Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

CENTERS FOR MEDICARE & MEDICAID SERVICES SHOULD IMPROVE PREVENTATIVE AND DETECTIVE CONTROLS TO MORE EFFECTIVELY MITIGATE THE RISK OF COMPROMISE

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Amy J. Frontz
Deputy Inspector General
for Audit Services

May 2023
A-18-20-08001

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG) is to provide objective oversight to promote the economy, efficiency, effectiveness, and integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of the people they serve. Established by Public Law No. 95-452, as amended, OIG carries out its mission through audits, investigations, and evaluations conducted by the following operating components:

Office of Audit Services. OAS provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. The audits examine the performance of HHS programs, funding recipients, and contractors in carrying out their respective responsibilities and provide independent assessments of HHS programs and operations to reduce waste, abuse, and mismanagement.

Office of Evaluation and Inspections. OEI's national evaluations provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. To promote impact, OEI reports also provide practical recommendations for improving program operations.

Office of Investigations. OI's criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs and operations often lead to criminal convictions, administrative sanctions, and civil monetary penalties. OI's nationwide network of investigators collaborates with the Department of Justice and other Federal, State, and local law enforcement authorities. OI works with public health entities to minimize adverse patient impacts following enforcement operations. OI also provides security and protection for the Secretary and other senior HHS officials.

Office of Counsel to the Inspector General. OCIG provides legal advice to OIG on HHS programs and OIG's internal operations. The law office also imposes exclusions and civil monetary penalties, monitors Corporate Integrity Agreements, and represents HHS's interests in False Claims Act cases. In addition, OCIG publishes advisory opinions, compliance program guidance documents, fraud alerts, and other resources regarding compliance considerations, the anti-kickback statute, and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC

at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Report in Brief
Date: May 2023
Report No. A-18-20-08001

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

The Centers for Medicare & Medicaid Services Should Improve Preventative and Detective Controls To More Effectively Mitigate the Risk of Compromise

Why OIG Did This Audit

We conducted a cyber threat hunt assessment of the Centers for Medicare & Medicaid Services' (CMS's) information systems to independently assess the effectiveness of CMS's cybersecurity defenses, identify potential indicators of compromise, determine whether any breaches have gone undetected, and review its incident response capabilities.

Our objectives were to determine whether: (1) CMS's cybersecurity defenses were effective, (2) there were active threats on the CMS network or whether there had been a past cyber breach, and (3) CMS was able to detect breaches and respond appropriately.

How OIG Did This Audit

We performed the cyber threat hunt of CMS's endpoints from August through November 2020. The assessment was performed on approximately 8,400 endpoints that CMS manages. We contracted with Accenture Federal Services (AFS) to conduct the cyber threat hunt of CMS. AFS provided subject matter experts during the initial planning, preparation, technology deployment, and discovery phases of the cyber threat hunt. OIG IT auditors completed the cyber hunt analysis and reporting phases of the cyber threat hunt. The assessment was performed in accordance with generally accepted government auditing standards and agreed-upon rules of engagement between OIG, AFS, and CMS.

What OIG Found

Although CMS had implemented some security controls for detecting and preventing threats on its network, CMS's cybersecurity controls needed improvements to better detect and prevent cyber threats on its network. We found multiple security controls at CMS that were not operating effectively, including controls related to monitoring and controlling communications at the CMS boundary, configurations to provide only essential capabilities, and controlling and preventing the installation of unauthorized software by users. Although we did not identify evidence of a past breach, we found one active and one potential threat to the CMS network. We promptly shared these findings with CMS during our audit period. Lastly, we concluded that CMS did not consistently detect threat activity that could lead to a potential breach. Specifically, CMS did not identify an active threat and other control weaknesses we found during the audit. Because we did not identify a breach within CMS's network, we have no opinion about CMS's ability to respond appropriately to a breach.

The security control failures that we identified occurred because CMS did not effectively align some of its security controls with their security policies or with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, requirements. For certain controls, CMS did not establish effective policies and procedures to periodically assess whether these controls were in place and operating effectively in accordance with the most current NIST SP 800-53 controls. As a result, cyber threat actors may have been able to successfully carry out a cyberattack or insiders may have been able to bypass CMS security controls that would allow them to exfiltrate sensitive data or allow the attacks to go undetected.

