JUNE 2025

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

The US is about to undertake an experiment. What happens when a national government decides to disinvest in cybersecurity? While we have plenty of examples of countries and organizations not investing enough in cybersecurity, we have not seen a country or organization that has deliberately decided to reduce its investment in cybersecurity over the past 20 years. This reduction in capacity at the Federal level in the US will pose challenges across an array of organizations and for the cybersecurity industry and its effects will take years to play out.

In light of these reductions, how should the cybersecurity industry respond? This quarter's newsletter showcases some of the ways that industry can fill the gap left by the US government. Our them is by taking collective responsibility, the idea that all of us bear some responsibility for everyone's security in a networked world. We cannot escape being connected (sometimes even when we WANT to disconnect), and our on-line actions affect far more than ourselves. As a result, collective responsibility is more than just a nice, aspirational phrase; the concept should guide how the cybersecurity industry operates.

Fortunately, the industry has a long history of operating under the concept of collective responsibility. In particular, CTA's members and partners showcase the power of collective responsibility on a daily basis, whether through our automated sharing program, the early sharing of finished intelligence, or the collaboration on joint analytic reports. In this issue, Minsait Indra highlights the need for collaboration in Mexico, SANDs Lab talks about how to improve the quality of threat intelligence through collective action, and Tinexta Cyber discusses how working together accelerates innovation. The newsletter profiles CUJO AI and how it benefits from membership in a larger group. As these stories demonstrate, when we work together, we can meet challenges that no one company or NGO could meet on its own.

From my perspective, the reductions in US government cybersecurity capabilities will increase our cyber risk and reduce our resilience. However, that's not the end of the story. The private sector now has a responsibility to fill as much of the gap as it can. CTA will strive to do just that and continue to embody the concept of collective responsibility. If you are already a member, thank you for being part of this effort. If not, come join us on this journey. We all have a part to play.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

WELCOME TO THE CTA BOARD OF DIRECTORS

We're excited to welcome several distinguished leaders to the CTA Board of Directors. Joining as newly-elected Affiliate-member board directors are **Mounir Hahad**, Head of Juniper Threat Labs and Cloud Security Engineering at Juniper Networks, and **Raj Samani**, Senior Vice President and Chief Scientist at Rapid7. We also welcome **Nataly Kremer**, Chief Product Officer at Check Point Software Technologies, and **Matt Olney**, Director of Talos Threat Intelligence and Interdiction at Cisco, as newly appointed CTA Charter-member directors.

They join our current Charter-member board directors **Derek Manky**, Chief Security Strategist and Global VP of Threat Intelligence at Fortinet, and **Michael Sikorski**, VP & CTO of Unit 42 at Palo Alto Networks, along with elected Affiliate members **Jaya Baloo**, Stealth Startup, and **Joe Chen**, Operating Partner at Crosspoint Capital Partners.

The CTA Board plays a vital role in guiding our mission to enhance global cybersecurity by promoting collaboration and the exchange of cyber threat intelligence across our member community.

Mounir Hahad
Juniper Networks

Raj Samani
Rapid7

Nataly Kremer
Check Point

Matt Olney
Cisco Talos

CYBER THREAT ALLIANCE

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>13.6 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	46%
IP ADDRESS	19%
DOMAIN NAME	7%
URL	5%
NETWORK TRAFFIC	15%
FILE PROPERTIES	5%
HOST	3%

TOTAL EARLY SHARES

3-5
PER WEEK

1,250+

CTA Member Feature

COLLECTIVE RESPONSIBILITY: UNIFYING INDUSTRY EFFORTS AGAINST CYBERCRIME

Today's digital world is becoming increasingly complex, as companies adopt new technologies while facing ever more sophisticated threats from cyber attackers.

Cybercrime has grown into a complex ecosystem made up of organized cartels, state-backed hackers, and mercenary groups. The expanding attack surface driven by hybrid and cloud IT environments, the rise of AI platforms, and the tightly connected nature of modern supply chains gives cybercriminals more opportunities than ever to exploit digital blind spots and hidden vulnerabilities.

We're dealing with highly sophisticated operations- organized crime rings, nation-state hackers, and cyber mercenaries. These groups collaborate, share tools, and constantly adapt. What was once just a buzzword, 'collective defense', has become a real-world necessity. It means businesses, government agencies, and even competitors must join forces to defend against a common and growing threat.

