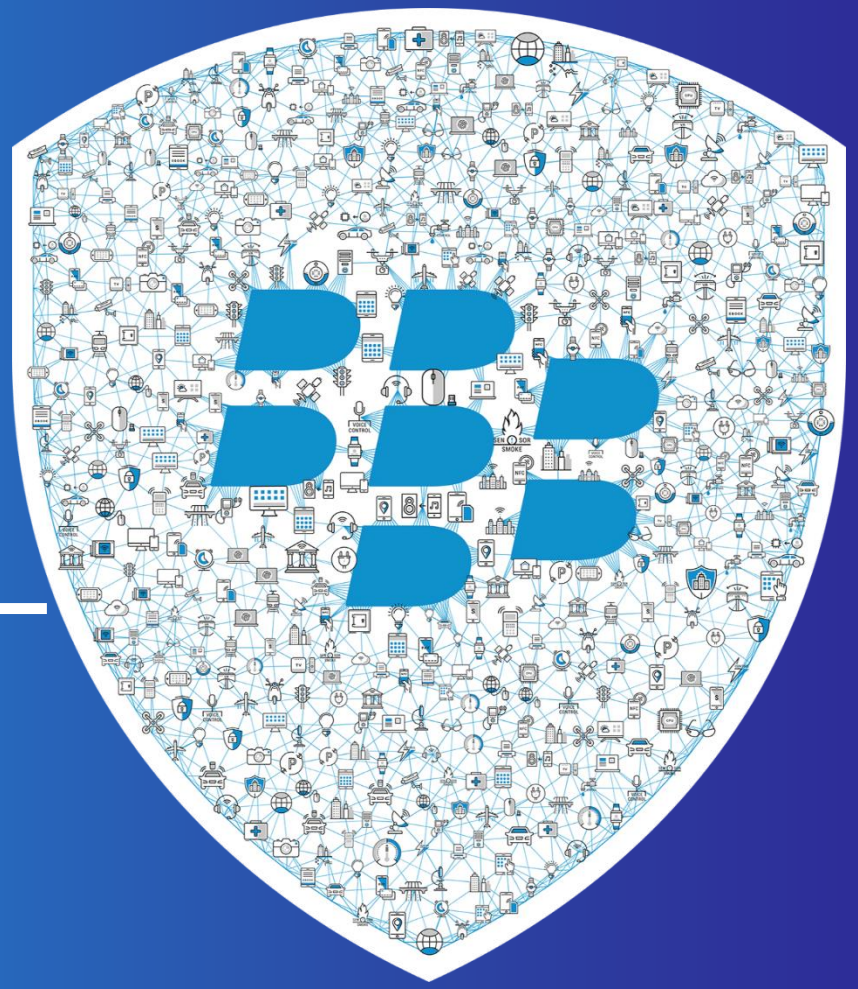
BLACKBERRY
OSS MATURITY MODEL

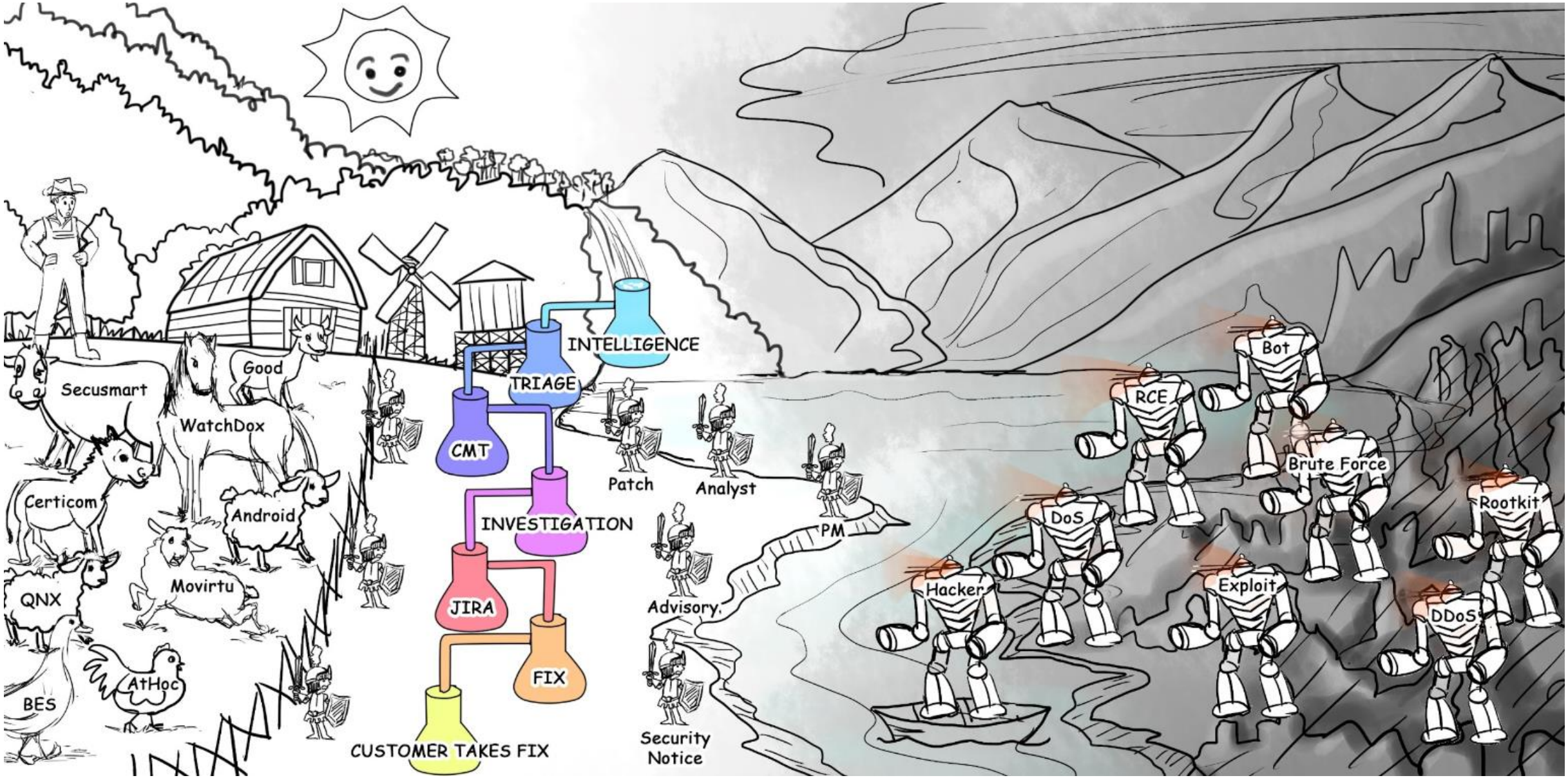


FIRST - June 2017

Christine Gadsby
Director, Product Security

Product Security Incident Response Team

- **Global PSIRT**
  - Solely focused on the security of in-market products and services
  - Not tied to ‘other’ security for a reason
  - Operations, Security Program Managers tied to specific products, Security Response Engineers



The Farm….

QNX | BlackBerry Subsidiary

Good | Powered By BlackBerry

movirtu | By BlackBerry

secusmart | BlackBerry Subsidiary

WatchDox | By BlackBerry

AtHoc | Division of BlackBerry

certicom | BlackBerry Subsidiary

BlackBerry Secure Smartphone Powered by Android™

The Enterprise Of Things

BlackBerry, Securely Connecting The World

What happens when you lose control….Android

Adding Android to the mix
Response in a world where your front-door is open

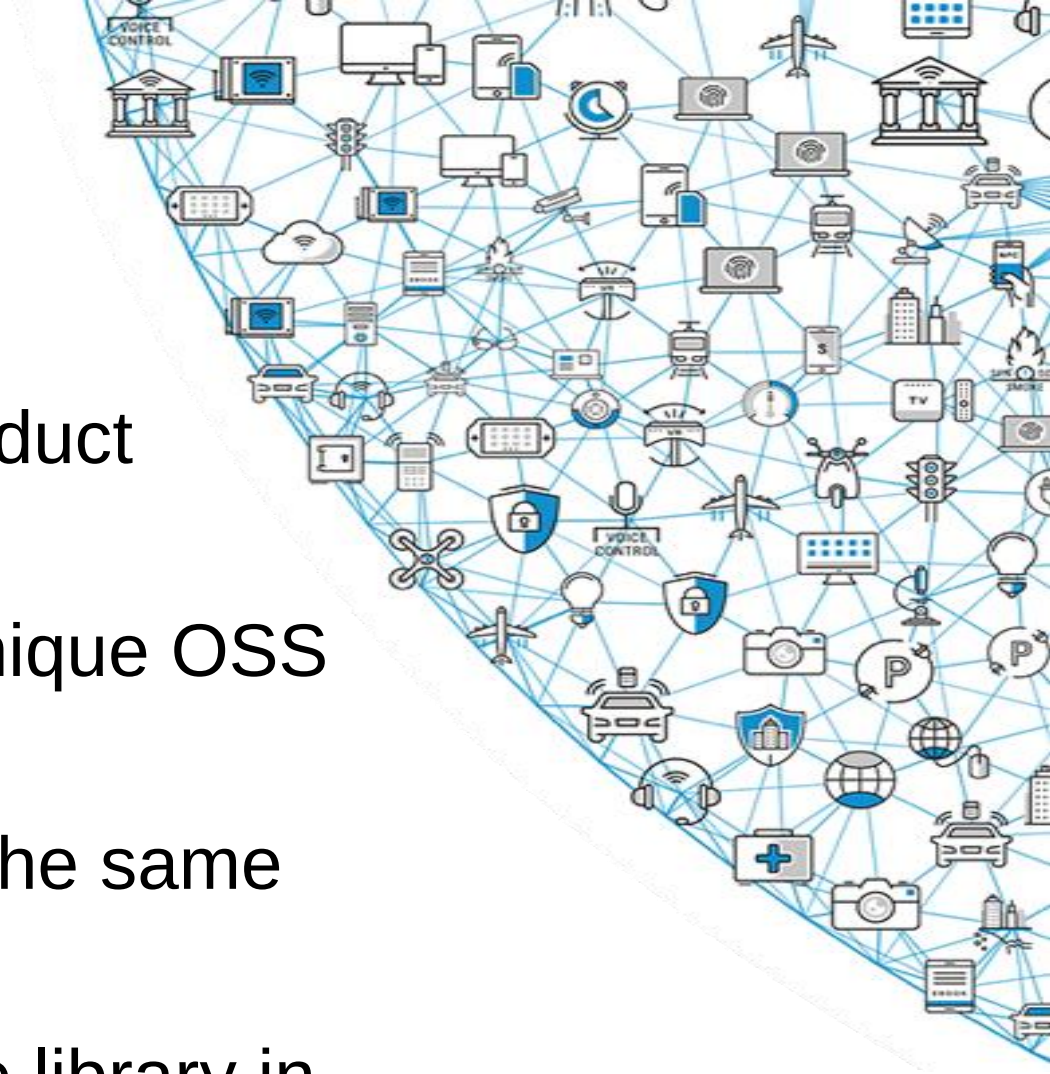
- Moving from covering your own home-grown OS to being an integrator/customizer
- Living in a world that is inherently public
- Volume of vulnerabilities is an order of magnitude larger than what BlackBerry was accustomed to with its own operating systems
- Surprise! Monthly patching initiative announced by Google less than 3 months before first device launched

Android 30-day patching reality… 12/2015 and 18 releases in

- Almost double the amount of CVE's for BES5/10/12/Good/UEM combined
- High month was 127 CVE's
  - x3 devices almost 400 CVEs all in the span of 4 business days
- Majority of fixes come from upstream components (SoC providers, Google, etc)
  - OEMs dependent on these vendors to provide fixes to meet Google defined requirements

SO….What’s the BIG deal?

