



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

Jake Kouns
CISO
Risk Based Security
@jkouns

Christine Gadsby
Director, Product Security
BlackBerry
@christinegadsby



J U L Y 3 0 - A U G U S T 4 , 2 0 1 6 / M A N D A L A Y B A Y / L A S V E G A S



@jkouns

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



- Director, Product Security
- Cybersecurity Consultant
- SEA to DFW
- Interested in safety critical systems



@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



What
is OSS ?



OPEN

SOURCE

SOFTWARE

ACCESS

FREE

COPYRIGHT

SYSTEM

INNOVATION

CONCEPT

NEW

LICENSE

USING

FORMAT

LAW

PRODUCTS

ECONOMIC

SCIENTIFIC

DEVELOPMENT

ONE

AVAILABLE

MEDIA

CULTURE

INTERNATIONAL

MOVEMENT

COST

COMPANY

RESEARCH

TECHNOLOGY

OPEN-SOURCE

COMPUTER

PROJECTS

MANUFACTURERS

CREATIVE

INTERNET

PUBLIC

ANYONE

ALSO

INFORMATION

NETWORK

SHARING

ECONOMICS

DIGITAL

PHARMACEUTICALS

MESSAGEBOARDS

BLOGS

RAYMOND

INCLUDING

DOWNLOAD

EDIT

COMMONS

ISSN

MODEL

LIKE

OTHERS

FILM

TERMS

IDEA

ERIC

PUBLISHING

EXAMPLES

POLITICAL

SIMILAR

INITIATIVE

ETHICS

DESCRIBE

COMMUNITIES

POTENTIAL

ORIGINAL

SYSTEMS

MADE

COMPANIES

EXAMPLE

TECHNOLOGIES

PRODUCTION

EXPRESS

COSTS

CONTENT

PRODUCT

BUSINESS

PRESS

PDF

BEER

MANY

CALL

HARDWARE

CODE

MOVIE

GOODS

LICENSES

USED

BEGAN

WEB

VOL

LIMITED

LIQUID

AUDIO

BASED

TIME

DATA

RIGHTS

WIKIPEDIA

WITHOUT

WORKS

RICHARD

RESOURCES

CONCEPT

CREATED

NEW

LICENSE

USING

FORMAT

LAW

PRODUCTS

ECONOMIC

SCIENTIFIC

DEVELOPMENT

ONE

AVAILABLE

MEDIA

CULTURE

INTERNATIONAL

MOVEMENT

COST

COMPANY

RESEARCH

TECHNOLOGY

OPEN-SOURCE

COMPUTER

PROJECTS

MANUFACTURERS

CREATIVE

INTERNET

PUBLIC

ANYONE

ALSO

INFORMATION

NETWORK

SHARING

ECONOMICS

DIGITAL

PHARMACEUTICALS

MESSAGEBOARDS

BLOGS

RAYMOND

INCLUDING

DOWNLOAD

EDIT

COMMONS

ISSN

MODEL

LIKE

OTHERS

FILM

TERMS

IDEA

ERIC

PUBLISHING

EXAMPLES

POLITICAL

SIMILAR

INITIATIVE

ETHICS

DESCRIBE

COMMUNITIES

POTENTIAL

ORIGINAL

SYSTEMS

MADE

COMPANIES

EXAMPLE

TECHNOLOGIES

PRODUCTION

EXPRESS

COSTS

CONTENT

PRODUCT

BUSINESS

PRESS

PDF

BEER

MANY

CALL

HARDWARE

CODE

MOVIE

GOODS

LICENSES

USED

BEGAN

WEB

VOL

LIMITED

LIQUID

AUDIO

BASED

TIME

DATA

RIGHTS

WIKIPEDIA

WITHOUT

WORKS

RICHARD

RESOURCES

CONCEPT

CREATED

NEW

LICENSE

USING

FORMAT

LAW

PRODUCTS

ECONOMIC

SCIENTIFIC

DEVELOPMENT

ONE

AVAILABLE

MEDIA

CULTURE

INTERNATIONAL

MOVEMENT

COST

COMPANY

RESEARCH

TECHNOLOGY

OPEN-SOURCE

COMPUTER

PROJECTS

MANUFACTURERS

CREATIVE

INTERNET

PUBLIC

ANYONE

ALSO

INFORMATION

NETWORK

SHARING

ECONOMICS

DIGITAL

PHARMACEUTICALS

MESSAGEBOARDS

BLOGS

RAYMOND

INCLUDING

DOWNLOAD



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

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



2016 Future of Open Source Survey Results

90% of respondents said Open Source Improves:

Interoperability



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.

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

2016 Future of Open Source Survey Results

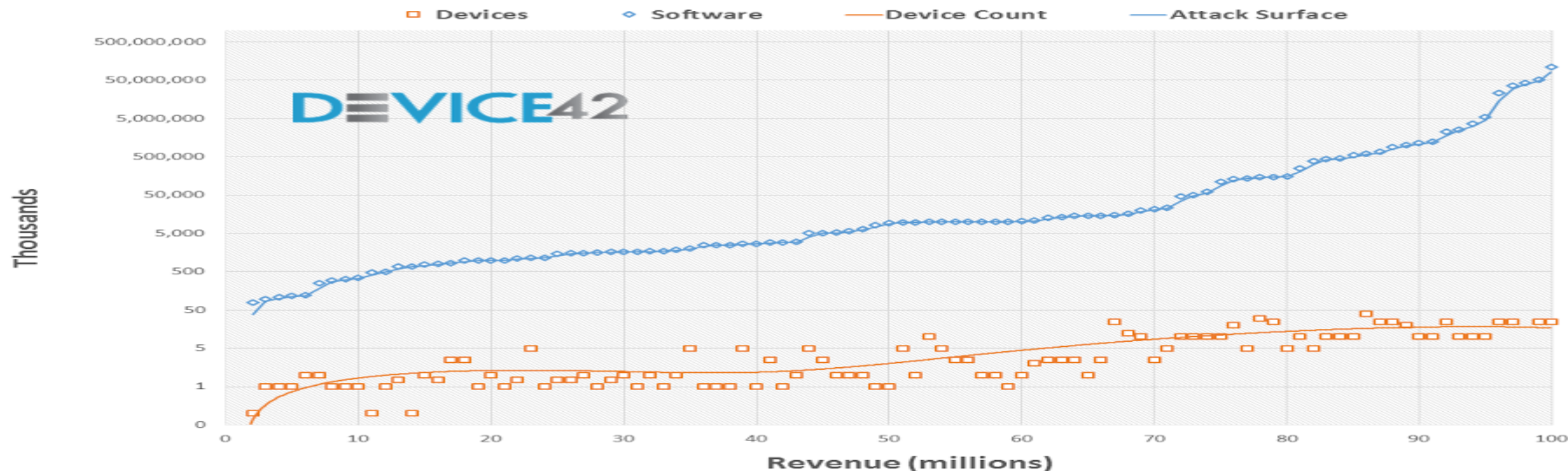
Security and Management:

- 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.

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

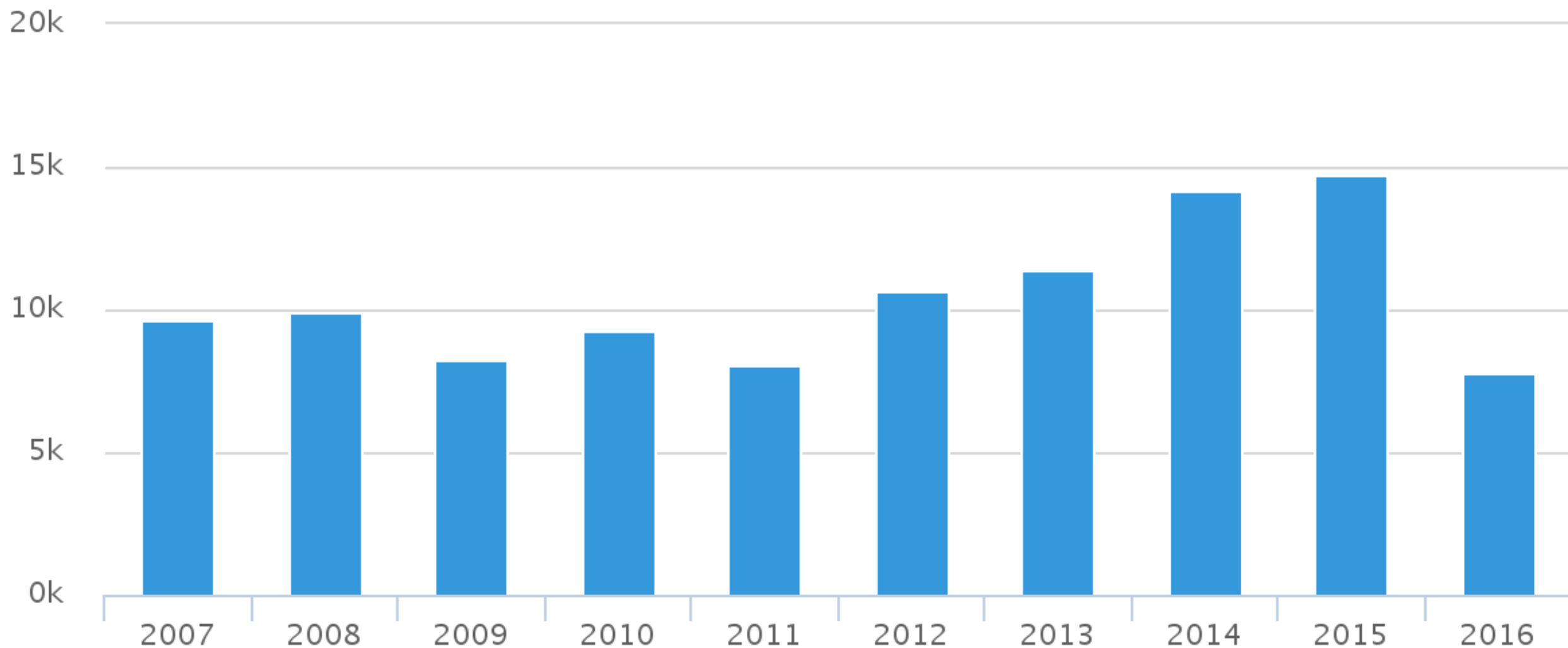


Relative Attack Surface vs. Company Size (Revenue)



- Larger companies (by revenue) have exponentially more servers, more software, and therefore a larger attack surface to manage
- Each server hosts on average 120 pieces of software counting versions as distinct

Vulnerabilities over the last 10 years



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



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!

You Just Mean HeartBleed Right?



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

Stagefright (libstagefright)

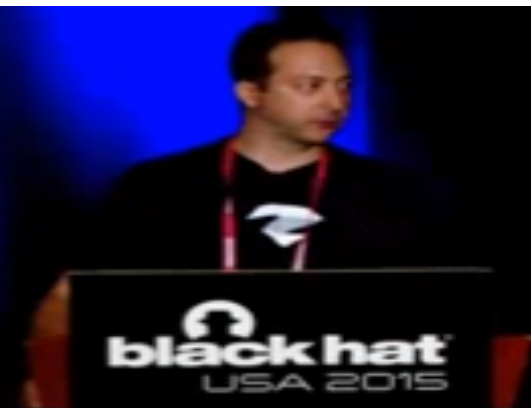
Stagefright: Scary Code in the Heart of Android

Researching Android Multimedia
Framework Security



Joshua "jduck" Drake
August 7th 2015
Black Hat USA

1



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, also seen in other embedded devices as well

