DECEMBER 2024

# CTA IN FOCUS

## LETTER FROM THE PRESIDENT & CEO

Cooperation and competition are embedded deeply into the structures of the digital world. For example, it takes cooperation between telecommunications companies for the internet to function – otherwise, packets could not get to every destination. At the same time, competition in pricing between routes forms the basis for the protocols that determine how packets flow at any given moment. Both modes of interaction are necessary for the digital world to function properly.

For those operating in Western business culture, however, competition is by far the dominant mode of interaction between organizations. In fact, we even have outlawed some forms of cooperation through our anti-trust statutes, and we often look askance at companies that work together. Yet we know that if we want to protect our digital world, we need private sector companies to work together. We also know that we need the private sector, the public sector, and the non-profit sector to work together, or we will not be able to reach the level of security and resilience we want.

That's where an organization like the Cyber Threat Alliance comes in. We provide the platform, structure, and processes needed to achieve unity of purpose while fostering competition among our members. We provide neutral ground for organizations to collaborate, sharing intelligence and insights that make every participating organization more effective at their mission. We enable our members to unify around key threats to the digital ecosystem and ensure a common understanding of threats. Thus, we demonstrate the power of unity every day in how we operate. On the flip side, by making our members more effective at their missions, we also enhance competition, because those members have better capabilities or improved insights through their participation.

The digital ecosystem needs organizations like CTA, because tapping into the power of unity is difficult without them. Yet, organizations often worry about whether sharing and collaborating will run afoul of anti-trust laws or expose them to legal liability in some way. Therefore, the degree of threat sharing we have achieved so far critically depends on the legal clarity provided by existing statutes that such activities are lawful and have liability protection.

This dependence makes statutes like the US Cybersecurity and Information Sharing Act of 2015 crucial to the information flows. As laws like these come up for reauthorization in the US or are being considered for the first time in other countries, we should articulate the benefits these statutes provide to a broader audience. We need to ensure that policy makers understand their value and criticality, and not take support for granted.

As 2024 comes to a close, I am proud of the work CTA has done to foster both cooperation and competition in the cybersecurity industry. By demonstrating the power of unity, we show what is possible. I am looking forward to continuing this work in 2025.

J. Michael Daniel

*President & CEO, Cyber Threat Alliance*

## IN MEMORIAM

*Jason Minnick*

*July 4, 1977 – October 5, 2024*

CTA is saddened to share that Jason Minnick, our long time Chief Technology Officer, passed away in October 2024 after a private and incredibly brave battle with brain cancer.

Jason served as CTO from 2017-2024 and played a key role in developing the CTA platform, Magellan, into what it is today.

Jason started his career in the technology arena in the late 1990s and was a respected leader in the software industry. Over the course of his career, he advanced from a software engineer to serving as our CTO. His mentorship shaped the careers of many in the field. Jason's passion for technology was matched only by his dedication to those around him, leaving a profound mark on both his colleagues and the companies he contributed to.

Jason was a valuable member across the CTA community and will be deeply missed by all his family, friends, and colleagues.

CYBER THREAT ALLIANCE

## MEMBER SHARING SNAPSHOT

### OBSERVABLES SUBMITTED

**>14.5 MILLION**

MONTHLY AVERAGE

### OBSERVABLE DIVERSITY

(AVERAGE)

| | |
|---|---|
| FILE HASH | 44% |
| IP ADDRESS | 12% |
| DOMAIN NAME | 8% |
| URL | 6% |
| NETWORK TRAFFIC | 18% |
| FILE PROPERTIES | 10% |
| HOST | 2% |

### TOTAL EARLY SHARES

**3-5**

PER WEEK

**1,150+**

K7 COMPUTING

CTA Member Profile

# MEMBER SPOTLIGHT: K7 COMPUTING

### WHY DID K7 JOIN CTA?

*Sharing is Caring.* We at K7 knew we had something valuable and wholesome to contribute on a global platform like CTA towards a common goal in the cybersecurity industry, viz. Relevant, Timely, Actionable and Contextual threat intelligence data for a cybersecure world. We appreciate the opportunity to stand shoulder-to-shoulder with other renowned cybersecurity providers in this noble mission.

