

IT Asset Management

National Cybersecurity Center of Excellence

Increasing the deployment and use of
standards-based security technologies

May 19, 2016



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

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

A misconfigured IT asset is a vulnerable asset

- ▶ Increase visibility, utilization, efficiency
- ▶ Know what devices are on your network
- ▶ Know what software your devices are running
- ▶ Know what your assets are doing

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

The Situation:

- ▶ 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.
- ▶ 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.)

Reduce Vulnerabilities

- ▶ Automatic patching
- ▶ Automatic vulnerability scanning
- ▶ Automatic threat updates
- ▶ Detect new devices
- ▶ Configuration reporting enforcement

Enforce Policy

- Choose what software to allow
 - No BitTorrent, no TOR, only the latest Java
- Restrict what Internet sites are allowed
 - No porn, no gambling
- Disallow USB thumb drives

Increase Asset Utilization/ROI

- ▶ How much is being wasted on software licenses?
 - ▶ How many software licenses are installed?
 - ▶ Are employees actually using expensive software?

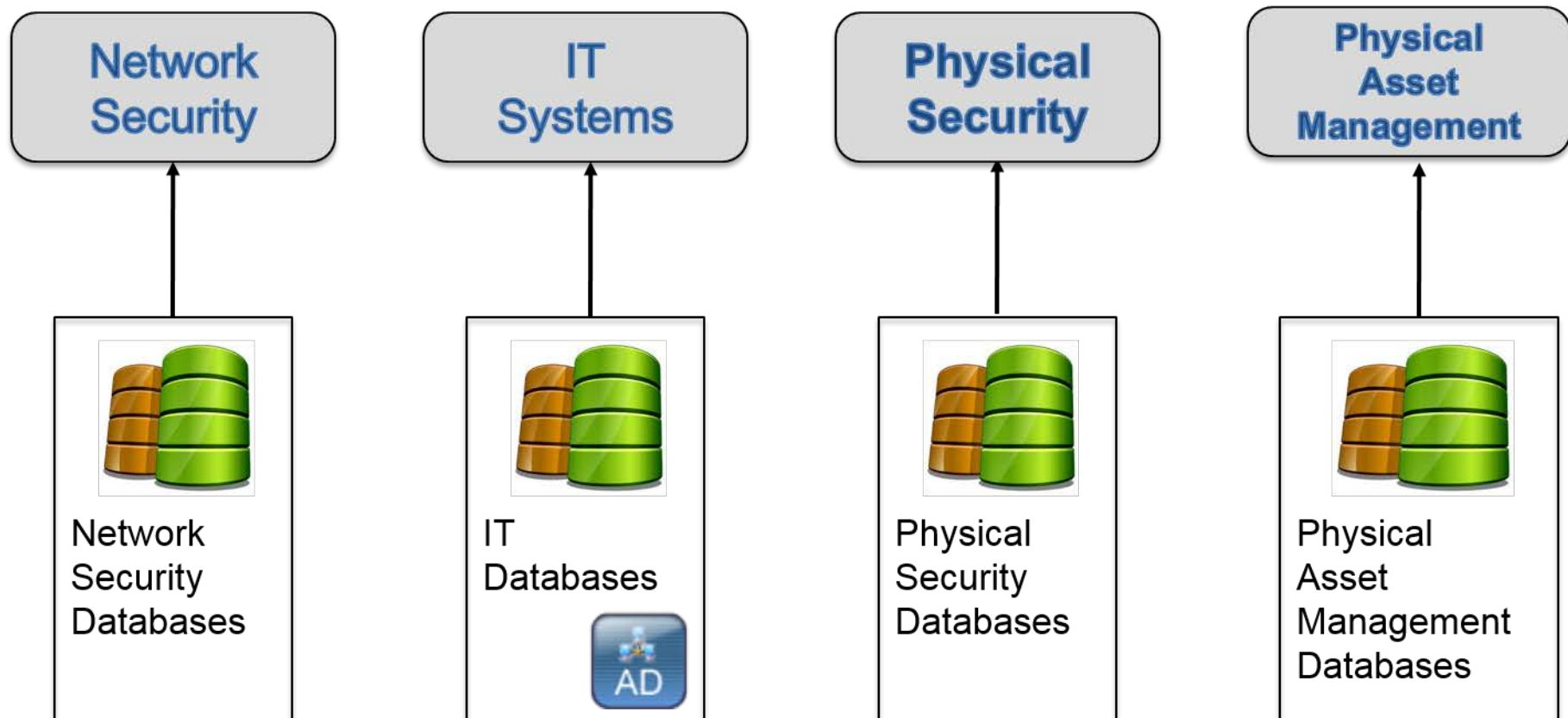
- ▶ What's the most popular web browser?
 - ▶ Reduce support costs

- ▶ Are servers fully utilized?
 - ▶ Reduce maintenance, power, space and cooling

