SEPTEMBER 2023

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

At more than six years old, CTA occupies a place familiar to many entrepreneurs. We're not the "shiny new thing" anymore, but we haven't reached a "steady state" either. We're not new, as six years arguably spans 20 percent of the cybersecurity industry's entire existence. Yet, we're hardly done growing and changing, because we are still discovering ways to make threat sharing more valuable and useful. Effective threat intelligence is challenging, and some of our initial assumptions about how it would work proved incorrect. Updating our business processes to reflect updated assumptions is the next step in CTA's evolution.

One assumption was that if we adopted a standard data format, the shared data would be, well, standardized. However, even though we rigorously enforce the use of the STIX 2.0 format, certain inputs within that structure can vary and still be valid. The resulting variations in spelling, capitalization, and hyphenation in kill chain phase names, for example, create inconsistencies in our shared data. Spelling may seem like a trivial issue, but it imposes analytic costs – for example, how do you know you have found all the variants of the name within the data set? Reducing the variation in submissions (asking members to adhere to a more specific format) and employing automation (automatically updating a submitted field to the correct format) will help address this problem. As we reduce inconsistencies, CTA's data becomes easier to use and even more valuable.

Another assumption was that cybersecurity providers would just know how to plug into CTA and make use of the shared intelligence to maximum value. While the industry has always engaged in sharing and cybersecurity companies ingest data from many different sources, CTA does not fit the standard data source mold. We are not an intelligence "feed," our data spans a wide range of indicator types along with varying amounts of context, and the sharing must be bidirectional. To help prospective members derive value from the Alliance more easily, we have taken steps such as developing a code repository for the basic scripts needed to send data to and receive data from CTA and using the concept of a "data journey" for evaluating our shared data. As we make it easier to join and be part of the CTA, we are steadily increasing our value proposition.

These examples reflect only a few of the ways we are making CTA more effective at achieving our mission – helping our members better protect their customers, supporting the disruption of malicious cyber activity, and increasing the security of the digital ecosystem. We've proven that cybersecurity companies can and will share threat intelligence through an organization like CTA. We've shown that we can foster community defense of cyberspace. Our model clearly works. But we can make it even better and that's exactly what we're doing.

Thanks to all our current members for your support as we continue to take on the hard problem of intelligence sharing. For any potential members, I invite you to join us in this effort. You won't want to miss out.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

CTA'S ENGAGEMENT IN THE CYBERSECURITY COMMUNITY

CTA is proud to sponsor the **Virus Bulletin Threat Intelligence Practitioners' Summit (TIPS)** in London, October 4th-6th, featuring how 'The Community Effect' enhances your cyber defense. More information is available here.

Join us at **CyberNextDC 2023** in Washington, D.C. on October 10th to hear government and industry experts discuss policy trends and initiatives, cyber threats, potential legislation, DEI, and more. Register here.

The **26th International AVAR Conference** is November 28th-December 1st. Join us in Dubai to hear talks around this year's 'Secure Ecosystem: Strategic, Pragmatic, Futuristic' theme. Register here.

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>10 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	40%
IP ADDRESS	15%
DOMAIN NAME	4%
URL	4%
NETWORK TRAFFIC	29%
FILE PROPERTIES	7%
HOST	1%

TOTAL EARLY SHARES

3-5
PER WEEK

900+

CTA Member Profile

MEMBER SPOTLIGHT: CHECK POINT

WHY IS INFORMATION SHARING IMPORTANT IN TODAY'S TURBULENT CYBERSECURITY ENVIRONMENT?

We're seeing cybercriminals sharing information among themselves on the newest hacking tools and vulnerabilities. This enables them to not only breach more organizations but also to do more damage and demand higher ransoms. It's critical for the cyber defenders to also share knowledge about what they are seeing and what the hackers are up to. By sharing information, we can gain insights from different technologies across verticals, customers, and geographies, leading to a more complete understanding of what is happening across the entire threat landscape.

WHAT DO YOU SEE AS THE MOST SIGNIFICANT EMERGING CYBERSECURITY CHALLENGES?

