CMMC ASSESSMENT GUIDE

Level 3

Version 2.1 | July 2023

NOTICES

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing CMMC requirements under the law or departmental policies.

[DISTRIBUTION STATEMENT A] Approved for public release.

TABLE OF CONTENTS

Introduction

This document is intended to provide guidance in the prearation for and execution of a Level 3 Certification Assessment under the Cybersecurity Maturity Model Certification (CMMC) Program as set forth in section 170.18 of title 32, Code of Federal Regulations (CFR).. Certification at each CMMC level occurs independently. Guidance for conducting a CMMC Level 1 self-assessment can be found in *CMMC Self-Assessment Guide – Level 1*. Guidance for conducting a CMMC Level 2 assessment, both self-assessment and Level 2 Certification Assessment, can be found in *CMMC Assessment Guide – Level 2*. More details on the model can be found in the *CMMC Model Overview* document.

A *CMMC Assessment* as defined in 32 C.F.R. § 170.4 means the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system, or organization as defined in 32 C.F.R. § 170.15 to 32 C.F.R. § 170.18. A CMMC Level 3 *Assessment* as defined in 32 C.F.R. § 170.4 is the activity performed by the Department of Defense (DoD) to evaluate the CMMC level of an Organization Seeking Certification (OSC). For CMMC Level 3, assessments are performed exclusively by the DoD.

An OSC seeking a CMMC Level 3 Certification must have first received a CMMC Level 2 Final Certification, as set forth in 32 C.F.R. § 170.18, for all applicable information systems within the assessment scope, and the OSC must implement the Level 3 requirements specified in 32 C.F.R. § 170.14(c)(4). . This is followed by the CMMC Level 3 assessment conducted by the DoD.

OSCs may also use this guide to perform CMMC Level 3 self-assessment (for example, in preparation for an annual affirmation); however, they are not eligible to submit results from a self-assessment in support of a CMMC Level 3 Certification. Only the results from an assessment by the DOD are considered for award of a CMMC Level 3 Certification. Level 3 reporting and affirmation requirements can be found in 32 C.F.R. § 170.18 and 32 C.F.R. § 170.22.

CMMC Level 3 Description

CMMC Level 3 consists of the security requirements derived from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*, with DoD-approved parameters where applicable. CMMC Level 3 only applies to systems that have already achieved a CMMC Level 2 Final Certification. CMMC Level 2 consists of the security requirements specified in NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

Like CMMC Level 2, CMMC Level 3 addresses the protection of Controlled Unclassified Information (CUI), as defined in 32 C.F.R. § 2002.4(h):

> *Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see paragraph (e) of this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.*

CMMC Level 3 provides additional protections against advanced persistent threats (APTs), and increased assurance to the DoD that an OSC can adequately protect CUI at a level commensurate with the adversarial risk, to include protecting information flow with the government and with subcontractors in a multitier supply chain.

Purpose and Audience

This guide is intended for assessors, OSCs, and information technology (IT) and cybersecurity professionals. to use as part of preparation for a CMMC Level 3 assessment.

Document Organization

This document is organized into the following sections:

- **Assessment and Certification:** Provides an overview of the CMMC Level 3 assessment and certification process, guidance regarding OSC size, and the assessment scope as defined in 32 C.F.R. § 170.19.
- **Assessment Criteria and Methodology:** Provides guidance on the criteria and methodology (i.e., *interview*, *examine*, and *test*) to be employed during a CMMC Level 3 assessment, as defined in 32 C.F.R. § 170.4, as well as requirement findings.
- **CMMC-Specific Terms:** Incorporates definitions from 32 C.F.R. § 170.4, definitions included by reference from 32 C.F.R. § 170.2, and provides clarification of the intent and scope of specific terms as used in the context of CMMC.
- **Requirement Descriptions:** Provides the assessment specifics for each CMMC Level 3 requirement.

Assessment and Certification

The DoD will use the assessment methods defined in NIST SP 800-172A, *Assessing Enhanced Security Requirements for Controlled Unclassified Information*, and the supplemental information in this guide to conduct CMMC Level 3 assessments. Assessors will review information and evidence to verify that an OSC meets the stated assessment objectives for all of the requirements.

An OSC can achieve a CMMC certification for an entire enterprise network or for specific enclave(s), depending on the CMMC Assessment Scope as defined in 32 C.F.R. § 170.19 (d).

Assessment Scope

Prior to conducting a CMMC assessment, the Level 3 CMMC Assessment Scope must be defined as addressed in 32 C.F.R. § 170.19(d) and the *CMMC Assessment Scope – Level 3* document[1]. The CMMC Assessment Scope informs which assets within the OSC's environment will be assessed and the details of the assessment.

The OSC must have received CMMC Level 2 certification of all systems included within the Level 3 CMMC Assessment Scope prior to requesting the Level 3 assessment, as set forth in 32 C.F.R. § 170.18. The Level 3 assessment scoping is based on the scoping guidance provided in 32 C.F.R. § 170.19(d) and the *CMMC Assessment Scope – Level 3* document. The *CMMC Assessment Scope – Level 3* document is available on the official CMMC documentation site at https://dodcio.defense.gov/CMMC/Documentation/. If a Level 2 Final Certification has not already been achieved for the desired CMMC Assessment Scope, the OSC may not proceed with the Level 3 assessment.

[1] Note that an OSC may request a Level 2 assessment based on Level 3 scoping guidance.

CMMC-Specific Terms

The CMMC Program has specific terms that align with program requirements. Although some terms may have other definitions in open forums, it is important to understand these terms as they apply to the CMMC Program. The definitions set forth below are defined in 32 C.F.R. § 170.4 and also are included in the *CMMC Glossary and Acronyms*.The specific terms associated with CMMC Level 3 are:

- **Assessment:** (as defined 32 C.F.R. § 170.4) The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization defined in 32 C.F.R. § 170.15 to 32 C.F.R. § 170.18. *CMMC Level 3 Assessment* as defined in 32 C.F.R. § 170.4 is the term used for the activity performed by the DoD to evaluate the CMMC level of an OSC.
- **Asset (Organizational Asset):** Anything that has value to an organization, including, but not limited to, another organization, person, computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards) [included by reference from NIST Interagency Report (NISTIR) 7693, NISTIR 7694 (32 C.F.R. § 170.2)]. Understanding *assets* is critical to identifying the *CMMC Assessment Scope*; for more information see *CMMC Assessment Scope – Level 3*.
- **Assessment Scope:** (32 C.F.R. § 170.4) is defined in 32 C.F.R. §170.19 and includes all *assets* in the OSC's environment that will be assessed against CMMC requirements defined in § 170.19.
- **Conditional Certification:** (as described in 32 C.F.R. § 170.17 (a) (1)) Obtaining a temporary 180-day CMMC certificate from a C3PAO or the DoD with a Plan of Action and Milestones (POA&M as defined in 32 C.F.R. §170.4) that meets all CMMC POA&M requirements.
- **Conditional Assessment Certification**: (defined in 32 C.F.R. §170.18) The OSC is considered to have achieved CMMC Level 3 Conditional Assessment Certification if their POA&M meets all CMMC Level 3 POA&M requirements listed in § 170.21(a)(3).
- **Final Certification:** (as described in 32 C.F.R. § 170.17 (a) (1) (iii)) Obtaining a CMMC Certificate from a C3PAO or the DoD with no open CMMC POA&M items, resulting in a perfect score published in the Supplier Performance Risk System (SPRS).
- **Event:** Any observable occurrence in a network or system, as defined in NIST SP 800-37 Revision 2, incorporated by reference in 32 C.F.R. § 170.2. *Events* sometimes provide indication that an *incident* is occurring.
- **Incident:** An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or

196 transmits or that constitutes a violation or imminent threat of violation of security
197 policies, security procedures, or acceptable use policies [NIST SP 800-171 Rev 2].

198 • **Monitor:** The act of continually checking, supervising, critically observing, or
199 determining the status in order to identify change from the performance level required
200 or expected at an *organization-defined* frequency and rate [NIST SP 800-160 (adapted)].

201 • **Organization-Defined:** As determined by the OSC being assessed . except as defined in
202 the case of Organization-Defined Parameter (ODP). This can be applied to a frequency
203 or rate at which something occurs within a given time period, or it could be associated
204 with describing the configuration of a OSC's solution.

205 • **Organization-Defined Parameter (ODP):** ODP means selected enhanced security
206 requirements contain selection and assignment operations to give organizations
207 flexibility in defining variable parts of those requirements, as defined in NIST SP 800-
208 172A. ODPs are used in NIST SP 800-172 and NIST SP 800-172A to allow Federal
209 agencies, in this case the DoD, to customize security requirements. Once specified, the
210 values for the assignment and selection operations become part of the requirement and
211 objectives, where applicable. The assignments and selections chosen for CMMC Level 3
212 are underlined in the requirement statement and objectives. In some cases, further
213 specificity of the assignment or selection will need to be made by the OSC. In those
214 cases, the term and abbreviation ODP is used in the assessment objectives to denote
215 where additional definition is required.

216 • **Periodically:** Occurring at regular intervals. As used in many requirements within
217 CMMC, the interval length is *organization-defined* to provide OSC flexibility, with an
218 interval length of no more than one year.

Assessment Criteria and Methodology

The *CMMC Assessment Guide – Level 3* leverages the assessment procedure described in NIST SP 800-172A Section 2.1:

> *An assessment procedure consists of an assessment objective and a set of potential assessment methods and objects that can be used to conduct the assessment. Each assessment objective includes a set of determination statements related to the CUI enhanced security requirement that is the subject of the assessment. Organization-defined parameters (ODP) that are part of selected enhanced security requirements are included in the initial determination statements for the assessment procedure. ODPs are included since the specified parameter values are used in subsequent determination statements. ODPs are numbered sequentially and noted in bold italics.*
>
> *Determination statements reflect the content of the enhanced security requirements to ensure traceability of the assessment results to the requirements. The application of an assessment procedure to an enhanced security requirement produces assessment findings. The findings are used to determine if the enhanced security requirement has been satisfied.*
>
> *Assessment objects are associated with the specific items being assessed. These objects can include specifications, mechanisms, activities, and individuals.*
>
> - *Specifications are the document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, architectural designs) associated with a system.*
> - *Mechanisms are the specific hardware, software, or firmware safeguards employed within a system.*
> - *Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic).*
> - *Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.*
>
> *Assessment methods define the nature and the extent of the assessor's actions. The methods include examine, interview, and test.*
>
> - *The examine method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities).*
> - *The interview method is the process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence.*

- *The test method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior.*

The purpose of the assessment methods is to facilitate understanding, achieve clarification, and obtain evidence. The results obtained from applying the methods are used for making the specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.

Criteria

Assessment objectives are provided for each requirement and are based on existing criteria from NIST SP 800-172A. The criteria are authoritative and provide a basis for the assessor to conduct an assessment of a requirement.

Methodology

During the CMMC assessment, the assessor will verify and validate that the OSC has properly implemented the requirements. Because an OSC can meet the assessment objectives in different ways (e.g., through documentation, computer configuration, network configuration, or training), the assessor may use a variety of techniques, including one or more of the three assessment methods described above from NIST SP 800-172A, to determine if the OSC meets the intent of the requirements.

The assessor will follow the guidance in NIST SP 800-172A when determining which assessment methods to use:

Organizations [DoD] are not expected to use all of the assessment methods and objects contained within the assessment procedures identified in this publication. Rather, organizations have the flexibility to establish the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and objects are deemed to be the most useful in obtaining the desired results). The decision on level of effort is made based on how the organization can accomplish the assessment objectives in the most cost-effective and efficient manner and with sufficient confidence to support the determination that the CUI enhanced security requirements have been satisfied.

The primary deliverable of an assessment is a compliance score and accompanying report that contains the findings associated with each requirement. For more detailed information on assessment methods, see Appendix C of NIST SP 800-172A.

Figure 1 illustrates an example of an assessment procedure for requirement AC.L3-3.1.3e.

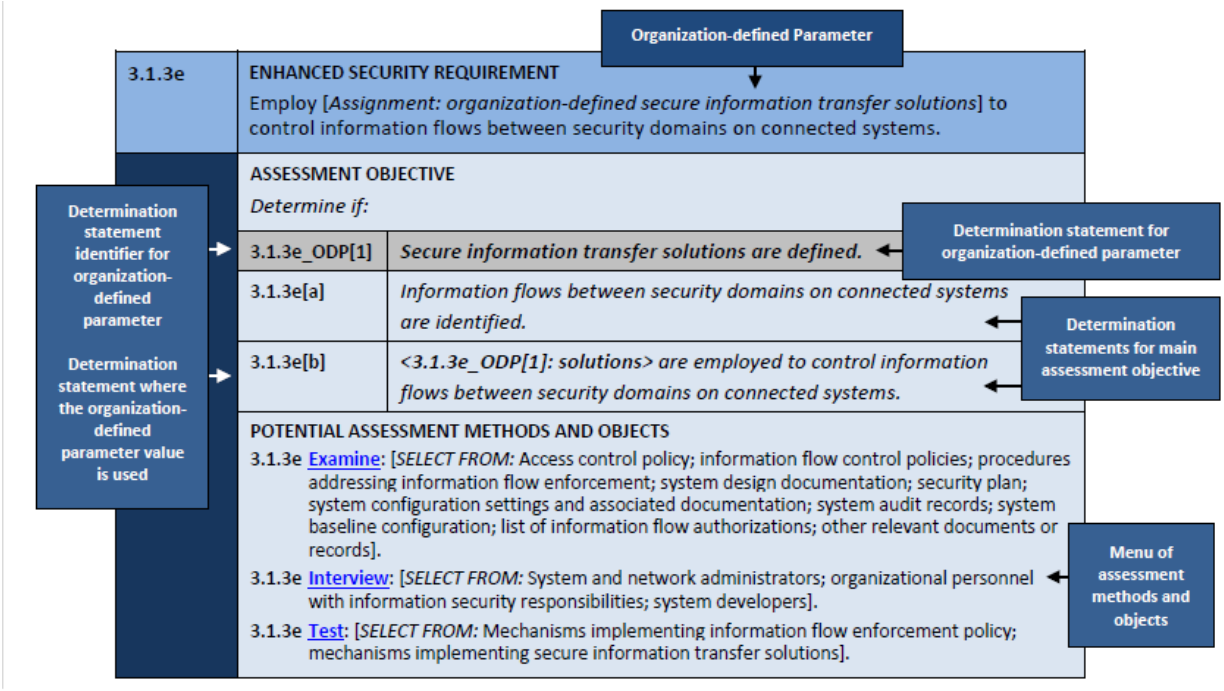

FIGURE 1: ASSESSMENT PROCEDURE FOR CUI ENHANCED SECURITY REQUIREMENT

Who Is Interviewed

The assessor has discussions with OSC staff to understand if a requirement has been addressed. Interviews with applicable staff (possibly at different organizational levels) determine if CMMC requirements are implemented and if adequate resourcing, training, and planning have occurred for individuals to perform the requirements.

