CIM

TECHNICAL GUIDE

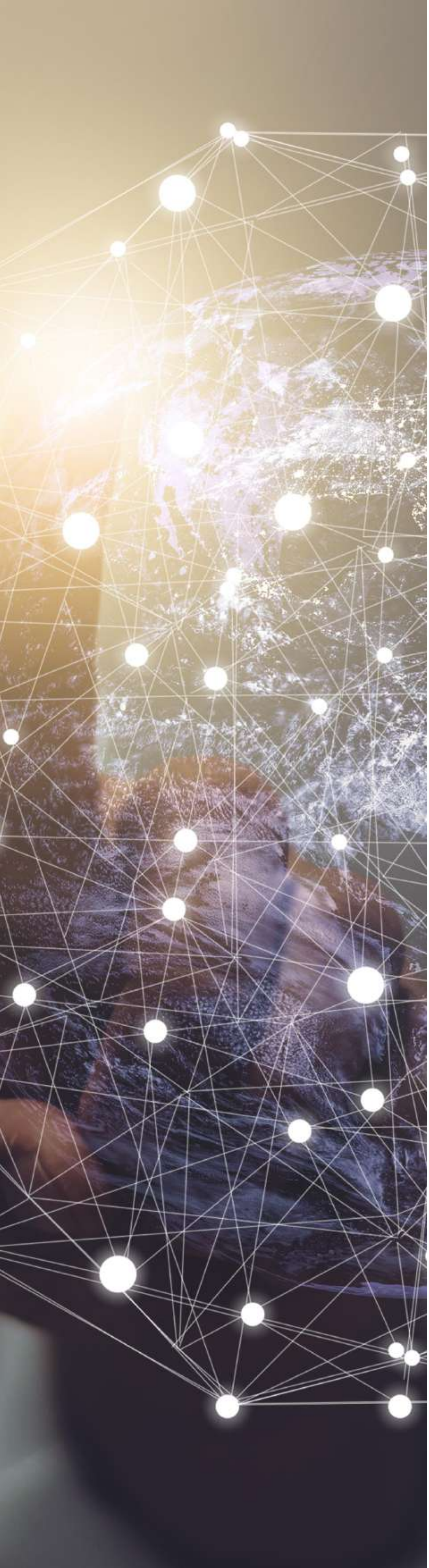
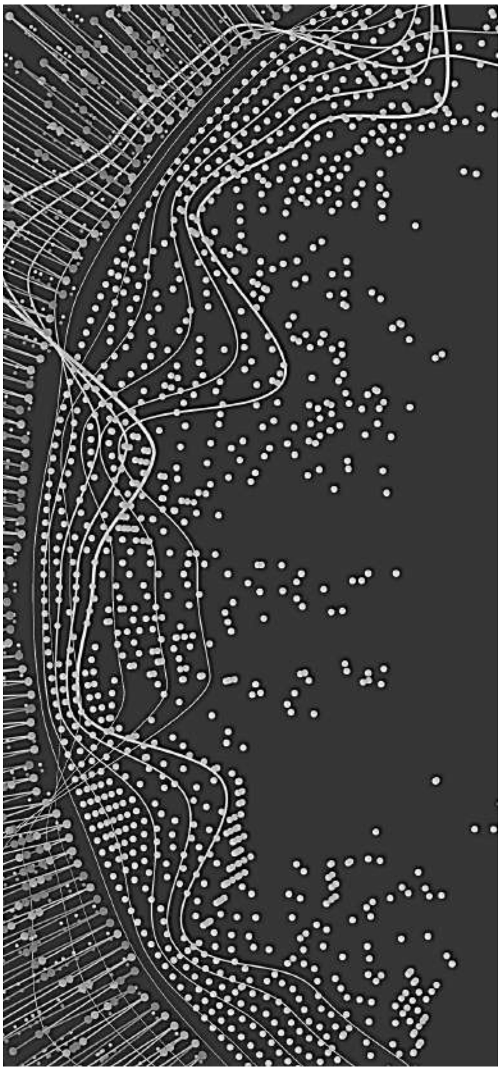


Table of Contents



EXECUTIVE SUMMARY

Analysts will generally look for attack evidence 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 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 **verify and filter these alerts by correlating curated threat intelligence with internal threat markers.** Threat intelligence alone can present a number of challenges. Indicators of Compromise (IOCs) can number in the millions and the process of identifying which are relevant is labor-intensive. **Cyber Intel Matrix (CIM)** is designed to automatically manage threat intelligence for faster insight into cyber threats.