Fun BlackBerry OSS facts



- 536 unique libs tracked across 83 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

How we feel right about now

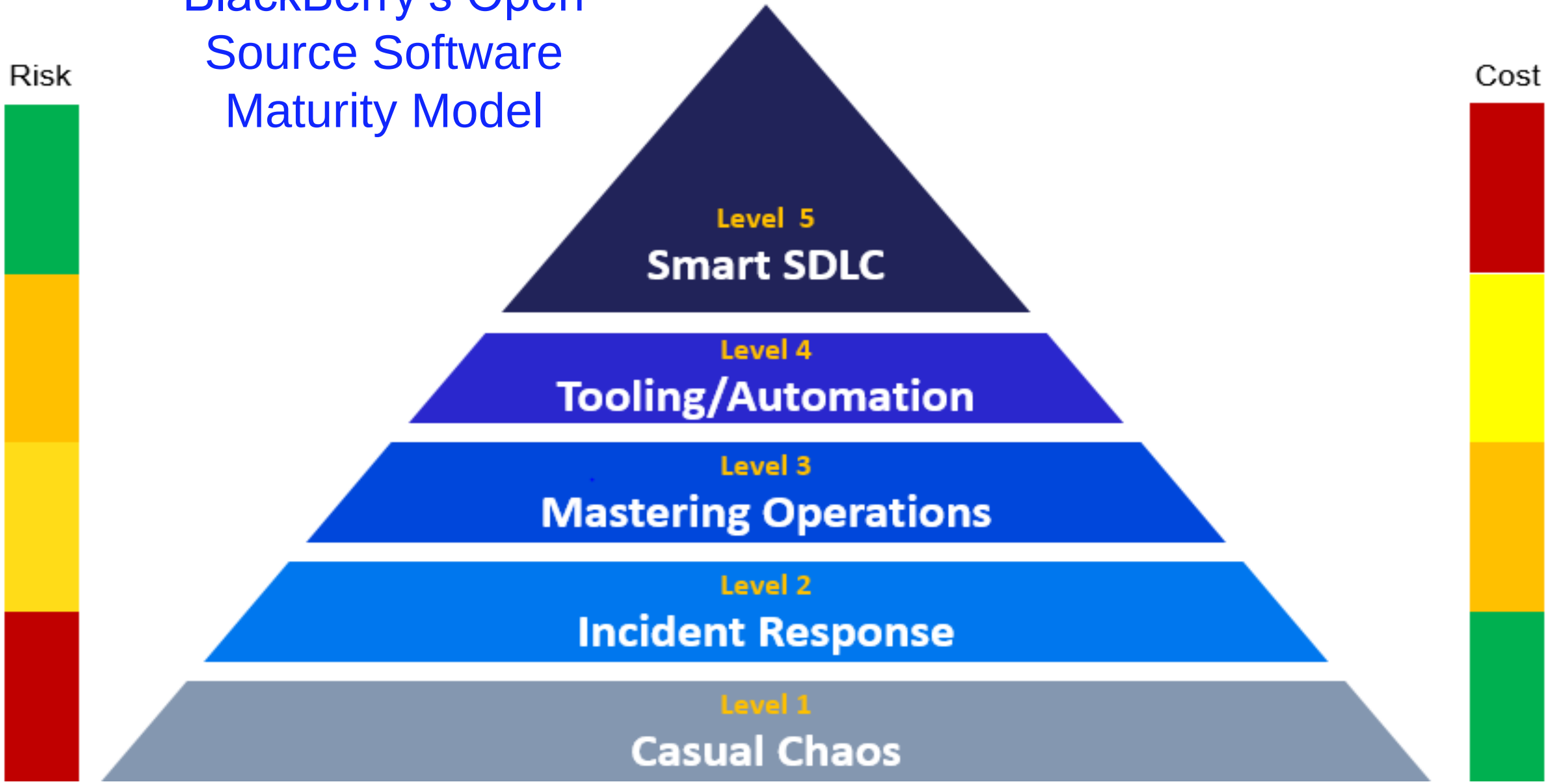
SO….What does this mean?

Software Erodes over time….

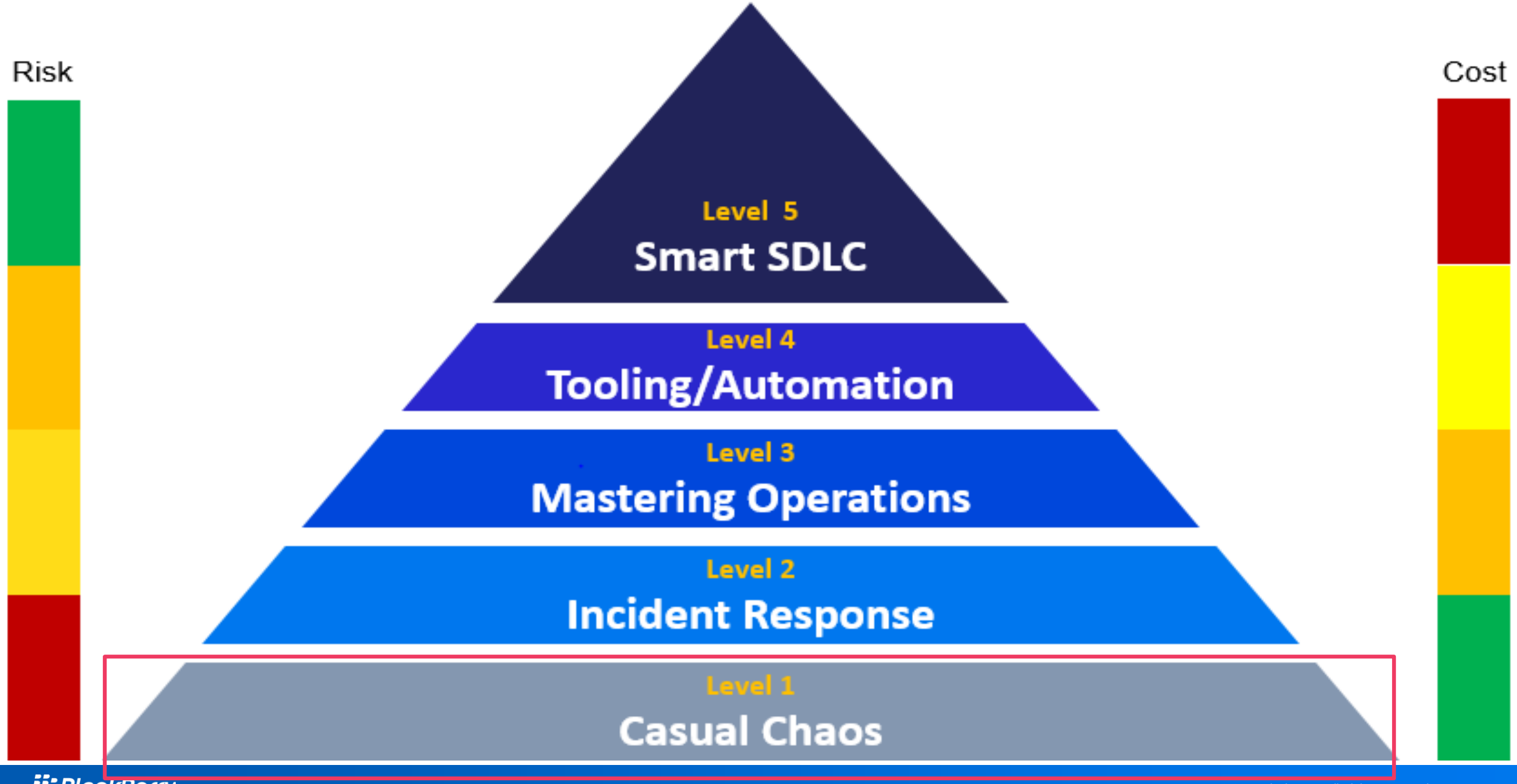
SO….What’s the solution…..