### WHAT VALUE DO YOU GET OUT OF CTA AND HOW DOES IT HELP K7 PROVIDE GREATER SECURITY FOR CUSTOMERS?

CTA's Magellan platform is an invaluable hub for threat intelligence data shared by various globally-recognised cybersecurity organisations. This data, along with that from CTA's Early Sharing programme, is used to protect our customers proactively and quickly, including via automation with appropriate vetting. Magellan also allows us to hunt specific, campaign-related data and pivot on that for broader and deeper insights. This global exposure with statistical data puts us in the right spot. We value the unstinting mutual trust and respect between CTA and us over the years.

We have also had the great opportunity to present our research, ideas and advice at several of CTA's Virus Bulletin Threat Intelligence Practitioners Summit (TIPS) tracks over the years. Thus, CTA even helps promote the K7 brand on various fora.

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

CTA is an independent, non-partisan, non-profit entity which provides a unique, global platform, a sturdy multi-directional, multi-dimensional bridge of sorts, for threat intelligence sharing amongst trusted members. CTA, as a Cybersheperd, even curates intelligence reports for the public at large.

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

No single entity has omniscient visibility in an increasingly complex digital environment, and therefore cannot succeed alone in the mission of safeguarding global cyberspace. However, together we are stronger than the sum of our parts.

We at K7, one of the oldest, independent cybersecurity product companies in the world with indigenous Indian technology, value both 'Aatmanirbharta' ["self-reliance"] as well as the *'One World, One Family'* concept in our common, united fight against threat actors who are evolving rapidly through technology, space and time.

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

Complex cyber attacks, human errors, and most importantly lack of security awareness, are the most significant challenges in cybersecurity. Many organisations are working towards mitigating the fallout of complex cyber attacks, but only a few are taking up initiatives to create security awareness amongst common people to help prevent such attacks in the first place. CTA, being a global community, can influence security companies to bring in and propagate such awareness programs.

### WHERE DO YOU SEE CTA IN 5 YEARS?

A trusted global leader in sharing threat intelligence data, including a repository for digital signing certificate revocation metadata.

CHECK POINT

CTA Member Feature

# POWER OF UNITY: CREATING A STRONGER SHIELD WITH AI SECURITY COLLABORATION

As cyber threats become more sophisticated and relentless, the power of collaboration within the CTA has become invaluable for advancing AI-driven security measures. The CTA's collaborative intelligence-sharing approach empowers each member to harness AI and machine learning to prevent, detect, and respond to emerging cyber threats with unprecedented agility. At Check Point Software Technologies, we recognize that the strength of our AI defenses is amplified by the insights and innovations contributed by our CTA partners.

AI-powered threat intelligence enhances our ability to detect and respond to threats before they manifest as major incidents. Through shared data and analytical models, CTA members gain access to a collective intelligence framework that identifies emerging attack patterns across various industries. Check Point's ThreatCloud AI leverages this shared intelligence to fortify our security products, which analyze millions of threat indicators and enable real-time threat prevention. This collaboration strengthens not only individual defenses but also the global security landscape by constantly updating algorithms to recognize and counteract newly evolving tactics used by adversaries.

One of the most significant advantages of CTA collaboration is the proactive approach it enables. AI tools powered by collective intelligence predict potential attack vectors, empowering Check Point to stay ahead of threats with preemptive countermeasures. Machine learning models can rapidly detect unusual patterns and flag them, while automated systems can launch preventive actions across the Check Point Infinity Platform and our security solutions—such as Check Point Harmony Endpoint and Quantum Security Gateways. This approach, built on AI-driven insights from CTA members, reduces response time and optimizes defenses against zero-day threats and AI-enhanced attacks.

CTA's collaborative model embodies the principle that cybersecurity is stronger when unified. As threat actors increasingly employ AI to design complex attacks, a shared approach allows all member organizations to benefit from a fortified defense ecosystem. Together, we foster an environment of security that adapts as fast as the threats evolve, ensuring that our users benefit from the latest in AI-enhanced protection.

