

# The 10x Tool Development Force Multiplier For Workday

Ethan Lewis

Security Tools Development, Workday

.conf2016

splunk >

# Agenda

- Background
- Pre-Splunk Solution
- Splunk Rebuild
- Future

# Background



.conf2016

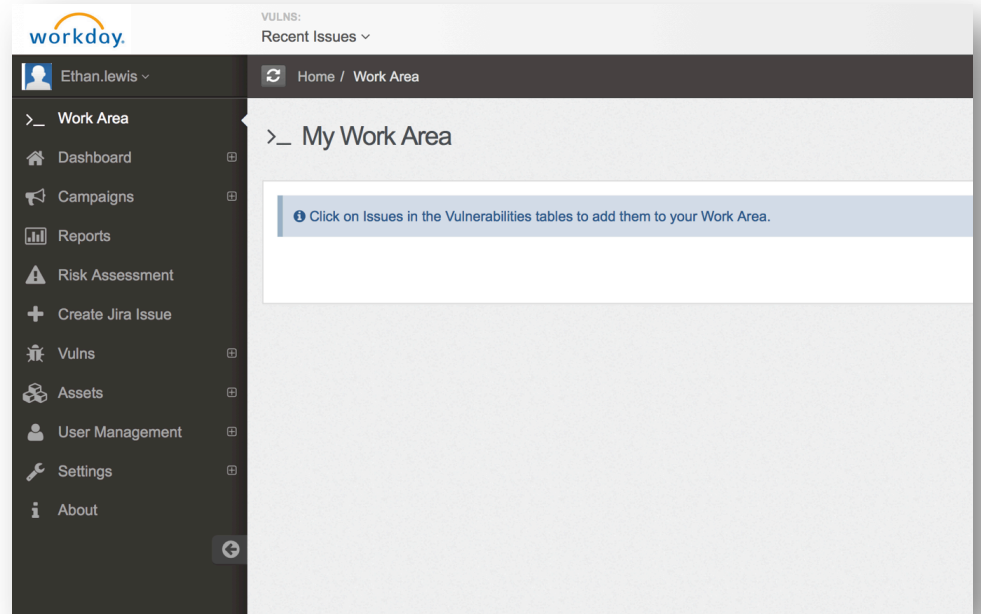
splunk >

# Goal: Vulnerability Management

- Merge data from multiple vulnerability sources
  - Automated scanning appliances
  - Internal and external penetration tests
- Integrate with ticketing systems
- Generate overview visualizations for management

# pre-Splunk

- Custom internal application
- Java backend
- Difficulties:
  - Long dev time for new features
  - Long onboarding for new developers
  - Limited support resources



# pre-Splunk

Total development time:

