
# Domino's Delivery of a Faster Response was No Standard Order

**Michael Sheppard, Domino's Application Security Manager**

@AppSecShepp

www.appsecshepp.com

October 2018 | Version 1.0

# MICHAEL SHEPPARD

Manager, Application Security

splunk> .conf18

# DOMINO’S

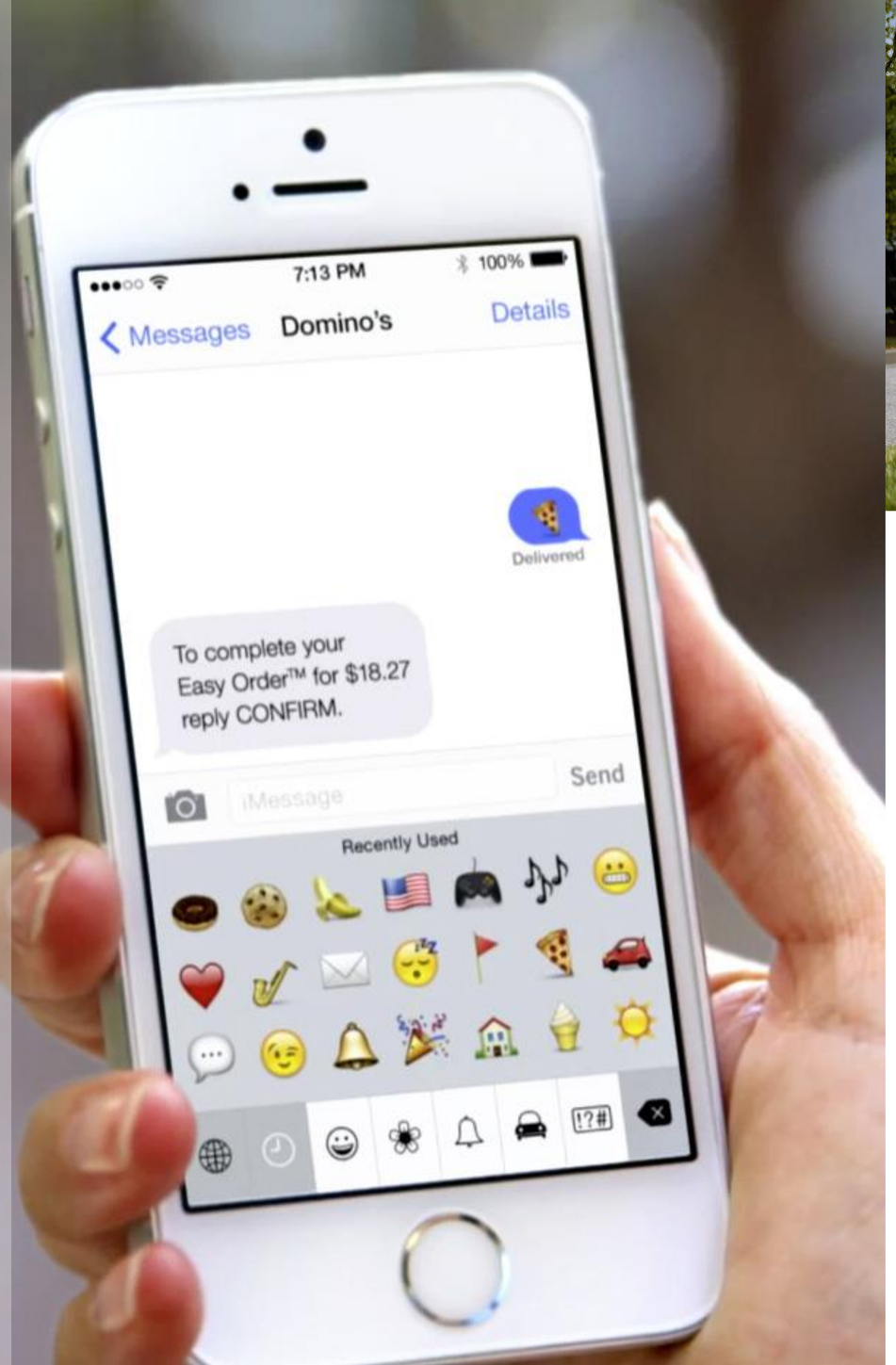
#1 in Pizza Delivery
-OH YES WE DID-

# A technology company that delivers pizza

## More than 14,000+ stores

## In over 85 international markets.

## $5.6 Billion in Global Digital Sales

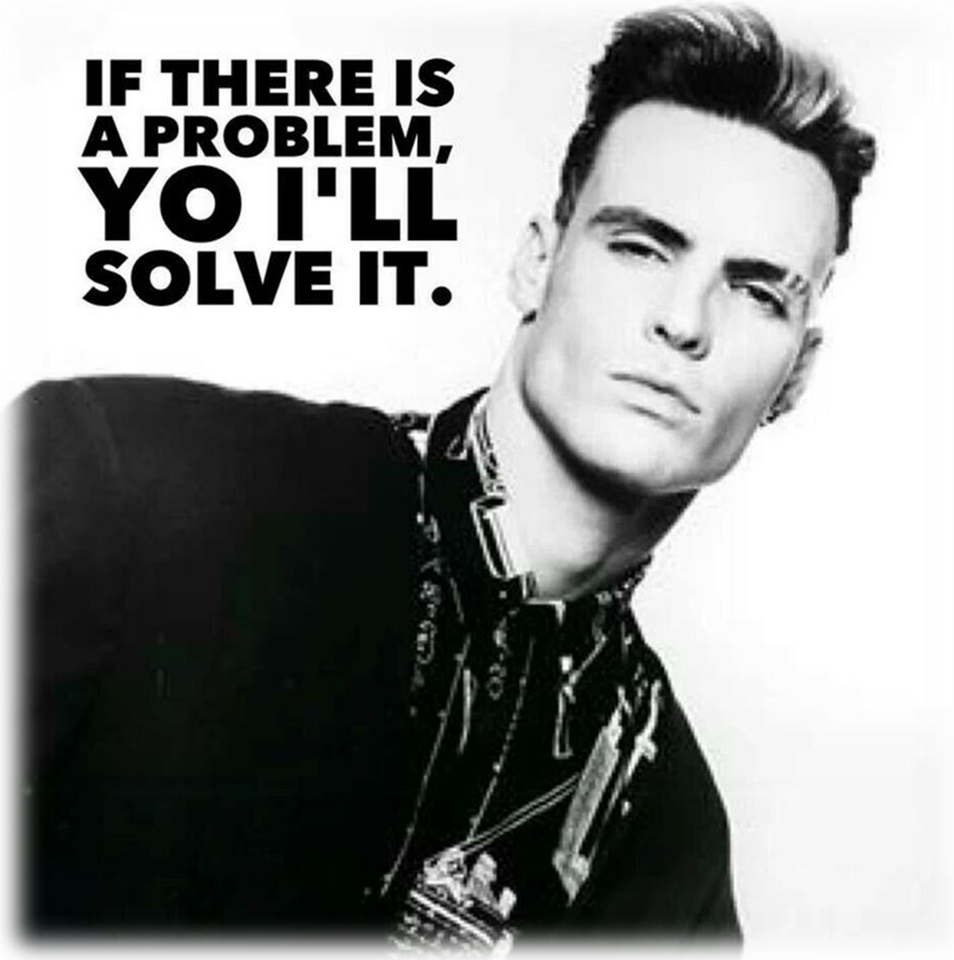




PROBLEM – A MATTER OR SITUATION REGARDED AS UNWELCOME OR HARMFUL

# Our security review process sucked.

# Very few teams engaged security and thus Risk was



“

**They wouldn’t even lift a finger to save their own grandmothers from the Ravenous Bugblatter Beast of Traal without orders signed in triplicate, sent in, sent back, queried, lost, found, subjected to public inquiry, lost again, and finally buried in soft peat for three months and recycled as firelighters.”**

