



# Software Assurance Analysis and Visual Analytics



## Cyber Security Division 2012 Principal Investigators' Meeting

October 10, 2012

Ken Prole

Principal Investigator

[Ken.Prole@securedecisions.com](mailto:Ken.Prole@securedecisions.com)

631-759-3907

DHS SBIR Topic H-SB09.2-004

Contract # N10PC20014



Home Projects Options About Admin Logout Logged in as admin

Code Dx APPLIED VISIONS SecDecisions

WebGoat > Analysis Run 3 Created on 6/14/2012 Uploaded on 6/14/2012 830 total weaknesses

Weakness count 272 / 830

Filters Clear all filters

Displaying weaknesses whose Triage Status is Escalated or Fixed

Bulk Operations Status Setter Select a status... Report Generator Select report format ... Actions will be for the 272 matching weaknesses

Weakness Flow

Weaknesses

ID	Weakness Name	Severity	Codebase Location	Status
1563	null_var	Unspecified	HammerHead.java	Escalated
1564	null_var	Unspecified	HammerHead.java	Escalated
1565	null_var	Unspecified	HammerHead.java	Escalated
1566	lock_assign	Unspecified	HammerHead.java	Escalated
1571	null_var	Unspecified	lessons/BlindScript.java	Escalated
1572	null_var	Unspecified	lessons/BlindScript.java	Escalated
1573	null_var	Unspecified	lessons/BlindScript.java	Escalated
1574	null_var	Unspecified	lessons/BlindScript.java	Escalated
1591	null_var	Unspecified	lessons/FailOpenAuthentication.java	Escalated
1592	weak_cmp	Unspecified	lessons/JavaScriptValidation.java	Escalated
1593	weak_cmp	Unspecified	lessons/JavaScriptValidation.java	Escalated
1597	string_cmp	Unspecified	lessons/WeakAuthenticationCookie.java	Escalated
1599	string_cmp	Unspecified	lessons/XMLInjection.java	Escalated
1600	string_cmp	Unspecified	lessons/XMLInjection.java	Escalated
1601	string_cmp	Unspecified	lessons/XMLInjection.java	Escalated
1602	null_var	Unspecified	lessons/XPATHInjection.java	Escalated
1607	null_var	Unspecified	session/LessonTracker.java	Escalated
1608	weak_cmp	Unspecified	session/RandomLessonTracker.java	Escalated
1614	run_nosync	Unspecified	util/ThreadWatcher.java	Escalated
1717	concurrent_call	Unspecified	session/DatabaseUtilities.java	Escalated
1718	concurrent_call	Unspecified	session/DatabaseUtilities.java	Escalated

# About Us

- Founded 1987
- 40 people in Northport and Albany, NY
- Commercial software product development
  - Hallmark, Reuters, AC Nielsen
- Significant visualization experience
  - Software Vis, Cyber Security Vis, Military C2 Vis
- Secure Decisions security division launched in 2000
  - Visual analytics of network data, Visual systems for CND training, Mission impact of cyber attacks
- Classified portfolio



APPLIED  
VISIONS



SECURE  
DECISIONS  
A DIVISION OF APPLIED VISIONS, INC.

# There's lots of bad software out there

## Our industry still hasn't learned how to deploy secure software...

// **Software Assurance:** poorly written software is at the root of all of our security problems

Doug Maughan, DHS

Top 10 Hard Problems in Cyber Security, CACM 53(2)

