Technical Review

ThreatConnect TC Identify Delivers Threat Intelligence

By Tony Palmer, Senior Validation Analyst; and Dom Amato, Associate Validation Analyst

July 2018

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.

Abstract

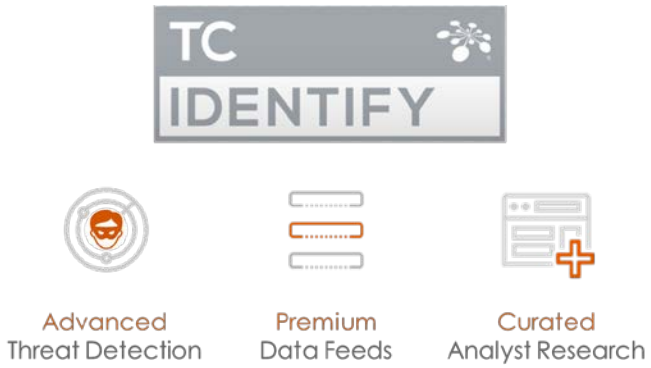
This ESG Lab Review documents hands-on testing of ThreatConnect TC Identify and evaluates its ability to accelerate and simplify threat detection. ESG Lab focused on how TC Identify provides IT managers with the tools to configure threat intelligence from more than 100 open source data feeds and premium feeds that the organization subscribes to, summarize and score potential threats with insights from the ThreatConnect Research Team, and optimize data dissection by integrating with other tools such as a SIEM or firewall.

Background

Research from ESG and the Information Systems Security Association (ISSA) reveals that 70% of cybersecurity professionals believe that the global cybersecurity skills shortage has impacted their organizations.[1] Based upon this research, it's clear that most organizations don't have enough cybersecurity staffers and/or the necessary cybersecurity skills. Today, 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.

ESG research also 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.[2] 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 solution that enables security professionals to analyze and respond to incidents quickly while building threat intelligence continuously to overcome the skills shortage.

ThreatConnect TC Identify



ThreatConnect TC Identify is designed to provide in-depth threat intelligence from more than 100 open source and premium threat intelligence data feeds, supplemented with insights from ThreatConnect's veteran research team, to give organizations a full-featured threat detection foundation. With TC Identify, IT teams can aggregate, customize, and monitor the sources they want for threats. The added ability to search feeds for activity while adding tags, filters, and notes for any indicators keeps threat detection activity focused and viewable in a single space. Using ThreatConnect's proprietary CAL (Collective Analytics Layer), TC Identify also reveals frequency of both threats and false positives from other ThreatConnect users. Issues can be easily marked as false positives and users can leave contextual notes for later review. IT managers are also free to send any intelligence to other tools such as SIEMs or firewalls to hone threat detection capabilities and learn from each experience. TC Identify comes bundled with the ThreatConnect Intelligence source, which is produced by ThreatConnect's in-house analysts and provides additional insights on indicators and known adversaries, giving users insights and context into threats that they may not have the personnel or skill set to develop on their own.

