GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Warne, Dallin

"How-to: NIST Asset Management & Inventory (ID.AM-1 & ID.AM-2)"

Dallinwarne.com

20 December 2017

URL: dallinwarne.com/security/nist-asset-inventory/

Accessed: 04 June 2019

Synopsis: Imagine security analysts easily finding answers to questions about your organization's network such as: What devices have port 445 enabled? What servers are running an old version of Apache? How many web cameras are on our network? Envision automatic notifications when outdated or vulnerable software is detected in your organization! That's the value of the NIST asset inventory in the cybersecurity framework.

How-to: NIST Asset Management & Inventory (ID.AM-1 & ID.AM-2)

DECEMBER 20, 2017 / DALLIN WARNE / 0 COMMENTS

Imagine security analysts easily finding answers to questions about your organization's network such as: What devices have port 445 enabled? What servers are running an old version of Apache? How many web cameras are on our network? Envision automatic notifications when outdated or vulnerable software is detected in your organization! That's the value of the NIST asset inventory in the cybersecurity framework.

Introduction to NIST Cybersecurity Framework

The NIST cybersecurity framework is powerful, but many organizations struggle with adopting it. A lone cybersecurity professional may be overwhelmed with how much the NIST cybersecurity framework asks, and the sysadmin wanting to bolster his systems' security may find it too much to sift through. In reality, most security-conscious professionals want to follow best practices, but don't know how to specifically in their organization. Unlike most technical problems, you are unlikely to find a quick answer to a Google search specific to your situation.

This article is Part 1 in a series is designed to help people get started or find a practical approach to the Identify category in the NIST cybersecurity framework. Yes the framework is technology and policy neutral, but it can be time-consuming and difficult for some to bring the abstract to concrete systems for an organization. By giving examples and exploring technical architectures, professionals can learn how to better aligned with NIST.

Let's now examine the Identify Asset Management (ID.AM) category. This is where:

1. Physical devices and systems within the organization are inventoried
2. Software platforms and applications within the organization are inventoried
3. Organization communication and data flows are mapped
4. External information systems are catalogued
5. Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value

6. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

The purpose of the Asset Management category is to help cybersecurity professionals know what computers (in full sense of the term) is in their organization, what's happening on and between those computers, find a way to classify them, and figure out who will be in charge or responsible for what. This article will examine ID.AM-1 and ID.AM-2.

Possible Solutions for Asset and Software Inventory

For a small organization of just a few employees and assets, a simple spreadsheet and a day's work can adequately catalog the assets and software. But that doesn't scale to larger enterprises, nor does it keep an inventory automatically updated.

Of course, one could purchase a solution that helps track IT assets. Perhaps the organization already has software that stores licenses, warranties, location, etc. This is a good start, but don't settle for just a supposed all-in-one solution or else you are going to miss something and fail down the road. Worse, it can give you a false sense of security. These types of solutions can track managed devices, but what about the unmanaged or unknown devices especially BYOD or IoT devices? As CIS control #1 and #2 say, you need an "Inventory of authorized and *unauthorized* devices… and software."

