Version: 6.2

21 June 2021

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

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

Teams and Tools Collaborating Together

In a way, ThreatConnect 6.2 is all about collaboration. When we think of "collaboration" we usually think about groups of people working together, maybe from different teams, to achieve a common goal. In cybersecurity, that may mean the threat intelligence team provides much-needed context to the SOC, or the SOC team feeds telemetry back to generate new intel. ThreatConnect 6.2 covers that use case, but there's also so much more to *collaboration*.

The word comes from the Latin, *collaborare*, which means "to work with," to work together; it's the same root as labor. Co. Labor. The thing is, it's not just people who work together. Software can work together, too, like when a detection rule is sent to the SIEM, which triggers an alert, which queries some data, which initiates a block action. Humans with humans. Humans with software. Software with software.

6.2 gives our customers access to our new browser extension, which allows anyone on the security team to benefit from rich, contextualized threat intelligence from any web page or SaaS tool. If your SOC needs intel in the moment of an investigation, this is it: next-level collaboration between intel and ops. 6.2 also includes a total revamp of our Playbooks capability, giving you more power and flexibility to get your tools talking to each other: it's collaboration via automation. Interactive Playbooks allows anyone on the team to get up and running collaborating with another Playbook builder.

Using a platform like ThreatConnect and changing how security works starts by creating a foundation of collaboration between teams and tools, and ThreatConnect 6.2 makes it easier than ever. We're looking forward to collaborating with you on the next phase of your ThreatConnect journey!

Dan Cole

Senior Director of Product Management, ThreatConnect

dcole@threatconnect.com

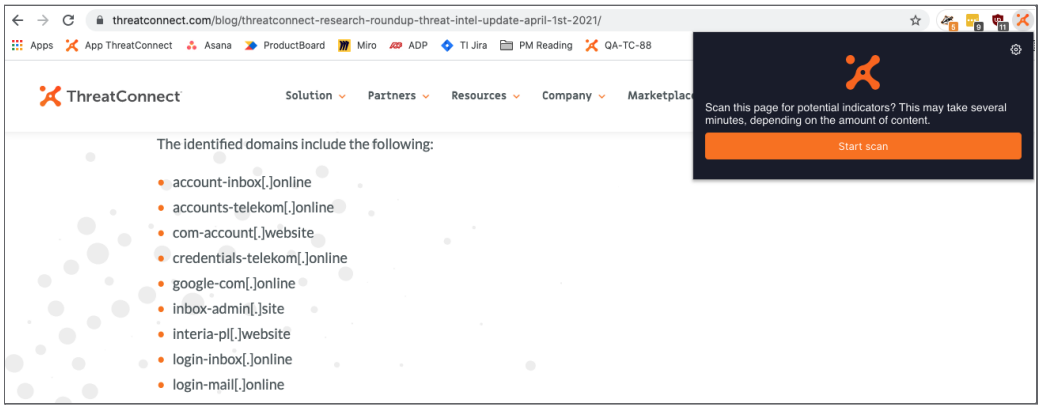
New Features and Functionality

ThreatConnect Browser Extension

The ThreatConnect Browser Extension expands the functionality of the ThreatConnect Platform to enable users to query their ThreatConnect instance without having to copy and paste indicators into the Search field or manually enter indicators in Search or Browse.

