OSS Security Maturity: Time To Put On Your Big Boy Pants!

Jake Kouns
CISO
Risk Based Security
@jkouns

Christine Gadsby
Director
Product Security Response
BlackBerry
@christinegadsby

RiskBased SECURITY

BLACKBERRY

JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

- CISO at Risk Based Security
- Vulnerability Intelligence
- Vendor Risk Ratings
- Cyber Liability Insurance Expert
- Colts Fan (yes, sportsball!)

@jkouns

RiskBased SECURITY

BLACKBERRY

- Director, Security Response
- SEA to DFW
- Weight Lifter
- Pink Ribbon Earner
- Mom & Wife

@christinegadsby

Agenda

- Part I:
  - Introduction to (OSS) Security Issues (brief!)
  - Vulnerabilities
  - Legal Concerns
  - Evaluating OSS and 3rd Party Libraries
- Part II:
  - Why OSS Management Is Important To BlackBerry
  - Open Source Security Maturity Model Presentation
  - Tools
  - Case Study/Cost of OSS

RiskBased SECURITY

BLACKBERRY

OFF STATE STREET
OHIO STATE SUCKS
OBVIOUSLY SPARTY SUCKS
OUR SIGNATURE SAUSAGES
OLD SCHOOL SAUSAGES
OUR SAUSAGE SHOP
OPEN SOURCE SAUSAGES
ONE STOP SHOP

RiskBased SECURITY

BLACKBERRY

Open Source Software (OSS)

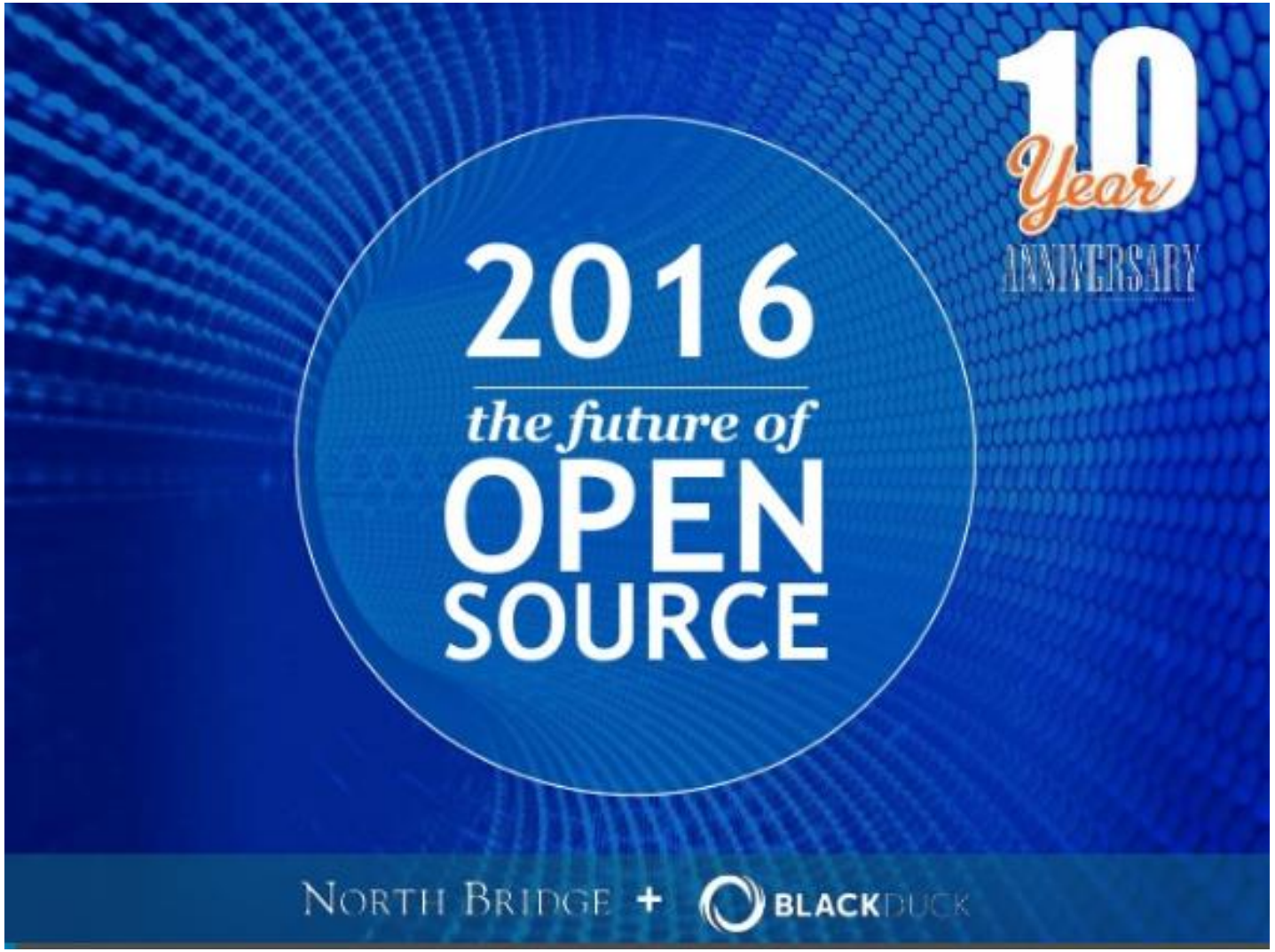
- OSS = Open Source Software
  - Source code made available with an open license
- Not just Linux
  - There is more than just flavors of *NIX operating systems
- Not just Databases
  - There is more than all the open source big data options.
- Not just Applications
  - There is more than just applications published on Github

- So what else is there?

3rd Party Libraries

OSS & 3rd Party Libraries

- Developers using established third-party libraries to:
  - Speed up the development process, accelerate time to market
  - Realize quality improvement
    - Rather than creating an in-house proprietary solutions
  - Competitive features and technical capabilities
  - Better Interoperability
- Better, Faster, Cheaper!



- Sponsored by Black Duck & North Bridge
- Over 1,300 responses
- 10th Year

https://www.blackducksoftware.com/2016-future-of-open-source

RiskBased SECURITY

BLACKBERRY

2016 Future of Open Source Survey Results

90% of respondents said Open Source Improves:

- Efficiency
- Interoperability
- Innovation

RiskBased SECURITY

BLACKBERRY

https://www.blackducksoftware.com/2016-future-of-open-source

2016 Future of Open Source Survey Results

Open Source Participation:

- 67% of respondents report actively encouraging developers to engage in and contribute to open source projects.
- 65% of companies are contributing to open source projects.
- 59% of respondents participate in open source projects to gain competitive edge.
- One in three companies have a full-time resource dedicated to open source projects.

https://www.blackducksoftware.com/2016-future-of-open-source

2016 Future of Open Source Survey Results

Top Ways Companies Review Open Source Code:

- 48% - Development Teams manually keep track of open source usage
- 30% - Ask developers about open source content
- 21% - Use third party tools to scan for open source content

https://www.blackducksoftware.com/2016-future-of-open-source

2016 Future of Open Source Survey Results

Security and Management:

- 50% of companies have no formal policy for selecting and approving open source code.
- 47% of companies don't have formal processes in place to track open source code, limiting their visibility into their open source and therefore their ability to control it.
- More than 1/3 of companies have no process for identifying, tracking or remediating known open source vulnerabilities.

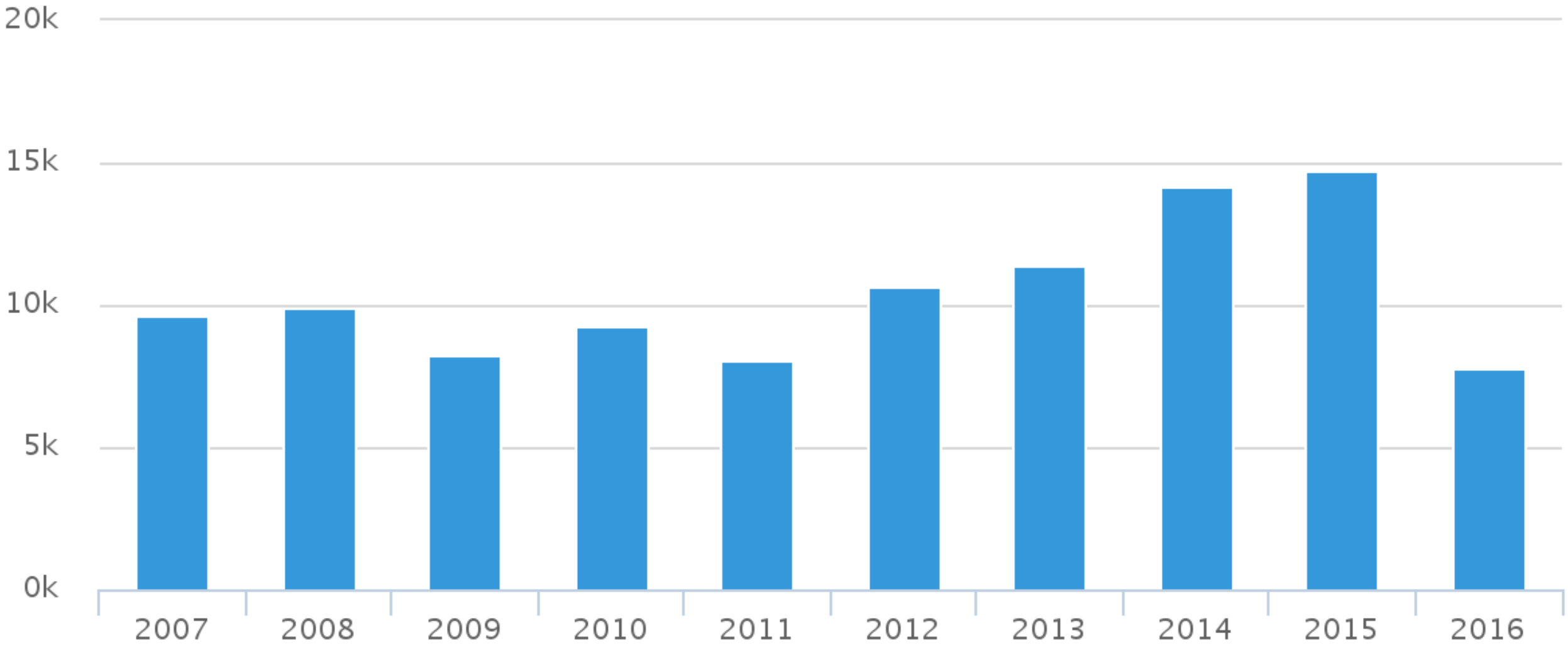
https://www.blackducksoftware.com/2016-future-of-open-source