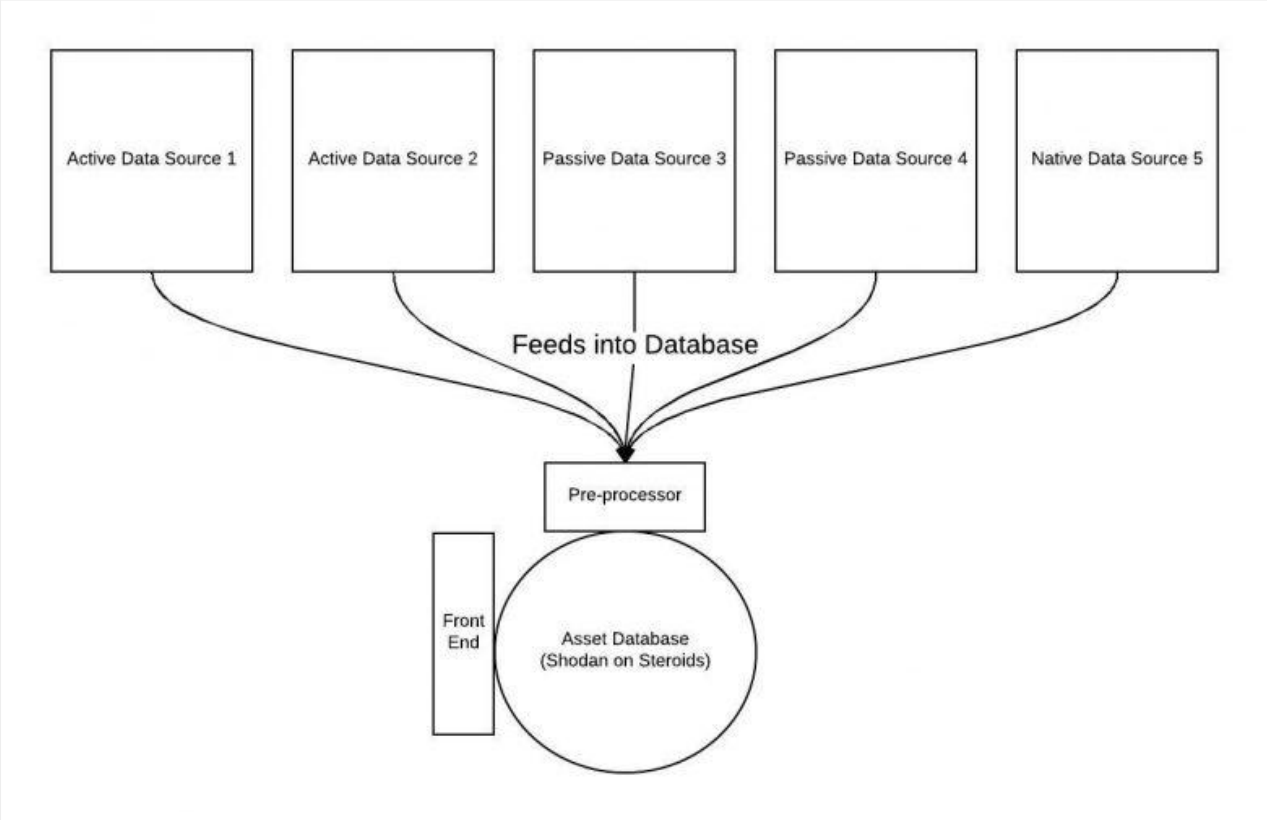
What does it take to identify all assets? As much data as possible from as many sources as possible automatically combined together into an easily-usable centralized repository. Get data out of the silos of various applications and systems, and into a centralized database. It will take work, but the reward is a more complete picture of what's on the network, what's accessing your systems, what software is being used, and what users are involved. There isn't an all-in-one solution (that I'm aware of at this time of writing) that can take data from disparate sources to form an asset identity.

What you do and how well you implement an asset inventory and software inventory (ID.AM-1 and ID.AM-2) will correlate to the success of the other phases. All other

categories and functions depend on identifying what's in your organization. You can't protect what you don't know, and you can't make sound decisions based on half-truths.

Design Phase for an Asset Inventory

Just as companies create structures from blueprints, cybersecurity personnel need to plan and architect an inventory system. What you are building is the ultimate asset and software inventory, a Shodan.io or Censys.io on steroids. Take a look at the generic diagram below. It's high-level view gives a minimal picture of the what to be working towards.



Pull in data (logs, configuration files, etc) from as many sources as you can get your hands on. The more data sources you have, the more complete your inventory will be. Remember, security should be layered. If, for example, you have both firewall and intrusion detection system logs, include both!

