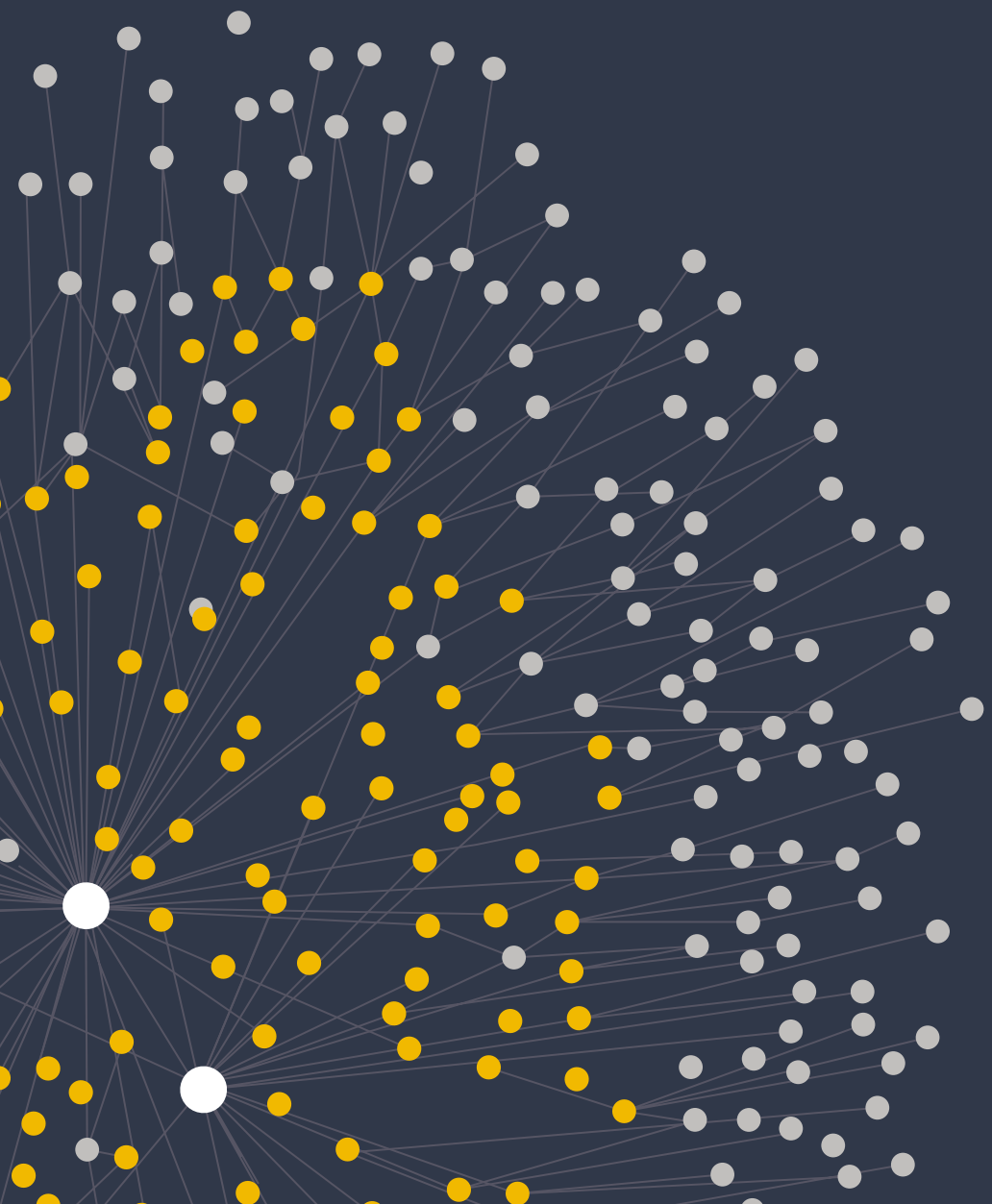
TOP 13 THREAT INTELLIGENCE PROVIDERS FOR SOC TEAMS



MALTEGO

Maltego Recommends:
Threat Intel for SOC Teams

A SOC team is tasked with continuously monitoring its environment in order to detect, analyze, and respond to cybersecurity incidents, and ultimately improve the security posture of the organization

However, to effectively monitor their environment, it isn't enough for SOC teams to deploy security systems and tools that will alert them to an indiscriminate number of events. They need to know what threat actors are doing, what their activity may look like, and how to find traces of said activity across their infrastructure.

