

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

How We Implemented Security in Agile for 20 SCRUMs- and Lived to Tell

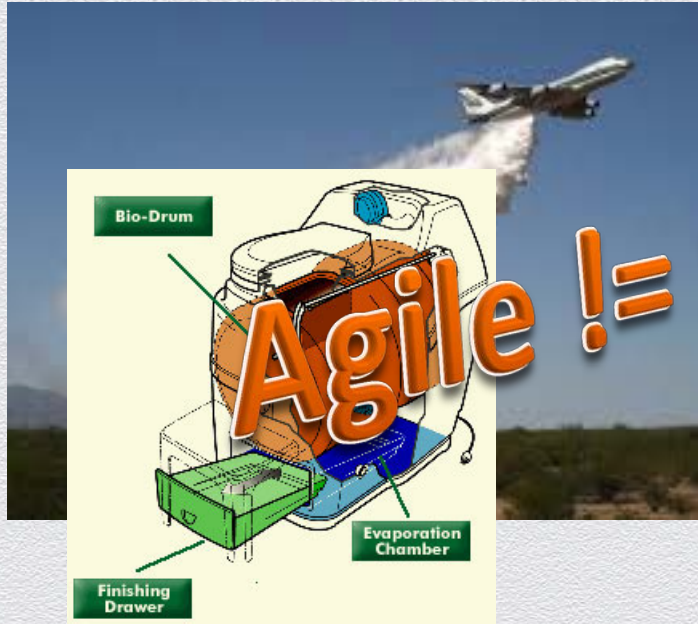
SESSION ID: ASEC-R03

Yair Rovek

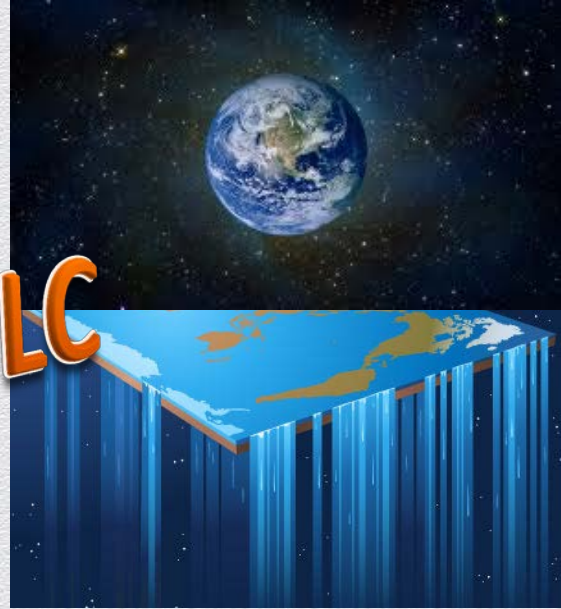
Security Specialist
LivePerson
@lione_heart



Challenged by Agile



Agile != SDLC



In the Next 45 Min

- ◆ LivePerson and Application Security
- ◆ Where did it all Began
- ◆ LivePerson And Agile
- ◆ Security Checkpoints in the Process
- ◆ Bringing it All Together in the Continuous Integration
- ◆ Summarize the Challenges
- ◆ Key Success Factors

LivePerson ID

What we do?



SaaS platform for creation of meaningful connections through real-time engagement

How it works?



**Monitor web visitor's behavior
(Over 1.5 B visits each month)**



Conduct behavioral ranking



**Provide the engagement platform
(Over 10 M chats each month)**



SaaS & Cloud only



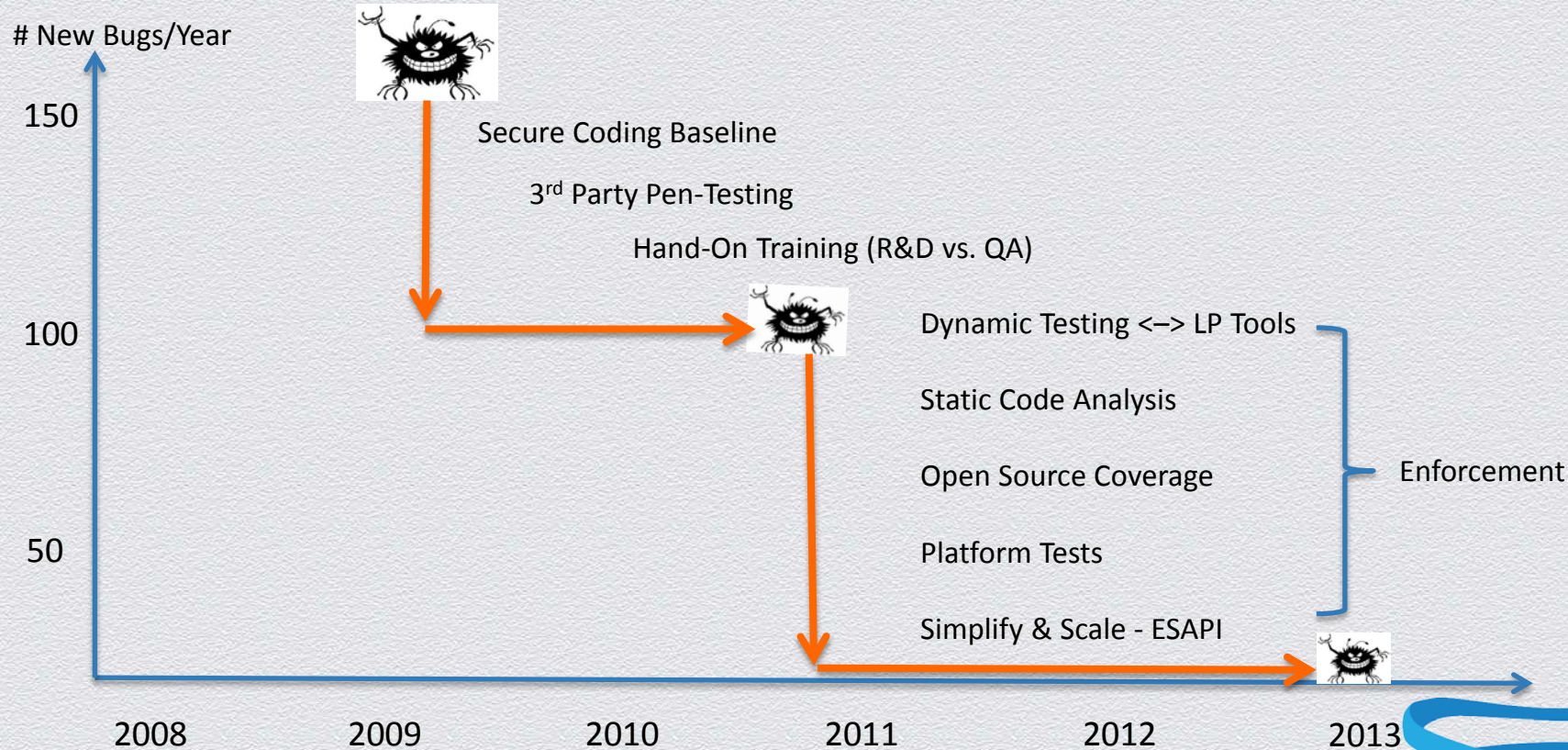
Security is NOT optional...

