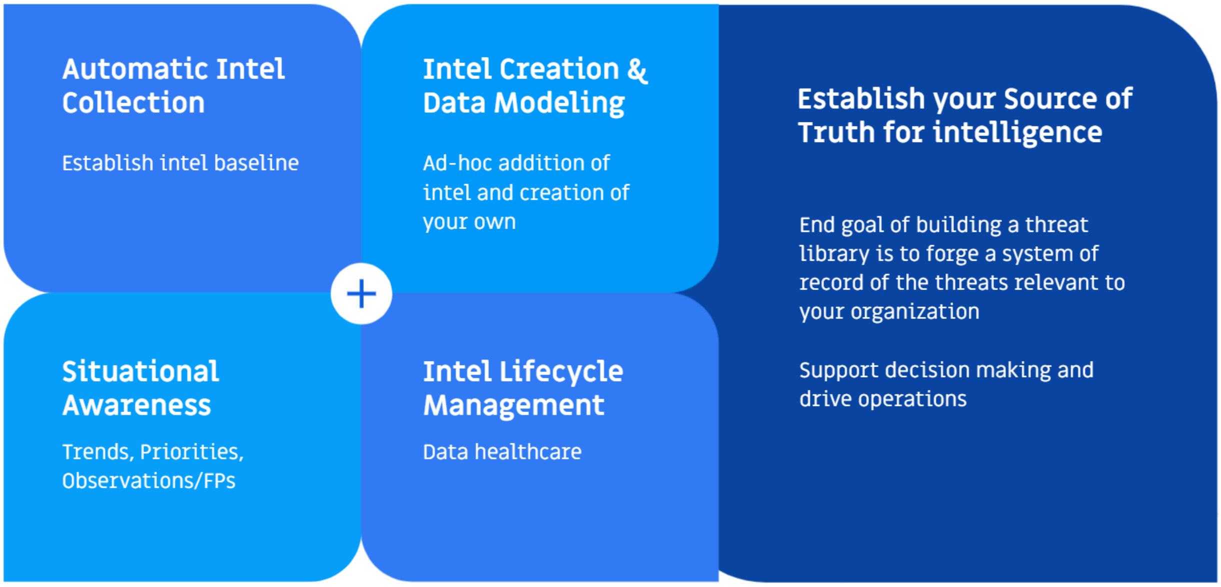
Building a Threat Library

Chris Adams

Building a Threat Library is a fundamental capability for cyber threat intelligence teams. Designed and managed correctly, a threat library is the underpinning of decision support systems for the security team and drives operations. At the most basic level, with the restrictions of time and resources, threat intelligence promises to channel focus onto that which matters most.

There are four main categories of activity captured in the use case of operating a threat library:

- Automatic Intel Collection
- Situational Awareness
- Intel Creation & Data Modeling
- Intel Lifecycle Management



Automatic Intel Collection

Establish intel baseline

Intel Creation & Data Modeling

Ad-hoc addition of intel and creation of your own

Situational Awareness

Trends, Priorities, Observations/FPs

Intel Lifecycle Management

Data healthcare

Establish your Source of Truth for intelligence

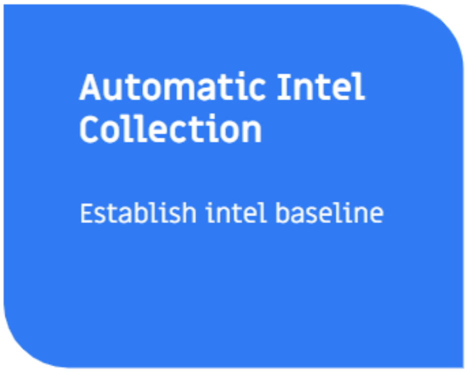
End goal of building a threat library is to forge a system of record of the threats relevant to your organization

Support decision making and drive operations

Figure 1: Activity Captured to Establish Source of Truth

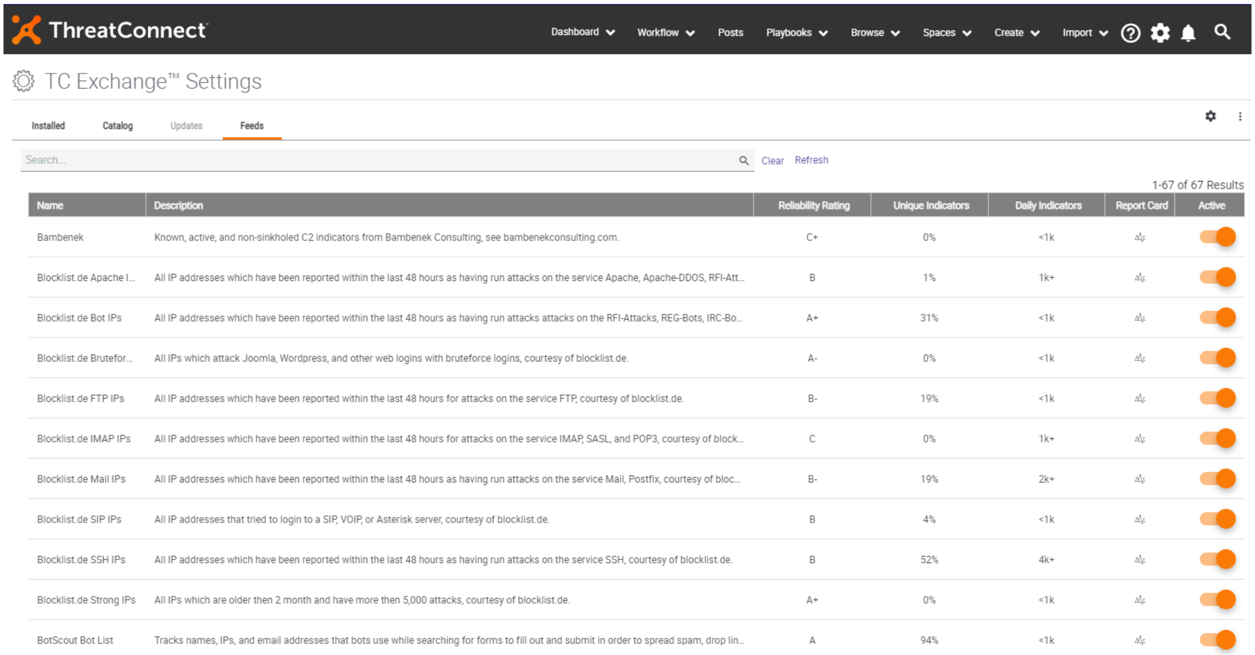
We'll walk through each of these segments in a bit more detail, but note that the key objective we aim to achieve for customers is to establish the source of truth, or system of record, for the threats that are most relevant to your organization. The outcome of that objective is to create an environment that supports decision making for analysts and helps drive security operations.

Automatic Intel Collection



Establishing an intelligence baseline means just that - starting out with an initial set of open source or premium feeds that start you in the direction of applying intel to your decision making and driving operations.

ThreatConnect® provides open source intelligence out of the box. Use the Feed Explorer to decide which feeds are available as part of our open source content.

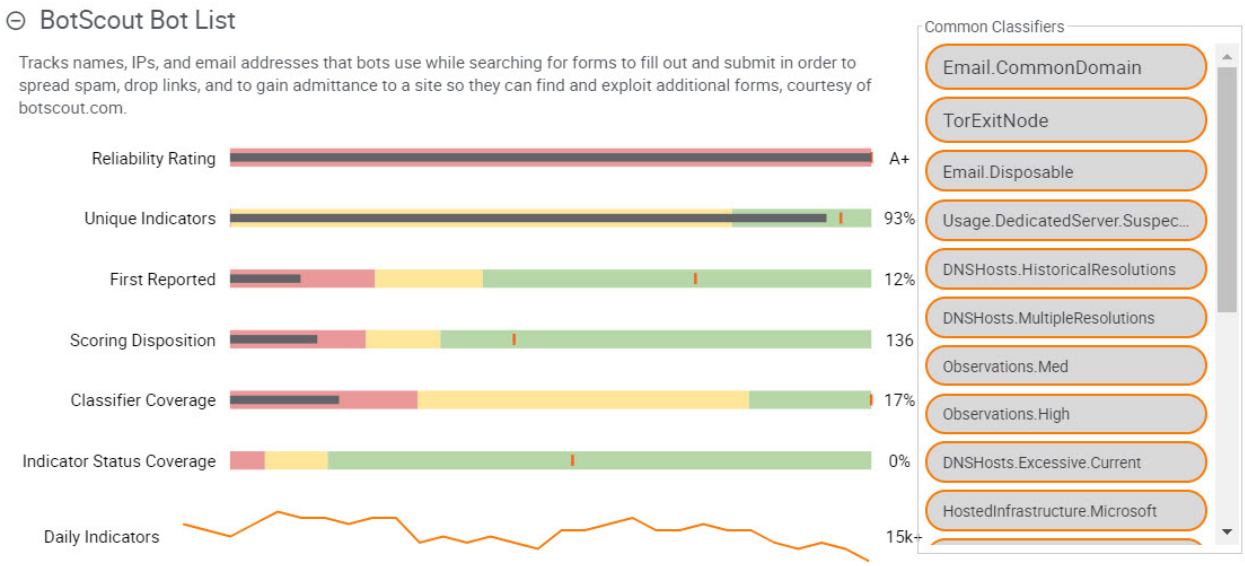


1-67 of 67 Results

Name	Description	Reliability Rating	Unique Indicators	Daily Indicators	Report Card	Active
Bambenek	Known, active, and non-sinkholed C2 indicators from Bambenek Consulting, see bambenekconsulting.com.	C+	0%	<1k		●
Blocklist.de Apache I...	All IP addresses which have been reported within the last 48 hours as having run attacks on the service Apache, Apache-DDOS, RFI-Att...	B	1%	1k+		●
Blocklist.de Bot IPs	All IP addresses which have been reported within the last 48 hours as having run attacks attacks on the RFI-Attacks, REG-Bots, IRC-Bo...	A+	31%	<1k		●
Blocklist.de Brutefor...	All IPs which attack Joomla, Wordpress, and other web logins with bruteforce logins, courtesy of blocklist.de.	A-	0%	<1k		●
Blocklist.de FTP IPs	All IP addresses which have been reported within the last 48 hours for attacks on the service FTP, courtesy of blocklist.de.	B-	19%	<1k		●
Blocklist.de IMAP IPs	All IP addresses which have been reported within the last 48 hours for attacks on the service IMAP, SASL, and POP3, courtesy of block...	C	0%	1k+		●
Blocklist.de Mail IPs	All IP addresses which have been reported within the last 48 hours as having run attacks on the service Mail, Postfix, courtesy of bloc...	B-	19%	2k+		●
Blocklist.de SIP IPs	All IP addresses that tried to login to a SIP, VOIP, or Asterisk server, courtesy of blocklist.de.	B	4%	<1k		●
Blocklist.de SSH IPs	All IP addresses which have been reported within the last 48 hours as having run attacks on the service SSH, courtesy of blocklist.de.	B	52%	4k+		●
Blocklist.de Strong IPs	All IPs which are older then 2 month and have more then 5,000 attacks, courtesy of blocklist.de.	A+	0%	<1k		●
BotScout Bot List	Tracks names, IPs, and email addresses that bots use while searching for forms to fill out and submit in order to spread spam, drop lin...	A	94%	<1k		●

Figure 2: Feed Explorer

Feed metrics and report cards make it simple to review which feeds may be most impactful. This is accomplished using rating qualifiers and common classifiers, as shown in Figure 3.



