

# Mature PSIRTs need Mature Tools (Part II)

Tania Ward

Dell EMC Product Security Office



# Once upon a time....

## A tool?

You may have handled these reports in email or even used a spreadsheet to handle and respond to the vulnerability reports



Path of progression



## Reassess. Define the future.

What did we want our process workflow to be.  
What behavior did we want to drive based on the data we were collecting.

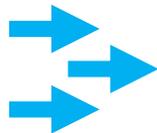


## Vulnerability Reports

Vulnerability Reports from third party researchers.  
Customer Support escalating vulnerability reports from customers.

# Drive product teams to self-management

**A PSIRT'S  
ABILITY TO FIX  
VULNERABILITIES**



**A PRODUCT TEAM'S  
ABILITY TO FIX  
VULNERABILITIES**



Enabling self management within the product team becomes necessary for success and scale.

Reassess. Define the future.



01

# Tracking Tool



# A tool to help scale out



- ..... **01** Vulnerability Response Champions
- ..... **02** Clear workflow. Expectations are set
- ..... **03** Response is in our name.
- ..... **04** Build agility through overrides.
- ..... **05** SDL Interlock

# Our process methodology



Third Party Component Monitoring

*High risk components / to be automated all products*



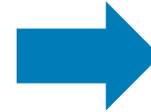
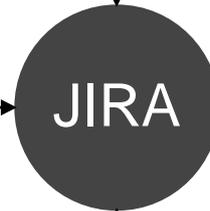
Customer Escalation Portal

*Service desk ->Triage*



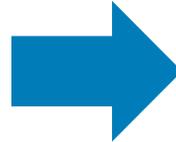
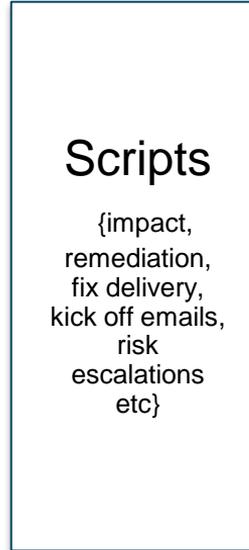
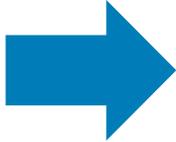
Others

*Manual*



# Our Jira Workflow

- High Profile
- Customer Support requests



Disclosure Release



Fix Delivery



Remediation Plan



Impact Statement

JIRA

We have the data. Let's visualize it



02

# Data Visualization Tools



# The dashboard. The lag.



Help product teams prioritize



Measure how proactive teams are in managing third party components



How am I doing overtime. Show progress.

# Example data - Open

## Vulnerability Response Status

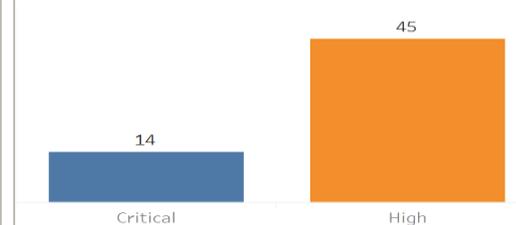
<b>Product Business Unit</b> (All) ▼	<b>Severity</b> (Multiple v... ▼)	<b>Status</b> (Multiple v... ▼)
<b>Type</b> (All) ▼	<b>Product Line</b> (All) ▼	

Product Line	Remedy in Progress	Remediation Plan Pending	Impact Statement Pending	Grand Total
Database-DDD	13			13
Storage_XX		1		1
STORAGE-YYY		1		1
Toys Division A	1			1
Toys Division C	1			1
Toys Division D	14	3		17
Web UI	20	4	1	25
<b>Grand Total</b>	<b>49</b>	<b>9</b>	<b>1</b>	<b>59</b>

### Vulnerability Response SLO Allocation



### Vulnerability by Severity



### Third Party Component Proactive Rate

15.6%

# Example data - Open

## Vulnerability Response Status

This dashboard displays all the open vulnerabilities that are being tracked by the PSRC. For definition of a vulnerability, see <https://productsecurity.emc.com/kb/resources/glossary.html#term-public-vulnerability>

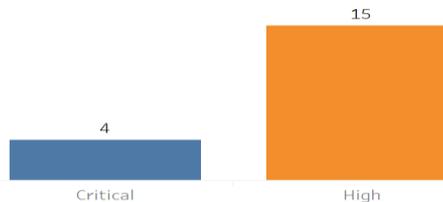
<b>Product Business Unit</b> Toys Division	<b>Severity</b> (Multiple v...)	<b>Status</b> (Multiple v...)
<b>Type</b> (All)	<b>Product Line</b> (All)	

Product Line	Remediation Plan Pending	Remedy in Progress	Grand Total
Toys Division A		1	1
Toys Division C		1	1
Toys Division D	3	14	17
<b>Grand Total</b>	<b>3</b>	<b>16</b>	<b>19</b>

### Vulnerability Response SLO Allocation



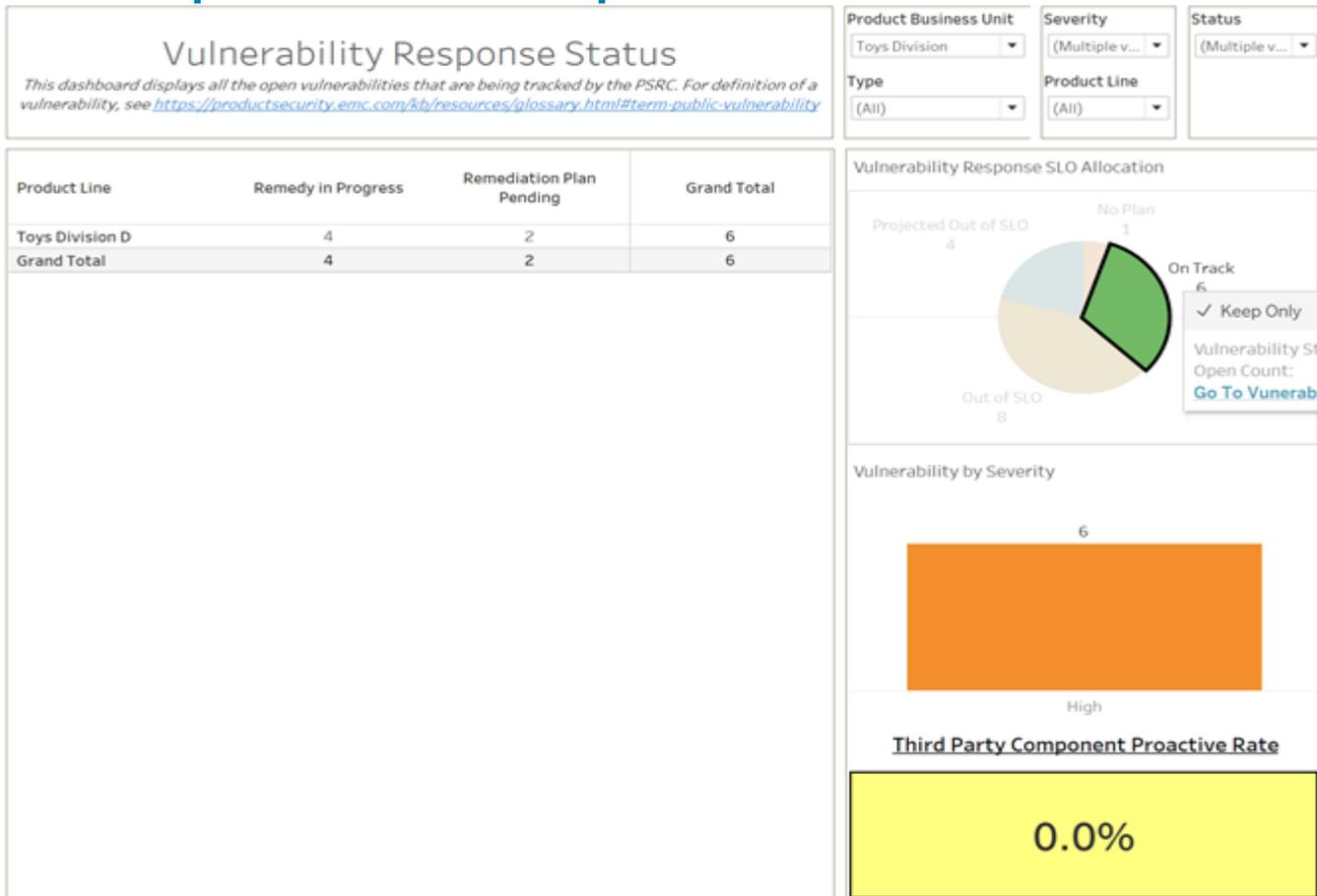
### Vulnerability by Severity



### Third Party Component Proactive Rate

7.7%

# Example data – Open details



# Example data – Open Details

## Vulnerability Response Detail

Provides a view on the actual details of the vulnerabilities based on the query selected in the Vulnerability Response Health Dashboard.

Key	Product Name	Reported Date	Target Remedy D..	SLO Remedy Due	
	Toys Division Authentica..	11/6/2017	2/28/2018	3/6/2018	114 Days Open
	Toys Division Missed pla..	1/3/2018	3/19/2018	3/19/2018	56 Days Open
	Toys Division Missed pla..	1/3/2018	3/16/2018	3/19/2018	56 Days Open
	Toys Division Identity G..	12/29/2017	4/15/2018	4/28/2018	61 Days Open
	Toys Division Identity G..	2/13/2018	TBD	5/14/2018	15 Days Open
	Toys Division Identity G..	2/13/2018	TBD	5/14/2018	15 Days Open

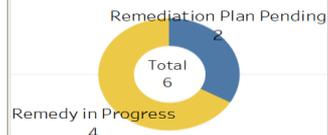
Key	Is Proactive?	Affected Version	Versions Fixed	Engineering Defect Num..	SLO Target (Days)	Remaining (Days)
	N/A	Toys Divisio..	TBD	TBD	90	75
	N/A	Toys Divisio..	TBD	TBD	90	75
	N/A	7.0.2 P4	7.1.0, 7...	ATM-83000	120	59
	No	TBD	Snacks 3..	TBD	75	19
	No	TBD	3.5.2.6.1	TBD	75	19
	N/A	Web IIS 7.1..	8.0.2	NA	20	6



### Vulnerability Response Allocation SLO Detail



### Vulnerability Response Status Allocation Detail



# Example data – Actual Remediation Rate

## Vulnerability Response Health

The Vulnerability Response Health Dashboard displays key metrics on how effective and proficient product teams are in handling and responding to public software vulnerability announcements.

Product Business Unit

(All)

Product Line

(All)

Type

(All)

Severity

(Multipl...)

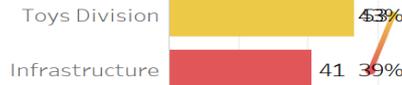
Date Remedy Due

Last 3 quarte...

Company Remediation Ra..

41.5%

### Product Business Unit



Product Name	# Total	# Within SLO	Remediation Rate	Avg Days to Remediate	Proficiency	Proactive Rate
STORAGE-YYY	2	1	50%	77		100%
Toys Division Validat..	1	0	0%	112		100%
Storage_XX	11	9	82%	44		91%
Toys Division Securit..	9	7	78%	43		89%
Database-Storage	13	0	0%	67		17%
Toys Division 3D Sec..	1	0	0%	49		0%
Toys Division A	6	2	33%	123		0%
Toys Division AcMiss..	3	1	33%	76		0%
Toys Division D	12	6	50%	64		0%
Toys Division Digital ..	2	0	0%	60		0%
Toys Division Federa						

### Quarter of Actual Remediation Rate Due

Product Business Unit	2017 Q3	2017 Q4	2018 Q1
Infrastructure	83%	7%	48%
Toys Division	43%	37%	55%
Grand Total	52%	24%	50%

### Culmulative Actual Remediation Rate

Product Business Unit	2017	2018
Infrastructure	30%	48%
Toys Division	40%	55%
Grand Total	37%	50%

# Example data – Actual Remediation Rate

## Vulnerability Response Health

The Vulnerability Response Health Dashboard displays key metrics on how effective and proficient product teams are in handling and responding to public software vulnerability announcements.

Product Business Unit

(All) ▼

Product Line

(All) ▼

Type

(All) ▼

Severity

(Multipl... ▼

Date Remedy Due

Last 3 quarte... ▼

Company Remediation Ra..

83.3%

Product Business Unit

Infrastructure  83%

Product Name	# Total	# Within SLO	Remediation Rate	Avg Days to Remediate	Proficiency	Proactive Rate
Storage_XX	4	3	75%	58		100%
STORAGE-YYY	1	1	100%	63		100%
Database-DDD Appli..	1	1	100%	19		
<b>Grand Total</b>	<b>6</b>	<b>5</b>	<b>83%</b>	<b>53</b>		<b>100%</b>

Quarter of Actual Remediation Rate Due

Product Business Unit

2017 Q3

2017 Q4

2018 Q1

Infrastructure	83%	7%	48%
Toys Division	43%	37%	55%
<b>Grand Total</b>	<b>52%</b>	<b>24%</b>	<b>50%</b>

Cumulative Actual Remediation Rate

Product Business Unit

2017

Infrastructure	83%
<b>Grand Total</b>	<b>83%</b>

# Example data – Actual Remediation Rate

## Vulnerability Response Health Details

Provides a view on the actual details of the vulnerabilities based on the query selected in the Vulnerability Response Status Dashboard.



Key	Product Name	Target Remedy Date	Reported Date	Closed Date	
	Storage_XX	4/13/2017	4/3/2017	4/11/2017	8 Days Open : Remedy Due: 7/2/2017
	Storage_XX	6/7/2017	4/25/2017	6/6/2017	42 Days Open : Remedy Due: 7/24/2017
	STORAGE-YYY	7/28/2017	5/29/2017	7/31/2017	63 Days Open : Remedy Due: 8/12/2017
	Storage_XX	10/5/2017	6/21/2017	10/4/2017	19 Days Open : Remedy Due: 8/8/2017
	Database-DD..	9/20/2017	7/19/2017	8/7/2017	78 Days Open : Remedy Due: 8/8/2017
	Storage_XX	9/8/2017	6/21/2017	9/7/2017	

### Remediation Allocation



Key	Affected Version	Versions Fixed	Engineering Defect Nu..	SLO Target (Days)	Days Actual to Remediate
	Storage_XX 2...	Hot fix (HF4..	TBD	90	82
	Current Release	Storage_XX..	TBD	90	48
	TBD	4.2 Patch	TBD	75	12
	TBD	2.4.1 and 2...	TBD	90	-15
	TBD	3.1	NA	20	1
	TBD	2.4.1 and 2...	TBD	90	12

### Remediation Allocation Detail



# Example data – Forecast Remediation Rate

## Vulnerability Response Health Forecast

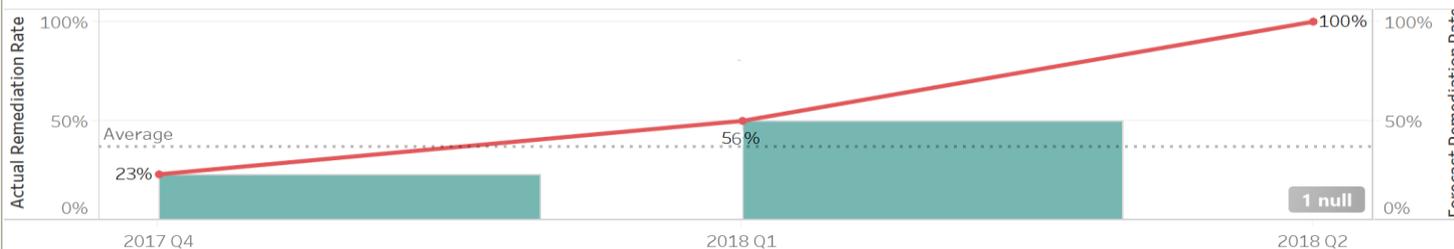
**Severity**

**Product Business Unit**

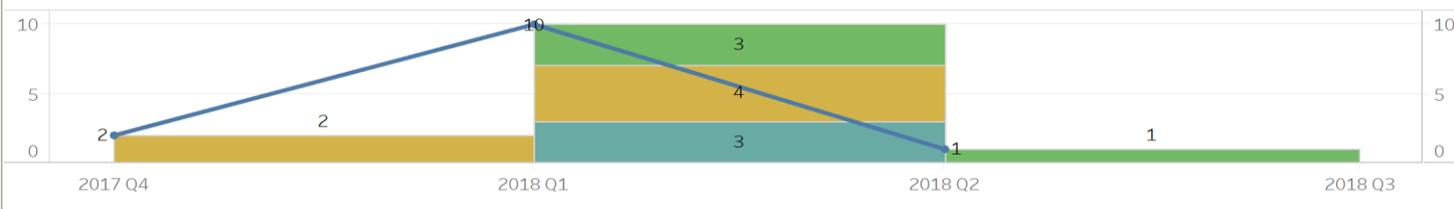
**Type**

**Product Line**

### Forecast Open Vulnerability Summary



### Open Vulnerabilities by Quarter Date Remedy Due



Key	Remedy Due	Vulnerability Status	Severity	Product Name	SLO Target (Days)	Remaining (Days)
	12/16/2017	Out of SLO	High	Toys D..	120	-77
	11/15/2017	Out of SLO	Critical	Toys D..	15	-108

Efficient. Measured.  
How effective?

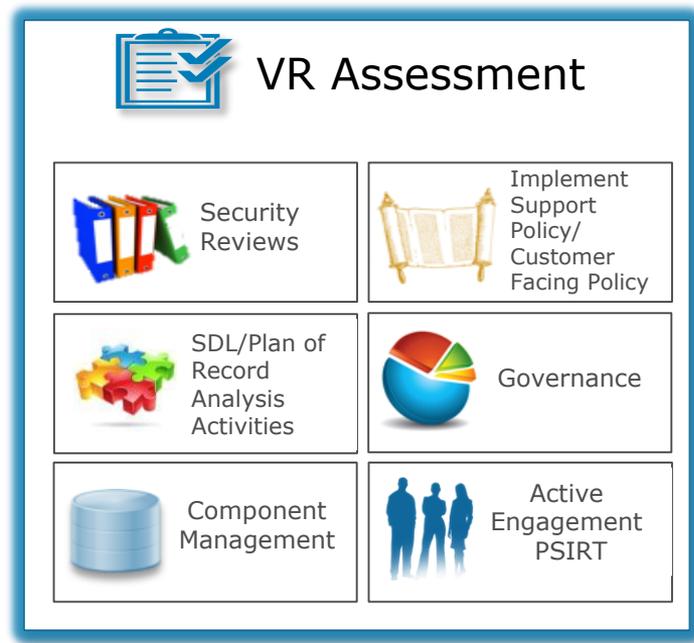
03

# Measure Maturity



# Vulnerability Response Assessment 1.0 - “Learning”

FIND YOUR EFFECTIVENESS  
UNDERSTAND THE CAUSES  
**USE THE INFORMATION**



# - Vulnerability Response Assessment

Vulnerability Response

Software Security

My Product Security > Active System Mgr - VR Summary > Active System Mgr - VR Assessment

Vulnerability Handling

Vulnerability Response

Governance

1. In the last 6 months, have any externally reported vulnerabilities on your product been closed as No Response?

Yes

No

2. When delivering security fixes for critical and high vulnerabilities (Dell EMC Product code/third party component), does your product:

Patch multiple supported product versions (N, N-1, N-2 etc)

Patch the latest supported product version (N)

Patch the current and immediately prior major release (N and N-1)

Patch plan varies - can be 1 or more of the above

3. Does your product ship with any third party components such as OpenSSL or Apache?

Yes

No

## Recommendations

### Vulnerability Handling

- Active engagement with PSRC
- Implement Dell EMC Support Policy

### Vulnerability Response

- Deliver Out of Band Patch (Dell EMC Proprietary Code)
- Publish Security Notifications

### Governance

- Manage Security Risk
- Adopt SDL Analysis Activities and have a SCG
- Perform Security Reviews

Preview

# - Vulnerability Response Assessment

Vulnerability Response

Software Security



My Product Security

Active System Mgr - VR Summary

Active System Mgr - VR Assessment

Vulnerability Handling

Vulnerability Response

Governance

1. Do you have the ability to release an out of band patch (Hotfix/Emergency Patch) for Dell EMC Proprietary Code vulnerabilities?

Yes

No

2. How do you disclose fixes (for Dell EMC Proprietary Code or Third Party Components) to your customers for vulnerabilities identified in your product?

Do not notify

Release Notes / Patch Notes

Release or Patch Notes and ESA

Security Advisory

## Recommendations

### Vulnerability Handling

- Active engagement with PSRC
- Implement Dell EMC Support Policy

### Vulnerability Response

- Third Party Component update strategy
- Publish Security Notifications

### Governance

- Manage Security Risk
- Adopt SDL Analysis Activities and have a SCG
- Perform Security Reviews

Preview

# Active System Mgr - Vulnerability Response Assessment

Vulnerability Response

Software Security



My Product Security

Active System Mgr - VR Summary

Active System Mgr - VR Assessment

Vulnerability Handling

Vulnerability Response

Governance

1. In the last 24 months, has your product shipped with any outstanding critical or high severity Dell EMC Proprietary code vulnerabilities that were not remediated within 6 months from the GA date?

Yes

No

2. Do you adopt the [Security Development Lifecycle Analysis Activities](#) and have a [Security Configuration Guide](#) (see Recommendations)?

Full Adoption

Partial Adoption

No Adoption

3. Are your active externally reported security vulnerabilities reviewed by senior management at least once a quarter? Common examples of review forums include TCE, BMT and PMT.

Yes

No

## Recommendations

### Vulnerability Handling

- [Active engagement with PSRC](#)
- [Implement Dell EMC Support Policy](#)

### Vulnerability Response

- [Third Party Component update strategy](#)
- [Publish Security Notifications](#)

### Governance

- [Manage Security Risk](#)
- [Adopt SDL Analysis Activities and have a SCG](#)
- [Perform Security Reviews](#)

Preview



## Your VR Assessment proficiency is at 83%

Your product team is moderately proficient in performing all the required activities to handle and respond to public vulnerabilities. Recommendations on how to improve your proficiency in specific areas can be found in the Recommendations Section.

Category	Grade	Recommendations
<b>Vulnerability Handling</b> Demonstrates how proficient your team is at handling public vulnerabilities.	A	No guidance necessary. Keep up the good work!
<b>Vulnerability Response</b> Provides insight into how well your team is at responding to these public vulnerabilities whether by providing a fix or the appropriate communication deliverables.	B	<ul style="list-style-type: none"><li>◦ <a href="#">Publish Security Notifications</a></li></ul>
<b>Governance</b> Provides an overview of how proficient your team is at managing the risk that comes with handling and responding to public vulnerabilities.	C	<ul style="list-style-type: none"><li>◦ <a href="#">Adopt SDL Analysis Activities and have a SCG</a></li></ul>

[Update](#)[Delete](#)[Show History](#)

In conclusion..

# Recap

“Simple can be harder than complex: You have to work hard to get your thinking clean to make it simple. But it’s worth it in the end because once you get there, you can move mountains.” – Steve Jobs



Tracking Tool. Define the future.



Measure efficiency. Bad or Good. It’s the landscape.



Measure effectiveness. Our maturity model.



Keep process & tools simple.

To be continued...

**D**  **LEMC**