What OIG Recommends and CMS Comments

We recommend that CMS: (1) remediate the seven security control findings OIG identified, (2) update security controls to align with the most current NIST SP 800-53 requirements, and (3) enhance policies and procedures to periodically identify and assess whether security controls are in place and operating effectively in accordance with the most current NIST SP 800-53 controls and remediate weak controls timely. In written comments on our draft report, CMS concurred with all recommendations and described the actions it has taken. CMS disagreed with our assertion that scanning attempts of a web server represented an active threat on the CMS network. We agreed with CMS and made changes to the report accordingly. However, we consider the external scans a potential threat that could adversely impact organizational operations or assets because they provide valuable information about vulnerabilities to potential attackers that they can exploit.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

The Department of Health and Human Services (HHS), Office of Inspector General (OIG), Office of Audit Services (OAS), Cybersecurity and Information Technology Audit Division (CITAD), conducted a series of penetration test audits to evaluate the effectiveness of security controls at eight HHS operating divisions (OpDivs). These audits provided a snapshot of HHS's cyber defenses at the eight OpDivs and identified almost 200 vulnerabilities across HHS.[1]

Based on the results from the penetration test audits, we initiated a series of cyber threat hunts on a subset of HHS OpDivs' information systems to identify potential indicators of compromise (IOCs) on those systems and to determine whether any breaches have gone undetected.[2] As part of this body of work, we conducted a cyber threat hunt of selected Centers for Medicare & Medicaid Services (CMS) information systems in accordance with guidance outlined by the National Institute of Standards and Technology (NIST).

OBJECTIVES

Our objectives were to determine whether:

- CMS's cybersecurity defenses were effective,
- there were any active threats on the CMS network or whether there had been a past cyber breach, and
- CMS was able to detect breaches and respond appropriately.[3, 4]

[1] Report in Brief for the *Summary Report for Office of Inspector General Penetration Testing of Eight HHS Operating Division Networks*, A-18-18-08500, issued on Mar. 1, 2019.

[2] Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats.

[3] An active threat is an ongoing event or behavior with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service.

[4] A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose.

BACKGROUND

Computer hackers use a variety of techniques in their persistent attempts to gain unauthorized access to sensitive Government information systems and data. Common attack methods include denial of service, spear phishing, unauthorized malicious software (malware), and Structured Query Language Injection attacks against websites.[5, 6] CMS cybersecurity personnel must successfully defend against these attack methods while also addressing the risks presented by adversaries through the software supply chain and other attack vectors.

We recognize that cybersecurity defenses will not prevent all breaches from occurring. However, to reduce the likelihood of a breach, agencies must ensure that proper controls (such as effective patching, proper configuration management, access restrictions, and physical protections) are in place and operating effectively. Two of the best tactics to test the effectiveness of the control environment are penetration testing and cyber threat hunts that search for IOCs.[7]

Centers for Medicare & Medicaid Services

CMS is the primary Federal agency that oversees two of largest Federal health care programs, Medicare and Medicaid. CMS also oversees the Health Insurance Exchanges and the Children's Health Insurance Program.[8, 9] CMS estimates that during fiscal year 2023, it will administer programs for over 150 million Americans. CMS provides coverage that aims to offer peace of mind; transforms health care by reducing disparities; and strengthens program integrity by reducing fraud, waste, and abuse, and promotes innovation. Within CMS, the goal of the information security program is to safeguard the confidentiality, integrity, and availability of its information and systems. Because of the importance of CMS's mission and the value of the sensitive Medicare and Medicaid information stored on its networks, CMS or its contractors could be a target for cybercrime and cyber espionage. For example, a recent ransomware

[5] Attacks that look for websites that pass insufficiently processed user input to the database allowing the attacker to read sensitive data from the database or perform other database functions through the website.

[6] Malware is any software program designed to damage or execute unauthorized actions on a computer system. Examples of malware include computer viruses, worms, or Trojan horses.

[7] Penetration tests are intended to identify vulnerabilities and security flaws in systems, devices, and controls that are in place to protect customer information and resources. This type of information security testing typically attempts to simulate attacks that are either internal to an organization's computer network (i.e., employees) or outside an organization's network boundary (e.g., State sponsors and organized crime).

