Detecting Counterfeit Assets & Stomping Out The Competition w/ Splunk Enterprise

Last verified by Jitin Aware on 07-30-2021

The US Social Security Administration (SSA) has developed a strategic plan to modernize their data center operations, titled Data Center Optimization Initiative (DCOI) and asked the Splunk Account Team how Splunk can help streamline their operations, specifically around counterfeit assets detection. Link to plan: https://www.ssa.gov/digitalstrategy/datacenteroptimizationstrategicplan.pdf

There was also a **competitive threat** from ServiceNow, who claimed to have an OOTB solution that detects counterfeit assets without the need for storing data in Splunk.

Naturally, I sprung into action and started working on a demo to showcase Splunk's capabilities. The result is a set of dashboards that authoritatively:

- report on assets physically within SSA's datacenters as well as assets observed in network scans
- correlate across these data sources to find discrepancies,
- and report in deep detail on these anomalous assets

While this use case was initially brought to us from the Infrastructure team (IT Ops), it overlaps into security use cases as well and really **illustrates Splunk's ability to break down silos** within organizations.

Link to slide deck and demo:

- https://docs.google.com/presentation/d/1ChQZkdnkjRYdCKzvH2Gj2t91j6eUtl9R/edit#slide=id.gccebcae2c7_2_483
- https://splunk.zoom.us/rec/share/i9QlpzrFWojnyRPoyTkK2AxLoi9U1ECyCs8vUf6rki99AF2WX3KdcOa1RyXh-wqQ.yxfKNGX72c9ifMQE
    - Passcode: $@Dm64jw

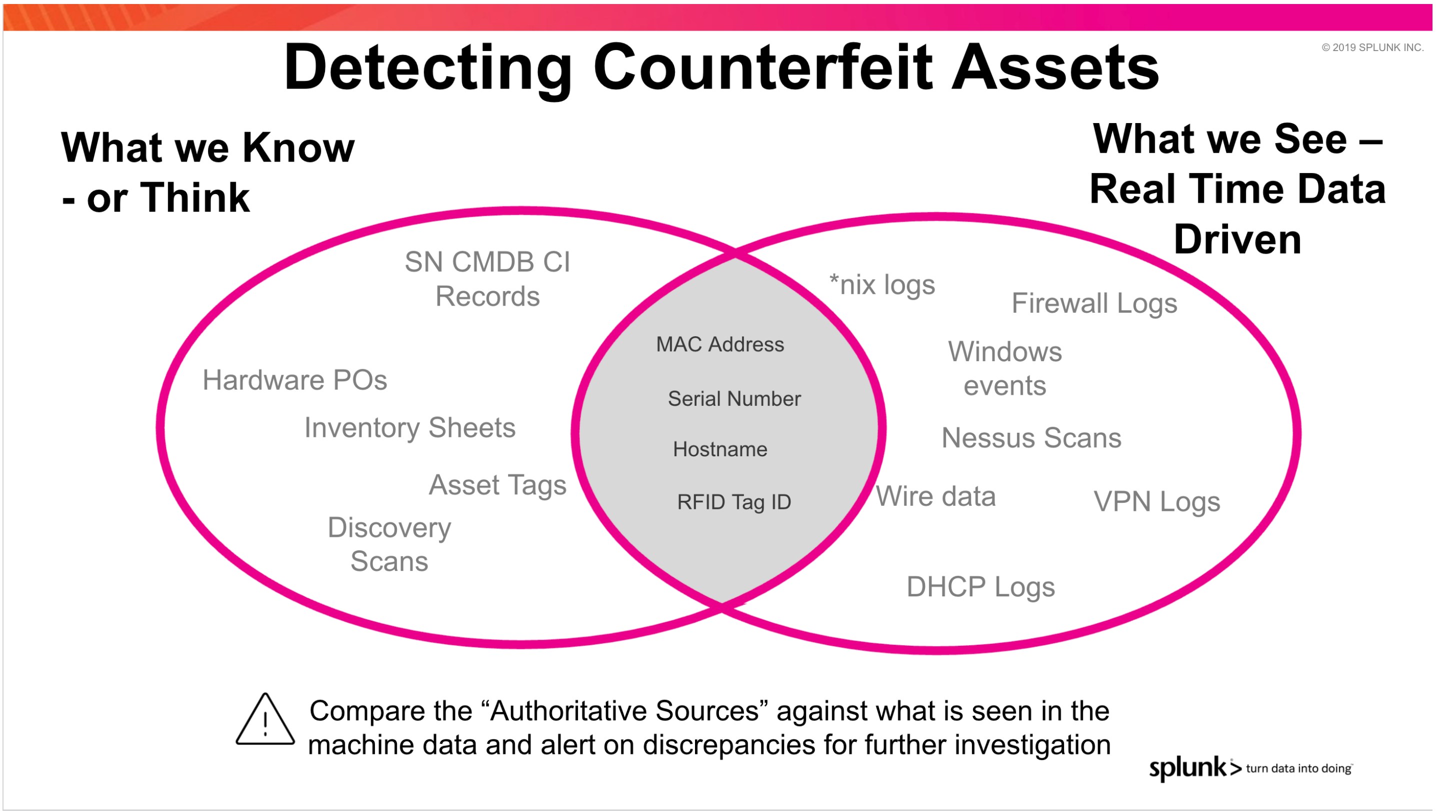
Background

WHAT THE HECK IS A "COUNTERFEIT ASSET" ANYWAY?

The first step was to define Counterfeit Assets (hint: each organization has its own definition). During my research, I came up with 3 main problems that most organizations were looking to solve:

- Suspicious/abnormal assets detected on the network (network/vulnerability scans)
- Suspicious/abnormal assets discovered in the datacenter (physical inventory)
- Assets' hardware modified from manufacturing plant (supply chain attack)

Next, our wonderful ITOps CSE Brady McClary illustrated how we can compare authoritative sources ("sources of truth") such as CMDB data, purchase orders, asset tags, and inventory sheets with what we observe in the machine data within the environment: things like network scans, as well as OS, firewall, and other network logs. We can then **correlate across these disparate data sources** to create a final source of truth, and alert on anything that deviates from that.



