Software Asset Management (SWAM) Capability Description

Purpose

Provides an organization visibility into the software installed and operating on their network(s) so they can appropriately manage authorized software and remove unauthorized software. It also provides a view of software management responsibility (i.e., who patches the software, who configures the software, who decides what versions are allowed for the organization) such that prioritized defects can be presented to the responsible party for mitigation actions and risk acceptance decisions. This capability is dependent on the existence of a set of device roles defined for the D/A and an authorized hardware inventory as developed for the Hardware Asset Management Capability.

How does it work?

Proper management of software assets begins with lists of authorized (whitelist) and unauthorized (blacklist) software products and executables. Some lists, like known bad executable files may be defined globally, while others like authorized software products are defined per device role. The D/A actively monitors the network for software installed or executing on devices, by hash-type signatures and other residual information in the system such as registry entries, filenames, or running processes. This is compared against the authorized software inventory for that device. If a piece of software is not authorized for use, the D/A will mitigate the risk by either removing it or properly authorizing the software for use. If the software is explicitly blacklisted, then the D/A will mitigate the risk by removing the software.

Special software –anti-malware or antivirus – is installed on devices to detect (and if configured to do so, protect against) known malicious and other unauthorized software (as defined by the D/A) from being downloaded, existing on the device, or executing. SWAM also ensures that lists or signatures used by this special software are kept up to date in accordance with the D/A's policy.

Additionally, any discovered software that is not explicitly listed in the D/A's whitelist or blacklist will be initially placed into a graylist. Software included in the D/A's graylist will either be treated-as-authorized and be permitted to remain installed on the device until authorization is determined, or treated-as-unauthorized and uninstalled until authorization is determined. Items on the graylist must be moved to either a whitelist or a blacklist within some time frame, ensuring that the D/A continues to improve upon this capability.