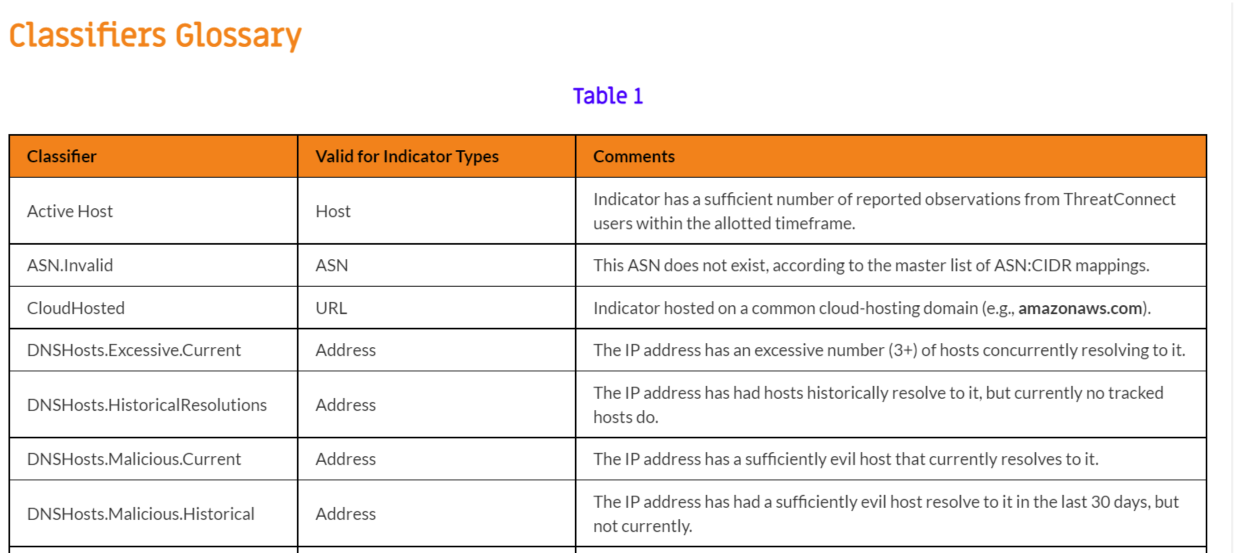
⊖ BotScout Bot List

Tracks names, IPs, and email addresses that bots use while searching for forms to fill out and submit in order to spread spam, drop links, and to gain admittance to a site so they can find and exploit additional forms, courtesy of botscout.com.

Figure 3: Report Card

Context is king in the world of threat intelligence. ThreatConnect uses data analytics and machine learning algorithms to derive contextual information pertaining to the threat data and presents that context using CAL classifiers. Analysts should be familiar with the CAL Classifiers glossary so that context is understood, the following table shows only a small portion of classifiers.

Table 1

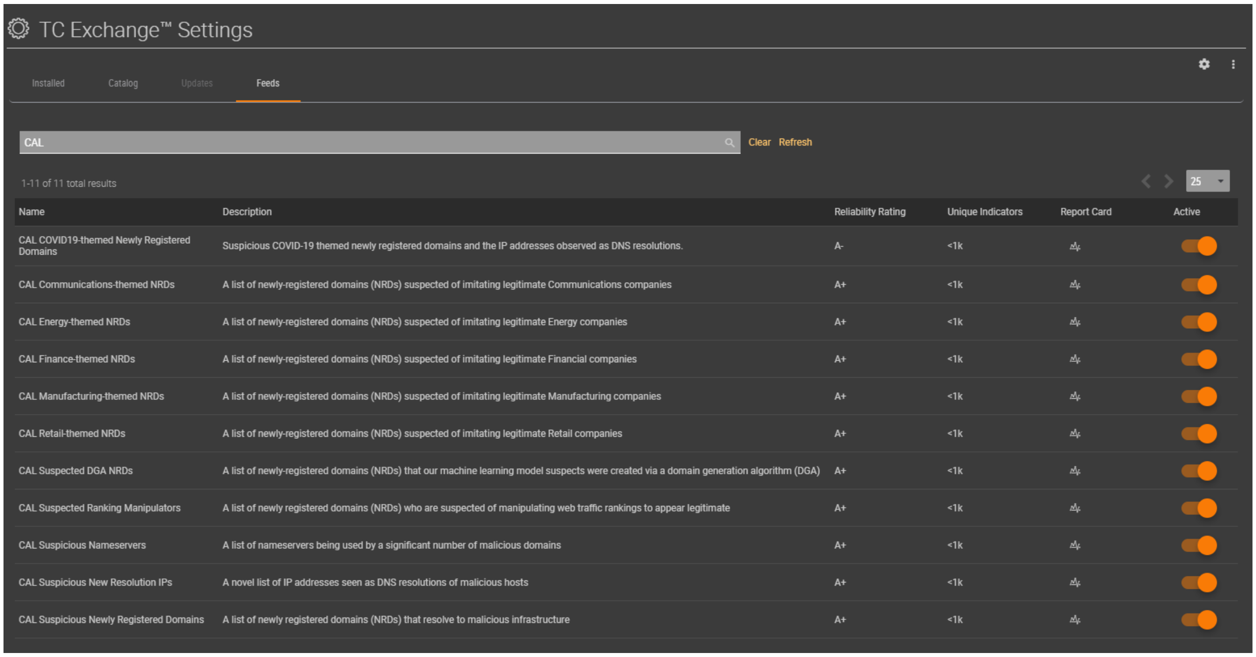


Classifiers Glossary

Table 1

Classifier	Valid for Indicator Types	Comments
Active Host	Host	Indicator has a sufficient number of reported observations from ThreatConnect users within the allotted timeframe.
ASN.Invalid	ASN	This ASN does not exist, according to the master list of ASN:CIDR mappings.
CloudHosted	URL	Indicator hosted on a common cloud-hosting domain (e.g., **amazonaws.com**).
DNSHosts.Excessive.Current	Address	The IP address has an excessive number (3+) of hosts concurrently resolving to it.
DNSHosts.HistoricalResolutions	Address	The IP address has had hosts historically resolve to it, but currently no tracked hosts do.
DNSHosts.Malicious.Current	Address	The IP address has a sufficiently evil host that currently resolves to it.
DNSHosts.Malicious.Historical	Address	The IP address has had a sufficiently evil host resolve to it in the last 30 days, but not currently.

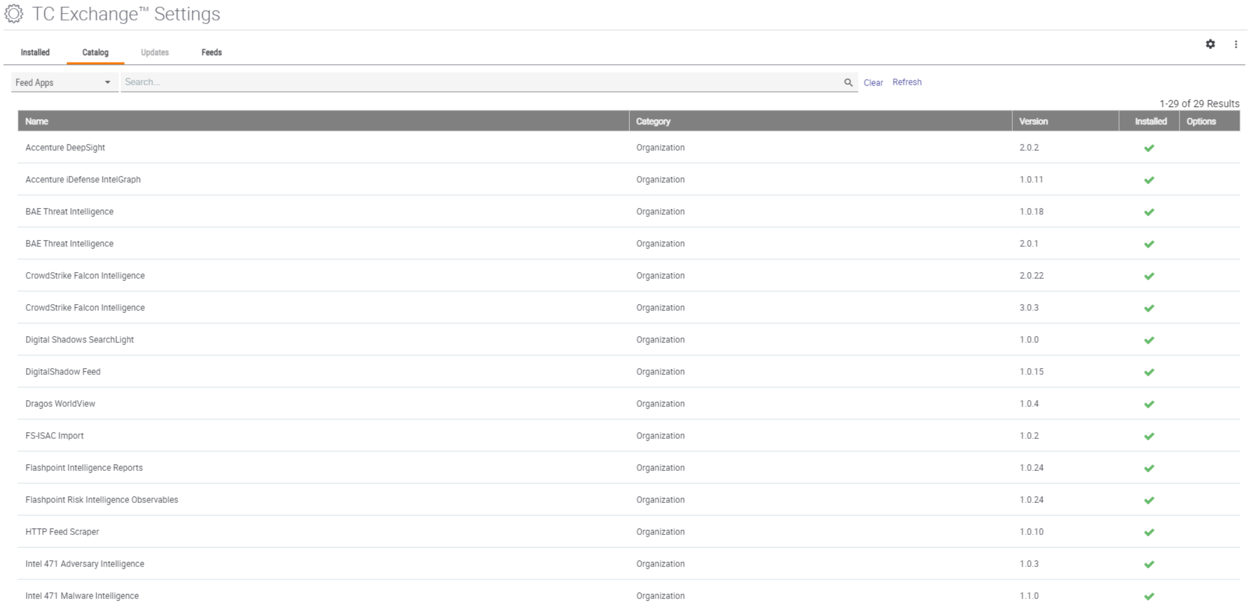
ThreatConnect Collective Analytic Layer Feeds are a combination of the immense CAL dataset and analytics along with the tradecraft of our Research team to identify pockets of intelligence that are fertile hunting grounds. Packaging this intelligence and pushing it directly to your ThreatConnect instance, we're providing a broad set of theme-based and suspicious intel threat teams should be aware of - consider this an added benefit to making ThreatConnect your Threat Library of choice.



