Technical Review

ThreatConnect TC Analyze Threat Intelligence Platform

By Alex Arcilla, Validation Analyst; and Tony Palmer, Senior Validation Analyst

July 2018

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 Analyze to verify its ability to reduce an organization's mean time to respond to security incidents and threats. We focused on how TC Analyze can help security operations center (SOC) and incident response (IR) analysts to enrich threat data and create intelligence about identified threats, import files or emails to extract potential threats, manage action items related to specific threats and incidents, and create customized dashboards.

The Challenges

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. 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 such as 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 in-house threat intelligence continuously to mitigate the skills shortage.

The Solution: ThreatConnect TC Analyze

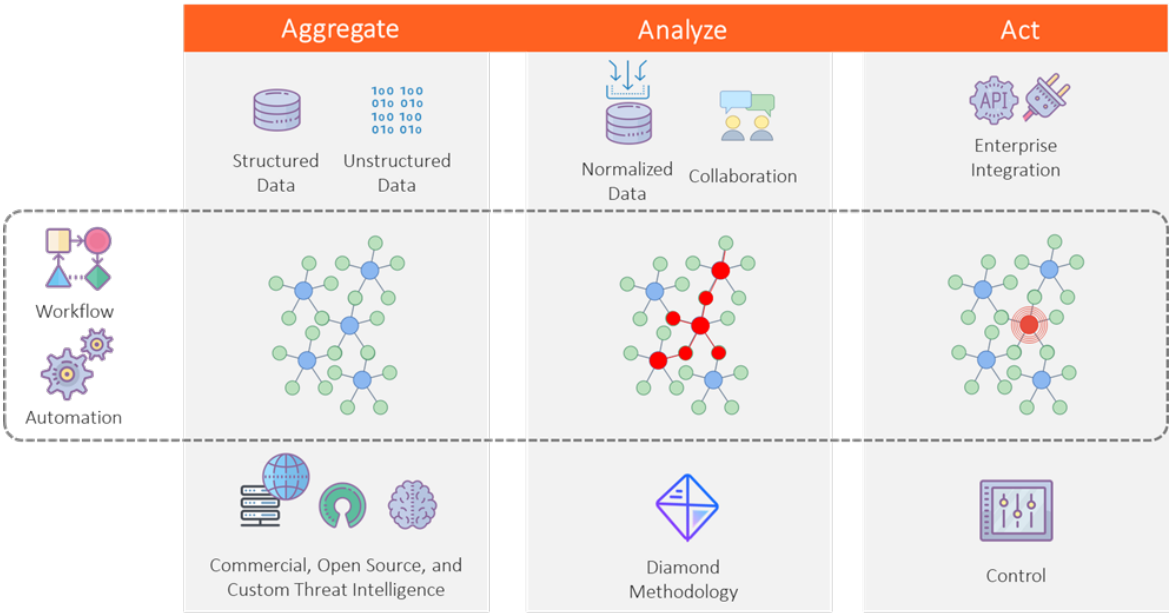
TC Analyze provides security analysts with insights into gathered intelligence about known threats and leverages that intelligence to uncover potential threats. With feeds from open source or fee-based security intelligence sources, TC Analyze aggregates and filters existing data that enables organizations to prioritize actions as well as educate current and future analysts on the evolving threat landscape. TC Analyze allows analysts to:

- *Ingest files*—to extract potential threats and begin tracking them.
- *Build upon existing threat intelligence*—within TC Analyze and share this knowledge throughout the organization.
- *Manage incidents and threats to their resolution*—by assigning tasks to other team members.
- *Create custom dashboards*—to track events of particular interest.

TC Analyze can best serve security teams that want to decrease the mean time to respond to threats as they face an ever-increasing amount of data to consume, analyze, and understand.

[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.

