MARCH 2024

CTA IN FOCUS

CYBER THREAT ALLIANCE

LETTER FROM THE PRESIDENT & CEO

CTA's theme for 2024 is resilience through collaboration. It's easy to think "resilience" is just another marketing buzzword that will be quickly replaced by something else. However, like authentication or segmentation, resilience is (or should be) a foundational concept in cybersecurity.

As the cybersecurity field has matured, practitioners have realized that errors, bugs, judgment lapses, and occasional laziness cannot be eliminated. On the other hand, malicious actors have strong motivations for their actions, and they cannot be deterred from every kind of malicious action all the time. This combination of defensive limitations and intruder motivation means that malicious actors will achieve some degree of success some of the time.

What does this assertion mean for defenders? If the bad guys will inevitably succeed some of the time, then organizations have to prepare for that outcome. They must be ready to operate through a cyber incident, while responding to it rapidly. They have to contain the incident and limit the damage. Then they have to be able to recover and return to regular operations as swiftly as possible. In other words, they have to be resilient. That's why this concept isn't simply going to fade away; it's a necessary element of succeeding as an organization in the digital age.

Although companies have several options for becoming more resilient, one way to increase resilience is through collaboration. Working with peers, cybersecurity companies, and government agencies provides access to information, resources, and ideas that organizations would otherwise not have. Thus, collaboration increases the likelihood that an organization's resilience will prove adequate to the task, whether that organization is a large enterprise, a small business, or a cybersecurity provider.

That's why we chose "resilience through collaboration" as our 2024 theme. Of course, we want to prevent as many incidents as possible and we want to impose costs on malicious actors. Collaboration certainly helps achieve those goals, too, but we also want to raise the level of resilience across the digital ecosystem. This newsletter will highlight a few of the efforts CTA members have underway to achieve that goal. I am looking forward to seeing what we can do together.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

CARO2024

Driving Back the Shadows: Connecting Research to Action

May 1st – 3rd, 2024
Greater Washington, DC Area

CTA is excited to host the CARO Workshop 2024! The workshop is specifically dedicated to computer security research and fighting cybercrime. Information is shared by security researchers and law enforcement in a closed environment. The workshop is all about cutting edge research and new ideas in cybersecurity. We hope to see you there!

Register Today: https://www.caro2024.org/registration/

Explore the Agenda: https://www.caro2024.org/agenda/

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>10 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	34%
IP ADDRESS	15%
DOMAIN NAME	5%
URL	5%
NETWORK TRAFFIC	29%
FILE PROPERTIES	10%
HOST	2%

TOTAL EARLY SHARES

3-5
PER WEEK

985+

CTA Member Feature

RESILIENCE THROUGH COLLABORATION

As information security professionals, we navigate the ever-evolving landscape of cybersecurity threats that challenge our organizations' information assets. In this dynamic environment, resilience has emerged as a cornerstone of an effective cybersecurity strategy. However, resilience extends beyond robust technological defenses and recovery plans; it is significantly enhanced through strategic collaboration. This post explores the unique benefits and often overlooked opportunities of fostering resilience through collaboration from a CISO's perspective, targeting fellow cybersecurity professionals.

One of the paramount benefits of collaboration in cybersecurity is the ability to share threat intelligence in real-time. In an era where cyber threats are increasingly sophisticated and fast-moving, the traditional siloed approach to threat intelligence is no longer sufficient. Collaborative platforms and partnerships, such as Information Sharing and Analysis Centers (ISACs) and other membership-oriented groups (like CTA), provide a mechanism for organizations across industries to share insights about emerging threats, vulnerabilities, and mitigation strategies. This collective wisdom enables participants to proactively defend against threats before they impact their own environments, exemplifying the adage "forewarned is forearmed."

Another significant advantage of collaboration is the enhancement of incident response capabilities. Cyber incidents are inevitable, but their impact can be drastically reduced through coordinated response efforts. Collaborative exercises, such as cross-industry simulations and tabletop exercises, allow organizations to test and refine their incident response plans in a controlled, but realistic environment. These exercises not only improve readiness but also foster a culture of continuous improvement and learning across organizations. This extends to the international realm of cyber defense to geopolitical situations like the Ukrainian conflict that persists today.

Moreover, collaboration presents an often-underutilized opportunity to leverage collective bargaining power when procuring cybersecurity solutions and services, or when looking to influence government and industry organizations. By pooling resources and requirements, organizations can negotiate more favorable terms, access better technology, and amplify a collective voice when shaping cyber policy. This collective approach not only reduces individual costs but also accelerates the adoption of innovative security measures across the board.

