



# Building and Maturing your PSIRT

Lessons Learned from the trenches

Hello there!

Lisa Bradley, NVIDIA



CRob, Red Hat

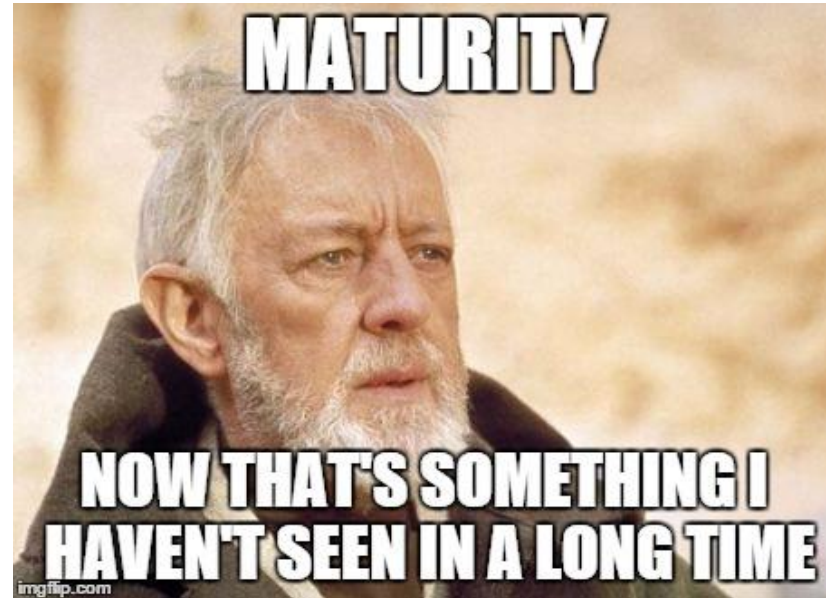




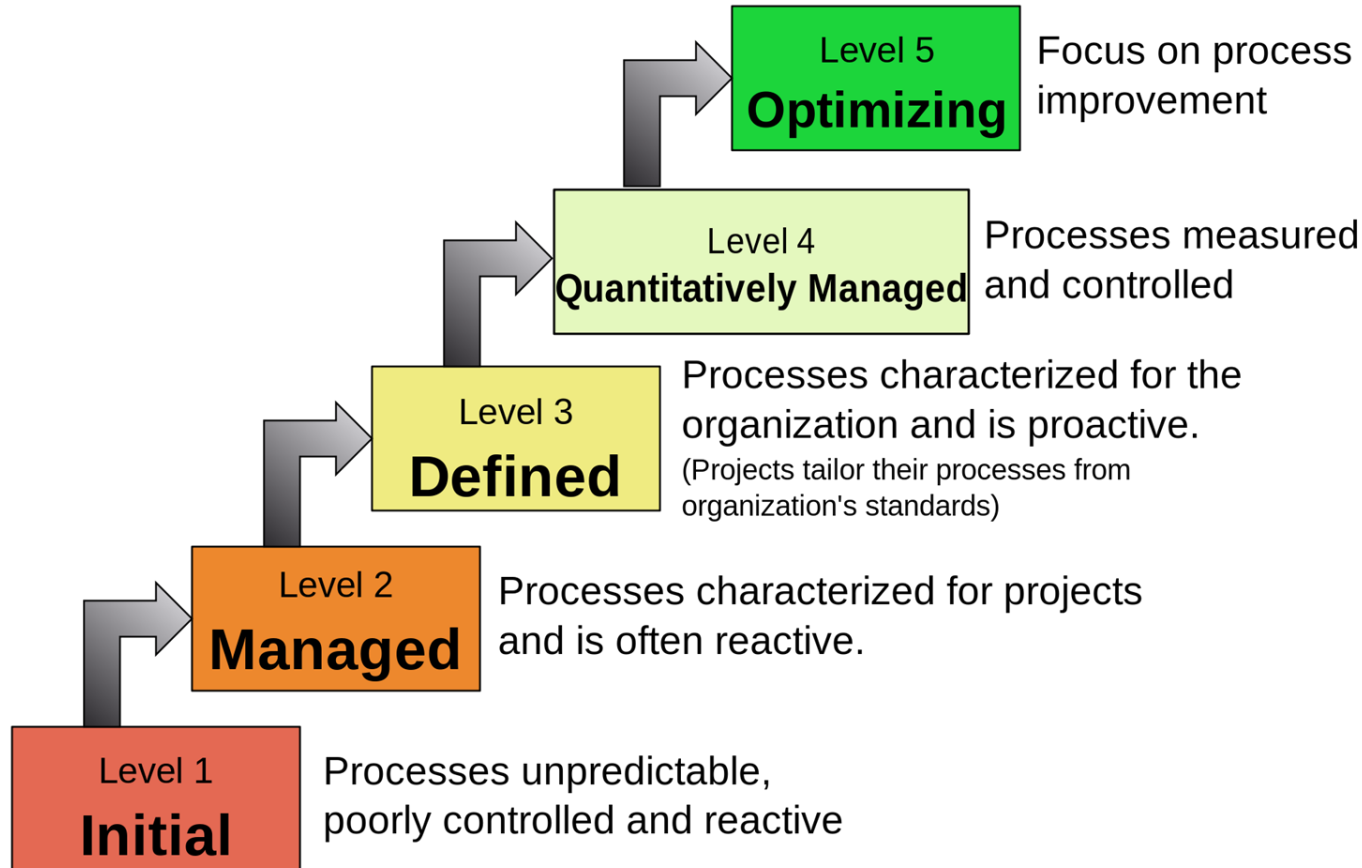