Goal: To Create a model to support Consistent tracking, control, monitoring, and patching of OSS across BlackBerry’s products and services

BlackBerry's Open Source Software Maturity Model

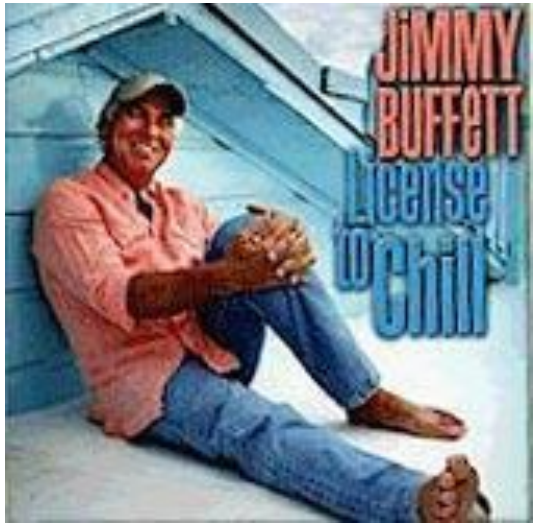


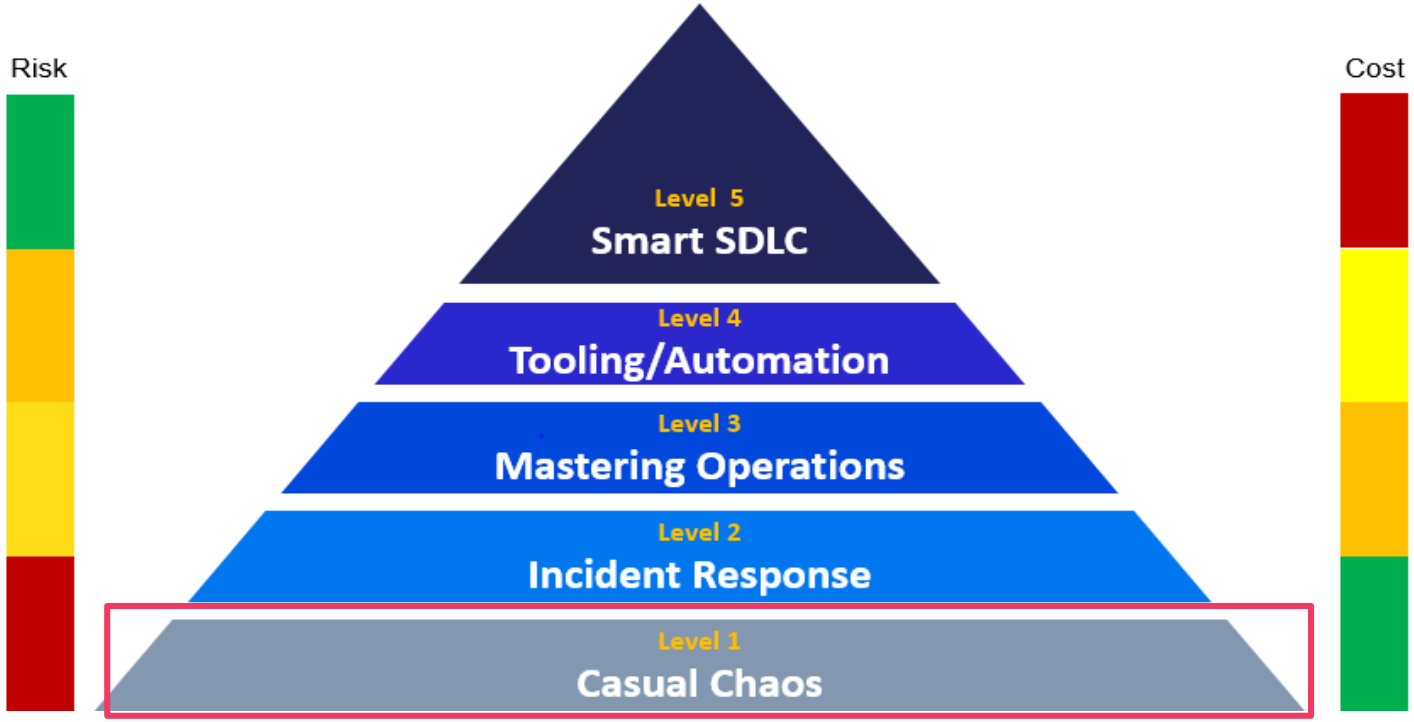
IN the BEGINNING…….



Level 1 – Casual Chaos

- No formal incident response process or accountability
- Using email to discuss solutions
- Press is your vuln notification; media drives fear
- CEO calls and you duck and cover

