בע"ה

ISE Southeast Executive Forum and Awards
Nominee Showcase Presentation

August 11, 2010

Company Name: Travelport GDS
Project Name: Code Assurance
Presenter: Ariel Silverstone, CISSP
Presenter Title: Director, Information Security

Company Overview

- One of the largest and most diverse travel organizations worldwide

- Offers comprehensive solutions and services to thousands of companies that operate in the global travel industry.

- 1/3rd of all global travel goes through our systems

- Worldspan, Galileo and Apollo

Code Assurance

- Travel industry – and a software house
- Some of the most sensitive information anywhere
- 31 Billion transactions annually
- 20 Million per day
- Tens-to-hundreds of millions of lines of code

Overview of Business Challenge

- Over seven separate development groups (VP)
- Previously, virtually all code testing driven by PCI
- Each VP decided which release needs testing, by whom, and at what frequency
- No uniform scope for testing
- Many different vendors

Overview of Business Challenge II

Cost per PCI Audit - Code Review	Number of Applications	Average Releases - per Year	Total Potential Cost
$ 40,000			$ 9,600,000
	60+	4	
$ 100,000			$ 24,000,000

Project Scope/Goals

Can we test by ourselves and satisfy PCI?

↓

Will it be cost effective?
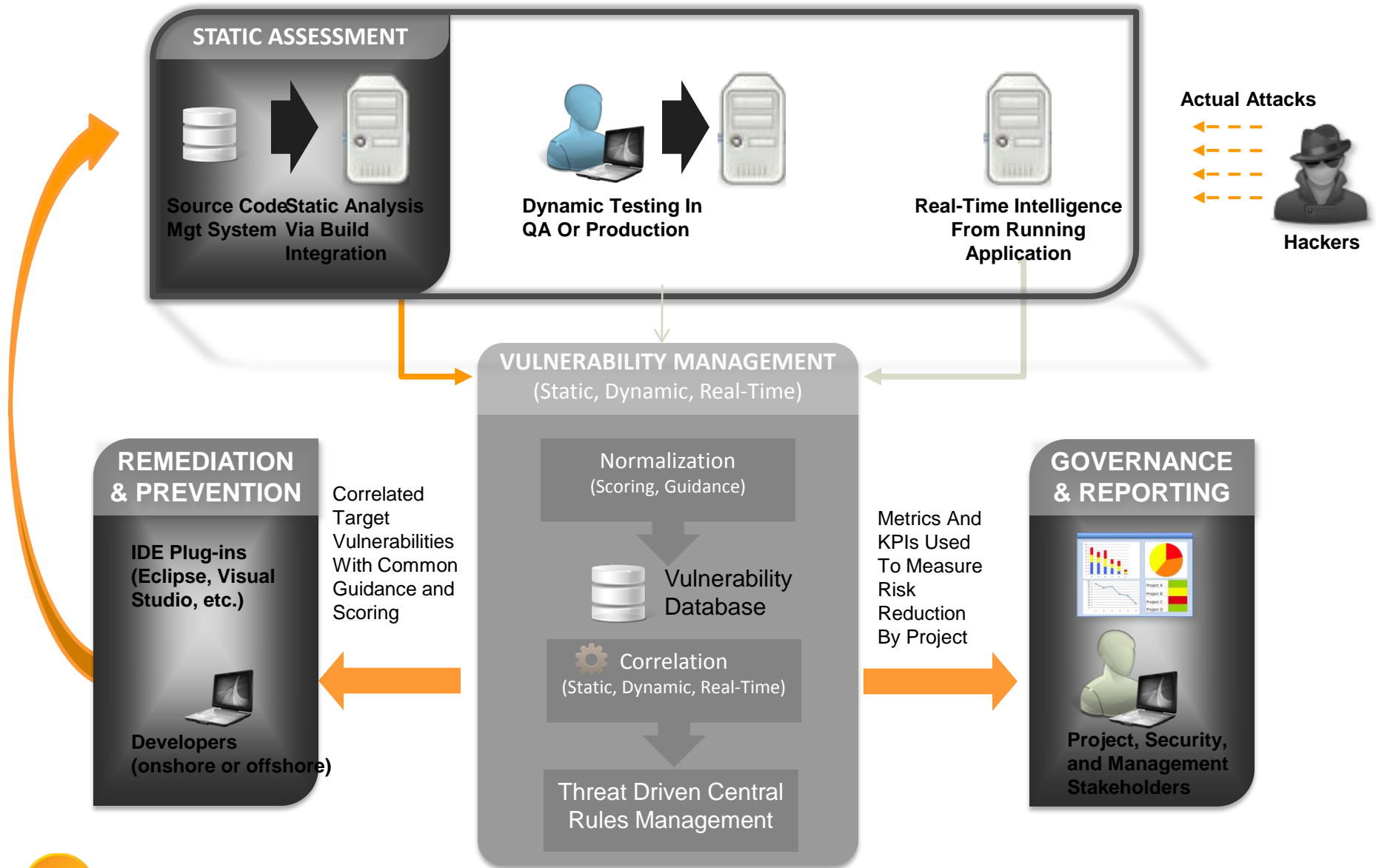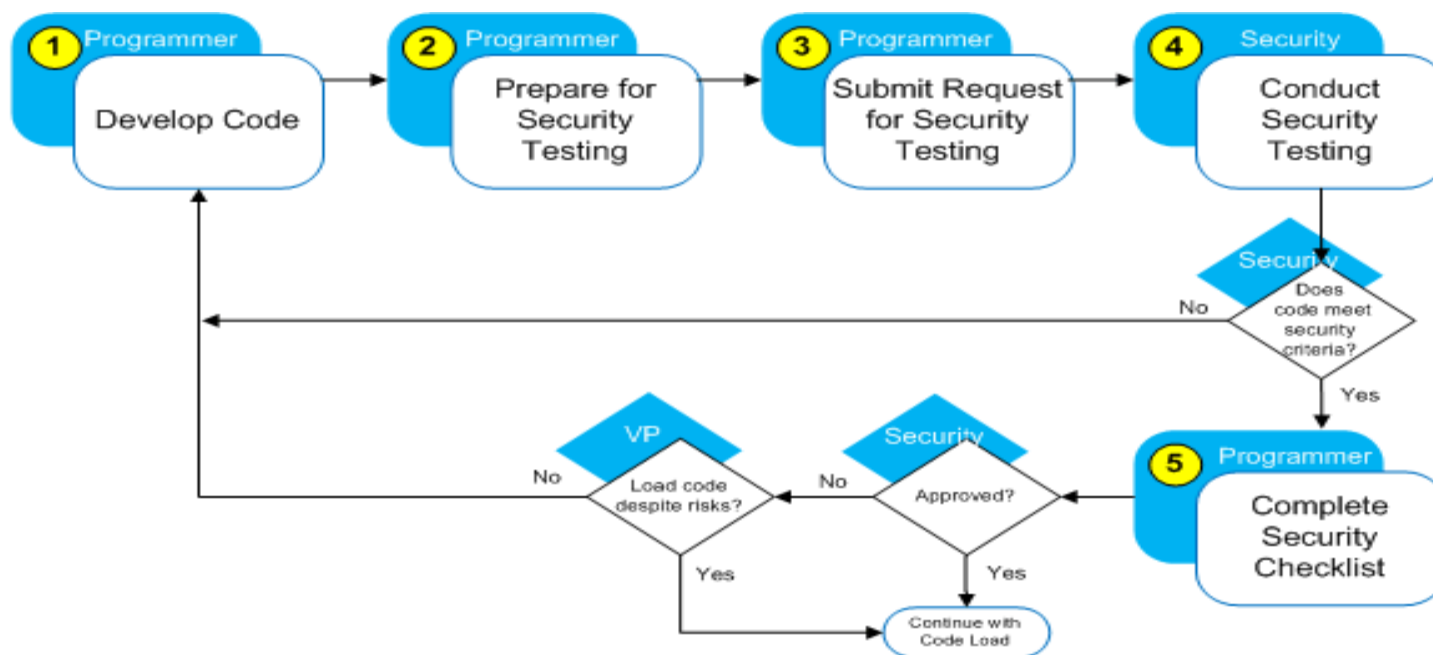
| Hardware | Software | Training | Facility | FTE |

↓

- Leader in Software Security Assurance
- Over 700 enterprise customer references around the world.

