
black hat
USA 2018
AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS
STOP THAT RELEASE,
THERE'S A VULNERABILITY!
#BHUSA / @BLACK HAT EVENTS

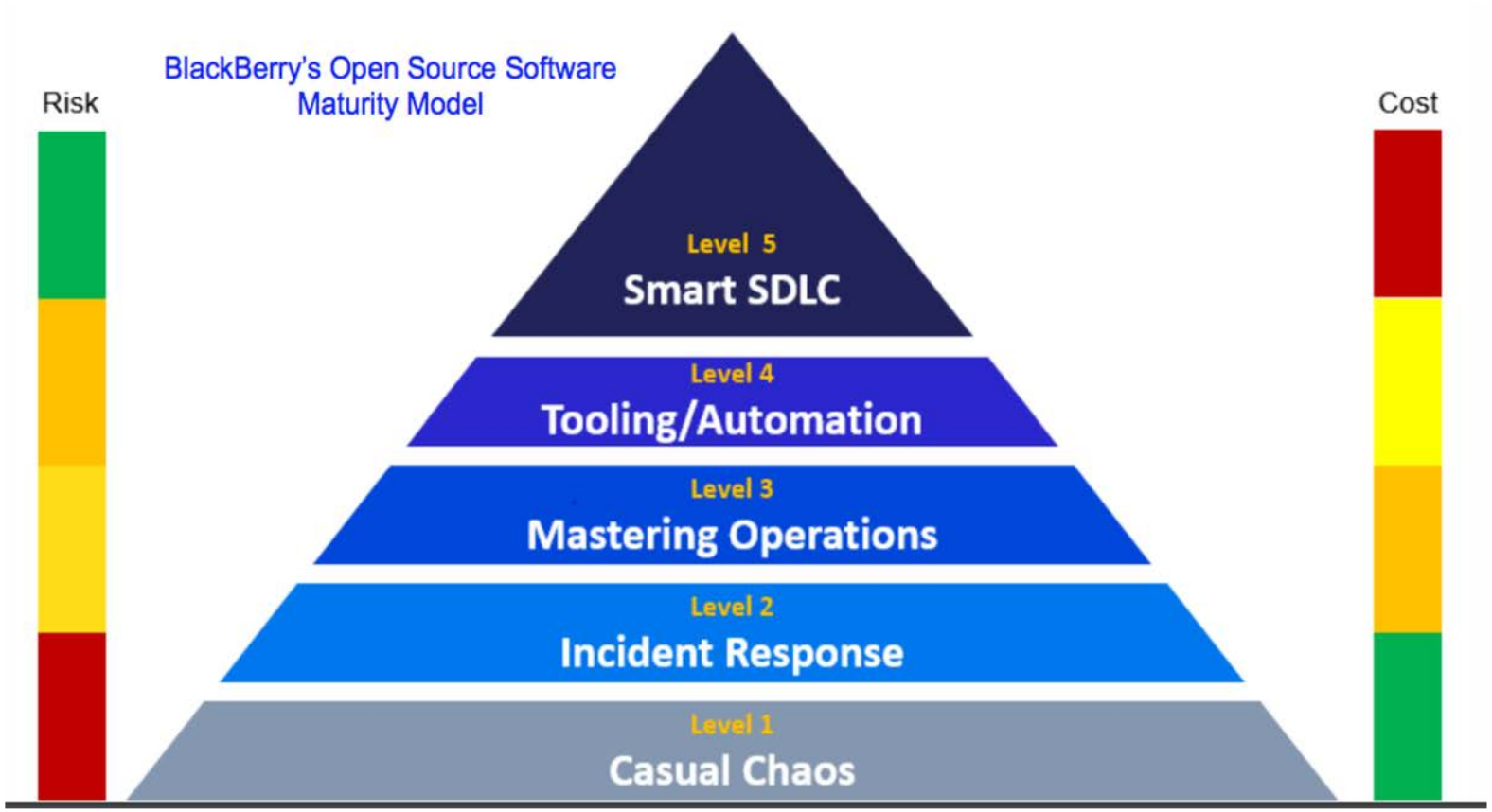
Christine Gadsby
Director - Product Security Operations

