Enterprise Strategy Group | **Getting to the bigger truth.™**

ESG Lab Validation

ThreatConnect Security Operations and Analytics Platform

Orchestrate Security Processes, Analyze Data, and Proactively Hunt Threats Based on Vetted, Relevant Threat Intelligence

By Tony Palmer, Senior Validation Analyst; Alex Arcilla, Validation Analyst; and Domenic Amato, Associate Validation Analyst

January 2019

This ESG Lab Report was commissioned by ThreatConnect
and is distributed under license from ESG.

Contents

ESG Validation Reports

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

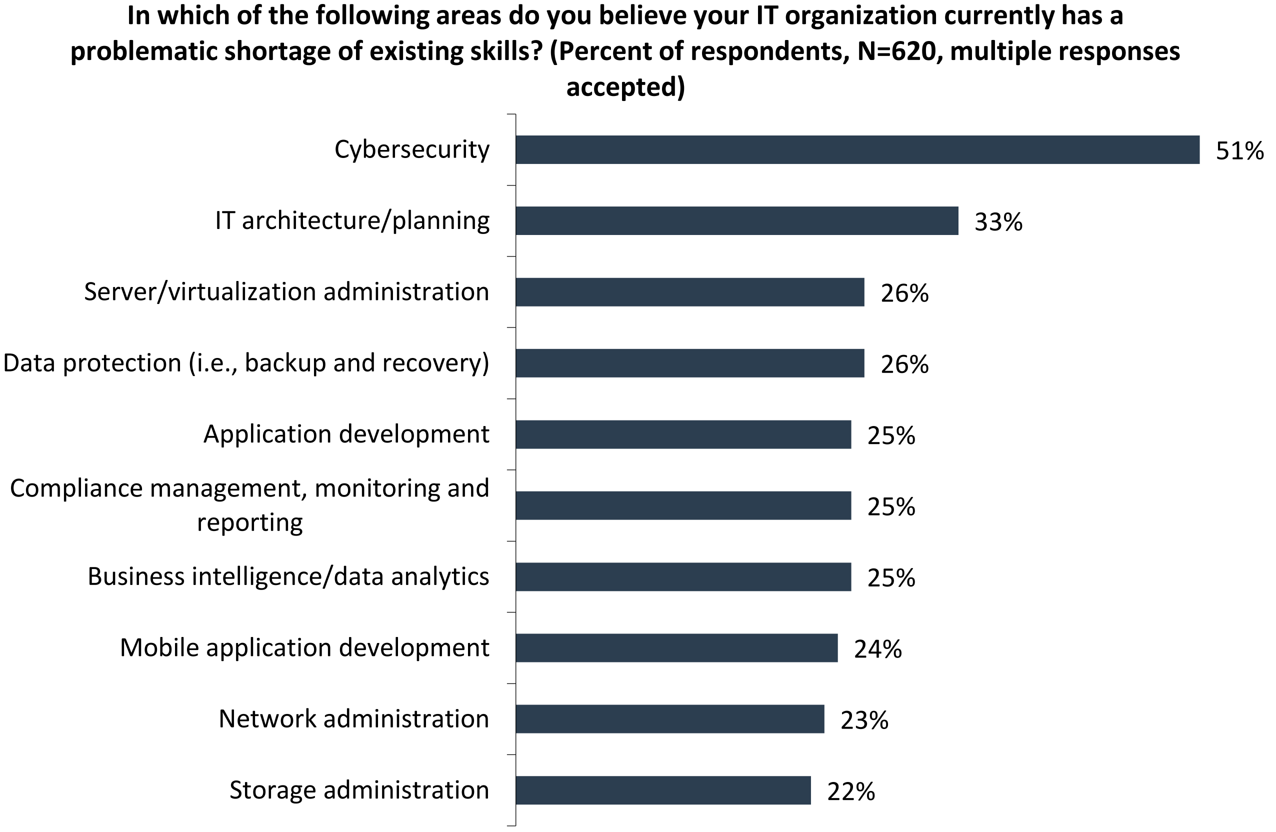
Introduction

ESG Lab evaluated the ThreatConnect threat intelligence, analytics, and orchestration platform to validate how it enables organizations to identify, manage, and block threats. We also gauged the extensibility of the platform to enable users to adapt and create automation for their processes, rather than forcing them to adapt their processes to ThreatConnect's paradigm.

Background

Research from ESG and the Information Systems Security Association (ISSA) reveals that 70% of cybersecurity professionals believe that the global cybersecurity skills shortage (see Figure 1)[1] has impacted their organizations.[2] Based upon this research, it's clear that most organizations don't have enough cybersecurity staffers, don't have some necessary cybersecurity skills, or both—a daunting situation. Meanwhile, the number of security incidents that businesses must investigate and respond to has grown exponentially; the proliferation of new systems and applications is creating more security incident scenarios, while better detection tools are generating more alerts. The cybersecurity skills shortage makes it prohibitively difficult to respond to these security challenges by simply adding more personnel. If the security analysts and investigators you have don't have the best incident response tools, investigation and resolution of security events will almost certainly take longer, increasing the prospect of a damaging data breach.

Figure 1. Top Ten Areas of IT Skills Shortages



Source: Enterprise Strategy Group

[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

[2] Source: ESG Research Report, *ESG/ISSA Research Report: The Life and Times of Cybersecurity Professionals*, November 2017.

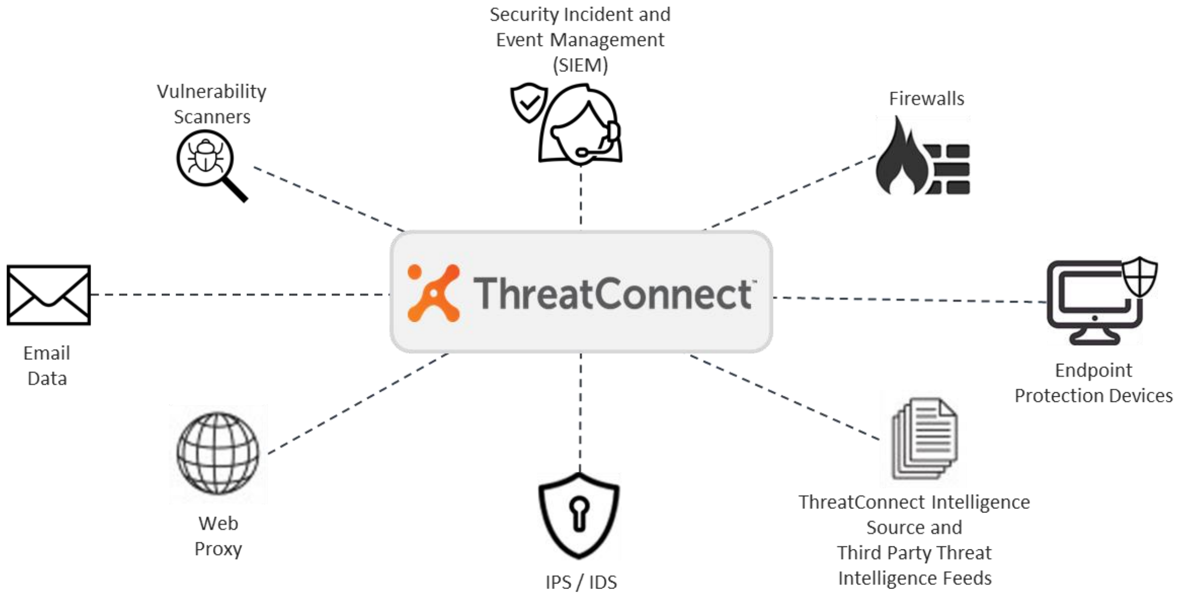
ESG research reveals that the cybersecurity landscape is becoming increasingly difficult to manage, with 72% of respondents reporting cybersecurity analytics/operations to be somewhat or significantly more difficult today than it was two years ago.[3] Organizations' critical assets, including but not limited to intellectual property, customer information, and financial data, are increasingly at risk of compromise. Repercussions from a breach are severe, including financial penalties, impact to brand and company valuation, and lawsuits. Organizations need a sophisticated incident response strategy to respond to incidents with agility and minimize risks.

The Solution: The ThreatConnect Platform

ThreatConnect is a security operations and analytics platform that harmonizes all the features of a threat intelligence platform with security automation and orchestration. The ThreatConnect platform is designed to give organizations the tools needed to gain visibility on potential threats while maximizing efficiency by automating security measures and data digestion from dozens of sources. Orchestrating security and analytics not only frees up time for IT administrators but also builds confidence in their threat intelligence.

ThreatConnect aims to provide an all-encompassing platform for your security team to reduce mean time to detect and mean time to respond, and to make informed strategic decisions about your security strategy, as shown in Figure 2. ThreatConnect combines data processing and organization with team workflow management tools and dynamic dashboards for drilling into specific threats. More than 100 intelligence feeds are filtered and combed to fit an organization's requirements before being sent as honed intelligence to tools like SIEMs, firewalls, or analyst reports. ThreatConnect enables users to orchestrate threat response with custom playbooks that can be integrated with third-party tools. Then, its customizable dashboards let your management team and day-to-day users get a complete picture of the information they need.

Figure 2. ThreatConnect's Complete Security Platform


Security Incident and Event Management (SIEM)
Vulnerability Scanners
Firewalls
ThreatConnect
Email Data
Endpoint Protection Devices
Web Proxy
IPS / IDS
ThreatConnect Intelligence Source and Third Party Threat Intelligence Feeds

As cybersecurity becomes more important (and difficult) to manage, ThreatConnect's consolidated platform approach has been engineered to give organizations a leg up with threat intelligence. ThreatConnect's customizable threat response playbooks require no prior coding experience to give security analysts and IT admins the ability to automate data digestion and enrichment from dozens of open source and premium feeds, and keep their organizations informed and ready to act.

[3] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.

