



# ThreatConnect for Incident Response



## Maximize Incident Response With Threat Intelligence and Automation

With ThreatConnect, you're able to centralize your intelligence and automate your processes out of one Platform, maximizing insights, efficiency, and collaboration for your incident response team:

### Make Your Incident Response Fast, Precise, and Effective with Automation

The key to making IR activities easier, highly effective, and scalable to the number of threats targeting organizations is through automation. ThreatConnect's Playbook Automation leveraging low-code, drag and drop simplicity enables automation of the critical tasks and processes used by the IR team. ThreatConnect knows speed is critical when responding to an incident. Minimizing the spread of a threat actor can be the difference between a minor and major event. Precision is also important, insuring a threat is dealt effectively while minimizing the impact to business operations and users. Playbook Automation makes this happen.

### Maximize Insights Within Ticketing System Data

The knowledge and intelligence captured in case and ticketing systems is essential for incident response. ThreatConnect's native case management allows for comprehensive intelligence and data to be centrally leveraged by incident responders. A wide variety of flexible integration options provided through our REST API, and integration and playbook apps allow for easy collaboration with other popular case and ticketing tools like ServiceNow and Jira.

### Maximize Incident Response Efficiency and Consistency

ThreatConnect Workflows enable IR teams to embed and follow best practices into their activities. When responding to an incident, using the best practices and tradecraft across IR activities is critical. Consistent and repeatable processes is required when dealing with incidents that require handling according to industry, regulatory, and legal standards and requirements. Workflows are a powerful capability to ensure IR teams are all aligned, and working fast and efficiently when handling incidents.

### Maximize Collaboration for Better Communication

For all stages of incident response, communication is critical. Collaboration features are baked into the Platform, and information can be shared through integrations with other collaboration tools like Slack and Teams.

### Centralized Knowledge Capture

ThreatConnect can act as a storage repository for all the knowledge related to specific cases, as well as serve as a place to document all actions and notes related to cases, artifacts, or evidence in a structured format. This gives security teams efficient and rapid access to each other's notes and provides additional context when they need it.

#### THE CHOICE OF THE GLOBAL 2000

Nearly 200 enterprises worldwide protect their organizations with ThreatConnect

ORACLE®

workday

GENERAL DYNAMICS  
Information Technology

IBM

SONY



[www.threatconnect.com](http://www.threatconnect.com)

[sales@threatconnect.com](mailto:sales@threatconnect.com)

+1 (800) 965.2708

# An Example of ThreatConnect in Action

## Maximize Efficiency With Automated Case Management

ThreatConnect® automates data enrichment and case creation for smarter and faster incident response activities. ThreatConnect provides a central location for security analysts and incident responders to record, analyze, and interact with all information related to the case at hand. .

## Make Incident Management Smarter and Seamless

During response efforts, having everyone involved in an incident operating from the same intelligence and knowledge, regardless of what case or ticket system they are using, is critical. ThreatConnect connects a wide-variety of tools and automates knowledge capture and dissemination to ensure everyone is on the same page, working quickly and efficiently to resolve the incident.

## Create Threat Intelligence from Cases

Whether you are using the native case functionality in the ThreatConnect Platform or Integrating it with another ticketing system or incident response platform, it allows you to add intelligence captured from working those cases back into the Threat Library. This allows your team to maximize insights and close the threat intelligence loop. This important feedback loop ensures you are leveraging all the intelligence from your internal cases to make better decisions in the future.



## ● The ThreatConnect Platform

The cybersecurity environment continues to grow more challenging. Security teams are often overwhelmed by the constant stream of threats, and system vulnerabilities, against the backdrop of limited resources and immature processes.

The ThreatConnect Platform uniquely leverages risk insights and automation to help focus limited organizational resources on the organization's top priorities. The Platform operationalizes threat intelligence and knowledge to drive every decision and action faster to maximize impact with increased effectiveness, efficiency, better decision-making and strategic collaboration.

The benefits of the ThreatConnect Platform are clear - your security team will move from reactive to proactive engagement. Your team will better leverage risk insights and more effectively use threat intelligence and knowledge to drive better decisions and more effective action.

Reach out to learn how the ThreatConnect Platform can make you and your team more effective, decisive, and collaborative.

+1 (800) 965.2708 - or - <https://threatconnect.com/request-a-demo>

## ThreatConnect.

By operationalizing threat and cyber risk intelligence, The ThreatConnect Platform changes the security operations battlefield, giving your team the advantage over the attackers. It enables you to maximize the efficacy and value of your threat intelligence and human knowledge, leveraging the native machine intelligence in the ThreatConnect Platform. Your team will maximize their impact, efficiency, and collaboration to become a proactive force in protecting the enterprise. Learn more at [www.threatconnect.com](http://www.threatconnect.com).

ThreatConnect.com

3865 Wilson Blvd., Suite 550  
Arlington, VA 22203

[sales@threatconnect.com](mailto:sales@threatconnect.com)  
1.800.965.2708