DOUGLAS ADAMS, THE HITCHHIKER’S GUIDE TO THE GALAXY

## PREVIOUS PROCESS

**Broken / Manual**

**Meetings, lots of Meetings**

**No Alignment**

**No Visibility**

## PROCESS AFTER AUTOMATION

**Integrated**

**Streamlined**

**Automated**

**Monitored**

## PREVIOUS PROCESS

Broken / Manual

Meetings, lots of Meetings

No Alignment

No Visibility

## PROCESS AFTER AUTOMATION

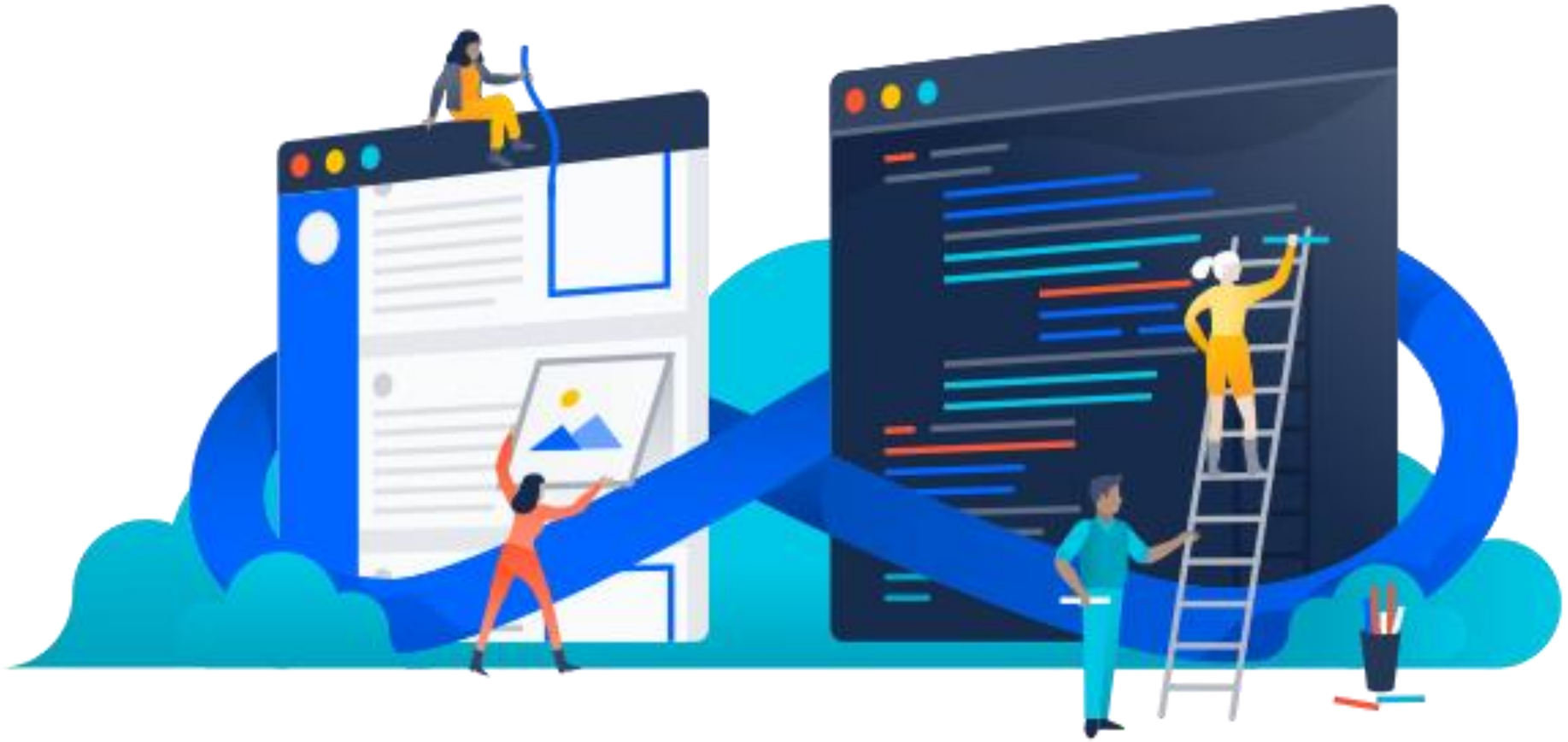
Integrated

Streamlined

Automated

Monitored

# Confluence + JIRA + Splunk



# How did we *unsuck* our Security Process

- We had to go to were the developers live. (Confluence and JIRA)
- Created a Form on Confluence using Adaptavist Forms for Confluence.
- Asked 8 Critical questions to ascertain the risk of a project.
- Partnered with Adaptavist and developed our JIRA Form Handler application that handles incoming form data & automatically performs Risk decisioning.
- Created and assigned JIRA tickets which detail out key Domino’s Security requirements.
- Presented detailed Key Performance Indicators metrics in Splunk Dashboard from JIRA Security Tickets

# How did we *unsuck* our Security Process

- We had to go to were the developers live. (Confluence and JIRA)
- Created a F[illegible]ce using Adaptavist Forms for Confluence.
- Asked 8 Critical questions to ascertain the risk of a project.
- Partnered with Adaptavist and developed our JIRA Form Handler application that handles incoming form data & automatically performs Risk decisioning.
- Created and assigned JIRA tickets which detail out key Domino’s Security requirements.
- Presented detailed Key Performance Indicators metrics in Splunk Dashboard from JIRA Security Tickets

# How did we *unsuck* our Security Process

- We had to go to were the developers live. (Confluence and JIRA)
- Created a Form on Confluence using Adaptavist Forms for Confluence.
- Asked 8 Critical questions to ascertain the risk of a project.
- Partnered with Adaptavist and developed our JIRA Form Handler application that handles incoming form data & automatically performs Risk decisioning.
- Created and assigned JIRA tickets which detail out key Domino’s Security requirements.
- Presented detailed Key Performance Indicators metrics in Splunk Dashboard from JIRA Security Tickets

# How did we *unsuck* our Security Process

- We had to go to were the developers live. (Confluence and JIRA)
- Created a Form on Confluence using Adaptavist Forms for Confluence.
- Asked 8 Critical questions to ascertain the risk of a project.
- Partnered with Adaptavist and developed our JIRA Form Handler application that handles incoming form data & automatically performs Risk decisioning.
- Created and assigned JIRA tickets which detail out key Domino’s Security requirements.
- Presented detailed Key Performance Indicators metrics in Splunk Dashboard from JIRA Security Tickets

# How did we *unsuck* our Security Process

- We had to go to were the developers live. (Confluence and JIRA)
- Created a Form on Confluence using Adaptavist Forms for Confluence.
- Asked 8 Critical questions to ascertain the risk of a project.