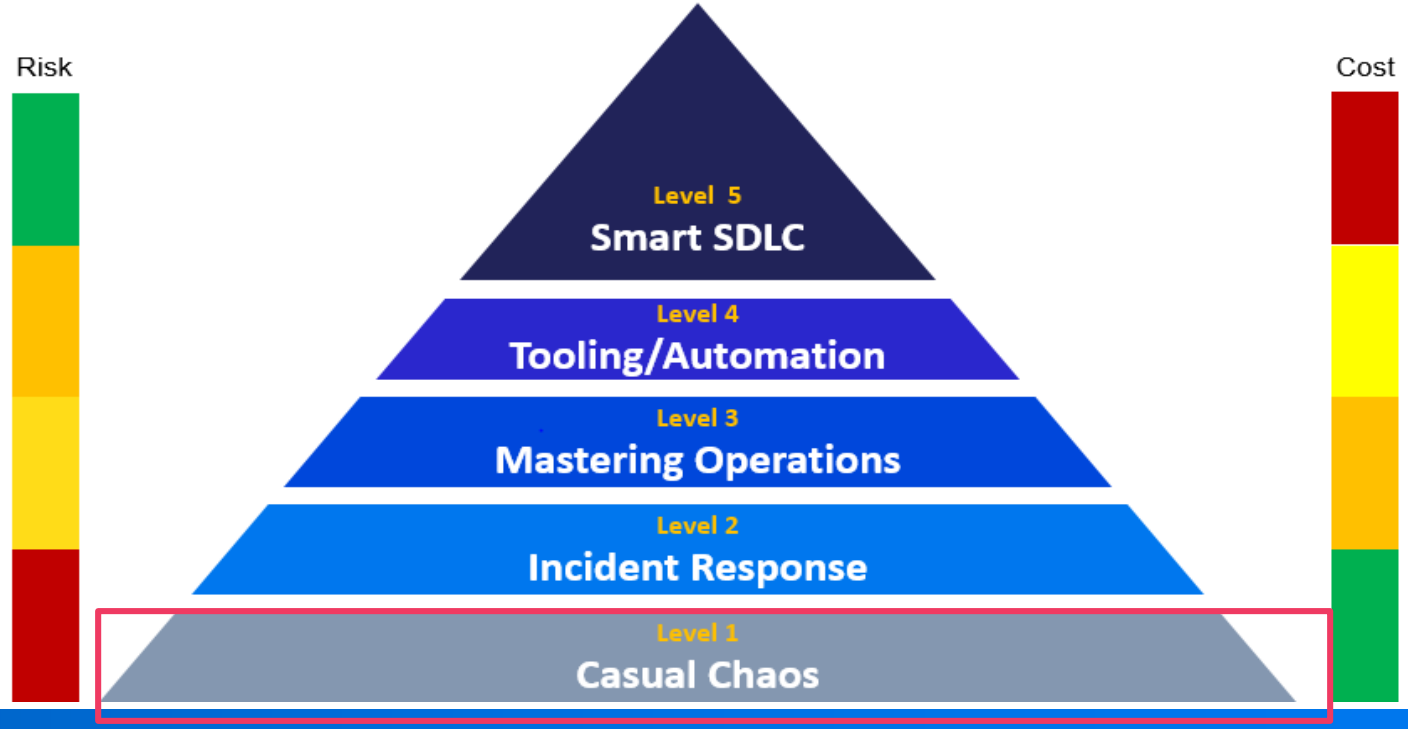




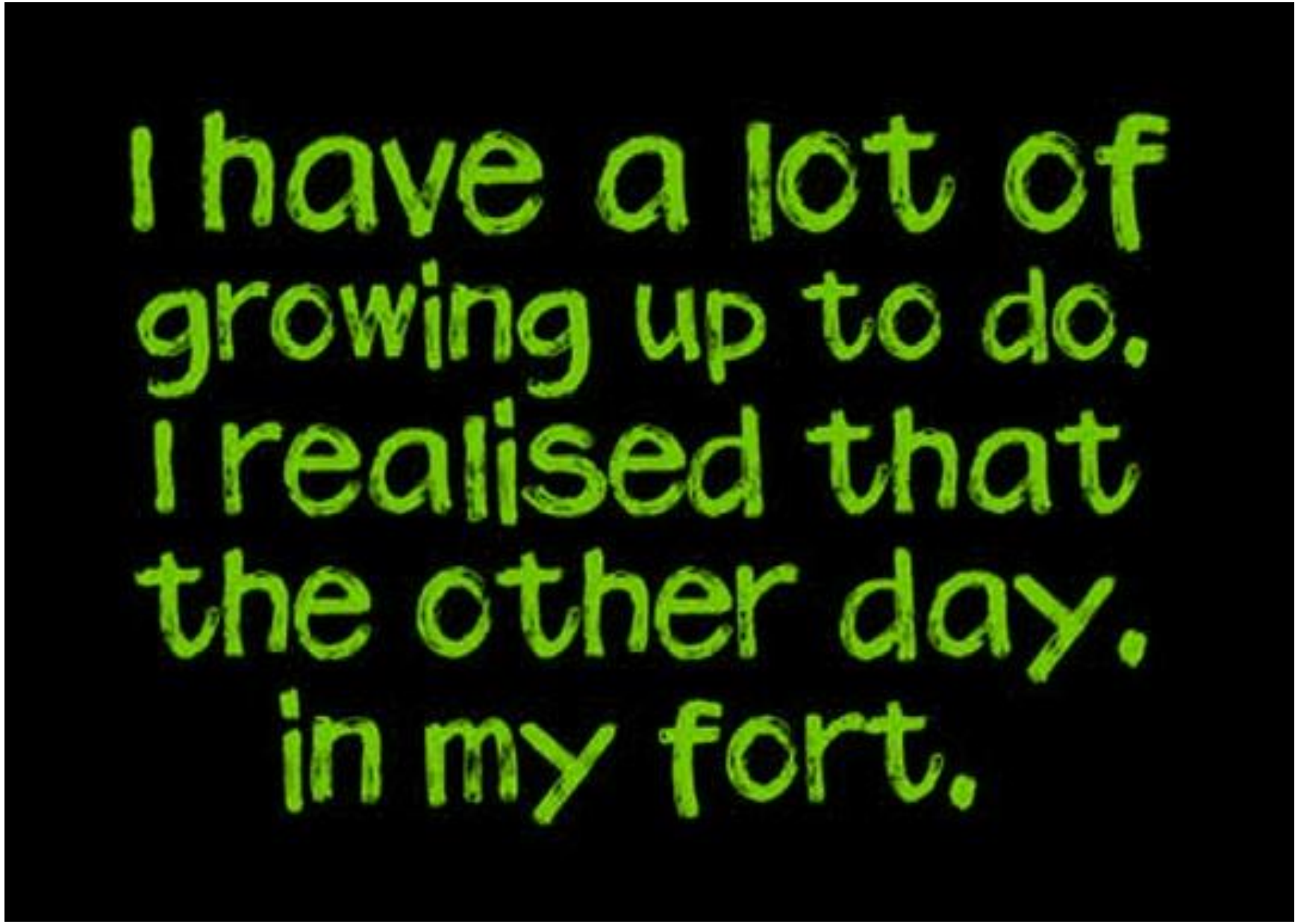
Level 1 – Casual Chaos [Develop

***At this level** …even this is possible*

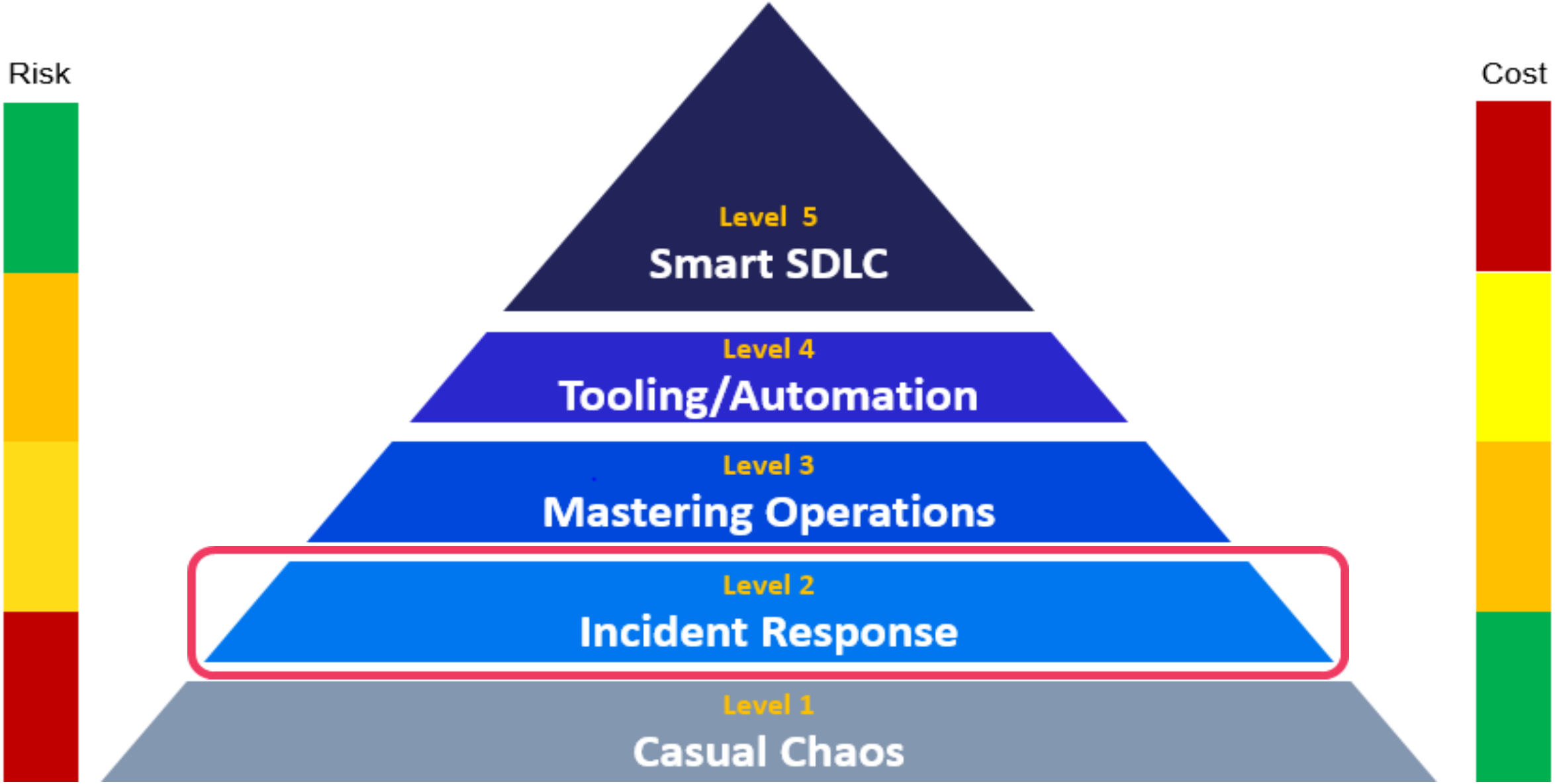
- General OSS redundancy
- Using OSS blindly
- No understanding of risk or spread
- Patching? Maintenance? Versions?