There are a couple of challenges we have observed. The most spoken about these days is the impact of AI. As AI becomes a tool for attackers, we will see an increase in the breadth and depth of attacks. There will be more personalized and tailored campaigns leveraging AI based social engineering, deep fakes. The attacks may grow in scale when operated by AI. In addition, when introducing new technologies, more attack vectors are raised and with AI there are many potential new challenges like the leakage of data through the usage of AI or attacks against the data or AI models. Due to the advancements and increased accessibility of this technology, even the most juvenile of hackers now have the capacity to create and spread attacks, quickly.

Second is the frequency of supply chain attacks, a technique that allows cybercriminals to access larger organizations by targeting smaller third-party providers. A lack of due diligence, coupled with the widening skills gap and the potential payoff for hackers, makes this route more and more appealing. Some supply chain attacks are using software zero-day vulnerabilities and we need to increase the vendor responsibility to improve the basic software hygiene. It is our aim to educate as many businesses as we can about the risks and ensure they evaluate their partners' security posture with the same scrutiny as their own.

The last one I would mention is the geopolitical situation and the emergence of state sponsored cyber-attack organizations that are well funded and structured. These professional organizations quickly adopt new methods and quickly escalate the cyber security landscape.

WHAT ARE THE CHALLENGES/BENEFITS OF AI IN CYBERSECURITY?

AI is a great tool to improve effectiveness and efficiencies in software. It will greatly improve the ability of defenders to develop better defenses, to automate operations (or make them autonomous) or to investigate and hunt cyber incidents. At the same time it helps attackers be more effective and efficient. It helps them develop more spear phishing and personalized attacks and it enables them to do that at scale.

In addition, more generally, AI is introducing change and will drive new methods to conduct the business. It was seen in history that new technologies and methods will typically open new frontiers for attacks. Some clearly expected ones include leveraging data leaked to large language models, attacking the AI models, and attacking data and systems quickly built to operate AI methods inside organizations.

All businesses need to level up their operation to use the great advancements that AI brings and at the same time, they will all need to be leveling up their approach to cybersecurity if they want to remain secure.

BY DR. DORIT DOR
CHIEF TECHNOLOGY OFFICER

CTA Member Feature

FOSTERING COMMUNITY DEFENSE

BY VAL SAENGPHAIBUL, DIRECTOR, FORTIGUARD LABS

As ransomware and other cybersecurity attacks continue to proliferate, cybercriminals and nation state attackers are leveraging increasingly advanced tactics, techniques, and procedures (TTPs) to pull off more damaging campaigns. Cybercrime is increasingly organized, with syndicates around the globe operating like enterprises. Nation state attacks operate with the backing of a hostile adversary and are professional-scale operations designed to fly under the radar.

One result of these ongoing attacks is that massive volumes of data are being collected and updated about said threat actors. However, this information is often disjointed and isolated. It usually remains within the jurisdiction of just a few companies and/or organizations. One of the keys to helping reduce and mitigate cyberthreats on a global scale is threat intelligence sharing. Organizations across the spectrum, both private and public, need to find a way to share this information in real time.

Access to the latest threat trends, intrusion activity, and criminal methodologies is invaluable when it comes to disrupting cybercrime. Without a more robust picture of the threat landscape, organizations can't fight effectively. For the private sector, especially, the idea of sharing information with competitive vendors may seem counterintuitive. However, the reality is that none of this information should exist in isolation and the focus should be about the greater good of the industry.

This is the premise of CTA. By enabling organizations to share threat intelligence more freely in real time, the members and customers of CTA members all benefit. When one member identifies new threats, the rest of the members are alerted before this information is made public.

This allows each member's teams to conduct internal analysis and create protections for their customers preemptively. As a group we can proactively prepare and come up with mitigation strategies in advance. As threats evolve and become more sophisticated, and as critical infrastructure becomes a bigger target for bad actors, this type of early warning is invaluable.