MUST READ **WINDOWS 10 FREE UPGRADE IS STILL AVAILABLE USING WINDOWS 7 AND 8 PRODUCT KEYS**

850 million Android devices still at risk of hijack by Stagefright bug

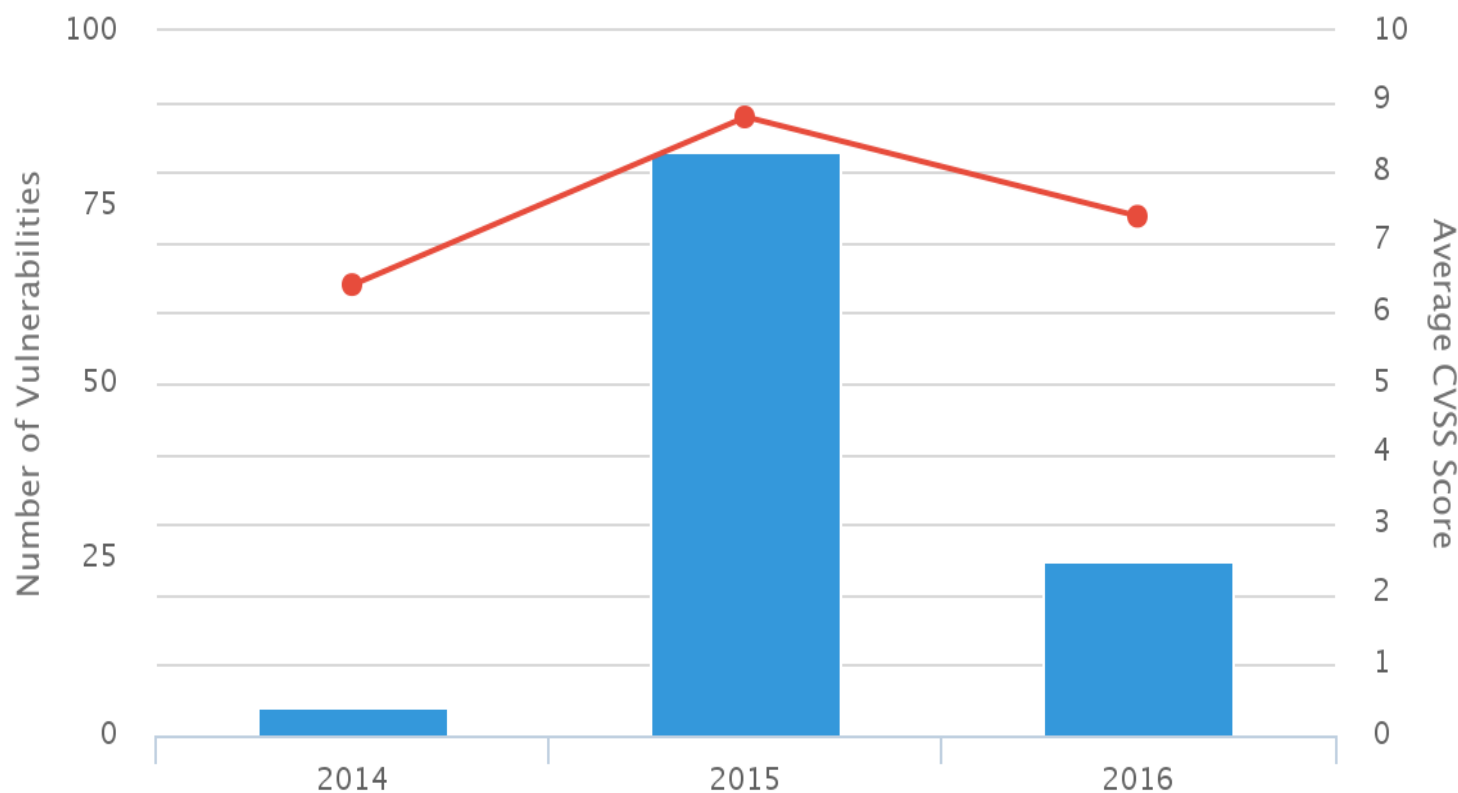
Security researchers say fragmented manner of Android operating system restricts protections against bug.



By [Danny Palmer](#) | March 24, 2016 -- 15:31 GMT (08:31 PDT) | Topic: [Security](#)

Stagefright (libstagefright)

Vulnerabilities and Average CVSS scores over time



Total Vulnerabilities

112



Max CVSS Score

10.0



Average CVSS Score

8.36

Symantec Vulnerabilities



Following

Project Zero

Multiple remote memory corruption vulns in all Symantec Norton antivirus products, including stack buffer overflows. [bugs.chromium.org/p/project-zero/...](https://bugs.chromium.org/p/project-zero/issues/detail?id=100)

News and updates from the Project Zero team at Google

RETWEETS
275

LIKES
171



2:07 PM - 28 Jun 2016



Following

“These vulnerabilities are as bad as it gets.”

How to Compromise the Enterprise Endpoint

Symantec is a popular vendor in the enterprise security market, their flagship product is [Symantec Endpoint Protection](#). They sell various products using the same core engine in several markets, including a consumer version under the [Norton](#) brand.

Today we're publishing details of multiple critical vulnerabilities that we discovered, including many wormable remote code execution flaws.

These vulnerabilities are as bad as it gets. They don't require any user interaction, they affect the default configuration, and the software runs at the highest privilege levels possible. In certain cases on Windows, vulnerable code is even loaded into the kernel, resulting in remote kernel memory corruption.

Another round of testing, more new Symantec bugs. Another report on the way. [#antivirus](#)

RETWEETS
105

LIKES
128



3:20 PM - 30 Jun 2016

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

P1

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

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.

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 a 3rd Party Library vulnerability!

VulnDB ID: 140642

⚡ libmspack Multiple Unspecified Memory Corruption Arbitrary Code Execution

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.

“...but 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.

**IF YOU COULD JUST PUT
YOUR BIG BOY PANTS
ON**

**THAT WOULD BE
GREAT**

Liability – FTC Expanding Role

The FTC's expanding cybersecurity influence



By *Dan Verton*

SEPTEMBER 16, 2014 1:30 PM

BIO ▼

The answer to who is in charge of the federal effort to bolster the nation's cybersecurity posture may not be as difficult to uncover as previously thought. As the Department of Homeland Security awaits public comments on its voluntary framework initiative—due Oct. 10—the Federal Trade Commission has been making an aggressive push to expand its authorities and force companies that have lax security programs to bolster their defenses.

To be fair, the DHS-backed program, known as the Framework for Improving Critical Infrastructure Cybersecurity and developed by the National Institute of Standards and Technology with extensive input from the private sector, is only seven months old. But despite more than a year of development work and meetings around the country, nobody is really sure yet how many private sector firms have adopted the voluntary standards or what impact the standards have had on the nation's

Liability - TRENDnet



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

[Contact](#) | [Stay C](#)

[ABOUT THE FTC](#)

[NEWS & EVENTS](#)

[ENFORCEMENT](#)

[POLICY](#)

[TIPS & ADVICE](#)

[News & Events](#) » [Press Releases](#) » [FTC Approves Final Order Settling Charges Against TRENDnet, Inc.](#)

FTC Approves Final Order Settling Charges Against TRENDnet, Inc.

FOR YOUR INFORMATION

February 7, 2014

TAGS: [Bureau of Consumer Protection](#) | [Consumer Protection](#) | [Privacy and Security](#) | [Data Security](#)

Following a public comment period, the Federal Trade Commission has approved a final order settling charges that electronics company TRENDnet, Inc.'s lax security practices led to the exposure of the private lives of hundreds of consumers on the internet for public viewing.

The FTC's complaint alleged that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring, and claimed in numerous product descriptions that they were "secure." In fact, the cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address.

Liability – FTC “concerned”

FTC concerned over weak consumer provisions in automotive cybersecurity rules



By [Steve Brachmann](#)
October 27, 2015

 [Print Article](#)  0



Twitter



Facebook 8



LinkedIn 7



Google+



Email



More



A rush of high tech components which are being incorporated into the coming generations of automobiles has been a major coverage area of focus this year on IPWatchdog ever since [the advent of the autonomous vehicle was heralded at this year's Consumer Electronics Show](#). Self-driving tech is by no means the sole research and development focus of the auto industry,

where [a dramatic increase in patenting activity underscores widespread innovations](#) in heads-up displays, telematics units and more. Much of this development is fueled by the growing [Internet of Things \(IoT\)](#) sector and the incorporation of wirelessly connecting information technologies into all objects, including cars.

Liability - ASUS



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

[Contact](#) | [Stay Co](#)

[ABOUT THE FTC](#)

[NEWS & EVENTS](#)

[ENFORCEMENT](#)

[POLICY](#)

[TIPS & ADVICE](#)

[News & Events](#) » [Press Releases](#) » [ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers](#)

ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk

FOR RELEASE

February 23, 2016

TAGS: [deceptive/misleading conduct](#) | [Technology](#) | [Bureau of Consumer Protection](#) | [Consumer Protection](#) | [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#)

Taiwan-based computer hardware maker ASUSTeK Computer, Inc. has agreed to settle Federal Trade Commission charges that critical security flaws in its routers put the home networks of hundreds of thousands of consumers at risk. The administrative complaint also charges that the routers' insecure "cloud" services led to the compromise of thousands of consumers' connected storage devices, exposing their sensitive personal information on the internet.

The proposed consent order will require ASUS to establish and maintain a comprehensive security program subject to independent audits for the next 20 years.

Liability - FTC

THE WALL STREET JOURNAL.

[Home](#) [World](#) [U.S.](#) [Politics](#) [Economy](#) **[Business](#)** [Tech](#) [Markets](#) [Opinion](#) [Arts](#) [Lifestyle](#)



Uber's
Capitulation to Didi
Illustrates Hard Road
in China



Elon Musk's
Tesla, SolarCity to
Merge in \$2.6 Billion
Deal



Coal Glut,
Environmental
Pushback Derail
Coast Port Plans

LAW BLOG

FTC Hands Itself Data-Security Win

By **BRENT KENDALL**

Jul 29, 2016 12:59 pm ET

 0 COMMENTS

The Federal Trade Commission Friday overturned an in-house judge's ruling that had handed the agency a notable loss in its efforts to target some companies' allegedly weak protections for computerized consumer information.

The FTC's move sets up a high-stakes federal court battle with LabMD, a former medical testing company that the commission accused of failing to provide reasonable or appropriate cybersecurity protections for patient data.



Liability

“FTC has increased

Reed Smith LLP

maximum fine from \$16,000

On June 2, 2015, the FTC announced that it had increased the civil penalties for violations of Section 5 of the FTC Act.

which prohibits unfair and

deceptive acts or practices.

the FTC Act.



**Where
Are
My
Pants?**

Software Liability vs Product Liability

- It's not software that hurts the people, it's a component of a larger finished product, making it a product failure not just the software.
- ***MacPherson v. Buick Motor Co.***, 217 N.Y. 382, 111 N.E. 1050 (1916)
 - Donald C. MacPherson was injured when one of the wooden wheels of his 1909 "Buick Runabout" collapsed
 - Buick Motor Company, had manufactured the vehicle, but not the wheel, which had been manufactured by another party but installed by defendant.
- Software responsibility is going to be on final goods manufacturer (no matter what) that is delivering the final product
- If you use 3rd Party Code in your product, you are responsible for the security of it as well!

Software Liability



Software Liability?: The Worst Possible Idea (Except for all Others)

Jake Kouns

Chief Information Security Officer
Risk Based Security
@jkouns

Joshua Corman

CTO
Sonatype
@joshcorman



0:19 / 1:01:19



#RSAC

@RSAConference



Webcast: Software Liability?: The Worst Possible
Idea (Except for all Others)

<https://www.youtube.com/watch?v=PsHgaJZVkDw>

Clear Need To Manage OSS and 3rd Party Code

- “Whack A Mole” fixing of vulnerabilities is critical, not just in your own code!
- How will you be notified of new issues?
- Why does the cadence of release cycle matter?
 - Too few? Leaves you open to risks, compromise and liability
 - Too many? Huge cost of ownership and potentially not possible
 - Need the porridge to be JUST right and prefer secure coding from the beginning



Clear Need To Evaluate OSS and 3rd Party Code

- Based on the issues, companies should evaluate OSS prior to usage!
- Companies need to determine if they think the project is mature enough to rely on
- Is the project End of Life? Or still seeing regular updates?
- Determine if there are known vulnerabilities that are not fixed
- Determine the true Cost of Ownership
 - Initial free usage looks amazing
 - But are they hidden costs to maintain that are not factored in properly?

How To Evaluate OSS and 3rd Party Code

- Evaluate The Viability Of A Project
 - Sponsorship? Risk that the project/code get abandoned?
- Evaluate The Health of the project
 - # of contributors , # of updates, size of code base, etc.
- Determine Support Options
- Do they publish security advisories?
- Do they have a contact person/vehicle for security reports?
- Vulnerability Timeline Metrics can help!
 - How long does it take for researchers to get a response?
 - How long does it take to provide a patch?

SO WHAT?

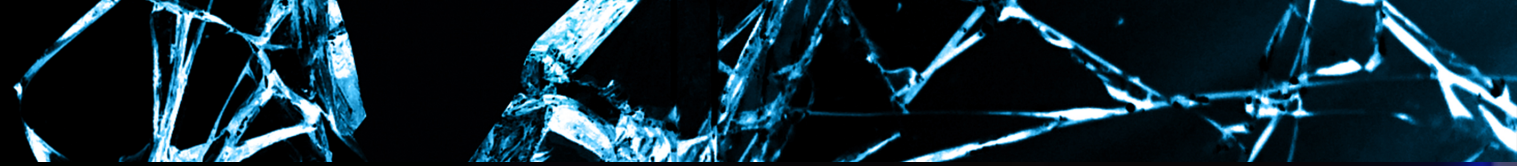


EPIDEMIOLOGY OF SOFTWARE VULNERABILITIES: A STUDY OF ATTACK SURFACE SPREAD

Kymberlee Price
@Kym_Possible
Director of Strategic Operations
Synack

Jake Kouns
@jkouns
CISO
Risk Based Security





Stranger Danger! What Is The Risk From 3rd Party Libraries?



Jake Kouns
CISO
Risk Based Security
@jkouns



Kymberlee Price
Senior Director of Researcher Operations
Bugcrowd
@Kym_Possible



WELL THEN

**SOMEONE IS WEARING HER BIG GIRL
PANTS**



OSS Security Management At Black Berry

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





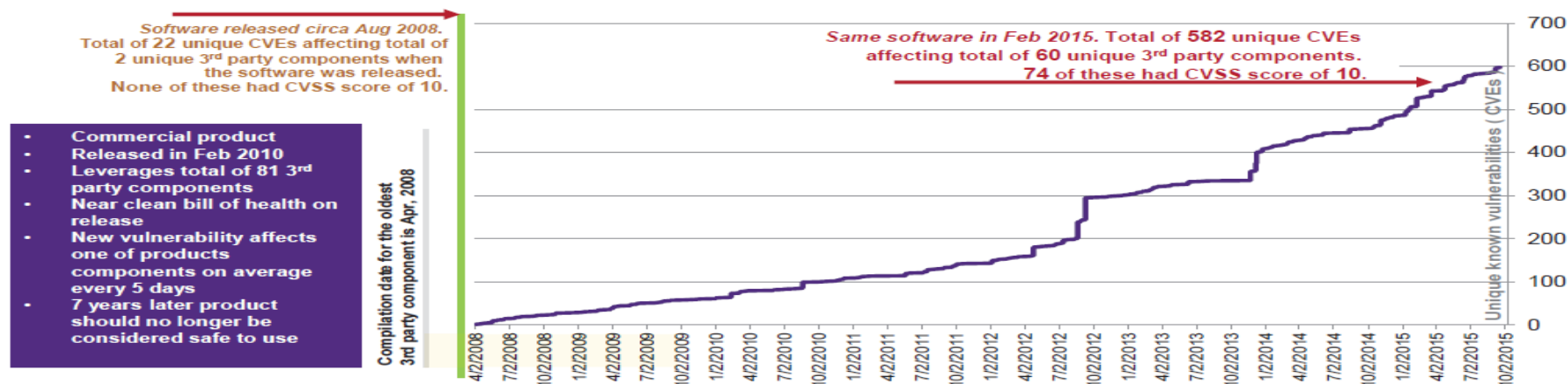


Fun BlackBerry OSS facts

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

Why?

