

## Application Security Vulnerability Scanning



**Steve Fox**

Chief Information Officer

---

12/12/2012

## **Agenda**

---

- **Introduction**
- **Conversations**
- **Why do we need Fortify?**
- **Fortify Components**
- **Software Security Assurance Process**
- **Fortify Evaluation**
- **Questions**

## Conversations

- **ISO: Are the developers writing secure code?**
- **Development: Sure, as far as I can tell, with the knowledge of my training class 3 years ago, “Intro to Security 101”. I did also take a one hour webinar last year...**
  
- **ISO: Microsoft releases monthly security patches, why don't we?**
- **Development: I believe our code is secure, but I am not a security expert. Why, have we been hacked?**
  
- **ISO: I need documentation of our information security risks for auditors.**
- **Development: Isn't it your job to write that stuff? I am still trying to evaluate our software for risks, much less fix any of them...**

## Conversations

- **ISO: What is the scope of our security vulnerabilities?**
- **Development: We have millions of lines of code written since 1995 by dozens of developers. I don't have time to analyze every line of code, so I cannot answer that question. And even if I did have time, I lack the training to recognize every possible security threat as they change daily. We would need a full-time development team to stay up to date with the latest security threats.**

## Realization:

- **Our developers want to write secure code, but they lack the proper training to understand threats. This cannot be addressed simply by security training, because security threats evolve rapidly.**

## Why do we need Fortify?

- **Our developers require ongoing feedback to stay abreast of information security threat vectors and best practices**
- **Development staff need to know where to concentrate their efforts on fixing security vulnerabilities**
- **IT management and auditors need easy access to data on potential risks in our software**
- **While we are working to improve our software, our Agency needs protection from threats which may exploit existing vulnerabilities**

## **Fortify has 3 Main Components**

### **Fortify RTA (Real-Time Analyzer)**

- **Blocks attacks and logs suspicious activity**
- **Logs potential security issues for ISOs to review**

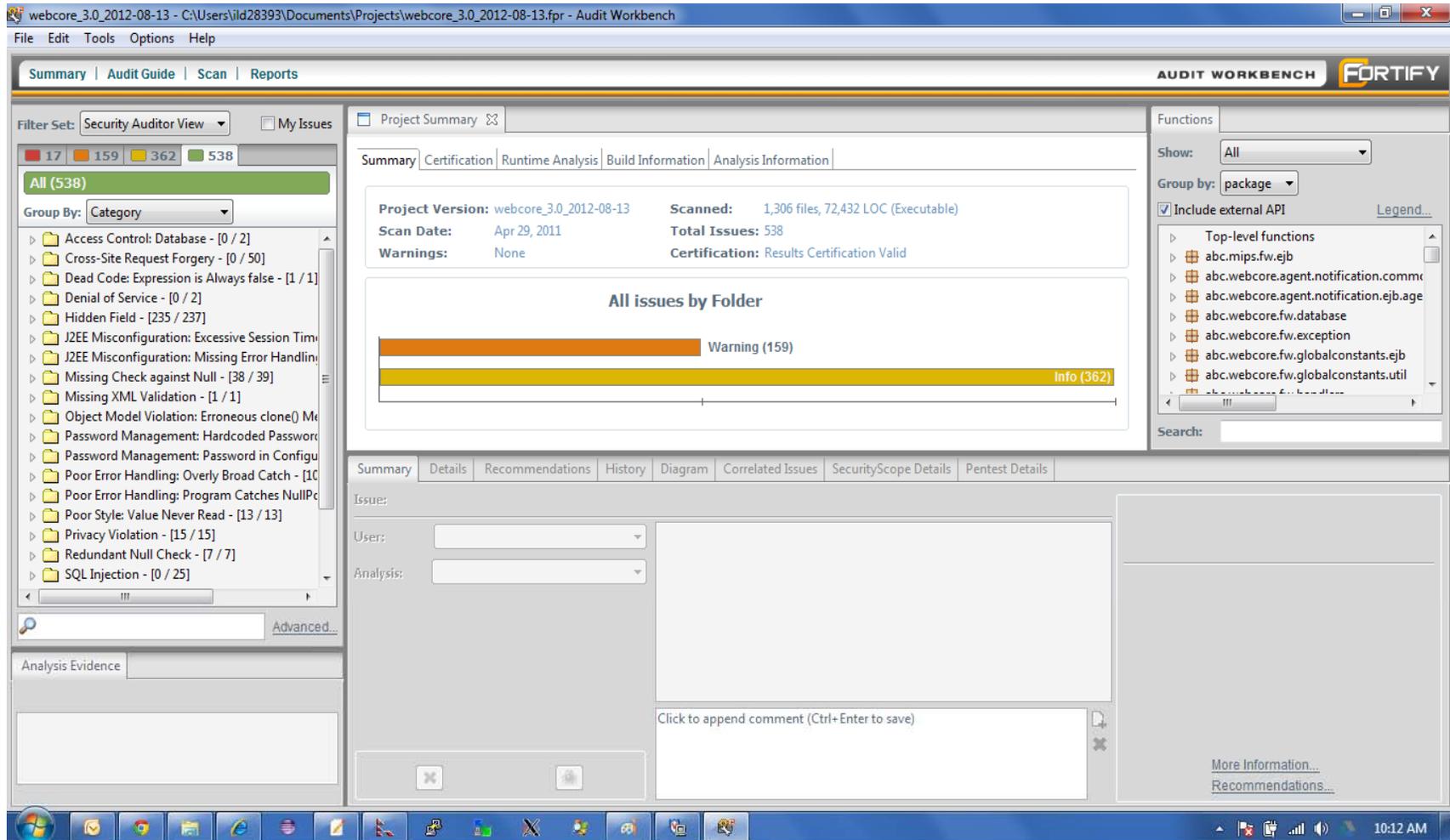
### **Fortify SCA (Source Code Analyzer)**