Fortify Software Security Assurance Overview

STATIC ASSESSMENT

Source Code Mgt System

Static Analysis Via Build Integration

Dynamic Testing In QA Or Production

Real-Time Intelligence From Running Application

Actual Attacks

Hackers

VULNERABILITY MANAGEMENT
(Static, Dynamic, Real-Time)

Normalization
(Scoring, Guidance)

Vulnerability Database

Correlation
(Static, Dynamic, Real-Time)

Threat Driven Central Rules Management

REMEDIATION & PREVENTION

IDE Plug-ins (Eclipse, Visual Studio, etc.)

Developers (onshore or offshore)

Correlated Target Vulnerabilities With Common Guidance and Scoring

Metrics And KPIs Used To Measure Risk Reduction By Project

GOVERNANCE & REPORTING

Project, Security, and Management Stakeholders

The Process


```
1  Programmer          2  Programmer          3  Programmer          4  Security
   Develop Code           Prepare for            Submit Request         Conduct
                          Security               for Security           Security
                          Testing                Testing                Testing
```

Security
Does code meet security criteria? — No / Yes

VP — Load code despite risks? — No / Yes

Security — Approved? — No / Yes

5 Programmer — Complete Security Checklist

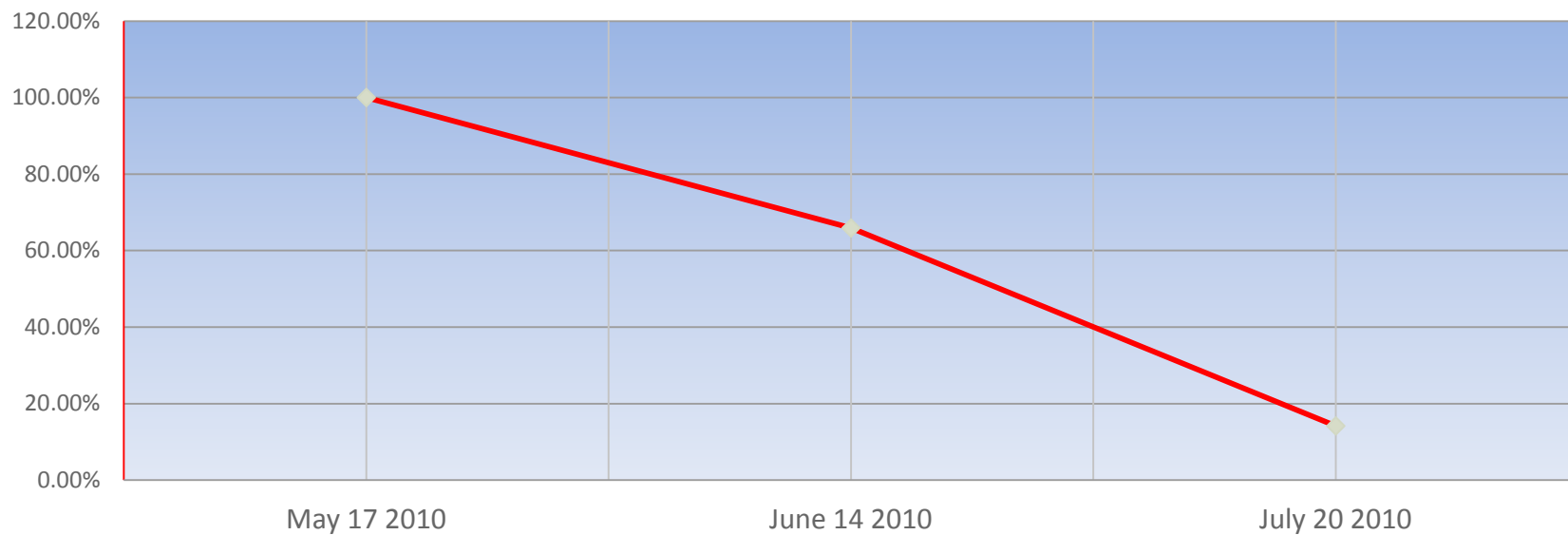Continue with Code Load

KEY
VP = Vice President

Project Results

ProductX Vulnerability Count Over Time

Over 90% Reduction!

By The Numbers

- 134 Projects and Releases Scanned
- 9,937,502 Lines of Code Tested
- 7% Improvement in Overall Code Security
- 15 Projects <u>Re</u>scanned with ZERO Criticals, Highs and Mediums
- <5% False Positive Rate
- > $7,000,000 saved!
- 1 Award Nomination ☺

Lessons Learned/Best Practices

- Train, Train, Train.

- Internal champions

- Partner for expertise

Thank you and Questions

- Questions?