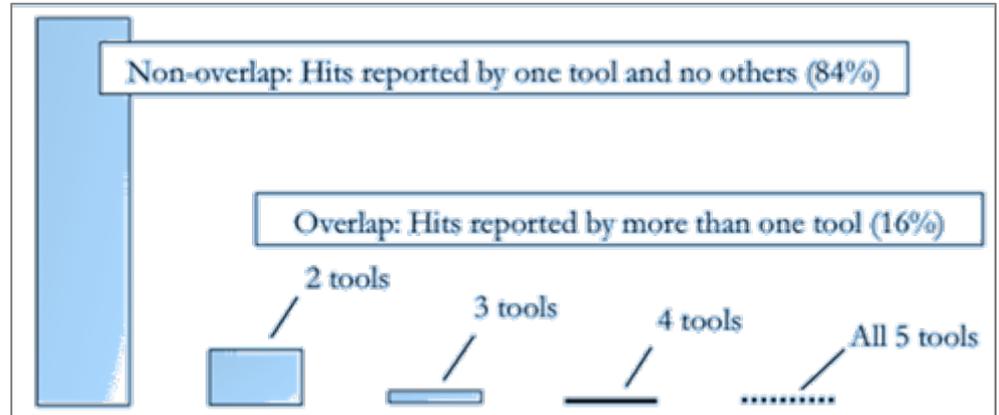
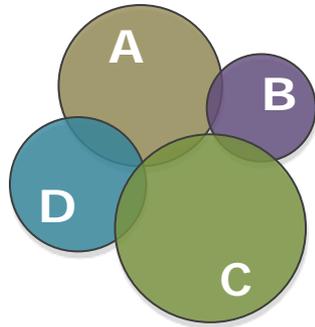


A screenshot of an ABC News article titled "6.4 Million Passwords Reportedly Stolen From LinkedIn Website". The article is dated June 6, 2012, and is by Colleen Curry. The main text states: "The social networking website LinkedIn is investigating claims that more than 6 million passwords were stolen and uploaded to a Russian-language web forum today." The article includes a video player showing a close-up of a computer screen displaying the LinkedIn website. The video player has a play button in the center. The article also has a "Recommend" button with a count of 2.7k. The ABC 20/20 logo is visible in the top left corner of the article content area.

## The **tools exist** to help us deploy safer software...

...but there's no single solution

Different tools identify different problems...



Source: MITRE

One static analysis tool on average will only detect

**14%**

of all weaknesses

No tool stands out as an uber-tool. Each has its strengths and weaknesses.

Kris Britton, Technical Director  
NSA's Center for Assured Software



Coverity® Integrity Manager

Admin User | Sign out | Preferences | Help | About | Jump to CID:

Dashboard | **Projects** | Configuration | Administration

Projects >> Covtel Kernel Code >> New View\*

Defects | Source | Metrics | Trends | Dashboard

[Edit Selected](#) | [Configure Columns](#) | [CSV](#) | [XML](#)

Filter results by:

**Defect Type:**

- Any
- High Impact: only
- Medium Impact: only
- Low Impact: only
- Memory - corruptions
  - Memory - illegal accesses
- Resource leaks
  - Resource leak
    - RESOURCE\_LEAK
- Uninitialized variables
  - Uninitialized scalar variable
  - UNINIT
- API usage errors
- Control flow issues
- Error handling issues
- Incorrect Expression
- Insecure data handling
- Integer handling issues
- Null pointer dereferences
- Program hangs
  - Infinite loop
    - INFINITE\_LOOP
- Build system issues
- Code maintainability issues
- Performance inefficiencies
- Security best practices violations
- Warnings

**Severity:**

- Any
- Unspecified: only
- Major: only
- Moderate: only
- Minor: only
- Various: only

**Status:**

- Any
- Outstanding
- Resolved
- Inspected
- New: only

59 of 4700 defects match (clear filters)

Filters Applied: Checker X Status X Detected In X

CTD	Checker	Severity	Status	Owner	Classification	Action	Function
10001	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	acpi_ex_store()
10002	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	acpi_ex_opcode_1A_0T_1R()
10005	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	skb_copy_datagram()
10006	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	rt_fil_info()
10007	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	rt6_fil_node()
10008	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	tcp_sendpage()
10009	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	tcpdiag_bc_run()
10012	BAD_FREE	Unspecified	New	Unassigned	Unclassified	Undecided	sdtp_endpoint_destroy()
10013	BAD_FREE	Unspecified	New	Unassigned	Unclassified	Undecided	sdtp_transport_destroy()
10014	BAD_FREE	Unspecified	New	Unassigned	Unclassified	Undecided	sdtp_association_free()
10028	BUFFER_SIZE	Unspecified	New	Unassigned	Unclassified	Undecided	fat_new_dir()
10031	BUFFER_SIZE	Unspecified	New	Unassigned	Unclassified	Undecided	vfat_fill_slots()
10039	BUFFER_SIZE	Unspecified	New	Unassigned	Unclassified	Undecided	packet_getname_spkt()
10328	NEGATIVE_RETURNS	Unspecified	New	Unassigned	Unclassified	Undecided	handle_intrd()
10556	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	DAC960_V2_ReadControllerConfiguration()
10560	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cmd_free()
10565	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_coax_request()
10566	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10567	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10568	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10569	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10570	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10571	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10572	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10573	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10574	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10575	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10576	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10577	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_ksa_request()
10800	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	rd_load_image()
10801	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	rlmp_open_lsap()
10802	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	ax25_connect()