#RSAC

RSACONFERENCE2014



From Pen-Testing to SDLC

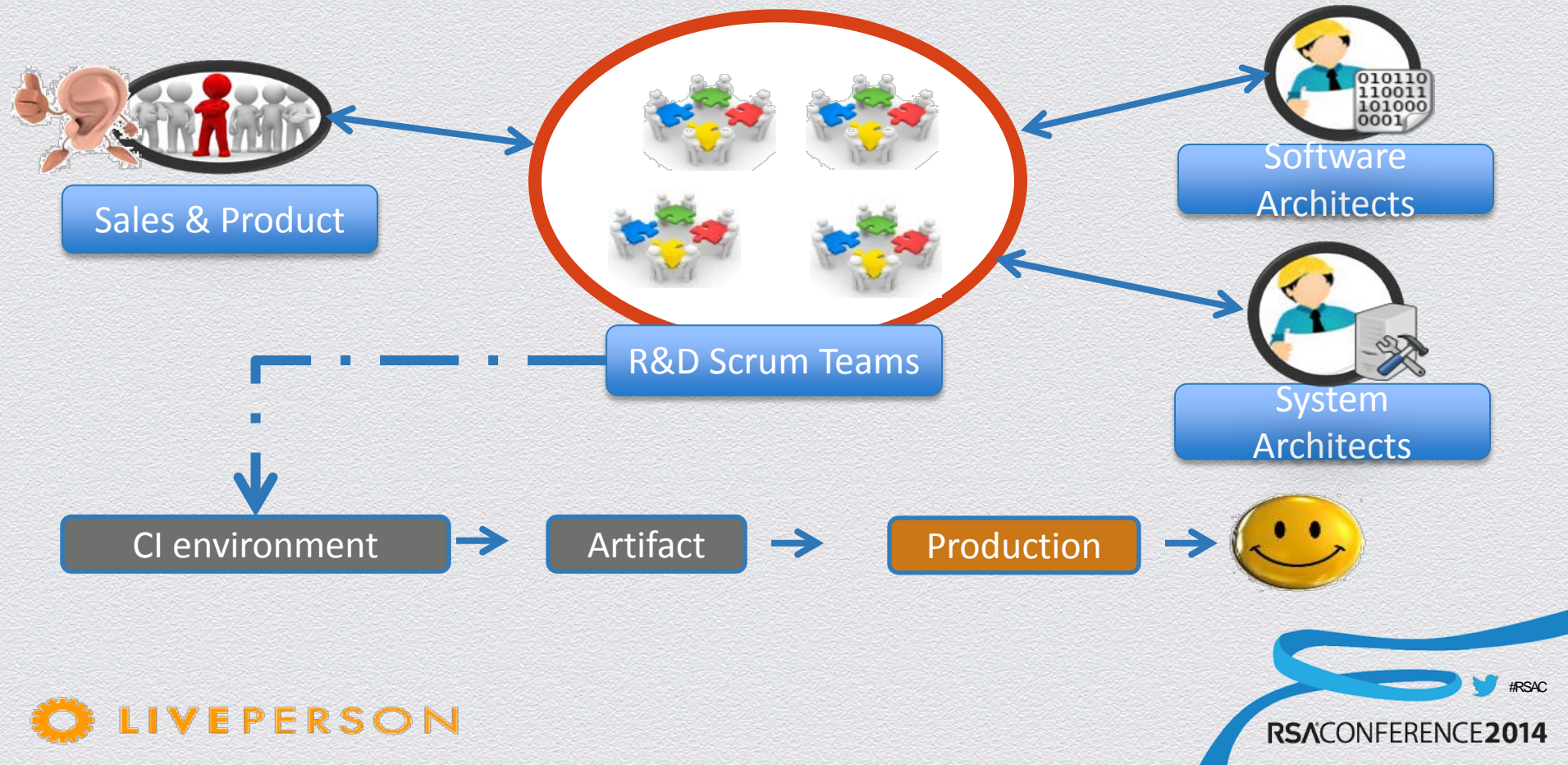


LIVEPERSON

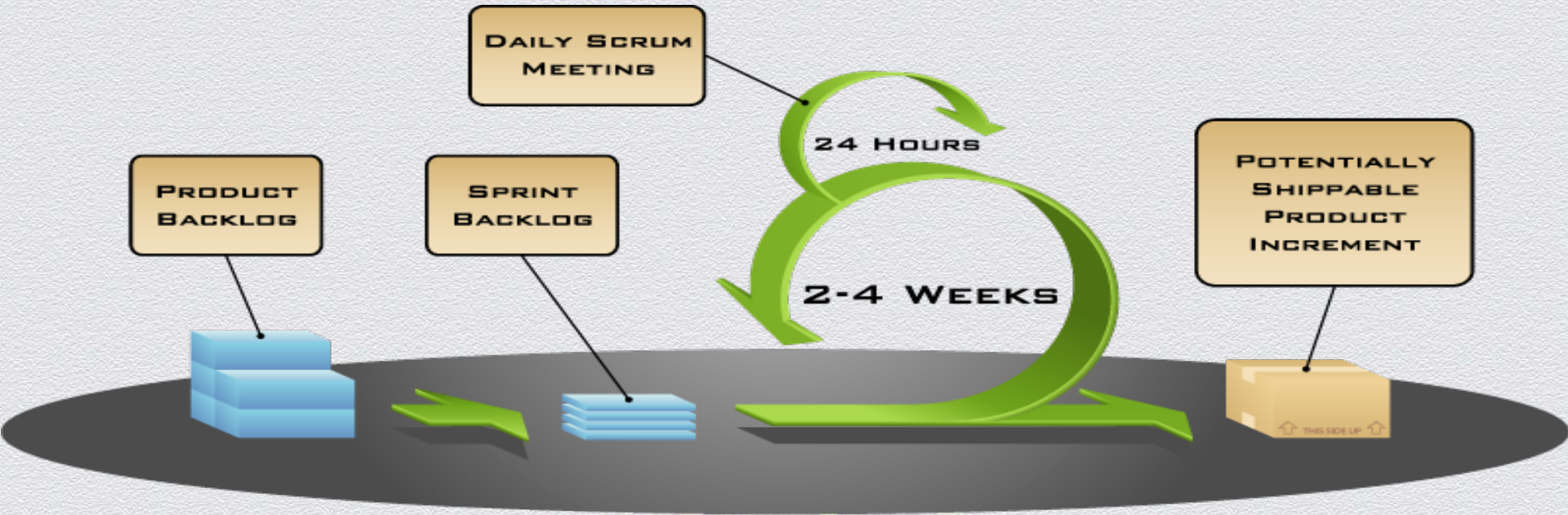
#RSAC

RSACONFERENCE2014

Who are the Key Players?

