MARCH 2025

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

For the past eight years, the Cyber Threat Alliance has worked to make the digital ecosystem safer. This work is not easy. We operate in an area of cybersecurity where competition typically reigns supreme and cooperation is often perceived as counter to a company's business interests. When it was founded as an independent non-profit in January 2017, it was certainly not a given that CTA would succeed.

Yet, here we are in 2025. We have grown from our initial six founding members to over thirty companies from 11 countries around the world. We have diversified the technical threat intelligence we share to more than 40 different observable types and members can share finished intelligence products under embargo prior to general publication. As an alliance, we publish joint analytic reports on topics of mutual interest, such as cyber threats to nongovernmental organizations and adversary use of generative AI tools. CTA sponsors a track at the Virus Bulletin conference, and it will hold its own inaugural conference in May of 2025. CTA conducts webinars, maintains a blog, and produces a quarterly newsletter. The list goes on.

Of course, we are still learning and evolving. Some of the evolution is driven by changes in technology (the emergence of AI), some by changes in the threat landscape (ransomware was just beginning to be a serious threat in 2017), and others by changes in the geopolitical environment (Russia's invasion of Ukraine). The other key evolutionary driver is the needs of our members. CTA always strives to make our intelligence sharing better, more effective, and more useful to our members. For example, we are transitioning to a new sharing format (STIX 2.1), adding capabilities to our automated platform (accepting detection rules in addition to observables), and reviewing how we assign point values to shared intelligence.

I want to thank our members, whether you have been with us since the beginning or have recently joined us on our journey. You have invested heavily in this ongoing experiment, and we appreciate that support. We look forward to continuing to evolve and grow with you as we pursue our mission. For those of you who haven't yet joined the Alliance, you will always be welcome.

CTA has shown that fierce competitors can cooperate in threat intelligence sharing and still compete in the marketplace. It turns out that cybersecurity competition and cooperation is not an either/or proposition. It's a both/and. A harder path to take? Of course. But ultimately worth it? Definitely.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

WELCOME TO THE CTA TEAM

CTA is excited to onboard two new staff to help drive our mission forward in 2025. We are looking forward to their contributions to CTA.

Jason Cooper

Chief Data Sharing Officer

Jason Cooper will be joining CTA as our new Chief Data Sharing Officer and will be responsible for CTA's analysis and sharing technology portfolio.

Jason will be bringing to CTA years of cybersecurity executive experience with several large corporations. He has deep experience in security strategy, risk and threat management, incident response, and performance management. Jason brings extensive experience with government and law enforcement collaboration.

Emerson Johnston

Cyber Threat Report Analyst

Emerson Johnston is our new Cyber Threat Report Analyst and will be responsible for our Joint Analytic Report (JAR) program.

Emerson will soon graduate in International Policy with a specialization in cyber policy and security from Stanford. She has experience with cyber research working with the Atlantic Council and Hoover Institution, as well as experience with cyber partnerships. Emerson also served in the U.S. Army Reserve as a Civil Affairs Specialist.

CYBER THREAT ALLIANCE

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>12.5 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	48%
IP ADDRESS	15%
DOMAIN NAME	7%
URL	8%
NETWORK TRAFFIC	9%
FILE PROPERTIES	8%
HOST	5%

TOTAL EARLY SHARES

3-5
PER WEEK

1,200+

CTA Member Profile

MEMBER SPOTLIGHT: GEN

WHY DID GEN JOIN CTA?

Gen has joined the Cyber Threat Alliance to enhance our telemetry and protection capabilities through new feeds and Indicators of Compromise (IoCs). By being part of CTA, we can leverage the collective intelligence of the alliance to better understand and mitigate emerging threats. This collaboration allows us to stay ahead of cybercriminals and provide our customers with the highest level of security.

HOW DOES MEMBERSHIP IN CTA HELP GEN PROVIDE GREATER SECURITY FOR CUSTOMERS?

Membership in CTA affords Gen access to valuable intelligence from other partners. CTA also facilitates information sharing on new threats, collaborative efforts on campaigns, and engagement with other industry vendors. This collective approach helps us make cyberspace safer for everyone, aligning with our company's mission.

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

CTA plays a crucial role in the broader cybersecurity landscape by providing expert guidance and driving policy changes to improve security postures. The alliance offers support during challenging times, such as the Cyber Defense Assistance Collaboration (CDAC) and the ongoing conflict in Ukraine. By fostering collaboration and information sharing, CTA helps the cybersecurity community address complex threats more effectively.

