Threat Hunting

July 13, 2023

Fiscal Year 2023 Report to Congress

Homeland Security

Cybersecurity and Infrastructure Security Agency

Message from the Director

July 13, 2023

The following report, "Threat Hunting," was prepared by the Cybersecurity and Infrastructure Security Agency (CISA).

This document has been compiled pursuant to direction in the Joint Explanatory Statement that accompanies the Fiscal Year (FY) 2023 Department of Homeland Security Appropriations Act (P.L. 117-328). The report provides an overview of CISA's ability to provide cyber defense and incident response services for the Federal Civilian Executive Branch (FCEB); state, local, tribal, and territorial (SLTT) governments; and all critical infrastructure (CI) sectors.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable David Joyce
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Henry Cuellar
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Chris Murphy
Chair, Senate Appropriations Subcommittee on Homeland Security

The Honorable Katie Britt
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to the CISA Office of Legislative Affairs at (202) 819-2612.

Sincerely,

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

The Threat Hunting (TH) subdivision is part of CISA's Cybersecurity Division, which collectively works to reduce cybersecurity risk facing American organizations. As part of this mission, TH's mission is to "hunt cyber threats against U.S. infrastructure to mitigate national risk." To achieve this mission, TH leverages authorities and sophisticated capabilities to search proactively through networks, endpoints, and datasets to identify malicious, suspicious, or risky activities that have evaded detection by existing tools. Information gathered is used to inform stakeholders so that they may remediate cyber threat activity.

TH uniquely is positioned to synthesize and enrich diverse data from across FCEB, SLTT, CI, and partners, including via CISA's Joint Cyber Defense Collaborative, the Intelligence Community (IC), Department of Defense, federal law enforcement partners, and private-sector cybersecurity firms, to detect, understand, and drive mitigation of malicious cyber activity rapidly. TH leverages unique technical visibility across a diverse stakeholder group to develop and drive execution of actions mitigating risk to U.S. CI entities.

TH tracks, correlates, and analyzes cyber threat information from IC partners, private-sector firms, and CISA's data holdings to build a comprehensive picture of the cyber threat environment and to drive operational priorities. To execute this mission, TH maintains and is developing a variety of operational capabilities, including persistent hunting of network traffic from the evolving National Cybersecurity Protection System, CyberSentry host and network metadata within partner infrastructure, and newly available and growing host-level visibility into FCEB partner environments, enabling CISA's FY 2021 National Defense Authorization Act Section 1705 authorities (codified at Title 44 of the U.S. Code § 3553(b)(7)) to "hunt[] for and identif[y], with or without advance notice to or authorization from agencies, threats and vulnerabilities within Federal information systems." TH capabilities also extend to the ability to conduct malware reverse engineering and manual forensic analysis on suspected compromised media. Findings from TH analyses and engagements are disseminated widely via cybersecurity advisories and/or alerts jointly produced with CISA partners to enable broad identification and remediation of cyber threats.

Many of TH's capabilities are designed to be persistent and scalable; indeed, the breadth of the threat facing the Nation demands scalability. In some unique cases, TH provides a resource-intensive engagement service intended to identify and mitigate adversary activity on stakeholder systems and to discover tactics, techniques, and procedures not yet publicly available in the cybersecurity community.

When considering CISA's "total capacity of threat hunting and incident response capability," as directed by Joint Explanatory Statement, it is important to note this fundamental transition from reactive response to persistent hunting. TH's goal is to maintain continuous visibility into threat activity targeting FCEB agencies and the highest-risk nonfederal organizations, allowing immediate intervention to address threat activity before malicious actors can achieve their objectives. In this new model, it is less relevant to measure the number of "incidents" or "engagements" to which CISA can respond, and instead to consider how the breadth of persistent visibility enables execution of this new model.

