
COBWEBS
TECHNOLOGIES
eBook
There's More to Threat Intelligence than IOCs

TABLE OF CONTENTS

INTRODUCTION

Threat intelligence is often associated with indicators of compromise (IOCs) and attack (IOA). An IOC is a piece of data that indicates, with high probability, that a system or network has been compromised. An IOA focuses on identifying attacker activity while the attack is taking place. Both types of indicators are used by threat intelligence (TI) analysts to detect threats such as breaches and malware infections.

While automated IOC feeds are often the first thing that comes to mind when thinking of threat intelligence, there's also a lot of manual work involved, including reverse-engineering attacks and extensive reading of relevant content related to possible threats. Analysts need to look at where the information came from, what the vulnerabilities being targeted by threat actors are, and more - all of this data requires manual processing.

WHAT IS THREAT INTELLIGENCE

Threat intelligence, sometimes called cyber threat intelligence, is a term used to refer to the data which gives organizations a better understanding of the threats to their assets and vulnerabilities bad actors may exploit. Once an organization has this information it can then be used to ensure that the system can identify and prevent cyber attacks. Threat intelligence provides organizations with data about who the attacker is, what their capabilities are, and what weak points in a system should be monitored. This allows organizations to make data-driven decisions to remediate cybersecurity gaps.

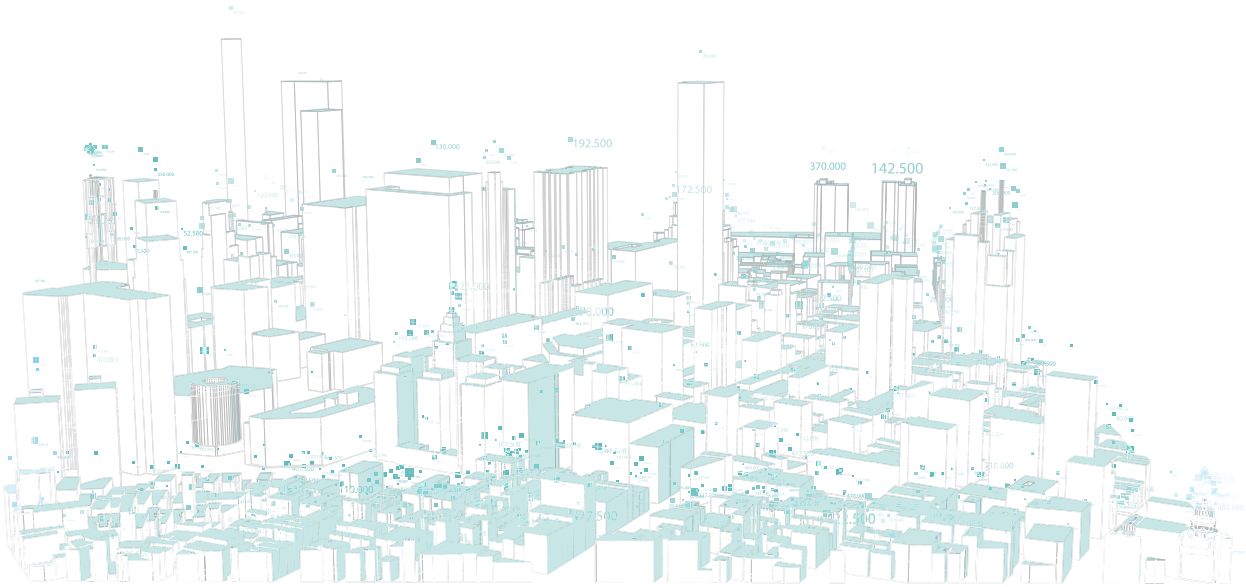
The results achieved from having access to threat intelligence vary due to the different sources of information, data requirements, and goals. As a result, threat intelligence can be divided into three sub-categories:

- **Strategic -** Offers users a general impression of the organization's threat landscape. As it is intended for executives or other decision-makers to make informed critical decisions around their organization's security, it is generally presented in a less technical way. Effective strategic intelligence is made to improve executives' understanding of the risks that certain courses of action may lead to or to present broad patterns in the tactics used by cyber attackers, as well as offer deeper insight into geopolitical events and trends. This category of threat intelligence is generally sourced from non-governmental policy documents, news media or subject matter experts, white papers, research reports, and other such content produced by security organizations.

