Enabling Better Security Automation by Adding Context

National Cybersecurity Center of Excellence

Increasing the deployment and use of standards-based security technologies

September 9, 2015

Michael Stone
Michael.Stone@nist.gov

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

INTRODUCTION AND OVERVIEW

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

Standards-based

Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards

Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions

Commercially available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry

Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results

NATIONAL CYBERSECURITY EXCELLENCE PARTNERS

Overall Goal:

To automate the remediation of policy violations

(Yes, attacks are policy violations)

How:

- Write policy based on business assets and rules
- *Gather accurate data regarding assets*
- *Monitor and collect accurate data regarding activity (including attacks)*
- *Put activity into context of business assets*
- Remediate based on business policy rules

Italics = included in this project

The situation:

Everything can generate logs/messages.
Most people enable logging.
Most organizations forward logs to a central location.
Most organizations archive their logs.
Hardly anyone reads or analyzes their logs.

Most analysis is done during a forensic investigation after everything has already been stolen.

Why:

I have more important stuff to do
There are so many log entries

thousands = needle in a haystack problem

They all look different (multiple syslog formats, common log format, CEF, extended log format, etc.)

"The nice thing about standards is that you have so many to choose from." - Andrew S. Tanenbaum (https://en.wikiquote.org/wiki/Andrew_S._Tanenbaum)

You can't protect what you don't know about:

- If you don't know that you have a machine how can you be expected to know how it is configured, what it is doing or if it is secure.
- Likewise, if you don't know how a machine is configured and operating how can you be sure that it is compliant to your policies.
- Proper asset management also allows for better utilization of assets.

Fundamental to everything else:

- NIST Cybersecurity Framework *(http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf)*
  - Identify.Asset Management (ID.AM)
- SANS Critical Security Controls *(https://www.sans.org/critical-security-controls/)*
  - Inventory of Authorized and Unauthorized Devices
  - Inventory of Authorized and Unauthorized Software
  - Secure Configurations for Hardware and Software…

CYBERSECURITY FRAMEWORK CORE

Function	Category	Subcategory
Identify (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	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-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources are prioritized based on their classification, criticality and business value
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established

Goal:

The goal of this project is to connect 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.

Status:

Integrating, testing and documenting. Developing analytics, dashboards and demos.

11 companies working with us on this use case.

15 products installed and integrated.

Practice guide is due in September

Definition: The circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood and assessed.[1]

Synonyms: circumstances, conditions, factors, state of affairs, situation, background, scene, setting[1]

