

ThreatConnect Analytics Team

Bringing More Data, Better Context, and Actionable Insights to Decision Making

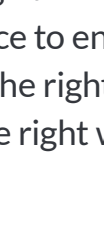
Data has a lot to offer, but it takes a specific set of skills and expertise to understand it, package it, and apply the findings to decision-making. Data, along with Information and Knowledge, make up the atomic building blocks of intelligence. When adequately curated, analyzed, and understood, past data becomes intelligence, and that intelligence allows us to be proactive. We all recognize data as an important ingredient in our security buzzword gumbo, but you need analytics to turn it into a proper meal for your organization to really feast upon.

At ThreatConnect, we prioritize figuring out how to harness the power of data science and analytics. This allows us to build solutions that focus on applying that insight to analysis, investigation, and making more confident decisions across the entire security team (analytics is not just for threat intel analysts). The ThreatConnect Analytics Team collects anonymized telemetry from participating users across the ThreatConnect ecosystem and uses it to create solutions that provide actionable insights for your organization. Access this information directly from the ThreatConnect User Interface or deliver across your security enterprise with our seamless integrations.



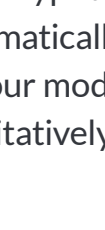
Dedicated Team with the Experience Needed to Build Unique Solutions

With roles explicitly dedicated to identifying and building Analytics solutions, our team is committed to finding ways to replicate analyst expertise scientifically to scale alongside your data.



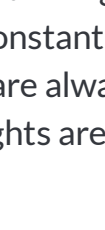
Product Managers

On the whiteboard, our Product Managers leverage their security experience to ensure we're tackling the right problems the right way.



Data Scientists

On the blackboard, our Data Science team ensures that our hypotheses are mathematically tested and our models are quantitatively sound.



Engineers

On the keyboard, our Engineering team builds and maintains the engine so that data is constantly flowing, analytics are always running, and insights are available.

With ThreatConnect's Analytics Solutions, stop scrambling for additional context and information and spend time focusing on how to protect your organization better.


Leverage the Insights of 1000's of Analysts and Billions of Indicators with ThreatConnect

ThreatConnect's CAL (Collective Analytics Layer) is an engine which identifies how many times participating ThreatConnect Platform instances observe potential threats. CAL anonymously leverages the thousands of analysts worldwide and offers immediate insight into how widespread and relevant a threat is - providing global context that has never before been available.

Leverage CAL insights to remove junk IOC's from your system. Don't clog up ThreatConnect, your SIEM, or your workflow with indicators we know aren't worth your time. Using CAL for Indicator Status occurs automatically, this means less time wasted on false positives, less alert fatigue, and more time spent on essential things. CAL can make status recommendations on over a billion indicators already, and that number grows daily.

Over a 30 day timeframe, ThreatConnect saved an average of **38 HOURS** of analysts' time by providing automated enrichments and steering them clear of false positives. Analysts spend an average of 7 minutes per indicator when doing their investigation -- wouldn't you rather spend them on the *right* indicator?

Additionally, CAL applies a standard vocabulary of over 100 labels, known as Classifiers, to help you decide what to do next. Classifiers enable faster decision-making by identifying things like an IOC's infrastructure provider, what services they are responsible for, and how it's performing across all participating ThreatConnect users.