Simran Sidhu
Social Media Specialist

Diahann Gooden
Senior Operations Program Manager

Tyler Townes
Manager – Product Security Response


black hat
USA 2016


BlackBerry's Open Source Software Maturity Model
Risk
Cost
Level 5
Smart SDLC
Level 4
Tooling/Automation
Level 3
Mastering Operations
Level 2
Incident Response
Level 1
Casual Chaos

Meet Lucy the Whoodle

- Service for Dog Autism

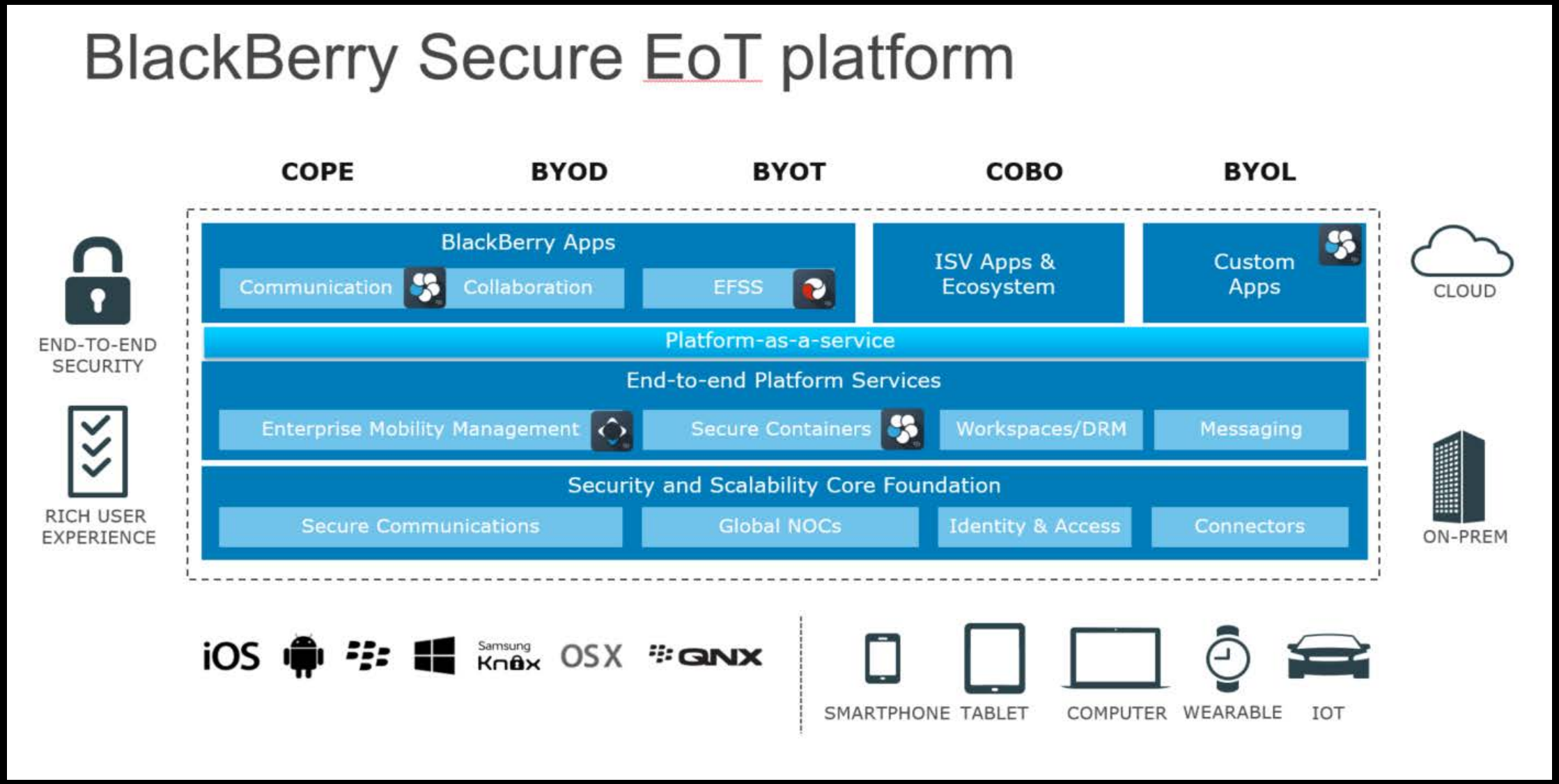
Lucy needs maintenance

Why are software releases important?