RiskBased SECURITY

BLACKBERRY

Do You Have Your Big Boy Pants & Your Snack?!

Vulnerabilities over the last 10 years



You Just Mean HeartBleed Right?

- While HeartBleed / OpenSSL helped raise awareness about 3rd Party Libraries
- We are not talking about OpenSSL!

Stagefright (libstagefright)

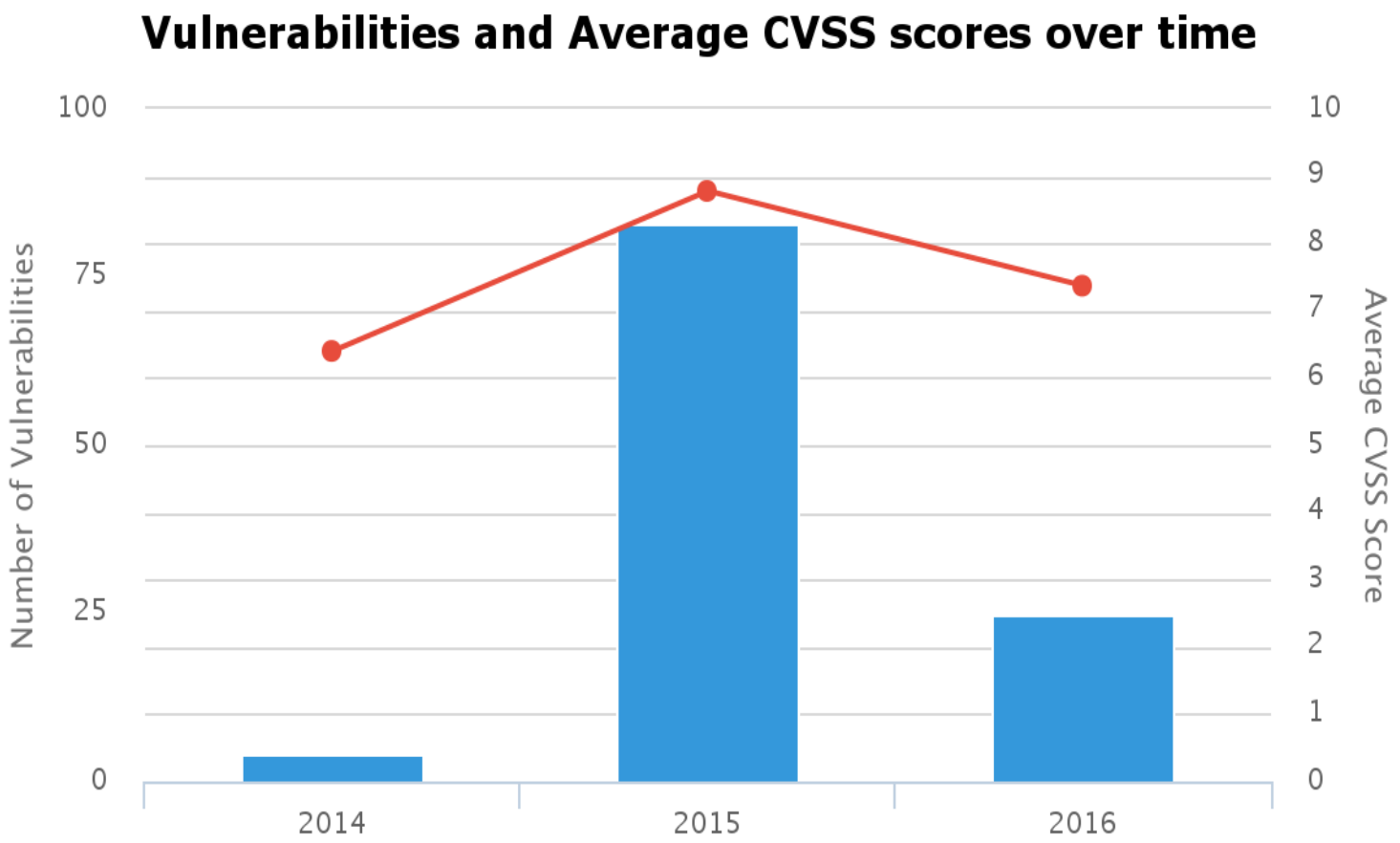
RiskBased SECURITY

BLACKBERRY

Stagefright (libstagefright)

- Android's Multimedia Framework library
  - Handles all video and audio files, playback, extracts metadata for Gallery, etc
- Six critical vulnerabilities leaving Android phones open to an attack delivered by a simple multimedia text
- All remote code execution
- Stagefright also used in Firefox, Firefox OS, MAC OS X, Windows

Stagefright (libstagefright)



Total Vulnerabilities
112

Max CVSS Score
10.0

Average CVSS Score
8.36

RiskBased SECURITY

BLACKBERRY


IF YOU COULD JUST PUT YOUR BIG BOY PANTS ON
THAT WOULD BE GREAT
memegenerator.net

Symantec Vulnerabilities

These vulnerabilities are as bad as it gets.

Symantec Vulnerabilities

CVE-ID	
CVE-2016-2207	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The AntiVirus Decomposer engine in Symantec Advanced Threat Protection (ATP); Symantec Data Center Security:Server (SDCS:S) 6.x through 6.6 MP1; Symantec Web Gateway; Symantec Endpoint Protection (SEP) before 12.1 RU6 MP5; Symantec Endpoint Protection (SEP) for Mac; Symantec Endpoint Protection (SEP) for Linux before 12.1 RU6 MP5; Symantec Protection Engine (SPE) before 7.0.5 HF01, 7.5.x before 7.5.3 HF03, 7.5.4 before HF01, and 7.8.0 before HF01; Symantec Protection for SharePoint Servers (SPSS) 6.0.3 through 6.0.5 before 6.0.5 HF 1.5 and 6.0.6 before HF 1.6; Symantec Mail Security for Microsoft Exchange (SMSMSE) before 7.0_3966002 HF1.1 and 7.5.x before 7.5_3966008 VHF1.2; Symantec Mail Security for Domino (SMSDOM) before 8.0.9 HF1.1 and 8.1.x before 8.1.3 HF1.2; CSAPI before 10.0.4 HF01; Symantec Message Gateway (SMG) before 10.6.1-4; Symantec Message Gateway for Service Providers (SMG-SP) 10.5 before patch 254 and 10.6 before patch 253; Norton AntiVirus, Norton Security, Norton Internet Security, and Norton 360 before NGC 22.7; Norton Security for Mac before 13.0.2; Norton Power Eraser (NPE) before 5.1; and Norton Bootable Removal Tool (NBRT) before 2016.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory access violation) via a crafted RAR file that is mishandled during decompression.

Symantec Vulnerabilities

- CVE-2016-2207
  - Description just discusses Symantec/Norton products
  - Product impacted are also only Symantec/Norton products
- And while they are affected……

This is a 3rd Party Library vulnerability!

VulnDB ID: 140636 Pu

UnRAR unpack15.cpp Unpack::ShortLZ() Function Array Indexing Memory Corruption

RiskBased SECURITY BLACKBERRY

Symantec Vulnerabilities

CVE-ID	
CVE-2016-2211	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The AntiVirus Decomposer engine in Symantec Advanced Threat Protection (ATP); Symantec Data Center Security:Server (SDCS:S) 6.x through 6.6 MP1; Symantec Web Gateway; Symantec Endpoint Protection (SEP) before 12.1 RU6 MP5; Symantec Endpoint Protection (SEP) for Mac; Symantec Endpoint Protection (SEP) for Linux before 12.1 RU6 MP5; Symantec Protection Engine (SPE) before 7.0.5 HF01, 7.5.x before 7.5.3 HF03, 7.5.4 before HF01, and 7.8.0 before HF01; Symantec Protection for SharePoint Servers (SPSS) 6.0.3 through 6.0.5 before 6.0.5 HF 1.5 and 6.0.6 before HF 1.6; Symantec Mail Security for Microsoft Exchange (SMSMSE) before 7.0_3966002 HF1.1 and 7.5.x before 7.5_3966008 VHF1.2; Symantec Mail Security for Domino (SMSDOM) before 8.0.9 HF1.1 and 8.1.x before 8.1.3 HF1.2; CSAPI before 10.0.4 HF01; Symantec Message Gateway (SMG) before 10.6.1-4; Symantec Message Gateway for Service Providers (SMG-SP) 10.5 before patch 254 and 10.6 before patch 253; Norton AntiVirus, Norton Security, Norton Internet Security, and Norton 360 before NGC 22.7; Norton Security for Mac before 13.0.2; Norton Power Eraser (NPE) before 5.1; and Norton Bootable Removal Tool (NBRT) before 2016.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted CAB file that is mishandled during decompression.