The data gets sent to some type of pre-processor that gives context or adds metadata to the data being sent before inserting that data into a database. Unfortunately, the pre-processor is the piece of the system where there are few, if any, tools readily available. An example of what the pre-processor does is when it receives a log from a

server that includes an internal IP address. The pre-processor can takes the IP address from that log, lookup the hostname or better yet look it up in Active Directory, append the information, and send it on to the database/inventory. If the device has to be registered before accessing the network, add the owner's IT support contact. Now instead of just identifying a possibly dynamic IP address, you are building an identity around the device and maybe even the user. The device identity from the inventory can then be accessed on a front-end.

There are many types of front ends available already. Kibana is popular for Elasticsearch, but you can find other front-ends for other database management systems as well.

It is important to realize that this database isn't just your SIEM or central logging system, although in a select few organizations it could be and in many others it will be integrated with one. Network systems are dynamic, and you won't see every characteristic of a device all at once. The inventory system needs to be able to track these traits even as devices move to different networks, open or close ports, remove or install software, and so forth. You won't know what device performed actions across multiple log sources just throwing in logs into one place.

Data Source Types

A good asset inventory will include data from different types of sources. There are three classifications of data sources:

- Active
- Passive
- Native

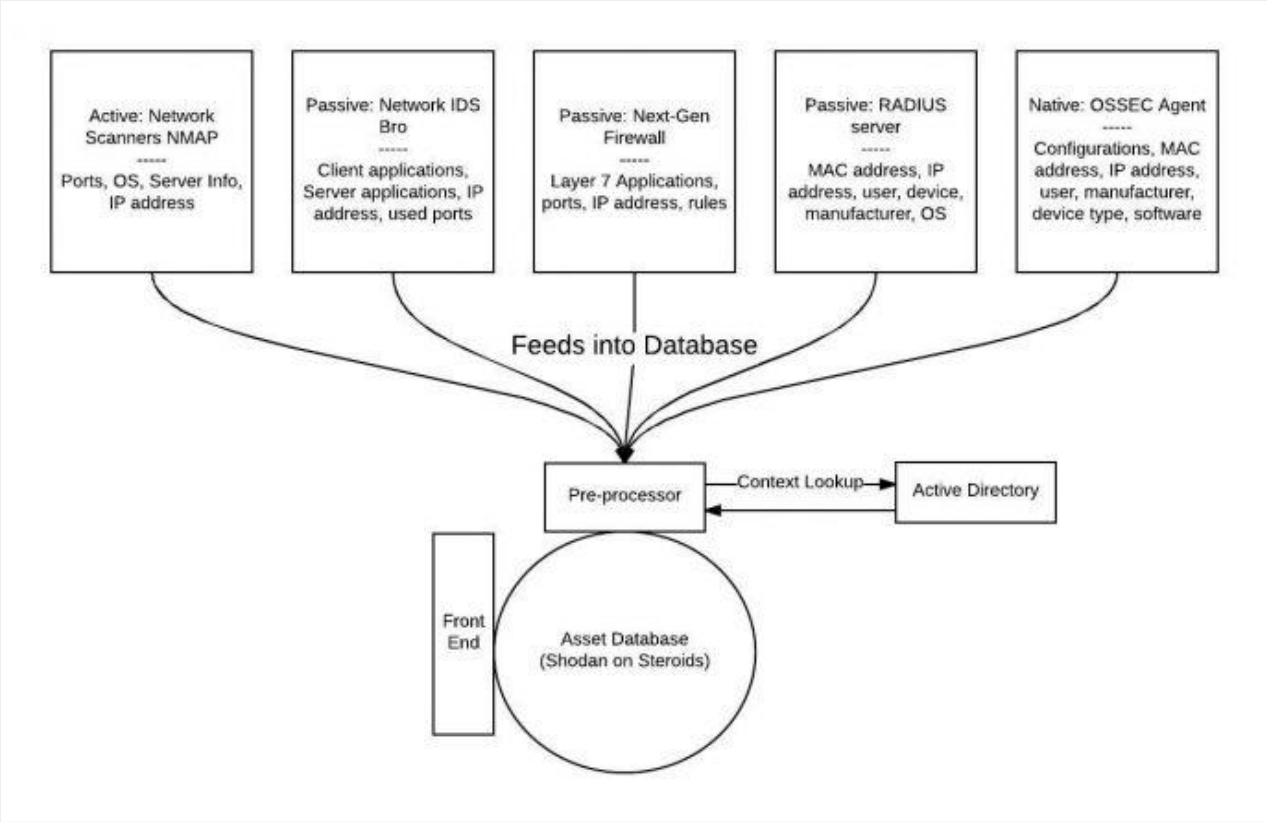
An active data source is an application that takes action directly with a service to determine a status. For example, a network scanner scans (an action) a computer to determine what ports are open.

