SCAP Metrics

Metricon 4.0: A Case Study

Ed Bellis VP, CISO

Orbitz Worldwide

Context Matters...

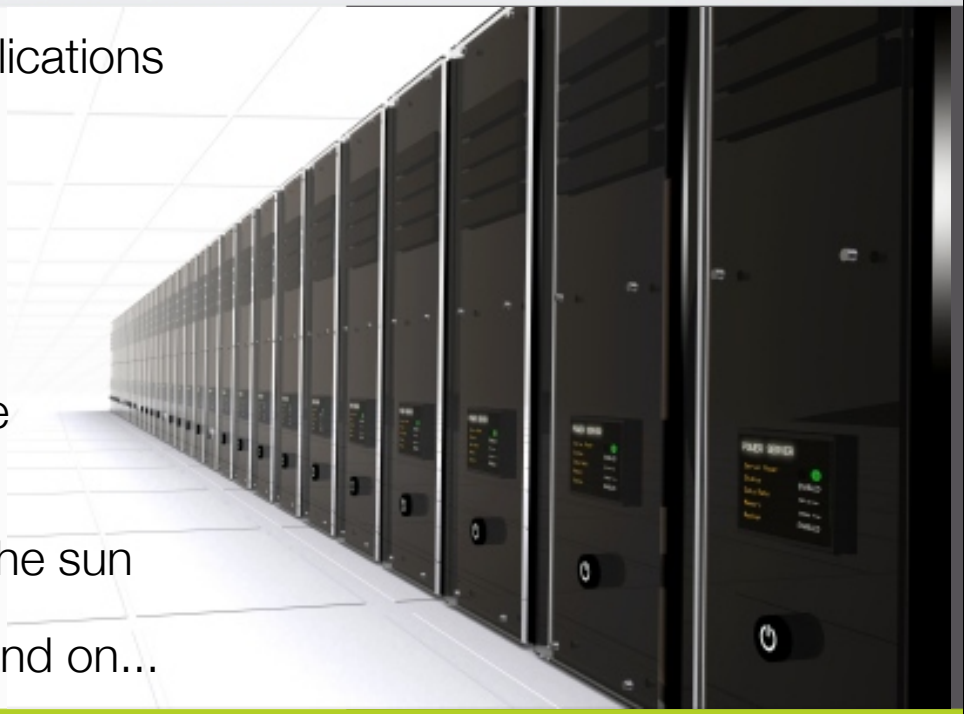
- Orbitz Worldwide
  - Orbitz & OFB
  - Cheaptickets
  - Away.com
  - eBookers
  - HotelClub & Rates2Go
  - Traveler Care
  - AA & NWA Booking engines
  - msn.orbitz.com
  - Southwest Hotels
  - Trip.com
  - Orbitzgames.com
  - RBS Rewards

...and on and on and on...

Context Matters...

- 100's of Endless Applications
- 1000's of Servers
- 1000's of Devices
- 100's of DBs
- Data centers: multiple continents
- Call centers - follow the sun

...and on and on and on...



Context Matters...