Software 'decays' over time without patches



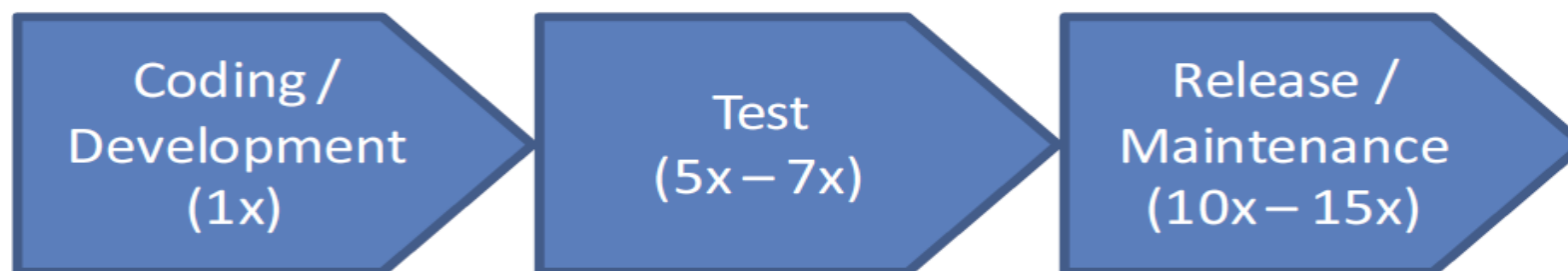
Challenge: Many products are delivered with unpatched, known vulnerabilities

© 2016 Synopsys, Inc.

SVNOPSYS™

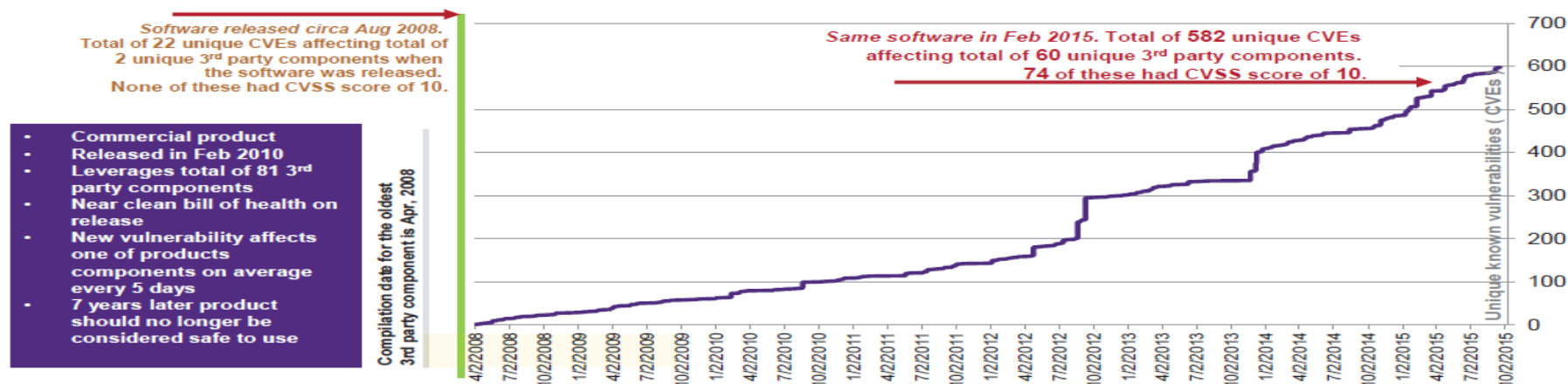
Figure 2

SDL Relative Costs Of Remediating Security Vulnerabilities²



Why?

Software 'decays' over time without patches



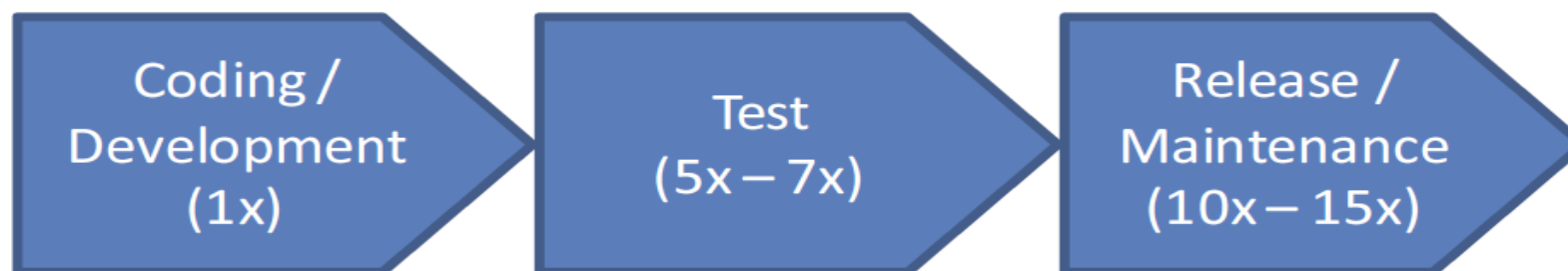
Challenge: Many products are delivered with unpatched, known vulnerabilities

© 2016 Synopsys, Inc.

SYNOPSYS

Figure 2

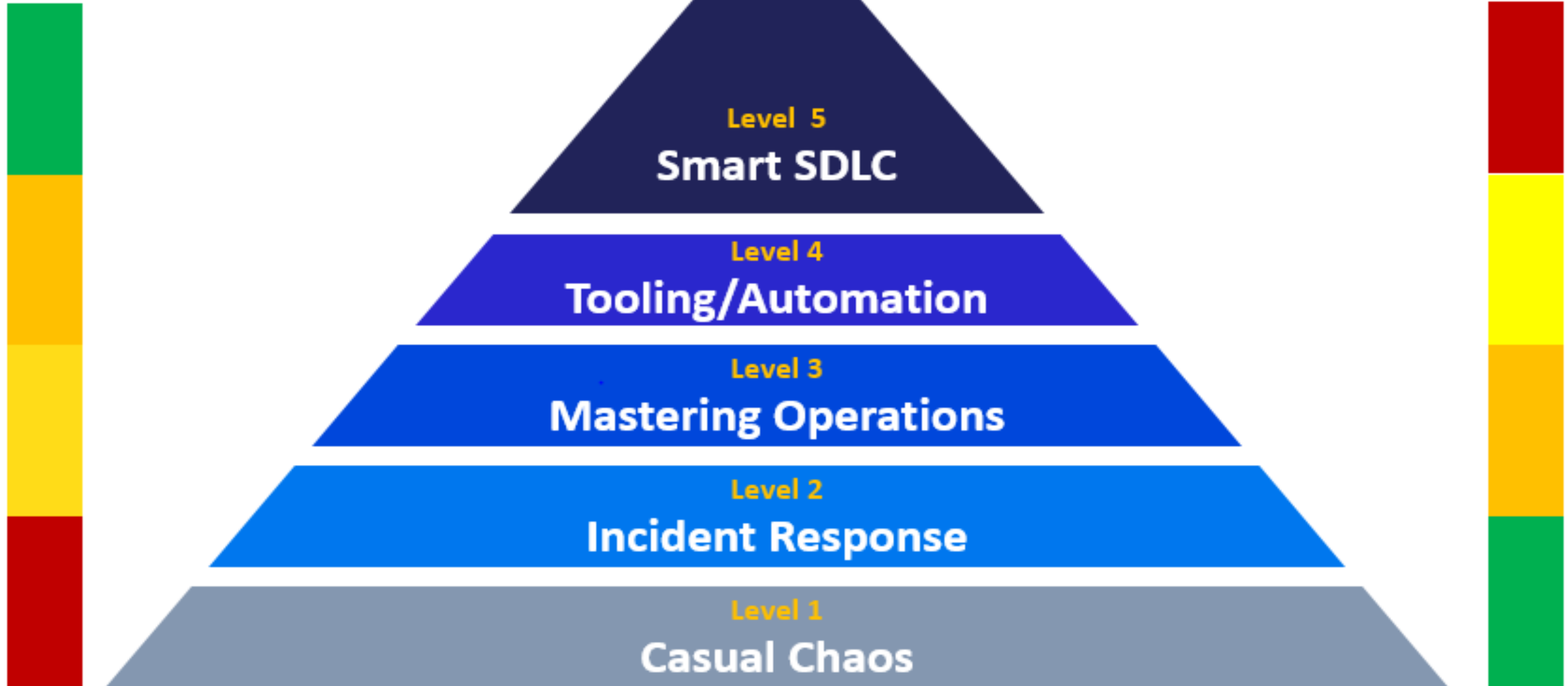
SDL Relative Costs Of Remediating Security Vulnerabilities²