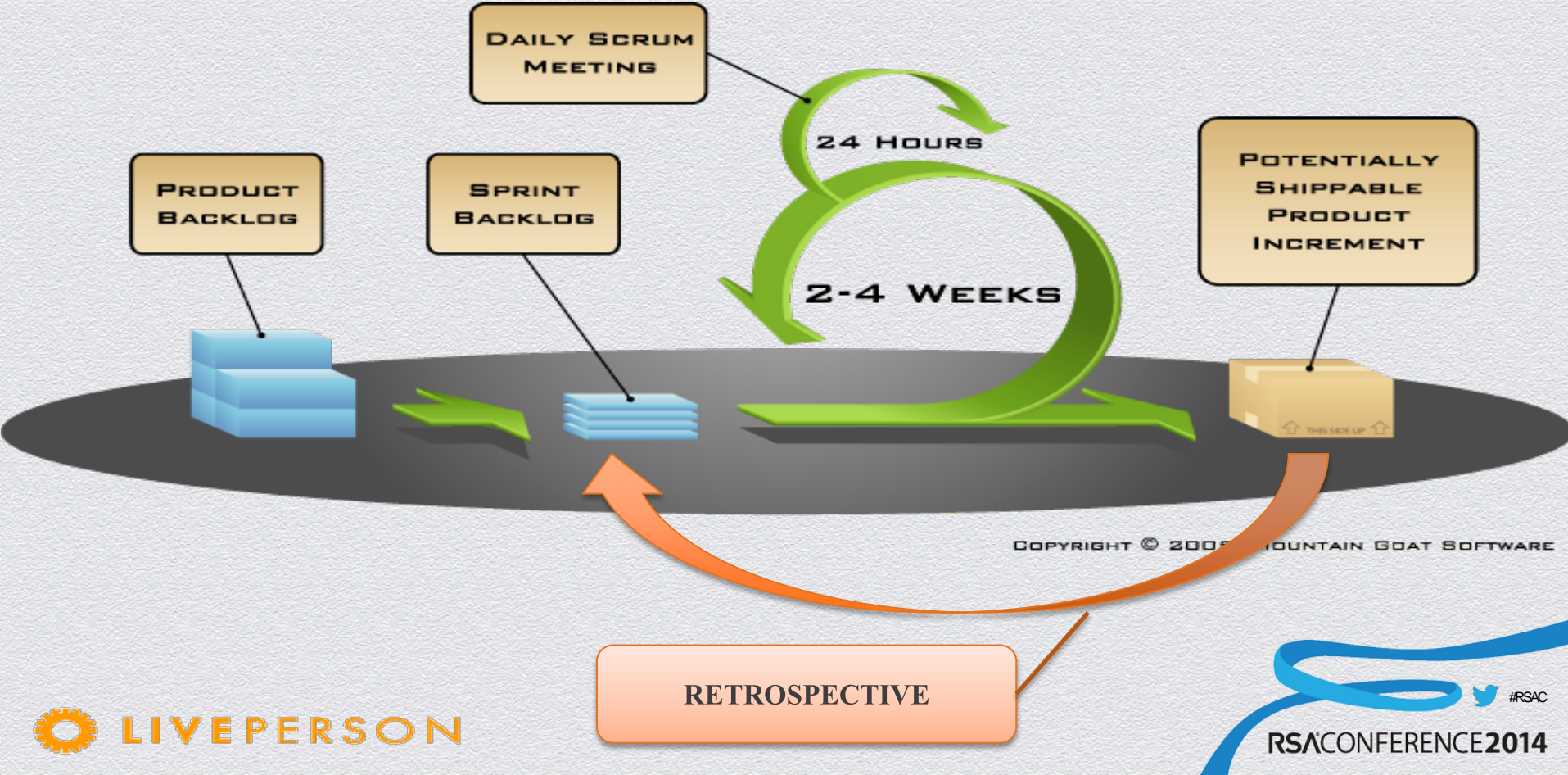


Agile Framework



COPYRIGHT © 2005, MOUNTAIN GOAT SOFTWARE

Agile Framework



LIVEPERSON

RETROSPECTIVE

#RSAC

RSACONFERENCE2014

Add Security to the Agile Process

Scrum Actions

Release Planning

Sprint Planning

Coding

Code Freeze

Q&A – Regression Tests

Release

Add Security to the Agile Process

Scrum Actions

Release Planning

Sprint Planning

Coding

Code Freeze

Q&A – Regression Tests

Release

Security Control

Security High-Level Design

Add Security to the Agile Process

Scrum Actions

Release Planning

Sprint Planning

Coding

Code Freeze

Q&A – Regression Tests

Release

Security Control

Security High-Level Design

Guide-in the teams On-Demand

Add Security to the Agile Process

Scrum Actions

Security Control

Release Planning

Security High-Level Design

Sprint Planning

Guide-in the teams On-Demand

Coding

ESAPI & SCA checks for each build

Code Freeze

Q&A – Regression Tests

Release

Add Security to the Agile Process

Scrum Actions

Security Control

Release Planning

Security High-Level Design

Sprint Planning

Guide-in the teams On-Demand

Coding

ESAPI & SCA checks for each build

Code Freeze

Automated Security Tests

Q&A – Regression Tests

Release

Add Security to the Agile Process

Scrum Actions

Security Control

Release Planning

Security High-Level Design