RiskBased SECURITY BLACKBERRY

Symantec Vulnerabilities

- CVE-2016-2211
  - Description just discusses Symantec/Norton products
  - Product impacted are also only Symantec/Norton products
- And while they are affected……

This is actually a 3rd Party Library vulnerability!

VulnDB ID: 140642

libmspack Multiple Unspecified Memory Corruption Arbitrary Code Execution

RiskBased SECURITY

BLACKBERRY

Symantec Vulnerabilities

As with all software developers, antivirus vendors have to do vulnerability management. This means monitoring for new releases of third party software used, watching published vulnerability announcements, and distributing updates.

Nobody is perfect at this, but that is a core part of security software development.

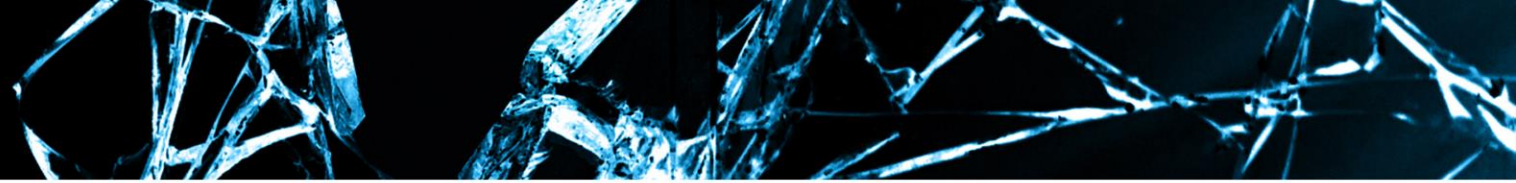
Symantec dropped the ball here. A quick look at the decompressor library shipped by Symantec showed that they were using code derived from open source libraries like libmspack that hadn't updated them in at least 7 years.

Dozens of public vulnerabilities in these libraries affected Symantec, some with public exploits. We sent Symantec some examples, and they verified they had fallen behind on releases.

...but hadn't updated them in at least 7 year.

RiskBased SECURITY

BLACKBERRY



SO WHAT?

RiskBased SECURITY

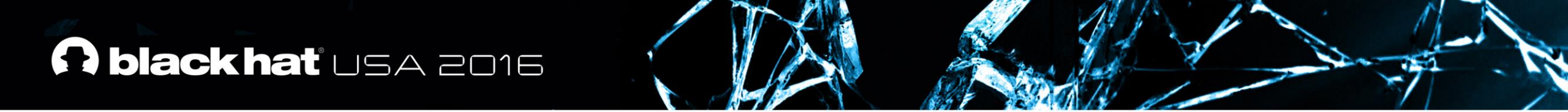
BLACKBERRY

black hat USA 2016

black hat USA 2016


WELL THEN
SOMEONE IS WEARING HIS BIG BOY PANTS
memegenerator.net


black hat
USA 2016
OSS Security Management At Black Berry
JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS



QNX | BlackBerry Subsidiary

Good | Powered By BlackBerry

movirtu | By BlackBerry

secusmart | BlackBerry Subsidiary

WatchDox | By BlackBerry

AtHoc | Division of BlackBerry

certicom | BlackBerry Subsidiary

Priv | BlackBerry Secure Smartphone Powered by Android™

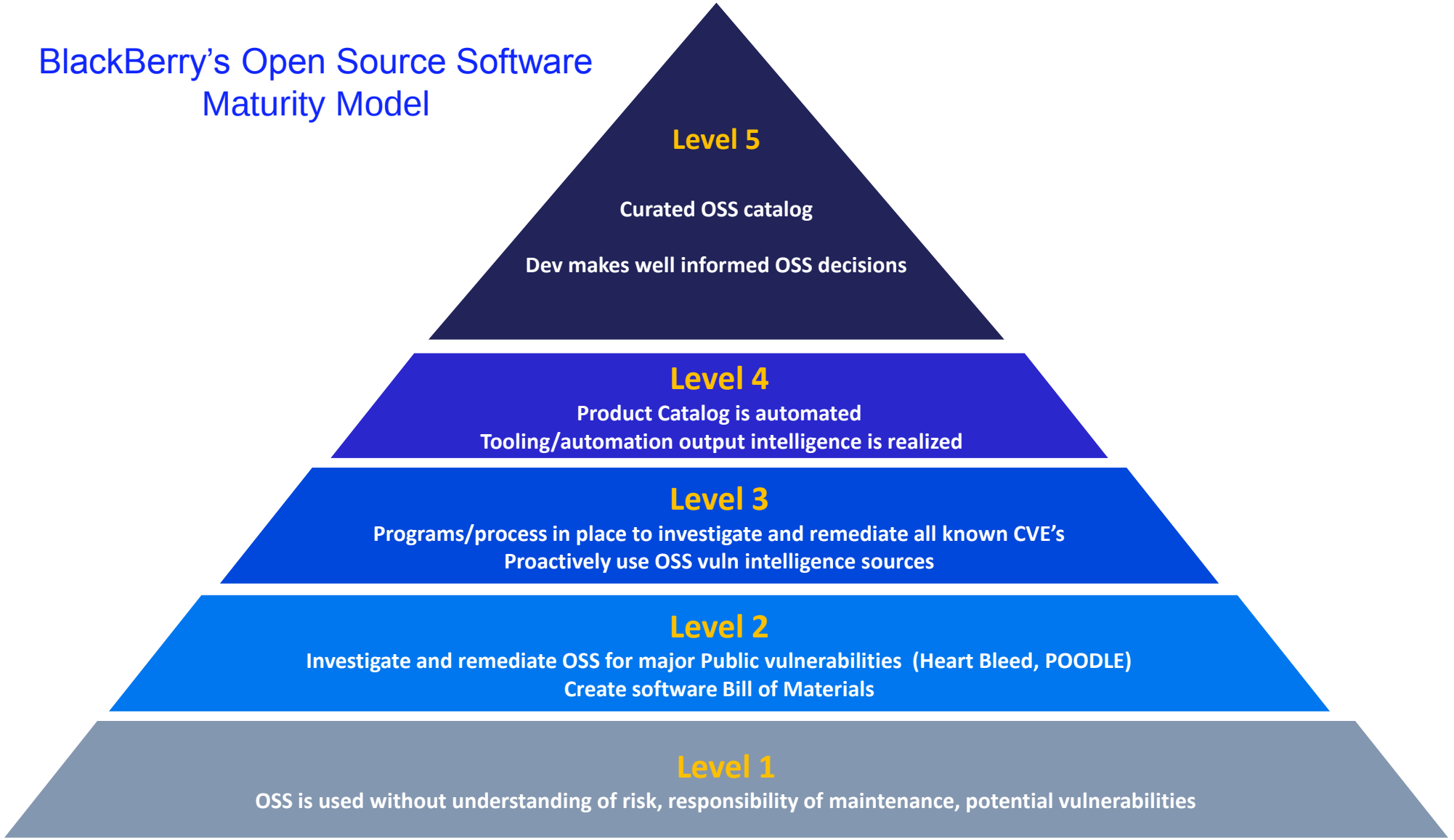
Fun BlackBerry OSS facts

- 536 unique libs tracked across 75 product variants
- Up to 16 different versions of a unique library in a single product
- 195 unique OSS libs in a single product
- A product could contain 47 copies of the same library