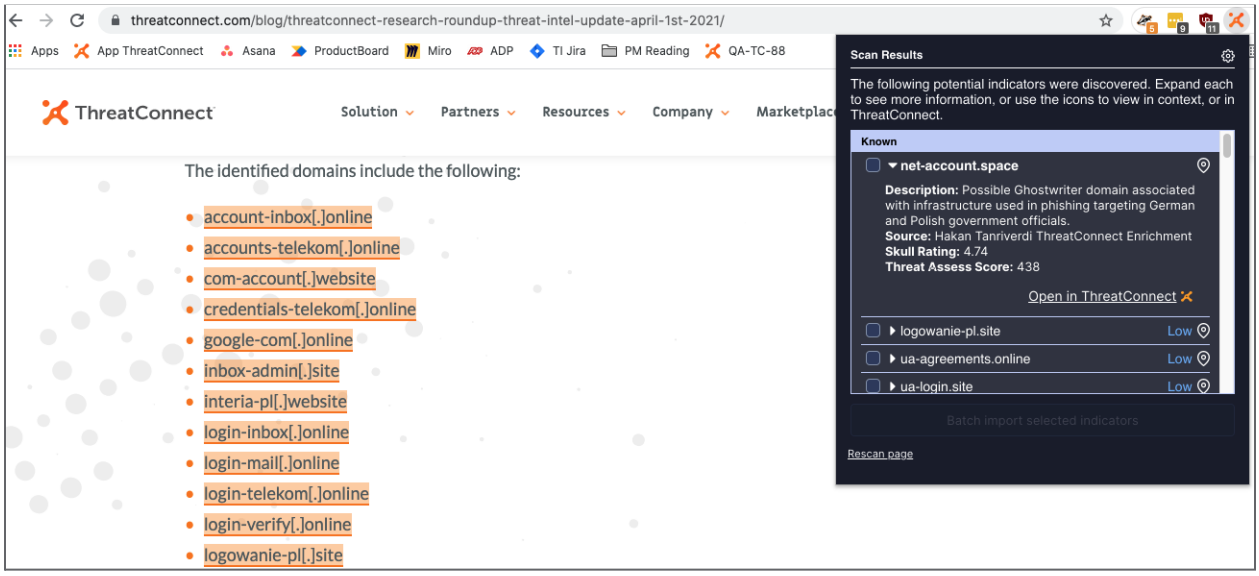
The best part? The Browser Extension can function as a *generic integration point* between the ThreatConnect SOAR and any SaaS-based product.

At the touch of a button, users can scan a web page for potential indicators and see what ThreatConnect knows about those items.



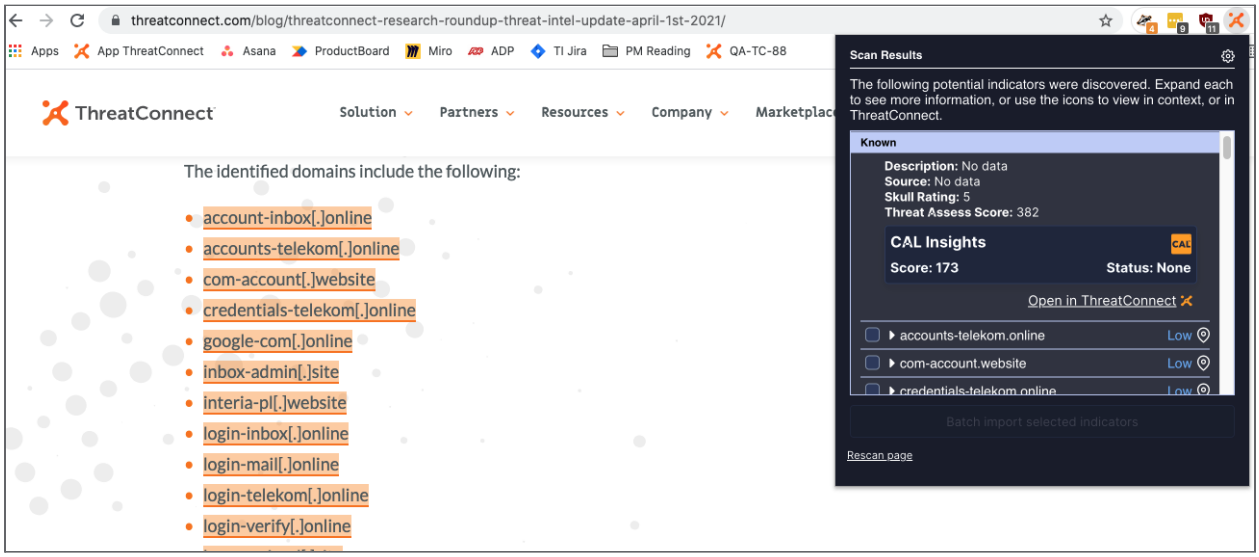
Scan webpages in Chrome and Firefox

Get contextual information about the indicators, view the ThreatAssess Score, and more!