WHAT VALUE DO YOU GET OUT OF THE CTA?

Gen derives substantial value from CTA's Threat Intelligence feeds, which encompass not only Indications of Compromise (IoCs) but also labels that are rapidly gaining prominence. Our participation in the CTA community facilitates knowledge sharing, conference participation, and collaborative report development. For instance, we recently contributed to a joint report on artificial intelligence (AI), offering valuable insights into the application of AI in the field of cybersecurity.

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

The cybersecurity landscape is vast and constantly evolving, encompassing a wide range of platforms and attack types. Organizations require a comprehensive view of the threat landscape, as each entity only observes a portion of the situation through their own telemetry. Information sharing is paramount for comprehending the issue in its entirety and addressing it effectively. By collaborating to share intelligence, we can collectively enhance our defenses and respond to threats more efficiently.

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

One of the most exciting aspects of our work through CTA is the ability to understand what other vendors are observing and compare notes. Each vendor represents different user groups and attack methods, providing a diverse perspective on the threat landscape. This collaboration helps us stay informed about how attackers are using technologies like GenAI in their attacks and how advancements in technology are driving scams, misinformation, and other social engineering attacks.

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

Participation in CTA's Working Groups provides Gen with valuable insights into specific threat campaigns and events. For instance, during the GenAI discussions, we gained knowledge about the various ways attackers are leveraging AI in their operations. This knowledge helps us develop more effective countermeasures and stay ahead of emerging threats. Additionally, collaborating with other vendors in these groups fosters a collaborative environment where we can share best practices and strategies.

WHAT DOES GEN VALUE MOST ABOUT CTA MEMBERSHIP?

Gen values its membership in the CTA community, where we can share information and collaborate to enhance cybersecurity. The collaborative nature of CTA allows us to contribute to joint efforts, learn from other experts, and collectively address the challenges posed by cyber threats. This sense of community and shared purpose is what we value most about our membership.

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

Some of the most significant emerging cybersecurity challenges include human-centric attacks such as scams and phishing, which are often connected to financial fraud. The misuse of AI for malicious purposes is also a growing concern. It is our prediction that attackers will continue to leverage automated, AI-powered systems such as OpenAI Operator. CTA can help mitigate these concerns by facilitating information sharing, providing guidance on best practices, and fostering collaboration among industry stakeholders.

WHERE DO YOU SEE CTA 5 YEARS FROM NOW?

By staying adaptable and responsive to the evolving threat landscape, CTA will continue to play a crucial role in enhancing global cybersecurity.

ANYTHING ELSE YOU WOULD LIKE TO ADD?

We are proud to be part of the CTA community and look forward to continuing our collaboration to make cyberspace safer for everyone. The collective efforts of CTA members are essential in addressing the complex and ever-changing cybersecurity landscape. Together, we can achieve more and provide better protection for our users.

JOIN, LEARN, & SAVE. CTA MEMBERS ENJOY $150 OFF RSAC 2025 CONFERENCE.

RSAC 2025 brings together passionate thinkers, innovators, and problem-solvers from Apr. 28 – May 1 in San Francisco. Together, we'll break new ground, sharpen our skills, and push the boundaries of what's possible in cybersecurity. Register by March 28 to save $600 on a Full Conference Pass! Plus, Cyber Threat Alliance members can unlock additional savings of $150 by using code 1U5CTAFD. Secure your spot.

CTA and Nonprofit Cyber organizations are again hosting a happy hour reception during RSAC 2025. Join us for nibbles and drinks and chat with the Nonprofits that are impacting the foundation of our internet security, policy, privacy, and safety on Tuesday, April 29th at 6-7 PM in Esplanade 153 Moscone South.

Many Voices.
One Community.

RSAConference2025
San Francisco | April 28 – May 1 | Moscone Center

CTA Member Feature

STANDING TOGETHER FOR 8 YEARS

PROMOTING COOPERATION AND COLLABORATION

96 percent of software leverages open source software in some manner. Most of us use many different software products on any given work day, all of which likely have multiple open source dependencies. The maintainers of these dependencies are not compensated, vetted, or required to push updates at any frequency. Given the pace at which the world works and the general lack of any sort of legislation or other regulations on a software developer's third party audit process, it's likely that a few open source dependencies escape inspection. While most of the world carries about business as usual, threat actors have noticed this crack in the system.