Risk

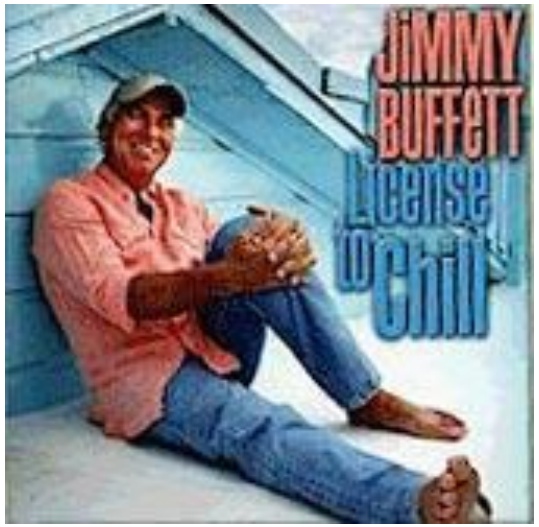
Cost

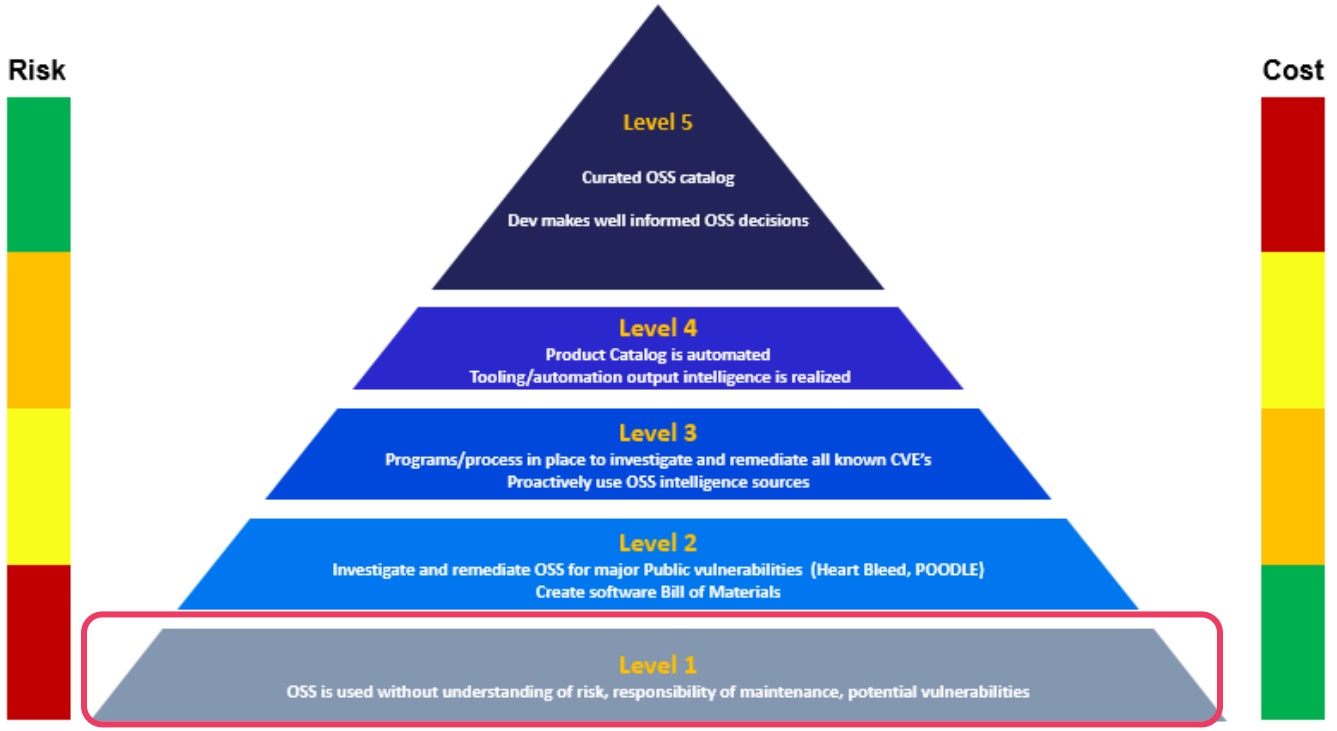
BlackBerry's Open Source Software Maturity Model



Level 1 – Casual Chaos

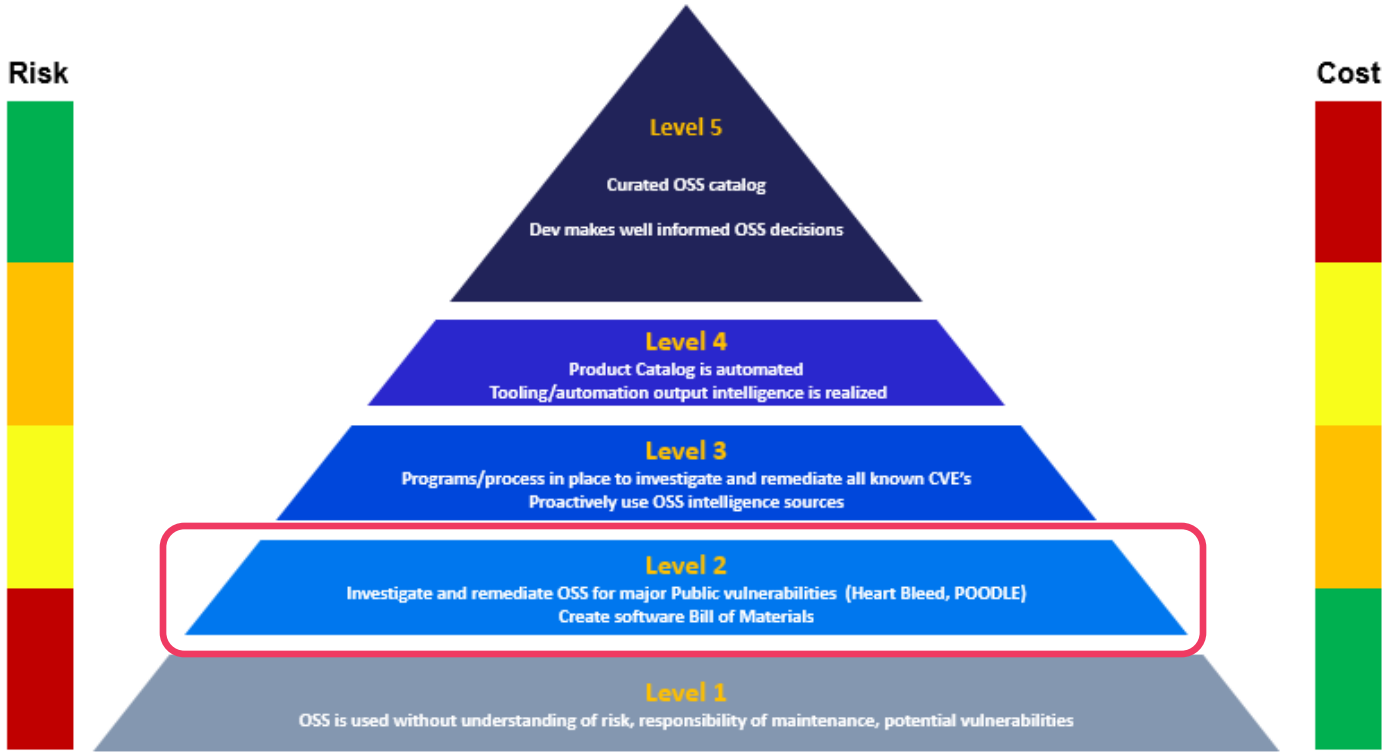
- Using OSS blindly
- No understanding of risk or spread
- Press is your vuln notification; media drives fear
- CEO calls and you duck and cover





