USE CASE

IT ASSET MANAGEMENT

Securing Assets for the Financial Services Sector

V.2 – Final Draft
May 1, 2014
financial_nccoe@nist.gov

This revision incorporates comments from the public.

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices.

This document is a detailed description of a particular problem that is relevant across the financial services sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the sector and vendors of cybersecurity solutions. The solutions proposed by this effort will not be the only ones available in the fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at financial_nccoe@nist.gov.

1. DESCRIPTION

Goal

To effectively manage, utilize and secure an asset, you first need to know the asset's location and function. While many financial sector companies label physical assets with bar codes and track them with a database, this approach does not answer questions such as, "What operating systems are our laptops running?" and "Which devices are vulnerable to the latest threat?" The goal of this project is to provide answers to questions like these by tying existing data systems for physical assets, security systems and IT support into a comprehensive IT asset management (ITAM) system. In addition, financial services companies can employ this ITAM system to dynamically apply business and security rules to better utilize information assets and protect enterprise systems and data. In short, this ITAM system will give companies the ability to track, manage and report on an information asset throughout its entire life cycle, thereby reducing the total cost of ownership by reducing the number of man-hours needed to perform tasks such as incident response and system patching.

Motivation

Financial services companies, like most U.S. industries, design their asset management practices around the key physical products and intellectual property residing within the internal corporate environment they own, control and manage.

An effective ITAM system increases security by providing visibility into what assets are present and what they are doing. Organizations are collecting more asset-related data than ever before, but often have a difficult time turning that data into actionable information. Records related to assets are stored in numerous locations such as asset databases, configuration systems, vulnerability scanners, network monitoring tools and patch managers. This ITAM system provides a complete picture by combining data from asset management along with data from various monitoring tools. Following a security

incident, the security analyst can use ITAM system to track an alert down to the exact location, machine, software and user. A properly administered and implemented ITAM system addresses numerous security controls, including the top three from SANS[1] , while providing for more effective resource utilization, patch management and policy enforcement.

Example Scenarios

Scenario 1: A new laptop computer is purchased

In this scenario, the ITAM system will access data from a physical asset management system, directory service and the laptop.

- **Phase 1** – When a new laptop is acquired, an asset manager records certain data attributes in a traditional physical asset management system before provisioning. Attributes might include the laptop make, model, price/value, location, business unit and owner, or other characteristics.
- **Phase 2** – The asset manager submits the new laptop to IT support for provisioning. IT support equips the new laptop with the company's baseline load of an operating system, software and required configurations. The load may include ITAM system software. IT support also adds the new laptop to the enterprise directory service during this phase.

  Phase 3 – IT support assigns and delivers the new laptop to an end user. The end user can now add additional software—in accordance with company policy (enforced via ITAM or existing mechanisms linked to ITAM)—and make personal configuration changes (e.g., backgrounds, icons, menus, etc.). The ITAM system will detect and log any changes made to the laptop and automatically update relevant administrative systems.

Scenario 2: A server is transferred from one department to another

In this scenario, the ITAM system will be used to update a physical asset management system, directory service and the server itself.

- **Phase 1** - Assume that the server is already part of the ITAM system and has the required software installed. The development department generates a work order to IT support ordering the server transferred from the development department to the sales department.
- **Phase 2** – IT support updates the software baseline of the server by removing software needed by the development department and adding software required by the sales department. The ITAM system updates its records during this process as changes are made.
- **Phase 3** – IT support uses the ITAM system to update ownership information pertaining to the server. The ITAM system uses this new information to update

[1] SANS 20 Critical Security Controls: http://www.sans.org/critical-security-controls/

other required systems, such as the physical asset management system.

- **Phase 4** – The destination department receives their new server that has been correctly configured and added to the inventory. The ITAM system detects and logs any changes made on the server while it is in use and automatically updates the required systems. The ITAM system also detects and reports on all assets running on the server, such as virtual machines and applications.