…..On the Brightside, this is incredibly cost efficient

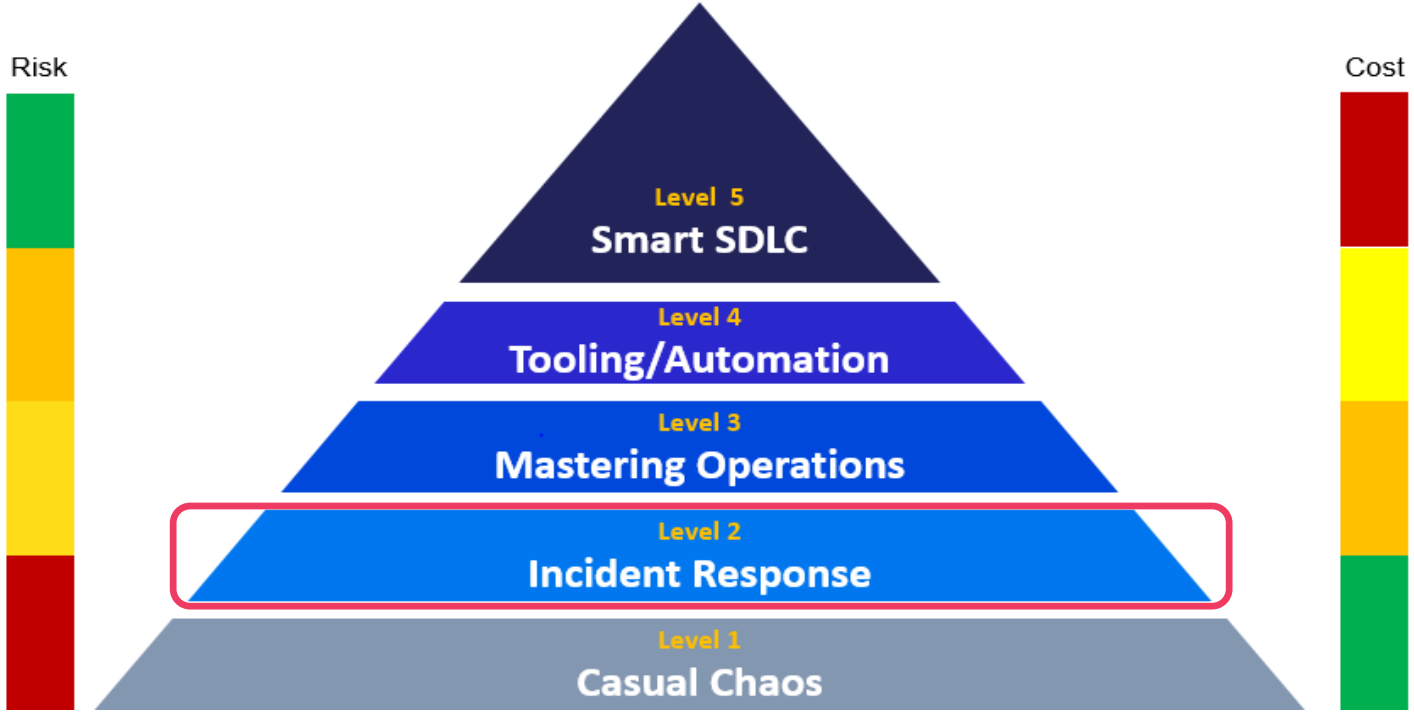


Level 2 – Incident Response is born



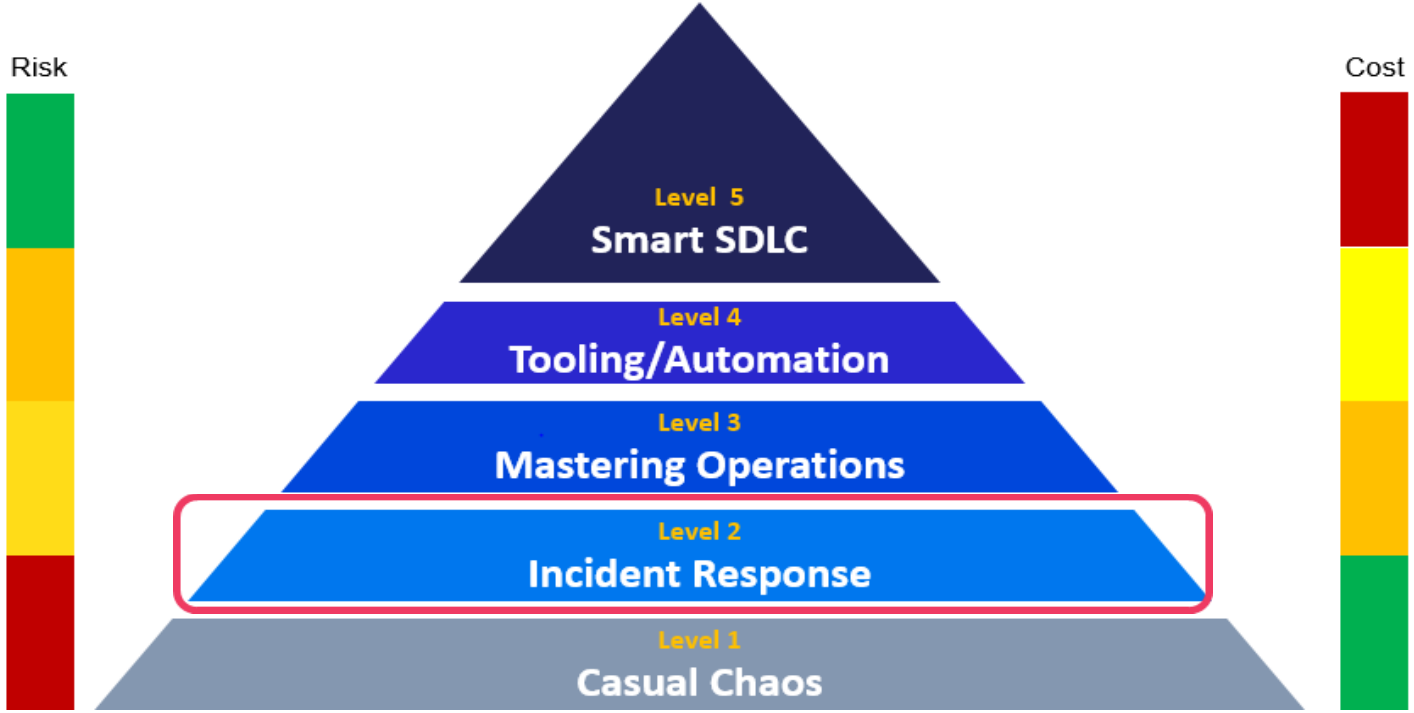
Level 2 – Incident Response

- Create software BOM
- Investigate + track + remediate public OSS vulns

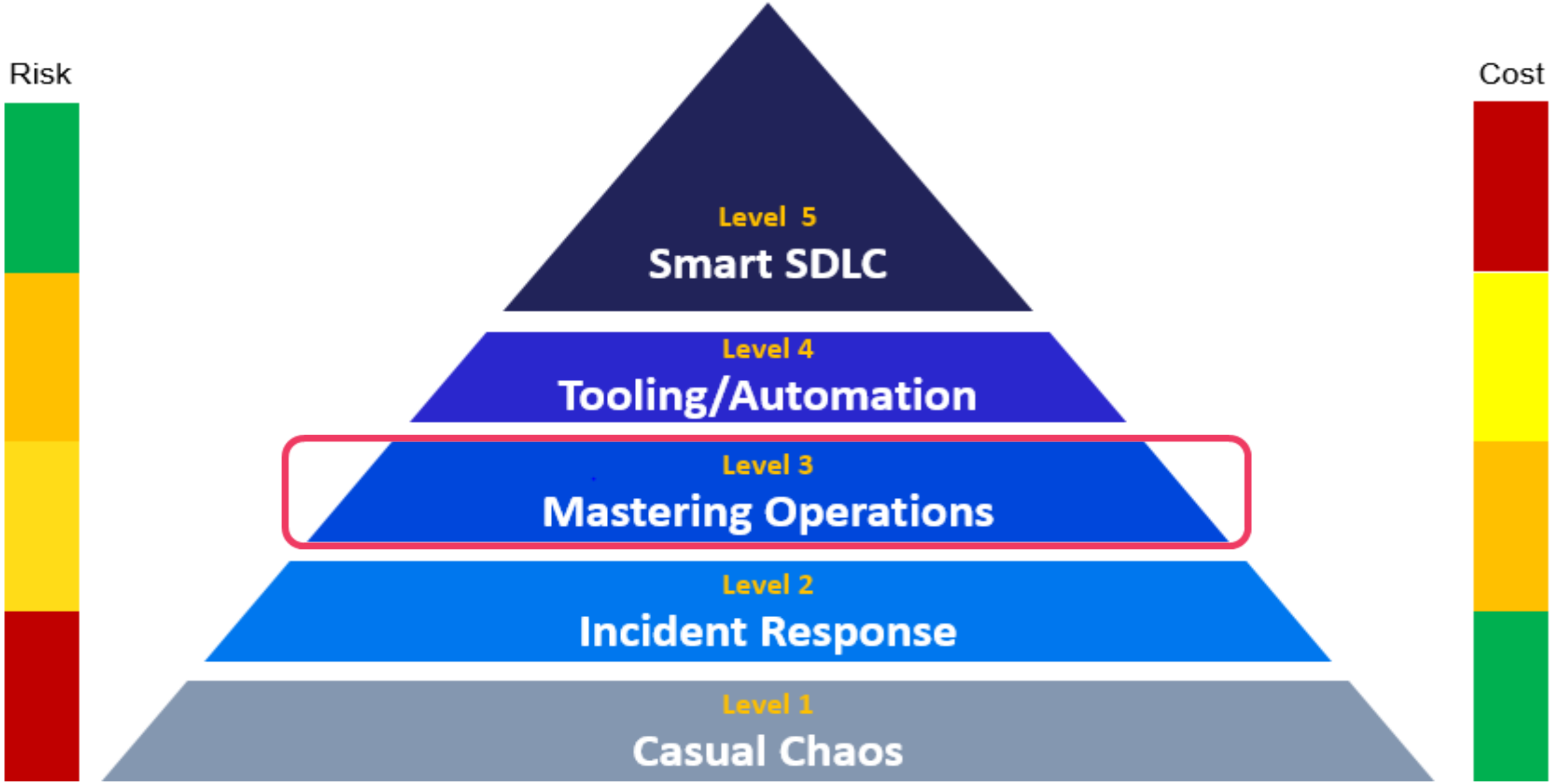


Level 2 – Incident Response [Development]

- Work with ops/development for Incident Response based on the impact of vulnerabilities