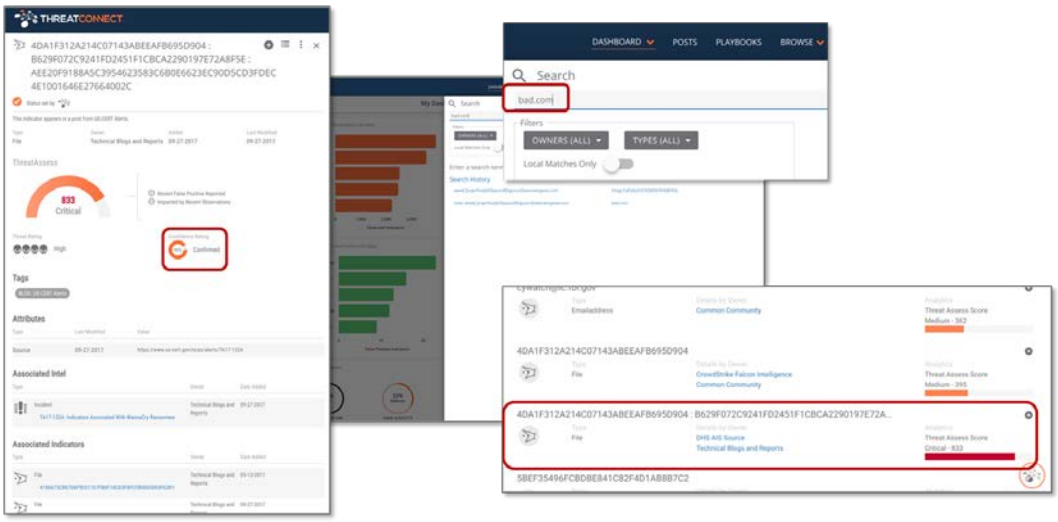
Figure 1. ThreatConnect TC Analyze



ESG Lab Tested

ESG Lab began by examining how TC Analyze flags potential intrusions using the search function (see Figure 2). 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 Analyze 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.

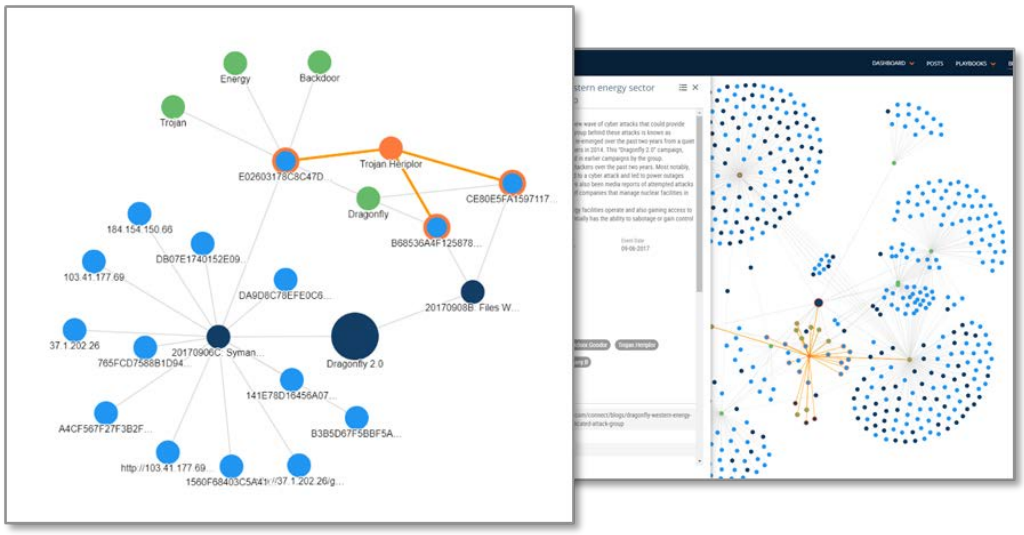
Figure 2. Using Search to Find and Prioritize Intrusions