As each member organization shares new insights, all benefit from a stronger shield against cyber threats, effectively embodying the CTA's mission: leveraging the "Power of Unity" to safeguard digital spaces. This spirit of collaboration builds a resilient, interconnected cybersecurity landscape that serves as a first line of defense for businesses and individuals worldwide.

**BY JASON MIN**
HEAD OF BUSINESS AND CORPORATE DEVELOPMENT

RAPID7

CTA Member Feature

# PUBLIC-PRIVATE PARTNERSHIPS:

## A GROWING FORCE IN THE FIGHT AGAINST CYBER THREATS

In today's rapidly evolving digital age, public-private partnerships (PPPs) have become a crucial component of the cybersecurity equation. This shift arises from the vast amount of digital assets and data now existing beyond the traditional realms of government control. A surge in internet-connected devices, especially post-COVID, has expanded the attack surface for malicious actors, ranging from nation-states to cybercriminals utilizing ransomware-as-a-service.

This complex reality underscores that no single entity, government, or private organization can manage the entire cyber landscape alone. It is why it's important governments spend time developing effective collaboration programs and partnership models for PPPs, designing such initiatives around transparency, accountability, and flexibility, as well as creating a baseline of shared context.

There are myriad reasons PPPs are vital. For one, they facilitate the sharing of threat intelligence and cybersecurity best practices, fostering a collaborative defense mechanism. Governments and private entities can jointly analyze and respond to cyber threats, leveraging each other's strengths. Structured collaborations ensure actionable outcomes, driving continuous improvement in cybersecurity practices.

Looking ahead, the evolution of PPPs in cybersecurity is likely to be shaped by several key trends.

First, there will be a growing emphasis on involving more industry specific risks and context in PPPs and trying to get that information from new and different sources. For example, small and medium-sized enterprises are increasingly seeing heightened cyber risk in their businesses; they are recognizing the importance of robust cybersecurity practices and will seek greater collaboration with governments and larger corporations.

Second, intra-regional government collaborations will intensify. Such initiatives will not only bolster individual country defenses, but also strengthen regional security against collective cyber threats.

Finally, PPPs that are designed with more transparency and flexibility will complement formal government partnership models by providing a nimble and incident-based rapid response model that can help governments and the private sector be more responsive in a crisis. That model can then be used to develop more robust and long-term system changes that reduce overall cyber risk.

The future of cybersecurity lies in the strength of PPPs. By fostering collaboration, sharing intelligence, and building capacity, these partnerships will enhance our collective ability to defend against ongoing cyber threats. As governments and private entities continue to recognise their shared responsibility in this domain, the evolution of PPPs will play a pivotal role in shaping a secure digital future for all.

**BY SABEEN MALIK**
VP OF GLOBAL GOVERNMENT AFFAIRS AND PUBLIC POLICY

# SAVE THE DATE FOR TIPS 2025!

THREAT INTELLIGENCE PRACTITIONERS' SUMMIT CONFERENCE

## Breaking Through the Barrier: Making Threat Intelligence Useful

May 14—15, 2025

**Arlington, Virginia, USA**

CTA will be hosting the Threat Intelligence Practitioners' Summit Conference May 14-15th, 2025. The event will be held at the Westin Hotel in Arlington, Virginia.

More details will be available on our website — coming soon!

CTA Member Feature

# UNITY IN DIVERSITY: NAVIGATING THREAT DEFENSES IN A GEN AI WORLD

*By Abhishek Karnik and German Lancioni*

The Cyber Threat Alliance (CTA) recently undertook the creation of a Joint Analytic Report where our members discussed Generative AI (GenAI) and its impact on cybersecurity. The CTA provided a safe framework for multiple organizations to debate, discuss and understand the challenges across government, consumer and enterprise security. A key take-away from these interactions was that no single organization had all the answers. A diverse set of perspectives is key to help garner insights, deepen our understanding and effectively navigate an expanding attack surface that is brewing thanks to the easy accessibility and democratization of powerful GenAI tools.