[8] Health Insurance Exchanges provide consumers and small businesses in every State (including the District of Columbia) access to obtain health and dental insurance coverage. The Exchanges are operated by States or the Federal Government.

[9] CMS Agency Overview. Available online at: https://www.cms.gov/About-CMS. Accessed on Feb. 16, 2023.

attack on a CMS's subcontractor corporate network may have resulted in the compromise of the personally identifiable information and protected health information, which may have included bank routing and account information for up to 254,000 Medicare enrollees.[10, 11] In another example, CMS had to respond to a breach in October 2018 that affected data for 75,000 people enrolled in the Federally Facilitated Exchange. Attackers were able to compromise a system used by agents and brokers to assist consumers in applying for coverage within the CMS Exchange website.[12]

HOW WE CONDUCTED THIS AUDIT

We performed the cyber threat hunt of the CMS network from August through November 2020. To assist us with the cyber threat hunt, we relied on the work of specialists. We contracted with Accenture Federal Services (AFS) to perform a cyber threat hunt on a subset of CMS's information systems. AFS provided subject matter experts during the initial planning, preparation, technology deployment, and discovery phases of the cyber threat hunt. OIG information technology (IT) auditors completed the cyber hunt analysis and reporting phases of the cyber threat hunt. We performed the cyber threat hunt in accordance with the agreed-upon rules of engagement (ROE) document, signed and completed by OIG, AFS, and CMS management in July 2020. To provide the most accurate results possible, we asked CMS officials to not alert individual users about the cyber threat hunt while it was in progress.

Cyber threat hunts assist IT professionals in detecting data breaches, malware infections, and other threatening activities. Our cyber threat hunts searched for IOCs, which are data that indicate potentially malicious activity on a system or network. For example, during the CMS cyber threat hunt, we looked for unusual outbound network traffic or connections to foreign Internet Protocol (IP) addresses, abnormal user account activity, digital signatures of malware files, suspicious registry, or system file changes, and examined adversary tactics and techniques based on the MITRE ATT&CK framework.[13] We describe our cyber threat hunt methodology in Appendix A.

As outlined in the ROE, we reported any significant vulnerabilities and IOCs identified during the cyber threat hunt to CMS. To verify that the reported vulnerabilities did not have national

[10] Available online at: https://www.cms.gov/newsroom/press-releases/cms-responding-data-breach-subcontractor. Accessed on Jan. 26, 2023.

[11] According to CMS, no CMS systems were breached and no Medicare claims data was involved in the incident.

[12] Available online at: https://www.cms.gov/newsroom/press-releases/cms-responding-suspicious-activity-agent-and-broker-exchanges-portal. Accessed on Jan. 26, 2023.

[13] MITRE ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

security implications or were related to an ongoing investigation, we referred those matters to our Office of Investigations (OI) Computer Crimes Unit (CCU) for further review. The OI CCU assessed the reported vulnerabilities and shared its recommendations with us. We then shared the vulnerabilities and the recommended actions with CMS.

To begin the cyber threat hunt, we worked with CMS to deploy the Endgame sensor package across selected endpoints in the CMS network.[14, 15] We configured the sensor to communicate with our Endgame server. We assisted CMS in deploying the Endgame sensor package to approximately 8,400 endpoints identified by CMS.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A contains the details of our audit scope and methodology, Appendix B contains the tools we used to conduct the audit, and Appendix C contains the Federal requirements we used to evaluate CMS's controls.

FINDINGS

Although CMS had implemented some security controls for detecting and preventing threats on its network, CMS's cybersecurity controls needed improvements to better detect and prevent cyber threats on its network. We found multiple security controls that were not operating effectively. The most significant of which were related to monitoring and controlling communications at the CMS external network boundary, configuring CMS information systems to provide only essential capabilities, and controlling and preventing the installation of unauthorized software by users. Although we did not identify evidence of a past breach, we found one active and one potential threat to the CMS network.[16] Specifically, we found multiple potentially unwanted programs with a high probability of being malware and one that CMS confirmed as being malicious. In addition, a CMS web server accessible to the internet was scanned multiple times throughout the day by malicious IP addresses. Although we did not find a connection was established, these scans were not detected or stopped by CMS controls. We promptly shared these findings with CMS during our audit period for its immediate follow

[14] Endgame is an application software tool used to identify IOCs on a system or network and to analyze systems for active threats. Threats are rated with a numerical malware score indicating the likelihood of malware.

