Revealed Threats

WHITEPAPER

CONTENTS

EXECUTIVE SUMMARY

Analysts will look for evidence of an attack by examining alerts from various security solutions, typically a Security Information and Event Management (SIEM) system. However, because SIEMs were built to process and store all of an organization's insider data, many alerts that are generated are not real threats. These false positives are not actually malicious and usually take up a lot of time to investigate. With an already limited staff, this can be crippling to the effectiveness of a security team. Threat intelligence helps analysts to verify and filter through these alerts by correlating curated threat intelligence with internal threat markers.

Threat intelligence itself can present a number of challenges. IOCs can number in the millions and the process of identifying which are relevant is labor-intensive. Revealed Threats is designed to automatically manage threat intelligence for faster insights into cyber threats.

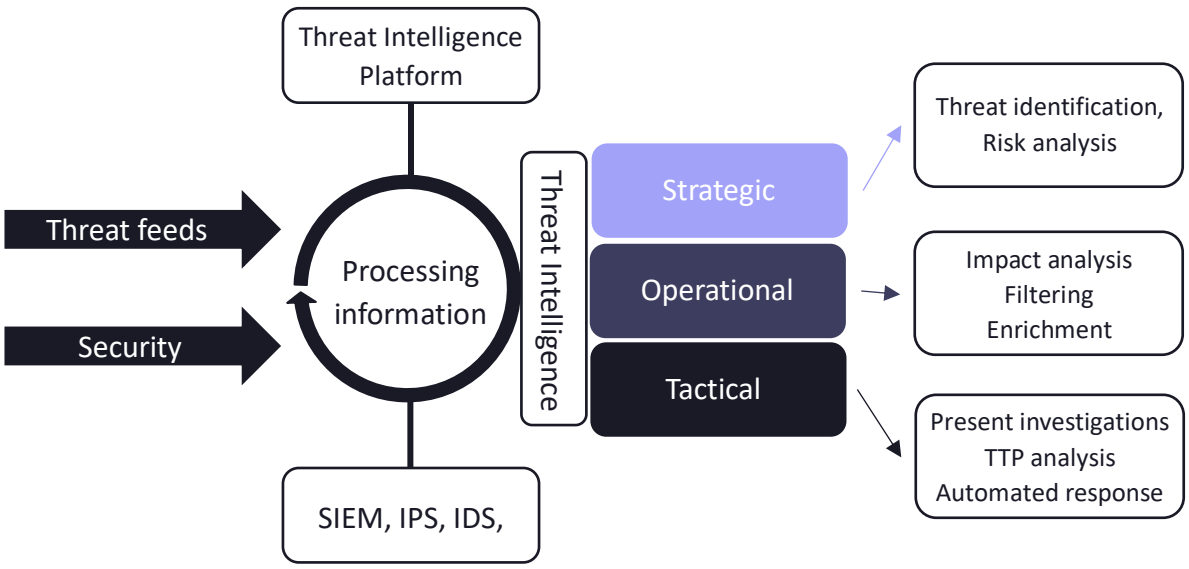
Raw data is transformed into finished intelligence that is easily understood, readily shareable, and most importantly—actionable. With intelligence, automation, and integration with existing security tools, organizations are able to understand threats that are relevant to them. The most frequent users of threat intelligence platforms include:

- Security Operations Center (SOC) Analysts
- Threat Intelligence Analysts
- Incident Response (IR) Teams
- Chief Information Security Officers (CISOs)
- C - level managers

The data that Revealed Threats has collected, de-duplicated, aggregated and ran through its Machine Learning algorithms is passed on to the available intelligence. IOCs, Threat Actors, Tactics Techniques and Procedures and other similar tags get attributed for easier and quicker analysis.

