

ThreatConnect® Release Notes

Software Version 6.7

October 12, 2022

ThreatConnect, Inc. 3865 Wilson Blvd., Suite 550, Arlington, VA 22203 P: 1.800.965.2708 | F: 703.229.4489 www.ThreatConnect.com

Table of Contents

New Features and Functionality	2
Cross-Owner Associations	2
Browser Extension v3 - Natural-Language Processing	5
Add to the Exclusion List from the Details Screen	6
Visualize Cases in Threat Graph	7
Intel-Powered Case Associations	8
User Management API v1	9
Improvements	10
Dashboards	11
Explore In Graph	11
Playbooks	11
Workflow	12
Task Due Dates	12
System Settings	12
User Settings	13
Browser Extension	13
API & Under the Hood	13
Bug Fixes	14
Threat Intelligence	14
Playbooks	14
Workflow	15
Organization Administration	15
API & Under the Hood	15
Dependencies & Library Changes	15
Maintenance Releases Changelog	15
2023-06-22 6.7.3-M0622S [Latest]	15
Bug Fixes	15
2023-01-20 6.7.3b	16
Bug Fixes	16
2023-01-13 6.7.3a	16
Bug Fixes	16
2022-12-13 6.7.3	16
Dependencies & Library Changes	16



Improvements	17
Bug Fixes	18
2022-11-16 6.7.2	19
Improvements	19
Bug Fixes	20
2022-10-26 6.7.1b	21
Bug Fixes	21
2022-10-22 6.7.1a	21
Bug Fixes	21
2022-10-19 6.7.1	21
Improvements	21
Bug Fixes	22



New Features and Functionality

Cross-Owner Associations

In ThreatConnect[®] version 6.7, we address one of the most commonly raised challenges faced by our users: the inability to associate items across owners.¹ With this feature, you will be able to associate objects from Sources, Communities, and Organizations to one another without needing to use the "Copy to my Org" functionality. We also introduce a new search and filtering capability within the "Add Associations" functionality on the **Details** screen that enables you to more easily locate objects that you want to associate.

APT28 /												
Isplane In Graph Q. Pivet 💼 Delete 🛓 Download PDF											. ni	6 0 9
tew Tasks Activity Associations Sharing Spaces	Add Group						×				Folio	w Item
escription	Add Group	2									Graph	Table
oduct Team says:	Q. APT28		V								CAL Aliases	æ
T28 (https://attack.mitre.org/groups/G0007) is a threat group that has been attributed to Russia's Genera	Type 11	Group Type			Owner 14	Last Modified 1	Date Added	Dwner		Date Added		
TsSS] military unit 26165 (Citation: NSA/FBI Drovorub August 2020) This group has been active since at li licitment Jul 2018) (Citation: Crowdstrike DNC June 2016) (Citation: FireEye APT28) (Citation: SecureWork R) (Citation: Schary DealersChoice) (Citation: Palo Alto Sofacy 05-2018) (Citation: Symantec APT28 Oct 2	incident	Event, Incident	~		ThreatConnect Intelligence	08-11-2017	02-24-2022	roduct Team		08-25-2021		I
UAIQ (Clasters Online) beamins/bence) (Clasteron Han Adio Sottes; Uni-2011) (Clasteron Symanities AdV120 UCL 2012) (Italys: Adv120, UCL) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) Committee In 2016 in an attempt to inserfere with the U.E. presidential electrico. (Clasterial Italiano Claster 2012) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano Santa) (Italiano (Italiano Santa) (Italiano Santa) (Ita	Signature	Owners V		ThreatConnect Intellig		08-11-2017	02-24-2022					æ
	🗋 Incide 🗹 Any owner			10-05-2018	03-04-2022	Dwner	Threat Rating	Date Added				
	Signa Organ	izations	Sources		Communities	10-05-2018	03-04-2022	hoduct Team		01-13-2022		1
	🗌 Repo 🗹 Pr	oduct Team	 abuse.ch CryptoWall Ransomwere C2 Domain Blocklist 		Product Community	01-13-2022	01-13-2022					æ
curity Labels	indrus		abuse ch Feodo Tracker			12-22-2021	12-22-2021					
🛏 Choose Security Labels 🗸	intrus		 abuse.ch Locky Ransomware C2 Domain Blocklist 			01-26-2022	01-26-2022					e
tributes	intrus		abuse.ch Bansomware		Apply	03-05-2022	03-05-2022					e
urce	intrus		Domain Blocklist			05-14-2022	07-20-2022					
* None	incident	APT28 and Upcoming Election	s: evidence of possible interference 🕑		Technical Blogs and Reports	04-12-2019	09-12-2021					
try URL					K	< 1 - 10 of 36	> > 10 ∨					
ps://attack.mitre.org/groups/G0007												
ation												
728 itation: FireEye APT28) (Citation: SecureWorks TG-4127) (Citation: Crowdstrike DNC June 2016) (Citation:						Cancel	Add Groups					