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

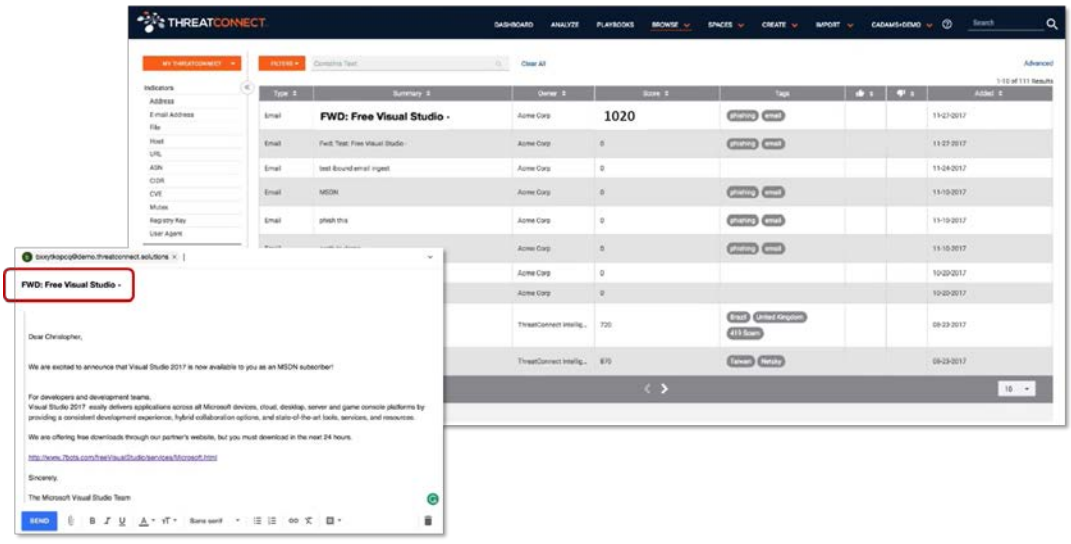
indicator, group, and tag. ThreatConnect offers several options to control how many and which type of nodes appear on the graph to simplify analysis (see Figure 3). On the left, the trojan Heriplor (orange circle) connects two separate incidents in our test environment (dark blue) by way of a series of file hashes (blue and orange lines). That view is expanded in the second image to identify patterns and campaigns in the wild.

Figure 3. The ThreatConnect Graph View



ESG Lab then examined how TC Analyze helps to build an organization's threat intelligence by ingesting an email and extracting IOCs (see Figure 4). We first set up an email address in ThreatConnect to receive phishing messages, then forwarded a sample message to that address. We noted that TC Analyze can help an analyst to view all phishing email inboxes and associated risk scores, assess threat severity, and prioritize attention on those items.

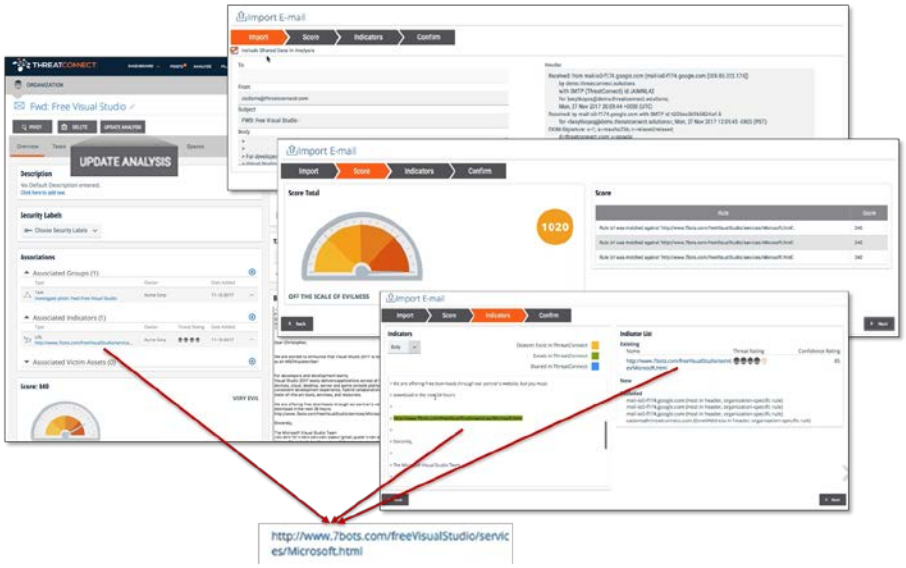
Figure 4. Creating an Inbox to Gather Phishing Emails