Take this example: when a threat actor starts exploiting a vulnerability, like a zero-day in a widely used VPN, organizations with early visibility can raise the alarm and share Indicators of Compromise (IoCs) with others. Everyone benefits from that kind of collaboration. This kind of intelligence sharing happens on platforms like the Cyber Threat Alliance, where we contribute technical reports, attack analyses, and behavioral insights to help others respond faster and more effectively.

Collective defense also powers innovation. When organizations come together, they don't just share, they build the best defense in the world. Cross-industry partnerships have led to the development of advanced AI-powered threat detection systems, capable of spotting anomalies in cloud-native environments or detecting suspicious lateral movement inside networks. The latest case is the collaboration 'Rosetta Stone' where industry powerhouses are developing a conjunct naming convention for threat actors, a much needed and highly anticipated proof of solidity.

This collaboration also incentives innovation, accelerating the development and implementation of cutting-edge technologies, such as AI-driven threat detection and machine learning models tailored to identify anomalies in cloud and interconnected environments. At the technical core of collective defense lies the rapid exchange of threat intelligence.

Ultimately, a company's strategic goals must be deliberately and structurally aligned with its cybersecurity priorities. This isn't a side consideration, it's foundational. When security isn't embedded into strategic planning, it risks being underfunded or deprioritized, leaving critical blind spots that sophisticated threat actors can exploit. In this context, collaboration and shared responsibility aren't just helpful, they're essential to success.

BY LUIGI MARTIRE
CYBER THREAT INTELLIGENCE &
RESEARCH LEADER

CTA Member Feature

LEARNING TOGETHER: EVOLVING BEYOND ONE-WAY THREAT INTELLIGENCE SHARING

Cyber threat intelligence (CTI) sharing has become a critical foundation for collective cyber defense. Alliances like CTA facilitate real-time information exchange across industries and borders, enabling faster detection, broader visibility, and more coordinated responses. As the scale and sophistication of threat actors grow, so too must the quality and structure of our collaborative defenses.

However, the expansion of intelligence sharing frameworks also brings new challenges — most notably, the issue of data utility and trustworthiness. In practice, organizations often encounter high volumes of threat data that lack sufficient context or verification. IOC feeds, extracted without analytical backing or filtered through automated pipelines, can generate excessive noise. This overload not only consumes the recipient's resources but may also delay their response to actual threats. Over time, indiscriminate sharing diminishes the credibility of the CTI ecosystem as a whole.

To address this, we must rethink how we share, validate, and utilize threat intelligence. First, shared indicators should be accompanied by supporting evidence — such as behavioral traces, packet captures, or sandbox analysis results — which allow recipients to evaluate the origin, severity, and relevance of the threat. Raw data alone, without context, is often insufficient to drive meaningful detection or mitigation.

Second, we need to introduce metadata that reflects cross-organizational observations. Intelligence that is corroborated across multiple entities carries inherently higher confidence and can help prioritize response actions. Sharing this kind of observational metadata, such as frequency, distribution, and environmental impact, provides valuable insight into a threat's operational footprint.

Third, we need a well-defined feedback loop that tracks how shared intelligence is consumed and utilized. Was the data used to generate a detection rule? Did it inform a broader campaign analysis? Was it re-shared, enriched, or correlated with other intelligence? Establishing visibility into downstream usage transforms sharing into a two-way learning process and encourages more thoughtful contributions. Moreover, this transparency enables a shift from quantity-based scoring models to ones that reward impactful, high-quality contributions.

At SANDS Lab, we believe that threat intelligence must be verifiable, analyzable, and actionable. Only then can we build a cyber defense architecture that is both scalable and resilient. The future of CTI lies not in the volume of shared data, but in the strength of the collaborative learning ecosystem we create around it. It is time to move from tactical exchanges to strategic cooperation — one built on evidence, accountability, and collective responsibility. We are proud to work with the Cyber Threat Alliance as they take the necessary steps towards this vision.

BY KIHONG KIM
CEO

minsait

An Indra company

CTA Member Feature

THE IMPORTANCE OF COLLABORATION IN CYBER INTELLIGENCE IN MEXICO AND OTHER COUNTRIES

In the digital age, where threats know no borders, collaboration has become one of the most powerful tools in cybersecurity. Today, coordinated efforts among governments, businesses, academia, and international organizations are essential to counter increasingly sophisticated and organized cyberattacks.