## Agenda

Hi. We're Lisa and CRob, and we're here to talk to you about stuff and things.....

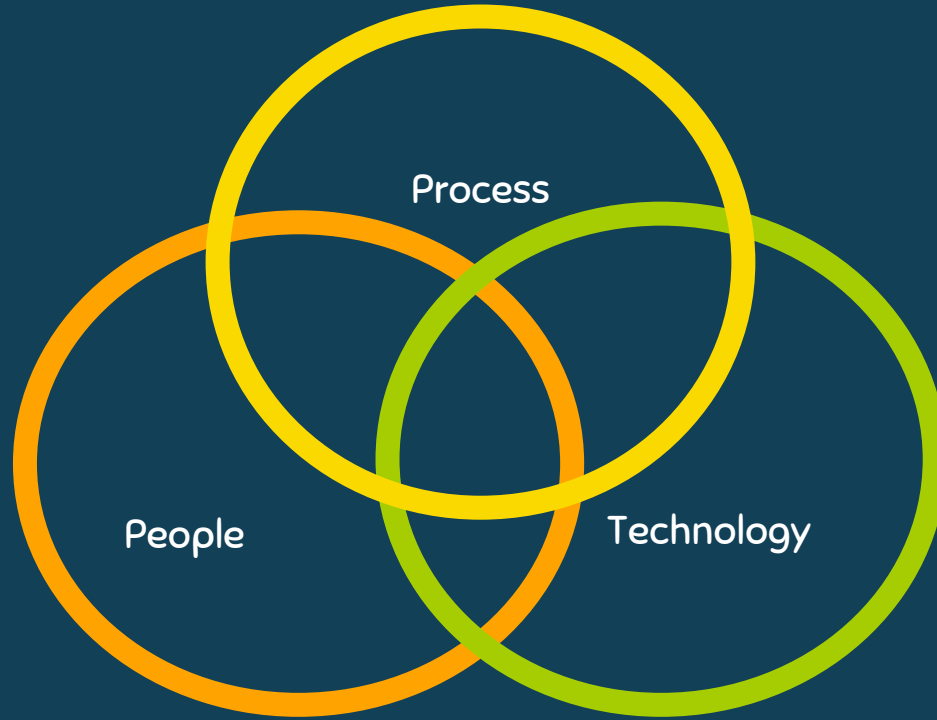
- Characteristics of the Maturity Model
- Novice PSIRT
- Advanced PSIRT
- Expert PSIRT