New search and filtering functionality available when adding associations on the **Details** screen

In addition to the ability to associate items across owners, we have added a new **CAL Aliases** button that can be leveraged by our users who have the Collective Analytics Layer (CAL[™]) turned on.² When clicked, this button queries your ThreatConnect instance for any Groups with a summary (name) matching one or more of the known aliases for the Group being viewed. This functionality is intended to help you identify related information faster so you can spend your time on things other than keeping track of threat actor aliases.

¹ThreatConnect[®] is a registered trademark of ThreatConnect, Inc.

² CAL[™] is a trademark of ThreatConnect, Inc.

erview Tasks Activity					×	Follo	ow Item
	Groups Vi	a CAL Aliases			^		
Description	CAL Aliases reco	mmends group associations based on CAL gro	oup alias information			Graph	Table
Product Team says:						-	
Mone None	(i) Searching fo	r Aliases:				CAL Aliases	Ð
PT28 (https://attack.mitre			Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127	7		Date Added	
taff Main Intelligence Dire Citation: NSA/FBI Drovoru						08-25-2021	:
ndictment Jul 2018) (Citat Citation: FireEye APT28) ((Q APT28		V				
RIZZLY STEPPE JAR) (Cit							æ
ymantec APT28 Oct 2018	□ Type 1	Name/Summary 11	Owner 11	Last Modified 1	Date Added 1	Date Added	
PT28 (https://attack.mitre emocratic National Comn	Intrusion Set	APT28 [Mandiant Advantage	12-22-2021	12-22-2021	01-13-2022	
ttempt to interfere with the						01-13-2022	:
dicted five GRU Unit 2616 perations (including close	Intrusion Set	APT28 🖸	Mandiant Threat Intel	01-26-2022	01-26-2022		
oping Agency (WADA), the	Intrusion Set	APT28 [MITRE ATT&CK	03-05-2022	03-05-2022		۲
hemical Weapons (OPCW istrict Court Indictment G		APT28 [2]	Destautore	04 44 0000	07.00.0000		
4455, which is also referre	Intrusion Set	AP120	Product Team	06-14-2022	07-20-2022		۲
				K < 1-4 of 4	> > 10 ~		
ecurity Labels							\oplus
,							
- Choose Security Labe							
ttributes							
Source							

Use the CAL Aliases button to quickly identify other Groups that are likely to be related to the one being viewed

It is important to note that the cross-owner associations functionality is turned off by default in ThreatConnect 6.7. This is because we want to make sure that the teams who decide to leverage this functionality are aware of when it is turned on and off. Some users may not want to make associations between items in different sources for one reason or another, and we want to make sure they are able to keep the separation of owners in place if they want. Those teams that choose to leverage the feature can rest assured that there are permissions checks before information is presented to a given user to make sure that users have access only to information they have permission to view.