1-11 of 11 total results

Name	Description	Reliability Rating	Unique Indicators	Report Card	Active
CAL COVID19-themed Newly Registered Domains	Suspicious COVID-19 themed newly registered domains and the IP addresses observed as DNS resolutions.	A-	<1k		●
CAL Communications-themed NRDs	A list of newly-registered domains (NRDs) suspected of imitating legitimate Communications companies	A+	<1k		●
CAL Energy-themed NRDs	A list of newly-registered domains (NRDs) suspected of imitating legitimate Energy companies	A+	<1k		●
CAL Finance-themed NRDs	A list of newly-registered domains (NRDs) suspected of imitating legitimate Financial companies	A+	<1k		●
CAL Manufacturing-themed NRDs	A list of newly-registered domains (NRDs) suspected of imitating legitimate Manufacturing companies	A+	<1k		●
CAL Retail-themed NRDs	A list of newly-registered domains (NRDs) suspected of imitating legitimate Retail companies	A+	<1k		●
CAL Suspected DGA NRDs	A list of newly-registered domains (NRDs) that our machine learning model suspects were created via a domain generation algorithm (DGA)	A+	<1k		●
CAL Suspected Ranking Manipulators	A list of newly registered domains (NRDs) who are suspected of manipulating web traffic rankings to appear legitimate	A+	<1k		●
CAL Suspicious Nameservers	A list of nameservers being used by a significant number of malicious domains	A+	<1k		●
CAL Suspicious New Resolution IPs	A novel list of IP addresses seen as DNS resolutions of malicious hosts	A+	<1k		●
CAL Suspicious Newly Registered Domains	A list of newly registered domains (NRDs) that resolve to malicious infrastructure	A+	<1k		●

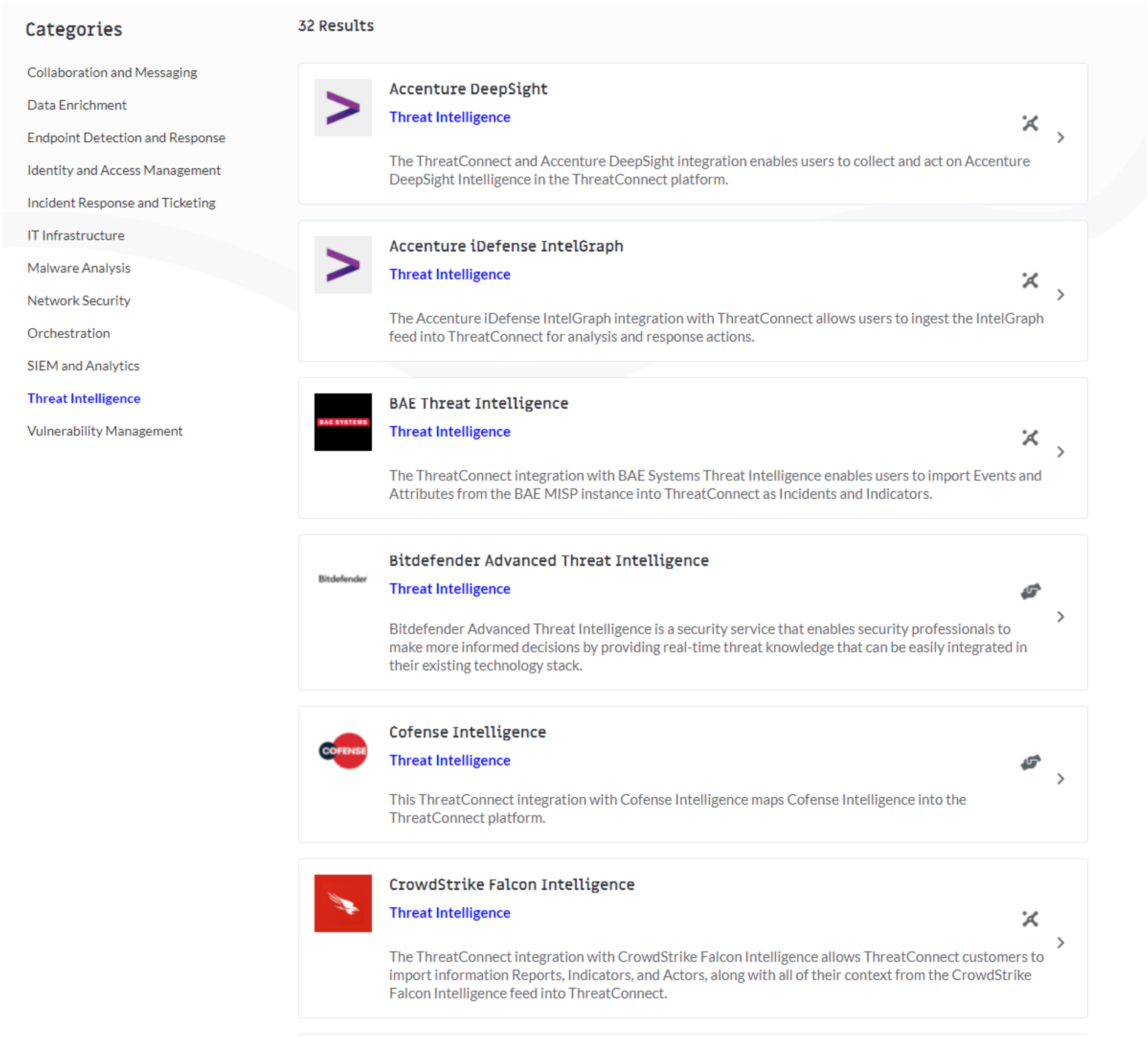
Next, consider what you can gain from premium feeds, there are an extensive list of vendors whose feed apps can be deployed simply with a valid license.



1-29 of 29 Results

Name	Category	Version	Installed	Options
Accenture DeepSight	Organization	2.0.2	✓	
Accenture iDefense IntelGraph	Organization	1.0.11	✓	
BAE Threat Intelligence	Organization	1.0.18	✓	
BAE Threat Intelligence	Organization	2.0.1	✓	
CrowdStrike Falcon Intelligence	Organization	2.0.22	✓	
CrowdStrike Falcon Intelligence	Organization	3.0.3	✓	
Digital Shadows SearchLight	Organization	1.0.0	✓	
DigitalShadow Feed	Organization	1.0.15	✓	
Dragos WorldView	Organization	1.0.4	✓	
FS-ISAC Import	Organization	1.0.2	✓	
Flashpoint Intelligence Reports	Organization	1.0.24	✓	
Flashpoint Risk Intelligence Observables	Organization	1.0.24	✓	
HTTP Feed Scraper	Organization	1.0.10	✓	
Intel 471 Adversary Intelligence	Organization	1.0.3	✓	
Intel 471 Malware Intelligence	Organization	1.1.0	✓	

Premium feeds can provide great value with sector-specific, or threat-specific context that your organization may need to stay ahead of threats. Here is a list of currently supported providers.



Categories

- Collaboration and Messaging
- Data Enrichment
- Endpoint Detection and Response
- Identity and Access Management
- Incident Response and Ticketing
- IT Infrastructure
- Malware Analysis
- Network Security
- Orchestration
- SIEM and Analytics
- Threat Intelligence
- Vulnerability Management

32 Results

Accenture DeepSight
Threat Intelligence
The ThreatConnect and Accenture DeepSight integration enables users to collect and act on Accenture DeepSight Intelligence in the ThreatConnect platform.

Accenture iDefense IntelGraph
Threat Intelligence
The Accenture iDefense IntelGraph integration with ThreatConnect allows users to ingest the IntelGraph feed into ThreatConnect for analysis and response actions.

BAE Threat Intelligence
Threat Intelligence
The ThreatConnect integration with BAE Systems Threat Intelligence enables users to import Events and Attributes from the BAE MISP instance into ThreatConnect as Incidents and Indicators.

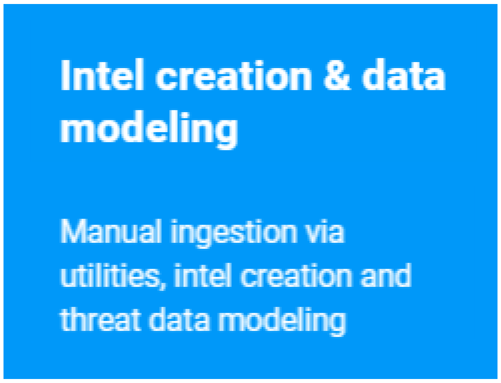
Bitdefender Advanced Threat Intelligence
Threat Intelligence
Bitdefender Advanced Threat Intelligence is a security service that enables security professionals to make more informed decisions by providing real-time threat knowledge that can be easily integrated in their existing technology stack.

Cofense Intelligence
Threat Intelligence
This ThreatConnect integration with Cofense Intelligence maps Cofense Intelligence into the ThreatConnect platform.

CrowdStrike Falcon Intelligence
Threat Intelligence
The ThreatConnect integration with CrowdStrike Falcon Intelligence allows ThreatConnect customers to import information Reports, Indicators, and Actors, along with all of their context from the CrowdStrike Falcon Intelligence feed into ThreatConnect.

ISACs & government agencies are beginning to adopt STIX/TAXII in greater form so ingesting intelligence from TAXII sources, or by ingesting bulletin emails, is a native capability of the platform. More complex methods for extracting detailed information from emails can also be achieved with email-trigger based playbooks.

Now that you have some content loaded, take a peek at the data by using Browse. You'll see data that is ingested in normalized, de-duplicated and maintained in each individual source so as to preserve context and scoring.



Intel creation & data modeling

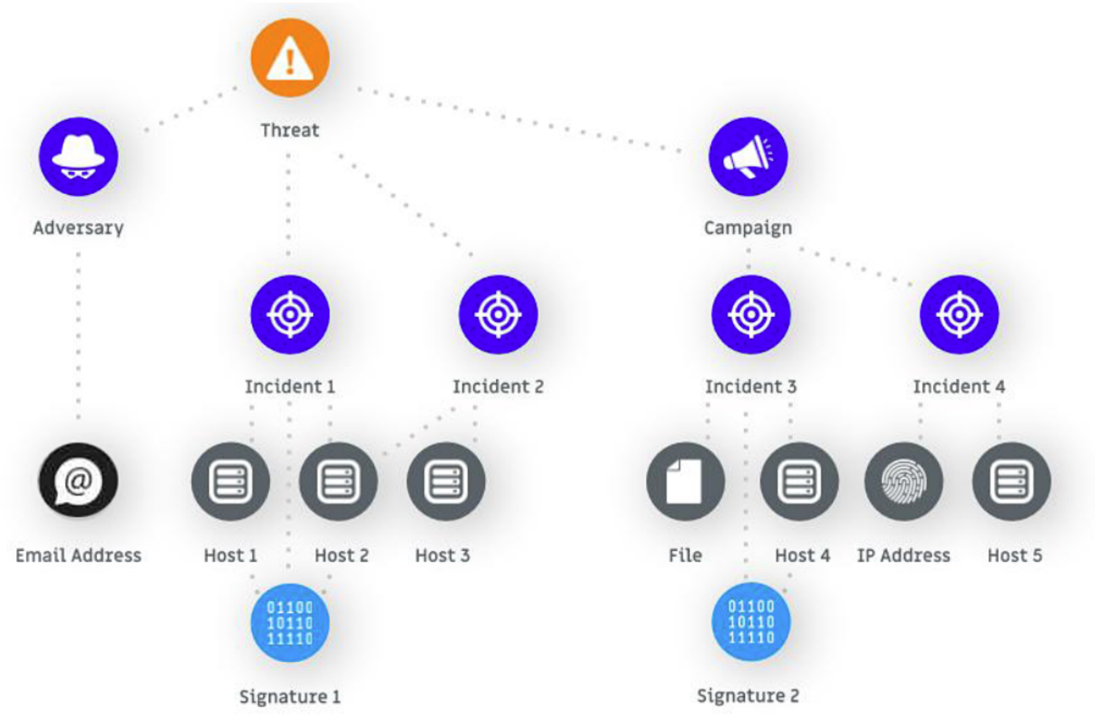
Manual ingestion via utilities, intel creation and threat data modeling

Okay you have a baseline, now what…

Many times the best intelligence is in the analyst’s own network, server logs or items that team members share in ad hoc forms. ThreatConnect provides a number of tools to help teams build threat models and collect important information that are a part of your threat landscape.

