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> turn data into doing

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

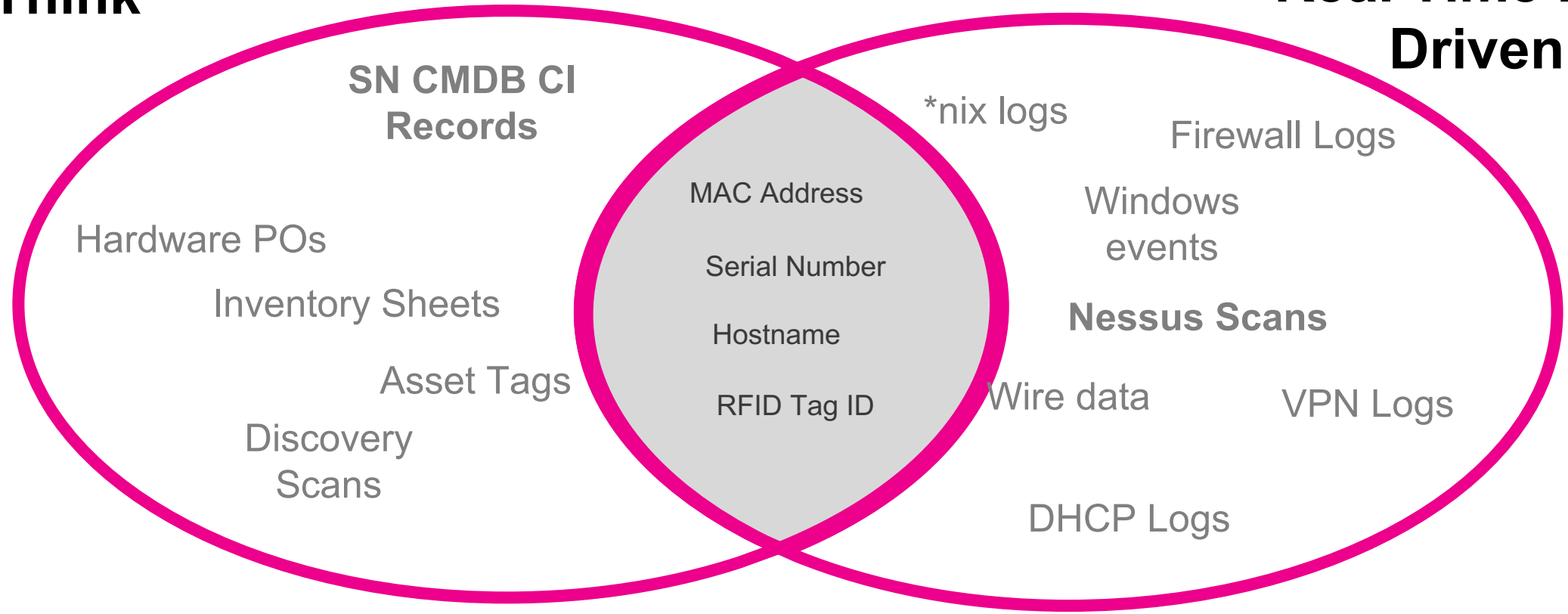
Everyone has a different definition

- 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

What we See – Real Time Data Driven



⚠ 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

What We Know

- **CMDB** — Laptops, Servers, Configurations, etc.
- **Users** — Identity, Users, Roles
- **Inventory** — Purchase Orders, Vendor Checks, etc.

What We See

- **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

splunk> turn data into doing

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™