[15] An endpoint is any device that is physically or virtually an end point on a network. Laptops, desktops, mobile phones, tablets, servers, and virtual environments can all be considered endpoints.

[16] See footnote 3.

up. Lastly, we concluded that CMS did not consistently detect threat activity that could lead to a potential breach. We based this conclusion on the fact that CMS did not identify an active threat and other control weaknesses we found during the audit. Because we did not identify a breach within CMS's network, we have no opinion about CMS's ability to respond appropriately to a breach.

The Federal Information Security Modernization Act (FISMA) of 2014, section 3554 (P.L. 113–283), directs agencies to comply with the policies, procedures, standards, and guidelines promulgated under section 11331 of Title 40, which requires, in part, that Federal information systems meet the minimum information security system requirements described under section 20(b) of the NIST (15 U.S.C. 278g-3). In response to FISMA, NIST developed the Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, as a mandatory Federal standard. To comply with the Federal standard, Federal agencies must meet the minimum-security requirements using NIST Special Publication (SP) 800-53. CMS did not correctly implement the following NIST SP 800-53, Revision 4, security controls in the table on the next page.

Table: Weak CMS Security Controls, Ordered by Risk Rating

NIST SP 800-53, Revision 4, Security Control	Security Control Finding	Control No.*	Risk Rating†
Least Functionality	CMS did not adequately configure certain information systems to provide only essential capabilities, and it did not effectively prohibit or restrict the use of certain functions, ports, protocols, and/or services.	CM-7	High
User Installed Software	CMS did not adequately govern the installation of software by users and did not enforce and monitor the compliance of its software installation policy within its network.	CM-11	High
Boundary Protection	CMS did not implement effective controls at the external boundaries of the system to monitor and control communications associated with certain servers.	SC-7	High
Information System Monitoring	CMS did not adequately monitor their information system to detect indicators of potential attacks to their information systems.	SI-4	High
Information Flow Enforcement	CMS did not implement effective controls to restrict web requests to the Internet that are not from their internal web proxy server.	AC-4	High
Authenticator Management	CMS did not adequately protect authenticator content from potential unauthorized disclosure by storing only cryptographically protected passwords.	IA-5	High
Unsuccessful Logon Attempts	Certain CMS systems did not adequately enforce limits for consecutive invalid logon attempts by users and did not lock the accounts after users exceeded the maximum number of unsuccessful attempts.	AC-7	Medium

* The Control No. is the abbreviation of the control family name and the number of the specific control within NIST SP 800-53, Revision 4.

† NIST SP 800-53, Revision 4, Security Control Risk Rating as determined by CITAD.

The security control failures that we identified occurred because CMS did not effectively align some of its security controls with their security policies or with NIST SP 800-53, Revision 4, requirements. In addition, for certain controls, CMS did not establish effective policies and procedures to periodically assess whether these controls were in place and operating effectively in accordance with the most current NIST SP 800-53 controls. Furthermore, CMS established detection controls and procedures were not effective at identifying weak controls in a timely manner.

As a result of CMS not correctly implementing these controls, cyber threat actors may have been able to successfully carry out a cyberattack or insiders may have been able to bypass CMS security controls that would allow them to exfiltrate sensitive data or allow the attacks to go undetected. The likelihood of successful cyberattacks and unauthorized access to sensitive data is more likely in environments where these types of security controls are not enforced.

RECOMMENDATIONS

We recommend that the Centers for Medicare & Medicaid Services:

- remediate the seven security control findings OIG identified,
- update security controls to align with the most current NIST SP 800-53 requirements, and
- enhance policies and procedures to periodically identify and assess whether security controls are in place and operating effectively in accordance with the most current NIST SP 800-53 controls and remediate weak controls timely.

CMS COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, CMS concurred with all our recommendations and described actions it has taken to mitigate risk to the CMS network.

CMS disagreed with our assertion that scanning attempts of a web server represented an active threat on the CMS network. We agreed with CMS and made changes to the report accordingly. However, we consider those external scans a potential threat that could adversely impact organizational operations or organizational assets because they provide valuable information to potential attackers and help them identify vulnerabilities or weaknesses that they can exploit. We commend CMS for taking immediate actions to address the active threat identified and for looking into long-term solutions to minimize additional threats as stated in its comments.