Save View | Share View | Create Link | **New Action**

59 of 4700 defects match (clear filters)

50,000 weaknesses..

Where do I start?



## Software Assurance Visual Analysis

An application that brings together **disparate** SwA analysis runs and ...

... normalizes the results in a standard format

... removes overlapping results

... visualizes and prioritizes key trouble spots by severity and frequency

... uses code context to assess the impact of those results

... filters and highlights based on weakness type and software class

... shows who is responsible for weaknesses

... helps assign repair of weaknesses

... uncovers trends

**KDM Analytics**<sup>™</sup>

Tool Output Integration Framework

**Coverage**

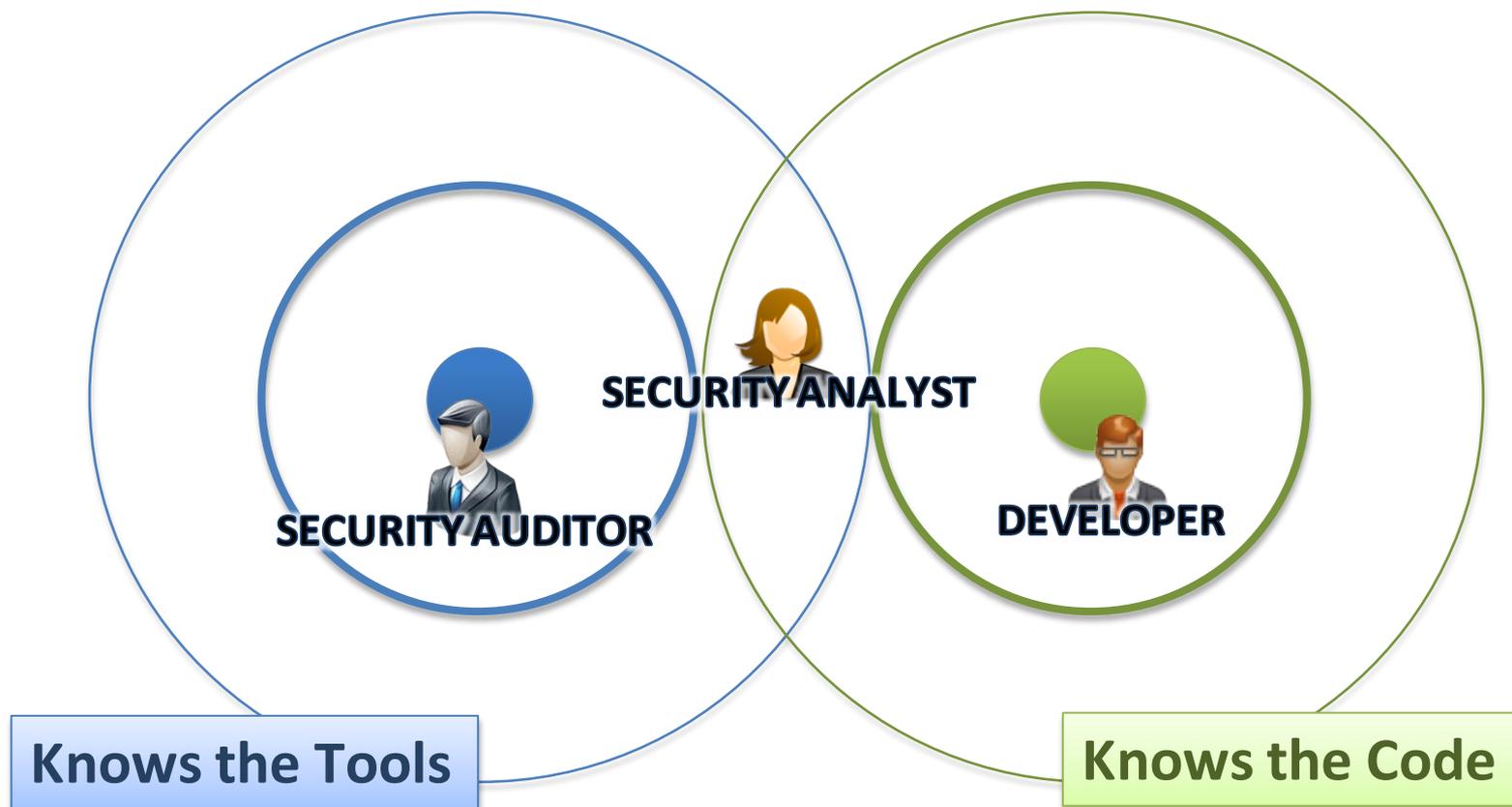
**Priority**

**Traceability**

**Remediation**

**Enhances the speed and coverage for detection and remediation of software weaknesses**

# Target Users for Code Dx



# Code Dx Workflow

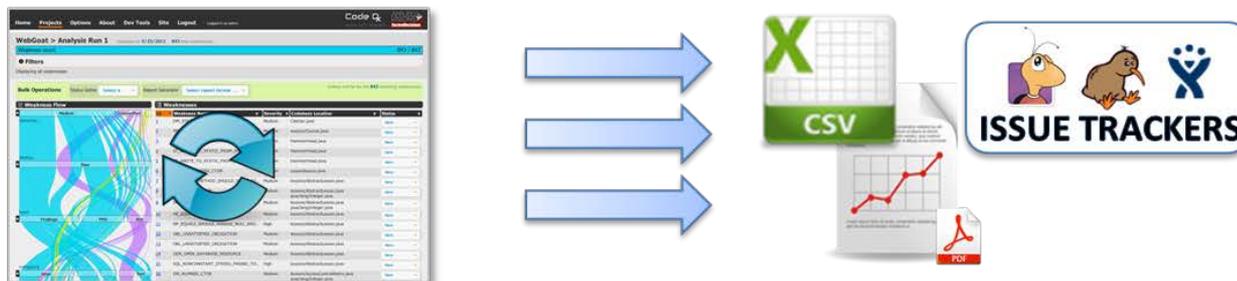
## Step 1 – Generate and upload data



## Step 2 – Automatic correlation and normalization of the tool results



## Step 3 – Visual analytics, weakness triage, and results dissemination



# WebGoat > Analysis Run 1 > Weakness 504 MS\_SHOULD\_BE\_FINAL detected by FindBugs

First seen on 6/22/2012 8 weaknesses in this file 3 similar weaknesses in this analysis run

Status  
New

Triage status

### Description

A mutable static field could be changed by malicious code or by accident from another package. The field could be made final to avoid this vulnerability.

Remediation guidance

### Detailed Information

### Source Code

The weakness goes from line 61 to 61 in file lessons/XMLInjection.java  
show more: (1 weaknesses currently hidden from view)

```
51  *
52  * @author Sherif Koussa <a href="http://www.softwaresecured.co
53  */
54  public class XMLInjection extends LessonAdapter
55  {
56
57      private final static Integer DEFAULT_RANKING = new Integer(
58
59      private final static String ACCOUNTID = "accountID";
60
61      public static HashMap<Integer, Reward> rewardsMap = new Has
62
63      public final static A MAC_LOGO = new A().setHref("http://ww
64
65      protected static HashMap<Integer, Reward> init()
66      {
67          Reward r = new Reward();
68
69          r.setName("WebGoat t-shirt");
70          r.setPoints(50);
71          rewardsMap.put(1001, r);
```

Source code details

show more: (5 weaknesses currently hidden from view)