Scenario 3: A virtual machine migrates between physical servers

In this scenario, a virtual machine will be moved from physical server 1 to physical server 2.

- **Phase 1** – The hypervisor determines that a virtual machine needs to be migrated due to impending maintenance on server 1. The hypervisor, in coordination with ITAM, determines that server 2 is an appropriate location and begins the migration process.
- **Phase 2** – Just after the hypervisor completes the migration process and the virtual machine is now running on server 2, the ITAM system recognizes the change and updates the appropriate administrative systems.

Scenario 4: Incident response and prevention

In this scenario, an advisory is received describing a particular piece of software with a critical vulnerability. A software patch is also available to prevent this vulnerability.

- **Phase 1** – The software mentioned in the advisory is added to the "blacklist" of unauthorized software for the enterprise.
- **Phase 2** – The ITAM system then scans to determine if any systems have the vulnerable software installed. A report is generated identifying the vulnerable assets and those assets are moved off of the production network into a quarantine zone.
- **Phase 3** – The patch is entered into the existing enterprise patch management system and pushed out to all machines (including those in the quarantine zone).
- **Phase 4** – The ITAM system performs another scan to determine if any systems still have the vulnerable software installed (effectively double checking that the patch management system was effective). A report is generated identifying any assets that are still vulnerable. If a system is still vulnerable, manual patching or other remediation may be necessary.
- **Phase 5** – Clean systems are moved back into the production network.

2. Desired Solution Characteristics

The ITAM system will

- be capable of interfacing with multiple existing systems
- complement existing asset management, security and network systems

- provide APIs for communicating with other security devices and systems such as firewalls and intrusion detection and identity and access management (IDAM) systems
- know and control which assets, both virtual and physical, are connected to the enterprise network
- provide fine-grain asset accountability supporting the idea of data as an asset
- automatically detect and alert when unauthorized devices attempt to access the network, also known as asset discovery
- integrate with ways to validate a trusted network connection
- enable administrators to define and control the hardware and software that can be connected to the corporate environment
- enforce software restriction policies relating to what software is allowed to run in the corporate environment
- record and track the prescribed attributes of assets
- audit and monitor changes in the asset's state and connection
- integrate with log analysis tools to collect and store audited information

3. Business Value

ITAM can be thought of as a foundational part of any security infrastructure: ITAM shows that the highest valued assets have the greatest security controls assigned to them and that everything is configured as it should be.

A properly implemented and administered ITAM system can:

- enhance visibility – know where assets are and how they are configured
- improve asset management by reporting on asset utilization – save money by removing underutilized computing assets
- mitigate operational and regulatory risk by providing better accounting and reporting of assets, thereby reducing opportunities for exploitation
- reveal the software that is actually used, allowing for savings on licenses
- centralize views of enterprise-wide activity and security alerts
- join existing asset management systems with enabling technologies such as automated endpoint visibility, access and security
- allow asset-related questions to be answered quickly and accurately
    - For example, questions such as "Which systems are running Windows 7 SP1?" can be answered in minutes with an ITAM system.

- reduce mean-time to repair due to increased awareness of asset relationships and dependencies

4. RELEVANT STANDARDS

- NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote the protection of critical infrastructure
  http://www.nist.gov/itl/cyberframework.cfm

- ASTM Asset Management Standards
  http://www.astm.org/Standards/asset-management-standards.html

- ISO 55000 International Standard for Asset Management
  http://www.assetmanagementstandards.com/

- ISO Standards for Software Asset Management, ISO/IEC 19770-1:2006 SAM Processes
  https://www.microsoft.com/sam/en/us/iso.aspx

- PAS55 Asset Management
  http://pas55.net/

- ISO/IEC 19770 International Standards about Software Asset Management
  http://www.19770.org

- SANS 20 Critical Security Controls
  http://www.sans.org/critical-security-controls/

- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

5. Security Control Map

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

Example Characteristic		Cybersecurity Standards & Best Practices						
Security Characteristics	**CSF Functions**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27002**	**SANS CAG20**	**COBIT**	**PCI/DSS 3.0**
be capable of interfacing with multiple existing systems	Identify	Asset Management Risk Assessment	ID.AM-4: External information systems are catalogued ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	AC-1 Access Control Policy and Procedures AC-2 Account Management AC-3 Access Enforcement AC-20 Use of External Information System	10.8: Exchange of Information			
complement existing asset management, security and network systems	Identify Protect	Business Environment Access Control	ID.BE-4 Dependencies and critical functions for delivery of critical services are established PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	AC-20 Use of External Information System	10.8: Exchange of Information 11.6: Application and Information Access Control	15 - Account Access Based on Need to Know 16 - Account Monitoring and Control	APO03: Manage Enterprise Architecture	
provide APIs for communicating with other security devices and systems such as firewalls and intrusion detection and identity and access management (IDAM) systems	Detect	Anomalies and Events Detection Processes	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors DE.DP-4: Event detection information is communicated to appropriate parties		10.8: Exchange of Information			

	Example Characteristic		Cybersecurity Standards & Best Practices						
	Security Characteristics	**CSF Functions**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27002**	**SANS CAG20**	**COBIT**	**PCI/DSS 3.0**
	know and control which assets, both virtual and physical, are connected to the enterprise network	Identify Detect	Asset Management Security Continuous Monitoring	ID.AM-1: Physical devices and systems within the organization are inventoried ID.AM-2: Software platforms and applications within the organization are inventoried ID.AM-5: Resources are prioritized based on their classification, criticality and business value DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed	CA-7 Continuous Monitoring CM-3 Configuration Change Control IA-3 Device Identification and Authentication IA-4 Identifier Management SC-7 Boundary Protection SC-30 Virtualization Techniques SC-32 Information System Partitioning	7.1: Responsibility for Assets 7.2: Information Classification	1 - Inventory of Authorized and Unauthorized Devices 4 - Continuous Vulnerability Assessment and Remediation 13 - Boundary Defense 19 - Secure Network Engineering	BAI09: Manage Assets	10: Track and monitor all access to network resources and cardholder data
	detect and alert when unauthorized devices attempt to access the network	Detect Protect	Anomalies and Events Security Continuous Monitoring Protective Technology	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed PR.PT-1: Audit/log records are determined, documented, implemented and reviewed in accordance with policy	AU-2 Auditable Events AU-3 Content of Audit Records CA-7 Continuous Monitoring IA-3 Device Identification and Authentication IA-4 Identifier Management IR-5 Incident Monitoring IR-6 Incident Reporting	10.6: Network Security Management 11.4: Network Access Control	1 - Inventory of Authorized and Unauthorized Devices 4 - Continuous Vulnerability Assessment and Remediation 13 - Boundary Defense 19 - Secure Network Engineering	DSS02: Manage Service Requests and Incidents	10: Track and monitor all access to network resources and cardholder data

Example Characteristic		Cybersecurity Standards & Best Practices						
Security Characteristics	**CSF Functions**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27002**	**SANS CAG20**	**COBIT**	**PCI/DSS 3.0**
integrate with ways to validate a trusted network connection	Identify Protect Detect Respond	Asset Management Access Control Security Continuous Monitoring Protective Technology Communications	ID.AM-1: Physical devices and systems within the organization are inventoried ID.AM-2: Software platforms and applications within the organization are inventoried ID.AM-5: Resources are prioritized based on their classification, criticality and business value PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed RS.CO-2: Events are reported consistent with established criteria	AU-2 Auditable Events CA-7 Continuous Monitoring IA-3 Device Identification and Authentication IR-5 Incident Monitoring IR-6 Incident Reporting PE-4 Access Control for Transmission Medium	11.4: Network Access Control	4 - Continuous Vulnerability Assessment and Remediation		10: Track and monitor all access to network resources and cardholder data
enable administrators to define and control the hardware and software that can be connected to the corporate environment	Identify Detect	Asset Management Security Continuous Monitoring	ID.AM-1: Physical devices and systems within the organization are inventoried ID.AM-2: Software platforms and applications within the organization are inventoried DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed	IA-3 Device Identification and Authentication IA-4 Identifier Management	7.1: Responsibility for Assets 11.4: Network Access Control 11.5: Operating System Access Control 11.6: Application and Information Access Control	1 - Inventory of Authorized and Unauthorized Devices 2 - Inventory of Authorized and Unauthorized Software 4 - Continuous Vulnerability Assessment and Remediation 13 - Boundary Defense 19 - Secure Network Engineering	BAI09: Manage Assets	6: Develop and maintain secure systems and applications