REVEALED THREATS

Revealed Threats is a CTI, a data collector and analyzer that is hunting for threats, enemy actors and information, for the augmentation of the organization's security. By processing and identifying the relevant data, it enables for the entity, to recognize the possible IoCs for an attack, attach to them potential threat actors, attack vectors and other relevant information gathered from a vast number of sources. Ultimately, it will help the organization prevent or identify early the attack.
Assessing the entity's attributes and fine-tuning RevealedThreats we can achieve a previously unseen net of protection at the borders of the organization.
Once a user subscribes to RevealedThreats, it will enter the information of its own infrastructure data and therefore will be getting exclusively the threats that are relevant to them. The security tools like SIEM and SOAR systems will not be overloaded with useless threat information, and the correlations produced by the SIEM system will be much more effective and time-consuming, reducing the false positives considerably.
Indicators are sent to firewalls and intrusion detection systems for active blocking, correlated against information in SIEMs to prioritize alerts, and may be sent to orchestration platforms to improve workflows. The flexibility of these integrations rapidly improves the ability of a security team to identify and counter threats.



RevealedThreats is a combined Open Source Intelligence (*OSINT*), Human Intelligence (Cyber-HUMINT) and Technical Intelligence (TECHINT) asset, which is collecting and analyzing information and Indicators of Compromise (*IoC*), from public and private sources, to assess the existing and possible future threats, regarding the environment in scope. It is built on the foundations and data on the deep and the dark web, and it's most important task is to identify the latest methods and trends in the three major threat segment:

- Computer crime
- Hacktivism
- Cyber espionage

PLANNING

For the definition of CTI, we have to assess the position and the cybersecurity risks of the entity. In this assessment, there is a need to chart the network infrastructure, applications, operating systems, appliances and the human workforce of the organization. This assessment is mandatory to determine who can attack the organization, with which methods and exploits.

DATA COLLECTION

One of the most important CTI planning processes is data collection. Within this process, the entity has to think about which kind of information needs to be collected, from which sources and if there is enough processing power to analyze it.
It's mandatory to get relevant and up-to-date information and for this, multiple data sources are needed, as they can be correlated to each other and they can back each other's credibility. With multiple data sources, the entity/sector can get ahead it's possible attackers.
There is also a need to analyze the internal data sources, as they can give a picture regarding the entity's internal structure and with the alerts from the SIEM, IDS and IPS systems, most of the threats can be neutralized.
Both the internal and the external data sources are equally important and they are augmenting each other to form a protecting web around the organization.

Internal Data Sources

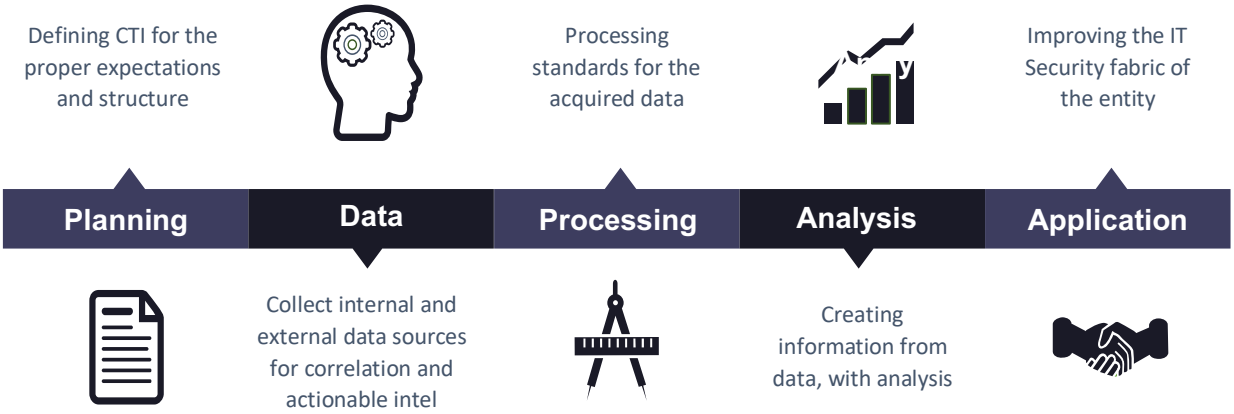
The internal sources are the data streams collected inside the entity's infrastructure. As most of the organizations have experienced cyber-attacks in the past, the CTI system can find the similarities and connections within these. By analyzing past attacks, the prevention and forecast of further incidents will be easier.
Nowadays, most of the organizations are using data collection and analytical applications, like SIEM, IDS and IPS systems. These systems aren't just for the tracking of ongoing events, but they can also be useful for the forecast and prevention of future ones.
If you add CTI to the mix, it can help discover anomalies in the network traffic and the logs, which can help discover recently started attacks and incidents. This information-rich environment can also help with root-cause analysis, by uncovering attack patterns, vulnerabilities and possible attack vectors from last incidents and to generate a hypothesis.
To build a proper internal data source, it's necessary to create and properly document these incidents, as they're critical for both the root-cause analysis and the forecasting of incidents.