CMS also provided technical comments, which we addressed as appropriate. CMS's comments, excluding technical comments, are included as Appendix D.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

To assist us with the OIG cyber threat hunt, we relied on the work of specialists. We contracted with AFS to conduct the cyber threat hunt of CMS. AFS provided subject matter experts during the initial planning, preparation, technology deployment, and discovery phases of the cyber threat hunt. OIG IT auditors completed the cyber hunt analysis and reporting phases of the cyber threat hunt. We performed the cyber threat hunt of CMS's network from August through November 2020. Before the start of the assessment, CMS completed a Network Environment Survey document. As requested in the Network Environmental Survey, CMS provided OIG with a list of public-facing network subnets. OIG provided to CMS an Endgame sensor software package, which CMS deployed to selected endpoints authorized by CMS leadership.

Regarding the testing of internal controls during our audit, we identified the component "control activities" as significant to our audit objectives.[17] We reviewed various NIST SP 800-53, Revision 4, security controls including but not limited to:

- AC-4 Information Flow Enforcement
- AC-7 Unsuccessful Logon Attempts
- CM-7 Least Functionality
- CM-11 User Installed Software
- IA-5 Authenticator Management
- SC-7 Boundary Protection
- SI-4 Information System Monitoring

Based on our cyber threat hunt we assessed the operating effectiveness of these internal controls and identified deficiencies that we believe could affect CMS's ability to detect or effectively prevent certain cyberattacks. The internal control deficiencies we identified are listed as security control findings in the Findings section of this report. However, the cyber threat hunt we performed may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

We conducted our audit remotely on approximately 8,400 endpoints with varying operating systems. Over the course of the cyber threat hunt assessment, we received more than 18,000

[17] *Standards for Internal Control in the Federal Government, GAO-14-704G*

individual alerts through the Endgame platform. We excluded third-party cloud service providers from the cyber threat hunt.

METHODOLOGY

To accomplish our objectives, OIG and CMS prepared the ROE document that outlined the general rules, logistics, and expectations for the cyber threat hunt assessment. We obtained signatures from CMS and AFS management indicating that they agreed with the ROE. We conducted our cyber threat hunt remotely from the OIG/OAS Cyber Range.

To accomplish our objectives, we:

