Version: 6.1

01 February 2021 (Cloud Release)
22 February 2021 (General Availability)

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

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

The Tao of Intel-Led Operations

This was one of the first graphics we created for ThreatConnect, but it's one that's still very meaningful to our latest release. It's quaint, isn't it? The graphics have certainly improved over the years, but the vision remains the same: threat intelligence can guide security operations towards better decisions, and security operations serve as the source of some of your best (native) threat intelligence.

If our launch of Workflow in 2020 was a big step towards realizing that vision, then 6.1 takes it to the next level. For the first time, we're giving threat intel analysts a direct window into ground-truth operational data, and we're giving SOC analysts a single-page view of relevant, contextualized intelligence, all the way to the adversary level. We also have some new features to help analysts on any team make more effective, well-informed decisions.

6.1 demonstrates the importance of having a single platform, which truly intertwines the capabilities of a TIP and a SOAR into one for the first time ever in the market.

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

Dan Cole

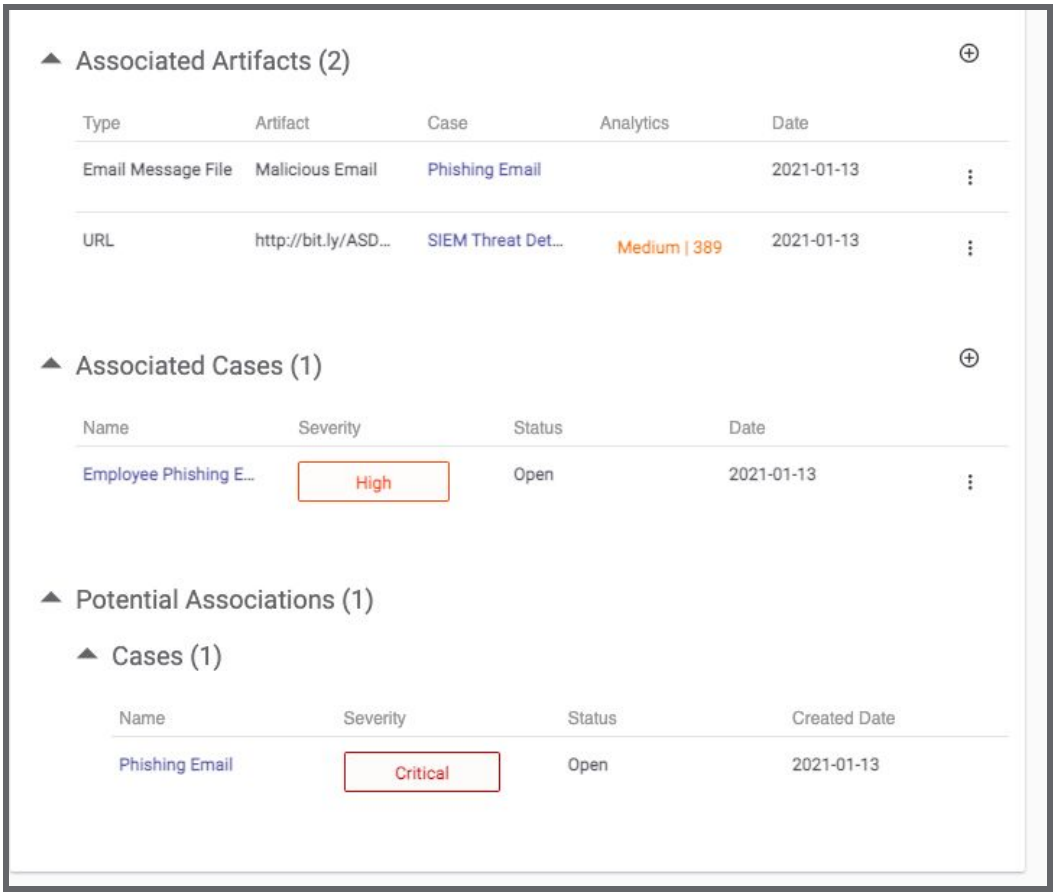
Senior Director of Product Management, ThreatConnect

dcole@threatconnect.com

New Features and Functionality

Link Intelligence and Cases

We have added several new features for linking Cases in Workflow with your source-of-truth, memorialized threat intelligence… and vice versa!



