Requiring Electronic Identification Data

The issue of identifying software is slightly different from managing entitlement data. Currently, when SAM tools do inventory, they return various details about the software that is installed on the devices within an organization, however this information can vary from release to release and is not consistent between vendors and often is not consistent even between products from the same vendor. SAM tools use libraries to translate the granular inventory data into software product names that relate to what the organization licensed. Although the paper is older, TagVault.org did a review of application recognition libraries and identified that these libraries were very inconsistent in providing correct results (see http://tagvault.org/wp-content/uploads/2013/02/analysis-of-software-identification-tools.pdf).

This inconsistency applies to much more than the requirements of an effective SAM program – it has a direct and negative impact on cybersecurity for an organization. The National Institute for Standards and Technology (NIST) has been part of the team developing the ISO standards for SAM because the data needed by SAM tools is a huge benefit for more effective Cybersecurity (See – **Error! Reference source not found.** – below)

There is an ISO standard, *ISO/IEC 19770-2:2015, Part2: Software Identification Tag* that provides the exacting detail required to more fully automate SAM functions. This standard specifies exactly what a software vendor needs to provide as a file embedder with their product for a product identification that will link software product inventory automatically to software entitlement data as well as to the national vulnerability database.

In terms of market support for SWID tags, IBM is currently providing SWID tags with every product released and Microsoft provides SWID tags with some of products they release. Red Hat is supporting SWID tags and have a utility that can convert RPM installation data to a standard SWID tag for consumption by inventory tools. Finally, all 3 major Windows based software installation script creation tools (Advanced Installer, InstallShield and WiX) support the creation of SWID tags, in most cases the tags are created by default. This means that there is generally no extra work for vendors developing Microsoft software to create SWID tags.

The following terms should be included in software contracts to ensure that the organizations receive SWID tags embedded in all software products:

> Offeror agrees to include the International Organization for Standardization/International Electrotechnical Commission 19770-2 (ISO/IEC 19770-2:2015) standard identification tag (SWID Tag) as an embedded element in the software. An ISO/IEC 19970-2 tag is a discoverable identification element in software that provides licensees enhanced asset visibility. Enhance visibility supports both the goals of better software asset management and license compliance. Offerors may use the National Institute of Standards and Technology (NIST) document “NISTIR 8060: Guidelines for Creation of Interoperable Software Identification (SWID) Tags,” December 2015 to determine if they are in compliance with the ISO/IEC 19770-2 standard.
>
> Note, the NISTIR 8060 can be found here - http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8060

Including the above terms in software purchasing agreements will:

- Ensure that software inventory systems properly identify products that are installed on a device rather than taking an archeological approach to product identification and trying to deduce the best guess from inventory of various components.

- Ensure that all details about the software product are known (publisher, product name, edition colloquial version and full product version). This data is critical to security products and is often not available to those products either.

- Ensure that all details about the software product are canonical since they are provided by the publisher.

- Ensure that the products identified on devices will have a direct association with the entitlement data included in the publisher provided 19770-3 entitlement schema.

Requiring Electronic Entitlement Data

Dealing with hundreds of thousands of rows of data and relying on manual data entry puts the purchasing organization at a severe disadvantage. In today's economy, software entitlements are one of the last hold-outs of data that is being handled manually.

Many of the larger software vendors either have or are building portals where a customer may be able to view the entitlements they have licensed. These portals are unique for every vendor (and often, there will be multiple different portals per vendor) and they do tend to be modified over time as the vendors especially as metrics are modified. This means that the customer is again responsible for interpreting the data from the vendors portal and manually entering it into the SAM tool.

There is an international standard defined that will provide all the entitlement data required by the SAM tool in a completely automated manner. The standard is *ISO/IEC 19770-3:2016, Part 3: Entitlement schema* and this schema has been tested by large software vendors to ensure the schema supports the wide range of metrics that are used currently, including those metrics that apply to cloud and service-based environments.

To ensure that entitlement data is provided – either directly as part of the purchase, or potentially as an export from the software vendors portal, all software contracts should include the following requirements:

> Offeror agrees to provide entitlement data for every software purchase using the International Organization for Standardization/International Electrotechnical Commission 19770-3 (ISO/IEC 19770-3:2016) entitlement schema. The ISO/IEC 19970-3 enables automatic importing of licensed entitlements into software asset management tools which provides more automated and significantly more accurate software asset management and license compliance processes.
>
> Offerors must provide Entitlement data that adheres to the requirements in Section 5 Interoperability as well as providing all required elements as Identified in section 8.6.1 Requirements Levels with M1 requirements being common to all entitlements and M2 requirements being Mandatory in the context of the element.
>
> Offerors may provide Entitlement data at the time of the purchase or allow the customer to export their entitlement data from an Internet portal, or both. If access is provided via an Internet Portal, access to the 19770-3 Entitlement Schema data must also be available via a well-documented programmatic means.

Including the above terms in software purchasing agreements will:

- enables a much more automated approach to accessing entitlements, removing the manual and often error prone manual data entry that is done today

- ensures that the vendor and the customer are working from the same set of data, allowing the customer to validate that the vendor entitlement matches what the organization licensed

- lowers the cost of managing a SAM program significantly because a SAM tool can automatically download and validate entitlement data from vendors who provide licensing portals

- Increases the value customers receive from their SAM tools because general SAM reports and license compliance reports are significantly more accurate.