BlackBerry's Open Source Software
Maturity Model

Risk

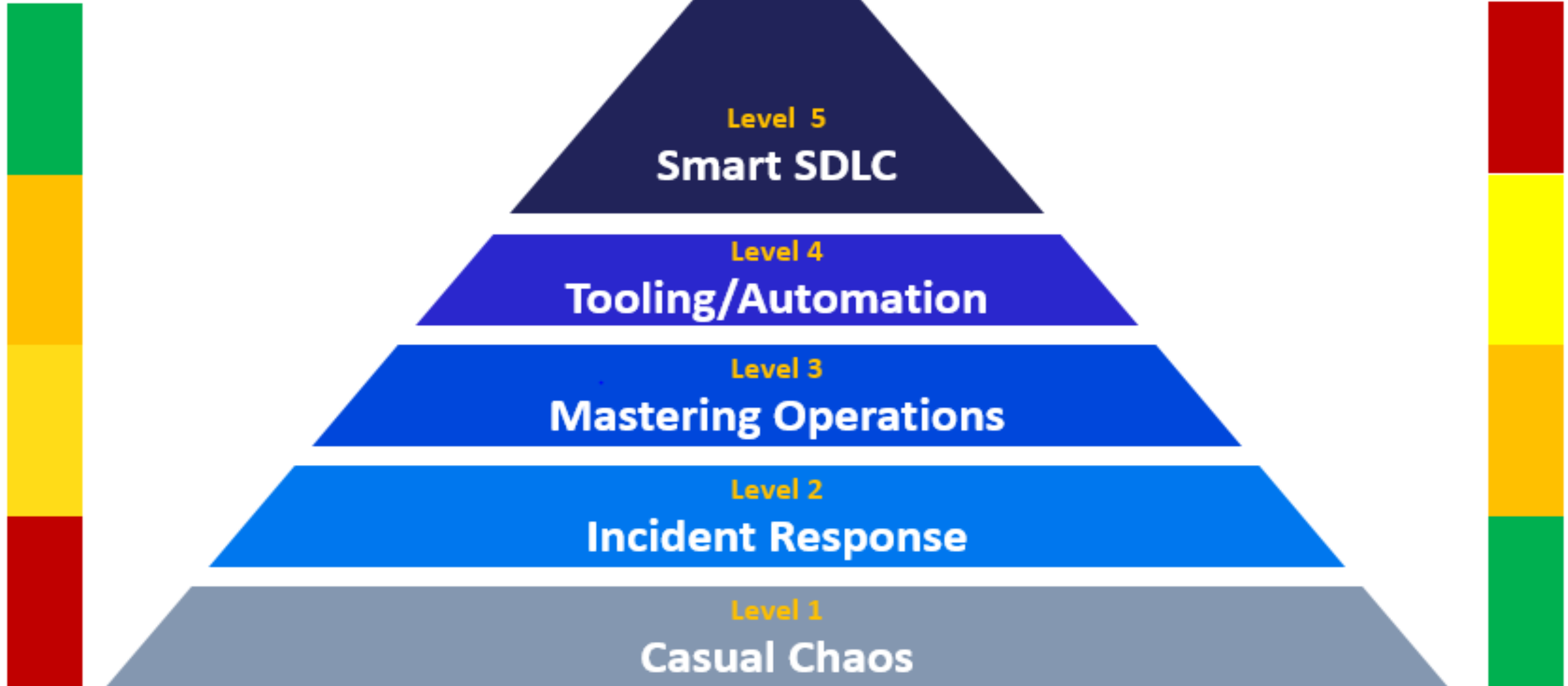
Cost



BlackBerry's Open Source Software
Maturity Model

Risk

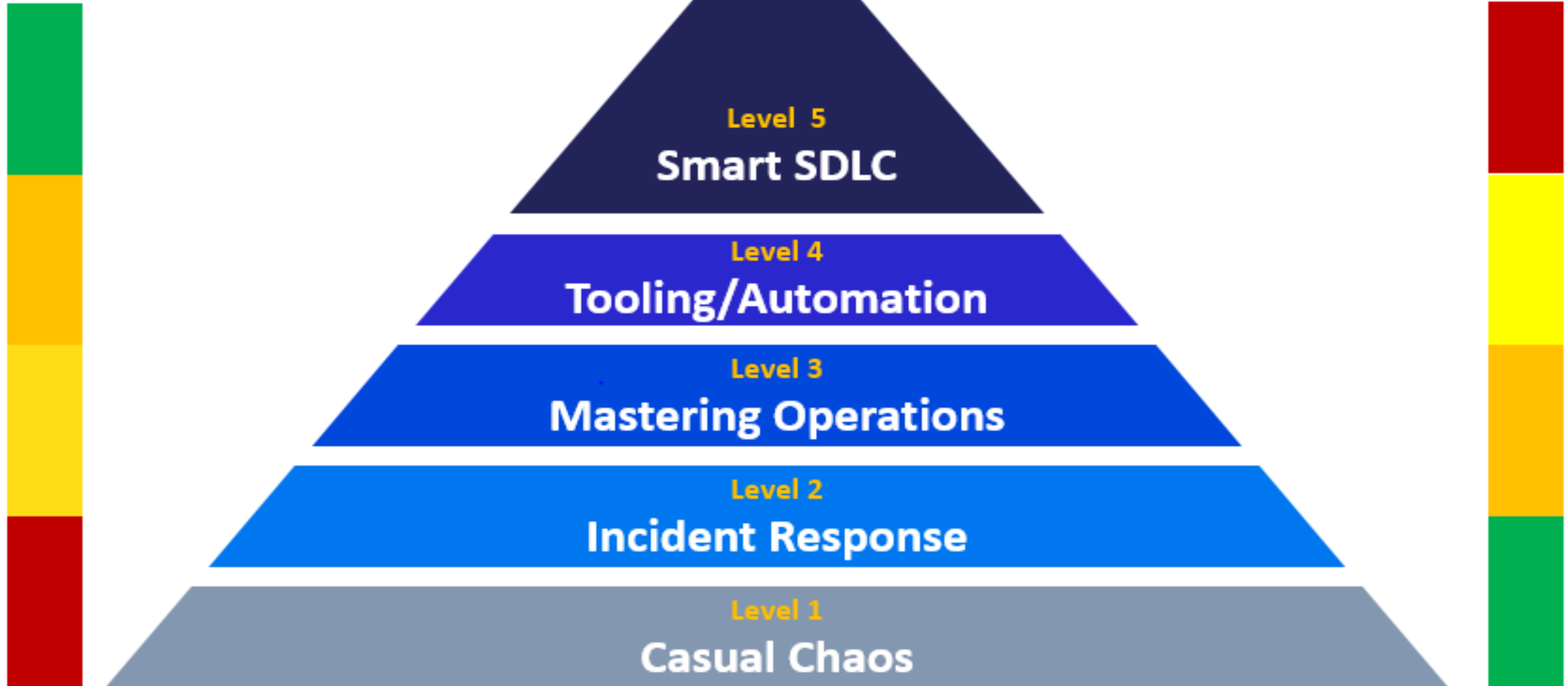
Cost



BlackBerry's Open Source Software
Maturity Model

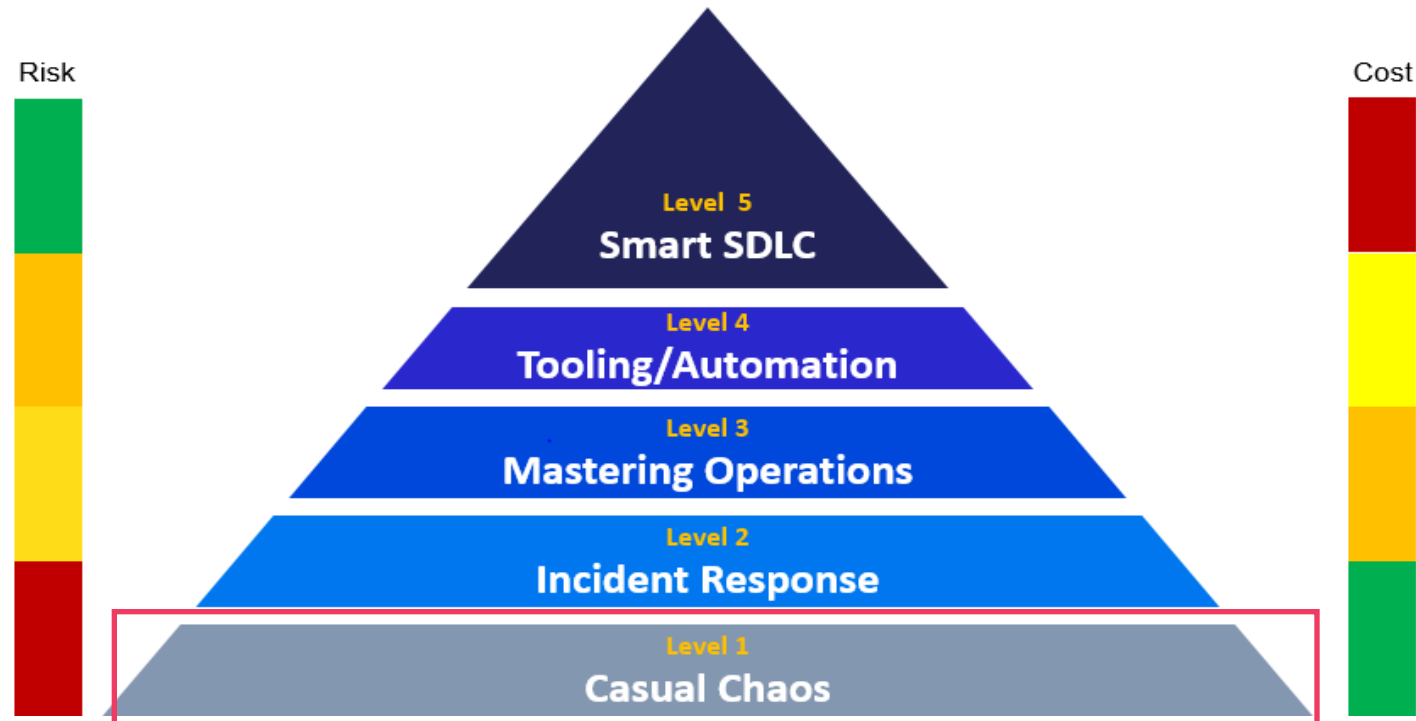
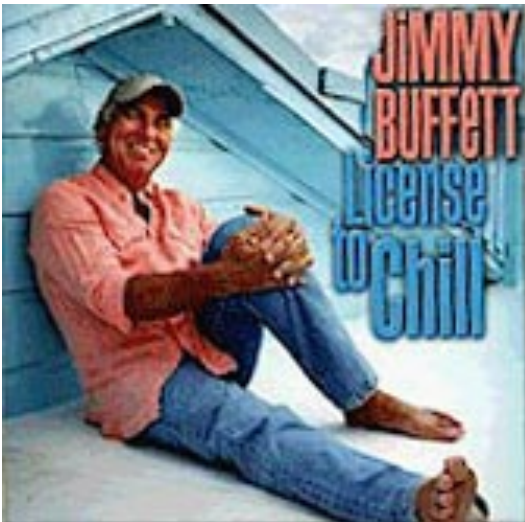
Risk

Cost



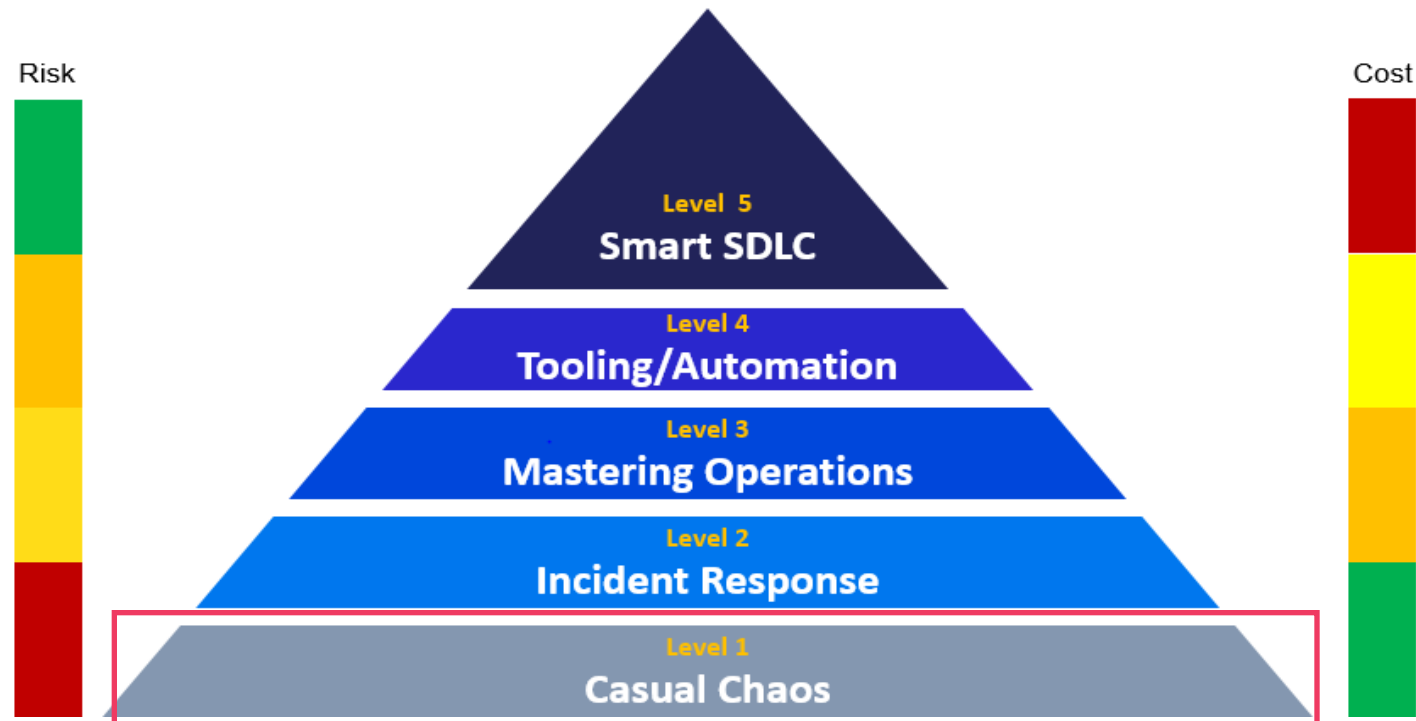
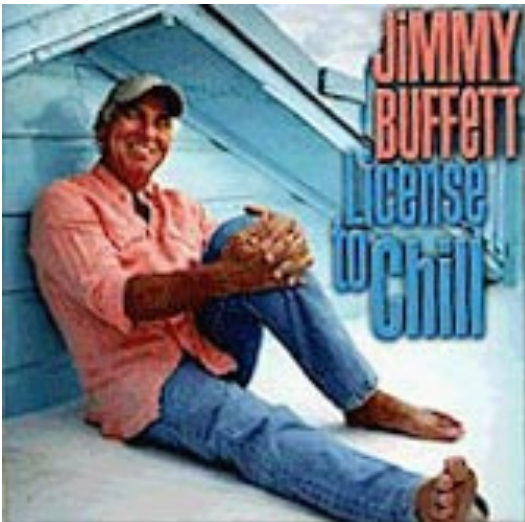
Level 1 – Casual Chaos