These indicators are known to this ThreatConnect instance

Browser Extension users can also choose to return results from ThreatConnect's Collective Analytics Layer (CAL). This gives them some information about indicators that may not exist in the Sources and Owners in their ThreatConnect instance. Additionally, users can view Observations, Impressions, and False Positives reported in the Browser Extension. This can help them determine whether an indicator is relevant to or impacting their organization specifically.



See CAL insights and the CAL score in the Browser Extension!

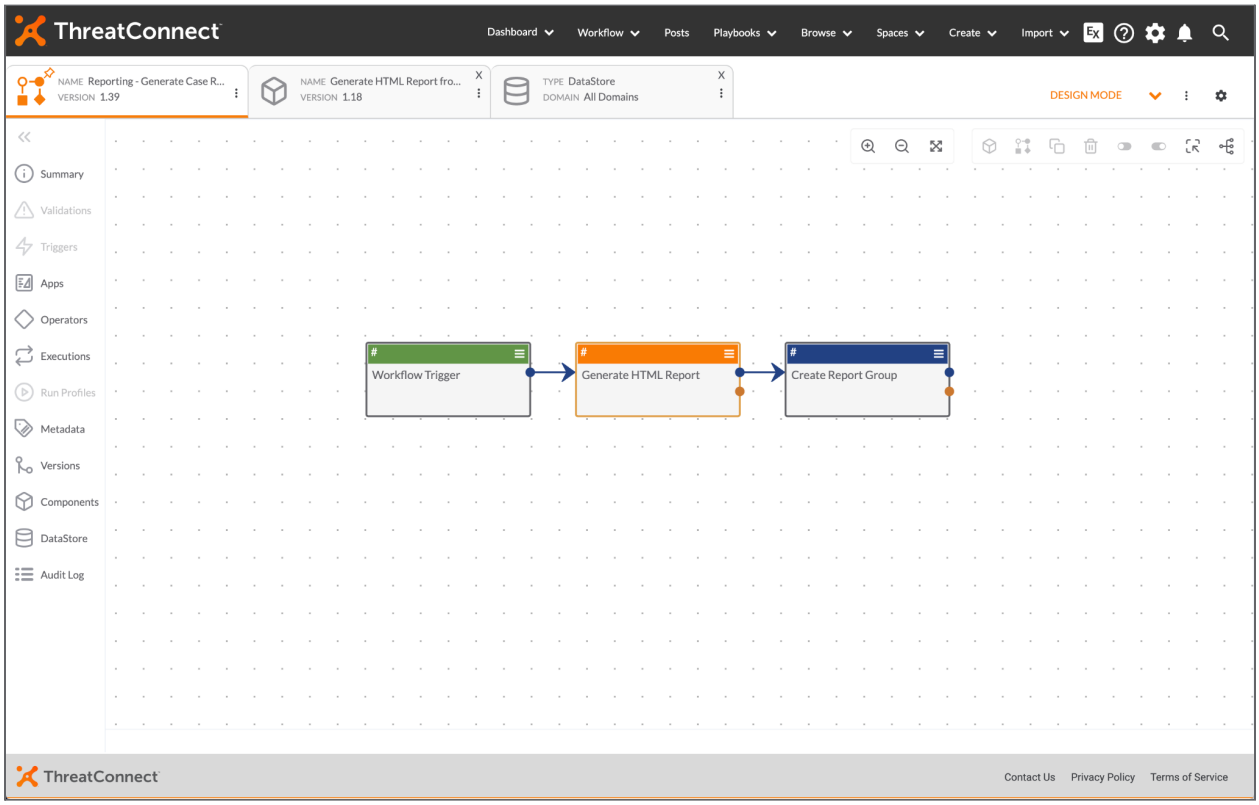
The Browser Extension works with any existing ThreatConnect customer account, so install it from the Chrome or Firefox app store alongside 6.2 to customize it and get started right away!

