Rapid Product Security Incident Response Using a Workflow Based Solution

Diane Mickelson, dmickel@us.ibm.com
Rod Henderson, rodhende@us.ibm.com
Please Note:

• IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion.

• Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

• The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

• The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

• Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.
Agenda

• IBM PSIRT
• Tooling Design Challenge
• Workflow-Based PSIRT
• PSIRT Demo
IBM PSIRT Roles

Main players

- **PSIRT Operations** – Oversees PSIRT Tool and compliance
- **Product Responder** – Performs detailed analysis and creates remediation plan
- **Brand Lead** – Monitors actions of Brand team to ensure activity and progress
- **Pillar Lead** – Oversees vulnerability assessments performed by the Product Teams
- **Scorer (IBM X-Force)** – Determines severity of the vulnerability and provides both the Common Vulnerability Scoring System (CVSS) details and the Common Vulnerability and Exposure (CVE)
- **Other Reviewers**

PSIRT users responsibility:

- Collaborate with PSIRT and Brand team
- Validate vulnerability
- Multi-tiered review of Remediation and Communication Plan (approach and timeline to address issue)
- Adhere to plan
- Prevent disclosure of sensitive information
Tooling Design Challenge
Simple scenario PSIRT process workflow

- **Create Advisory**
  - Advisories represent security vulnerabilities
  - Brand Lead, Pillar Lead or Responder - Internally found or Customer

- **Create Product Record(s)**
  - Responder
  - PSIRT Operations

- **Responder researches vulnerabilities and requests scoring**

- **Responder documents Remediation and Communication Plan**

- **X-Force updates advisory with CVE and CVSS Details**

- **Event notification sent**

- **Remediation Plan Reviewers**
  - Remediation Plan Reviewer
  - PSIRT Leadership*
  - Other Reviewers*

- **Review Plan**

- **Develop Fix**

- **Draft Security Bulletin**
  - Security Bulletin Reviewer
  - PSIRT Operations
  - Other Reviewers*


- **Publish Fix and Bulletin**

* Additional reviews may not be needed
PSIRT Process problems before workflow tool

1. Unstructured tasks and communication (paper or email)
2. Inefficient working environment spans systems
3. Inconsistent prioritization
4. Incomplete or inaccurate data flow between systems
5. Lack of control over system and business events (exceptions)
6. Poor visibility into process performance
Workflow-Based PSIRT Tool
BPM is an integrated approach to aligning the key activities of an organization into processes that you can consistently measure to optimize value to your organization and its end customers.
PSIRT Process problems before workflow tool

- Inefficient
- Ineffective
- Inaccurate
- Incomplete
- Inconsistent
- Inflexible
- Invisible
PSIRT Process with workflow

- Automate workflow & decision making
- Helps reduce errors and improve consistency
- Standardize resolution across geographies
- Leverage existing systems and data
- Monitor for business events and initiate actions
- Real-time visibility and process control

Benefits:
- Potential reduction in manual work and errors
- Faster, more consistent issue resolution
- Metrics, measurements, visibility and business-friendly reports
- Rapid, agile and iterative process improvements
Overview of PSIRT Tool with Workflow

• Workflow based tooling helps ensure timely identification, analysis, resolution and reporting of security vulnerabilities in IBM products

• PSIRT Process is integrated into the tool, where the steps within the process follow a managed workflow with tasks and notifications

• Tool supports Product Responders, Pillar Leads, Brand Leads, Reviewers, IBM X-Force and PSIRT Operations

• Each task has a task due date to ensure teams stay on track

• Tool features:
  – Workflow engine
  – Event notification
  – Task lists
Workflow engine

• Work flow engine guides the PSIRT users through the necessary steps in the PSIRT process

• The tool is like a big flow chart – where your next task depends on the answers you provide in your current task

• All PSIRT related transactions should occur inside the tool
Event notifications

• Event notifications are used to alert users when
  – Advisory created
  – Product Record created
  – Product Record closed
  – Product Record Remediation Plan created
  – Other reviews are required
  – Product Record Remediation Plan has completed reviews
  – New task assigned
  – Task almost due
  – Task overdue
Task based

• Task – an action a user needs to complete (to-do)
• Each user’s to-do’s are organized into a series of tasks
• The tool generates tasks for the appropriate person to complete for each PSIRT Process step
  – Workflow is role based - each task is designed to be completed by a particular role
  – Each users tasks are listed in their PSIRT Task list
  – Users must complete a task in order for the tool to progress to the next task
• All Brand and Pillar Leads are able to view all tasks for every role to track progression of a record
• Users need to claim a task to work on it; once claimed no one else can work the task
Workflow-Based PSIRT Tool benefits