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



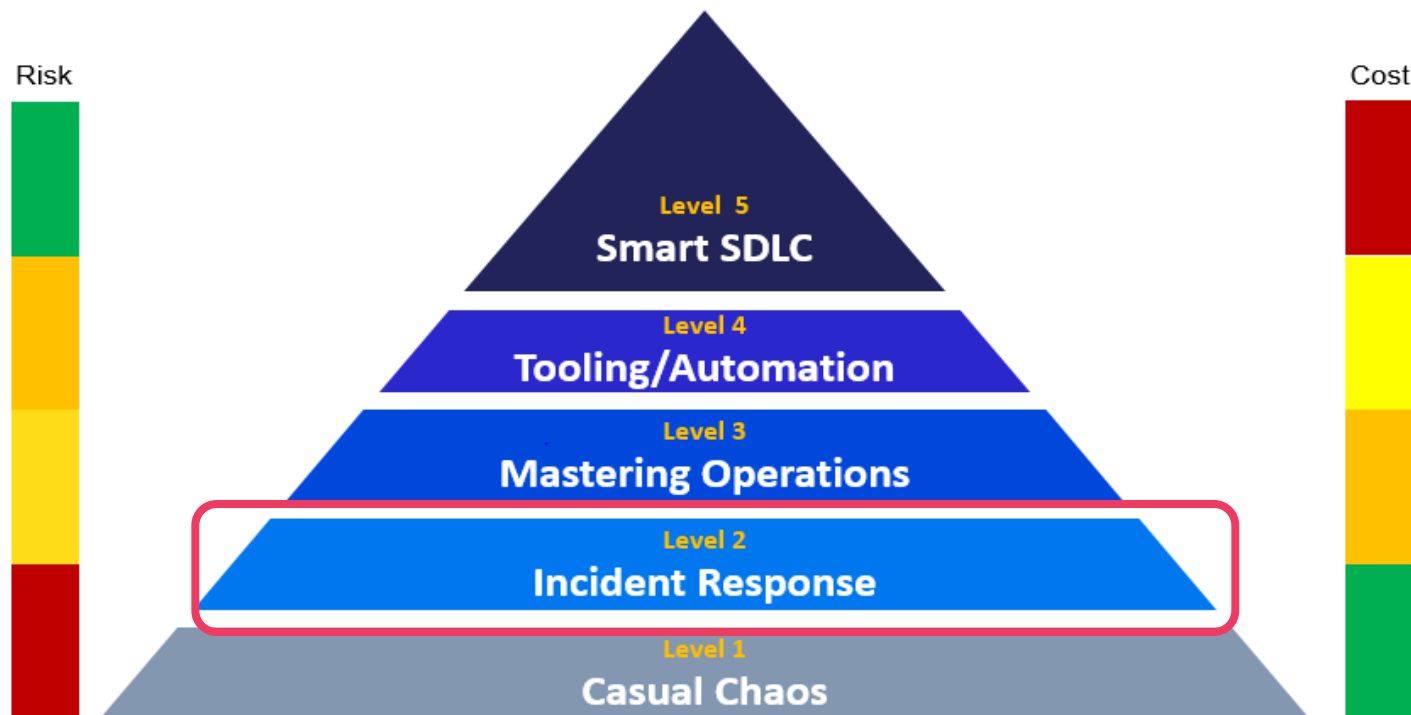
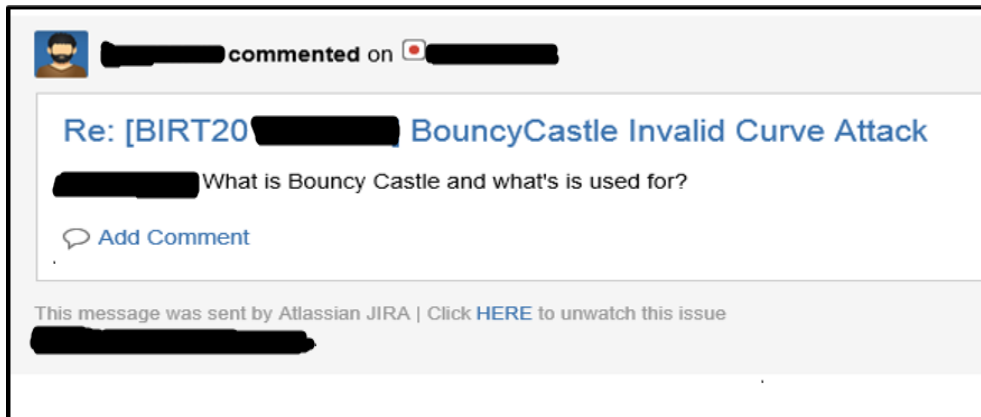
Level 1 – Casual Chaos

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



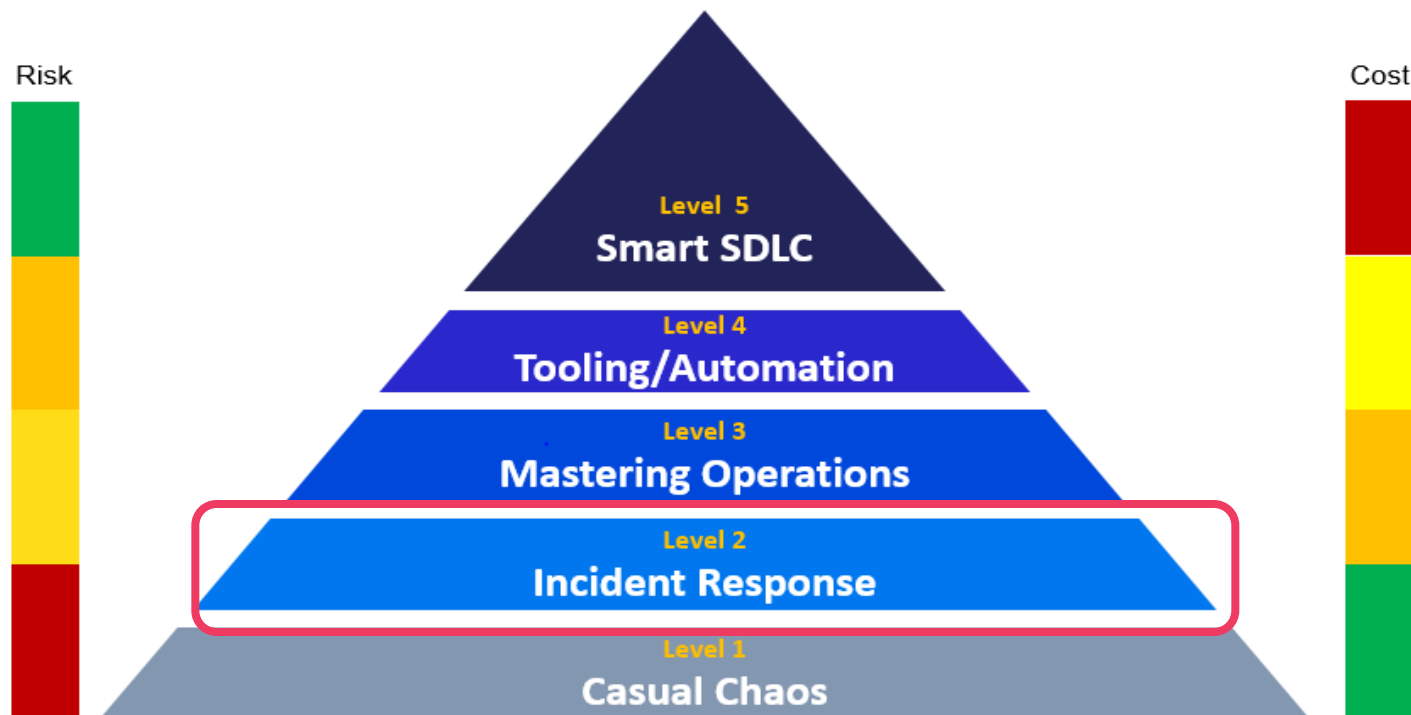
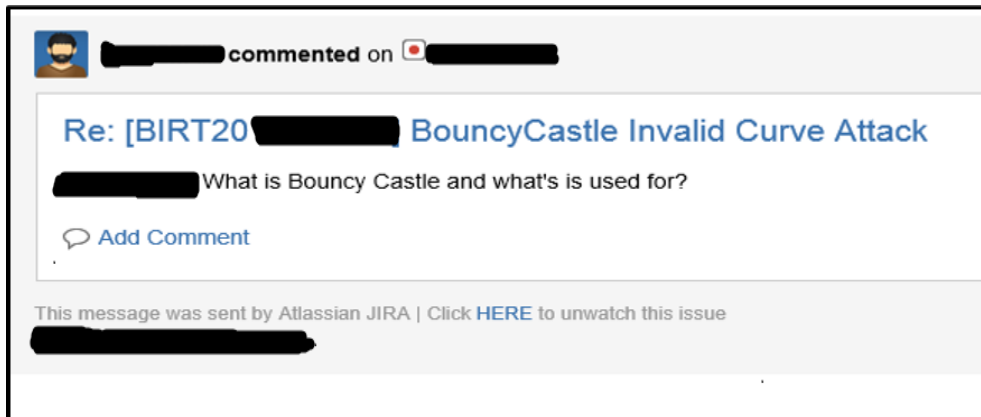
Level 2 – Incident Response is born

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



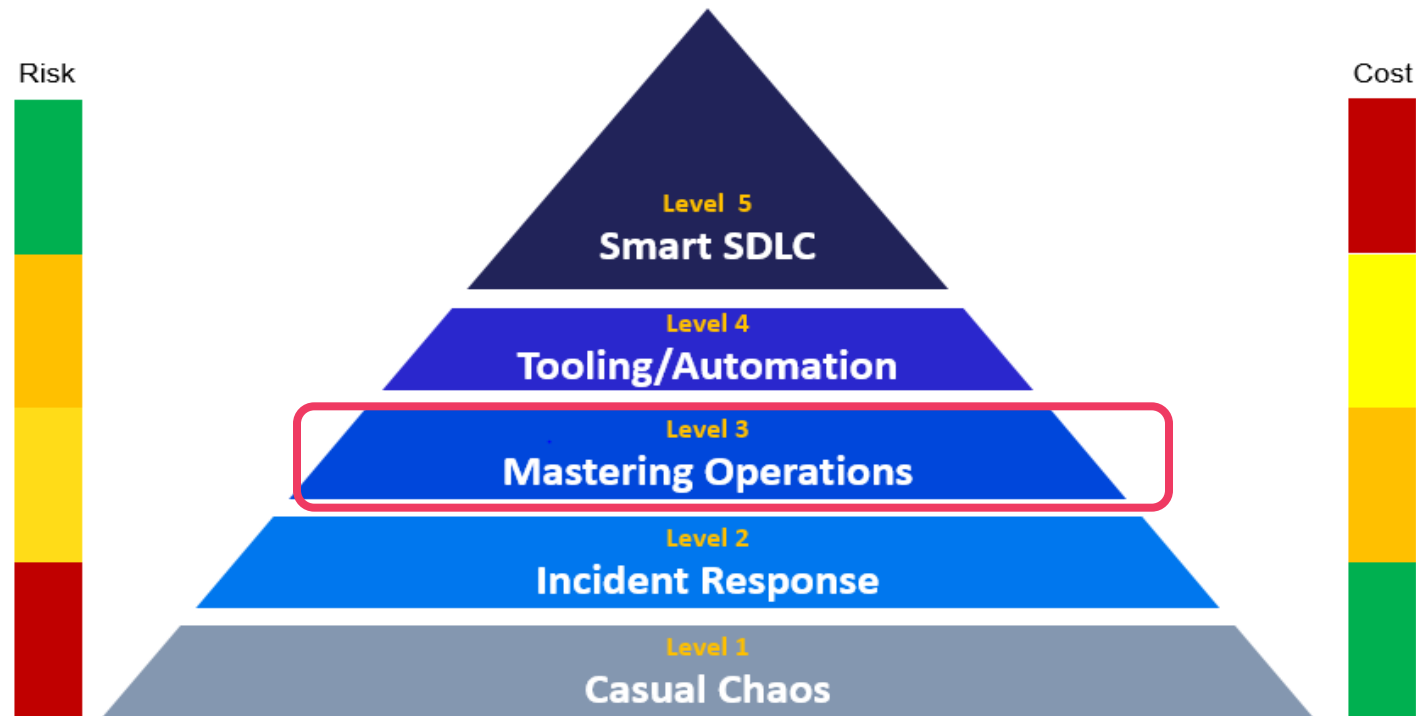
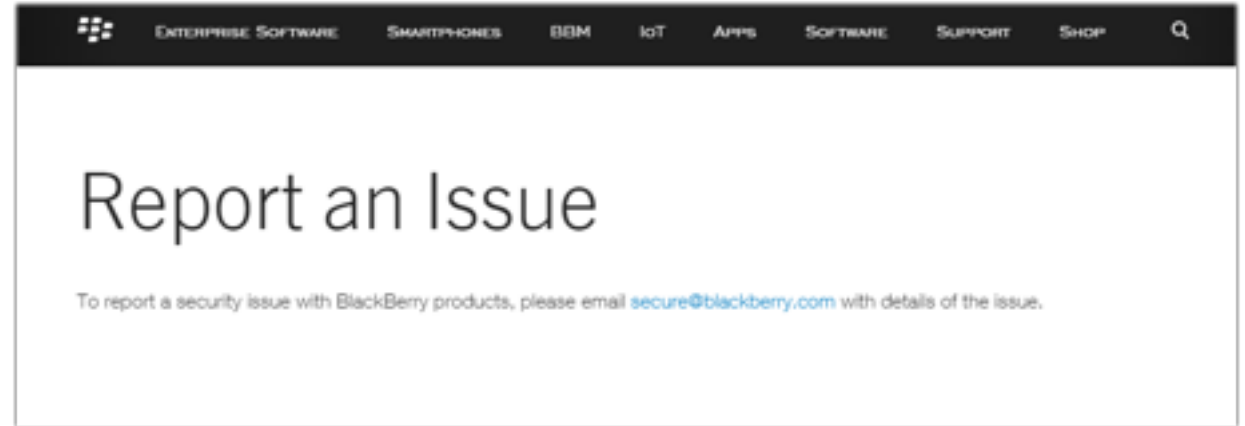
Level 2 – Incident Response is born