- **Tactical -** Provides an outline of the tactics, techniques, and procedures (TTPs) of possible threat actors. It provides defenders with specific details on how the organization may be attacked and the best defenses to use against these attacks to prevent or diminish them. Usually, more technical than strategic intelligence, tactical intelligence is used by system architects, administrators, and other staff directly involved in security and defense. The information included in tactical threat intelligence reports is usually sourced from reports created by security organizations. These reports include detailed information on which vulnerabilities are targeted and how attackers may be avoiding detection.
- **Operational -** Intended to allow incident response teams to get a deeper insight into the nature, timing, and intent of particular attacks by giving them a focused look at the information surrounding the cyber-attack, campaign, or event. Generally, it includes extremely technical information such as which attack vector was used and which vulnerabilities have been exploited. As a result, it is also known as technical threat intelligence. It is most commonly sourced from data feeds.

The purpose of threat intelligence is to provide organizations with the ability to understand the threats to their assets and brand, and to make informed security decisions.

When correctly implemented, threat intelligence allows teams to find proactive solutions to potential security threats and allows the team to remain up-to-date on threats, vulnerabilities, bad actors, and the methods used by attackers. Threat Intelligence may even provide enough data on the pattern of attacks for cybersecurity teams to be able to identify the signs and prevent an attack before it has the chance to happen.



WHAT ARE THREAT FEEDS

A threat intelligence feed also called a "TI feed", is the continuous data stream that provides organizations with information relevant to current or potential threats to the security of the organization. The feed gives the organization data which is constantly updated with information on possible sources of attack.

TI feeds are often said to include "threat data" and not "threat intelligence" because the feeds consist of raw data that has not yet been analyzed or processed. Feeds, and free feeds, in particular, cannot be relied on for complete accuracy, and free feeds, in particular, can create issues around accuracy. As a result, most industry professionals agree that manual analysis or review is still crucial to avoid unnecessarily blocking benign IP addresses or domains and lost traffic, however, this can take a long time and leaves room for human error when done manually.

A TI ANALYST'S TYPICAL WORKFLOW

Let's say an organization is concerned about an attack from an Eastern European country. In such a situation, the TI analyst will start reading about known attacks originating from this region to learn about possible threat actors. Once relevant threat actors are discovered, the analyst dives deeper into their research to learn about each threat actor, how long they've been active, who was responsible for the most recent attack, what methods they use, and what motivates them. For example, one threat actor could be politically motivated and focused on IoT attacks, while another could be more interested in making money with cyber espionage. Each type of attack, tool, and malware family is analyzed even further.

Everything the analyst learns needs to be organized in a way that enables actionable insights for smarter decisions that protect the organization. This is a challenging process, and typically, analysts will use various tools and graphs to organize the information so that overlaps of threats, techniques, and procedures (TTPs) can be detected. This helps the analyst decide where to focus their research moving forward. For example, if there is a significant prevalence of hash attack techniques, an organization can prioritize their defensive checkpoints there to mitigate the risk of a successful attack. This not only increases the efficiency of security measures within the organization but also reduces redundant efforts; for example, insights may indicate an organization should de-prioritize time-stamping because it is unlikely to impact security.

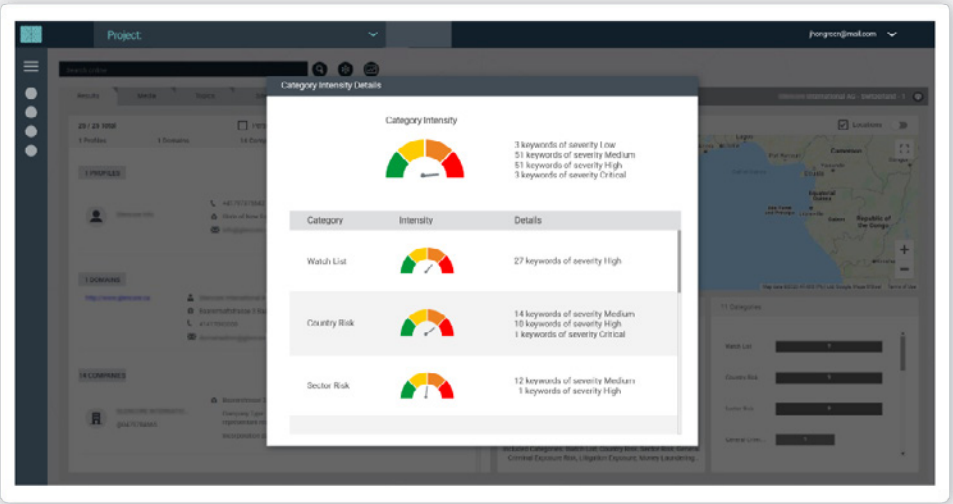
All of this is typically done manually, which leaves too much room for human error and missed information that could be critical to the process.