ReversingLabs open source software threat research team actively scans popular third party software repositories for emerging threats. To those unfamiliar with the space, the volume of would-be malware existing in these open source libraries is shocking. For your run-of-the-mill script kiddie, typosquatting or impersonation of trusted authors or libraries are among options. More sophisticated threat actors may compromise an existing open source library and hijack the trust its users place in it to push malicious code, as was the case with popular AI library Ultralytics. This is just one example of the many compromised libraries identified on a daily basis.

This kind of research is difficult to scale and the identification of emerging and novel threats tends to require some level of human intervention. There aren't enough threat researchers in the world to go over each commit to an open source library with a fine tooth comb for lurking malicious code, but in the interest of trying, security vendors must band together. By pooling knowledge and sharing threat intelligence, vendors can ease the strain of resource limitation.

The whack-a-mole game of defenders is ever evolving. Over the years, Cyber Threat Alliance's membership has expanded to encompass many different facets of the security world. Not only has CTA curated an information sharing pool spanning diverse inputs and perspectives, but they have also worked to standardize and maximize the usefulness of this data.

BY ASHLEE BENGE
DIRECTOR
THREAT INTELLIGENCE

CTA Member Feature

STANDING TOGETHER FOR 8 YEARS

There is, it seems, an unending set of circumstances to divide "Us" from the dreaded "Them." There are the obstacles that have seemingly always existed: organizational boundaries and bureaucracy, silos, geography and time zones. Increasingly, there are walls appearing that divide us at home, at work, and in our communities. However, we need not be defined by what divides us.

Having the opportunity to reflect on an unlikely non-profit that came into being as a group of fierce competitors that found a way to come together as a force for good on the world's cybersecurity stage, then, is a blessing. It is a time to remember key allies and partners who charted the course that led to this point. It's a time to think about the innovations and successes and even the struggles and disagreements we've gone through together. But, most of all, it's an opportunity to appreciate the impact and scope of the Cyber Threat Alliance.

To take just one key factor that has led to the CTA's success, I'd say it is collective visibility. It is an unfortunate truth that you can only collect telemetry and other information where your sensors are. Every vendor has a unique cross-sectional view of the world, and we strive to do amazing things based on that view. Being a CTA member comes with an obligation to provide intelligence to a common pool that members can access. This common pool becomes a source of intelligence and visibility that members wouldn't necessarily have access to.

This visibility also comes in the form of preshares—a good faith effort for all CTA members to share copies of forthcoming reports amongst our group before they are published. This allows us to build protections early, before the research is made public, giving us a collective edge against the bad guys. Frequently, this is also an opportunity to talk to the analysts behind that research, which can be incredibly useful to fully understand the threat.

The final benefit of working with the CTA is the collective vision that only comes with regularly discussing problems in your field with likeminded experts. From these discussions have come national policy recommendations, guidance on emerging threats and an opportunity to understand problems that other smart people believe are worth giving time to.

The CTA is a reminder that the big-tent approach to problem solving still holds value. It reinforces the idea that the "They" isn't nearly as important as the "Us," and that even in the midst of perceived differences, we all share some collective goals in keeping people and organizations safe and doing the right thing. Most importantly, it demonstrates that just while there can be substantial obstacles to working together, those obstacles can – and in some cases must – be overcome.

Cisco is proud of its work with the Cyber Threat Alliance, and we're grateful for the partnerships we've experienced, the friends we have made and the victories we've shared. Here's to many more years of effective collaboration.

BY MATT OLNEY
DIRECTOR OF TALOS THREAT
INTELLIGENCE AND INTERDICTION

RETAIL & HOSPITALITY ISAC

CTA Partner Feature

THE POWER OF COMMUNITY

In a time where information is more abundant than ever, the ability to effectively share and process it has become crucial. Whether in business, cybersecurity, or daily life, communities play a fundamental role in ensuring knowledge is distributed, refined, and applied effectively. The strength of a community lies in its ability to bring together different perspectives, add another piece to the puzzle, and share expertise to create a collective intelligence that benefits all members.