Why IT Asset Management is Difficult

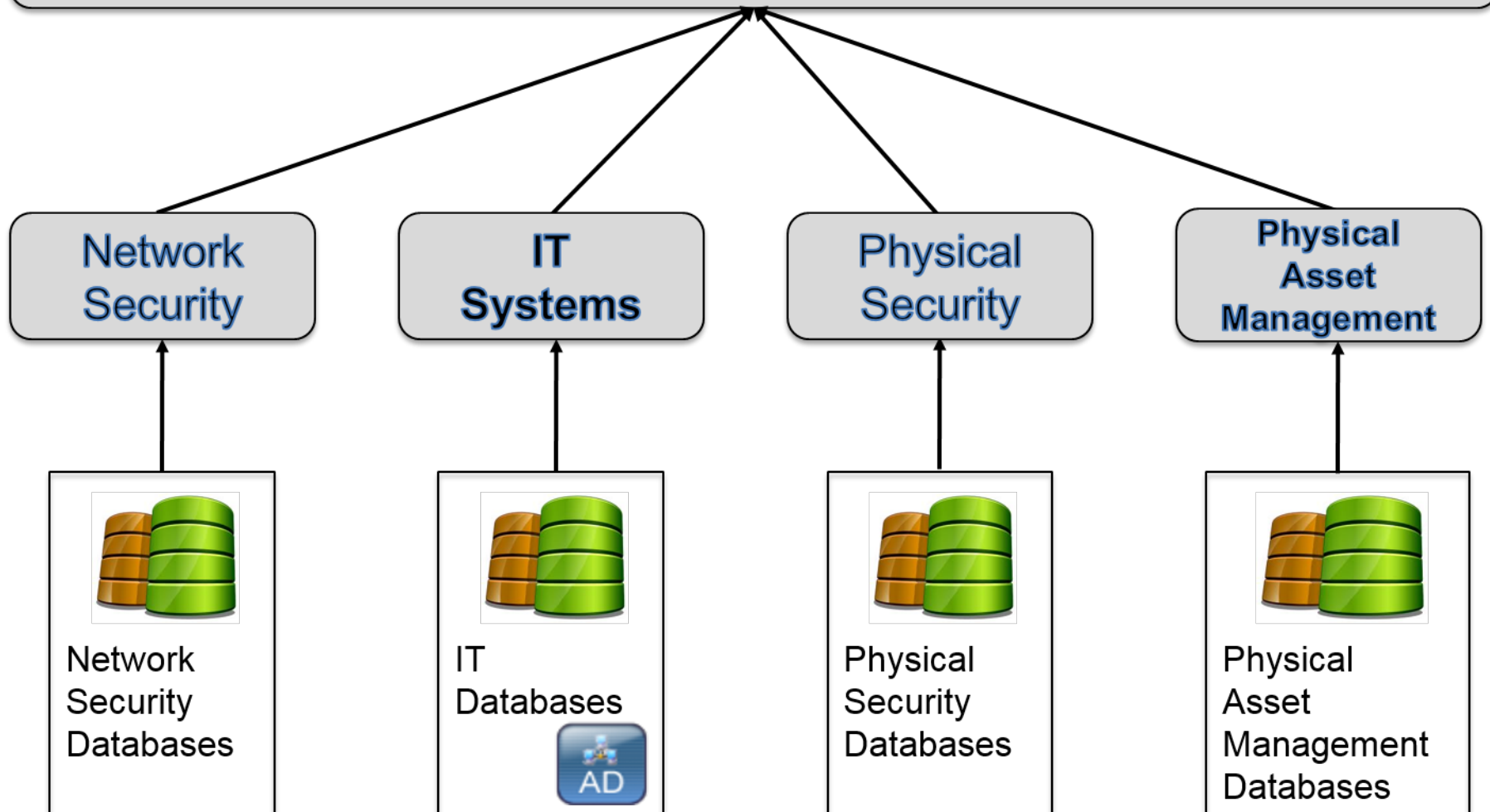
- ▶ Large number of devices
- ▶ Lack of consolidated information
- ▶ Employee role changes and turnover
- ▶ Multiple locations spread over large geographic location
- ▶ Complex corporate organization

