Features and Benefits of ThreatConnect Powered by SAP HANA®

- Determine which intelligence feeds provide the most relevant data for your team to analyze and act on
- Pull all structured and unstructured threat data into one centralized platform including leading threat intelligence feeds, STIX-formatted data
- Automates normalization of data and allows teams to analyze and pivot between different data points to uncover patterns
- Flexible API allows you to integrate and connect all of your current critical network security products – more than 50 currently, and more in development
- Reduces or eliminates manual tasks, allowing teams to focus on resolving real threats
- Evaluate groups and incidents and create incident, adversary, and threat reports in PDF format for executive review
- Share threat intelligence with vendors, partners, and communities including ISAC, ISAO, and privately managed communities
- Leadership can create tactical Playbooks for their teams to ensure the best possible defense is in place, using all resources effectively
- Increase decision confidence and inform real-time decision making and take action based on detailed curation of what's happening in the moment

Schedule your demo today.

ThreatConnect

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

E: sales@threatconnect.com
P: 1.800.965.2708

NS2 NATIONAL SECURITY SERVICES

SAP National Security Services (SAP NS2®)
1101 Wootton Parkway
Rockville, MD 20852

E: info@sapns2.com
P: 877-9-SAPNS2
www.sapNS2.com

ThreatConnect

THREATCONNECT POWERED BY SAP HANA®

Intelligence-Driven Defense Supercharged with In-Memory Computing

HOW ARE ENTERPRISES HANDLING FRAGMENTATION AND THE VOLUME, VELOCITY, AND VARIETY OF DATA?

The Challenge

Organizations of all sizes share several similar and critical cybersecurity challenges. First, teams and tools are often disconnected. They don't communicate, they can't prioritize incident/event response efforts, and they can't benefit from leveraging historical data. Second, the sheer volume and variety of threat data and the velocity at which it pours in can be overwhelming. Security teams are often stuck sorting through endless raw data from free and open source intelligence feeds, struggling to make connections manually. When smart people are bogged down with manual labor, and when their tools don't enable collaboration, threats slip through the cracks.

The Solution

ThreatConnect was created to solve the fragmentation problem that security teams of all sizes face. It has since become the leading Platform for uniting cybersecurity people, processes, and technologies behind a cohesive, intelligence-driven defense. ThreatConnect's intelligence-drive security operations platform enables organizations to benefit from the collective knowledge and talents of the internal team, and also from trusted communities of peers and partners. Today, ThreatConnect customers use the Platform to develop security processes and workflows, and leverage existing security technologies to more effectively identify, protect, and respond to threats. **With ThreatConnect, organizations can process even more data and get real-time analytics with SAP HANA®.**

Currently, thousands of organizations worldwide use ThreatConnect to overcome fragmentation, improve effectiveness, and better protect their business' and customers' data.

ThreatConnect.com/SAP-HANA

ThreatConnect Powered by SAP HANA®

The ThreatConnect Platform, the first and industry-leading security operations and analytics platform is specifically designed to empower an intelligence-driven security program and mitigate threats faster using intelligence. Using ThreatConnect, customers are processing millions of indicators daily and the number is growing steadily. The latest edition of the ThreatConnect Platform powered by SAP HANA® is built on SAP's groundbreaking in-memory computing technology and has proven to be 54 times faster than prior versions of the Platform not powered by SAP HANA®. One of the most challenging roadblocks to threat intelligence is not having a platform that can adapt to the quantity of data and at the same time being able to perform analytical processing. With ThreatConnect powered by SAP HANA®, you are able to move at the same speed as your adversary – with the same robust features analysts, SOCs, and IR teams depend on: delivering actionable insights from volumes of threat data faster, more comprehensively, and more precisely.

Real-World Use Cases

How Teams Use ThreatConnect Powered by SAP HANA®

Threat Intelligence Team

Your Threat Intelligence teams (TI teams) are tasked with finding out everything they can about a particular compromise. TI analysts use ThreatConnect Powered by SAP HANA® to work faster and more efficiently.

- Pivot on indicators to find every discoverable detail about a threat
- Easily identify patterns to find out more about the adversary
- Better block attacks

SOC Team

Security Operations Center (SOC) teams face numerous incidents with no background information, and therefore no way to prioritize. Your SOC teams can use ThreatConnect Powered by SAP HANA® to thwart the threat before it takes a toll on your organization.

- Rapidly search your organization's threat repository for similar incidents and scope
- Estimate the kill chain stage of the threat
- Proactively estimate future threats and how to block them

Incident Response Team

Your SIEM is overwhelmed with logs, data, incidents, and more. The data isn't prioritized and your IR team doesn't know what to act on, or in what order. With ThreatConnect Powered by SAP HANA®, you can eliminate the guesswork. Your team is able to hone in on the most important incidents, ensuring that they focus on the real threats.