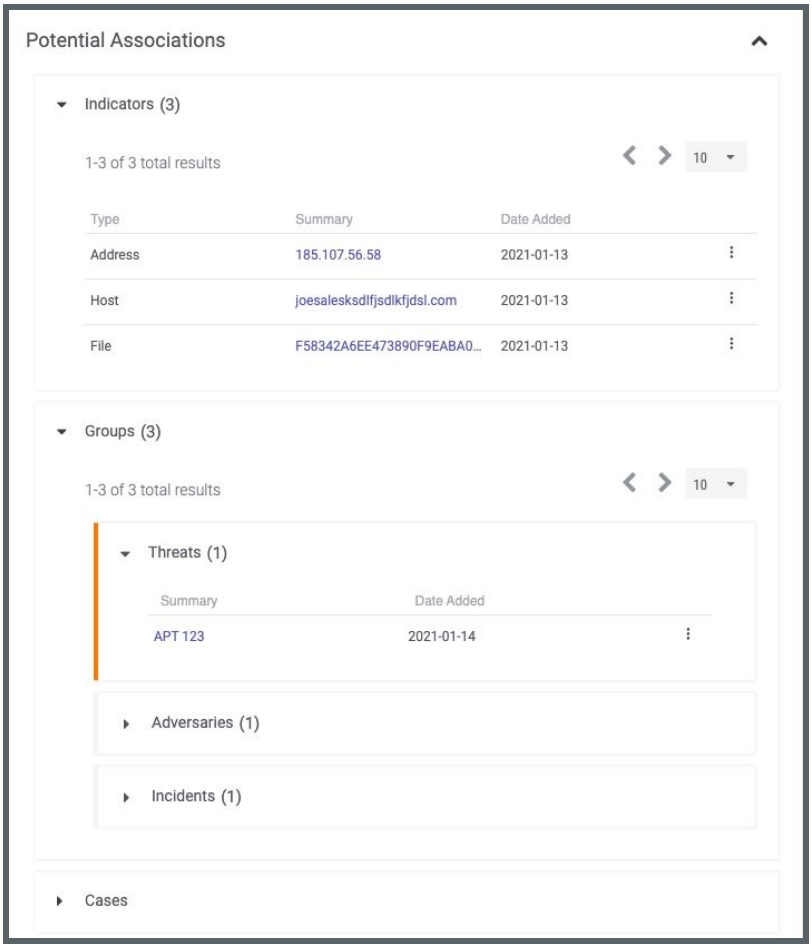
This Indicator of Compromise also appears as an Artifact in several Cases.

Users can now directly link Cases and Artifacts to Indicators and Groups. For example, when investigating an case involving a particular Malware Family, the Case can be linked directly to the Threat or Adversary involved.

Potential Associations

Allowing an analyst to set new relationships between the data is a great way to provide context. But what if the analyst doesn't know the relationship exists? That's where **Potential Associations** come in. Even if an

active link hasn't been provided or established, ThreatConnect will *suggest* relationships that might exist. For example, suppose an analyst is working a phishing investigation as part of a case and comes across a malicious attachment. If the file hash for that attachment has been historically related to a particular adversary, the user will be immediately notified that a potential link exists between the case they're working on and that adversary.



This threat hunting case has uncovered Potential Association to several threats and indicators.

There is no additional setup, configuration, or enrichment needed. Because ThreatConnect provides SOAR and TIP in one platform, all of the native threat intelligence you have is automatically made available to all users in a common language for common context.