In conclusion, as professionals operating in the modern world, we must recognize that our strength lies not just in the technologies we deploy, but in the networks we build. By prioritizing collaboration, we not only enhance our resilience but also contribute to the broader security ecosystem. This approach allows us to stay ahead of threats, reduce the impact of incidents, and drive the cybersecurity agenda forward through shared knowledge and resources. Let us embrace collaboration as a key strategy in our resilience toolkit, for together, we are stronger.

BY DAVID BEABOUT
CISO
NTT SECURITY HOLDINGS INC.

CTA Member Feature

STRENGTH AND RESILIENCE THROUGH COLLABORATION

In the past, we were concerned that the unique threats facing the Latin American region might not garner the attention of a broader alliance. However, it quickly dispelled five years ago when the CTA proposed to SCITUM to become a member, a strategic step that significantly enhanced our visibility. We took that decision based on the understanding that in the cyber realm, no single entity holds all the answers or can see the entirety of the threat landscape. The alliance promised a collaborative environment where shared intelligence and direct engagement with researchers would bolster each member's capacity to defend its customers and the world.

That promise was true because a distinctive feature setting the CTA apart from other alliances is its emphasis on direct, swift communication between members and researchers, which accelerates the pace at which threats are understood and countered while enhancing the depth of collective knowledge. By enabling members to query investigators about their recent findings directly, the CTA ensures that nuanced insights are shared, leading to more effective and timely responses to cyber threats.

On the other hand, the CTA has successfully cultivated an ecosystem where the finest minds in cybersecurity converge to share their expertise. This collaborative network includes a range of Threat Intelligence specialists whose combined efforts provide a formidable weapon against cyber adversaries. The alliance's resilience lies in its diversity, with members with different strengths pooling their knowledge to devise comprehensive defense mechanisms while facing the same threat.

The alliance's strategy goes beyond mere information exchange; it fosters a culture of innovation and continuous improvement in cybersecurity measures. The CTA enhances each member's protective capabilities through technical discussions and collaborations with other entities.

As SCITUM celebrates five years within the Cyber Threat Alliance, it reflects on the profound benefits of being part of a community that thrives on collaboration and shared intelligence. This journey has fortified SCITUM's cybersecurity capabilities and contributed to the broader mission of creating a safer digital environment for all. In the face of escalating cyber threats, the story of the members and the CTA stands as a potent reminder that our unity is our strength, and together, we forge a path toward greater resilience.

BY IMELDA FLORES
HEAD OF SCILABS
TELMEX SCITUM

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.

FORTINET

CTA Member Profile

MEMBER SPOTLIGHT: FORTINET

FORTINET IS A FOUNDING MEMBER OF CTA. WHY DID YOU DECIDE TO WORK ACROSS THE INDUSTRY, INCLUDING WITH YOUR FIERCE COMPETITORS, TO SHARE THREAT INFORMATION?

Fortinet is proud to be a founding member of the Cyber Threat Alliance. Collaboration is at the heart of the CTA mission and is a core part of our DNA at Fortinet. Shared intelligence is a crucial part of how our industry ensures timely and precise responses when attackers strike. The more we collaborate across the public and private sectors, the more effective we can be at disrupting cybercrime.

The CTA's work to improve the cybersecurity of our global digital ecosystem by enabling near-real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field is aligned with our own mission to secure people, data, and devices everywhere. Collaboration with the public sector and industry has been a fundamental aspect of Fortinet's strategy for many years. We strive to ensure a secure and productive economy for all through partnerships, industry collaboration, and information sharing. We actively work with the industry, CERTs, government entities, and academia to proactively exchange threat information and enhance cyber resilience globally. This is just one example of how we work to be a responsible member of a larger cybersecurity ecosystem.

WHAT DOES FORTINET VALUE MOST ABOUT CTA MEMBERSHIP?

The CTA is the first industry trade association designed exclusively by and for the cybersecurity industry. Today, many organizations are working to gather and distribute threat intelligence, but often, they're focused on just one piece of the puzzle. There are many silos in the industry, and no single individual or organization has complete insight into all the threats that exist. Halting bad actors in their tracks requires a coordinated, unified front, because security professionals need a comprehensive view of the threat landscape to make the best decisions about securing their organization's networks. CTA's efforts are critical components to helping organizations act quickly on information, enable the proper protections within their environment, and disrupt cybercriminal activities.

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

Turning the tide against cybercrime requires a culture of collaboration, transparency, and accountability on a broad scale. Every organization plays a role in disrupting cyber threats. Through constant technology innovation and collaboration across industries and working groups, such as the CTA, we collectively improve protections and aid in the fight against cybercrime globally. Collaboration, cooperation, and disclosure are essential pieces of the process that can only be accomplished when organizations rally around a common goal.