- Accelerate the time required to investigate, analyze and respond to threats
- Boil down millions of events to a manageable amount for triage
- Easily prioritize the events that your IR team needs to focus on
- Accelerate the time required to investigate, analyze and respond to threats

People Working Together in One Place

Your Security Teams With Your Trusted Partners, and Your Communities

Not only your Threat Intel, SOC, and IR teams will be able to work seamlessly together in ThreatConnect Powered by SAP HANA®, but also your private communities of partners, and any public communities of peers you collaborate with.

Private Communities of Partners

Your security team is no longer confined by data gathered solely within a department or your organization. With ThreatConnect's private communities, your team has the power to:

- **Share data with vendors, trusted partners, and supply chain to benefit from everyone's collective knowledge**
- **Improve efficiency by evaluating which communities and partners provide the most relevant data for your network defense efforts**
- **Leverage ThreatConnect Playbooks to triage events faster and automate mundane tasks**

Public Communities of Peers

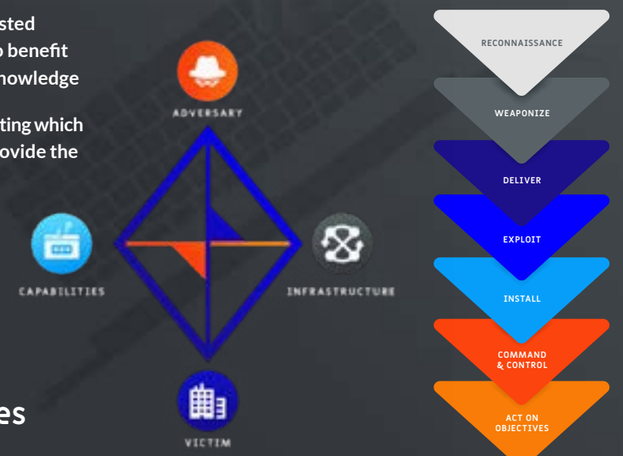
Evaluate and compare threat intelligence gathered by a global community of intel experts. You'll gain broader understanding of the evolving threat landscape and receive guidance on how to act.

- **Collaborate on objectives: focus on emerging threats or long-term missions**
- **Proactive defense: use intelligence from others to stop attacks before they happen**
- **Strength in numbers: collaborate with 10,000 individual users and 20+**

Build Processes to Identify, Protect, and Respond

Use Leading Cyber Threat Analysis and Response Methodologies

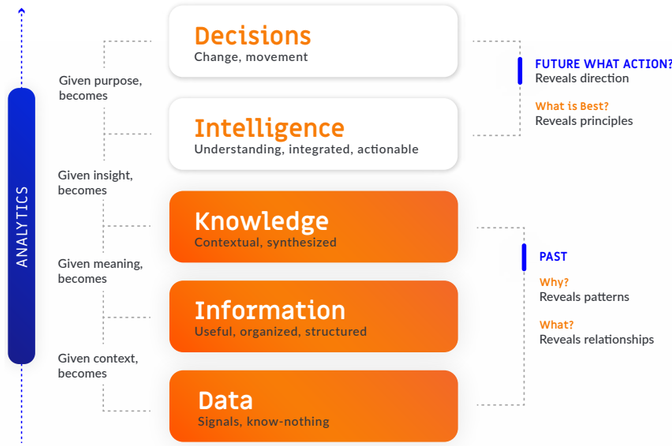
ThreatConnect is built around the Diamond Model for Intrusion Analysis. This proven Department of Defense threat intelligence methodology enables you to gain a complete understanding of an adversary or event. ThreatConnect also supports the kill chain and other methodologies, thanks to its flexibility and configurability. Analysts and security teams are not confined to a single analysis or operations model.



Manage All of Your Security Operations in One Place

Build processes to manage your security infrastructure from one central hub. Build cyber threat analysis and response processes based around ThreatConnect's built-in workflow features and integrations with leading security products.

Make Your Current Security Technologies Better, Smarter, and Faster



This illustrates how intelligence flows through every aspect of your security program; that your entire team is connected to intelligence, each other, and the tools; that a feedback loop from the people and tools is built-in to improve the intelligence. And, throughout the entire process, analytics are constantly enabling sound, fast decision-making.

Benefits for ThreatConnect Users

ThreatConnect Powered by SAP HANA® eliminates critical seconds in the incident detection and response process, and delivers added depth of analysis for improved protection.

Increase Speed and Performance

- Automated operations to cut down precious time
- Increased processing speed enables broader automation
- Dramatically reduce the manual labor of analysis

More Powerful Extensibility

- Build, host, and share custom applications to accomplish business or mission-relevant operations within the ThreatConnect platform
- Create advanced analytics, security workflows, and network protection with 50+ supported integrations with ease

Improve Threat Hunting on Your Network

- Added speed allows you to reach deeper into your own network, even while new data is coming in
- Form a comprehensive picture of threats to your business
- Act more quickly to profile and interdict threats that already exist
- Gather intelligence to shape a proactive posture against threats that are still emerging

Improve Ability to Identify and Prioritize Threats

- Easily aggregate and normalize threat data from any source or format – real-time or historical
- Pivot on enriched intelligence more quickly to discover patterns and context about an indicator