Threat Hunting

Table of Contents

I. Legislative Language

This report was compiled in response to direction in the Joint Explanatory Statement that accompanies the Fiscal Year (FY) 2023 Department of Homeland Security (DHS) Appropriations Act (P.L. 117-328), which states:

> *Threat Hunting*.—Not later than 60 days after the date of enactment of this Act, CISA shall provide a report to the Committees on the total capacity of threat hunting and incident response capability it has developed, using a metric by which its ability to respond to the severity and quantity of incidents can be measured.

II. Background

*Our Mission – to **hunt cyber threats** against U.S. Infrastructure to **mitigate national risk**.*

Our Vision – a nation fortified and highly resilient against cyber threats

Threat Hunting (TH), a subdivision within the Cybersecurity and Infrastructure Security Agency's (CISA), Cybersecurity Division (CSD), is designated as the lead organization for cyber asset response for the Federal Civilian Executive Branch (FCEB); state, local, tribal, and territorial (SLTT) governments; and the 16 critical infrastructure (CI) sectors. TH seeks to identify, detect, assess, and respond to urgent cybersecurity risks through information sharing and utilization of detection and preventive technologies, and by providing incident response and "hunt" services to help the Nation to respond to and minimize the impact of significant incidents, wherever possible, through persistent rather than reactive capabilities.

TH's mission-critical functions (MCF) are responsibilities that are considered essential and are related directly to accomplishing CISA's mission, as set forth in its statutory or executive authorities. TH has identified the following as their MCFs:

- Analyze information pertinent to cyber threat actors' tactics, techniques, and procedures (TTP);
- Respond to cyber incidents;
- Hunt for nation-state cyber actors;
- Share information for network administrators, system owners, and technical audiences at all proficiency levels to use in their defensive activities;
- Provide technical assistance and subject matter expertise with respect to cyber threat information, defensive cybersecurity capabilities, risk management, and cyber incidents, which may include attribution, mitigation, and remediation; and
- Author cybersecurity guidance and directives for the purpose of protecting federal, SLTT, and CI systems from cybersecurity risks.

With these MCFs in mind, it is vital to commence this report by acknowledging that TH's mission is evolving at a pace unmatched in the subdivision's history. This means that the way in which TH measures progress is also in flux.

Currently, TH measures capacity in three ways: first, through the number of services delivered to stakeholders; second, through the time required to execute a given service; and, third, through the number of personnel required to deliver a given service. Section IV of this report is devoted to explaining this measurement approach; however, it is imperative to note that TH is evolving its metrics to focus on proactive, rather than reactive, activities in line with the evolving mission. Through a proactive approach, CISA will reduce the impact of incidents and increasethe efficiency with which partners can respond and recover. CISA's proactive efforts include

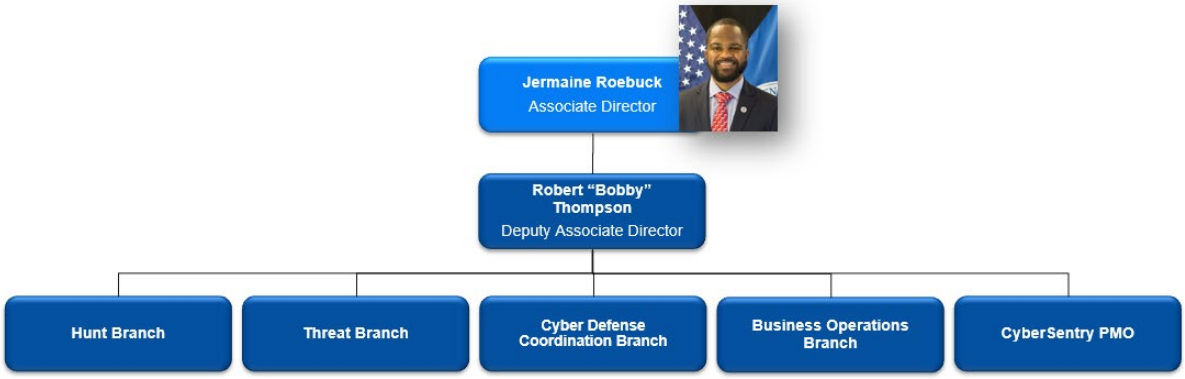
continuous monitoring and analysis of host-level data and establishing requirements for organizations to collect and retain security logs.