# Characteristics of the Maturity levels



What will make you better is NOT new news

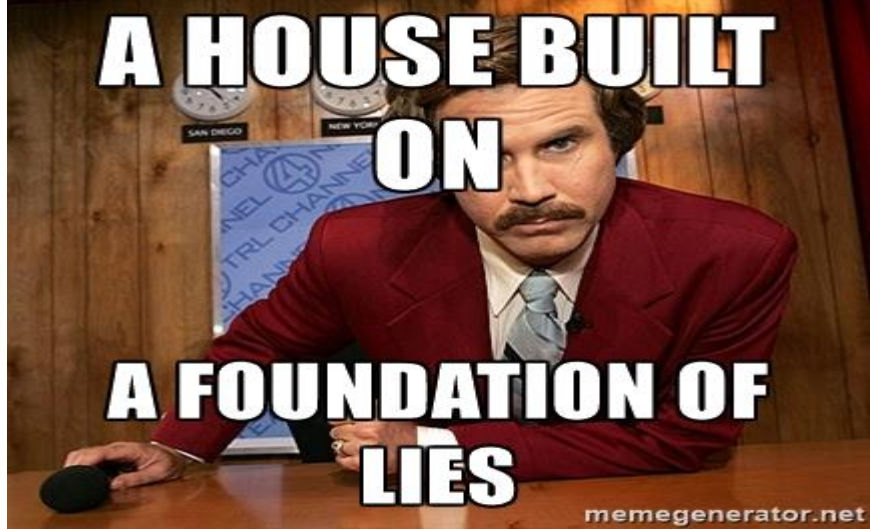


# 1

Level 1

**Initial**

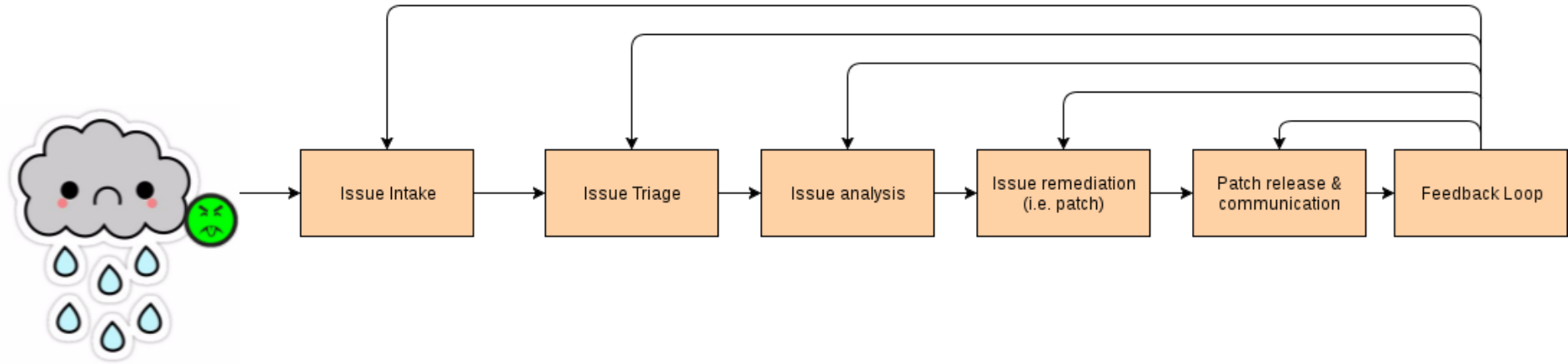
Processes unpredictable,  
poorly controlled and reactive



## Novice

Let's start with the beginning

## A High-level PSIRT process overview



# Executive and Organizational Support

The single most important thing a PSIRT needs is executive leadership buy-in and support. Without it, PSIRT will not be able to be effective in fulfilling its role.





## Using industry standards

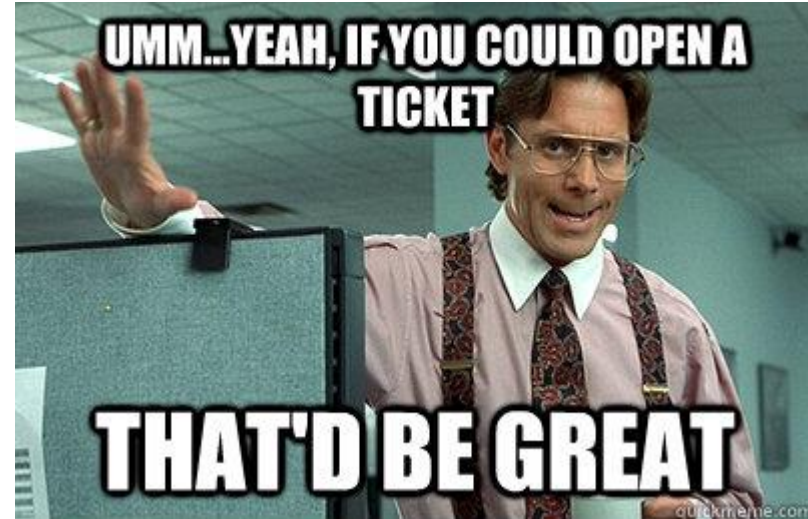
Tools like CVE, CWE, CVSS, etc. are the common language that spans Products and Technologies and allows different organizations to understand