What Is Examined

Examination includes reviewing, inspecting, observing, studying, or analyzing assessment objects. The objects can be documents, mechanisms, or activities. The primary focus will be to examine through demonstrations during interviews.

For some requirements, the assessor reviews documentation to determine if assessment objectives are met. Interviews with OSC staff may identify the documents uses. Documents need to be in their final forms; working papers (e.g., drafts) of documentation are not eligible to be submitted as evidence because they are not yet official and are still subject to change. Common types of documents that can be used as evidence include:

- policy, process, and procedure documents;
- training materials;
- plans and planning documents; and
- system-level, network, and data flow diagrams.

This list of documents is not exhaustive or prescriptive. An OSC may not have these specific documents, and other documents may be used to provide evidence of compliance.

In other cases, the requirement is best assessed by observing that safeguards are in place by viewing hardware or associated configuration information or observe staff exercising a process.

What Is Tested

Testing is an important part of the assessment process. Interviews tell the assessor what the OSC staff believe to be true, documentation provides evidence of intent, and testing demonstrates what has or has not been done and is the preferred assessment method when posible. For example, staff may talk about how users are identified and documentation may provide details on how users are identified, but seeing a demonstration of user identification provides evidence that the requirement is met. The assessor will determine which requirements or objectives within a requirement need demonstration or testing. Most objectives will require testing.

Assessment Findings

The assessment of a CMMC requirement results in one of three possible findings: MET, NOT MET, or NOT APPLICABLE as defined in 32 C.F.R. § 170.24. To achieve Level 3 Certification as described in 32 C.F.R. § 170.18, the OSC will need a finding of MET or NOT APPLICABLE on all CMMC Level 3 requirements.

- **MET:** All applicable objectives for the security requirement are satisfied based on evidence. All evidence must be in final form and not draft. Unacceptable forms of evidence include working papers, drafts, and unofficial or unapproved policies..
- **NOT MET:** One or more applicable objectives for the security requirement is not satisfied During an assessment, for each requirement objective marked NOT MET, the assessor will document why the evidence provided by the OSC does not conform
- **NOT APPLICABLE (N/A):** A security requirement and/or objective does not apply at the time of the CMMC assessment.. For example, SI.L3-3.14.3e might be N/A if there are no Internet of Things (IoT), Industrial Internet of Things (IIoT), Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, or test equipment included in the Level 3 CMMC Assessment Scope.

An OSC can inherit requirement objectives and compliance from other parts of the enterprise or service providers. A requirement objective that is inherited is MET if adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP) as defined in 32 C.F.R. § 170.4, performs the requirement objective. An ESP may be external people, technology, or facilities that the OSC uses, including cloud service providers, managed service providers, managed security service providers, and cybersecurity-as-a-service providers.

Evidence from the enterprise or entity from which the objectives are inherited should show they are applicable to in-scope assets as described in 32 C.F.R. § 170.19 and that the

assessment objectives are met. The assessor will review the evidence and determine if additional testing i s required. For each requirement objective that is inherited, the assessor includes statements that indicate how they were evaluated and from where they are inherited. If the OSC cannot demonstrate adequate evidence for all assessment objectives, through either OSC evidence or evidence of inheritance, the OSC will receive a NOT MET for the requirement.

Requirement Descriptions

This section provides detailed information for assessing each CMMC requirement beyond what is provided in the *CMMC Model Overview* document. The section is organized by domain (DD) then requirement (REQ). Each requirement description contains the following elements as described in 32 C.F.R. § 170.14 (c) (4):

- **Requirement Number, Name, and Statement:** Headed by the requirement identification number in the format DD.L#-REQ (e.g., AC.L3-3.1.2e); followed by the requirement short name identifier, which is meant to be used for quick reference only; and finally followed by the complete CMMC requirement statement. In the case where the original NIST SP 800-172 requirement requires an assignment and/or selection statement, the CMMC Level 3 assignment (and any necessary selection) text is emphasized using underlining. See Section 2.2 in NIST SP 800-172 for the discussion on assignments and selections.
- **Assessment Objectives [NIST SP 800-172A]:** Identifies the specific list of objectives that must be met to receive MET for the requirement as defined in NIST SP 800-172A and includes the CMMC Level 3 assignment/selection text (as appropriate). In cases where a CMMC Level 3 assignment fully satisfies the definition(s) required in an organization-defined parameter (ODP) in NIST SP 800-172A, the ODP statement is not included as an objective, since that objective has been met by the assignment itself. However, when the assignment does not fully contain all required aspects of a NIST SP 800-172A ODP, the ODP is included as its own objective, using the original NIST SP 800-172A ODP number (e.g., "[ODP4]"). See the breakout box *ORGANIZATION-DEFINED PARAMETERS* in Section 2.1 of NIST SP 800-172A for additional details on an ODP. In all cases where an assignment is used within an objective, it it also emphasized using underlining.
- **Potential Assessment Methods and Objects [NIST SP 800-172A]:** Defines the nature and extent of the assessor's actions. Potential assessment methods and objects are as defined in NIST SP 800-172A. The methods include *examine*, *interview*, and *test*. Assessment objects identify the items being assessed and can include specifications, mechanisms, activities, and individuals.
- **Discussion [NIST SP 800-172]:** Contains discussion from the associated NIST SP 800-172 security requirement.
- **Further Discussion:**
    - Expands upon the NIST content to provide supplemental information on the requirement intent.
    - Contains examples illustrating how the OSC might apply the requirement. These examples provide insight but are not intended to be prescriptive of how the requirement must be implemented, nor comprehensive of all assessment objectives necessary to achieve the requirement. The assessment objectives met within the example are referenced by letter in brackets (e.g., [a,d] for objectives "a" and "d")

within the text. Note that some of the examples contain company names; all company names used in this document are fictitious.

- Provides potential assessment considerations. These may include common considerations for assessing the requirement and potential questions the assessor may ask when assessing the objectives.

- **Key References:** Lists the security requirement from NIST SP 800-172. The *CMMC Model Overview* provides additional references.

Access Control (AC)

AC.L3-3.1.2E – ORGANIZATIONALLY CONTROLLED ASSETS

Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Information resources that are owned, provisioned, or issued by the organization are identified and

[b] Access to systems and system components is restricted to only those information resources that are owned, provisioned, or issued by the organization.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Access control policy; procedures addressing the use of external systems; list of information resources owned, provisioned, or issued by the organization; security plan; system design documentation; system configuration settings and associated documentation; system connection or processing agreements; system audit records; account management documents; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for restricting or prohibiting the use of non-organizationally owned systems, system components, or devices; system and network administrators; organizational personnel responsible for system security].

Test

[SELECT FROM: Mechanisms implementing restrictions on the use of non-organizationally owned systems, components, or devices].

DISCUSSION [NIST SP 800-172]

Information resources that are not owned, provisioned, or issued by the organization include systems or system components owned by other organizations and personally owned devices. Non-organizational information resources present significant risks to the organization and complicate the ability to employ a “comply-to-connect” policy or implement component or device attestation techniques to ensure the integrity of the organizational system.

FURTHER DISCUSSION

Implementing this requirement ensures that an organization has control over the systems that can connect to organizational assets. This control will allow more effective and efficient application of security policy.

Example

You are the chief network architect for your company. Company policy states that all company-owned assets must be separated from all non-company-owned (i.e., guest or employee) assets. You decide the best way forward is to modify the corporate wired and wireless networks to only allow company-owned devices to connect [b]. All other devices are connected to a second (untrusted) network that non-corporate devices may use to access the internet. The two environments are physically separated and are not allowed to be connected. You also decide to limit the virtual private network (VPN) services of the company to devices owned by the corporation by installing certificate keys and have the VPN validate the configuration of connecting devices before they are allowed in [b].

Potential Assessment Considerations

- Can the organization demonstrate a non-company-owned device failing to access information resources owned by the company [b]?
- How is this requirement met for organizational devices that are specialized assets (GFE, restricted information systems) [a,b]?
- Does the company allow employees to charge personal cell phones on organizational systems [b]?

KEY REFERENCES

- NIST SP 800-172 3.1.2e

AC.L3-3.1.3E – SECURED INFORMATION TRANSFER

Employ secure information transfer solutions to control information flows between security domains on connected systems.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[ODP1] Secure information transfer solutions are defined;

[a] Information flows between security domains on connected systems are identified and

[b] Secure information transfer solutions are employed to control information flows between security domains on connected systems.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; security plan; system configuration settings and associated documentation; system audit records; system baseline configuration; list of information flow authorizations; other relevant documents or records].

Interview

[SELECT FROM: System and network administrators; organizational personnel responsible for information security; system developers].

Test

[SELECT FROM: Mechanisms implementing information flow enforcement policy; mechanisms implementing secure information transfer solutions].

DISCUSSION [NIST SP 800-172]

Organizations employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Transferring information between systems in different security domains with different security policies introduces the risk that the transfers violate one or more domain security policies. In such situations, information owners or information stewards provide guidance at designated policy enforcement points between connected systems. Organizations mandate specific architectural solutions when required to enforce logical or physical separation between systems in different security domains. Enforcement includes prohibiting information transfers between connected systems, employing hardware mechanisms to enforce one-way information flows, verifying write permissions before accepting information from another security domain or connected system, and implementing trustworthy regrading mechanisms to reassign security attributes and labels.

Secure information transfer solutions often include one or more of the following properties: use of cross-domain solutions when traversing security domains, mutual authentication of the sender and recipient (using hardware-based cryptography), encryption of data in transit and at rest, isolation from other domains, and logging of information transfers (e.g., title of file, file size, cryptographic hash of file, sender, recipient, transfer time and Internet Protocol [IP] address, receipt time, and IP address).

FURTHER DISCUSSION

The organization implementing this requirement must decide on the secure information transfer solutions they will use. The solutions must be configured to have strong protection mechanisms for information flow between security domains. Secure information transfer solutions control information flow between a CMMC Level 3 enclave and other CMMC or non-CMMC enclaves. If CUI requiring CMMC Level 3 protection resides in one area of the environment or within a given enclave outside of the normal working environment, protection to prevent unauthorized personnel from accessing, disseminating, and sharing the protected information is required. Physical and virtual methods can be employed to implement secure information transfer solutions.

Example

You are the administrator for an enterprise that stores and processes CUI requiring CMMC Level 3 protection. The files containing CUI information are tagged by the company as CUI. To ensure secure information transfer, you use an intermediary device to check the transfer of any CUI files. The device sits at the boundary of the CUI enclave, is aware of all other CUI domains in the enterprise, and has the ability to examine the metadata in the encrypted payload. The tool checks all outbound communications paths. It first checks the metadata for all data being transferred. If that data is identified as CUI, the device checks the destination to see if the transfer is to another, sufficiently certified CUI domain. If the destination is not a sufficient CUI domain, the tool blocks the communication path and does not allow the transfer to take place. If the destination is a sufficient CUI domain, the transfer is allowed. The intermediary device logs all blocks.

Potential Assessment Considerations

- Has the organization defined the secure information transfer solutions it is using [b]?

- Has the organization defined domains, boundaries, and flows between those domains that need to be controlled [a]?
- Has the organization defined attributes to be associated with the CUI, and both source and destination objects [b]?
- Has the organization defined metadata or some other tagging mechanism to be used as a means of enforcing CUI flow control [b]?
- Has the organization defined filters to be used as a basis for enforcing flow control decisions [b]?
- Has the organization identified CUI flows for which flow control decisions are to be applied and enforced [a,b]?

KEY REFERENCES

- NIST SP 800-172 3.1.3e

Awareness and Training (AT)

AT.L3-3.2.1E – ADVANCED THREAT AWARENESS

Provide awareness training upon initial hire, following a significant cyber event, and at least annually, focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors are identified;

[b] Awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors is provided upon initial hire, following a significant cyber event, and at least annually;

[c] Significant changes to the threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors are identified; and

[d] Awareness training is updated at least annually or when there are significant changes to the threat.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Awareness training policy; procedures addressing awareness training implementation; appropriate codes of federal regulations; awareness training curriculum; awareness training materials; security plan; training records; threat information on social engineering, advanced persistent threat actors, suspicious behaviors, and breaches; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for awareness training; organizational personnel responsible for information security; organizational personnel comprising the general system user community].

Test

[SELECT FROM: Mechanisms managing awareness training; mechanisms managing threat information].

DISCUSSION [NIST SP 800-172]

An effective method to detect APT activities and reduce the effectiveness of those activities is to provide specific awareness training for individuals. A well-trained and security-aware workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy to protect organizations against malicious code injections via email or web applications. Threat awareness training includes educating individuals on the various ways that APTs can infiltrate organizations, including through websites, emails, advertisement pop-ups, articles, and social engineering. Training can include techniques for recognizing suspicious emails, the use of removable systems in non-secure settings, and the potential targeting of individuals by adversaries outside the workplace. Awareness training is assessed and updated periodically to ensure that the training is relevant and effective, particularly with respect to the threat since it is constantly, and often rapidly, evolving.

[NIST SP 800-50] provides guidance on security awareness and training programs.

FURTHER DISCUSSION

All organizations, regardless of size, should have a cyber training program that helps employees understand threats they will face on a daily basis. This training must include knowledge about APT actors, breaches, and suspicious behaviors.

Example

You are the cyber training coordinator for a small business with eight employees. You do not have your own in-house cyber training program. Instead, you use a third-party company to provide cyber training. New hires take the course when they start, and all current staff members receive refresher training at least once a year [b]. When significant changes to the threat landscape take place, the company contacts you and informs you that an update to the training has been completed [c,d] and everyone will need to receive training [b]. You keep a log of all employees who have gone through the cyber training program and the dates of training.

Potential Assessment Considerations

- Does the organization have evidence that employees participate in cyber awareness training at initial hire and at least annually thereafter or when there have been significant changes to the threat [b]?