- **Scans for vulnerabilities and poor coding techniques (Memory leaks, unused variables, password issues)**

### **Fortify 360**

- **Shows developers most critical areas to address risks**
- **Shows progress over product lifecycle**
- **Provides reports for ISO and auditors**

## Screen Shot – Audit Categories



The screenshot displays the Fortify Audit Workbench interface. The top navigation bar includes 'Summary', 'Audit Guide', 'Scan', and 'Reports'. The main window is titled 'Project Summary' and shows the following details:

- Project Version:** webcore\_3.0\_2012-08-13
- Scanned:** 1,306 files, 72,432 LOC (Executable)
- Scan Date:** Apr 29, 2011
- Total Issues:** 538
- Warnings:** None
- Certification:** Results Certification Valid

The 'All issues by Folder' bar chart shows the following data:

Issue Category	Count
Warning	159
Info	362

The left sidebar lists various audit categories with their respective counts:

- Access Control: Database - [0 / 2]
- Cross-Site Request Forgery - [0 / 50]
- Dead Code: Expression is Always false - [1 / 1]
- Denial of Service - [0 / 2]
- Hidden Field - [235 / 237]
- J2EE Misconfiguration: Excessive Session Tim
- J2EE Misconfiguration: Missing Error Handlin
- Missing Check against Null - [38 / 39]
- Missing XML Validation - [1 / 1]
- Object Model Violation: Erroneous clone() Me
- Password Management: Hardcoded Passwor
- Password Management: Password in Configu
- Poor Error Handling: Overly Broad Catch - [10
- Poor Error Handling: Program Catches NullPc
- Poor Style: Value Never Read - [13 / 13]
- Privacy Violation - [15 / 15]
- Redundant Null Check - [7 / 7]
- SQL Injection - [0 / 25]

The right sidebar shows a 'Functions' list with a search bar and a 'Legend...' link. The bottom of the interface features a taskbar with various application icons and a system tray showing the time as 10:12 AM.

## Screen Shot – Dash Board

Fortify 360 Server - Windows Internet Explorer provided by VA IT Infrastructure Partnership

http://borg.abc.virginia.gov:8080/f360/flex/index.jsp

Fortify 360 Server

Welcome cmlumpn  
[Logout](#) | [Account](#) | [Preferences](#) | [About](#)

Dashboard | Projects | Runtime | Reports | Administration

Page 1

### Alert Notifications

0 records found

Select item and...

Date	Type	Message

### Issues

Legend: MIPS - 1.0, CMS - 1.4.3, Asgard - 1.0, CMS - 1.4.4, MIPS - 8.1.1

### Audit Status

10 records found

Select item and...