Raw data is transformed into finished intelligence that is easily understood, readily shareable, and most important—actionable. With intelligence, automation, and integration with existing security tools, organizations are able to understand relevant threats. 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 executives

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

SECTION 1

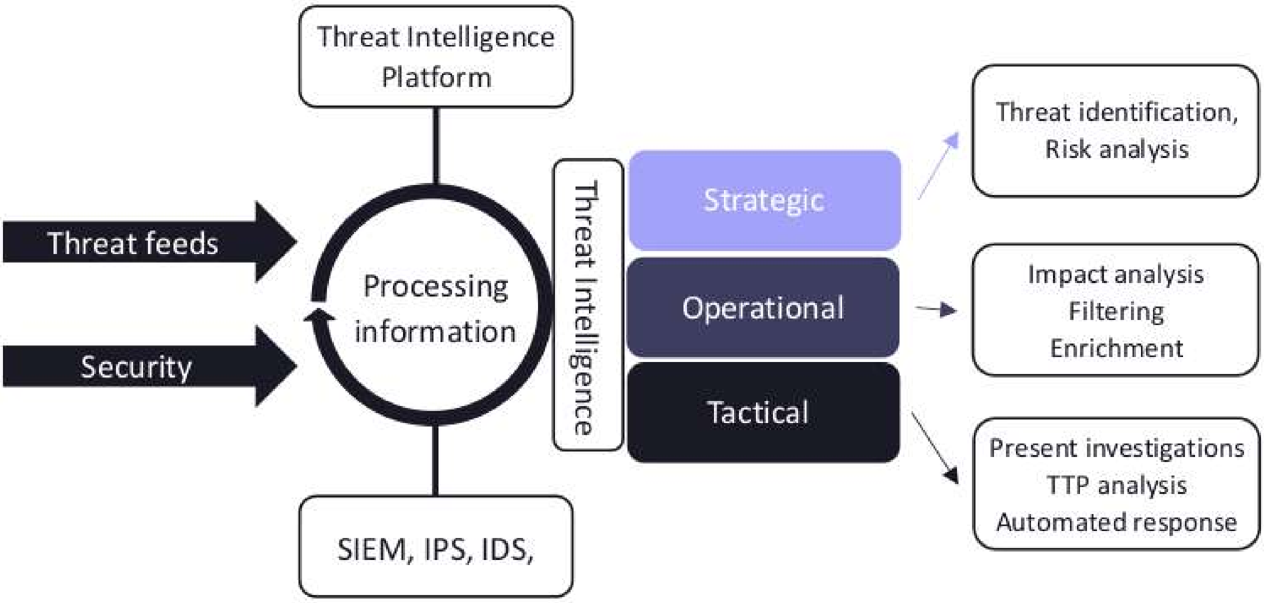
CYBER INTEL MATRIX

CIM is a CTI, a data collector and analyzer that hunts for threats, enemy actors, and information, for the augmentation of existing security. By identifying and processing relevant data, CIM enables alerts to possible IOCs, attaches to them potential threat actors, attack vectors, and other relevant information gathered from a vast number of sources. Ultimately, CIM CTI will help identify or prevent the attack.

Assessing attributes and fine-tuning CTI, we can achieve a previously unattainable net of protection around the perimeter of any organization.

Once a user subscribes to CIM, that user enters specific infrastructural data, and only receives relevant threats. 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, saving time and reducing the false positives considerably.