A passive data source is an application that doesn't interact with a system, but watches to determine a status. An example would be a firewall that logs (passively watches) a connection containing what port is being used.

A native (and perhaps there could be a better name for it) data source is some type of application that reports a status. Two examples are an SNMP trap fires off a log, or a server reporting a list of open ports from its configuration settings. Some might argue this is really an active data source, but it is a component that does not interact with the provided service to gather its data.

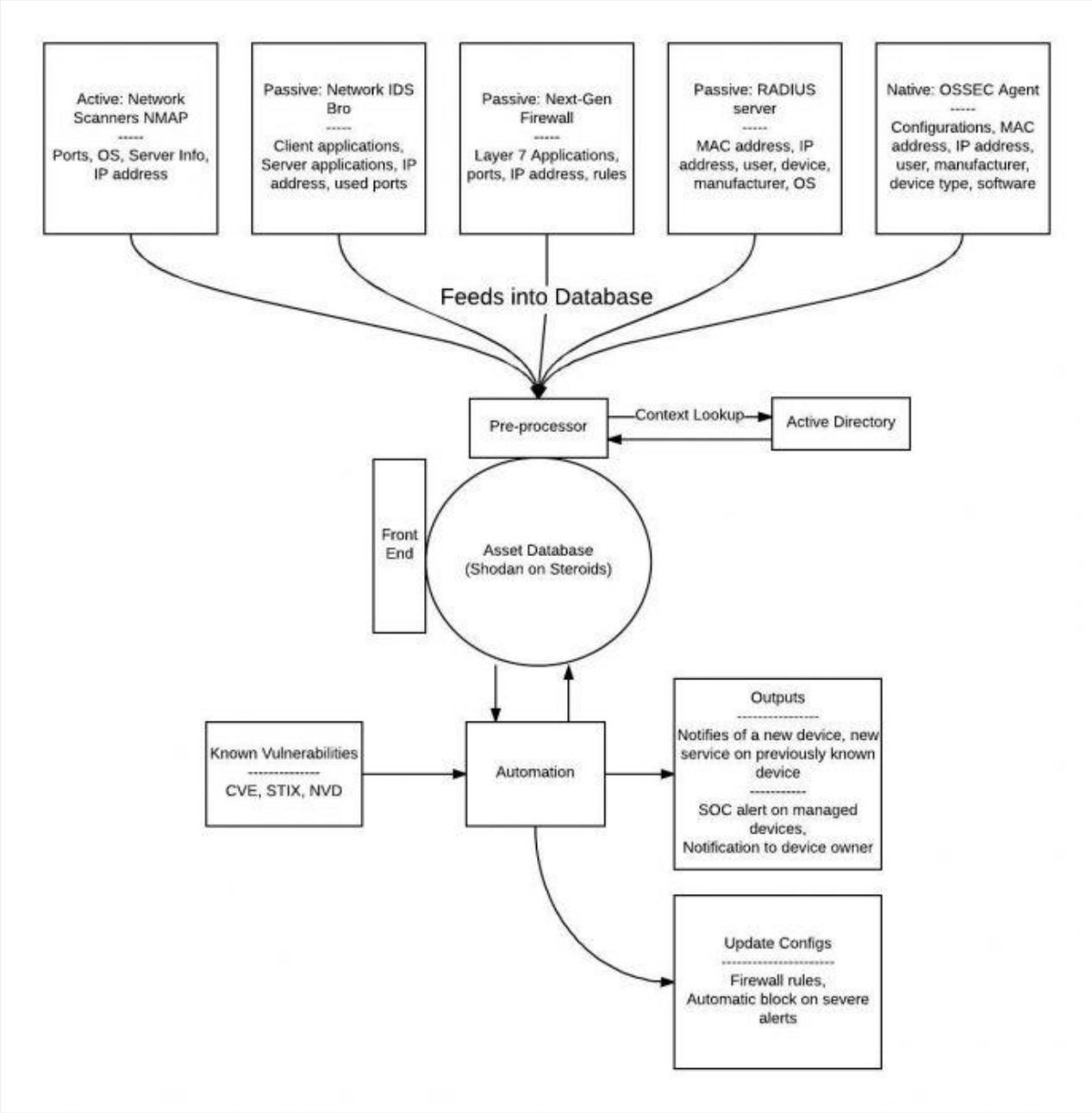
Note that each one can provide information that the other might not be able to provide. All three are needed for verification. For example, a port scanner might not detect a server port is open. The passive firewall sees a connection to that port. Who is lying? By checking the native server configuration, an IP table shows up accepting connections from only a single IP address. Another scenario along these same lines is the native server configuration is reporting a port is open, but the scanner or firewall can't reach it.

