

# ThreatConnect SOAR

Optimize Your Security Processes, Increase Team Efficiency, and Reduce Time to Respond with an Intel-Driven Approach to Automation and Orchestration

ThreatConnect's Security Orchestration, Automation, and Response (SOAR) Platform provides a central location to integrate not only your security tools but all of your security team's processes. Document those processes within ThreatConnect and increase efficiency with automation and orchestration. Continuously leverage high confidence threat intelligence stored within ThreatConnect when making decisions related to both tactics and strategy. ThreatConnect enables the automation and continuation of this feedback loop throughout your entire security team.

## How ThreatConnect Helps

Below are actual results achieved by ThreatConnect customers during their first year of adoption.



### Resolve Alerts Faster

Average single alert resolution decreased from 30 minutes to 3 minutes, significantly reducing MTTR.



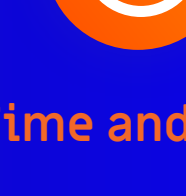
### Automate Repetitive Tasks

Repetitive analyst actions automated across 40 Playbooks to save 1000's of hours previously spent on tasks like manual lookups and notifications.



### Prevent Employee Burn Out

A reduced burden on analysts by 50% in the first year - decreasing burnout and attrition.



### Save Time and Money

Over \$1.3 million per year saved in labor costs with 60 automated workflows.

## What You Get with ThreatConnect SOAR

### HIGH CONFIDENCE INTELLIGENCE BAKED IN

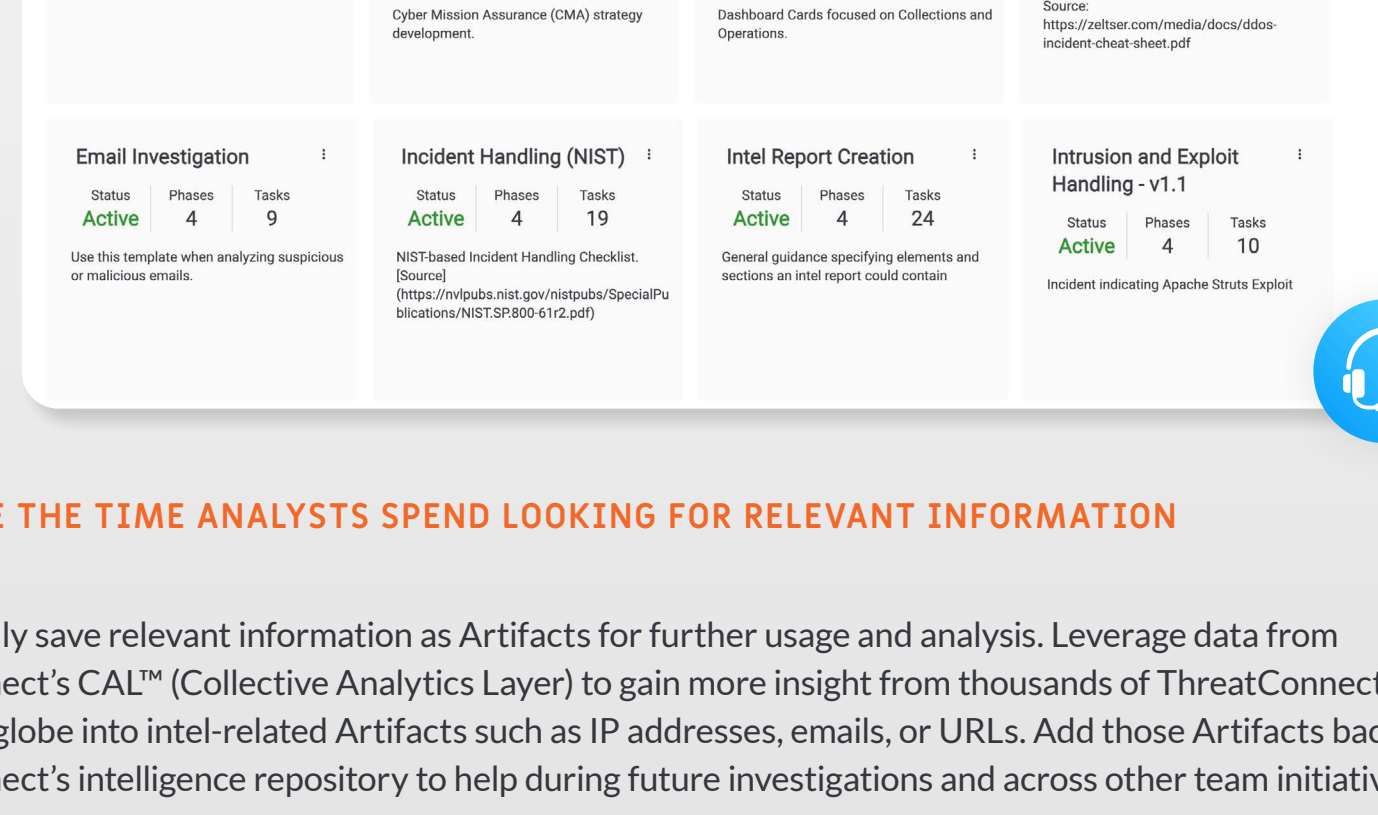
Receive access to various pre-populated intelligence sources packaged in a digestible and easy-to-use format. Because it's baked in, there's no need for complicated data manipulation or time-intensive lookups: it's all converted to a predictable and easily understood format while still preserving the source's attribution information and reputation details.