Sprint Planning

Guide-in the teams On-Demand

Coding

ESAPI & SCA checks for each build

Code Freeze

Automated Security Tests

Q&A – Regression Tests

Automated Security Tests

Release

Add Security to the Agile Process

Scrum Actions

Security Control

Release Planning

Security High-Level Design

Sprint Planning

Q&A On-Demand

Coding

ESAPI & SCA checks for each build

Code Freeze

Automated Security Tests

Q&A – Regression Tests

Automated Security Tests

Release

External Pen-Test



LIVEPERSON

#RSAC

RSACONFERENCE2014

Add Security to the Agile Process

Scrum Actions

Security Control

Release Planning

Security High-Level Design

Sprint Planning

Guide-in the teams On-Demand

Coding

ESAPI & SCA checks for each build

Code Freeze

Automated Security Tests

Q&A – Regression Tests

Automated Security Tests

Release

External Pen-Test



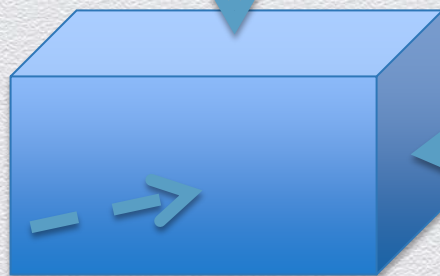
LIVEPERSON

#RSAC

RSACONFERENCE2014

Screening Code in 3D

Delivered



Dependencies and Open Source

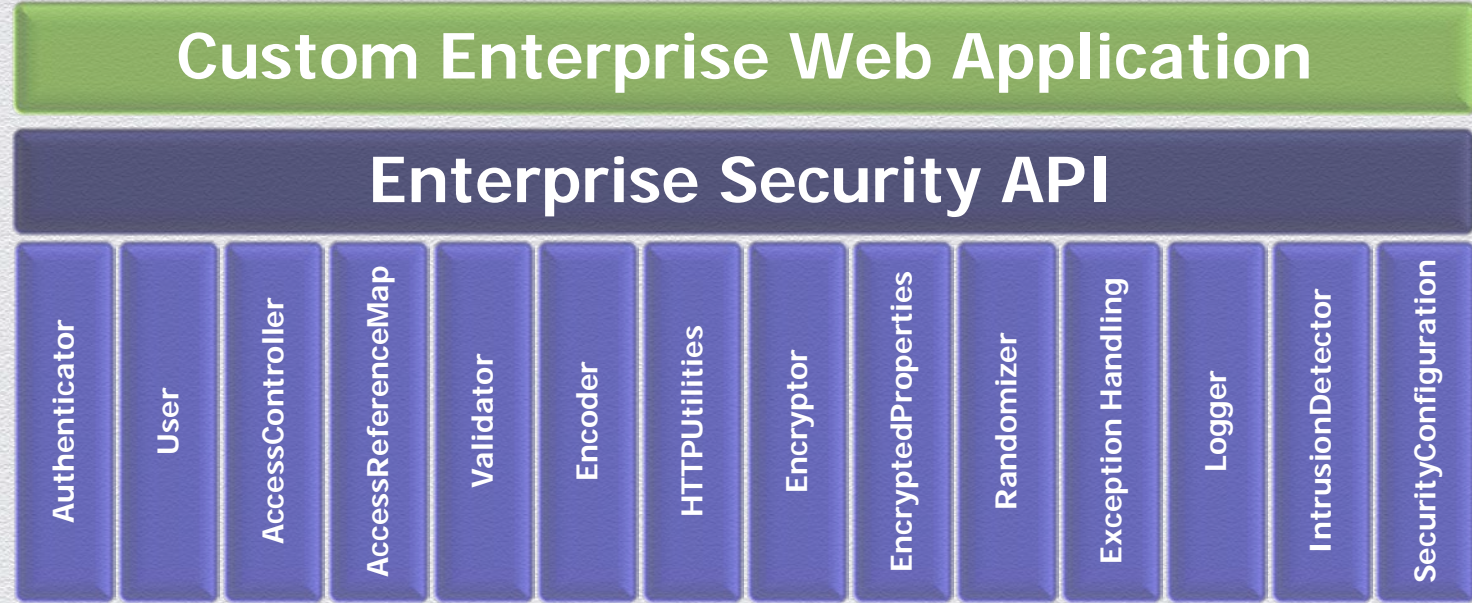
Developer Code

- ESAPI/AntiSamy/CSRF Guard...
- Utilities
- SCA

```
<project>
<parent>
  <groupId>com.mycomp</groupId>
  <artifactId>my-app</artifactId>
  <version>1.0</version>
</parent>
<modelVersion>4.0.0</modelVersion>
<groupId>com.mycomp</groupId>
<artifactId>my-app</artifactId>
<version>1.0</version>
```