Playbooks 2.0

A complete revamp of our Playbooks functionality, Playbooks 2.0 takes the power and flexibility of Playbooks to new heights. Users will find a familiar but vastly improved user experience and powerful new features for building, troubleshooting and collaborating around Playbooks.

Look and Feel

One of the first things you'll notice is the new look and feel of the Playbooks Designer. With a new side navigation and tabbed layout manager the Designer is now more organized and user friendly. Everything you need to build, collaborate and support a Playbook is just a click away.



Simple and clean.

- **Maintain Filters on Playbooks List Page** - The Playbooks listing page will now maintain the filter state between sessions so a user can now set their filters to match the Playbooks they care about, leave the page, and see the same filters and results when they return. Now you can set your filters to what you care about once and know they will be there when you return.

- **Designer Side Navigation** - The new side navigation brings all the things related to building a Playbook together in an intuitive and accessible menu. To save even more space, it can be collapsed down to icons only. In addition to some brand new features, the following existing features have been consolidated and moved to the new side navigation:
    - Summary & ROI
    - Validations
    - Triggers
    - Apps
    - Operators
    - Executions
    - Metadata
    - Versions
    - Components

- **Tabbed Layout Manager** - Now when you open up certain Playbook features such as Components or Executions they will open in a new tab on the Designer. No more having to switch between browser tabs or remembering where you left off! The Tabbed Layout also maintains a users state between sessions; for example, if you stop working on a Playbook with six tabs open, you'll see those same six tabs when you return to it later.

Playbooks Designer Improvements

- **Rename HttpLink Trigger references to WebHook** - The HttpLink Trigger has been renamed across the UI to Webhook Trigger in order to better reflect its intended purpose.
- **Editable WebHook Trigger URL's** - Webhooks are wonderful, but long universally unique identifier's (UUID) in the URL path make them hard to identify. Users can now provide a custom path for their WebHook Trigger URLs making it easy to understand a WebHooks purpose.
- **New Global Variables** - Users can now utilize a new Global scoped Variable which is available anywhere in the Playbook. These variables can be set, updated and referenced anywhere in the Playbook, even inside nested components and iterators. This eliminates the need for the Merge operator in many cases and provides an easy way to track settings, counts, and other important information throughout a Playbooks execution.
- **View Parameters on Active Playbooks** - Users can now view App configuration parameters while a Playbook is active. You no longer need to deactivate a running Playbook to view its configuration. .
- **KeyValue List Ordering & Editing** - Users can now change the sort order of KeyValue lists throughout Playbook Triggers and Apps. No more re-creating variables just to change the sort order. Additionally, you can also now edit KeyValue lists inside Component and Workflow triggers.
- **Realtime Design Validations** - Users will now see Validation errors in real time as they make changes to their Playbooks. In prior versions, validation occurred when activating a Playbook. Now

users will see warnings in real time enabling them to address issues immediately and with the context of what they just changed.

- **Designer Audit Logging** - Users can now view an Audit Log of all Playbook changes. Ever wish you could see who changed a Playbook you were working on or what happened to an App that is no longer working? Every change to the Playbook is now logged and can be viewed and searched in the new Audit Log making it easy to know what happened, when it happened and who did it.
- **DataStore Explorer** - The new DataStore Explorer gives users the ability to interact with DataStore via the UI. Previously the only way to interact with the DataStore was through the DataStore Playbook app. Ever wish you could upload a CSV file or POST JSON data and reference it as part of a Playbook? Now you can do this easily in the UI and have your Playbook reference the data during execution. For instance, you could upload a CSV of internal IP ranges and reference them for decision making inside the Playbook.
- **Run Profiles on Triggers** - Users can now set up Run Profiles as a way to easily trigger a Playbook execution in a repeatable manner. Run Profiles allow a user to define the trigger outputs that are available to the Playbook and then use that profile to test the Playbook end-to-end in Active Mode or as a starting point for the new Interactive Mode (see below).
- **Playbook Failure Notifications** - We know that Playbook failures can be frustrating to diagnose. To make it easier, users can now set a notification email address for notifications when a Playbook fails for any reason. Log files can be included (optional).