- Partnered with Adaptavist and developed our JIRA Form Handler application that handles incoming form data & automatically performs Risk decisioning.
- Created and assigned JIRA tickets which detail out key Domino’s Security requirements.
- Presented detailed Key Performance Indicators metrics in Splunk Dashboard from JIRA Security Tickets

# How did we *unsuck* our Security Process

- We had to go to were the developers live. (Confluence and JIRA)
- Created a Form on Confluence using Adaptavist Forms for Confluence.
- Asked 8 Critical questions to ascertain the risk of a project.
- Partnered with Adaptavist and developed our JIRA Form Handler application that handles incoming form data & automatically performs Risk decisioning.
- Created and assigned JIRA tickets which detail out key Domino’s Security requirements.
- Presented detailed Key Performance Indicators metrics in Splunk Dashboard from JIRA Security Tickets

# Application Security Engagement Request

Created by Michael Sheppard (IT - SecDomEcom), last modified on May 05, 2017

Adaptavist

## Application Security Engagement

### Step One

Applicant Name:* sheppam

Please provide your name

Service Name*

Please provide Service Name (ex. kiosk-service). If the service name has not yet been identified, please use (tbd-service).

What Jira Project Key Name is this Application / Service under*

Please list the Jira Project Key Name

Step One | Step Two | Step Three | Final

Back | Next

# Application Security Engagement Request

Adaptavist

Created by Michael Sheppard (IT - SecDomEcom), last modified on May 05, 2017

## Application Security Engagement

### Step Two

Is the Service public facing? i.e. (Yes or No)*
Please Select
Please choose one

Does it handle Sensitive Data? i.e. (PCI, PII, Credentials, etc.)*
Please Select
Please choose one

Does it use any of the following HTTP Methods / Verbs? i.e. (POST, PUT, DELETE)*
Please Select
Please choose one

Step One — Step Two — Step Three — Final

Back Next

# Application Security Risk Form

Adaptavist

Created by Michael Sheppard (IT - IT_CORE), last modified by Holly Marsh (IT - InfIntEcom) on Jun 22, 2017

## Step Three

Does this Service connect to a back-end database?* Please Select

Please choose one

Does this Service make calls to any other internal Services?* Please Select

Please choose one

Does this Service initiate a call down to stores? (E.g. RemotePulseAPI)* Please Select

Please choose one

Step One — Step Two — Step Three — Final

Back Next

# Application Security Risk Form

Created by Michael Sheppard (IT - IT_CORE), last modified by Holly Marsh (IT - InfIntEcom) on Jun 22, 2017

Adaptavist

## Final

Does this Service send data to external 3rd parties*
Please Select
Please choose one

Is this Service under any regulatory or governmental requirements? i.e. (PCI, SOX, GLBA, etc.)*
Please Select
Please choose one

If available, please provide Confluence link for Architectural Diagrams.
Please provide link in Confluence

Special Notes:
ex. This service is a supported by a third party.
Please provide any additional information

Explain the Business Logic
ex. This service sends nutrition data to the government.
Brief description of what this Service does.