This report was compiled with this mentality of rapid and innovative change, and it is CISA's intent that future reporting continues to build on this mindset in a manner that demonstrates TH's capacity to evolve.

III. The Organization

TH's organization is led by Associate Director Jermaine Roebuck and Deputy Associate Director Bobby Thompson and is composed of five branches. The following is a graphical representation of the subdivision, followed by a brief description of each branch.

Figure 1: TH Organizational Structure



Hunt Branch

The Hunt Branch is responsible for proactively hunting for and reactively responding to malicious cyber activity occurring within federal departments and agencies; SLTT governments; and (upon request and within specific parameters) within the 16 CI sectors. The Hunt Branch assists organizations by providing detection methods, incident response services, and mitigation strategies designed to improve an organization's ability to detect and mitigate cyber threats. The Hunt Branch has three critical functions:

- Prepare for the adversary,
- Hunt for the adversary, and
- Respond to adversary presence.

These duties are essential to executing the mission of proactively searching for and reactively responding to malicious cyber activity. These duties often are enabled by other branches within TH, subdivisions, and divisions within CISA, federal departments and agencies, and other public/private sector organizations.

Threat Branch

The Threat Branch is an all-source analytic organization that integrates knowledge, information, and data from a variety of partners, including the U.S. Intelligence Community (IC), SLTT governments, the private sector, international partners, and U.S. CI entities. The Threat Branch uses all available information to assess, identify, and track adversaries to plan and prioritize cyber defense operations effectively. Collected cyber threat information enhances the ability of

CISA's operational elements to detect malicious cyber activity by analyzing adversary capability, opportunity, and intent as well as their TTPs.

Cyber Defense Coordination Branch

The Cyber Defense Coordination Branch supports, coordinates, prioritizes, deconflicts, and ensures execution of TH operational mission priorities, including coordination with organizations across CISA's CSD, such as the Joint Cyber Defense Collaborative, and with key operational partners, such as the Federal Bureau of Investigation and the IC.

Business Operations Branch

The Business Operations Branch manages mission-support and organizational requirements on behalf of the subdivision by focusing on the following three key components:

- Budget and procurement,
- Project management, and
- Human capital.

CyberSentry Program Management Office

CISA's CyberSentry Program is a voluntary public-private partnership program with a select set of CI organizations across the United States. CyberSentry enables CISA to hunt proactively for malicious cyber activity, to advise on mitigation strategies, and to provide CI partners with recommendations for improving overall network and control system security. CyberSentry seeks to onboard a representative sample of the highest-risk CI entities within the National Critical Functions to gain insights into adversary TTPs. This enables collective cyber defense through sharing of indicators of compromise (IOC), dissemination of defensive countermeasures, and continuous hunt.

IV. Incident Response Landscape

TH's mission is evolving rapidly, and its metrics to evaluate impact and capacity are evolving in turn. Currently, TH measures capacity in three ways: first, through the number of services delivered to stakeholders; second, through the time required to execute a given service; and, third, through the number of personnel required to deliver a given service. It is critical to note that TH is in the midst of a fundamental shift to persistent and proactive hunt operations, which, in turn, will require development of new metrics focused on breadth of visibility and efficacy in interdicting threat actors. Although TH will continue to provide reactive incident response and TH services upon request, TH expects that the preponderance of efforts going forward will focus on persistent and proactive hunt operations where TH has unique access.