Playbooks Management (Import, Export, and Sharing)

- **Playbook Sharing using Share Tokens** - Users can now share Playbooks using nothing more than a sharing token. No more keeping track of PBX or PBXZ files. Just copy the sharing token and send it to another user. When they enter the token they can download the shared Playbook from a new sharing server.
- **Playbook Zip Bundle Migration** - Goodbye PBX and hello PBXZ. Playbooks will now be exported as a PBXZ file containing the PBX file along with additional resources like a PNG preview image, debug execution logs and more.
- **Full Modernization of the Playbooks UI -** The Playbooks UI was updated to use the latest technologies and now supports a more robust user experience in areas like the Import and Export Wizards.
- **PNG Image with Playbook PBXZ Export** - There is now a PNG image of the Playbook exported as part of the PBXZ package. This PNG is used when importing a Playbook manually or through Sharing tokens.
- **PNG Preview on Playbook Import** - Users will now see a PNG preview of the Playbook during import. This provides validation they are importing the Playbook they expect and a chance to cancel if not.
- **Improved Playbook Import for Service triggers** - Users can now select which Service they want to use on import when more than one of the same type of Service is configured.

Select Actions

- **Build Component/Workflow** - Users can now select multiple Apps and Operators inside a Playbook and build them as a Component or Workflow Playbook. This makes it easier for users to create new components that can be reused inside other Playbooks.
- **Clone Apps** - Users can now select multiple Apps and Operators and clone them inside the existing Playbook instead of having to copy each app individually.
- **Disable Apps & Triggers** - Users can now select multiple Apps and Operators and disable them from executing as part of the Playbook. If you're used to coding, this is like commenting out a line of code!
- **Improve Selection Tool and Ghost Selections** - We improved how selections work to be more descriptive of the selected apps and expanded what you can do with them in a simple to use toolbar.
- **Keyboard Shortcuts** - Users can now interact with Playbooks using almost 40 new Keyboard Shortcuts. A reference guide is available from the vertical ellipsis menu in the Playbook Designer.

New Execution Navigator

The Execution Navigator has been completely redesigned to take advantage of tabbed layouts and to make it easier to step through a Playbook execution. Users will now be able to open each execution in a new tab and visualize the steps a Playbook took.

- **Download All App Log Bundle** - Users can now download a bundle of log files containing the execution logs for every app in a playbook. Previously, users would have to download each app's logs individually.

