JUNE 2024

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

This quarter's newsletter focuses on using cyber threat intelligence sharing to bridge gaps. Our members and partners have many different perspectives on the gaps we face, and those differences come through in the different articles. They talk about gaps in understanding a threat, knowing what actions to take, or prioritizing policy actions. The common theme, though, is that we rarely know enough on our own – and sharing is the only way to get the information needed.

While sharing may be CTA's primary mission, we hardly have a monopoly on it. In fact, we are working hard to increase the level of sharing in our digital ecosystem outside of CTA; we collaborate with many different efforts including the World Economic Forum's Partnership Against Cybercrime, the Ransomware Task Force, and the Common Good Cyber initiative. Again, a common theme across these efforts is that they require sharing to work well. Without sharing, the initiatives are just ideas. Cybersecurity is challenging as an issue because it crosses almost every boundary you can imagine. As a result, the only way to tackle it is by sharing to bridge the gaps between companies, industries, countries, or disciplines.

Despite these challenges, though, I will make a bold assertion – we are starting to bridge the cybersecurity gaps. We still have a long way to go, but we know what we need to do and we know how to do it. We are starting to develop the empirical basis to assess which cybersecurity actions produce the best results. We have frameworks in place to prioritize decisions, and we are starting to collect the data we need to make better policy decisions. The outlines of how we can collectively make the digital world safer and more resilient are coming into focus. The problems may be serious, but we have some reasons for optimism.

I hope this issue of CTA's newsletter provides some insights into how you might be able to bridge a gap that is preventing a desired outcome. And if you want to know more about what CTA or its members or partners are doing, please do not hesitate to reach out. We'd be happy to share with you – that is our mission after all.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

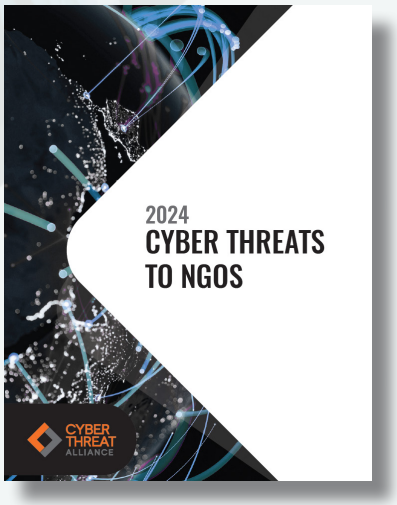
CYBER THREATS AGAINST NGOS

CTA's newest Joint Analytic Report is now available, Cyber Threats to NGOs. This project was led by Chelsea Conard, CTA's Cyber Threat Report Analyst, and was funded by a generous grant from Craig Newmark. Numerous CTA members and partners provided essential collaboration in creating this report. We would like to express our gratitude for your contributions.

Non-governmental organizations (NGOs) face unique challenges addressing cyber threats. This report outlines prevalent threats, suggests remediation strategies, and provides guidance for the executive leadership to enhance their nonprofit's cybersecurity posture.

Aimed at empowering NGOs, this report is designed to equip organizations with an understanding of prevalent cyber dangers and to arm them with effective countermeasures.

This report serves as a call to action, urging NGOs and the cybersecurity industry to address these cybersecurity challenges head-on. By fostering a culture of proactive cybersecurity management, NGOs can significantly enhance their resilience against cyber threats.



CYBER THREAT ALLIANCE

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>10 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	41%
IP ADDRESS	16%
DOMAIN NAME	6%
URL	5%
NETWORK TRAFFIC	23%
FILE PROPERTIES	7%
HOST	2%

TOTAL EARLY SHARES

3-5
PER WEEK

1,000+

CTA Member Profile

MEMBER SPOTLIGHT: PALO ALTO NETWORKS

WHAT DOES PALO ALTO NETWORKS VALUE MOST ABOUT CTA MEMBERSHIP?

We value the ability to regularly communicate with our competitors to see what insights they have, what threats they are seeing and to bounce ideas off of them. Being able to collaborate across organizations allows us to see a much bigger picture of an attack, an adversary or novel techniques.