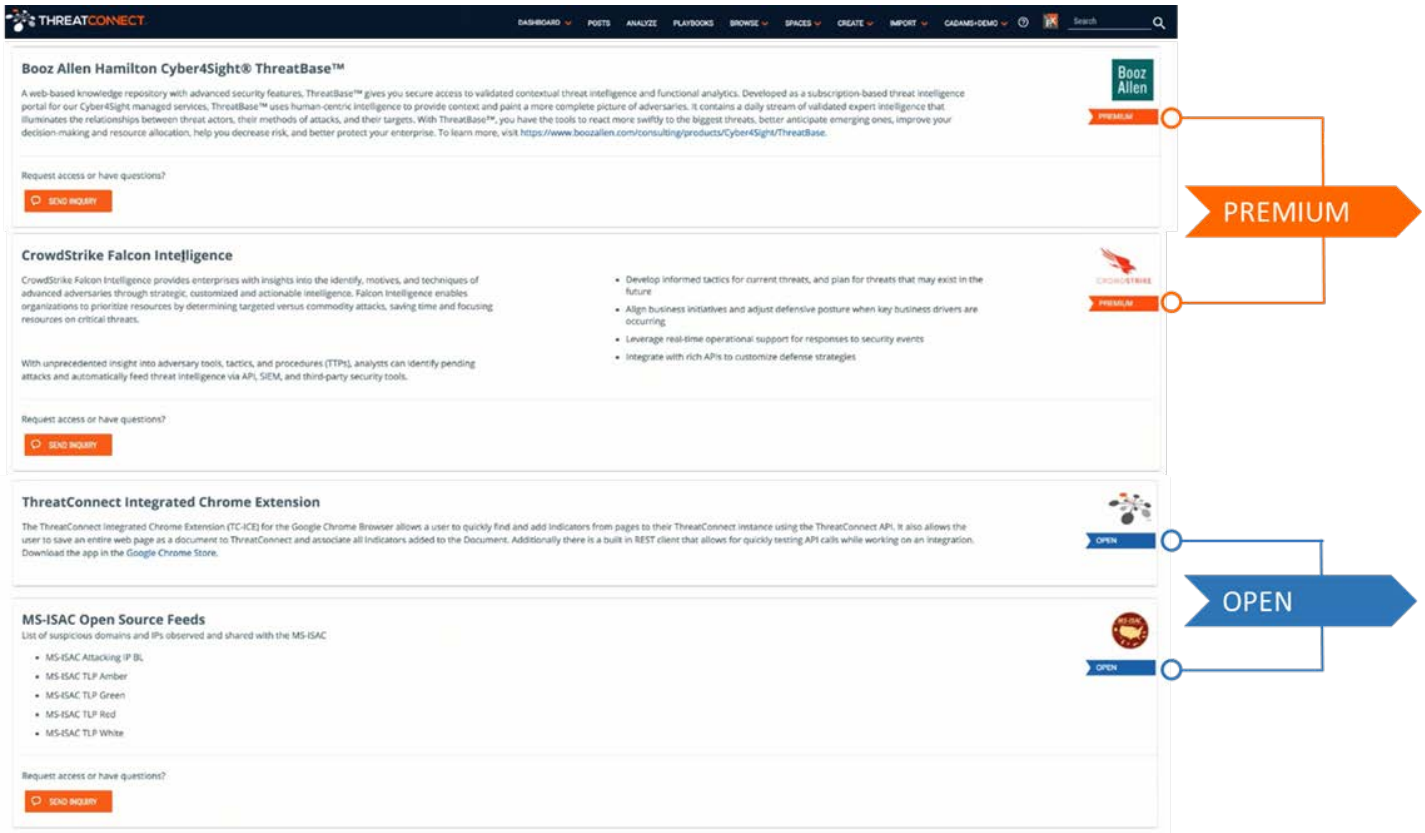
ESG Lab Tested

ESG Lab began by exploring ThreatConnect's library of source feeds. TC Identify provides a library of more than 100 open source threat intelligence feeds and recommends numerous premium subscription-based sources, all of which could be

[1] Source: ESG Research Report, *ESG/ISSA Research Report: The Life and Times of Cybersecurity Professionals*, November 2017.
[2] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.

