The 10x Tool
Development Force Multiplier For Workday

Ethan Lewis

Security Tools Development, Workday

Agenda

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

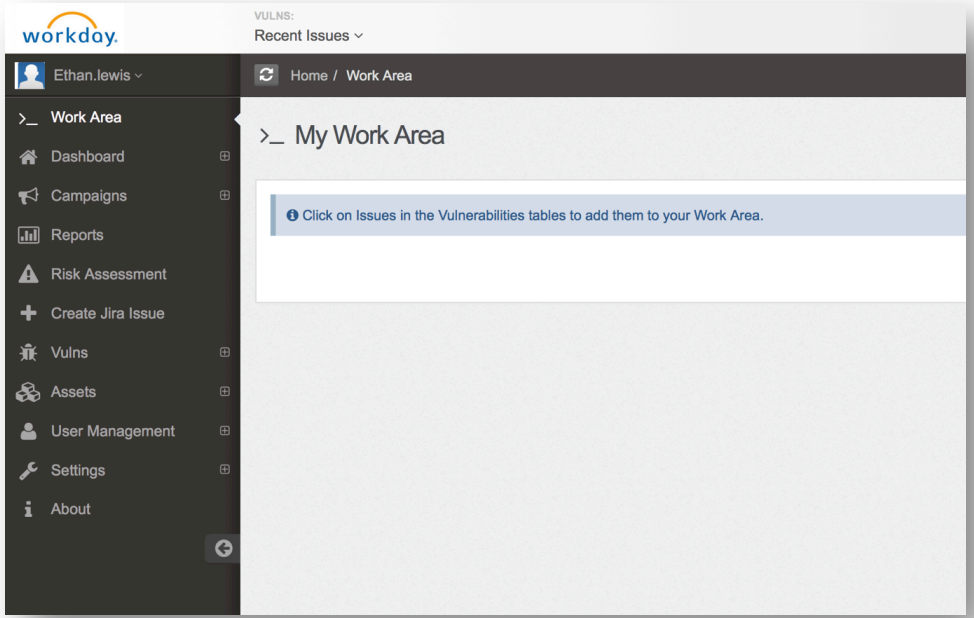
Background