Usually, the sort of traces that are left behind by threat actors and picked up by the monitoring systems will be either observables or even indicators of compromise (IoC)—IP addresses, host and domain names, email address, filename and file hashes—which on their own and out of context won't be enough to conduct an in-depth investigation.

For a proper analysis that can lead to attribution as well as to effective countermeasures against similar attacks being built, SOC analysts need to enrich and contextualize the traces found in their internal systems.

This is where an often-confusing concept comes in: Threat intelligence. To better understand it, we will walk through the most popular elements related to the subject matter.

Threat Intelligence: Sources, Feeds, Platforms, and Providers

Threat intelligence is actionable and timely knowledge that is rooted in data. It provides analysts with the necessary context to understand threat actor's motivations, methods, tools, and infrastructure, thus helping them prevent or mitigate attacks.

Practically speaking, threat intelligence relevant to an organization is generated when combining the traces found in the organization's internal telemetry—such as firewall and DNS logs—with threat data and information, be it via sources, feeds, platforms or providers.

Sources and Feeds

Open source intelligence (OSINT) and network telemetry constitute examples of threat intelligence sources. Threat intelligence feeds are non-prioritized streams of data that usually consist of non-contextualized IoCs or digital artifacts and focus on specific areas or data types such as suspicious domains, known malware hashes, and IP addresses associated with malicious activity, amongst others.

While free feeds are usually gathered from open sources, paid threat feeds may provide curated data from closed sources such as forums or constitute an aggregation of open-source feeds.

Platforms and Providers

A threat intelligence platform (TIP) is a software used to organize several feeds—free and paid—into a single stream. Lastly, a threat intelligence provider is a vendor that produces threat intelligence reports, for which they sometimes use a mix of human and automated analysis. The provider then offers the intelligence via premium data feeds, as a report, or as part of a software product. The human generated part may include TTP's and attribution to a known Actor. The automated part is providing lists of observables in machine readable format.

A Dilemma: Incorporating Threat Intel into the SOC Team

It's easy to see how one may stumble around in search for the right product to incorporate into their SOC team just by looking at the variety of options out there. With that in mind, SOC teams should first gain a comprehensive understanding of the following:

1. Their network infrastructure
2. The type of risks unique to their industry
3. Where their security posture stands based on their current resources and capabilities to manage defensive and reactive activities
4. Their available budget
5. Resources they can dedicate to the project

However, even with the previous elements established, it is often difficult for SOC teams to choose the threat intelligence solution best suited to them, and to determine how to properly take advantage of the data it provides without further burdening the analysts. This is especially true for smaller, less mature teams that may not have the necessary tools, processes, or resources to help them prioritize data.

Maltego's Top Recommendations on Threat Intel for Small SOC Teams

According to the 2021 SANS Cyber Threat Intelligence CTI survey published in January 2021, the types of threat intelligence that are most helpful to SOC team operations are:

- Information about vulnerabilities being targeted by attackers
- Detailed information about malware being used in attacks
- Specific IoCs to plug into IT and security infrastructure to block or find attacks
- Broad information about attacker trends
- Threat behaviors and tactics, techniques, and procedures (TTPs) of the adversary (how they work)

Based on these criteria, we provide a list of high-quality threat intel options for small SOC teams that

have proven to be amongst our end-users' favorites and are suitable for all budget sizes. The list is sorted in alphabetical order and doesn't indicate any ranking or preference.

AlienVault OTX (Open Threat Exchange)

Crowdsourced Intelligence | Threat Pulses

The AlienVault OTX is an open threat intelligence community providing access to a global body of over 100 thousand threat researchers and security professionals where over 19 million threat indicators are contributed every day. OTX's "open community" concept makes it possible for analysts to research and collaborate with other subscribers to investigate threats directly on the platform.

Its feed provides "pulses" or summaries of threats with a view into the software they are targeting and the related indicators of compromise (IoCs) that can be used to detect the threat. The IoCs include IP addresses, domain names, file hashes, and CVE numbers amongst others. Maltego will be releasing an integration with AlienVault's OTX DirectConnect API in Spring 2021.

CrowdStrike Falcon X

All Team Sizes | Intel Reports | YARA/SNORT Rules

The CrowdStrike Falcon X threat intel solution is designed for teams of all sizes that struggle to respond to cybersecurity alerts and lack the time or expertise to tackle emerging threats. Falcon X provides actionable and customized intelligence in the form of IoCs, intelligence reports from the global CrowdStrike Intelligence team, and YARA/SNORT rules created and validated by CrowdStrike experts. All Falcon X options integrate with the Falcon endpoint platform to perform investigations, speed up response times, and enable teams to be more proactive.