Feed Explorer & Feed Report Cards

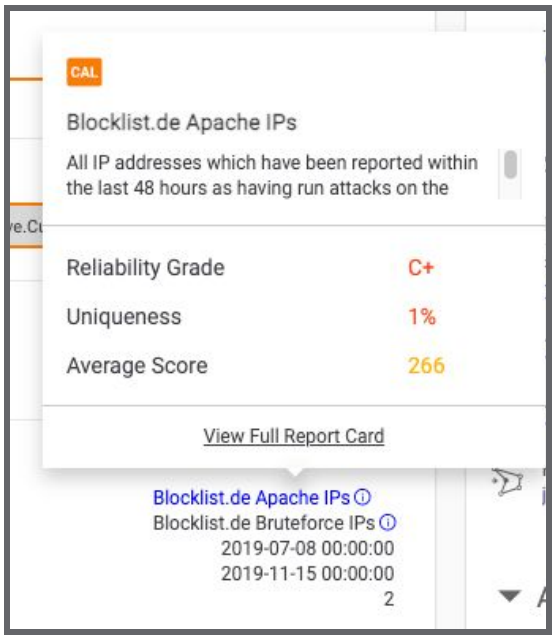
With a news article, understanding the validity and bias of the source is just as critical as the content of the article itself. Intelligence is the same way: when viewing an indicator, you might ask of the feed reporting it:

- How often does this feed report a false positive?
- How timely is this feed compared to other feeds?
- Does this feed provide a wide breadth of information (e.g. is it only interested in phishing domains, or does it cover other topics)?
- Do indicators in this feed tend to be more critical / malicious then others?

ThreatConnect now offers answers to these and more questions in the form of our new Feed Explorer.

View reports on dozens of OSINT feeds.

In addition to the Feed Explorer, we also wanted to make sure that users could get this context throughout the platform. You can access a miniature version of the Feed Report Card when directly viewing an Indicator as part of the CAL Insights portion of the Details Page.



Click "View Full Report Card" for more details!

New Management API

We have added tons of new API features designed to help some of our more technical users with various backend tasks. These new endpoints include a host of new metrics that improve the transparency of application health for automated management purposes, including:

- Playbook usage and execution metrics
- Overall system health metrics
- Database information
- Feed health

Please consult our administration documentation for a full list.

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

- Organization Administrators can now download Service logs.
- Users can now sign up for error notifications via email when a Service app fails to execute. These notifications also include relevant diagnostic logs.

Browse Screen

- The Browse screen now provides a much more helpful error when a user enters an invalid TQL query.

Data Updates

- Updated Threat Type Attribute Validation rule to include "Threat Actor" in the list of options.
- Added new entries and removed old entries from Indicator Exclusion Lists.

Playbooks

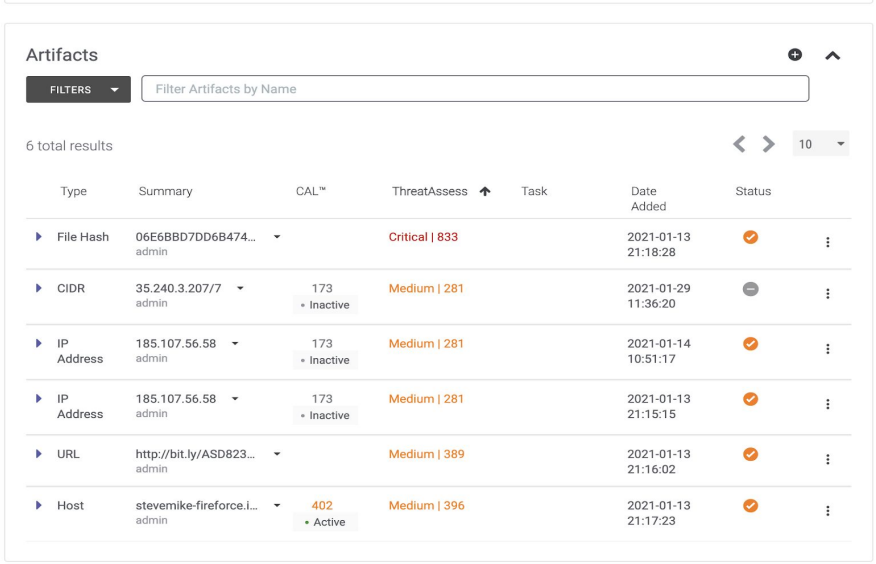
- We have implemented performance improvements for users who set Playbooks to run in TRACE logging mode.