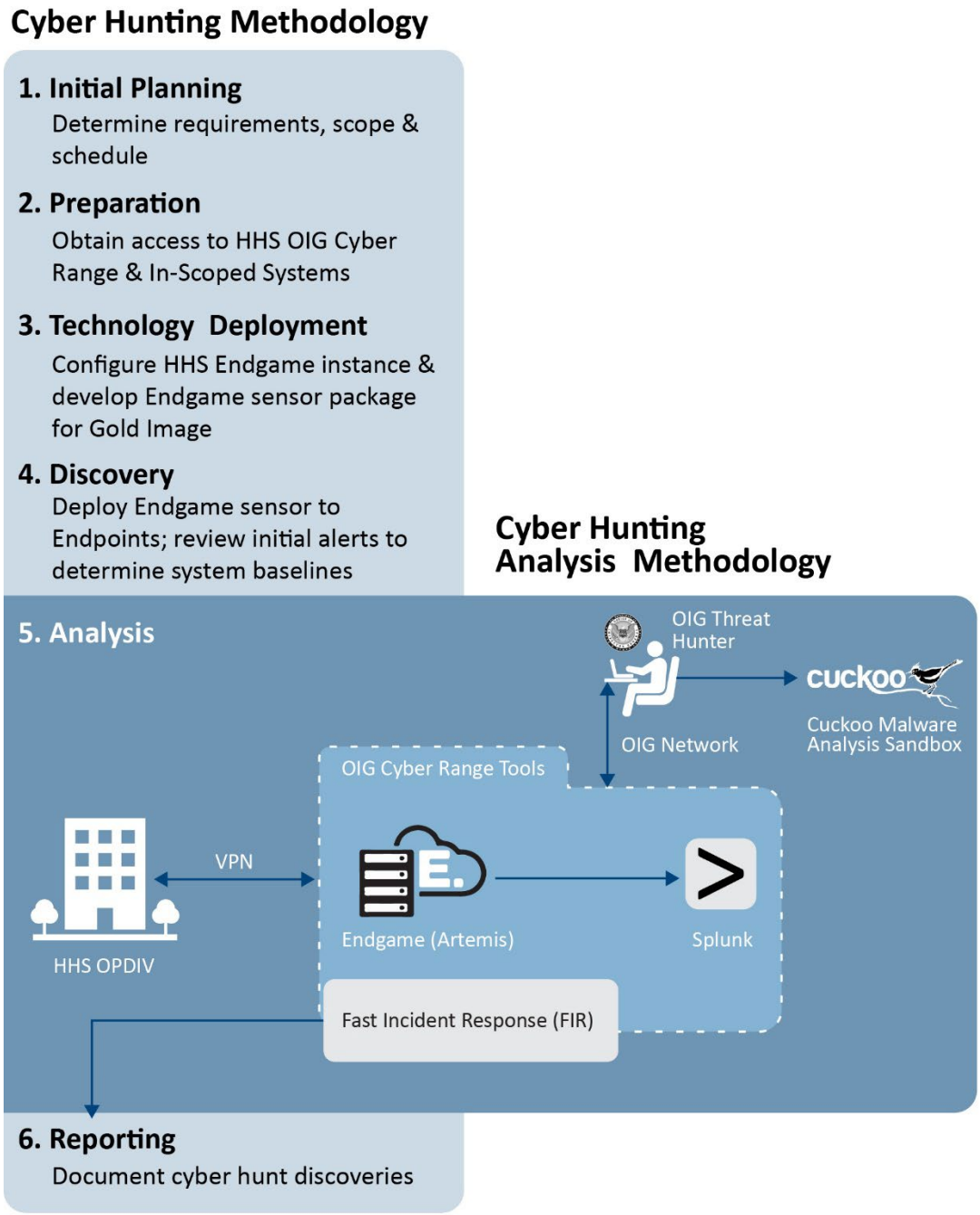
- reviewed Federal and CMS policies and procedures,
- interviewed cybersecurity personnel,
- assisted CMS in deploying the Endgame sensor software to CMS endpoints,
- executed the Cyber Hunt Methodology,
- assessed CMS systems for anomalies that posed a significant risk to the CMS enterprise network,
- responded to Endgame-generated alerts and hunted across the CMS environment for anomalies among processes, persistence mechanisms, and user log-ons,[18] and
- shared significant findings with CMS during the audit and provided detailed documentation about our findings in advance of issuing our draft report.

CYBER HUNT METHODOLOGY

The cyber hunt methodology consisted of six core phases: (1) initial planning, (2) preparation, (3) technology deployment, (4) discovery, (5) analysis, and (6) reporting. (See the figure on the next page).

[18] *Persistence Mechanisms* are techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

Figure: Cyber Hunt Methodology Overview



Initial Planning

We worked with CMS to determine the requirements of the cyber hunt, defined the scope of IT assets on which to deploy tools for hunting, and developed the schedule for all phases of the cyber hunt.

Preparation

We obtained the necessary access to the OIG Cyber Range and to the systems identified as in-scope by CMS during the Initial Planning Phase.

Technology Deployment

We configured the Endgame instance in the OIG Cyber Range and developed the Endgame sensor package deployed by CMS to its endpoints (workstations and servers).[19]

Discovery

CMS deployed the Endgame sensors to the endpoints. Once deployed, the endpoints began to report data back to the Endgame instance in the form of alerts. We reviewed these alerts to understand the system baselines and to remove any false positive data.

Analysis

The cyber hunt analysis phase focused on searching for threat actor activity using known indicators of compromise and determining the impact of these threats on CMS systems and the network. We focused on analyzing anomalies in the CMS infrastructure and determining whether these anomalies were valid threats to the CMS infrastructure. We identified these anomalies by feeding Endgame data into Splunk, which we used to analyze the data for any malicious or suspicious activity.[20] Endgame allowed us to analyze system activity and to identify and triage security concerns.

Reporting

This phase involved documenting the cyber hunt discoveries. This included disclosing affected systems and providing recommendations on how to improve the security posture of the CMS network environment and systems contained therein.

[19] An Instance is a virtual server in the Amazon Web Services cloud environment.

[20] Splunk is a software platform to search, analyze and visualize the machine-generated data gathered from the websites, applications, sensors, devices, etc.