Detecting Counterfeit Assets

What we Know - or Think

What we See – Real Time Data Driven

SN CMDB CI Records

Hardware POs

Inventory Sheets

Asset Tags

Discovery Scans

MAC Address

Serial Number

Hostname

RFID Tag ID

*nix logs

Firewall Logs

Windows events

Nessus Scans

Wire data

VPN Logs

DHCP Logs

⚠ Compare the "Authoritative Sources" against what is seen in the machine data and alert on discrepancies for further investigation

Finally, my research yielded some common characteristics of successful implementations of this use case:

Strong Physical Security: Access Control (badge readers, fingerprint readers), Monitoring (security cameras, badge entry logs), RFID tags, Tamper-proof chassis + racks
Strong Agency-Supplier Relationship

Immutable Fabric (such as Hyperledger)
Case Study: Microsoft Corp. uses Blockchain + Splunk for supply chain insight

Security should be thought of as an onion, made up of a shield of defensive layers that support each other. If one fails, the next one is there to jump in and back it up. A strong defense-in-depth approach to security can help organizations maintain a resilient security posture.

NOTE: while some organizations may not be mature enough to adopt technologies such as Hyperledger fabric and blockchain today, it's important to introduce these concepts early on and get customers familiar with them on their maturity journey.

SSA DATACENTER WORKFLOW

SSA's workflow primarily consisted of:

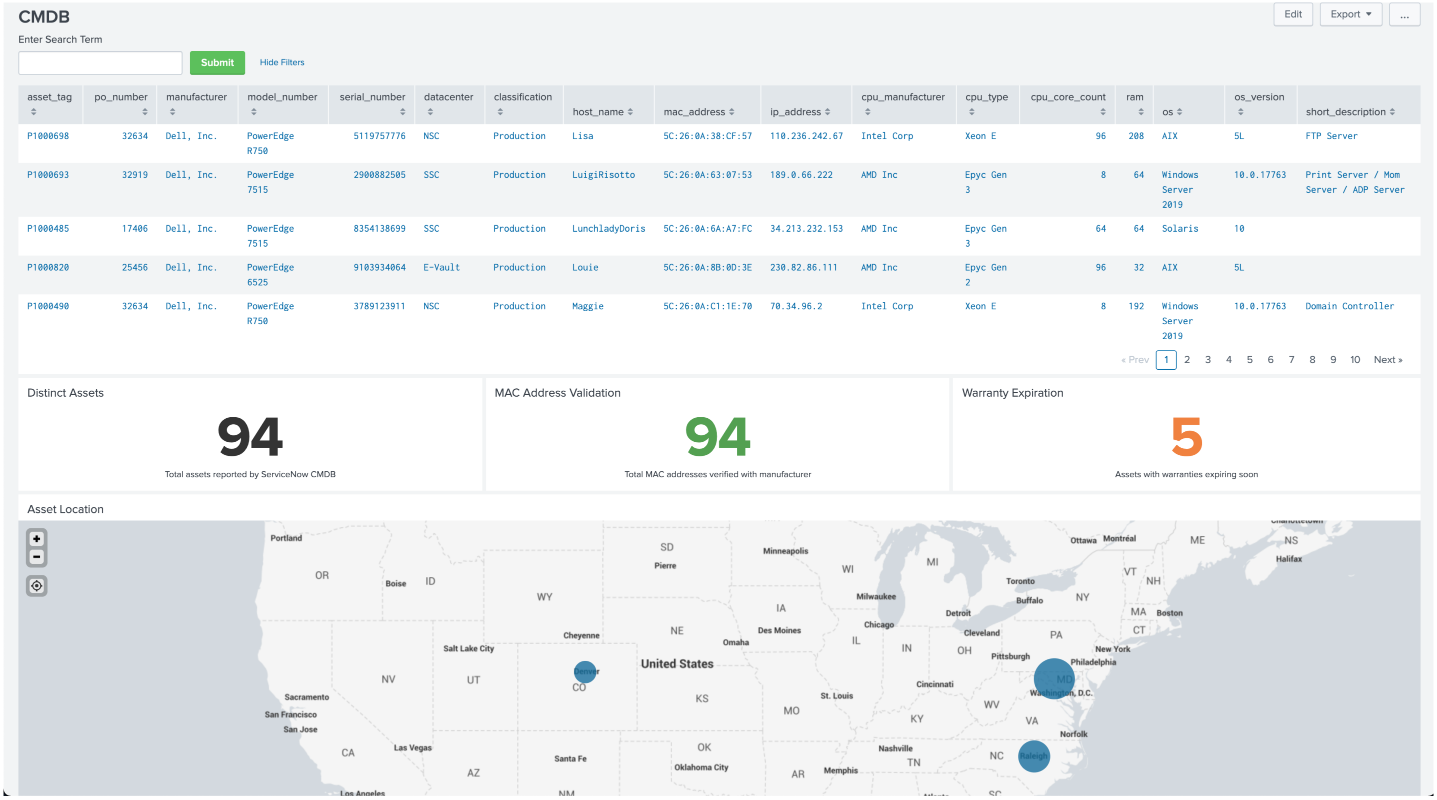
1. The datacenter team receiving hardware and verifying with Purchase Order
2. Applying an RFID tag containing asset info
3. Scanning the RFID tag into VisiTrac Asset Manager
4. VisiTrac then updates ServiceNow CMDB

It was important to not disrupt their existing workflow or tooling; rather, I wanted to augment them with the capabilities of Splunk Enterprise. In addition, I aimed to make this a repeatable process and tooling-agnostic, so it could be applied across agencies (and private sector organizations) even if they didn't use VisiTrac or ServiceNow.

I also found the physical locations of SSA's datacenters in the course of my research and found a cool way to incorporate this data in the solution (details below).