You are either here.....

OR you are here.....

Why is this important to BlackBerry?



Enterprise-scale
Vulnerability Management

- 100s products to manage
- 100s of sources of threat intel
- 1000s of vulnerabilities to investigate
- ..and many strained relationships

BlackBerry® Secure™

SDLC – Bringing a secure product to market

What DEV teams think .....

What Product and Software Security Does .....

That's it, right?.

It's Launch Day, YAY!

AND then....
Open hunting season begins

What should we be doing?

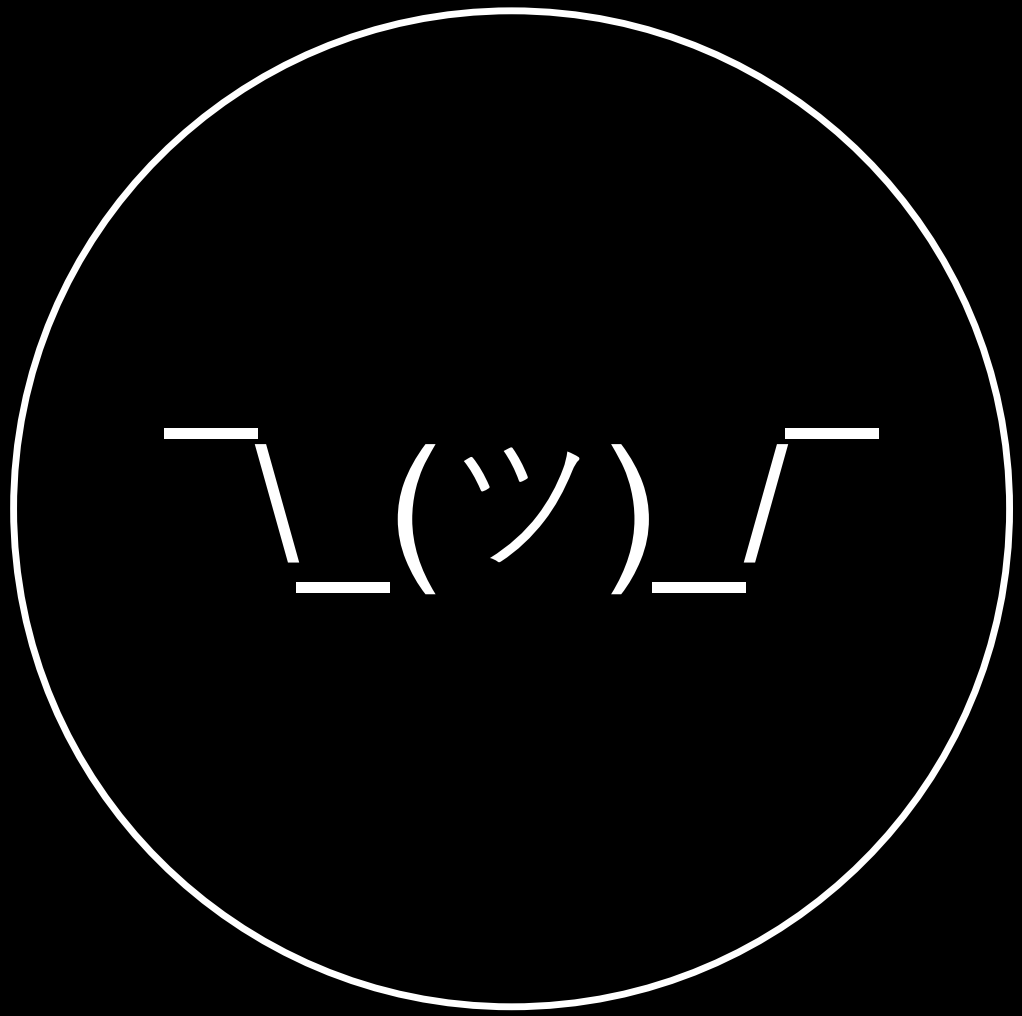
Software Readiness Review Program

Adding security review to release criteria

- Mitigating risk on behalf of your customers
- Multiple software versions of the same product are in market concurrently
- Know the security posture of your products
- Customers don't like upgrading! It's expensive and time consuming and is often a double-edged sword
- **Ensure you have a ship vehicle for all your patches!**