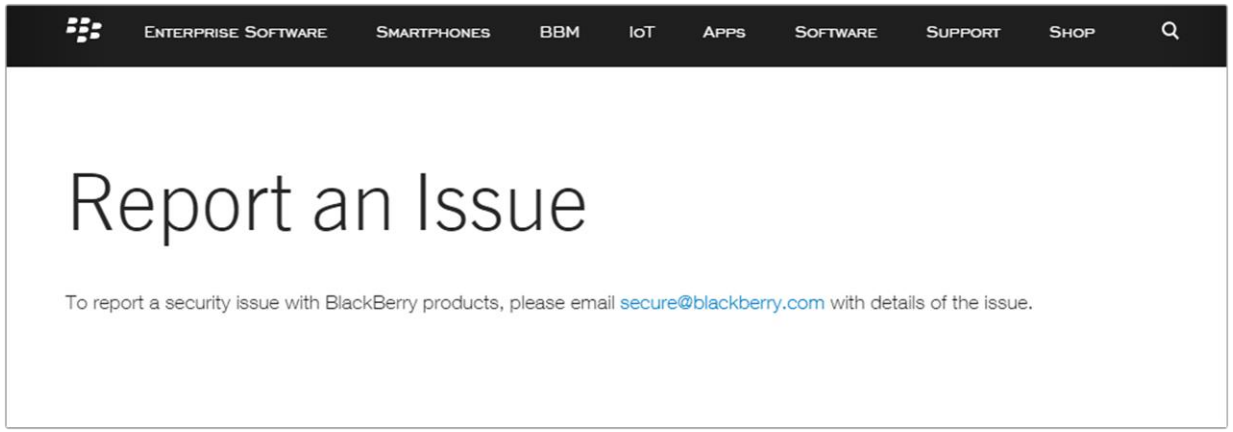
Level 2 – Incident Response is born

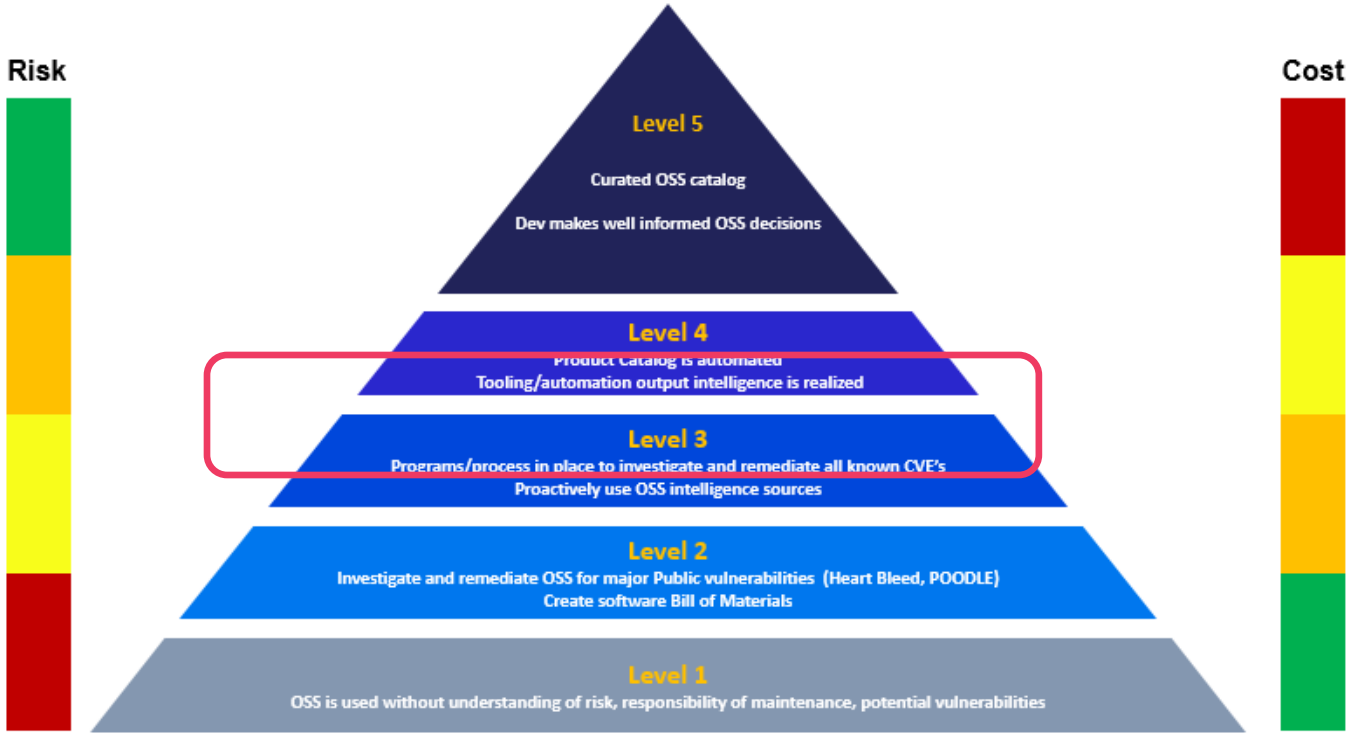
- Create software BOM
- Investigate and remediate public OSS vulns
- Tracking vulns and fixes
- Plan in place with dev for Incident Response



Level 3 – Mastering Ops

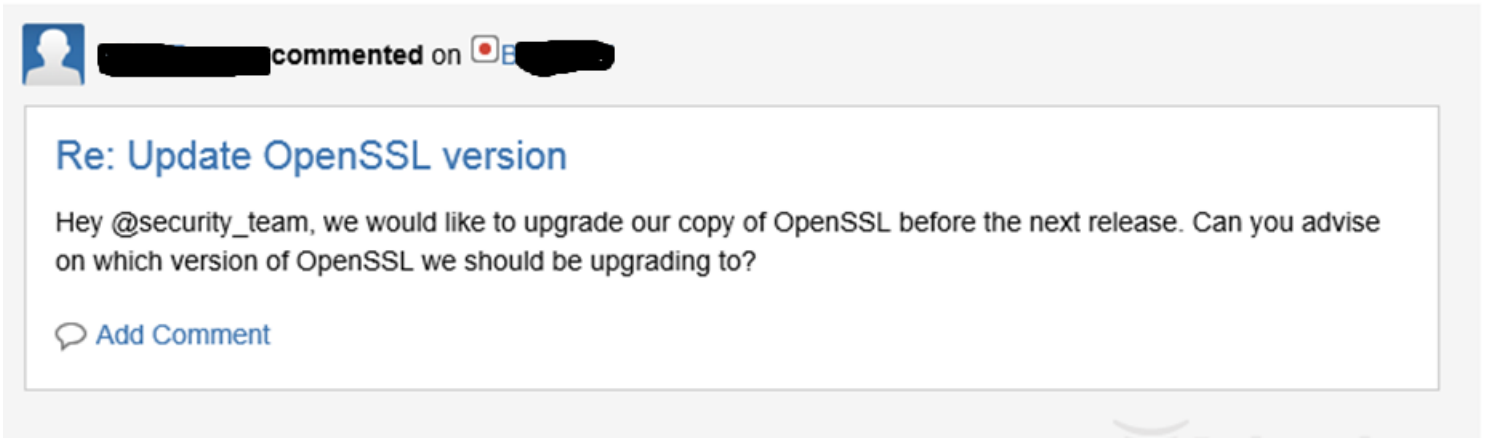
- Proactively use OSS vuln intelligence sources
- Process for OSS vuln lifecycle
- Fixes VS. Features with fix vehicle
- Notification to customers
- Security Researchers know where to report OSS vulns
- Public Vuln disclosure policy

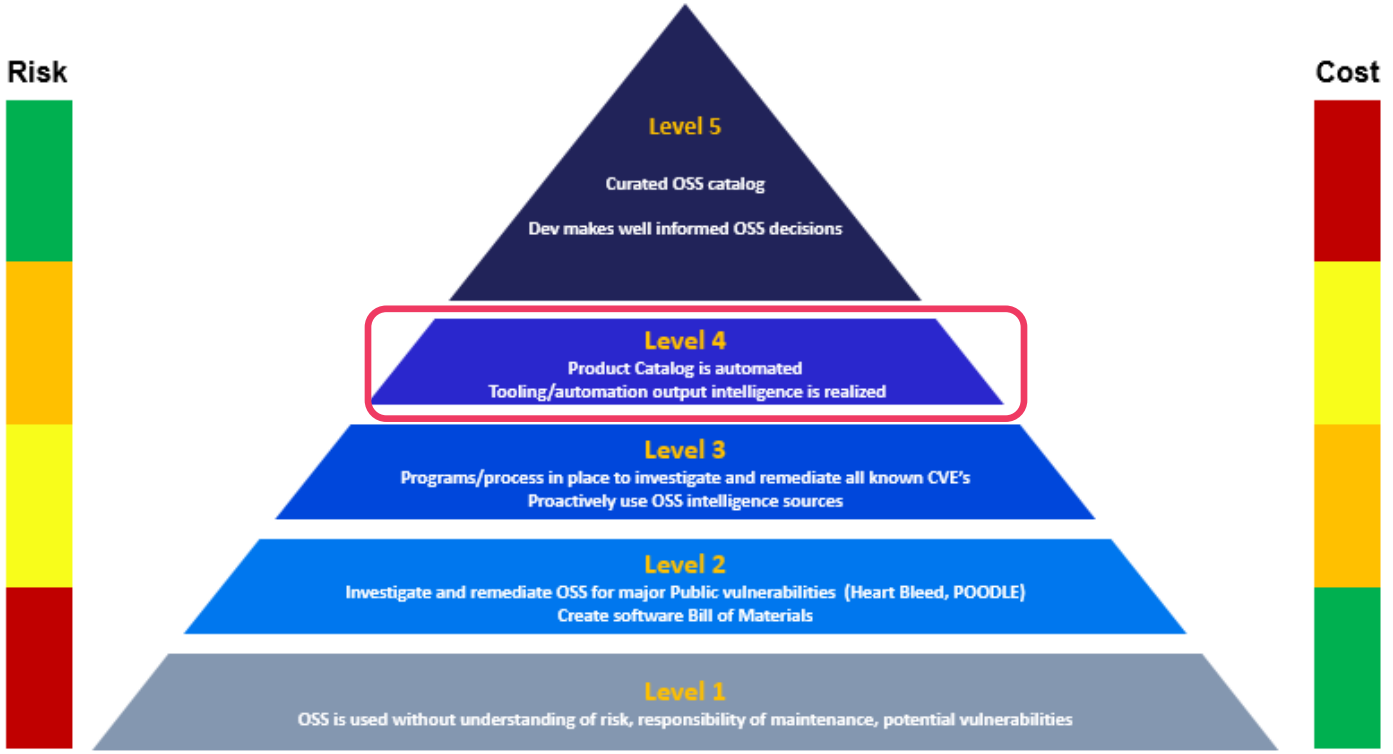




Level 4 – Tools

- Using your vuln data proactively
- Product Catalog is automated/tracked
- Using tooling and automation to drive efficient vulnerability handling
- Dev proactive involvement with security
- OSS vuln debt has exec visibility