Solution Overview

CMDB Dashboard



CMDB

Enter Search Term

asset_tag	po_number	manufacturer	model_number	serial_number	datacenter	classification	host_name	mac_address	ip_address	cpu_manufacturer	cpu_type	cpu_core_count	ram	os	os_version	short_description
P1000698	32634	Dell, Inc.	PowerEdge R750	5119757776	NSC	Production	Lisa	5C:26:0A:38:CF:57	110.236.242.67	Intel Corp	Xeon E	96	208	AIX	5L	FTP Server
P1000693	32919	Dell, Inc.	PowerEdge 7515	2900882505	SSC	Production	LuigiRisotto	5C:26:0A:63:07:53	189.0.66.222	AMD Inc	Epyc Gen 3	8	64	Windows Server 2019	10.0.17763	Print Server / Mom Server / ADP Server
P1000485	17406	Dell, Inc.	PowerEdge 7515	8354138699	SSC	Production	LunchladyDoris	5C:26:0A:6A:A7:FC	34.213.232.153	AMD Inc	Epyc Gen 3	64	64	Solaris	10	
P1000820	25456	Dell, Inc.	PowerEdge 6525	9103934064	E-Vault	Production	Louie	5C:26:0A:8B:0D:3E	230.82.86.111	AMD Inc	Epyc Gen 2	96	32	AIX	5L	
P1000490	32634	Dell, Inc.	PowerEdge R750	3789123911	NSC	Production	Maggie	5C:26:0A:C1:1E:70	70.34.96.2	Intel Corp	Xeon E	8	192	Windows Server 2019	10.0.17763	Domain Controller

Distinct Assets

94

Total assets reported by ServiceNow CMDB

MAC Address Validation

94

Total MAC addresses verified with manufacturer

Warranty Expiration

5

Assets with warranties expiring soon

Asset Location

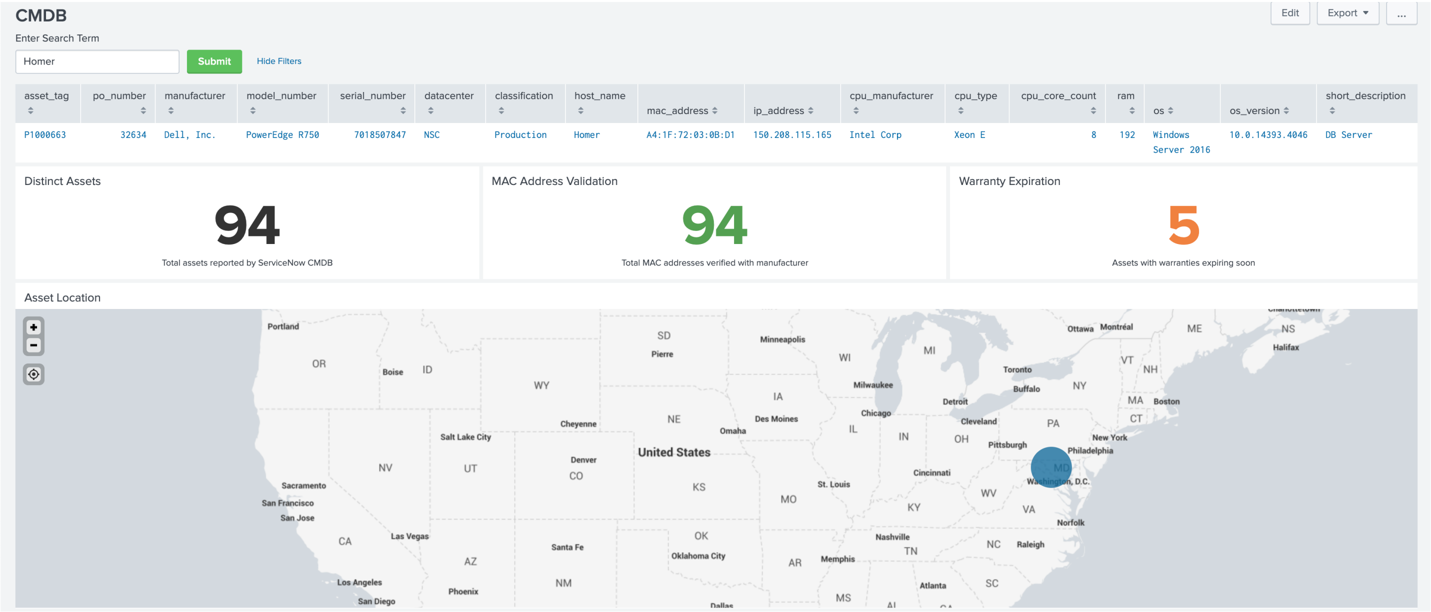
> *Guess who can't come up with hostnames and uses characters from The Simpsons instead?*

Since the ServiceNow App became End of Life, I created a new dashboard populated by data from ServiceNow CMDB (but can be used with other CMDBs). This dashboard's objective is to serve as an authoritative source as to what's physically in a customer's datacenter(s).

The primary panel displays the existing inventory as reported by a typical CMDB: asset tag, purchase order number, manufacturer, model and serial numbers, which datacenter the hardware is located in, along with hardware details such as processor and RAM configuration.

It's also dynamic: customers can search and filter via asset tag, hostname, purchase order number, and more. The Asset Location panel helps visualize where SSA's assets live geographically based on the three datacenters SSA owns - this panel is dynamically updated as well based on a user's search.