A FIX IN THE BUILD IS BETTER THAN TWO IN THE REPOSITORY!!!!!!!

So now what?

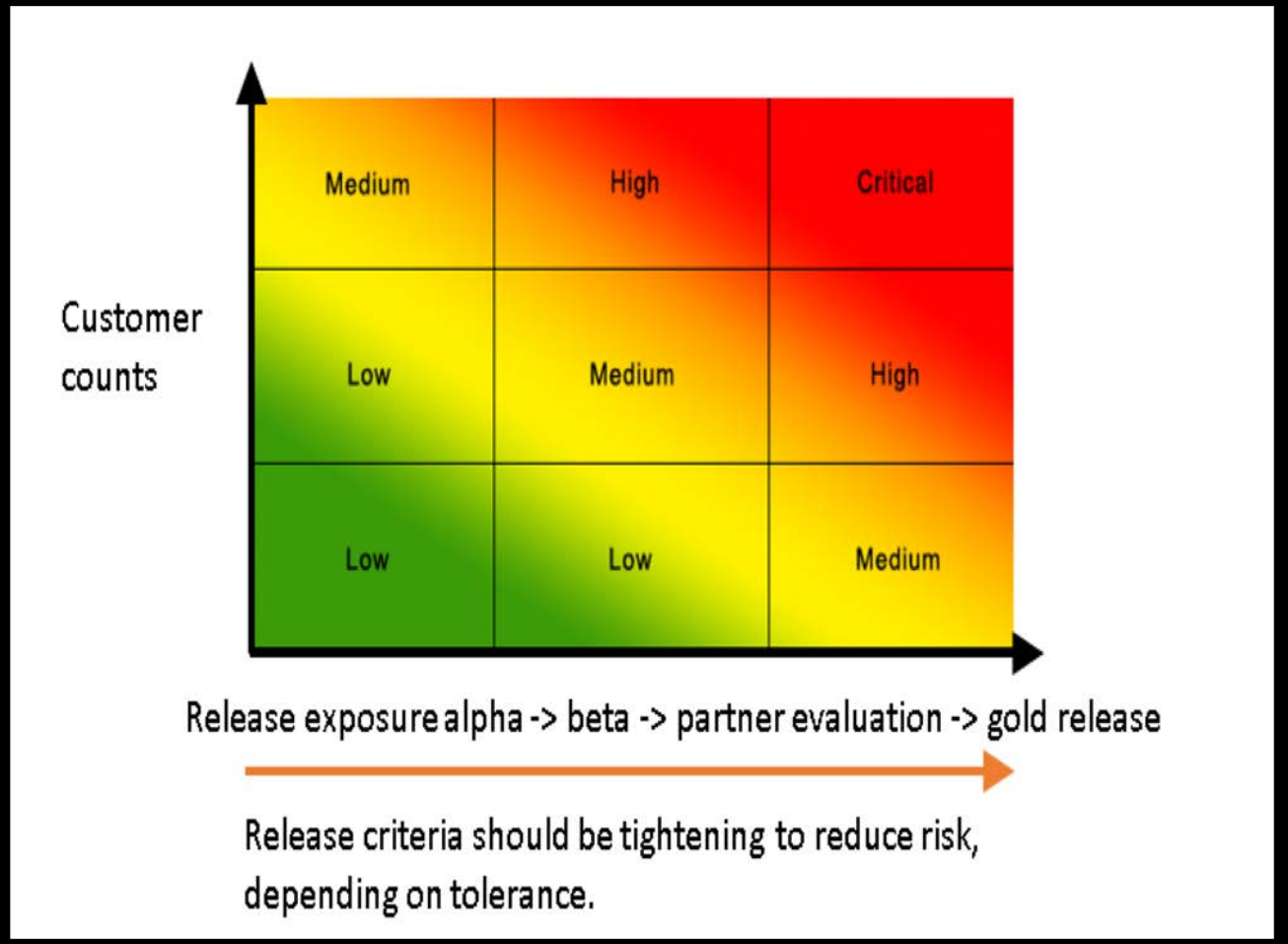


Identify a Common language

Step ONE: GET SUPPORT

Step TWO: define a vulnerability

- Define based on risk to your customers, stakeholders, partners and brand.
- Assess risk level definitions – Agree on what "critical" really means.
- Ensure security and development are able to agree with prioritization to fixes... and what happens when they don't. (We fail them....!)



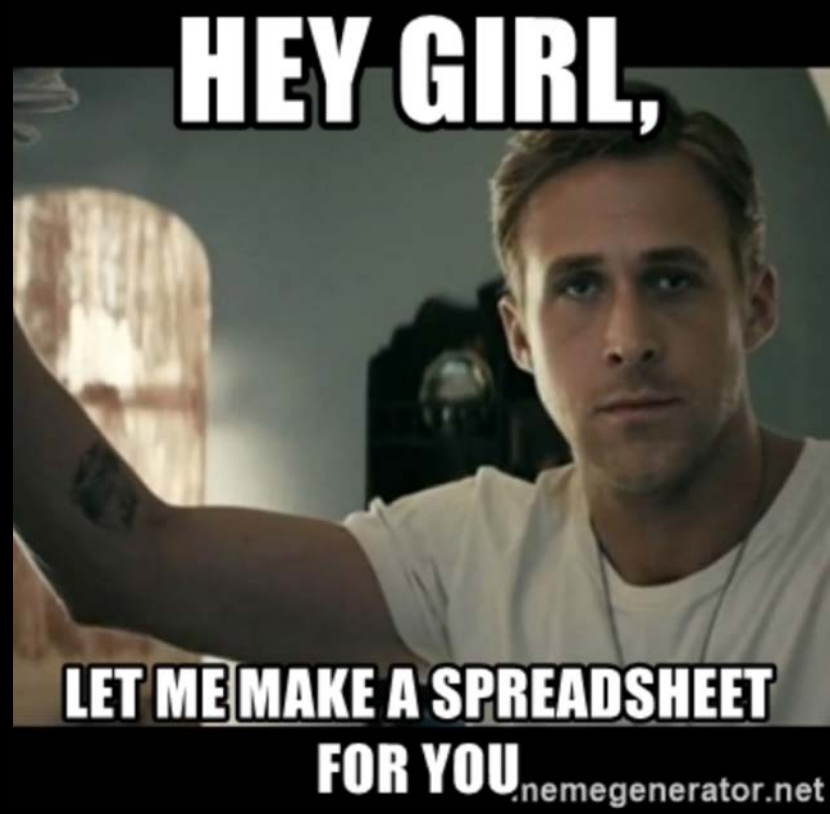
Create your own Software Readiness Review

Step THREE: Create standards

- Establish leadership support to use a SRR program as a security control
- **Understand the security posture of each software release**
- Tag vulnerabilities for ease of identification and tracking
- Define your risk threshold (SRR pass/fail criteria)
- Outline exception process (waiver)
- **You need templates and standardization!**


HEY GIRL,
LET ME MAKE A SPREADSHEET FOR YOU
memegenerator.net


HEY GIRL,
LET ME MAKE A SPREADSHEET FOR YOU
memegenerator.net


HEY GIRL,
LET ME MAKE A SPREADSHEET FOR YOU
memegenerator.net

SWSI Calculator (Should We Ship It?)