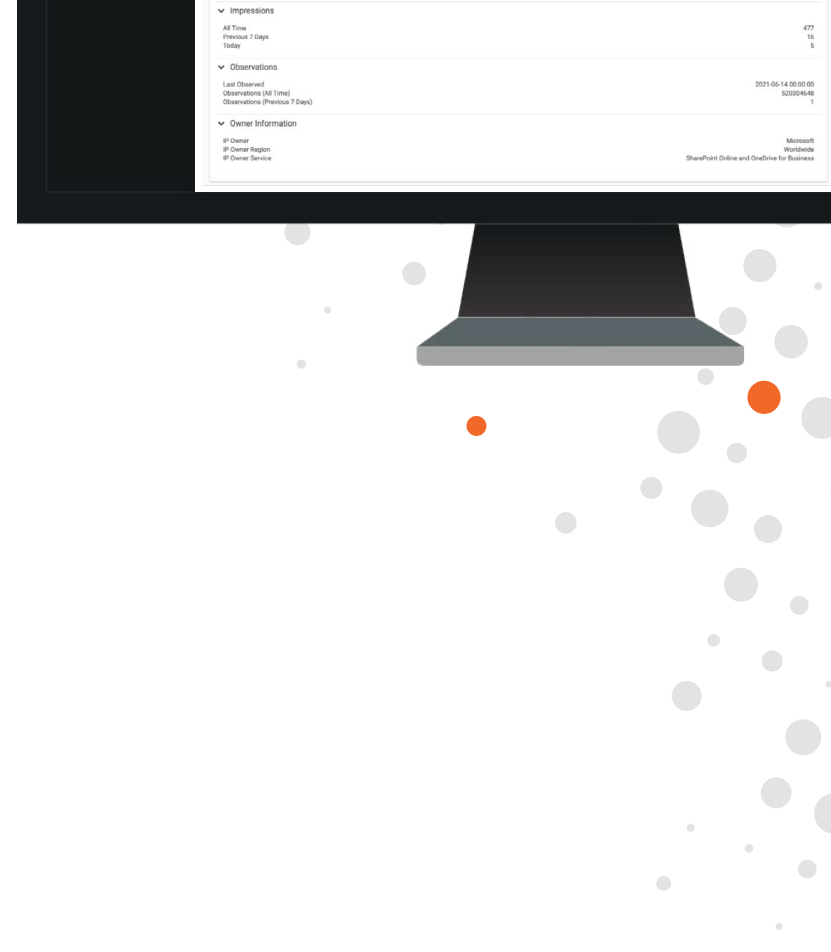


Combine Multiple Datapoints Into a Single, Actionable Score with ThreatAssess

ThreatAssess captures and conveys indicator reputation, providing a baseline risk assessment of an indicator of compromise using a standardized scale. Distill down multiple data points to a single, actionable score based on an indicator's weighted, configurable consensus of indicator reputation across all sources, false-positive votes, and recent activity from sensors in your environment.

ThreatAssess provides a holistic view of an indicator using scoring from available threat intelligence feeds and your environment and through insights provided by CAL. Giving users a global perspective and more contextual scoring than what's traditionally available in the market, ThreatAssess leads you to a score backed by a robust data set that you can feel confident with using.

When it comes to configuring how the score is created, depending on the maturity and desires of your security team, pull the levers and define your consensus or rely on CAL to build it for you. ThreatConnect customers are able to fine tune their ThreatAssess score over time as they learn more about adversaries and what Intelligence matters most to them.



Indicator Reputation Isn't One Size Fits All

Balancing Local and Global Insights for Increased Relevancy

Indicator reputation looks very different across different organizations. A scary indicator for you may not matter for another organization, and here's why: You've got to consider what pieces of the puzzle exist in your local environment.

Your organization's geography, technologies, and work product all dictate priorities for you and your adversary. These inputs provide an answer to relevance. However, there's a second image that comes into focus when you assemble your pieces of the puzzle with peers across the security industry.

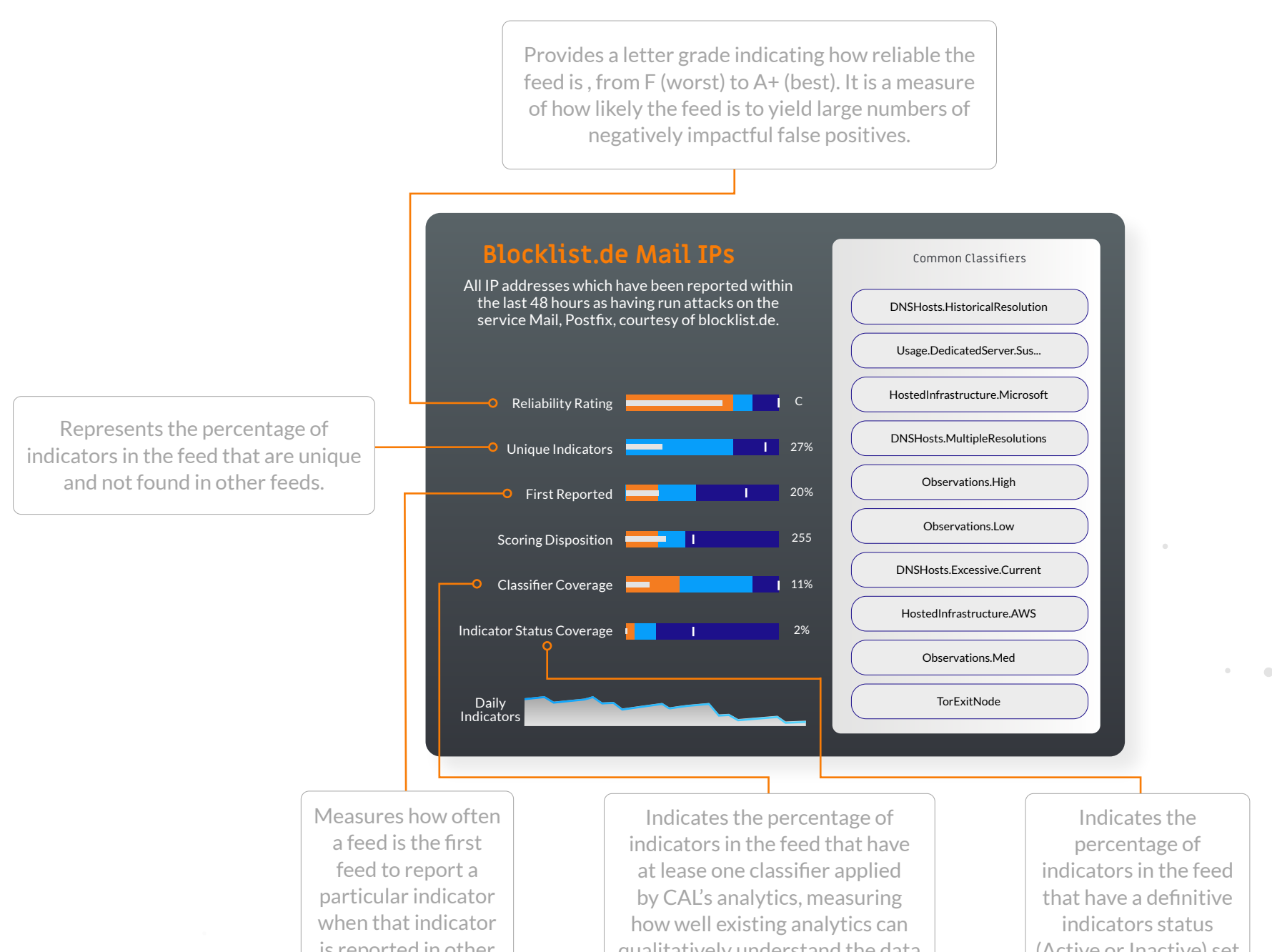
- What are other organizations in your industry seeing?
- What things are "universally" true?
- What things are helpful in the absence of local data?