It's important to review how Threatconnect organizes threat information. ThreatConnect leverages the Diamond Model for intrusion analysis as a principle in that there are both strategic and tactical views of an intrusion that help you understand the root of attacks and give you the best chance toward defending yourself from future attacks.

Simply put, ThreatConnect helps you organize information so that key elements or objects involved in an attack are captured, along with the intent of malicious activity, along with the relationships between those objects. Below is an example of a model ThreatConnect helps create and store.



A lot of what we base our data model comes from industry standards like STIX, where relationships between data elements help forge a sense of strategy - strategic relationship between actors and victims, knowing what tools are used to attack and which infrastructure is used to accomplish the attack - that is what the diamond model is all about.

Behavior is captured using MITRE ATT&CK and attribution can be applied using methods such as Kill Chain or Phase of Intrusion.

One of the most common needs from analysts is an easy way to create intelligence from unstructured sources.   For example, Analysts can ingest content by importing it and create a model from it.   As threat data is collected or products, analysts are given tools to qualify and enrich the data ingested to give you a clue to its relevancy. ThreatConnect's Collective Analytics Layer (CAL) is a major part of that.

This process is best described in a scenario:

[Note there are also internal training documents that provide materials to demo]

1. Alert kicks off because of a policy violation on a windows server, noting an escalation of privs. After inspection suspicious files are found in a folder called *Urgent-Srv-update*
2. Analyst sends me a list of tactical threat indicators, concerned they are malicious. Take the list and pull them into the platform, tag them and associate them to an incident. Until we know more, not associating them to any particular actor.

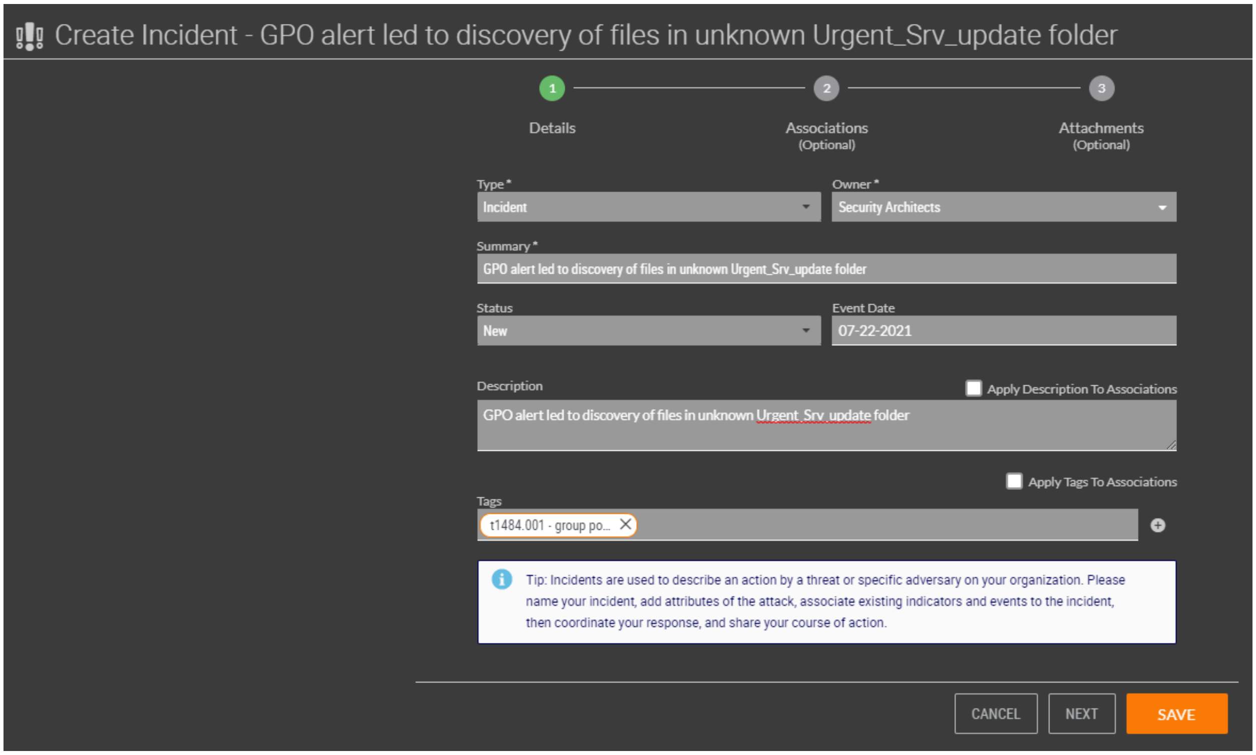
3. List of indicators taken from a windows server file_hashes.txt, that were stored in a folder called Urgent-Srv-update

   File_hashes.txt

   ```
   ---------------------------------------------------
   ec4cdc752c2ecd0d9f97491cc646a269
   edb648f6c3c2431b5b6788037c1cd8ef
   ee3e297abd0a5b943dce46f33f3d56fb
   ee4862bc4916fc22f219e1120bea734a
   ef14448bf97f49a2322d4c79e64bb60b
   ef2738889e9d041826d5c938a256bc45
   ef6fcdd1b55adf8ad6bcdf3d93fd109e
   ```

4. Incident response team that were discovered on a server which some security software triggered an alert when escalation of privs [T1484], domain policy modification

5. Step 1.
   a. Create an incident
   b. Summary: GPO alert led to discovery of files in unknown Urgent_Srv_update folder
   c. Reference MITRE ATT&CK to determine the appropriate TTP. In this case, we are looking for group policy modification T1484.001



Create Incident - GPO alert led to discovery of files in unknown Urgent_Srv_update folder

Type *: Incident

Owner *: Security Architects

Summary *: GPO alert led to discovery of files in unknown Urgent_Srv_update folder

Status: New

Event Date: 07-22-2021

Description: GPO alert led to discovery of files in unknown Urgent_Srv_update folder

□ Apply Description To Associations

□ Apply Tags To Associations

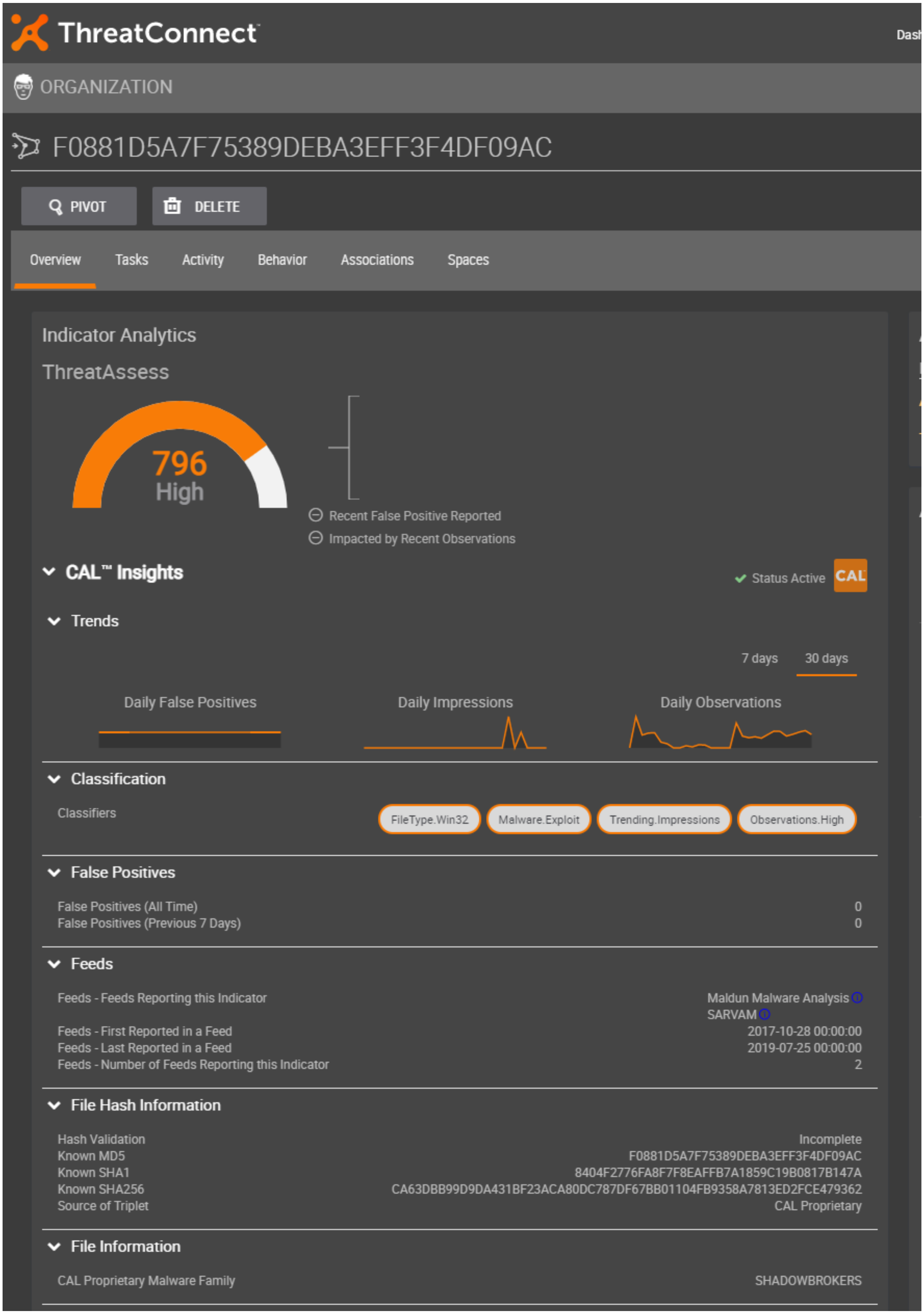
Tags: t1484.001 - group po...

Tip: Incidents are used to describe an action by a threat or specific adversary on your organization. Please name your incident, add attributes of the attack, associate existing indicators and events to the incident, then coordinate your response, and share your course of action.

