ThreatConnect + DOMAINTOOLS

ThreatConnect & DomainTools

Together, ThreatConnect® and DomainTools® Iris Investigate allow security analysts to automate intel processes, investigations, alert triage, and response actions leading to faster detection and response.

Integrated Products:

DomainTools Iris Investigate

ThreatConnect

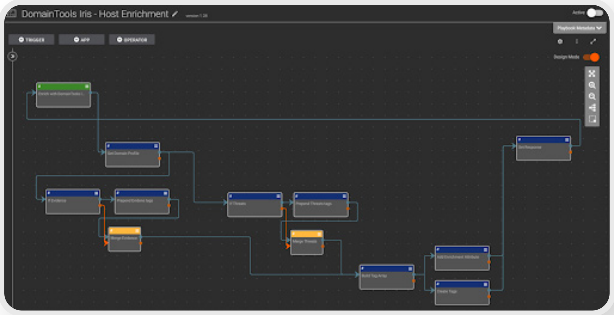
Integration Overview

DomainTools Iris Investigate allows researchers and threat hunters to monitor changes in adversary infrastructure and enrich data as part of the investigative process. By combining this with the power of ThreatConnect, they can now automate investigative and hunting actions that allow users to respond to threats and protect their network against sophisticated attacks.

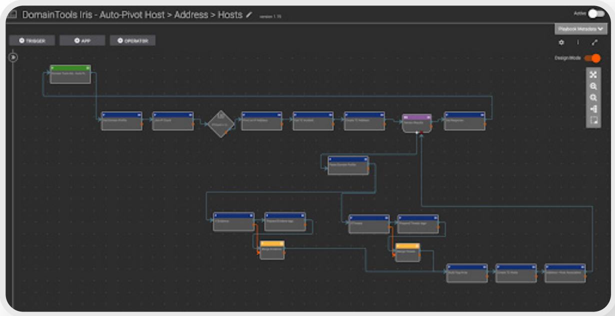
Use Case #1: Perform Auto-Enrichment/ Enrich Indicators

Action: Get Single Domain Profile, Get Multiple Domain Profiles

With this Playbook App, analysts can automatically enrich domain artifacts that are part of alerts or incidents. Additionally, they have the ability to enrich Indicators or processes with Domain Profile information by submitting single or multiple domains at once. By automating enrichment with Playbooks, analysts can work through investigations more efficiently.



*Playbook Template Available**



*Playbook Template Available**

Use Case #2: Auto-Pivot an Investigation

Action: Search and Pivot

With this Playbook App, analysts can auto-pivot to expand their investigation to additional levels by quickly identifying which attributes of a domain name are connected with a relatively small number of other domain names. The ability to auto-pivot allows them to narrow down their investigation and work through them more quickly.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

Use Case #3: Perform a Reverse Search

Action: Parse Domain Profile Results

With this Playbook App, analysts can perform a Reverse Search on one or more search fields --IP address, SSL hash, email, or more -- and the integration will return Domain Profile information for any domain name with a record that matches the search. The ability to parse Domain Profile results provides analysts more context and helps them to make informed decisions.

Use Case #4: Build Automated Processes

Action: Get Search Hash Results

Build automated processes between analyst work in the Iris Investigation platform by monitoring for Search Hash results or matching Tags. The ability to get search hash results directly in Playbooks will save analysts time switching between screens and platforms.

Features and Benefits

- ✓ Add valuable context to threat data to help prioritize, and eventually mitigate threats
- ✓ Retrieve the DomainTools Risk Scores, Classification, Evidence, and Threats, then use these as a decision factor for scoring domain indicators or taking further actions
- ✓ Instantly access DomainTools' comprehensive data on domain name, DNS and related data
- ✓ Automate proactive cyber threat operations
- ✓ Inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

How to Get Started

If you are already a ThreatConnect customer, these Playbooks can be downloaded and installed from the ThreatConnect App Catalogue or by contacting your Customer Success Representative. If you are not a current ThreatConnect customer or user and would like to know more about this, or any of our other third-party apps or integrations, please email sales@threatconnect.com.

About DomainTools

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity at http://www.domaintools.com or follow us on Twitter:@domaintools

ThreatConnect

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