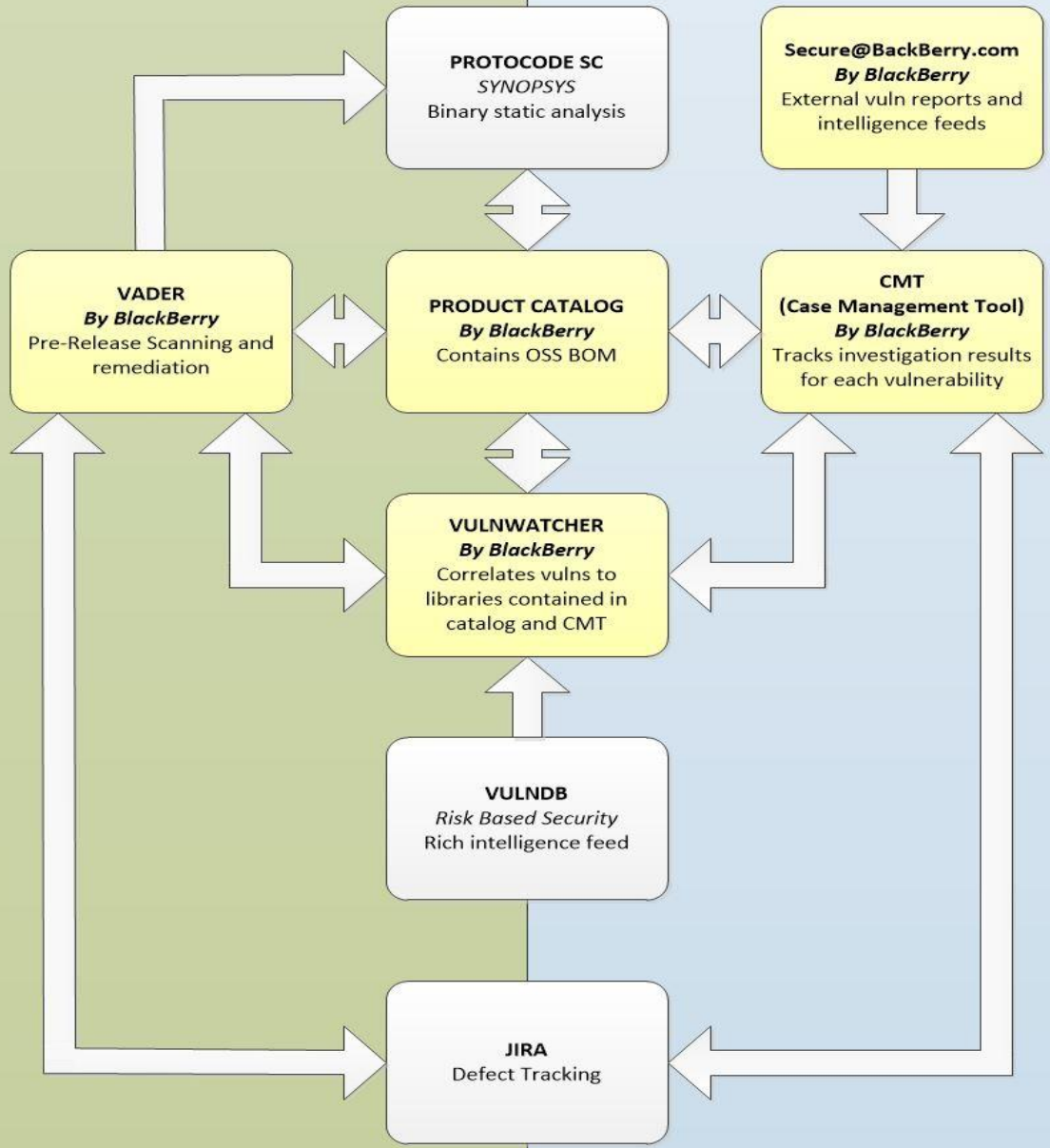
BlackBerry Custom Tooling

VADER – Pre-release Products
- Protecode-SC scan returns BOM and known vulns
- Automated defect creation

Product Catolog
- Detailed BOM for each products
- Every instance of OSS captured

CMT – Case Management Tool
- Tracks vulnerability investigations
- Records affected/not for every vulnerability and each instance within products
- Automated defect filing

VulnWatcher
- Flags new vulns affecting OSS used in our products
- Lists vulnerabilities not yet investigated across products
- Automated Case open



3rd Party Tooling Integration

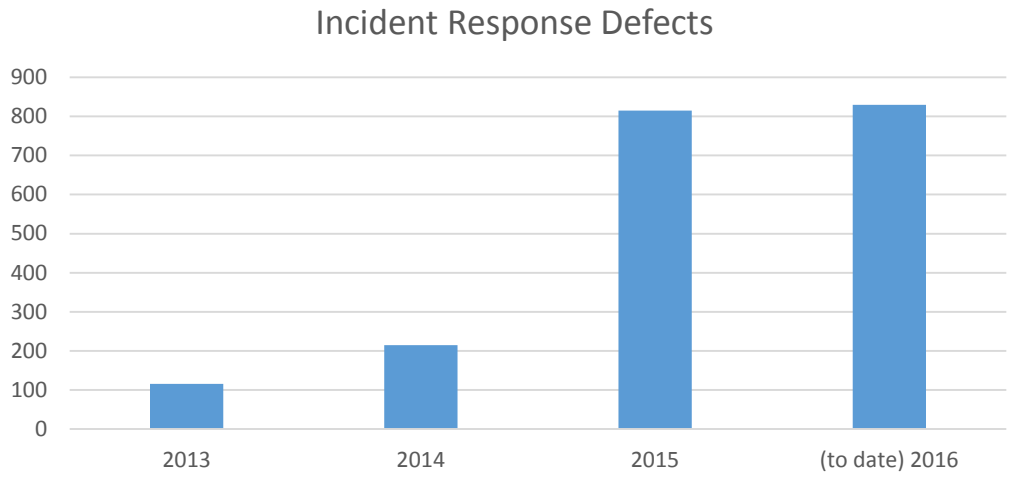
Synopsys Protecode – SC
(formerly Codenomicon AppCheck)
- Binary static analysis detects OSS
- Output feeds BOM creation in Product Catalog

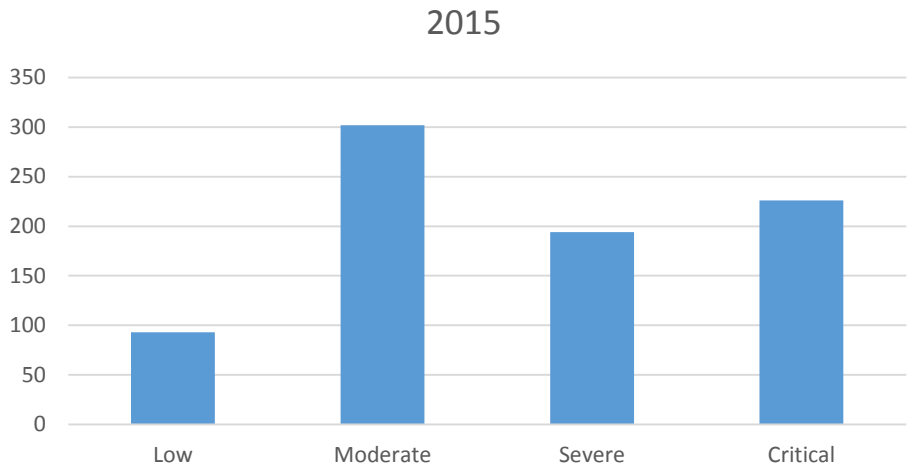
RiskBased SECURITY – VulnDB
- Intelligence feed for vulnwatcher
- Rich data to assist investigation

