RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: ASD-R03

Stop That Release, There's A Vulnerability!

Christine Gadsby

Head of Product Security Operations
BlackBerry
@christinegadsby

Agenda

- Managing software releases in the Software Maturity Model
- Why we care so much
- Risk landscape
- Working with development
- Why the release process is challenged
- How to build your own Software Security review process
- Templates and take away(s)

RSAConference2019

Audience Poll Question

Poll the Audience

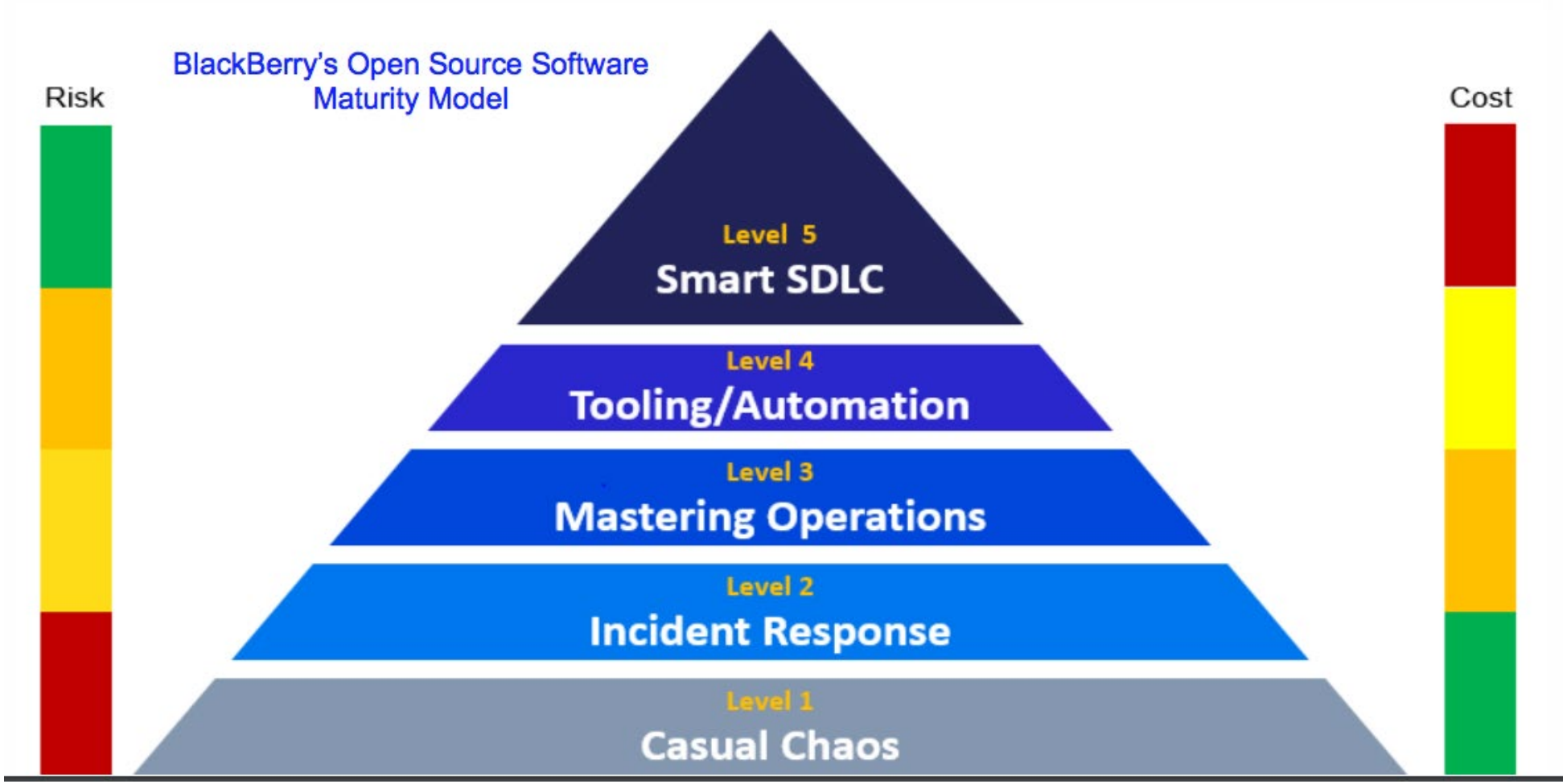
- ASD-R03
- Are you comfortable with the security oversight that your company and its suppliers have with regards to Open Source Software (OSS)?
  - Yes
  - No
  - I don't know

https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3841

RSAConference2019

Managing Software Releases in the Software Security Maturity Model

BlackBerry's Open Source Software Maturity Model



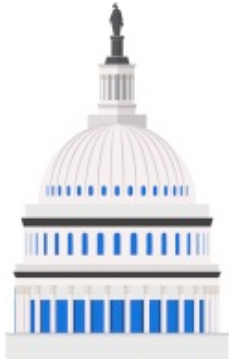
Smart SDLC

- Efficiency and customer protection
- Regulation and legislation requirements
- Sustained engineering
- Security governance during software release