KEY REFERENCES

- NIST SP 800-172 3.2.1e

AT.L3-3.2.2E – PRACTICAL TRAINING EXERCISES

Include practical exercises in awareness training for all users, tailored by roles, to include general users, users with specialized roles, and privileged users, that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Practical exercises are identified;

[b] Current threat scenarios are identified;

[c] Individuals involved in training and their supervisors are identified;

[d] Practical exercises that are aligned with current threat scenarios are included in awareness training for all users, tailored by roles, to include general users, users with specialized roles, and privileged users; and

[e] Feedback is provided to individuals involved in the training and their supervisors.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Awareness training policy; procedures addressing awareness training implementation; appropriate codes of federal regulations; awareness training curriculum; awareness training materials; security plan; training records; threat information on social engineering, advanced persistent threat actors, suspicious behaviors, breaches, or other relevant adversary tactics, techniques, or procedures; feedback on practical exercises and awareness training; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for awareness training; organizational personnel responsible for information security; organizational personnel with roles identified for practical exercises; supervisors of personnel with roles identified for practical exercises].

Test

[SELECT FROM: Mechanisms managing awareness training; mechanisms managing threat information].

DISCUSSION [NIST SP 800-172]

Awareness training is most effective when it is complemented by practical exercises tailored to the tactics, techniques, and procedures (TTP) of the threat. Examples of practical exercises include unannounced social engineering attempts to gain unauthorized access, collect information, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Rapid feedback is essential to reinforce desired user behavior. Training results, especially failures of personnel in critical roles, can be indicative of a potentially serious problem. It is important that senior management are made aware of such situations so that they can take appropriate remediating actions.

[NIST SP 800-181] provides guidance on role-based security training, including a lexicon and taxonomy that describes cybersecurity work via work roles.

FURTHER DISCUSSION

This requirement can be performed by the organization or by a third-party company. Training exercises (including unannounced exercises, such as phishing training) should be performed at various times throughout the year to encourage employee readiness. After each exercise session has been completed, the results should be recorded (date, time, what and who the training tested, and the percent of successful and unsuccessful responses). The purpose of training is to help employees in all roles act appropriately for any given training situation, which should reflect real-life scenarios. Collected results will help identify shortcomings in the cyber training and/or whether additional instructional training may be needed.

General exercises can be included for all users, but exercises tailored for specific roles are important, too. Training tailored for specific roles helps make sure individuals are ready for actions and events specific to their positions in a company. Privileged users receive training that emphasizes what permissions their privileged account has in a given environment and what extra care is required when using their privileged account.

Example

You are the cyber training coordinator for a medium-sized business. You and a coworker have developed a specialized awareness training to increase cybersecurity awareness around your organization. Your training includes social media campaigns, social engineering phone calls, and phishing emails with disguised links to staff to train them beyond the standard cybersecurity training [a,b].

To send simulated phishing emails to staff, you subscribe to a third-party service that specializes in this area [a]. The service sets up fictitious websites with disguised links to help train general staff against this TTP used by APTs [d]. The third-party company tracks the individuals who were sent phishing emails and whether they click on any of the of the links within the emails. After the training action is completed, you receive a report from the third-party company. The results show that 20% of the staff clicked on one or more phishing email links, demonstrating a significant risk to your company. As the cyber

training coordinator, you notify the individuals, informing them they failed the training and identifying the area(s) of concern [e]. You send an email to the supervisors informing them who in their organization has received training. You also send an email out to the entire company explaining the training that just took place and the overall results [e].

Potential Assessment Considerations

- Are the individuals being trained and the results recorded [e]?
- Are the training exercises performed [c]?
- Are the exercises set up for all users? Are there tailored exercises based on roles within the organization (general users, users with specialized roles, and privileged users) [d]?
- Does the organization have documentation recording the training exercises, who participated, and feedback provided to those who participated in a training session [c,e]?

KEY REFERENCES

- NIST SP 800-172 3.2.2e

Configuration Management (CM)

CM.L3-3.4.1E – AUTHORITATIVE REPOSITORY

Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Approved system components are identified;

[b] Implemented system components are identified;

[c] An authoritative source and repository are established to provide a trusted source and accountability for approved and implemented system components; and

[d] An authoritative source and repository are maintained to provide a trusted source and accountability for approved and implemented system components.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system and system component inventory records; inventory reviews and update records; security plan; system audit records; change control audit and review reports; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for configuration management; organizational personnel responsible for system component inventory; organizational personnel responsible for configuration change control; organizational personnel responsible for information security; system/network administrators; members of a change control board or similar].

Test

[SELECT FROM: Mechanisms that implement configuration change control; mechanisms supporting configuration control of the baseline configuration; mechanisms supporting and/or implementing the system component inventory].

DISCUSSION [NIST SP 800-172]

The establishment and maintenance of an authoritative source and repository includes a system component inventory of approved hardware, software, and firmware; approved system baseline configurations and configuration changes; and verified system software and firmware, as well as images and/or scripts. The authoritative source implements integrity controls to log changes or attempts to change software, configurations, or data in the repository. Additionally, changes to the repository are subject to change management procedures and require authentication of the user requesting the change. In certain situations, organizations may also require dual authorization for such changes. Software changes are routinely checked for integrity and authenticity to ensure that the changes are legitimate when updating the repository and when refreshing a system from the known, trusted source. The information in the repository is used to demonstrate adherence to or identify deviation from the established configuration baselines and to restore system components from a trusted source. From an automated assessment perspective, the system description provided by the authoritative source is referred to as the desired state. The desired state is compared to the actual state to check for compliance or deviations. [NIST SP 800-128] provides guidance on security configuration management, including security configuration settings and configuration change control.

[NIST IR 8011-1] provides guidance on automation support to assess system and system component configurations.

FURTHER DISCUSSION

Trusted software, whether securely developed in house or obtained from a trusted source, should have baseline data integrity established when first created or obtained, such as by using hash algorithms to obtain a hash value that would be used to validate the source prior to use of the software in a given system. Hardware in the repository should be stored in boxes or containers with tamper-evident seals. Hashes and seals should be checked on a regular basis employing the principle of separation of duties.

Example

You are the primary system build technician at a medium-sized company. You have been put in charge of creating, documenting, and implementing a baseline configuration for all user systems [c]. You have identified a minimum set of software that is needed by all employees to complete their work (e.g., office automation software). You acquire trusted versions of the software and build one or more baselines of all system software, firmware, and applications required by the organization. The gold version of each baseline is stored in a secure configuration management system repository and updated as required to maintain integrity and security. Access to the build repository for updates and use is carefully controlled using access control mechanisms that limit access to you and your staff. All interations with the repository are logged. Using an automated build tool, your team builds each organizational system using the standard baseline

Potential Assessment Considerations

- Does an authoritative source and repository exist to provide a trusted source and accountability for approved and implemented system components [c,d]?

KEY REFERENCES

- NIST SP 800-172 3.4.1e

CM.L3-3.4.2E – AUTOMATED DETECTION & REMEDIATION

Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, remove the components or place the components in a quarantine or remediation network to facilitate patching, re-configuration, or other mitigations.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Automated mechanisms to detect misconfigured or unauthorized system components are identified;

[b] Automated mechanisms are employed to detect misconfigured or unauthorized system components;

[c] Misconfigured or unauthorized system components are detected; and

[d] After detection, system components are removed or placed in a quarantine or remediation network to facilitate patching, re-configuration, or other mitigations.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; authoritative source or repository; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system procedures addressing system configuration change control; configuration settings and associated documentation; change control records; change control audit and review reports; agenda/minutes from configuration change control oversight meetings; alerts/notifications of unauthorized baseline configuration changes; security plan; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for configuration management; organizational personnel responsible for information security; organizational personnel responsible for configuration change control; system developers; system/network administrators; members of a change control board or similar roles].

Test

[SELECT FROM: Automated mechanisms supporting configuration control of the baseline configuration; automated mechanisms that implement security responses to changes to the baseline configurations; automated mechanisms that implement configuration change

control; automated mechanisms that detect misconfigured or unauthorized system components].

DISCUSSION [NIST SP 800-172]

System components used to process, store, transmit, or protect CUI are monitored and checked against the authoritative source (i.e., hardware and software inventory and associated baseline configurations). From an automated assessment perspective, the system description provided by the authoritative source is referred to as the desired state. Using automated tools, the desired state is compared to the actual state to check for compliance or deviations. Security responses to system components that are unknown or that deviate from approved configurations can include removing the components; halting system functions or processing; placing the system components in a quarantine or remediation network that facilitates patching, re-configuration, or other mitigations; or issuing alerts and/or notifications to personnel when there is an unauthorized modification of an organization-defined configuration item. Responses can be automated, manual, or procedural. Components that are removed from the system are rebuilt from the trusted configuration baseline established by the authoritative source.

[NIST IR 8011-1] provides guidance on using automation support to assess system configurations

FURTHER DISCUSSION

For this requirement, the organization is required to implement automated tools to help identify misconfigured components. Once under an attacker's control, the system may be modified in some manner and the automated tool should detect this. Or, if a user performs a manual configuration adjustment, the system will be viewed as misconfigured, and that change should be detected. Another common example is if a component has been offline and not updated, the tool should detect the incorrect configuration. If any of these scenarios occurs, the automated configuration management system (ACMS) will notice a change and can take the system offline, place the system in a quarantined network, or send an alert so the component(s) can be manually removed. Once this is accomplished, a system technician may need to manually inspect the system or rebuild it using the baseline configuration. Another option is for an ACMS to make adjustments while the system is running rather than performing an entire rebuild. These adjustments can include replacing configuration files, executable files, scripts, or library files on the fly.

Example 1

As the system administrator, you implement company policy stating that every system connecting to the company network via VPN will be checked for specific configuration settings and software versioning before it is allowed to connect to the network, after it passes authentication [a,b]. If any deviations from the authoritative baseline are identified, the system is placed in a VPN quarantine zone (remediation network) using a virtual local area network (VLAN) [b,c,d]. This VLAN is set up for system analysis, configuration changes, and rebuilding after forensic information is pulled from the system. Once the

system updates are complete, the system will be removed from the quarantine zone and placed on the network through the VPN connection.

Example 2

As the system administrator, you have chosen to use a network access control (NAC) solution to validate system configurations before they are allowed to connect to the corporate network [a]. When a system plugs into or connects to a local network port or the VPN, the NAC solution checks the hash of installed system software [b,c]. If the system does not pass the configuration check, it is put in quarantine until an administrator can examine it or the ACMS updates the system to pass the system checks [d].

Potential Assessment Considerations

- Can the organization explain the automated process that identifies, quarantines, and remediates a system when a misconfiguration or unauthorized system component is identified [a,b,c,d]?
- Does the organization have a patching and rebuild process for all assets that may be taken offline [d]?

KEY REFERENCES

- NIST SP 800-172 3.4.2e

CM.L3-3.4.3E – AUTOMATED INVENTORY

Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Automated discovery and management tools for the inventory of system components are identified;

[b] An up-to-date, complete, accurate, and readily available inventory of system components exists; and

[c] Automated discovery and management tools are employed to maintain an up-to-date, complete, accurate, and readily available inventory of system components.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Configuration management policy; configuration management plan; procedures addressing system component inventory; procedures addressing the baseline configuration of the system; configuration management plan; system design documentation; system architecture and configuration documentation; security plan; system configuration settings and associated documentation; configuration change control records; system inventory records; change control records; system maintenance records; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for information security; organizational personnel responsible for configuration management; organizational personnel responsible for managing the automated mechanisms implementing the system component inventory; system developers; system/network administrators].

Test

[SELECT FROM: Automated mechanisms implementing baseline configuration maintenance; automated mechanisms implementing the system component inventory].

DISCUSSION [NIST SP 800-172]

The system component inventory includes system-specific information required for component accountability and to provide support to identify, control, monitor, and verify configuration items in accordance with the authoritative source. The information necessary for effective accountability of system components includes the system name, hardware and

software component owners, hardware inventory specifications, software license information, software version numbers, and— for networked components—the machine names and network addresses. Inventory specifications include the manufacturer, supplier information, component type, date of receipt, cost, model, serial number, and physical location. Organizations also use automated mechanisms to implement and maintain authoritative (i.e., up-to-date, complete, accurate, and available) baseline configurations for systems that include hardware and software inventory tools, configuration management tools, and network management tools. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels.

FURTHER DISCUSSION

Organizations use an automated capability to discover components connected to the network and system software installed. The automated capability must also be able to identify attributes associated with those components. For systems that have already been coupled to the environment, they should allow remote access for inspection of the system software configuration and components. Another option is to place an agent on systems that performs internal system checks to identify system software configuration and components. Collection of switch and router data can also be used to identify systems on networks.

Example

Within your organization, you are in charge of implementing an authoritative inventory of system components. You first create a list of the automated technologies you will use and what each technology will be responsible for identifying [a]. This includes gathering information from switches, routers, access points, primary domain controllers, and all connected systems or devices, whether wired or wireless (printers, IoT, IIoT, OT, IT, etc.) [b]. To keep the data up-to-date, you set a very short search frequency for identifying new components. To maximize availability of this data, all information will be placed in a central inventory/configuration management system, and automated reporting is performed every day [c]. A user dashboard is set up that allows you and other administrators to run reports at any time.

Potential Assessment Considerations

- Can the organization explain the process by which current inventory information is acquired [a]?
- Is the organization able to produce an inventory of components on the network [b,c]?
- Has the organization implemented a valid frequency for the component discovery solution [b,c]?
- Can the organization demonstrate that the inventory is current and accurate [b]?
- Has the organization developed a defined list of identifiable attributes for each component type, and is that list adequate to support component accountability [a]?

- Is the organization able to track, monitor, and verify configuration items in accordance with the organization's authoritative list of components [b,c]?

KEY REFERENCES

- NIST SP 800-172 3.4.3e

Identification and Authentication (IA)

IA.L3-3.5.1E – BIDIRECTIONAL AUTHENTICATION

Identify and authenticate systems and system components, where possible, before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[ODP1] Systems and system components to identify and authenticate are defined;

[a] Bidirectional authentication that is cryptographically-based is implemented;

[b] Bidirectional authentication that is replay-resistant is implemented; and

[c] Systems and system components, where possible, are identified and authenticated before establishing a network connection using bidirectional authentication that is cryptographically-based and replay-resistant.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Identification and authentication policy; procedures addressing device identification and authentication; network connection policy; security plan; system configuration settings and associated documentation; system design documentation; list of devices requiring unique identification and authentication; device connection reports; system audit records; list of privileged system accounts; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for system operations; organizational personnel responsible for account management; organizational personnel responsible for device identification and authentication; organizational personnel responsible for information security; system/network administrators; system developers].

Test

[SELECT FROM: Cryptographically-based bidirectional authentication mechanisms; mechanisms supporting and/or implementing network connection policy; mechanisms supporting and/or implementing replay-resistant authentication mechanisms; mechanisms supporting and/or implementing an identification and authentication capability; mechanisms supporting and/or implementing a device identification and authentication capability].