🔅 Sys	tem Setti	ngs		
Settings	E-mail Scoring	Indicators Investigation Links Attribut	te Validation Attribute Types Artifacts Security Labels	License Login Messages Info Logs Styling
Data				CLEAR ENTITY CACHE CLEAR MASTER SECRET KEY CREATE SEARCH INDEX SEND SYSTEM MESSAGE
Setup		importSignatureAllowedMediaTypes	\b(application/xml text/plain)\b	The Regex for MediaTypes allowed in the Signature upload
Advanced		importSignatureFileSize	1000 + KB	The maximum file size limit for a Signature import in KB
Apps		importSignatureTypes	Snort, YARA, CybOX, OpenIOC, ClamAV, Suricata, Bro, Regex, SPL, Sigm	Signature file types allowed in the Signature upload
Data				
Logging		Taxii Services		
Monitors Storage		taxiiPollServiceIndicatorExportLimit	500 + Indicators/Request	Limit for how many indicators the Taxii Server can provide for each request. Subsequent indicators can be pulled via multi-part poll exchange.
System		taxiiPollServiceMaxDateRange	24 <u>+</u> hours	Maximum time frame for which data may be pulled via Taxii Service.
Email Terr Variables		Threat Intel		
		crossOwnerAssociationEnabled	🗹 Enabled	Turns on or off support for creating cross owner associations.
		Workflow		
		caseResolutionList	Containment Achieved, Deferred / Delayed, Escalated, False Positiv	A comma separated list of possible Case Resolution values.
				CANCEL SAVE

Cross-owner associations can be enabled in the **Data** section of **System Settings** in ThreatConnect 6.7

This is version 1 of ThreatConnect's cross-owner association functionality. Stay tuned for upcoming releases in which we iterate on this feature to make it even easier for you to see information across owners.

Browser Extension v3 - Natural-Language Processing

The newest version of the ThreatConnect Browser Extension adds some exciting new functionality around natural-language processing (NLP). With Browser Extension v3, you can scan a web page and query the CAL NLP engine for matches on MITRE ATT&CK® techniques.³ This feature doesn't look for exact wording matches. Instead, it scans the contents of a sentence and determines whether the text is indicative of a specific ATT&CK technique, and then it serves that information to you in an updated Browser Extension UI.

³ MITRE ATT&CK[®] and ATT&CK[®] are registered trademarks of The MITRE Corporation.



MANDIANT	Platform Solutions Intelligence Services Ret 🔀 Scan Results	? 🔅 for Fr
	environment starting in 2018 by using a combination of se detailed <u>in our guidance</u> . Croups	
	Bypassing Multi-Factor Authentication (MFA): From 201 assortment of methods to satisfy strong authentication r environments for lateral movement. These included enro	
	bypassing it via legacy authentication, adding credentiale app registrations, and utilizing precomputed cookies to b	
	and log in successfully without raising any alarms. The gr legitimate credentials to abuse repeated MFA push notifi legitimate device until the user accepted the authenticat T1105 Ingress Tool Transfer	
	group evolve from using Golden Tickets to access sensiti systems to <u>Golden SAML</u> (Security Assertion Markup Lan	
	environments that used cloud hosted resources. Both tee bypass authentication requirements and access the victi privileges and as any user, even after a domain-wide pass	
	accounts. • Maintaining a Light Malware Footprint: APT29 shifted aw	
	customized tools to maintaining a relatively light malware due to extensive open-source reporting on the group's to Posc	an page
	detection opportunities by anti-virus engines and compli The group appears to favor the use of stolen credentials, adusing native hicrosort features to maintain access to victim environments. In some cases, we have	
	observed the group shift from deploying custom tools after gaining a foothold to deploying BEACON. This is likely due to the success, availability, modification optimitial and attribution complications provided by BEACON. Econ 2018 to 2021	

Leverage CAL's NLP to identify ATT&CK techniques not explicitly mentioned in the text of a web page

Unlike previous versions of the Browser Extension, this version does not require you to install and enable an App Service. However, it does require you to be on ThreatConnect version 6.7 or newer.

Add to the Exclusion List from the Details Screen

Also in version 6.7, System Administrators and Organization Administrators will have the option to add an Indicator to their Organization's Exclusion List directly from the Indicator's **Details** screen. This functionality has been requested by multiple customers and will make it easier for administrators to add Indicators to the Exclusion List without interrupting their flow of work.

