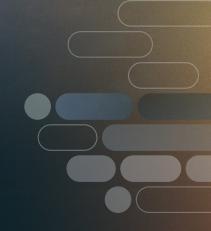# ThreatConnect CAL™

(Collective Analytics Layer)
Enhance Intelligence With Global Context

Maximize Insights About Global Threats

ThreatConnect's CAL™ provides a way to learn how widespread and relevant a threat is by anonymously leveraging the billions of data points from the many thousands of analysts that use the ThreatConnect Platform.

Maximize Efficiency with Indicator Reputation

CAL combines data about the disposition of billions of indicators gathered from various open source, proprietary data sources, and analytics, with the in-platform scoring of the ThreatConnect Platform's ThreatAssess to present the criticality of an IOC on a single numeric scale.

Faster Decisions Using Classifiers

CAL applies Classifiers to indicators to enable the security team to maximize efficiency with faster decision-making.

Prioritize IOCs to Reduce Alert Fatigue

CAL's analytics help you maximize efficiency by removing low or no priority IOC's from your system.

Compare Feeds to Optimize Performance

CAL's Report Cards allow you to understand how your intelligence source feeds are performing.

CAL Analytics Leverage ATL Data Sources

The CAL Automated Threat Library (ATL), an evolution of the popular Technical Blogs and Reports (TBR) Source, now can leverage the ThreatConnect Data model. Native integration includes access to Mitre ATT&CK, the vulnerabilities from the National Vulnerability Database (NVD), and much more. Attacker techniques can now be identified through CAL's quick analysis of English sentence structure using trained and turnkey natural language processing. ATL uses CAL's insights to normalize Source data, improve ThreatAssess mappings and provide improved inclusion of CAL's Indicator Status.

Move From Reactive to Proactive

CAL Feeds can identify new and important areas of insight for your team that merit investigation. CAL combines large datasets and analytics to discover actionable and timely insights for teams of all sizes and maturity levels.

Find out more about how CAL can help here.

THE CHOICE OF THE GLOBAL 2000

Nearly 200 enterprises worldwide protect their organizations with ThreatConnect

ORACLE

IBM   **SONY**

workday.   **RBC**

GENERAL DYNAMICS
Information Technology

Data Sharing and Protection

Participation – How Does it Work?

CAL records the query and returns rich contextual information when users view an indicator's details or search for it. This includes details such as who 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.

The ThreatConnect instance will regularly query CAL with a bundle of indicators from your organization's instance to get more information as part of the ThreatAssess scoring system. CAL will then provide the respective indicators' scores and status recommendations.

Organizations can maximize efficiency and benefit from CAL's insights by querying CAL directly for indicator enrichment. This can help build out Playbooks and allows organizations to build workflows around context and data enrichment that CAL has already completed.

Indicators may be withheld from CAL by marking these indicators as private so they will not leave your organization's instance. In this case, these indicators will not receive any enrichment from CAL.

Protecting Private Data

CAL does not track individual user or organization data. CAL will only track aggregated indicator metadata from your organization's instance which includes the indicators themselves, false positive and observation counts, indicator status, and the query.

CAL immediately drops any identifying information, as submitted data from all instances is combined to power analytics across the aggregated dataset. This aggregated dataset 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 the sources of the Observations

Restrictions and Limitations

- 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 data privacy.

- CAL does not collect content surrounding indicators. It does not collect tags, comments, associations, or Group objects (e.g. Incidents and Threats).

- CAL only provides information about indicators for which it has been queried.

● 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.