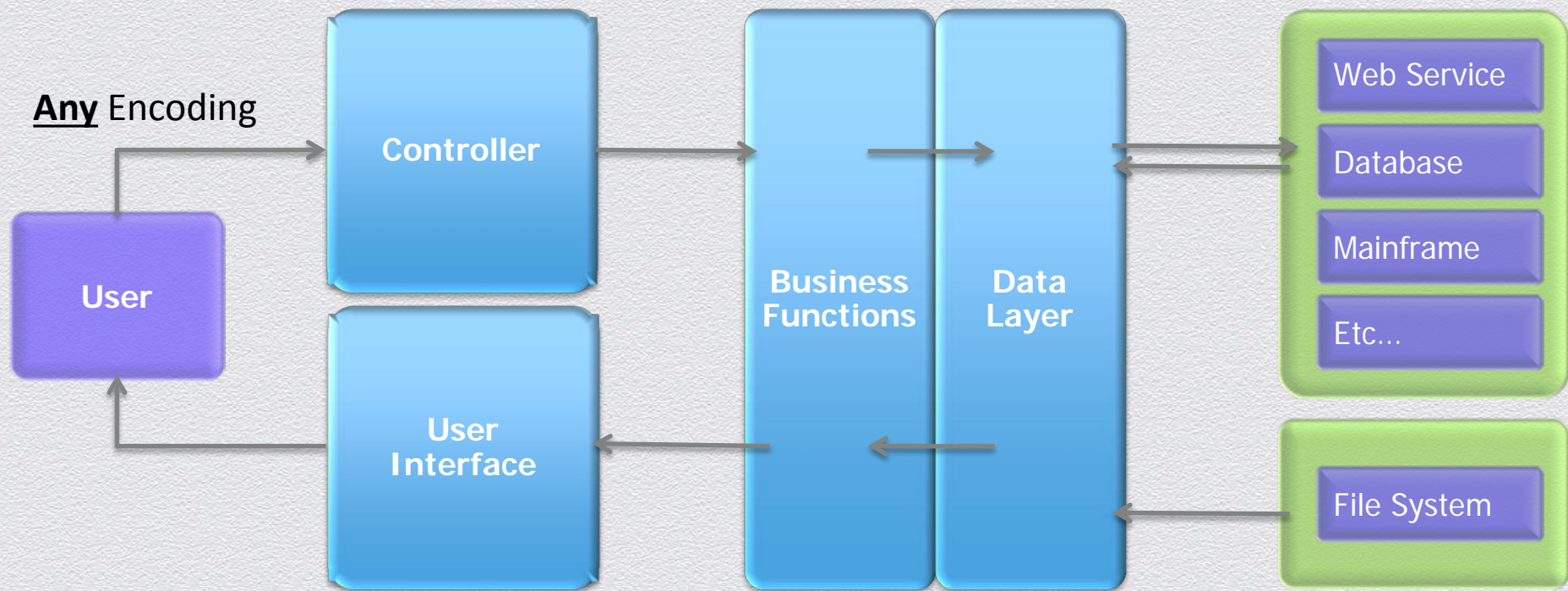


ESAPI Building Blocks

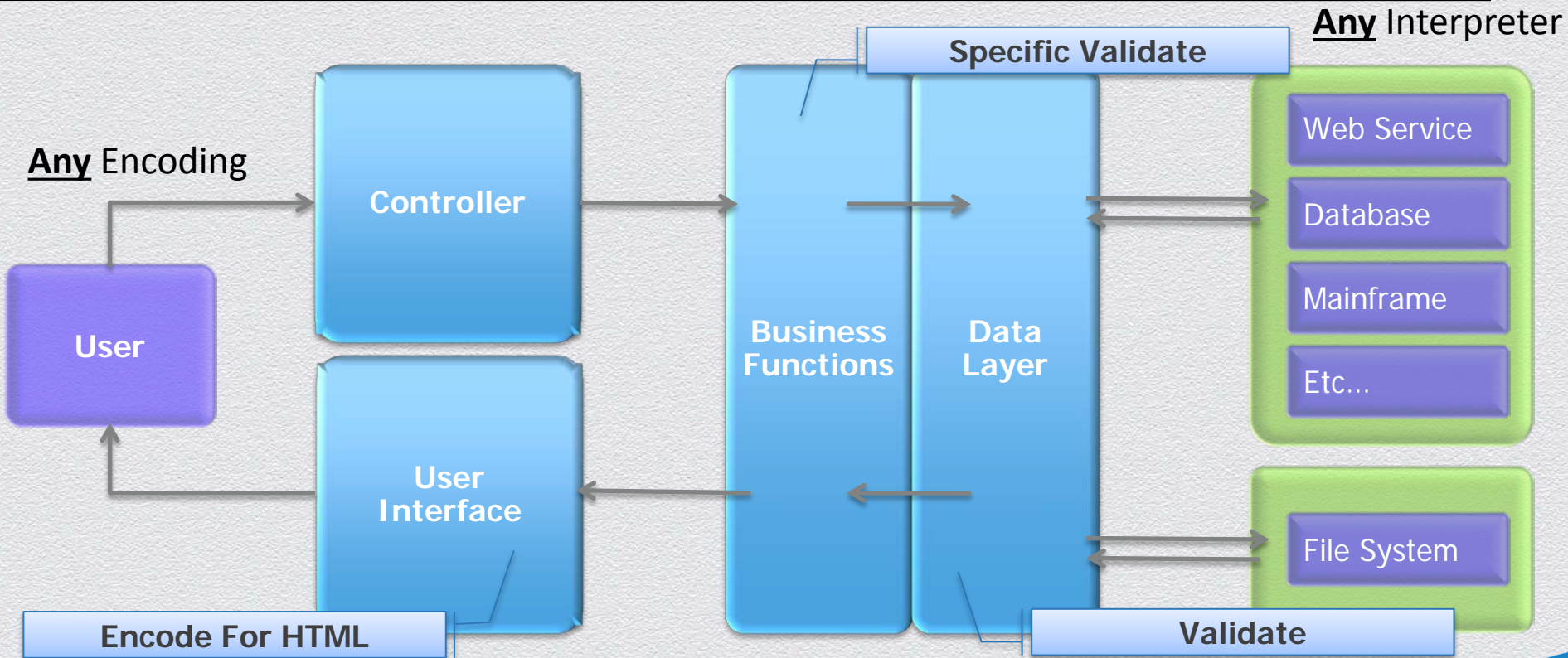


Where Do I Put my Validation ?

Any Interpreter



Where Do I Put my Validation ?