Case #: 2896478	Scoring			Rating	Base CVSS Score: 5.2 SWSI Score
REVENUE IMPACT					
Tier 1 (< $100,000) Tier 2 ($100,000 - $9999,999) Tier 3 ($1MM+)	1	2	3	2	.52
EASE OF DISCOVERY					
Tier 1 (Hard - Requires complex reverse engineering) Tier 2 (Moderate – Pen tester would find during an audit) Tier 3 (Easy – Automated tools could find)	1	2	3	1	1.04
MEDIA / PUBLICITY					
Tier 1 (obscure blog/ twitter user) Tier 2 (industry website) Tier 3 (MSM, Direct inquiry)	1	2	3	1	2.08
IMPACT TO THE BUSINESS					
Tier 1 (customer loses confidence in the business) Tier 2 (Frustrates customer with high value contract) Tier 3 (Prevents deal from closing)	1	2	3	2	1.04
RESEARCH TRENDS					
Tier 1 (New focus on a subsystem that hasn't faced rigorous testing) Tier 2 (new platform with research expected) Tier 3 (new area of research w/ high likelihood of further discovery)	1	2	3	2	1.04
				Total SWSI Rating	5.2

SWSI Calculator (Should We Ship it?)

Case #: 2896478	Scoring			Rating	Base CVSS Score: 5.2 SWSI Score
REVENUE IMPACT					
Tier 1 (< $100,000) Tier 2 ($100,000 - $9999,999) Tier 3 ($1MM+)	1	2	3	2	.52
EASE OF DISCOVERY					
Tier 1 (Hard - Requires complex reverse engineering) Tier 2 (Moderate – Pen tester would find during an audit) Tier 3 (Easy – Automated tools could find)	1	2	3	1	1.04
MEDIA / PUBLICITY					
Tier 1 (obscure blog/ twitter user) Tier 2 (industry website) Tier 3 (MSM, Direct inquiry)	1	2	3	1	2.08
IMPACT TO THE BUSINESS					
Tier 1 (customer loses confidence in the business) Tier 2 (Frustrates customer with high value contract) Tier 3 (Prevents deal from closing)	1	2	3	2	1.04
RESEARCH TRENDS					
Tier 1 (New focus on a subsystem that hasn't faced rigorous testing) Tier 2 (new platform with research expected) Tier 3 (new area of research w/ high likelihood of further discovery)	1	2	3	2	1.04
				Total SWSI Rating	5.2
				Overall rating	10.4

It's not that easy...!

- Threat landscape is unpredictable – There's no Patch Tuesday for OSS!
- Difficulties with multi-party disclosure
- Weighing business priorities and technical risk
  - Who will own the liability?
- Tracking fix commitments – keeping business units honest
- Standardized Process between business units
- Managing relationships

So, what happens when you don't agree on what to release?

We need a plan to escalate!