# Ticketing/Tracking

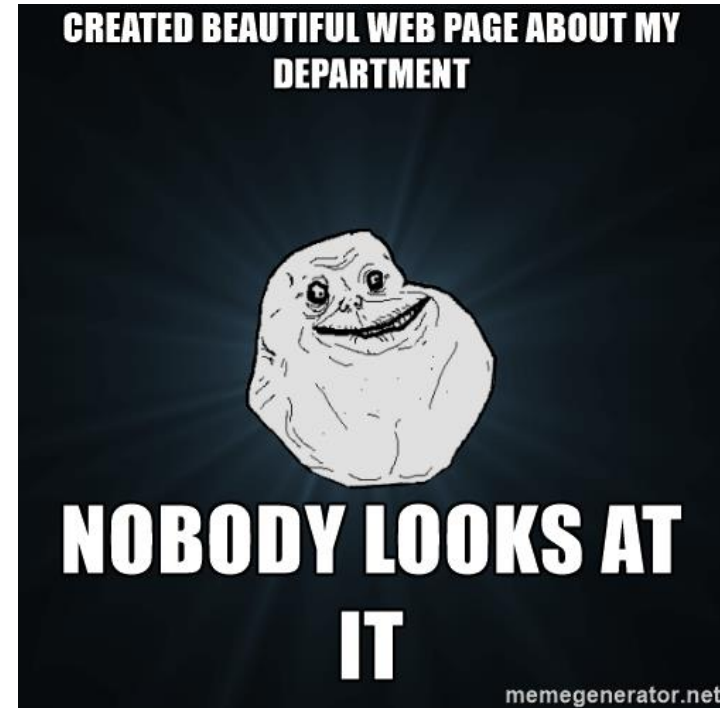
Core to PSIRT operations, making the right choices up front will drive your process/workflow down the road.... Choose wisely

Can you leverage an existing bug system?



# External Product Security Page

Customers and partners should have a simple way to see your processes/policies and be able to contact you.



# 2-3

Level 2

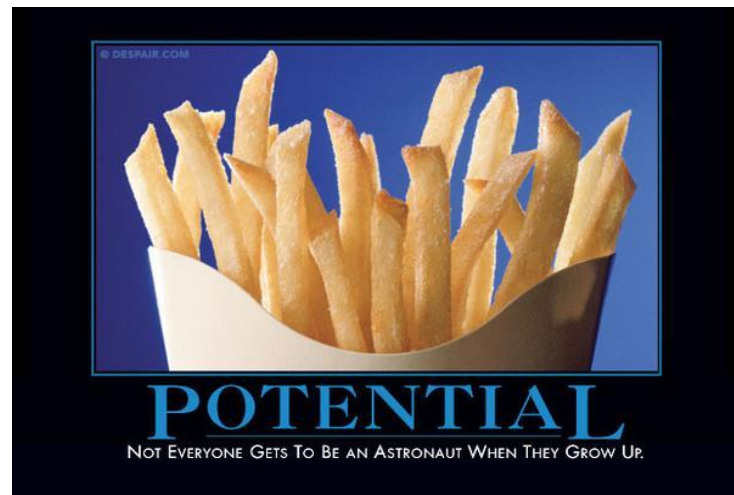
**Managed**

Processes characterized for projects and is often reactive.

Level 3

**Defined**

Processes characterized for the organization and is proactive.  
(Projects tailor their processes from organization's standards)