Indicators are sent to firewalls and intrusion detection systems for active blocking, are correlated against information in SIEMs to prioritize alerts, and then 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.


Threat Intelligence Platform
Threat feeds
Security
Processing information
SIEM, IPS, IDS,
Threat Intelligence
Strategic
Operational
Tactical
Threat identification, Risk analysis
Impact analysis Filtering Enrichment
Present investigations TTP analysis Automated response

CIM is a combined Open Source Intelligence (OSINT), Human Intelligence (Cyber- HUMINT) and Technical Intelligence (TECHINT) asset, which collects and analyzes information and IOCs, from public and private sources, to assess existing and potential future threats, always taking into consideration the entire scope of the relevant environment, industry niche. CIM is built on the foundation and data in the deep and the dark webs.

CIM's most important ongoing task is to identify the latest trends and methods in three major threat segments:

- Computer crime
- Hacktivism
- Cyber espionage

Planning

For achieving true CTI, we must first assess the cybersecurity risks of any organization. This includes charting the network infrastructure, applications, operating systems, appliances and the human resources. Without this assessment, there is no way to accurately determine who can attack the organization, and with which methods and exploits.

Data Collection

One of the most important CTI planning processes is data collection. An organization must assess which information needs to be collected, from what sources, and if there is enough processing power to analyze it. Because a constant flow of relevant and up-to-date information is necessary, multiple data sources are needed, so they can be correlated and create redundancy for reliability. With multiple data sources, any entity, or even an entire sector, can get ahead of possible attackers. Internal data sources must also be analyzed, as they can paint a picture of the internal structure. 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; only together do they form a protective web around the organization.

Internal Data Sources

The internal sources are the data streams collected inside an organization's infrastructure. Given the nature of most cyber-attacks in the past, the CTI system can find the similarities and connections within these streams. By analyzing past attacks, the prevention and forecast of future incidents will be easier.

Most organizations are using data collection and analytical applications like SIEM, IDS, and IPS systems. These systems aren't just for tracking ongoing events, but they can also be useful for forecasting and preventing future ones. If you add CTI to the mix, it can help discover anomalies in 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 the last incidents, which, in turn, generates 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 root-cause analysis and incident forecasting.