THE THREAT LANDSCAPE HAS EVOLVED

Over the past two decades, the threat landscape has evolved to something far more complex than it was when it first started. Corporations today use more technological solutions, enable remote access to employees and third parties, and operate on global scales - the attack surface has grown and there are too many attack vectors to keep track of. As more security methods develop, threat actors and hackers adjust their strategies and use more complex methods to successfully breach networks and access sensitive data. There are too many methods to keep track of, and many are nearly impossible to avoid without 100% cooperation and awareness from all employees - for example, email-based threats such as BEC scams.

Threat intelligence has become a critical tool to achieve cyber resilience and is often part of an organization's business strategy discussed at the highest executive levels. Employing effective threat intelligence practices affects more than just the cybersecurity of an organization's networks; it is used to prevent insider threats when hiring, ensure reliable business partners before entering agreements, complete effective due-diligence before M&As, and even gain insights into geographical locations before entering new markets.

Preventing attacks and getting actionable insights into risks, vulnerabilities, and threat actors require in-depth analysis of content on all of the web's layers - open, deep, and dark. From hidden forums and marketplaces to public content on blogs and social media platforms, the data is vast and impossible for any security analyst, or team of analysts, to fully analyze.



WHERE TO USE THREAT INTELLIGENCE

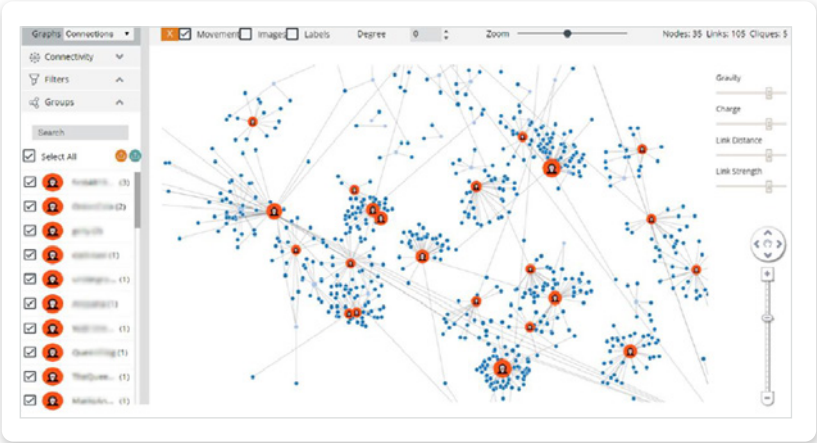
Threat Intelligence has a diverse range of uses; it is not only limited to the cybersecurity sector but is an extremely valuable resource across any data-driven organization. While its main use is preventing any attacks or security breaches, it serves as an invaluable tool for more effective vulnerability management, risk analysis, and information-based decision making. Some of the other areas in which threat intelligence can contribute include:
The results achieved from having access to threat intelligence vary due to the different sources of information, data requirements, and goals. As a result, threat intelligence can be divided into three sub-categories:

Incident Response

Incident response analysts have earned a reputation for having one of the most stressful jobs in the industry, as incidents of cyber attacks have been rising steadily over the past 20 years, and a high number of the alerts received end up being false positives. Instead of having analysts manually sort through reams of data in order to evaluate the situation, threat intelligence can be used to automatically locate and dismiss false positives, add real-time context to alerts, and compare the information received from both internal and external sources. This speeds up the risk analysis process, allowing cybersecurity teams to devote their valuable time only to incidents that truly require their expertise.

Vulnerability Management

As vulnerabilities increase so do threats, but research shows that a majority of threats all target the same small proportion of vulnerabilities. Additionally, while threat actors may have learned to target vulnerabilities soon after they are announced, effective threat intelligence can identify the important vulnerabilities that can actually put an organization at risk.



Security Operations

SOC (Security Operations Center) teams manage huge amounts of alerts. To triage these alerts would take too much time, and as a result, many are ignored. Analysts afflicted with “alert fatigue” no longer take alerts seriously and are often overworked and stressed. Threat intelligence solutions, particularly when powered by AI, are capable of gathering information on threats quickly and accurately, filtering out false alarms, streamlining incident analysis, and hastening triage, allowing analysts to no longer waste time on false positive or irrelevant alerts.

