ThreatConnect. elastic

Amplify Threat Detection and Response in Elastic with the Power of ThreatConnect

The Challenge

Analysts monitoring, analyzing, and responding to threats are drowning in alerts, with limited means to determine which alerts and incidents are the most critical to address in order to protect the organization. Add to that all the false positives analysts have to contend with, and it creates an even more stressful situation. This leads to missed alerts, longer times to detect and respond to threats, and stressed-out staff.

Why ThreatConnect + Elastic?

The combination of Elastic Security and the unified, high-fidelity threat intelligence supplied by the ThreatConnect Threat Intelligence Operations (TI Ops) Platform enables SOC analysts, incident responders, and threat hunters to do their work faster, with greater effectiveness and efficiency, making their organizations more resilient to cyber attacks.

Key Benefits

- Strengthen threat detection, analysis, and response
- Prioritize and respond to incidents with speed and accuracy
- Make threat hunting more effective and productive
- Highly customizable integration enables higher-fidelity intel use in Elastic
- Not just a feed of raw indicators. Easily access additional intel context and relationship data in ThreatConnect.

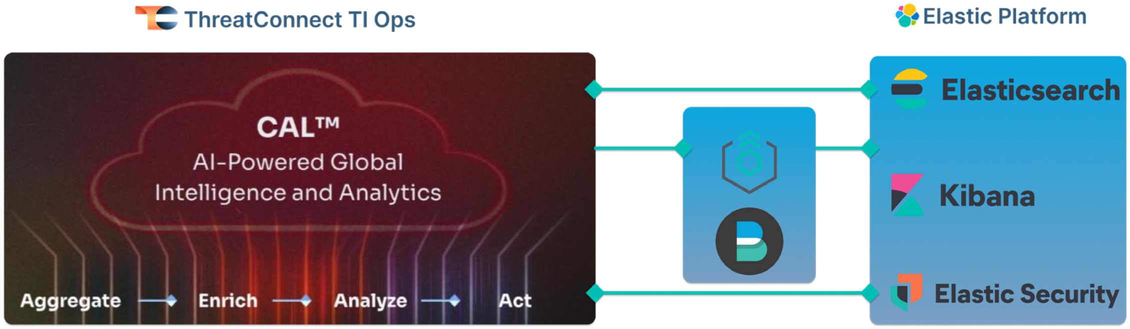
Get Results with ThreatConnect + Elastic

A native integration in Elastic along with Job and Service Apps in ThreatConnect allows the platforms to be connected in minutes. The integration enhances a range of use cases, like:

Threat detection, monitoring, and analysis - Leverage native threat scoring in the ThreatConnect Platform to optimize the Indicators sent to the Elastic Platform to improve threat detection and prioritization, while minimizing false positives.

Incident response - Reduce MTTD and MTTR through faster, more precise alert triage in Elastic leveraging relevant intel and rich context provided via ThreatConnect.

Threat hunting - Make threat hunting more robust and effective by leveraging relevant intel to define your hypotheses and starting points for hunts. Threat Graph in the ThreatConnect Platform augments the Elastic Platform for digging into threat intel and uncovering new relationships and threat actor insights.



How to Get Started

ThreatConnect and Elastic customers can install the integration directly from Elastic and in the TI Ops Platform App Catalog under 'Elastic Security.' If you're interested in learning more, please visit our Marketplace, or reach out to speak with a ThreatConnect expert at https://threatconnect.com/request-a-demo/ or sales@threatconnect.com.

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. More than 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

threatconnect.com | +1-703-229-4240 | sales@threatconnect.com

ThreatConnect.