DECEMBER 2023

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

The theme for this quarter's newsletter, Bridging Borders Building Trust, concisely expresses CTA's purpose. Our role as an intelligence sharing organization is to enable relevant information to move across the boundaries that exists between cybersecurity providers. Of course, the task is not easy. If it were, then an organization like CTA wouldn't be needed to help facilitate it. So how does the CTA help build bridges? We make threat intelligence sharing scalable, sustainable, standardized, and reliable.

Many sharing relationships in the cybersecurity community are based on personal contacts. While those personal relationships help ensure trust, they are difficult to scale, limiting their reach. CTA scales sharing up to a broader set of recipients. It allows for sharing to occur in a one-to-many fashion, spreading intelligence to 35 members from 11 countries. CTA membership gives an organization access to a wide array of threat intelligence from many different sources that would be difficult to build on an ad hoc, individual basis. CTA's bridges connect many destinations.

We have all seen sharing initiatives spring up around a specific issue or threat, only to wither away over time. Those efforts usually rely on volunteer staff and donated infrastructure, which is why they tend to fade. Those bridges are useful, but they don't last. By having dedicated employees and permanent infrastructure, CTA's sharing model is sustainable. It can continue to operate as specific threats evolve and individuals change jobs. CTA's bridges are enduring.

Standardization enables distributed processes in many industries. However, CTA doesn't just encourage the use of standards for threat intelligence sharing, we enforce it. Members must use a standard format to share automated threat information with CTA. This policy requires members to make an upfront investment, but once achieved, this standardization makes it much easier to ingest and utilize threat intelligence, reducing the transactions costs often associated with sharing. CTA's bridges are consistent.

Finally, CTA makes information sharing more reliable. Our model requires members to stand behind the intelligence they share, because all IOCs and finished analysis remain associated with the submitting member. Members can trace the provenance of any shared intelligence and they know that other members have an incentive to carefully choose what they share. These factors allow members to more easily rely on intelligence shared through CTA. CTA's bridges are trustworthy.

Taken together, CTA's model reduces the friction associated with sharing activities. While we don't eliminate all the barriers to sharing, we reduce the cost and increase the benefits, making sharing easier and more cost effective. Further, any bridges built through CTA are here for the long-haul, because they can remain in place indefinitely. That's how CTA builds bridges and raises the level of cybersecurity across the digital ecosystem.

The rest of this newsletter highlights the way our members and partners contribute to building CTA's bridges. I hope you enjoy reading it and, if you are not already a member, that it prompts you to check us out more thoroughly. We always need more destinations for CTA's bridges.

J. Michael Daniel

J. Michael Daniel

President & CEO, Cyber Threat Alliance

CARO Workshop 2024

Driving Back the Shadows: Connecting Research to Action

CARO Workshop 2024 is the 17th annual conference event. CARO is focused on cybersecurity research and relevant cyber topics. CTA will host the 2024 workshop May 1st-3rd, 2024 in Arlington, VA.

Join us as we confront cyber threat research head-on. We will explore how groundbreaking research seamlessly integrates with actionable measures, shaping the future of our digital defenses. Dive into the intersection of research and practical solutions as we navigate the evolving threat landscape and challenges. The Call for Papers is **NOW OPEN!**

CYBER THREAT ALLIANCE

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>10 MILLION

MONTHLY AVERAGE

OBSERVABLE DIVERSITY

(AVERAGE)

FILE HASH	38%
IP ADDRESS	14%
DOMAIN NAME	5%
URL	5%
NETWORK TRAFFIC	27%
FILE PROPERTIES	8%
HOST	4%

TOTAL EARLY SHARES

3-5

PER WEEK

950+

RAPID7

CTA Member Profile

MEMBER SPOTLIGHT: RAPID7

WHY DID RAPID7 JOIN CTA?

We often hear terms such as “information sharing” used within the industry as a panacea for addressing the deluge of threats. However, in practice, doing so effectively and in a timely fashion can be challenging. CTA provides a platform to meet this challenge, supporting the sharing of indicators and knowledge between practitioners and serving as an important source of intelligence.

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

We know that threat actors routinely share information, and with the asymmetry of information benefiting them, defenders must do everything possible to tip the scales in the favor of the cybersecurity industry. Information sharing greatly helps the speed and accuracy of protection development for organizations that are being bombarded every minute with attempts to breach networks.

WHAT DOES RAPID7 VALUE MOST ABOUT CTA MEMBERSHIP?

We witnessed the broad impact of regulations on the cybersecurity industry when access to WHOIS data was restricted in response to GDPR, which resulted in incident investigations becoming more difficult. The opportunity to collaborate with industry partners to be more proactive and provide a singular, coherent voice on proposed regulation is imperative.