### Activity Stream

Activity Stream input field with a back arrow button

You can write your comments using markdown

admin changed status to New

3 days ago

admin changed status to Assigned to jane

3 days ago

admin changed status to Escalated

3 days ago

admin changed status to Assigned to jane

3 days ago

admin changed status to Escalated

3 days ago

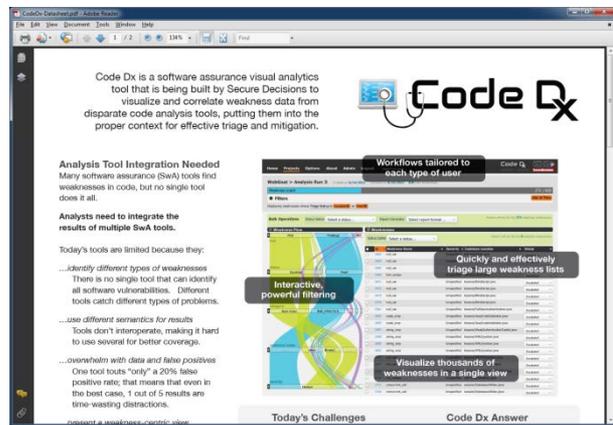
admin changed status to New

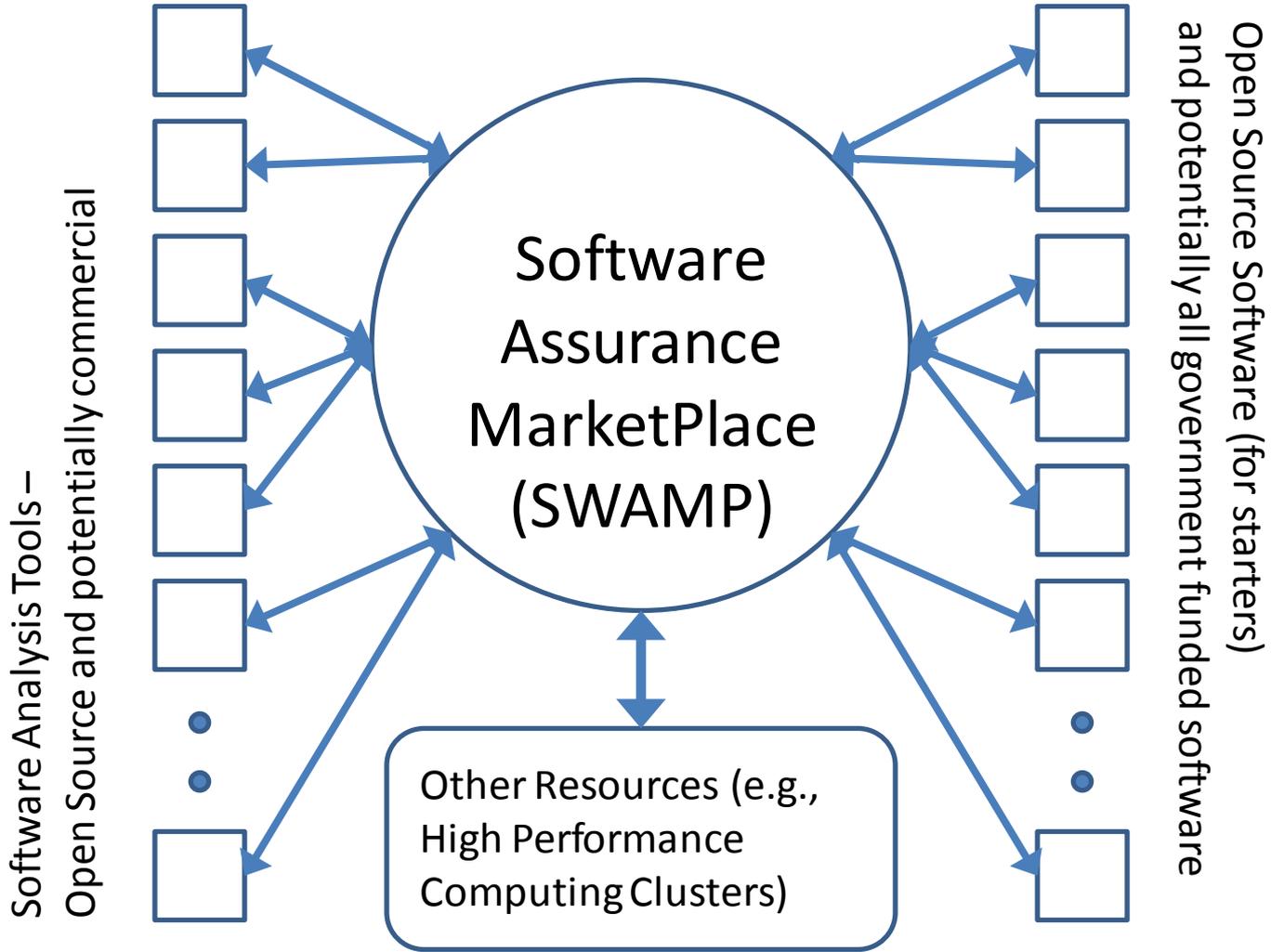
21 days ago

Real-time collaboration

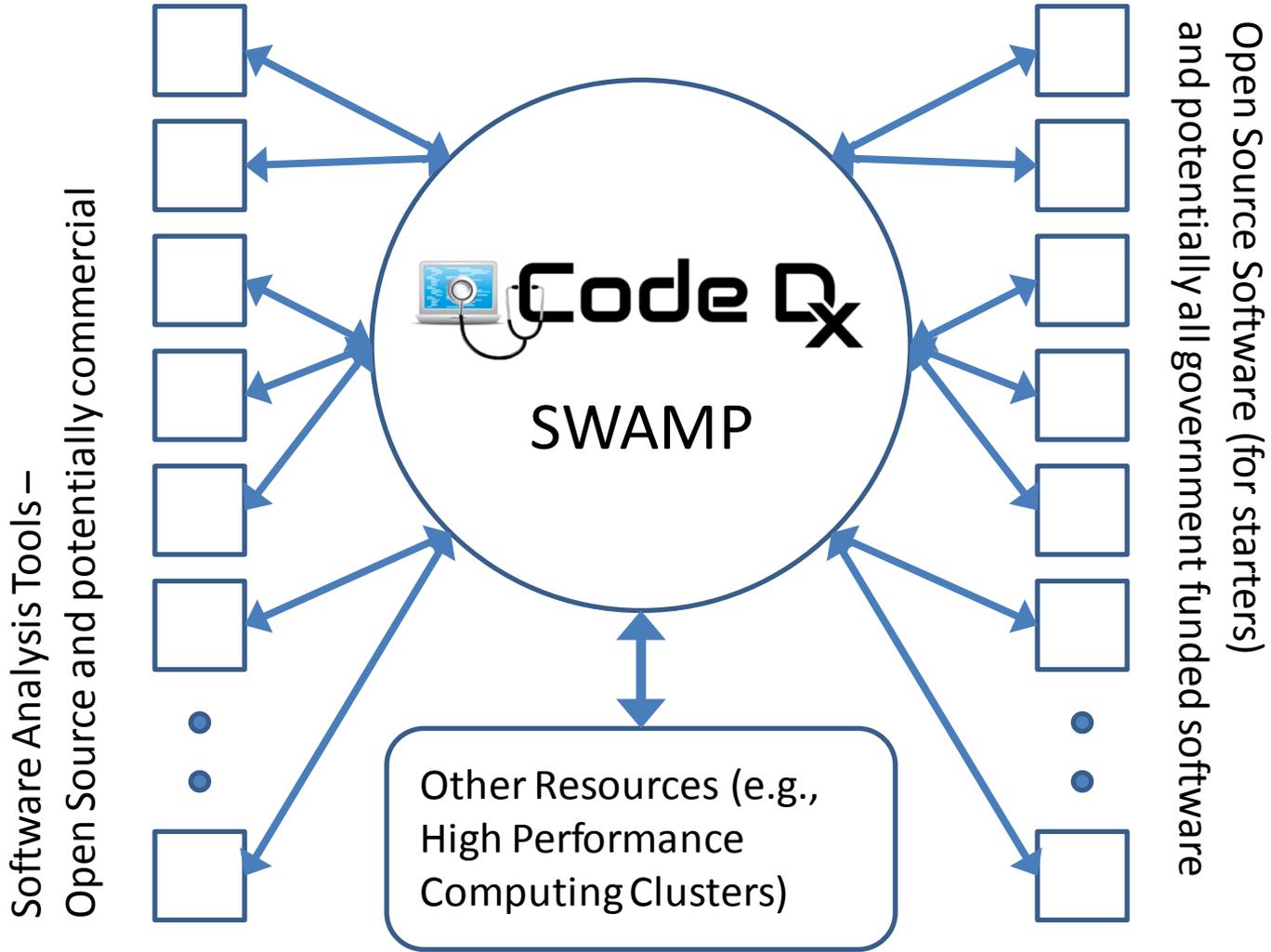
# Technology Transition

- Phase II contract scheduled to end Jan 9, 2013
- Alpha prototype made available in July 2012
  - Evaluations sent to over 30 government and commercial organizations
- Beta prototype scheduled for Dec 2012
- Datasheet and marketing movie available at: [securedecisions.com/codedx](http://securedecisions.com/codedx)