6. CAL clues me into something regarding hash
   `F0881D5A7F75389DEBA3EFF3F4DF09AC`

[redacted]

7. CAL tells me a bit more about this indicator, which makes me more suspicious, update ranking.



F0881D5A7F75389DEBA3EFF3F4DF09AC

Indicator Analytics

ThreatAssess

796
High

⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

CAL™ Insights

✓ Status Active

Trends

Daily False Positives

Daily Impressions

Daily Observations

Classification

Classifiers: FileType.Win32, Malware.Exploit, Trending.Impressions, Observations.High

False Positives

False Positives (All Time)	0
False Positives (Previous 7 Days)	0

Feeds

Feeds - Feeds Reporting this Indicator	Maldun Malware Analysis SARVAM
Feeds - First Reported in a Feed	2017-10-28 00:00:00
Feeds - Last Reported in a Feed	2019-07-25 00:00:00
Feeds - Number of Feeds Reporting this Indicator	2

File Hash Information

Hash Validation	Incomplete
Known MD5	F0881D5A7F75389DEBA3EFF3F4DF09AC
Known SHA1	8404F2776FA8F7F8EAFFB7A1859C19B0817B147A
Known SHA256	CA63DBB99D9DA431BF23ACA80DC787DF67BB01104FB9358A7813ED2FCE479362
Source of Triplet	CAL Proprietary

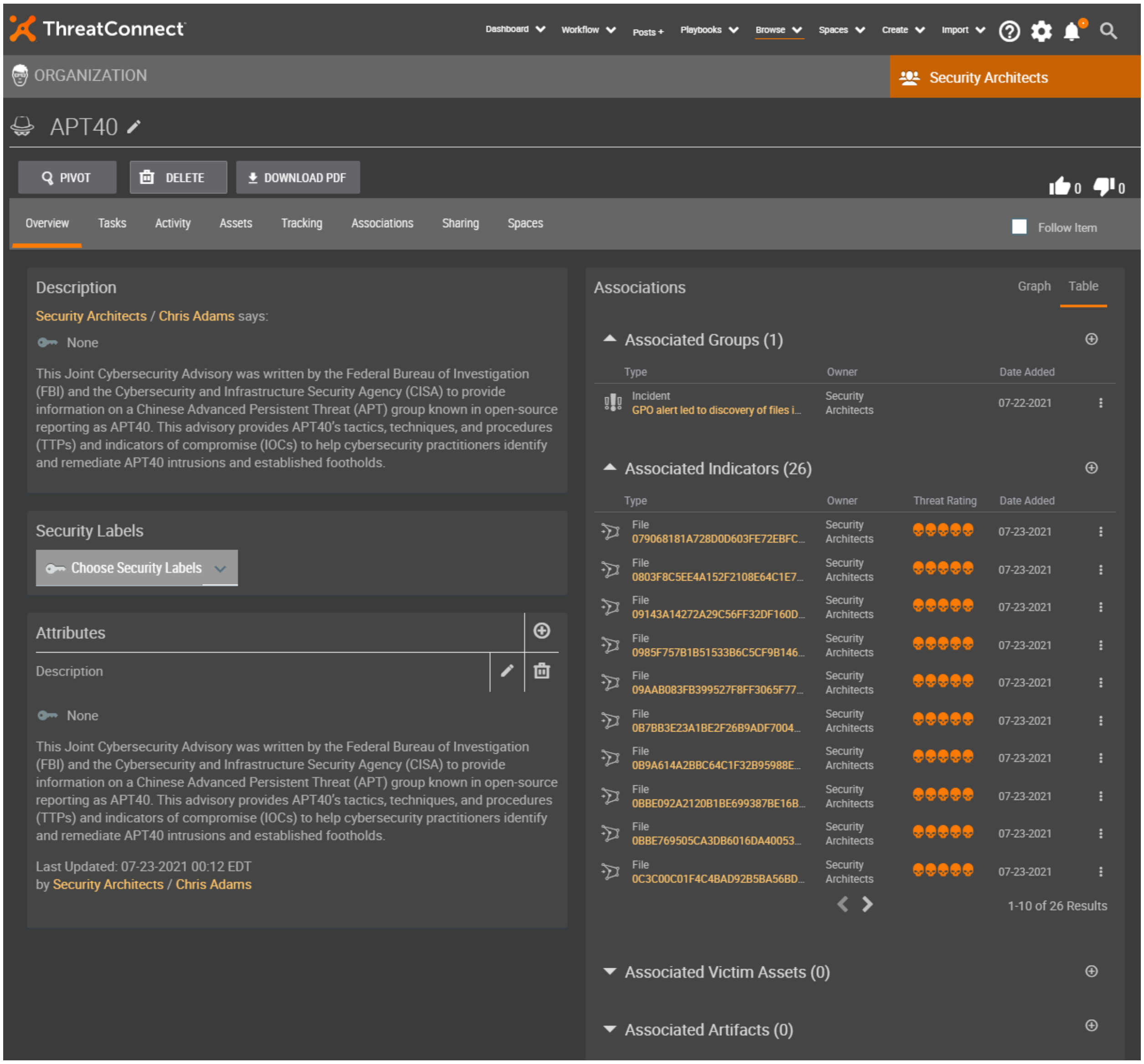
File Information

CAL Proprietary Malware Family	SHADOWBROKERS

Google search brings me to https://us-cert.cisa.gov/ncas/alerts/aa21-200a

So I pop open my favorite browser, loaded with the ThreatConnect Browser Extension and begin to scan the page. There are a large number of indicators, hashes and URLs, that I should probably know about since they could be related to the indicator. I'm going to collect those indicators and associate them to the threat actor described in the alert.

8. Create a new Adversary APT40 and associate the collected indicators, hashes and URLs, then associate the Incident to the adversary.



APT40

Description

Security Architects / Chris Adams says:

None

This Joint Cybersecurity Advisory was written by the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to provide information on a Chinese Advanced Persistent Threat (APT) group known in open-source reporting as APT40. This advisory provides APT40's tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help cybersecurity practitioners identify and remediate APT40 intrusions and established footholds.

Security Labels

Attributes

Description

None

This Joint Cybersecurity Advisory was written by the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to provide information on a Chinese Advanced Persistent Threat (APT) group known in open-source reporting as APT40. This advisory provides APT40's tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help cybersecurity practitioners identify and remediate APT40 intrusions and established footholds.

Last Updated: 07-23-2021 00:12 EDT
by Security Architects / Chris Adams

Associations

Associated Groups (1)

Type	Owner	Date Added
Incident GPO alert led to discovery of files i...	Security Architects	07-22-2021

Associated Indicators (26)

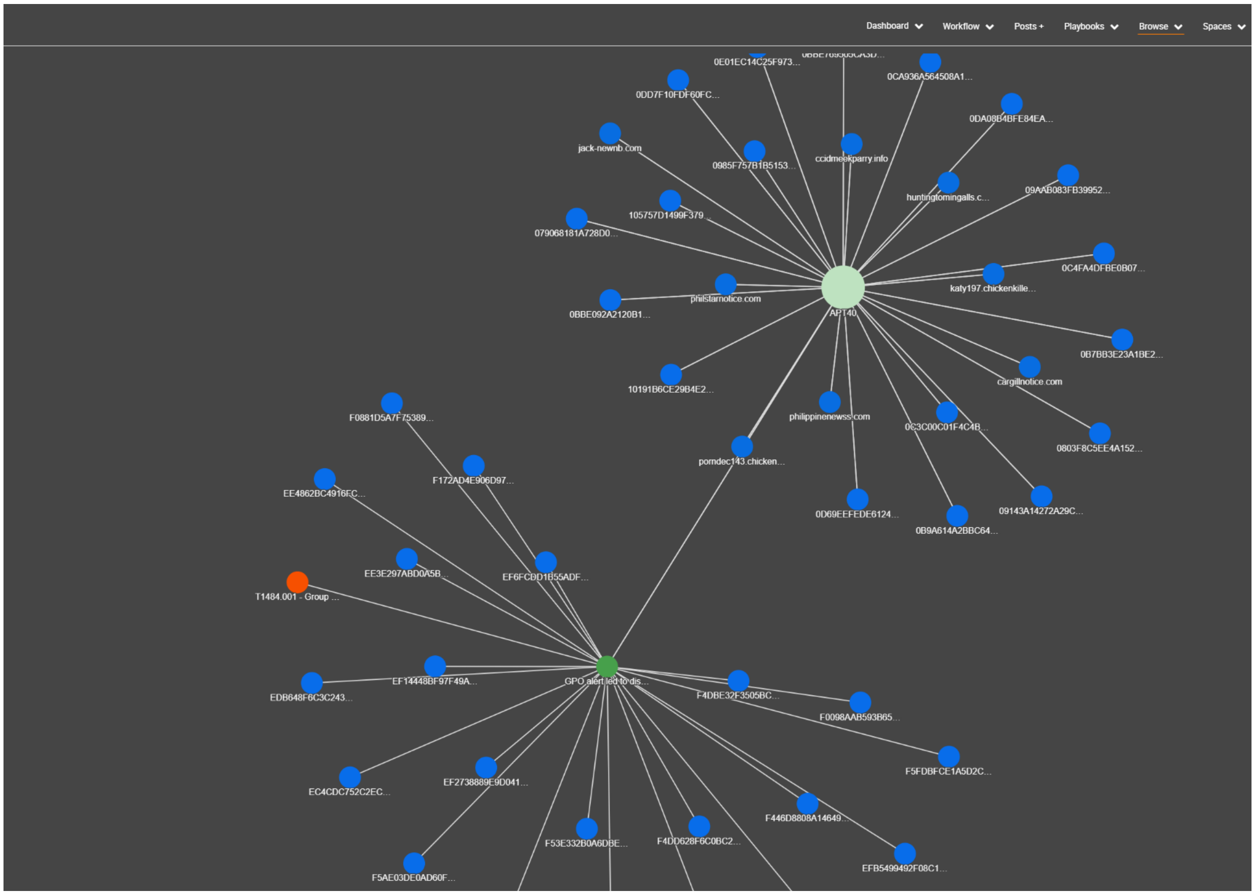
Type	Owner	Threat Rating	Date Added
File 079068181A728D0D603FE72EBFC...	Security Architects	☠☠☠☠☠	07-23-2021
File 0803F8C5EE4A152F2108E64C1E7...	Security Architects	☠☠☠☠☠	07-23-2021
File 09143A14272A29C56FF32DF160D...	Security Architects	☠☠☠☠☠	07-23-2021
File 0985F757B1B51533B6C5CF9B146...	Security Architects	☠☠☠☠☠	07-23-2021
File 09AAB083FB399527F8FF3065F77...	Security Architects	☠☠☠☠☠	07-23-2021
File 0B7BB3E23A1BE2F26B9ADF7004...	Security Architects	☠☠☠☠☠	07-23-2021
File 0B9A614A2BBC64C1F32B95988E...	Security Architects	☠☠☠☠☠	07-23-2021
File 0BBE092A2120B1BE699387BE16B...	Security Architects	☠☠☠☠☠	07-23-2021
File 0BBE769505CA3DB6016DA40053...	Security Architects	☠☠☠☠☠	07-23-2021
File 0C3C00C01F4C4BAD92B5BA56BD...	Security Architects	☠☠☠☠☠	07-23-2021

1-10 of 26 Results

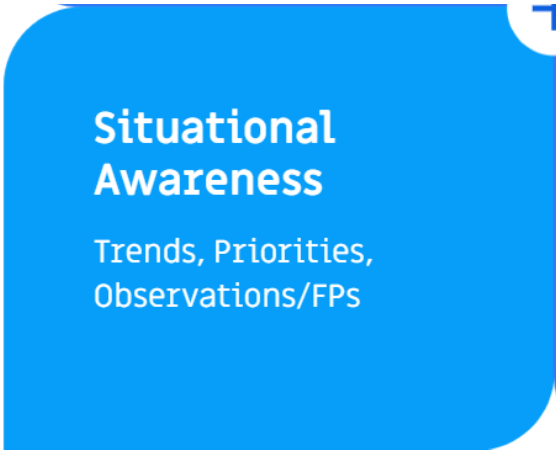
Associated Victim Assets (0)

Associated Artifacts (0)

You can now present your findings so far and begin the analysis of determining what actions to take based on your discovery.