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

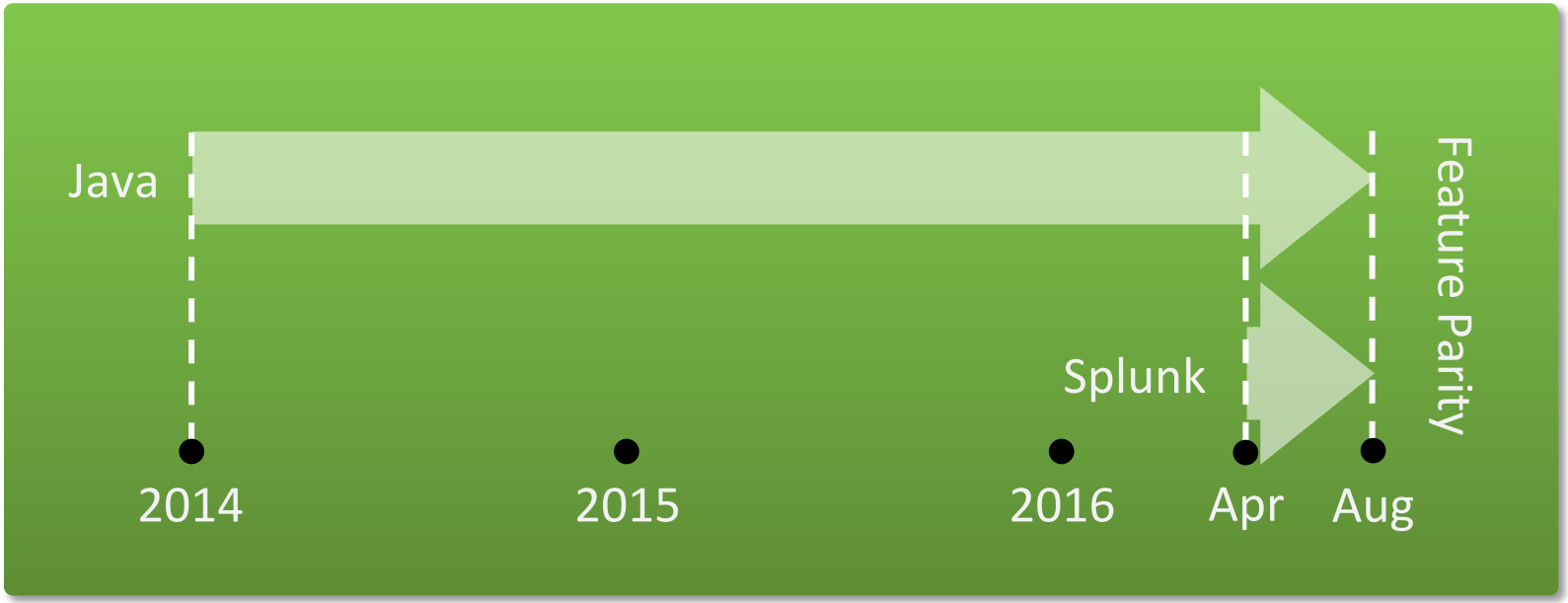
Time Passes…


Enter splunk>
.conf2016
splunk>

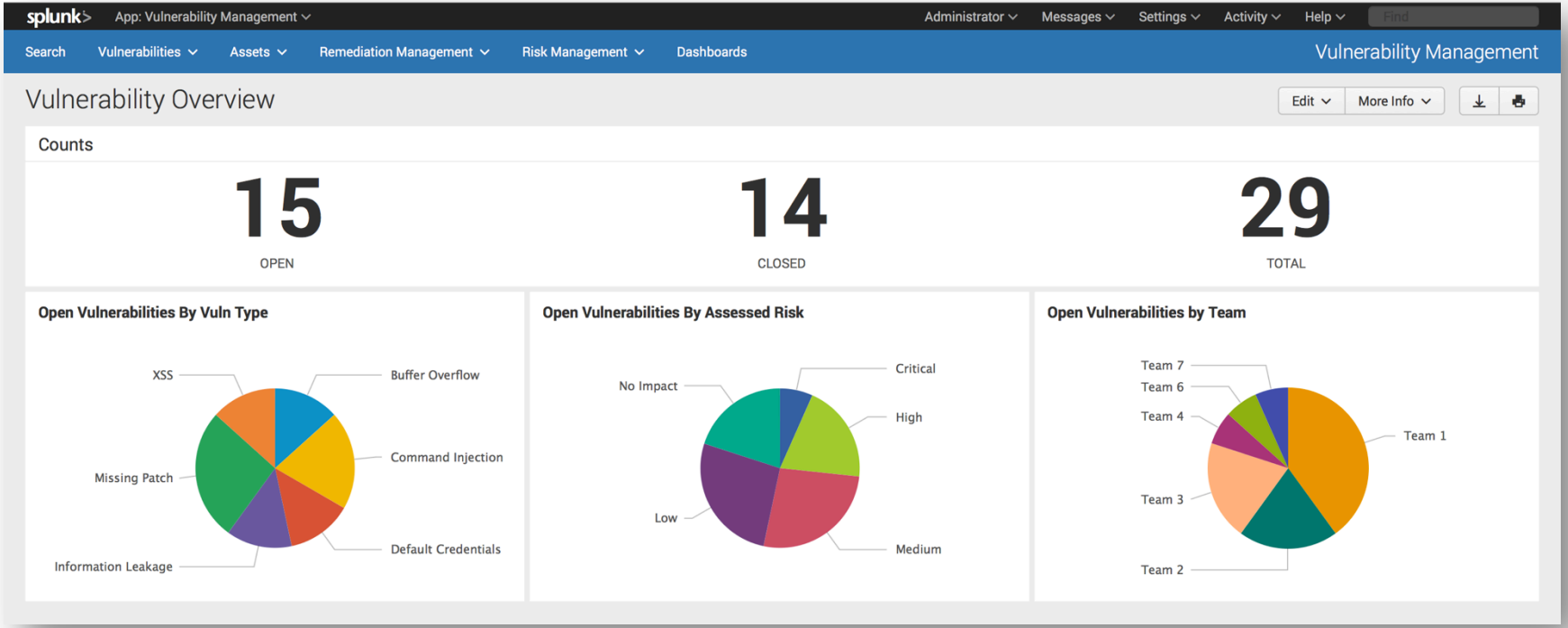
post-Splunk

- 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

