ThreatConnect + SHODAN

# ThreatConnect & Shodan

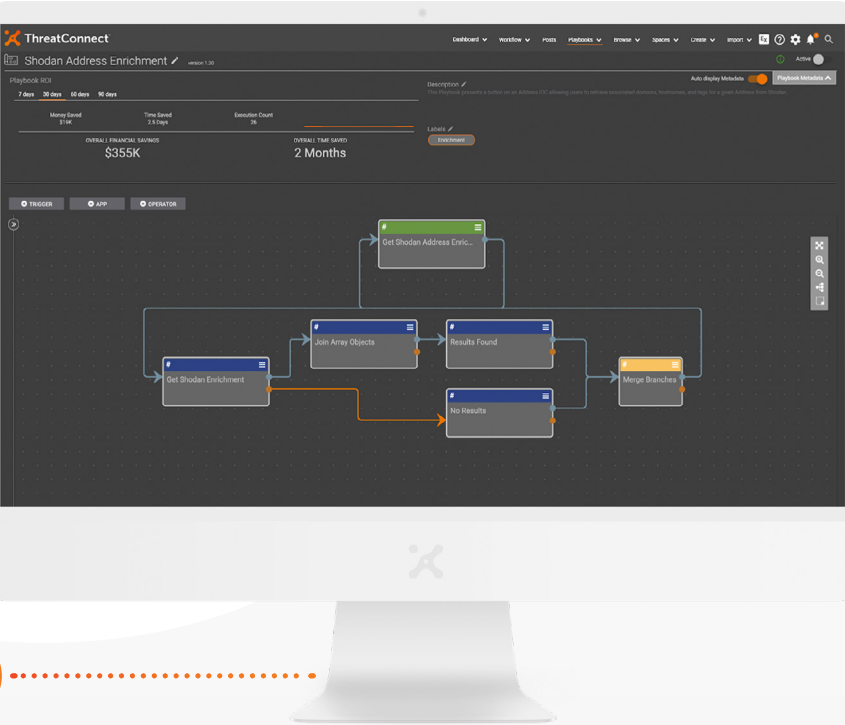
ThreatConnect® and Shodan® allow users to enrich their threat data and enhance their decision-making skills when performing an investigation.

Integrated Products

Shodan
ThreatConnect

## Integration Overview

This app allows you to retrieve multiple types of enrichment information for IOCs, craft custom Shodan searches to retrieve result sets based on numerous factors, and monitor your own potentially open and vulnerable infrastructure. Shodan is a powerful data enrichment platform and with the combined power of ThreatConnect Playbooks, security analysts will save time and resources.



Shodan Address Enrichment version 1.20

Playbook ROI

7 days 30 days 60 days 90 days

Money Saved $19K

Time Saved 2.5 Days

Execution Count 26

OVERALL FINANCIAL SAVINGS $355K

OVERALL TIME SAVED 2 Months

Description

This Playbook presents a button on an Address IOC allowing users to retrieve associated domains, hostnames, and tags for a given Address from Shodan.

Labels

Enrichment

### Use Case #1: Aggregate Enrichment Data Sources for a More Holistic Understanding of Threats

**Action: Get enrichment**

This Playbook will allow analysts to aggregate various outside sources that provide enrichment and analysis capabilities into one location - the ThreatConnect Platform. You will have a more holistic understanding of potential threats to make the most informed decision as part of your analytic, investigative, and remediation actions. The Playbook will retrieve sandbox results, correlate with intelligence sources and request EDR platform to find and block the malicious files.

Shodan Address Enrichment Playbook App

### Use Case # 2: Corroborate or Dispute Outputs for More Confident Decision Making

**Action: Search Shodan**

Corroborate or dispute the output from other tools and services to perform an all-source assessment. Because operations feed intelligence in a continuous loop, your Security Operations Center (SOC) and Incident Response (IR) teams can leverage the Threat Intelligence team's work during their investigations.

ThreatConnect.com

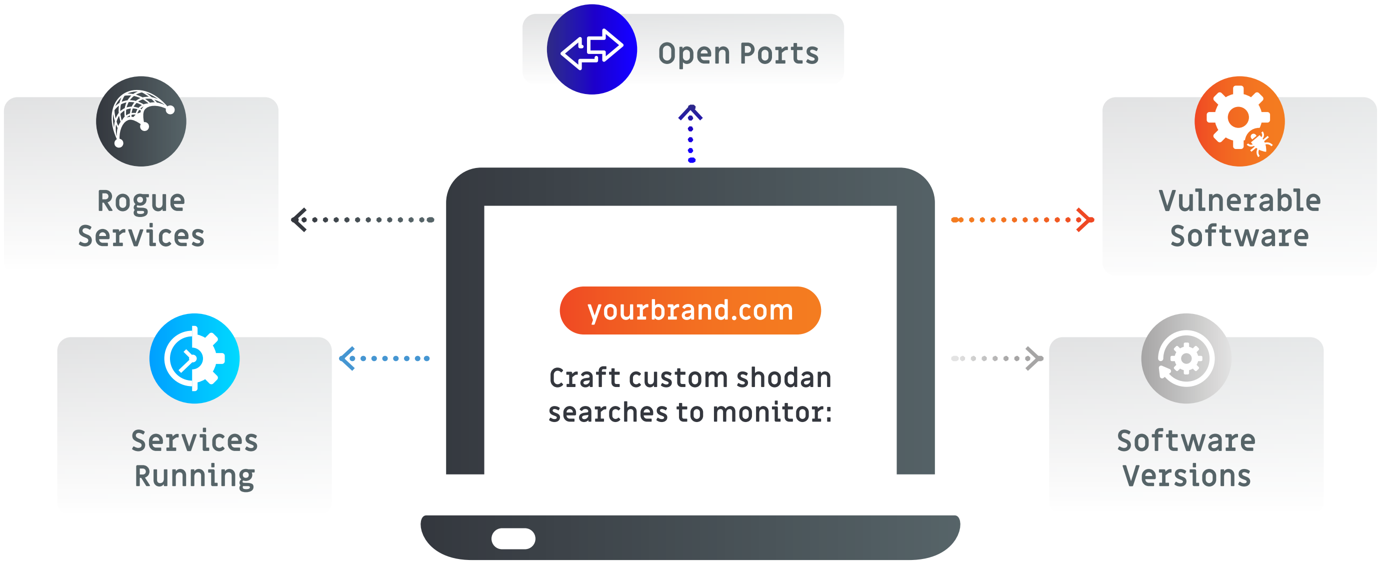
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

## Use Case #3: Monitor your Infrastructure

**Action: Search Shodan**

Craft custom Shodan searches to retrieve result sets based on many factors such as software versions being run, services running, open ports, rogue services, vulnerable software, and more. This means you can monitor for potential instances of your own enterprise's infrastructure appearing in the Shodan data set allowing direct and immediate value to be derived.



Open Ports

Rogue Services

Vulnerable Software

yourbrand.com

Craft custom shodan searches to monitor:

Services Running

Software Versions

## Features and Benefits

- ✓ Utilize information from Shodan to aid and corroborate intelligence analysis or validate security alerts accuracy and severity
- ✓ Add valuable context to threat data to help prioritize and eventually mitigate threats
- ✓ Automate processes with Playbooks and automate investigations with Workflow, saving your team time, bandwidth, and budget

### 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.

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