

Counterfeit Assets Detection w/ Splunk Enterprise

January 2022

Kyle Raftery | Account Executive

Tyler Rodichok | Sr. Solutions Engineer

splunk> turn data into doing™



Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

A discussion of factors that may affect future results is contained in our most recent annual report on Form 10-K and subsequent quarterly reports on Form 10-Q, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov, including descriptions of the risk factors that may impact us and the forward-looking statements made in this presentation. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2021 Splunk Inc. All rights reserved.

Agenda

⇒ Detecting & Tracking Counterfeit Assets with Splunk

⇒ Demo

- CMDB Asset Inventory
- Correlating Disparate Data Sources to Detect Suspicious or Counterfeit Assets

⇒ Next Steps



Defining Counterfeit Assets

Everyone has a different definition

- Suspicious/abnormal assets detected on the network
- Suspicious/abnormal assets discovered in the datacenter
- Assets' hardware modified from manufacturer (supply chain attack)

Detecting Counterfeit Assets

**What we Know
- or Think**

Hardware POs

Inventory Sheets

Asset Tags

Discovery
Scans

SN CMDB CI
Records

MAC Address
Serial Number
Hostname
RFID Tag ID

*nix logs

Windows
events

Nessus Scans

Wire data

VPN Logs

DHCP Logs

**What we See –
Real Time Data
Driven**

Firewall Logs



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

Detecting Counterfeit Assets

Splunk is the platform for continuous monitoring, visibility, analytics and automation

	CMDB Laptops, Servers, Configurations, etc.	What We Know
	Users Identity, Users, Roles	
	Inventory Purchase Orders, Vendor Checks, etc.	
	Network Wire Data, Firewall Logs, etc.	
	Applications Usage, Experience, Performance, Quality	
	Security Threats, Behavior, Anomalies	



- Real-Time Visibility**
- Continuous Monitoring**
- Behavior Analytics**
- Continuous Risk Scoring**
- Automation/Orchestration**
- Compliance**
- Service Insights**



SaaS



Cloud

No System Is Perfect

Notable Implementations

Physical Security

Access Control

Monitoring

RFID tags

Tamper-proof chassis + racks

Agency-Supplier Relationship

Immutable Fabric

Case Study: Microsoft Corp. uses Blockchain + Splunk for supply chain insight

US Federal Agency Implementation: Existing Workflow Does Not Change

Detecting Counterfeit Assets

- > Datacenter Team receives hardware
- > applies RFID tag
- > scans into VisiTrac Asset Manager
- > VisiTrac communicates with ServiceNow CMDB (via JDBC call)
- > SNOW CMDB bi-directional communication with Splunk

Demo

splunk® turn data into doing™



splunk>enterprise Apps ▾

Administrator 5 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Datasets Reports Alerts Dashboards

Counterfeit Assets Detection Demo

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

Observed	Hostname	MAC Address	IP Address	Manufacturer	Serial Number
9/7/21	AgnesSkinner	00:01:E7:6C:11:B5	225.68.37.137 22.124.149.19	HPE	6999353817
9/7/21	AkiraKurosawa	00:01:E7:BE:45:5D	168.35.138.153 237.183.28.87	HPE	7198809144
9/7/21	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

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	DC2
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	DC2
5161402752	Dell, Inc.	PowerEdge R750	A4:BA:DB:39:4D:61 A4:BA:DB:C1:0B:CE	DC1

< Prev **1** 2 Next >

CPU Validation Failures - Overview **7** Number of assets that failed CPU verification

CPU Validation Failures - Breakdown

Processor	Hostname	IP Address	MAC Address
Intel Celeron 6205 1700 Mhz	SantasLittleHelper	18.219.215.99	E0:DB:55:23:9C
Intel Celeron 6205 1700 Mhz	RalphWiggum	223.130.76.154	E0:DB:55:50:DB
Intel Core i5-11400T 1300 Mhz	MrBurns	173.236.74.62	BC:30:5B:B8:92

CPU Validation Failures - Detail