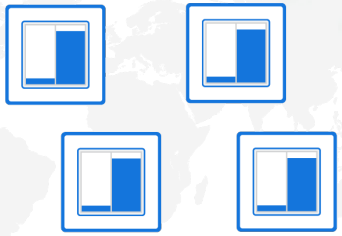
RSAConference2019

Why we Care

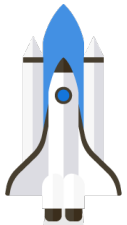
SURPRISING WAYS BLACKBERRY TOUCHES YOUR LIFE



Protecting governments
BlackBerry is trusted by 7 of the G7 and 16 of the G20 to keep people and data safe and secure.



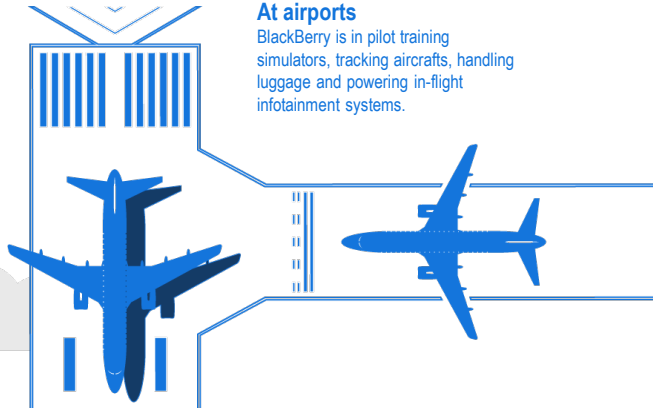
Flipping the lights on
BlackBerry is used in power generator systems, from wind turbines to hydroelectric plants, that produce electricity.



In outer space
BlackBerry powers NASA's Space Station camera system.

On the factory floor
BlackBerry powers robots that build things such as cars, HVAC, and a variety of unbranded goods.

At airports
BlackBerry is in pilot training simulators, tracking aircrafts, handling luggage and powering in-flight infotainment systems.



Advancing Autonomous Innovation
BlackBerry is used in many autonomous trials, not just cars, but also drones, ships and trains.

Producing nuclear power
BlackBerry helps nuclear power plants stay up and running 24/7, 365 days of the year.

On a train
BlackBerry is used to coordinate traffic, control locomotives, manage cockpit controls, power black boxes and even perform tilt control.

In universities
BlackBerry keeps students safe in times of crisis, whether it's a natural disaster, evacuation or active shooter situation.

In hospitals
BlackBerry can be found in many life-saving and therapeutic equipment, from ECG machines to CT scanners and medical surgical robots.

BlackBerry facilitates patient confidentiality. Doctors and hospital staff use BlackBerry to send secure messages on any device for real-time collaboration and communication

In big rigs
BlackBerry enables secure and on-time delivery of goods to homes and businesses.

BlackBerry

Enterprise-Scale Vulnerability Management

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

Risk Landscape is ALWAYS Changing

- Discovery rate/public announcement of vulnerabilities are unpredictable
- 2017 – 2018 growth
  - 23% more investigations
  - 200% increase in vulnerabilities per investigation
  - 56% more defects filed
  - 50% more customer vulnerability inquiries

RSAConference2019

Audience Poll Questions

Poll the Audience

- ASD-R03
- Does your company have a software quality checkpoint before release?
  - Yes
  - No
  - I don't know

https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3839

Poll the Audience

- ASD-R03
- Is security debt included as part of your software quality checkpoint?
  - Yes
  - No
  - I don't know

https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3840

RSAConference2019

We JUST Need to Sell Products, man...

And other reasons why security is 'hard'

SDLC - Bringing a Secure Product to Market

What development teams think …

Requirements → Design → Development → Testing → Deployment

FIX THAT VULN!!!
IT'S A SUPER BAD, CRITICAL SHOWSTOPPER

Why the Release Process is Sometimes 'Security Challenged'

The Reality of why all Software Releases are Important

You are either here …

OR, you are here …

RSAConference2019

How to WIN Patches and Influence Developers

Prep: What is Security-Ready?

- Customer reported issues: Public? Stuff? All fixed?
- Any coordinated disclosure vulnerabilities currently in flight?
- OSS security debt?
- Have security fixes been pulled into the release branch?
  - A fix in the build is better than two in the repository

Step 1: Who's Your Release Owner?