Under the Hood

- Whois lookups in ThreatConnect are now provided by WhoisXML API.
- ThreatConnect now supports secure inbound SMTP connections via TLS.
- ThreatConnect has many logging and storage capabilities that have the potential to introduce disk space issues. In order to manage these issues, we have introduced a disk space monitoring service.
- Playbooks running as HIGH priority now have an underlying priority value of 7. This allows Playbooks designed to monitor system diagnostics at a higher level of priority.
- We have streamlined our patch process with a new, lightweight patch installer.
- ElasticSearch has been upgraded to v7.7.0.
- All SAML authentication now uses Keycloak instead of Picketlink.

Workflow

- Users can now configure Workflow to exclude certain Artifacts when automatically relating Cases. This should significantly reduce false positive associations from being made (e.g. you don't want to relate cases on 127.0.0.1).
- We have significantly expanded the amount of context provided to an analyst when viewing Case Artifacts. Users can now see which Task added the Artifact, CAL details, derived indicators, and much more. This means that a SOC Analyst investigating a Case is armed with the threat intelligence they need to make more informed decisions **without leaving the page.**



- The Artifact list on a Case can now be sorted by ThreatAssess, allowing the most critical items to bubble up to the top of the list.

Bug Fixes

API

- Updating the name of a Document now only requires updating the name, not the fileName.

Apps, App Services, & Feeds

- Fixed an issue that was breaking inbound TAXII feeds when the allowApps permission was disabled.
- Fixed a UTF8 encoding issue that was causing certain feeds to fail.
- Fixed an issue that was producing an ElasticSearch error when running the FS-ISAC job app.
- Configuring a Service on a specific Organization will no longer also add System when saving.
- The Feed Deployer will no longer fail when deploying the iDefense Intelgraph app.

Browse Screen

- Fixed an issue that was causing problems on instances running PostgreSQL when performing complex sorts.

Dashboards

- Datatable dashboard cards no longer error out when sorting them by Tags.

Login

- Logging in with multifactor authentication will now take the user directly to the URL they were attempting to access rather than to the dashboard.

Playbooks

- Users are now notified when activating a Playbook that uses a custom Trigger which fails to validate properly.
- Playbooks now execute in the correct priority order rather than queued order.
- The Signature trigger will now properly fire each time rather than only the first time.
- Fixed an error that was occurring when users with certain permissions attempted to access the Playbooks Activity tab.

Search

- Group Attributes with long values are now properly indexed by ElasticSearch, allowing them to be searched on. A reindex is necessary after upgrading to pick up the values.

Workflow

- The Case timeline is now properly paginated.
- We have removed the “Choose Preset” option in the Case and Task Lists as it’s no longer required.

Miscellaneous

- While Safari is not officially supported by ThreatConnect, we have corrected a RegEx issue that was breaking certain areas of the platform.
- Banned API users can no longer see the Owner they’re banned from in a /v2/owners API call.
- Fixed an issue with Batch API progress monitoring that caused errors and slowdown of processing under certain conditions.
- Removed broken Pastebin Investigation Links.

Dependencies

6.1 has the following dependencies:

- ElasticSearch 7.7.0
- Environment Server v2.1.2, which is available via download directly from ThreatConnect.

In addition, users coming from older versions (pre-6.0) require 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

6.1 is the latest version. There have been no maintenance releases at this time.