Step One — Step Two — Step Three — Final

Back | Submit

Decision Points | Ticket Templates | Actions | Score Ranges | Request Results

| Decision Point | Match Type | Answer | Action Type | Score |
|---|---|---|---|---|
| public_facing | Equal_To | Yes,Y,y | Create_New_Ticket | 5 |
| third_parties | Equal_To | Yes,Y,y | Create_New_Ticket | 4 |
| regulatory_requirements | Equal_To | Yes,Y,y | Create_New_Ticket | 5 |
| sensitive_data | Equal_To | Yes,Y,y | Score_Range_Calculation | 7 |
| http_method | Equal_To | Yes,Y,y | Score_Range_Calculation | 5 |
| backend_database | Equal_To | Yes,Y,y | Score_Range_Calculation | 5 |
| stores | Equal_To | Yes,Y,y | Score_Range_Calculation | 4 |
| other_services | Equal_To | Yes,Y,y | Score_Range_Calculation | 3 |

Decision Points | Ticket Templates | Actions | Score Ranges | Request Results

| Name | Lower Range | Upper Range | Service Tickets |
|---|---|---|---|
| Critical Range | 30 | 40 | Secure Coding Guidelines Ticket<br>Security Architecture Review Ticket<br>Threat Modeling Engagement Ticket<br>Non-Functional Requirements Ticket<br>Functional Requirements Ticket |
| High Range | 20 | 29 | Secure Coding Guidelines Ticket<br>Security Architecture Review Ticket<br>Threat Modeling Engagement Ticket<br>Non-Functional Requirements Ticket<br>Functional Requirements Ticket |
| Medium Range | 10 | 19 | Secure Coding Guidelines Ticket<br>Security Architecture Review Ticket<br>Non-Functional Requirements Ticket<br>Functional Requirements Ticket |
| Low Range | 0 | 9 | Secure Coding Guidelines Ticket<br>Functional Requirements Ticket |

# [confluence] AppSecRiskForm

DP

Delton Perez
Today, 3:53 PM
Michael Sheppard (IT - SecDomEcom)

Reply all

> Label: Default 18 Month Delete (1 year, 6 months, and 3 days) Expires: 2/13/2020 2:53 PM

applicant_name: perezd3
service_name: Pulse
jira_key: PUL
public_facing: No
sensitive_data: No
http_method: No
backend_database: No
other_services: No
stores: No
third_parties: No
regulatory_requirements: No
confluence_link:
special_notes: ex. This service is a supported by a third party.
business_logic: This change is to limit printing of Loyalty receipt for non-members on transactions under a dollar amount.

# JIRA Security Requirements Ticket

Dashboards Projects Issues Boards Tests AIO Reports Create Search

**InfoSec Projects**
IAM Phase 2 Kanban

- User story map
- Kanban board
- Releases
- Reports
- Issues
- Components
- Roles
- Tests

InfoSec Projects / IP-135

## Request for a Web Application Penetration Test by Ron Ulko for Service One

Edit | Comment | Assign | More | Backlog | Selected for Development | Workflow | Export

### Details

| | | | |
|---|---|---|---|
| Type: | Task | Status: | BACKLOG (View Workflow) |
| Priority: | Major | Resolution: | Unresolved |
| Labels: | None | | |

### Description

Service One
condluence.com
ex. This service sends nutrition data to the government.
ex. This service is a supported by a third party.

*****Web Application Penetration Testing Requirement Ticket

This ticket requires you the TDM to ensure your project has been reviewed by Ron Ulko and a determination made by Ron Ulko as to whether or not your project requires Web Application Penetration Testing.

TDM - It is your responsibility to ensure this requirement is met.

TDM - This security requirement is considered met;

A.) When Ron Ulko determines Web Application Penetration Testing is not required for your project and notates as such in the comments field for this ticket whereby you the TDM can then close this ticket.

B.) Or a Web Application Penetration Test is performed on your project and Ron Ulko notates in the comments field for this ticket that this requirement has be met and you are cleared and or have satisfied this particular requirement.

****TDM - You are not to CLOSE this ticket until this specific security requirement is met and or Ron Ulko determines by notating the comments field in this ticket that Web Application Penetration Test is not required for your project.

Task Assignee: Ron Ulko

*****Ron Ulko you are responsible within 72 hours of receiveing notification via e-mail of this security requirements ticket to contact the project TDM via e-mail and or phone and schedule an initial meeting to review / determine whether or not this project requires a Web Application Penetration Test

TDM Next Steps - TDM your next step is to meet with Ron Ulko once engaged by Ron Ulko and have your project reviewed and have a determination made by Ron Ulko as to whether your project requires a Web Application Penetration Test. If Ron Ulko determines that your project does in fact require a Web Application Penetration Test then TDM you are responsible for working with Ron Ulko to schedule the Web Application Penetration Test.

If a determination is made by Ron Ulko that your project requires a Web Application Penetration Test then TDM you are responsible for;

Working with Ron Ulko to Schedule the Web Application Penetration Testing for your project.

Provide necessary itmes to perform the Web Application Penetration Test for your project.