The additional authorities and resources provided over the past several years have put CISA on a positive modernization path to acquire capabilities that will expand operational visibilities and will overcome legacy analysis gaps significantly. CISA intends to have comprehensive visibility across FCEB networks and enhanced visibility into highly critical private-sector networks. This will be accomplished through sophisticated capabilities such as endpoint detection and response, host level visibility, and information technology (IT) and operational technology (OT) visibility via the CyberSentry program, and cloud visibility. It is only through a comprehensive set of capabilities and highly expert technical personnel that CISA will be able to identify current or new threats affecting stakeholders' environments and to provide the ability to respond more quickly and share more thorough information to protect the broader community.

Furthermore, CISA's authorities continue to grow with the signing into law of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The enactment of CIRCIA marks an important milestone in improving America's cybersecurity by, among other things, mandating CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA. These reports will allow CISA to:

- Deploy resources and render assistance to victims suffering attacks rapidly,
- Analyze incoming reporting across sectors to spot trends, and
- Share that information quickly with network defenders to warn other potential victims.

V. Incident Response Services/Throughput

Incident Intake/Triage

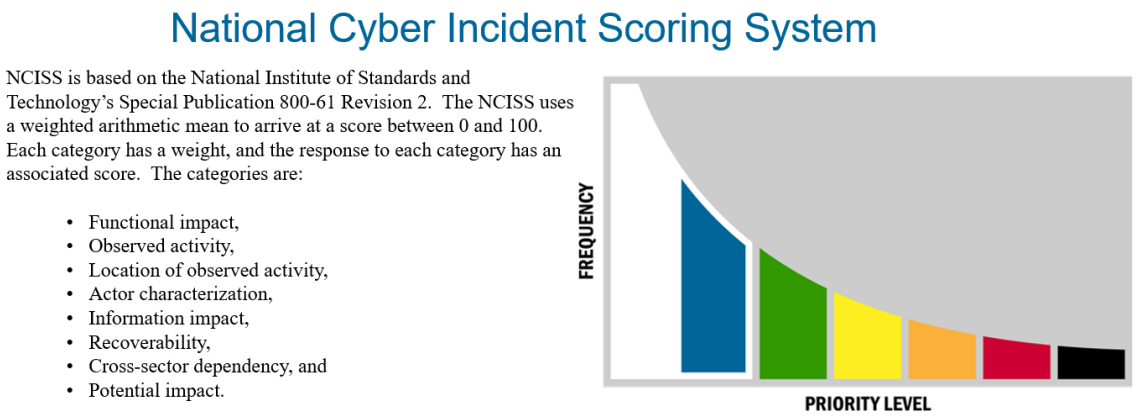
Incident management for TH begins with one of three triggers: (1) submission of an incident report by the victim, (2) incident identification through persistent hunting activities, or (3) notification of a compromise by a third party such as a researcher or an IC partner.

Once incidents are received, TH performs additional outreach with the victim as necessary to collect additional or pertinent information to determine the severity of the potential incident. TH leverages the National Cyber Incident Scoring System (NCISS)[1] to assess incident prioritization and to evaluate risk severity from a nationwide perspective. The NCISS aligns with the National Cyber Incident Severity Schema, which came out of the White House Presidential Policy Directive (PPD) on US Cyber Incident Coordination (PPD-41).

NCISS is designed to provide a repeatable and consistent mechanism for objectively evaluating the risk of a cybersecurity incident in the national context. The system is tailored to include entity-specific potential impact categories. This system allows CISA to provide objective assessments of national-level risk for routine and high-risk cybersecurity events via a repeatable process, facilitating better prioritization and more timely responses to the needs of CISA's constituents and mission partners. NCISS uses a weighted arithmetic mean to produce a score from 0 to 100. This score drives CISA's incident triage and escalation processes and assists in determining the prioritization of limited incident response resources and the necessary level of support for each incident. The system currently is not designed to support cases where multiple correlated incidents may increase overall risk, such as multiple simultaneous compromises of organizations in a specific sector or region. However, such events still can be escalated with expert human intervention. CISA will be establishing campaign tracking, trends, and analysis services as outlined in CIRCIA. The inputs to the scoring system are a mixture of discrete and analytical assessments.