Cyber attackers now operate in organized networks, share resources, and target critical sectors such as finance, energy, healthcare, supply chains, and government institutions. The solution? A collective and coordinated intelligence approach that allows to anticipate these attacks before they materialize.

Borderless Cyberattacks

Advanced Persistent Threats (APTs), Ransomware-as-a-Service (RaaS), and digital disinformation are recognized as global issues. And since attackers cooperate internationally, defense must also be global.

Key benefits of cyber intelligence collaboration include:

- Early threat detection
- Reduced response time
- Access to validated indicators with tactical and business context
- Improved defensive strategies
- Coordinated recovery and resilience efforts

Additionally, companies that collaborate build trust among customers, partners, and investors.

Global Collaboration

Initiatives such as the CTA demonstrate the effectiveness of collaboration. CTA acts as a bridge for companies to share technical and strategic intelligence in real time, using structured and automated formats. Their members not only provide better protection to customers but do so without having to build all the infrastructure from scratch. This strengthens the global ecosystem and reduces operational costs.

In Mexico, the need for collaboration is critical. Organizations such as the National Banking and Securities Commission (CNBV), the National Guard, the National Autonomous University of Mexico (UNAM), and strategic sectors like finance and energy have both the responsibility and the opportunity to build a united front. The exchange of structured information and indicators of compromise can make the difference between containing a threat and suffering a devastating cyberattack.

Under a Governance Model

At its 2025 edition in Davos, the World Economic Forum discussed creating governance mechanisms for cyber intelligence sharing, strengthening digital sovereignty without losing international cooperation, and responding collectively to high-impact attacks. Cybersecurity is no longer just a technical issue; it is a matter of geopolitical and economic stability.

Integrating cyber intelligence collaboration into an organization's strategy is a smart decision. It means staying one step ahead, reducing risks, containing attacks more effectively, and creating a safer environment.

Unity Strengthens Defense

In an environment where attackers are increasingly organized, the best response is a defense based on shared intelligence and cross-sector coordination. Cyber intelligence collaboration is more than just a strategy—it is a necessity for organizations to protect their economy, their data, and to thrive in the digital world.

BY ERIK MORENO
DIRECTOR OF CYBERSECURITY AT
MINSAIT IN MEXICO

THREAT INTELLIGENCE PRACTITIONERS' SUMMIT (TIPS) CONFERENCE

CTA held our inaugural Threat Intelligence Practitioners' Summit (TIPS) conference on May 13th–15th.

- *May 13th Workshop — Indicators of Behavior And Attack Flow*
- *May 14th–15th — 2 full days of main conference talks and keynotes*

We're excited to share that our inaugural conference was a resounding success! Thanks to your incredible support and commitment, the event surpassed all expectations and laid a strong foundation for future gatherings. A special thank you to our inspiring speakers, whose thought-provoking presentations sparked meaningful conversations throughout our community.

We proudly recognize our first award winners:

- *Ecosystem Winner* – **Jason Healey**
- *CTA Booster* – **Kathi Whitbey**
- *Most Impactful Early Share* – **Palo Alto Networks; *Global Companies Are Unknowingly Paying North Koreans: Here's How to Catch Them***

We are deeply grateful to our sponsors, whose generous support made this event possible.

CISCO — DIAMOND SPONSOR

paloalto NETWORKS — GOLD SPONSOR

FORTINET — ASSOCIATE SPONSOR

VENABLE LLP — ASSOCIATE SPONSOR

CUJO AI

CTA Member Profile

MEMBER SPOTLIGHT: CUJO AI

WHY DID CUJO AI JOIN CTA?

CUJO AI had been considering joining the Cyber Threat Alliance for quite some time before finally making the decision. The CTA brings together key players in the cybersecurity industry who are actively engaged in research and operations. We recognized, and continue to recognize, a significant opportunity with CTA to exchange highly valuable data, information, and insights on ongoing malicious actor campaigns, malware analysis, and innovative methods to combat cybercrime.

CUJO AI believes that this collaboration is precisely what is needed — sharing information among researchers and subject matter experts to enhance companies' capabilities in fighting cybercrime and making the Internet a safer and better place.