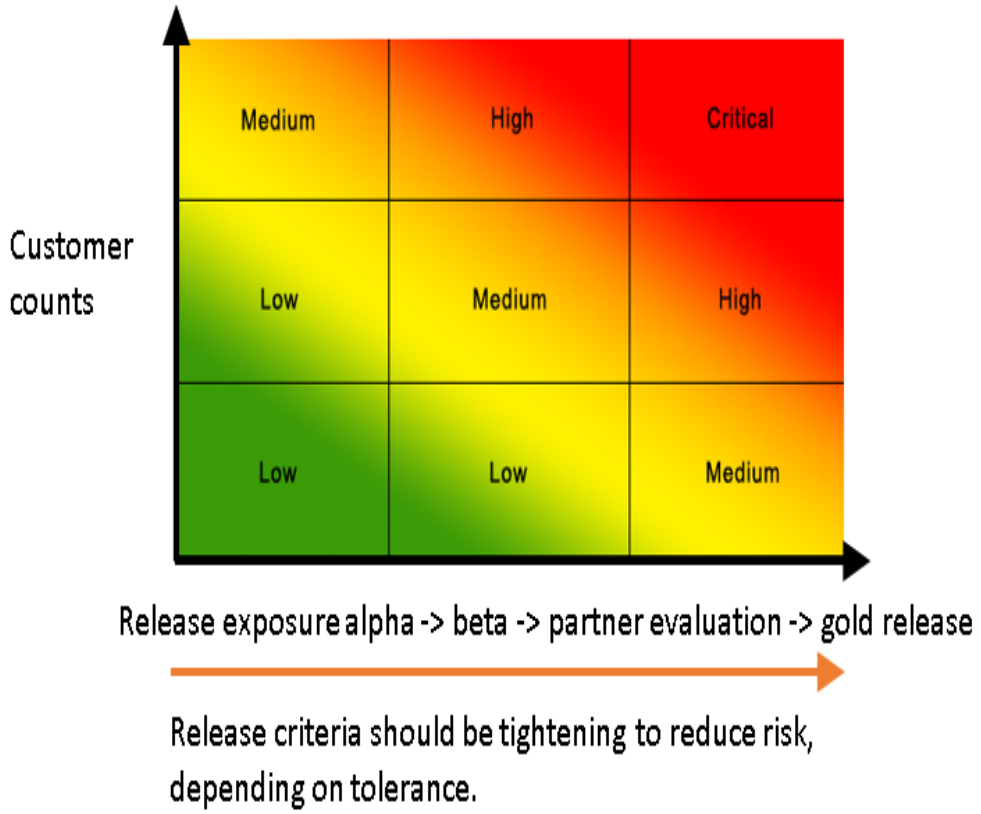
- Release owner strives for timeliness
  … AND quality!
- Teach them the vulnerability management lifecycle
- Ask: How much of the software release is for security?
- Don't cry wolf every time (unless there is a wolf)

Step 2: Integrate Security Into Your own Software Quality Checkpoint

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

Step 3: Identify a Common Language

- What is a vulnerability? (define it!)
  - 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 on prioritization of fixes, and what happens when they don’t (we fail them!)



Step 4: Regular Security Control Metrics Touchpoint

- Don't rely on your counterparts to look for security issues
- Share information on a regular cadence so that security debt has visibility
- Open and frequent dialogue shows dedication to the product, and support for the release's success

Day of Software Release Quality Checkpoint

- Understand the security posture of each software release
- What's changed since the day of the build?
- You've discovered risk and liability that impacts the build, now how do you manage that until the next release?
- Do you ask for a respin?

Filing Critical Vulnerabilities on the day of the Build: A Primer in Burning Bridges

RSAConference2019

Templates & Tools

Should we Ship it (SWSI) Calculator

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

BlackBerry

Should we Ship it (SWSI) Calculator

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

Now WHAT? Escalation Plan

- Justification for exception
- Risk/impact statement
- Fix plan
- Joint agreement for path forward between development and security teams

… document the decision!

Technical Assessment - Escalation

Issue ID	Date Created	Severity	Public (Y/N)	Remediation Schedule	Missed Release Vehicles	Risk Level	Additional Details

RSAConference2019

Create your OWN Software Security Review Process

It's a Matter of Process: Review and Get Started

- **Review your software release process**
  - Is the process uniform across the company?
  - Does each release have security criteria?
  - Is it compliance based or opt-in?
- **Find your release/security champion**
  - Influence the influencer
  - Teach them the unpredictability of the vulnerability landscape
- **Close the GAPs**
  - Compliance to process over ad-hoc escalation
  - Define the exception policy

It's a Matter of Process Continued: Review and Get Started

- **Standardize criteria and decision making**
  - Track exceptions for future reference
  - Exceptions must be well documented
- **Measure compliance at the business level**
  - Are all lines of business yielding similar results?
  - Continue to target the under performers

Expect the Bump-in-the-Night!

- Threat landscape is unpredictable – there is 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
  - Standardizing process between business units
  - Managing relationships

Defenders are a Small Community

- Highly sought after content
- There's no playbook
- We need more of you to share your process, templates, etc.

Contact us

Christine Gadsby
cgadsby@blackberry.com
@BBSIRT

BlackBerry Careers: blackberry.com/company/careers

Github: https://github.com/ProductSecurity

BBSIRT: blackberry.com/BBSIRT

Questions?