968 ## DISCUSSION [NIST SP 800-172]

969 Cryptographically-based and replay-resistant authentication between systems,
970 components, and devices addresses the risk of unauthorized access from spoofing (i.e.,
971 claiming a false identity). The requirement applies to client-server authentication, server-
972 server authentication, and device authentication (including mobile devices). The
973 cryptographic key for authentication transactions is stored in suitably secure storage
974 available to the authenticator application (e.g., keychain storage, Trusted Platform Module
975 [TPM], Trusted Execution Environment [TEE], or secure element). Mandating
976 authentication requirements at every connection point may not be practical, and therefore,
977 such requirements may only be applied periodically or at the initial point of network
978 connection.

979 [NIST SP 800-63-3] provides guidance on identity and authenticator management.

980 ## FURTHER DISCUSSION

981 The intent of this practice is to prevent unauthorized devices from connecting to one
982 another. One example satisfying this requirement is a web server configured with transport
983 layer security (TLS) using mutual authentication. At a lower level in the OSI stack, IPsec
984 provides application-transparent mutual authentication. Another example would be
985 implementing 802.1X technology to enforce port-based NAC. This is done by enabling
986 802.1X on switches, wireless access points, and VPN connections for a given network.
987 802.1X defines authentication controls for devices trying to access a given network. NAC
988 controls authorization and policy management. For this to be implemented, bidirectional
989 authentication must be turned on via 802.1X. Once successfully authenticated, the device
990 may communicate on the network. A final example, at the application-server level, involves
991 the use of Kerberos to control 1) which files a client can access and 2) the transmission of
992 sensitive data from the client to the server.

993 ### Example 1

994 You are the network engineer in charge of implementing this requirement. You have been
995 instructed to implement a technology that will provide mutual authentication for client
996 server connections. You implement Kerberos.

997 On the server side, client authentication is implemented by having the client establish a
998 local security context. This is initially accomplished by having the client present credentials
999 which are confirmed by the Active Directory Domain Controller (DC). After that, the client
1000 may established context via a session of a logged-in user. The service does not accept
1001 connections from any unauthenticated client.

1002 On the client side, server authentication requires registration, using administrator
1003 privileges, of unique Service Provider Names (SPNs) for each service instance offered. The
1004 names are registered in the Active Directory Domain Controller. When a client requests a
1005 connection to a service, it composes an SPN for a service instance, using known data or
1006 data provided by the user. For authentication, the client presents its SPN to the Key
1007 Distribution Center (KDC), and the KDC searchs for computers with the registered SPN

before allowing a connection via an encrypted message passed to the client for forwarding to the server.

Example 2

You are the network engineer in charge of implementing this requirement. You have been instructed to implement a technology that will provide authentication for each system prior to connecting to the environment. You implement the company-approved scheme that uses cryptographic keys installed on each system for it to authenticate to the environment, as well as user-based cryptographic keys that are used in combination with a user's password for user-level authentication [a,c]. Your authentication implementation is finalized on each system using an ACM solution. When a system connects to the network, the system uses the system-level certificate to authenticate itself to the switch before the switch will allow it to access the corporate network [a,c]. This is accomplished using 802.1x technology on the switch and by authenticating with a RADIUS server that authenticates itself with the system via cryptographic keys. If either system fails to authenticate to the other, the trust is broken, and the system will not be able to connect to or communicate on the network. You also set up a similar implementation in your wireless access point.

Example 3

You are the network engineer in charge of implementing the VPN solution used by the organization. To meet this requirement, you use a VPN gateway server and public key infrastructure (PKI) certificates via a certification authority (CA) and a chain of trust. When a client starts a VPN connection, the server presents its certificate to the client and if the certificate is trusted, the client then presents its certificate to the server [a]. If the server validates the client certificate, an established communications channel is opened for the client to finish the authentication process and gain access to the network via the VPN gateway server [c]. If the client fails final authentication, fails the certification validation, or the VPN gateway fails the certificate check by the client, the communication channel will be denied.

Potential Assessment Considerations

- Are cryptographic keys stored securely [a]?
- Has the requirement been implemented for any of the three use cases, where applicable: client-server authentication, server-server authentication, and device authentication [b,c]?

KEY REFERENCES

- NIST SP 800-172 3.5.1e

IA.L3-3.5.3E – BLOCK UNTRUSTED ASSETS

Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] System components that are known, authenticated, in a properly configured state, or in a trust profile are identified;

[b] Automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems are identified; and

[c] Automated or manual/procedural mechanisms are employed to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Configuration management policy; identification and authentication policy; system and information integrity policy; procedures addressing system component inventory; procedures addressing device identification and authentication; procedures addressing device configuration management; procedures addressing system monitoring tools and techniques; configuration management plan; security plan; system design documentation; system configuration settings and associated documentation; system inventory records; configuration management records; system monitoring records; alerts/notifications of unauthorized components within the system; change control records; system audit records; system monitoring tools and techniques documentation; documented authorization/approval of network services; notifications or alerts of unauthorized network services; system monitoring logs or records; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for managing the mechanisms implementing unauthorized system component detection; organizational personnel responsible for device identification and authentication; organizational personnel responsible for information security; organizational personnel responsible for installing, configuring, and/or maintaining the system; system/network administrators; organizational personnel responsible for monitoring the system; system developers].

1076 ### Test

1077 [SELECT FROM: Mechanisms implementing the detection of unauthorized system
1078 components; mechanisms supporting and/or implementing a device identification and
1079 authentication capability; mechanisms for providing alerts; mechanisms supporting and/or
1080 implementing configuration management; cryptographic mechanisms supporting device
1081 attestation; mechanisms supporting and/or implementing a system monitoring capability;
1082 mechanisms for auditing network services].

1083 ## DISCUSSION [NIST SP 800-172]

1084 Identification and authentication of system components and component configurations can
1085 be determined, for example, via a cryptographic hash of the component. This is also known
1086 as device attestation and known operating state or trust profile. A trust profile based on
1087 factors such as the user, authentication method, device type, and physical location is used
1088 to make dynamic decisions on authorizations to data of varying types. If device attestation
1089 is the means of identification and authentication, then it is important that patches and
1090 updates to the device are handled via a configuration management process such that the
1091 patches and updates are done securely and do not disrupt the identification and
1092 authentication of other devices.

1093 [NIST IR 8011-1] provides guidance on using automation support to assess system
1094 configurations.

1095 ## FURTHER DISCUSSION

1096 This requirement can be achieved in several ways, such as blocking based on posture
1097 assessments, conditional access, or trust profiles. A posture assessment can be used to
1098 assess a given system's posture to validate that it meets the standards set by the organization
1099 before allowing it to connect. Conditional access is the set of policies and configurations that
1100 control devices receiving access to services and data sources. Conditional access helps an
1101 organization build rules that manage security controls, perform blocking, and restrict
1102 components. A trust profile is a set of factors that are checked to inform a device that a
1103 system can be trusted.

1104 ### Example 1

1105 In a Windows environment, you authorize devices to connect to systems by defining
1106 configuration rules in one or more Group Policy Objects (GPO) that can be automatically
1107 applied to all relevant devices in a domain [a]. This provides you with a mechanism to
1108 apply rules for which devices are authorized to connect to any given system and prevent
1109 devices that are not within the defined list from connecting [b,c]. For instance, universal
1110 serial bus (USB) device rules for authorization can be defined by using a USB device's serial
1111 number, model number, and manufacturer information. This information can be used to
1112 build a trust profile for a device and authorize it for use by a given system. You use security
1113 policies to prevent unauthorized components from connecting to systems [c].

Example 2

You have been assigned to build trust profiles for all devices allowed to connect to your organization's systems. You want to test the capability starting with printers. You talk to your purchasing department, and they tell you that policy states every printer must be from a specific manufacturer; they only purchase four different models. They also collect all serial numbers from purchased printers. You gather this information and build trust profiles for each device [a,b]. Because your organization shares printers, you push the trust profiles out to organizational systems. Now, the systems are not allowed to connect to a network printer unless they are within the trust profiles you have provided [b,c].

Example 3

Your organization has implemented a network access control solution (NAC) to help ensure that only properly configured computers are allowed to connect to the corporate network [a,b]. The solution first checks for the presence of a certificate to indicate that the device is company-owned. It next reviews the patch state of the computer and forces the installation of any patches that are required by the organization. Finally, it reviews the computer's configuration to ensure that the firewall is active and that the appropriate security policies have been applied. Once the computer has passed all of these requirements, it is allowed access to network resources and defined as a trusted asset for the length of its session [a]. Devices that do not meet all of the requirements are automatically blocked from connecting to the network [c].

Potential Assessment Considerations

- If the organization is using a manual method, is the method outlined in detail so any user will be able to follow it without making an error [b,c]?
- If the organization is using an automated method, can the organization explain how the technology performs the task? Can they explain the steps needed to implement [a,b,c]?
- Can the organization provide evidence showing they have trust profiles for specific devices [a,b,c]?
- Can the organization explain how their system components authenticate to a system if they are not using trust profiles [b,c]?

KEY REFERENCES

- NIST SP 800-172 3.5.3e

Incident Response (IR)

IR.L3-3.6.1E – SECURITY OPERATIONS CENTER

Establish and maintain a security operations center capability that operates 24/7, with allowance for remote/on-call staff.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] A security operations center capability is established;

[b] The security operations center capability operates 24/7, with allowance for remote/on-call staff; and

[c] The security operations center capability is maintained.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident handling; procedures addressing the security operations center operations; mechanisms supporting dynamic response capabilities; incident response plan; contingency plan; security plan; other relevant documents or records].-

Interview

[SELECT FROM: Organizational personnel responsible for incident handling; organizational personnel responsible for contingency planning; security operations center personnel; organizational personnel responsible for information security].

Test

[SELECT FROM: Mechanisms that support and/or implement the security operations center capability; mechanisms that support and/or implement the incident handling process].

DISCUSSION [NIST SP 800-172]

A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The SOC is staffed with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers); in some instances operates 24 hours per day, seven days per week; and implements technical,

management, and operational controls (e.g., monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to security-relevant event data from multiple sources. Sources of event data include perimeter defenses, network devices (e.g., gateways, routers, and switches), and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. An SOC capability can be obtained in many ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such a capability.

[NIST SP 800-61] provides guidance on incident handling. [NIST SP 800-86] and [NIST SP 800-101] provide guidance on integrating forensic techniques into incident response. [NIST SP 800-150] provides guidance on cyber threat information sharing. [NIST SP 800-184] provides guidance on cybersecurity event recovery.

FURTHER DISCUSSION

Security operations centers are created to monitor and respond to suspicious activities across an organization's IT applications and infrastructure. A SOC may be implemented in a variety of physical, virtual, and geographic constructs. The organization may also opt to not hire their own staff but to engage a third-party external service provider to serve as their SOC.

The SOC is typically comprised of multiple levels of cybersecurity analysts. Each tier of cybersecurity analysts works on increasingly complex aspects of Incident Response. The SOC may also have dedicated cybersecurity engineers to support configuration and management of defensive cyber tools. The SOC may work with staff in IT operations who provide support to the SOC.

SOC capabilities run 24/7, and while staff may not always be performing tasks for the SOC, the capability alerts staff members and directs them to go to a facility or perform SOC actions from a remote location. Staff members should be scheduled or on call to ensure they are available when needed.

Example

You are the Chief Information Security Officer (CISO) of a medium-sized organization. To meet the goal of 24/7 SOC operation, you have decided to adjust the current SOC, which operates five days a week for 12 hours a day, by minimizing active staff members and hiring trusted expert consultants to have on call at all times (i.e., seven days a week, 24 hours a day) [a,b]. You design your SOC to be remotely accessible so your experts can access your environment when needed. You also decide to set up a very strong automated capability that is good at identifying questionable activities and alerting the appropriate staff. You create a policy stating that after an alert goes out, two members of the SOC team must remotely connect to the environment within 15 minutes to address the problem. All staff members also have regular working hours during which they perform other SOC activities, such as updating information to help the automated tool perform its functions [c].

1217 ### Potential Assessment Considerations

1218 • How does the organization enable 24/7 SOC capabilities? Does the organization have
1219 people in seats 24/7 or on-call members? If on-call members are used, what are the
1220 trigger and alerting mechanisms that allow for 24/7 coverage [a,b]?

1221 • Does the organization have sufficient trained full-time equivalent staff to enable 24/7
1222 SOC services [a,b]?

1223 ## KEY REFERENCES

1224 • NIST SP 800-172 3.6.1e

1225

IR.L3-3.6.2E – CYBER INCIDENT RESPONSE TEAM

Establish and maintain a cyber incident response team that can be deployed by the organization within 24 hours.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] A cyber incident response team is established;

[b] The cyber incident response team can be deployed by the organization within 24 hours; and

[c] The cyber incident response team is maintained.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Incident response policy; procedures addressing incident response; incident response plan; security plan; other relevant documents or records].-

Interview

[SELECT FROM: Organizational personnel responsible for incident response; organizational personnel from the incident response team; organizational personnel responsible for information security].

Test

[SELECT FROM: Mechanisms supporting and/or implementing incident response].

DISCUSSION [NIST SP 800-172]

A cyber incident response team (CIRT) is a team of experts that assesses, documents, and responds to cyber incidents so that organizational systems can recover quickly and implement the necessary controls to avoid future incidents. CIRT personnel include, for example, forensic analysts, malicious code analysts, systems security engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. The team members may or may not be full-time but need to be available to respond in the time period required. The size and specialties of the team are based on known and anticipated threats. The team is typically pre-equipped with the software and hardware (e.g., forensic tools) necessary for rapid identification, quarantine, mitigation, and recovery and is familiar with how to preserve evidence and maintain chain of custody for law enforcement or counterintelligence uses. For some organizations, the CIRT can be implemented as a cross organizational entity or as part of the Security Operations Center (SOC).

[NIST SP 800-61] provides guidance on incident handling. [NIST SP 800-86] and [NIST SP 800-101] provide guidance on integrating forensic techniques into incident response. [NIST SP 800-150] provides guidance on cyber threat information sharing. [NIST SP 800-184] provides guidance on cybersecurity event recovery.

FURTHER DISCUSSION

The CIRT's primary function is to handle information security incident management and response for the environments the SOC oversees. The primary goals of the CIRT are triage and initial response to an incident. They also communicate with all the proper people to ensure understanding of an incident and the response actions, including collection of forensic evidence, have been conveyed.

If and when an incident is detected by the organization's SOC, the IR team is responsible for handling the incident and communicating what has happened to the appropriate people within the organization, as well to the authorities (as needed).

