ThreatConnect™

Gain Immediate Access to Intelligence with ThreatConnect

Along with a subscription to ThreatConnect, users receive access to a variety of pre-populated intelligence sources. Those sources include both open source intelligence that has been collected from publicly available sources and packaged for you in a digestible and easy-to-use format, as well as Premium Intelligence curated by the ThreatConnect Analytics team.

ThreatConnect Premium Intelligence

ThreatConnect Premium Intelligence is so much more than a typical threat feed that delivers meaningless indicators with no context. The ThreatConnect Analytics Team creates actionable intelligence that provides real insight for your organization, building out additional information about a threat from adversary activity, country of origin, phase of intrusion, and more. With ThreatConnect Premium Intelligence, you can finally stop scrambling for additional information and spend time focusing on how to best protect your organization.

ThreatConnect CALFs (Collective Analytics Layer Feeds)

CAL Suspicious Newly Registered Domains (NRDs): NRD's aren't inherently malicious – new domains get registered every day, but a subset of those are at least suspicious or interesting. By virtue of being new, they eliminate one of the big questions we always have to ask with intel: "how old is it?" We've identified NRDs that we think are leveraging suspicious infrastructure, which narrows down the pool. These domains can be a rich hunting ground for reusing infrastructure, registration techniques, and more.

CAL Suspected Domain Generation Algorithms (DGAs) NRDs: Consists of a list of recently registered DGAs, as determined by our machine learning model. As CAL aggregates hundreds of thousands of domains, they're run through our neural network with the goal of identifying domains that are "suspiciously junky".

CAL COVID-19 Themed NRDs: NRDs that contain COVID-19 themed keywords and variants thereof that have a particular footprint in terms of DNS resolutions. It's important to remember that there are a lot of legitimate efforts among these NRDs: there is an information need and many governments and organizations are mobilizing to get information to the public. To find the signal in the noise, we're using CAL's analytics to identify resolution patterns that we think make something look interesting.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

Industry-Specific CAL Feed NRDs: Inspects Suspicious NRDs we've identified, to look for variations of popular and legitimate brand names. We've separated these CALFs by industry type to help you keep an eye on the things that are relevant to you and your peers. The following are currently available:

- CAL Energy-themed NRDs
- CAL Communication-themed NRDs
- CAL Finance-themed NRDs
- CAL Manufacturing-themed NRDs
- CAL Retail-themed NRDs

CAL Suspected Ranking Manipulators: When we started to explore NRDs, we noticed an interesting trend. There are a number of really new domains that seem to be highly ranked in some of the industry's "Top 1 Million Websites" list. These domains may not be directly targeted against you, but if you're a research geek like us you're probably just as curious. These domains have a "weirdness" to them that we're hoping to sink our teeth into. That weirdness smacks of nefarious activity that we don't know much about and may not want to leave unchecked.

CAL Suspicious Nameservers: We've paired CAL's dataset with analysis from our Analytics Team to figure out a way to identify suspicious nameservers at scale. Nameserver usage (and reusage) can help us identify shady neighborhoods on the internet, and thus adds an important data point to any hosts that use them.

CAL Suspicious New Resolution IPs: We are ingesting nearly 100 open source feeds into CAL to improve our understanding of intel. So when we see something new, it's at least interesting. This feed of IPs are the DNS resolutions from identified malicious hosts that aren't being reported anywhere else. Here's your chance to shift to the proactive – don't wait for an analyst to ingest, triage, document, and share these IPs in their "spare time." Let our code do it for you, as these malicious hosts come online you'll have the first peek at their underlying infrastructure.

External OSINT

The ThreatConnect Analytics team has taken some of the most reliable and diverse OSINT available and packaged it into easy-to-digest and operationalize intelligence sources, that can be 'turned on' as soon as you become a ThreatConnect customer, enabling instant sources of content for your analysis and investigation efforts.

OSINT Feeds

The following is a list of current OSINT available in our ThreatConnect TIP & SOAR solutions:

- abuse.ch Feodo Tracker
- abuse.ch URLHaus
- Bambenek
- Blocklist.de Apache IPs
- Blocklist.de Bot IPs
- Blocklist.de Bruteforce IPs
- Blocklist.de FTP IPs
- Blocklist.de IMAP IPs
- Blocklist.de IRCbot IPs
- Blocklist.de Mail IPs
- Blocklist.de SIP IPs
- Blocklist.de SSH IPs
- Blocklist.de Strong IPs
- BotScout Bot List
- Botvrij Domains
- Botvrij IPs
- BruteForceBlocker Blocklist
- Cert-pa.it Latest Malware Analysis
- CINS Army IP List
- Cybercrime Tracker
- dan.me Tor Exit Nodes
- Disconnect.me Malvertising
- DShield.org Recommended Blocklist CIDRs
- Firebog Airelle Hrsk Domains
- Firebog Prigent Malware Domains
- Firebog Prigent Phishing Domains
- Firebog Shalla Malware Domains
- GreenSnow Blocklist
- Haley SSH Bruteforce IPs
- hpHosts Latest Additions
- Hybrid Analysis
- Maldun Malware Analysis
- MalShare Daily Malware List
- MalwareConfig
- OpenPhish
- PhishTank
- Rutgers Attacker IPs
- StopForumSpam Toxic CIDRs
- VXVault

Technical Blogs and Reports

The Technical Blogs and Reports Source is a curated collection of over 100 open-source information security blogs and reports aggregated in ThreatConnect on a daily basis. Each blog is automatically parsed for indicators of compromise, CVE numbers, and detection rules like YARA and Snort – saving you countless hours of manual data aggregation and import efforts.

ThreatConnect

ThreatConnect, Inc. provides cybersecurity software that reduces complexity for everyone, makes decision-making easy by turning intelligence into action, and integrates processes and technologies to continually strengthen defenses and drive down risk. Designed by analysts but 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.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708