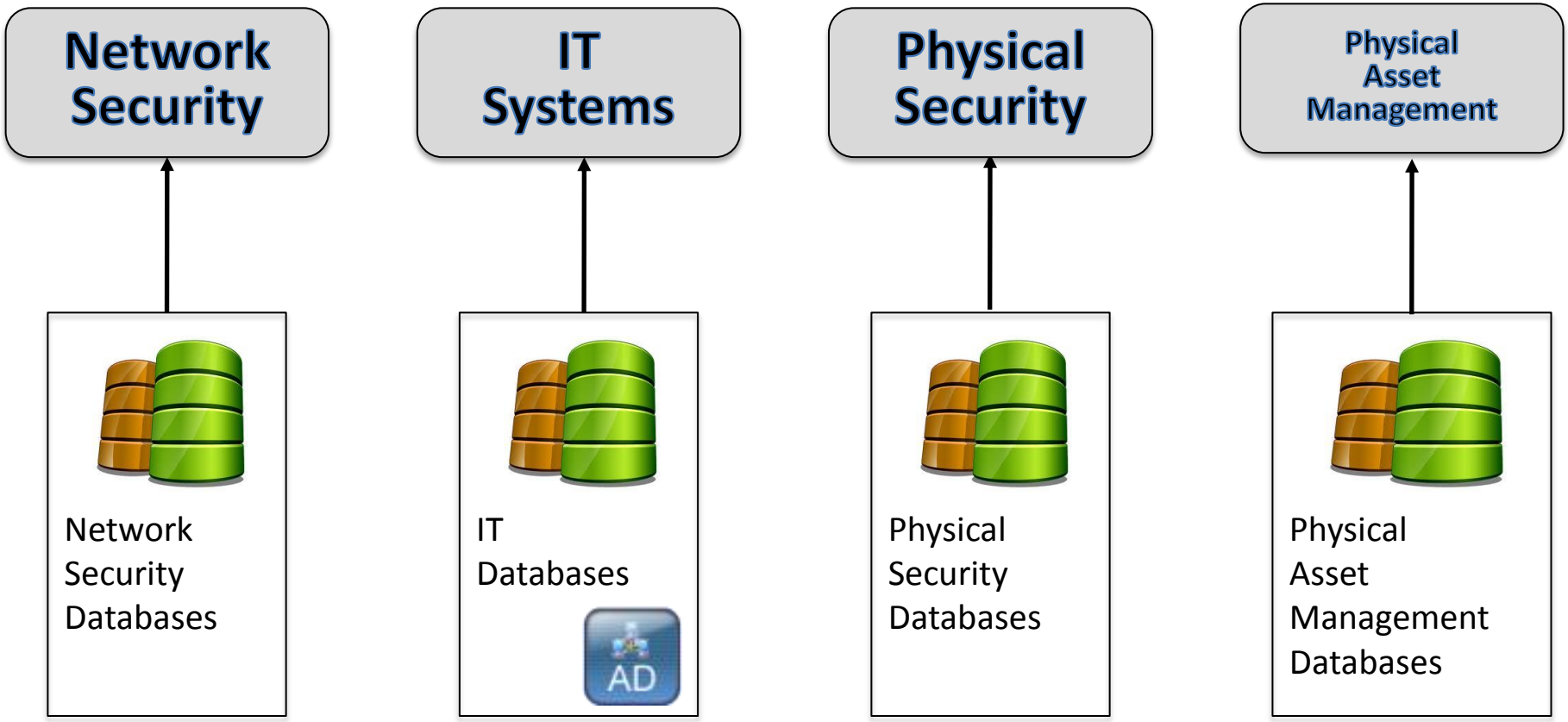
Context Examples

- Machine state: up, down, configuration, hardware, software
- Recent changes
- Ownership and location information
- Known vulnerabilities
- Recent events
- Uniqueness
- Value (basic $ and business value)

[1]http://www.oxforddictionaries.com/us/definition/american_english/context

CURRENT STATE

Most of the information required for ITAM and security automation is there but in separate silos. Information sharing is the key to better visibility and situational awareness.



Example alert from Snort:

11/05-22:08:59.705515 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak][Priority: 2] {ICMP} 192.168.206.129 - 192.168.100.5

Information:

Timestamp = 11/05-22:08:59.705515

Rule number = 1:469:3

Description = ICMP PING NMAP

Classification = Attempted Information Leak

Priority = 2 (Note: priority 1 is the highest)