 ✓ 52.38.151.45 ☑ Explore In Graph				Active Add to Exclusion I CAL Status Lock	ator Status – X
Overview Tasks Activity DNS Resolutions Associations Spaces				Follo	ow Item
Indicator Analytics ThreatAssess	Associations			Graph	Table
TilleauAssess	Associated Groups (0)				\oplus
281 O Recent False Positive Reported O Impacted by Recent Observations	Туре	Owner		Date Added	
Medium	 Associated Indicators (0) 				Ð
CAL [™] Insights	Туре	Owner	Threat Rating	Date Added	

Organization and System Administrators can add Indicators to the Organization Exclusion List from the *Details* screen

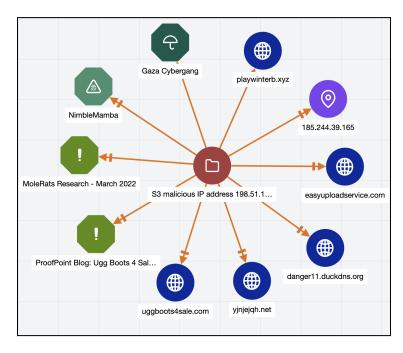


It is important to note that once an Indicator is added to the Exclusion List, the administrator will need to remove the item from the Exclusion List via the **Indicator Exclusions** tab of the **Organization Config** screen. The **Add to Exclusion List** checkbox cannot be cleared manually.

Visualize Cases in Threat Graph

One of the most critical challenges analysts face today is the lack of a bird's-eye view of the threat landscape, forcing them to work in silos. With the 6.7 release, we bring Cases into the Threat Graph (formerly known as Graph View), providing you with a holistic view of your threats and their relationships with the Cases in your Organization.

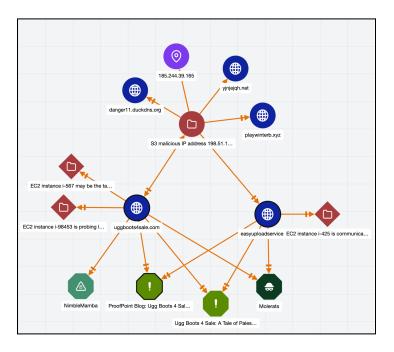
You can now launch the Threat Graph from Workflow Cases. When you click the **Explore in Graph** button at the upper-right corner of a Case, you will be able to pivot on associated Indicators or Groups for the Case. This functionality helps you understand complex attacks and gain more contextual relationships between the IoCs, threat actors, Adversaries, Campaigns, etc., involved in the Case.



Threat Graph for a Case and its associated Indicators and Groups

Investigations can be built by pivoting on these Indicators and Groups to identify similar Cases that share them. This process helps to speed up investigations, as the action taken for one Case could be easily leveraged for other Cases.





Holistic view of Cases and shared Indicators and Groups

Intel-Powered Case Associations

Due to the sensitive nature of breaches, it is crucial for analyst teams to rely heavily on external threat intelligence sources and to learn about the techniques commonly used by attackers. This information helps them respond to threats confidently and with precision. With version 6.7 of ThreatConnect, we bring in relevant potential associations from external sources to add more context to Workflow Cases.

In a Workflow Case, analysts collect Indicators on the **Artifacts** card as part of their investigation. Prior to this release, only matching Indicators in your Organization and their associated Groups were suggested as potential associations. With version 6.7, users can now view matching Indicators and their related Groups from selected external feeds (Communities and Sources) on a Case's **Potential Associations** card.

Organization Administrators can enable external feeds for potential associations in Workflow on the **Communities/Sources** tab in **Organization Settings**. There is a new column–**Enable for Potential Case Associations**–from which administrators can select Communities and Sources.



Product Team - Organiza	tion Settings					
Membership Communities/Sources Groups	Invitations Activity Variables Metrica	Settings Email Apps Styling				
'seudonym: dcole-pm-org						
Name	Туре	Default Role	Anonymous	Joined	Options	Enable for Potential Case Associations
abuse.ch CryptoWall Ransomware C2 Domain Blocklist	Source	User		12-10-2021	Ô	
abuse.ch Feodo Tracker	Source	User		12-10-2021	ŵ	⊻
abuse.ch Locky Ransomware C2 Domain Blocklist	Source	User		12-10-2021	÷	
abuse.ch Ransomware Domain Blocklist	Source	User		12-10-2021	ė.	
abuse.ch Ransomware Tracker	Source	User		12-10-2021	ŵ	
abuse.ch TeslaCrypt Ransomware C2 Domain Blocklist	Source	User		12-10-2021	۵	
abuse.ch TorrentLocker Ransornware C2 Domain Blocklist	Source	User		12-10-2021	ė	
abuse ch URUHaus	Source	User		12-10-2021	ē	⊻
abuse ch Zeus Tracker	Source	User		12-10-2021	ē	☑
Accenture iDefense IntelOraph	Source	User		01-13-2022		
		(1 of 10	» < <u>1</u> 2345678910	» 10 ~		
						SAVE

Organization Administrators can select Communities and Sources for potential Case associations

When Indicators are collected as Artifacts in a Workflow Case investigation, each Indicator is automatically looked up in these selected feeds. If any of the feeds contains the Indicator, then the Indicator and its associated Groups will be added to the Case's **Potential Associations** card. However, Indicators marked as inactive or a false positive will not be included. This new functionality will help you speed up your investigations by enabling you to discover malicious Indicators involved in the Case more quickly.