Fraud Prevention

Responding to threats already attacking the system is not enough. To truly keep an organization protected, it is important to make sure that the brand and its data aren’t being exploited for fraudulent uses. Gathering threat intelligence from criminal communities allows for a glimpse into the methods, motives, and strategies of threat actors, particularly when this information correlates with information sourced from the surface web. Using threat intelligence in this way can help prevent payment fraud, compromised data, and phishing or typosquatting.

Risk Analysis

Organizations often prioritize investments based on risk modeling, but risk models can often be unspecific and lack concrete quantified output. Many times, they are compiled from half-baked information or assumptions, or it can be difficult to determine a clear path of action from them. Threat intelligence provides the context that risk models are missing, creating more definable and clearer risk models through which a proactive course of action may be determined.

Security Leadership

Security leaders such as CISOs are responsible for risk management and must try to create a balance between limited resources and the need to continue upgrading security against threats that continue to evolve. Threat intelligence can delineate the threat landscape and calculate the risk, allowing CISOs to hand their security personnel and executive decision-makers the information and context needed to make educated decisions faster. Threat intelligence is a crucial resource for risk assessment and strategic planning as it can identify:

- What types of attacks are increasing or decreasing in frequency
- Which are the costliest attacks for the victim
- New types of threat actors, as well as what their targets are
- The most and least effective security practices and tools used to stop or prevent such attacks.

THREAT INTELLIGENCE FOR DECISION MAKING

Threat intelligence can allow security groups to evaluate whether a new threat is likely to specifically target their brand or enterprise based on factors such as industry, geography, technology, and method of attack. This type of information allows decision-makers to make security decisions based on a broad and informed understanding of the risks their enterprise faces as well as the cyber risk landscape as a whole.
Threat Intelligence aids security leaders in their decision making particularly in four critical areas in particular:

Communication

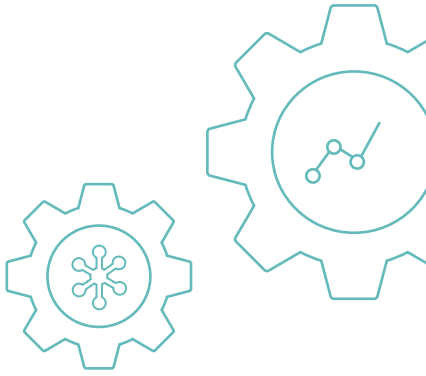
CISOs are often faced with the challenging task of describing threats and explaining countermeasures to business leaders who are not necessarily aware of the technicalities behind them. Threat intelligence solutions with visual reporting capabilities can serve as a powerful tool to explain the possible consequences of an attack by providing illustrative examples such as the effect similar attacks have had on companies of comparable size in other industries, or by showing information or trends from the dark web that show that the enterprise is at risk of being targeted.

Mitigation

Security leaders rely on threat intelligence for data that allows them to prioritize the weaknesses and vulnerabilities most likely to be targeted by threat actors. This provides the TTPs which those threat actors use with the context necessary to understand which vulnerabilities they are more likely to take advantage of.

Security Skills Gap

Cybersecurity leaders find themselves struggling with a skill shortage, and many organizations are short-staffed. As a result, existing staff is often overworked and struggling with large workloads. By automating some of the more laborious and repetitive tasks such as collecting data, connecting information from multiple intelligence sources, deciding which risks to prioritize, and reducing alerts, security and analyst teams can devote themselves to more important tasks.



Leadership Support

Threat Intelligence gives security leaders a realistic view of the latest trends, threats, and events relevant to their organization and its security posture. This allows them to react or report the possible results of such an event to business leaders in a quick and effective manner and remediate gaps quickly to mitigate the damage.

WHAT AI ADDS TO THREAT INTELLIGENCE

AI, or artificial intelligence refers to any intelligence displayed by a machine. Today, AI is often used with machine learning, which enables it to "learn", process data, and reach its own conclusions based on what it has been taught in the past. Today, AI and machine learning solutions are used to analyze vast amounts of data, identify patterns, and reach logical conclusions in minutes, where a manual process conducted by humans would take years or would be impossible altogether. In threat intelligence, and in today's digital world, being able to process and analyze streams of data from multiple sources is critical.