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

One of the most effective actions we can take in the cybersecurity industry to fight against cybercriminals is to collaborate and forge new partnerships. Fortinet has a longstanding reputation as a leading, trusted security partner driven by innovation, continuous improvement, and transparency. By sharing threat intelligence and working with other threat intelligence organizations, we can improve protections for organizations of all sizes and across all industries, enhancing the effectiveness of the entire industry.

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

CTA's commitment to cross-collaboration and intelligence sharing is paramount, and this is evident in the many working groups CTA hosts. This unique model allows CTA members to share timely, actionable, and campaign-based intelligence that can be used to improve products and services to better protect their customers, systematically stop adversaries, and improve the security of the digital ecosystem. Moreover, alliance membership aims to improve the cybersecurity of the global digital ecosystem by significantly reducing time to detection and closing gaps in the detection-to-deployment life cycle.

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

Between the global threat landscape intensifying and an industrywide cybersecurity skills shortage, it's more challenging than ever for businesses to properly manage complex infrastructure composed of disparate solutions, let alone keep pace with an increasing volume of alerts. Collectively, the efforts of the CTA will help enhance cyber resilience globally on many levels.

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

CTA members, including Fortinet, are better able to protect their customers in real time and prioritize their resources based on collective knowledge. Strong partnerships should include the bi-directional sharing of knowledge and information. We believe that organizations must work together to disrupt adversaries at as many points in their ecosystem as possible. Everyone has a role to play. Cultivating relationships and sharing information creates trust, and greater trust among public and private organizations opens the door for everyone to increase their cyber resilience.

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

Fortinet's mission to secure people, data and devices everywhere, is foundational to achieving just and sustainable societies. We believe we are responsible for delivering on that vision by addressing cybersecurity risks to society, diversifying cybersecurity talent, respecting the environment, and promoting responsible business practices across our value chain. One related effort is protecting the internet's common good, which requires coordinated efforts to enable the sharing of intelligence to combat sophisticated global cyberattacks. By bringing the industry together, including competitors, to contribute unique threat insights, the CTA builds an enriched understanding that helps entities of all shapes and sizes provide enhanced protection against global attacks.

WHERE DO YOU SEE CTA IN 5 YEARS?

The threat landscape is dynamic and constantly changing, and organizations need to move quickly to stay ahead of increasingly sophisticated threats. As organizations join this effort, our collective defenses and resources increase. As the CTA continues to grow in membership and scope, it furthers the industry in achieving the vision of CTA as a global hub of cybersecurity information and defense, providing teams with access to real-time intelligence to protect their networks and customers' networks. Also, improving critical resources and fostering collaboration will create new ideas and spark additional industry innovation.

CYBER NONPROFITS RECEPTION

- Date: Tuesday, May 7th
- Time: 6PM-7:30 PM
- Location: Esplanade 153 – Moscone South

Cyber Threat Alliance
&
Nonprofit Cyber

organizations are co-hosting a happy hour reception during RSA Conference 2024.

Join us for nibbles & drinks and chat with the Nonprofits that are impacting the foundation of our internet security, policy, privacy & safety.

All are welcome to attend.

RSAC is the world's leading and largest cybersecurity conference.

Use code **14UCTAFD** for a discount off RSA full conference membership.

CYBER THREAT ALLIANCE

MITRE ENGENUITY Center for Threat Informed Defense

Nonprofit Cyber

CSA cloud security alliance®

CREST

CYBER READINESS INSTITUTE

CIS Center for Internet Security®

OPEN CYBERSECURITY ALLIANCE

CYBERNEXT BRUSSELS 2024

Over the last seven years, the Cybersecurity Coalition and CTA have hosted CyberNext DC in Washington, D.C., a policy summit that brings together experts from industry and the government to discuss some of the most pressing cyber policy issues.

This year, the Cybersecurity Coalition is hosting the inaugural CyberNext Brussels conference on March 21. The EU has cemented itself as key player in cybersecurity policy development with the passage of the NIS2 Directive, the certification schemes stemming from its Cyber Security Act and, of course, the Cyber Resilience Act (CRA).

The event takes place as the EU is at an inflection point: beginning the implementation process for several tech regulations, including the CRA and the AI Act, as well as with the upcoming Parliamentary elections. The next five years will be critical in setting a strong basis for European cybersecurity as the EU moves to implement this plethora of new cybersecurity and technology regulations.

The agenda can be found here. Attendees can register for the free event here.

Find CTA Online!

Check out CTA's blog where we share expert analysis and news on the most important issues facing the cybersecurity industry.

CTA BLOG »

On our YouTube channel, you'll find our full library of CTA webinars and member testimonials.

CTA YOUTUBE »