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

CUJO AI benefits from both direct and indirect impacts through its membership in CTA. Directly, we exchange Indicators of Compromise (IoCs) with several selected threat intelligence providers. As a network-based protection solution, our focus is on network-based IoCs such as IP addresses, domains, and URLs. Additionally, shared file hashes from the latest findings by CTA members are invaluable for our threat researchers, aiding in the analysis of malicious actor activities and campaigns. CUJO AI ingests these exchanged IoCs, enriches them, and makes them useful for our end customers.

Indirectly, the membership provides access to fresh articles, research papers, and collaboration opportunities, which are particularly beneficial for CUJO AI's growth and enhanced customer protection. Collaborating with strong and leading industry partners serves as an invaluable source of inspiration and knowledge.

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

CTA plays a pivotal role in ensuring that critical cybersecurity issues are recognized globally and that significant decisions are made regarding cyber intelligence sharing and regulations. By uniting the strongest players in the cybersecurity industry, CTA leverages their collective expertise to shape and transform the global cybersecurity landscape.

WHAT VALUE DO YOU GET OUT OF THE CTA?

Access to actionable intelligence, early access to research papers before publication, direct contact with key cybersecurity professionals from globally leading organizations, and numerous collaboration opportunities.

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

In the interconnected and globalized world of cybersecurity, working in isolation yields limited results. Regardless of the size of an organization, the greatest value comes from information sharing and collaborative efforts to address cybersecurity challenges. Different perspectives on the same problem, various methods to combat it, and diverse layers of data accessible to different protection solution providers all contribute to a more comprehensive defense strategy. By sharing this information through CTA, we collectively make the Internet a safer space for everyone.

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

Collaboration with other researchers and industry partners.

vb 2025 BERLIN

24-26 Sept 2025

CTA is proud to once again sponsor the 35th Virus Bulletin International Conference Threat Intelligence Practitioners' Summit (TIPS)!

The conference will be held September 24th-26th, 2025 in Berlin, Germany. Note that the CTA-sponsored TIPS track will be held Thursday, September 25th.

Our theme for the TIPS track is ***Community Driven Threat Defense***.

VB2025 features an international line-up of speakers who are all experts in their field and provides three days of learning opportunities and networking with industry experts. The program will cover topics that relate to critical security issues and emerging threats.

Check out the VB2025 programme and speakers here.

VB2025 will be held at the JW Marriott Hotel Berlin (Stauffenbergstrasse 26 Berlin, Germany, 10785).

CTA HOSTED WEBINARS ON DEMAND

https://www.cyberthreatalliance.org/resources/webinars/

CYBER THREAT ALLIANCE

CYBER THREAT ALLIANCE WEBINAR

CISA 2015 REAUTHORIZATION: WHAT'S ALL THE FUSS ABOUT?

MICHAEL DANIEL, President & CEO, Cyber Threat Alliance

AMY SHUART, VP, Technology & Innovation, Business Roundtable

MIKE FLYNN, VP and Counsel, Government Affairs, Information Technology Industry Council

ARI SCHWARTZ, Managing Director of Cybersecurity Services, Venable

KEMBA WALDEN, President, Paladin Global Institute

May 20th, 2025
7:00am PT - 7:45am PT
10:00am ET - 10:45am ET

CYBER THREAT ALLIANCE

CYBER THREAT ALLIANCE WEBINAR

CYBER SURPRISES AND CONTINUITY: PREDICTIONS FOR 2025

MICHAEL DANIEL, President & CEO, Cyber Threat Alliance

ADAM BENNETT, CEO, Red Piranha

SAMIR MODY, VP Threat Research, K7 Computing

TAKAHIRO KAKUMARU, Director of Cyber Intelligence Group, NEC Corporation

February 25th, 2025
7:00pm PT - 7:45pm PT
10:00pm ET - 10:45pm ET

CYBER THREAT ALLIANCE

CYBER THREAT ALLIANCE WEBINAR

CTA TIPS 2025

CEO PANEL WITH CTA'S FOUNDING MEMBERS

Fortinet, McAfee, Palo Alto Networks, & Symantec

KEN XIE

MICHAEL DANIEL

MARK MCLAUGHLIN

CHRIS YOUNG

GREG CLARK

May 14th, 2025
12:00pm ET - 12:30pm ET