SEPTEMBER 2024

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

The September 11th attacks changed our view of physical security. As a result, everyone had to invest more in protecting their people and facilities. At the time I was in charge of the Office of Management and Budget's Intelligence branch, and we received numerous requests to fund physical security upgrades. What was interesting to me, though, was that the proposed investments were not consistent. Some agencies requested funding to concentrate their people and facilities in one location, because consolidation would allow them to protect those people and buildings more effectively and reduce risk. Other agencies asked for funding to spread out their people and buildings, because having them all in one location was too risky. These varying approaches to physical security reflected a tension between two types of risk, complexity and concentration, and which one to prioritize eliminating. There is not necessarily a "right" way to resolve this tension; rather, leaders have to continuously make choices about which risk is most important to address at a particular time.

This same tension plays out almost every day in cybersecurity. Complexity is the enemy of cybersecurity, but so are monocultures and flat networks. In an ideal world, organizations would have just enough complexity in their networks, applications, and tools to make it challenging for the adversary, but not so much complexity that it interferes with productivity or the ability to defend against threats. Sourcing your cybersecurity from multiple vendors helps ensure that you are protected against a wide array of threats, but if those vendors don't work well together, then those benefits may be outweighed by the complexity of being your own integrator. Organizations face both complexity and concentration risks in their cybersecurity efforts. At any given point, they have to decide which risk to prioritize reducing.

CTA helps cybersecurity providers navigate their version of the concentration versus complexity trade off. We want cybersecurity providers to gain the benefits of concentration through threat intelligence sharing, while avoiding the risks associated with single points of failure. Conversely, we enable members to share threat intelligence with low friction, thereby reducing complexity, yet still retaining their unique perspectives and capabilities. All of CTA's activities balance this mix of complexity and concentration.

These characteristics are hallmarks of Community Driven Defense, the theme of this quarter's newsletter. This kind of defense requires organizations to work across boundaries without concentrating security in just one company or platform. It's not an easy task. Reducing complexity enough to make effective cybersecurity possible without elevating concentration risk too high is a delicate balance. Organizations dedicated to this purpose, like CTA, make this task just a little bit easier and it's one of our primary roles in the ecosystem. I hope you enjoy reading about why and how our members are contributing to making Community Driven Defense a reality through CTA.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

VIRUS BULLETIN 2024

CTA is proud to once again sponsor the 34th Virus Bulletin International Conference Threat Intelligence Practitioners' Summit (TIPS) on Thursday, October 3rd. Our theme for the TIPS track is **Resilience Through Collaboration**.

VB2024 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 the critical security issues and emerging threats.

Check out the VB2024 program and speakers here.

VB2024 will be held at the Clayton Hotel Burlington Road in Dublin (Leeson Street Upper, Dublin 4, Ireland D04 A318). Hotel bookings can be made via this link.

We hope to see you there!

vb 2024 DUBLIN 2–4 Oct 2024

CYBER THREAT ALLIANCE

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>14 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	33%
IP ADDRESS	17%
DOMAIN NAME	7%
URL	6%
NETWORK TRAFFIC	29%
FILE PROPERTIES	6%
HOST	2%

TOTAL EARLY SHARES

3-5
PER WEEK

1,100+

CTA Member Feature

PLAYING DEFENSE: HOW CYBERSECURITY IS A TEAM SPORT

A few months back at RSA 2024, I spoke to a threat analyst who still stays with me. Let's call this analyst "John," who works for a cybersecurity company called "Cyberdons" for the sake of anonymity. This company curates a wealth of threat intelligence with sensors that can quickly see a relatively large amount of internet traffic.

John recounted a very well-known, large-scale cyber-attack that took place a few months back. John boasted that Cyberdons was aware of the Command-and-Control server the malware backdoor was reaching out to months before the attack occurred. Even with that intel, the cyberattack was successful, and Cyberdon's knowledge did not prevent it from happening.

Unfortunately, this isn't a new story in the world of cybersecurity. Prospects are often fed empty promises, like "If you become our customer, we will keep your business protected." While that may be true, cybersecurity practitioners respond to a higher calling. Yes, the bottom line pays the bills, but how can we achieve the best level of protection for our customers and, by extension, the public at large? If this requires working across company lines, so be it.

That's why Juniper chose to become part of the Cyber Threat Alliance. We know that as a member, we are all working towards a common goal. For example, when Juniper Threat Labs identifies a piece of malware, analyzes it, and extracts additional IOCs from the Advanced Threat Protection Cloud sandboxes, we can share this threat data with the members of the alliance which the customer has chosen as an EDR to keep our common customers protected.

Cybersecurity is a team sport. Threat researchers and analysts understand that and effectively share threat information across our closed online channels. But we're barely scratching the surface of what we can do together regarding a structured collaboration between cybersecurity vendors.

Juniper Networks chose to join CTA because of its members' quality, the real-time threat intelligence (TI) sharing platform quality, and the early share program of pre-publication research.

There have also been several attempts at cybersecurity interoperability between tools, but I don't see a universal standard emerging. Interoperability enables tools to collaborate in identifying and eradicating threats while giving the user a common view for situational awareness.

