PROJECT DESCRIPTION

DATA INTEGRITY

Detecting and Responding to Ransomware and Other Destructive Events

Tim McBride
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Michael Ekstrom
Lauren Lusty
Julian Sexton
Anne Townsend
The MITRE Corporation

February 2018

di-nccoe@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a community of interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

ABSTRACT

Ransomware, destructive malware, insider threats, and even honest mistakes present an ongoing threat to organizations that manage data in various forms. Database records and structure, system files, configurations, user files, application code, and customer data are all potential targets of data corruption and destruction.

A quick, accurate, and thorough detection and response to a loss of data integrity can save an organization time, money, and headaches. While human knowledge and expertise is an essential component of these tasks, the right tools and preparation are essential to minimizing downtime and losses due to data integrity events. The NCCoE, in collaboration with members of the business community and vendors of cybersecurity solutions, will build an example solution to address these data integrity challenges. This project will detail methods and potential tool sets that can detect, mitigate, and contain data integrity events in the components of an enterprise network. It also will identify tools and strategies to aid in a security team's response to such an event.

KEYWORDS

Data integrity, malware, ransomware, attack vector, malicious actor, malware detection, malware response

DISCLAIMER

TABLE OF CONTENTS

1 Executive Summary

Purpose

To defend against data integrity attacks, policies and tools must be in place with the capability to detect and respond to data integrity events. Prior to an event, information must be gathered to understand the range of normal activity within the enterprise environment; tools must be in place to detect the occurrence of a data integrity event; and policies must be established to respond efficiently and effectively. The purpose of this project is to help guide organizations in establishing the tools and procedures to detect data integrity events and respond in a way that is appropriate and timely.

The project described in this document could help organizations detect and respond to data integrity events. NCCoE projects include an architectural description and a reference design—an example solution—that addresses a technical challenge. Reference designs integrate commercial and open source products to demonstrate an implementation of standards and best practices. This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement our cybersecurity reference design that addresses this challenge.

Scope

This project will answer specific questions pertaining to detecting and responding to data integrity events:

- What is the baseline activity of systems and networks?
    - Identifying the baseline activity will prepare for detection of anomalous activity.
- When has a data integrity event occurred and what is the impact?
- How will a previously established response plan be executed?
- How will incidents be contained and mitigated?

This project will address:

- A network baselining solution to establish normal parameters for activity.
- An event detection solution with components that monitor:
- Systems for integrity events, including malicious code, unauthorized connections and devices, and similar events.
- Networks for unusual activity and potential cybersecurity events.
- An event data aggregation and correlation solution to assist in the detection, containment, mitigation, and response to a data integrity event.
- A vulnerability scanning solution to identify potential vectors for data integrity attacks.
- A forensic solution to assist forensic investigators in responding to a data integrity event.

This project will not address:

- Data security issues related to confidentiality or availability.

Assumptions/Challenges

Security Team

The size, budget, and expertise of members of a security team varies significantly among organizations. Both detection, and to a larger degree, response to a data integrity event depend on qualified security employees to analyze and act on the data presented by cybersecurity tools. This project will make assumptions about the core competencies of an organization's security team.

Implementation Decisions

There is a trade-off between the strength of protections on data and the time and resources spent maintaining those protections. Organizations should make decisions as to what data should be considered sensitive and warrant extra protections. This project will assume organizations can identify their sensitive data and tune the final reference architecture to suit their needs. We will aim to include, as part of the reference architecture, tools that will allow organizations to classify data as sensitive. However, we will not be able to provide guidance as to what data should be considered sensitive.

Background

In May 2017, the WannaCry ransomware infected more than 200,000 systems worldwide, causing widespread data loss. The ransomware exploited a vulnerability for which a patch was publicly released two months earlier. The Petya ransomware, which was discovered in 2016, used a vulnerability in an update system as an initial attack vector, and infected email attachments as a propagation vector. It attempted to encrypt both the user's files and the Master Boot Record (MBR). The adage "an ounce of prevention is worth a pound of cure" certainly holds true for enterprises—keeping systems patched and up-to-date is often a cost-effective and successful means of preventing the loss of data integrity. Unfortunately, even taking all possible preventative measures will not always stop the loss of data integrity, in which case the ability to quickly detect and respond to events is paramount.