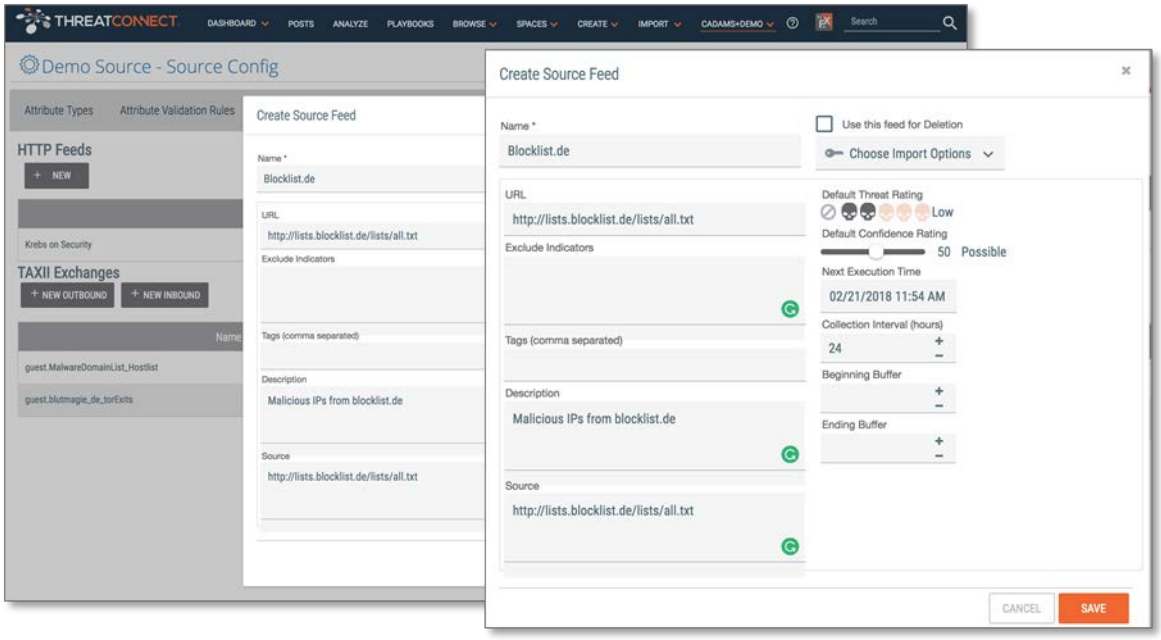
found in *TC Exchange*. Each recommended source was described here in detail (see Figure 1), and just by scrolling down the page, ESG Lab could easily glean whether sources were paid or free, and what to expect from each one. The open source library was particularly extensive, with more than 100 feeds. Recommendations and highlights for each source help provide a quick summary for the user to prevent the need to inquire about each individual option.

Figure 1. ThreatConnect Exchange Source Library



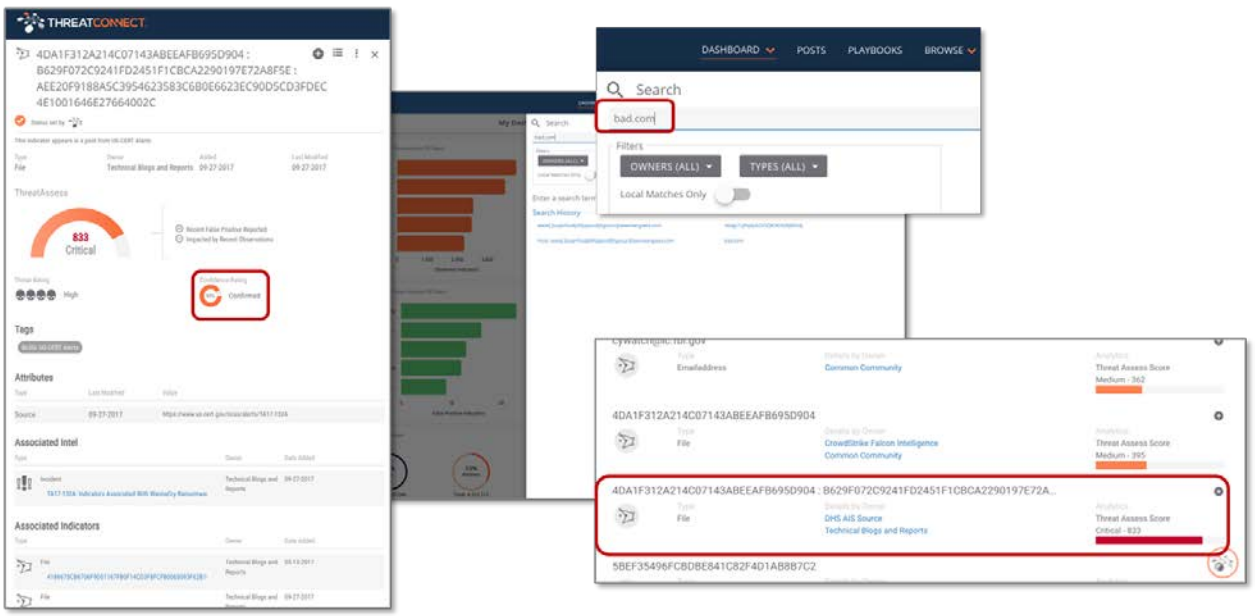
Next, ESG Lab validated that the list of sources could be supplemented with a custom feed of the user's choosing. Setting up the ingest of a simple feed of indicators was straightforward in the user interface. Navigating to the *Posts* section by clicking the button on the ThreatConnect ribbon brought ESG Lab to the library of activated sources. From here, users can click on any available source feed to see details, any associations the source has, and even user-created posts. Selecting a particular feed also brings the user to the ***Source Config*** page that displays source attributes and properties. ESG Lab created a custom source feed from this page by clicking on the pencil button to edit the feed, then selected a specific feed URL to be targeted (see Figure 2). Users can specify import instructions, assign a default threat rating, and more. The next time TC Identify combs this source for threat intel, the process will be automated and get the user the relevant information much faster and at an interval of her choosing.