The diagram below exemplifies what an organization's inventory architecture might look like and the data points each source contributes.



Utilizing the Asset Inventory

Once the inventory is automatically populated and updated, NIST encourages you to take advantage of it! Perhaps your organization has a policy banning certain software. Incorporate a script that checks the inventory against the list of banned software and response in someway, such as alert you or the asset owner when something is detected. A similar script can check servers against expected or baseline configurations, check for CVEs, or find services that should not be enabled. An analyst can find answers to questions such as, What devices have port 445 enabled? What servers are running an old version of Apache? How many web cameras are on our network?



Identify Asset and Software Inventory Gaps

By adding your data sources and their types to the diagram, you start to see what information you have available to you, and where you might be lacking. You can start considering options to obtain the additional information you need, or accept that you can live without that data move on. Knowing what you have missing instead of believing that you have something when you do not will prevent issues down the road.

NIST Security Control Catalog

CM-8 is the section in the NIST Security Control Catalog that describes what to do to meet ID.AM-1 and ID.AM-2. You can see how the architecture and components described in this article can meet each point in CM-8, which are referenced below.

Implement Priority 1. Low: CM-8. Mod: CM-8 (1) (3) (5). High: CM-8 (1) (2) (3) (4) (5)

- **CM-8 (1):** The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.
- **CM-8 (2):**The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.
- **CM-8 (3)**:The organization:
  - **(a)** Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the
    information system; and
  - **(b)** Takes the following actions when unauthorized components are detected: [Selection (one or
    more): disables network access by such components; isolates the components; notifies
    [Assignment: organization-defined personnel or roles]].
- **CM-8 (4)**:The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name;

position; role], individuals responsible/accountable for administering those components.

- **CM-8 (5):**The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories
- **CM-8 (6):** The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.
- **CM-8 (7):** The organization provides a centralized repository for the inventory of information system components
- **CM-8 (8):** The organization employs automated mechanisms to support tracking of information system components by geographic location.
- **CM-8 (9):** The organization:
  - **(a)** Assigns [Assignment: organization-defined acquired information system components] to an information system; and
  - **(b)** Receives an acknowledgement from the information system owner of this assignment

For further reference and generating ideas to help build an asset and software inventory, check out the National Cybersecurity Center of Excellence (CCOE) IT Asset Management Practice Guide. It gives a practical, in-depth and vendor-specific example for both an executive and an engineer.

Keep an eye out for the next article that addresses the remaining subcategories of asset management.

Security

ASSET INVENTORY ID.AM NIST