API Example

```
private String getValidInput(String attributeName, String attributeValue, FILTER filter, int maxLength, boolean allowNull) {
    if(log.isDebugEnabled()){
        log.debug(String.format("Attribute:%s value: %s",attributeName,attributeValue));
        log.debug(String.format("filter:%s length:%d allowNull:%s", filter.name(), maxLength, allowNull));
    }
    try {
        return ESAPI.validator().getValidInput(attributeName, attributeValue, filter.name(), maxLength, allowNull);
    } catch (ValidationException e) {
        log.error(String.format("ESAPI ValidationException while parsing parameter name: %s, value: %s",attributeName,attributeValue),e);
    } catch ( IntrusionException e) {
        log.error(String.format("ESAPI IntrusionException while parsing parameter name: %s, value: %s",attributeName,attributeValue),e);
    }
    return null;
}
```

```
public String getValidString(String attributeName, String attributeValue, int maxLength, boolean allowNull) {
    return getValidInput(attributeName, attributeValue, FILTER.SafeString, maxLength, allowNull);
}
```

Define Relevant
Filters

Automated Test Example

```
//////// safe string test
@Test()
public void StringTest() throws Exception {
    GenericTestRunner runner = new GenericTestRunner("safeString"){
        public String validate(String value) {
            return validator.getValidString("safeString", value, 100000, false);
        }
    };
    runner.validValuesTest();
    runner.invalidValuesTest();
}
```

Black/ White
Listing

Filter

Integrating Automated Testing: Example Preventing RegEx DoS and Performance Issues

LivePerson ESAPI Implementation

**Live Person
Security API
(LPSAPI) -
In-House Security
Package based on
ESAPI project**

For Each Product

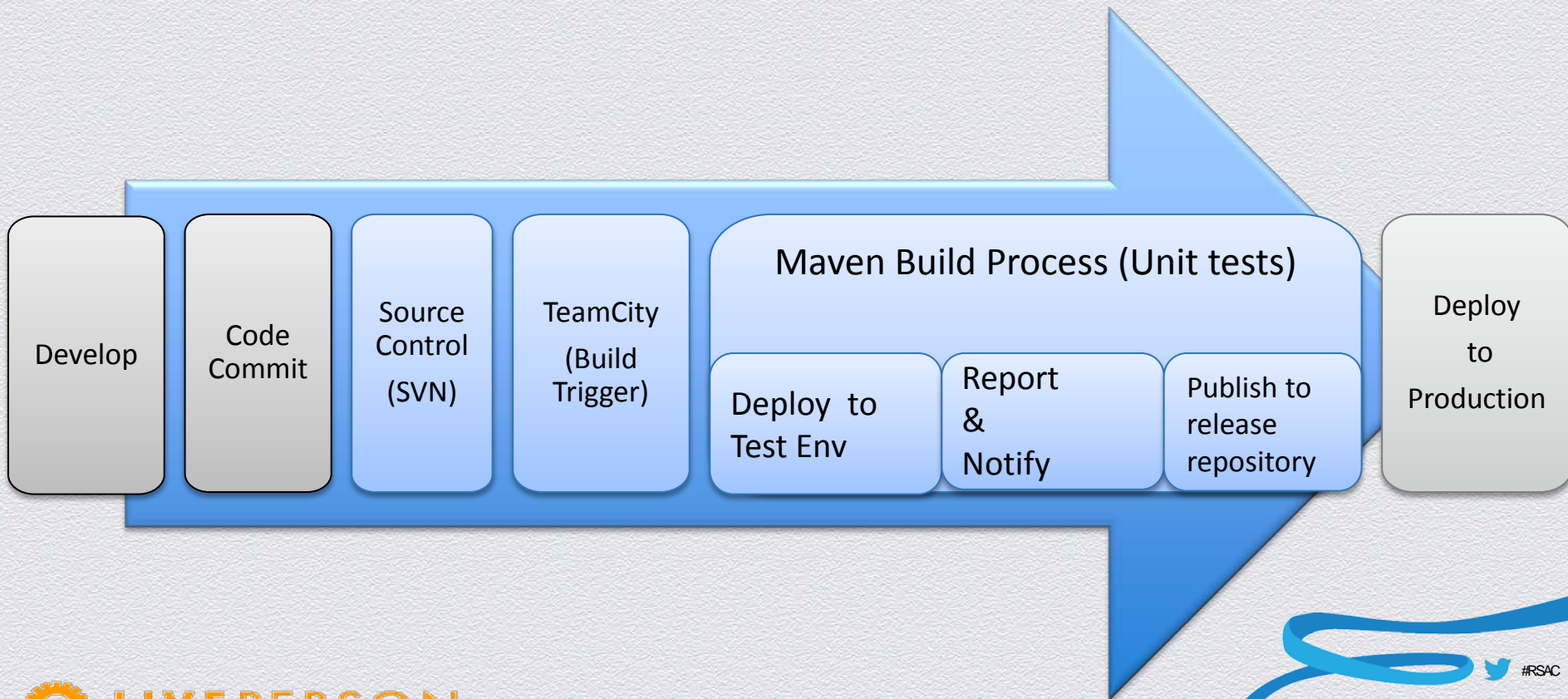
Imports LPSAPI

Enforces correct usage via Source Code
Analysis (SCA)