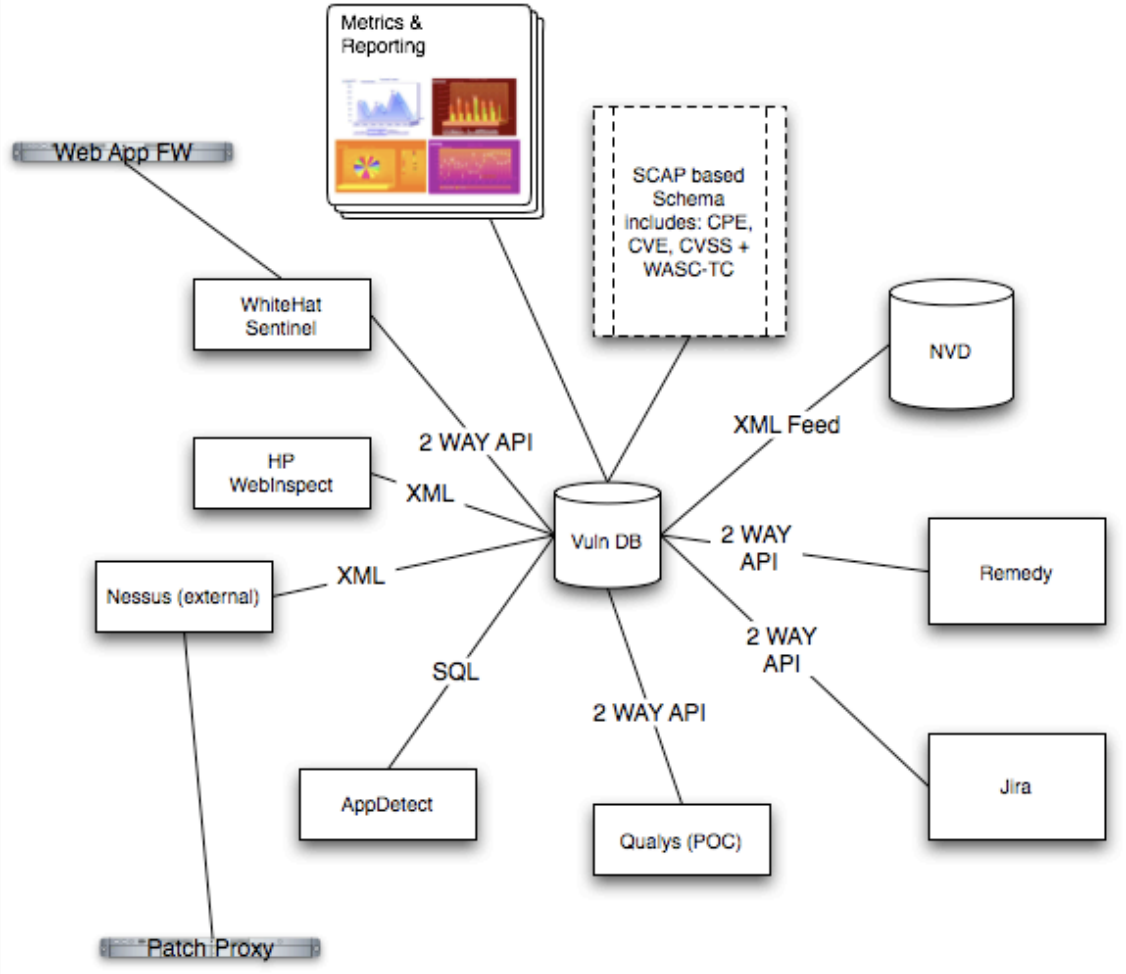
- VA Tools
  - Application
  - Network & Host
  - Database
- Remediation Tracking
  - Jira
  - Remedy

...and on and on and on...

