Kick Starting A CMDB With Splunk

Stacy Patten

Cyber Security Operations Manager, QuikTrip

The Problem

- Existing SIEM offered little in the way of asset intelligence
- Islands of asset data
  - Active Directory
  - Network Management Tool
  - MDM
  - Client Management Tool
  - Spreadsheets
- Minimal ownership information
- Minimal application to asset relationships

The Solution

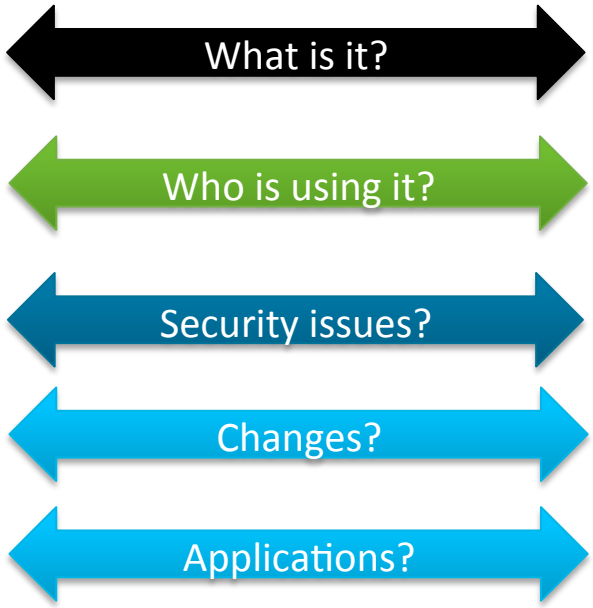
- Purchased Splunk & Splunk ES
- Professional Services assisted with implementation
  - Configuration of Splunk ES kicked off the asset plan
- What sources of data do we have?
- What is important or relevant?
- How can we use it?

The Result

- We have consolidated all asset sources into one repository.
- Now we can feed our CMDB with truth and expedite IT maturity.
- Now we know;
  - Hardware and/or OS
  - Who is using it
  - Where it is
  - What applications it is running
  - What it's talking to
  - Information Security issues
  - What changes were made by who

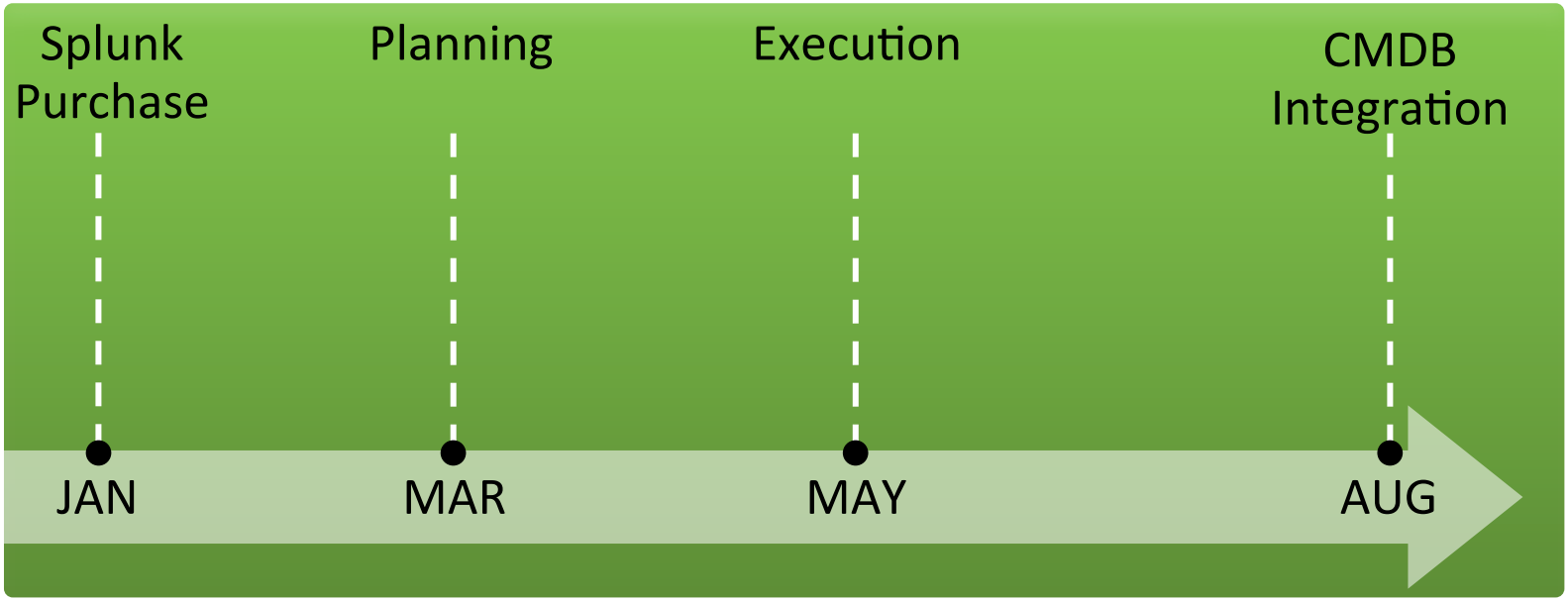
The How

splunk>



MDM	Network Mgmt.
Other SQL Data	MS SCCM
Active Directory	Splunk UF
Rapid7	Security Apps
Firewall Logs	Network Logs
App Logs	Splunk Stream

Asset Intelligence Timeline



THANK YOU

splunk>