

2013 DHS S&T/DoD ASD (R&E)  
CYBER SECURITY SBIR WORKSHOP

# Code Dx: Visual analytics for triage of source code vulnerabilities

Secure Decisions, a division of Applied Visions, Inc.

Anita D'Amico

*July 24, 2013*



Homeland  
Security

Science and Technology



# Secure Decisions



We help you **make sense of data**

- Analyze security *decision-making* processes
- Build *visual analytics* to enhance security decisions and training

Our expertise starts where automated security sensors and scanners leave off

We **transition** our R&D into **operational use**, in government and industry



Grounded in commercial software and product development

- Division of Applied Visions, developer of commercial software
- 40 people, most with clearances, and secure facilities

# Hackers are paid bounties to find software flaws

## The New York Times

JULY 13, 2013

// In 2010, Google started paying hackers up to \$3,133.70 ... for bugs in its Web browser.

Last month, Microsoft sharply increased the amount it was willing to pay for such flaws, raising its top offer to \$150,000.

# Software Assurance

## *SwA Terminology*

**Weakness** Source code defect that an attacker *might* exploit

**Vulnerability** Source code defect *known* to be exploitable

- For simplicity, we'll use “vulnerability” in this presentation

**SAST** Static Application Security Testing tools

- Find vulnerabilities and poor quality in static source code
- Rapidly growing market

Commercial: Fortify, AppScan, Armorize ...

Open source: FindBugs, Jlint, cppcheck ...

**Focus of Code Dx**

**Other categories of tools**

**DAST** Dynamic Application Security Testing tools

- Penetration testing of web applications during execution

**Binary code analysis**

- Finding vulnerabilities through analysis of compiled code

# The Need

## *Stop shipping insecure software*



// **90%** of reported security incidents result from **exploits** of application software **defects**

**Build Security In Website, DHS**

<https://buildsecurityin.us-cert.gov/bsi/mission.html>

On average, one SAST tool finds only **14%** of vulnerabilities; you need lots of different tools to **cover** the vulnerabilities



50,000 weaknesses in 200,000 lines of code ...  
*Where do I start? What's most important?*



# Code Dx Approach

## *Find the most important vulnerabilities*

### Challenge

- Incomplete vulnerability coverage by single tool
- Difficult to compare tool results; different semantics
- Tens of thousands of vulnerabilities reported
- Format of results impedes communication and collaboration
- Expensive tools; hard to use for non-experts



### Code Dx Solution

- Imports and correlates results from multiple tools
- Normalizes results; common severity scale
- Visual analytics to rapidly triage results, remove false positives
- Common UI with custom detail for security analysts, developers, and CISOs
- *Code Dx Bundle* embeds open source SAST tools for use with or without commercial tools

# Visual Analytics for triage, remediation, and communication

Workflows tailored to each type of user

Code Qx SECURE DECISIONS  
version 0.9.6 - 6/14/2013

Home Projects About Admin Logout Logged in as [user]

WebGoat > Analysis Run 1 Created on 6/11/2013 Uploaded on 6/11/2013 2,123 total weaknesses Options

Weakness Flow

Displaying weaknesses whose Tool Overlaps is 1 Tool

Bulk Operations for the 1,953 matching weaknesses Select a status... Generate Report...

Weaknesses

Id	Tool	Severity	Codebase Location	Status
2074	Unreleased Resource - Database	High	MultiLevelLogin2.java	New
2006	Unreleased Resource - Database	High	RefreshDBScreen.java	New
1996	Unreleased Resource - Database	High	RandomLessonAdapter.java	New
1941	Unreleased Resource - Database	High	MultiLevelLogin2.java	New
1920	Unreleased Resource - Database	High	UpdateProfile_I.java	New
1857	Unreleased Resource - Database	High	MultiLevelLogin2.java	New
1851	Unreleased Resource - Database	High	SqlNumericInjection.java	New
1786	Unreleased Resource - Database	High	UpdateProfile_I.java	New
1754	Unreleased Resource - Database	High	DatabaseUtilities.java	New
1748	Unreleased Resource - Database	High	SqlNumericInjection.java	New
1740	Unreleased Resource - Database	High	SqlModifyData.java	New
1735	Unreleased Resource - Database	High	RandomLessonAdapter.java	New
1714	Unreleased Resource - Database	High	RandomLessonAdapter.java	New
1667	Unreleased Resource - Database	High	BackDoors.java	New
1661	Unreleased Resource - Database	High	MaliciousFileExecution.java	New
1648	Unreleased Resource - Database	High	BlindNumericSqlInjection.java	New
1641	Unreleased Resource - Database	High	MultiLevelLogin1.java	New
1628	Unreleased Resource - Database	High	StoredXss.java	New
1622	Unreleased Resource - Database	High	SqlStringInjection.java	New