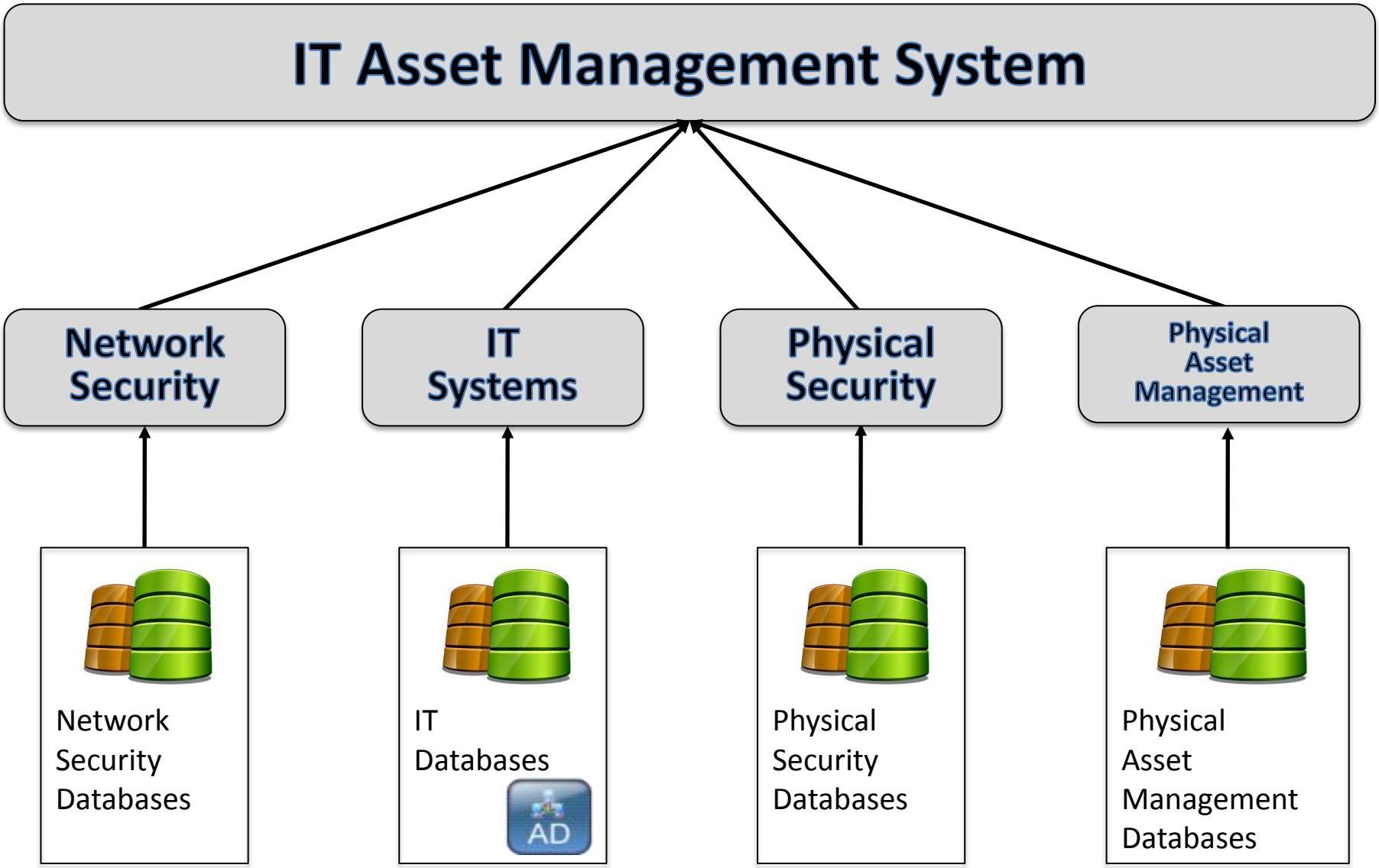
Protocol = ICMP

Source IP address = 192.168.206.129

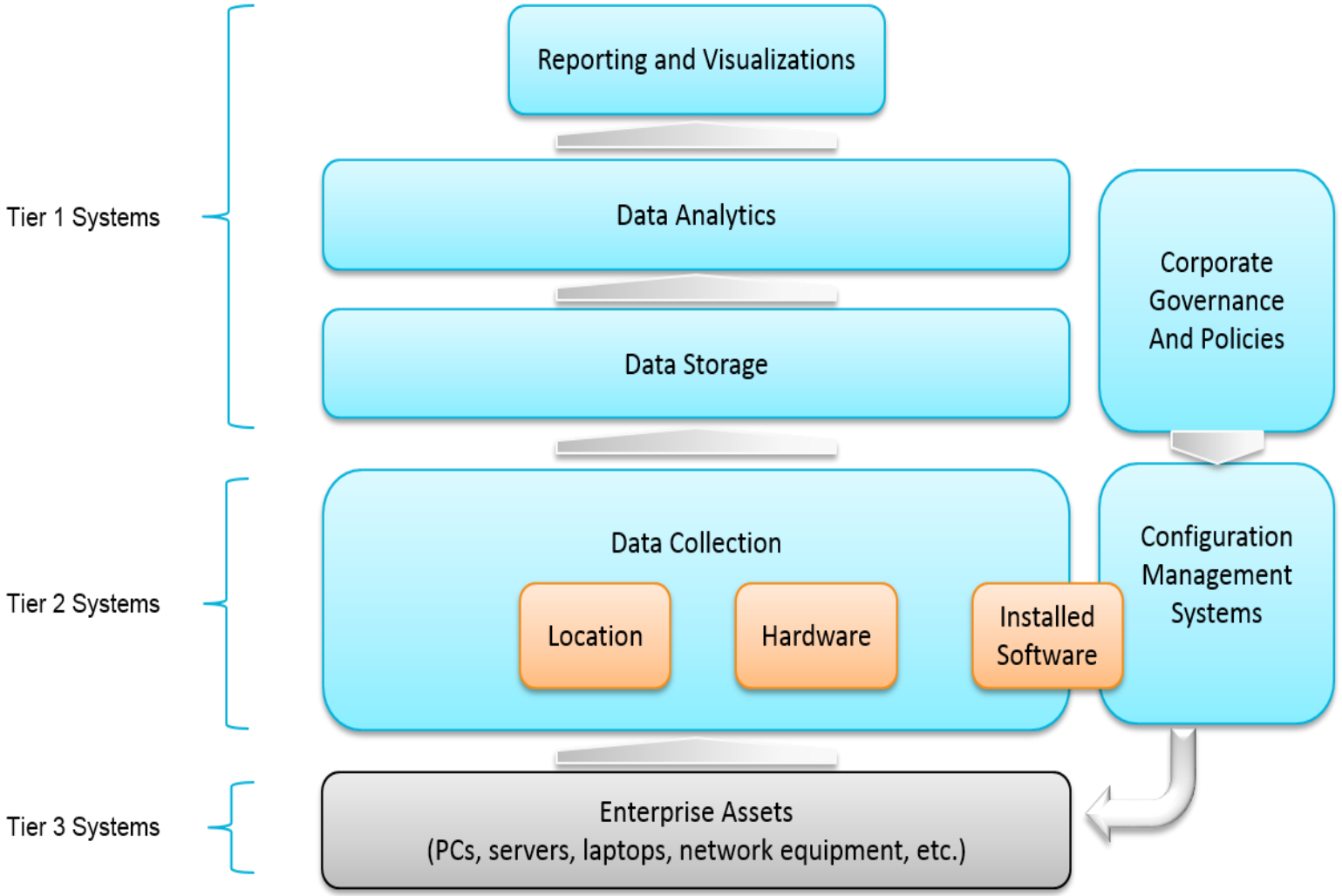
Destination IP address = 192.168.100.5

BETTER STATE

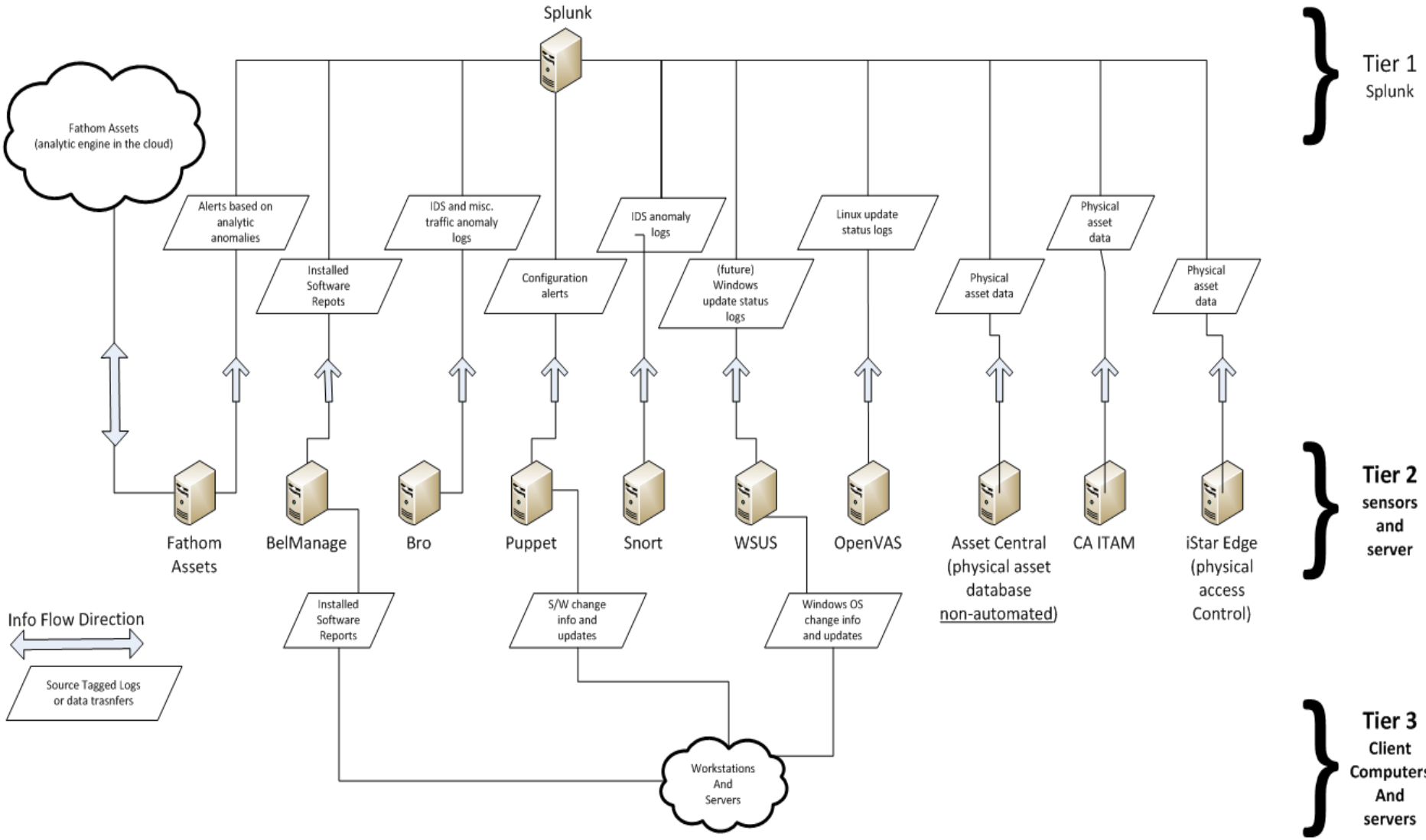
Data is sent to a centralized location for analysis and reporting.



DATA TO INFORMATION FLOW



ALL OF THE PARTS WORKING TOGETHER



Each asset needs to be assigned a value:

Not something like Server42 = $1000

More along the lines of Server42 = **HIGH** because it is running the consumer facing web server virtual machines and we loose $1000 an hour when they are down.

Values should be standardized across an organization.

Aggregate values should represent the highest common denominator.

Example: A physical server running multiple virtual machines

10 virtual machines each valued at **LOW**

1 virtual machine valued at **HIGH**

Overall value = **HIGH**

Values should be realistic and reviewed.

Firewall Examples:

Sales workstations can talk to the sales email server

Sales email server can talk to central email server

Deny all

Remediation Examples:

If any server < 70 connects to a known-bad host:

Move to quarantine VLAN

Contact security and system administrators – medium priority

If any server >= 70 connects to a known-bad host:

Contact security and system administrators – high priority

If any workstation connects to a workstation:

Move to quarantine VLAN

Contact security and system administrators – medium priority

Original alert from Snort:

11/05-22:08:59.705515 [**] [1:469:3] ICMP PING NMAP [**]
[Classification: Attempted Information Leak][Priority: 2] {ICMP}
192.168.206.129 - 192.168.100.5

Expanded alert:

Timestamp:11/05-22:08:59, Description: Probable Ping Sweep, Priority:1, Confidence: High, Source:(192.168.206.129,Web Server, DMZ), Destination:(Internal subnets)

BEST STATE

Analyst automation:

The idea here is to learn from the analyst and remove mundane and repetitive tasks from their queue.