Everything is currently in separate silos



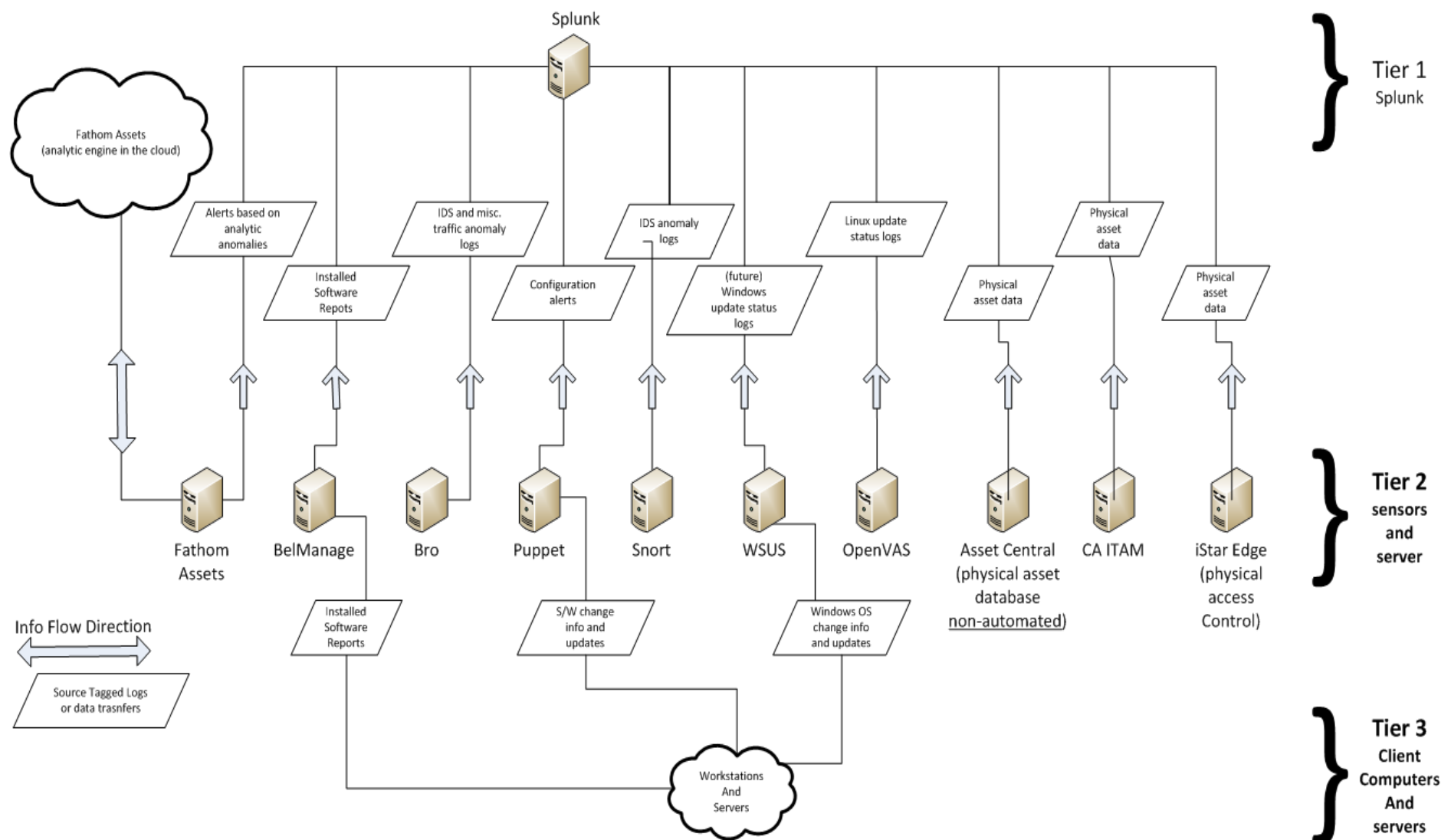
Bring everything together

IT Asset Management System



- Multiple data sources all sending data to a central location
 - Passive and active sensors
 - Network and host based sensors
- Existing data sources do not lose their original functionality
 - Not a rip and replace solution
- Answers must be fast
- Create pre-configured dashboards and reports for multiple user roles
 - Inventory, security, compliance, etc.





1. Get individual data sources online (Bro, Snort, WSUS, etc.)
2. Send data from data sources into Splunk Enterprise
3. Normalize data (common names, common formats)
4. Develop simple dashboards for each data source (dashboard for Snort, dashboard for Bro, dashboard for WSUS, etc.)
5. Aggregate similar data into indexes (“alerts” index made up of events from Bro, Snort and firewalls)
6. Develop reports and dashboards to answer business questions (e.g. how many machines need critical patches?)

Syslog:

Native support in Splunk. Syslog info from servers and firewalls are sent to Splunk and stored in the “syslog” index.

Splunk DB Connect V2:

Connects to multiple databases (MS SQL, MySQL), issues SQL queries and stores the results into an index. Each sensor using Splunk DB Connect V2 has its own index including: BelManage, CA ITAM and AssetCentral.

Splunk Universal Forwarder:

Copies data from log files over the network to Splunk Enterprise. Takes into account file growth and log rotation. Used for Bro, Snort, Puppet and OpenVAS.