ThreatConnect's analytical models support balancing all local and global data sources to supply you with a ThreatAssess score relevant to your organization. Since you and your adversary are always changing, your approach to indicator scoring needs to as well. When you're ready, you can tune ThreatAssess to your organization's needs, pulling every lever and tweaking every weight to prioritize the data sources and decision points that matter most.



Understand the Quality of Intelligence Sources with Intel Report Cards

Analysts often find themselves asking a simple question: "Who's telling me this, and how much do I care?" Intel Report Cards seeks to tackle this problem on a few fronts, giving you insight into how specific feeds perform across the ThreatConnect ecosystem. For example, painting a picture of various intelligence feeds can help guide the decision of which feeds to enable in your instance and how much credibility a particular IOC may have based on what you know about its source



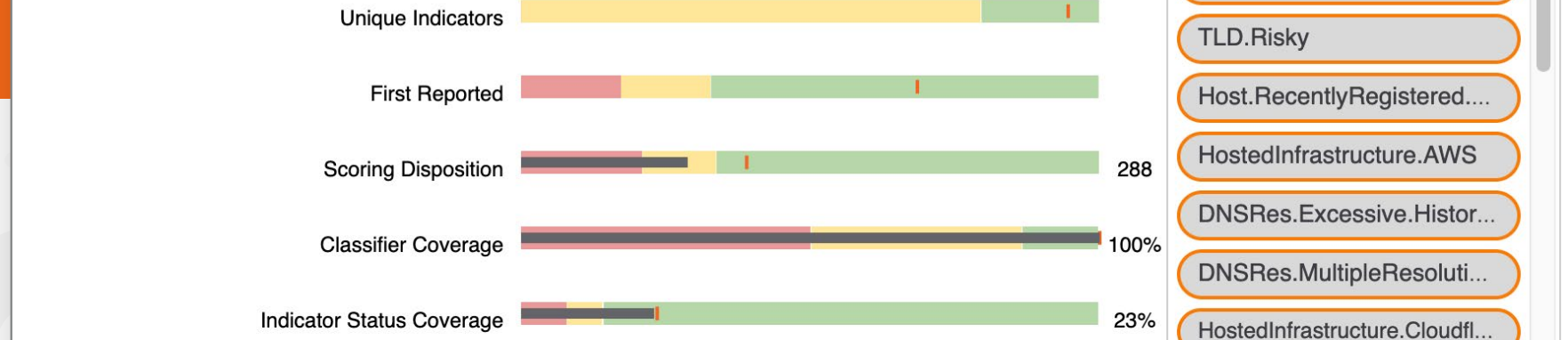
Proactively Discover Pockets of New Suspicious and Interesting Intelligence with CAL Feeds

With CAL Feeds, the massive dataset and analytics already found within CAL are paired with our in-house expertise to identify pockets of intelligence that are suspicious and potentially worth looking deeper into. Presenting on average 98% unique indicators, these intelligence feeds provide fertile hunting grounds for teams of all sizes and maturity levels.

A sample of Available CAL Feeds Include:

- ✓ CAL Suspicious New Resolution IPs
- ✓ CAL Suspicious Newly Registered Domains (NRDs)
- ✓ CAL Suspicious Nameservers
- ✓ CAL Suspected Ranking Manipulators
- ✓ Suspicious NRDs Impersonating Legitimate Brands, broken down by industry:
 - Energy
 - Communications
 - Finance
 - Manufacturing
 - Retail
 - Healthcare

And there's more being developed all the time!



About ThreatConnect®

ThreatConnect, Inc. provides cybersecurity software that reduces complexity for everyone, makes decision-making easy by turning intelligence into action, and integrates built for the entire team (security leadership, risk, security operations, threat intelligence, and incident response). ThreatConnect's decision and operational support platform is the only solution available today with cyber risk quantification, intelligence, automation, analytics, and workflows in one. To learn more about our Cyber Risk Quantification, Threat Intelligence Platform (TIP) or Security Orchestration, Automation, and Response (SOAR) solutions, visit www.ThreatConnect.com.