By providing an easier and quicker way to share and ingest threat intelligence, the CTA is helping foster community defense at a very critical time. Cybersecurity requires collective participation if we are going to defeat bad actors.

Having access to information sharing through CTA allows vendors to stop bad actors in their tracks – with the goal of disrupting cybercrime. And that's good for everyone – except the bad guys.

CTA STAFF UPDATES

CTA is proud to announce that Michael Daniel, CTA President & CEO, has once again been named a Washingtonian Tech Titan in the 2023 **Cyber World: INVENTORS, AGITATORS, AND DEFENDERS** category.

Congratulations, Michael!

The CTA team is pleased to welcome Chelsea Conrad, Cyber Threat Report Analyst, and Linda Beverly, Lead Threat Analyst, to CTA. Their work will be instrumental in furthering CTA's analytic capabilities and helping us demonstrate the collective power of CTA.

CHELSEA CONRAD
CYBER THREAT REPORT ANALYST

LINDA BEVERLY
LEAD THREAT ANALYST

CTA Member Feature

CYBERCRIMINALS ARE MORE ORGANIZED THAN EVER, AND WE MUST BE TOO

It should come as no surprise that we are up against a well-connected and organized cybercrime industry. The rise of 'as-a-service' offerings, such as malware-as-a-service, has lowered the barrier of entry for new threat actors with little operational knowledge or experience. Add the emergence of underground AI tools to the mix, enhancing the speed and frequency of new threats, and you have a recipe for disaster.

Cyber risk is growing, and so are the requirements from regulators. Take for example the 2022 update to ISO 27002 which includes 11 new controls, including the addition of threat intelligence control 5.7.

These requirements, as well as the potential business impact of a successful attack, has caught the attention of business leaders who are increasing budgets, and working more and more closely with security professionals to enhance existing security measures. Still, it may not be enough. Cybersecurity professionals must think beyond security tools alone, to match the sophistication of today's attacks.

Collaboration can be powerful

Global partnerships like CTA not only promote knowledge and information sharing, but establish a trusted community against cyber adversaries. Outpost24 has been an active contributor on CTA's exchange platform since joining in 2021. Our threat intelligence solution, Threat Compass, analyzes tens of thousands of malware samples on a daily basis, using CTA as a critical source of these malware investigations. For our customers, this translates to real-time retrieval of credentials obtained by malware.

Collaboration enables high-quality threat intelligence. New threats emerge every day, and there's more data than ever before. This means context has never been more important. We know we can't possibly block every single threat, but through collaboration, and a common language (STIX 2.0), we can minimize information overload, and mitigate the most likely threats.

BY VICTOR ACIN
OUTPOST24 LABS MANAGER

CTA Member Feature

FOSTERING COMMUNITY DEFENSE: TOGETHER WE CAN GO FURTHER

Despite the overwhelming challenges we still face in the world of cyber security, we have come a very long way since the early days of cyber security. Starting from those challenging early days at the turn of the century, when attackers were roaming around user systems and thwarting the industry, we are now much more aware and better equipped to fight back more effectively against attackers. This is thanks to the growing expertise and better technology, but, above all, thanks to a mature industry, which is much better prepared overall to combat the threats. What exactly does this improvement in the industry consist of?

One of the keys to having succeeded in raising the level of effectiveness in the industry is in fact mutual support. It is not possible to create a strong industry without the cooperation between the different personas, which leads to a strong community that supports each other. There is no point in fighting wars separately. A very positive thing in today's defense industry is the acknowledgment that collaborating as a community is an advantage and beneficial to all of us. Communicating knowledge, sharing information, partnering to work more efficiently, reporting new discoveries, or even admitting attacks with transparency. All of this is already part of the routine activities that the industry carries out without any complexes, thereby benefiting the rest of us. Thanks to this we can be successful and enjoy clear benchmarks.

Telefónica Tech clearly believes this and our contribution to CTA is a good example of this. Having a place to share information, contextualize it and contribute to improving the security of customers and, therefore, of the entire community, is something that has proven its effectiveness many times over, both to defend our customers' and our own infrastructure and devices.