[1] https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System

Figure 2: NCISS Criteria and Priority Levels



The following table outlines the number of incidents received, scored, prioritized, and tracked by TH in FY 2022. Each reported cyber incident requires a cyber analyst to review the received information, to gather additional information, and to assign the incident for one or all of the following services to be performed

Figure 3: FY 2022 Incidents Reported to TH (Categorized by NCISS Score)

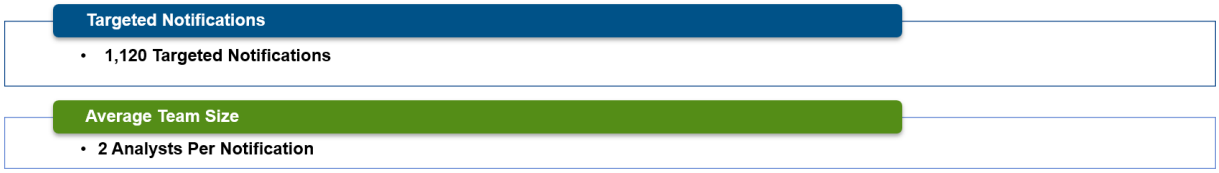
Partner	Baseline 0-29	Minimal 30-49	Low 50-59	Medium 60-74	High 75-84	Severe 85-94	Emergency 95-100	Total Tickets
Private Sector	53	46	10	4	0	0	0	**113**
State, Local, Tribal, and Territorial	22	16	9	2	0	0	0	**49**
Government Facilities	208	250	41	1	0	0	0	**500**
Totals	**283**	**312**	**60**	**7**	**0**	**0**	**0**	**662**

Targeted Notifications Services

Aside from victim reporting or persistent hunting activities, TH also receives information on compromises from third parties such as researchers or IC partners. TH reviews information from third-party sources to identify whether any U.S. entities may be targeted or compromised by adversaries. This includes the preparation of information required for notifications, requests for additional information needed to conduct the notifications, and the coordination of notifications with U.S. Government partners.

Once TH has the required information, coordination occurs with relevant U.S. Government partners to determine a unified U.S. Government notification approach, which often is executed by CISA's regional cybersecurity personnel. The following outlines the number of notifications that were issued by TH in FY 2022.

Figure 4: TH Targeted Notifications Statistics



Persistent Hunting

Persistent Hunting is the continuous analysis of cyber defense sensor data using a variety of enterprise tools and capabilities with the intent of finding sophisticated adversarial activity. CISA's visibility into threat activity has expanded exponentially over the past 2 years because of new authorities and resources and represents the future model for the TH mission. Currently, TH operates the following capabilities:

- **EINSTEIN:** Provides situational awareness of threats to FCEB networks and near real-time identification and prevention of malicious cyber activity. In FY 2022, TH produced 239 analysis reports leveraging EINSTEIN, of which 127 were confirmed as malicious activity. Currently, there are three different capabilities within EINSTEIN:

  1) E1 – Monitors the flow of network traffic transiting to and from FCEB agencies.
  2) E2 – Identifies malicious or potentially harmful activity in Federal Government network traffic on the basis of known signatures.
  3) E3A – Leverages classified indicators to allow CISA to detect and block certain types of cyberattacks. DHS approved the sunsetting of the legacy E3A program in 2022. CISA is currently in the process of replacing the legacy E3A capabilities with modern commercial shared services that provide additional protections and richer data to enable the TH mission.

- **CyberSentry:** Composed of a compilation of commercial off-the-shelf hardware and software that is deployed physically to uniquely CI partners on a voluntary basis. CyberSentry provides CISA with invaluable operational visibility of critical IT/OT networks and the ability to detect and drive remediation of threat activity that could cause severe impact to National Critical Functions.