After sending the phishing email, TC Analyze extracted associated indicators and assigned a risk score. On the screen detailing compiled intelligence about the *FWD: Free Visual Studio* email, we clicked on the ***Update Analysis*** button to examine the entire email body (see Figure 5). As we clicked through the ***Import***, ***Score***, and ***Indicator*** options, we ingested the email contents, confirmed the high threat rating, and discovered another potentially malicious URL. TC Analyze identified this by searching through its associated intelligence sources and found that the indicator already existed in the

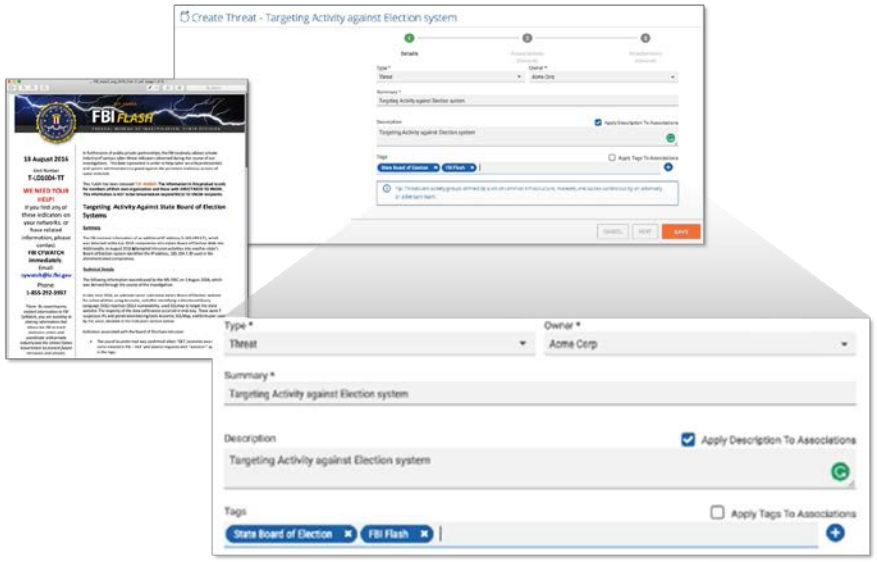
current ThreatConnect Platform. TC Analyze saved this specific URL to build upon the existing threat intelligence associated with the email address, thus informing other analysts in the future should they encounter the URL again.

Figure 5. Extracting Associated Indicators from Imported Phishing Email



An analyst can also use TC Analyze to create a potential threat to track. ESG Lab examined this use case with a report from a widely used intelligence source, the FBI. We prompted TC Analyze to ingest the file and extract any contained IOCs. We proceeded to create a threat named *Targeting Activity against Election System*. Then, we inputted details such as the organization name associated with the tracker, summary title of the threat, description, and tags and clicked ***Save*** (the orange button in Figure 6).

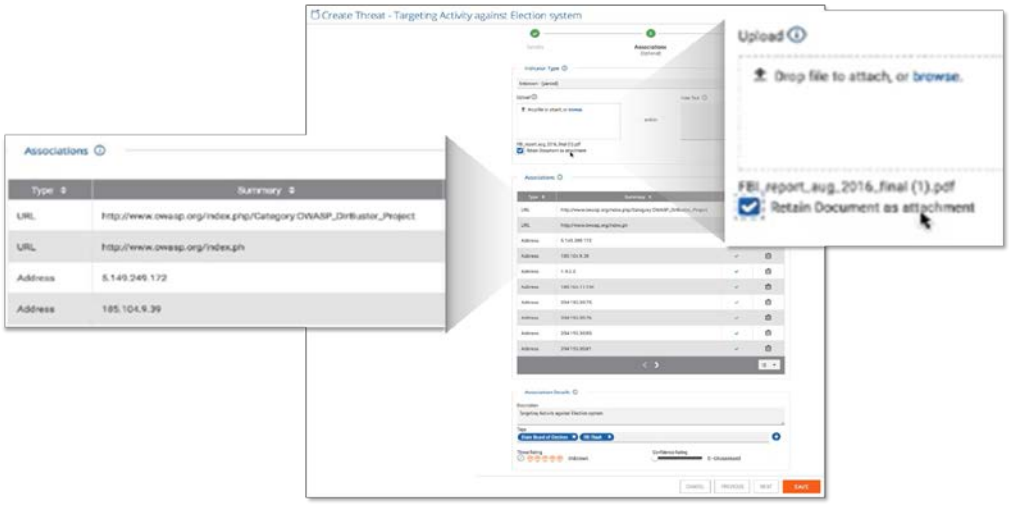
Figure 6. Create New Threat by Extracting IOCs from File