ESG Lab Validation

ESG Lab performed hands-on evaluation and testing of the ThreatConnect platform. Testing was designed to validate how ThreatConnect enables organizations to identify, manage, and block threats, with additional focus on the extensibility of ThreatConnect as a true enterprise platform—designed to enable users to adapt and create automation for their processes.

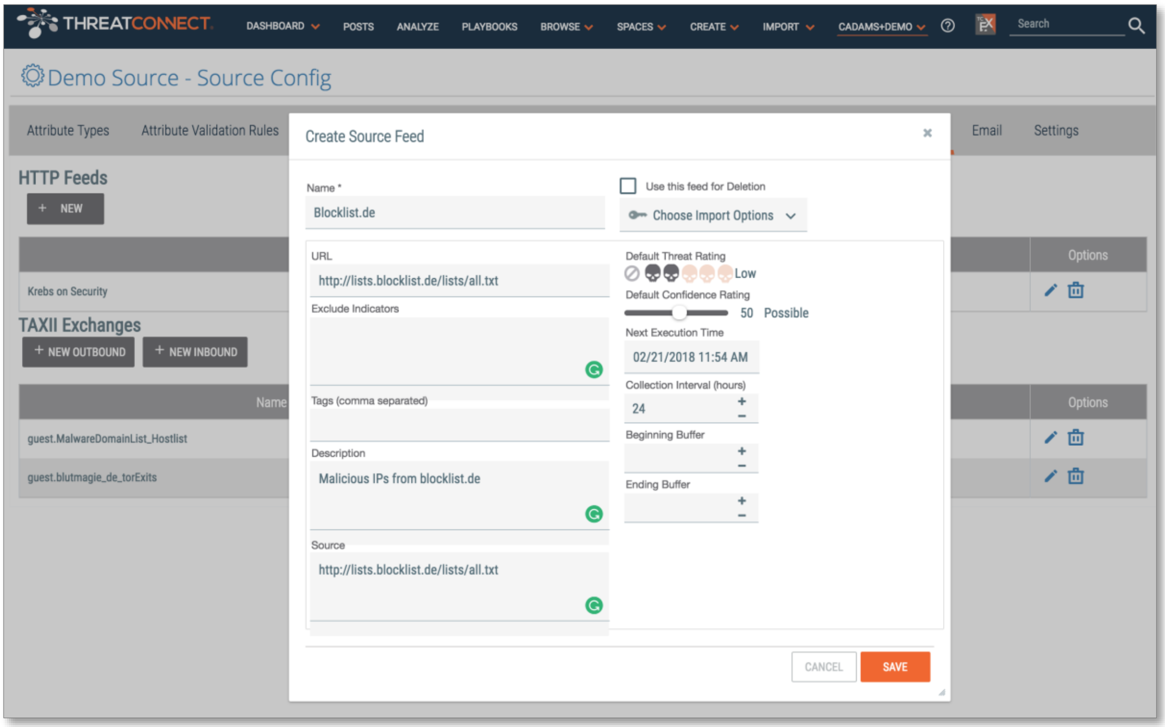
Reducing Mean Time to Detect Threats

An organization's threat intelligence is only as good as the sources it relies on, and ThreatConnect enables organizations to ingest all the intelligence feeds from both their own systems as well as open source and premium feeds. The platform already supports more than 100 carefully selected open source feeds that come standard and integrates with all the major premium threat feeds. ESG looked at the multiple ways users can access and ingest threat feeds and how ThreatConnect leverages all this data to reduce the time it takes to detect threats.

ESG Lab Testing

Setting up the ingest of a simple feed of indicators was straightforward in the user interface. In the *Posts* section, users can click on any available source feed to see details, any associations the source has, and even user-created posts. ESG Lab created a custom source feed by clicking on the pencil button to edit a feed, then selected specific indicators to be targeted (see Figure 3). The next time ThreatConnect combs this source for threat intel, the process will be automated and get the user the relevant information much faster.

Figure 3. Custom-configuring a Source Feed



Demo Source - Source Config

Krebs on Security

guest.MalwareDomainList_Hostlist

guest.blutmagie_de_torExits

Create Source Feed

Name *: Blocklist.de

□ Use this feed for Deletion

Choose Import Options

URL: http://lists.blocklist.de/lists/all.txt

Exclude Indicators:

Tags (comma separated):

Description: Malicious IPs from blocklist.de

Source: http://lists.blocklist.de/lists/all.txt

Default Threat Rating: Low

Default Confidence Rating: 50 Possible

Next Execution Time: 02/21/2018 11:54 AM

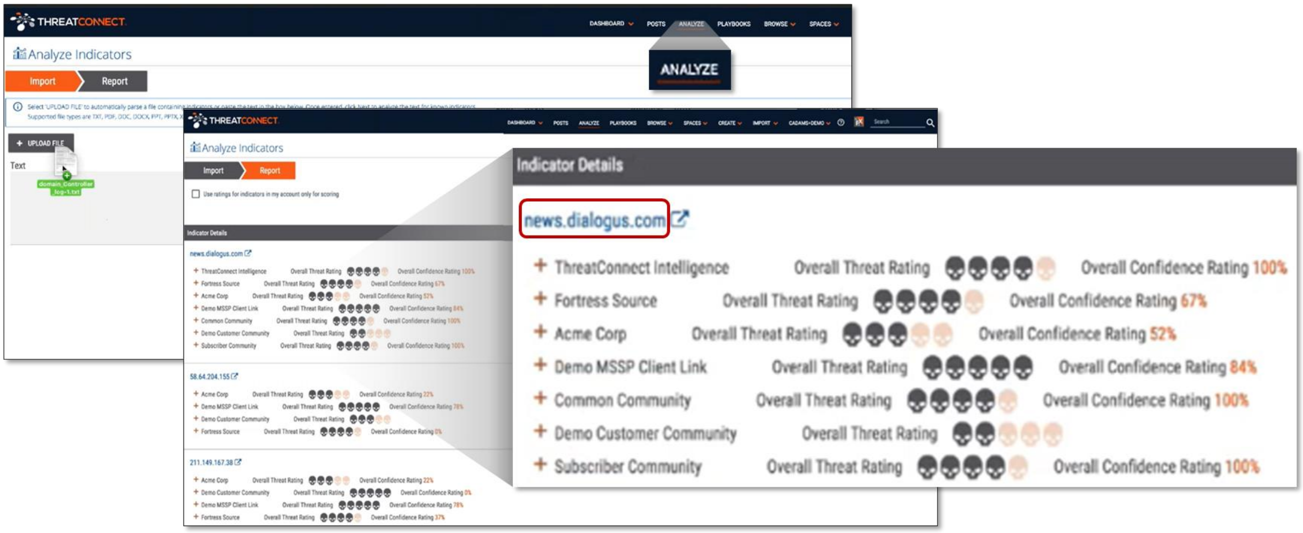
Collection Interval (hours): 24

Beginning Buffer:

Ending Buffer:

Next, ESG Lab examined how ThreatConnect can highlight potential intrusions by matching indicators of compromise to manually uploaded log, email, or any arbitrary files. It is noteworthy that ThreatConnect offers this capability in its free product as well. We navigated to the **Analyze Indicators** page by clicking on the **Analyze** menu option (see Figure 4). We input the file named *domain_Controller_log-1.txt* by dragging its icon onto the **+Upload File** button. Dragging the file icon automatically inputs the file contents into the text box. ThreatConnect then parsed the content to extract indicators of potential security threats, such as URLs and IP addresses. The indicators are listed in blue text under **Indicator Details**. Under each indicator, ThreatConnect calculates both a threat rating and confidence rating, derived from intelligence sources to which the organization subscribes. While the threat rating indicates how severe the potential for harm is, the confidence rating communicates how likely it is that the threat will cause issues. ThreatConnect also calculates an overall score to help the analyst assess the indicators relative to one another, with a higher score showing the more critical ones to address.

Figure 4. Log Ingestion Using the Analyze Tool



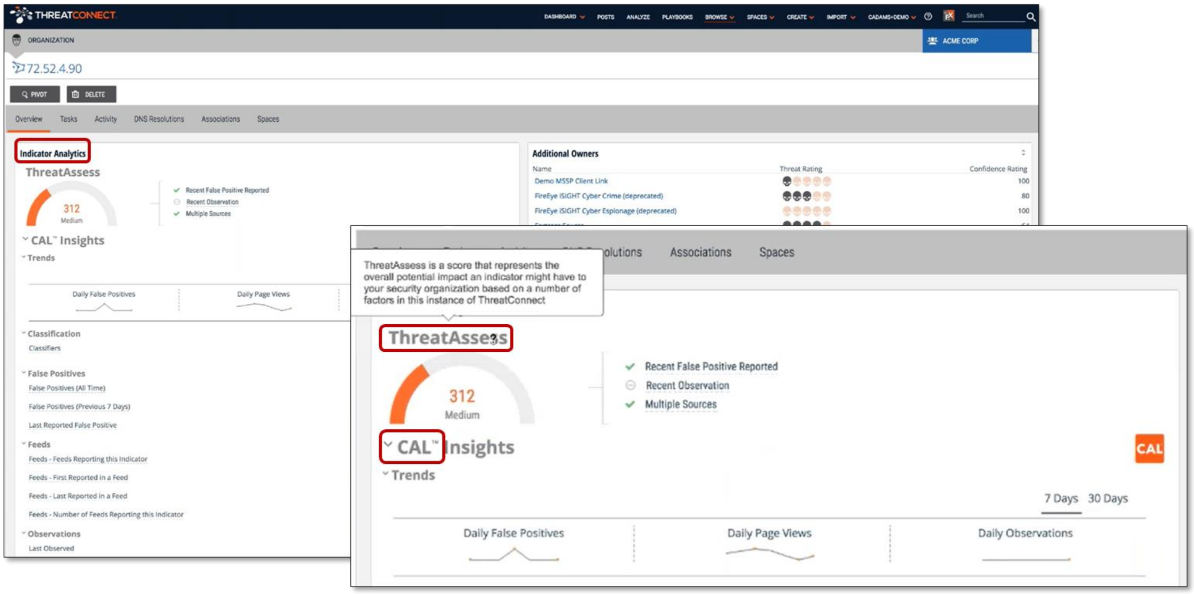
Indicator Details

news.dialogus.com

+ ThreatConnect Intelligence	Overall Threat Rating	Overall Confidence Rating 100%
+ Fortress Source	Overall Threat Rating	Overall Confidence Rating 67%
+ Acme Corp	Overall Threat Rating	Overall Confidence Rating 52%
+ Demo MSSP Client Link	Overall Threat Rating	Overall Confidence Rating 84%
+ Common Community	Overall Threat Rating	Overall Confidence Rating 100%
+ Demo Customer Community	Overall Threat Rating	
+ Subscriber Community	Overall Threat Rating	Overall Confidence Rating 100%

The next step in the process was to use ThreatConnect's ThreatAssess and Collective Analytics Layer (CAL) to find relevant threat intel on a singular indicator (see Figure 5). ThreatAssess uses an algorithm based on activity from subscribed source feeds around the indicator to give an easy-to-read threat score. CAL provides a lot more information, the most impressive being how many times this indicator has been seen in other infrastructures, investigated, or claimed as a false positive. It was easy to see how users can quickly draw conclusions around potential threats to find critical matches in seconds rather than spending hours manually reading a log or googling IP addresses for results.

