



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



ORBITZ[®]
WORLDWIDE




honeyapps
conduit LLC

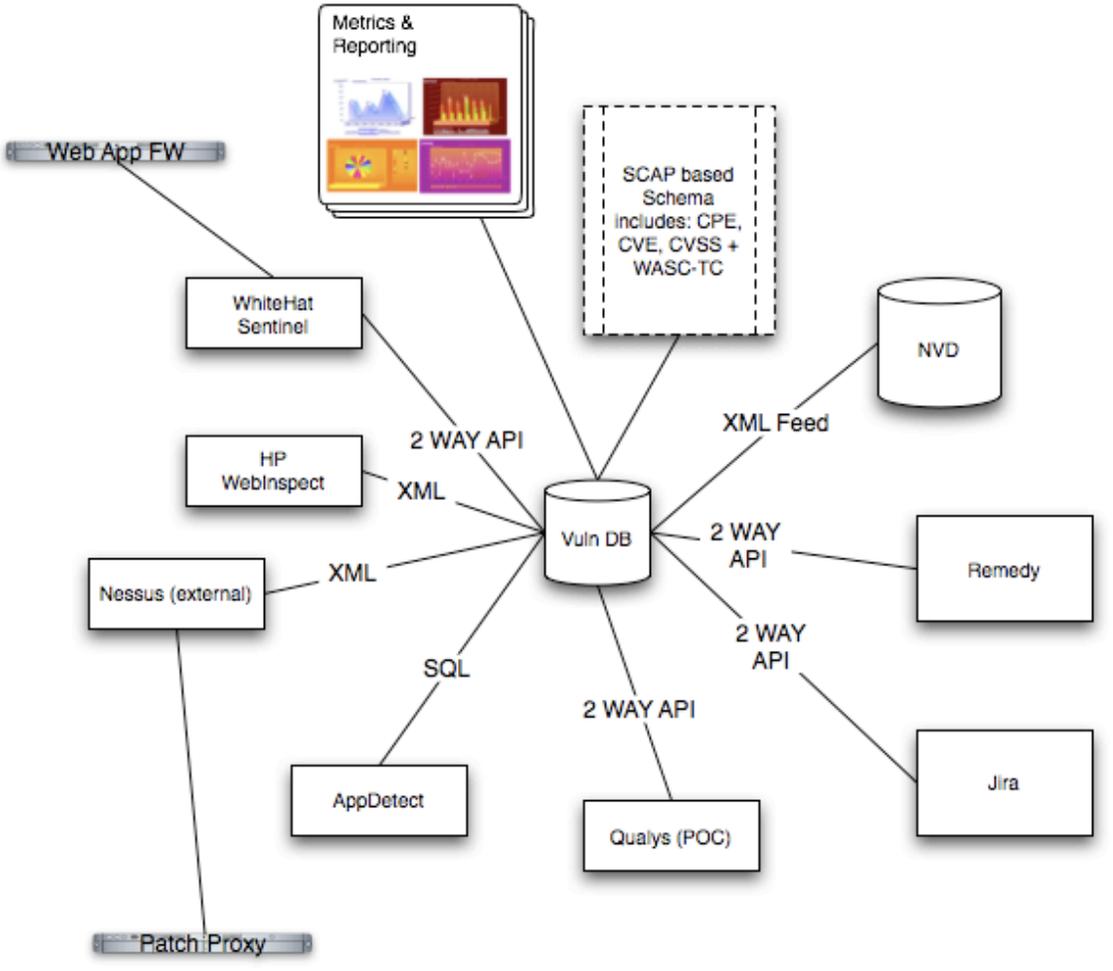
Using Standards to Compare & Measure



A word cloud of educational standards acronyms. The most prominent words are SCAP, CVSS, and OVAL. Other visible acronyms include WASC-TC, CVE, CWE, CP, CCEM, XCCDF, ARF, OCRL, CMSS, and CCSS.