I hope that when it comes to new tools like Gen AI that they will bridge the gap that standard APIs have been unable to do.

BY MOUNIR HAHAD
HEAD OF JUNIPER THREAT LABS & CLOUD SECURITY ENGINEERING

CTA Partner Feature

COMMUNITY AND COLLABORATION ARE KEY TO DEFENSE

The interconnected nature of technology poses a range of security challenges. But it also provides opportunities for network defenders and their ability to collaborate. It allows organizations to sync faster and easier than ever before. Twenty years ago, corporate network defenders operated in silos, largely disconnected from peers in other companies. Today a vast global network exists through which companies can connect, combating a common set of digital threats and security challenges. This can lead to better security outcomes.

A connected defense is essential. When new dangers emerge, spreading awareness and information quickly leads to fewer organizations getting caught off-guard. A network defense makes prevention and detection easier and recovery more manageable. Building this network, however, requires more than setting up a couple of listservs and a sharing platform. It requires building a sense of community and a common purpose, which enables companies to both add to the community's collective knowledge as well as benefit from it.

For example, the Information Technology-Information Sharing and Analysis Center (IT-ISAC) has developed an array of Adversary Attack Playbooks – over 200 guides on various adversaries, mapped to the MITRE ATT&CK® Framework. Each piece of information shared by member organizations helps build out a more robust library of playbooks that can then be used by organizations to defend against future attacks.

Additionally, working with member companies, the IT-ISAC developed the Predictive Adversary Scoring System (PASS), a tool built from the Attack Playbooks' data. This tool, presented at this year's CARO Workshop, helps organizations highlight which adversaries they should prioritize monitoring. Its creation was driven by the help of a number of member organizations who volunteered their time, expertise, and data; the tool now helps at-risk companies target potential threats they may not have known about without the help of shared data and intelligence.

These are just a few examples of the power of community-driven information sharing. Of course, the Cyber Threat Alliance serves as another success example, demonstrating that there is more than one model. The overall goal is to collaborate outside one's own organization to multiply their knowledge many times over. Doing so not only bolsters self-defense, but helps create a safer digital environment for all.

BY SCOTT C. ALGEIER
EXECUTIVE DIRECTOR OF IT-ISAC

CTA HOSTED WEBINARS ON DEMAND

https://www.youtube.com/channel/UCKF94z58tZRp9kBLJmjzVzA

CTA: COMMUNITY DRIVEN DEFENSE — THE POWER OF UNITY

The Cyber Threat Alliance (CTA) has been a catalyst in uniting cybersecurity vendors from around the globe to identify, share, and counteract cyber threats. This united front harnesses collective intelligence, resources, expertise, and industry best practices to fortify the security stance of the entire community. Pooling cyber threat intelligence enables participants to tackle emerging threats swiftly and more effectively.

When it comes to cyber intelligence, the more data, context, and metadata you have the better your decisions can be. Access to data enables security teams to identify threats as they are emerging and respond quickly when they do. The CTA embodies this spirit of cooperation, drawing on diverse sources, perspectives, and expertise that improves the detection and protection capabilities of our members and provides stronger security defenses for their customers.

CTA members understand that we are stronger when we work together. No single cybersecurity vendor possesses all the data necessary to fully comprehend an attack's intricacies. Therefore, it is essential that the industry work together and share threat intelligence. Cybersecurity vendors should understand that they compete on their technology, not the data. To get that holistic picture of the cyber threat landscape, what allows us all to better protect our organization and customers, we must work together and share intelligence.

CTA members recently surpassed a major milestone, having shared 500 million indicators of compromise. This allows for more thorough understanding of malicious activity and allowing for better and faster cyber protection across their respective customers. Tailored to meet the unique requirements of each member, the CTA platform bolsters the collective strength of the cybersecurity industry. The richness of shared data, context, and metadata enhances decision-making, allowing security teams to swiftly identify and counter cyberthreats.

CTA also plays a pivotal role in the unified response to major cyber incidents, including the Log4j vulnerability, SolarWinds breach, and others. This collaboration enables members to align their understanding of threats, focusing on effective detection and mitigation strategies, thereby streamlining research and conserving resources. Such coordination is crucial in accelerating response and fortification efforts.

CTA members recognize the amplified strength achieved through unity. Sharing threat intelligence is vital for a comprehensive understanding and effective countermeasures, underscoring the importance of industry-wide collaboration. The power of unity ensures better protection for all.

Of course, collaboration isn't free. It requires time and money to be effective. However, CTA members recognize the benefits that come through collaboration, both for themselves and the broader community, and they have invested in CTA to tap into that strength. If you take a look, we think you'll reach the same conclusion – the benefits of CTA membership are worth the investment. Come and join us in our adventure – and make both yourself and your community better off.

BY JEANNETTE JARVIS
CHIEF MEMBERSHIP AND COMMUNICATIONS OFFICER

CyberCX

CTA Member Feature

DELIVERING INTEL WITH SPEED AND ACCURACY TO MANAGED SERVICES CUSTOMERS

CyberCX joined the Cyber Threat Alliance in August 2022 and has been an active and valuable contributor to CTA since.