This does not mean that such relationships will stop the problems, but it does mean that without such a community defense, the difficulty of keeping ourselves protected would be significantly greater by several orders of magnitude. Attackers have also evolved, they have collaborated with each other, and they have become sophisticated enough to pose a serious threat that we must keep fighting. But we have the tools to confront them, both technically and in terms of collective knowledge. After all, alone we can go faster, but together we can go further.

BY SERGIO DE LOS SANTOS
HEAD OF INNOVATION AND LABS

CTA Member Feature

SECUREBRAIN: ALIGNING WITH CTA

In February 2019, SecureBrain formalized our membership and joined forces with CTA with the intent to share cyber threat intelligence with top security vendors around the world. When it comes to cybersecurity, knowledge about up-and-coming cybersecurity threats is crucial. We at SecureBrain are dedicated to staying on top of global cybersecurity shifts.

At SecureBrain, we believe that sharing cyber threat intelligence is critical when developing and providing security solutions to our customers. Through our membership with CTA, we share cyber threat intelligence with many of the top security vendors across the globe and better help protect our customers against new cyber-attacks.

SecureBrain specializes in providing cybersecurity solutions designed to protect enterprises' web applications from cybercrime such as phishing and web hacking. We have built our own advanced security research center and have initiated multiple joint research projects to continuously innovate and develop cybersecurity solutions and software to protect against global cyber threats. To ensure that we provide the best protection to our customers, it is important for us at SecureBrain to be on top of global cybersecurity trends and threats and collaborate with the world's key cybersecurity players. Through our strategic decision to join CTA, we are eager to share information with top security vendors from across the globe.

Our partnership with CTA allows us to gain information about the latest cybersecurity trends across the world from top security vendors using a central intelligence depository. In turn, we aim to provide cybersecurity support to companies across Japan. Likewise, the partnership opens a conversation regarding the threats that are local to each country. Through this exchange of security intelligence, we believe our partnership fortifies the cybersecurity field.

Through our partnership with CTA, we are confident that we will grow more as a cybersecurity provider and look forward to continuing strengthening our partnership with CTA.

BY MOTO YAMAMURA
CO-FOUNDER AND COO/CTO

SANDS Lab

CTA Member Feature

STRENGTHENING COMMUNITY DEFENSE THROUGH CYBER THREAT INTELLIGENCE

THE IMPORTANCE OF CREATING THREAT INTELLIGENCE BASED ON OBJECTIVE FACTS, AND THE NECESSITY TO STRENGTHEN THE COMMUNITY'S CAPABILITIES ACCORDINGLY

Economic crises such as recession and inflation often trigger a surge in 'Subsistence crimes', which are crimes committed for survival, such as robbery, theft and fraud. For instance, during the foreign exchange crisis that hit Korea in the late 1990s, robbery and theft crimes soared by 58% compared to the past. Cases like this are foreshadowing that subsistence crimes may increase as the economic downturn worsens.

A survey by the Korea Internet & Security Agency (KISA) revealed that cyber attacks surged by over 40% year-on-year in the first half of 2023. Various issues, such as the war in Ukraine, along with inflation and economic recession, are fueling the activities of these cybercriminals.

As the digital world becomes an increasingly attractive target for criminals, the economic downturn exacerbates the cybercrime threat, since the scope of modern crime is expanding from the real world to the digital world. A sluggish economy may compel companies to cut back on their IT security spending, resulting in a shortage of skilled security personnel.

Such environmental changes and security vulnerabilities create opportunities for hackers, since they employ existing malware or automated tools and bots to launch large-scale attacks. Some recently even used artificial intelligence technology to automate attacks. In this situation, these sophisticated attacks are hard to counter with limited security manpower and resources.

Cyber threat intelligence (CTI) technology has been getting attention recently, since it helps to overcome this limitation by identifying various current threats and sharing this information with relevant organizations. This reduces unnecessary repetitive analysis and enables efficient response. Various CTI specialized companies leverage the expertise of professional threat analysts to deeply analyze the collected information, disclose and share the results in standardized formats such as STIX and IoC to widely spread response experience to others.