Items:
Availability of Application and or Service
Test Data for Application and or Service
Test Credentials for Application and or Service

### People

| | |
|---|---|
| Assignee: | Ronald Ulko (IT - IT_CORE) |
| | Assign to me |
| Reporter: | Michael Sheppard (IT - IT_CORE) |
| Votes: | 0 |
| Watchers: | 3 Stop watching this issue |

### Dates

| | |
|---|---|
| Created: | 4 days ago |
| Updated: | 4 days ago |

### Development

Create branch

### Agile

View on Board

### HipChat discussions

| | |
|---|---|
| Dedicated room: | Create a room Choose a room |
| Other rooms: | Issue mentioned in 0 rooms |

# The Raw Numbers

## Application Security Risk Form Usage over 18 months

**#400**

**Form Submissions**

**#2,000**

**Tickets Created**

**#800**

**Engagements Opened**

**#320**

**Requirements Not Met**

**#600**

**Engagements Closed**

**#4,000**

**Requirements Met**

splunk> .conf18

# Change the Conversation w/Security

## Standardize

Create Consistent Engagement across the Enterprise.

## Easier

Remove the dependency on meetings and provide project teams clear direction on approval requirements and next steps

## Faster

Make input and decision workflow take minutes instead of hours.

# Other Internal Use Cases

Finance

E-Commerce

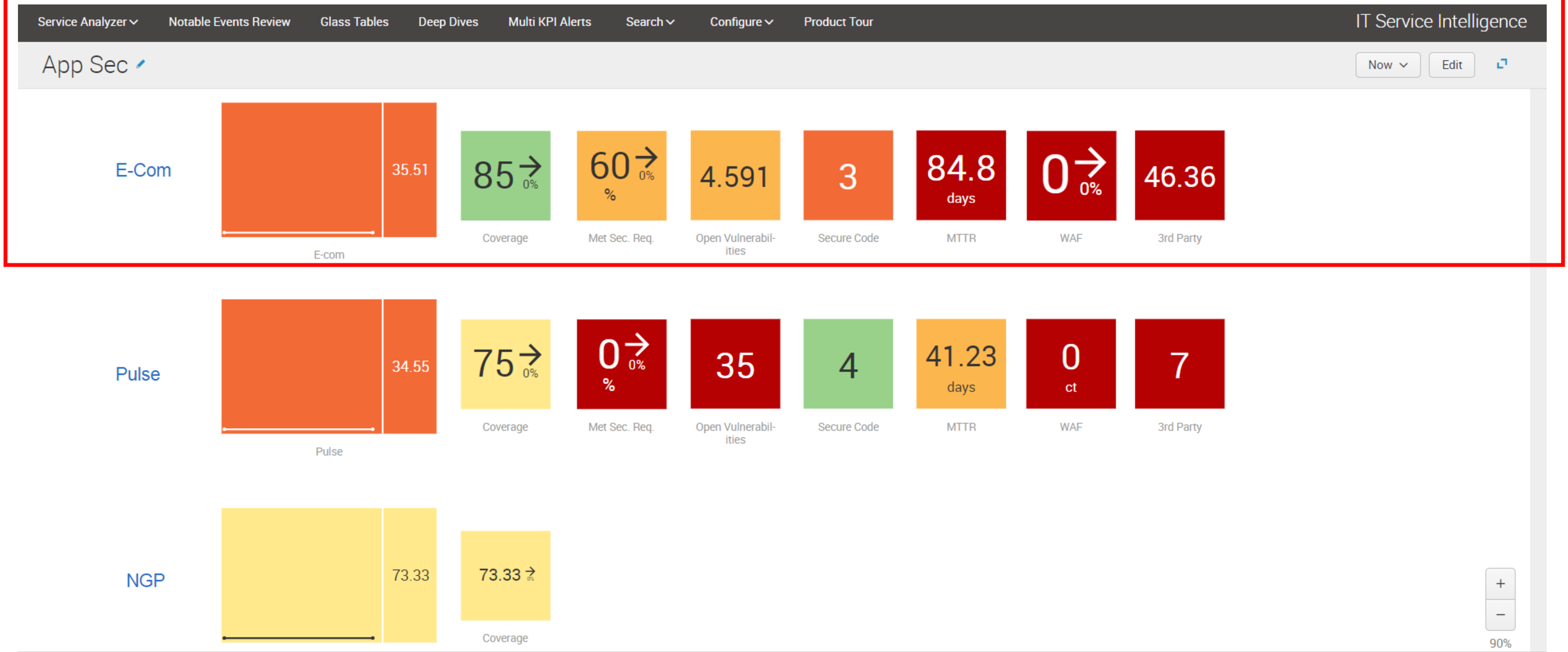
PMO

SRE

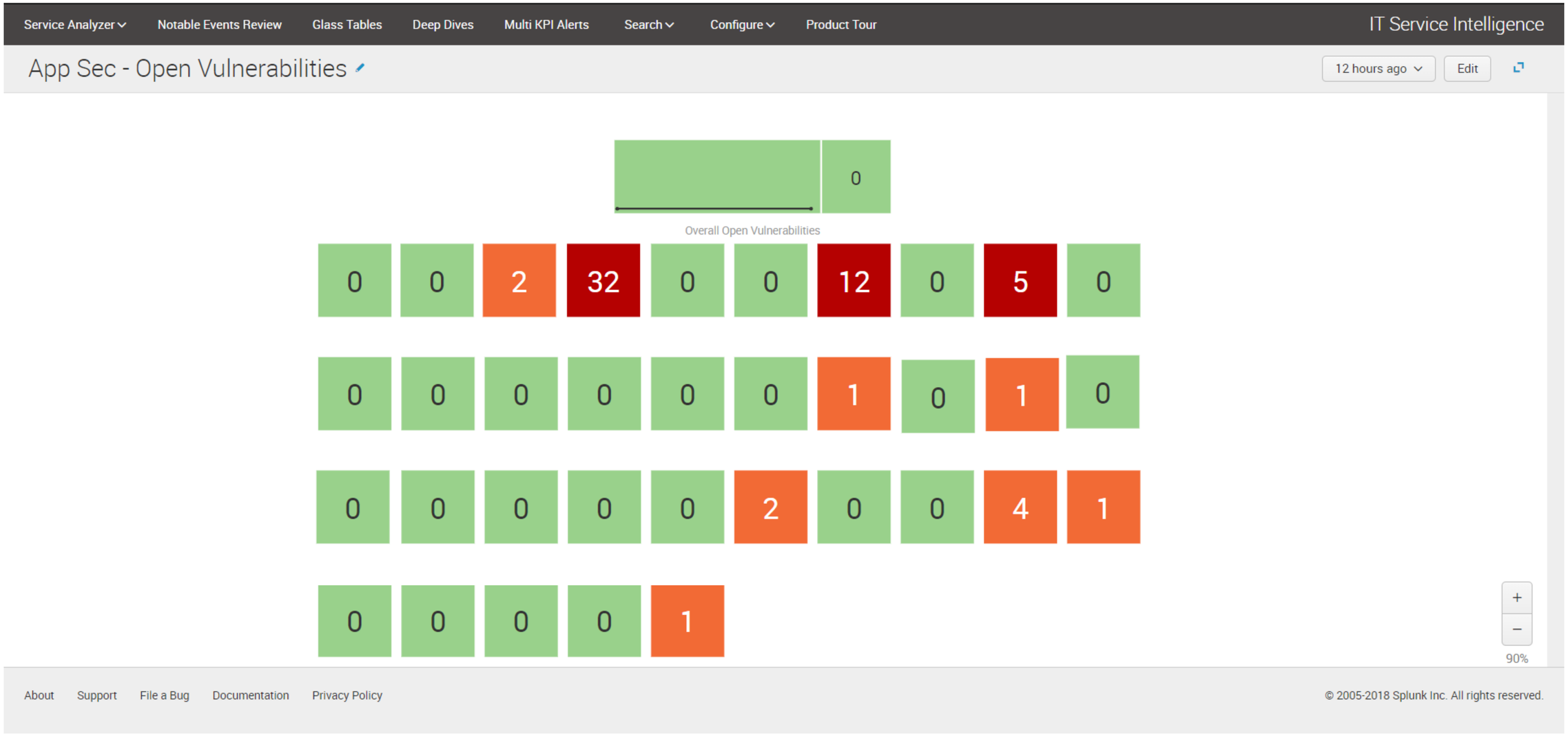
SOC

# Now that we've streamlined and automated!  It's time to Monitor.

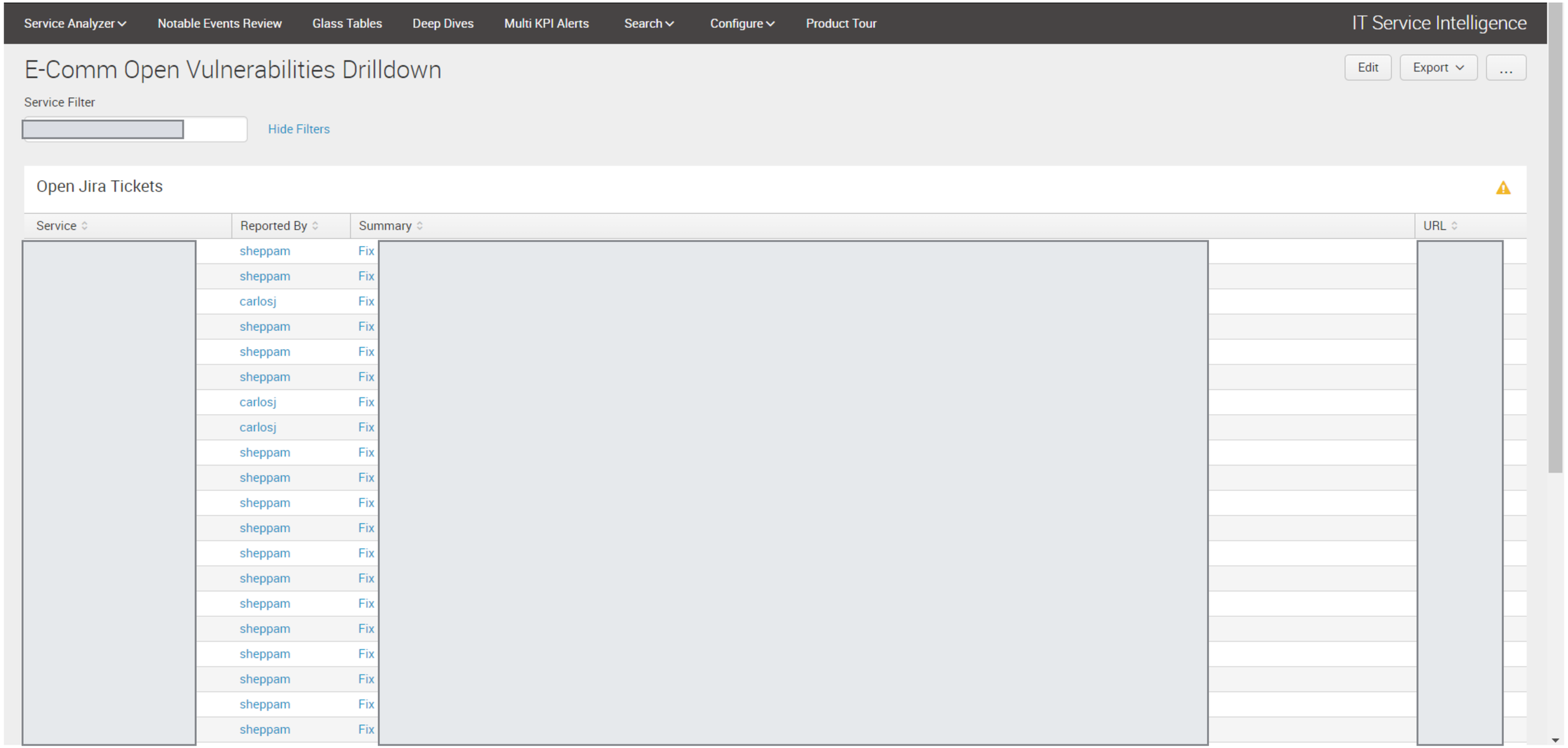
# AppSec Metrics Dashboard – Executive View