External data sources

The second leg of the CTI systems. Due to the nature of these external data streams, their reliability and relevance can be low, and they can also be redundant. Also, the processing of this volume of data can be taxing in terms of hardware. So these sources have to be chosen and vetted carefully.
To obtain these data streams, there are open Threat Intelligence streams, open governmental data, Social Media and the Dark Web and closed diversified honeypot networks.

A part of the sources of a CTI is open Threat Feeds. They have curated feeds regarding threats and Indicators of Compromise (IoC), like IP addresses with a bad reputation, malware hashes, C2 domains, and others. Most of these IoC is about existing and valid threats.
On the other hand, there are Information Sharing and Analysis Centers (*ISACs*), which are inter-entity information sharing centers for industry sectors and governmental agencies. The ISAC lists are also curated and containing relevant data. One of the main sources of information is the E-ISAC of ICS/OT sector, that brings invaluable amounts of energy-specific intelligence, best practices, and case studies.
The third, curated source is the governmental Open Data. This is collected by governmental sources, agencies (ICS-CERT; *US-CERT, etc*). Their data is also highly relevant and quantifiable.

The above three, curated sources are containing IOCs regarding the existing threats, but there are others lurking in the shadows. To shed light on them, the CTI is using other feeds, like Social Media and Dark Web crawlers. And when these are filtered by professionals, it can be used to uncover future attacks.
In addition, there is the CVE database. CVE is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE is a dictionary of publicly disclosed cybersecurity vulnerabilities and exposures. RevealedThreats scans through these databases and presents the ones that are relevant to your organization.
The protective mesh of the CTI comes by combining internal and external data sources. While the internal sources are the answer of the question "What happened?", the external sources are about what may happen next, what are the "forecasts" to which you can and should prepare. By carefully mixing the two, we can proactively patch and harden the infrastructure of the clients, rendering it very difficult to penetrate.



PROCESSING

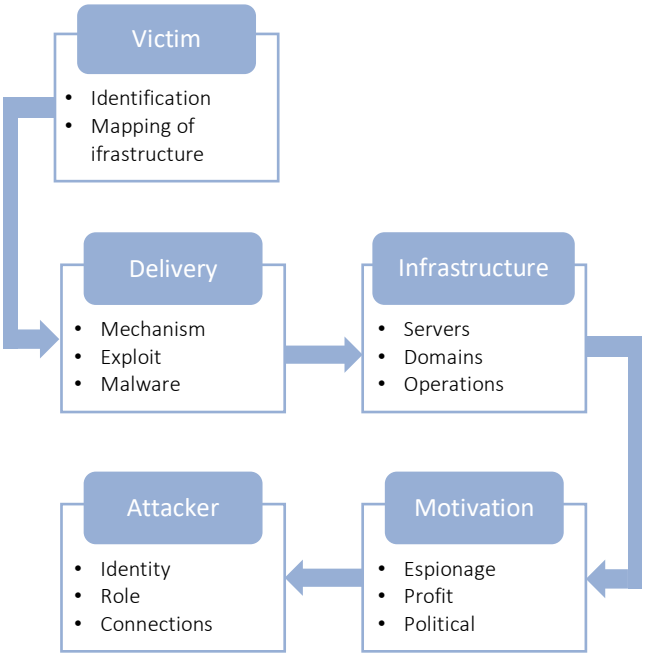
After the "Data Collection" phase, the data needs to be processed to convert it to useful and relevant information. For this, the information, gathered from internal and external sources, needs to be validated. It's important to note, that without validation, the data is not useful, it's not information or intelligence.