Figure 5. ThreatAssess Score and CAL Insights

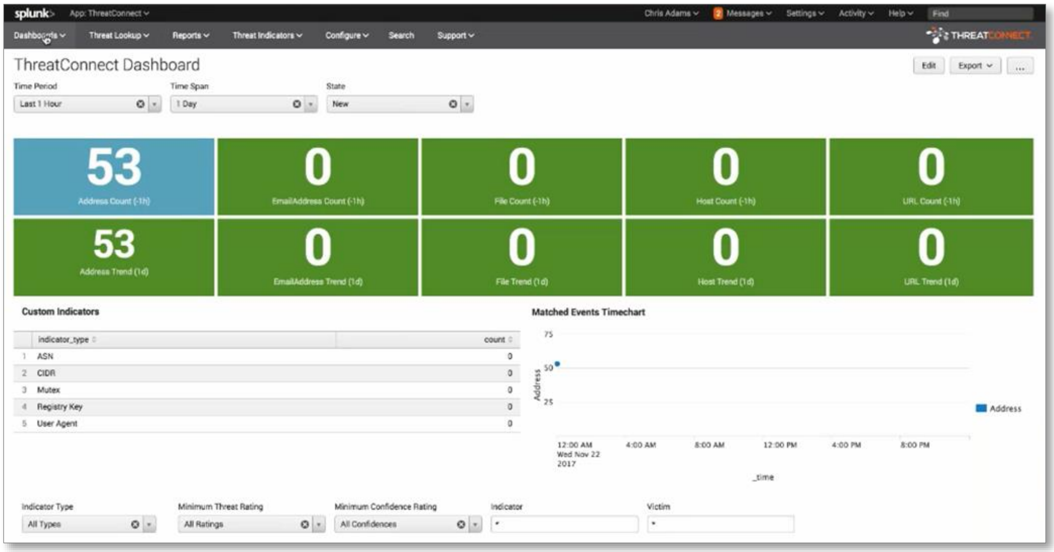


Name	Threat Rating	Confidence Rating
Demo MSSP Client Link		100
FireEye iSIGHT Cyber Crime (deprecated)		80
FireEye iSIGHT Cyber Espionage (deprecated)		100

ThreatAssess is a score that represents the overall potential impact an indicator might have to your security organization based on a number of factors in this instance of ThreatConnect

The speed at which ThreatConnect dissected the standard and custom sources became much more evident when integrated with a SIEM like Splunk, a software platform that can collect and store machine-generated data from websites, applications, sensors, and devices associated with an organization. Using the ThreatConnect application in Splunk Base, ESG Lab watched as threat intel was updated for users on a dashboard. The ThreatConnect app took indicator traffic from the user's firewall and redisplayed anything that flowed through Splunk recently. Over the span of an hour, 53 different matches were found and each could be drilled into for a detailed report in the event triage dashboard (see Figure 6).

Figure 6. ThreatConnect Dashboard Results in Splunk Base



ThreatConnect Dashboard

Time Period: Last 1 Hour
Time Span: 1 Day
State: New

53	0	0	0	0
Address Count (-1h)	EmailAddress Count (-1h)	File Count (-1h)	Host Count (-1h)	URL Count (-1h)
53	0	0	0	0
Address Trend (1d)	EmailAddress Trend (1d)	File Trend (1d)	Host Trend (1d)	URL Trend (1d)

Custom Indicators

	indicator_type	count
1	ASN	0
2	CIDR	0
3	Mutex	0
4	Registry Key	0
5	User Agent	0

Matched Events Timechart

Indicator Type: All Types
Minimum Threat Rating: All Ratings
Minimum Confidence Rating: All Confidences
Indicator: *
Victim: *

Why This Matters

According to ESG research, 51% of surveyed organizations believe that their organizations have a problematic shortage of existing cybersecurity skills in their workforces.[4] These gaps, from inexperience with the technologies to a lack of familiarity with intelligence sources and a limited understanding of initial threat detection, are exposing organizations to increased risk. IT managers are also limited by the technology they have in place. Popular threat detection technologies such as SIEMs and next-gen firewalls lack awareness of an organization's entire IT ecosystem.

ThreatConnect was designed to address these issues and to give users the tools to increase threat recognition accuracy and shorten the time it takes to detect them. ThreatConnect provides users access to a source library of more than 100 open source threat feeds, which are vetted by the ThreatConnect research analysts and can be shared or expanded on by an entire community of users. In addition, users may ingest their own feeds or third-party premium feeds. Each feed is automatically digested in the system and can propagate threat data to other parts of the customer's infrastructure such as a SIEM or their firewall. ThreatConnect shows how an event is connected to other events to present users the full picture.

ESG Lab validated The ThreatConnect platform's ability to digest dozens of sources from a subscription-based library that can be tailored to use cases such as a specific type of threat or industry. ThreatConnect combined with Splunk proved that the solution quickly combs sources for threat intel that can easily be sent to a SIEM or flagged for later review. ESG Lab saw how ThreatConnect enables users to save threat searches, source activity, and user behavior to run in CAL to further decrease the mean time to identify threats.

[4] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Reducing Mean Time to Respond

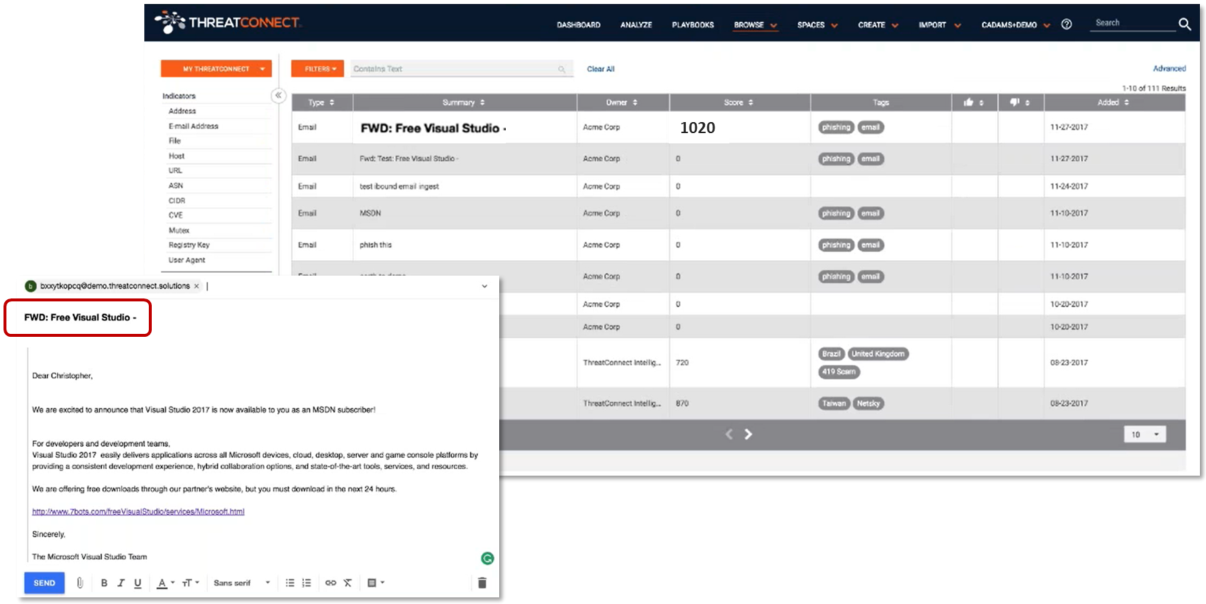
The ThreatConnect platform provides security analysts with insights into gathered intelligence about known threats and leverages that intelligence to uncover potential threats. With feeds from security intelligence sources, ThreatConnect aggregates and filters existing data that helps security analyst teams to prioritize actions and educate current and future analysts on the organization's threat landscape. ThreatConnect also allows analysts to ingest files (such as emails) to extract potential threats and begin tracking them. Analysts can also build upon existing threat intelligence within ThreatConnect and share this knowledge throughout the organization.

The ThreatConnect platform can help security teams to further develop their in-house threat intelligence, track action items, and create custom dashboards to focus on threats specific to their organizations. These teams want to decrease the mean time to respond to threats as they face an ever-increasing amount of data to consume, analyze, and understand the effects on their organizations. ESG examined ThreatConnect with the goal of validating its ability to reduce an organization's mean time to respond to threats.

ESG Lab Testing

ESG Lab began by examining how analysts can use ThreatConnect to protect against phishing emails. We associated an email address with a received phishing message, then forwarded a sample message to that address. ThreatConnect can view all phishing email inboxes and their risk scores to assess threat severity. ThreatConnect assigned the "FWD: Free Visual Studio" inbox a score of 1,020.