Figure 2. Custom-configuring a Source Feed



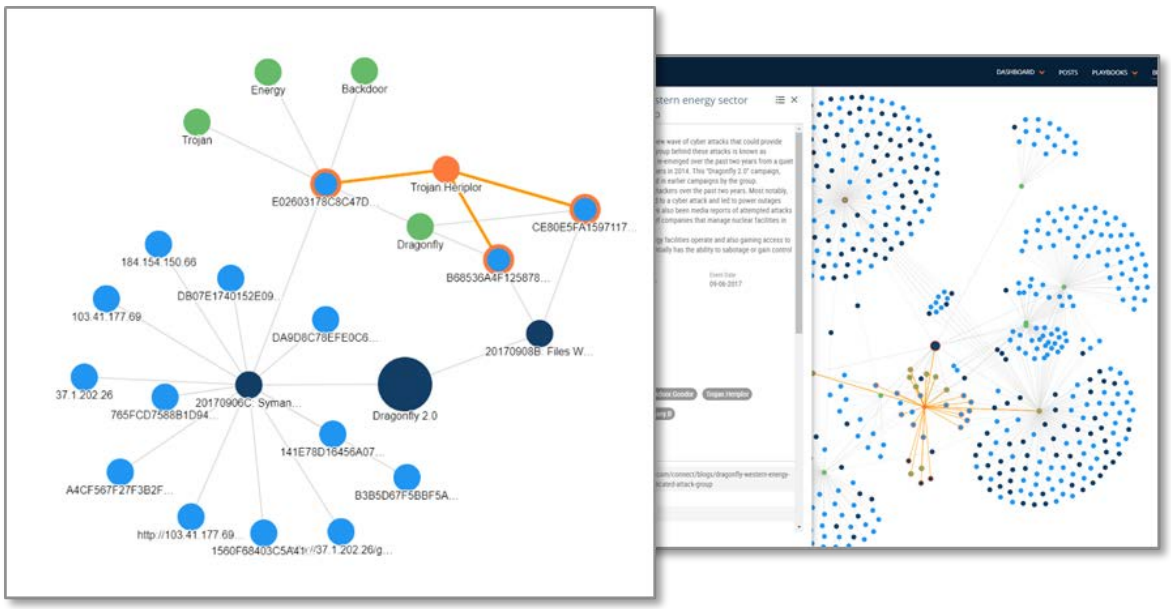
Next, ESG Lab examined how TC Identify flags potential intrusions using the search function (see Figure 3). It is worth noting that this feature is available as part of TC Open, ThreatConnect's free offering. Clicking on the search icon at the top left—bad.com in this case—brought up a list of indicators that contained a match. The source of the data is listed in blue text and TC Identify automatically calculates an overall *Threat Assess* score to help the user assess the indicators relative to one another without any manual analysis. Higher scores help the analysts prioritize the most critical threats to address. Clicking on the indicator with the highest score opened the details view on the left, which showed the Confidence Rating, derived from intelligence sources to which the organization subscribes. The Confidence Rating communicated how likely it was that the threat would cause issues.