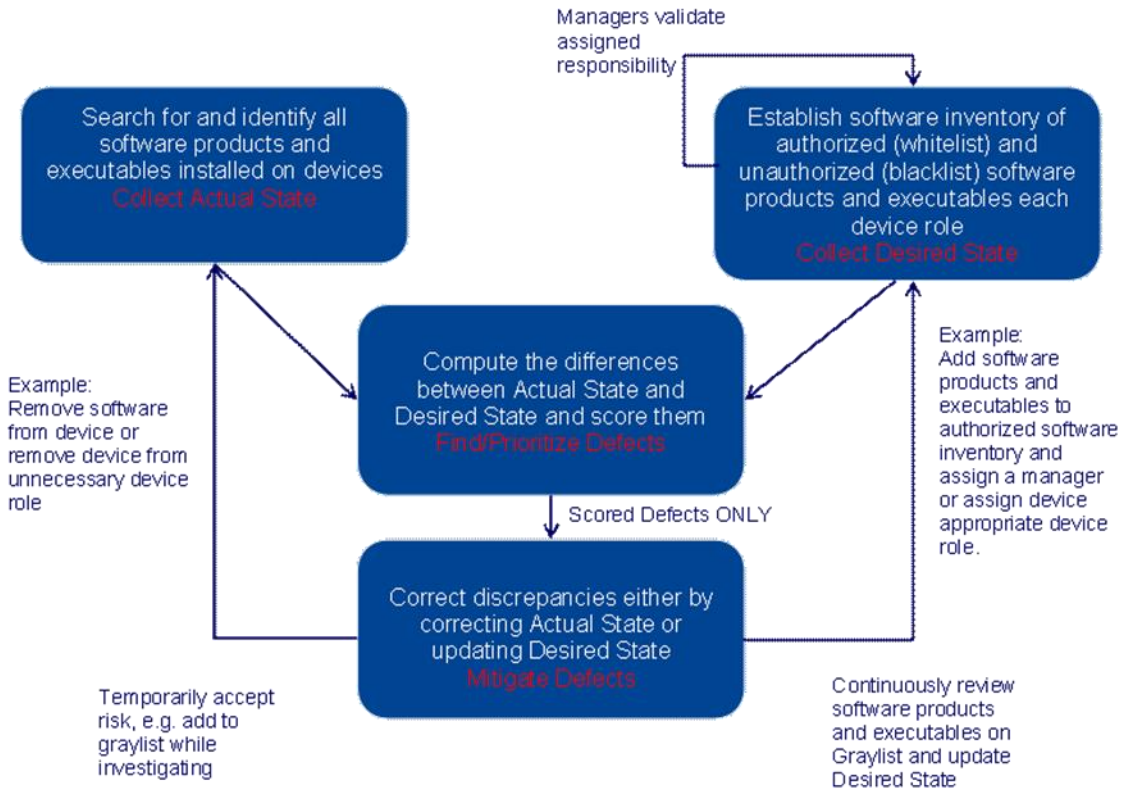

Figure 1 The SWAM Capability Process

How does the lack of software asset management impact the network?

Attackers continually scan for software that they can exploit to gain control of and use to access other devices, accounts, and data. If the D/A is unaware of software running on the network, they are unlikely to maintain proper security updates and configurations, increasing the likelihood of successful attack and compromise. In addition, attackers develop malicious software (malware) to be installed on information systems by unsuspecting users, which can then be used to compromise the network. Additional attack vectors are exposed if software authorized for one type of device, such as a web server, is installed on a device for which it is not intended, such as a workstation.

Collect Actual State

Use tools to collect information about what software is actually present on each device on the network. Methods to detect software (when it was first seen, and when/where it was last seen) include (but are not limited to)[1]:

---

[1] While passive listening to collect application information from traffic from devices (i.e., banner grabbing) can be used, the information collected is often not specific or accurate enough to identify a software product down to the required version/patch level for use in SWAM.

- Active methods (e.g., credentialed scanning software) to collect data from the device[2]
- Active agents on the device to detect, collect, and report data on installed software, files, and processes

The CDM process will identify the software assets actually on the network and can provide the information required to compare them with the authorized software inventory. Also, you will need to identify how much of the network is being monitored to discover the software installed on it.

Collect Desired State

There are multiple Desired State specifications required to efficiently and effectively monitor software authorization processes and detect unauthorized software. The first Desired State specification is a listing of the authorized device roles to include any hierarchy that may be defined for the device roles. The second Desired State specification is a listing of all software authorized for any system in scope at a D/A. The third Desired State specification lists all mutually exclusive device roles as defined by policy. For example, the D/A has a policy that states that the same device cannot be both a web server and a user workstation.

The forth Desired State specification lists the software profile for each device role. The software profile includes authorized firmware, software products, and executable files for the associated device roles. The software profile also includes blacklists of specifically prohibited software that are defined or identified to assist in rapid decision-making during the identification and remediation process. There will most likely be two types of blacklists, one containing prohibited software products and the other containing known malware or known bad executables. The prohibited software products blacklist is created and maintained by the organization to explicitly state products and versions that are not allowed by policy (i.e., WindowsNT or Adobe Acroread versions 8 or below). The known malware blacklist is usually maintained by an antivirus/antimalware vendor and continuously kept up to date with all the latest known bad signatures.

The fifth Desired State specification lists the device role combinations that result in a modification to any software profile and the rules associated with those modifications. For example, the software profile for both file servers and web servers state that the antivirus signature file must be updated every 24 hours, but if a device is both a file server and a web server, then the antivirus signature file must be updated every 12 hours.

The final Desired State specification is a listing of all authorized devices and their assigned device roles.