Figure 7. Protecting against Phishing Emails – Creating Phishing Email Inbox



1-10 of 111 Results

Type	Summary	Owner	Score	Tags	👍	👎	Added
Email	FWD: Free Visual Studio -	Acme Corp	1020	phishing email			11-27-2017
Email	Fwd: Test: Free Visual Studio -	Acme Corp	0	phishing email			11-27-2017
Email	test ibound email ingest	Acme Corp	0				11-24-2017
Email	MSDN	Acme Corp	0	phishing email			11-10-2017
Email	phish this	Acme Corp	0	phishing email			11-10-2017
		Acme Corp	0	phishing email			11-10-2017
		Acme Corp	0				10-20-2017
		Acme Corp	0				10-20-2017
		ThreatConnect Intellig...	720	Brazil United Kingdom 419 Scam			08-23-2017
		ThreatConnect Intellig...	870	Taiwan Netsky			08-23-2017

bxxytkopcq@demo.threatconnect.solutions

FWD: Free Visual Studio -

Dear Christopher,

We are excited to announce that Visual Studio 2017 is now available to you as an MSDN subscriber!

For developers and development teams,
Visual Studio 2017 easily delivers applications across all Microsoft devices, cloud, desktop, server and game console platforms by providing a consistent development experience, hybrid collaboration options, and state-of-the-art tools, services, and resources.

We are offering free downloads through our partner's website, but you must download in the next 24 hours.

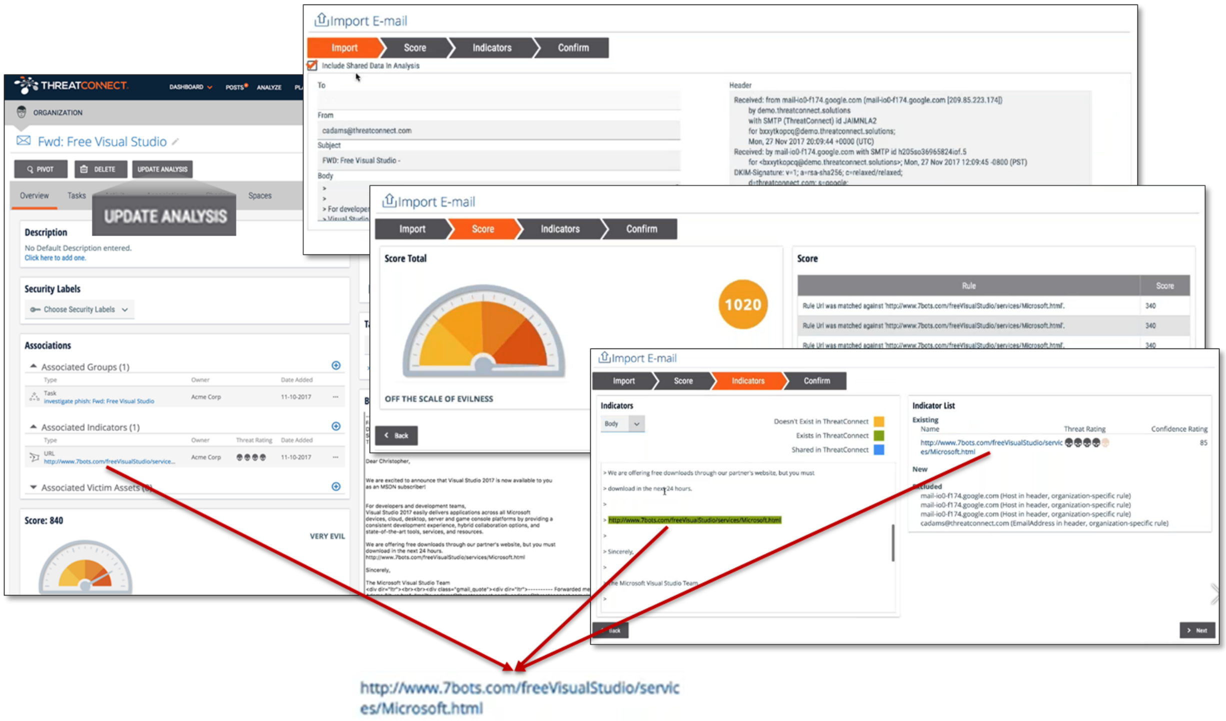
http://www.7bots.com/freeVisualStudio/services/Microsoft.html

Sincerely,

The Microsoft Visual Studio Team

After uploading the phishing email, ThreatConnect extracted associated indicators originating from the email's source. On the screen detailing compiled intelligence about the "FWD: Free Visual Studio" inbox, we clicked on the ***Update Analysis*** button to examine the entire email body (see Figure 7). As we clicked through the ***Import***, ***Score***, and ***Indicator*** options, we ingested the email contents, confirmed the high threat rating, and discovered another potential malicious email address (see Figure 8). ThreatConnect identified the malicious email by searching through its associated intelligence sources and found that the indicator already existed in the current ThreatConnect platform. The address was then saved so that this new data would be shared with other analysts to identify future threats.

Figure 8. Extracting Associated Indicators from Phishing Email



Fwd: Free Visual Studio

Description

No Default Description entered.
Click here to add one.

Security Labels

Choose Security Labels

Associations

Associated Groups (1)

Type	Owner	Date Added
Task investigate phish: Fwd: Free Visual Studio	Acme Corp	11-10-2017

Associated Indicators (1)

Type	Owner	Threat Rating	Date Added
URL http://www.7bots.com/freeVisualStudio/service...	Acme Corp	●●●●	11-10-2017

Associated Victim Assets (0)

Score: 840

☑ Include Shared Data In Analysis

To

From: cadams@threatconnect.com

Subject: FWD: Free Visual Studio -

Body

Header

```
Received: from mail-io0-f174.google.com (mail-io0-f174.google.com [209.85.223.174])
    by demo.threatconnect.solutions
    with SMTP (ThreatConnect) id JAIMNLA2
    for bxxytkopcq@demo.threatconnect.solutions;
    Mon, 27 Nov 2017 20:09:44 +0000 (UTC)
Received: by mail-io0-f174.google.com with SMTP id h205so36965824iof.5
    for <bxxytkopcq@demo.threatconnect.solutions>; Mon, 27 Nov 2017 12:09:45 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=threatconnect.com; s=google;
```

Score Total

Score

Rule	Score
Rule Url was matched against 'http://www.7bots.com/freeVisualStudio/services/Microsoft.html'.	340
Rule Url was matched against 'http://www.7bots.com/freeVisualStudio/services/Microsoft.html'.	340
Rule Url was matched against 'http://www.7bots.com/freeVisualStudio/services/Microsoft.html'.	340

Dear Christopher,

We are excited to announce that Visual Studio 2017 is now available to you as an MSDN subscriber!

For developers and development teams,
Visual Studio 2017 easily delivers applications across all Microsoft devices, cloud, desktop, server and game console platforms by providing a consistent development experience, hybrid collaboration options, and state-of-the-art tools, services, and resources.

We are offering free downloads through our partner's website, but you must download in the next 24 hours.
http://www.7bots.com/freeVisualStudio/services/Microsoft.html

Sincerely,

The Microsoft Visual Studio Team
<div dir="ltr">

<div class="gmail_quote"><div dir="ltr">---------- Forwarded me

Indicators

Body

Doesn't Exist in ThreatConnect 🟧
Exists in ThreatConnect 🟩
Shared in ThreatConnect 🟦

```
> We are offering free downloads through our partner's website, but you must
> download in the next 24 hours.
>
> http://www.7bots.com/freeVisualStudio/services/Microsoft.html
>
> Sincerely,
>
> The Microsoft Visual Studio Team
>
```

Indicator List

Existing

Name	Threat Rating	Confidence Rating
http://www.7bots.com/freeVisualStudio/services/Microsoft.html	●●●●	85

New

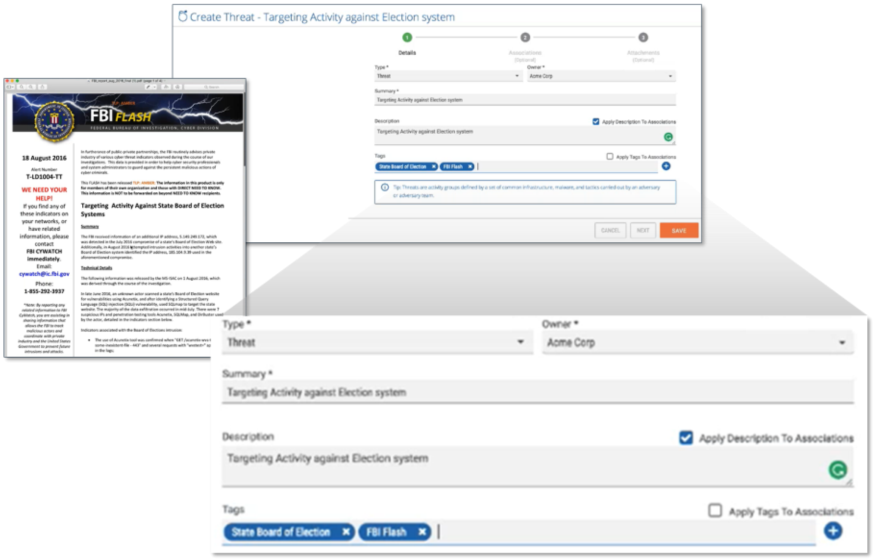
Excluded

mail-io0-f174.google.com (Host in header, organization-specific rule)
mail-io0-f174.google.com (Host in header, organization-specific rule)
mail-io0-f174.google.com (Host in header, organization-specific rule)
cadams@threatconnect.com (EmailAddress in header, organization-specific rule)

http://www.7bots.com/freeVisualStudio/services/Microsoft.html

ESG Lab then evaluated how an analyst can configure a threat to be tracked, monitored, and addressed via ThreatConnect. We evaluated the use case in which an analyst analyzes a report from a widely used intelligence source, the FBI. We began by creating a tracker for an individual threat. Using a public FBI bulletin, we entered details such as the organization name associated with the tracker, summary title of the threat, description, and tags. We then clicked on the orange ***Save*** button to go to the next screen (see Figure 9).