Example 1: Hostname Search



CMDB

Enter Search Term

Homer

asset_tag	po_number	manufacturer	model_number	serial_number	datacenter	classification	host_name	mac_address	ip_address	cpu_manufacturer	cpu_type	cpu_core_count	ram	os	os_version	short_description
P1000663	32634	Dell, Inc.	PowerEdge R750	7018507847	NSC	Production	Homer	A4:1F:72:03:0B:D1	150.208.115.165	Intel Corp	Xeon E	8	192	Windows Server 2016	10.0.14393.4046	DB Server

Distinct Assets

94

Total assets reported by ServiceNow CMDB

MAC Address Validation

94

Total MAC addresses verified with manufacturer

Warranty Expiration

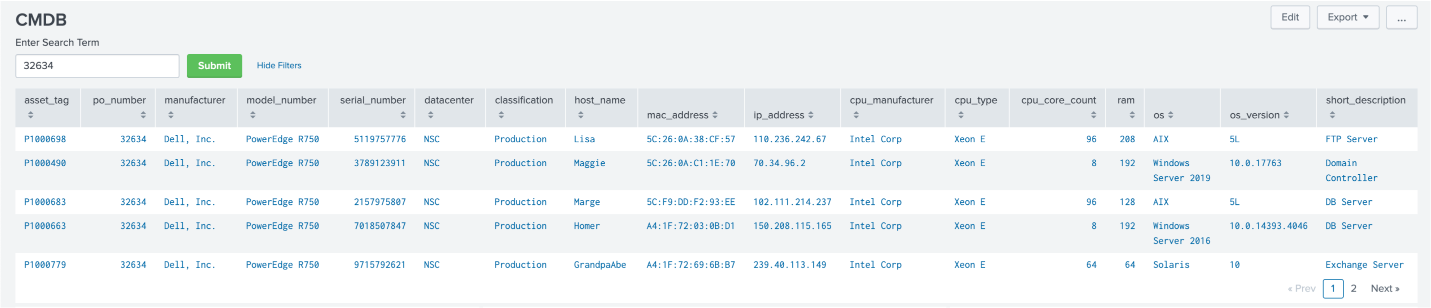
5

Assets with warranties expiring soon

Asset Location

> *Users can filter for specific hosts via search: searching for the hostname 'Homer' we can see more details such as hardware info and physical location.*

Example 2: Purchase Order Number Search



CMDB

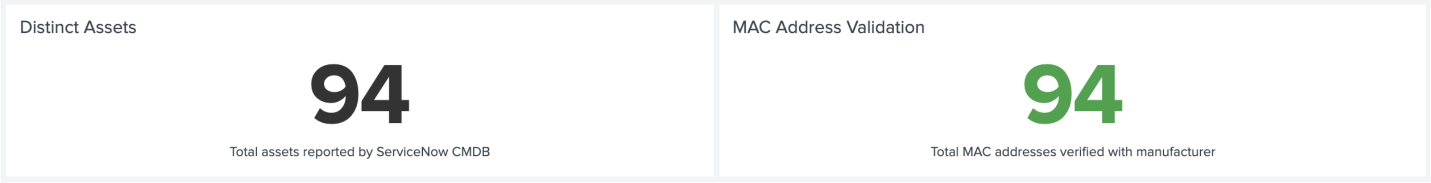
Enter Search Term

32634

asset_tag	po_number	manufacturer	model_number	serial_number	datacenter	classification	host_name	mac_address	ip_address	cpu_manufacturer	cpu_type	cpu_core_count	ram	os	os_version	short_description
P1000698	32634	Dell, Inc.	PowerEdge R750	5119757776	NSC	Production	Lisa	5C:26:0A:38:CF:57	110.236.242.67	Intel Corp	Xeon E	96	208	AIX	5L	FTP Server
P1000490	32634	Dell, Inc.	PowerEdge R750	3789123911	NSC	Production	Maggie	5C:26:0A:C1:1E:70	70.34.96.2	Intel Corp	Xeon E	8	192	Windows Server 2019	10.0.17763	Domain Controller
P1000683	32634	Dell, Inc.	PowerEdge R750	2157975807	NSC	Production	Marge	5C:F9:DD:F2:93:EE	102.111.214.237	Intel Corp	Xeon E	96	128	AIX	5L	DB Server
P1000663	32634	Dell, Inc.	PowerEdge R750	7018507847	NSC	Production	Homer	A4:1F:72:03:0B:D1	150.208.115.165	Intel Corp	Xeon E	8	192	Windows Server 2016	10.0.14393.4046	DB Server
P1000779	32634	Dell, Inc.	PowerEdge R750	9715792621	NSC	Production	GrandpaAbe	A4:1F:72:69:6B:B7	239.40.113.149	Intel Corp	Xeon E	64	64	Solaris	10	Exchange Server

> *Searching by PO number gives us results for all of the servers that were purchased on that PO.*

Total Assets and MAC Address Validation



Distinct Assets

94

Total assets reported by ServiceNow CMDB

MAC Address Validation

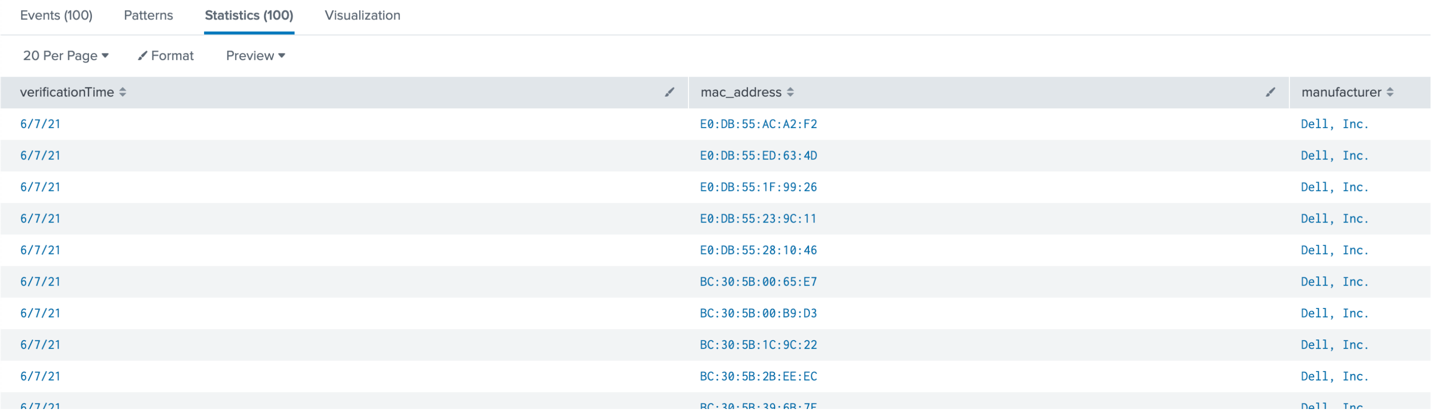
94

Total MAC addresses verified with manufacturer

Next, I added panels to calculate the total number of assets reported in the CMDB (useful later on in the counterfeit assets detection) as well as MAC address validation. Each of these drills down to the full inventory detail.