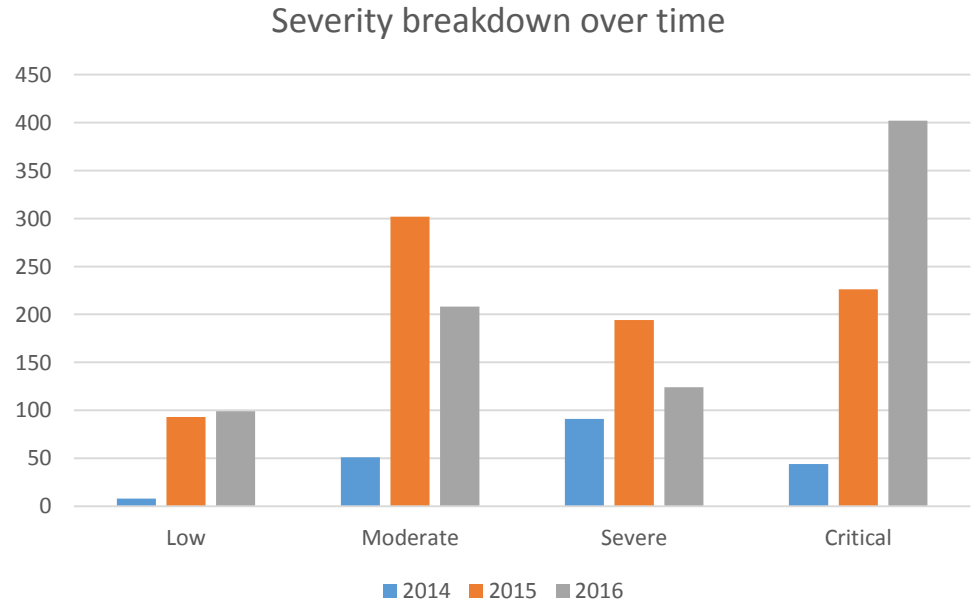
Jira
- Security Defect Tracking

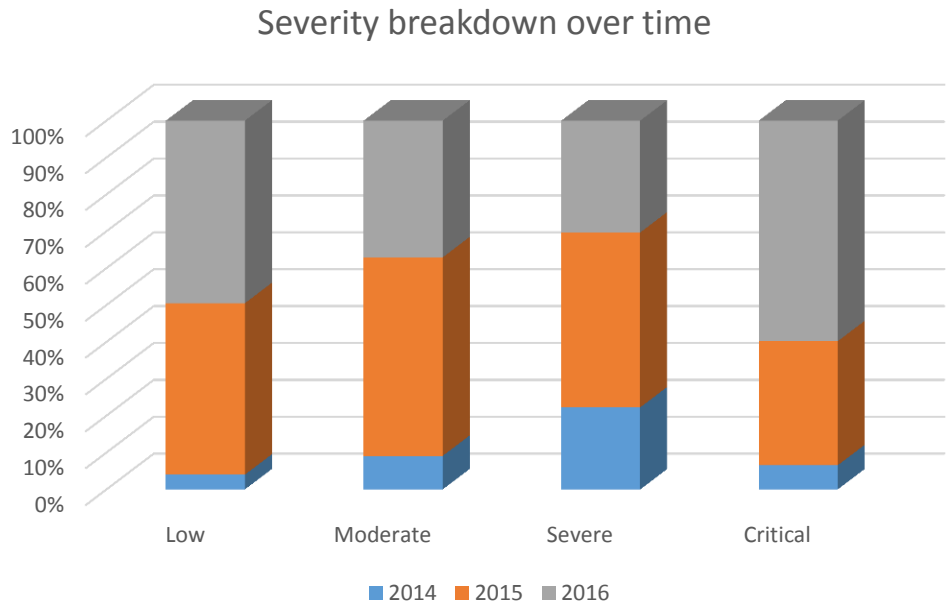
DEVELOPMENT

IN-MARKET

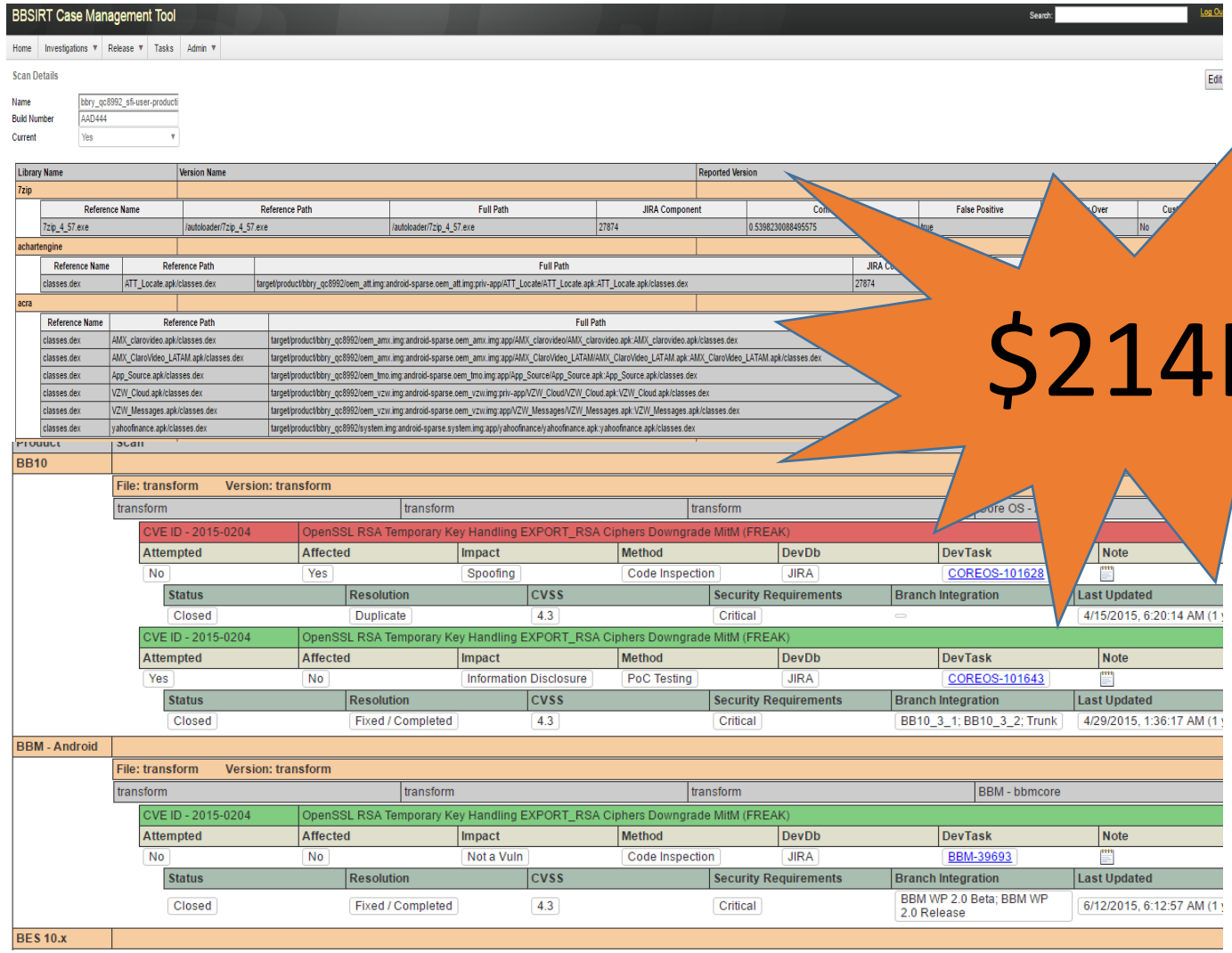

Incident Response Defects
900
800
700
600
500
400
300
200
100
0
2013
2014
2015
(to date) 2016


2015
350
300
250
200
150
100
50
0
Low
Moderate
Severe
Critical


Severity breakdown over time
450
400
350
300
250
200
150
100
50
0
Low
Moderate
Severe
Critical
2014
2015
2016


Severity breakdown over time
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Low
Moderate
Severe
Critical
2014
2015
2016

OpenSSL 'Freak'


BBSIRT Case Management Tool

Home | Investigations | Release | Tasks | Admin

Scan Details

Name: bbry_qc8992_sfi-user-producti
Build Number: AAD444
Current: Yes

Library Name	Version Name	Reported Version
7zip		

Reference Name	Reference Path	Full Path	JIRA Component	Com	False Positive	Over	Cus
7zip_4_57.exe	/autoloader/7zip_4_57.exe	/autoloader/7zip_4_57.exe	27874	0.5398230088495575	true		No

achartengine				
Reference Name	Reference Path	Full Path	JIRA Co	
classes.dex	ATT_Locate.apk/classes.dex	target/product/bbry_qc8992/oem_att.img:android-sparse.oem_att.img:priv-app/ATT_Locate/ATT_Locate.apk:ATT_Locate.apk/classes.dex	27874	

acra		
Reference Name	Reference Path	Full Path
classes.dex	AMX_clarovideo.apk/classes.dex	target/product/bbry_qc8992/oem_amx.img:android-sparse.oem_amx.img:app/AMX_clarovideo/AMX_clarovideo.apk:AMX_clarovideo.apk/classes.dex
classes.dex	AMX_ClaroVideo_LATAM.apk/classes.dex	target/product/bbry_qc8992/oem_amx.img:android-sparse.oem_amx.img:app/AMX_ClaroVideo_LATAM/AMX_ClaroVideo_LATAM.apk:AMX_ClaroVideo_LATAM.apk/classes.dex
classes.dex	App_Source.apk/classes.dex	target/product/bbry_qc8992/oem_tmo.img:android-sparse.oem_tmo.img:app/App_Source/App_Source.apk:App_Source.apk/classes.dex
classes.dex	VZW_Cloud.apk/classes.dex	target/product/bbry_qc8992/oem_vzw.img:android-sparse.oem_vzw.img:priv-app/VZW_Cloud/VZW_Cloud.apk:VZW_Cloud.apk/classes.dex
classes.dex	VZW_Messages.apk/classes.dex	target/product/bbry_qc8992/oem_vzw.img:android-sparse.oem_vzw.img:app/VZW_Messages/VZW_Messages.apk:VZW_Messages.apk/classes.dex
classes.dex	yahoofinance.apk/classes.dex	target/product/bbry_qc8992/system.img:android-sparse.system.img:app/yahoofinance/yahoofinance.apk:yahoofinance.apk/classes.dex

BB10

File: transform Version: transform

transform | transform | transform | ore OS -

CVE ID - 2015-0204 — OpenSSL RSA Temporary Key Handling EXPORT_RSA Ciphers Downgrade MitM (FREAK)

Attempted	Affected	Impact	Method	DevDb	DevTask	Note
No	Yes	Spoofing	Code Inspection	JIRA	COREOS-101628	

Status	Resolution	CVSS	Security Requirements	Branch Integration	Last Updated
Closed	Duplicate	4.3	Critical		4/15/2015, 6:20:14 AM (1

CVE ID - 2015-0204 — OpenSSL RSA Temporary Key Handling EXPORT_RSA Ciphers Downgrade MitM (FREAK)

Attempted	Affected	Impact	Method	DevDb	DevTask	Note
Yes	No	Information Disclosure	PoC Testing	JIRA	COREOS-101643	

Status	Resolution	CVSS	Security Requirements	Branch Integration	Last Updated
Closed	Fixed / Completed	4.3	Critical	BB10_3_1; BB10_3_2; Trunk	4/29/2015, 1:36:17 AM (1

BBM - Android

File: transform Version: transform

transform | transform | transform | BBM - bbmcore

CVE ID - 2015-0204 — OpenSSL RSA Temporary Key Handling EXPORT_RSA Ciphers Downgrade MitM (FREAK)

Attempted	Affected	Impact	Method	DevDb	DevTask	Note
No	No	Not a Vuln	Code Inspection	JIRA	BBM-39693	

Status	Resolution	CVSS	Security Requirements	Branch Integration	Last Updated
Closed	Fixed / Completed	4.3	Critical	BBM WP 2.0 Beta; BBM WP 2.0 Release	6/12/2015, 6:12:57 AM (1

BES 10.x

$214K

Product List

Search by library: openssl — Add

Product	Build
BBM - Android	2.13.0.13
BES 10.x	10.2.7
BB10	10.3.2
Core	unknown
oGo - Android	1.0.0.1838
	6.6.0
	294.0.0.14

BlackBerry Security Communications Release

BlackBerry Confidential – Internal Use Only. Do Not Distribute Externally In Entirety. Use Content As Directed.