Our Solution: A Case Study

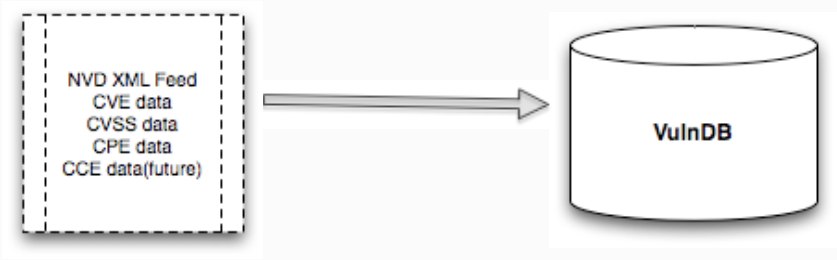
Using Standards to Compare & Measure

Centralizing the Data: Overview



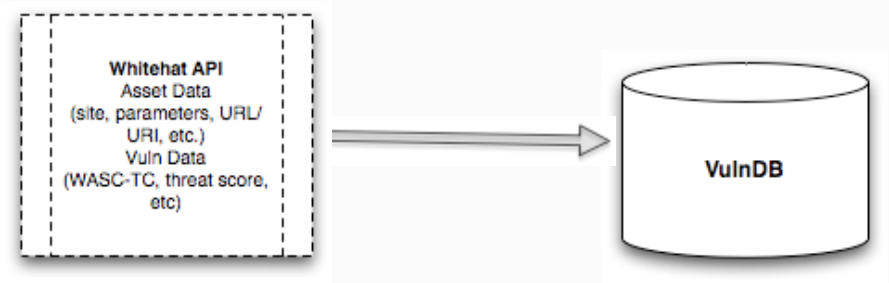
A Workflow Use Case

1. NVD feed is pulled in daily



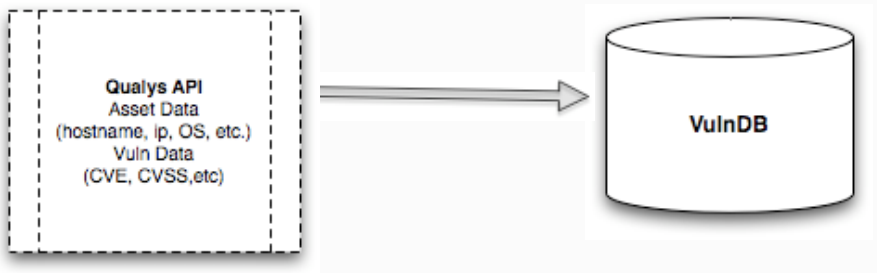
A Workflow Use Case

2. Whitehat connector runs on a predefined schedule.



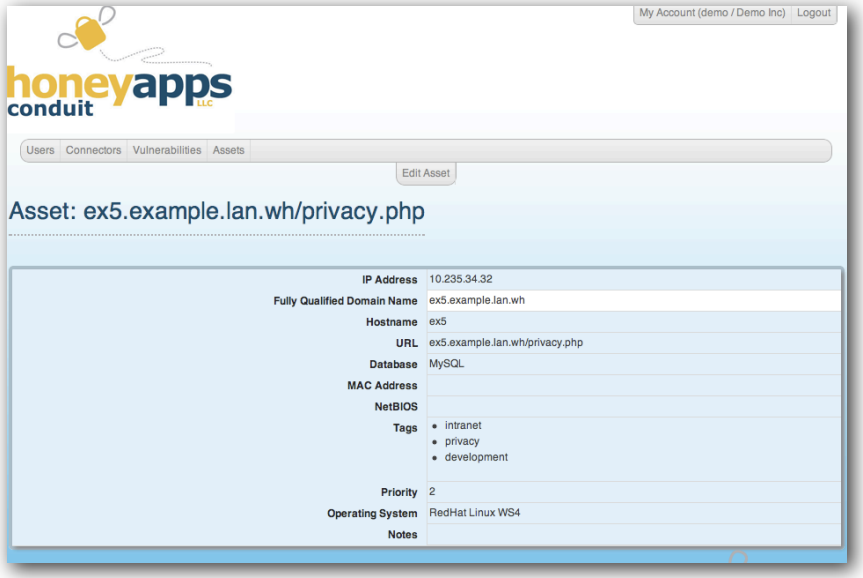
A Workflow Use Case

3. Qualys connector runs on a predefined schedule



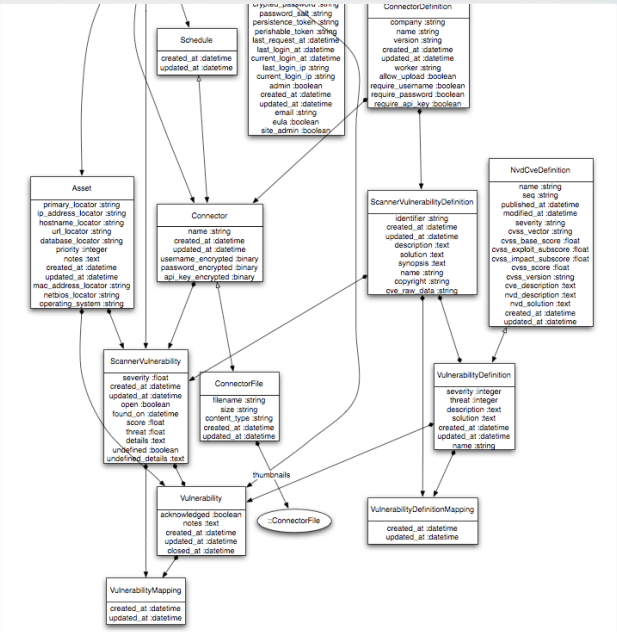