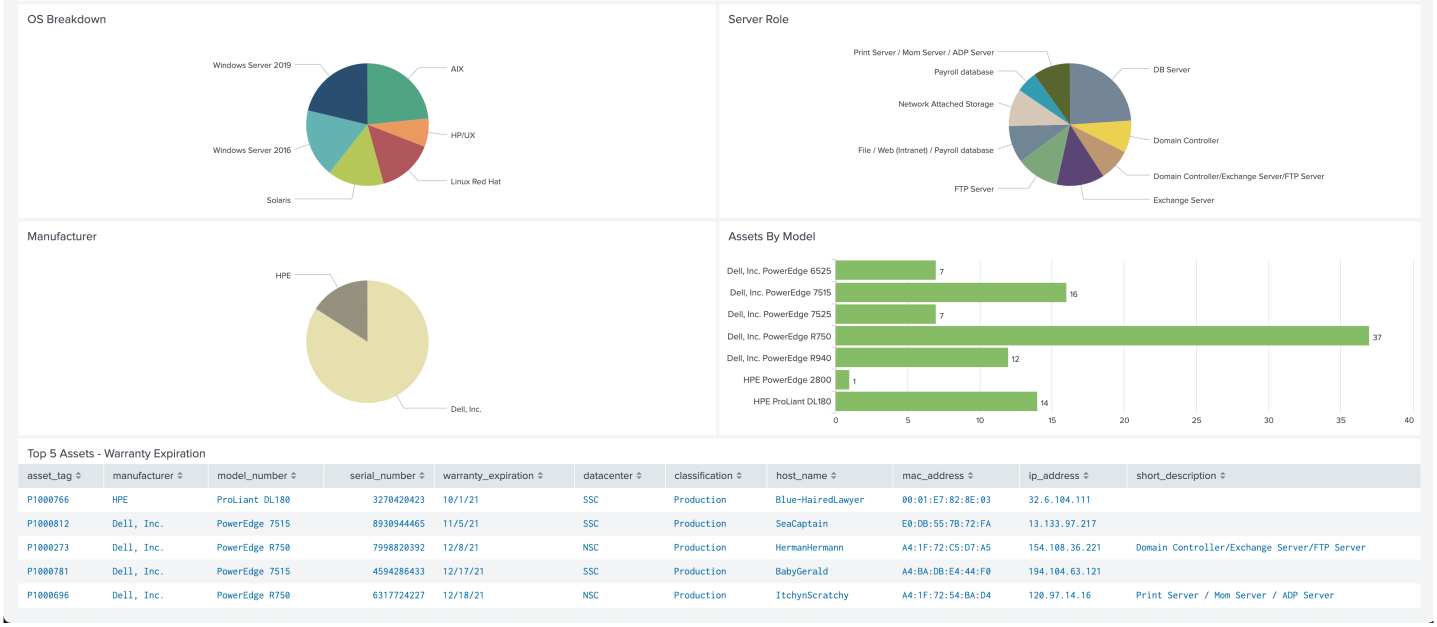
Why validate MAC addresses?

The first 3 octects (6 characters) in a given MAC address are universally assigned to a particular manufacturer. We can perform API calls to a MAC address lookup website using only the first 3 octects (so we're not transmitting full MAC addresses) to validate whether the CMDB-reported MAC Addresses truly belong to a particular manufacturer. I used http://www.macvendorlookup.com/api



verificationTime	mac_address	manufacturer
6/7/21	E0:DB:55:AC:A2:F2	Dell, Inc.
6/7/21	E0:DB:55:ED:63:4D	Dell, Inc.
6/7/21	E0:DB:55:1F:99:26	Dell, Inc.
6/7/21	E0:DB:55:23:9C:11	Dell, Inc.
6/7/21	E0:DB:55:28:10:46	Dell, Inc.
6/7/21	BC:30:5B:00:65:E7	Dell, Inc.
6/7/21	BC:30:5B:00:B9:D3	Dell, Inc.
6/7/21	BC:30:5B:1C:9C:22	Dell, Inc.
6/7/21	BC:30:5B:2B:EE:EC	Dell, Inc.
6/7/21	BC:30:5B:39:6B:7E	Dell, Inc.

Finally, the remaining panels report other insights such as OS and manufacturer breakdown, server roles, and even warranty expiration details.