There is too much information for analysts to monitor, and they often don't really know what they're looking for. The risk of human error or just missed information is high, and organizations can't simply increase manpower to overcome it. Artificial intelligence combined with machine-learning technology is the only way to collect, analyze, and monitor the data to provide TI analysts with real-time alerts and actionable insights they can use to strengthen the organization's cyber resilience.

Machine learning and AI-powered technology developed by Cobwebs Technology eliminates the need for this manual process by taking volumes of unstructured data and connecting the dots, structuring it without the need for human intervention. AI and machine learning can cope with vast volumes of data in real-time, so that new data is constantly analyzed to enable quick action. One single lead can be transformed into a clear, comprehensive, in-depth report for the analyst to review.

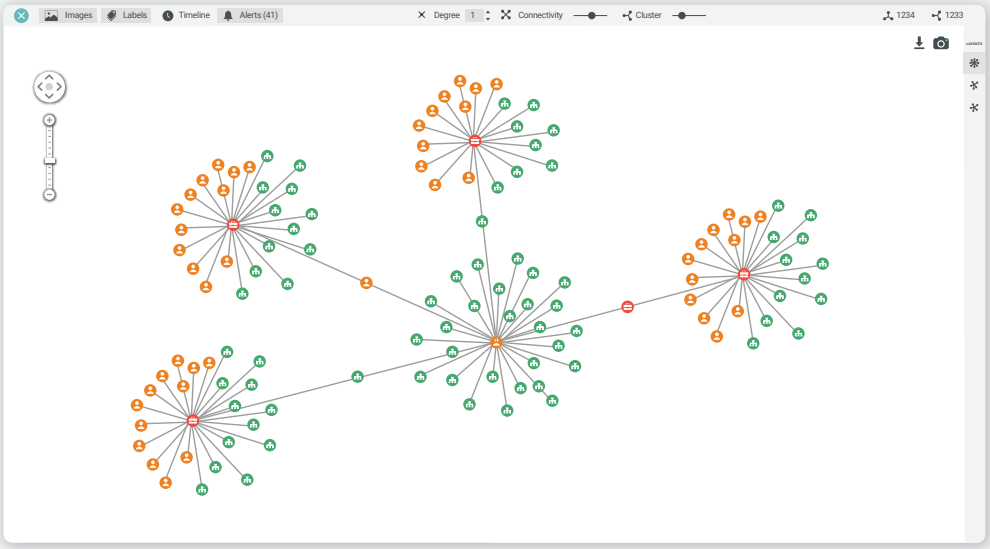
"There is simply too much information to sift through, and it contains critical data needed to protect organizations from threat actors. We created our AI-powered platform to do the heavy lifting, and provide analysts with the bottom line insights they need."

Shay Attias | Co-Founder & CTO at Cobwebs Technologies

From a TI analyst's perspective, the platform's input in vast amounts of unstructured data that the analyst can access, and the output is actionable insights like the TTP graphs which would have been created manually. This includes the identification of threat actors and their network of connections, their motivations, and sentiments based on NLP combined with machine-learning algorithms that provide in-context analyses, and vulnerabilities being discussed throughout the web's open and hidden layers, such as names of malware attacks, discovered vulnerabilities in networks, and more.

With Cobwebs Technologies, there is never too much data. The platform enables analysts to automate and streamline their threat intelligence processes to make them faster and more efficient while using fewer resources.

By providing security and threat intelligence analysts with a centralized platform, corporate security teams don't have to rely on siloed solutions for their investigations. A centralized platform reduces wasted resources and human error and provides all of the needed features and capabilities in one place, including image analysis, face recognition, natural language processing, predictive analysis, pattern recognition, real-time alerting, and more. These capabilities rely on AI and machine learning technology to effectively analyze content, provide context and sentiment insights, and connect the dots between threat actors, networks, and different types of data.



ABOUT COBWEBS

Cobwebs Technologies brings extensive years of vast experience in the global intelligence market. The company team is comprised of an experienced group of individuals from military and intelligence agencies, along with high-tech expertise. Our extensive background in web intelligence, gained through years of active participation in field-specific projects, allowed us to identify the lack of adequate intelligence solutions coping with current technological challenges. We offer innovative, cutting-edge systems to national security agencies and private sectors, as our solutions pinpoint web relations, criminal activities, and terrorist threats with the click of a button.

Working with clients worldwide, Cobwebs assists them with investigations and analysis of targeted data with a range of products, from robust, end-to-end solutions, to professional services and detailed analyst reports.

www.cobwebs.com | info@cobwebs.com