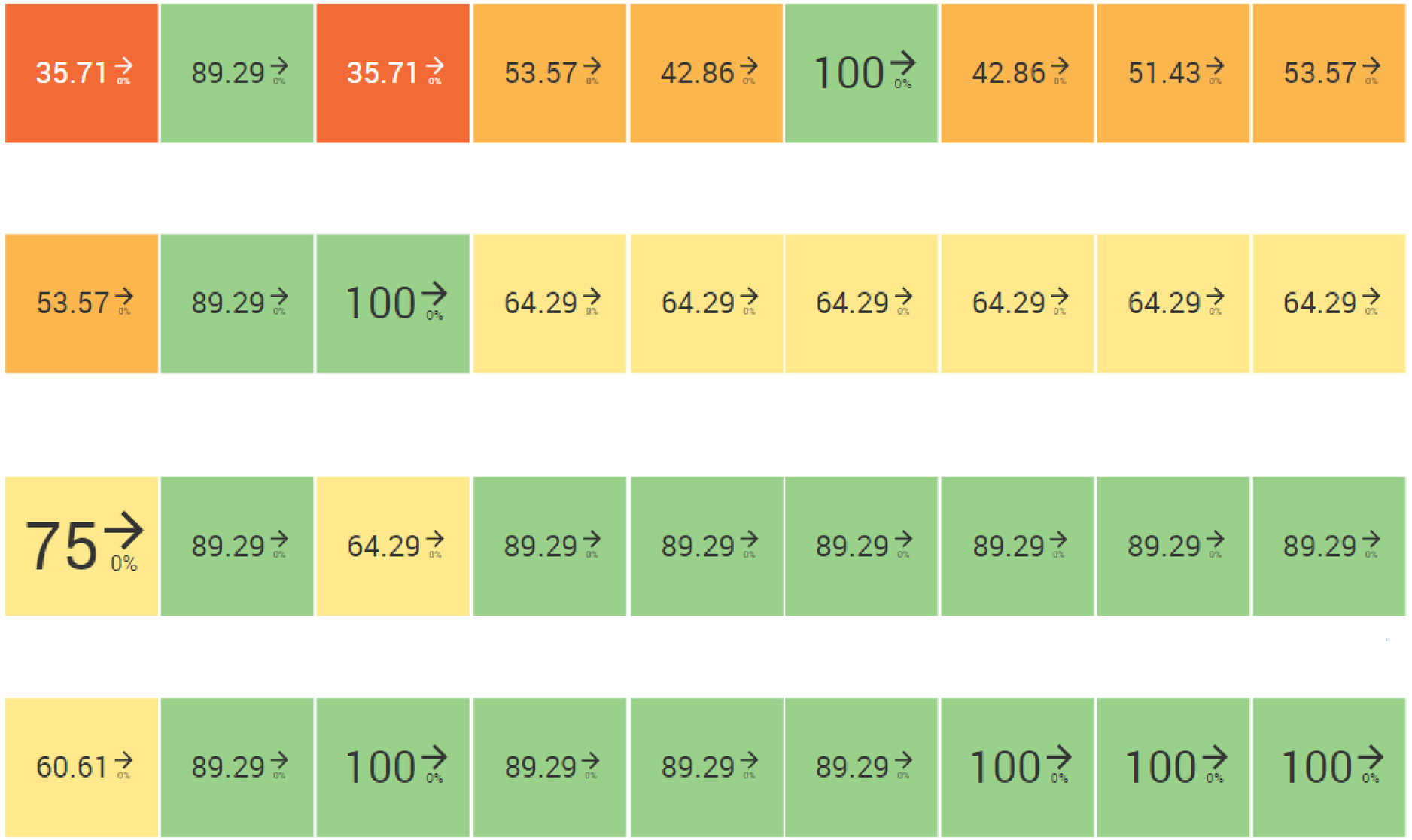
# KPI Metrics Drill-down



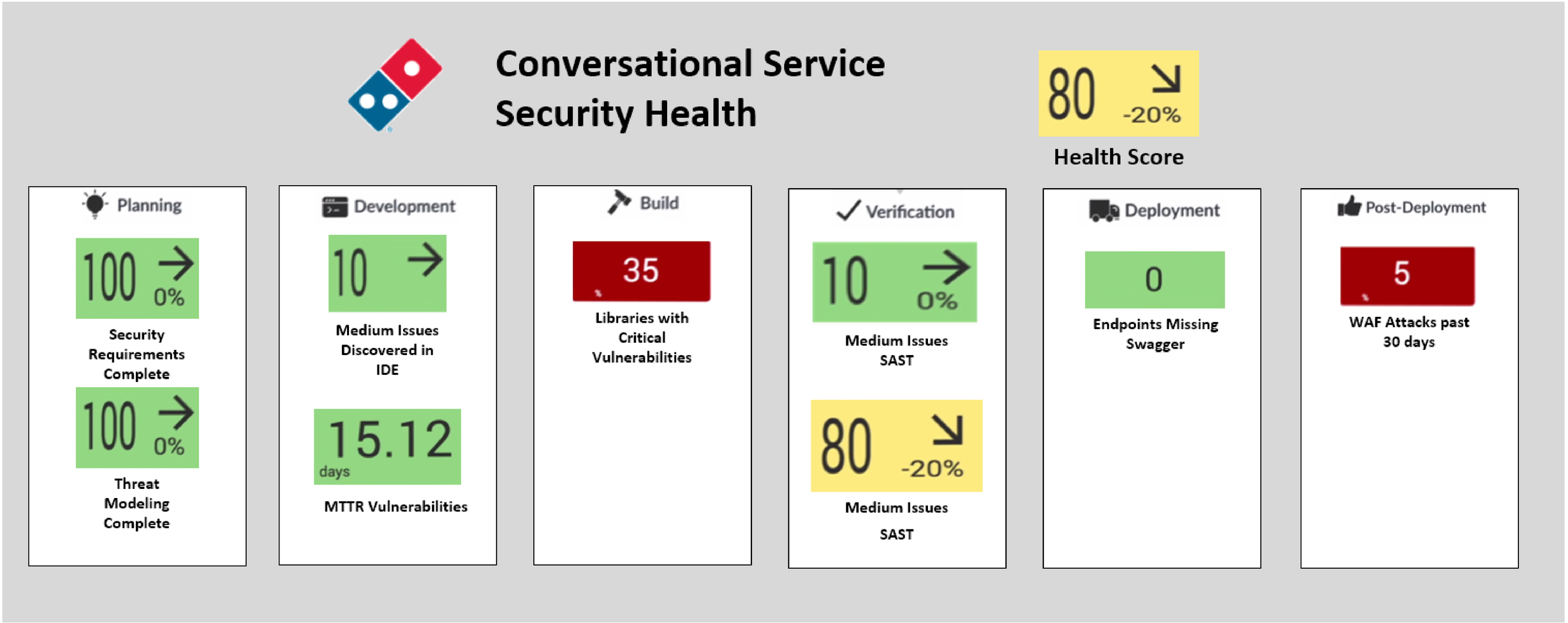
# Drill-down to Tickets



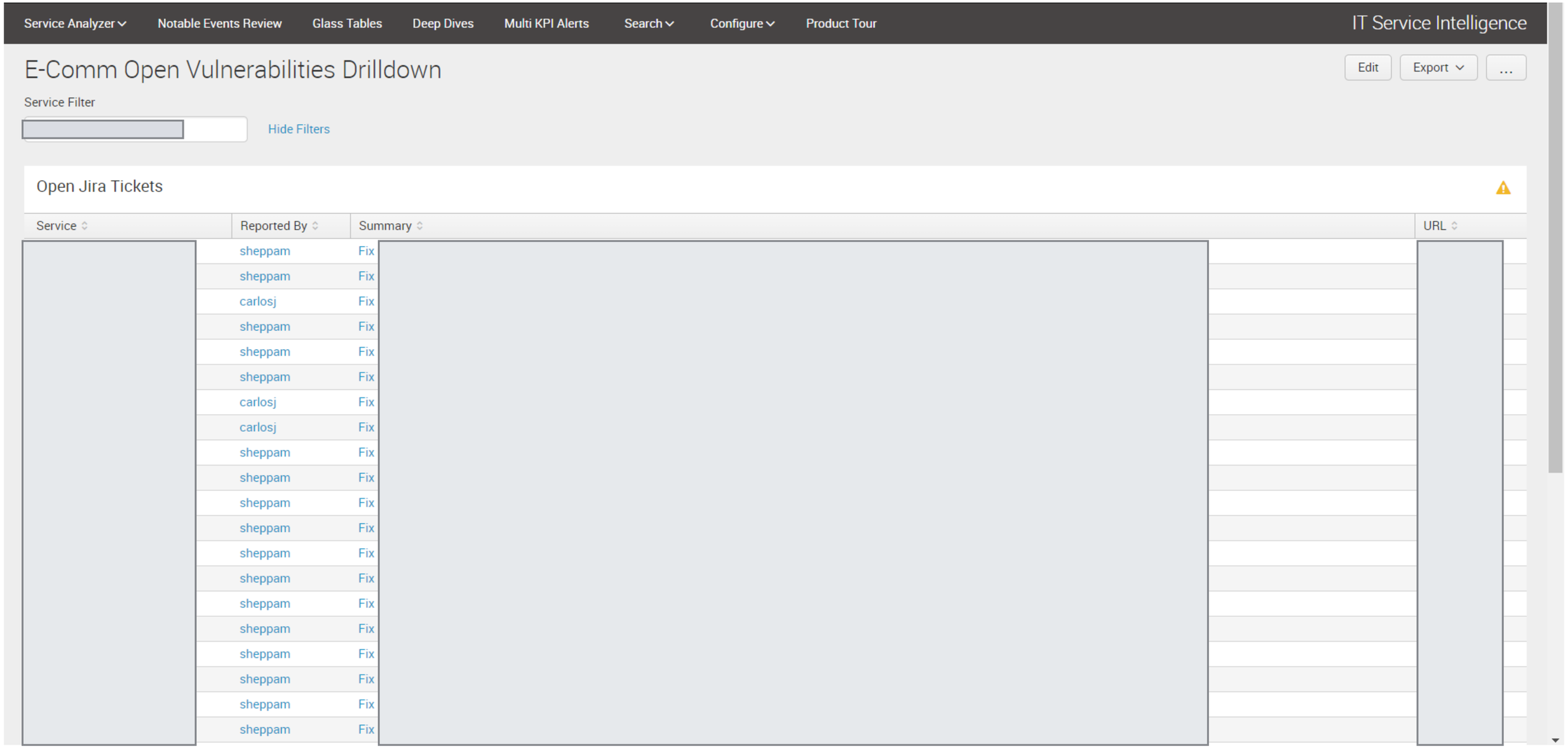
# Services Security Health Score



# AppSec KPI Metrics Dashboard



# Drill-down to Tickets



# Metrics

# 3000 +hrs

**of meetings gone per year!**

# $300,000

**Estimated saved per year by reduced engagement time!**

# 75%

**Risk Reduction per project!**

# Conclusion

- Always look to Automate
- Look to Empower Teammates
- Pick Good Partners
- Monitor and Show your Metrics

# Security is Everyone's Job

# Thank You

**Don't forget to rate this session in the .conf18 mobile app**