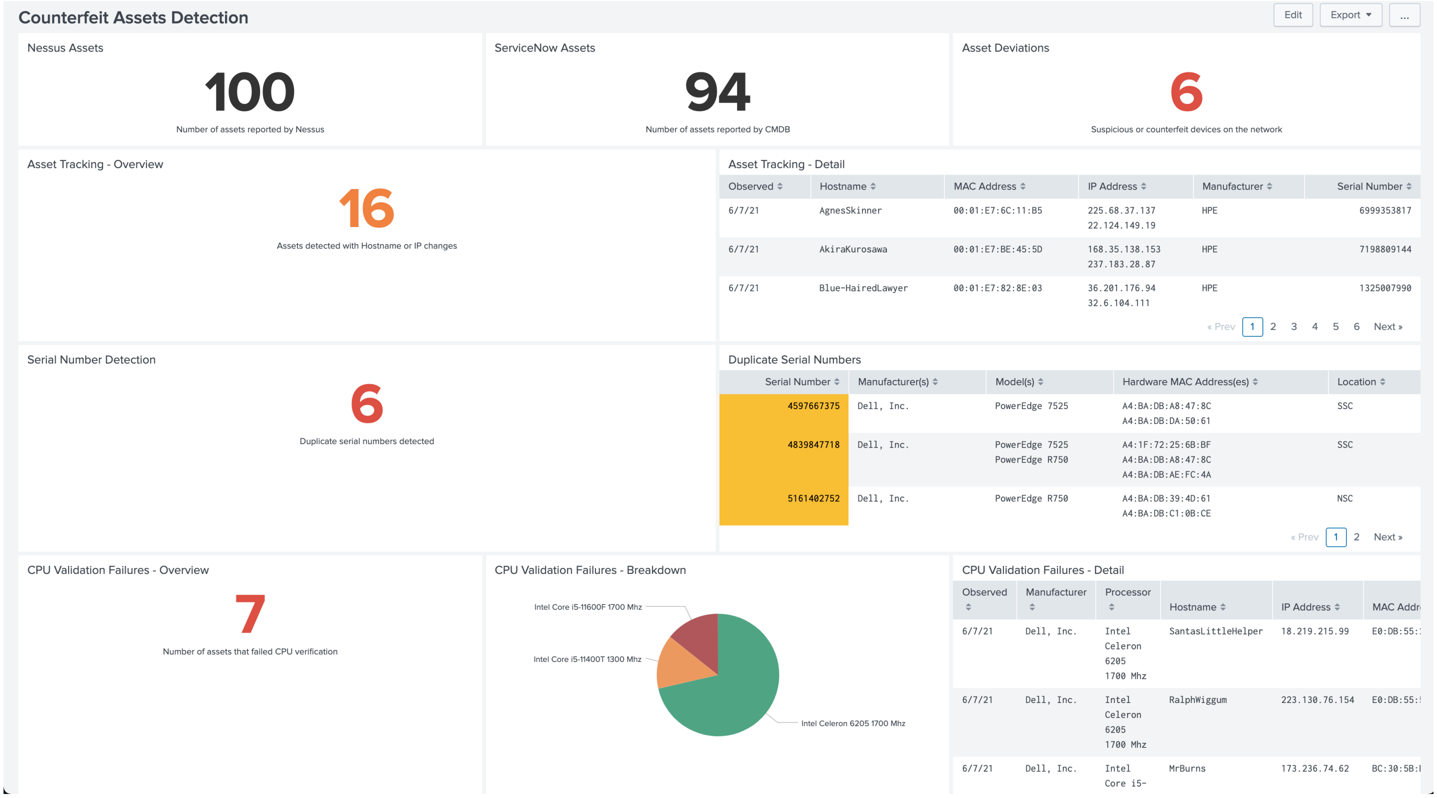


Top 5 Assets - Warranty Expiration

asset_tag	manufacturer	model_number	serial_number	warranty_expiration	datacenter	classification	host_name	mac_address	ip_address	short_description
P1000766	HPE	ProLiant DL180	3270420423	10/1/21	SSC	Production	Blue-HairedLawyer	00:01:E7:82:8E:03	32.6.104.111	
P1000812	Dell, Inc.	PowerEdge 7515	8930944465	11/5/21	SSC	Production	SeaCaptain	E0:DB:55:7B:72:FA	13.133.97.217	
P1000273	Dell, Inc.	PowerEdge R750	7998820392	12/8/21	NSC	Production	HermanHermann	A4:1F:72:C5:D7:A5	154.108.36.221	Domain Controller/Exchange Server/FTP Server
P1000781	Dell, Inc.	PowerEdge 7515	4594286433	12/17/21	SSC	Production	BabyGerald	A4:BA:DB:E4:44:F0	194.104.63.121	
P1000696	Dell, Inc.	PowerEdge R750	6317724227	12/18/21	NSC	Production	ItchynScratchy	A4:1F:72:54:BA:D4	120.97.14.16	Print Server / Mom Server / ADP Server

This is helpful for a high level overview of what's within our infrastructure as reported by CMDB.

Counterfeit Assets Detection Dashboard


Edit
Export ▾
...
Intel Core i5-11600F 1700 Mhz
Intel Core i5-11400T 1300 Mhz
Intel Celeron 6205 1700 Mhz

Counterfeit Assets Detection

Nessus Assets

100

Number of assets reported by Nessus

ServiceNow Assets

94

Number of assets reported by CMDB

Asset Deviations

6

Suspicious or counterfeit devices on the network

Asset Tracking - Overview

16

Assets detected with Hostname or IP changes

Asset Tracking - Detail

Observed	Hostname	MAC Address	IP Address	Manufacturer	Serial Number
6/7/21	AgnesSkinner	00:01:E7:6C:11:B5	225.68.37.137 22.124.149.19	HPE	6999353817
6/7/21	AkiraKurosawa	00:01:E7:BE:45:5D	168.35.138.153 237.183.28.87	HPE	7198809144
6/7/21	Blue-HairedLawyer	00:01:E7:82:8E:03	36.201.176.94 32.6.104.111	HPE	1325007990

« Prev 1 2 3 4 5 6 Next »

Serial Number Detection

6

Duplicate serial numbers detected

Duplicate Serial Numbers

Serial Number	Manufacturer(s)	Model(s)	Hardware MAC Address(es)	Location
4597667375	Dell, Inc.	PowerEdge 7525	A4:BA:DB:A8:47:8C A4:BA:DB:DA:50:61	SSC
4839847718	Dell, Inc.	PowerEdge 7525 PowerEdge R750	A4:1F:72:25:6B:BF A4:BA:DB:A8:47:8C A4:BA:DB:AE:FC:4A	SSC
5161402752	Dell, Inc.	PowerEdge R750	A4:BA:DB:39:4D:61 A4:BA:DB:C1:0B:CE	NSC

« Prev 1 2 Next »