Pot	ential A	ssociations							0		
	 Indica 	ators (4)									
	1-4 of 4 to	otal results									
	Туре	Summary				CAL™ ②	ThreatAssess ③	Date Added			
	Host	uggboots4sale.com			•	181 Active	396	2022-02-08	:		
	Host	yjnjejqh.net			Alienv	ault OTX	7	2022-08-04	:		
	Address	185.244.39.165			•	173 Active	363	2022-09-08	:		
	Host	easyuploadservice.com			•	181 Active	396	2022-09-13	:		
•		4) I total results Adversaries (2)									
		Summary		Date	Added						
		Molerats		2022	2-01-24		:				
	Gaza Cybergang		Ali	Alienvault OTX				:			
	 Incidents (2) 										

Potential Case associations with Indicators and Groups seen in external sources

User Management API v1

Historically, user management has been available only through the ThreatConnect GUI, which becomes problematic when working with large numbers of users. Administrators have had to use the GUI to manually create and configure users individually, which is a very time-consuming process. To solve this problem, we have made enhancements to the existing **v3/security/users** endpoint to support tasks related to user account management. Using this endpoint, API users with an Organization role of Organization Administrator can retrieve all users of an Organization, retrieve a single user by user ID, create a user, update a user, and delete a user. A user must be authenticated with the instance using HMAC or Token Authentication to use this API endpoint.



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.

Dashboards

• When querying by Case Tasks in a datatable on a Query card, you now have options to view the Case ID, the date the Task was assigned, the Task's due date (including a timestamp), the Task's status, and the Task's assignee.

Explore In Graph

• You can now pivot on Indicators and Groups in CAL and view CAL alias information for Groups without having to install the **CAL Association Graph Service** App and configure a corresponding Service on your instance of ThreatConnect.

Playbooks

- There is a new Case Trigger that initiates Playbook execution on the following actions: Case created, Case deleted, Tag applied to Case, Tag removed from Case, Case opened, Case closed, specific resolution set, specific severity set.
- You can now hold down the Ctrl (Windows[®]) or Command (Mac[®]) key and rotate the mousewheel (or swipe down and up on a Magic Mouse[®], Magic Trackpad[®], or built-in Mac trackpad with one or two fingers, depending on the device's configuration) to zoom in and out in the Playbook Designer.⁴
- The maximum number of Playbook Workers has been increased to 146.
- The memory footprint for Delay/Resume/MEO Playbook events has been reduced to prevent out-of-memory errors when too many of these types of events are queued up.
- Organization Administrators can now create, view, and administrate Playbook Services in their own Organization.

⁴ Windows[®] is a registered trademark of Microsoft Corporation. Mac[®], Magic Mouse[®], and Magic Trackpad[®] are registered trademarks of Apple, Inc.



Workflow

Task Due Dates

- When creating or editing a Workflow, you can now specify **Task** due dates in days, hours, or minutes.
- When filtering on due dates on the **Tasks** screen, you can now specify the range by date and timestamp in your time zone.
- Users and members of user groups assigned to a Task that is not completed by its due date will now receive a notification that the Task is overdue. The method of delivery of the notification (e.g., email, push notification) will depend on each user's settings in the **Notifications Center**.
- Two new filters have been added to the Tasks screen: All Past Due Date Tasks and My Past Due Date Tasks. These filters' functionality is not available in ThreatConnect 6.7.0, but will be available in an upcoming patch release.

