CISA
CYBERSECURITY
ADVISORY
COMMITTEE

REPORT TO THE CISA DIRECTOR

Technical Advisory Council

Vulnerability Discovery and Disclosure Recommendations

June 22, 2022

Introduction:

The Technical Advisory Council Subcommittee was established to leverage the imagination, ingenuity, and talents of technical experts from diverse background and experiences for the good of the nation. The subcommittee was asked to evaluate and make recommendations tactical and strategic in nature. These Cybersecurity Advisory Committee (CSAC) recommendations for the June Quarterly Meeting focus on vulnerability discovery and disclosure.

CSAC conducted interviews with sector-specific agencies such as the Food and Drug Administration (FDA), product vendors, and CISA staff to determine the current state of vulnerability discovery and disclosure practices across government and industry and provide meaningful recommendations.

The act of disclosing a security vulnerability for an impacted system at first seems simple: Contact the maker or party responsible for a hardware or software system and report the problem. Unfortunately, in today's world it is not that simple, with competing equities, jurisdictions, regulations, legalities, and sometimes no clear reporting contact. Some manufacturers are responsive to reports, while others are hostile. What if the manufacturer can't be located or no longer exists?

The reporting party now has an ethical dilemma. They could stay silent while everyone dependent on the vulnerable system continues to use it, oblivious to the risk. They could make a public announcement revealing the vulnerability to put everyone on notice while also putting everyone at risk.

In this environment, CISA, acting as the nation's civilian defense agency, has the opportunity to improve the disclosure process through improved coordination, collaboration, and making the process more attractive to researchers, academics, and hackers wishing to do the right thing by reporting vulnerabilities.

Findings:

CISA is best positioned to support, enable, facilitate, promote, and shepherd collaboration between effected parties including asset owners, sector specific agencies, state, local, tribal, territorial, international government partners, product vendors, and security researchers to reduce the exposure of the nation to emerging cyber security threats. CISA should communicate cross-sector norms and baselines and work with sector-specific agencies to determine impact. CISA should provide existing tools and training that facilitate collaboration and transparent workflows between stakeholders in the vulnerability discovery, resolution, and coordinated disclosure lifecycle.

The challenge for CISA is to determine how to add value by increasing coordination and reducing duplication of effort. Some sector-specific agencies already operate their own incident response centers, including coordinating and sharing information with organizations in the particular sector. The maturity of the sector-specific agencies varies depending on budget, availability of scalable staff, how well they have integrated their workflows with others, etc.

It is not uncommon for researchers reporting vulnerabilities to be individual contributors, and as such have limited time and energy to navigate complex or lengthy vulnerability coordination processes. The more they are tied up with bureaucratic requirements, the less likely they are to want to engage with the disclosure process in the future. Reducing friction for those disclosing is important in creating a healthy ecosystem of researchers. If it is too difficult to report the vulnerability, the risk of researchers publicly disclosing or not reporting at all, increases.

Effective vulnerability programs are engaging, transparent, timely, properly staffed, and have a proactive feedback loop between product teams, security researchers, and sector-specific agencies. Each one of these elements offers an opportunity to improve the overall effectiveness of the program. For example, successful vulnerability disclosure programs rely on a number of incentives to attract researchers to their program. Such incentives include bounty payments, public recognition of their contribution, and professional and peer respect.

Recommendations:

CISA should implement the following actions in the respective timeframes to include:

- Develop incentives and access to information to aid security researchers who will submit vulnerabilities affecting critical systems. Examples include:
    - Grow the pool of potential researchers through work visa sponsorships and streamlined training opportunities.
    - Encourage continued participation by providing rewards such as public recognition and cash awards.
    - Make vulnerability reporting beneficial to researcher careers through internships and career networking opportunities.
    - Work with Congress and the Department of Justice to reduce legal liabilities for those wishing to report vulnerabilities with good faith, such as the DMCA exceptions for security research[i].
    - Standardize the reporting experience to reduce the back and forth necessary to clarify details.
    - Encourage the use of RFC 9116, security.txt which describes how to create a standardized way to inform security researchers on how to report a vulnerability[ii].
        - For the Federal civilian agencies for which CISA has strong authorities, make this a mandatory requirement.