There is also value in pre-sharing threat intelligence before public disclosure, to get in front of a threat and deploy protections across all of our customers. Sharing critical information allows us to be ready to address questions about a threat from our leadership and customers.

HOW DOES BEING PART OF CTA HELP PALO ALTO NETWORKS PROVIDE GREATER SECURITY FOR CUSTOMERS?

Being part of CTA shows we are focused on protecting customers first. We're sitting side by side with our competitors, showing up consistently and working towards that collective goal. Sharing indicators, TTPs and context across the CTA allows us to have a continuous stream of data. No one company has all of the information, together we paint a better picture of who the adversaries are and how we can fight them together.

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

We hope the CTA can be an example of the type of sharing that can happen between government organizations, public/private partnerships, and others. The CTA also moves the needle by participating in various work groups that focus on specific threats to large events (e.g., summer Olympics or elections) or industry verticals (e.g., NGOs).

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

We're excited about the relationships built with both the CTA staff themselves and the member companies, where we hold each other accountable. Also about the commitment to what we are collectively trying to achieve, with the realization that we all have businesses to operate. These types of relationships really raise the bar for Palo Alto Networks, and we help to raise the bar for everybody else in return. We can also be a unified force to hold entities not in CTA accountable.

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

AI is one of those things where businesses are very quick to roll it out and don't often think through what they are building and deploying, security concerns, personal information, customer data, etc. Could there be potential vulnerabilities inside the tooling they are using and building in AI? How do we best position the CTA to be the standard that organizations aspire to be a part of, learning from the lessons CTA already has under its belt?

WHERE DO YOU SEE CTA IN 5 YEARS?

We see it getting at least 2-3 times the size it is today, with a lot more participation from organizations, getting greater value from the data we are sharing. Rather than focusing on mass sharing of IoCs, we can focus more on how we collaborate and scale, and how we quickly create workgroups to solve complex problems that help to protect all of our customers. We see us showing the world how we make the world a safer place.

CTA Member Feature

BE THE GUARDIAN OF CYBER SPACE

TEHTRIS
FACE THE UNPREDICTABLE

The Power of Shared Intelligence

In the ever-evolving digital landscape, being the guardian of cyber space requires more than just advanced technology; it demands shared intelligence and collaboration. TEHTRIS values ethics, collaboration, resilience, innovation, and trust, believing that sharing threat intelligence is crucial to maintaining a secure cyber environment. Organizations can become guardians of cyber space by partnering with cybersecurity experts who share the vision of securing freedom for everyone and everywhere.

The Importance of Sharing Threat Intelligence

Sharing threat intelligence is vital for a proactive cybersecurity strategy. By exchanging information about potential or existing cyber threats, organizations can enhance their ability to detect, respond to, and mitigate risks. This collective approach provides a holistic view of the threat landscape, helping identify patterns and connections that might otherwise go unnoticed. By collaborating, organizations can create a stronger, more resilient defense against cyber adversaries, embodying TEHTRIS' values of collaboration and resilience.

How Shared Threat Intelligence Works

The process involves collecting, analyzing, and disseminating threat data. Organizations use various tools to gather intelligence from different sources. This data is then analyzed to provide actionable insights. TEHTRIS exemplifies innovation and trust through its Cyber Threat Intelligence (CTI) integrated with its Extended Detection and Response (XDR) platform, offering real-time, contextualized intelligence that enhances detection and response capabilities. By leveraging data from multiple endpoints and users, TEHTRIS can better anticipate and mitigate emerging threats.

TEHTRIS and CTA

TEHTRIS is committed to being a guardian of cyber space by engaging with CTA, a nonprofit dedicated to improving global cybersecurity through sharing high-quality, near-real-time threat information. By contributing its extensive cyber intelligence via its innovative XDR solution, TEHTRIS enhances the detection and anticipation capabilities of the entire alliance.

By sharing intelligence and fostering synergies across sectors and regions, TEHTRIS and CTA strengthen the cyber defense landscape, promoting a safer digital environment worldwide. It not only protects its clients but also fortifies the broader digital ecosystem, turning every organisation into a guardian of the cyber space.