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



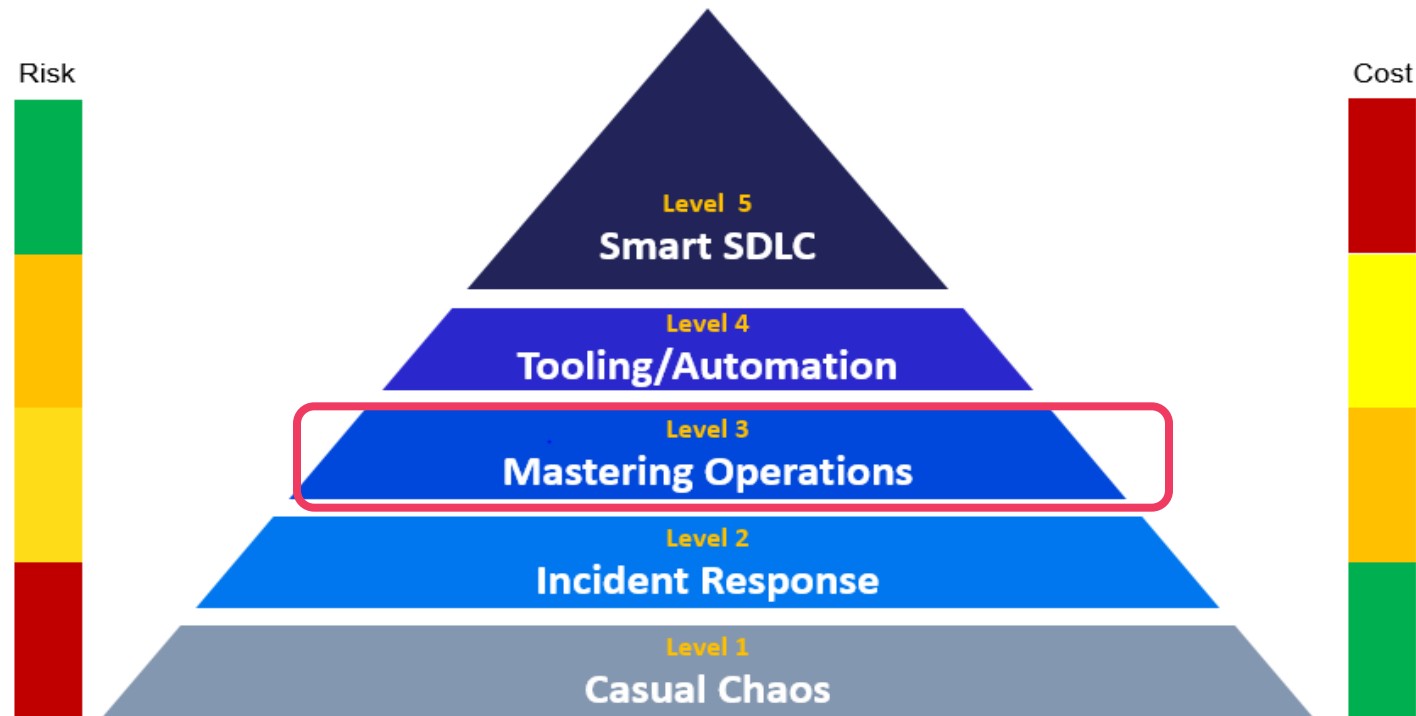
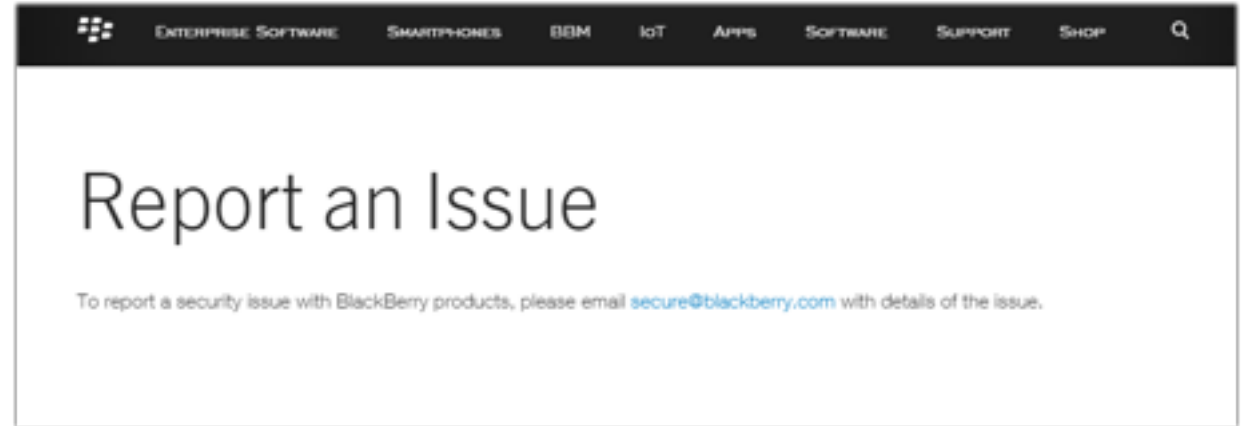
Level 3 – Mastering Ops

- 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



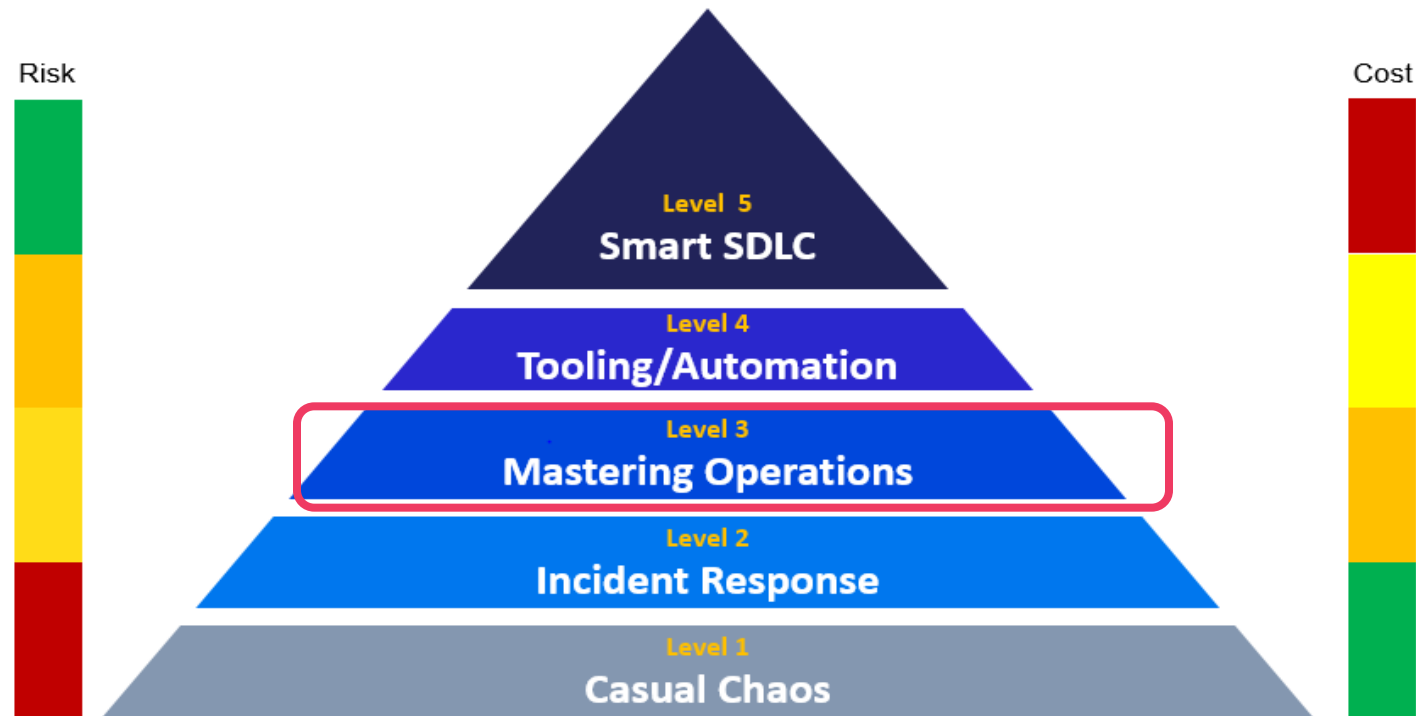
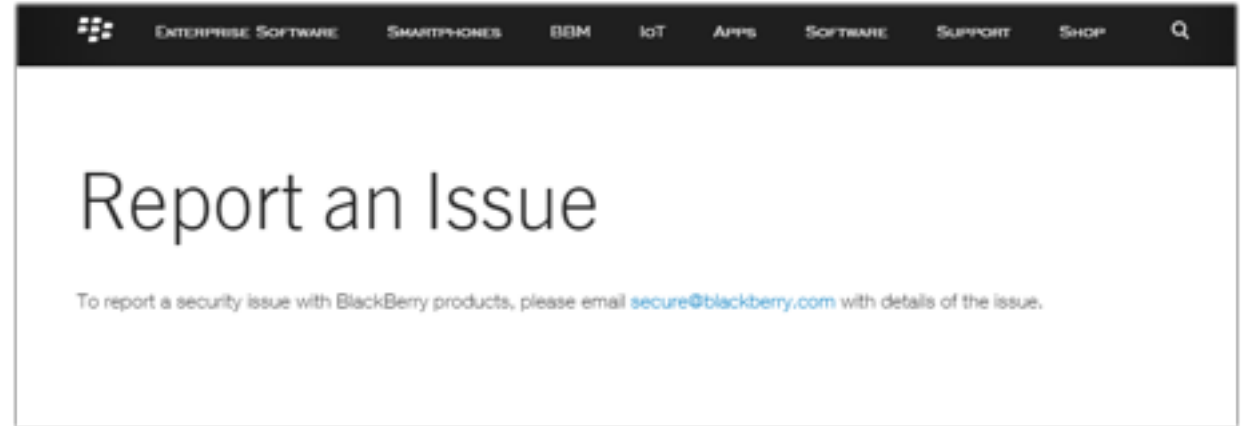
Level 3 – Mastering Ops

- 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



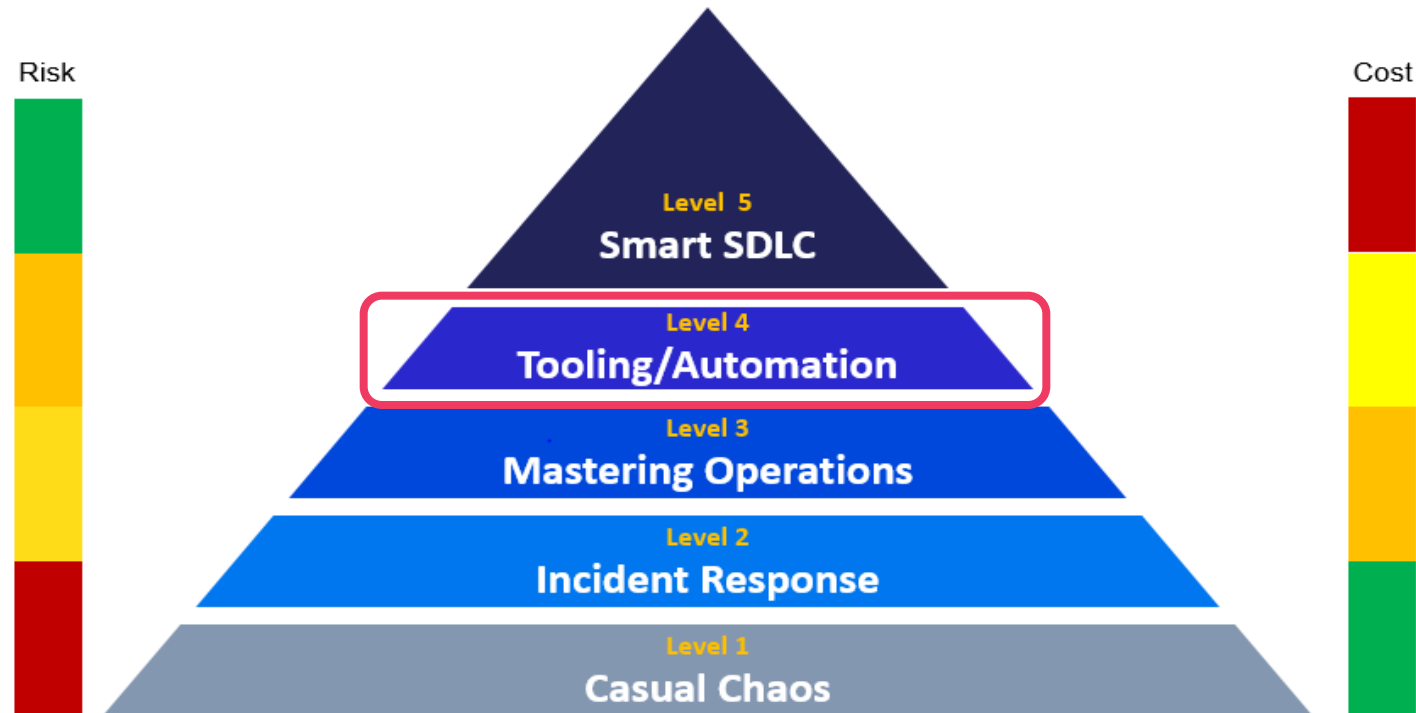
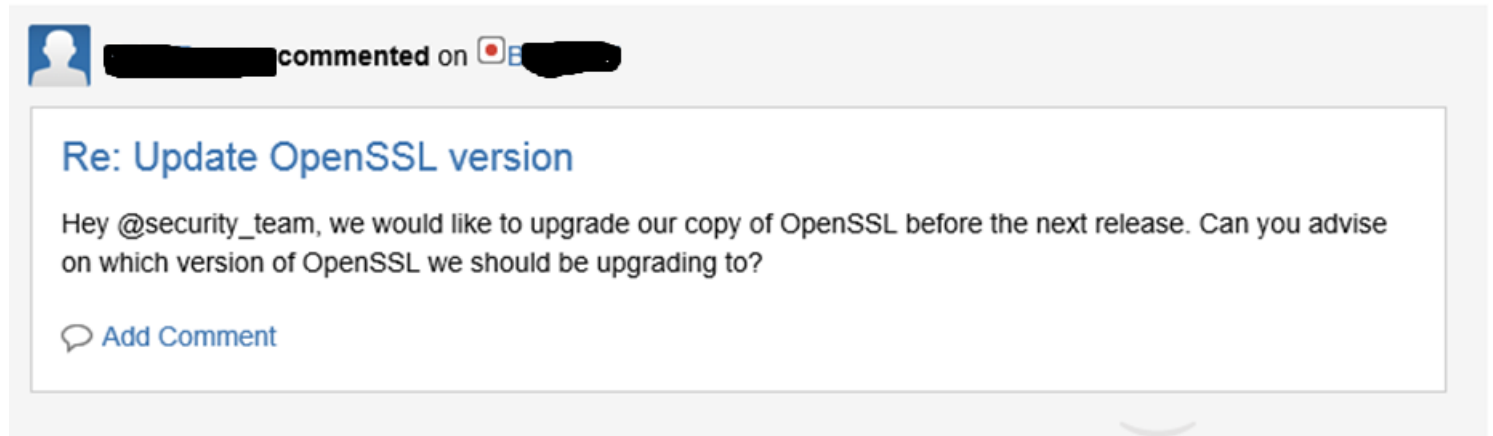
Level 3 – Mastering Ops