### DECREASE AMBIGUITY TO MAKE MORE CONFIDENT DECISIONS

Capture, correlate, and make decisions based on high-fidelity intelligence relevant to your organization. Adjust decisions on the fly based on the changes seen in the intelligence that is influencing the process. Automatically incorporate the latest intelligence to inform decision-making consistently.

### INTEGRATE SEAMLESSLY WITH EXISTING TOOLS FOR MORE EFFICIENT PROCESSES

Integrations with the tools and technologies in users' existing ecosystems make security easy and effective. Whether pre-built templates or completely customizable workflows are preferred - ThreatConnect supports the integrations required to power the use cases you need.



### MINIMIZE THE TIME ANALYSTS SPEND LOOKING FOR RELEVANT INFORMATION

Automatically save relevant information as Artifacts for further usage and analysis. Leverage data from ThreatConnect's CAL™ (Collective Analytics Layer) to gain more insight from thousands of ThreatConnect users around the globe into intel-related Artifacts such as IP addresses, emails, or URLs. Add those Artifacts back into ThreatConnect's intelligence repository to help during future investigations and across other team initiatives.

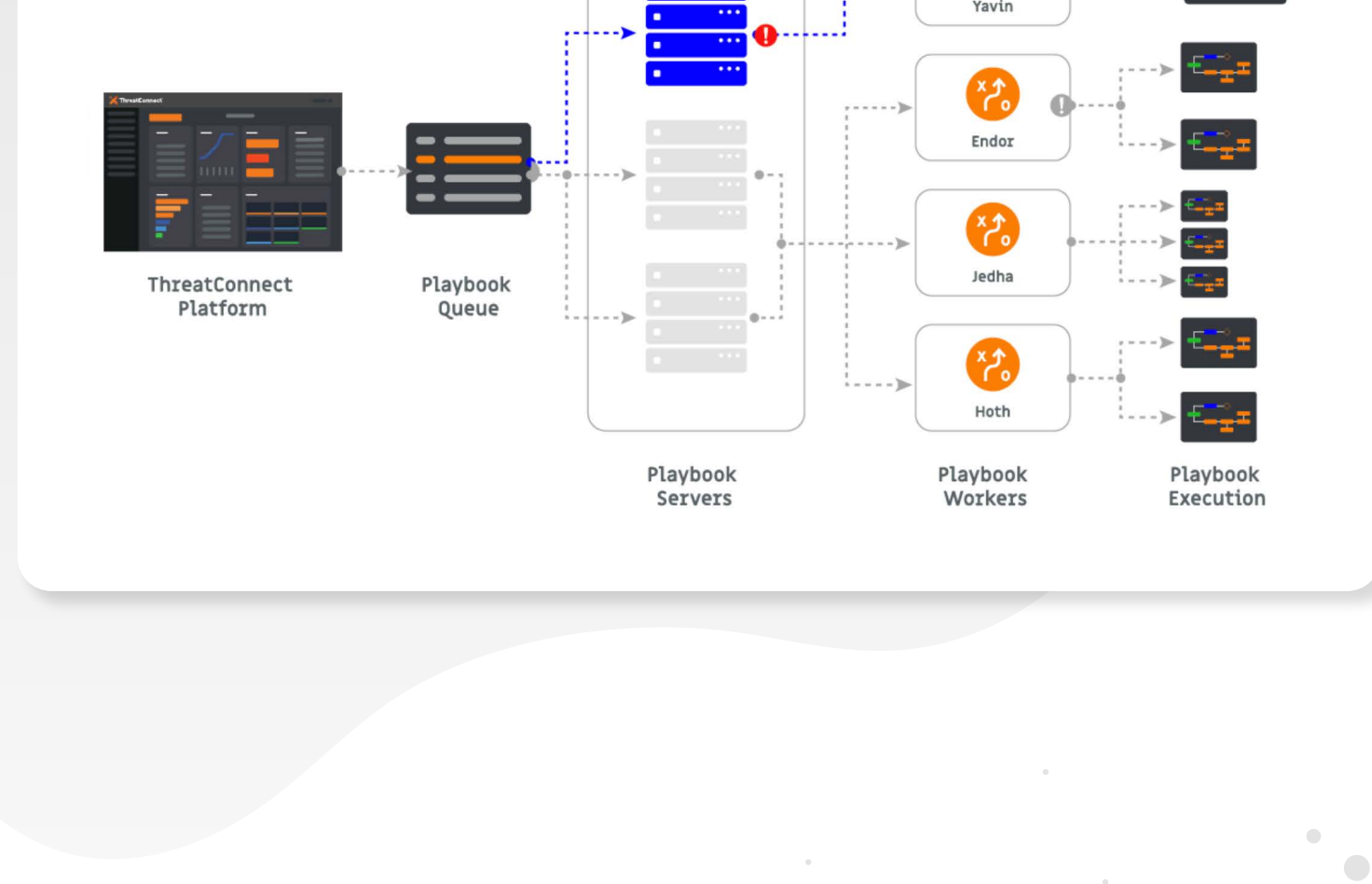
Artifacts						
Filter Artifacts by Name						
6 total results						
Type	Summary	CAL™	ThreatAssess	Task	Date Added	Status
File Hash	06E6B87DD6B474...	admin	Critical   833		2021-01-13 21:18:28	
CIDR	35.240.3.207/7	admin	173 Inactive		2021-01-09 11:36:20	
IP Address	185.107.56.58	admin	173 Inactive		2021-01-14 10:51:17	
IP Address	185.107.56.58	admin	173 Inactive		2021-01-13 21:15:15	
URL	http://bit.ly/ASD823...	admin	Medium   389		2021-01-13 21:16:02	
Host	stevemike-fireforce.L...	admin	402 Active		2021-01-13 21:17:23	