This project is a follow-on to the NCCoE's first Data Integrity project, NIST SP 1800-11, "Data Integrity: Recovering from Ransomware and Other Destructive Events." That project began by working with organizations across a set of critical infrastructure industries. The NCCoE also met with representatives of the Financial Services Information Sharing and Analysis Center (FS-ISAC) for guidance, and worked with the FS-ISAC Destructive Malware Data Integrity Task Force to help scope the first project's challenge. These collaborations identified the need for a data integrity solution focused on recovery.

Additionally, the NCCoE held a workshop to identify key issues that affect consumer data protection, with workshop proceedings encapsulated in NISTIR 8050. Workshop participants identified data integrity (among other items) as a key cybersecurity issue that needs to be addressed, with many noting that malicious actors are continuously devising methods of corrupting data within organizations. The data corruption includes data modification as well as data destruction.

As this first project matured, additional topics arose that fell outside of the "Recover" phase of a data integrity attack, and aligned better with either "Identify," "Protect," "Detect," or "Respond" functions of the NIST Framework for Improving Critical Infrastructure Cybersecurity (referred to as the Cybersecurity Framework, or CSF). Thus, the evolution of the next two data integrity projects began. These projects have been broken into: (1) Identify and Protect and (2) Detect and Respond. The grouping was created due to the lifecycle of a data integrity attack. In

the stages prior to the attack, organizations must be able to identify their infrastructure and develop a protection capability. During an attack, organizations must be able to detect the occurrence and respond in accordance with their response plan. After an attack, organizations must be able to recover. The data integrity projects have been developed in accordance to this methodology.

2 SCENARIOS

The example scenarios below illustrate some of the challenges that this project will address. The relevant functions and categories from the CSF that can be employed to mitigate the events throughout the attack are listed below. The specific CSF subcategories are listed in parentheses in each table.

Scenario 1: Ransomware

For financial gain, an organized crime group has set up a seemingly legitimate domain with destructive malware disguised as a legitimate virus-scanning program. Once installed, it encrypts the organization's file system and demands a ransom payment in order to decrypt the files. Left unmitigated, the malware on one system is designed to move laterally within the network to other client and server systems within an organization's network, encrypting those systems and demanding ransom in exchange for their files.

The project addresses Detect and Respond CSF categories.

- User visits a phishing site.
  - Detect: Phishing site is identified as malicious (PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2).
  - Respond: Download is stopped (PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2).
  - Detect/Respond: Malware scans are performed to identify impact (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
  - Respond: Phishing site is added to list of blocked sites (RS.RP-1, RS.MI-1, RS.MI-2).
- Ransomware is downloaded from the phishing site.
  - Detect: Ransomware executable is identified as malicious (DE.AE-5, DE.CM-4, DE.CM-7, DE.DP-2, RS.CO-2).
  - Detect/Respond: Ransomware executable is contained, sandboxed, and analyzed (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
  - Respond: Ransomware executable is added to blacklist or blocked by whitelist, and security is notified of breach (RS.RP-1, RS.MI-1, RS.MI-2).
- Ransomware executes and attempts to move laterally and communicate with home server.
  - Detect: Ransomware communication is intercepted (DE.AE-1, DE.AE-5, DE.CM-1, DE.CM-7, DE.DP-2, RS.CO-2).
  - Detect: Attempts to gain remote access to a remote server through vulnerability exploitation are detected (DE.AE-1, DE.CM-1, DE.CM-7, DE.DP-2).

The project does not address these Identify, Protect, and Recover categories.

- Before ransomware is downloaded from a phishing site.
  - Identify:
    - Inventory of systems (ID.AM-1, ID.AM-2)
    - Identification of vulnerabilities (ID.RA-1, ID.RA-2, ID.RA-5, DE.CM-8)
  - Protect:
    - Network vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Host vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Create backups (PR.IP-4, PR.DS-1).
    - Utilize secure storage (PR.DS-1).
    - File system integrity information is baselined (PR.DS-6).
    - Logs of normal activity are captured (PR.PT-1).
    - Maintenance infrastructure for vulnerability mitigation is operational (PR.MA-2).
- Ransomware executes and attempts to move laterally and communicate with home server.
  - Recover: Backups are used to remediate the damage (RC.RP-1).

Scenario 2: Data Destruction Malware

An adversary wishing to impact an organization's operations leaves several infected Universal Serial Bus (USB) drives in the parking lot of the building. When an unsuspecting employee plugs in the drive, it immediately modifies text files and deletes media files on the user's machine.