Component Improvements

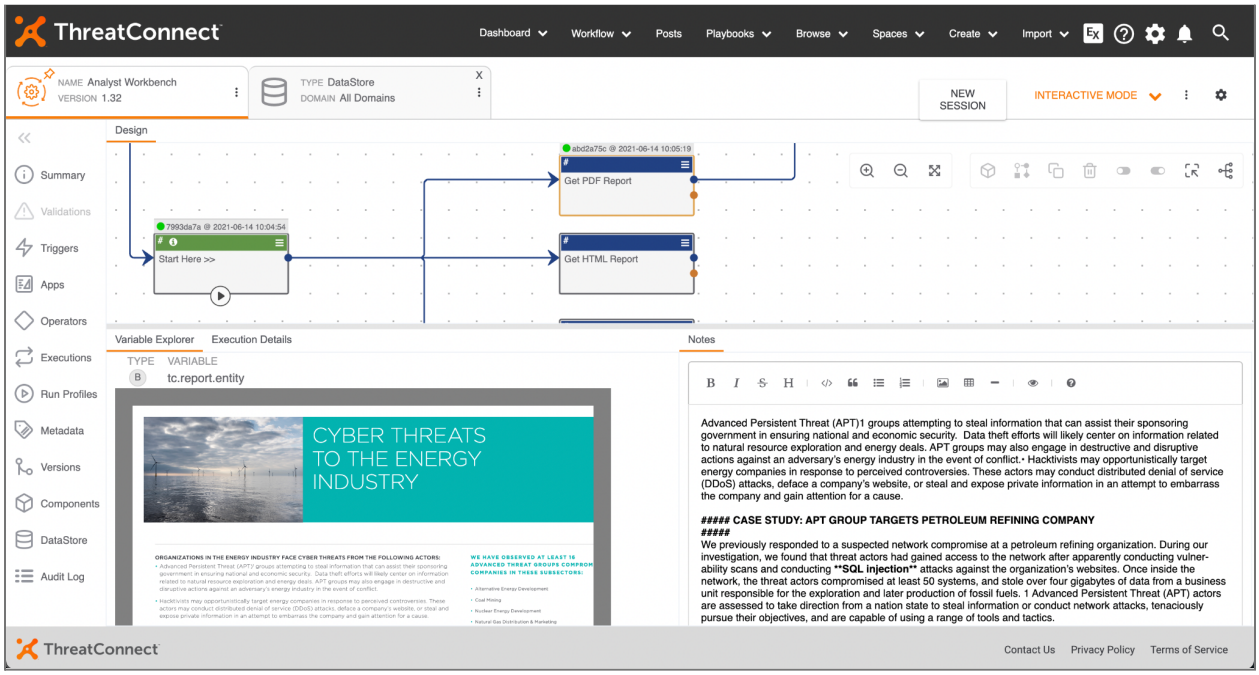
- **Editable Components When Referenced by Active Playbooks** - Users can now edit Components even when they are being used by an active Playbook. No more turning Playbooks on and off!
- **Revamped Component Trigger Input** - The Component trigger input editor has been completely reworked based on the App Builder parameter editor. Users will now see a familiar and more intuitive interface for editing Component triggers.

Miscellaneous

- **Add filter on TC Exchange Settings page** - Users can now filter apps in TC Exchange by Status, Proxy and Remote filters, making it easier to find the apps you're looking for.
- **CPU Based Fork Pool Sizing** - We've added more robust support for Playbook branching. Now the Playbook engine will scale with server hardware and reduce the risk of blocking for Playbooks that have a large number of branches.
- **Recreate Environment Server Keystore when Server Keystore Changes** - Fixed an issue where updated certificates wouldn't update in the bundled Environment Server.

- **Background Workers** - Fixed a design limitation where App Builder debug sessions would consume a worker. Now all App Builder and Interactive Mode sessions will offload to background workers, while allowing Playbook workers to only process live Playbooks.
- **App Builder Export/Import Support for Structured Directory Zip** - New ABX2 format generates a project zip file with a full directory tree making App projects usable outside of App Builder.
- **Playbook Audit Server Logging** - Users can now see System Audit Log entries for changes to Playbooks like deleting, activation, and sharing. Changes to mission critical Playbooks can now be tracked via Server Audit Logs.
- **Improve regex pattern matching on app parameter loading** - App editing and loading performance has been improved

Interactive Playbooks



Reduce frustration and allow anyone on the team to leverage Playbooks for automation and analysis.