## Advanced

Moving up the maturity scale

## Maturity Improvement

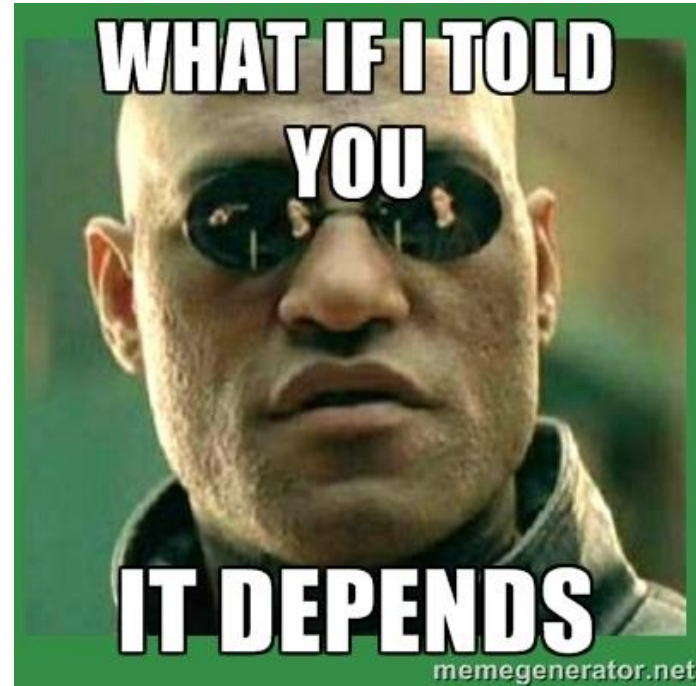
What do we want to be when we grow ?

- Once the basics are put into place and running smoothly, you'll start thinking about how to improve things....



## Dealing with 3rd party reporters

Odds are someone that isn't you will find flaws in your products...how are you going to work with them?



# Extending your team – Security Champions

- Helps lead security activities
- Develops security strategies and processes
- Helps to evaluate issues
- Reviews exceptions to policies
- Scores vulnerabilities
- Proactively monitors security





# Policies and Lifecycles

It's important to have

- Branch/Version Support Policies
- Date Policy - Delivery SLA
- Exception process
- Lifecycles

Documented for customers and employees

In the middle of one isn't the best time to figure that out





# Metrics

## Active reporting:

- Count by BU and source
- Aging for each BU

## Fixed issues reporting:

- Count by source
- Time to fix by source and BU

## Other:

- Exception stats
- CWE for fixed issues

Consider audience for your metrics



# Embargos

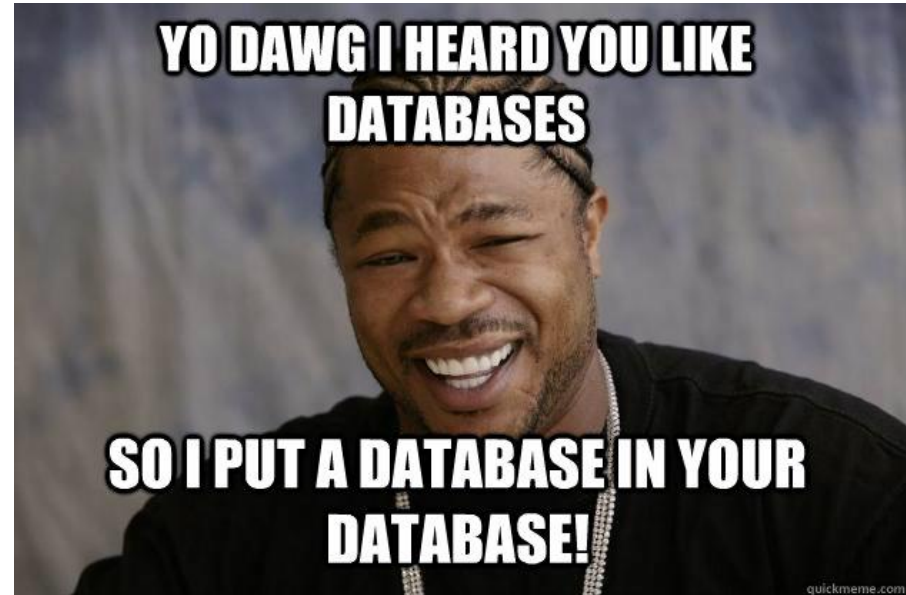
Sometimes issues need to/are asked to be kept secret. How will you deal with it?

Is it in the best interest to the customer?



# Product Registry

- Name and alias names
- What are you?
- Functional BU
- More info:
  - Product lifecycle
  - Supported versions
  - Release schedule
  - Partners
  - Download page
  - OSS dependencies



# 4-5

Level 4 <b>Quantitatively Managed</b>	Processes measured and controlled
Level 5 <b>Optimizing</b>	Focus on process improvement



## Expert

It really is all flying cars and silver spacesuits...