ESG Lab 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 contained IOCs that alert analysts of the highlighted threat. After clicking on the ***Save***

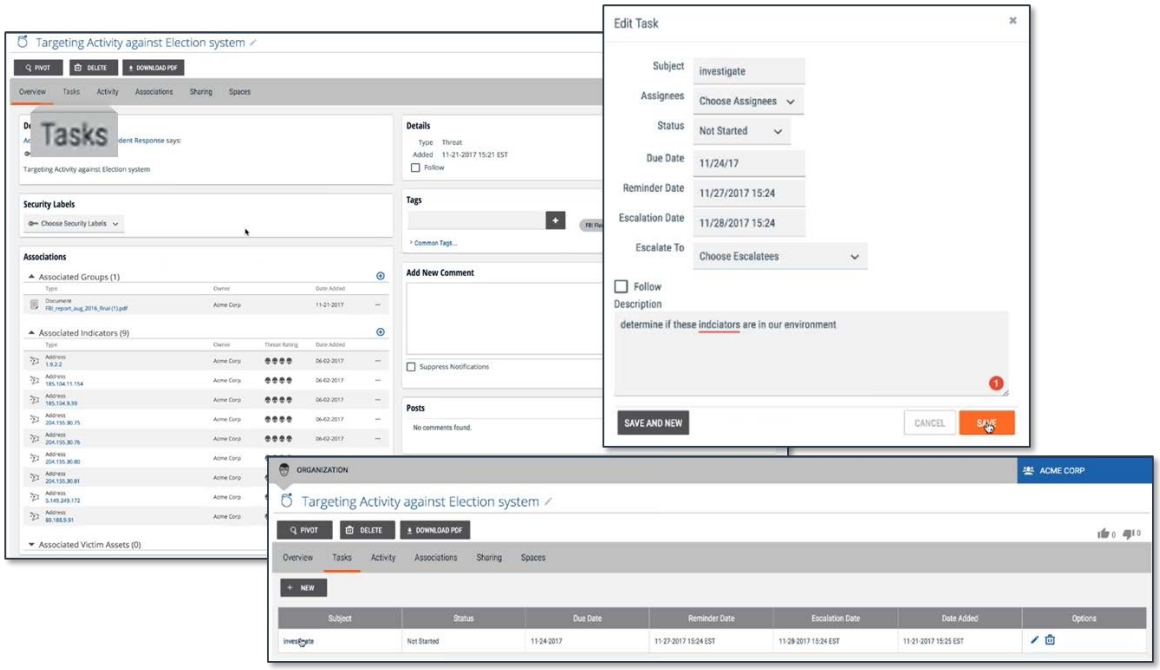
button, TC Analyze extracted the indicators, as seen in Figure 7. As in the previous example, we dragged the file icon representing the FBI report onto the box below the *Upload* heading.