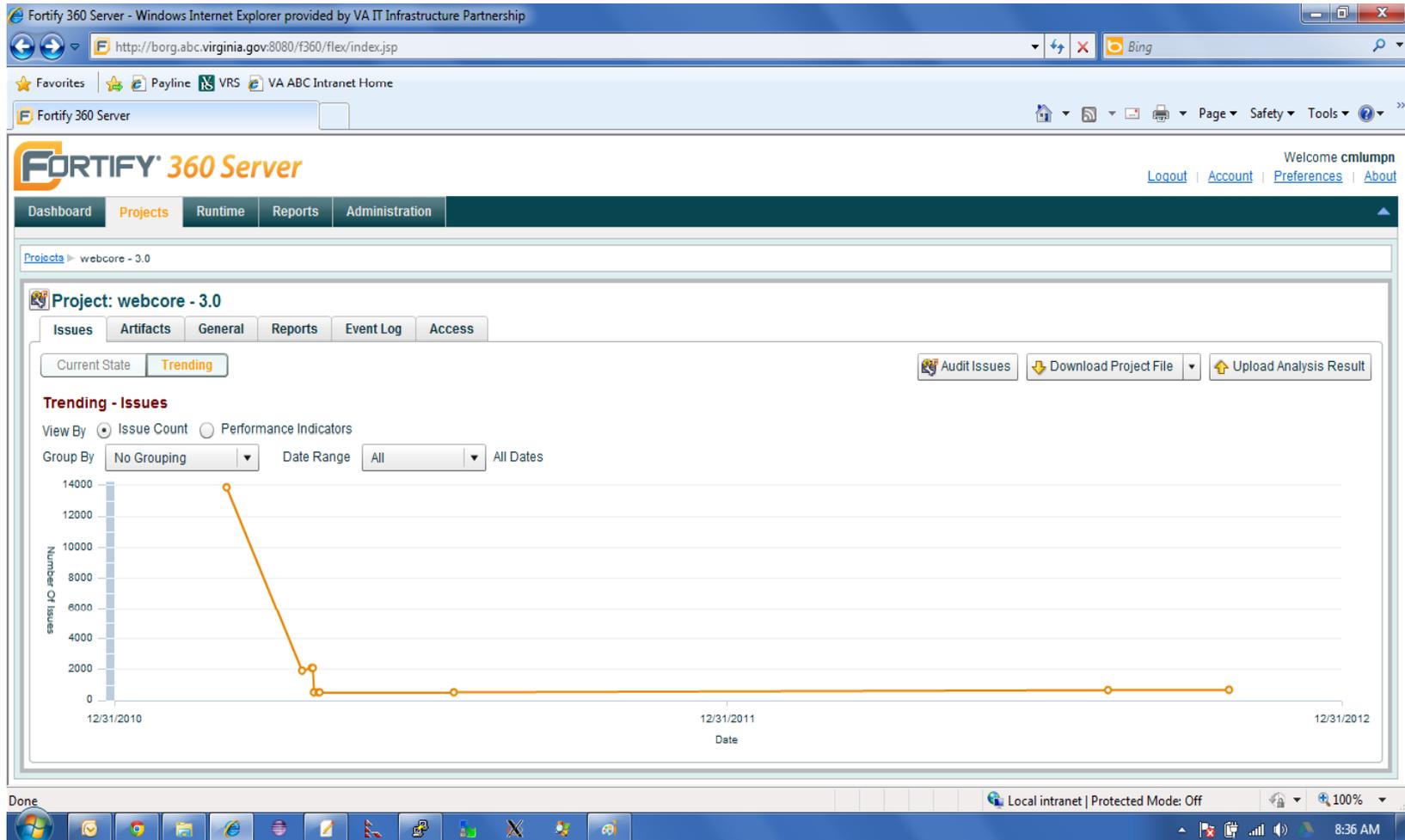
Project Version	Last Upload Date	Total Issues	Audit Percentage
ActivityTracker - 1.0	08/21/2012 2:41:28 PM	0	0.00%
Asgard - 1.0	04/19/2011 4:10:37 PM	692	0.14%
Assets - 1.0	09/05/2012 8:23:37 AM	0	0.00%