System Settings

- The following new system settings were added:
 - crossOwnerAssociationEnabled: This setting enables the ability to create associations between Cases, Groups, and Indicators in a user's Organization and Groups and Indicators that exist in Communities or Sources to which they have access. It also enables Super Users to create these associations between objects in the Organizations on their instance and between those in the Communities and Sources to which they have access.
 - excludeFromDetailsEnabled: For Dedicated Cloud instances, this setting determines whether to allow Organization and System Administrators to add an Indicator to an Organization-level Exclusion List from the Indicator's Details screen. When this setting is enabled, the Add to Exclusion List checkbox will be displayed in the Indicator Status section of the Details screen for all Indicators.
 - indicatorStatusLock: This setting determines whether to prevent automated system processes, except for scheduled Threat Deprecation, from modifying the Indicator Status for all Indicators on the ThreatConnect instance. When this setting is enabled, the default Indicator Status for new Indicators will be Active, and the Indicator Status of Indicators in each owner will remain



constant regardless of activity affecting the Indicator Status of the same Indicators in other owners or CAL.

- The commit hash for the ThreatConnect version is now displayed under **System Settings > Settings > Information**.
- The import rule for URL Indicators has been updated to allow for TCP and file path URIs to be added as URL Indicators in ThreatConnect.

User Settings

• When on an On-Premises or Dedicated Cloud license, two new logout interval options are available on the **My Profile** screen: 8 hours and 12 hours.

Browser Extension

• The CIDR IPV6 regex was updated to identify all IPV6 CIDR blocks, including ones with compressed notation, when scanning web pages with the ThreatConnect Browser Extension.

API & Under the Hood

• On instances where cross-owner associations are enabled, v3 API users can create associations between Cases, Groups, and Indicators in their Organization and Groups and Indicators in the Communities and Sources to which they have access.



Bug Fixes

Threat Intelligence

- An issue causing a unique constraint violation to occur when copying data to a Community on some customer instances running on HANA databases has been resolved.
- An issue preventing passive-DNS functionality from being available for Hosts and Addresses in Communities and Sources has been fixed.
- An issue causing the Structured Indicator Import feature to attempt to import duplicate Indicators if the **Back** button is pressed on the **Confirm** step has been corrected.
- An issue causing the **DELETE** button not to display on the **Browse** screen for Standard Users viewing only objects in their Organization has been resolved.
- An issue causing the **DNS** and **Whois** checkboxes not to display on the **Optional Data** tab of the Unstructured Indicator Import feature on instances running ThreatConnect 6.5.*x* and 6.6.*x* has been fixed.

Playbooks

- An issue causing a mismatch between the Iterator count shown in error messages under **Execution Details** and the Iterator count shown on the Iterator Operator in the **Playbook Designer** has been fixed.
- An issue causing TCEntity objects generated by a Workflow Trigger to have an empty **value** has been resolved.
- An issue preventing the **Update Global Variable** App from saving default values in its configuration has been fixed.
- An issue preventing Playbooks from being shared via Share Tokens has been fixed.
- An issue causing a mismatch between Iterator index counts and the execution details for the Iterator has been resolved.

Workflow

• An issue causing users with a certain custom owner role configuration to experience an error when attempting to open a Workflow Case has been resolved.



Organization Administration

- An issue preventing Organizations from being deleted when they contain a Run Profile for a Playbook Trigger has been fixed.
- Previously, setting an Organization's status to **Expired** on the **Organizations** tab of the **Account Settings** screen did not automatically disable all of the user accounts in the Organization. Now the user accounts will be disabled once the status change occurs.

API & Under the Hood

- An issue causing an error when using the v3 API to assign a Case to a user group has been fixed.
- An issue preventing Tags from being deleted in a Community or Source via the **v3/tags** branch has been fixed.
- Batch deleting via the v2 API now works as expected.



Dependencies & Library Changes

• Red Hat® Enterprise Linux® (RHEL) version 8 is now officially supported.⁵

⁵ Red Hat[®] Enterprise Linux[®] (RHEL) is a registered trademark of Red Hat, Inc.



Maintenance Releases Changelog

2023-06-22 6.7.3-M0622S [Latest]

Bug Fixes

• An issue causing duplicate key values to be created, resulting in a unique constraint error, when using the batch API to update custom Indicators has been resolved.

2023-01-20 6.7.3b

Bug Fixes

- An issue causing TQL queries to return an invalid response when configured to time out between 30 and 60 seconds was causing an application error. This issue has been resolved.
- An issue causing Management API requests for App session logs to return a **500** error instead of a **404** error when they were unable to find the log directory has been fixed.