CTI, as well as all the other technology, is a double-edged sword. It can only serve as useful information when it is accurate and objective. Errors or biased information may lead to confusion and interfere with critical decisions. Experts' interpretations are based on their experiential knowledge, which may vary from one another. This makes it challenging to determine the optimal timing for response.

Let's take an example. Let's assume that Company A receives a document via email, and the document turned out to be a malicious file. Depending on whether the source is North Korea or China, response strategies and resources deployed may vary. Diplomatic warfare may even be necessary. Therefore, in these situations, accurate, objective, and flawless information must be the standard for judgment.

The cyber world is similar to a real battlefield. Numerous malicious codes are continuously being created, and in order for a company or organization to be protected, it is important to properly identify the threat and establish a long-term response strategy. Eventually, CTI serves as an important tool in this process.

The advancement of big data and artificial intelligence have enabled us to rapidly analyze and interpret vast amounts of data. However, its true value can only be demonstrated if it is based on accurate data without error or bias. Information exchange within the community of leading CTI companies in each country particularly requires accuracy and objectivity, and this should entail thorough verification, transparent technology, and the provision of sufficient evidence. Instead of relying on personal experience or know-how of individual analysts, objective facts derived from the traces of attackers in the files, code-blocks, the IP and domain information, and the malicious code detection through URL must be accompanied.

The value of CTI will rise further, provided that all the prerequisites are satisfied. Moreover, the importance of communities that share and provide relevant information will become more evident. A global response strategy based on this will lay the foundation for effectively tackling mass security threats in the era of artificial intelligence.

BY KIHONG KIM
CEO

K7 COMPUTING

CTA Member Feature

FOSTERING COMMUNITY DEFENSE

As we all know, Cybersecurity has evolved from being a predominantly technical field focused on safeguarding digital assets, to becoming a significant strategic issue of global relevance. At this scale it is essential to understand that no single organization can possibly know about and tackle all cyber threats independently. Community Defense offers stakeholders enhanced visibility of the threat landscape, and is a vital component in identifying, comprehending, and addressing cyber threats, thus better protecting users.

In recent years, Community Defense has evolved beyond the mere exchange of Indicators of Compromise (IOCs). The increase in complexity and sophistication of cyber threats, coupled with advancements in detection techniques, have resulted in the generation of a large volume of contextual meta data related to threat behavior and threat actor attributions. Even the IoC meta data from OSINT tools increases the value to a great extent and gives us researchers an understanding of the threat actor TTPs. However, although such a data feed is marketed as a plug-and-play feature, in reality it requires thorough vetting before it can be incorporated into a security product.

In practice Community Defense comes with a lot of challenges, one of which pertains to preserving the context of the IOC; similar to the misinterpretations of a game called 'Pass it On', the signal of the why and how of the IOC could be lost in communication. Another challenge is related to scraping the internet for IOCs, where the credibility of an IOC generated by a single source, is amplified when reported by multiple "copycat" sources. Even though Community Defense may sound like a cost-effective solution, it takes a good bit of effort, time, and skill to validate this feed and make it usable for real-time, real-world defenses. Data overload and false positives are a major issue with community feeds, and ensuring that the data remains current, relevant, and accurate takes a lot of time and resources. Fortunately, CTA's Magellan platform and early-share program help in addressing these issues. Of the industry, by the industry, for the industry.

Community exchange platforms will play an increasingly crucial role in correlating data, which will aid in protecting users and apprehending and prosecuting threat actors. The continuous feed of high-quality threat data will help all the stakeholders on a global scale. At present, most detection efforts are focused on developing rapid mitigation strategies for known common issues. However, with the aid of community threat intelligence and AI/ML technologies, we are moving towards generating nuanced mitigation techniques. I believe that community exchange platforms will play a vital role in this process as we move forward.

BY ARUN KUMAR S
TEAM LEAD—THREAT INTEL, K7 LABS