- PSIRT Tool supports the PSIRT Process and guides users through a series of tasks
- PSIRT Policies and rules are incorporated into the PSIRT Tool
  - Plans are checked by a compliance checker
  - Out of compliance records have different workflows with extra approvals
- Leads are able to easily pinpoint a Product Record’s progression through the PSIRT Process
- PSIRT Operations and Leads can better monitor records that are non-complaint
- Reduction of rework due to exceptions and errors
- Significant reduction in emails
PSIRT Demo
All of a user’s tasks are in one convenient location, clearly marked with due dates.
Complete audit trail of every product record

Email reminders to ensure tasks are handled on time
All relevant information is available for each step of the process.

Direct links to the Knowledge Center.
Built in checks for duplicate records
<table>
<thead>
<tr>
<th>Brand:</th>
<th>Product ID:</th>
<th>PSIRT Blog Tag:</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSIRT Test 1</td>
<td>3169</td>
<td></td>
</tr>
<tr>
<td>Pillar Name:</td>
<td>Product short name:</td>
<td>PSIRT Test 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product Name:</td>
<td>Is Product archived?</td>
<td>PSIRT Test 1</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Product Type:</td>
<td></td>
<td>On-Premises</td>
</tr>
</tbody>
</table>

### Product Analysis Has Begun

- **Alternate process paths triggered automatically when required**

### Product Analysis

- *Are you ready to report right now on whether the Product is vulnerable to issue described in Advisory?*
  - Yes
  - No

### Product Analysis

**Is Product vulnerable to issue described in Advisory? If no, must provide reason:**
- Yes, this product is vulnerable to this issue
- No, this product is not vulnerable to this issue

- **I am only affected due to a product that I bundle and will ONLY be publishing a Bundling Bulletin and do not need to provide a fix**

### Expedited Status

**Is this Product Record an Expedited Product Record? Only change this to OVERRIDE the Expedited status of the related Advisory.**
- Yes
- No

### Expedited Status

**Product Record Expedited Comments:**

- For each edit, add a new line at the top with a description of the edit. Don’t overwrite previous entries, just add a new top line.

If you are requesting a DIFFERENT Expedited Status for this Product Record than the Expedited Status for the related Advisory, PSIRT Operations must approve this request before the Product Record can proceed.

Similarly, if you are requesting a DIFFERENT Not-to-exceed Date for this Product Record than the Expedited Not-to-exceed Date for the related Advisory, PSIRT Operations must approve this request before the Product Record can proceed.
Built in compliance checking

Pull Scoring information directly from X-Force database
Appropriate Reviews are determined and requested by the tool.

Captures review history and plan modifications.
Reviewers can see comments left by previous reviewers.
Security Bulletin

Security Bulletin Plan

Will security bulletin be issued?  Planned Security Bulletin Publish Date
- Yes, a security bulletin will be issued  3/12/2016
- No, a security bulletin will not be issued

Will a vulnerability-specific Advisory Security Bulletin template be provided by PSIRT Ops?
- Yes
- No

Security Bulletin Content

Important! When you are ready to publish the Security Bulletin, BEFORE you do so, read all reviewer’s comments to check for necessary typo fixes or other important information. Reviewers may select “Review Completed” for the Security Bulletin even though typo fixes are needed before publication.

Relevant CVE Information:

CVEID: CVE-2016-0001
DESCRIPTION: description
CVSS Base Score: 5.7
CVSS Temporal Score: See url for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:L/AC:L/Au:S/C:P/I:C/A:P)

* This is a Bundling Bulletin.

* If you use DCF, draft your bulletin in DCF and put the DCF preview link here. You should ONLY use the editor below if you are NOT using DCF:

DCF preview link:

If you are NOT using DCF, then use the editor below to draft your Security Bulletin:

* Things marked in red are DCF fields where you would enter data
* Things marked in GREEN are where you would put your product unique data
Remains open until every task is complete
Team Performance – Overview of task status

- Brand Lead can see overall Brand performance
- Pillar Lead can see overall Pillar performance
Notices and Disclaimers

Copyright © 2016 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.
Notices and Disclaimers Con’t.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM’s products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services ®, Global Technology Services ®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli®, Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.
Thank You