Example Characteristic		Cybersecurity Standards & Best Practices						
Security Characteristics	**CSF Functions**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27002**	**SANS CAG20**	**COBIT**	**PCI/DSS 3.0**
enforce software restriction policies relating to what software is allowed to run in the corporate environment	Protect Detect	Access Control Protective Technology Security Continuous Monitoring	PR.AC-1: Identities and credentials are managed for authorized devices and users **AND SOFTWARE** PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed	AC-16 Security Attributes MP-2 Media Access	10.10: Monitoring 11.6: Application and Information Access Control	2 - Inventory of Authorized and Unauthorized Software	DSS02: Manage Service Requests and Incidents	10: Track and monitor all access to network resources and cardholder data
record and track the prescribed attributes of assets	Detect	Security Continuous Monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed	CA-7 Continuous Monitoring SI-4 Information System Monitoring	10.10: Monitoring		MEA01: Monitor, Evaluate and Assess Performance and Conformance	10: Track and monitor all access to network resources and cardholder data
audit and monitor changes in the asset's state and connection	Detect Protect	Security Continuous Monitoring Protective Technology	DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	CA-7 Continuous Monitoring SI-4 Information System Monitoring	10.10: Monitoring	14 - Maintenance, Monitoring and Analysis of Audit Logs 18 - Incident Response and Management	DSS01: Manage Operations	10: Track and monitor all access to network resources and cardholder data
integrate with log analysis tools to collect and store audited information	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	IR-5 Incident Monitoring IR-6 Incident Reporting	13: Information Security Incident Management	14 - Maintenance, Monitoring and Analysis of Audit Logs 18 - Incident Response and Management		6: Develop and maintain secure systems and applications 10: Track and monitor all access to network resources and cardholder data

Example Characteristic		Cybersecurity Standards & Best Practices						
Security Characteristics	CSF Functions	CSF Category	CSF Subcategory	NIST 800-53 rev4	IEC/ISO27002	SANS CAG20	COBIT	PCI/DSS 3.0
utilizes secure communications between all components	Protect	Protective Technology Data Security	PR.PT-4: Communications and control networks are protected PR.DS-2: Data-in-transit is protected	SC-8 Transmission Integrity SC-9 Transmission Confidentiality SC-12 Cryptographic Key Establishment and Management SC-13 Use of Cryptography SC-17 Public Key Infrastructure Certificates SC-23 Session Authenticity	12.3: Cryptographic Controls	19 - Secure Network Engineering	DSS05: Manage Security Services	4: Encrypt transmission of cardholder data across open, public networks
does not introduce new attack vectors into existing systems	Detect	Security Continuous Monitoring	DE.CM-8: Vulnerability scans are performed	RA-5 Vulnerability Scanning SI-7 Software and Information Integrity SC-3 Security Function Isolation SA-11 Developer Security Testing	12.6: Technical Vulnerability Management	19 - Secure Network Engineering	DSS05: Manage Security Services	6: Develop and maintain secure systems and applications