Figure 9. Create New Threat for an Organization to Track



Create Threat - Targeting Activity against Election system

18 August 2016

Alert Number T-LD1004-TT

WE NEED YOUR HELP!

Targeting Activity Against State Board of Election Systems

Type *: Threat

Owner *: Acme Corp

Summary *: Targeting Activity against Election system

Description: Targeting Activity against Election system

☑ Apply Description To Associations

Tags: State Board of Election ✕ FBI Flash ✕

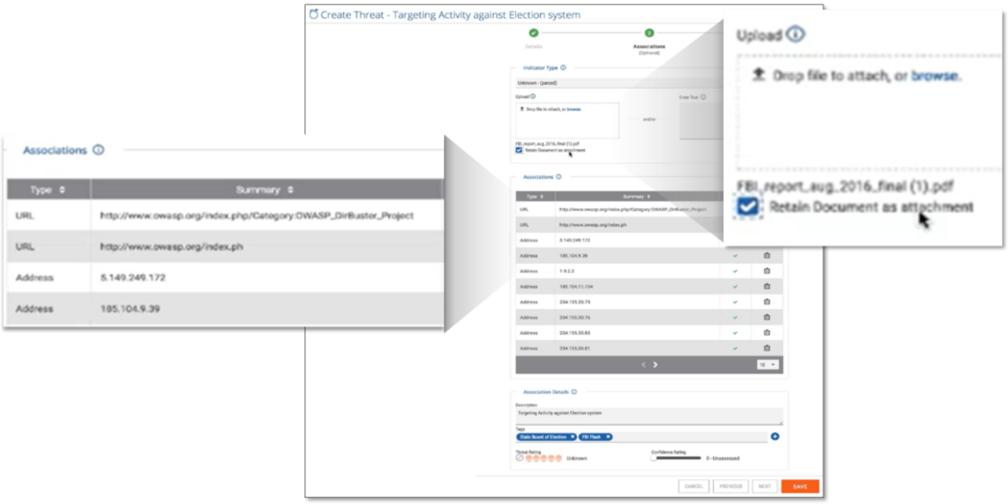
☐ Apply Tags To Associations

Tip: Threats are activity groups defined by a set of common infrastructure, malware, and tactics carried out by an adversary or adversary team.

We then observed how an analyst can input associations specific to this threat. According to ThreatConnect, a threat is defined as "an activity group defined by a set of common infrastructure, malware, and tactics carried out by an adversary or adversary team." The FBI report contains indicators that alert analysts of the highlighted threat. The indicators are called

Associations by ThreatConnect. After clicking on the ***Save*** button, we extracted the associations, as seen in Figure 10. As in the previous example, we dragged the file icon representing the FBI report onto the box below the ***Upload*** heading. The analyst also has the option to manually enter text.

Figure 10. Extract Associations for Specific Threat



Create Threat - Targeting Activity against Election system

Indicator Type: Unknown - (parsed)

FBI_report_aug_2016_final (1).pdf

☑ Retain Document as attachment

Associations

Type	Summary
URL	http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
URL	http://www.owasp.org/index.ph
Address	5.149.249.172
Address	185.104.9.39
Address	1.9.2.2
Address	185.104.11.154
Address	204.155.30.75
Address	204.155.30.76
Address	204.155.30.80
Address	204.155.30.81

Association Details

Description: Targeting Activity against Election system

Tags: State Board of Election, FBI Flash

Threat Rating: Unknown

Confidence Rating: 0 - Unassessed

Once ThreatConnect ingested the FBI report, detailed indicators—URLs, IP addresses, etc.—appeared in the middle of the screen. This enabled us to compile all the necessary data into a tracker that we could use to assess the threat continuously.

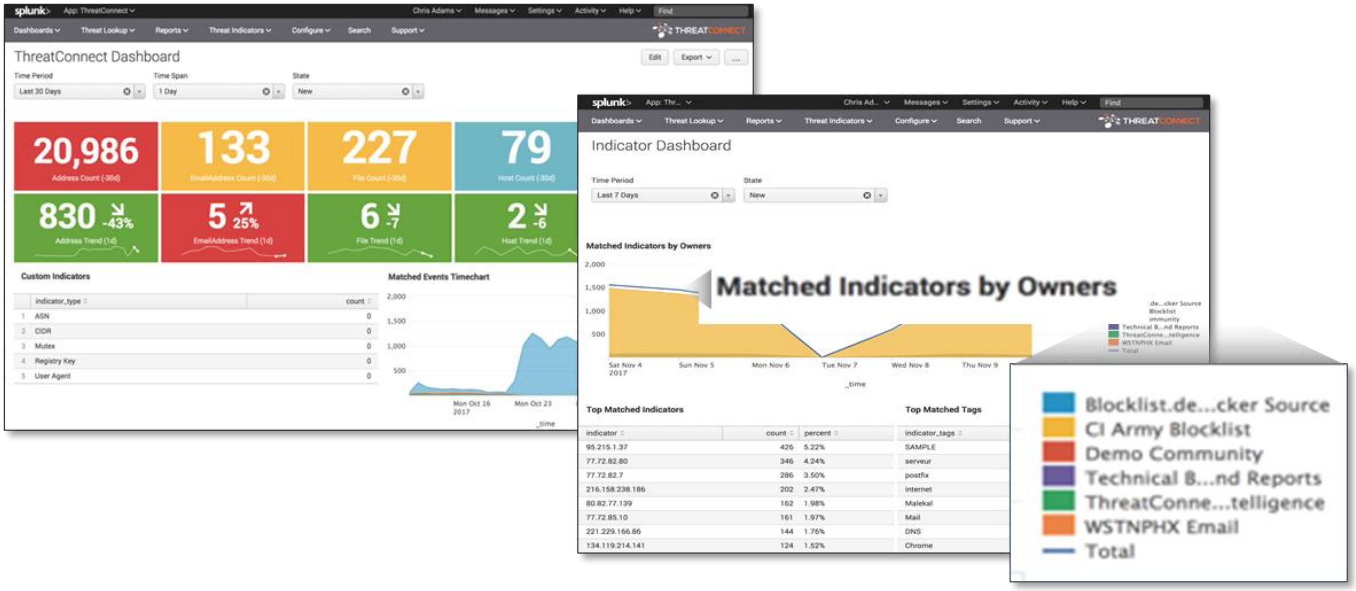
ESG Lab then observed how The ThreatConnect platform can ingest data from a large repository with multiple feeds to enhance response. Once again, we looked at ThreatConnect's Splunk integration to see how it would work with a SIEM. Given the copious data a SIEM can collect, it is unreasonable to expect a human to manually analyze them. We found that ThreatConnect can enable an analyst to quickly parse Splunk data, uncover indicators and threats, and augment existing threat intelligence.

We first navigated to the Splunk dashboard, which provided a clear view of the counts of potential indicators such as emails, files, and hosts, depending on the range of time chosen via a drop-down menu (see

Figure 11. Splunk Integration with ThreatConnect – Dashboard with Cumulative Counts and Indicator Trends

). We then navigated to the ***Indicator Dashboard***, which revealed the number of indicators uncovered per subscribed intelligence source (or ***Owners*** as stated in the screen) over time. Intelligence sources were listed in the legend. We saw that this use case is applicable when a security team wants to determine those subscriptions that have served them best. Thus, the team can make informed decisions regarding what subscriptions to continue or discard.

Figure 11. Splunk Integration with ThreatConnect – Dashboard with Cumulative Counts and Indicator Trends



ThreatConnect Dashboard

Time Period: Last 30 Days
Time Span: 1 Day
State: New

Custom Indicators

	indicator_type	count
1	ASN	0
2	CIDR	0
3	Mutex	0
4	Registry Key	0
5	User Agent	0

Indicator Dashboard

Time Period: Last 7 Days
State: New

Top Matched Indicators

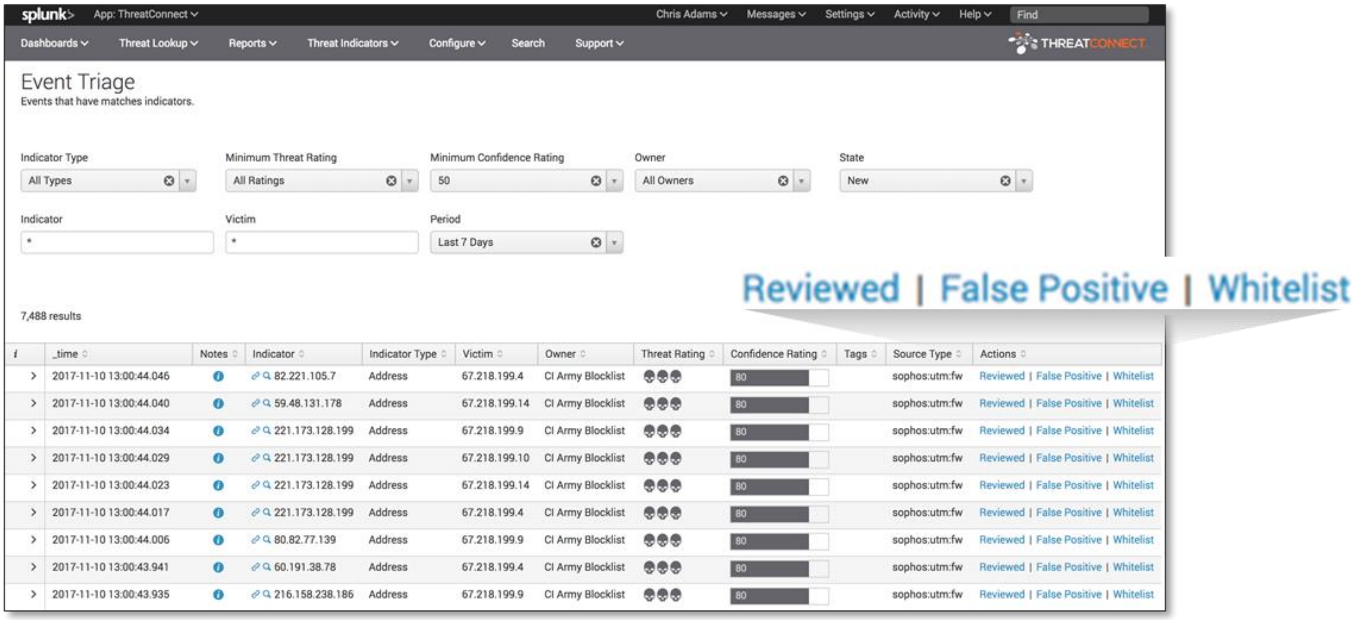
indicator	count	percent
95.215.1.37	426	5.22%
77.72.82.80	346	4.24%
77.72.82.7	286	3.50%
216.158.238.186	202	2.47%
80.82.77.139	162	1.98%
77.72.85.10	161	1.97%
221.229.166.86	144	1.76%
134.119.214.141	124	1.52%

