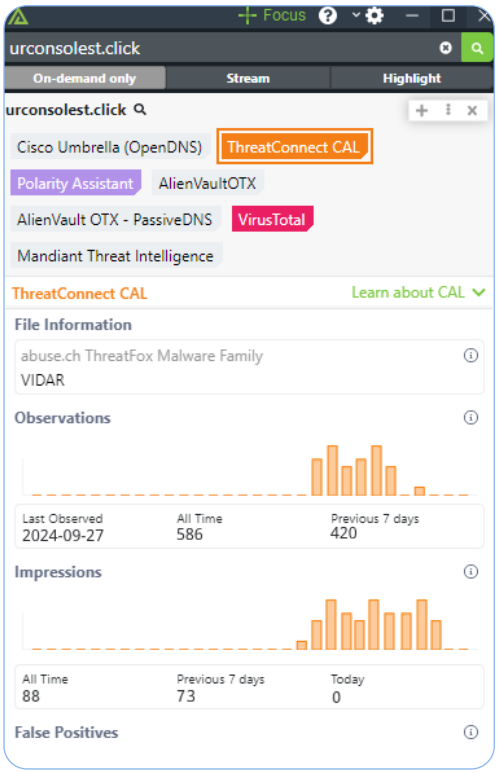
POLARITY
BY ThreatConnect.

ThreatConnect CAL Integration – Now Included with Polarity

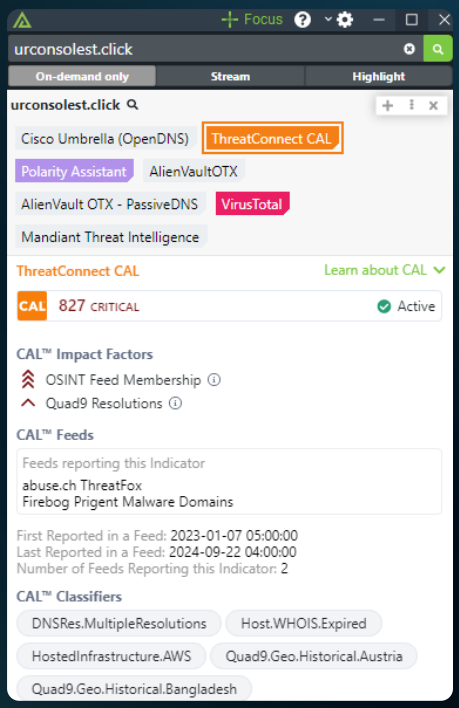
Ground Truth Insights. Hundreds of Intel Sources. Unavailable Anywhere Else.

Global, Ground-Truth Insights on Threats in the Wild

None of us is as smart as all of us. The insights an analyst gets at another company or organization can give advance warning of threats targeting you. CAL captures billions of these insights, anonymizes them, and gives you the benefit of experience gained by tens of thousands of analysts.



This indicator was recently reported in real SIEMs across the globe, and other analysts have looked at it in the past week. No one has identified it as a false positive. It's probably worthy of attention!



Aggregated insights from hundreds of intelligence sources distilled to an actionable score along with other decision-driving information.

Timely Insights During Decision and Action

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

ThreatConnect.

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

sales@threatconnect.com
+1.703.229.4240

Prioritize IoCs and Reduce Alert Fatigue with Indicator Reputation

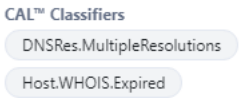
CAL combines data about the disposition of billions of indicators gathered from various open and proprietary data sources and analytics. This is distilled to a single score to clearly present the criticality of an IOC. CAL's analytics also help you maximize efficiency by identifying low- or no-priority IOCs.

CAL has identified this indicator as Active and a Critical threat.

Faster Decisions Using Machine Learning

CAL uses machine learning and other techniques to automatically classify every indicator that it collects, including insights like:

- **Suspicious Host Classification:** Identifies hosts that have resolved to known malicious IPs or have shown suspicious activity patterns.
- **Dynamic DNS and Tor Exit Node Detection:** Flags indicators related to anonymization services, like dynamic DNS and Tor nodes, that are often associated with malicious behaviors.
- **Cloud Infrastructure Detection:** Distinguishes indicators tied to cloud service providers like AWS, Google Cloud, or Azure to identify infrastructure that might be used for hosting attacks.
- **Malicious IP Resolution:** Tracks indicators resolving to IP addresses known for hosting malware or phishing content.
- **Frequency of Resolution:** Detects hosts that rapidly resolve to different IP addresses, which can be an indicator of malicious command and control (C2) infrastructures.
- **Suspected DGA:** The host may have been generated by a domain generation algorithm (DGA), a tactic frequently employed by malicious actors to create multiple domains to leverage during cyber attacks.



Automatic classifiers can inform whether to investigate, escalate, act, or deprioritize.

CAL — Your Favorite Threat Intel Sources in One

CAL compiles data from hundreds of blogs, intel feeds, government bulletins, and other sources into a single dataset. All of these indicators are made machine-readable and available to analysts through Polarity.

Intelligence not Available Anywhere Else

Multisourcing intelligence is valuable, but there can be a lot of overlap across intelligence sources, so finding unique insights can mean the difference between stopping a threat and having it lost in the noise. Because CAL's data includes a mix of proprietary and rare intelligence sources, you can almost guarantee that you'll find something rare and valuable.

Reach out to learn how CAL and Polarity by ThreatConnect can make you and your team more effective, decisive, and collaborative.

+1 (800) 965.2708 - or - threatconnect.com/request-a-demo

ThreatConnect.

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. Over 250 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets. **Learn more at** www.threatconnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708