CYBER HUNT ANALYSIS METHODOLOGY

While conducting the analysis phase, we used the following methodology to determine the validity of an alert. We first reviewed the alert to determine whether it was a type that warranted further analysis. If we needed to perform further analysis, we performed a full analysis of the alert utilizing tools such as Artemis and the Cuckoo Sandbox.[21, 22]

Alerts

The cyber hunt began by addressing Endgame alerts that are system-generated notifications that detect potentially malicious activity on monitored endpoints. This type of activity may include but is not limited to ransomware, process injection, or permission theft.[23, 24] We used the alerts to help identify abnormal behavioral patterns that might require analysis. Alerts are the result of previously configured tradecraft protections that are enabled when a sensor is deployed to an endpoint.[25] They specify what endpoint activity the sensor monitors and the action the sensor should take if it detects potential malicious activity. In general terms, alerts were generated for any activity that was determined to be outside of the baseline for that system.

Manual Analysis

We created custom searches to collect and analyze targeted data across multiple endpoints. This was initiated by assigning one or more hunts to selected endpoints. These hunts then searched for specified artifact values in the target device(s) and reported findings back to us.[26] Some of the items we searched for were IOCs that we had already found in Endgame alerts during the cyber hunt. We also searched for specific registry values, process trees, specific binaries, user account activity, and network connections that we had identified as a possible

[21] Artemis is Endgame's natural language interface to facilitate queries and expedite detection and responses.

[22] Cuckoo Sandbox is an open-source automated malware analysis system.

[23] Process injection is a defense evasion technique employed often within malware, which runs custom code within the address space of another process.

[24] Permission theft is the unauthorized theft of identity or permissions.

[25] Endgame's tradecraft protections, monitor system activity in real-time, alerting on techniques across all tactics defined in the MITRE ATT&CK.

[26] An artifact value is a piece of data that may or may not be relevant to an investigation/response.

threat.[27, 28, 29] We then filtered the data by tailored analytics and distinguished actual incidents from false positives.

The main goal of this phase was to identify suspicious activity and report it to CMS so that it could take remedial action.

[27] A registry value is an actual entry within the Microsoft's Windows Registry that contain specific instructions that Windows and applications look for to perform its functions.

[28] A binary describes a numbering scheme in which there are only two possible values for each digit: 0 and 1. The term also refers to any digital encoding/decoding system.

[29] A process tree is a tool for visualizing and archiving the processes of planning and development projects in chronological order. It brings several types of information together in one place, thus, creating a general picture of the matter at hand.

APPENDIX B: TOOLS WE USED TO CONDUCT THE AUDIT

Endgame

Endgame is a centralized software application that monitors endpoints (e.g., workstations or servers.) Endgame sensors collect data and perform active queries on individual endpoints across the OpDiv network. Endgame also collects data to feed Splunk.

Splunk

Splunk is a robust analytical tool used to collect and visualize data. We used Splunk, which is designed to be highly scalable and customizable, to review and parse data in bulk. Splunk's data search allows for a comparison of historical data across all endpoints. We leveraged Splunk's ability to exclude known good artifacts to search for an entire list of IOCs across Endgame collection results.

Artemis

We used Endgame's artificial intelligence assistant, Artemis, to combine hunts for both current and historical process data across one or more specified endpoints. Artemis allowed limited historical data queries that allowed us to search for and analyze events over time.

Cuckoo Sandbox

We used an OIG internal Cuckoo Sandbox environment to analyze and reverse engineer binary files. Cuckoo Sandbox reports provided us with additional IOCs, such as malicious websites, initiated network connections, malware classifications, and other relevant details to triage suspicious binary files. We used this information to tailor additional manual analysis against the OPDIV environment.

Fast Incident Response

The Fast Incident Response (FIR) is a cybersecurity incident management platform designed for agility and speed. It allows for easy creation, tracking, and reporting of cybersecurity incidents. We used the FIR in the reporting phase to document potential incidents.

APPENDIX C: FEDERAL REQUIREMENTS

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* states:

AC-4 Information Flow Enforcement

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content.

AC-7 Unsuccessful Logon Attempts:

Control: The information system:

a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system

components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels.

CM-7 Least Functionality

Control: The organization:

a. Configures the information system to provide only essential capabilities; and

b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].