## The Future of PSIRTs

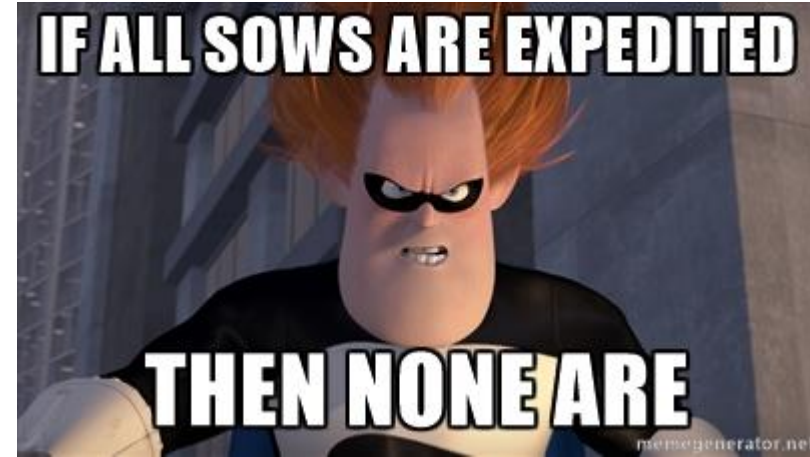
So you've got a PSIRT, and you've got some process and tooling, you're doing some stuff....what next?



# Advanced process and policies

## Expedited Process

- Whatever you call it, High Touch, Media events, Branded flaw, Expedited, yada yada... what do you plan to DO about it WHEN it happens?



# Dependency Management

Do you really KNOW what's inside your products?

- How are you tracking what your devs are “baking in”?
- What will you do when THEIR stuff breaks?

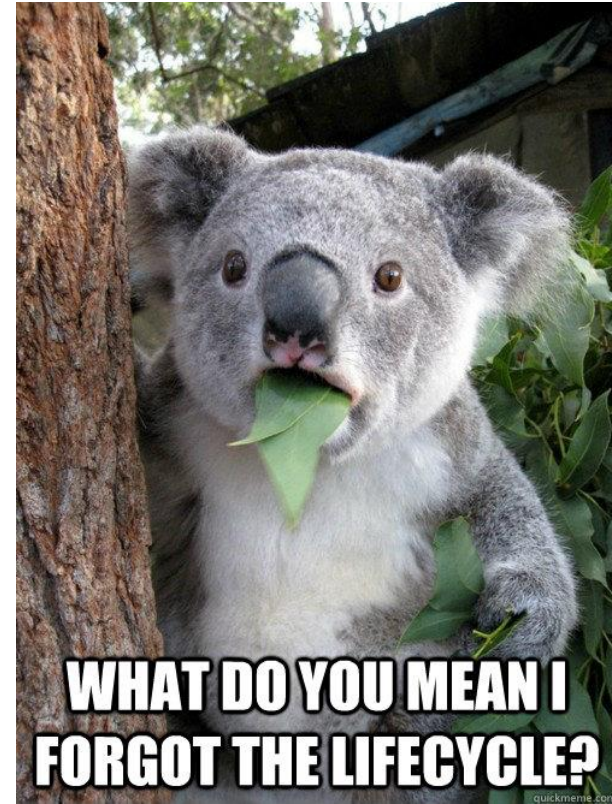




# End-of-Lifecycle

Is it really a lifecycle if nothing ever dies?

- Know thy Customers
- **DON'T LET SALES DEFINE YOUR LIFECYCLE!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!**
- How are products EoL communicated?
- Do you use a Phased approach?
- When the lifecycle changes, what are you going to do? Can it change?
- How are you managing “bundled” products?





# Bug Bounties

This is a thing that exists.  
You may or may not elect to participate.

- You will be contacted by people brokering vulns. What will you do?
- B.B.'s do offer private services.



# Advanced Risk Management

Using methods like STRIDE, threat modeling, risks matrixes, Options & Impacts, or others can help the PSIRT convey the level of Risk the organization is facing.

Once you get here, think about determining the costs of vulnerabilities & vuln mgmt.