- 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



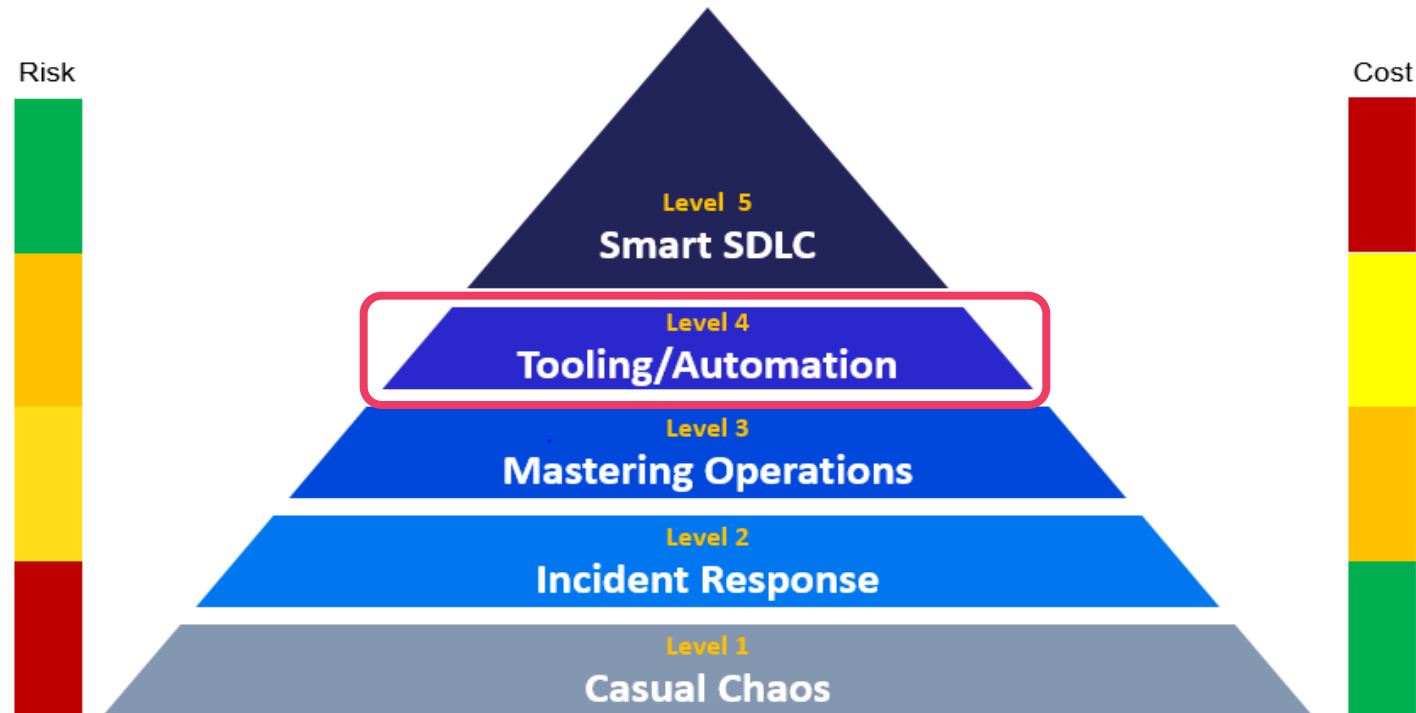
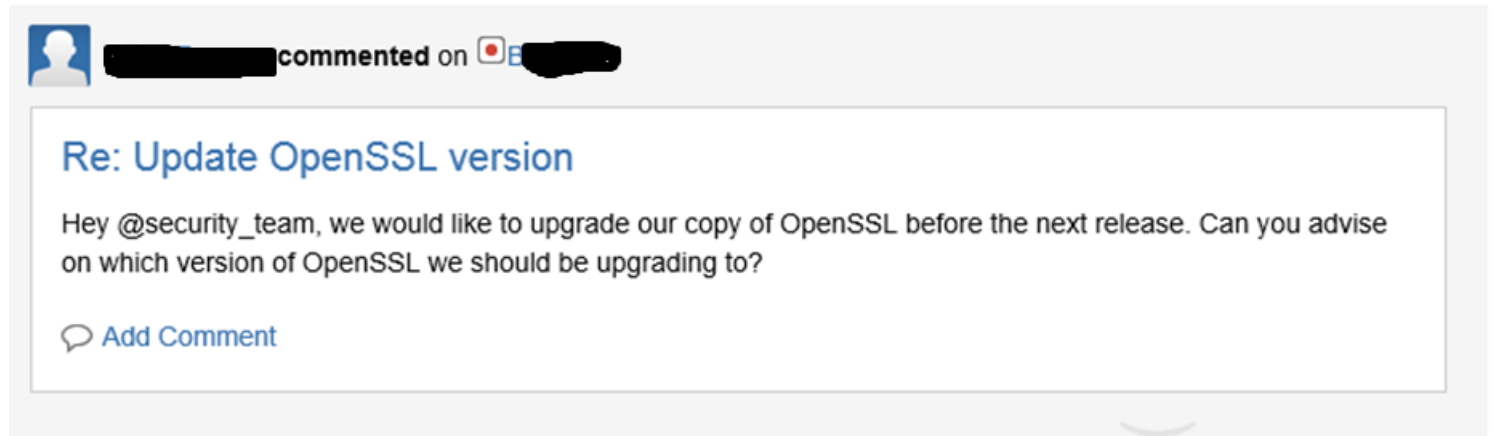
Level 4 – Tools

- 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



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 Catalog

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

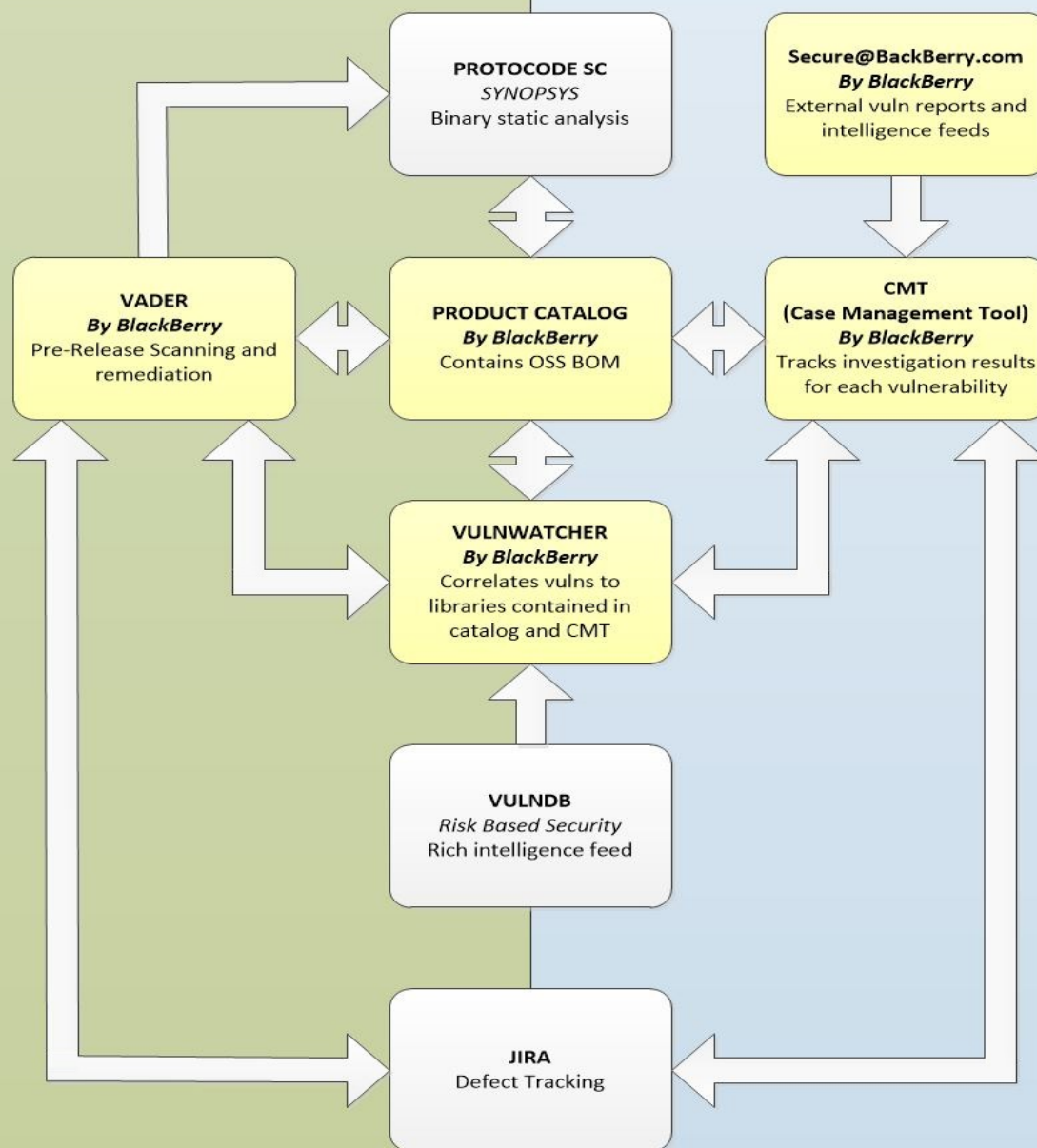
CMT – Case Management Tool

- 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

DEVELOPMENT



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

IN-MARKET

BlackBerry Custom Tooling

VADER – Pre-release Products

- Protecode-SC scan returns BOM and known vulns
- Automated defect creation

Product Catalog

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

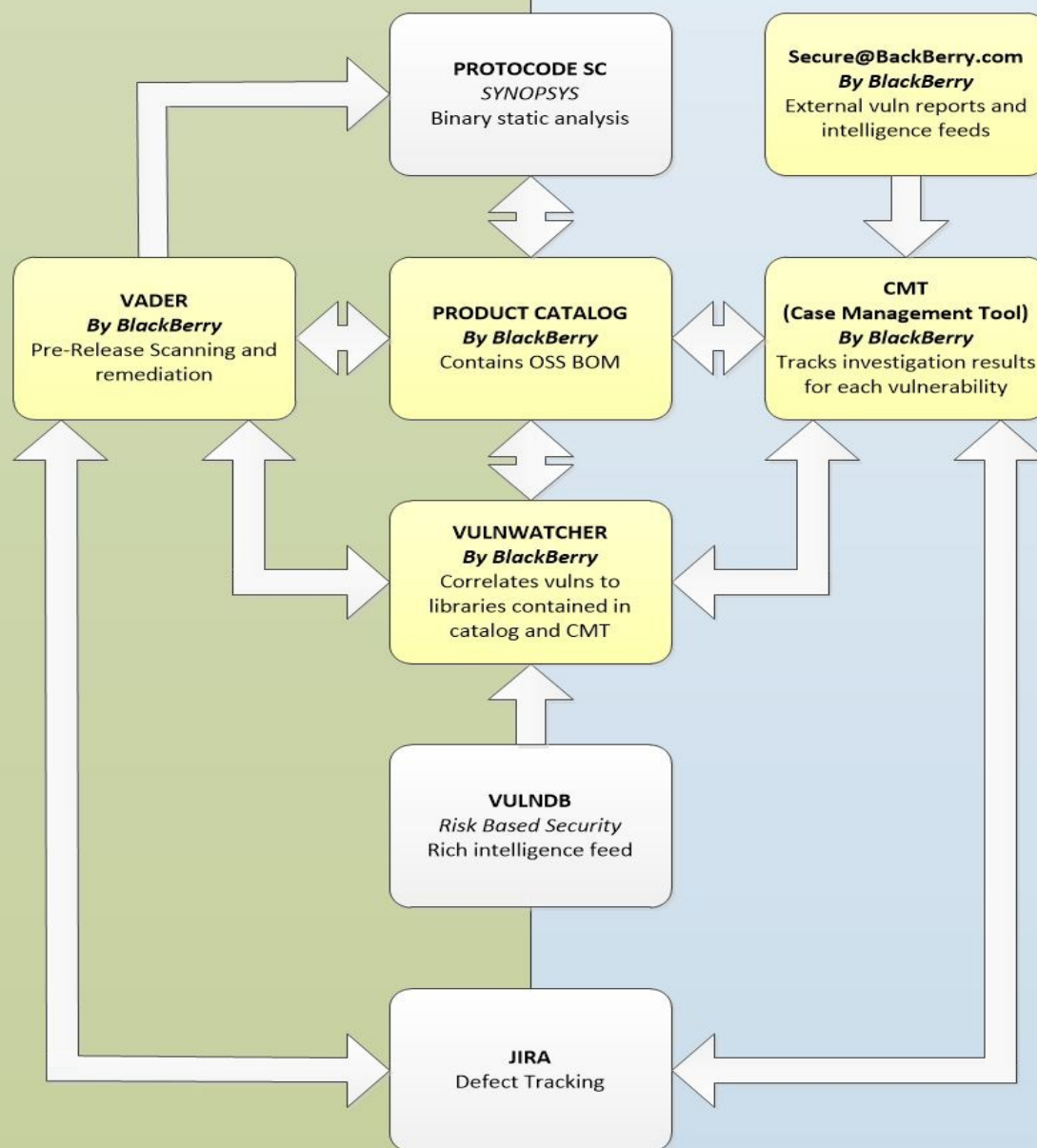
CMT – Case Management Tool

- 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

DEVELOPMENT



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

IN-MARKET

OpenSSL 'Freak'