2023-01-13 6.7.3a

Bug Fixes

• An issue causing the **cases** and **tasks** v3 API endpoints to be disabled when no additional fields were requested has been resolved.

2022-12-13 6.7.3

Dependencies & Library Changes

• PostgreSQL[®] version 14 is now officially supported.⁶

⁶ PostgreSQL[®] is a registered trademark of PostgreSQL Global Development Group.



Improvements

• The maximum filename length for a File occurrence was increased to 255 characters.

Bug Fixes

- An issue causing an application error to occur in Chrome[™] and Microsoft Edge[™] browsers when selecting an autofill suggestion for a field in a Playbook App has been fixed.^{7,8}
- An issue causing Workflows to exhibit inconsistent behavior in saving user groups as the default assignee for a Task has been resolved.
- An issue preventing users from deleting a Community that has a TAXII[™] Exchange Feed with a Job referenced in it has been fixed.⁹
- An issue causing Playbooks with an active Trigger and one or more disabled Triggers to execute via a disabled Trigger has been resolved.
- All Community members except for Banned users will now be able to view the **Community Info** screen and adjust their **Notification Options**. The tabs that are displayed and the information that is displayed on each tab depend on the user's Community role.
- An issue preventing Task completion in a Workflow Case after a selection is made from a SelectOne (Yes or No) Artifact has been fixed.
- The **Event Date** field for an Event Group no longer includes a timestamp.
- log4j[™] vulnerabilities were identified and remediated.¹⁰
- When you delete an Organization, any Communities and Sources owned by the Organization will now be assigned to your Organization instead of to the System Organization if there is no System Organization on your instance. In this case, when you perform the delete operation, a window listing the names of the Communities and Sources to be assigned to your Organization will be displayed, and you will be able to decide whether to continue with the delete operation. This fix resolves an issue causing Communities and Sources owned by deleted Organizations to be "orphaned" and uneditable in **Account Settings** on some instances.
- The information returned by the **createdBy** field in the v3 API was modified to omit extraneous information.

⁷ Chrome[™] is a trademark of Google, Inc.

⁸ Microsoft Edge[™] is a trademark of Microsoft Corporation.

⁹ TAXII™ is a trademark of The MITRE Corporation.

¹⁰ log4j[™] is a trademark of The Apache Software Foundation.



- Sources created via the Feed Deployer are populated and displayed without you having to log out and back in.
- An issue causing the v3 API to save Address Indicators incorrectly and prevent searches on CIDRs has been fixed.
- An issue causing an error to occur on the **Resource** field in the configuration for the **Microsoft Graph Notification Service** App Trigger has been fixed.
- An issue causing an application error to occur when starting from the **Dashboard** screen and viewing the **Details** drawer for an Indicator linked in search results in the **Search** drawer (the drawer that is displayed when you click the magnifying glass on the top navigation bar) has been resolved.
- An issue causing the **Known** column not to be displayed in the table of parsed Indicators in the **Add Indicators** window when adding Indicator associations to a Group has been fixed.

2022-11-16 6.7.2

Improvements

• A new Service App type, **FeedApiService**, allows you to use the Feed Deployer to deploy feeds as Services.

Bug Fixes

- Case sensitivity was adjusted for Indicator retrieval using the v3 API. Specifically, API calls to retrieve Address, E-mail Address, File, and Host Indicators are case insensitive; API calls to retrieve URL Indicators are case sensitive; and API calls to retrieve custom Indicators maintain case sensitivity based on the **Case Rules** configured for that Indicator type.
- An issue causing an out-of-memory error to occur when viewing the **Details** screen for a Group with a very large number of associated Indicators was fixed.
- An issue causing the installer on PostgreSQL instances to return a false **Database test failed!** error has been resolved.
- An issue causing double execution of Playbooks that fire when a new Document Group is created on HANA instances has been fixed.
- Previously, searching for the same data on the **Browse** screen and via the **Search** drawer yielded different results for some search phrases. The behavior on the **Search**



drawer was incorrect and sometimes resulted in a **Search Results Warning** error. The error no longer occurs, and the **Search** drawer now returns correct results.