6. Component List

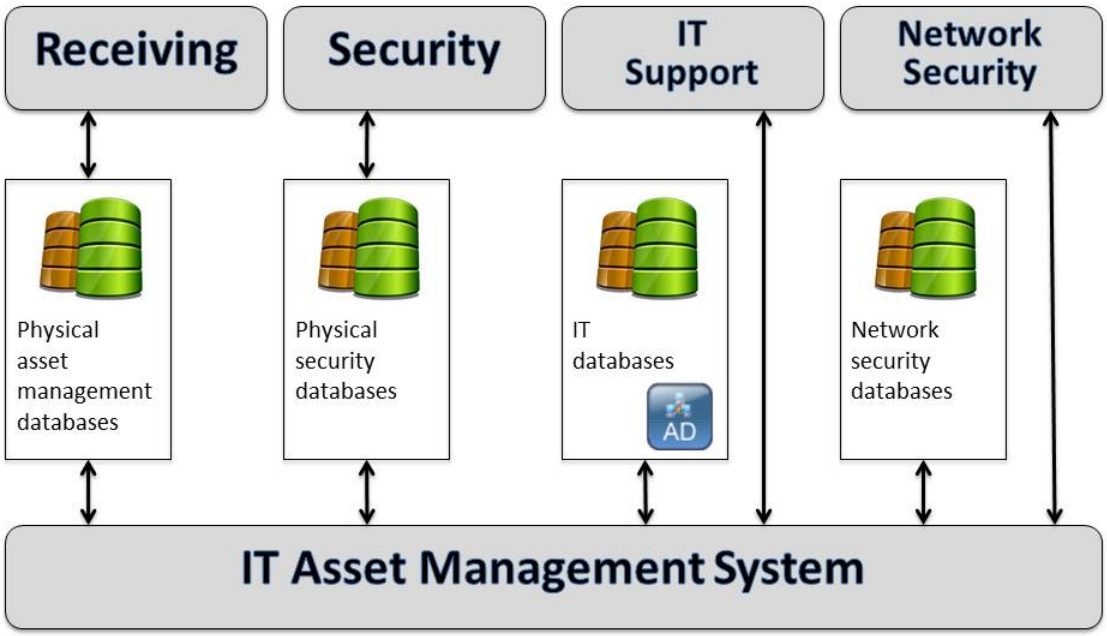
The NCCoE has a test environment for hosting development of the use case including the following features:

- network with machines using a directory service
- virtualization servers
- network switches
- remote access solution with Wi-Fi and VPN

Partners will need to provide any specialized components and capabilities to realize this use case including, but not limited to:

- physical asset management system/database
- physical security management system/database
- multiple virtual testing networks and systems simulating receiving, security, IT support, network security, development and sales departments
- physical access controls with standard network interfaces

7. High-Level Architecture



8. COMMENTS

We received five comments regarding the draft use case. We have provided a response to each comment and revised the use cases accordingly.

1. Provide for collision detection and prevention amongst two changes that share an asset.

   Response: We added the requirement that a central ITAM system should allow for only one owner of an individual asset.

2. Another benefit of a functioning ITAM system is reduced mean-time to repair because of awareness of asset relationships and dependencies.

   Response: We added "Reduce mean-time to repair due to increased awareness of asset relationships and dependencies" to the Business Value section at line 133.

3. Support data as an asset.

   Response: We added "fine-grain asset accountability supporting the idea of data as an asset" to Desired Solution Characteristics at line 105.

4. Include support for relationships outlining components of a service or application, e.g., hardware, software, connectivity and data.

   Response: This document already mentions hardware, software and data. The connectivity portion will be addressed by the upcoming Software Asset Management building block (http://csrc.nist.gov/nccoe/Building-Blocks/conmon.html), and a follow-on version of this use case will provide a "real-time" view of connections.

5. Provide for automated asset discovery and the ability to deal with restricted parts of a network

   Response: We have added this to the desired solution characteristics, modifying line 106 to read: "automatically detect and alert when unauthorized devices attempt to access the network, also known as asset discovery."