BBSIRT Case Management Tool

Home

Investigations

Release

Tasks

Admin

Search:

Log Out

Scan Details

Name

lbry_qc8992_sf-user-product

Build Number

A4D444

Current

Yes

Library Name	Version Name	Reported Version					
7zip							
Reference Name	Reference Path	Full Path	JIRA Component	Component	False Positive	Over	Cu
7zip_4_57.exe	/autolader/7zip_4_57.exe	/autolader/7zip_4_57.exe	27874	0.5398230088495575	True		No
achartengine							
Reference Name	Reference Path	Full Path	JIRA Component				
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_att_img/android-sparse.oem_att_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_att_img/android-sparse.oem_att_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_att_img/android-sparse.oem_att_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	transform	transform	transform	transform	transform
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	COREQS-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	COREQS-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	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							

\$214

\$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
Go - Android	1.0.0.1838
	6.6.0
	794 0 0 14

BlackBerry Security Communications Release

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

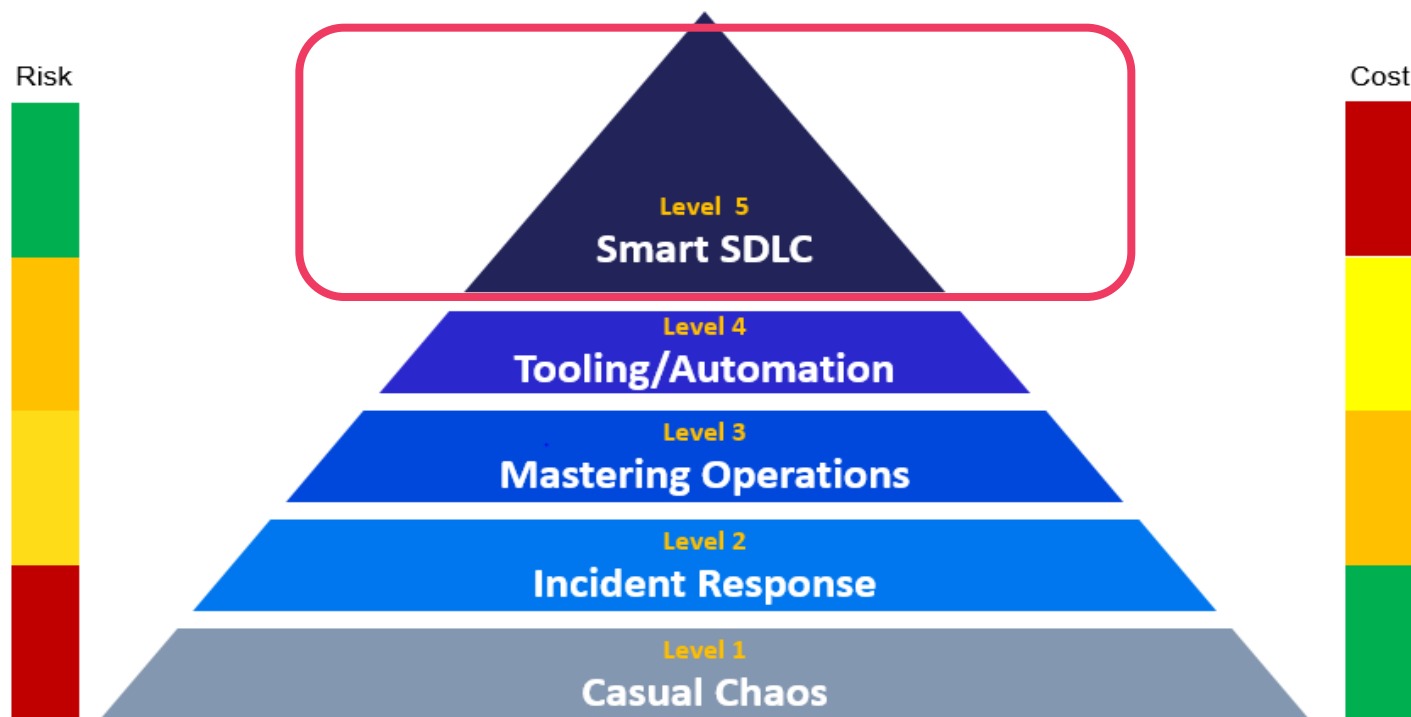
You can use this communications release as directed to respond to and advise customers and carriers regarding the industry wide security issue in OpenSSL named 'FREAK'.

Contents

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

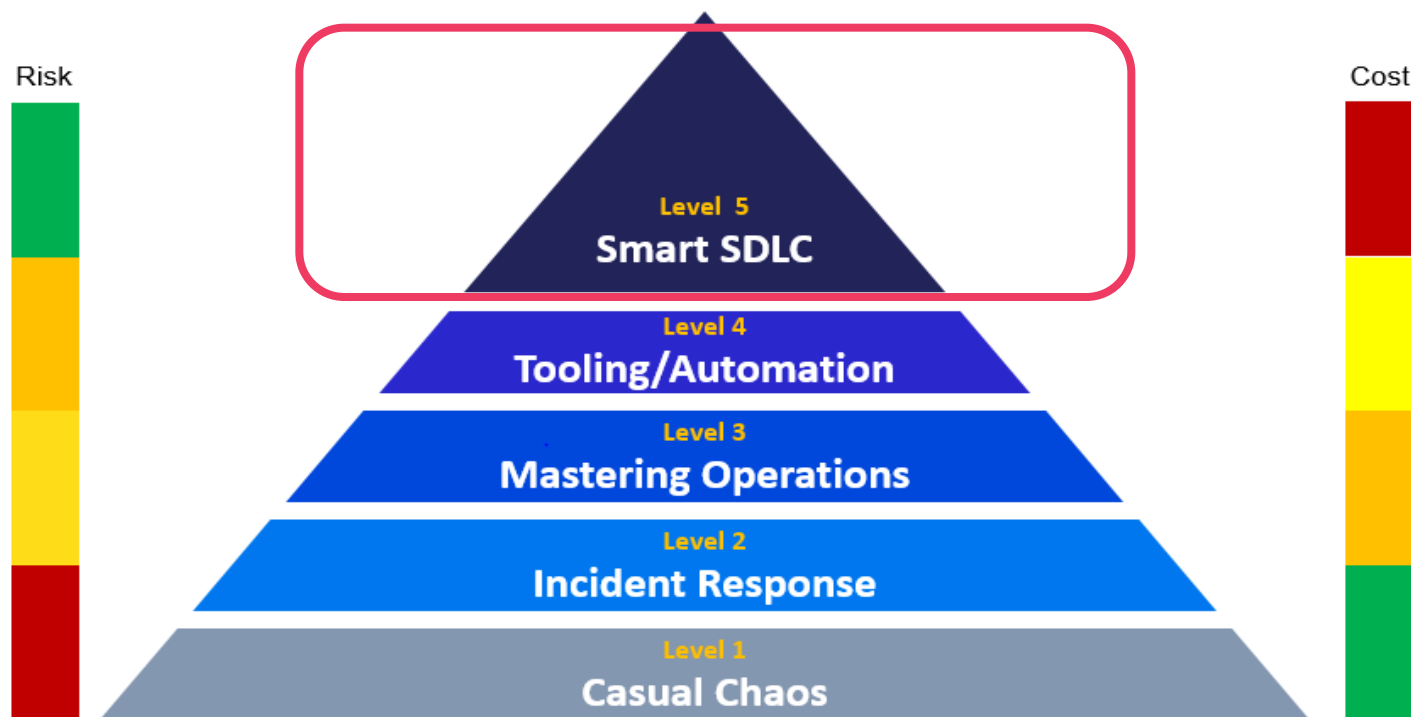
Level 5 – Using your OSS security intelligence

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



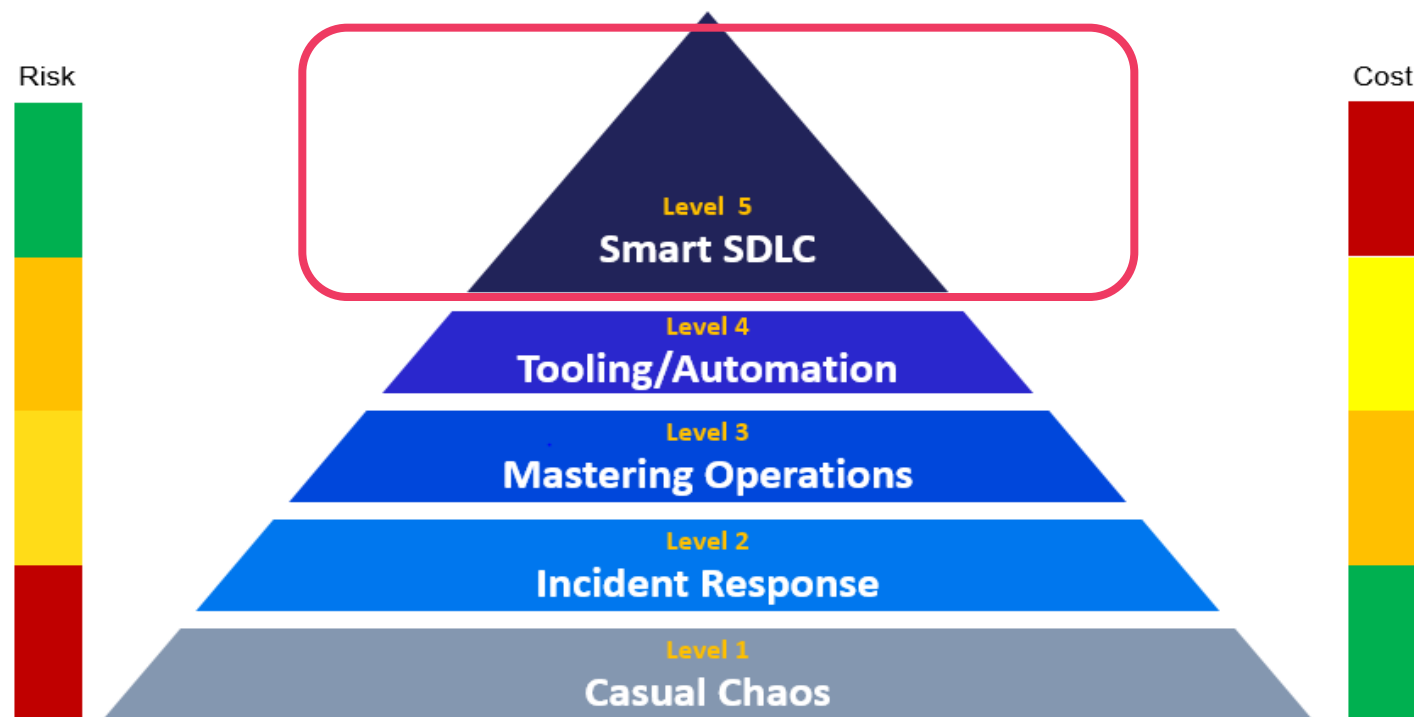
Level 5 – Using your OSS security intelligence

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



Level 5 – Using your OSS security intelligence

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



PANTS YOU SAY?

**I LIKE THIS JAM. TELL ME
MORE....**

What will this do for me?

*Cost to manage free OSS in 2015

*libpng \$203,678
 *OpenSSL \$370,690
 *cURL \$200,345

Cost is 59% less than 2 years ago !!!

	case ↑	resolution time ↓
libpng	84%	85%
OpenSSL	356%	77%
cURL	88%	57%

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Costs	(\$25,000)	(\$1,179,332)	(\$1,271,582)	(\$1,352,057)	(\$3,827,971)	(\$3,163,835)
Benefits	\$0	\$3,552,210	\$3,213,001	\$3,420,535	\$10,185,746	\$8,454,553
Net benefits	(\$25,000)	\$2,372,878	\$1,941,418	\$2,068,478	\$6,357,774	\$5,290,718
ROI						167%

A commissioned study conducted by Forrester Consulting on behalf of Synopsys in July of 2016

Source: Forrester Research, Inc.

Benefits

of a Mature OSS Security Program

As of Jan 2016

+87% increase in OSS

- **\$87,837** saved in large media events
- SIRT filed **401%** more defects against OSS
- Cost of supporting OSS decreased **62%** per product
- Intelligence to defect **87%** more efficient
- Investigation time is **46%** faster
- Fixes getting to customers **12x** faster

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)
- Kymberlee Price (BugCrowd)



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