Figure 3. Using Search to Find and Prioritize Intrusions



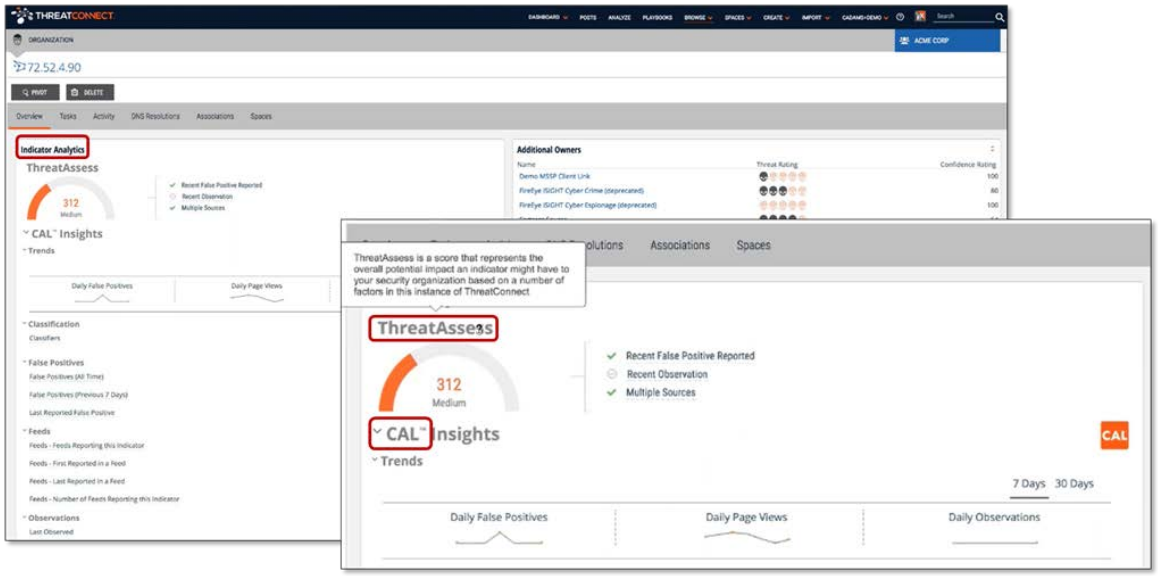
Threat intelligence is essentially a relational dataset. Hosts resolve to IP addresses, IP addresses are associated with adversaries, adversaries perpetrate campaigns. How the pieces of this puzzle fit together is best provided visually. ThreatConnect provides a graphical visualization of intelligence. The graph view is available on the *Details* page for every indicator, group, and tag. ThreatConnect offers several options to control how many and which type of nodes appear on the graph to simplify analysis (see Figure 4). On the left, the trojan Heriplor (orange circle) connects two separate incidents in our test environment (dark blue) by way of a series of file hashes (blue and orange lines). That view is expanded in the second image to identify patterns and campaigns in the wild.