- Encourage an environment that works to enable frustration-free vulnerability research and reporting.
    - Work with Congress and sector-specific regulatory agencies to require that manufacturers supply firmware images of every released version for the industry, which should be ultimately archived for future automated analysis.

- Invest in a central platform to facilitate the intake of suspect vulnerabilities and communication between security researchers, agencies, and vendors:
    - In order to help provide security researchers with a 'one-stop-shop' that will enable better disclosures and help them navigate government bureaucracies.
    - To improve visibility, transparency, communication, and resolution of vulnerabilities that affect multiple critical sectors.
- Simplify the reporting process and provide feedback to those reporting. Streamline the process to triage reported vulnerabilities and streamline the reporting process to reduce later uncertainty.

  - CISA should invest in a centralized role in coordinating with sector-specific agencies, to ensure high quality evaluation and communication of vulnerabilities identified in products in their sector constituents.
  - Ensure security researchers have visibility into the triage status of vulnerabilities they have submitted in the workflow.
  - Enhance information sharing by create interagency workflows with sector-specific agencies, product vendors, asset owners, and trusted security researchers.
  - Mitigate barriers to the technical community working with CISA by promoting, and improving upon, the existing portals such as Vulnerability Information and Coordination Environment (VINCE) to target specific industries.
  - Support and promote key industry-specific international security standards and actively participate in their working groups. For example, part 4-1 of ISA/IEC 62443, which requires product vendors to have Product CERT teams that include support and collaboration for vulnerability disclosure and discovery would enhance industry coordination, and CISA could participate in the 62443 committee working groups.

- Improve the notification processes after a disclosure has been verified and acted on.
  - Standardize the way in which reports are disseminated, in both human and machine-readable formats.
  - If applicable, connect the disclosure to the existing ATT&CK Framework[iii].
  - Ensure the disclosure information is easily searchable and can be sorted by make, model, brand, versions, and impacted sectors. Work with the community to leverage open-source projects (e.g., Industrial Control Systems (ICS) Advisory Project) and past ICS-CERT and US-CERT page approaches.

Conclusion:

The Vulnerability Disclosure lifecycle in complex, depending on human interactions and judgement calls on how critical a disclosure may be. Standardizing as many steps as possible while considering the burden of disclosure can help reduce the friction to researchers. Better coordination between parties, through automation or more actionable notices, will help reduce the gap between when a disclosure is made and when a defensive action can be taken.

CISA, acting as a coordinator and source of trusted expertise, is in a unique position to improve the Vulnerability Disclosure Process not just for Department of Homeland Security or the civilian federal government, but to act as a model for everyone.

The committee will continue to interview necessary stakeholders and provide more research, observations, feedback, and recommendations that will enable CISA to better serve the critical infrastructure community and provide greater incentives and experiences for security researchers to continually improve responsible discovery and disclosure.

CISA CYBERSECURITY ADVISORY COMMITTEE

Cyber Threat Intelligence Sharing Recommendations

Introduction:

The Technical Advisory Council Subcommittee was established to leverage the imagination, ingenuity, and talents of technical experts from diverse background and experiences for the good of the nation. The subcommittee was asked to evaluate and make recommendations tactical and strategic in nature. These Cybersecurity Advisory Committee (CSAC) recommendations for the June Quarterly Meeting focus on cyber threat intelligence (CTI).

CTI is leveraged by Defenders, Blueteams, Security Operations, and Information Technology staff small and large as a means to narrow the superset of potential threats and adversaries to a smaller, actionable set. In best case scenarios, high-quality threat intelligence shared in a timely and efficient manner will enable defenders to take actions. When positioned within a simple Protect, Detect, and Respond security framework, cyber threat intelligence has the following value proposition:

- Protect:
  CTI can be used to increase the security posture of entities including blocking traffic associated with an inbound threat, hardening specific configurations associated with an attack, patching, and reducing attack surface. CTI can also assist in identifying new patterns of attack which require additional controls.
- Detect:
  CTI, including Indicators of Compromise (IOC), can be used to analyze and hunt for adversary activity in an environment helping to scope the broad set of threats being monitored into a known set of active threats.
- Respond:
  Connected to detection, actionable IOCs can help Data Forensics and Incident Response (DFIR) and adversary eviction by sharing IOCs and general intel on how to remediate an active threat.