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

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

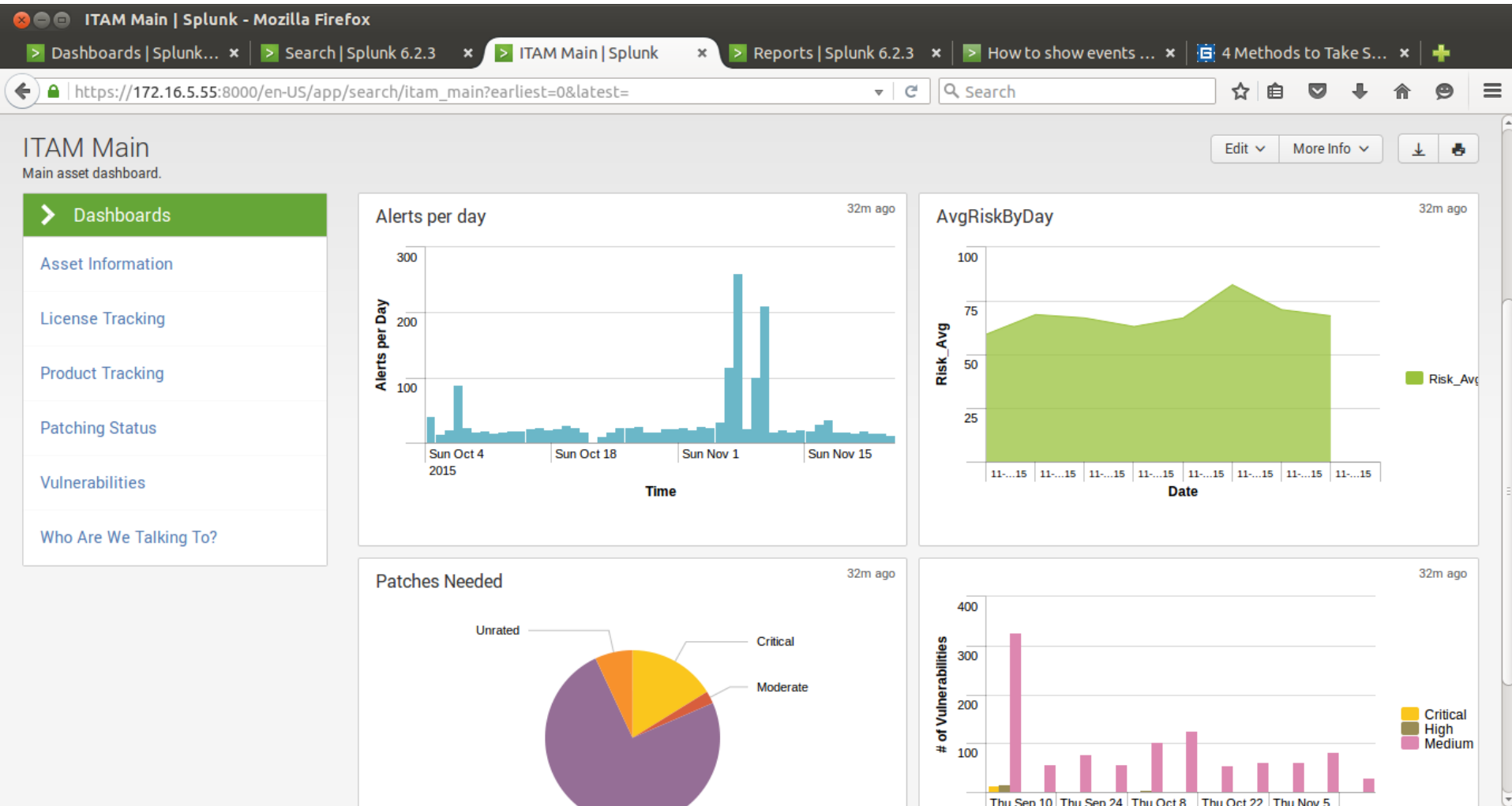
Expanded Alert:

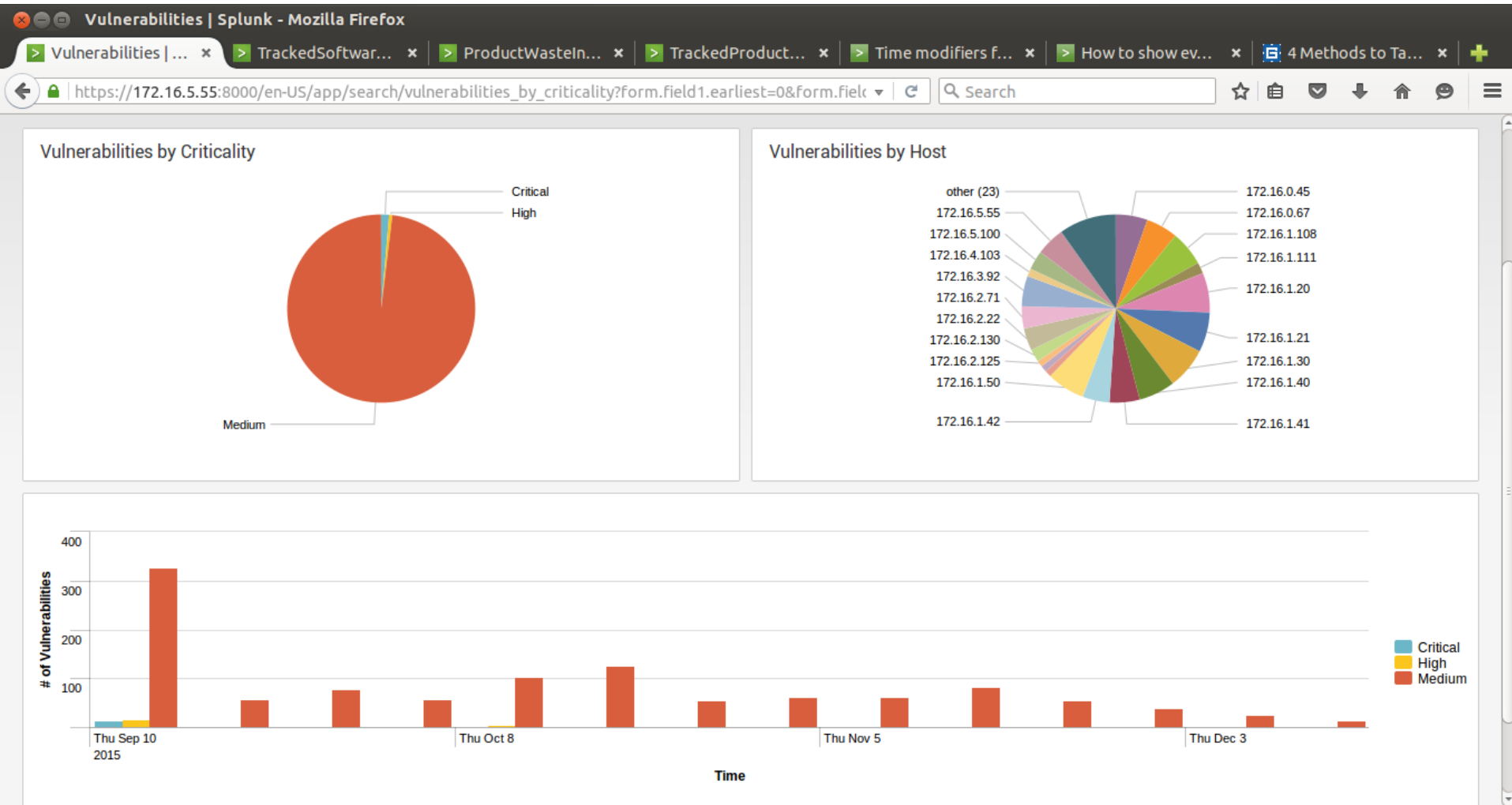
Timestamp:11/05-22:08:59, Description: Probable Ping Sweep, Priority:1,
Confidence: High, Source:(192.168.206.129,Web Server, DMZ),
Destination:(Internal subnets)