CyberCX was founded in 2019, with the vision of creating a sovereign cyber security company capable of handling significant cyber projects. Our mission, "Securing our communities," reflects our commitment to helping customers secure their businesses as well as the communities in which they operate. Headquartered in Melbourne, Australia, we are the largest end-to-end cyber security provider in the region, with a global footprint stretching into the United Kingdom and United States.

Australia and New Zealand's remoteness brings both pros and cons. A challenge is that many threat intel companies focus on the US and European markets. This is understandable given the scale of these markets but often means less relevant information for our region. This is why CyberCX built its own in-house intel capability. Our platform aggregates millions of data points each month. These are analyzed and enriched through automation and daily human analysis by our cyber threat intelligence practitioners. We extract and validate indicators of compromise (IOC), build threat actor profiles and map threat actor networks and relationships through the unique information and insight we have in our region. We collect, collate and share threat information – we also create intelligence through analysis, expertise and regional insights.

We faced several challenges: obtaining region-specific information and intelligence, delivering it swiftly to 200+ Managed Services Customers using diverse logging platforms like Splunk and Sentinel. Fortunately, we had scalable methods for managing these platforms. We needed a way to deliver intelligence from partners and our CyberCX Intelligence team to customers, capture sightings, and share anonymized data with other CyberCX teams.

We built a middleware platform to accept and disseminate information quickly. When our Digital Forensics and Incident Response (DFIR) team finds and enters an IOC, our intelligence team validates and releases it. Managed Security Services (MSS) then distributes it to customers in under 30 minutes, triggering new alerts and performing automatic backward checks. Sightings are collected, anonymized, enriched, and stored for further analysis. Within the first week of operations, our intelligence team identified a new botnet operating only in this region.

We have since advanced beyond detection to actively blocking threats. Internally, we use file hashes identified by DFIR in our application control product. We manage dynamic lists of curated IOCs, which customers can implement in firewalls or other tools to block and return sightings.

We developed a method to deliver IOCs to Defender for Endpoint, or Defender for Office 365, including unmanaged devices, to block and return sightings. We are testing similar capabilities for other Endpoint Detection and Response tools, with positive results. The intent is to provide this capability to smaller organizations who cannot do so themselves.

BY MARK HOFMAN
CHIEF SECURITY OFFICER
CYBERCX

Telefónica Tech

CTA Member Profile

MEMBER SPOTLIGHT: TELEFÓNICA TECH

WHY DID TELEFÓNICA TECH JOIN CTA?

We believe in collaboration and thus joined the CTA to share cyber threat information between different organizations. Joining CTA is one crucial element enabling us to be a part of and provide our security knowledge together in return, take advantage of an extensive global network for revealing threat information that enhances the speed which we can protect all our customers around the world.

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

As a member of CTA, we receive real-time, actionable insight into new threats so that organizations can preemptively adopt defenses against them. All this intelligence sharing helps us process and neutralize threats faster and more effectively, which in translation means better security for our customers.

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

CTA is a staple in the cybersecurity landscape as it ensures collaboration between many sectors. By encouraging sharing and collaboration among all participants, the platform equips everyone with information that can help to improve overall cyber resilience while coalescing a more tight-knit security ecosystem.

WHAT VALUE DO YOU GET FROM CTA?

Our CTA membership has provided us with tremendous value, such as high-quality threat intel and avenues for collaboration amongst fellow cybersecurity industry thought leaders, while co-developing cyber secure best practices & standards. This is complementing our services and strengthening our standing in the market.

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

The rapid evolution of cyber threats with the sophistication and coordination required to attack security posture makes information sharing a critical component in today's cybersecurity landscape. By sharing information, organizations can more easily predict what attacks will be coming and from where and they are able to reduce response time and restrict the impact of cyberattacks.

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

We are enthusiastic about the cutting-edge collaborations and combined projects we have pursued through CTA. These efforts have not only enhanced our capabilities to identify and respond but also led the security industry into various novel cybersecurity methods, countermeasures or strategies.

WHAT DOES TELEFÓNICA TECH VALUE MOST ABOUT CTA MEMBERSHIP?

What we value most about our CTA membership is the collaborative network and access to cutting-edge threat intelligence. The ability to work alongside other industry leaders and share knowledge keeps us at the forefront of cyber threats and continuously enhances our services.

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

Participating in CTA Working Groups provides us with specialized insights and a deeper understanding of specific threats and critical events. This enables us to tailor our defenses and services to better protect our clients during high-risk events, ensuring a rapid and effective response.

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

One of the most significant emerging challenges is the rise of sophisticated, coordinated attacks by state actors and organized criminal groups. CTA can help mitigate these concerns by strengthening intelligence sharing, promoting collaboration between the public and private sectors, and developing advanced strategies and technologies to combat these threats.

WHERE DO YOU SEE CTA IN 5 YEARS?

We see CTA as an even more integral and crucial organization for global cybersecurity, expanding its member network and continuously improving its information-sharing capabilities. We expect CTA to lead key initiatives that strengthen collective resilience and set new industry standards