- **Endpoint Detection and Response and Host Level Visibility:** Enabled by funding first provided in the American Rescue Plan Act of 2021 (P.L. 117-2), CISA continues to expand deployment of tools that expand visibility and that enable analysts to continue their investigations down to endpoints (e.g., workstations and servers) within agency environments. This capability significantly improves operational efficiencies and CISA's ability to detect and understand malicious activity quickly.

When TH analysts observe suspicious traffic within the aforementioned capabilities, TH produces a technical report called an Initial Network Analysis Report, which is delivered to the affected organization. These reports often are targeted to a specific stakeholder and identify a

potential compromise in the stakeholder's infrastructure. Where needed, TH also may initiate an Incident Response Engagement, as described further below.

Incident Response Engagements

TH uses a risk-based approach to applying response resources, leveraging the NCISS and the Engagement Risk Matrix (ERM). ERM generates a risk score, centered on risk and impacts on National Critical Functions and CISA's ability to learn new information that will enable broader cyber defense.

NCISS and ERM consist of a series of questions that are broken down into specific subquestions eliciting a score. It is expected that scores change over time as more details emerge about the specifics of the incident. The risk score enables TH to prioritize affected entities and the application of TH services.

TH personnel have expertise across several technical domains (network, host, cloud, and industrial control systems) to support stakeholders with response, containment, and mitigation recommendations related to cyber incidents or events. TH's technical engagements vary in duration and specific activities and may involve multiple internal and external partners who also may be involved in providing support.

The following is a brief description of the engagements that TH provides today:

- **Hunt:** Proactively hunt for malicious cyber actor presence or actions within selective stakeholder environments and identify advanced threats that evade existing security solutions. During a proactive hunt, the team may develop tailored mitigation recommendations to address identified threats or recommendations for enhancing the overall security posture. This service is driven by information received through intelligence reporting or by stakeholder requests. Hunt requests are evaluated based on several factors, to include:
    - Whether the information provided is detailed enough to support a directed hunt;
    - Ability to get visibility on key networks or system assets to be able to execute the hunt;
    - Risk to national critical functions as related to suspected or known actors and the target entity and system(s) effected; and
    - Resources available to support hunt activities.

- **Incident Response:** Reactive in nature and may be utilized when: 1) a confirmed or suspected cyber incident occurs; 2) the affected entity does not have the capabilities to respond appropriately; or 3) CISA can derive enduring information value from analyzing the threat actor behaviors believed to be present to more effectively protect other potential victims.

- **Forensic Artifact Analysis:** Involves analysis of discrete artifacts from a stakeholder environment (system images, logs, etc.) and is intended to: 1) confirm compromise; 2) assist in scoping (for additional service offerings); or 3) identify IOCs/TTPs for use

across CISA's operational visibility holdings and for external cyber information-sharing purposes.

- **Advisory:** Requested when legal requirements or stakeholder preference preclude CISA from directly interacting with stakeholder networks or datasets. In this model, TH analysts gather details about the incident as well as offer expert advice and guidance. The advisory role also can serve to assist stakeholders in assessing the scope of an incident and can inform the decision to spin up another service offering if necessary.

The above services can be accomplished through various service delivery/deployment methods. These different service delivery/deployment methods are as follows:

- **Remote Deployment:** No physical deployment of personnel other than to install and configure operations equipment that can be accessed remotely.

- **Onsite Deployment:** Equipment and personnel are deployed physically to the victim's location. Typically, onsite deployment of personnel is used when remote deployment is not an option. This deployment method often depends on the comfort level of the affected organization to access their systems remotely.

- **Hybrid:** Combination of remote and onsite. Equipment and personnel are deployed, and analysis is conducted both onsite and remotely. An example of a hybrid engagement would be the deployment of personnel who specialize in host and network forensics to perform their functions onsite when circumstances dictate, along with concurrent analysis of cloud-based telemetry (which innately lends itself to remote analysis) conducted from a CISA facility by cloud forensics specialists.