Diagnose (By Finding and Prioritizing Defects)

Comparing the list of software discovered on a device with the appropriate software profile(s) for that device will identify unauthorized software that needs to be addressed. Verifying that all the appropriate Desired State specifications exist and are updated according to policy will identify any issues with the

[2] Data collected from the device to determine the presence of software is in SWAM. Passive listening to traffic from a device to identify malware-related communications are not in SWAM but in other CDM capabilities.

software authorization and device role assignment processes that can create an additional security risk. Additional defects related to software management (e.g., mandatory software) may be defined by the D/A. See the Defect Type Table for a list of general SWAM defects. After these conditions are detected, they will be automatically scored and prioritized (using federal and D/A defined criteria)[3].

Mitigate Defects

The CDM dashboard will generally be organized to show worst problems first. Worst problems should be mitigated first. The following table shows the most important defect types and mitigation options. The full set of Defects and mitigations are documented in the *Software Asset Management Datasheet*.

Defect Type	Detection Rule	Mitigation Options
Unauthorized Software	In Actual State but not in Desired State	• Remove Software • Authorize Software OR • Accept Risk
Unmanaged Software	In Actual State and in Desired State but no "appropriate" manager assigned	• Remove Software • Assign Software OR • Accept Risk
Device Role Policy Violation	Actual State less secure than Desired State	• Remove device from incompatible device role OR • Update policy OR • Accept Risk
Blacklist is out of date.	Actual State less secure than Desired State	• Update the blacklist for the device OR • Restore updating process OR • Remove device OR • Accept Risk
Non-reporting	Actual State data unavailable	• Deploy collection capability OR • Restore collection OR • Remove device OR • Accept Risk

[3] Many defects will have a "grace period" built into the scoring function. For CDM, these grace periods are calculated from the time the defect is first identified, not when the desired state specification or actual state changed.

Appendix A - Definitions

Term	Definition
Authorized Hardware Inventory	List of authorized hardware assets for an organization or subnet.
Authorized Software Inventory	Managed whitelisted and blacklisted software for the organization and each device role.
Blacklist	List of unauthorized software for a D/A or device.
Common Platform Enumeration (CPE)	Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.[4]
Defect	A condition where the Desired State specification and the Actual State do not match in a manner that incurs risk to the organization.
Device	IP-addressable asset on the network or a non-addressable component (e.g. removable media) able to interact with the D/A's data and resources.
Device Role	An enterprise-wide label for a business or mission function that is associated with D/A-defined information technology assets. The device role is intended allow the refinement of authorization policies related to hardware and software in a manner that ensures that they are appropriately addressing mission needs/risks.
Executable file	For CDM, a specific file in persistent memory that can be loaded into active memory and executed by the CPU.
Graylist	List of software not authorized, but not explicitly prohibited.
Hardware Asset Management (HWAM) Capability	The Continuous Diagnostic and Mitigation (CDM) capability that ensure unauthorized and/or unmanaged hardware is removed from the organization's network, or authorized and assigned for management, before it is exploited, compromising confidentiality, integrity, and/or availability.
Scoring	The process of calculating the risk points for a defect. Identified defects will be "scored" based on the amount of perceived risk they create. The CDM program will be providing a scoring system that is generic across D/As. Each D/A may adapt this with additional D/A specific information to better prioritize defects for action.
Software	For CDM, software includes firmware, basic input/output systems (BIOS), operating systems, applications, services, and malware such as rootkits, trojans, viruses, and worms.

[4] http://nvd.nist.gov/cpe.cfm

Term	**Definition**
Software Asset Management (SWAM) capability	The CDM capability that ensures unauthorized and/or unmanaged software is 1) identified, 2) authorized, and 3) assigned for management, or 4) removed before it can be exploited compromising confidentiality, integrity, and availability.
Software identification tag (SWID)	Software ID tags provide authoritative identifying information for installed software or other licensable item.[5]
Software product	The level of abstraction by which software is typically licensed, listed in registries during installation, and executed by users. Software products are roughly equivalent to the software identified by the NIST Common Product Enumeration (CPE) codes, and also by the ISO SWIDs.
Whitelist	List of authorized software for a D/A or device.

[5] ISO/IEC 19770-2: Software identification tag