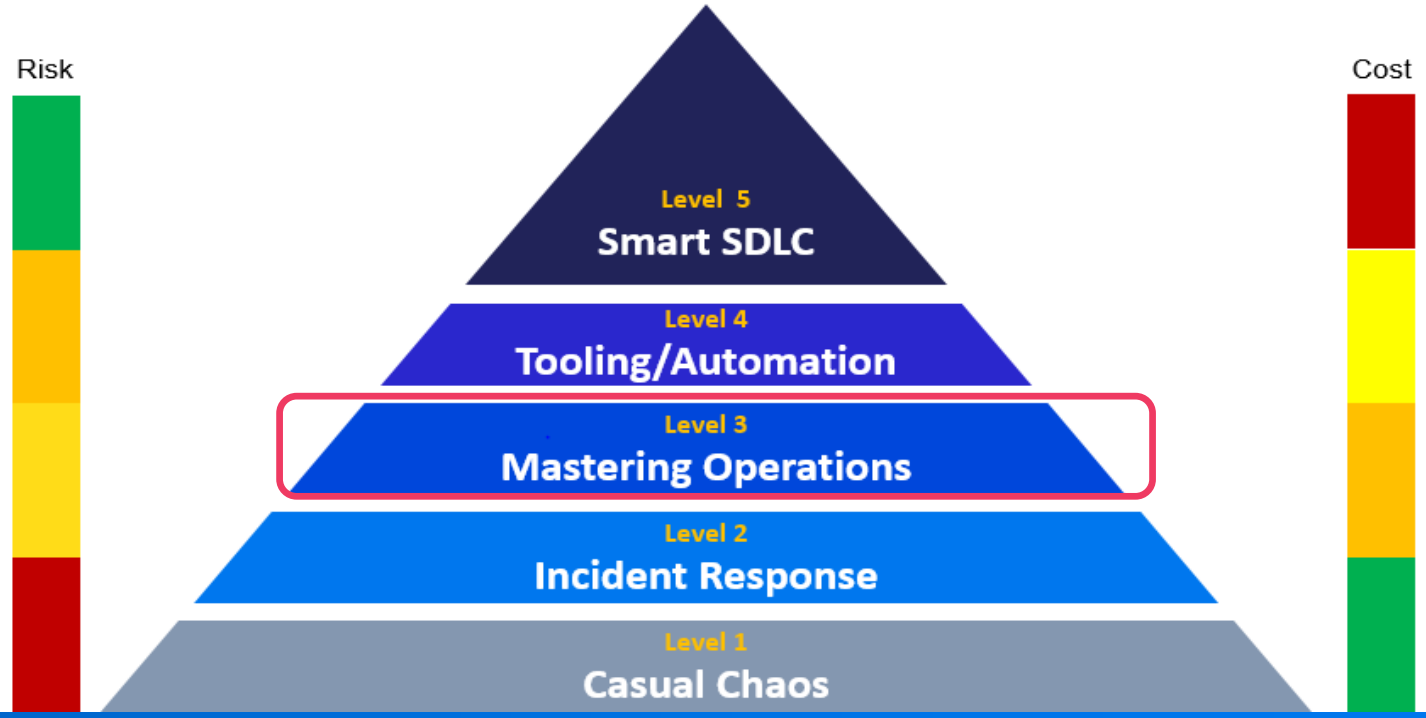


Level 3 – Mastering Ops



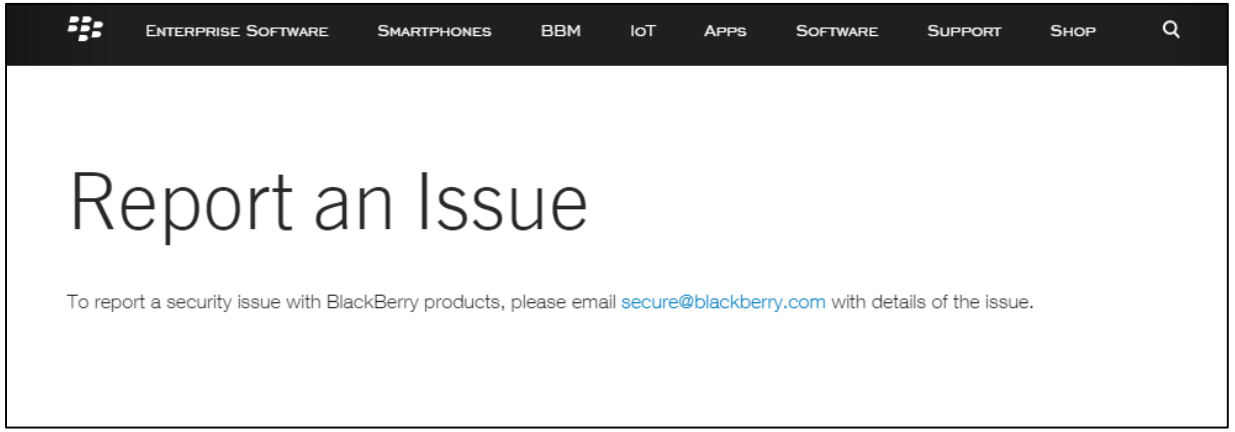
Level 3 – Mastering Ops

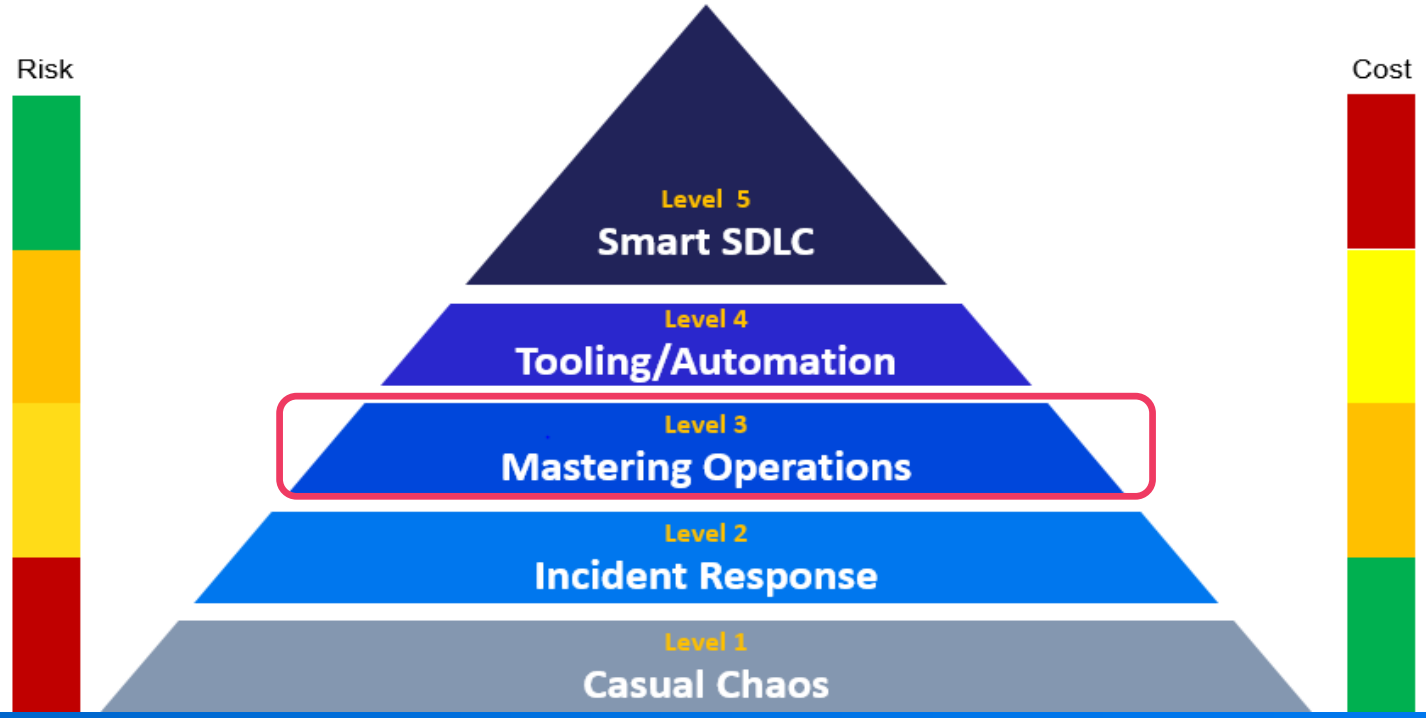
- Proactively use OSS vuln intelligence sources
- Process for OSS vuln lifecycle
- Fixes VS. Features with fix vehicle



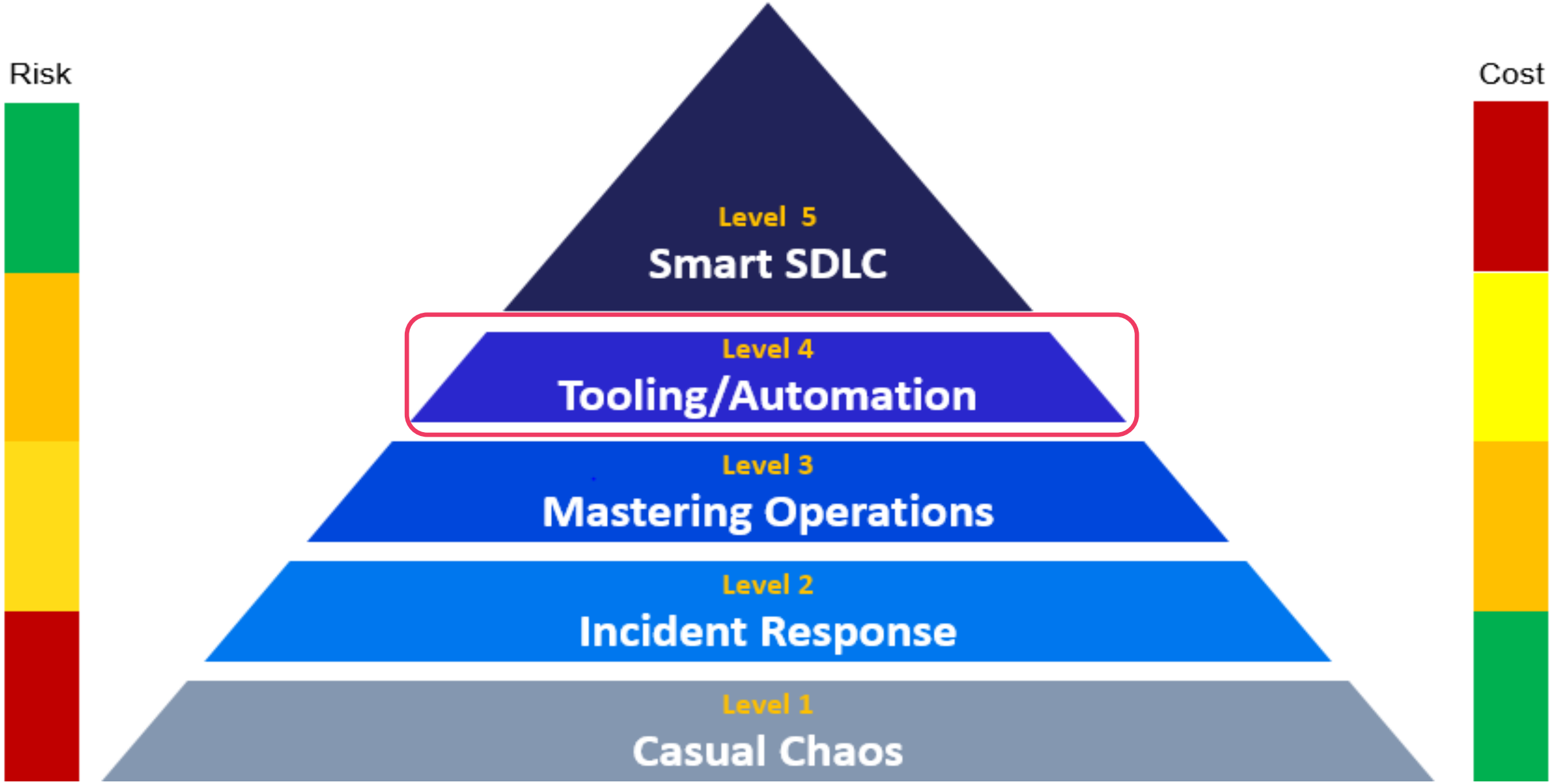
Level 3 – Mastering Ops

- Notification to customers
- Security Researchers know where to report OSS vulns
- Public Vuln disclosure policy