1. Help advance the quality and adoption rate of SWA tools
2. Lower the threshold for using them
3. Make it easier to interpret and use their output



1. Help advance the quality and adoption rate of SWA tools
2. Lower the threshold for using them
3. Make it easier to interpret and use their output



Do you have feedback? Please share it with us [directly](#).

- Home
- CWE Categories
- Browse Weaknesses
- Contact us

### Highlight

Text

Language

None

SDLC Phase

None

### What

What you are seeing are all the categories in the CWE. The categories in the inner-most ring are the top level categories and each level below that contains the sub-categories for the one above.

### Tip

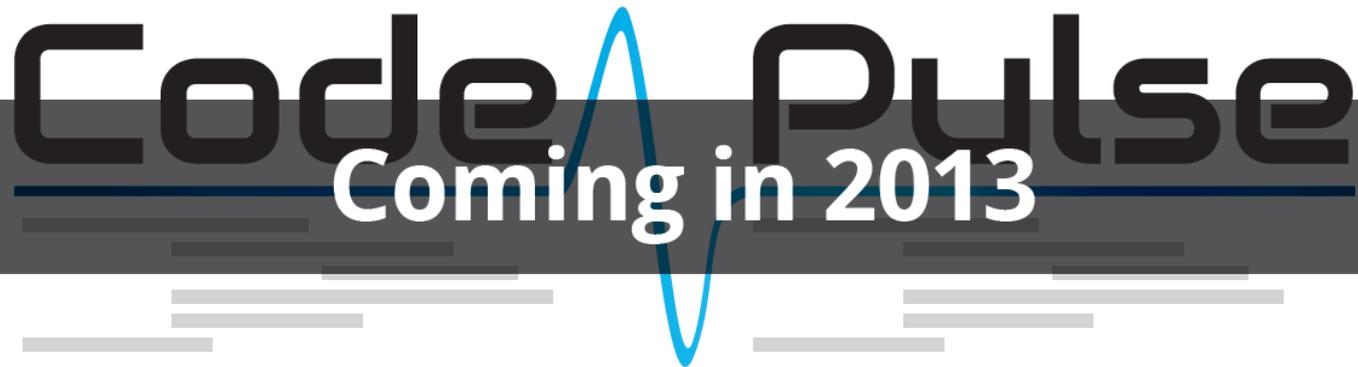
You can zoom with the mouse wheel and pan around with the left mouse button.



**Focus on resolving vulnerabilities in  
the most important code paths**

# Code Pulse

Coming in 2013

The logo for 'Code Pulse' features the words 'Code' and 'Pulse' in a bold, black, sans-serif font. A blue pulse line starts at the top of the 'e' in 'Code', rises to a peak, falls to a trough, and then rises again to end at the top of the 'e' in 'Pulse'. Below the text is a dark grey horizontal bar. The text 'Coming in 2013' is written in white, sans-serif font across the middle of the grey bar. Below the grey bar, there are several horizontal lines of varying lengths and shades of grey, suggesting a stylized waveform or data visualization.

**Code Pulse will provide an execution  
context for static source analysis**

# Questions?



**Ken Prole**

[Ken.Prole@securedecisions.com](mailto:Ken.Prole@securedecisions.com)

631-759-3907