Currently, Maltego offers **CrowdStrike Intel Transforms** for the Falcon Intelligence API, enabling customers to benefit from a rich feed of information that will allow them to perform attribution and obtain additional data on indicators of compromise, and see correlation between adversaries, indicators, malware families, and campaigns.

DomainTools Iris

Domain Intel | Passive DNS | Risk Scoring

Iris is DomainTools' threat intelligence and investigation platform that combines domain intelligence and risk scoring with passive DNS data from Farsight Security and other prominent providers that help teams quickly and efficiently investigate potential cybercriminal activities.

With the **Maltego Transforms for DomainTools Iris**, investigators can perform infrastructure risk assessment and map connected infrastructure, run correlations, look at attribution, highlight risky domains, and many more actions to surface meaningful insights.

HYAS Insight

Domain Intel | IOCs | Infrastructure Datea

HYAS Insight is a threat and fraud investigation solution using exclusive data sources and non-traditional mechanisms that improves visibility and triples productivity for analysts and investigators while increasing accuracy. HYAS Insight connects attack instances and campaigns to billions of indicators of compromise to understand and counter adversary infrastructure.

The **Maltego Transforms for HYAS Insight** allow analysts to query and visualize HYAS' exclusive, in-depth database of compromise indicators which will help them to better fingerprint events, actors, and infrastructure. With over 22 Transforms, users can query a broad range of data types ranging from domain names to malicious files and IP network details.

Intel471

Threat Actors | Malware | Vulnerabilities

The intelligence provided by Intel471 covers in-depth and time-sensitive adversary, malware, and vulnerability data that is automatically aggregated and globally relevant. Simply put, they provide actionable insights into threat actors and their motivations, tools, malware, techniques and alliances, thus equipping analysts with the necessary context to understand and stay ahead of the threat.

The **Maltego Transforms for Intel 471** allows security teams to visualize threat profiles to support threat hunters and analysts, as well as incident responders within the SOC team. Most relevant perhaps, with Maltego, analysts can access Intel 471 intelligence collected from operators and native speakers around the globe who engage with top-tier cybercriminals on an ongoing basis.

MISP: Malware Information Sharing Platform

Open Source | IOCs & Vulnerabilities | Financial Fraud

MISP is a free, open source threat intelligence platform used for sharing, storing, and correlating indicators of compromise (IoCs) of targeted attacks, and threat intelligence, as well as information on financial fraud, vulnerabilities, and even counter terrorism.

Maltego includes an out-of-the-box **Hub item for MISP** with Entities and Transforms that analysts may use to query data from a MISP Threat Sharing instance and visually browse through MISP events, attributes, objects, and galaxies. This integration also allows access and visualization of the full MITRE ATT&CK framework.

OpenCTI

Open Source | Knowledge Management | Technical & Non-technical Intel

A free, open source platform that allows organizations to manage their cyber threat intelligence knowledge and observables, OpenCTI was developed to structure, store, organize and visualize both technical (TTPs, observables, etc.) and non-technical information (suggested attribution, victimology, etc.) about cyber threats.

The goal of the project was to create a comprehensive tool that allows users to capitalize technical and non-technical information while linking each piece of information to its primary source (a report, a

MISP event, etc.). OpenCTI also includes features such as links between each information, first and last seen dates, levels of confidence, and more. Maltego will be releasing a Hub item for OpenCTI in Spring 2021.

Recorded Future

Machine + Human Analysis | Dark Web | Intel Reports

Recorded Future is a threat intelligence vendor that delivers technically advanced security intelligence to disrupt adversaries, empower defenders, and protect organizations. Using a sophisticated combination of patented machine and expert human analysis, Recorded Future fuses a set of open source, dark web, technical sources, and original research to deliver real time relevant threat insights.

The **Recorded Future Transforms for Maltego** give analysts visibility into which indicators should be prioritized based on real-time Recorded Future risk scores. Analysts using Maltego can access Recorded Future intelligence (risk scores, risk rules, Insikt Group Analyst Notes, etc.) in a simpler and faster way for deeper investigations.

RiskIQ PassiveTotal

Passive DNS | Infrastructure Data | Data Triage

PassiveTotal aggregates data from the whole internet, absorbing intelligence to identify threats and attacker infrastructure. It also leverages machine learning to scale threat hunting and response. With PassiveTotal, analysts can get context on who is attacking them, their tools and systems, and indicators of compromise outside their firewall.