CPU Validation Failures - Overview

7

Number of assets that failed CPU verification

CPU Validation Failures - Breakdown

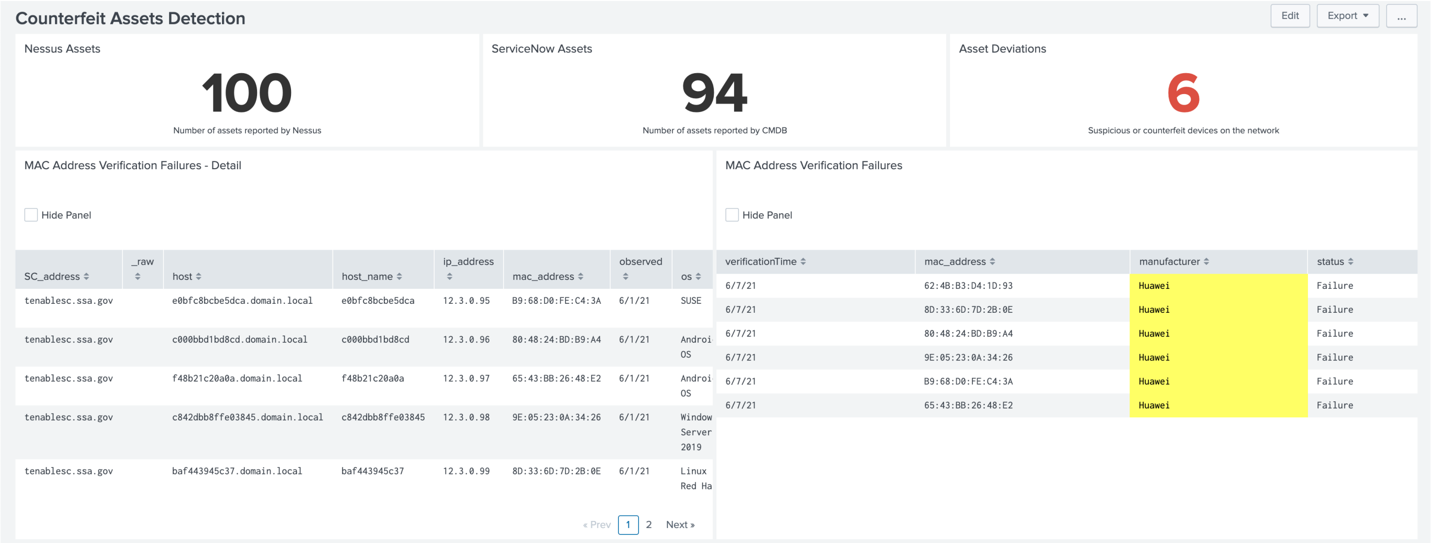
CPU Validation Failures - Detail

Observed	Manufacturer	Processor	Hostname	IP Address	MAC Addr
6/7/21	Dell, Inc.	Intel Celeron 6205 1700 Mhz	SantasLittleHelper	18.219.215.99	E0:DB:55:
6/7/21	Dell, Inc.	Intel Celeron 6205 1700 Mhz	RalphWiggum	223.130.76.154	E0:DB:55:
6/7/21	Dell, Inc.	Intel Core i5-	MrBurns	173.236.74.62	BC:30:5B:

Using the CMDB dashboard as an authoritative source on "what we know" to be in our datacenters, we can then leverage **Splunk's inherent ability to correlate across multiple, disparate data sources** and give us insights--in this case, "what we see" on the network via Nessus scans.

The Counterfeit Assets Detection Dashboard compares the CMDB inventory data to Nessus scans and reports on the deltas, which we can deem as "suspicious".

We can also drill down into those deltas and determine if there are any MAC address validation failures:



Counterfeit Assets Detection

Nessus Assets: **100**, Number of assets reported by Nessus

ServiceNow Assets: **94**, Number of assets reported by CMDB

Asset Deviations: **6**, Suspicious or counterfeit devices on the network

MAC Address Verification Failures - Detail

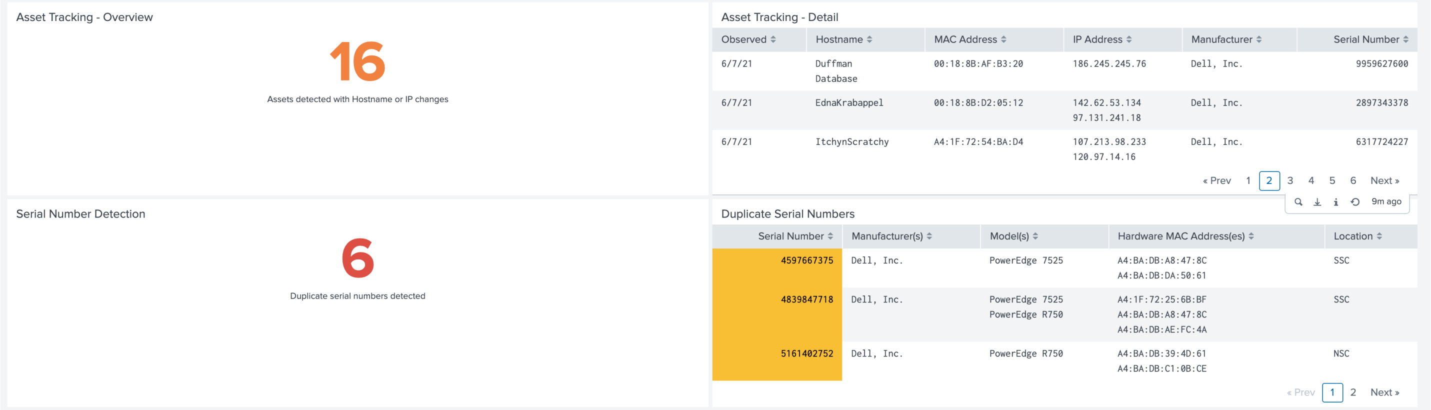
SC_address ⇕	_raw ⇕	host ⇕	host_name ⇕	ip_address ⇕	mac_address ⇕	observed ⇕	os ⇕
tenablesc.ssa.gov		e0bfc8bcbe5dca.domain.local	e0bfc8bcbe5dca	12.3.0.95	B9:68:D0:FE:C4:3A	6/1/21	SUSE
tenablesc.ssa.gov		c000bbd1bd8cd.domain.local	c000bbd1bd8cd	12.3.0.96	80:48:24:BD:B9:A4	6/1/21	Androi OS
tenablesc.ssa.gov		f48b21c20a0a.domain.local	f48b21c20a0a	12.3.0.97	65:43:BB:26:48:E2	6/1/21	Androi OS
tenablesc.ssa.gov		c842dbb8ffe03845.domain.local	c842dbb8ffe03845	12.3.0.98	9E:05:23:0A:34:26	6/1/21	Window Server 2019
tenablesc.ssa.gov		baf443945c37.domain.local	baf443945c37	12.3.0.99	8D:33:6D:7D:2B:0E	6/1/21	Linux Red Ha