The goal of this exercise was to get a sense for the utilities that ThreatConnect offers in order to collect intelligence from Ad Hoc sources and organize the data in a way that helps analysts understand the relationship between the items. As the last step using the visualizer depicts, many relationships can be formed at deeper levels that have associations that allow analysts to draw conclusions.



Situational Awareness

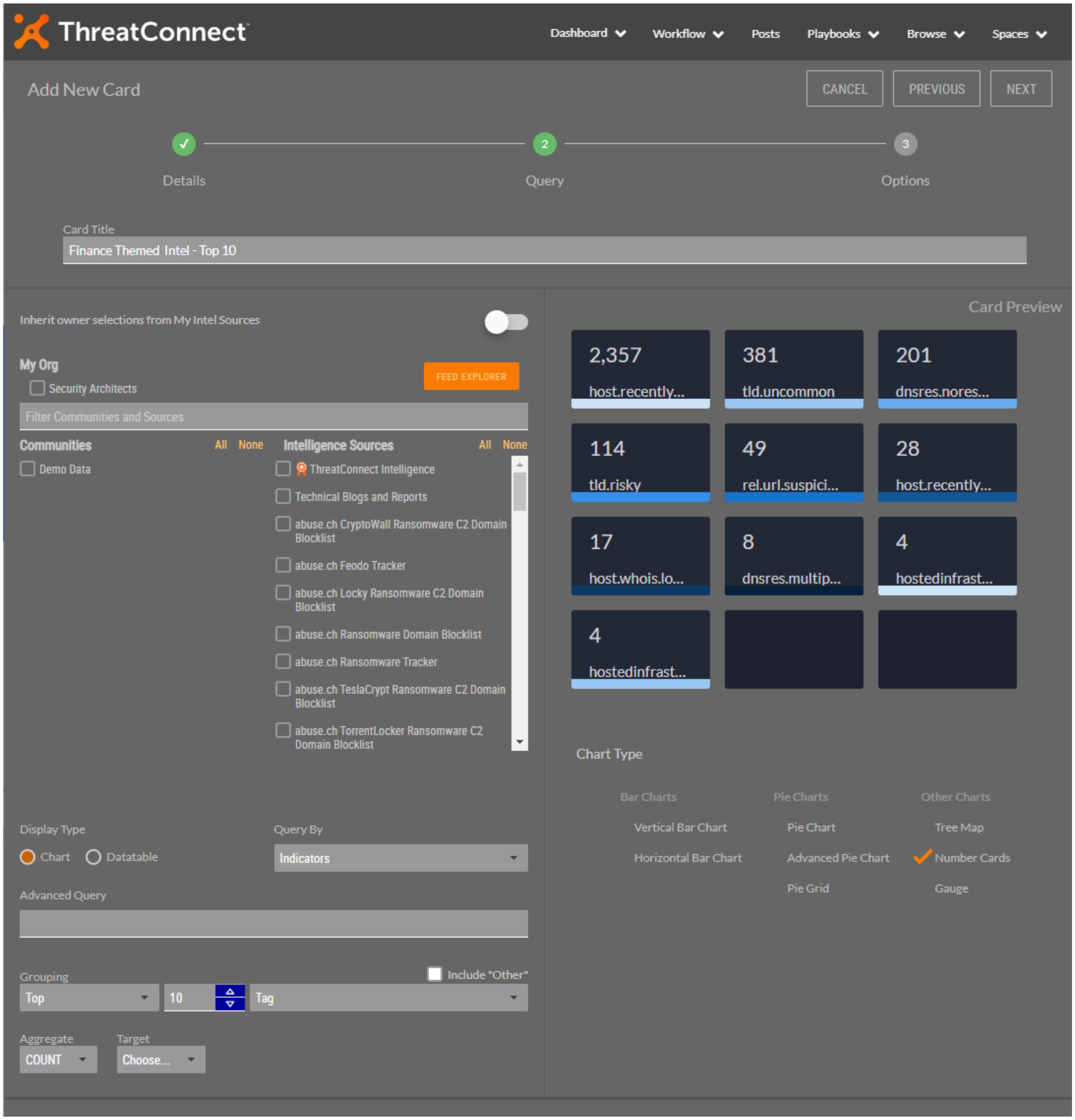
Trends, Priorities, Observations/FPs

Identify trends and stay abreast of what’s important to your organization.

You want to track intel that can have an impact on your organization and keep abreast of trends in the industry, across all of your sources of data, including the intelligence created by your own teams. In the previous example, we collected files from a folder that seemed suspicious and were able to determine potential relationships with well-known threat actors in a few number of steps. The next obvious question becomes how do I present or track the information I'm processing for the remainder of the security team?

Dashboards give you the ability to do all of that and share findings, trends, and priorities with team mates and leadership. Dashboard cards can be built with wizards to easily produce the content or use TQL to create custom queries that get to specific perspectives.

Example of something I’m looking for (Search - saved) - data set unique for the sector or level of interest



Card Title: Finance Themed Intel - Top 10

Inherit owner selections from My Intel Sources

My Org
□ Security Architects

Communities
□ Demo Data

Intelligence Sources
□ ThreatConnect Intelligence
□ Technical Blogs and Reports
□ abuse.ch CryptoWall Ransomware C2 Domain Blocklist
□ abuse.ch Feodo Tracker
□ abuse.ch Locky Ransomware C2 Domain Blocklist
□ abuse.ch Ransomware Domain Blocklist
□ abuse.ch Ransomware Tracker
□ abuse.ch TeslaCrypt Ransomware C2 Domain Blocklist
□ abuse.ch TorrentLocker Ransomware C2 Domain Blocklist

Display Type: ● Chart ○ Datatable

Query By: Indicators

Advanced Query:

Grouping: Top 10 Tag □ Include "Other"

Aggregate: COUNT

Target: Choose...

2,357 host.recently...	381 tld.uncommon	201 dnsres.nores...
114 tld.risky	49 rel.url.suspici...	28 host.recently...
17 host.whois.lo...	8 dnsres.multip...	4 hostedinfrast...
4 hostedinfrast...		

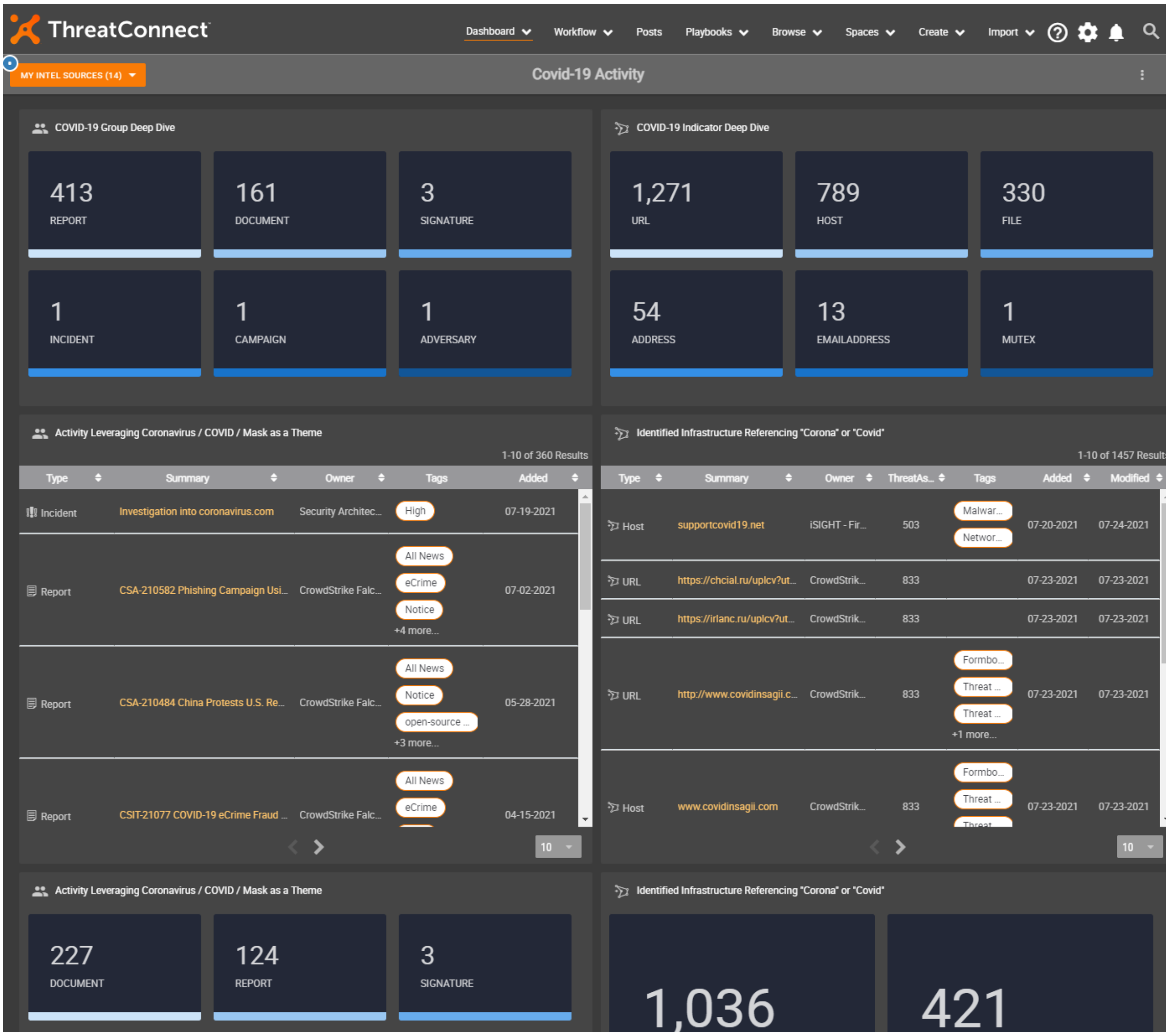
✓ Number Cards

Identification of Cyber Threat Intelligence Requirements

One of the primary functions of any threat intelligence team should be the successful establishment and fulfillment of individual priority intelligence requirements (PIRs). For example, what unique profiles, threat vectors, actors, exploits are you most concerned with that can impact your organization? Analysts can create content filters to collect and present the data sought for unique and focused intel cards.

Example, if your organization's security IAM solution is based on Microsoft AD, then clearly you want knowledge of AD, Windows-type vulnerabilities so you can know what to look for, get COA on how to defend or protect against them.

Perhaps your business is involved in the pharma sector and are concerned about threat actors using COVID-19 topics as a means to draw attention and clicks. Create a dashboard that centers on intel related to the pandemic.