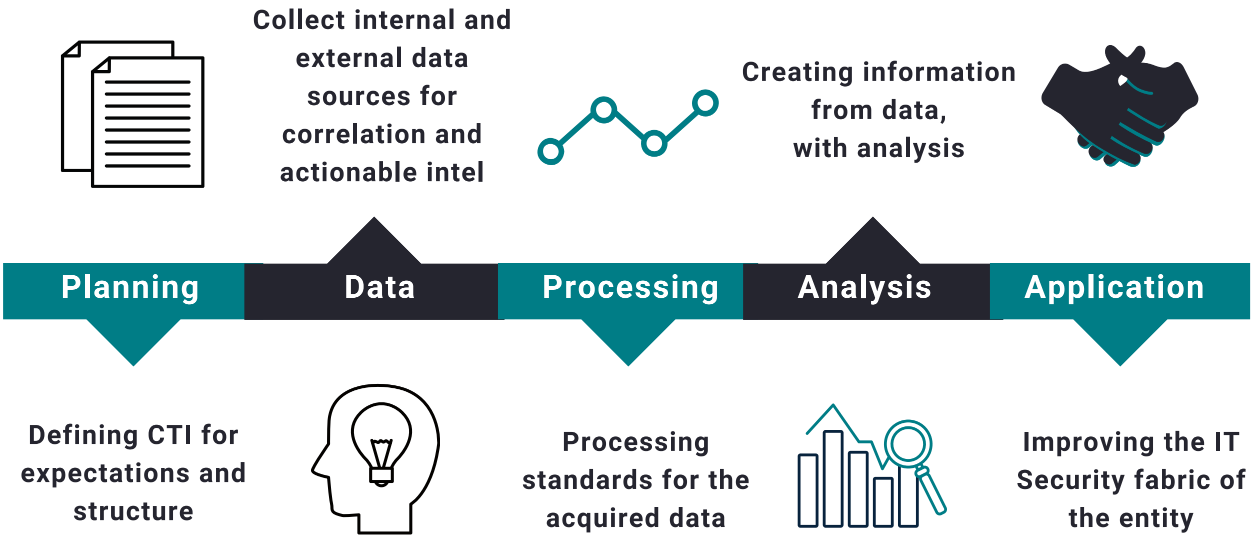
External Data Sources

These voluminous data sources are the second leg of CTI systems. Due to their nature, their reliability and relevance can be low, and they can be redundant. Also, processing this volume of data can tax hardware. These sources therefore should be chosen and vetted carefully. To obtain these data streams, CIM employs open Threat Intelligence streams, open government data, Social Media, and the Dark Web, as well as a closed, highly diversified honeypot network.

Open Threat Feeds are a critical part of CTI. They have curated feeds regarding threats and IOCs, such as IP addresses with a bad reputation, malware hashes, and C2 domains. Most of these IOCs are existing and valid threats. On the other hand, there are Information Sharing and Analysis Centers (ISACs), which are industry sector- and critical infrastructure-based information gathering and sharing member organizations. The ISAC lists are also curated and contain relevant data. One of the main sources of information is the Electricity Information Sharing and Analysis Center (E-ISAC) of the ICS/OT utility sector, which brings invaluable energy-specific intelligence, best practices, and case studies. The third, curated source is the governmental Open Data. This is collected by government sources, agencies (ICS-Computer Emergency Readiness Team (CERT); US-CERT, etc). Their data is also highly relevant and quantifiable.

These three curated sources contain IOCs regarding existing threats, but there are others lurking in the shadows. To shed light on them, the CTI uses other feeds, like Social Media and Dark Web crawlers. When these are filtered by analysts, they can be used to uncover future attacks. In addition, there is the Common Vulnerabilities and Exposures (CVE) database. CVE is an encyclopedic list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CIM scans through these databases and presents vulnerabilities relevant to the organization.

The protective mesh of CTI comes by combining internal and external data sources. While the internal sources answer the question "What happened?", the external sources are about what may happen next--the forecasts that enable any organization to prepare. By carefully mixing the two, we can proactively patch and harden a client's infrastructure, rendering it very difficult to penetrate.


Collect internal and external data sources for correlation and actionable intel
Creating information from data, with analysis
Planning
Data
Processing
Analysis
Application
Defining CTI for expectations and structure
Processing standards for the acquired data
Improving the IT Security fabric of the entity