### Project Inventory

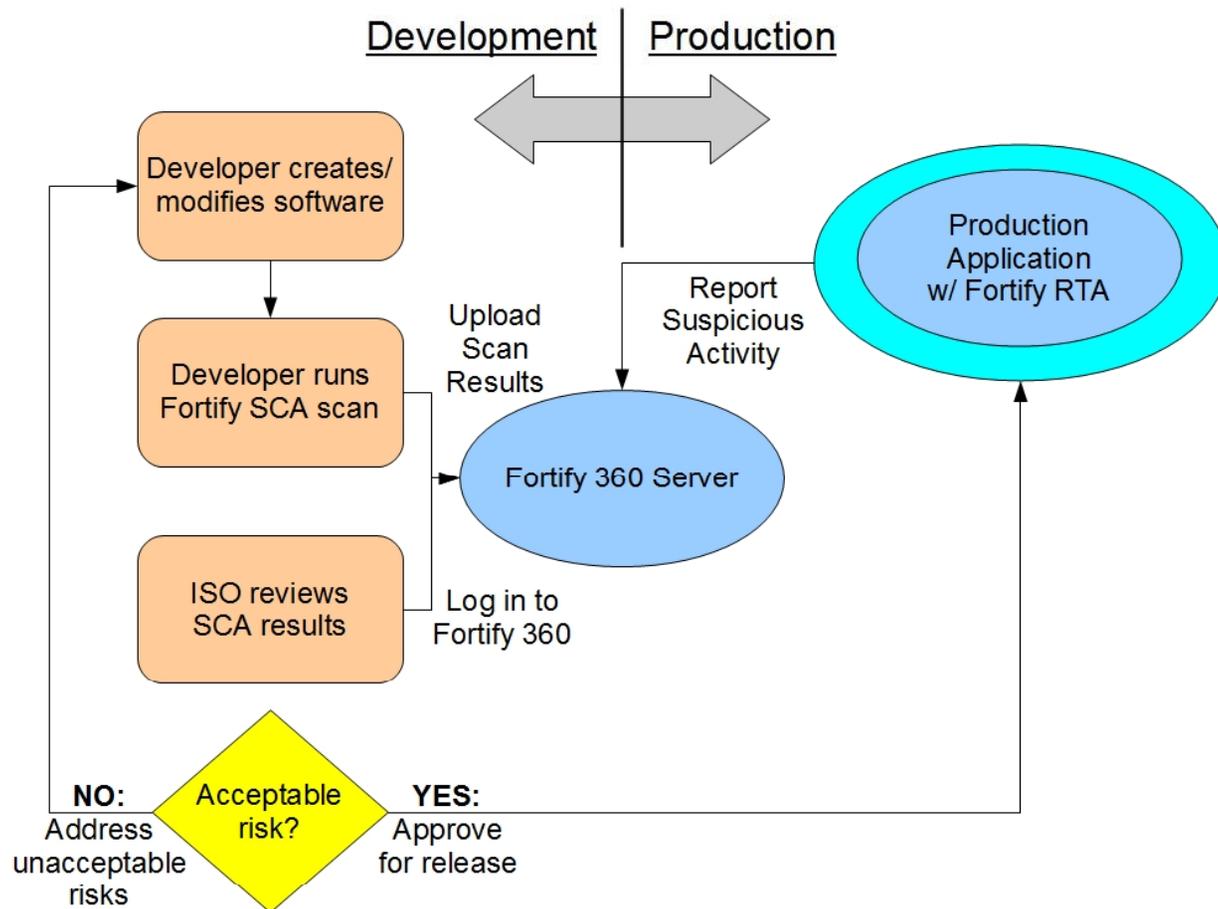
Legend: Internal Network..., External Public...

Done Local intranet | Protected Mode: Off 100% 8:25 AM

## Screen Shot – Project Trend



## Software Security Assurance Process



## Fortify Evaluation

- **Fortify SCA does very intelligent pattern matching. It traces through blocks of code to determine if data is handled correctly**
- **Fortify SCA is not a substitute for good developers, but it can assist good developers in writing secure code**
- **Fortify SCA sometimes flags false positives, so a significant amount of time is spent evaluating vulnerabilities**
- **Fortify RTA – No news is good news**
- **Software Security Assurance is a process, not a tool.**



