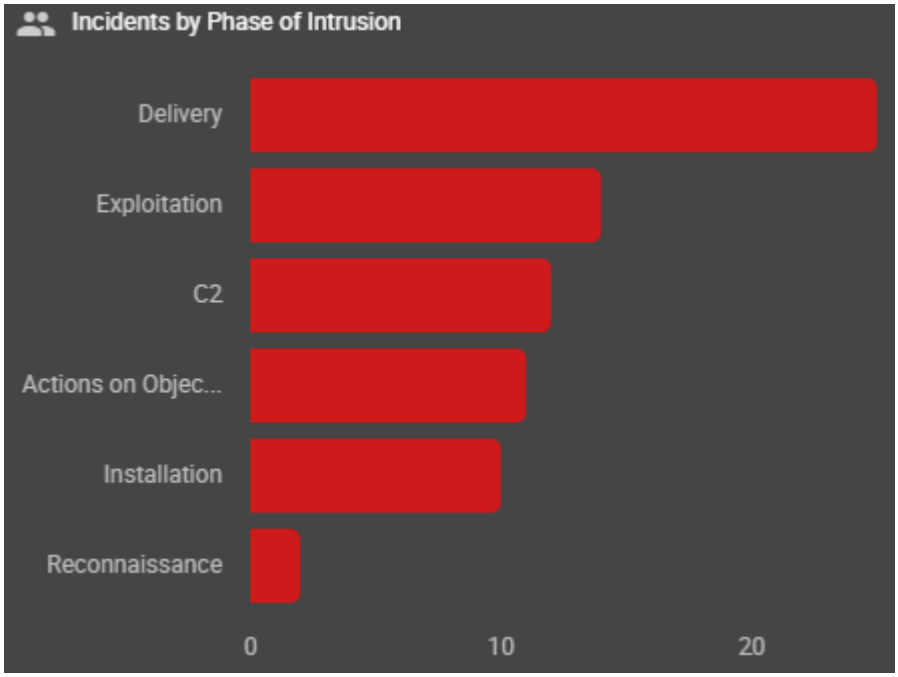
Webhooks - Receive push type events that require normalization or filtering (e.g. Splunk CIM Trigger, Pager Duty Alert Trigger, Slack Event Trigger, etc.)

APIs - Build custom APIs for 3rd party integrations (e.g. TAXII Server, Custom API Extensions, etc.)

We will be using this capability to introduce new integrations like Apache Kafka and McAfee DXL. Users can build their own custom Python services using App Builder or v2.0 of the ThreatConnect® TcEx App Framework.

Improved Dashboard Reporting

Attributes are a flexible method of extending ThreatConnect's data model, but until now you were restricted to the details or query level. In 6.0, you can now aggregate typed Attributes on the Dashboard. This includes our out-of-the-box Attributes like Phase of Intrusion, but also custom ones that you create. This significantly extends the types of information that can be visualized on a dashboard for action. As with many other dashboard cards, this feature also supports drilldown, so in the example below you can click the C2 bar to view the dozen or so Incidents in question.



Create graphs that break down your adversaries by their favorite ice cream flavor if that's your thing. Maybe it helps with attribution, who knows?

For integer-based Attributes, as well as any Custom Metrics, you can also aggregate by MAX, MIN, COUNT, AVERAGE, and SUM.

New Permissions and User Groups

Administrators have two new ways of managing users. **User Groups** allow you to create buckets of users to power Notifications and Task or Case Assignments. So rather than assigning a Task to an individual analyst, you can assign the Task to their entire team (e.g. "SOC Analysts" or "AsiaPac Response Team").

We have also completely revamped how Permissions works in ThreatConnect. Admins can create their own custom user roles and apply the same set of permissions across all users assigned those roles (e.g. "Playbooks Designers" or "Analyst Interns"). We've also added dozens of new permission controls that you can use with this new framework, including controls for who can Modify and Activate Playbooks, as well as which users can execute User Action Playbooks.