Examples:

- If an analyst deletes the an event with similar characteristics more than 4 times, don't show it again (still record the event though).
- Automatically send specific events to specific analysts – Windows server events go to Bob and Linux server events go to Alice
- Enable links to run scripts or access other data.

The comfort factor is high here because humans are still involved in each transaction. Humans can interpret the data before making a decision. Humans also have limits on how fast and effectively they can work. Humans are also known to make mistakes.

Full automation:

When an event is generated there are corresponding rules on how to remediate that are automatically executed.

This can be done safely on events that are easily recognized as **ALWAYS** bad (no gray areas):

Visit to known bad site – always bad

Malware detected – always bad

Surfing the Internet as Domain Admin – always bad

No different than any other “if-then” statement

Requires really well defined policies.

Requires sensors to detect the bad activity.

Requires methods of remediation – block port, add firewall rule, disable account, etc.

Requires a way for everything to communicate.

Custom scripting:

Not the most scalable solution but it can get the job done.

Examples:

The event data (alerts) can be sent from Splunk to a custom python script that performs the remediation.

A database update can cause a trigger to run a custom script that performs the remediation.

Overall solutions:

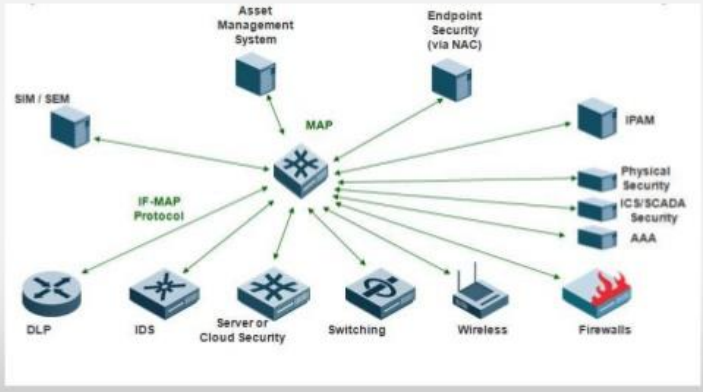
Utilize centralized databases with policy decision points and policy enforcement points. Scales very well but requires your endpoints (routers, switches, workstations, etc.) to support the solution.

Examples:

- IF-MAP from the Trusted Computing Group (http://if-map.org)
- pxGrid from Cisco (https://developer.cisco.com/site/pxgrid/)

IF-MAP(THE INTERFACE FOR METADATA ACCESS POINTS)

IF-Map is a SOAP based protocol for publishing data to the MAP-server and querying or subscribing to get data from it.
IF-Map is an open, non-proprietary standard that is multi-vendor compatible.



Everything needs to be tested and verified:

There should be a test harness validates the enforcement of every **policy.**
The test harness should be run every time a change in policy is made.

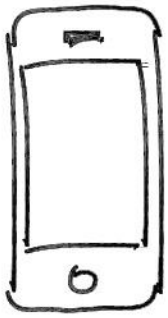
People should be trained on how to use the system.

- Typical usage
- How to respond to events
- How to respond to the unknown (who do you call, what do you do)

The entire **system** needs to be tested periodically.
Everyone runs fire drills but most organizations don't run attack drills.

"The will to win means nothing without the will to prepare." – Juma Ikangaa[1]
"What is difficult in training will become easy in a battle." – Alexander Suvorov[1]

[1]*http://www.forcexinc.com/trainer-tips/*

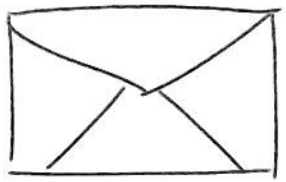


240-314-6800

Participate

http://nccoe.nist.gov

nccoe@nist.gov
Financial_NCCOE@nist.gov
Michael.Stone@nist.gov



9600 Gudelsky Drive
Rockville, MD 20850