Visualize thousands of weaknesses in a single view

Interactively, powerful filtering

Quickly and effectively triage large weakness lists

# Benefits

- **Better Coverage** - Find more important vulnerabilities
  - **Combine** multiple tool results to find **more** vulnerabilities
  - **Prioritize** combined results to highlight **most important**
  - **Filter out** overlapping results and false positives
- **Efficiency** - Save remediation **time** and **resources**
  - Developers can remediate **highest priority** vulnerabilities first
    - *Remediation can take 7–10 hours per vulnerability*
- **Communicate** more effectively up and down the chain
  - Visual analytics and reports, based on **roles** and **expertise**
- **Easy** to get started
  - *Code Dx Bundle* (Q4 2013) **auto-runs** open source tools
  - **Affordable** to small and mid-sized businesses

# Current Status

## Technology Readiness Level 7

- More than **10 beta testers**, incl. ITT, NSA, Raytheon, RTI, Univ. of Nebraska ...
- Systematic collection of **feedback**

*"I really like the visualization. ..tying [the tools] together and being able to work with that data is very useful."*

*"...at the present state, it seems to require the user to do a lot of work and formatting that the software itself could do."*

*"After a few minutes, I was able to manipulate the filters well enough to focus on particular discoveries."*

- Currently being **evaluated** by NIST, DHS S&T CIO, TSA, McAfee, Domestic Nuclear Detection Office, Indiana Univ.
- Working with Morgridge Institute to integrate into **SWAMP**
- **Training** program already developed



# Code Dx Roadmap

Version	Description	Target Users	Anticipated Release																	
			13	2014				2015												
			Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4									
Bundle 1.0	Embeds and auto-runs open source tools within Code Dx	Small businesses; Commercial SAST tool users seeking increased vulnerability	▲																	
Bundle 2.0	More open source tools; Increased function; option for dynamic tracing	Bundle 1.0 users plus more sophisticated users who want value of						▲												
SW 1.0	More tool adaptors; Modified for integration in SWAMP beta	SWAMP users	▲																	
SW 1.1	Upgrades for SWAMP IOC	SWAMP users		▲																
SW 2.0	Functionality and robustness for SWAMP Year 2. Add dynamic tracing from DHS Code	SWAMP users						▲												
SW 3.0	Upgrades for SWAMP Yr 3 custom needs	SWAMP users																		▲
ED 1.0	Code Dx Bundle modified for education, offered free to training orgs	Academic institutions training software developers in SwA practices		▲																
ED 1.1	Upgrades based on trainer and learner feedback	Academic institutions training software developers in SwA practices						▲												
SIEM 1.0	Feed pre-correlated SAST data to SIEMS; Add Code Dx filters based on SIEM	SIEM vendors; SIEM users				TBD														

# Next 120 days towards transition

## *We can use some help with these*

1. Get Code Dx transitioned into **government programs**
  - Complete integration into SWAMP Beta version
  - Determine effectiveness in NIST SATE program
  -  – Get accepted for operational use at NSA CAS
  -  – Have other government agencies evaluate Code Dx
  -  – Incorporate into proposals for other programs
2. Conduct full **commercialization**
  - Complete set-up of a reseller program
  - Determine pricing model
  -  – Gain active use by at least one Fortune 500 company
  -  – Procure outside investment

# What do you think?



Diagnosis and triage of source code vulnerabilities

***Looking for real, operational users!***

Anita D'Amico, Ph.D.  
Director, Secure Decisions  
(631) 759-3909  
anita.damico@securedecisions.com

Ken Prole  
Principal Investigator  
(631) 759-3907  
ken.prole@securedecisions.com