Figure 4. The ThreatConnect Graph View



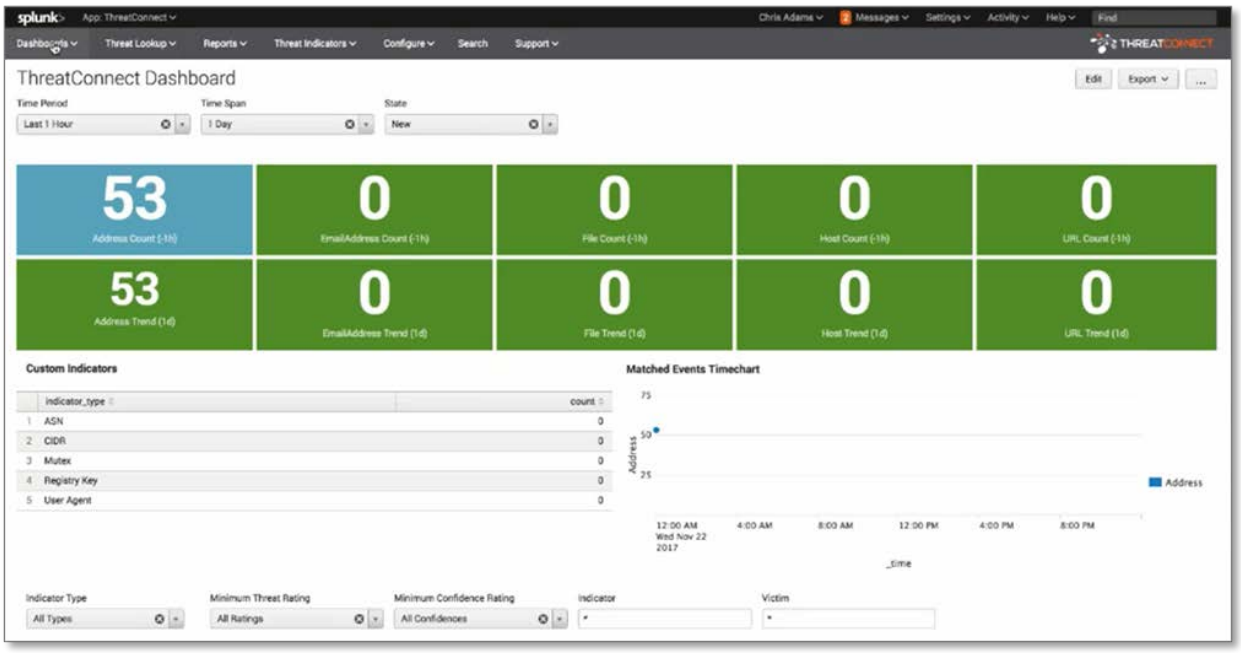
The next step in the process was to use TC Identify's ThreatAssess and CAL to find relevant threat intel on a singular indicator (see Figure 5). By selecting a specific indicator, ESG Lab drilled down into its activity history with an easily digested readout. The Indicator Analytics on this page showed all activity for the indicator, providing a ThreatAssess score and multiple ways to examine false positives, feed sightings, and more. ThreatAssess provides a single score for each indicator by using an algorithm that reads its activity from the organization's subscribed sources. CAL Insights in TC Identify provided 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



ESG Lab noted that TC Identify's speed at dissecting an organization's mix of free and premium sources was boosted even further 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. To detect any activity, the ThreatConnect app used indicator traffic from the organization's firewall and returned any addresses that had recently passed through Splunk. 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