HOW DOES BEING PART OF CTA HELP RAPID7 PROVIDE GREATER SECURITY FOR CUSTOMERS?

The early visibility into community intelligence enables organizations to respond quickly to help roll out detections, and it provides more context into the activity of threat actors to assist with ongoing visibility.

WHAT VALUE DOES RAPID7 GAIN FROM PARTICIPATING IN THE VARIOUS WORKING GROUPS THAT FOCUS ON SPECIFIC THREAT CAMPAIGNS OR SPECIFIC EVENTS, LIKE THE OLYMPICS OR ELECTIONS?

Major world events often act as a lightning rod for all manner of threat activity. Take COVID, for example, where everything from phishing emails to more capable campaigns surfaced. We believe that collating related insights into actionable intelligence for all stakeholders is an imperative for preserving the integrity of business operations as well as events such as national elections.

HOW DO YOU SEE CTA FITTING INTO THE BROADER CYBERSECURITY LANDSCAPE MOVING FORWARD?

We believe that CTA has the potential for longevity through its ability to provide a coherent voice from the industry, as opposed to the smaller, more fragmented voices we have seen in the past.

WHAT ARE YOU MOST EXCITED ABOUT IN TERMS OF THE WORK YOU HAVE BEEN ABLE TO DO THROUGH CTA?

"Speaking from my own personal involvement," says Raj Samani, SVP and Chief Scientist, "I believe that some of the working groups have the opportunity to truly change not only cybersecurity as a whole but help inspire the next generation of practitioners."

WHAT DO YOU SEE AS THE MOST SIGNIFICANT EMERGING CYBERSECURITY CHALLENGES AND HOW CAN CTA HELP MITIGATE THESE CONCERNS?

We are witnessing more rapid exploitation of previously unidentified vulnerabilities from threat groups that historically have not demonstrated this level of capability. Are they getting better, or getting help? Either way, this is certainly presenting a challenge that will have to be met with information sharing.

WHERE DO YOU SEE CTA IN 5 YEARS?

Hopefully with many more members and building on the already impressive body of excellent deliverables.

CTA Member Feature

LOCAL THREAT INTEL HAS A GLOBAL IMPACT

CUJO AI

CUJO AI protects billions of devices across tens of millions of home networks, and actionable, high-quality, and timely threat intelligence is very important when tracking malicious actors and their campaigns. Working with finite resources and talent, we have to focus on information which can be efficiently transformed into insights and allow us to eventually disrupt and prevent attacks. That is why active feedback between trusted information sharing partners is so important. CTA provides the environment for this with automated IoC exchange, quality controls, and recurring meetings between the Alliance’s experts from different fields, ranging from government to consumer cybersecurity. At the same time, the CTA benefits from active feedback about the quality and usefulness of IoC information that is made available.

Local issues, such as compromised IoT devices, can have a global impact on the safety and functionality of the Internet. A good recent example is the Killnet group, which has been using compromised consumer devices to target governments and organizations in multiple countries, causing damage globally. Tracking its operations and infrastructure requires a lot of active intelligence sharing. When done right, it allows different organizations, including CUJO AI, to add context to such malicious activities, and improve their countermeasures. Eventually, disruptive actions can be taken against such groups, e.g., by detecting and isolating residential proxy nodes used in the attacks to relay attack traffic from the less trusted networks. For these disruptive actions to have a lasting impact, they need to be coordinated across cybersecurity companies, governments, and law enforcement. No single cybersecurity organization can do this alone. It is good to see how CTA is active in this front, and, as a member of the CTA, CUJO AI sees a lot of value in contributing both local and global cybersecurity insights from real-world consumer networks.

BY KIMMO KASSLIN
VP OF RESEARCH LABORATORIES
CUJO AI

THE ART OF POSSIBLE

RSAConference™2024

San Francisco | May 6 – 9 | Moscone Center

CTA is proud to be an Association sponsor for RSAC 2024. Join us May 6th-9th at RSAC 2024, the ultimate cybersecurity destination. Immerse yourself in expert-led sessions, connect with industry leaders, and discover the latest trends and best practices. Elevate your cybersecurity game and be a part of shaping the industry's future. Don't miss this opportunity to advance your skills and network with the best in the field.

Register here to get a $150 discount off the full conference price.

Mark your calendars for Tuesday, May 7th when CTA will hold a member and partner reception. RSAC is the world’s leading and largest cybersecurity conference. We hope to see you there!