Covid-19 Activity

COVID-19 Group Deep Dive

413 REPORT	161 DOCUMENT	3 SIGNATURE
1 INCIDENT	1 CAMPAIGN	1 ADVERSARY

COVID-19 Indicator Deep Dive

1,271 URL	789 HOST	330 FILE
54 ADDRESS	13 EMAILADDRESS	1 MUTEX

Activity Leveraging Coronavirus / COVID / Mask as a Theme

1-10 of 360 Results

Type	Summary	Owner	Tags	Added
Incident	Investigation into coronavirus.com	Security Architec...	High	07-19-2021
Report	CSA-210582 Phishing Campaign Usi...	CrowdStrike Falc...	All News eCrime Notice +4 more...	07-02-2021
Report	CSA-210484 China Protests U.S. Re...	CrowdStrike Falc...	All News Notice open-source ... +3 more...	05-28-2021
Report	CSIT-21077 COVID-19 eCrime Fraud ...	CrowdStrike Falc...	All News eCrime	04-15-2021

10

Identified Infrastructure Referencing "Corona" or "Covid"

1-10 of 1457 Result

Type	Summary	Owner	ThreatAs...	Tags	Added	Modified
Host	supportcovid19.net	iSIGHT - Fir...	503	Malwar... Networ...	07-20-2021	07-24-2021
URL	https://chcial.ru/uplcv?ut...	CrowdStrik...	833		07-23-2021	07-23-2021
URL	https://irlanc.ru/uplcv?ut...	CrowdStrik...	833		07-23-2021	07-23-2021
URL	http://www.covidinsagii.c...	CrowdStrik...	833	Formbo... Threat ... Threat ... +1 more...	07-23-2021	07-23-2021
Host	www.covidinsagii.com	CrowdStrik...	833	Formbo... Threat ... Threat	07-23-2021	07-23-2021

10

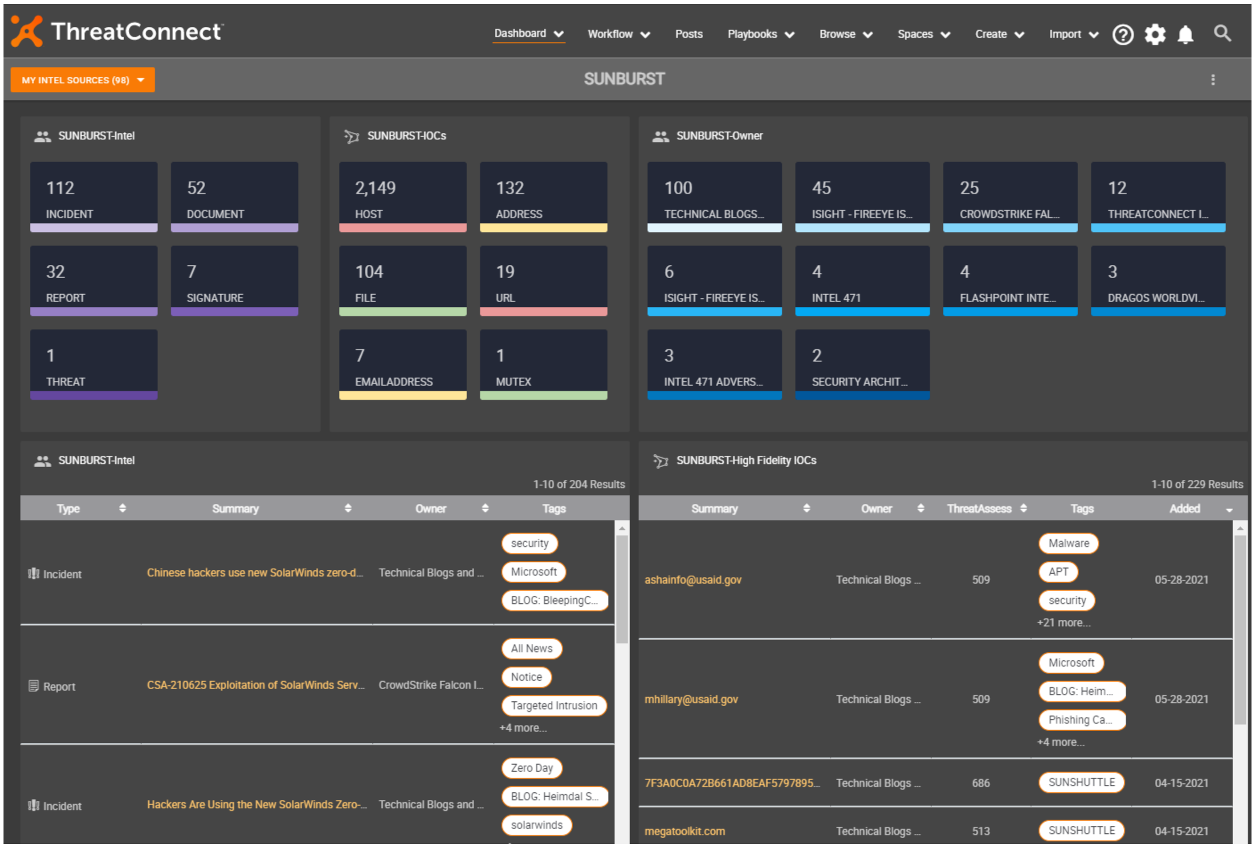
Activity Leveraging Coronavirus / COVID / Mask as a Theme

227 DOCUMENT	124 REPORT	3 SIGNATURE

Identified Infrastructure Referencing "Corona" or "Covid"

1,036	421

Or perhaps your infrastructure may be vulnerable to the Sunburst threat vector.



SUNBURST

SUNBURST-Intel

112 INCIDENT	52 DOCUMENT
32 REPORT	7 SIGNATURE
1 THREAT	

SUNBURST-IOCs

2,149 HOST	132 ADDRESS
104 FILE	19 URL
7 EMAILADDRESS	1 MUTEX

SUNBURST-Owner

100 TECHNICAL BLOGS...	45 ISIGHT - FIREEYE IS...	25 CROWDSTRIKE FAL...	12 THREATCONNECT I...
6 ISIGHT - FIREEYE IS...	4 INTEL 471	4 FLASHPOINT INTE...	3 DRAGOS WORLDVI...
3 INTEL 471 ADVERS...	2 SECURITY ARCHIT...		

SUNBURST-Intel

1-10 of 204 Results

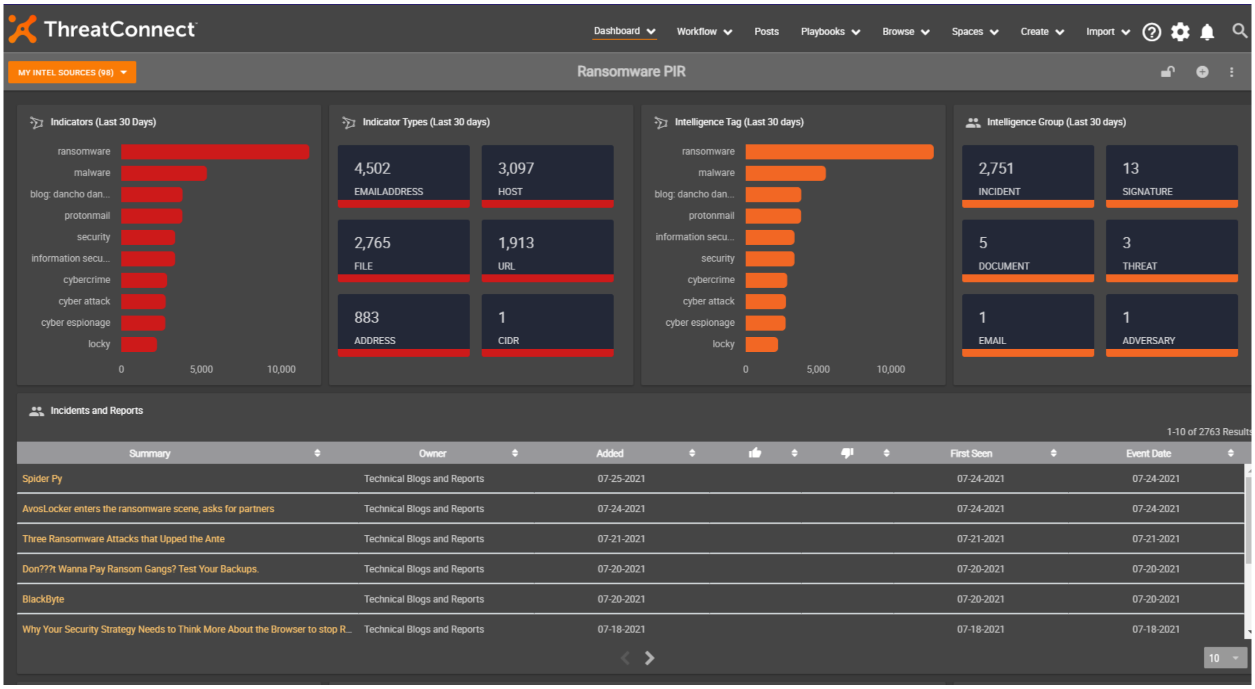
Type	Summary	Owner	Tags
Incident	Chinese hackers use new SolarWinds zero-d...	Technical Blogs and ...	security Microsoft BLOG: BleepingC...
Report	CSA-210625 Exploitation of SolarWinds Serv...	CrowdStrike Falcon I...	All News Notice Targeted Intrusion +4 more...
Incident	Hackers Are Using the New SolarWinds Zero-...	Technical Blogs and ...	Zero Day BLOG: Heimdal S... solarwinds

SUNBURST-High Fidelity IOCs

1-10 of 229 Results

Summary	Owner	ThreatAssess	Tags	Added
ashainfo@usaid.gov	Technical Blogs ...	509	Malware APT security +21 more...	05-28-2021
mhillary@usaid.gov	Technical Blogs ...	509	Microsoft BLOG: Heim... Phishing Ca... +4 more...	05-28-2021
7F3A0C0A72B661AD8EAF5797895...	Technical Blogs ...	686	SUNSHUTTLE	04-15-2021
megatoolkit.com	Technical Blogs ...	513	SUNSHUTTLE	04-15-2021

Or perhaps one of the main concerns from leadership is that a business partner just experienced a ransomware attack. Create a PIR dashboard that focuses on that topic of choice and recreate others using some of the same saved queries used to generate previous cards.