Data	Information
Raw, unfiltered	Processed and filtered, actionable
Unprocessed	Curated by professionals
Can be from any source	Coming from vetted sources, correlated, deduplicated
Can be irrelevant and not whole	Whole, relevant and up-to-date

The validation process is about grouping and correlating the collected data, to find the missing pieces. After correlation, the fake and invalid data needs to be removed, to get actionable and trusted intelligence from the raw data. This information now will be indexed. Thanks to this process, the hardware needed for storing and processing the information is drastically reduced.

ANALYSIS

After processing, the database contains actionable intelligence, which is relevant to the entity. This data is now enabling the further hardening of the organizational infrastructure and enhancing the detection and response capabilities of the internal security systems.
It also provides viable information regarding possible future attack patterns and helps to assess the damages of past incidents. Valuable for creating "Early Warning" systems and helps with IT Security related strategic decision making.
RevealedThreats also sends the CVE database onto the internal network for recently uncovered vulnerabilities and alerts users of the need for patching or remediating. The information described above can create a previously unseen situational awareness.



APPLICATION

With filtered and processed information, the entity can identify the patterns of the attacks and avoid them with the existing security infrastructure. According to SANS research, **63% of the CTI user organizations confirmed, that CTI helped to augment their incident detection and response**. Also, 28% experienced a faster and more accurate incident reaction and handling. With these improvements, the incident damages may also lower.

HOW THREAT MANAGEMENT FITS INTO YOUR ORGANIZATIONS SECURITY LIFECYCLE

PLANNING

Security teams have to plan for every possibility. They assess what threats their organization is most likely to face based on what product or service they produce, their geolocation, their political affiliations, and more. Analysts gain more visibility into what threats are relevant to them and how those threat actors operate. RevealedThreats enables analysts to select and utilize what tools will be most effective for prevention and mitigation.

MONITORING AND DETECTION

Pulling in external, verified context on threat actors and their TTPs eliminates the need for security analysts to do the research to determine what is and isn't malicious. Organizations can quickly identify whether or not those malicious indicators are present by correlating threat intelligence with data from their existing security systems. Anything identified as suspicious can be automatically sent to integration points for monitoring. This makes it more likely to block something before it enters the network.

INVESTIGATION ANALYSIS

Once malicious entities are uncovered, analysts will conduct investigations to determine the impact on their organizations. Revealed Threats provides a workbench for analysts to examine evidence where they can link different pieces of information. Analysts pivot off of individual IOCs to look up WHOis information, PassiveDNS, AbuseIPDB and more to uncover previously unknown threats.

RESPONSE AND REMEDIATION

During an incident, RevealedThreats can help you identify patterns and threat actors associated with them to inform your next action and remediate and respond more quickly. It can tell you that a particular actor is known to use a specific tool or tactic during an incident that you can investigate further.

FEEDBACK

The feedback phase is critical for improving on your current security. Revealed Threats is useful for assessing where to improve because they sit in between tools and information.
Key areas to consider are:

- The monitoring phase to see whether the sources of information used are helpful to identify and block threats
- The detection and analysis phase to see how long it took to come up with a conclusion.
- The response and remediation phase to determine whether you had the right information and how long it took to react. For example, if a malicious actor successfully infects a system, you can see whether information about that threat was already available in the repository or, if not, what other source contains that information.

Cybercriminals today are working overtime to target organizations for exploitation. Your organization benefits from understanding your vulnerabilities, staying ahead of threats and remediating events quickly. Investigating all these incidents can quickly overwhelm your security team, which is likely already stretched thin due to the cybersecurity talent shortage. We can expect a global shortage of cybersecurity professionals... 350k cybersecurity positions are currently open and there is roughly 3,5 M shortfall predicted by 2021 by Cyber Security Ventures.

RevealedThreats lets you focus on the real threats and vulnerabilities that are relevant to your organization's infrastructure, saving you time and resources and allowing you to get intelligence that really matters.