RiskIQ offers over 100 **PassiveTotal Transforms for Maltego**, making it possible to query Entities such as domain, IPv4 address, URL, email, SSL certificates, and many other artifacts enabling analysts to conduct data triage with the help of Maltego.

Shodan

IOT Vulnerabilities | SCADA Systems | Infrastructure Data

Shodan is a search engine that gathers various types of publicly available data from internet-connected devices, concentrating on SCADA systems. The types of devices that are indexed range from small desktop computers to nuclear power plants, and everything in between. This answers the need that cyber investigators often have to go beyond what is traditionally considered as infrastructure to paint a full picture of the risks to which a system might be exposed. This is precisely where Shodan is an invaluable source of insight and information.

With **Maltego Transforms for Shodan**, investigators are able to gain access to and visualize intelligence about the global IoT and infrastructure data in their investigative workflows within Maltego. These Transforms can be used with all tiers of Shodan API keys.

ThreatConnect

Aggregated Intelligence | OSINT | Blogs & RSS Feeds

The ThreatConnect Platform provides aggregated intelligence from a diverse set of data sources such as OSINT feeds, Blogs, or RSS feeds; or indicators being sent from a threat intel feed provided by an Information Sharing and Analysis Center (ISAC) or a Premium Provider.

With more than 100 Maltego Transforms to query and pivot through **ThreatConnect's data**, investigators can easily model threat and the relationships between malware, domains, IPs, and other indicators to the incidents they were observed in, threats they are associated to, or adversary personas.

ThreatMiner

Open Source | Data Aggregation | IOC Context

ThreatMiner is a threat intelligence portal created to free analysts' time spent on data collection and provide threat intelligence analysts with a portal on which they can carry out their tasks, from reading reports to pivoting and data enrichment. The emphasis of ThreatMiner isn't just about indicators of compromise (IOCs) but also to provide analysts with contextual information related to the IOC they are looking at.

ThreatMiner is a data aggregator relying on a number of open source data feeds. However, it's important to note that it does automatic enrichment based on the following data feeds: CIRCL, VirusTotal, Malwr.com, Hybrid-Analysis, AlienVault OTX, IPinfo, Robtex, CleanMX, VirusShare, Sinica, Native. ThreatMiner offers a set of Transforms for Maltego that were designed to make the ThreatMiner data as easy to pivot through as possible while allowing seamless integration with other popular free and paid transforms analysts may be using.

VirusTotal

Malware Research | IOCs | Crowdsourced Intelligence

With a database of over two billion analyzed files, VirusTotal is one of the most renowned and best rated data sources within the cybersecurity sphere, particularly when it comes to malware research. VirusTotal is popular not only because it is a community-oriented solution, but also because it fills a gap for many companies which experience a lack of resources to collect their own malware samples and related indicators of compromise (IoCs).

Maltego offers integrations for both the public and the premium **VirusTotal APIs**. Both Hub items have been developed using the new VirusTotal APIv3. This has allowed Maltego to take advantage of the improvements made by the VirusTotal team in terms of richer data exposure of static information for files, crowdsourced detection details, and many others.

Integrate Your Threat Intelligence the Right Way!

It is important to remember that if threat intelligence is well implemented and integrated into the existing stack, it enables SOC teams to better prioritize and filter the overwhelming number of alerts they receive. This directly impacts the number of investigations incident responders and threat intelligence analysts need to undertake.

Link analysis tools such as Maltego are built and designed to be a centralized interface to query disparate data sources and aggregate data relationships into visualizations. This enables SOCs to:

Integrate all data in one interface

with one click, thereby reducing time and frustration spent on going back-and-forth between interfaces

Visually finding connections

in seemingly disparate datasets automatically, thereby significantly speeding up investigations

Collaborate effectively

with internal and external stakeholders to provide greater visibility on unknown threats, thereby building upon insights for faster remediation

At Maltego, the integration of all types of data sources and solutions in a single interface is a central theme of our solution for cybersecurity operations and SOC teams. If you would like to learn more about Maltego and its capability to integrate all SOC tools into an interface, get in touch with us!

About Maltego

Maltego empowers investigators worldwide to speed up and increase the precision of their investigations through easy data integration in a single interface, aided by powerful visualization and collaborative capabilities to quickly zero in on relevant information. Maltego is a proven tool that has empowered over one million investigations worldwide since its first launch in 2008. Due to its wide range of possible use cases ranging from threat intelligence to fraud investigations, Maltego is used by a broad audience, from security professionals and pen testers to forensic investigators, investigative journalists, and market researchers.

For more information, please visit: **maltego.com**