Processing

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

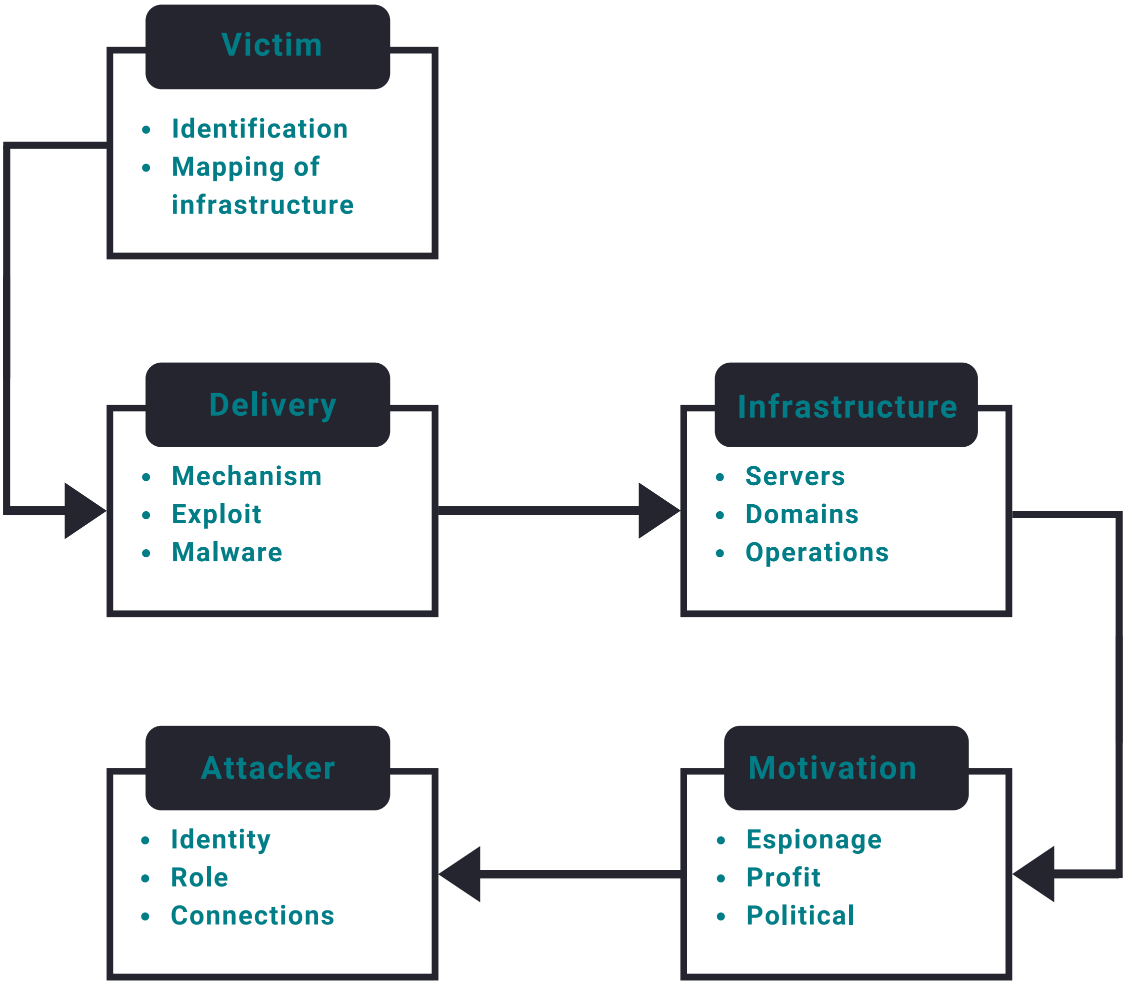
The validation process is about grouping and correlating the collected data, in order to find the missing pieces. After correlation, the fake and invalid data needs to be removed, in order to get actionable and trusted intelligence from the raw data. This information then will be indexed. Thanks to this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

Analysis

After processing, the database contains actionable, relevant intelligence. This data is now ready to help further harden the organizational infrastructure, which enhances the detection and response capabilities of the internal security systems.

The intel also provides viable information regarding possible future attack patterns, as well as helps to assess the real damage of past incidents. All of this is valuable for creating Early Warning systems and helps with IT Security-related strategic decision making.

CIM also sends the CVE database onto the internal network for recently uncovered vulnerabilities, and alerts users when patching or remediating is necessary. This system creates a previously unattainable situational awareness.



Application

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

SECTION 2

HOW THREAT MANAGEMENT FITS INTO YOUR ORGANIZATION'S SECURITY LIFECYCLE

Planning

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

Monitoring and Detection

Pulling in external, verified context on threat actors and their Tactics, Techniques, and Procedures (TTPs) eliminates the need for security analysts to research what is and isn’t malicious. Organizations can quickly identify whether or not 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

During an incident, CIM can help identify patterns and threat actors, in order to inform the next action, so organizations can remediate and respond more quickly. CIM can tell if a particular actor is known to use a specific tool or tactic during an incident, and can alert organizations when to investigate further.