CTA Member Feature

BRIDGING THE GAP WITH SHARED CYBER THREAT INTELLIGENCE:

HOW RED PIRANHA AND CTA ARE HELPING UKRAINE IN THE EFFORTS AGAINST RUSSIA

Red Piranha has participated in the recent call for collaboration to assist Ukraine in its efforts against Russia. The Cyber Defensive Collaborative (CDAC) has been working to enhance Ukrainian cyber defensive efforts by sharing threat intelligence across critical assets.

This shared cyber threat intelligence fosters a culture of collective defense. Rather than operating in isolation, organizations benefit from the combined expertise and insights of a diverse network of stakeholders. This collaborative ecosystem strengthens the overall resilience of the cybersecurity community and enhances the ability to thwart sophisticated cyber attacks.

As cyber threats continue to evolve and grow in sophistication, organizations across all sectors face an ongoing challenge in safeguarding their systems and data from malicious actors. Red Piranha designed its platform Crystal Eye to include Automatic Actionable Intelligence. This idea of shared cyber threat intelligence enhances situational awareness by pushing intelligence into the operations stack for immediate outcomes. This data is then contextualized and shared with other nodes, as well as being fed back into the platform. Red Piranha can then share intelligence and collaborate with industry peers via the Cyber Threat Alliance that includes government agencies and cybersecurity vendors. Organizations gain a broader perspective on emerging threats, attack techniques, and vulnerabilities faster and more efficiently. This collective intelligence between the CDAC, CTA, and participating partners like Red Piranha enables Ukraine to stay ahead of evolving threats and proactively fortify their defenses in real time.

The Cyber Threat Alliance shared threat intelligence facilitates faster detection and response. With access to real-time threat feeds and intelligence reports, organizations can quickly identify suspicious activities and then use this information to protect organizations globally. This early detection minimizes the dwell time of threats, reducing the potential impact of cyber incidents and improving incident response capabilities.

By leveraging insights from collaborative platforms and information-sharing communities, organizations can prioritize their security efforts based on the most relevant and prevalent threats. This targeted approach ensures that limited resources are directed towards addressing the most critical risks. Shared cyber threat intelligence plays a vital role in bridging the gap in cybersecurity by enhancing situational awareness, enabling faster detection and response, optimizing resource allocation, and fostering a culture of collective defense.

BY ADAM BENNETT
CEO

CTA Partner Feature

BRIDGING THE GAP WITH SHARED INTELLIGENCE:

CYBER INTELLIGENCE SHARING FOR SMALL FIRMS

With multiple regulations around the world emphasizing the need to share cybersecurity information, the question of how to comply with these demands can be daunting for a small company.

Historically, threat intelligence teams were viewed as a luxury even for medium to large firms. A small firm could have a dozen cyberdefense tasks under one or two people. In such a situation, specialization is impossible. So how do you engage in information sharing effectively without staff dedicated (or trained) for it?

Three Steps to Information Sharing

First, understand what your true needs for intelligence are. One should not engage in information sharing just to be compliant with a regulator's recommendation. Threat intelligence can drive a prioritized and focused cyberdefense team that supports the needs of the business lines.

Second, understand what your business requires from information security. In most institutions, that includes keeping sensitive information confidential, maintaining the products and services available to your customers, and ensuring the data held by your company is free from corruption. Examining your IT environment and your business itself will reveal your critical processes and partners/vendors. If able, engage with a managed security service provider (MSSP) to support the simpler security tasks of consuming automated data feeds so your internal staff can focus on consuming threat intelligence.

Finally, identify the means of sharing information. FS-ISAC's real-time information-sharing network provides a secure platform to connect with and learn from peers.

Sharing Information Helps Small Firms Use Cyber Intelligence

For smaller institutions, sharing with your peers offers multiple advantages.

As your budget likely constrains hiring a large team – not to mention the ever-present challenge of a talent shortage – you can leverage your peers to crowdsource what you are unable to specialize in. Peers usually face the same cyber threat actors and have the same tool sets, so their knowledge of the threat augments your own resources. However small your piece of the threat landscape may be, it is one piece of a much larger jigsaw puzzle that peer-to-peer intelligence sharing can clarify.

Sharing can also improve your supply chain risk calculations. Many of your peers will likely be using the same third parties that you are, so knowing vendor vulnerabilities and any historic or current threats against them can add to your knowledge bank.