One of the greatest advantages of a community is the pooling of knowledge. This is where the value of collaborative communities like Cyber Threat Alliance (CTA) and ISACs really shine. We see this almost daily at the Retail & Hospitality ISAC (RH-ISAC), where the sharing of one piece of information creates a ripple effect that culminates in information that can help secure an entire sector. Threats evolve rapidly, and staying ahead requires the pooling of real-time intelligence sharing.

In critical times, the value of collaboration becomes most apparent. In these moments, information-sharing communities enable faster and more effective responses. Through strong networks, our members can leverage trusted relationships to navigate challenges and find solutions quickly.

Fostering a strong and effective information-sharing community requires active participation, trust, and a commitment to collaboration. Organizations and individuals must be willing to contribute their insights, share their challenges, and work together toward common goals. The more openly members engage with one another, the more valuable the community becomes for everyone involved. Everyone has a place at the table, and everyone has the ability to provide that one missing puzzle piece.

The power of community in information sharing cannot be overstated. Collective intelligence enables faster problem-solving, stronger defenses, and greater innovation. By fostering environments of trust, participation, and collaboration, we can build networks that not only strengthen individuals and organizations but also contribute to the resilience and success of entire sectors and, in the case of CTA, our country. The future of information sharing relies on our ability to work together—because together, we are stronger.

BY SUZIE SQUIER
PRESIDENT
RH-ISAC

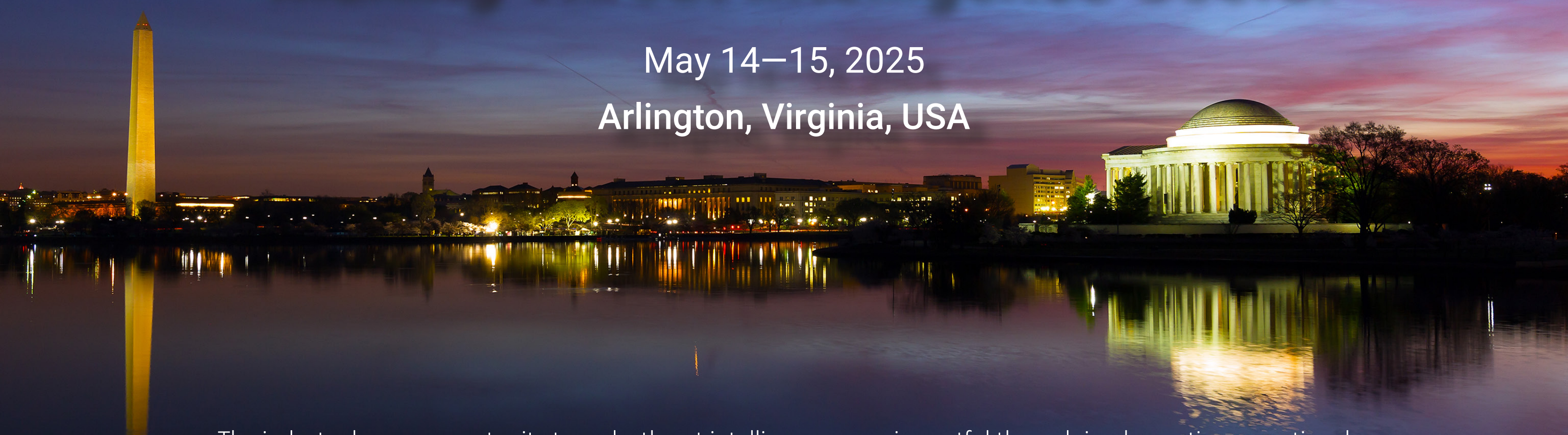
REGISTER NOW FOR TIPS 2025!

THREAT INTELLIGENCE PRACTITIONERS' SUMMIT CONFERENCE

Breaking Through the Barrier: Making Threat Intelligence Useful

May 14—15, 2025

Arlington, Virginia, USA



The industry has an opportunity to make threat intelligence more impactful through implementing operational improvements. Most threat intelligence goes to waste. Threat reports are often not written well for their intended audience because they don't answer the questions people have or they don't explain what actions to take in response to the threat. The TIPS Conference will explore how to change this dynamic and make threat intelligence more useful. Participants will explore cutting-edge strategies, innovative approaches, and the latest developments in the practice of cyber threat intelligence. Join us as we transform cyber threat intelligence into a powerful tool for everyone in cyberspace.

More details are available here on our website.

Contact CTA for sponsorship opportunities.