REVEALEDTHREATS KEY BENEFITS

OT THREAT INTELLIGENCE

Industrial control system (ICS) owners and operators and IT groups that have ICS in their environment should seek out and obtain an ICS threat intelligence product, regardless of whether they are already receiving generic threat intelligence.
Threat intelligence targets the various levels of the organization and informs them appropriately to maximize impact, and it comes in three main categories: Tactical, Operational and Strategic.
The Strategic category is for the security and organizational leadership, as it places threats into a business context and describes the strategic impact. Adversary background, intents and motivations, the business impact may be on their list of interest.
Tactical intelligence serves the network level action and remediation teams to act upon technical indicators and behaviors. They typically include IP addresses, domains, malware reverse engineering analysis and network traffic.
Operational intelligence serves Threat Hunters and incident responders and includes intelligence on holistic remediation, threat hunting, behavioral direction, data collection. It includes campaign history, end-to-end adversary operations, etc.
As for ICS impact, threat intelligence may be categorized as the following:

1. intelligence on activities of adversaries known to have an interest in control systems and operational networks.
2. Intelligence on threats affecting the operation of ICSs.
3. Intelligence on threats not associated with industrial control systems but have a high likelihood of disrupting their operation.

ICS AND SCADA HONEYPOTS

There is still little information about SCADA vulnerabilities and attacks, despite the growing awareness of security issues in industrial networks. As is the case with IT security, owner-operators are often unwilling to release attack or incident data. Although some vulnerability research is being conducted in this area, very little has been released publically and no "SCADA security tools" (whatever that might mean) have been released to the public.
By providing a range of common industrial control protocols we created the basics to build your own system, capable to emulate complex infrastructures to convince an adversary that he just found a huge industrial complex. To improve the deceptive capabilities, we also provided the possibility to server a custom human-machine interface to increase the honeypots attack surface. The response times of the services can be artificially delayed to mimic the behavior of a system under constant load.

BRAND MONITORING

Revealed Threats allows its clients to be monitoring their brand or legal names on the open and dark web, social media sites and other forums. Brand monitoring is a business analytics process concerned with monitoring various channels on the web or dark web in order to gain insight about the company, brand, and anything explicitly connected to the business.
Brand monitoring allows for CISOs and other C-level managers to scan keywords that they feel are relevant to their organization and find out if there is any mention of them in underground forums or dark web forums, or unauthorized social media presence.

Finding out about a whistleblow before it may occur has tremendous advantages for brand or company reputation.

ATO

Account Takeover (known as ATO) is a type of identity theft where a bad actor gains unauthorized access to an account belonging to someone else. With RevealedThreats you can get a tool that lets you scan the dark web or open web for your company's email addresses, looking for breached accounts. Finding your user's information first may hold your company from unwanted consequences and allows you to take the necessary steps to halt the attacks.
There may be various reasons behind this type of attacks. ATO targets regularly include gaming, technology, retail, restaurants, online travel, and reward programs where a criminal tries to obtain products and services. In other scenarios, the criminal's goal is to collect personally identifying information (PII) to be used for other forms of fraud and identity theft. These types of attacks often target healthcare, public sector, and even academic institutions.
Because ATO attacks rely heavily on the reuse of credentials exposed in 3rd party data breaches, an effective defense involves detecting logins using previously compromised credentials.

FEEDS INTO YOUR SIEM, SOAR, MISP AND THREAT HUNTING PLATFORMS

Using the RevealedThreats API you can take your own feed (adjusted to your own organization's infrastructure) and connect it into your SIEM system, adding intelligence to your correlations. Clearing the majority of the false positives identified by your SIEM system you can have less overworked security staff deal with the alerts that are truly important and investigate on the actually important incidents. APIs are available for popular SIEMs like IBM Qradar, Splunk and RSA.

MALWARE LAB

RevealedThreats offers you to load MS documents, PDFs, files, hashes, URLs onto our Malware Lab where your files will be thoroughly examined and scanned for malicious components, codes, macros, malware or trojans. It then separates the malicious component from the file, and it generates a report on the findings. You can get back the cleaned file when possible, and have alerted the Revealed Threats community of the malicious component it has found.
If the file is clean, it will get a „CLEAN" status shown in the list at the end of the examination.

For further information contact us

INFO@REVEALEDTHREATS.COM