Ransomware PIR

Indicators (Last 30 Days)

Indicator Types (Last 30 days)

4,502 EMAILADDRESS	3,097 HOST
2,765 FILE	1,913 URL
883 ADDRESS	1 CIDR

Intelligence Tag (Last 30 days)

Intelligence Group (Last 30 days)

2,751 INCIDENT	13 SIGNATURE
5 DOCUMENT	3 THREAT
1 EMAIL	1 ADVERSARY

Incidents and Reports

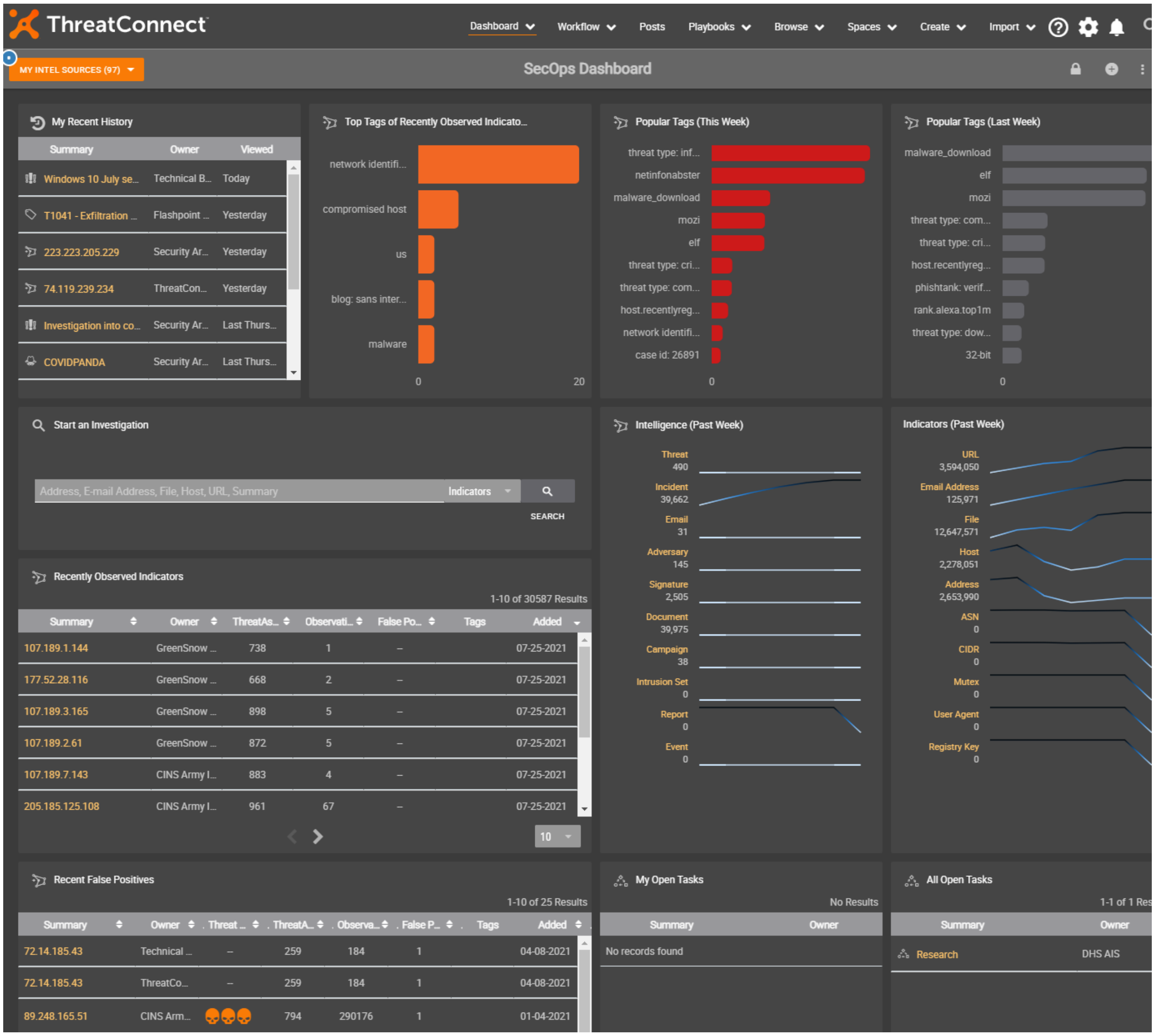
1-10 of 2763 Results

Summary	Owner	Added	👍	👎	First Seen	Event Date
Spider Py	Technical Blogs and Reports	07-25-2021			07-24-2021	07-24-2021
AvosLocker enters the ransomware scene, asks for partners	Technical Blogs and Reports	07-24-2021			07-24-2021	07-24-2021
Three Ransomware Attacks that Upped the Ante	Technical Blogs and Reports	07-21-2021			07-21-2021	07-21-2021
Don???t Wanna Pay Ransom Gangs? Test Your Backups.	Technical Blogs and Reports	07-20-2021			07-20-2021	07-20-2021
BlackByte	Technical Blogs and Reports	07-20-2021			07-20-2021	07-20-2021
Why Your Security Strategy Needs to Think More About the Browser to stop R...	Technical Blogs and Reports	07-18-2021			07-18-2021	07-18-2021

Threat intelligence must be able to answer these questions with actionable responses, enabling analysts to divide resources where they are most needed in a timely manner.

However, not that Operationalizing intelligence is where the rubber starts to meet the road. What intelligence is most relevant to your organization? Answer: That which is discovered in your network.

Observed indicators (referred to as *sightings* in STIX) signify that an IOC was found in security infrastructure and reported, in this case, in this Security Operations dashboard card named **Recently Observed Indicators**.



My Recent History

Summary	Owner	Viewed
Windows 10 July se...	Technical B...	Today
T1041 - Exfiltration ...	Flashpoint ...	Yesterday
223.223.205.229	Security Ar...	Yesterday
74.119.239.234	ThreatCon...	Yesterday
Investigation into co...	Security Ar...	Last Thurs...
COVIDPANDA	Security Ar...	Last Thurs...

Recently Observed Indicators

1-10 of 30587 Results

Summary	Owner	ThreatAs...	Observati...	False Po...	Tags	Added
107.189.1.144	GreenSnow ...	738	1	–		07-25-2021
177.52.28.116	GreenSnow ...	668	2	–		07-25-2021
107.189.3.165	GreenSnow ...	898	5	–		07-25-2021
107.189.2.61	GreenSnow ...	872	5	–		07-25-2021
107.189.7.143	CINS Army I...	883	4	–		07-25-2021
205.185.125.108	CINS Army I...	961	67	–		07-25-2021

Recent False Positives

1-10 of 25 Results

Summary	Owner	Threat ...	ThreatA...	Observa...	False P...	Tags	Added
72.14.185.43	Technical ...	–	259	184	1		04-08-2021
72.14.185.43	ThreatCo...	–	259	184	1		04-08-2021
89.248.165.51	CINS Arm...	💀💀💀	794	290176	1		01-04-2021

My Open Tasks

No Results

Summary	Owner
No records found	

All Open Tasks

1-1 of 1 Res

Summary	Owner
Research	DHS AIS

Returning to our previous example, strategic intel begins to come into view when we identify indicators observed in our network that have been associated with threat actors. That type of information becomes relevant to senior leadership, especially if the actor is known to exploit particular assets identified in your asset risk profile.

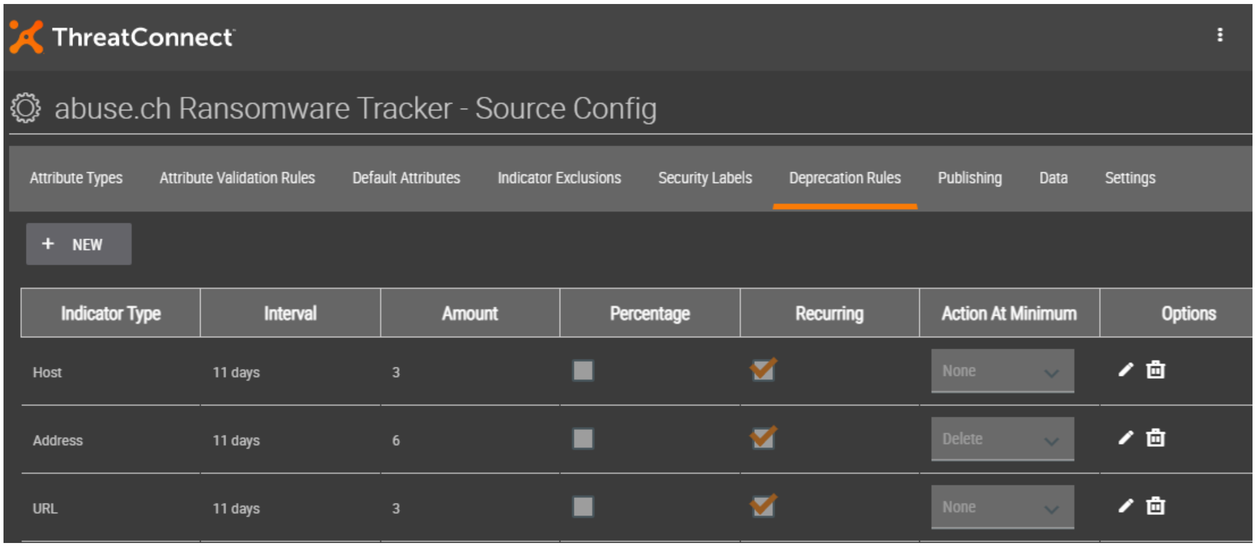
Intel Lifecycle Mgmt

Feed maintenance, deprecation, QoS

Managing a threat repository involves maintenance at the system-level, activities that are typically performed on the back end by DevOps for those who leverage dedicated cloud instances, and at the intel data-level. Data maintenance involves deprecation of stale data, altering the state of data between being active or inactive, tuning feeds based upon sightings and false positives, and monitoring feed growth over time.

Indicator confidence deprecation is a great way to allow ThreatConnect® Indicators to drop in Confidence Rating over time or be deleted if the Confidence Rating is not being maintained and updated. Confidence deprecation is used in the case of an Indicator, such as an IP Address, that is no longer being used for any malicious activity for a certain amount of time.

Below is an image of the configuration page where confidence deprecation is set, to the point of deletion if desired.



abuse.ch Ransomware Tracker - Source Config

Indicator Type	Interval	Amount	Percentage	Recurring	Action At Minimum	Options
Host	11 days	3	□	☑	None	✎ 🗑
Address	11 days	6	□	☑	Delete	✎ 🗑
URL	11 days	3	□	☑	None	✎ 🗑

Indicator Status categorizes Indicators in ThreatConnect as being in one of two states:

- Active: The Indicator is considered to be an Indicator of Compromise (IOC) at the current time and should be treated in accordance with its ThreatAssess score.

- Inactive: The Indicator is not currently considered an IOC, but is being kept in ThreatConnect for historical accuracy rather than being deleted.

Knowledge of whether an Indicator is active or not allows ThreatConnect users to make more informed analytical choices and helps prevent them from wasting time and resources on Indicators that do not have any recent activity or are outdated.

When noting observables and FPs we begin to get a sense of what to focus on from an intelligence perspective, which leads us to characterize the sources of data set up in the instance. Reducing impact of false positives gives time back to your team to focus on things that matter, hence formulating a strategy for tracking where FPs are most commonly occurring should be considered by threat intel teams. Recall that administrators can adjust their consumption of feeds by turning them off within Feed Explorer should it be discovered over time that certain feeds are more of a nuisance than benefit.

Lastly, administrators may want to monitor the growth of feeds over time to get a sense of which feeds are providing in terms of volume. It’s not uncommon for externally sourced feeds to go offline when their back-end systems are interrupted or fail, so knowing when they do is important.