CTA Member Feature

BRIDGING BORDERS AND BUILDING TRUST

In the ever-evolving landscape of cybersecurity, the battle against cyber threats is a collective effort. One of the key pillars of this joint defense is the exchange of threat intelligence. The importance of sharing information promptly cannot be overstated in the relentless fight against cyber adversaries. Cyber threats know no borders. They transcend geographical boundaries and target organizations indiscriminately. In such an interconnected world, the need for international and cross-organizational cooperation is paramount. Threat intelligence sharing allows security professionals, whether they are in the public or private sector, to collaborate across borders and develop a united front against malicious actors.

By sharing information about threats and vulnerabilities promptly, organizations can collectively develop more effective strategies for detecting, mitigating, and preventing cyberattacks and do it much quicker to prevent or minimize further related damage. This process is pivotal in safeguarding not just individual organizations but the digital realm as a whole.

This important effort often conflicts with the competitive nature of the cybersecurity market. As a result, some companies, rather than promptly disclosing information about new threats, choose to stash malware samples and vulnerabilities to gain a competitive advantage. This practice not only undermines the principles of trust and collaboration but also puts the entire cybersecurity community at risk. When organizations withhold crucial threat data, they prevent others from defending themselves effectively and contribute to a more vulnerable digital ecosystem. The repercussions of hoarding threat intelligence are far-reaching. Delayed or restricted information sharing hampers the ability to respond swiftly to new threats, potentially causing more widespread damage.

Furthermore, it fosters an atmosphere of distrust among cybersecurity professionals and organizations, undermining the very foundation of collective defense.

To combat this destructive practice, the cybersecurity community must emphasize the importance of prompt and open threat intelligence sharing. Companies should properly balance collaboration and competition when it comes to cybersecurity. It is perfectly fine to get well-deserved fame and attention for disclosing and investigating the attack, but barring others from joining the investigation along the way has more drawbacks than benefits for the community as a whole. The benefits of sharing threat data far outweigh any short-term competitive advantages here. By working together to build trust and share threat intelligence, we can form a united front against cyber threats and ensure a safer digital future for all.

BY ALEXEY KLEYMENOV
THREAT INTELLIGENCE MANAGER
NOZOMI NETWORKS

CTA Partner Feature

BRIDGING THE INFORMATION SHARING COMMUNITIES

I think most people would agree that Information sharing and collaboration to improve security and resilience in our organizations is a good idea. We could talk for hours about the challenges we have sharing and collaborating *within* our own communities, but how are we doing when it comes to sharing and collaborating *between* the communities?

In 2020, much of the sharing between ISACs was done via emails and conference calls – but it all relied on the valiant efforts of individual analysts who had the wherewithal to share with other ISACs. That year, Health-ISAC began a grassroots effort to improve inter-ISAC sharing. In 2020, most of the ISACs were using Cyware's Situational Awareness Platform (CSAP) as part of their internal operations. Health-ISAC worked with Cyware to create an ISAC-to-ISAC sharing platform. The goal was to:

- Leverage industry standards, such as STIX and TAXII
- Promote effective and efficient sharing
- Encourage Machine-to-Machine Sharing
- Create an environment for analysts' collaboration
- Provide a vendor-neutral solution

Working with Cyware, we created ATLAS with the primary benefit of ISAC-to-ISAC sharing through the click of a button. Information could be brought into the ISAC platform in draft status with all fields pre-populated, allowing the analyst to optionally add or update content and publish it to their ISAC community. ATLAS speeds up analyst productivity and introduces fewer errors – enabling ISAC-to-ISAC sharing without relying on copy and paste, which we've been doing for over 20 years.

Today, ATLAS is used by more than 20 organizations-- a dozen ISACs, several ISAOs and several international CERT teams. Analysts can share content, make it available to all ISACs (and ISAOs), and import that information easily into their own platform. The solution is vendor neutral – ATLAS can be used through an API for organizations not using CSAP. ATLAS also supports collaborative use cases including analyst Requests for Information (RFIs), Secure Chat, an analyst contact directory, a shared calendar and more.

We're a few years and still early into this journey. ATLAS has improved the level of collaboration and sharing. We're challenging each other to share meaningful information, but we've still got a long way to go. If we lead by example, other ISACs (and their member communities) will benefit from what's being shared and we'll develop a level of trust amongst the participants. I'm confident that through our collective leadership and trust, we will inspire people to share more through ATLAS.

Finally, we're very grateful to the team at Cyware for donating the ATLAS environment to the ISAC community.

To learn more or to participate in ATLAS, please contact Health-ISAC or email contact@h-isac.org.

BY ERROL WEISS
CHIEF SECURITY OFFICER
HEALTH-ISAC