The deployment of a team does not necessarily mean they are "physically deployed." Deployment may simply mean connecting to a remote system in a manner that is equivalent to being on the system's keyboard. Remote access can provide just as much capability as local access in many cases.

Some situations require physical access. For instance, if the company has a physically isolated environment located at a remote location, a team must be physically present at the remote facility to perform the duties required.

Example

You are the lead for an IR team within your organization. Your manager is the SOC lead, and she reports to the chief information officer (CIO). As the SOC is alerted and/or identifies incidents within the organization's environments, you lead and deploy teams to resolve the issues, including incidents involving cloud-based systems. You use a custom dashboard that was created for your team members to view and manage incidents, perform response actions, and record actions and notes for each case. You also have your team create an after action report for all incidents to which they respond; this information is used to determine if a given incident requires additional action and reporting [a].

One day, you receive a message from the SOC that your website has become corrupted. Within minutes, you have a team on the system inspecting logs, analyzing applications, preserving key information, and looking for evidence of tampering/attack [b]. Your team runs through a procedure set for this specific incident type based on a handbook the organization has created and maintains [c]. It is found that a cyberattack caused the corruption, but the corruption caused a crash, which prevented the attack from continuing. Your team takes note of all actions they perform, and at the end of the incident analysis, you send a message to the website lead to inform them of the issue, case number, and notes created by the team. The website lead has their team rebuild the system and validate that the attack no longer works. At the end of the incident, the CISO and CIO are informed of the issue.

1299 ### Potential Assessment Considerations

1300 • Does the organization have a response capability that has remote access to the
1301 organization's systems and system components within 24 hours in place of physical
1302 access [a,b]?

1303 ## KEY REFERENCES

1304 • NIST SP 800-172 3.6.2e

Personnel Security (PS)

PS.L3-3.9.2E – ADVERSE INFORMATION

Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Individuals with access to CUI are identified;

[b] Adverse information about individuals with access to CUI is defined;

[c] Organizational systems to which individuals have access are identified; and

[d] Mechanisms are in place to protect organizational systems if adverse information develops or is obtained about individuals with access to CUI.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Personnel security policy; system and services acquisition policy; procedures addressing personnel screening; records of screened personnel; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; security plan; list of individuals who have been identified as posing an increased level of risk; list of appropriate access authorizations required for system personnel; personnel screening criteria and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for personnel security; organizational personnel responsible for information security; organizational personnel responsible for system and services acquisition; organizational personnel responsible for personnel screening].

Test

[SELECT FROM: Organizational processes for personnel screening; mechanisms supporting personnel screening].

DISCUSSION [NIST SP 800-172]

If adverse information develops or is obtained about an individual with access to CUI which calls into question whether the individual should have continued access to systems containing CUI, actions are taken (e.g., preclude or limit further access by the individual, audit actions taken by the individual) to protect the CUI while the adverse information is resolved.

FURTHER DISCUSSION

According to Defense Counterintelligence and Security Agency, or DCSA (Industrial Security Letter ISL 2011-04, revised July 15, 2020), adverse information consists of any information that negatively reflects the integrity or character of an individual. This pertains to an individual's ability to safeguard sensitive information, such as CUI. Adverse information may simply be a report showing someone has sent sensitive information outside the organization or used unapproved software, against company policy. An organization may receive adverse information about an individual through police reports, reported violations of company policies (including social media posts that directly violate company policies), and revocation or suspension of DoD clearance.

When adverse information is identified about a given individual, the organization should take action to validate that information resources accessible by the individual have been identified and appropriate protection mechanisms are in place to safeguard information and system configurations. Based on organizational policy, an individual's access to resources may be more closely monitored or restricted until further review. Logs should be examined to identify any attempt to perform unauthorized actions.

Example

You learn that one of your employees has been convicted on shoplifting charges. Based on organizational policy, you report this information to human resources (HR), which verifies the information with a criminal background check [a,b,c]. Per policy, you increase the monitoring of the employee's access to ensure that the employee does not exhibit patterns of behavior consistent with an insider threat [d]. You maintain contact with HR as they investigate the adverse information so that you can take stronger actions if required, such as removing access to organizational systems.

Potential Assessment Considerations

- Does the organization define the protection mechanisms for organizational systems if adverse information develops or is obtained about an individual with access to CUI [d]?

KEY REFERENCES

- NIST SP 800-172 3.9.2e

Risk Assessment (RA)

RA.L3-3.11.1E – THREAT-INFORMED RISK ASSESSMENT

Employ threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources, as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[ODP1] Sources of threat intelligence are defined;

[a] A risk assessment methodology is identified;

[b] Threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources, are employed as part of a risk assessment to guide and inform the development of organizational systems and security architectures;

[c] Threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources, are employed as part of a risk assessment to guide and inform the selection of security solutions;

[d] Threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources, are employed as part of a risk assessment to guide and inform system monitoring activities;

[e] Threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources, are employed as part of a risk assessment to guide and inform threat hunting activities; and

[f] Threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources, are employed as part of a risk assessment to guide and inform response and recovery activities.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Information security program plan; risk assessment policy; threat awareness program documentation; procedures for the threat awareness program; security planning policy and procedures; procedures addressing organizational assessments of risk; threat hunting program documentation; procedures for the threat hunting program; risk assessment results relevant to threat awareness; threat hunting results; list or other documentation on the cross-organization, information-sharing capability; security plan; risk assessment; risk assessment results; risk assessment

reviews; risk assessment updates; contingency planning policy; contingency plan; incident response policy; incident response plan; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for information security program planning and plan implementation; organizational personnel responsible for the threat awareness and threat hunting programs; organizational personnel responsible for risk assessments; organizational personnel responsible for the cross-organization, information-sharing capability; organizational personnel responsible for information security; organizational personnel responsible for contingency planning; organizational personnel responsible for incident response; personnel with whom threat awareness information is shared by the organization].

Test

[SELECT FROM: Mechanisms supporting and/or implementing the threat awareness program; mechanisms supporting and/or implementing the cross-organization, information-sharing capability; mechanisms supporting and/or implementing the threat hunting program; mechanisms for conducting, documenting, reviewing, disseminating, and updating risk assessments; mechanisms supporting and/or implementing contingency plans; mechanisms supporting and/or implementing incident response plans].

DISCUSSION [NIST SP 800-172]

The constant evolution and increased sophistication of adversaries, especially the APT, makes it more likely that adversaries can successfully compromise or breach organizational systems. Accordingly, threat intelligence can be integrated into each step of the risk management process throughout the system development life cycle. This risk management process includes defining system security requirements, developing system and security architectures, selecting security solutions, monitoring (including threat hunting), and remediation efforts.

[NIST SP 800-30] provides guidance on risk assessments. [NIST SP 800-39] provides guidance on the risk management process. [NIST SP 800-160-1] provides guidance on security architectures and systems security engineering. [NIST SP 800-150] provides guidance on cyber threat information sharing.

FURTHER DISCUSSION

An organization consumes threat intelligence and improves their security posture based on the intelligence relevant to that organization and/or a system(s). The organization can obtain threat intelligence from open or commercial sources but must also use any DoD-provided sources. Threat information can be received in high volumes from various providers and must be processed and analyzed by the organization. It is the responsibility of the organization to process the threat information in a manner that is useful and actionable to their needs. Processing, analyzing, and extracting the intelligence from the threat feeds and applying it to all organizational security engineering needs is the primary

benefit of this requirement. Note that more than one source is required to meet assessment objectives.

Example

Your organization receives a commercial threat intelligence feed from FIRST and government threat intelligence feeds from both USCERT and DoD/DC3 to help learn about recent threats and any additional information the threat feeds provide [b,c,d,e,f]. Your organization uses the threat intelligence for multiple purposes:

- To perform up-to-date risk assessments for the organization [a];
- To add rules to the automated system put in place to identify threats (indicators of compromise, or IOCs) on the organization's network [e];
- To guide the organization in making informed selections of security solutions [c];
- To shape the way the organization performs system monitoring activities [d];
- To manage the escalation process for identified incidents, handling specific events, and performing recovery actions [f];
- To provide additional information to the hunt team to identify threat activities [e];
- To inform the development and design decisions for organizational systems and the overall security architecture, as well as the network architecture [b,c];
- To assist in decision-making regarding systems that are part of the primary network and systems that are placed in special enclaves for additional protections [b]; and
- To determine additional security measures based on current threat activities taking place in similar industry networks [c,d,e,f].

Potential Assessment Considerations

- Does the organization detail how threat feed information is to be ingested, analyzed, and used [a]?
- Can the organization's SOC or hunt teams discuss how they use the threat feed information after it is processed [e,f]?

KEY REFERENCES

- NIST SP 800-172 3.11.1e

RA.L3-3.11.2E – THREAT HUNTING

Conduct cyber threat hunting activities on an on-going aperiodic basis or when indications warrant, to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[ODP4] Organizational systems to search for indicators of compromise are defined;

[a] Indicators of compromise are identified;

[b] Cyber threat hunting activities are conducted on an on-going aperiodic basis or when indications warrant, to search for indicators of compromise in organizational systems; and

[c] Cyber threat hunting activities are conducted on an on-going aperiodic basis or when indications warrant, to detect, track, and disrupt threats that evade existing controls.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: System and information integrity policy; policy and procedures addressing system monitoring; threat hunting program documentation; procedures for the threat hunting program; threat hunting results; system design documentation; security plan; system monitoring tools and techniques documentation; security planning policy and procedures; system configuration settings and associated documentation; system monitoring logs or records; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for threat hunting program; system/network administrators; organizational personnel responsible for information security; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system and/or network].

Test

[SELECT FROM: Mechanisms supporting and/or implementing a threat hunting program; mechanisms supporting and/or implementing a system monitoring capability; mechanisms supporting and/or supporting and/or implementing incident response plans].

1501 ## DISCUSSION [NIST SP 800-172]

1502 Threat hunting is an active means of defense that contrasts with traditional protection
1503 measures, such as firewalls, intrusion detection and prevention systems, quarantining
1504 malicious code in sandboxes, and Security Information and Event Management (SIEM)
1505 technologies and systems. Cyber threat hunting involves proactively searching
1506 organizational systems, networks, and infrastructure for advanced threats. The objective is
1507 to track and disrupt cyber adversaries as early as possible in the attack sequence and to
1508 measurably improve the speed and accuracy of organizational responses. Indicators of
1509 compromise are forensic artifacts from intrusions that are identified on organizational
1510 systems at the host or network level and can include unusual network traffic, unusual file
1511 changes, and the presence of malicious code.

1512 Threat hunting teams use existing threat intelligence and may create new threat
1513 information, which may be shared with peer organizations, Information Sharing and
1514 Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and
1515 relevant government departments and agencies. Threat indicators, signatures, tactics,
1516 techniques, procedures, and other indicators of compromise may be available via
1517 government and non-government cooperatives, including Forum of Incident Response and
1518 Security Teams, United States Computer Emergency Response Team, Defense Industrial
1519 Base Cybersecurity Information Sharing Program, and CERT Coordination Center.

1520 [NIST SP 800-30] provides guidance on threat and risk assessments, risk analyses, and risk
1521 modeling. [NIST SP 800-160-2] provides guidance on systems security engineering and
1522 cyber resiliency. [NIST SP 800-150] provides guidance on cyber threat information sharing.

1523 ## FURTHER DISCUSSION

1524 For this requirement, threat hunting is conducted on an ongoing aperiodic basis. Ongoing
1525 aperiodic refers to activities that happen over and over but without an identifiable
1526 repeating pattern over time. For threat hunting, ongoing activities take place in an
1527 automated manner (e.g., collecting logs, automated analysis, and alerts). Aperiodicity
1528 includes humans performing the hunt activities, which take place on an as-needed or as-
1529 planned basis.

1530 APTs can penetrate an environment by means that defeat or avoid conventional monitoring
1531 methods and alert triggers—for example, by using zero-day attacks. Zero-day attacks
1532 become known only after the attack has happened and alerts are sent via threat
1533 intelligence feeds based on expert analysis. Because of the nature of zero-day attacks,
1534 automated alerts do not generally trigger when the event occurs but the activity is captured
1535 in system logs and forwarded for analysis and retention by the SIEM. Threat intelligence
1536 information is typically used by hunt teams to search SIEM systems, system event and
1537 security logs, and other components to identify activity that has already taken place on an
1538 environment. The hunt team will identify systems related to the event(s) and pass the case
1539 to Incident Response team for action on the event(s). The hunt team will also use indicators
1540 to identify smaller components of an attack and search for that activity, which may help
1541 uncover a broader attack on the environment.

Threat hunting can also look for anomalous behavior or activity based on an organization's normal pattern of activity. Understanding the roles and information flows within an organization can help identify activity that might be indicative of adversary behavior before the adversary completes their attack or mission.

Example

You are the lead for your organization's cyber threat hunting team. You have local and remote staff on the team to process threat intelligence. Your team is tied closely with the SOC and IR teams. Through a DoD (DC3) intelligence feed, you receive knowledge of an APT's actions attacking DIB companies related to a program similar to the ones your company performs for the DoD. The intelligence feed provided the indicators of compromise for a zero-day attack that most likely started within the past month. After receiving the IOCs, you use a template for your organization to place the information in a standard format your team understands. You then email the information to your team members and place the information in your hunt team's dashboard, which tracks all IOCs [a].

Your team starts by using the information to hunt for IOCs on the environment [b]. One of your team members quickly responds, providing information from the SIEM that an HR system's logs show evidence that IOCs related to this threat occurred three days ago. The team contacts the owner of the system as they take the system offline into a quarantined environment. Your team pulls all logs from the system and clones the storage on the system. Members go through the logs to look for other systems that may be part of the APT's attack [c]. While the team is cloning the storage system for evidence, you alert the IR team about the issue. After full forensics of the system, your team has verified your company has been hit by the APT, but nothing was taken and no additional attacks happened. You also alert DoD (DC3) about the finding and discuss the matter with them. There is an after action report and a briefing given to management to make them aware of the issue.

Potential Assessment Considerations

- Does the organization have a methodology for performing cyber threat hunting actions [b,c]?
- Has the organization defined all organizational systems within scope of cyber threat hunting, including valid and approved documentation for any organization systems that are not within scope [b,c]?
- Has the organization identified a specific set of individuals to perform cyber threat hunting [b,c]?
- Does the threat hunting team have qualified staff members using the threat feed information [b,c]?
- Does the threat hunting team use combinations of events to determine suspicious behaviors [b,c]?

- Does the organization have a documented list of trusted threat feeds that are used by their cyber hunt teams as the latest indicators of compromise during their efforts [a]?
- Does the organization have a clear methodology for processing threat feed information and turning it into actionable information they can use for their threat hunting approach [a]?