Response and Remediation

During an incident, Cyber Intel Matrix 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 current security. CIM is useful for assessing where to improve because the team sits 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 an organization had the right information and how long it took to react. For example, if a malicious actor successfully infects a system, analysts 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 exploit easy-target organizations. Every organization benefits from understanding its vulnerabilities, staying ahead of threats, and remediating events quickly. Investigating all of these incidents can quickly overwhelm any security team, which is likely already stretched thin due to the cybersecurity workforce shortage. We can expect a global shortage of cybersecurity professionals in the short to mid-term, with 350,000 cybersecurity positions currently unfilled, and roughly 3.5 million predicted by 2021, according to Cyber Security Ventures.

CIM enables IT to focus on the real threats and vulnerabilities, saving time and resources with intelligence that really matters.

SECTION 3

CYBER INTEL MATRIX KEY BENEFITS

Operational Technology Threat Intelligence

Industrial Control Systems (ICS) owners and operators, as well as 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 various levels of an organization and informs them appropriately to maximize impact.
The intel comes in three main categories: Strategic, Tactical, and Operational.

- The **Strategic category** is for the security and organizational leadership, as it places threats into a business context and describes the strategic impact. Within an adversary’s background, intent, and motivation, 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, and data collection. The intel includes campaign history, end-to-end adversary operations, etc

As for ICS impact, threat intelligence may be categorized as the following:

1. Intelligence on 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 Supervisory Control and Data Acquisition (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 nature of 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 publicly, 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 of emulating complex infrastructures, in order to convince adversaries that they just found a huge industrial complex. To improve the deceptive capabilities, CIM also provides the option for a custom human-machine interface, to increase the honeypots attack surface. Also, the response time of the services can be artificially delayed, to mimic the behavior of a system under constant load.

Brand Monitoring

CIM allows its clients to monitor their brand and legal names on the open and Dark webs, social media sites, and other forums. Brand monitoring is a business analytics process that monitors various channels in order to gain insight about the company, brand, and anything explicitly connected to the business. Brand monitoring allows for Chief Information Security Officers (CISOs) and other C-Level executives to scan keywords and find out if there is any mention of them in underground or dark web forums, or if there is an unauthorized social media presence. Brand integrity is mission-critical for organizations, especially for those that maintain highly sensitive customer data.

Finding out about a whistleblower, or a smear campaign, before it occurs can be essential for building or maintaining advantages for a solid reputation.

Account takeover (ATO)

ATO is a type of identity theft where a Threat Actor gains unauthorized access to an account belonging to someone else. With CIM, organizations get a tool to scan the Dark or Open web for the company's email addresses, looking for breached accounts. Finding the CIM subscribed individual user information first may keep the entire company from unwanted consequences, and allows the user to take necessary steps to halt attacks.

There may be various reasons behind ATO 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. They also often include targeting the intellectual property of an organization. Because ATO attacks rely heavily on the reuse of credentials exposed in third-party data breaches, an effective defense involves detecting logins using previously compromised credentials.

Feeds into SIEM, SOAR, MISP and other Threat Hunting platforms

Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), Malware Information Sharing Platform and Threat Sharing (MISP)

Using the CIM API, the CISO’s team can take their own feed (adjusted to the organization's infrastructure) and integrate it into the SIEM system, adding intelligence to correlations. Clearing most false positives identified by the SIEM system relieves overworked security staff, and enables them to deal with alerts that are truly important and investigate real incidents. **APIs are available for popular SIEMs like IBM Qradar, Splunk and RSA.**

Malware Lab

CIM offers to load MS documents, PDFs, files, hashes, and URLs onto our Malware Lab where a client’s 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 generates a report on the findings. When possible, clients can get back the cleaned file, and alert the CIM community about the malicious component, for future reference. If the file is clean, it will get a CLEAN status in the list at the end of the examination.

Contact Us

Andras Patkai
Sales Director
andras.patkai@cyberintelmatrix.com
202-321-2099

Mate Schmid
CEO
mate.schmid@cyberintelmatrix.com
+36 70 432 1386

CYBER INTEL MATRIX