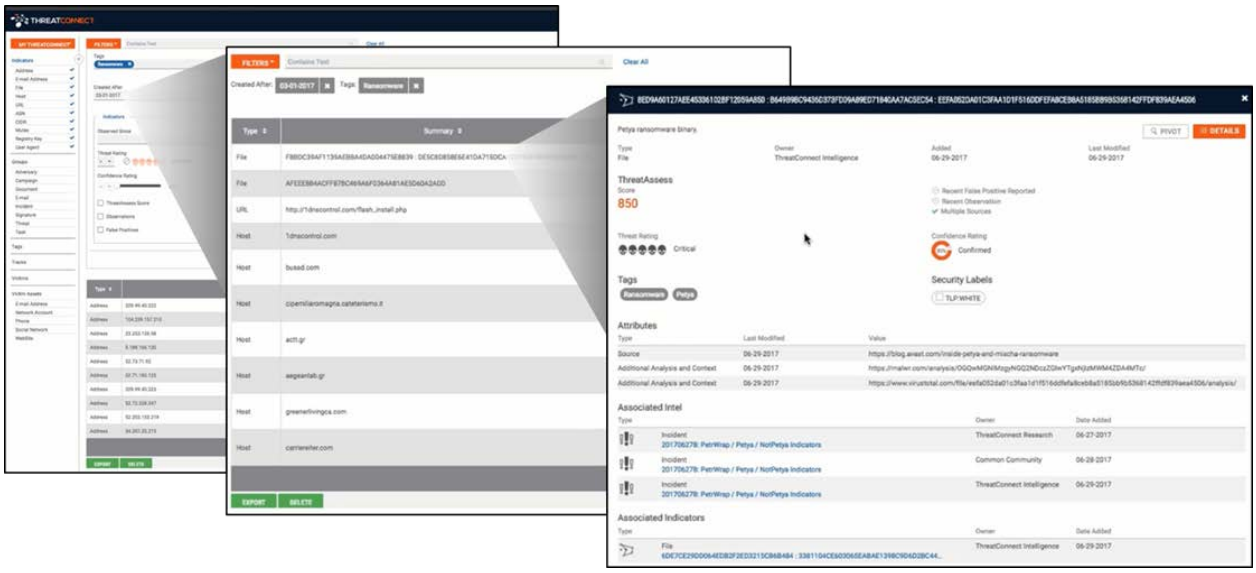


Finally, ESG Lab tested to see how each of TC Identify's tools came together to enable a live customized search for threat intelligence. In this case, ESG Lab wanted to consider recent ransomware incidents that affected health care organizations.

Selecting ***Browse*** from the top ribbon menu brought us to a discovery tool that allowed us to make advanced searches across enabled sources in TC Identify.

Selecting the ***Filters*** button expanded the search window and allowed for editing of these attributes. ESG Lab entered *Ransomware* in the ***Tags*** search bar to select it from a list of related options and changed the date filter to search for any threats having occurred since March 2017. Clicking the ***Apply*** button on the right side of the screen refreshed the search with the new filters in place, populating results instantly with any indicators matching the search parameters.

Figure 7. Ransomware Search as a Health Care Company



Results could be sorted by clicking the head of each column, allowing the user to prioritize indicators by different attributes such as Threat Rating or date added (see Figure 7). Clicking an indicator produced a window showing the highlights for that selection. ESG Lab instantly received additional details, such as any incidents the indicator was associated with and even other indicators that were part of the same incident. Hovering over the indicator on the search results screen prompted us with a "View Full Details" option that brought up the indicator screen showing ThreatAssess score and CAL insights.

ESG Lab also fashioned a search for these results using a different approach. TC Identify lets users search for any threats related to a specific sector, so we searched for known indicators to the health care sector. This scenario produced results like the first search, proving that organizations missing conventional security skills can still benefit from TC Identify's ability to quickly digest all the user's active source feeds.

The Bigger Truth

ESG research proves that cybersecurity is not only more difficult to manage than ever, but the supply of personnel to rely on has never been lower. While an organization's technical prowess and the services it employs are pivotal pieces of its cybersecurity strength, there is little customers can do with their money that replaces human experience with threat detection. Building a threat-conscious IT team to helm any infrastructure is a daunting enough task and sifting through log data with little to no points of reference other than precedent does not lend itself to a confident IT approach.

TC Identify offers a shrewd threat intelligence platform built specifically to shore up these vulnerabilities. While it won't hire a team of experts for customers, it does give them access to invaluable insights crafted by ThreatConnect's own veteran research team, along with the activity and content created by other organizations already experiencing the benefits of its source library and CAL. The ability to shape the experience for each sector hones its features and reduces the time it takes IT teams to detect relevant potential threats.

ESG Lab validated that TC Identify provides a thorough threat assessment experience for users by giving them the right tools to dive deep while connecting them with a firmly established cybersecurity community. If your organization would like to move beyond simple threat detection and learn the story behind the activity in your environment and how it's interconnected—so you can make confident decisions on how to respond—ESG Lab recommends you take a serious look at TC Identify.