A Workflow Use Case

4. Security Admin manages and modifies asset information discovered by VA tools - CPE



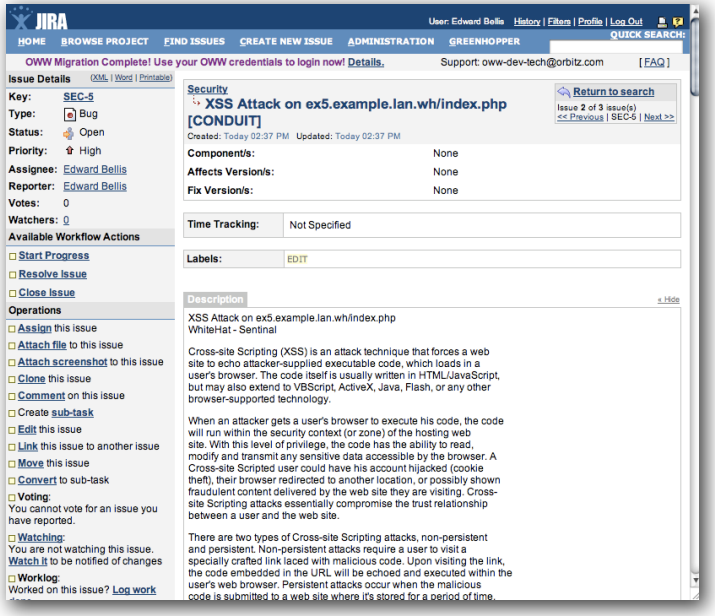
A Workflow Use Case

5. Vulnerability data is normalized and correlated across VA results utilizing CVE and WASC-TC. Vulns are scored using CVSS / WASC-TC plus Asset/CPE data.

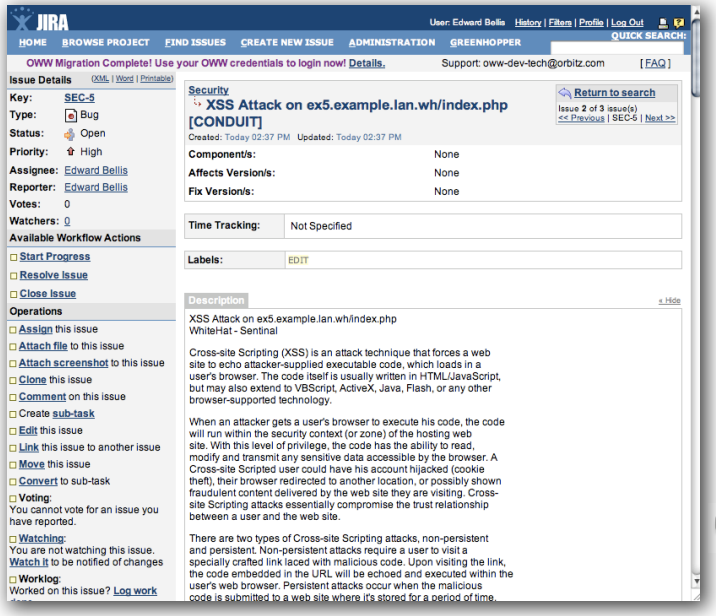


A Workflow Use Case

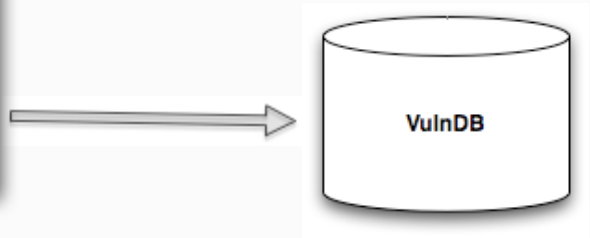
6. Single click defect creation from Conduit to Jira.



