ThreatConnect™

ThreatConnect's CAL (Collective Analytics Layer)

Enhance Intelligence With Global Context

Your Intel Just Got Exponentially Better

ThreatConnect's CAL™ (Collective Analytics Layer) provides a way to learn how many times potential threats were identified across all participating Platform instances. CAL anonymously leverages the thousands of analysts worldwide who use ThreatConnect.

By distilling billions of data points, this innovative architecture offers immediate insight into how widespread and relevant a threat is, providing global context that has never before been available.

Determine Indicator Reputation

CAL sheds light on the disposition of hundreds of billions of indicators using a variety of open source and proprietary data sources and analytics. This disposition can be combined with the in-platform scoring with ThreatConnect's ThreatAssess, which captures the threat criticality of an IOC (indicator of compromise) on a single numeric scale and helps to prioritize and triage decision-making.

Apply Classifiers to Indicators

CAL applies Classifiers to indicators to empower analysts and existing technology investments alike. This enables faster decision-making by identifying things like an IOC's infrastructure provider, what services it's used for, and how it's performing across all participating ThreatConnect users.

Prioritize What Matters

Leverage CAL's analytics to remove junk IOC's from your system. Don't clog up ThreatConnect, your SIEM (Security Information and Event Manager), or your workflow with indicators we know aren't worth your time. Using CAL for Indicator Status means less time wasted on false positives, less alert fatigue, and more time spent on important things. CAL can make status recommendations on hundreds of billions of indicators already, and that number grows daily.

Evaluate Data Feed Performance

CAL's analytics identify which feeds in a vast sea of Open Source intelligence are more likely to contribute to the "garbage in/garbage out" problem we all face. CAL's Report Cards allow you to track how feeds are performing in the real world. Learn which ones are providing unique IOC's, which ones are the first to report IOC's, and which ones are the most applicable to your organization's goals.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

Data sharing can be a sensitive subject, and we're sure you have questions. We've got answers.

What happens when I participate in CAL?

- When you view an indicator's details or search for it, CAL records the query and returns rich contextual information. This includes details such as which hosting company owns a malicious IP address, what Classifiers the CAL analytics applied to an indicator, and how it's performed across the ThreatConnect user base over time.
- As part of the ThreatAssess scoring system, your ThreatConnect instance will regularly query CAL with a bundle of indicators from your instance to get more information. CAL will respond back with the respective indicators' scores and status recommendations.
- When you build Playbooks, you can leverage CAL's insights by querying CAL directly for indicator enrichment. This allows you to build workflows around context and enrichments that CAL has already done for you.
- If you wish to withhold some indicators from CAL, you may mark them as private so they never leave your instance. The downside is that these indicators will not receive any enrichment from CAL.

How is my participation anonymized?

- CAL does not track individual user or Organization data, and will only track aggregated indicator metadata from your instance: the indicators themselves, false positive and observation counts, indicator status, and the query.
- CAL immediately drops any identifying information, and submitted data from all instances is combined to power analytics across the aggregated dataset. This aggregated dataset is what is used for analytics. For example, CAL may look at the total number of reported Observations across all participating instances to modify an indicator's reputation score.
- Only the aggregated insights, and the analytics they drive, are accessible to other users. For example, you may see that an indicator has 1,000 reported Observations across the aggregate dataset of all participating instances. You would not see how many came from whose instance.

What CAL doesn't do

- CAL does not track who you are or what you've looked at. No identifying information is collected, and your ThreatConnect instance identifier is dropped after authentication. All metadata is aggregated to protect privacy while still providing value.
- CAL does not collect content surrounding indicators. It does not collect tags, comments, associations, or Group objects (e.g. Incidents and Threats).
- CAL does not give users access to data they wouldn't know to ask for — it only responds about the indicators it's been asked about.

Request A Demo

Call **1.800.965.2708** or visit **threatconnect.com/request-a-demo**

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