5		1			2, 4
4			Current level of Product Risk		
3			5		
2		3		6	
1					
	1	2	3	4	5

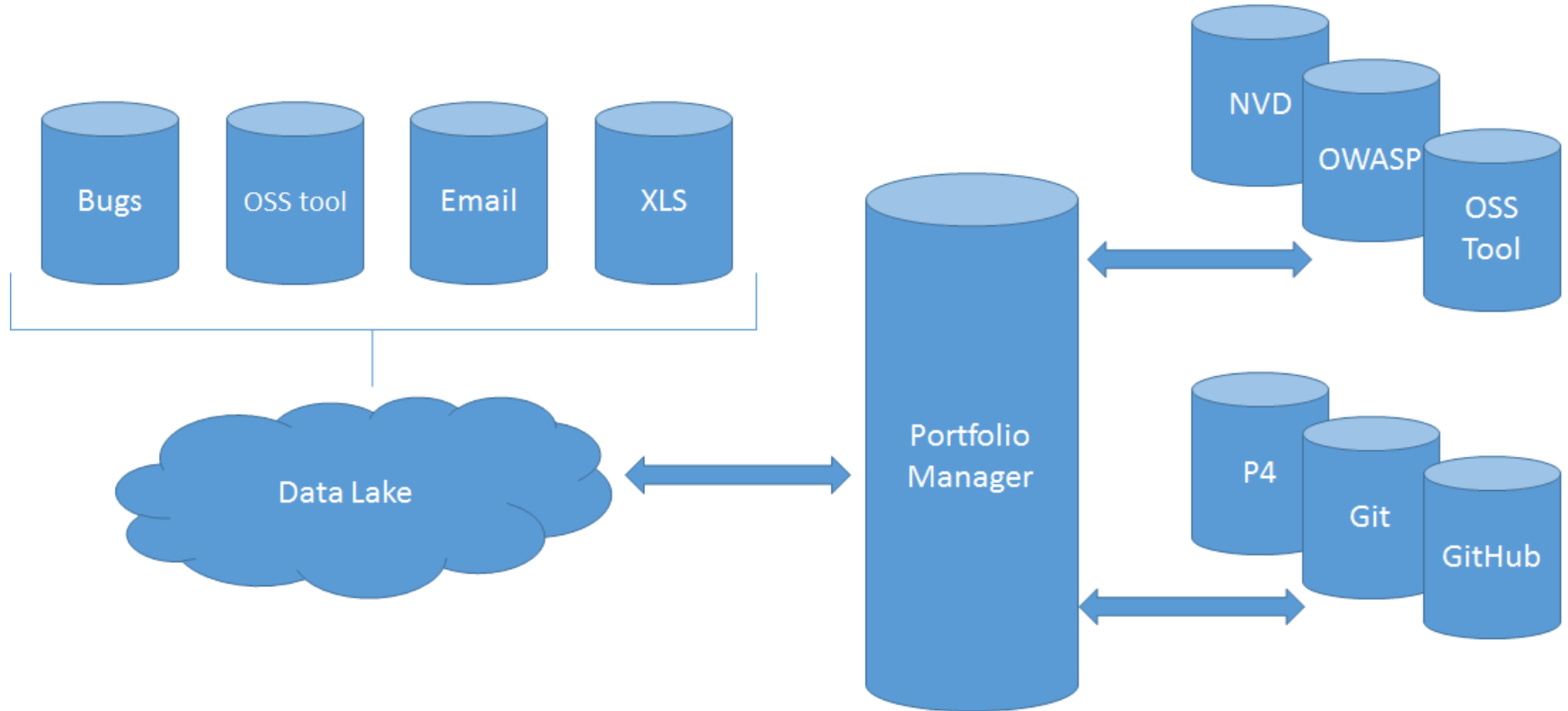
<b>Risk Categorization Values</b>					
<b>Category</b>	5	4	3	2	1
	100-81	80-61	60-41	40-21	20-0
<b>Likelihood</b>	Very likely to Virtually Certain	Quite Possible to Very Likely	Somewhat Possible to Quite Possible	Remotely Possible to Somewhat Possible	Very Unlikely (practically impossible) to Remotely Possible
<b>Impact</b>	(extremely material) to Extraordinary (survival is threatened)	Serious (very material) to Pervasive (extremely material)	Important (material) to Serious (very material)	Small (immaterial) to Important (Material)	Very Small (inconsequential) to Small (immaterial)
<b>RA Values L/I</b>					
5/5, 5/4, 5/3, 4/3, 5/2, 4/4, 4/5, 3/5, 3/4, 2/5	<b>Risk Assessment Scale</b>  High Risk: The loss of confidentiality, integrity, or availability, could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.  Moderate Risk: the loss of CIA could be expected to have a serious adverse effect on organization operations, org assets, or individuals  Low Risk: the loss of CIA could be expected to have a limited adverse effect on organization operations, org assets, or individuals.				
5/1, 4/1, 4/2, 3/3, 3/2, 1/5					
1/4, 2/4, 2/3					
2/2, 1/2, 2/1, 1/1					