CM-11 User-Installed Software

Control: The organization:

a. Establishes [Assignment: organization-defined policies] governing the installation of software by users;

b. Enforces software installation policies through [Assignment: organization-defined methods]; and

c. Monitors policy compliance at [Assignment: organization-defined frequency].

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.

IA-5 Authenticator Management

Control: The Organization manages information system authenticators by:

h. Protecting authenticator content from unauthorized disclosure and modification;

Control Enhancements:

(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

The information system, for password-based authentication:

(c) Stores and transmits only cryptographically-protected passwords;

(7) AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

SC-7 Boundary Protection

Control: The information system:

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Control Enhancements:

(5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

SI-4 Information System Monitoring

Control: The organization:

a. Monitors the information system to detect:

1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and

2. Unauthorized local, network, and remote connections.

HHS's Rules of Behavior for General Users — A. HHS Information Systems, states that "when using and accessing HHS information resources and systems . . ., [users] must [n]ot reconfigure systems and modify GFE, install/load unauthorized/unlicensed software or make configuration changes without proper official authorization."

APPENDIX D: CMS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: March 24, 2023

TO: Amy J. Frontz
Deputy Inspector General for Audit Services
Office of Inspector General

FROM: Chiquita Brooks-LaSure
Administrator
Centers for Medicare & Medicaid Services

SUBJECT: Office of Inspector General (OIG) Draft Report: The Centers for Medicare & Medicaid Services Should Improve Preventative and Detective Controls To More Effectively Mitigate the Risk of Compromise, A-18-20-08001

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the Office of Inspector General's (OIG) draft report.

The security of CMS systems and beneficiary health data is a top priority for CMS. To secure against potential vulnerabilities, CMS vigilantly monitors, tests, and strengthens its systems against cyber-attacks and has procedures and processes in place to quickly identify, mitigate, and remove threats, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) requirements and guidelines issued by the Cybersecurity & Infrastructure Security Agency (CISA).

Since 2015, CMS has participated in CISA's Continuous Diagnostics and Mitigation (CDM) program, which is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritizes these risks based upon potential impacts, and enables cybersecurity personnel to mitigate the most significant problems first. CMS continues to improve the overall security posture of the environment and enhance the tools used to monitor for vulnerabilities in CMS systems and datacenters.

During the course of OIG's audit, CMS promptly addressed OIG's findings to mitigate any risk to CMS's network and shared remediation evidence with OIG. Specific to the two active threats OIG identified during their review, CMS disagrees with the assertion that scanning attempts of a web server represented an active threat on the CMS network. CMS did not find any evidence of a connection to the network. CMS took immediate action to remove active threats identified and is looking into longer term solutions to minimize additional threats. CMS appreciates the OIG's suggestions of controls and processes that could be improved to further reduce or mitigate risk.

OIG Recommendation

OIG recommends that the Centers for Medicare & Medicaid Services remediate the seven security control findings OIG identified.

CMS Response:
CMS concurs with OIG's recommendation. CMS continues to address OIG's findings to mitigate any risk to CMS's network and will continue to share remediation evidence with OIG. CMS will also continue to share any additional remediation documentation OIG needs to verify corrections.

OIG Recommendation
OIG recommends that the Centers for Medicare & Medicaid update security controls to align with the most current NIST SP 800-53 requirements.

CMS Response:
CMS concurs with OIG's recommendation. CMS Acceptable Risk Safeguards (ARS) set the baseline for the minimum acceptable level of required security controls that CMS must implement to protect the security and privacy of information and systems. CMS updated the ARS in 2022 to comply with the most current NIST SP 800-53 requirements. CMS systems are required to be in compliance with the current version by April 1, 2023.

OIG Recommendation
OIG recommends that the Centers for Medicare & Medicaid implement policies and procedures to periodically identify and assess whether security controls are in place and operating effectively in accordance with the most current NIST SP 800-53 controls and remediate weak controls timely.

CMS Response:
CMS concurs with OIG's recommendation. Since the time of OIG's review, CMS has implemented additional monitoring and vulnerability scanning tools to periodically identify and assess whether security controls are in place and operating effectively in accordance with the most current NIST SP 800-53 controls. Upon identification of an issue, CMS takes action to remediate the issue in a timely manner according to required ARS timelines based on severity.