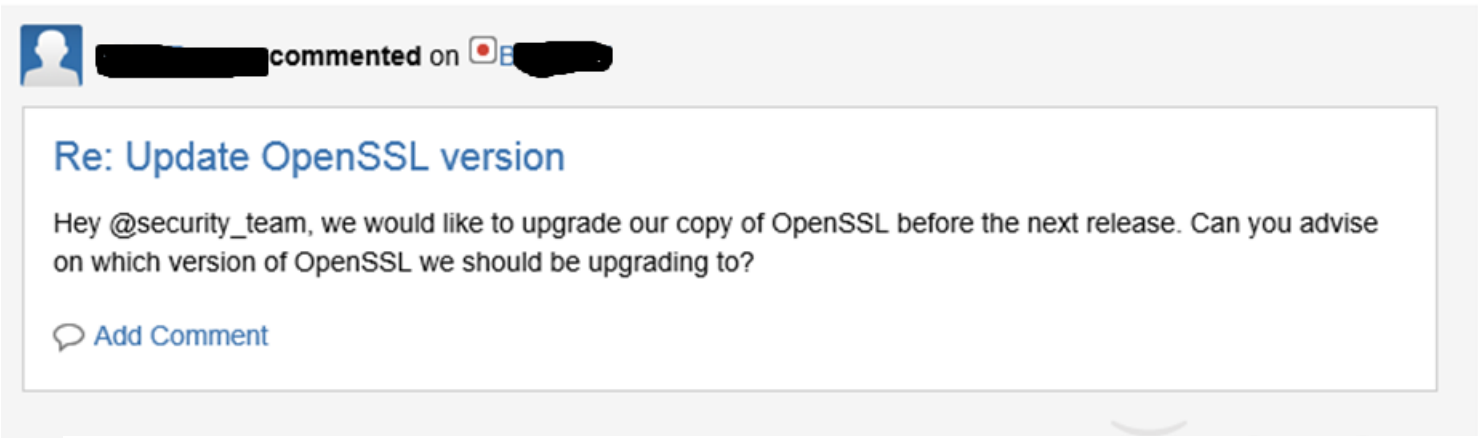


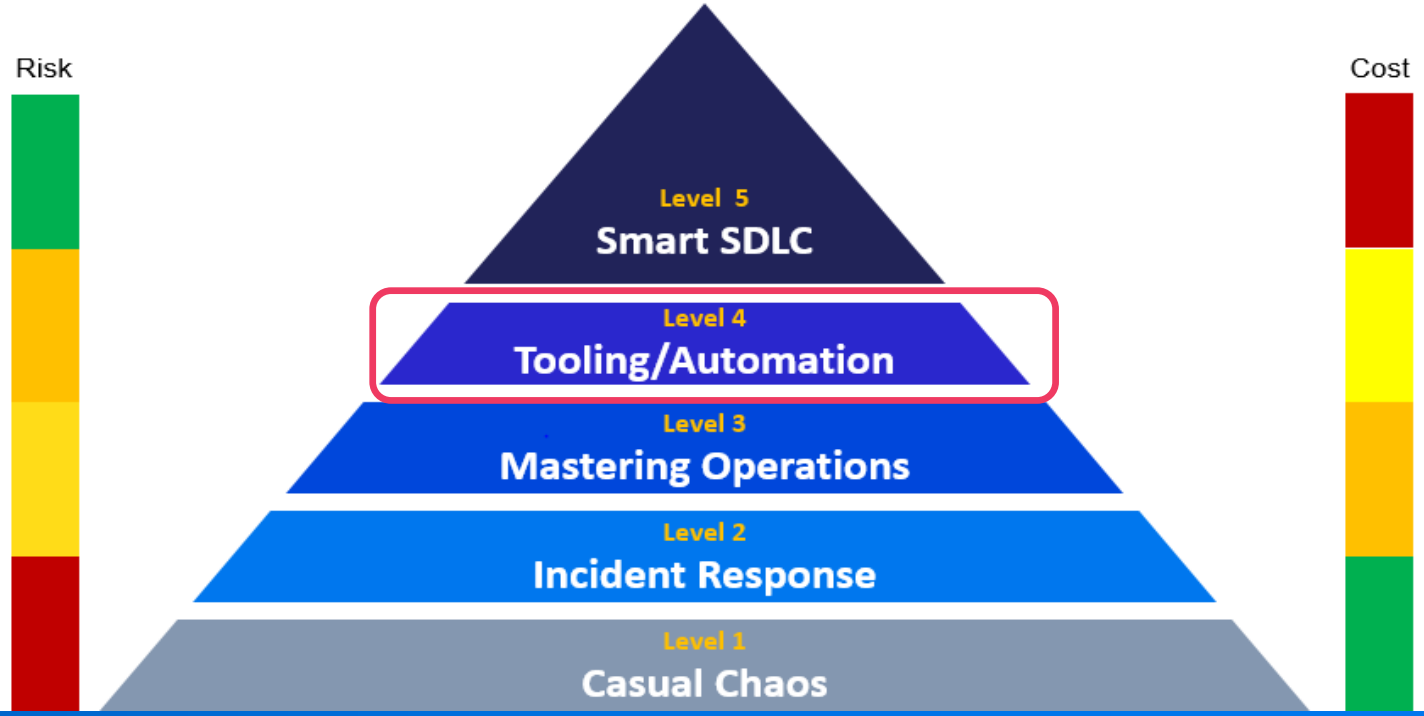
Level 4 – Tools



Level 4 – Tools

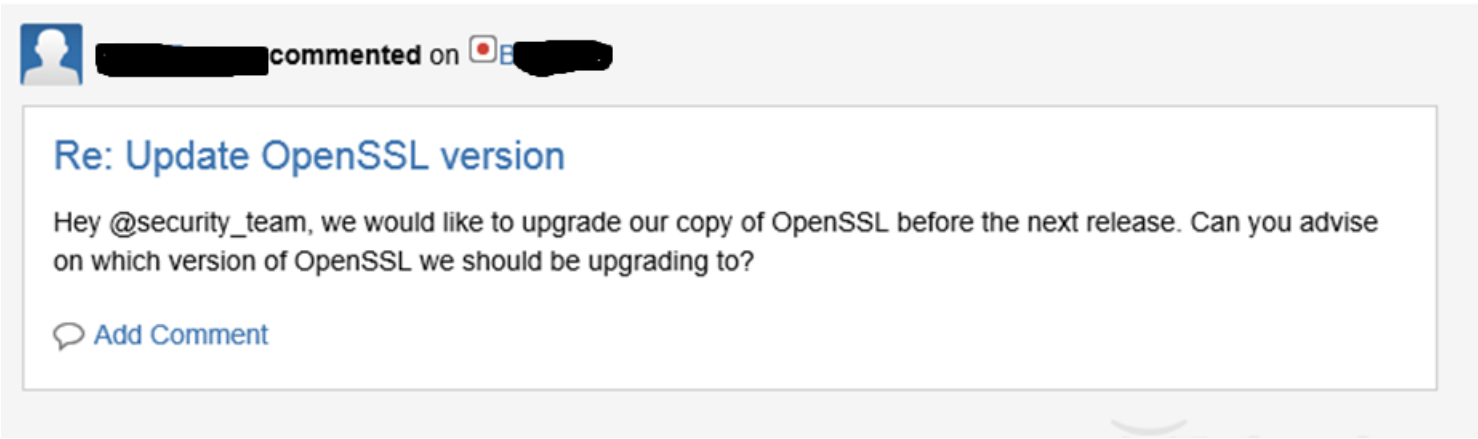
- Using your vuln data proactively
- Product Catalog is automated/tracked
- Using tooling and automation to drive efficient vulnerability handling

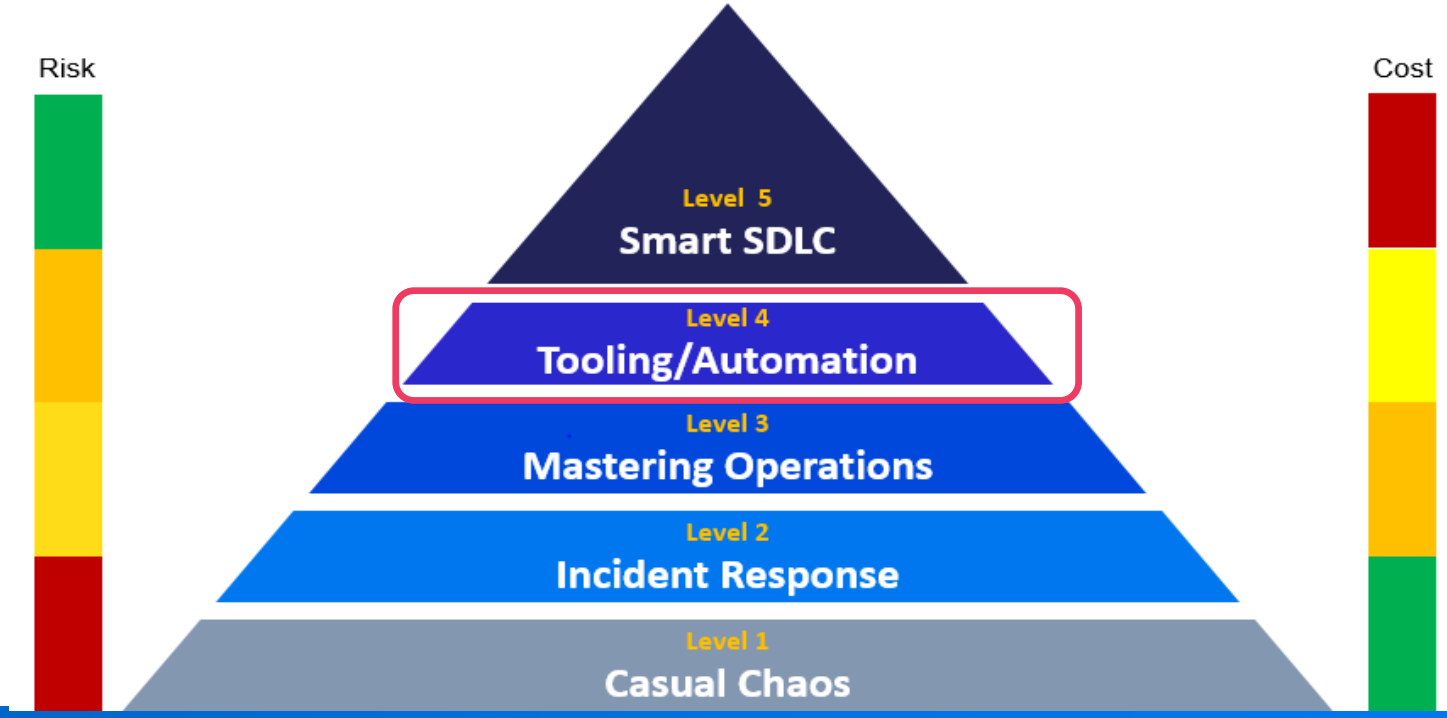




Level 4 – Tools [Dev]

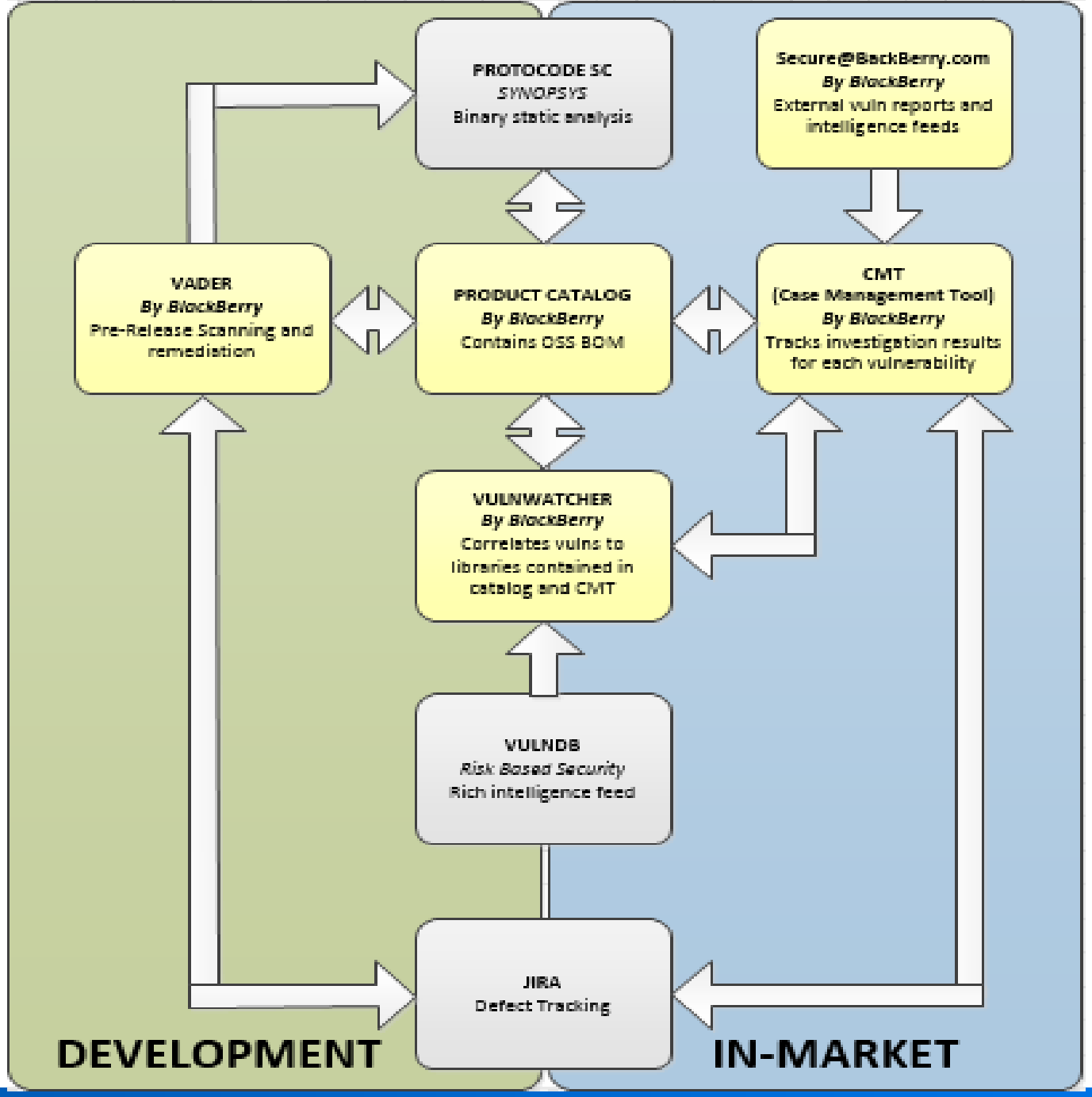
- Dev proactive involvement with security
- OSS vuln debt has exec visibility