KEY REFERENCES

- NIST SP 800-172 3.11.2e

RA.L3-3.11.3E – ADVANCED RISK IDENTIFICATION

Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Advanced automation and analytics capabilities to predict and identify risks to organizations, systems, and system components are identified;

[b] Analysts to predict and identify risks to organizations, systems, and system components are identified; and

[c] Advanced automation and analytics capabilities are employed in support of analysts to predict and identify risks to organizations, systems, and system components.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: System and information integrity policy; risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; procedures addressing system monitoring; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; security plan; risk assessment artifacts; risk assessment results; risk assessment reviews; risk assessment updates; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for information security; organizational personnel responsible for risk assessments; risk analysts; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring; system/network administrators].

Test

[SELECT FROM: Automated mechanisms supporting and/or implementing risk analytics capabilities; automated mechanisms supporting and/or implementing system monitoring capability; automated mechanisms supporting and/or implementing the discovery, collection, distribution, and use of indicators of compromise; automated mechanisms for conducting, documenting, reviewing, disseminating, and updating risk assessments].

DISCUSSION [NIST SP 800-172]

A properly resourced Security Operations Center (SOC) or Computer Incident Response Team (CIRT) may be overwhelmed by the volume of information generated by the proliferation of security tools and appliances unless it employs advanced automation and analytics to analyze the data. Advanced automation and predictive analytics capabilities are typically supported by artificial intelligence concepts and machine learning. Examples include Automated Workflow Operations, Automated Threat Discovery and Response (which includes broad-based collection, context-based analysis, and adaptive response capabilities), and machine-assisted decision tools.

[NIST SP 800-30] provides guidance on risk assessments and risk analyses.

FURTHER DISCUSSION

Advanced automation includes tools to correlate and reduce the cyber data overload created by defensive tools, making the data understandable to the analyst. Automation also allows the defensive mechanisms to respond rapidly when adversary events are identified. Examples of such capabilities are SIEM; Security Orchestration, Automation, and Response (SOAR); and Extended Detection and Response (XDR) tools. An example of an automated rapid response action is a security alert being pushed to the SIEM while the organization's SOAR solution communicates to the network firewall to block communications to the remote system identified in the security alert.

SIEM is primarily a log collection tool intended to support data storage and analysis. It collects and sends alerts to security personnel for further investigation. SOAR is a software stack that enables an organization to collect data about security threats and respond to security events without human assistance in order to improve security operations. Orchestration connects and integrates disparate internal and external tools. Automation, fed by the data and alerts collected from security orchestration, ingests and analyzes data and creates repeated, automated responses. SOAR incorporates these capabilities based on the SIEM data and enables disparate security tools to coordinate with one another. SOAR can use artificial intelligence to predict and respond to similar future threats, if such tools are employed.

XDR streamlines security data ingestion, analysis, prevention, and remediation workflows across an organization's entire security stack, providing a single console to view and act on threat data. However, the presence of these tools by themselves does not necessarily provide an advanced capability. It is essential that the security team employ critical thinking in support of the intrusion detection and threat hunting processes.

Example

You are responsible for information security in your organization. The organization holds and processes CUI in an enterprise. To protect that data, you want to minimize phishing attacks through the use of Security Orchestration and Automated Response (SOAR). Rather than relying on analysts to manually inspect each inbound item, emails containing links and/or attachments are processed by your automation playbook. Implementation of these

processes involves sending all email links and attachments to detonation chambers or sandboxes prior to delivery to the recipient. When the email is received, SOAR extracts all URL links and attachments from the content and sends them for analysis and testing [a]. The domains in the URLs and the full URLs are processed against bad domain and URL lists. Next, a browser in a sandbox downloads the URLs for malware testing. Lastly, any attachments are sent to detonation chambers to identify if they attempt malicious activities. The hash of the attachments is sent to services to identify if it is known malware [b]. If any one of the items triggers a malware warning from the sandbox, detonation chamber, domain/URL validation service, attachment hash check services, or AV software, an alert about the original email is sent to team members with the recommendation to quarantine it. The team is given the opportunity to select a "take action" button, which would have the SOAR solution take actions to block that email and similar emails from being received by the organization [c].

Potential Assessment Considerations

- Has the organization implemented a security information and event management system [a,c]?
- Has the organization implemented security orchestration, automation, and response tools [a,b,c]?
- Does the organization use automated processing integrated with the SIEM system to perform analytics [c]?
- Can the organization demonstrate use of relevant threat data to inform detection methods that in turn provide automated alerts/recommendations [c]?
- Has the organization implemented an extended detection capability [c]?
- Does the organization have the ability to merge traditional cyber data, such as network packet captures (e.g., PCAP), or process logs with enrichment data, such as reputation or categorization data [c]?
- Can the organization provide examples of both basic and emerging analytics used to analyze alert anomalies, e.g., both simple queries and unsupervised machine learning algorithms that both improve their effectiveness and automatically filter, reduce, or enrich alerting capabilities [c]?

KEY REFERENCES

- NIST SP 800-172 3.11.3e

RA.L3-3.11.4E – SECURITY SOLUTION RATIONALE

Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] The system security plan documents or references the security solution selected;

[b] The system security plan documents or references the rationale for the security solution; and

[c] The system security plan documents or references the risk determination.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: system security plan; records of security plan reviews and updates; system design documentation; security planning policy; procedures addressing security plan development; procedures addressing security plan reviews and updates; enterprise architecture documentation; enterprise security architecture documentation; system interconnection security agreements and other information exchange agreements; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for information security; organizational personnel responsible for developing, implementing, or approving system interconnection and information exchange agreements; personnel managing the systems to which the Interconnection Security Agreement/Information Exchange Agreement applies; system developers; organizational personnel responsible for security planning and plan implementation; organizational personnel responsible for boundary protection; system developers; system/network administrators].

Test

[SELECT FROM: Organizational processes for security plan development, review, update, and approval].

DISCUSSION [NIST SP 800-172]

System security plans relate security requirements to a set of security controls and solutions. The plans describe how the controls and solutions meet the security requirements. For the enhanced security requirements selected when the APT is a concern, the security plan provides traceability between threat and risk assessments and the risk-

based selection of a security solution, including discussion of relevant analyses of alternatives and rationale for key security-relevant architectural and design decisions. This level of detail is important as the threat changes, requiring reassessment of the risk and the basis for previous security decisions.

When incorporating external service providers into the system security plan, organizations state the type of service provided (e.g., software as a service, platform as a service), the point and type of connections (including ports and protocols), the nature and type of the information flows to and from the service provider, and the security controls implemented by the service provider. For safety critical systems, organizations document situations for which safety is the primary reason for not implementing a security solution (i.e., the solution is appropriate to address the threat but causes a safety concern).

[NIST SP 800-18] provides guidance on the development of system security plans.

FURTHER DISCUSSION

The System Security Plan (SSP) is a fundamental component of an organization's security posture. When solutions for implementing a requirement have differing levels of capabilities associated with their implementation, it is essential that the plan specifically document the rationale for the selected solution and what was acquired for the implementation. This information allows the organization to monitor the environment for threat changes and identify which solutions may no longer be applicable. Whle not required, it may also be useful to document alternative solutions reviewed and differing levels of risk associated with each alternative, as that information may facilitatefut ure analyses when the treat changes. In addition to the implementations required for CMMC Level 2 certification, which may not be risk based, at Level 3, the SSP must carefully document the link between the assessed threat and the risk-based selection of a security solution for the enhanced security requirements (i.e., all CMMC L3 requirements derived from NIST SP 800-172).

Example

You are responsible for information security in your organization. Following CMMC requirement RA.L3-3.11.1e – *Threat Informed Risk Assessment*, your team uses threat intelligence to complete a risk assessment and make a risk determination for all elements of your enterprise. Based on that view of risk, your team decides that requirement RA.L3-3.11.2e – *Threat Hunting* is a requirement that is very important in protecting your organization's use of CUI, and you have determined the solution selected could potentially add risk. You want to detect an adversary as soon as possible when they breach the network before any CUI can be exfiltrated. However, there are multiple threat hunting solutions, and each solution has a different set of features that will provide different success rates in identifying IOCs.

As a result, some solutions increase the risk to the organization by being less capable in detecting and tracking an adversary in your networks. To reduce risk, you evaluate five threat hunting solutions and in each case determine the number of IOCs for which there is a monitoring mechanism. You pick the solution that is cost effective, easy to operate, and

optimizes IOC detection for your enterprise; purchase, install, and train SOC personnel on its use; and document the risk-based analysis of alternatives in the SSP. In creating that documentation in the SSP, you follow the guidance found in NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems* [a,b,c].

Potential Assessment Considerations

- Has the organization completed a risk assessment and made a risk determinations for enterprise components that need to be protected [c]?
- Can the organization identify what is being protected and explain why specific protection solutions were selected [a,b]?
- Have all the decisions been documented in the SSP [a,b,c]?

KEY REFERENCES

- NIST SP 800-172 3.11.4e

RA.L3-3.11.5E – SECURITY SOLUTION EFFECTIVENESS

Assess the effectiveness of security solutions at least annually or upon receipt of relevant cyber threat information, or in response to a relevant cyber incident, to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Security solutions are identified;

[b] Current and accumulated threat intelligence is identified;

[c] Anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence is identified; and

[d] The effectiveness of security solutions is assessed at least annually or upon receipt of relevant cyber threat information, or in response to a relevant cyber incident, to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Risk assessment policy; security planning policy and procedures; security assessment policy and procedures; security assessment plans; security assessment results; procedures addressing organizational assessments of risk; security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; threat intelligence information; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for security assessments; organizational personnel responsible for risk assessments; organizational personnel responsible for threat analysis; organizational personnel responsible for information security].

Test

[SELECT FROM: Mechanisms supporting, conducting, documenting, reviewing, disseminating, and updating risk assessments; mechanisms supporting and/or implementing security assessments].

DISCUSSION [NIST SP 800-172]

Threat awareness and risk assessment of the organization are dynamic, continuous, and inform system operations, security requirements for the system, and the security solutions employed to meet those requirements. Threat intelligence (i.e., threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to help provide the necessary context for decision making) is infused into the risk assessment processes and information security operations of the organization to identify any changes required to address the dynamic threat environment.

[NIST SP 800-30] provides guidance on risk assessments, threat assessments, and risk analyses.

FURTHER DISCUSSION

This requirement requires the organization to analyze threat intelligence and consider the effectiveness of currently deployed cybersecurity solutions against existing, new, and emerging threats. The goal is to understand the risk to the systems and the organization based on threat intelligence and to make adjustments to security solutions to reduce the risk to an acceptable level. Analysis of solutions should include analysis of operational system settings of the deployed systems and not be solely a conceptual capability analysis. This analysis includes verifying configuration settings are configured as desired by the organization and have not been changed over time.

Threat information can be thought of as raw data that may be limited in terms of evaluating the effectiveness of controls across the enterprise. For example, knowledge of a threat that has not been correlated with other threats may result in evaluation of an implementation that only provides partial protection for one set of systems when, in fact, the emerging threat is applicable to the entire enterprise. Large organizations may also have the resources to aggregate, transform, analyze, correlate, interpret, and enrich information to support decision-making about adequacy of existing security mechanisms and methods.

Example

You are responsible for information security in your organization, which holds and processes CUI. The organization subscribes to multiple threat intelligence sources [b]. In order to assess the effectiveness of current security solutions, the security team analyses any new incidents reported in the threat feed. They identify weaknesses that were leveraged by malicious actors and subsequently look for similar weaknesses in their own security architecture[a,c]. This analysis is passed to the architecture team for engineering change recommendations, including system patching guidance, new sensors, and associated alerts that should be generated, and to identify ways to mitigate, transfer, or accept the risk necessary to respond to events if they occur within their own organization [d].

Potential Assessment Considerations

- Does the organization make adjustments during an incident or operational improvements after an incident has occurred [d]?
- Has the organization implemented an analytical process to assess the effectiveness of security solutions against new or compiled threat intelligence [b,c,d]?
- Has the organization implemented a process to identify if an operational security solution fails to contribute to the protections needed against specific adversarial actions based on new threat intelligence [a,b,c,d]?

KEY REFERENCES

- NIST SP 800-172 3.11.5e

RA.L3-3.11.6E – SUPPLY CHAIN RISK RESPONSE

Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Supply chain risks associated with organizational systems and system components are identified;

[b] Supply chain risks associated with organizational systems and system components are assessed;

[c] Supply chain risks associated with organizational systems and system components are responded to; and

[d] Supply chain risks associated with organizational systems and system components are monitored.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Risk assessment policy; procedures addressing organizational assessments of risk; security planning policy and procedures; supply chain risk management plan; security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; threat intelligence information; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for information security; organizational personnel responsible for risk assessments; organizational personnel responsible for supply chain risk management].

Test

[SELECT FROM: Mechanisms supporting, conducting, documenting, reviewing, disseminating, and updating risk assessments].

DISCUSSION [NIST SP 800-172]

Supply chain events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on a system and its information and, therefore, can also adversely impact organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other

organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

[NIST SP 800-30] provides guidance on risk assessments, threat assessments, and risk analyses. [NIST SP 800-161 Rev. 1] provides guidance on supply chain risk management.

FURTHER DISCUSSION

Organizations will have varying policies, definitions, and actions for this requirement. It is important for a single organization to be consistent and to build a process that makes sense for their organization, strategy, unique supply chain, and the technologies available to them.

Example

You are responsible for information security in your organization, which holds and processes CUI. One of your responsibilities is to manage risk associated with your supply chain that may provide an entry point for the adversary. First, you acquire threat information by subscribing to reports that identify supply chain attacks in enough detail that you are able to identify the risk points in your organization's supply chain [a]. You create an organization-defined prioritized list of risks the organization may encounter and determine the responses to be implemented to mitigate those risks [b,c].

In addition to incident information, the intelligence provider also makes recommendations for monitoring and auditing your supply chain. You assess, integrate, correlate, and analyze this information so you can use it to acquire monitoring tools to help identify supply chain events that could be an indicator of an incident. This monitoring tool provides visibility of the entire attack surface, including your vendors' security posture [d]. Second, you analyze the incident information in the intelligence report to help identify defensive tools that will help respond to each of those known supply chain attack techniques as soon as possible after such an incident is detected, thus mitigating risk associated with known techniques.

Potential Assessment Considerations

- Has the organization prioritized risks to the supply chain [a,b]?
- Does the organization have viable service-level agreements that describe and enable responses to supply chain incidents [c,d]?