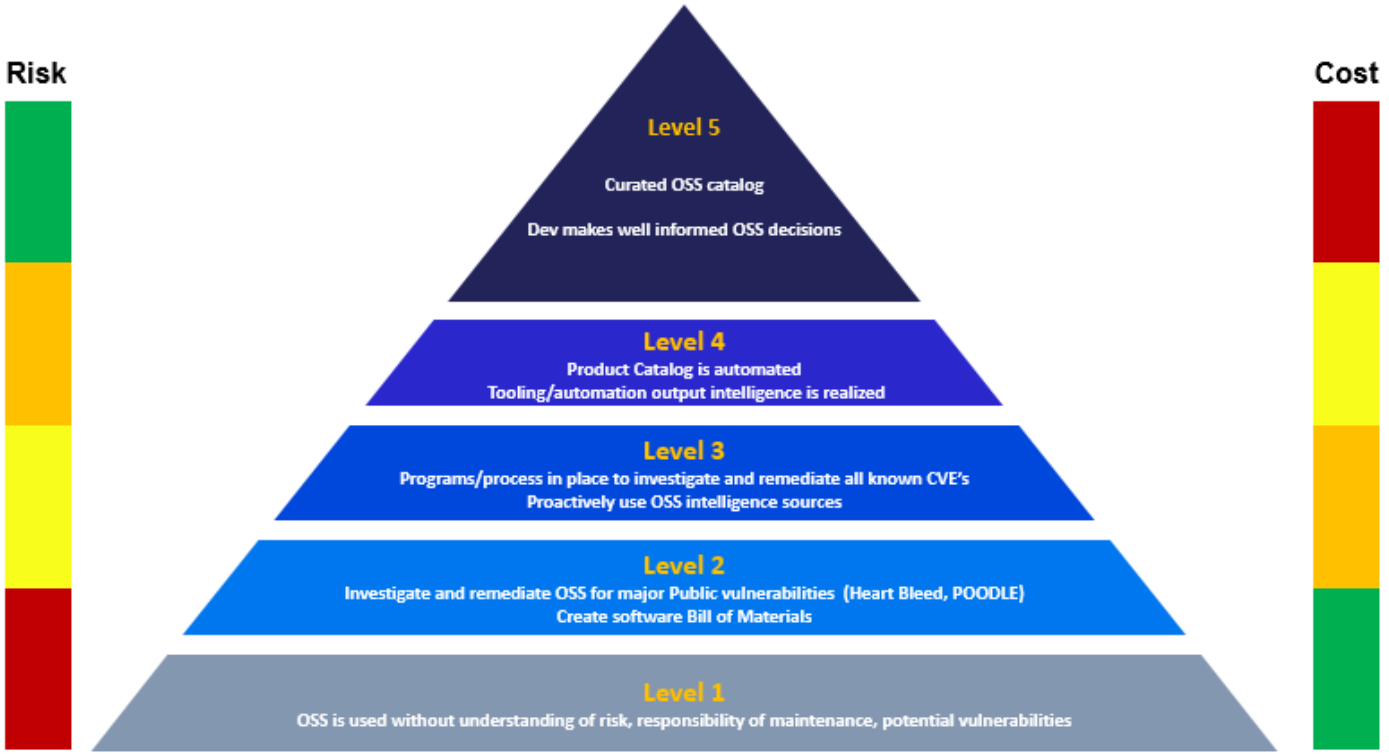
You can use this communications release as directed to respond to and advise customers and carriers regarding the industry wide security issue in OpenSSL named 'FREAK'.

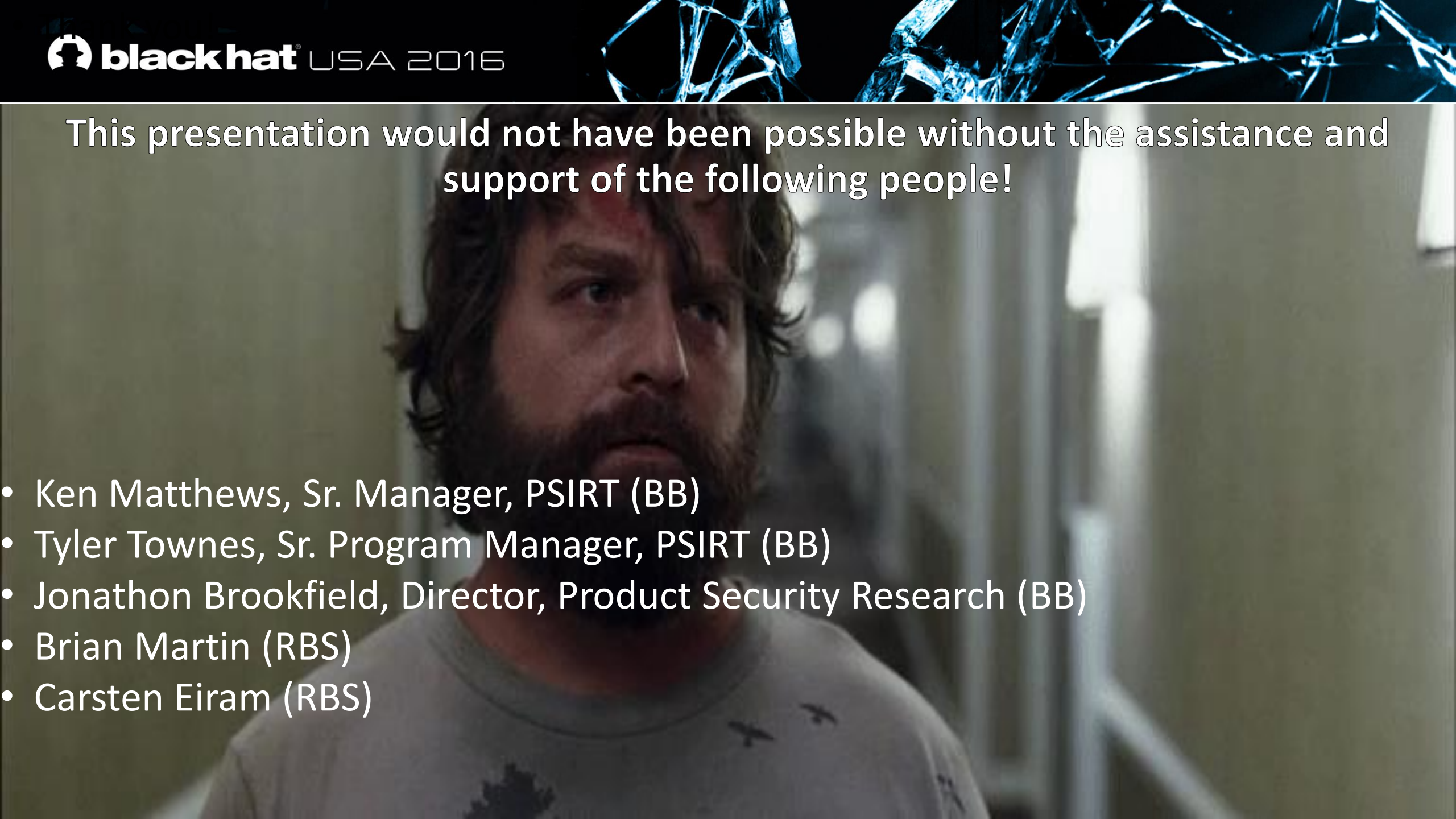
Contents

- Security Communications Statement
- Key Speaking Points
- Written Statement for Customers and Carriers

Level 5 – Using your OSS security intelligence

- **#1 put it in a box – minimize attack surface**
- **Curated OSS product Catalog**
- Developers makes well informed OSS decisions
- Using your own product vuln intel to create smarter products
- Proactive patching
- OSS Blacklisting
- Understand ROI





This presentation would not have been possible without the assistance and support of the following people!

- Ken Matthews, Sr. Manager, PSIRT (BB)
- Tyler Townes, Sr. Program Manager, PSIRT (BB)
- Jonathon Brookfield, Director, Product Security Research (BB)
- Brian Martin (RBS)
- Carsten Eiram (RBS)

OSS Security Maturity: Time To Put On Your Big Boy Pants!

Jake Kouns
CISO
Risk Based Security
@jkouns

Christine Gadsby
Director
Product Security Response
BlackBerry
@christinegadsby

RiskBased SECURITY

BLACKBERRY

JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS