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.

Vulnerability Reports

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

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.
Enabling self management within the product team becomes necessary for success and scale.
Reassess. Define the future.
Tracking Tool
A tool to help scale out

1. Vulnerability Response Champions
2. Clear workflow. Expectations are set
3. Response is in our name.
4. Build agility through overrides.
5. SDL Interlock
Our process methodology

Third Party Component Monitoring

Customer Escalation Portal

Others

High risk components / to be automated all products

Service desk -> Triage

Manual

JIRA

Workflow
Our Jira Workflow

- High Profile
- Customer Support requests

Scripts

- {impact, remediation, fix delivery, kick off emails, risk escalations etc}

- Disclosure Release
- Fix Delivery
- Remediation Plan
- Impact Statement

JIRA
We have the data. Let’s visualize it
02 Data Visualization Tools

Reports
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

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

### Vulnerability Response SLO Allocation

- **Projected Out of SLO**: 4
- **No Plan**: 5
- **On Track**: 19
- **Out of SLO**: 31

### Vulnerability by Severity

- **Critical**: 14
- **High**: 45

### Third Party Component Proactive Rate

15.6%
## 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](https://productsecurity.emc.com/kb/resources/glossary.html#term-public-vulnerability)

<table>
<thead>
<tr>
<th>Product Line</th>
<th>Remediation Plan Pending</th>
<th>Remedy in Progress</th>
<th>Grand Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toys Division A</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Toys Division C</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toys Division D</td>
<td>3</td>
<td>14</td>
<td>17</td>
</tr>
<tr>
<td>Grand Total</td>
<td>3</td>
<td>16</td>
<td>19</td>
</tr>
</tbody>
</table>

### Vulnerability Response SLO Allocation

- **Projected Out of SLO**: 4
- **No Plan**: 1
- **On Track**: 6
- **Out of SLO**: 8

### Vulnerability by Severity

- **Critical**: 4
- **High**: 15

**Third Party Component Proactive Rate**

7.7%
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

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Reported Date</th>
<th>Target Remedy Due</th>
<th>SLO Remedy Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toys Division Authentica</td>
<td>11/6/2017</td>
<td>3/6/2018</td>
<td>114 Days Open</td>
</tr>
<tr>
<td>Toys Division Missed pla...</td>
<td>3/19/2018</td>
<td>3/19/2018</td>
<td>56 Days Open</td>
</tr>
<tr>
<td>Toys Division Missed pla...</td>
<td>3/19/2018</td>
<td>3/19/2018</td>
<td>56 Days Open</td>
</tr>
<tr>
<td>Toys Division Identity G...</td>
<td>2/13/2018</td>
<td>5/14/2018</td>
<td>63 Days Open</td>
</tr>
<tr>
<td>Toys Division Identity G...</td>
<td>2/13/2018</td>
<td>TBD</td>
<td>1 Days Open</td>
</tr>
</tbody>
</table>

### Vulnerability Response Status Allocation Detail

<table>
<thead>
<tr>
<th>Key</th>
<th>Is Proactive?</th>
<th>Affected Version</th>
<th>Versions Fixed</th>
<th>Engineering Defect Num.</th>
<th>SLO Target (Days)</th>
<th>Remaining (Days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Toys Division</td>
<td>TBD</td>
<td>TBD</td>
<td>A</td>
<td>90</td>
<td>75</td>
</tr>
<tr>
<td>N/A</td>
<td>Toys Division</td>
<td>TBD</td>
<td>TBD</td>
<td>J</td>
<td>90</td>
<td>75</td>
</tr>
<tr>
<td>N/A</td>
<td>7.0.2 P4</td>
<td>7.1.0, 7... ATM-83000</td>
<td>...</td>
<td>100</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>TBD</td>
<td>Snacks 3.. TBD</td>
<td>H.</td>
<td>75</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>TBD</td>
<td>3.5.2.6.1 TBD</td>
<td>C.</td>
<td>75</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>Web IIS 7.1...</td>
<td>8.0.2 NA</td>
<td>S.</td>
<td>20</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

#### Vulnerability Response Allocation SLO Detail

- On Track: 6
- Remediation Plan Pending: 2
- Remedy in Progress: 4
- Total: 6
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**
  - Toys Division: 43%
  - Infrastructure: 41%

- **Product Name**
  - STORAGE YYY: 2, # Within SLO: 1, Remediation Rate: 50%, Avg Days to Remediate: 77
  - Toys Division Validat..: 1, 0%
  - Storage_XX: 11, 9, 82%
  - Toys Division Securit..: 9, 7, 78%
  - Database-Storage: 13, 0, 82%
  - Toys Division 3D Sec..: 1, 0, 0%
  - Toys Division A: 6, 2, 33%
  - Toys Division AcMiss..: 3, 1, 33%
  - Toys Division D: 12, 6, 50%
  - Toys Division Digital ..: 2, 0, 0%
  - Toys Division Feder..: 1, 0, 0%

- **Quarter of Actual Remediation Rate Due**
  - 2017 Q3: Infrastructure 83%, Toys Division 43%
  - 2017 Q4: Infrastructure 7%, Toys Division 37%
  - 2018 Q1: Infrastructure 48%, Toys Division 55%

- **Culminative Actual Remediation Rate**
  - 2017: Infrastructure 30%, Toys Division 40%
  - 2018: Infrastructure 48%, Toys Division 55%
**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

<table>
<thead>
<tr>
<th>Product Name</th>
<th># Total</th>
<th># Within SLO</th>
<th>Remediation Rate</th>
<th>Avg Days to Remediate</th>
<th>Proficiency</th>
<th>Proactive Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage XX</td>
<td>4</td>
<td>3</td>
<td>75%</td>
<td>58</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>STORAGE-YYY</td>
<td>1</td>
<td>1</td>
<td>100%</td>
<td>63</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Database-DDD Appli..</td>
<td>1</td>
<td>1</td>
<td>100%</td>
<td>19</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td><strong>6</strong></td>
<td><strong>5</strong></td>
<td><strong>83%</strong></td>
<td><strong>53</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

#### Quarter of Actual Remediation Rate Due

<table>
<thead>
<tr>
<th>Product Business Unit</th>
<th>2017 Q3</th>
<th>2017 Q4</th>
<th>2018 Q1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td>83%</td>
<td>7%</td>
<td>46%</td>
</tr>
<tr>
<td>Toys Division</td>
<td>43%</td>
<td>37%</td>
<td>55%</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td>52%</td>
<td>24%</td>
<td>50%</td>
</tr>
</tbody>
</table>

#### Culmulative Actual Remediation Rate

<table>
<thead>
<tr>
<th>Product Business Unit</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td>83%</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td>83%</td>
</tr>
</tbody>
</table>
Example data – Actual Remediation Rate
Example data – Forecast Remediation Rate
Efficient. Measured. How effective?
03 Measure Maturity

What do I need to do?
FIND YOUR EFFECTIVENESS
UNDERSTAND THE CAUSES
USE THE INFORMATION
- Vulnerability Response Assessment

Vulnerability Handling

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
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
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.

<table>
<thead>
<tr>
<th>Category</th>
<th>Grade</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Handling</strong></td>
<td>A</td>
<td>No guidance necessary. Keep up the good work!</td>
</tr>
<tr>
<td>Demonstrates how proficient your team is at handling public vulnerabilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Vulnerability Response</strong></td>
<td>B</td>
<td>Publish Security Notifications</td>
</tr>
<tr>
<td>Provides insight into how well your team is at responding to these public vulnerabilities whether by providing a fix or the appropriate communication deliverables.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>C</td>
<td>Adopt SDL Analysis Activities and have a SCG</td>
</tr>
<tr>
<td>Provides an overview of how proficient your team is at managing the risk that comes with handling and responding to public vulnerabilities.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In conclusion..
Recap

Tracking Tool. Define the future.

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

Measure effectiveness. Our maturity model.

Keep process & tools simple.

“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
To be continued...