Given a general understanding of the value of effective threat intelligence, what role could and should CISA play in helping to distribute and disseminate threat intelligence? CISA is in a unique position of influence and centrality which enables an organization to curate, arbitrate, and disseminate high quality threat intelligence across the government and private sector due to its mandate, authority, and position of trust.

CSAC recommends that CISA continue to invest in this capability as it has a proven value. CISA must make this CTI capability effective for its consumers across government and private sectors.

Findings:

Currently, CISA has multiple programs with the goal to effectively facilitate dissemination of threat intelligence artifacts including:

- Cyber Information Sharing and Collaboration Program
- Automated Indicator Sharing

The CSAC has reviewed the documentation related to both programs and was able to understand its goal and challenges directly from the stakeholders within this program.

Based on this initial information, the CSAC has identified several opportunities for improving the effectiveness of its intel sharing program for private and public sector users. The following areas of improvement include:

- Consumption of CISA cyber threat intelligence is currently a manual process for many organization.
  - Not every organization has the resources, infrastructure, or expertise to consume and apply much needed threat intelligence in defense in an automated and scalable manner. This limits the impact of the programs.

- Threat intelligence is optimized for detection and its current form is less useful for prevention and response which is a missed opportunity for impact.
  - The format and content of CTI deliverables like IOCs require a lot of knowledge and expertise on the part of the user to convert information into a form that can be applied as prevention capabilities. Examples include endpoint device and Operating System policy changes or infrastructure configuration to reduce the attack surface.
  - Similarly, current IOCs are not optimized for DFIR or recovery and lack critical details for response.

- Smaller organizations, like local governments, lack the tools, infrastructure, and expertise to apply threat intelligence for either detection or proactive controls.
  - Inconsistent capabilities across potential end users of threat intelligence limit the ability for it to have consistent application and thus impact. Many state and local governments have a need for defense and an understanding of the applicability but lack resources and expertise for security infrastructure.
  - While free and/or opensource software instances of critical defense software like threat intelligence management, endpoint detection and response, network monitoring, and Security Information and Event Management (SIEM) capabilities exist, many users may not be aware of them or have a simple mechanism to apply and deploy these capabilities.

- Indicators are not consistently enriched.
  - CISA is in a unique position at the nexus of private and public cybersecurity defense networks and communities. This means there is an opportunity to facilitate both technical enrichment (dynamic analysis, automated data intersection) and crowd sourcing of intel (comments, tagging, confidence votes) to improve the scope and impact of CTI indicators and make the Nation as a whole more secure. Today, only the base indicators are shared leaving an opportunity for impact.

These four problem areas are based on an initial assessment of CISA's threat intelligence sharing programs. More research, interviews, and analysis are required to identify more concrete challenges.

Recommendations:

- Invest in a program to make "threat intelligence as a service" available to all qualified users.
  - A portal which provides a fusion of indicators, automated feeds, crowd source comments, tagging, and enrichment with dynamic analysis would be a force multiplier for defenders who lack the resource or skill to create their own infrastructure. An example of a public service that exhibits many of these capabilities is Virustotal. A comparable service run by CISA and optimized for threat intelligence over malware analysis could have considerable impact and address many of the existing gaps.
  - Reducing the barrier to entry for consumption and application of threat intelligence will broaden its reach and impact smaller organizations, in particular.

- Invest in enriching threat intelligence reports to be more applicable across the three key layers of defense.
  - Non-durable IOCs, like Domain Name System or Internet Protocol information, have a limited time-to-live and are easily circumvented by attackers. If CISA was to increase focus on development and distribution of additional artifacts like group policy and configuration management scripts, and automated attack surface tooling given its unique view across industry and government, it would have a larger impact in defense by preventing attacks.