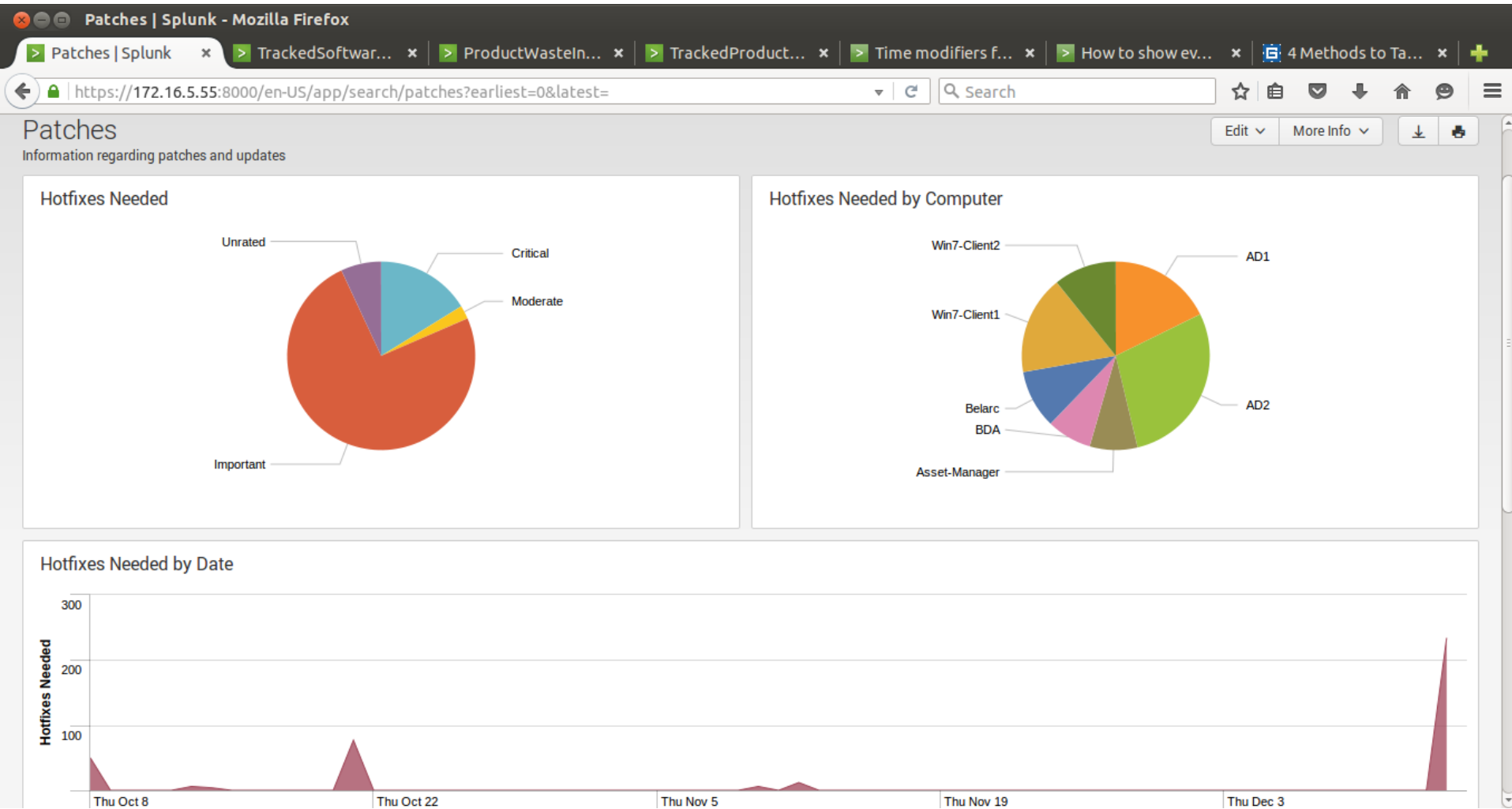
- 3 ways to identify known hardware
- Machines receive a NPE certificate when configured/baselined
 - The certificate contains information specific to that machine:
 - Barcode
 - Serial Number
 - Make/Model
 - An alert is triggered when a certificate from an unknown machine is seen.
- Machines with BelManage and/or Puppet agents are known
- Other devices can be added to a “whitelist” based on MAC address and/or IP address (last resort)