By focusing on prioritizing the threat intelligence you consume and engaging with peers on the primary threats against your firm and customers, even a small firm can use cyber intelligence.

BY TERESA WALSH
GLOBAL INTELLIGENCE OFFICER

CTA Member Feature

BRIDGING THE GAP WITH SHARED INTELLIGENCE

SONICWALL®

In a threat landscape where adversaries can change their exploitation tactics on a frequent basis, having access to the latest trends and patterns is vital for any IT security vendor or security team of an organization to effectively deploy necessary countermeasures and policies to detect and prevent potential threats. Hence, industry collaboration is vital for enabling everyone to provide the most comprehensive defense.

Timing

Timing is everything – it is not enough just to share latest threat intelligence, but also to do it in a timely manner. To ensure timing, it would be wise for the industry to invest in automation and cloud computing infrastructure specifically dedicated to sharing data, trends, sources and IOCs. Along with such infrastructure, additional software logic (AI/ML/etc..) should be developed to validate the artifacts as well as suggest possible protection policies and incident response and investigation action items directly to the threat hunting teams.

Diversity

Diversity of threat intelligence sharing participants is also very important. Some vendors have strong visibility only in specific geographical regions, other vendors have visibility and deployments only in specific verticals (schools and universities, etc...) and some are focused on SMBs or consumer segments, and some have strong presence in enterprise and Fortune 100 networks. Some have visibility into corporate network traffic, some directly on the endpoint and some are in private and public cloud. Because certain types of threats may primarily be observed only in certain types of environments – having comprehensive presence among sharing participants across deployment types, geographies and product types is essential in creating an effective shared threat intelligence environment.

Accuracy

Ensuring accuracy of shared data is also critical to building a viable shared threat intelligence. Shared threat intelligence platforms need to create a system of rules and processes which place an equivalent of an accuracy score on all shared data so that users of these platforms can determine where and how to apply policies using the shared data based on the score.

Commercial vs Voluntary Sharing Platforms

The emergence of well-established commercial IOC repository sharing platforms has created a trend where reliance of voluntary sharing has been reduced. The industry's goal here could potentially be a creation of a superset sharing platform model which combines voluntary and commercial sharing platforms.

CTA is a leading organization that enables industry collaboration among security vendors, government organizations, and other sources, and can be used as a forum for creation of such superset sharing platform.

BY ALEX DUBROVSKY
VICE PRESIDENT OF SOFTWARE ENGINEERING & THREAT RESEARCH

CYBER NONPROFITS RECEPTION

On May 7th, CTA and Nonprofit Cyber organizations sponsored a reception during RSA. Nonprofits are driving significant improvements to our internet security, policy, privacy, and safety. RSA attendees were able to learn about these important organizations and the amazing impact they are making to the foundation of a safe and secure internet for all.

Our immense gratitude goes to the reception sponsors. The event's success was made possible by their generosity. We are honored to have your support.

CYBER THREAT ALLIANCE · Nonprofit Cyber · MITRE ENGENUITY Center for Threat Informed Defense · CIS Center for Internet Security · CREST · CSA cloud security alliance · CYBER READINESS INSTITUTE · CyberPeace Institute · OPEN CYBERSECURITY ALLIANCE · SHADOWSERVER · SIGHTLINE SECURITY

CARO 2024 CONFERENCE

CTA hosted the CARO 2024 conference May 1-3rd in Washington, DC. We kicked off the conference with a reception at the SPY Museum and followed with two full days of presentations by leading cybersecurity industry experts focusing on our theme: *Driving Back the Shadows: Connecting Research to Action*. Our heartfelt thanks to the conference speakers for their invaluable presentations that were instrumental to the overall success of the event.

One highlight during the conference was the fascinating entertainment at our gala dinner, Magician Peter Wood, Collector of the Impossible. See CTA's own Michael Daniel flamboozoled by Peter's magic.

We are deeply grateful to our sponsors for their generous support. Thank you!

Palo Alto Networks, Diamond Sponsor
Fortinet, Silver Sponsor
NTT, Association Sponsor
SE Labs, T-shirt Sponsor