The banner feature of Playbooks 2.0, Interactive Playbooks is a brand new way of interacting with and collaborating around Playbooks. If you're familiar with Jupyter Notebooks: Interactive Playbooks is Jupyter Notebooks for Playbooks! If you're not familiar, Interactive Playbooks gives users the ability to do the following:

- **Exploratory Analysis** - Users can now view the results of running an app in-line without running a full playbook. Every app runs as a self contained unit of work that can be edited and checked for output at any time during a session. This new mode is superior to testing playbooks end-to-end because it enables exploratory debugging and data analysis.
- **Data Cached in Variable Explorer** - Users will now see the state of each app with the variable explorer. After each trigger or app execution, the variables are cached in the playbook session with outputs. Every execution will update the variables in the cache and the session will automatically be saved. Each variable is also exportable for tools outside the platform. For instance, users can download an app that extracts a malware file for analysis in an external sandbox environment.
- **Visualize Data** - Interactive Mode has support for multiple content types used for Playbooks. The variable explorer will automatically detect JSON content and render it with syntax highlighting or a user can choose to switch to the new table format and the JSON data will be converted to a tabular

view. Additionally, there is now support for HTML, PDF and several popular image types which will be rendered for the user in the Playbook designer.

- **Collaborate with Notes** - Users can now develop Playbooks collaboratively with notes. Each trigger and app in interactive mode can be marked up with notes and then shared when the playbook is exported. Notes are a great place to explain the app logic, results, and analysis. With markdown support, the notes section provides a living document for each playbook.
- **Improved Troubleshooting** - Interactive Mode isn't only for building and analyzing data in Playbooks. Playbook executions that are in trace or debug logging mode when they fail will automatically get trapped as an interactive session. Users can then investigate the failed playbook as an interactive mode session. All session state information at the time of the failure can be reviewed and analyzed for root causes.

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.

Workflow

- Users can now complete Case Tasks via the API.
- Users can now specify a field name for an Artifact via the API.
- Users can now use an existing Artifact to complete a Case Task.
- The UI for Case Assignments has been improved to better support organizations with hundreds of different Users.
- Artifacts can now be tied directly to a Task without the Task needing a dedicated Artifact field.
- Case Task fields will now autosave. Bye bye, Save button!

Miscellaneous

- Markdown now supports fenced in code blocks, which will make it easier to copy and paste.
- ThreatConnect now officially supports Microsoft Edge!

Bug Fixes

Administration

- Importing Attributes in system settings will now import the Attributes with the correct case.
- Organization Admins can now save IP Login and Playbook IP filters.
- An issue with the User Groups filter in Org Settings has been resolved.
- The System Info tab should now load more quickly on large instances.

API & Under the Hood

- Fixed an issue that was causing App Services to stop working in certain situations.
- The v3 API will now properly return Tags from outside the current Organization.
- The API was not returning the owners for file indicators when queried in lowercase. This has been fixed.
- Fixed a default replica setting in ElasticSearch due to a change in defaults with the recent ElasticSearch version upgrade.

Groups and Indicators

- Fixed an issue that was causing an error when trying to view Feed Report Card data on a feed that didn't have CAL data.
- Fixed a UI error that was occurring when viewing Groups or Indicators across multiple Owners.
- Fixed an issue that was causing users to need to refresh the page when adding multiple Indicators to a Group.

Import & Export

- Using batch import to create multiple copies of the same Group will no longer result in duplicate XIDs.
- Existing Indicators will no longer display twice when being Imported.
- Users are now warned when attempting to import an improperly-formatted CSV via Structured Import.
- Fixed an issue that was preventing users from exporting Indicators in certain situations.

Playbooks

- Playbook display notes can now be **bolded** in Chrome running on MacOS.

Workflow

- Fixed an issue that was causing Case Associations to show up twice in the Case Timeline.
- The Cancel button will no longer be partially hidden when creating an Automated Workflow Task.

Dependencies & Library Changes

- Wildfly has been upgraded to version 22.

Maintenance Releases Changelog

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

2021-07-13 6.2.1 (Latest)

Improvements

- The syslog stream from ThreatConnect can now be encrypted. This may be useful to some customers sending those logs to a SIEM. Unencrypted syslog streams are no longer supported.
- Users can now create dashboard cards to view a team's unassigned Cases. This is very helpful for team leaders who want to make sure that nothing falls through the cracks.
- Improved performance when Artifacts were sorted based on ThreatAssess score.