- Agents report on hardware changes.
 - Unauthorized changes trigger an alert

- Configuration files from network devices are analyzed for unauthorized changes.
 - New interfaces
 - New routes
 - New rules







LicenseTracking | Splunk - Mozilla Firefox

LicenseTracking | Sp... | Search | Splunk 6.2.3 | TrackedProductInfo... | Reports | Splunk 6.2.3 | How to show events ... | 4 Methods to Take S... | +

https://172.16.5.55:8000/en-US/app/search/licensetracking?earliest=0&latest=

splunk> App: Search & Reporting | Administrator | Messages | Settings | Activity | Help | Find

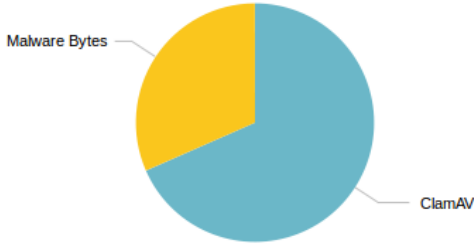
Search | Pivot | Reports | Alerts | Dashboards | Search & Reporting

LicenseTracking

Edit | More Info | Download | Print

2m ago

Tracked_Software



Software	Count
Malware Bytes	40
ClamAV	21

Malware Bytes License Count

2m ago

Purchased MalwareBytes Licenses: **40**

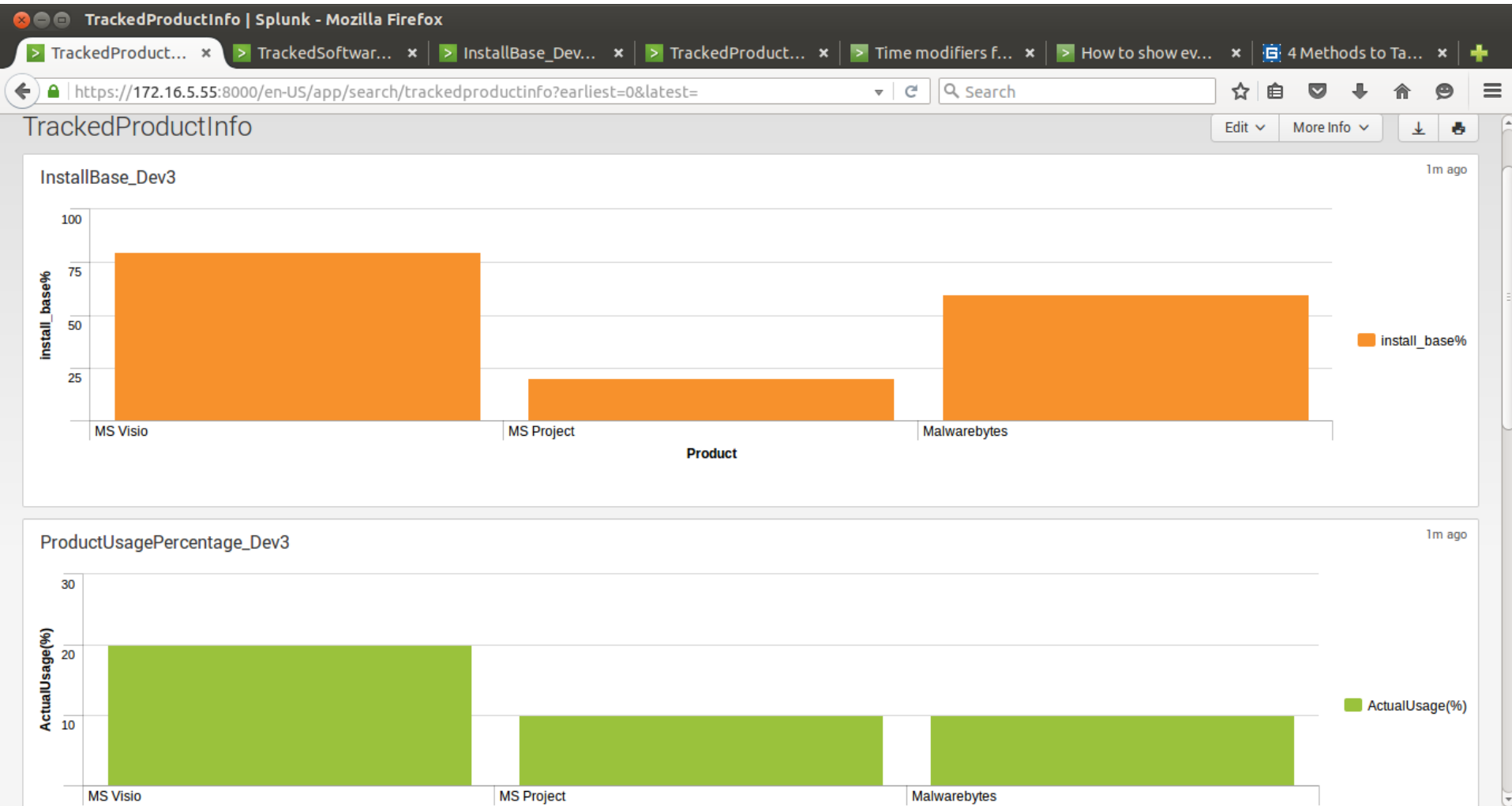
ClamAV License Count

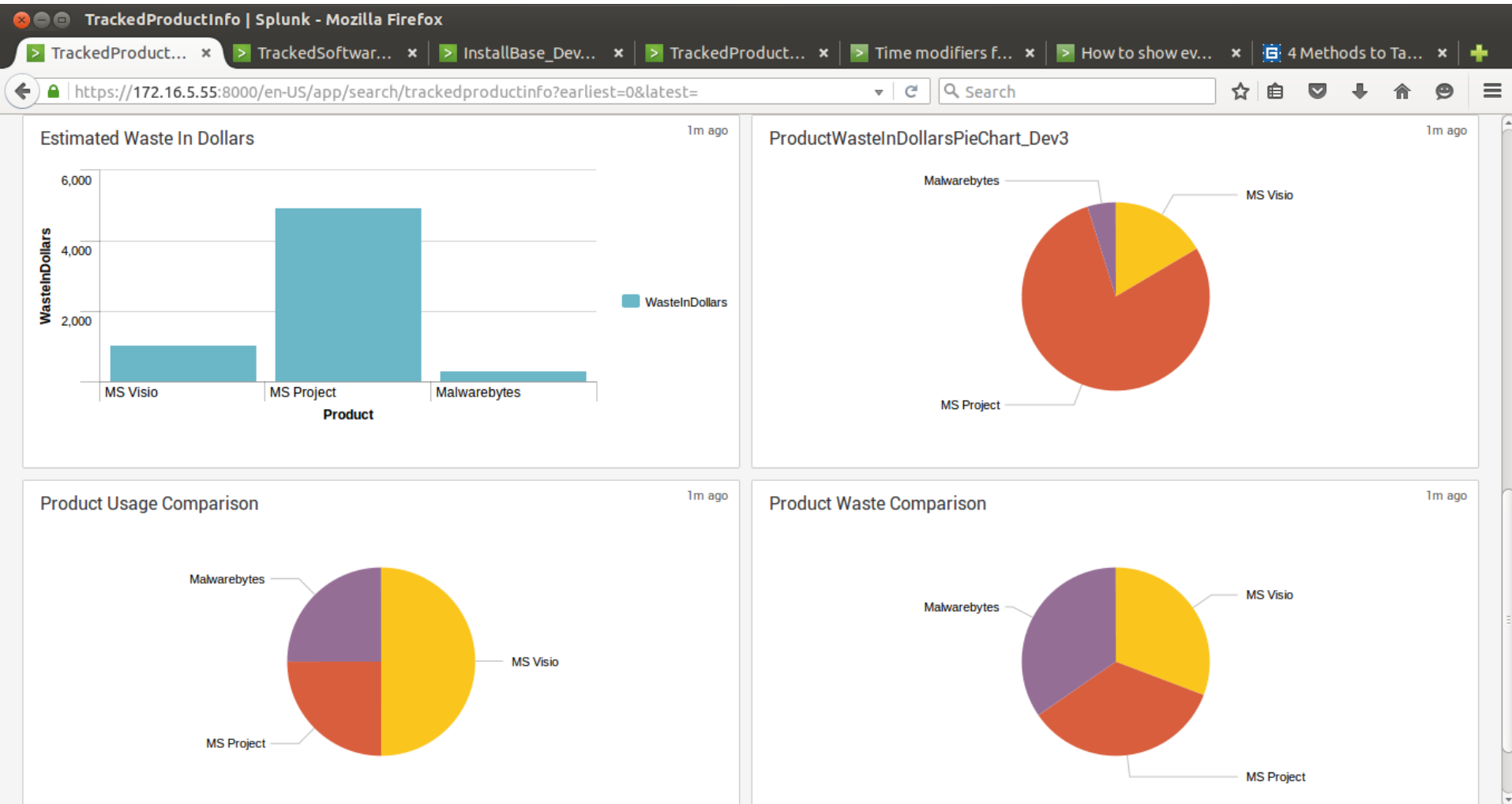
2m ago

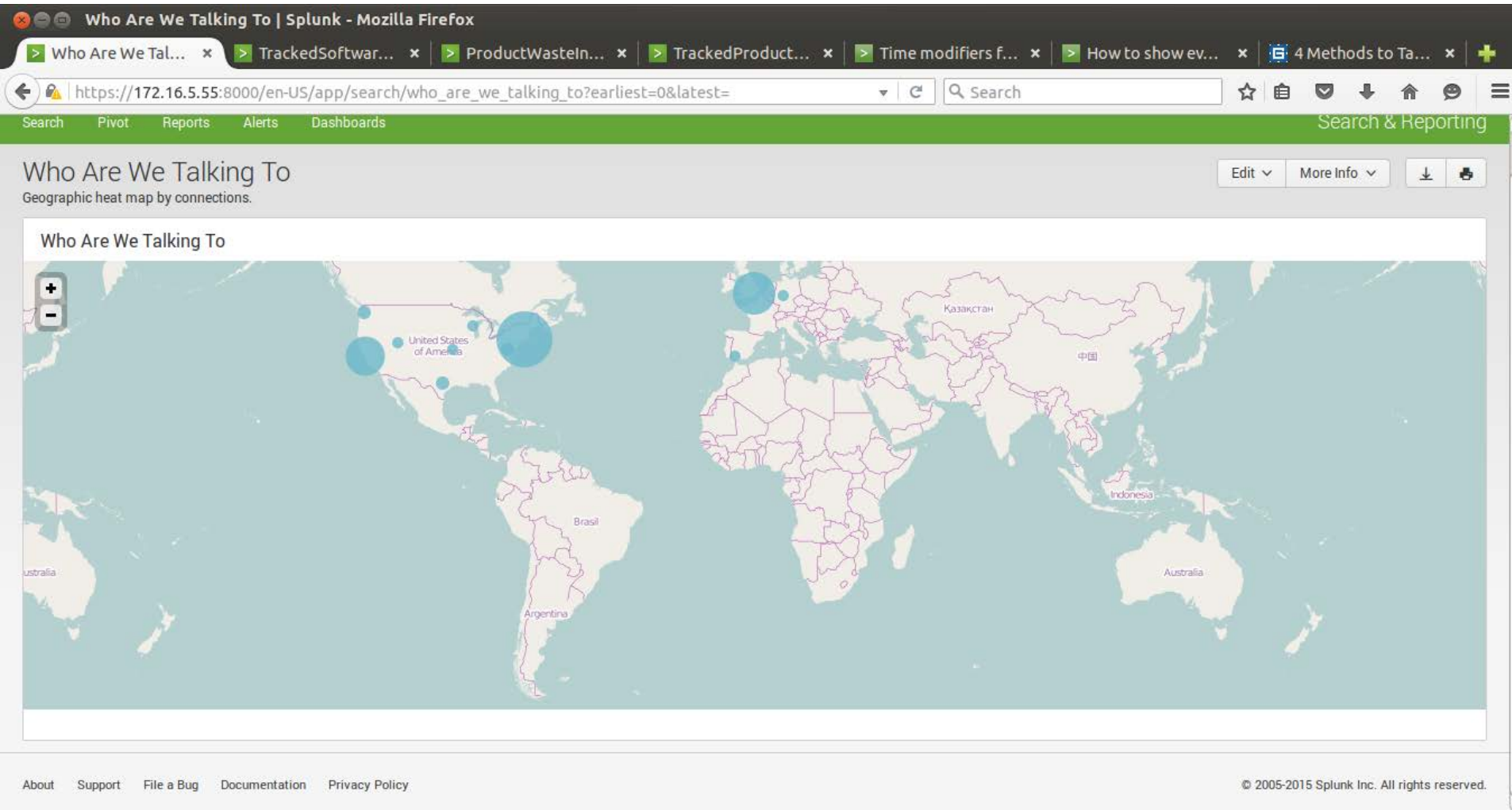
Purchased ClamAV Licenses: **21**

About | Support | File a Bug | Documentation | Privacy Policy

© 2005-2015 Splunk Inc. All rights reserved.







Asset Dashboard | Splunk - Mozilla Firefox

Dashboards | Splunk... x Search | Splunk 6.2.3 x Asset Dashboard | S... x Reports | Splunk 6.2.3 x How to show events ... x 4 Methods to Take S... x +

https://172.16.5.55:8000/en-US/app/search/asset_dashboard?form.AssetName=AD1&form.field2.earliest Search

splunk> App: Search & Reporting Administrator Messages Settings Activity Help Find

Search Pivot Reports Alerts Dashboards Search & Reporting

Asset Dashboard

Summary of an Asset

AssetName: AD1 Time Selector: All time

Asset Owner

<1m ago

	column	row 1
1	Last Name	Stone
2	First Name	Michael
3	Middle Name	NULL
4	Phone Number	2403146813

System Info

<1m ago

column	row 1
Status	Up
NetworkIPAddress	172.16.1.20
OSProductOptions	Standard
SystemSerialNumber	VMware-42 1b 32 59 b8 f5 93 bc-b9 2b 07 15 91 c4 f
PhysicalMemory	4096
CPUCount	1
CPUModel	Xeon E5-2660 0
Clock	2200
FreeDisk	24998

SW Info

<1m ago

Filename	Directory	Product_soft	Version_soft
cscript.exe	c:\Windows\System32	Windows Script Host	5.8.9600.16384

This entire project is detailed in *NIST Special Publication 1800-5* which can be found at:

https://nccoe.nist.gov/projects/use_cases/financial_services_sector/it_asset_management

All of the searches, dashboards and reports can be downloaded from:

https://nccoe.nist.gov/sites/default/files/nccoe/NIST_SP1800-5_FSITAM.zip

Engage

nccoe@nist.gov
Financial_NCCOE@nist.gov
mjstone2@nsa.gov