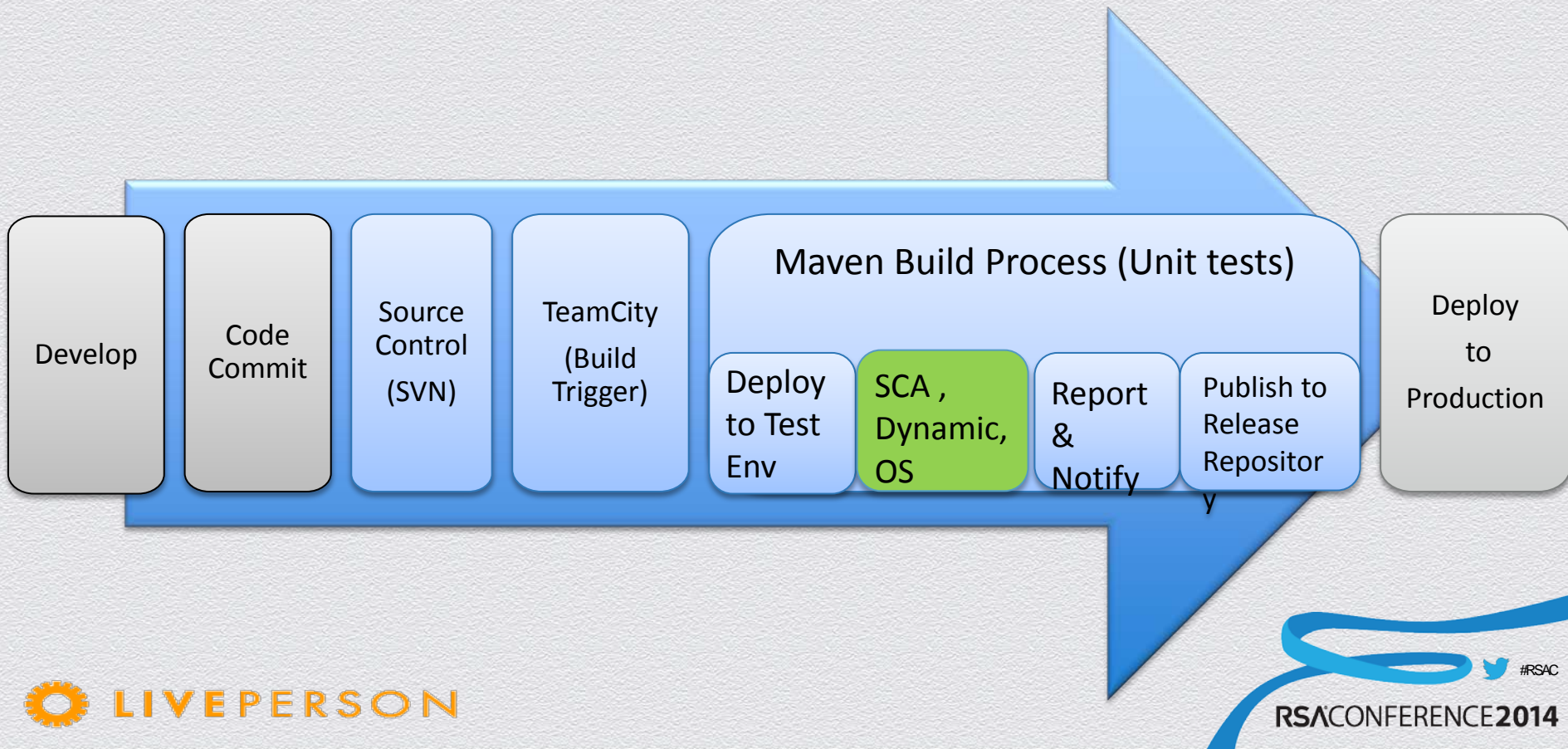
Enforce Open Source Policy

Test your infra BB

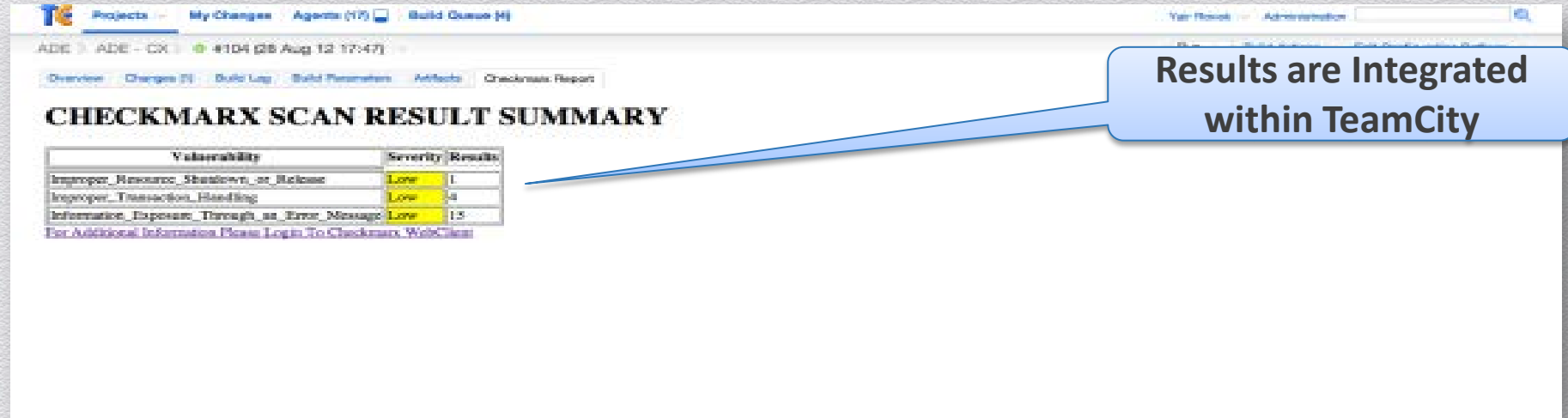
CI Environment



Security in CI Environment



One Dashboard



The screenshot shows the TeamCity web interface. At the top, there are navigation tabs: Projects, My Changes, Agents (17), and Build Queue (4). Below this, there's a breadcrumb trail: ADE > ADE - CX > #104 (28 Aug 12 17:47). A secondary set of tabs includes Overview, Changes (4), Build Log, Build Parameters, Artifacts, and Checkmarx Report. The main content area is titled "CHECKMARX SCAN RESULT SUMMARY". It contains a table with three columns: Vulnerability, Severity, and Results. The table lists three vulnerabilities, all with a "Low" severity. A blue callout bubble points to the table with the text "Results are Integrated within TeamCity".

Vulnerability	Severity	Results
Improper_Resource_Shutdowns_or_Release	Low	1
Improper_Transaction_Handling	Low	4
Information_Exposure_Through_an_Error_Message	Low	15

[For Additional Information Please Login To Checkmarx WebClient](#)

Dive into the Results

CHECKMARX SCAN RESULT SUMMARY

Vulnerability	Severity/Results
Improper_Resource_Shutdown_or_Release	Low 1
Improper_Transaction_Handling	Low 14
Informative_Error_Message_Through_an_Error_Message	Low 15

[For Additional Information Please Login To Checkmarx WebSite](#)

```
createNewEngagementInstance(EngagementInstance engagementInstance) {  
    accountData = ((AccountData)getSession().getAttribute(Constants.ACCOUNT_DATA));  
    enable.isAggServerVersionCompatible(accountData, 9730L) && //check the feature of "add Instance", but only when  
    enable.isFeatureEnabled(AccountData.Feature.ALLOW_ADD_INSTANCE_TO_ENGAGEMENT.toInt());  
    if("Not allowed to add Instance")  
        new IPWebApplicationException(Response.StatusCode.UNAUTHORIZED, "Not allowed to add Instance");  
    enable.enable();  
    if("Chat" != createNewEngagementInstance())  
        return;  
    accountData = ((AccountData)getSession().getAttribute(Constants.ACCOUNT_DATA));  
    engagementInstance.initNewInstance(accountData.getSiteId());  
}
```