Top Matched Tags

indicator_tags
SAMPLE
serveur
postfix
internet
Malekal
Mail
DNS
Chrome

Another view, Event Triage, listed indicators with common characteristics such as owner or source (see Figure 12). We found that this view can help analysts to examine the prevalence of a specific indicator in an organization. Analysts can then proactively act if it's deemed necessary. Indicators can be whitelisted, identified as false positives, or marked as reviewed. This offers another way for analysts to identify the intelligence sources most useful to them, as opposed to those that, for example, produce many false positives.

Figure 12. Splunk Integration with ThreatConnect – Event Triage



Event Triage

Events that have matches indicators.

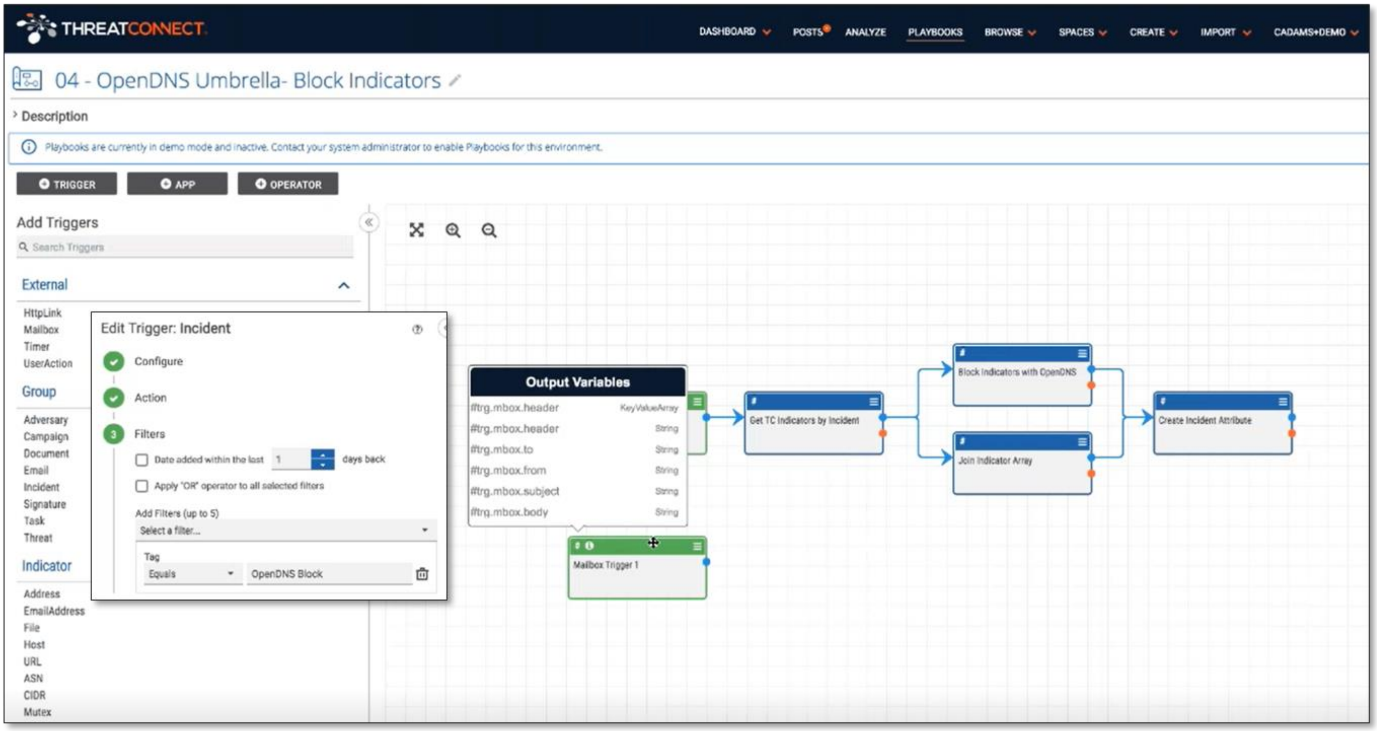
Indicator Type: All Types
Minimum Threat Rating: All Ratings
Minimum Confidence Rating: 50
Owner: All Owners
State: New
Indicator: *
Victim: *
Period: Last 7 Days

7,488 results

i	_time	Notes	Indicator	Indicator Type	Victim	Owner	Threat Rating	Confidence Rating	Tags	Source Type	Actions
>	2017-11-10 13:00:44.046	ⓘ	82.221.105.7	Address	67.218.199.4	CI Army Blocklist	●●●	80		sophos:utm:fw	Reviewed | False Positive | Whitelist
>	2017-11-10 13:00:44.040	ⓘ	59.48.131.178	Address	67.218.199.14	CI Army Blocklist	●●●	80		sophos:utm:fw	Reviewed | False Positive | Whitelist
>	2017-11-10 13:00:44.034	ⓘ	221.173.128.199	Address	67.218.199.9	CI Army Blocklist	●●●	80		sophos:utm:fw	Reviewed | False Positive | Whitelist
>	2017-11-10 13:00:44.029	ⓘ	221.173.128.199	Address	67.218.199.10	CI Army Blocklist	●●●	80		sophos:utm:fw	Reviewed | False Positive | Whitelist
>	2017-11-10 13:00:44.023	ⓘ	221.173.128.199	Address	67.218.199.14	CI Army Blocklist	●●●	80		sophos:utm:fw	Reviewed | False Positive | Whitelist
>	2017-11-10 13:00:44.017	ⓘ	221.173.128.199	Address	67.218.199.4	CI Army Blocklist	●●●	80		sophos:utm:fw	Reviewed | False Positive | Whitelist
>	2017-11-10 13:00:44.006	ⓘ	80.82.77.139	Address	67.218.199.9	CI Army Blocklist	●●●	80		sophos:utm:fw	Reviewed | False Positive | Whitelist
>	2017-11-10 13:00:43.941	ⓘ	60.191.38.78	Address	67.218.199.4	CI Army Blocklist	●●●	80		sophos:utm:fw	Reviewed | False Positive | Whitelist
>	2017-11-10 13:00:43.935	ⓘ	216.158.238.186	Address	67.218.199.9	CI Army Blocklist	●●●	80		sophos:utm:fw	Reviewed | False Positive | Whitelist

Finally, ESG Lab looked at the creation of playbooks for threat response automation. With only a few clicks, we created a playbook to orchestrate a coordinated group of actions in response to a specific trigger—in this case, the presence of a tag indicating OpenDNS Block, as seen in Figure 13. With ThreatConnect's playbooks, organizations can automate nearly any security operation or task, in series or in parallel, invoking other tools, and responding appropriately.

Figure 13. Creating a Custom Threat Response Playbook



04 - OpenDNS Umbrella- Block Indicators

Playbooks are currently in demo mode and inactive. Contact your system administrator to enable Playbooks for this environment.

Edit Trigger: Incident

□ Date added within the last 1 days back

□ Apply "OR" operator to all selected filters

Add Filters (up to 5)

Select a filter...

Tag Equals OpenDNS Block

Output Variables

#trg.mbox.header	KeyValueArray
#trg.mbox.header	String
#trg.mbox.to	String
#trg.mbox.from	String
#trg.mbox.subject	String
#trg.mbox.body	String

Why This Matters

As organizations grapple with a rising number of data breaches and cyber-attacks, security analysts must continually consume, comprehend, and utilize data from multiple sources, determine appropriate actions, and communicate those actions in a timely manner. Tools that will help organizations not only understand and identify current and emerging threats, but also know when and how to respond to them are needed.