Figure 7. Extract Associations for Specific Threat



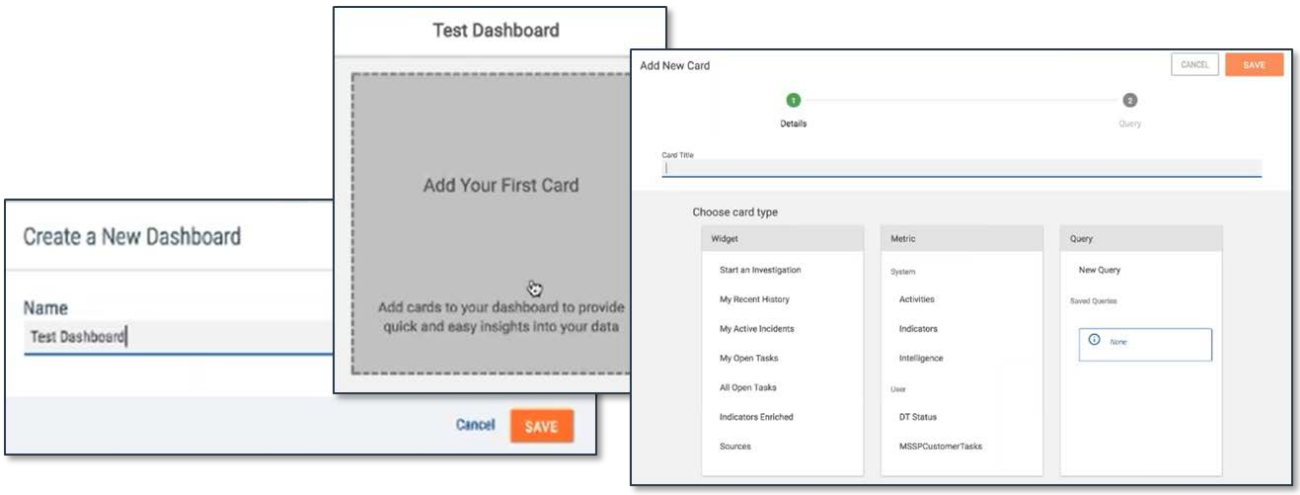
After creating a threat, ESG Lab then observed how an analyst can assign related tasks to other colleagues. Beginning with the record of the threat, *Targeting Activity against Election System*, we clicked on the ***Tasks*** menu and then clicked on the ***New*** button. We proceeded to fill in the fields on the ***Edit Task*** window such as assignee, due date, and description. After clicking ***Save***, the task named *Investigate* appeared on the ***Tasks*** list. We also observed that after clicking on the task, TC Analyze navigated back to the threat record. ESG Lab noted that the assignee can add additional information to the threat record as she completes the task. Given that an analyst can assign tasks associated with specific threats, ESG Lab noted how the workflow can foster collaboration and accountability within a security analyst team, helping to decrease the time to respond to a threat.

Figure 8. Creating and Assigning a Task to an Analyst



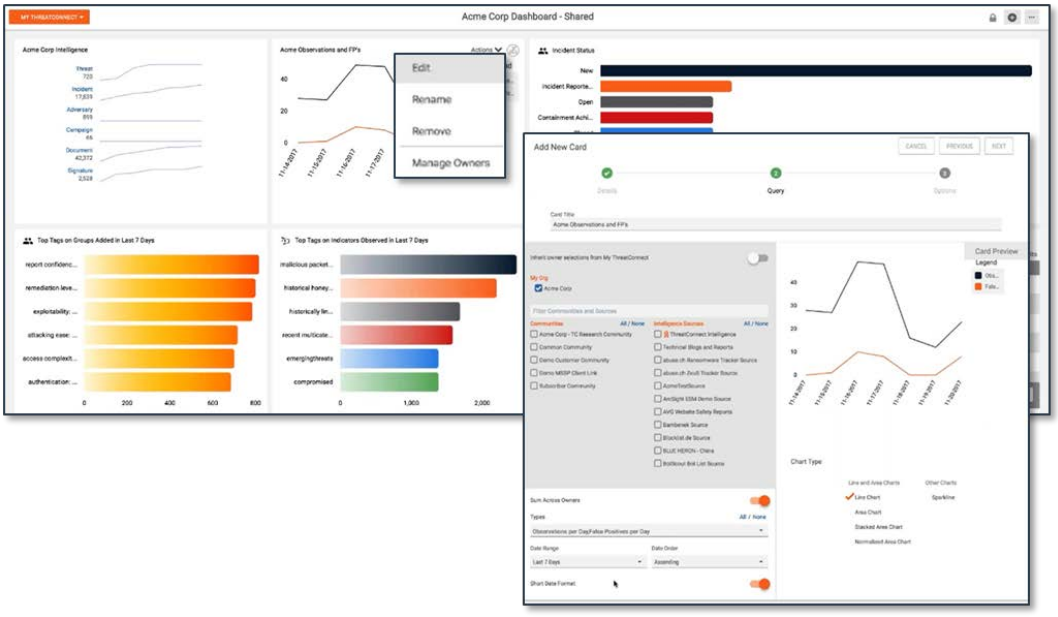
Finally, ESG Lab examined how an analyst can create custom dashboards. We clicked on ***Dashboard*** on the menu bar to display a drop-down menu. After clicking on ***New Dashboard***, we typed "Test Dashboard" in the *Create a New Dashboard* pop-up window (see Figure 9). We then saw the screens that allow the user to add cards and customize the content based on provided widgets (e.g., "Start an Investigation" and "My Active Incidents"), metrics (e.g., counting activities or indicators over time), and queries.