**2.50 years**

# Time Passes...



.conf2016

splunk >

# Enter splunk®

.conf2016

splunk®



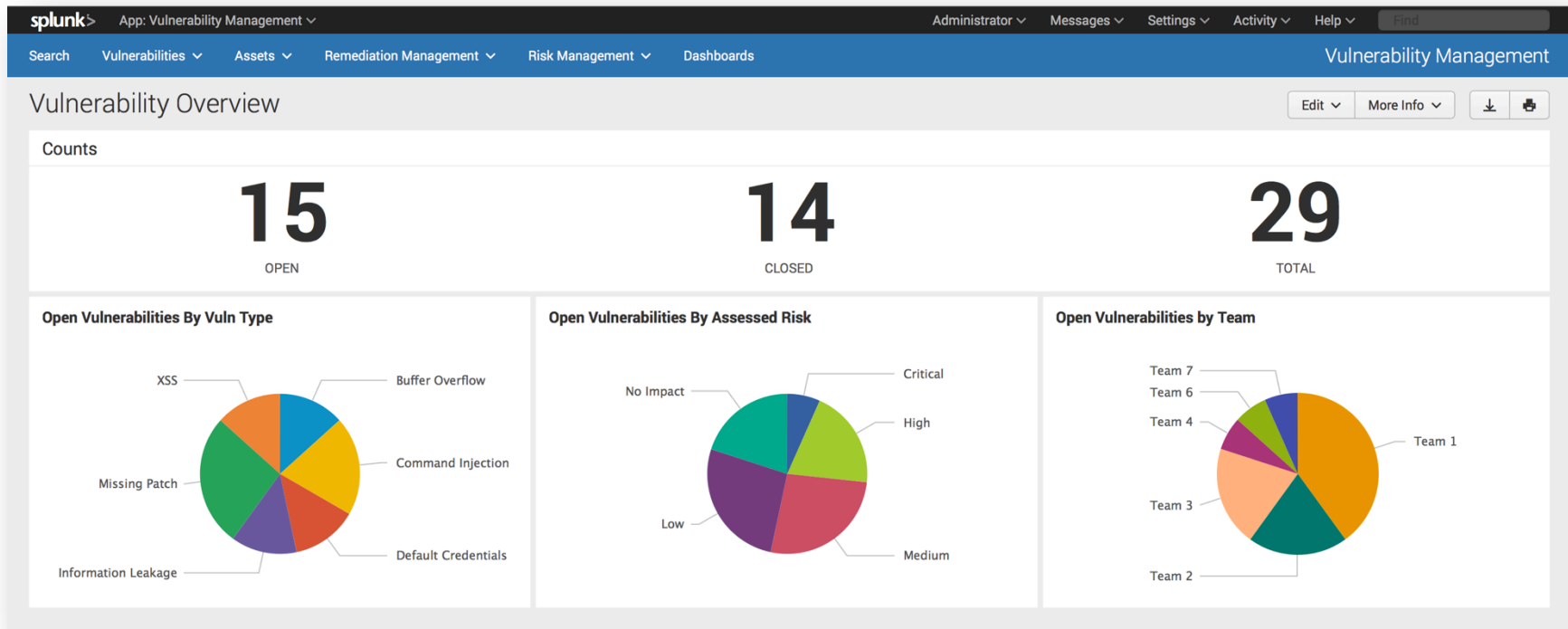
# post-Splunk

- Replicated tool functionality as a custom Splunk app
  - All existing reports and graphs
  - Ticketing integrations
- Immediate wins:
  - Two-way comparisons (e.g. all vulnerabilities on this host / all hosts with this vulnerability)
  - User creatable visualizations
  - Fewer bugs

# post-Splunk



# post-Splunk



# post-Splunk

splunk> App: Vulnerability Management ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Vulnerabilities ▾ Assets ▾ Remediation Management ▾ Risk Management ▾ Dashboards Vulnerability Management

## Asset Overview


View all assets defined in the INF Machine DB (MDB)

Data Center:  Silo:  Role:  Status:  Show IPs:

### Matching Assets


20

### Count By Data Center




Data Center	Count
DC1	15
DC3	3
DC2	2

### Count By Silo



Silo	Count
Silo1	10
Silo3	5
Silo2	5

### Count By Role



Role	Count
db	10
sv	5
fw	5

### Matching Asset Overview

dc	silo	role	fqdn	ip
DC1	Silo1	db	server1.dc1	127.0.0.1
DC1	Silo1	db	server2.dc1	11.102.234.0
DC1	Silo1	fw	server3.dc1	11.102.234.1
DC2	Silo1	fw	server1.dc2	11.102.234.2

# post-Splunk

The screenshot shows the Splunk Vulnerability Management interface. At the top, there is a navigation bar with 'splunk' and 'App: Vulnerability Management'. Below this is a secondary navigation bar with 'Search', 'Vulnerabilities', 'Assets', 'Remediation Management', 'Risk Management', and 'Dashboards'. The main header area includes 'Vulnerability Portal', 'Edit', 'More Info', and download/print icons. A search box for 'Vuln ID' contains '1234' and a 'Submit' button. The main content area is titled 'Overview' and features a large heading 'Ice cream fridge not properly secured'. Below the heading are three large numbers: '1234' (Vuln ID), '5' (Severity), and '8' (Currently Vulnerable Assets). A table below shows the 'Currently Vulnerable' assets with columns for 'current\_status', 'dc', 'silos', 'role', 'fqdn', and 'ip'. The table contains one row with the following data: 'ACTIVE', 'DC2', 'Silo1', 'fw', 'server1.dc2', and '11.102.234.2'.

App: Vulnerability Management

Administrator Messages Settings Activity Help Find

Search Vulnerabilities Assets Remediation Management Risk Management Dashboards Vulnerability Management

Vulnerability Portal Edit More Info

Vuln ID 1234 Submit

Overview

## Ice cream fridge not properly secured

1234 Vuln ID

5 Severity

8 Currently Vulnerable Assets

Assets

Currently Vulnerable

current_status	dc	silos	role	fqdn	ip
ACTIVE	DC2	Silo1	fw	server1.dc2	11.102.234.2

# post-Splunk

- Splunk advantages:
  - UI / visualizations / access control for free
  - New reports immediately using Splunk SPL, instead of weeks
  - Easily integrate new data sources
  - Piggyback on our existing Operations team and infrastructure

# post-Splunk

Total development time to date:

**0.25 years**

# THANK YOU

.conf2016