A Workflow Use Case

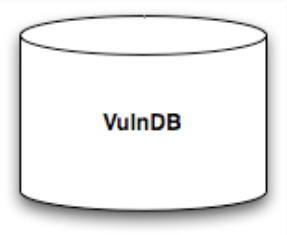


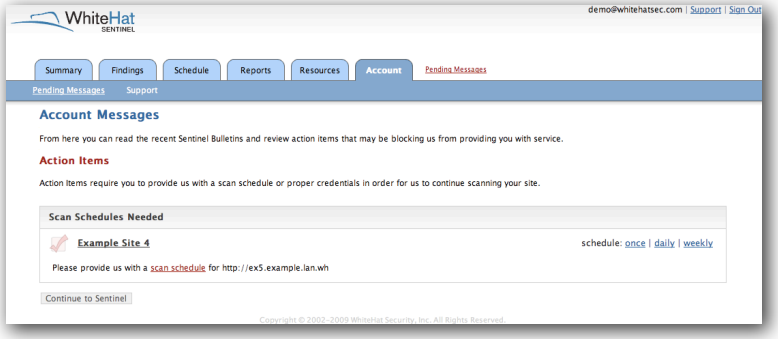
7. Security defect is remediated by developer and closed in Jira.



A Workflow Use Case

8. Conduit issues re-test of vulnerability via Sentinel API



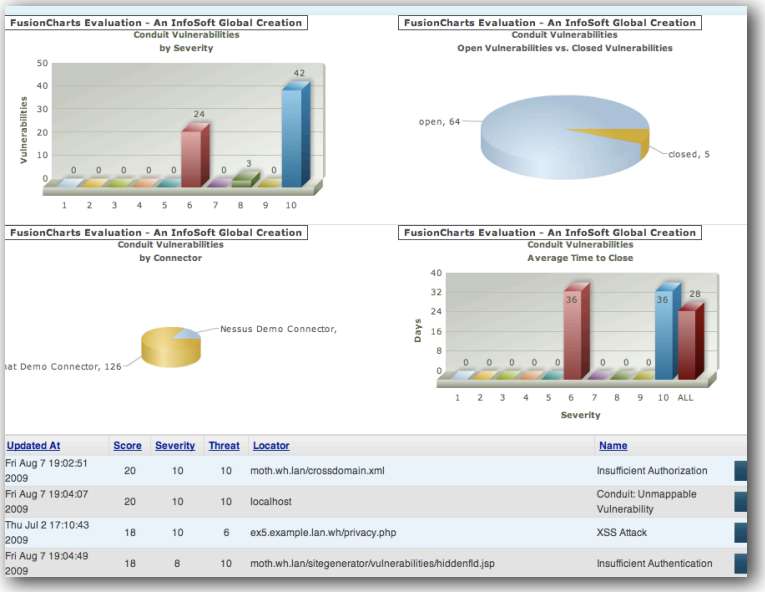


A Workflow Use Case

9. If re-test returns clean results are fed to Conduit and vulnerability is closed

A Workflow Use Case

10. Metrics can be viewed and filtered via tags added through asset mgmt



Metrics via Tag Lenses

- Pre-Defined Vulnerability Metrics
- Filtered by Asset Tags
- Many-to-Many Tag/Asset Relationship

The Standards

Today

CPE: Common Platform Enumeration
CVE: Common Vulnerability Enumeration
CVSS: Common Vulnerability Scoring System
WASC-TC: Web Application Security Consortium Threat Class

Roadmap

CCE: Common Configuration Enumeration
XCCDF: Extensible Configuration Checklist Description Format

Email: ebellis@orbitz.com
Twitter: http://www.twitter.com/ebellis

More Info On SCAP:
http://scap.nist.gov

More Info On Conduit:
http://conduit.honeyapps.com

Q&A