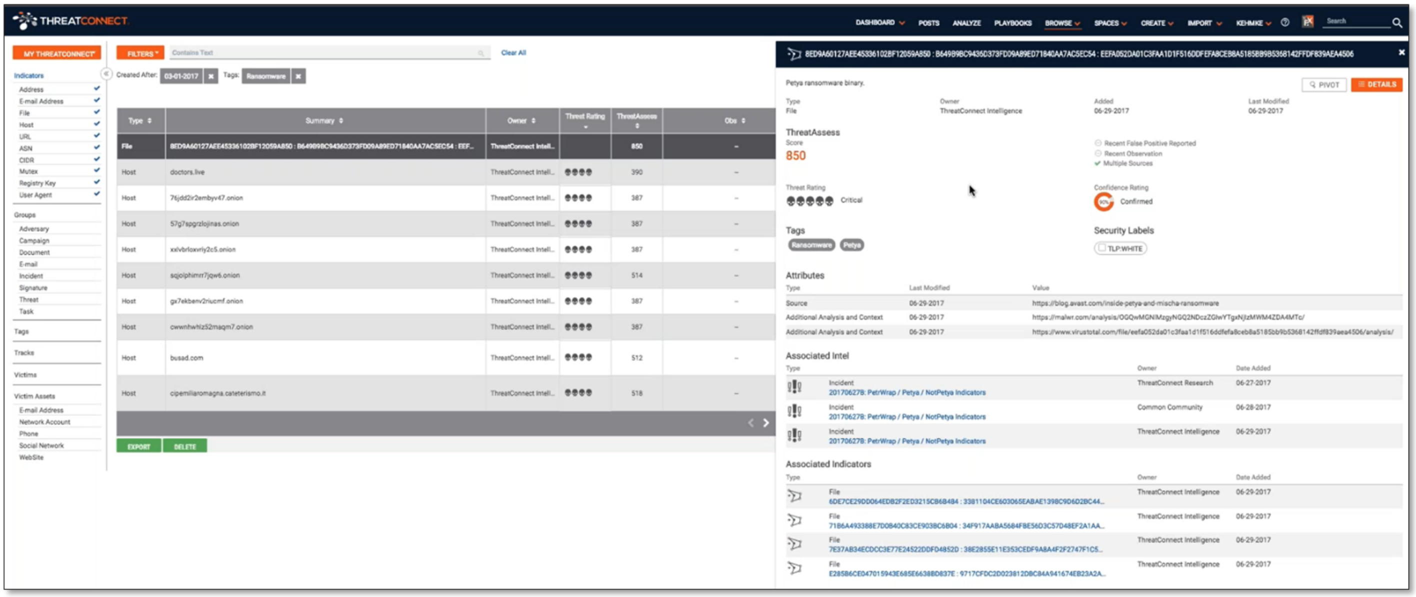
The ThreatConnect platform is designed to enable security teams to consume data from multiple sources and extract context on threats, thus allowing the team to act on those that present the most clear and present danger. The solution also enables analysts to collaborate on these threats by offering team communication within ThreatConnect via task assignment and additional insights. ThreatConnect also enables more comprehensive data analysis, leveraging data already collected, parsed, and organized to uncover potential threats that the organization may have not tracked previously.

ESG Lab verified that ThreatConnect can help security analyst teams reduce the mean time to respond to threats. We ingested new data in the form of reports from multiple security intelligence sources. ThreatConnect parsed and extracted data relevant to known threats, calculating ratings and scores to educate analysts on threat severity. ESG Lab also examined how ThreatConnect can extract key indicators that notify the analyst of a specific threat presence. The Splunk integration demonstrates how security analysts view and analyze large amounts of data quickly and easily between a SIEM and ThreatConnect. ThreatConnect playbooks are completely customizable and can be created and reconfigured on the fly to automate and orchestrate nearly any security operation or task, with no coding required.

Threat Hunting

Finally, ESG Lab examined ThreatConnect's ability to facilitate threat hunting, or advanced querying of the security data processed within the ThreatConnect platform. The ThreatConnect platform enables analysts to search for specific as-yet undetected or unobserved threats. In this case, ESG Lab wanted to consider recent ransomware incidents that affected healthcare organizations. Selecting ***Browse*** from the top ribbon menu brought us to a discovery tool that allowed us to make advanced searches across enabled sources in ThreatConnect (see Figure 14). Adding filters to the search to show any threats after March 1st that had been tagged for ransomware took just a few clicks. The search results populated in seconds and could be sorted by threat rating, type, and date in a single click. By selecting a single indicator, ESG Lab was shown a pop-up summary window populated by CAL that showed the ThreatAssess score, any associated threats, and other insights. ESG Lab could even drill into a specific ransomware variant, such as WannaCry.

Figure 14. Ransomware Search and Quick Insight Summary



Created After: 03-01-2017 ✖ Tags: Ransomware ✖

Type	Summary	Owner	Threat Rating	ThreatAssess	Obs
File	8ED9A60127AEE45336102BF12059A850 : B649B9BC94360373FD09A89ED71840AA7AC5EC54 : EEF...	ThreatConnect Intell...		850	–
Host	doctors.live	ThreatConnect Intell...	☠☠☠☠	390	–
Host	76jdd2ir2embyv47.onion	ThreatConnect Intell...	☠☠☠☠	387	–
Host	57g7spgrzlojinas.onion	ThreatConnect Intell...	☠☠☠☠	387	–
Host	xxlvbrloxvriy2c5.onion	ThreatConnect Intell...	☠☠☠☠	387	–
Host	sqjolphimrr7jqw6.onion	ThreatConnect Intell...	☠☠☠☠	514	–
Host	gx7ekbenv2riucmf.onion	ThreatConnect Intell...	☠☠☠☠	387	–
Host	cwwnhwhlz52maqm7.onion	ThreatConnect Intell...	☠☠☠☠	387	–
Host	busad.com	ThreatConnect Intell...	☠☠☠☠	512	–
Host	cipemiliaromagna.cateterismo.it	ThreatConnect Intell...	☠☠☠☠	518	–

8ED9A60127AEE45336102BF12059A850 : B649B9BC94360373FD09A89ED71840AA7AC5EC54 : EEFA052DA01C3FAA1D1F516DDFEFA8CEB8A5185BB9B5368142FFDF839AEA4506

Petya ransomware binary.

Type	Owner	Added	Last Modified
File	ThreatConnect Intelligence	06-29-2017	06-29-2017

ThreatAssess
Score
850

○ Recent False Positive Reported
○ Recent Observation
✓ Multiple Sources

Threat Rating
☠☠☠☠☠ Critical

Confidence Rating
90% Confirmed

Tags
Ransomware Petya

Security Labels
□ TLP:WHITE

Attributes

Type	Last Modified	Value
Source	06-29-2017	https://blog.avast.com/inside-petya-and-mischa-ransomware
Additional Analysis and Context	06-29-2017	https://malwr.com/analysis/OGQwMGNlMzgyNGQ2NDczZGlwYTgxNjlzMWM4ZDA4MTc/
Additional Analysis and Context	06-29-2017	https://www.virustotal.com/file/eefa052da01c3faa1d1f516ddfefa8ceb8a5185bb9b5368142ffdf839aea4506/analysis/

Associated Intel

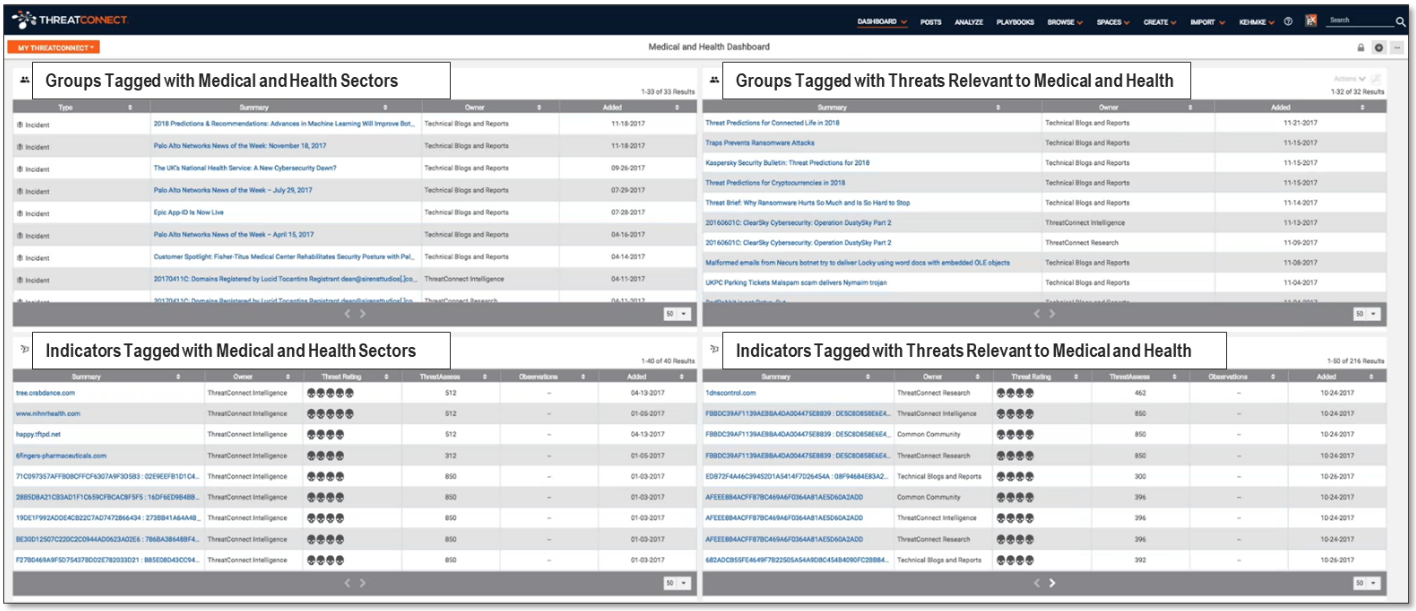
Type		Owner	Date Added
	Incident 20170627B: PetrWrap / Petya / NotPetya Indicators	ThreatConnect Research	06-27-2017
	Incident 20170627B: PetrWrap / Petya / NotPetya Indicators	Common Community	06-28-2017
	Incident 20170627B: PetrWrap / Petya / NotPetya Indicators	ThreatConnect Intelligence	06-29-2017

Associated Indicators

Type		Owner	Date Added
	File 6DE7CE29DD064EDB2F2ED3215CB6B484 : 3381104CE603065EABAE1398C9D6D2BC44...	ThreatConnect Intelligence	06-29-2017
	File 71B6A493388E7D0B40C83CE903BC6B04 : 34F917AABA5684FBE56D3C57D48EF2A1AA...	ThreatConnect Intelligence	06-29-2017
	File 7E37AB34ECDCC3E77E24522DDFD4852D : 38E2855E11E353CEDF9A8A4F2F2747F1C5...	ThreatConnect Intelligence	06-29-2017
	File E285B6CE047015943E685E6638BD837E : 9717CFDC2D023812DBC84A941674EB23A2A...	ThreatConnect Intelligence	06-29-2017

Of course, the opposite was also possible as we performed a reverse search on any threats that had been tagged as related to "Medical" (see Figure 15). Again, the search results populated in a matter of seconds and could be sorted in a single click. ESG Lab automated these searches via a ThreatConnect custom dashboard. In the ***Dashboard*** drop-down section on the ribbon, we clicked a custom *Medical & Healthcare* sector report. This dashboard showed four different searches based around threat activity attributed to medical and healthcare organizations. As with other individual searches, each instance could be sorted and clicked on to get additional details. Many of these dashboards come preconfigured with ThreatConnect, and users are free to edit them or create new ones as they see fit.

