



ThreatConnect for Security Operations

Make your existing technology investments smarter and establish a more efficient security operations team with ThreatConnect



With ThreatConnect, you're able to centralize your intelligence and automate your processes out of one Platform, driving multiple benefits for your business:



Reduce False Positives and Focus Triage Efforts

Automatically sort false positives in your SIEM and free your time to focus on triaging legitimate alerts. By cross-checking the data with ThreatConnect's CAL™ (Collective Analytics Layer) and external sources of threat intelligence — tech blogs, OSINT, and premium data feeds — you'll have the most complete information possible. Determine where a deeper investigation is needed with customized workflows and playbooks.



Streamline Communication Across Teams

Set up Playbooks to trigger based on time or a specific action, which allows for extensibility and predictability across your security operations. Then, notify team members in the Platform or in a tool where they already communicate with multiple integrations, like Slack.



Quicker, More Efficient Onboarding

The most time consuming parts of onboarding a new team member are training on your specific products and processes. ThreatConnect enables the automation of many processes, and, with a built-in document repository, you can keep all pertinent documentation in one easily accessible place for everyone.



Establish Consistent and Repeatable Processes

With ThreatConnect Playbooks, you can document processes more efficiently and consistently. Track metrics on completion, and time and dollars saved to demonstrate return on investment and the value of individual Playbooks.



ThreatConnect.com



3865 Wilson Blvd., Suite 550
Arlington, VA 22203



sales@threatconnect.com



1.800.965.2708

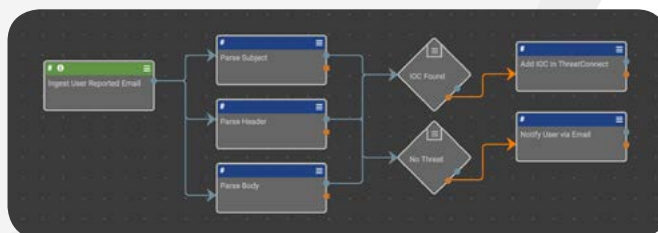
An Example of ThreatConnect in Action:

Automating Phishing Reporting, Analysis, & Response

Dealing with the management of user-reported phishing emails, sifting through the information to determine what's a legitimate threat and what's not, and acting accordingly is a necessary but extremely time consuming process. Do it in seconds with ThreatConnect.

Easy User Reporting

In ThreatConnect, set-up a mailbox for centralized reporting of potential phishing emails from all sources, including both humans and technologies like Email Security Gateways. When the mailbox receives a message, the rest of the Playbook is triggered to automate the analysis and corresponding response efforts.



Automated Email Analysis

Reported emails are parsed for indicators which are extracted from the email. Those indicators are automatically correlated against threat intelligence within ThreatConnect that has been aggregated by third party feeds and CAL. If indicators are found to be malicious, appropriate response efforts are seamlessly kicked-off.

Quicker Response Times

Emails containing malicious indicators trigger response efforts such as user and administrator notifications, as well as communicating with other technologies such as firewalls and secure web gateways. If the email is deemed safe, the user is appropriately notified and can be marked as a false positive for future considerations.

Request A Demo

Call **1.800.965.2708** or visit threatconnect.com/request-a-demo



Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.



ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708

Copyright © 2019 ThreatConnect, Inc.