INTSIGHTS
Threat Intelligence Realized.

Threat Intelligence Management

Ingest, Correlate, Enrich, Investigate and Prioritize IOCs

Benefits

- Prioritizes IOC data to minimize SIEM data model costs.
- Adds context and clarity by automatically enriching IOCs with threat intelligence sources.
- Delivers efficient way to extract strategic value from commoditized threat intelligence data feeds.
- Enables teams to focus on critical IOCs and avoid 'false positive fatigue.'

Key Features

- Intelligent aggregation and normalization of threat feeds.
- Enrichment of IOCs with automated appending of relevant data from inside and outside the organization.
- Automated assessment and scoring of IOCs based on relevance and severity of risk.
- Dashboards with anytime, anywhere access enable teams to triage IOCs rapidly for focused, decisive responses.

Indicators of compromise (IOCs) are valuable because they can tip off security teams to coming cyberattacks, active malware infections and network breaches. The problem is that these valuable 'droplets' are part of a torrent of tactical threat intelligence data that floods security teams every day.

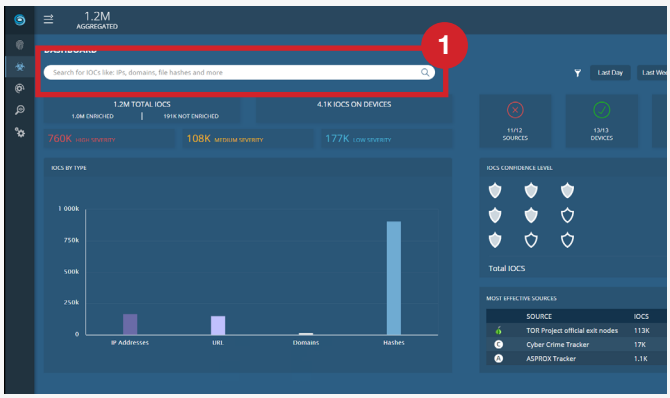
The volume and velocity of this data make it virtually impossible for threat hunters to compare it against logs to find matches to known threat sources. There's just too much data.

Even when valid matches are found, by the time teams send alerts, attackers have changed things up, and the once-dangerous threat isn't dangerous any longer. It's just one more among millions of false positives.

There is a more effective way to cull the most dangerous elements from generic threat feeds and illuminate them with contextual data for better understanding. There is also a faster way to operationalize that enhanced threat intelligence in rapid responses that thwart attacks.

These threat intelligence platform capabilities are built into **Insights' Enterprise Threat Intelligence & Mitigation Platform**.

1. Quickly and easily search for IOCs such as IPs, domains, file hashes and more to inform threat hunting and direct incident response activities.



Key Threat Intelligence Platform Capabilities

Integrated Threat Management & Incident Response

Investigate prioritized threats in real time, monitor suspicious IOCs based on relevance, initiate and track incident response workflows, prioritize and manage investigations, and minimize SIEM data model costs.

Threat Feed Aggregation & Correlation

Dynamically configure and ingest community, agency, commercial, open source and industry threat feeds and extract IOCs for analysis in a single dashboard.

Digital Footprint IOC Analysis

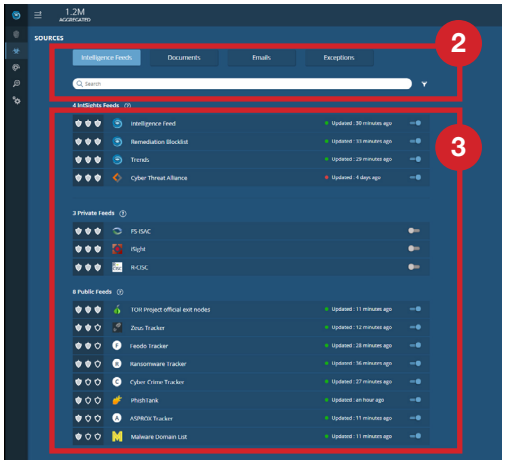
Automated and continuous IOC evaluation and scoring based on context, severity and relevance gained via tailored intelligence alerts specific to an organizations' digital footprint.

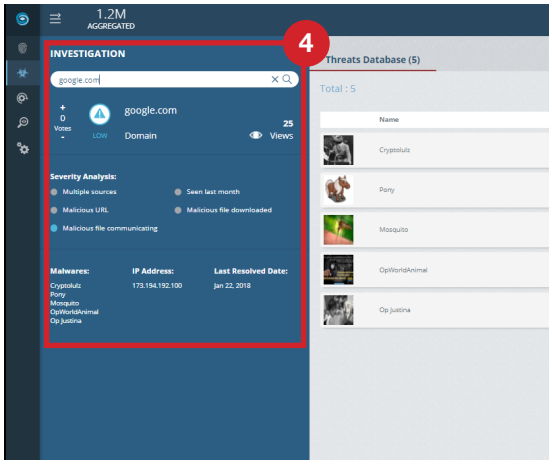
IOCs are usually known, problematic entities created by threat actors and cybercriminals. They include things such as IP addresses, URLs, domains, and file hashes. Their presence in a network can be telltale signs of impending or active cyberattacks, malware infections, or other breach activities.

As small data points within massive inflows of threat intelligence data, they are very difficult to pinpoint using manual processes. Without the additional context needed to 'connect the dots,' it is easy to overlook critical IOCs or find them too late – after the damage has been done.

That was yesterday. Today, threat hunters and SOC teams have a more efficient and effective way to manage IOCs to maximize protection for their organizations. IntSights' Enterprise Threat Intelligence & Mitigation Platform aggregates and normalizes threat feeds, enriches IOCs and prioritizes alerts to accelerate triage, streamline incident coordination, and speed response times.

2. Choose the intelligence source you need across feeds, documents and emails
3. Organize sources by type, quality and severity according to your risk profile and security strategy.
4. Investigate threats for real-time severity analysis, corresponding IP address information, related malware, last resolution date, and associated threat actors, etc.





> *We understand the need to be less reactive and more proactive, and IntSights helps our team meet that challenge. The IntSights Platform helps us to understand the threats and things that are happening outside our organization so they don't lead to events and issues inside.*
>
> ***Manager, IT Security & Governance | Leading Avionics Company***

Contact Us

To learn more about how tailored threat intelligence and the rest of ***IntSights' Enterprise Threat Intelligence & Mitigation Platform*** can give you the focused, early warnings required to protect your organization and it's brand, resources and people from cyberattacks, call us today at +1 (800) 532-4671, email us at **info@insights.com**, or visit us on the web at **www.intsights.com**.

Request a Demo

Contact us today to schedule a personalized, 30-minute demonstration of the IntSights Platform.

CLICK HERE

About IntSights

IntSights is redefining cybersecurity with the industry's first and only enterprise threat intelligence and mitigation platform that transforms tailored threat intelligence into automated security operations. Our groundbreaking data-mining algorithms and unique cyber reconnaissance capabilities continuously monitor an enterprise's external digital profile across the surface, deep and dark web, categorize and analyze tens of thousands of threats, and automate the risk remediation lifecycle — streamlining workflows, maximizing resources and securing business operations. This has made IntSights' one of the fastest growing cybersecurity companies in the world. IntSights has offices in Boston, Tel Aviv, Amsterdam, New York and Dallas and is backed by Glilot Capital Partners, Blumberg Capital, Blackstone and Wipro Ventures.