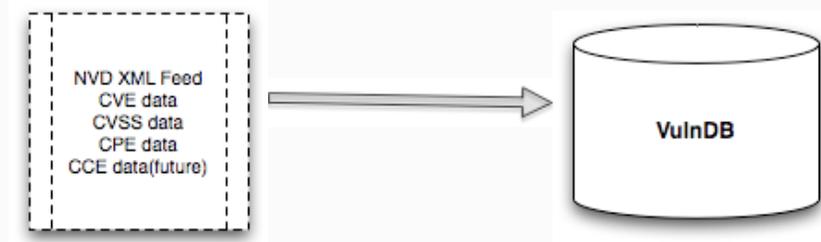
WASC-TC
SCAP
CVE
CWE
CP
CCEM
XCCDF
ARF
OCRL
CMSS
CCSS
OVAL
CVSS

Centralizing the Data: Overview



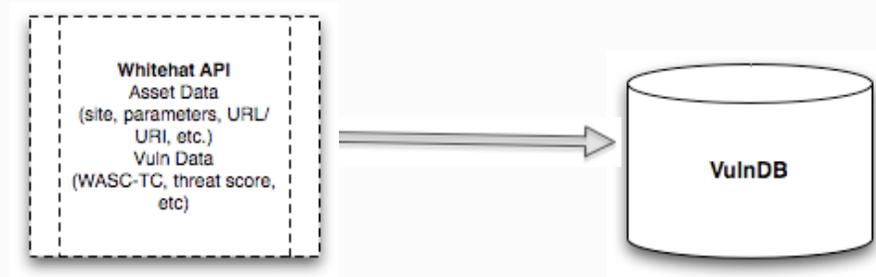
A Workflow Use Case

1. NVD feed is pulled in daily



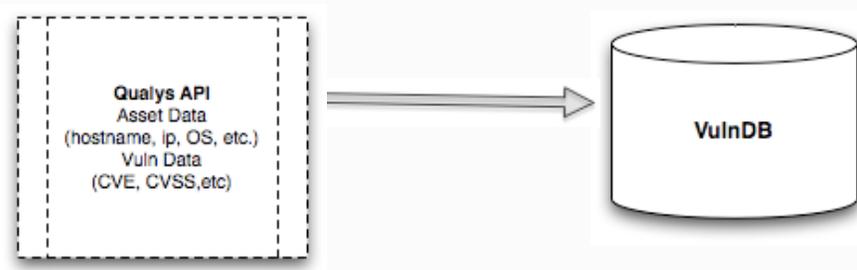
A Workflow Use Case

2. Whitehat connector runs on a predefined schedule.



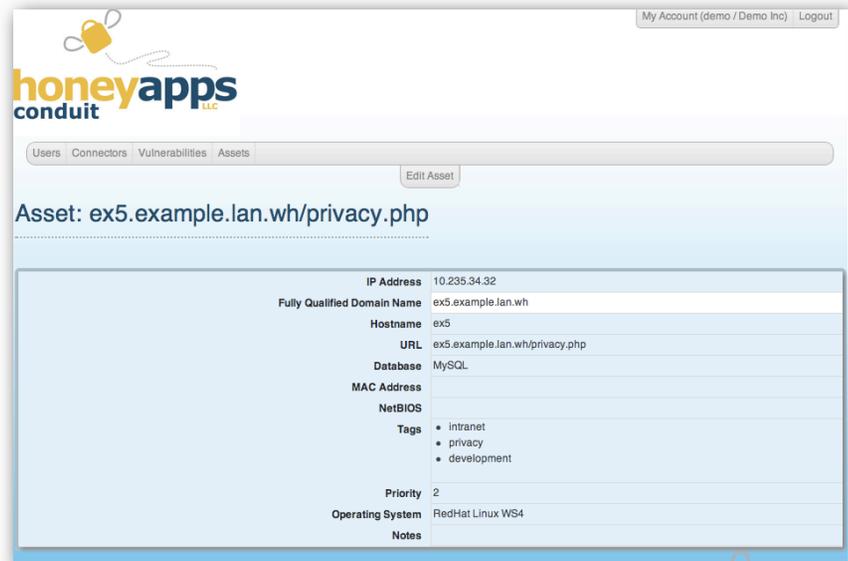
A Workflow Use Case

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

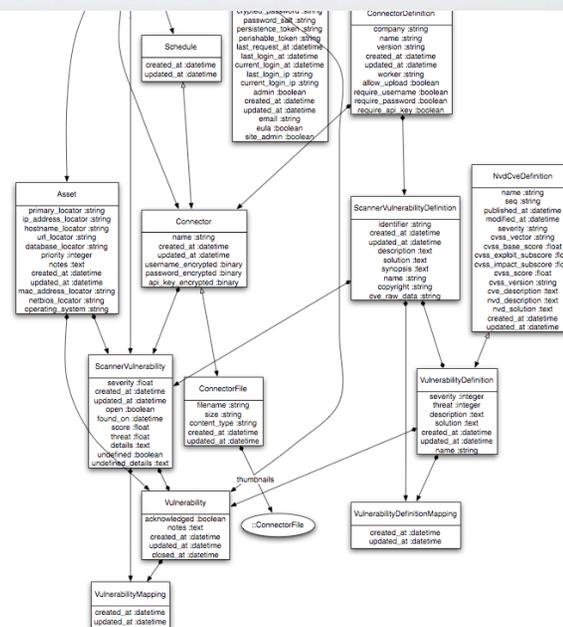


The screenshot displays the 'honeyapps conduit' web interface. At the top right, there is a user account link 'My Account (demo / Demo Inc) Logout'. Below the logo, a navigation bar contains 'Users', 'Connectors', 'Vulnerabilities', and 'Assets'. An 'Edit Asset' button is visible. The main content area shows the asset path 'Asset: ex5.example.lan.wh/privacy.php'. Below this, a table lists various attributes for the asset:

IP Address	10.235.34.32
Fully Qualified Domain Name	ex5.example.lan.wh
Hostname	ex5
URL	ex5.example.lan.wh/privacy.php
Database	MySQL
MAC Address	
NetBIOS	
Tags	<ul style="list-style-type: none">• intranet• privacy• development
Priority	2
Operating System	RedHat Linux WS4
Notes	

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.