Finally, for users working a Case in our new Workflow feature, you can restrict visibility on a per Case basis to individual users, which is useful when working with highly sensitive data.

Improvements

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

Administration

- Administrators can now add Read Only users directly from the Account Settings page.
- We have made several changes to TAXII logging, including adding counts of found versus saved Indicators in the UI log.

API

The following functionality has been added to the ThreatConnect v2 batch API:

- Attribute Append
- Tag Append
- Security Label Append
- Attribute Source

Data Model

- As with every release, we've updated some Attributes and refined the default system-level exclusion list.
- ThreatConnect now supports Sigma signatures, which are very popular when working with the MITRE ATT&CK framework.
- In support of certain integrations, we now support Email Subjects and Hashtags as Indicators.
- We now keep track of which user created a particular Group. This allow users to:
    - Perform TQL queries by creator
    - Create dashboard cards aggregated by creator
    - View the creator in dashboard datatables

Playbooks

- The Playbooks Timer Trigger now supports standard Quartz cron expressions, allowing users to create much more granular timer triggers.

UI

- We've added a button to the Browse screen () that allows users to open the Details page in a new tab with a single click.
- Tag Weight was causing confusion and has been removed.
- Minor text changes were added for additional clarity in the UI.
- The Created Before filter now appears after the Created After filter on the Browse Screen, reflecting these two parameters' function as a "between" or "range."

Under the Hood

These are improvements that, while not directly visible to front-end users, are working behind the scenes to improve the ThreatConnect experience. Many are also available to ThreatConnect developer users for building new and improved applications.

- Email Import size limit changed from 4MB to match the system limit.
- Added several validation checks on user names.
- Made improvements intended to reduce excessive logging in certain areas of the platform.

Bug Fixes

Administration

- Community Invites now support users who did not previously have a ThreatConnect account.
- Fixed an issue that was causing Source and Community Owner permissions to be reset when saving Source configuration.
- Users on instances that use SAML were getting an error when creating a new file variable. This has been fixed.
- System Health Checks now work properly on HANA instances.
- TC Exchange now recognizes the default Owner when configuring app delivery.
- Admin users were having some trouble clicking the upper right dropdown in Org Settings. This has been fixed.
- Environment Servers will now correctly update new apps at runtime.
- Fixed an issue that was causing Feed Apps to not be deployed to the correct owner.

API

- Registry Key indicators can now be created through the API.
- Fixed an issue with the bulk import API that caused it to error out when performing an import with a tag lookup.

Indicators & Groups

- Uploading a Signature with a different file name will now correctly update the file name even if the content of the Signature hasn't changed.
- Fixed an issue that was preventing users from re-rating Indicators.
- Users should no longer get stuck when adding a new Indicator association to a Group via the Details page.
- Attributes now handle line breaks properly.
- Items with multiple security labels will now only appear once in the Browse screen.

- Security Label activity will now correctly create Activity Log entries for Groups.
- Deleting a Document or Report will now include the name of the Document or Report in the delete dialog.

Playbooks & App Builder

- Custom Playbook Apps now support full logging instead of just showing the first 100 entries.
- HTTPlink triggers will now return variable values in the response body instead of the variable names.
- Components now properly use the Run As users from the calling Playbook.
- The Array Operations Playbook App should no longer duplicate its outputs.
- Users variables now export properly in Components that use keychain variables.

Miscellaneous

- The Follow Organization Posts checkbox now saves correctly.
- Fixed an issue that was causing Documents to not be pulled in from some feeds.
- Using different cases for Tags should no longer create duplicate Tags.

Dependencies

ThreatConnect v6.0 requires updates to the following software:

- Redis v5.0.x
- JDK 11
- ThreatConnect® TcEx App Framework version 2.0

Administrators who create new (or re-download old) Environment Servers will need to ensure they're running Java 11. Existing Environment Servers will continue working on Java 8.

Maintenance Releases Changelog

The changelog below contains ThreatConnect improvements and bug fixes introduced in maintenance or revision releases.

There are no new changes. 6.0 is the latest release.