Technical Assessment

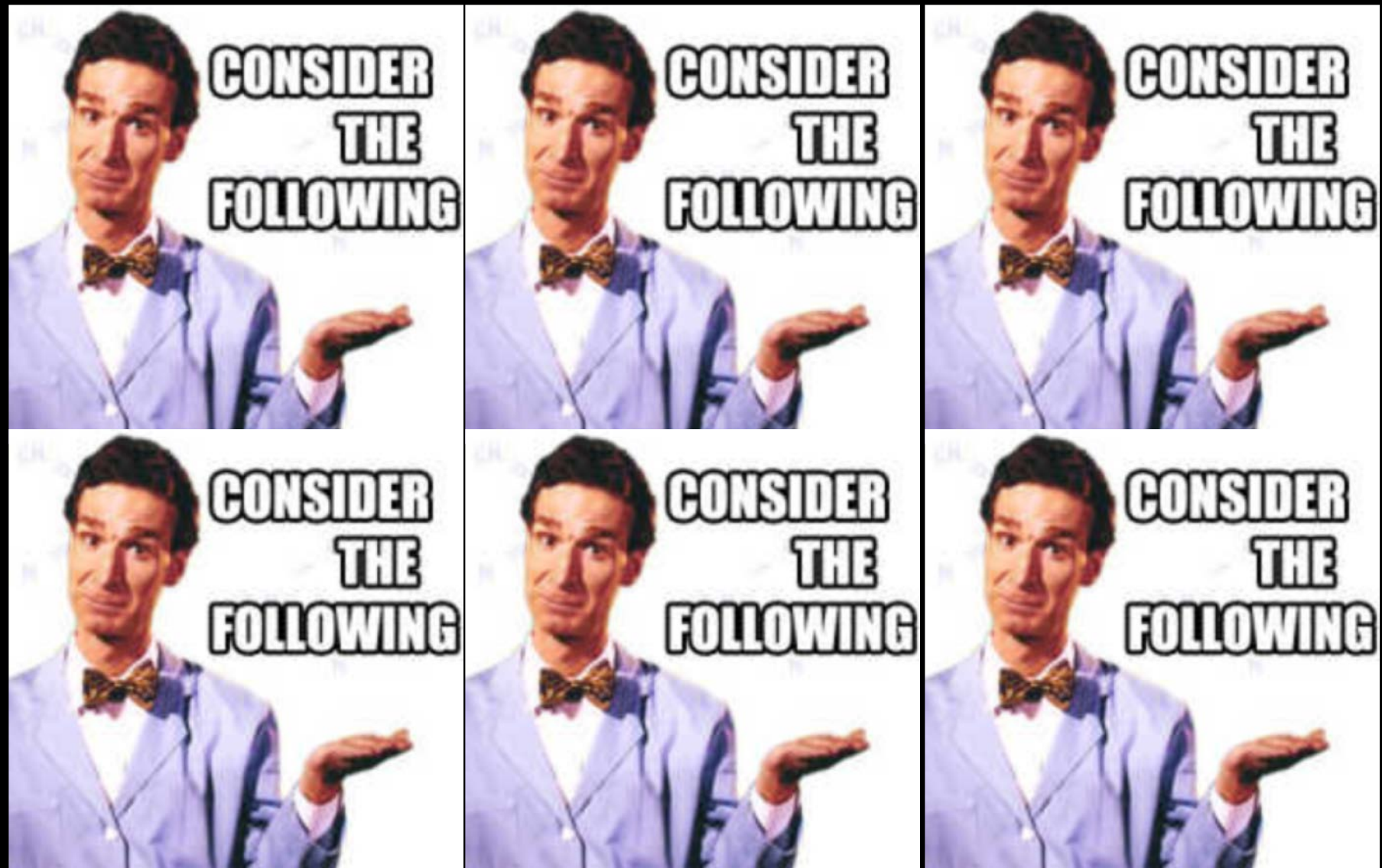
- Escalation -

Issue ID	Date created	Severity	Public (Y/N)	Remediation schedule	Missed release vehicles	Risk level	Additional details

Release Escalation

Issue backlog characteristics
1. List unresolved issues by severity.
2. Highlight lingering issues based on issue filing date (making sure to flag any publicly known issue)
3. Provide details causing delays in mitigation.
Technical reviews and recommendations
1. Provide remediation schedule as documented in the defect management system.
2. Highlight all missed release opportunities.
3. Summarize technical assessment findings and release recommendations.

Things to Remember!



But it's worth it.

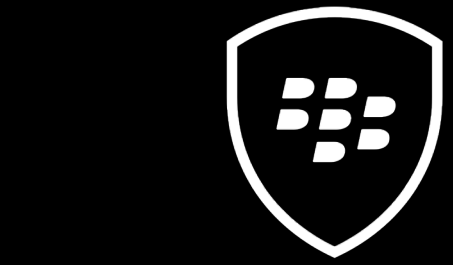
Risk landscape is ALWAYS changing

Numbers from 2017:

- ✓ On average, 8 potential vulnerabilities investigated against our product versions daily
- ✓ Reviewed a total of 515 releases

- Discovery rate / public announcements are unpredictable
- This is an on-going process; don't get hung up on each release not being perfect
- Focus on making progress
- Be a good partner, you're here to support the business

Christine Gadsby
- cgadsby@blackberry.com
- @BBSIRT



BlackBerry® Secure™

BlackBerry Careers - blackberry.com/company/careers

Github - https://github.com/ProductSecurity

BBSIRT - blackberry.com/enterprise/security/incident-response-team

Questions?