# Questions



## Department of Alcoholic Beverage Control

### For Follow On Questions

**Andrew McEnhimer    804-204-2304**

**Chris Lumpkin        804-213-4685**

# **Innotas**

## **Portfolio and Project Management Tool**

## Innotas Modules

### Complete set of PPM and APM features



Project Portfolio  
Management



Application Portfolio  
Management



Project Request  
Management



Service Request Management



Project Management



Application Management



Resource Management



Prioritization



Financial Management



Reports & Dashboards



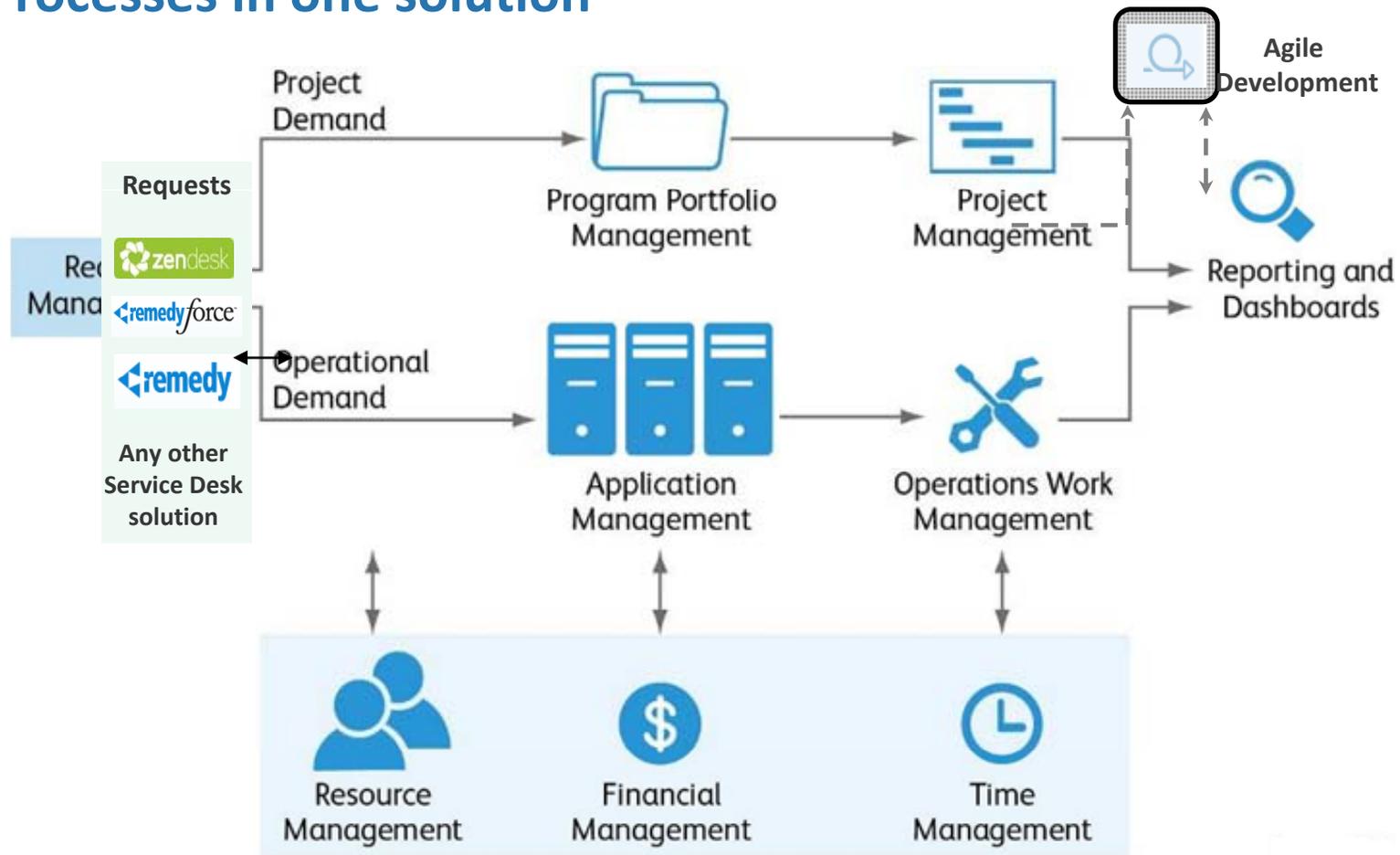
Time Tracking



Web Services

## The Innotas Process

Covering all IT & PMO  
Processes in one solution



## Innotas Integration Platform

Flexible integration of all business systems

- Robust, cloud-based integration solution managed by Innotas
- Seamless connectivity with any cloud or on-premise applications
- Managed and maintained by Innotas