The project addresses Detect and Respond CSF categories.

- User inserts an infected USB drive.
  - Detect: USB is identified as malicious (DE.AE-5, DE.CM-4, DE.CM-7, DE.DP-2, RS.CO-2).
  - Respond: Autorun is halted (DE.AE-5, DE.CM-4, DE.CM-7, DE.DP-2, RS.CO-2).
- The USB drive attempts to execute the malware.
  - Detect/Respond: USB's executable is contained, sandboxed, and analyzed (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
  - Respond: USB's executable is added to blacklist or blocked by whitelist, and security is notified of breach (RS.RP-1, RS.MI-1, RS.MI-2).
- Malware executes and attempts to modify the system's files.
  - Respond: Malware origin is identified and USB is removed (RS.RP-1, RS.MI-1, RS.MI-2).

The project does not address these Identify, Protect, and Recover categories.

- Before a USB containing destructive malware is inserted.
  - Identify:
    - Inventory of systems (ID.AM-1, ID.AM-2)
    - Identification of vulnerabilities (ID.RA-1, ID.RA-2, ID.RA-5, DE.CM-8)
  - Protect:
    - Network vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Host vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Create backups (PR.IP-4, PR.DS-1).
    - Utilize secure storage (PR.DS-1).
    - File system integrity information is baselined (PR.DS-6).
    - Logs of normal activity are captured (PR.PT-1).
    - Maintenance infrastructure for vulnerability mitigation is operational (PR.MA-2).
- Malware executes and attempts to modify the system's files.
  - Recover: Backups are used to remediate the damage (RC.RP-1).

Scenario 3: Virtual Machine Data Loss

A privileged user running automatic maintenance on the organization's virtual machines (VMs) accidentally deletes one of the VMs. The user does not immediately notice the accidental deletion.

The project addresses Detect and Respond CSF categories.

- Maintenance script deletes a VM.
  - Detect: VM deletion is identified as abnormal (DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2).
  - Detect/Respond: Impact of VM deletion is analyzed (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
  - Respond: Security team is notified about VM deletion (RS.RP-1, RS.MI-1, RS.MI-2).

The project does not address these Identify, Protect and Recover categories.

- Before the accidental change happens
  - Identify:
    - Inventory of virtual machines (ID.AM-2)
  - Protect:
    - Create virtual machine backups (PR.IP-4, PR.DS-1).
    - Utilize secure storage (PR.DS-1).
    - Logs of normal virtual activity are captured (PR.PT-1).
- Maintenance script deletes a VM.
  - Recover: Virtual machine backups are used to remediate the damage (RC.RP-1).

Scenario 4: Server Permissions Change

An adversary wishing to gain access to an organization's operations launches a spear-phishing campaign against privileged individuals in the target organization through the use of an infected email attachment. When one of the users opens the attachment, the malware immediately begins creating back doors for the adversary to use at a later point.

The project addresses Detect and Respond CSF categories.

- User receives spear-phishing email.
    - Detect: Email is identified as a phishing email (PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2).
    - Detect/Respond: Malware scans are performed to identify impact (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
    - Respond: Security team is notified about phishing attempt and email is automatically moved to spam across the enterprise (RS.RP-1, RS.MI-1, RS.MI-2).
- User downloads infected email attachment.
    - Detect: Attachment is identified as infected (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
    - Detect/Respond: Attachment executable is contained, sandboxed, and analyzed (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
    - Respond: Attachment is added to blacklist or blocked by whitelist, and security is notified of potential breach (RS.RP-1, RS.MI-1, RS.MI-2).
- User opens infected email attachment and malware executes.
    - Detect: Back door creation is logged and flagged as suspicious (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
    - Detect: Network activity related to these back doors is intercepted (RS.RP-1, RS.MI-1, RS.MI-2).
    - Respond: Security is notified of suspicious activity and back doors are disabled (RS.RP-1, RS.MI-1, RS.MI-2).

The project does not address these Identify, Protect, and Recover categories.

- Before the spear-phishing email is received
  - Identify:
    - Inventory of systems (ID.AM-1, ID.AM-2)
    - Inventory of account structure (ID.AM-2, ID.AM-3)
    - Identification of vulnerabilities (ID.RA-1, ID.RA-2, ID.RA-5, DE.CM-8)
  - Protect:
    - Network vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Host vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Create system state backups (PR.IP-4, PR.DS-1).
    - Utilize secure storage for these backups (PR.DS-1).
    - Logs of administrator activity are captured (PR.PT-1).
- User opens infected email attachment and malware executes.
  - Recover: System state backups are used to restore the account structure (RC.RP-1).