AI is not new to cybersecurity. Intrusion, spam, and malware detection systems have long leveraged Machine Learning and AI to manage rising threat volumes amidst a skill shortage. However, the emergence of Generative AI tools is empowering cybercriminals to widen the breadth and volume of automated attacks, more easily uncover vulnerabilities, and create sophisticated phishing schemes or deepfake content. The bar to entry has been lowered and we can expect to see a higher volume of more customized attacks in the future. Adaptive malware at scale and convincing social engineering scams will intensify the cyber arms race.

Consequently, collaboration within our community is paramount to ensure success as we align ourselves and coordinate our efforts, which will materialize by focusing on influencing the right areas:

1. **Casting a wide net**: ensuring diversity in thought by gaining perspectives from defenders across products, sectors and varying organizational roles. The exchange of ideas will accelerate innovation, establish ethical standards, and enable responsible deployment of AI technologies.
2. **Building a new set of signals and sensors that help identify AI-generated content**: Think of these as an Indicator of GenAI (IoG). Content that can be tagged as AI-generated inherently may not have mal-intent, but awareness will allow organizations and consumers to make informed decisions. Such signals will serve as attributes that enable smarter defense strategies.
3. **Empowering defenders with tools**: open-source initiatives will accelerate tool innovation, helping defenders create AI assistants that can rapidly analyze and generate detailed reports with minimal pre-training. These tools will enhance malware analysis, integrate seamlessly with existing tools, aid in threat analytics and prioritization as well as information exchange. Best practices and knowledge sharing will be key for successful defense.
4. **Influencing AI-as-a-Service providers**: although there has been some progress in this space, there needs to be a healthy balance between innovation and regulatory requirement to develop capabilities (such as watermarking) that help distinguish synthetic content from authentic data at the source. Guardrails should be based on personas, so multi-modal models can help cybersecurity professionals not hit guardrails while conducting malware analysis and yet only impose restrictions where intent is unclear. This would mean coordinating efforts with AI-as-a-Service providers, so we don't curb innovation yet have the right levers for balance.
5. **Bridging the Skills Gap**: partnerships between industry, academia, and governments can address the cybersecurity skills gap by accelerating education and training programs for new defenders.

Ultimately, defenders must focus on collaboration to build effective tools that make it more challenging and expensive for adversaries to meet their goals. Defense fundamentals — like zero trust and defense in depth — won't change, and remain critical and necessary, but coordinated efforts are needed now, to effectively address the increasing scale and complexity of attacks to come.


**ABHISHEK KARNIK**
DIRECTOR FOR THREAT RESEARCH AND RESPONSE

**GERMAN LANCIONI**
CHIEF DATA SCIENTIST FOR CTO OFFICE


## CTA IS PROUD TO BE AN ASSOCIATION PARTNER FOR RSA CONFERENCE 2025

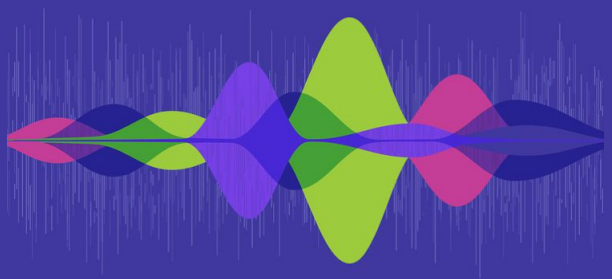
Many Voices. **One Community.**

Join us for RSAC 2025 in San Francisco from April 28 – May 1!

Immerse yourself in critical cybersecurity discussions, network with industry leaders, and uncover innovative ideas. Experience hands-on learning and deep-dive sessions. Register by Jan. 10 and save up to $800. Plus, Cyber Threat Alliance members save an additional $150 using code 1U5CTAFD. Don't miss this opportunity to enhance your skills and strengthen our cybersecurity community.

**Register now!**

We hope to see you there!



RSAConference™2025
San Francisco | April 28 – May 1 | Moscone Center