Level 4 – Tools

BlackBerry Custom Tools



3rd Party Tools

What will all this do?

OpenSSL ‘Freak’

BBSIRT Case Management Tool

Home | Investigations | Release | Tasks | Admin

Scan Details

Name: bbry_qc8992_sf-user-producti
Build Number: AAD444
Current: Yes

Library Name	Version Name	Reported Version
7zip		

Reference Name	Reference Path	Full Path	JIRA Component	Confidence	False Positive	Carry Over	Custom
7zip_4_57.exe	/autoloader/7zip_4_57.exe	/autoloader/7zip_4_57.exe	27874	0.5398230088495575	true	false	No

achartengine

Reference Name	Reference Path	Full Path	JIRA Component	Confidence	False Positive	Carry Over	Custom
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	0.23529411764705882	true	false	No

acra

Reference Name	Reference Path	Full Path	Confidence	Carry Over
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		

$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
Movirtu - Core	unknown
[illegible]ndroid	1.0.0.1838
[illegible]SDP	6.6.0
[illegible]	294.0.0.14

OPENSSL

Product	Scan
BB10	

File: transform Version: 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	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

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

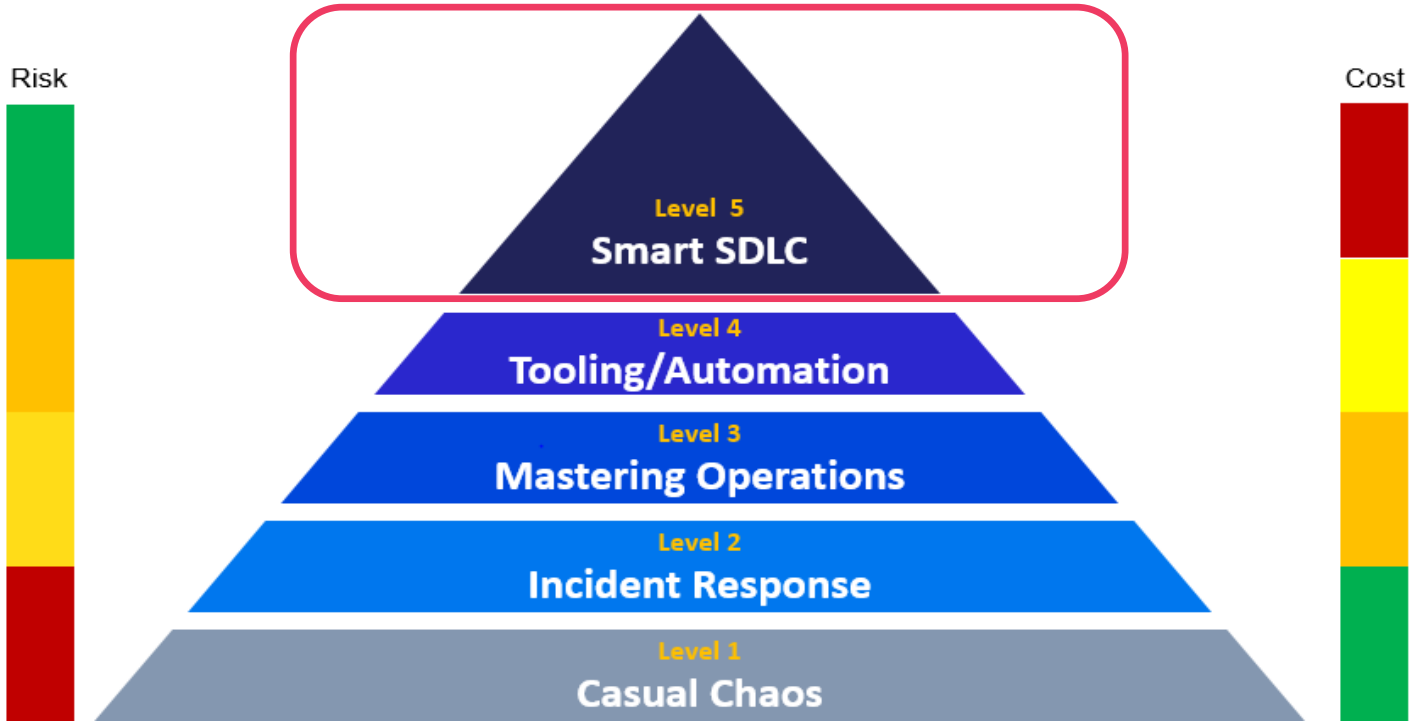
Android Tooling

- Automated bulletin intake, reducing labor cost by 80% and made patches available to developers up to 3 days soon
- Developing tooling to assist in patch verification
- Automated Bulletin creation
  - Was formerly taking up dozens of hours, manually verifying which CVEs needed to be advisoried
  - Leverages in-take automation to verify which CVEs need to be advisoried and programmatically builds a document
- Total automation efforts transformed the process from requiring the same data to be cut and paste 7+ times to 1x

Level 5 – Using your OSS security intelligence

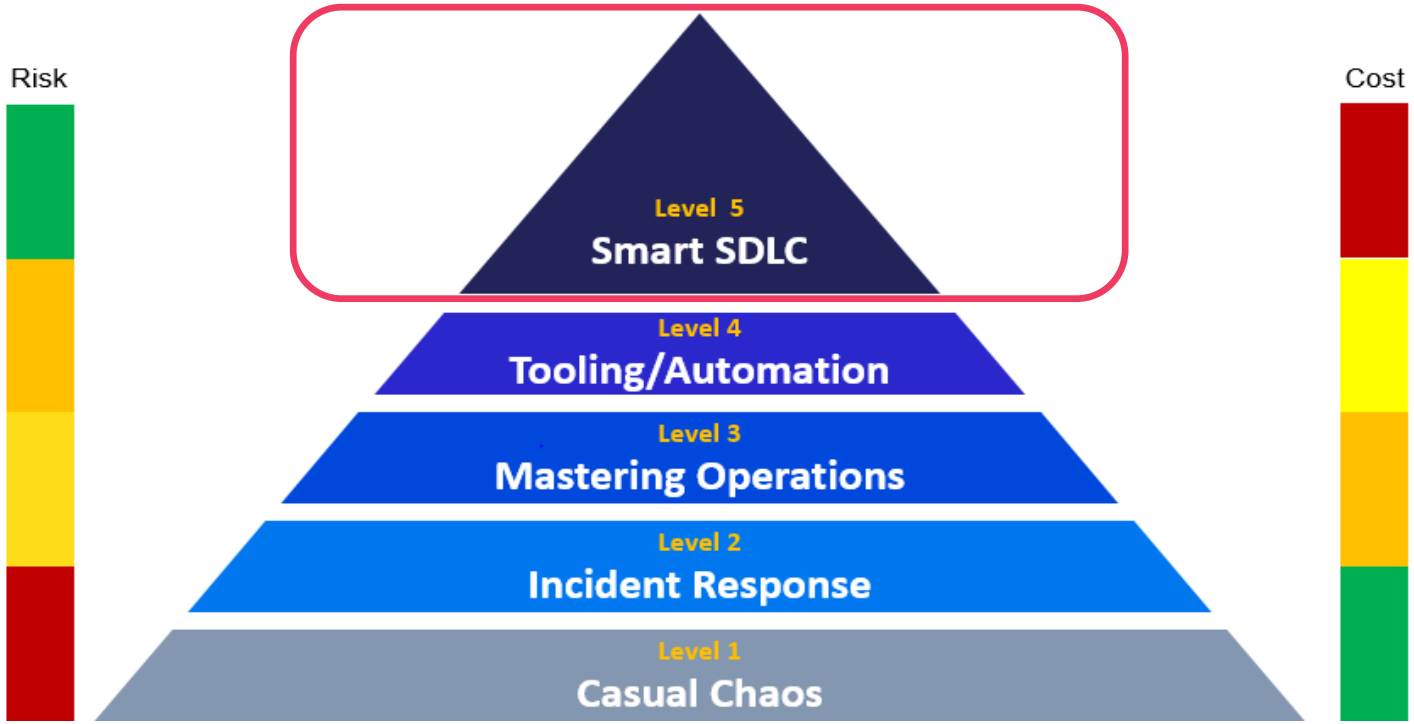
Level 5 – Using your OSS security intelligence

- Curated OSS product Catalog
- Using your own product vuln intel to create smarter products
- Proactive patching
- Understand ROI



Level 5 – Using your OSS security intelligence

- #1 put it in a box – minimize attack surface
- Developers make well informed OSS decisions
- OSS Blacklisting



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%

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