Scenario 5: Database Metadata Change

An insider seeking to disrupt an organization's operations for financial gain in the stock market makes changes to the database structure. These changes leave the applications relying on the affected database tables unable to function properly.

The project addresses Detect and Respond CSF categories.

- Insider changes directory structure.
  - Detect/Respond: Structure changes to the database and the associated user are noticed and reported (DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2).
  - Detect/Respond: Errors in connecting to the database and other impacted systems are noticed and reported (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
  - Respond: Security is notified of abnormal user activity (RS.RP-1, RS.MI-1, RS.MI-2).

The project does not address these Identify, Protect, and Recover categories.

- Before the insider makes changes to the database structure
  - Identify:
    - Inventory of database structure (ID.AM-2)
    - Inventory of systems relying on the database (ID.AM-1, ID.AM-2)
    - Identification of vulnerabilities (ID.RA-1, ID.RA-2, ID.RA-5, DE.CM-8)
  - Protect:
    - Network vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Host vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Create database backups (PR.IP-4, PR.DS-1).
    - Logs of queries are captured (PR.PT-1).
    - Database structure is baselined with integrity monitoring tool (PR.DS-6).
- Insider changes directory structure.
  - Recover: Database backups are used to restore the database structure (RC.RP-1).

Scenario 6: Insider File Changes

An insider seeking to gain shares in the company acquires the credentials of an administrator. Using these credentials, he searches for his name in the company records and backup records, attempting to increase the number of shares he receives as part of his yearly salary.

The project addresses these Detect and Respond categories.

- Insider changes organization's records.
  - Detect/Respond: Changes to the file and the associated user are noticed and reported (DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2).
  - Detect/Respond: Impact of file change is analyzed (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
  - Respond: Security is notified of abnormal user activity (RS.RP-1, RS.MI-1, RS.MI-2).

The project does not address these Identify, Protect, and Recover CSF categories.

- Before the insider makes changes to the records
  - Identify:
    - Inventory of systems (ID.AM-1, ID.AM-2)
    - Inventory of account structure (ID.AM-2, ID.AM-3)
    - Identification of vulnerabilities (ID.RA-1, ID.RA-2, ID.RA-5, DE.CM-8)
  - Protect:
    - Network vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Host vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Create backups of data (PR.IP-4, PR.DS-1).
    - Backups are encrypted and protected (PR.IP-4, PR.DS-1).
    - Logs of file changes are captured (PR.PT-1).
    - File changes are baselined by integrity monitoring tool (PR.DS-6).
- Insider changes directory structure
  - Recover: Backups are used to restore the files (RC.RP-1).

Scenario 7: Compromised Update Server

During routine machine updates, an update is downloaded and installed that contains a back door. A malicious outsider then uses this back door to gain unauthorized access to the machine.

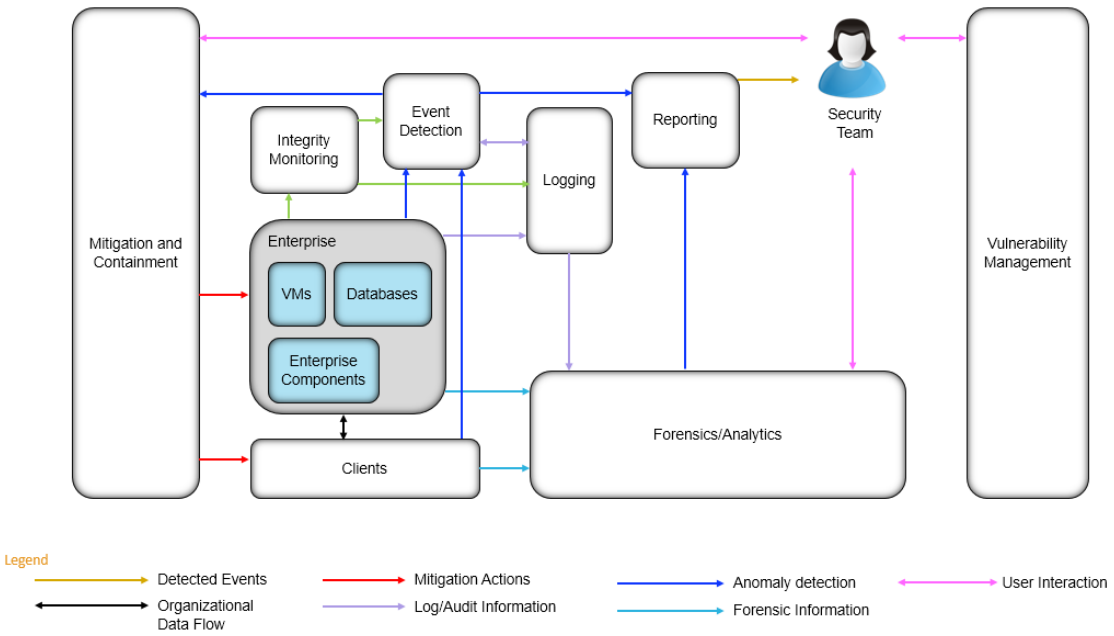
The project addresses these Detect and Respond CSF categories.