KEY REFERENCES

- NIST SP 800-172 3.11.6e

RA.L3-3.11.7E – SUPPLY CHAIN RISK PLAN

Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan at least annually, and upon receipt of relevant cyber threat information, or in response to a relevant cyber incident.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Supply chain risks associated with organizational systems and system components are identified;

[b] Organizational systems and system components to include in a supply chain risk management plan are identified;

[c] A plan for managing supply chain risks associated with organizational systems and system components is developed; and

[d] The plan for managing supply chain risks is updated at least annually, and upon receipt of relevant cyber threat information, or in response to a relevant cyber incident.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Risk assessment policy; supply chain risk management plan; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; threat intelligence information; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for information security; organizational personnel responsible for risk assessments; organizational personnel responsible for supply chain risk management].

Test

[SELECT FROM: Automated mechanisms supporting, conducting, documenting, reviewing, disseminating, and updating risk assessments].

DISCUSSION [NIST SP 800-172]

The growing dependence on products, systems, and services from external providers, along with the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase risk include the insertion or use of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain.

136

Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with both internal and external stakeholders. Supply chain risk management (SCRM) activities involve identifying and assessing risks, determining appropriate mitigating actions, developing SCRM plans to document selected mitigating actions, and monitoring performance against plans. SCRM plans address requirements for developing trustworthy, secure, and resilient systems and system components, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes.

[NIST SP 800-161 Rev. 1] provides guidance on supply chain risk management

FURTHER DISCUSSION

An organization is required to have a supply chain risk management plan that assesses and responds to the identified risks from those organizations that provide IT products or services, including any cloud or other third-party services with a role in the operation of the system. The organization should be cognizant of services outside the scope of the system but required for the operation of the system as part of their plan. Since the cyber environment changes rapidly and continuously, it is equally important for the organization to update the plan in response to supply chain cyber incidents or emerging information.

Example

You are responsible for information security in your organization, and you have created a supply chain risk management plan [a,b,c]. One of the organization's suppliers determines that it has been the victim of a cyberattack. Your security team meets with the supplier to determine the nature of the attack and to understand the adversary, the attack, the potential for corruption of delivered goods or services, and current as well as future risks. The understanding of the supply chain will help protect the local environment. Subsequently, you update the risk management plan to include a description of the necessary configuration changes or upgrades to monitoring tools to improve the ability to identify the new risks, and when improved tools are available, you document the acquisition of defensive tools and associated functionality to help mitigate any of the identified techniques [d].

Potential Assessment Considerations

- Does the organization's current supply chain risk management plan apply across the enterprise, or does it only apply to a limited portion of the supply chain [b]?

KEY REFERENCES

- NIST SP 800-172 3.11.7e

Security Assessment (CA)

CA.L3-3.12.1E – PENETRATION TESTING

Conduct penetration testing at least annually or when significant security changes are made to the system, leveraging automated scanning tools and ad hoc tests using subject matter experts.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Automated scanning tools are identified;

[b] Ad hoc tests using subject matter experts are identified; and

[c] Penetration testing is conducted at least annually or when significant security changes are made to the system, leveraging automated scanning tools and ad hoc tests using subject matter experts.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Security assessment policy; procedures addressing penetration testing; security plan; security assessment plan; penetration test report; security assessment report; security assessment evidence; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for security assessments; penetration testing team; system/network administrators; organizational personnel responsible for information security].

Test

[SELECT FROM: Automated mechanisms supporting security assessments; automated mechanisms supporting penetration testing].

DISCUSSION [NIST SP 800-172]

Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning. It is conducted by penetration testing agents and teams with particular skills and experience that include technical expertise in network, operating system, and application-level security. Penetration testing can be used to validate vulnerabilities or determine a system's penetration resistance to adversaries within specified constraints. Such constraints include

time, resources, and skills. Organizations may also supplement penetration testing with red team exercises. Red teams attempt to duplicate the actions of adversaries in carrying out attacks against organizations and provide an in-depth analysis of security-related weaknesses or deficiencies.

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes pretest analysis based on full knowledge of the system, pretest identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities. All parties agree to the specified rules of engagement before the commencement of penetration testing. Organizations correlate the rules of engagement for penetration tests and red teaming exercises (if used) with the tools, techniques, and procedures that they anticipate adversaries may employ. The penetration testing or red team exercises may be organization-based or external to the organization. In either case, it is important that the team possesses the necessary skills and resources to do the job and is objective in its assessment.

[NIST SP 800-53A] provides guidance on conducting security assessments.

FURTHER DISCUSSION

It is important that the organization has a repeatable penetration testing capability, regardless of who performs the penetration testing. This requirement entails performing tests against components of the organization's architecture to identify cyber weaknesses and vulnerabilities. It does not mean everything in the architecture requires penetration testing. This requirement provides findings and mitigation strategies that benefit the organization and help create a stronger environment against adversary efforts. It may be beneficial for the organization to define the scope of penetration testing. The organization's approach may involve hiring an expert penetration testing team to perform testing on behalf of the organization. When an organization has penetration testing performed, either by an internal team or external firm, they should establish rules of engagement and impose limits on what can be performed by the penetration test team(s).

Ensuring the objectivity of the test team is important as well. Potential conflicts of interest, such as having internal testers report directly or indirectly to network defenders or an external test team contracted by network defense leadership, must be carefully managed by organizational leadership.

Reports on the findings should be used by the organization to determine where to focus funding, staffing, training, or technical improvements for future mitigation strategies.

2065 ### Example

2066 You are responsible for information security in your organization. Leveraging a contract
2067 managed by the CIO, you hire an external expert penetration team annually to test the
2068 security of the organization's enclave that stores and processes CUI [a,c]. You hire the same
2069 firm annually or on an ad hoc basis when significant changes are made to the architecture
2070 or components that affect security [b,c].

2071 ### Potential Assessment Considerations

2072 • Does the organization have internal team members who possess the proper level of
2073 expertise to perform a valued penetration testing effort [b]?

2074 • If the penetration testing is performed by an internal team, are the individuals
2075 performing the testing objectively [b]?

2076 • Is a penetration testing final report provided to the internal team responsible for
2077 organizational defense?

2078 • If previous penetration tests have been conducted, can the organization provide
2079 samples of penetration test plans, findings reports, and mitigation guidance based on
2080 the findings [a,b,c]?

2081 ## KEY REFERENCES

2082 • NIST SP 800-172 3.12.1e

2083 System and Communications Protection (SC)

2084 SC.L3-3.13.4E – ISOLATION

2085 Employ physical isolation techniques or logical isolation techniques or both in
2086 organizational systems and system components.

2087 ASSESSMENT OBJECTIVES [NIST SP 800-172A]

2088 Determine if:

2089 [ODP1] One or more of the following is/are selected: physical isolation techniques;
2090 logical isolation techniques;

2091 [ODP2] Physical isolation techniques are defined (if selected);

2092 [ODP3] Logical isolation techniques are defined (if selected);

2093 [a] Physical isolation techniques or logical isolation techniques or both are employed in
2094 organizational systems and system components.

2095 POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

2096 Examine

2097 [SELECT FROM: System and communications protection policy; procedures addressing
2098 boundary protection; system design documentation; procedures addressing the use of thin
2099 nodes; list of key internal boundaries of the system; security plan; boundary protection
2100 hardware and software; system configuration settings and associated documentation;
2101 enterprise architecture documentation; system architecture; security architecture
2102 documentation; system audit records; system component inventory; list of security tools
2103 and support components to be isolated from other system components; other relevant
2104 documents or records].

2105 Interview

2106 [SELECT FROM: Organizational personnel responsible for information security;
2107 system/network administrators; system developers; organizational personnel responsible
2108 for boundary protection].

2109 Test

2110 [SELECT FROM: Mechanisms implementing the boundary protection capability;
2111 mechanisms implementing physical isolation techniques; mechanisms supporting and/or
2112 implementing the isolation of information security tools, mechanisms, and support
2113 components; mechanisms supporting and/or implementing the capability to separate
2114 system components supporting organizational missions and business functions;
2115 mechanisms implementing logical isolation techniques; mechanisms supporting or

implementing separate network addresses/different subnets; mechanisms supporting and/or implementing thin nodes]

DISCUSSION [NIST SP 800-172]

A mix of physical and logical isolation techniques (described below) implemented as part of the system architecture can limit the unauthorized flow of CUI, reduce the system attack surface, constrain the number of system components that must be secure, and impede the movement of an adversary. When implemented with a set of managed interfaces, physical and logical isolation techniques for organizational systems and components can isolate CUI into separate security domains where additional protections can be implemented. Any communications across the managed interfaces (i.e., across security domains), including for management or administrative purposes, constitutes remote access even if the communications remain within the organization. Separating system components with boundary protection mechanisms allows for the increased protection of individual components and more effective control of information flows between those components. This enhanced protection limits the potential harm from and susceptibility to hostile cyber-attacks and errors. The degree of isolation can vary depending on the boundary protection mechanisms selected. Boundary protection mechanisms include routers, gateways, and firewalls separating system components into physically separate networks or subnetworks; virtualization and micro-virtualization techniques; encrypting information flows among system components using distinct encryption keys; cross-domain devices separating subnetworks; and complete physical separation (i.e., air gaps).

System architectures include logical isolation, partial physical and logical isolation, or complete physical isolation between subsystems and at system boundaries between resources that store, process, transmit, or protect CUI and other resources. Examples include:

- Logical isolation: Data tagging, digital rights management (DRM), and data loss prevention (DLP) that tags, monitors, and restricts the flow of CUI; virtual machines or containers that separate CUI and other information on hosts; and virtual local area networks (VLAN) that keep CUI and other information separate on networks.
- Partial physical and logical isolation: Physically or cryptographically isolated networks, dedicated hardware in data centers, and secure clients that (a) may not directly access resources outside of the domain (i.e., all applications with cross-enclave connectivity execute as remote virtual applications hosted in a demilitarized zone [DMZ] or internal and protected enclave), (b) access via remote virtualized applications or virtual desktop with no file transfer capability other than with dual authorization, or (c) employ dedicated client hardware (e.g., a zero or thin client) or hardware approved for multi-level secure (MLS) usage.
- Complete physical isolation: Dedicated (not shared) client and server hardware; physically isolated, stand-alone enclaves for clients and servers; and (a) logically separate network traffic (e.g., using a VLAN) with end-to-end encryption using Public Key Infrastructure (PKI)-based cryptography or (b) physical isolation from other networks.

148

Isolation techniques are selected based on a risk management perspective that balances the threat, the information being protected, and the cost of the options for protection. Architectural and design decisions are guided and informed by the security requirements and selected solutions. Organizations consider the trustworthiness of the isolation techniques employed (e.g., the logical isolation relies on information technology that could be considered a high value target because of the function being performed), introducing its own set of vulnerabilities.

[NIST SP 800-160-1] provides guidance on developing trustworthy, secure, and cyber resilient systems using systems security engineering practices and security design concepts.

FURTHER DISCUSSION

For this requirement, organizations must identify the systems or enclaves that need to be isolated, then design and implement the isolation. The resulting isolation solutions are documented or referenced in the SSP. Documentation will be dependent on the design selected and may include a high-level diagram, but specific details that may change on some frequency would be omitted. During an assessment, providing details such as subnet and VLAN implementation identifiers, internal boundary protection hardware and software, interface device functionality, and system configuration and Access Control List (ACL) settings will be useful.

Example

You are responsible for information security in your organization, which holds and processes CUI. You have decided to isolate the systems processing CUI by limiting all communications in and out that enclave with cross-domain interface devices that implement access control [a]. Your security team has identified all the systems containing such CUI, documented network design details, developed network diagrams showing access control points, documented the logic for the access control enforcement decisions, described the interface and protocol to the identification and authentication mechanisms, and documented all details associated with the ACLs, including review, updates, and credential revocation procedures.

Potential Assessment Considerations

- Has the organization clearly identified where they use physical, logical, or both isolation techniques [a]?
- Can the organization describe the isolation techniques they have employed [a]?
- Has the organization deployed subnetting, internal firewalls, and VLANs to control packet flow between internal segments [a]?
- Does the organization employ metadata to inform isolation techniques [a]?

2194 ## KEY REFERENCES

2195 - NIST SP 800-172 3.13.4e

2196 System and Information Integrity (SI)

2197 SI.L3-3.14.1E – INTEGRITY VERIFICATION

2198 Verify the integrity of security critical and essential software using root of trust
2199 mechanisms or cryptographic signatures.

2200 ASSESSMENT OBJECTIVES [NIST SP 800-172A]

2201 Determine if:

2202 [ODP1] Security critical or essential software is defined;

2203 [a] Root of trust mechanisms or cryptographic signatures are identified and

2204 [b] The integrity of security critical and essential software is verified using root of trust
2205 mechanisms or cryptographic signatures.

2206 POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

2207 Examine

2208 [SELECT FROM: System and information integrity policy; procedures addressing software,
2209 firmware, and information integrity; system design documentation; security plan; system
2210 configuration settings and associated documentation; system component inventory;
2211 integrity verification tools and associated documentation; records of integrity verification
2212 scans; system audit records; cryptographic mechanisms and associated documentation;
2213 records of detected unauthorized changes to software, firmware, and information; other
2214 relevant documents or records].

2215 Interview

2216 [SELECT FROM: Organizational personnel responsible for information security;
2217 organizational personnel responsible for software, firmware, and/or information integrity;
2218 system developers; system/network administrators].

2219 Test

2220 [SELECT FROM: Software, firmware, and information integrity verification tools;
2221 mechanisms supporting and/or implementing integrity verification of the boot process;
2222 mechanisms supporting and/or implementing protection of the integrity of boot firmware;
2223 cryptographic mechanisms implementing software, firmware, and information integrity;
2224 safeguards implementing protection of the integrity of boot firmware].

DISCUSSION [NIST SP 800-172]

Verifying the integrity of the organization's security-critical or essential software is an important capability since corrupted software is the primary attack vector used by adversaries to undermine or disrupt the proper functioning of organizational systems. There are many ways to verify software integrity throughout the system development life cycle. Root of trust mechanisms (e.g., secure boot, trusted platform modules, Unified Extensible Firmware Interface [UEFI]), verify that only trusted code is executed during boot processes. This capability helps system components protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying the boot firmware. The employment of cryptographic signatures ensures the integrity and authenticity of critical and essential software that stores, processes, or transmits, CUI. Cryptographic signatures include digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Hardware roots of trust are considered to be more secure. This requirement supports 3.4.1e and 3.4.3.e.