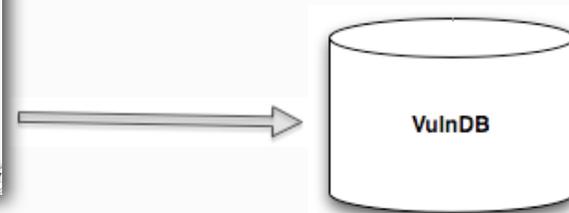


The screenshot shows the Jira issue details page for a security issue. The issue key is 'SEC-5', type is 'Bug', status is 'Open', and priority is 'High'. The assignee is 'Edward Bellis' and the reporter is 'Edward Bellis'. The issue title is 'XSS Attack on ex5.example.ian.wh/index.php [CONDUIT]'. The description includes a detailed explanation of Cross-site Scripting (XSS) attacks, noting that they force a user's browser to execute attacker-supplied code. The page also shows workflow actions like 'Start Progress', 'Resolve Issue', and 'Close Issue', along with a 'Description' field containing the attack details.

A Workflow Use Case

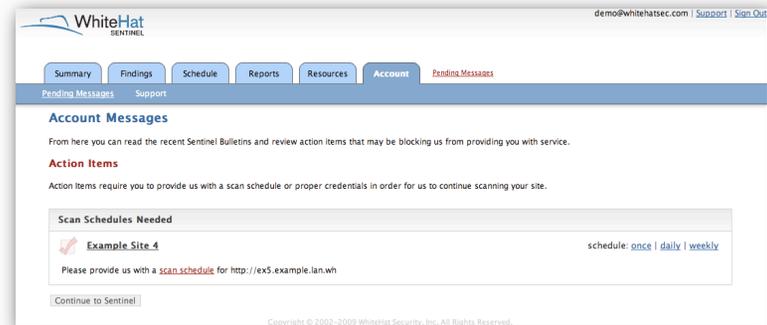
The screenshot shows a JIRA issue page for a security defect. The issue key is SEC-5, type is Bug, status is Open, and priority is High. The assignee and reporter are Edward Bellis. The issue title is "XSS Attack on ex5.example.ian.wh/index.php [CONDUIT]". The description details a Cross-site Scripting (XSS) attack on the specified URL, explaining that it forces a web site to execute attacker-supplied code, which can lead to account hijacking or data theft. The page also shows various workflow actions like "Start Progress", "Resolve Issue", and "Close Issue", and a "Description" section with a "Hide" button.

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



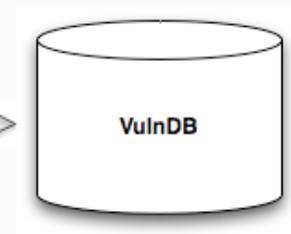
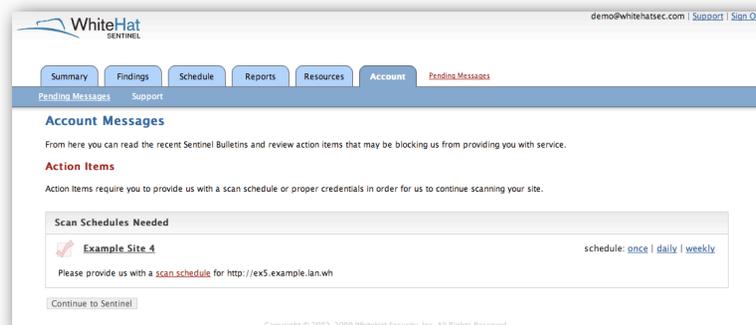
A Workflow Use Case

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



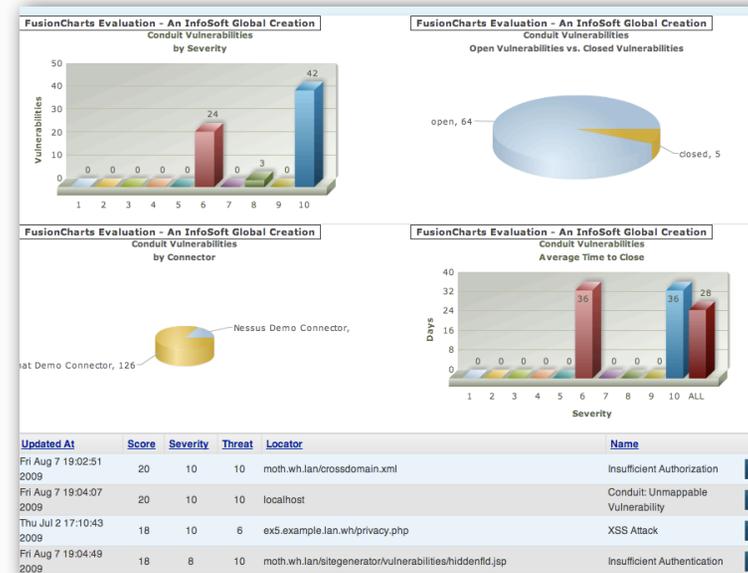
A Workflow Use Case

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