- Compromised update is downloaded.
  - Detect: Update site is identified as malicious (PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2).
  - Respond: Download is stopped (PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2).
  - Detect/Respond: Malware scans are performed to identify impact (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
  - Respond: Update is added to list of blocked downloads (RS.RP-1, RS.MI-1, RS.MI-2).
- Compromised update is installed
  - Detect: Update is identified as malicious (DE.AE-5, DE.CM-4, DE.CM-7, DE.DP-2, RS.CO-2).
  - Detect/Respond: Update is contained, sandboxed, and analyzed (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4).
  - Respond: Update is added to blacklist or blocked by whitelist, and security is notified of breach (RS.RP-1, RS.MI-1, RS.MI-2).
- Malicious outsider accesses the machine using the backdoor.
  - Detect: Unauthorized communication is intercepted (DE.AE-1, DE.AE-5, DE.CM-1, DE.CM-7, DE.DP-2, RS.CO-2).
  - Respond: Update is removed from affected systems (DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2)

The project does not address these Identify, Protect, and Recover categories.

- Before the compromised update is downloaded and installed.
  - Identify:
    - Inventory of systems (ID.AM-1, ID.AM-2)
    - Identification of vulnerabilities (ID.RA-1, ID.RA-2, ID.RA-5, DE.CM-8)
  - Protect:
    - Network vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Host vulnerabilities are mitigated (PR.IP-12, RS.MI-3).
    - Create backups of data (PR.IP-4, PR.DS-1).
    - Backups are encrypted and protected (PR.IP-4, PR.DS-1).
    - Logs of file changes are captured (PR.PT-1).
    - File changes are baselined by integrity monitoring tool (PR.DS-6)
    - Maintenance infrastructure for vulnerability mitigation is operational (PR.MA-2).
- Compromised update is installed.
  - Recover: Backups are used to remediate the damage (RC.RP-1).

3 High-Level Architecture



The above figure identifies a high-level architecture of the enterprise system and the associated components for this project. During the development of the laboratory environment implementing this project, the figure will be refined to describe detailed components and mapped to the physical architecture in the lab environment for the specific scenario being implemented. A goal of this figure is to help spur identification of project participants and hardware and software components for collaborative use in a laboratory environment to build open, standards-based, modular, end-to-end reference designs.

Component List

Data integrity solutions for this project include, but are not limited, to:

- integrity monitoring
- event detection
    - malicious software detection
    - unauthorized activity detection
    - anomalous activity detection
- logging and data correlation software
- reporting capability
- vulnerability management
- forensics/analytics tools
- mitigation and containment software

Desired Solution Characteristics

To address the scenarios in Section 2, this project will use a selection of commercially available technologies to demonstrate the security and functional characteristics of a data integrity solution designed to satisfy the Detect and Respond functions of the CSF. The solution shall:

- detect unauthorized or malicious
    - activity on the network
    - mobile code (such as web technologies like JavaScript, VBScript, and other code executed locally but loaded from an external site)
    - executables
    - behavior
- report unauthorized or malicious:
    - activity on the network
    - mobile code events
    - executables
    - behavior
- analyze the impact of unauthorized or malicious:
    - activity on the network
    - mobile code events
    - executables
    - behavior

- mitigate the impact of unauthorized or malicious:
    - activity on the network
    - mobile code events
    - executables
    - behavior
- contain unauthorized or malicious
    - activity on the network
    - mobile code events
    - executables
    - behavior