Id	Source Folder	Source Filename	Source Line	Source Object	Destination Folder	Destination Filename	Destination Line	Destination Object	Result State	Result Severity
1	sechal-stud...	Engagemen...	73	engagement...	sechal-stud...	Engagemen...	147	build	To Verify	High
2	sechal-stud...	Engagemen...	73	engagement...	sechal-stud...	Engagemen...	146	entity	To Verify	High
3	sechal-stud...	Engagemen...	73	engagement...	sechal-stud...	Engagemen...	146	engagement...	To Verify	High
4	sechal-stud...	Engagemen...	103	engagement...	sechal-stud...	Engagemen...	147	build	To Verify	High
5	sechal-stud...	Engagemen...	103	engagement...	sechal-stud...	Engagemen...	146	entity	To Verify	High
6	sechal-stud...	Engagemen...	103	engagement...	sechal-stud...	Engagemen...	146	engagement...	To Verify	High

Results are integrated within CI environment

Developer has all required info.
No need to involve the Security Team



LIVEPERSON

#RSAC

RSACONFERENCE2014

Challenges

- ◆ Management
- ◆ Developers
- ◆ Technology
- ◆ HR
- ◆ Formal Training VS Coaching and Continues Education
- ◆ Scale
- ◆ PenTest Quality



Key Success Factor Secure Agile Development

Key Success Factors



Identify the process within R&D and set a plan to become part of it



Set Security Package API to be consumed with each code (ESAPI AntiSamy CSRF Guard)



Screen and enforce your policy on your code
Open Source and platform



Use automation to collaborate with the
security dynamic test



Allow customer to run a pen test and work as a
community to succeed

Key Success Factors



Engage tech leaders as security champions by showing them the value



Train developers on a regular basis



Create a knowledge base and discussions around security



Break the build for any "High" or "Medium" findings



Start small but think big



LIVEPERSON

#RSAC

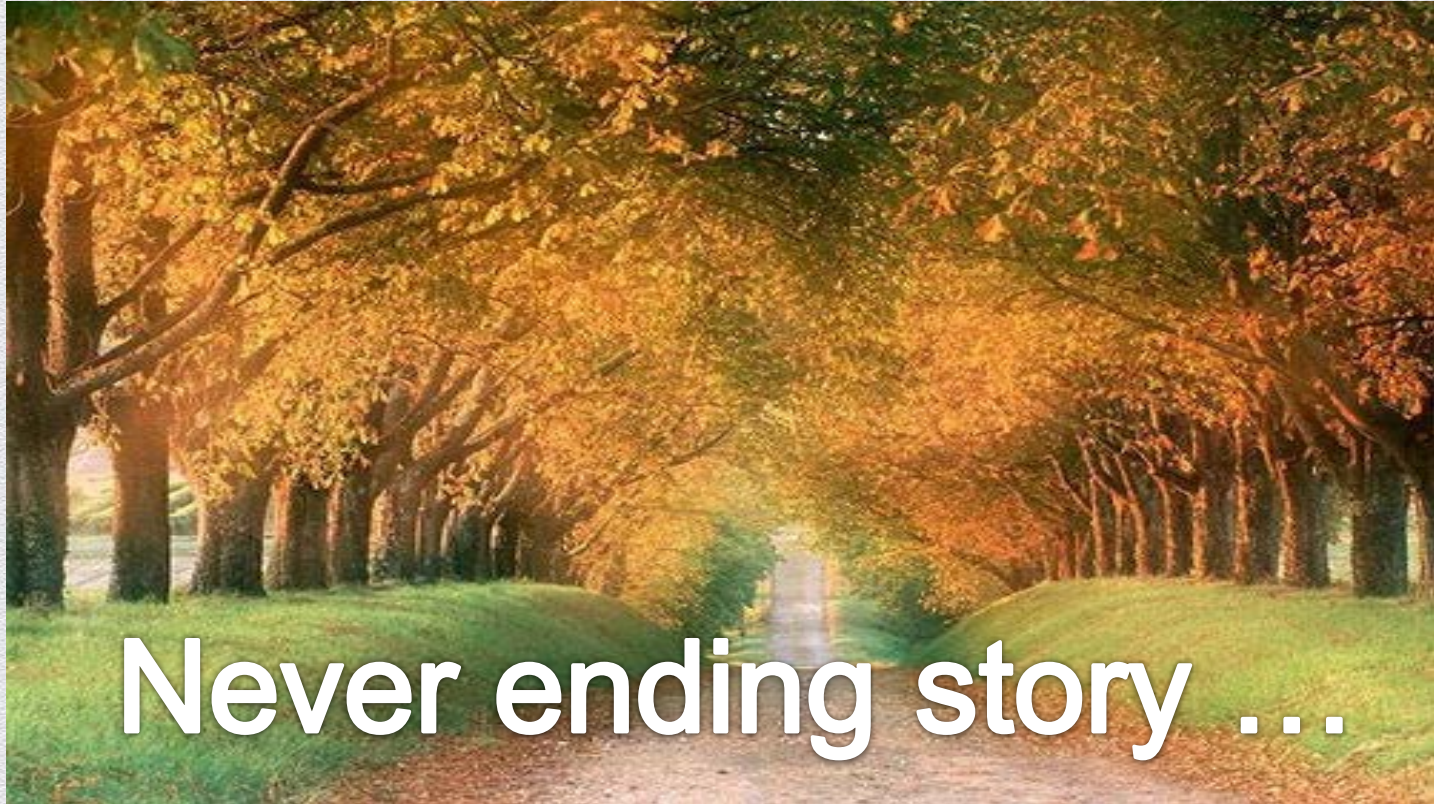
RSACONFERENCE2014

Q&A

Contact Me!

 yairr@liveperson.com

 @lione_heart



Never ending story ...

Links to Resources

- ◆ OWASP – https://www.owasp.org/index.php/Main_Page
- ◆ AGILE & SDLC - <http://www.ambysoft.com/essays/agileLifecycle.html>
- ◆ MS SDLC - <http://www.microsoft.com/security/sdl/default.aspx>