Figure 15. Medical and Healthcare Sector Automated Dashboard



Groups Tagged with Medical and Health Sectors — 1-33 of 33 Results

Type	Summary	Owner	Added
Incident	2018 Predictions & Recommendations: Advances in Machine Learning Will Improve Bot...	Technical Blogs and Reports	11-18-2017
Incident	Palo Alto Networks News of the Week: November 18, 2017	Technical Blogs and Reports	11-18-2017
Incident	The UK's National Health Service: A New Cybersecurity Dawn?	Technical Blogs and Reports	09-26-2017
Incident	Palo Alto Networks News of the Week – July 29, 2017	Technical Blogs and Reports	07-29-2017
Incident	Epic App-ID Is Now Live	Technical Blogs and Reports	07-28-2017
Incident	Palo Alto Networks News of the Week – April 15, 2017	Technical Blogs and Reports	04-16-2017
Incident	Customer Spotlight: Fisher-Titus Medical Center Rehabilitates Security Posture with Pal...	Technical Blogs and Reports	04-14-2017
Incident	20170411C: Domains Registered by Lucid Tocantins Registrant dean@sirenstudios[.]co...	ThreatConnect Intelligence	04-11-2017
Incident	20170411C: Domains Registered by Lucid Tocantins Registrant dean@sirenstudios[.]co...	ThreatConnect Research	04-11-2017

Groups Tagged with Threats Relevant to Medical and Health — 1-32 of 32 Results

Summary	Owner	Added
Threat Predictions for Connected Life in 2018	Technical Blogs and Reports	11-21-2017
Traps Prevents Ransomware Attacks	Technical Blogs and Reports	11-15-2017
Kaspersky Security Bulletin: Threat Predictions for 2018	Technical Blogs and Reports	11-15-2017
Threat Predictions for Cryptocurrencies in 2018	Technical Blogs and Reports	11-15-2017
Threat Brief: Why Ransomware Hurts So Much and Is So Hard to Stop	Technical Blogs and Reports	11-14-2017
20160601C: ClearSky Cybersecurity: Operation DustySky Part 2	ThreatConnect Intelligence	11-13-2017
20160601C: ClearSky Cybersecurity: Operation DustySky Part 2	ThreatConnect Research	11-09-2017
Malformed emails from Necurs botnet try to deliver Locky using word docs with embedded OLE objects	Technical Blogs and Reports	11-08-2017
UKPC Parking Tickets Malspam scam delivers Nymaim trojan	Technical Blogs and Reports	11-04-2017

Indicators Tagged with Medical and Health Sectors — 1-40 of 40 Results

Summary	Owner	Threat Rating	ThreatAssess	Observations	Added
tree.crabdance.com	ThreatConnect Intelligence	☠☠☠☠☠	512	–	04-13-2017
www.nihnrhealth.com	ThreatConnect Intelligence	☠☠☠☠☠	512	–	01-05-2017
happy.tftpd.net	ThreatConnect Intelligence	☠☠☠☠	512	–	04-13-2017
6fingers-pharmaceuticals.com	ThreatConnect Intelligence	☠☠☠☠	312	–	01-05-2017
71C097357AFFB0BCFFCF6307A9F3D5B3 : 02E9EEFB1D1C4...	ThreatConnect Intelligence	☠☠☠☠	850	–	01-03-2017
28B5DBA21CB3AD1F1C659CFBCAC8F5F5 : 16DF6ED9B48B...	ThreatConnect Intelligence	☠☠☠☠	850	–	01-03-2017
19DE1F992ADDE4CB22C7AD7472866434 : 273BB41A64A48...	ThreatConnect Intelligence	☠☠☠☠	850	–	01-03-2017
BE30D12507C220C2C0944AD0623A02E6 : 786BA38648BF4...	ThreatConnect Intelligence	☠☠☠☠	850	–	01-03-2017
F27B0469A9F5D754378DD2E782033D21 : B85E08D43CC94...	ThreatConnect Intelligence	☠☠☠☠	850	–	01-03-2017

Indicators Tagged with Threats Relevant to Medical and Health — 1-50 of 216 Results

Summary	Owner	Threat Rating	ThreatAssess	Observations	Added
1dnscontrol.com	ThreatConnect Research	☠☠☠☠	462	–	10-24-2017
FB8DC39AF1139AEBBA4DA004475E8839 : DE5C8D858E6E4...	ThreatConnect Intelligence	☠☠☠☠	850	–	10-24-2017
FB8DC39AF1139AEBBA4DA004475E8839 : DE5C8D858E6E4...	Common Community	☠☠☠☠	850	–	10-24-2017
FB8DC39AF1139AEBBA4DA004475E8839 : DE5C8D858E6E4...	ThreatConnect Research	☠☠☠☠	850	–	10-24-2017
ED872F4A46C39452D1A5414F7D26454A : 08F94684E83A2...	Technical Blogs and Reports	☠☠☠☠	300	–	10-26-2017
AFEEE8B4ACFF87BC469A6F0364A81AE5D60A2ADD	Common Community	☠☠☠☠	396	–	10-24-2017
AFEEE8B4ACFF87BC469A6F0364A81AE5D60A2ADD	ThreatConnect Intelligence	☠☠☠☠	396	–	10-24-2017
AFEEE8B4ACFF87BC469A6F0364A81AE5D60A2ADD	ThreatConnect Research	☠☠☠☠	396	–	10-24-2017
682ADCB55FE4649F7B22505A54A9D8C454B4090FC28B84...	Technical Blogs and Reports	☠☠☠☠	392	–	10-26-2017

Why This Matters

ESG asked IT executives and professionals to name the business initiative that would drive the most IT spending at their organizations in 2018. Forty four percent cited strengthening cybersecurity, making it the most cited option in the list.[5] The traditional approach to achieving this goal is to attempt to consolidate multiple point solutions, system logs, and threat feed data system logs using a SIEM or log management solution. The traditional SIEM approach—which can present thousands of events per hour with little to no context—presents the daunting task of manual analysis to a security analyst or team. Many organizations limit the threat intelligence feeds they utilize for this very reason, reducing visibility into the broader threat landscape.

What is needed is a solution that can harness the torrent of data collected from multiple threat intelligence sources and apply statistical analytics to provide organizations with the cross-correlated context they need to secure and manage operations in the modern IT ecosystem.

ESG confirmed the ability of The ThreatConnect platform to deliver stateful, context-aware visibility and enable analysts to hunt for threats leveraging data from dozens of open source and premium threat intelligence sources. This enables a security organization to discover, investigate, and manage responses without having to spend inordinate amounts of time and effort sifting through thousands of alerts and log entries.

[5] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

The Bigger Truth

It has become clear that the cybersecurity landscape is becoming increasingly complex and difficult to manage.[6] Intellectual property, customer information, and financial data are increasingly at risk of compromise, which can lead to serious consequences, including financial penalties, impact to brand and company valuation, and legal action. Meanwhile, businesses must investigate and respond to a steeply increasing number of security incidents; the proliferation of new systems and applications is creating more security incident scenarios, while better detection tools are generating more alerts. Organizations need a robust operations and analytics strategy if they hope to respond to incidents quickly enough to minimize risks.

The ThreatConnect Platform was designed to help organizations understand their adversaries, automate workflows, and mitigate threats leveraging threat intelligence. ThreatConnect aims to enable centralized security operations and analytics management—orchestration, data enrichment, incident and task management, etc.—with the goal of providing context to the data, enabling and recommending actions with defensive tools, and helping organizations make faster, more informed security decisions.

The goal of ThreatConnect is to infuse every aspect of an organization's security program with threat intelligence. Open source and premium feeds are combined with data from the organization's internal tools to create a pool of threat intelligence, with a built-in feedback loop from the people and tools back to ThreatConnect to continuously improve the intelligence. ThreatConnect's customizable threat response playbooks require no prior coding experience to give security analysts and IT admins the ability to automate data digestion and enrichment.

In ESG Lab testing, The ThreatConnect platform digested dozens of sources from a subscription-based library and tailored them to use cases like specific type of threat or industry. ThreatConnect combined with Splunk quickly combed sources for threat intel, which could easily be sent to a SIEM or flagged for later review. ThreatConnect enabled us to save threat searches, source activity, and user behavior to run in CAL to further decrease the mean time to identify threats.

The ThreatConnect platform parsed and extracted data from multiple security intelligence sources relevant to known threats, presenting ratings and scores to educate analysts on threat severity. ThreatConnect extracted key indicators that notified us of a specific threat presence. The Splunk integration allows security analysts to view and analyze large amounts of data quickly and easily. We created a new ThreatConnect playbook with just a few clicks. Playbooks are completely customizable and can be created and reconfigured on the fly to automate and orchestrate nearly any security operation or task, with no coding required.

ESG Lab validated that ThreatConnect's ThreatConnect security operations and analytics platform helps organizations overcome the cybersecurity skills gap with end-to-end detection, analytics, response, and automation capabilities. For organizations that want to move beyond the capabilities of legacy SIEM platforms and leverage threat intelligence throughout their environments to orchestrate intelligent, automated response, it would be worthwhile to take a closer look at ThreatConnect's security operations and analytics platform.

[6] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.