4 Relevant Standards and Guidance

- Office of Management and Budget Circular Number A-130 – Managing Information as a Strategic Resource
  https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
- NIST FIPS 140-2 – Security Requirements for Cryptographic Modules
  http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- NIST SP 800-37 Rev. 1 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf
- NIST SP 800-53 Rev. 4 – Security and Privacy Controls for Federal Information Systems and Organizations
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST SP 800-57 Part 1 Revision 4 – Recommendation for Key Management: Part 1 – General
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
- NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- NIST SP 800-83 Rev. 1 – Guide to Malware Incident Prevention and Handling
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf
- NIST SP 800-150 – Guide to Cyber Threat Information Sharing
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
- NIST SP 800-160 – Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
- NIST SP 800-184 – Guide for Cybersecurity Event Recover for Federal Information and Information Systems
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

- NIST Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1 https://www.nist.gov/sites/default/files/documents/draft-cybersecurity-framework-v1.11.pdf

5 Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF), and other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Table 1: Security Control Map

Solution Characteristics	NIST CSF Category	Informative References	Relevant Industry Standards
The solution will have the capability to detect unauthorized or malicious activity on its network	DE.AE-1, DE.CM-1, DE.CM-7, DE.DP-2	**NIST 800-53 Rev. 4** AC-2, AC-4, AU-12, CA-2, CA-3, CA-7, CM-2, CM-3, CM-8, PE-3, PE-6, PE-20, PM-24, SC-5, SC-7, SI-4 **ISO/IEC 27001:2013** A.18.1.4	**HIPAA** 164.308.a.6.ii
The solution will have the capability to report unauthorized or malicious activity on its network	DE.AE-5, RS.CO-2, RS.RP-1	**NIST 800-53 Rev. 4** AU-6, CP-2, CP-10, IR-4, IR-5, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2, A.16.1.5	
The solution will analyze the impact of unauthorized or malicious activity on its network	DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-4, RS.RP-1	**NIST 800-53 Rev. 4** AU-6, CA-7, CP-2, CP-10, IR-4, IR-5, IR-8, PE-6, RA-3, SI-4 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.1, A.16.1.4, A.16.1.5, A.16.1.6	
The solution will contain unauthorized or malicious activity on its network	RS.MI-1, RS.RP-1	**NIST 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2, A.16.1.5	
The solution will mitigate the impact of unauthorized or malicious activity on its network	RS.MI-2, RS.RP-1	**NIST 800-53 Rev. 4** C-2, CP-10, IR-4, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.12.2.1, A.16.1.2, A.16.1.5	**HIPAA:** 164.308.a.6.ii
The solution will have the capability to detect unauthorized or malicious mobile code on its hosts	PR.DS-6, DE.CM-5, DE.DP-2	**NIST 800-53 Rev. 4** CA-2, CA-7, PM-24, SI-4, SI-7 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.18.1.4	**HIPAA:** 164.308.a.6.ii, 164.308.a.6.ii
The solution will have the capability to report unauthorized or malicious mobile code on its hosts	DE.AE-5, RS.CO-2, RS.RP-1	**NIST 800-53 Rev. 4** AU-6, CP-2, CP-10, IR-4, IR-5, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2, A.16.1.5	