[FIPS 140-3] provides security requirements for cryptographic modules. [FIPS 180-4] and [FIPS 202] provide secure hash standards. [FIPS 186-4] provides a digital signature standard. [NIST SP 800-147] provides BIOS protection guidance. [NIST TRUST] provides guidance on the roots of trust project.

FURTHER DISCUSSION

Organizations verify the integrity of security critical and essential software every time that software is executed. Secure boot mechanisms for firmware and a cryptographically protected boot chain ensure the integrity of the operating system (OS) and security critical software, and cryptographic techniques ensure the essential software has not been tampered with after development prior to execution. If software is itself considered to be CUI or if it uses CUI, this requirement ensures it has not been compromised.

Software and information integrity verification tools can help check the integrity during the development process for those organizations developing software. As critical software is updated, the integrity of any configuration data and the software must result in updated signatures and an ongoing verification process.

Operating systems include mechanisms to validate digital signatures for installed software. Most software packages use signatures to prove the integrity of the provided software, and the organization should leverage these capabilities. Similarly, most hardware appliance vendors have secure boot checks in place for their devices and built-in features that check the digital signature of an upgrade/update package before they allow an upgrade to take place. For locally developed software, the organization should sign the software to ensure its integrity.

Example 1

You are responsible for information security in your organization. Your security team has identified the software used to process CUI, and the organization has decided it is mission-critical software that must be protected. You take three actions. First, you ensure all of the platform's configuration information used at boot is hashed and stored in a TPM [a]. Second, you ensure that the platforms used to execute the software are started with a digitally signed software chain to a secure boot process using the TPM. Finally, you ensure the essential applications are cryptographically protected with a digital signature when stored and the signature is verified prior to execution [b].

Example 2

Your organization has a software security team, and they are required to validate unsigned essential software provided to systems that do not have TPM modules. The organization has a policy stating no software can be executed on a system unless its hash value matches that of a hash stored in the approved software library kept by the software security team [a]. This action is performed by implementing software restriction policies on systems. The team tests the software on a sandbox system, and once it is proven safe, they run a hashing function on the software to create a hash value. This hash value is placed in a software library so the system will know it can execute the software [b]. Any changes to the software without the software security team's approval will result in the software failing the security tests, and it will be prevented from executing.

Potential Assessment Considerations

- Does the organization use cryptographic signatures to ensure the integrity and authenticity of critical and essential software and data [b]?
- Has the organization identified those devices that require integrity verification of the boot process [a]?
- Does the organization use a TPM to store hashes of pre-run time configuration parameters for those systems [b]?
- Does the organization leverage the TPM configuration hash to verify the hardware and software configuration is unchanged in order to determine that a system is trustworthy before running mission-essential applications [b,c]?
- Does the organization use the TPM for remote attestation to determine to which extent information can be trusted from another system [b,c]?
- Has the organization identified devices requiring organization-defined security safeguards that must be implemented to protect the integrity of boot firmware [a]?
- Has the organization defined security safeguards that will be implemented to protect the integrity of boot firmware in mission-essential devices [a]?
- Has the organization implemented organization-defined security safeguards to protect the integrity of boot firmware in organization-defined essential devices [b]?

2302 ## KEY REFERENCES

2303 • NIST SP 800-172 3.14.1e

2304

SI.L3-3.14.3E – SPECIALIZED ASSET SECURITY

Ensure that specialized assets including IoT, IIoT, OT, GFE, Restricted Information Systems and test equipment are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[a] Specialized assets including IoT, IIoT, OT, GFE, Restricted Information Systems and test equipment are included in the scope of the specified enhanced security requirements and

[b] Systems and system components that are not included in specialized assets including IoT, IIoT, OT, GFE, Restricted Information Systems and test equipment are segregated in purpose-specific networks.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: Access control policy; information flow control policies; system and services acquisition policy; system and communications protection policy; procedures addressing security function isolation; procedures addressing application partitioning; procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the system; procedures addressing information flow enforcement; procedures addressing access enforcement; system architecture; system design documentation; security plan; system component inventory; system configuration settings and associated documentation; system baseline configuration; list of security functions to be isolated from non-security functions; system audit records; security requirements and specifications for the system; list of approved authorizations (user privileges); list of information flow authorizations; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for access enforcement; system/network administrators; organizational personnel responsible for information security; system developers; system integrators; organizational personnel responsible for acquisition/contracting; organizational personnel responsible for determining system security requirements; system security architects; enterprise architects; organizational personnel responsible for system specification, design, development, implementation, and modification].

Test

[SELECT FROM: Mechanisms implementing the access control policy; mechanisms implementing the information flow enforcement policy; mechanisms supporting the application of security engineering principles in system specification, design, development, implementation, and modification].

DISCUSSION [NIST SP 800-172]

Organizations may have a variety of systems and system components in their inventory, including Information Technology (IT), Internet of Things (IoT), Operational Technology (OT), and Industrial Internet of Things (IIoT). The convergence of IT, OT, IoT, and IIoT significantly increases the attack surface of organizations and provides attack vectors that are challenging to address. Compromised IoT, OT, and IIoT system components can serve as launching points for attacks on organizational IT systems that handle CUI. Some IoT, OT, and IIoT system components can store, transmit, or process CUI (e.g., specifications or parameters for objects manufactured in support of critical programs). Most of the current generation of IoT, OT, and IIoT system components are not designed with security as a foundational property and may not be able to be configured to support security functionality. Connections to and from such system components are generally not encrypted, do not provide the necessary authentication, are not monitored, and are not logged. Therefore, these components pose a significant cyber threat. Gaps in IoT, OT, and IIoT security capabilities may be addressed by employing intermediary system components that can provide encryption, authentication, security scanning, and logging capabilities—thus, preventing the components from being accessible from the Internet. However, such mitigation options are not always available or practicable. The situation is further complicated because some of the IoT, OT, and IIoT devices may be needed for essential missions and business functions. In those instances, it is necessary for such devices to be isolated from the Internet to reduce the susceptibility to cyber-attacks.

[NIST SP 800-160-1] provides guidance on security engineering practices and security design concepts.

FURTHER DISCUSSION

Specialized Assets are addressed in the scoping guidance, which should be overlaid on this requirement. The OSC must document Specialized Assets in the asset inventory; develop, document, and periodically update system security plans; and include Specialized Assets in the network diagram. The Specialized Asset section of the SSP should describe associated system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Specialized Assets within the Level 3 CMMC assessment scope must be either assessed against all CMMC requirements or separated into purpose-specific networks. Specialized Assets may have limitations on the application of certain security requirements. To accommodate such issues, the SSP should describe any mitigations.

Intermediary devices are permitted to mitigate an inability for the asset itself to implement one or more CMMC requirements.

The high-level list of Specialized Assets includes:

- Government Furnished Equipment;
- IoT and IIoT devices (physical or virtual) with sensing/actuation capability and programmability features;
- OT used in manufacturing systems, industrial control systems (ICS), or supervisory control and data acquisition (SCADA) systems;
- Restricted Information Systems, which can include systems and IT components that are configured based on government requirements; and
- Test equipment.

Example

You are responsible for information security in your organization, which processes CUI on the network, and this same network includes GFE for which the configuration is mandated by the government. The GFE is needed to process CUI information [a]. Because the company cannot manage the configuration of the GFE, it has been augmented by placing a bastion host between it and the network. The bastion host meets the requirements that the GFE cannot, and is used to send CUI files to and from the GFE for processing. You and your security team document in the SSP all of the GFE to include GFE connectivity diagrams, a description of the isolation mechanism, and a description of how your organization manages risk associated with that GFE [a].

Potential Assessment Considerations

- Has the organization documented all specialized assets in asset inventory [a]?
- Has the organization documented all specialized assets in the SSP to show how risk is managed [b]?
- Has the organization provided a network diagram for specialized assets [a,b]?

KEY REFERENCES

- NIST SP 800-172 3.14.3e

SI.L3-3.14.6E – THREAT-GUIDED INTRUSION DETECTION

Use threat indicator information and effective mitigations obtained from, at a minimum, open or commercial sources, and any DoD-provided sources, to guide and inform intrusion detection and threat hunting.

ASSESSMENT OBJECTIVES [NIST SP 800-172A]

Determine if:

[ODP1] External organizations from which to obtain threat indicator information and effective mitigations are defined;

[a] Threat indicator information is identified;

[b] Effective mitigations are identified;

[c] Intrusion detection approaches are identified;

[d] Threat hunting activities are identified; and

[e] Threat indicator information and effective mitigations obtained from, at a minimum, open or commercial sources and any DoD-provided sources, are used to guide and inform intrusion detection and threat hunting.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-172A]

Examine

[SELECT FROM: System and information integrity policy; information security program plan; procedures addressing security alerts, advisories, and directives; threat awareness program documentation; procedures addressing system monitoring; procedures for the threat awareness program; risk assessment results relevant to threat awareness; records of security alerts and advisories; system design documentation; security plan; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; documentation on the cross-organization information-sharing capability; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel responsible for information security program planning and plan implementation; system/network administrators; organizational personnel responsible for the threat awareness program; organizational personnel responsible for the cross-organization information-sharing capability; organizational personnel responsible for information security; organizational personnel responsible for installing, configuring, and/or maintaining the system; organizational personnel security alerts and advisories; organizational personnel responsible for implementing, operating, maintaining, and using the system; organizational personnel, organizational elements,

and/or external organizations to whom alerts, advisories, and directives are to be disseminated; personnel with whom threat awareness information is shared by the organization; system developers].

Test

[SELECT FROM: Mechanisms supporting and/or implementing the threat awareness program; mechanisms supporting and/or implementing the cross-organization information-sharing capability; mechanisms supporting and/or implementing the system monitoring capability; mechanisms supporting and/or implementing the definition, receipt, generation, and dissemination of security alerts, advisories, and directives; mechanisms supporting and/or implementing security directives; mechanisms supporting and/or implementing threat hunting; mechanisms supporting and/or implementing intrusion detection; mechanisms supporting and/or implementing the discovery, collection, distribution, and use of indicators of compromise].

DISCUSSION [NIST SP 800-172]

Threat information related to specific threat events (e.g., TTPs, targets) that organizations have experienced, threat mitigations that organizations have found to be effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats that can occur) are sourced from and shared with trusted organizations. This threat information can be used by organizational Security Operations Centers (SOC) and incorporated into monitoring capabilities. Threat information sharing includes threat indicators, signatures, and adversary TTPs from organizations participating in threat-sharing consortia, government-commercial cooperatives, and government-government cooperatives (e.g., CERTCC, CISA/US-CERT, FIRST, ISAO, DIB CS Program). Unclassified indicators, based on classified information but which can be readily incorporated into organizational intrusion detection systems, are available to qualified nonfederal organizations from government sources.

FURTHER DISCUSSION

One way to effectively leverage threat indicator information is to access human- or machine-readable threat intelligence feeds. Effectiveness may also require the organization to create TTPs in support of operational requirements, which will typically include defensive cyber tools supporting incident detection, alerts, incident response, and threat hunting. It is possible that this requirement will be implemented by a third-party managed service provider, and in that case, it will be necessary to carefully define the boundary and responsibilities between the OSC and the ESP to guarantee a robust implementation. It is also important that the OSC validate threat indicator integration into the defensive cyber toolset by being able to (1) implement mitigations for sample industry relevant indicators of compromise (e.g., IP address, file hash), (2) identify sample indicators of compromise across sample endpoints, and (3) identify sample indicators of compromise using analytical processes on a system data repository.

2481 ## Example

2482 You are responsible for information security in your organization. You have maintained an
2483 effective intrusion detection capability for some time, but now you decide to introduce a
2484 threat hunting capability informed by internal and external threat intelligence [a,c,d,e]. You
2485 install a SIEM system that leverages threat information to provide functionality to:

2486 • analyze logs, data sources, and alerts;

2487 • query data to identify anomalies;

2488 • identify variations from baseline threat levels;

2489 • provide machine learning capabilities associated with the correlation of anomalous
2490 data characteristics across the enterprise; and

2491 • categorize data sets based on expected data values.

2492 Your team also manages an internal mitigation plan (playbook) for all known threats for
2493 your environment. This playbook is used to implement effective mitigation strategies
2494 across the environment [b]. Some of the mitigation strategies are developed by team
2495 members, and others are obtained by threat feed services.

2496 ## Potential Assessment Considerations

2497 • Which external sources has the organization identified as threat information sources
2498 [a]?

2499 • Does the organization understand the TTPs of key attackers [c,d]?

2500 • Does the organization deploy threat indicators to EDR systems, network intrusion
2501 detection systems, or both [c,d,e]?

2502 • What actions does the organization implement when a threat alert/indicator is signaled
2503 [c,d,e]?

2504 • Does the organization use internal threat capabilities within their existing security tools
2505 [e].

2506 • How does the organization respond to a third-party notification of a threat indicator
2507 [e]?

2508 ## KEY REFERENCES

2509 • NIST SP 800-172 3.14.6e

Appendix A – Acronyms and Abbreviations

AC	Access Control
ACL	Access Control List
ACM	Automated Configuration Management
ACMS	Automated Configuration Management System
APT	Advanced Persistent Threat
AT	Awareness and Training
C3PAO	CMMC Third-Party Assessment Organization
CA	Certification Authority
CA	Security Assessment
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIRT	Computer Incident Response Team; Cyber Incident Response Team
CISO	Chief Information Security Officer
CM	Configuration Management
CMMC	Cybersecurity Maturity Model Certification
CUI	Controlled Unclassified Information
DCSA	Defense Counterintelligence and Security Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoD	Department of Defense
DRM	Digital Rights Management
ESP	External Service Provider
FIPS	Federal Information Processing Standard
GFE	Government Furnished Equipment
GPO	Group Policy Object
HR	Human Resources
IA	Identification and Authentication
ICS	Industrial Control System
ID	Identification
IIoT	Industrial Internet of Things
IOC	Indicators of Compromise
IoT	Internet of Things

IP	Internet Protocol
IR	Incident Response
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
MEP	Manufacturing Extension Partnership
MLS	Multi-Level Secure
N/A	Not Applicable
NAC	Network Access Control
NARA	National Archives and Record Administration
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency (or Internal) Report
ODP	Organization-defined Parameters
OS	Operating System
OT	Operational Technology
PKI	Public Key Infrastructure
PS	Personnel Security
RA	Risk Assessment
SC	System and Communications Protection
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SI	System and Information Integrity
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SP	Special Publication
SSP	System Security Plan
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTP	Tactics, Techniques, and Procedures
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
XDR	Extended Detection and Response

2511


OFFICE OF THE UNDER SECRETARY OF DEFENSE
ACQUISITION AND SUSTAINMENT
CYBERSECURITY MATURITY MODEL
CERTIFICATION