Figure 9. Creating a New Dashboard



ESG Lab also observed how to add queries to a dashboard (see Figure 10). An analyst may need to track query results over time to uncover frequency of specific incidents or possible trends. We navigated to ***Acme Corp Dashboard*** from the ***Dashboard*** drop-down menu, clicked on a down arrow in one card, and chose ***Edit***. On the ***Add New Card*** pop-up window, we noted the fields that the analyst fills to track the query, including the language for generating the query (using ThreatConnect's in-house query language), query sources (e.g., intelligence feeds), metric type, time period, and chart type (e.g., line or bar). ESG Lab saw that an analyst can customize a dashboard to focus attention on critical items while helping to continually build the organization's threat intelligence knowledge base.

Figure 10. Adding New Query to Custom Dashboard



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. Organizations need tools that will help them not only understand and identify current and emerging threats, but also know when and how to respond to them.

TC Analyze can enable security teams to consume data from multiple sources and extract context on threats, allowing the team to prioritize those that present the most clear and present danger. The solution also enables analysts to collaborate on these threats by offering team communication within TC Analyze via task assignment and additional insights. TC Analyze 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 TC Analyze 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. TC Analyze parsed and extracted data relevant to known threats, calculating ratings and scores to educate analysts on threat severity. ESG Lab also examined how TC Analyze extracted key indicators that notify the analyst of a specific threat presence. For any identified threat, we saw how an analyst can assign tasks to colleagues, enabling analyst teams to collaborate on threat resolution. Finally, TC Analyze enables the creation of custom dashboards that focus analysts' attention on key events, allowing them to respond quickly should issues arise.

The Bigger Truth

ESG research confirms that the cybersecurity landscape is becoming increasingly complex and difficult to manage.[3] 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. 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. As part of an overall security program, organizations need robust analytics to respond to incidents quickly.

TC Analyze aims to enable centralized data enrichment and incident and task management to provide context to the data, enabling and recommending actions with defensive tools, and helping organizations make faster, more informed security decisions. TC Analyze combines open source and premium feeds 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 TC Analyze to continuously improve the intelligence.

In ESG Lab testing, TC Analyze demonstrated the ability to gather and enrich threat data from multiple security intelligence sources relevant to known threats, presenting ratings and scores to enable analysts to prioritize their time based on threat severity. TC Analyze extracted key indicators from files such as emails identifying a specific threat presence. TC Analyze demonstrated the ability to automatically share indicators to relevant tools and systems, which can enable various teams to collaborate on threat resolution. ESG Lab used TC Analyze to quickly and easily create a custom dashboard. Custom dashboards can help focus analysts' attention on key events, allowing them to respond quickly should issues arise.

ESG Lab validated that ThreatConnect's TC Analyze can help organizations overcome the cybersecurity skills gap with analytics and response capabilities while building in-house threat intelligence continuously. For organizations that want to move beyond the capabilities of legacy SIEM platforms and leverage threat intelligence throughout their environments, it would be worthwhile to take a closer look at ThreatConnect's TC Analyze.

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

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.