Solution Characteristics	NIST CSF Category	Informative References	Relevant Industry Standards
The solution will analyze the impact of unauthorized or malicious mobile code on its hosts	DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1	**NIST 800-53 Rev. 4** AU-6, AU-7, CA-7, CP-2, CP-10, IR-4, IR-5, IR-8, PE-6, RA-3, SI-4 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.1, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	
The solution will contain unauthorized or malicious mobile code on its hosts	RS.MI-1, RS.RP-1	**NIST 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2, A.16.1.5	
The solution will mitigate the impact of unauthorized or malicious mobile code on its hosts	RS.MI-2, RS.RP-1	**NIST 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.12.2.1, A.16.1.2, A.16.1.5	**HIPAA:** 164.308.a.6.ii
The solution will have the capability to detect unauthorized or malicious code execution	DE.CM-4, DE.CM-7, DE.DP-2	**NIST 800-53 Rev. 4** AU-12, CA-2, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, PM-24, SI-3, SI-4 **ISO/IEC 27001:2013** A.12.2.1, A.18.1.4	**HIPAA:** 164.308.a.5.ii.B, 164.308.a.6.ii
The solution will have the capability to report unauthorized or malicious code execution	DE.AE-5, RS.CO-2, RS.RP-1	**NIST 800-53 Rev. 4** AU-6, CP-2, CP-10, IR-4, IR-5, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2, A.16.1.5	**HIPAA:** 164.308.a.5.ii.B
The solution will analyze the impact of unauthorized or malicious code execution	DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1	**NIST 800-53 Rev. 4** AU-6, AU-7, CA-7, CP-2, CP-10, IR-4, IR-5, IR-8, PE-6, RA-3, SI-4 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.1, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	
The solution will contain unauthorized or malicious code execution	RS.MI-1, RS.RP-1	**NIST 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2, A.16.1.5	
The solution will mitigate the impact of unauthorized or malicious code execution	RS.MI-2, RS.RP-1	**NIST 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.12.2.1, A.16.1.2, A.16.1.5	**HIPAA:** 164.308.a.6.ii
The solution will have the capability to detect unauthorized or malicious user behavior	DE.CM-3, DE.CM-7, DE.DP-2	**NIST 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-2, CA-7, CM-3, CM-8, CM-10, CM-11, PE-3, PE-6, PE-20, PM-24, SI-4 **ISO/IEC 27001:2013** A.12.4.1, A.18.1.4	**HIPAA:** 164.308.a.6.ii, 164.312.b

Solution Characteristics	NIST CSF Category	Informative References	Relevant Industry Standards
The solution will have the capability to report unauthorized or malicious user behavior	DE.AE-5, RS.CO-2, RS.RP-1	**NIST 800-53 Rev. 4** AU-6, CP-2, CP-10, IR-4, IR-5, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2, A.16.1.5	
The solution will analyze the impact of unauthorized or malicious user behavior	DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1	**NIST 800-53 Rev. 4** AU-6, AU-7, CA-7, CP-2, CP-10, IR-4, IR-5, IR-8, PE-6, RA-3, SI-4 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.1, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	
The solution will contain unauthorized or malicious user behavior	RS.MI-1, RS.RP-1	**NIST 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2, A.16.1.5	
The solution will mitigate the impact of unauthorized or malicious user behavior	RS.MI-2, RS.RP-1	**NIST 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 **ISO/IEC 27001:2013** A.6.1.3, A.12.2.1, A.16.1.2, A.16.1.5	**HIPAA:** 164.308.a.6.ii

APPENDIX A - REFERENCES

[1] Jim McCarthy et al., *Identity and Access Management for Electric Utilities,* NIST Special Publication (SP) 1800-2, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2015. https://nccoe.nist.gov/sites/default/files/library/sp1800/es-idam-nist-sp1800-2-draft.pdf [accessed 10/2/17].

[2] B. Fisher et al., *Attribute Based Access Control,* NIST Special Publication (SP) 1800-3, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2017. https://nccoe.nist.gov/sites/default/files/library/sp1800/abac-nist-sp1800-3-draft-v2.pdf [accessed 10/2/17].

[3] *Cyber attack hits 200,000 in at least 150 countries: Europol,* Reuters [www.reuters.com], https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX [accessed 10/2/17].

[4] Lucian Constantin, *Petya ransomware is now double the trouble*, NetworkWorld [www.networkworld.com], https://www.networkworld.com/article/3069990/petya-ransomware-is-now-double-the-trouble.html [accessed 10/2/17].

[5] *Global ransomware attack causes turmoil*, BBC News [www.bbc.com], http://www.bbc.com/news/technology-40416611 [accessed 10/2/17].

[6] Leah Kauffman, et al., *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy,* NIST Internal Report (IR) 8050, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2, 2015. https://nccoe.nist.gov/sites/default/files/library/nistir-8050-draft.pdf [accessed 10/2/17].

[7] Tim McBride, et al., *DRAFT Data Integrity: Recovering from Ransomware and Other Destructive Events,* NIST Special Publication (SP) 1800-11, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2017. https://nccoe.nist.gov/publication/1800-11/ [accessed 10/2/17].

[8] *Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1,* National Institute of Standards and Technology, Gaithersburg, Maryland, January 2017. https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf [accessed 10/5/2017].

[9] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat 1936. https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

[10] Office of Management and Budget (OMB), *Management of Federal Information Resources,* OMB Circular No. A-130, November 2000. https://www.whitehouse.gov/omb/circulars_a130_a130trans4 [accessed 11/15/17].