# Advanced Tooling

- PSIRT Tool
- Scoring Tool
- Feeding reporting/CWEs - feedback into Secure Engineering
- Monitoring feeds and external sites - automatically pulling data from upstream sources to auto-generate a ticket (Dependency Tracking)



# Portfolio Management System



## To Summarize

**Back to Basics...**  
Do this and that

**Walk, then Crawl**  
Do that and this

**Flying Cars**  
MOAR Awesomeness

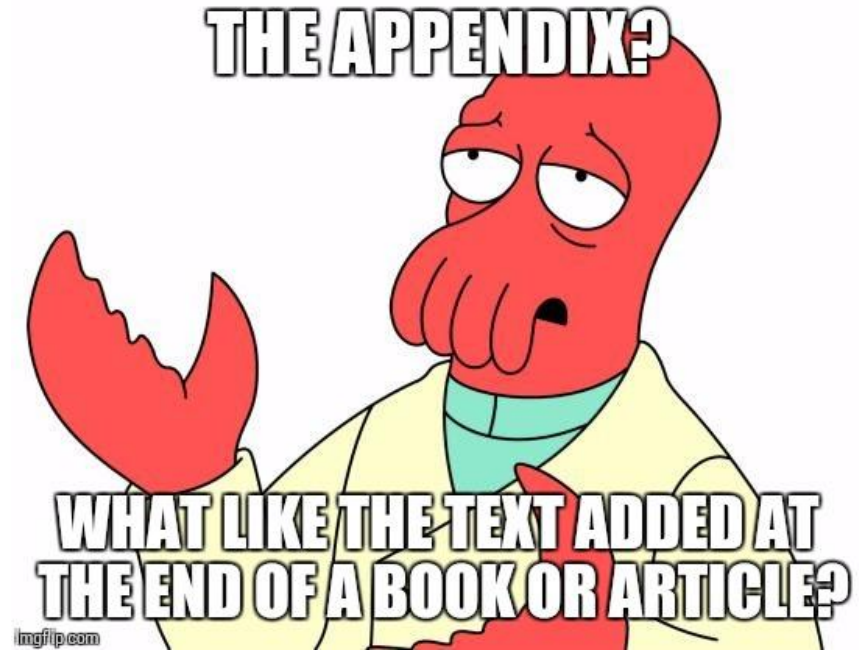


**THANKS!**

# Any questions?

You can find us at

[www.linkedin.com/in/lisambradley](http://www.linkedin.com/in/lisambradley) and [Lisa @ nvidia.com](mailto:Lisa@nvidia.com)  
[@RedHatCRob](mailto:@RedHatCRob) and [CRob @ RedHat.com](mailto:CRob@RedHat.com)



# Appendix

Level 1

**Initial**

Processes unpredictable,  
poorly controlled and reactive

Defining PSIRT Process, Steps

Email/submit/basic ticketing

Define Severity CVSS

CVE/CVSS industry standards

External Product Security Page

External Communication/Disclosure

Templates for Communication

Executive Support



Level 2

## **Managed**

Processes characterized for projects and is often reactive.

Dealing with 3rd party reporters

Cross organization support - Security Champions

Branch/Version Support Policies

Date Policy - Delivery SLA

Exception process

Lifecycles

Baseline Metrics

Embargo

Product Registry

Educating

Level 3

## Defined

Processes characterized for the organization and is proactive.

(Projects tailor their processes from organization's standards)

Community internal support - helping each other

External Groups FIRST

Alignment of security fixes for all versions/products

Enhanced Severity definitions

Integrating into SDLC

PSIRT Operations - having a real team

Level 4

**Quantitatively Managed**

Processes measured  
and controlled

Expedited Process

OSS tooling

Dependency Management

Risk Management

Determine cost of vulnerability management

Operational, trends, broad level Metrics

Fully established Lifecycle

PSIRT Tool and Scoring Tool

Feeding reporting/CWEs - feedback into Secure Engineering (RCCA)

Monitoring feeds and external sites - automatically pulling data to auto-generate a ticket

Level 5

## **Optimizing**

Focus on process  
improvement

Bug bounties - reaching to find issue