In line with previous discussions on the various means of measuring capabilities, the following table provides additional information surrounding various TH engagements in FY 2022. Of note, CISA expects the number of proactive hunt engagements (line 1) to expand significantly in FY 2023 given advances in persistent visibility. This is due, in part, to recently expanded congressional authorities in the realm of proactive hunt engagements; the subdivision is implementing these authorities rapidly. A proactive hunt is defined as an engagement to identify malicious activity in a government agency or private sector network within definitive evidence of a preexisting intrusion. A TH hunt is specifically focused on identifying threats from sophisticated threat actors that cannot be detected by traditional cyber security tools and techniques.

Figure 5: TH Engagement Types and FY 2022 Totals

Engagement Type	Typical Duration	Typical Engagement Team Size (in Full-Time Equivalents)	Engagements
Proactive Hunt: proactively hunt for cyber incidents on stakeholder networks	42 days	4-5	2
Incident Response: support stakeholders with the response, containment, and mitigation of cyber incidents	42 days	4-5	12
Advisory: providing subject matter expert technical support to stakeholder	14 days	1-2	7
Forensic Analysis: analysis of stakeholder media or code delivering a report to encourage stakeholder actions	14 days	1-2	33
			Total: 54

Code and Media Analysis Services

Code and Media Analysis focuses on analyzing malware samples received from victims experiencing malicious cyber activity. Malware analysis sits at the intersection of incident response, forensics, system and network administration, security monitoring, and software engineering. This capability involves analyzing received malware samples to determine the capability and origin of tools used during attacks, to understand the root cause of the infection and mitigation development. Malware analysis is performed through three principal methods:

- **Reverse Engineering:** Manual, detailed examination and deconstruction of suspected malicious artifacts by malware reverse engineers. Provides improved clarity, provenance, and threat level of submitted code. This effort is time- and resource-intensive and requires an advanced level of subject matter expertise.

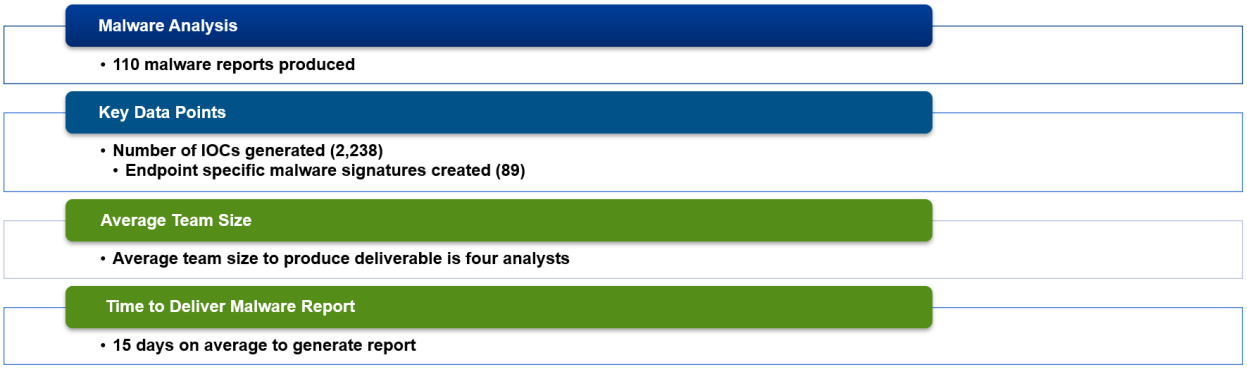
- **Automated Malware Analysis:** Automated examination of a malware sample typically used during initial triage of the sample. This quickly generates an automated report for submitters that provides IOCs, the MITRE Corporation's Adversarial Tactics, Techniques, and Common Knowledge characterization, and mitigation information.[2]

- **Media Analysis:** Manual digital forensic analysis using documented, verifiable, and repeatable processes and methods to analyze all types of media (hard drives, memory dumps, images, thumb drives, etc.). This analysis allows TH to extract IOCs with greater fidelity and validity to improve understanding of adversary activity on systems.