MAC Address Verification Failures

verificationTime ⇕	mac_address ⇕	manufacturer ⇕	status ⇕
6/7/21	62:4B:B3:D4:1D:93	Huawei	Failure
6/7/21	8D:33:6D:7D:2B:0E	Huawei	Failure
6/7/21	80:48:24:BD:B9:A4	Huawei	Failure
6/7/21	9E:05:23:0A:34:26	Huawei	Failure
6/7/21	B9:68:D0:FE:C4:3A	Huawei	Failure
6/7/21	65:43:BB:26:48:E2	Huawei	Failure

> *If we're primarily a Dell/HPE shop, why are Huawei (Chinese vendor) devices showing up on our network?*

The dashboard also tracks assets as they move throughout the network: whether assets have multiple hostnames or IPs as compared to CMDB inventory data, as well as any assets that have duplicate serial numbers:



Asset Tracking - Overview: **16**, Assets detected with Hostname or IP changes

Serial Number Detection: **6**, Duplicate serial numbers detected

Asset Tracking - Detail

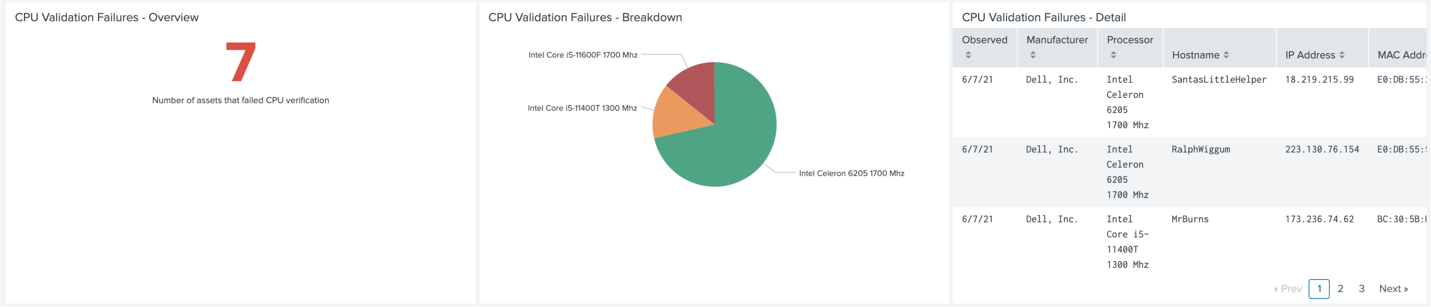
Observed ⇕	Hostname ⇕	MAC Address ⇕	IP Address ⇕	Manufacturer ⇕	Serial Number ⇕
6/7/21	Duffman Database	00:18:8B:AF:B3:20	186.245.245.76	Dell, Inc.	9959627600
6/7/21	EdnaKrabappel	00:18:8B:D2:05:12	142.62.53.134 97.131.241.18	Dell, Inc.	2897343378
6/7/21	ItchynScratchy	A4:1F:72:54:BA:D4	107.213.98.233 120.97.14.16	Dell, Inc.	6317724227

Duplicate Serial Numbers

Serial Number ⇕	Manufacturer(s) ⇕	Model(s) ⇕	Hardware MAC Address(es) ⇕	Location ⇕
4597667375	Dell, Inc.	PowerEdge 7525	A4:BA:DB:A8:47:8C A4:BA:DB:DA:50:61	SSC
4839847718	Dell, Inc.	PowerEdge 7525 PowerEdge R750	A4:1F:72:25:6B:BF A4:BA:DB:A8:47:8C A4:BA:DB:AE:FC:4A	SSC
5161402752	Dell, Inc.	PowerEdge R750	A4:BA:DB:39:4D:61 A4:BA:DB:C1:0B:CE	NSC

> *Duplicate serial numbers could indicate hardware spoofing, and multiple IP addresses suggest an asset is being moved or the CMDB information is outdated.*

Finally, I used Nessus scans and CMDB inventory data to detect if any hardware is modified in the datacenter, such as CPUs being stolen or replaced with a lower-spec model.



CPU Validation Failures - Overview

7

Number of assets that failed CPU verification

CPU Validation Failures - Breakdown

Intel Core i5-11600F 1700 Mhz
Intel Core i5-11400T 1300 Mhz
Intel Celeron 6205 1700 Mhz

CPU Validation Failures - Detail

Observed	Manufacturer	Processor	Hostname	IP Address	MAC Addr
6/7/21	Dell, Inc.	Intel Celeron 6205 1700 Mhz	SantasLittleHelper	18.219.215.99	E0:DB:55:
6/7/21	Dell, Inc.	Intel Celeron 6205 1700 Mhz	RalphWiggum	223.130.76.154	E0:DB:55:
6/7/21	Dell, Inc.	Intel Core i5-11400T 1300 Mhz	MrBurns	173.236.74.62	BC:30:5B:

> *We can easily observe server-grade processors (Intel Xeon and AMD Epyc) being replaced with consumer-grade processors (Intel Core i5 and Celeron) in some servers, because they use the same socket type.*

Summary & Impact

The solution was a huge hit with both ITOps and Security teams within SSA and I received great feedback. It clearly defined the concept of counterfeit assets, implemented SSA's existing tooling and workflow, and provided a creative solution that the agency hadn't considered before. Within a few days, our main champion at the agency described how excited everyone was so see the power of Splunk and this solution. She even suggested demo'ing it at a larger multi-agency conference, so other agencies could adopt it.

This solution successfully staved off ServiceNow's efforts to dethrone Splunk as the de facto platform for IT Operations at SSA.