### CORRELATE CRITICAL INTEL TO EVENTS AND REDUCE THE RISK OF OVERLOOKING INSIGHTS

ThreatConnect tells you about potential and known associations across threat intelligence and cases to give you an immediate understanding of previous or open investigations related to a piece of threat intelligence you're investigating and vice versa. Get insight into these relationships and the associated details automatically, before you even need to ask.

### FLEXIBLE DEPLOYMENT OPTIONS

Flexible deployments in Cloud or On-Premises get you up and running the way you want quickly. Multi Environment Orchestration allows for orchestration across cloud, multi-cloud or hybrid on-premises environments. Wherever your security controls reside, ThreatConnect connects them seamlessly.



## How it works



## What makes ThreatConnect SOAR Different

- ✓ High Confidence Intelligence Baked-In
- ✓ Bi-Directional Integrations with 100's of Products
- ✓ Leverage Insights from Other ThreatConnect Users
- ✓ Customizable Dashboards to Bubble Up What Matters Most
- ✓ Complete Investigations from a Single Interface
- ✓ Dedicated ThreatConnect Customer Success Team
- ✓ Deployment Support for Cloud and On-Premises
- ✓ Scale Incrementally Without Affecting Performance

### About ThreatConnect®

ThreatConnect, Inc. provides cybersecurity software that reduces complexity for everyone, makes decision-making easy by turning intelligence into action, and integrates processes and technologies to continually strengthen defenses and drive down risk. Designed by analysts but built for the entire team (security leadership, risk, security operations, threat intelligence, and incident response), ThreatConnect's decision and operational support platform is the only solution available today with cyber risk quantification, intelligence, automation, analytics, and workflows in one. To learn more about our Cyber Risk Quantification, Threat Intelligence Platform (TIP) or Security Orchestration, Automation, and Response (SOAR) solutions, visit [www.ThreatConnect.com](http://www.ThreatConnect.com).

