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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Background</td>
<td>3</td>
</tr>
<tr>
<td>The Solution: The ThreatConnect Platform</td>
<td>4</td>
</tr>
<tr>
<td>ESG Lab Validation</td>
<td>5</td>
</tr>
<tr>
<td>Reducing Mean Time to Detect Threats</td>
<td>5</td>
</tr>
<tr>
<td>ESG Lab Testing</td>
<td>5</td>
</tr>
<tr>
<td>Reducing Mean Time to Respond</td>
<td>8</td>
</tr>
<tr>
<td>ESG Lab Testing</td>
<td>8</td>
</tr>
<tr>
<td>Threat Hunting</td>
<td>14</td>
</tr>
<tr>
<td>The Bigger Truth</td>
<td>16</td>
</tr>
</tbody>
</table>

---

## 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) has impacted their organizations. 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

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td>51%</td>
</tr>
<tr>
<td>IT architecture/planning</td>
<td>33%</td>
</tr>
<tr>
<td>Server/virtualization administration</td>
<td>26%</td>
</tr>
<tr>
<td>Data protection (i.e., backup and recovery)</td>
<td>26%</td>
</tr>
<tr>
<td>Application development</td>
<td>25%</td>
</tr>
<tr>
<td>Compliance management, monitoring and reporting</td>
<td>25%</td>
</tr>
<tr>
<td>Business intelligence/data analytics</td>
<td>25%</td>
</tr>
<tr>
<td>Mobile application development</td>
<td>24%</td>
</tr>
<tr>
<td>Network administration</td>
<td>23%</td>
</tr>
<tr>
<td>Storage administration</td>
<td>22%</td>
</tr>
</tbody>
</table>

Source: Enterprise Strategy Group

---

1 Source: ESG Master Survey Results, 2018 IT Spending Intentions Survey, December 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](image)

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.

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

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 parses 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

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
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](image)

---

### 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. 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.

---

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

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.
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

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

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.
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.

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**

---

**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

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

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. 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.

---


© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.
Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.