- Develop and distribute a common opensource stack available to all.
    - Providing simple-to-download virtual machines or containers that include preconfigured threat intelligence management, SIEM, network analysis, and Endpoint Detection and Response agents along with training information would allow broader reach and impact of threat intelligence. This would enable smaller organizations to consume from CISA not only the information on threats but the means to apply this information in defense.

- Explore techniques to enable scalable and effective development of expertise in CTI.
    - Related areas of cybersecurity, such as Vulnerability Research and Penetration Testing, have mature and scalable educational resources, frameworks, and platforms that help in developing needed talent. However, analogous resources for CTI seem to be limited and ad hoc. CISA can encourage the development of and improve the visibility of comprehensive training material, aligned with the technical suggestions above, that could be used by smaller organizations to upskill existing talent.

Conclusion:

CISA is in a unique position to help all organizations in the U.S. become more secure by providing a real-time Threat Intelligence platform that not only has actionable IOCs but is also easily integrated with existing technology used by public and private organizations across the board. The CSAC will continue to investigate opportunities for improving CISA threat intelligence capabilities as the CSAC moves from draft to final form.

References:

1) *Vulnerability Information and Coordination Environment*
2) *Adolus: Framework for Analysis and Coordinated Trust*
3) *Finite State*
4) *NetRise Turbine: Next-Generation Firmware & IoT Security Platform*
5) *ICS Vulnerability Advisory Project Portal*
6) *Assessing the Potential Value of Cyber Threat Intelligence Feeds - Watson*
7) *Data-Driven Threat Hunting Using Sysmon - Vasileios Mavroeidis*
8) *MISP - Open Source Threat Intelligence Framework*
9) *Using Open Tools to Convert Threat Intelligence into Practical Defenses: Threat Hunting Summit 2016*

[i] https://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act#Anti-circumvention_exemptions

[ii] https://www.rfc-editor.org/rfc/rfc9116

[iii] https://attack.mitre.org/

Appendices (pertains to both Recommendation areas):

Acronyms

ACRONYM	DEFINITION
CERT	Cyber Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CISCP	Cyber Information Sharing and Collaboration Program
CVD	Coordinated Vulnerability Disclosure
DFIR	Data Forensics and Incident Response
DOE	Department of Energy
FDA	Food and Drug Administration
ICS OT	Industrial Control Systems Operational Technology
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IOC	Indicator of Compromise
ISA/IEC	International Society of Automation / International Electrotechnical Organization
IT	Information Technology
OS	Operating System
SIEM	Security Information and Event Management
TAC	Technical Advisory Council
TI	Threat Intelligence
TSA	Transportation Security Agency
US-CERT	US- Cyber Emergency Response Team
VINCE	Vulnerability Information and Coordination Environment

Acknowledgements:

Technical Advisory Council Members:

Mr. Jeff Moss, Subcommittee Chair, DEF CON Communications

Mr. Dino Dai Zovi, Security Researcher

Mr. Luiz Eduardo, Aruba Threat Labs

Mr. Isiah Jones, National Resilience Inc.

Mr. Kurt Opsahl, Electronic Frontier Foundation

Ms. Runa Sandvik, Security Researcher

Mr. Yan Shoshitaishvili, Arizona State University

Ms. Rachel Tobac, SocialProof Security

Mr. David Weston, Microsoft

Mr. Bill Woodcock, Packet Clearing House

Ms. Yan Zhu, Brave Software

Briefers and Other Subject Matter Experts:

Ms. Lindsey Cerkovnik, CISA Cybersecurity Division Vulnerability Disclosure

Mr. Jay Gazlay, CISA Cybersecurity Division Vulnerability Disclosure

Mr. Jeremiah Glenn, CISA Cybersecurity Division

Mr. Eric Goldstein, CISA

Ms. Aftin Ross, U.S. Food and Drug Administration

Mr. Rob Suarez, Becton, Dickinson, and Company

Ms. Nastassia Tamari, Becton, Dickinson, and Company

Ms. Jessica Wilkerson, U.S. Food and Drug Administration

Mr. Beau Woods, CISA