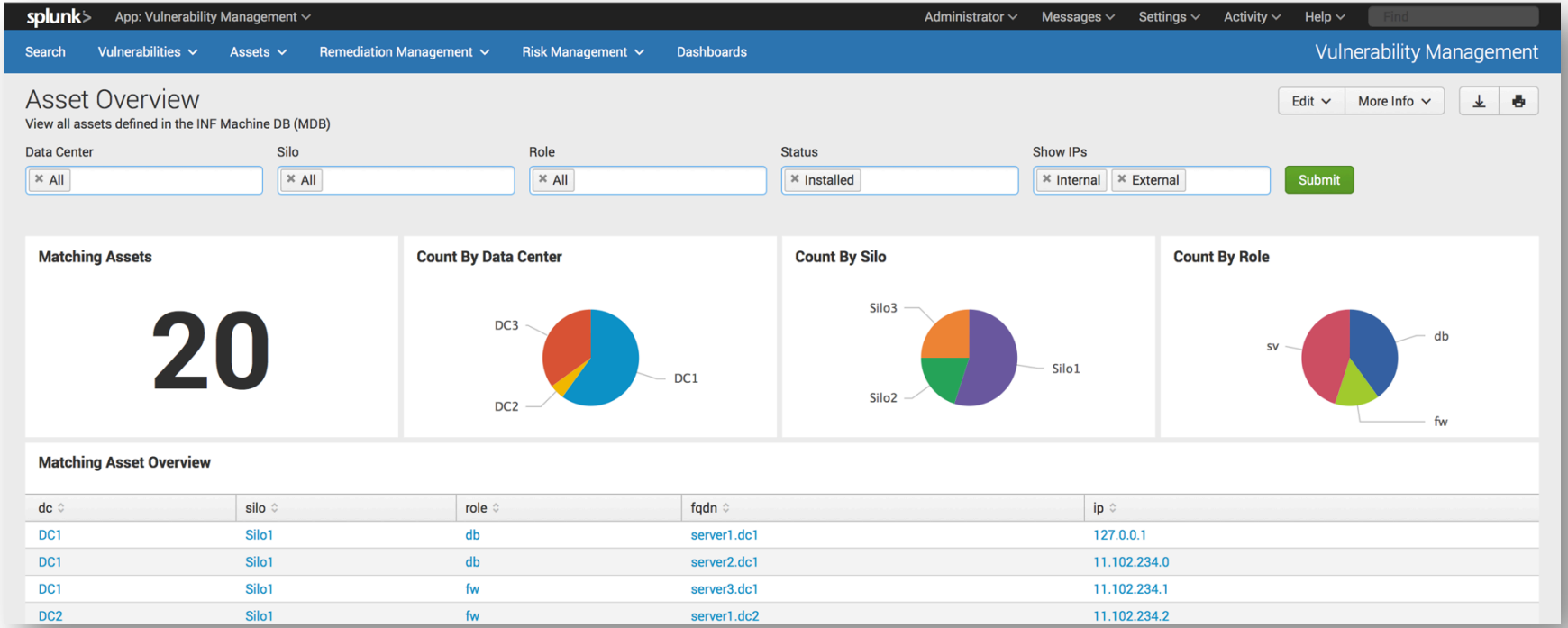
post-Splunk



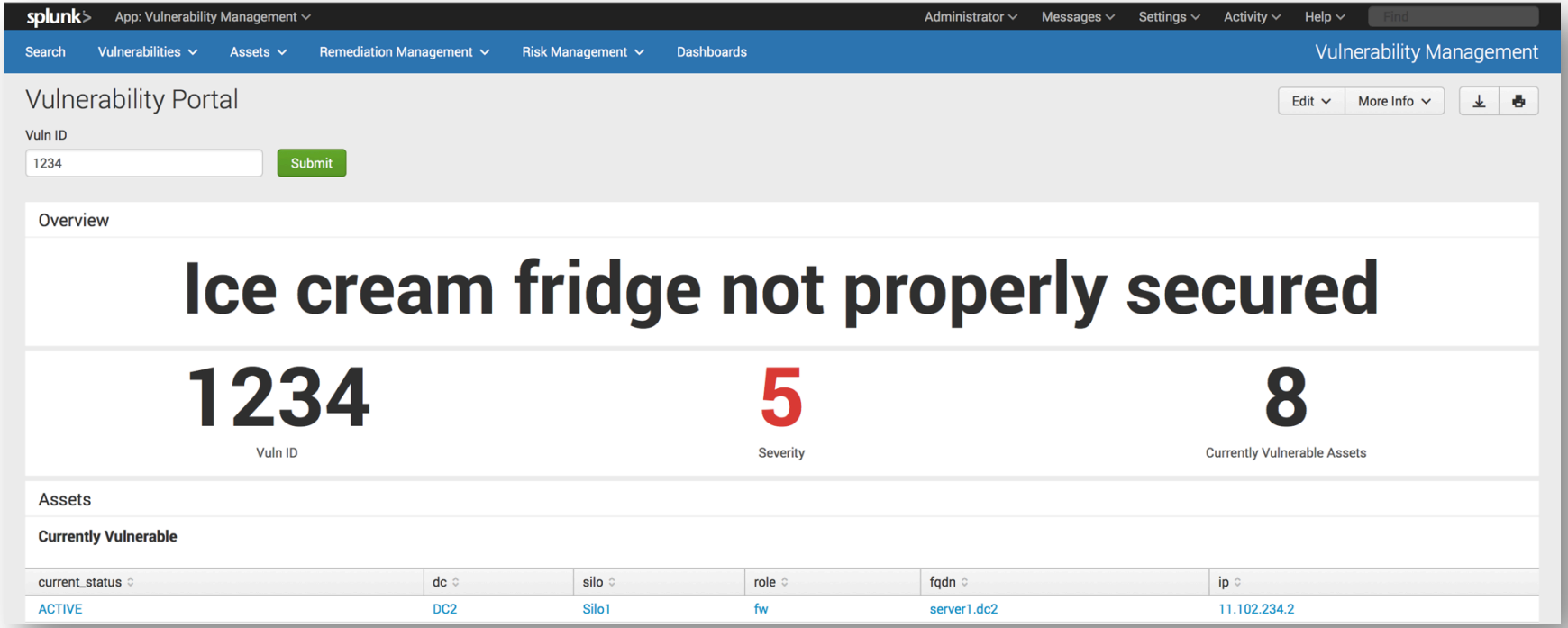
post-Splunk



post-Splunk



post-Splunk



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

splunk>