- An issue causing use of the **addressCidr** ThreatConnect Query Language (TQL) parameter to result in an error has been resolved.
- The **Filters** menu for adding a new association from a Victim Asset to a Group now displays the correct label of **Victim Asset Type** instead of **Group Type**, and the **Date Added** and **Last Modified** fields have been removed, as they are not relevant to Victim Assets.
- An issue causing Markdown lists to render incorrectly in Task descriptions in Workflow Cases has been fixed.
- An issue causing the **Kill** option on a Playbook execution to open the execution in a separate tab instead of displaying the **Confirm Kill** Playbook window was resolved.
- The timeout threshold on all requests to OpenSearch® was increased.¹¹
- An issue causing the **App Builder** (formerly **Apps**) menu option to not be displayed under **Playbooks** on the top navigation bar for users with an Organization role of App Developer was resolved.
- If a Playbook containing an Iterator Operator is designed and executed in a way that would cause an infinite loop, the infinite loop will now be prevented from occurring.
- An issue causing the v3 API to read Workflow data when the calling Organization doesn't have Workflow permissions has been resolved.

2022-10-26 6.7.1b

Bug Fixes

• An issue causing database tests to show as failed during PostgreSQL upgrade has been fixed.

2022-10-22 6.7.1a

Bug Fixes

• An issue preventing the creation of all associations when cross-owner associations are disabled was fixed.

¹¹ OpenSearch[®] is a registered trademark of Amazon Web Services.



• An issue preventing the **Add to Exclusion List** checkbox from being displayed on an Indicator's **Details** screen when this functionality has been enabled on Dedicated Cloud instances was resolved.

2022-10-19 6.7.1

Improvements

- Cross-owner associations are now fully functional across the **Associations** and **Potential Associations** cards of Workflow Cases:
 - You can now add Indicators and Groups in Communities and Sources directly

to the **Associations** card of a Workflow Case by clicking the ● icon in the **Indicators** or **Groups** section and selecting objects from the **Add Related Intelligence** drawer. Note that when you select an object, all copies of the object across all owners will be added to the **Associations** card.

- When adding an Indicator or Group on the Potential Associations card of a Workflow Case as an association, all copies of the object across all owners will move to the Associations card.
- When dissociating an Indicator or Group on the **Associations** card, all copies of the object across all owners will be removed from the **Associations** card.
- The Add Related Intelligence drawer that is displayed when adding an Indicator or Group to the Associations card of a Workflow Case now has an Owner column.
- The **Summary** cell for each Indicator and Group on the **Associations** and **Potential Associations** card now has a dropdown that displays all owners to which the object belongs. Each object is listed only one time on the card.
- Origin Country was added as a System Attribute to the following object types: Address, Email Address, File, Host, URL, ASN, CIDR, Mutex, Registry Key, User Agent, Document, E-mail, Event, Incident, Intrusion Set, Report, and Signature. Previously, it existed for only the following Group types: Adversary, Campaign, Malware, Threat, Tool.
- Security Labels on the System, Organization, and Community/Source level were updated to the current Traffic Light Protocol (TLP) standards: TLP: Red, TLP: Amber, TLP: Amber + Strict, TLP: Green, and TLP: Clear.
- A DNS resolution setting preventing certain proxies from working with the Environment Server's SSL handshake logic was removed from an embedded library.



Bug Fixes

- You can now view Workflow associations (Associated Artifacts, Associated Cases, and Potential Associations) on the Associations card of the Details screen for an Indicator or Group in a Community or Source.
- When viewing the **Details** drawer for an associated or potentially associated Indicator or Group in a Workflow Case via the **Details** option of the vertical ellipsis menu, the correct owner of an object, instead of "Details," is now displayed.
- An issue causing Attributes with an ampersand (**&**) in their name to be displayed incorrectly on the **Attributes** card of a Workflow Case has been fixed.
- An issue causing the **/v3/victims** endpoint in the v3 API to create a Victim object in the user's Organization rather than in the owner specified in the API call when using the **?owner=** query parameter has been resolved.
- When retrieving deleted Indicators using the **/v2/indicators/deleted** endpoint in the v2 API, results will now be paginated.
- An issue preventing validation errors from being displayed in the **Validations** tab of the App Builder has been fixed.