[11] U.S. Department of Commerce. *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards (FIPS) Publication 140-2, May 2001, 69pp. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf [accessed 11/15/17].

[12] R. Ross *et al*., *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST Special Publication (SP) 800-37, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2010, 101pp. http://dx.doi.org/10.6028/NIST.SP.800-37r1

[13] R. Ross *et al.*, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013, 461pp. http://doi.org/10.6028/NIST.SP.800-53r4

[14] E. Barker, *Recommendation for Key Management*, NIST Special Publication (SP) 800-57 Part 1 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2016, 159pp. https://doi.org/10.6028/NIST.SP.800-57pt1r4

[15] P. Cichonski *et al.*, *Computer Security Incident Handling Guide*, NIST Special Publication (SP) 800-61 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2012, 79pp. http://dx.doi.org/10.6028/NIST.SP.800-61r2

[16] M. Souppaya and K. Scarfone, *Guide to Malware Incident Handling and Prevention for Desktops and Laptops*, NIST Special Publication (SP) 800-83 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013, 46pp. https://doi.org/10.6028/NIST.SP.800-83r1

[17] C. Johnson *et al.*, *Guide to Cyber Threat Information Sharing*, NIST Special Publication (SP) 800-150, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2016, 42pp. https://doi.org/10.6028/NIST.SP.800-150

[18] R. Ross *et al.*, *Systems Security Engineering*, NIST Special Publication (SP) 800-160, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2016, 256pp. https://doi.org/10.6028/NIST.SP.800-160

[19] M. Bartock *et al.*, *Guide for Cybersecurity Event Recovery*, NIST Special Publication (SP) 800-184, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2016, 52pp. http://dx.doi.org/10.6028/NIST.SP.800-184

APPENDIX B - ACRONYMS AND ABBREVIATIONS

Provide a list of alphabetized acronyms and abbreviations spelled out here, using a borderless table.

CSF	Cybersecurity Framework
FIPS	Federal Information Processing Standard
FS-ISAC	Financial Sector Information Sharing and Analysis Center
ISAC	Information Sharing and Analysis Center
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
SP	Special Publication
USB	Universal Serial Bus
VM	Virtual Machine

APPENDIX C - GLOSSARY

Provide a list of alphabetized words and terms defined here, using a borderless table.

Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. SOURCE: SP 800-30
Analysis	The examination of acquired data for its significance and probative value to the case. SOURCE: SP 800-72
Attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. SOURCE: CNSSI-4009
Back Door	Typically unauthorized hidden software or hardware mechanism used to circumvent security controls. SOURCE: CNSSI-4009
Backup	A copy of files and programs made to facilitate recovery. SOURCE: SP 800-34; CNSSI-4009
Baselining	Monitoring resources to determine typical utilization patterns so that significant deviations can be detected. SOURCE: SP 800-61
Blacklist	A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity. SOURCE: SP 800-94
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks. SOURCE: CNSSI-4009
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted. SOURCE: CNSSI-4009
Data Integrity	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. SOURCE: CNSSI-4009
Data Loss	The alteration or deletion of proprietary, sensitive, personal, or otherwise critical data. Note: The definition in NIST IR 7298 describes data loss as a loss of confidentiality, for example, where data is stolen and leaked. Here, we refer to data loss as data being destroyed in some way.

Decryption	Conversion of ciphertext to plaintext through the use of a cryptographic algorithm. SOURCE: FIPS 185
Encryption	Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. SOURCE: FIPS 185
Enterprise	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. SOURCE: CNSSI-4009
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. SOURCE: SP 800-61
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. SOURCE: SP 800-60
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. SOURCE: SP 800-83
Master Boot Record	A section of partitioned drives that describes how information is stored on the drive. It also usually loads the installed operating system.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. Note: Some examples of software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, ActiveX, VBScript, etc. SOURCE: CNSSI-4009
Phishing	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. SOURCE: SP 800-83

Ransomware	A type of malware that encrypts data on a system, usually with the goal of selling the data back to the owner for money.
Security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. SOURCE: CNSSI-4009
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009
Virus	A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk. SOURCE: CNSSI-4009
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. SOURCE: SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200
Zero-day Exploit	An attack on an information system that makes use of a zero-day vulnerability.
Zero-day Vulnerability	A vulnerability in an existing system or application that is unknown to the vendor.