Bug Fixes

Administration & User Management

- Feed Explorer remained in Light mode even if Dark mode was set in the user's profile. This has been fixed.
- No Feeds were displayed when toggling 'Display only active feeds' to off in Feed Explorer. This has been fixed .
- Fixed an error when "Display only Group Members" was selected in Groups in Org Settings.
- Users were not able to delete Organizations if the user's notification settings were changed. This has been fixed.
- Occasionally Users were not able to delete Organizations when more data is added to the Case in a different Organization. This has been fixed.
- When a new source is selected to be added to an Organization, Users are not able to see the selected source as a tagged list. This has been fixed.
- Inconsistency between displayed and configured custom Attribute length has been fixed.
- Failure to login to ThreatConnect will now produce a more generic error message to protect against username harvesting.
- TAXII service was not shown as an option when creating a TAXII User. This has been fixed.

API / Under the Hood

- API users can now report Observations only if their permission level is set to include it.
- While doing batch import, Users were getting error messages when the Date Added field ended up as null in certain Indicator-Group associations. This has been fixed now.

- Running setup.sh as a ThreatConnect user was not saving SMTP authentication details. This has been fixed.

Browse

- Users will now be able to delete any Object with any Associations.
- Fixed an error when exporting Indicator data in CSV format.
- Sigma format type was not present as an option to filter in the Signature view. This has been fixed.
- Fixed an error when a TQL query with “contains” is run against an Attribute.

Dashboard

- Users can now view their newly added dashboard without a manual refresh.
- Adding a new Dashboard card will no longer displace all the other Dashboard cards.
- Users belonging to an assigned User Group will now be able view Cases assigned to them under the My Cases Dashboard card.
- The Dashboard dropdown is now in alphabetical order.

Groups

- Users should no longer see blank Group lists when they associate more Groups to an existing Group.
- In the Group Association view, users were not able to select and save groups from multiple pages. This has been fixed.
- When copying a Group to an Organization, Users will now be allowed to copy only to the same Group types to avoid discrepancies.
- Disassociating an Indicator will now correctly create an entry in Activity details.

Miscellaneous

- ThreatConnect would fail to connect to the MySQL database in some instances when inbound mail over TLS was enabled. This has been fixed.
- Fixed an error created in Email API service logs.

Playbooks & App Builder

- Fixed an issue that was preventing users from deleting key/value entries when inline steps were enabled in the ThreatConnect API or any multi action app.
- Fixed an issue that was preventing users with the “Standard User” permission level from being able to activate Playbooks or view them in Interactive Mode.

- Fixed an issue that resulted in users getting errors in logging services on a simultaneous Playbook execution.
- The Selection Tool in Playbooks now supports keyboard shortcuts.
- Certain Playbooks fail to activate. This has been fixed.
- Sometimes, Output variables for Playbook apps were not showing all available variables in the layout. This has been fixed.

Search

- Users searching for an IP address would encounter an application error when clicking the "ThreatConnect Intelligence" Owner link. This has been fixed.
- Some indicator searches through the API were being performed as case-sensitive rather than case-insensitive. This has been fixed.

Workflow

- Fixed an issue that was causing a 404 error when accessing Associated Cases in Workflow.
- If an Artifact is manually associated with a Group, Users will now be able to view Cases associated with that Artifact as a Potential Association.
- When a Case has a lot of data like Tasks, Associations, Artifacts, and Notes, the UI response to expand and collapse was slow. This has been fixed.
- Workflow Template name was not displayed correctly on the preview of Intel Details page. This has been fixed.
- Accessing Indicator Details associated with a Case was incorrectly showing CAL as disabled even if it was enabled. This has been fixed.
- Fixed an issue where a Workflow Case was getting unassigned from a User if an Artifact was removed from that Case.