At the conclusion of a malware reverse engineering effort, a malware analysis report (MAR) is created and provided to the submitter/victim with an in-depth look at how the tool was used, any additional capabilities observed, and information related to mitigations that can be applied to remediate the activity. In FY 2022, TH delivered 110 MARs to stakeholders. Separately, TH was able to generate 2,238 IOCs and 89 endpoint signatures that are shared publicly or are leveraged internally by TH analysts when performing persistent hunting and incident response services.

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

Figure 6: TH Malware Statistics



TH Service Summary by Partner

At the heart of CISA's mission is partnership and collaboration. As demonstrated throughout this report, CISA adheres to the principle that securing the Nation's cyber infrastructure is a shared responsibility. With this in mind, the following table visually captures the services previously described and correlates them to their provided partner recipients, to include a breakdown of both internal and external activities provided by TH. Through each of these engagements with many partners, TH teams advance this shared responsibility to mitigate these risks, both during and before the occurrence of major incidents.

Figure 7: TH External Services by Partner

External Product/Service	Federal Civilian Executive Branch Partners	Private-Sector Partners	State, Local, Tribal, and Territorial Partners	International Partners	Total TH External Activities
Incident Triage	683	246	166	0	**1,095**
Engagement	33	6	15	0	**54**
MAR	58	24	17	11	**110**
Targeted Notifications	N/A	1,086	34	N/A	**1,120**
Individual Network Analysis Reports	239	N/A	N/A	N/A	**239**
Internal Products/Services					**Total TH Internal Activities**
MAR IOCs					**2,238**
MAR Endpoint Signatures					**89**

VI. Conclusion

CISA is committed to leading the response to cybersecurity incidents and vulnerabilities to safeguard the Nation's critical assets. With the right authorities, resources, and partnerships, CISA will advance efforts to defend and secure cyberspace further and will lead national efforts to drive and enable effective national cybersecurity.

Additionally, CISA has been able to deploy improved capabilities needed to expand visibility across stakeholders and to reduce TH's time-to-effective detection, analysis, and reporting. These investments will bolster CISA's ability to take appropriate action to help victims, to share highly actionable and timely information to protect future targets, and to develop optimized guidance to prevent the most common and damaging attacks.

Lastly, CISA continues to implement strategies to cultivate and grow a high-performing workforce. CISA is dedicated to attracting and retaining the Nation's most talented cyber defenders. The Cyber Talent Management System is one flexible way that CISA has acquired to allow CSD to tap into a variety of cybersecurity skills at all stages of a career.

Over the past few years, CISA has received significant new authorities and responsibilities through a wide variety of legislation. CISA will continue to execute these authorities as directed and will use them to enable critical mission goals further. Throughout FY 2023, CISA also will continue efforts to develop and track rigorously new metrics that fully account for advances in persistent visibility and associated capability, all in order to move from reactive response to proactive hunt. This shift will allow CISA to make best use of finite resources while materially reducing the rate and impact of damaging intrusions targeting American networks.

VII. Appendix: Abbreviations

Abbreviation	Definition
CI	Critical Infrastructure
CIRCIA	Cyber Incident Reporting and Critical Infrastructure Act of 2022
CISA	Cybersecurity and Infrastructure Security Agency
CSD	Cybersecurity Division
DHS	Department of Homeland Security
FCEB	Federal Civilian Executive Branch
ERM	Engagement Risk Matrix
FY	Fiscal Year
IC	Intelligence Community
IOC	Indicator of Compromise
IT	Information Technology
MAR	Malware Analysis Report
MCF	Mission-Critical Function
NCISS	National Cyber Incident Scoring System
OT	Operational Technology
PPD	Presidential Policy Directive
SLTT	State, Local, Tribal, and Territorial
TH	Threat Hunting
TTP	Tactics, Techniques, and Procedures