IBM Secure Engineering

Overview

Kate Scarcella CISSP
MS Information Security
CyberSecurity Architect

2018

IBM

Please Note:

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

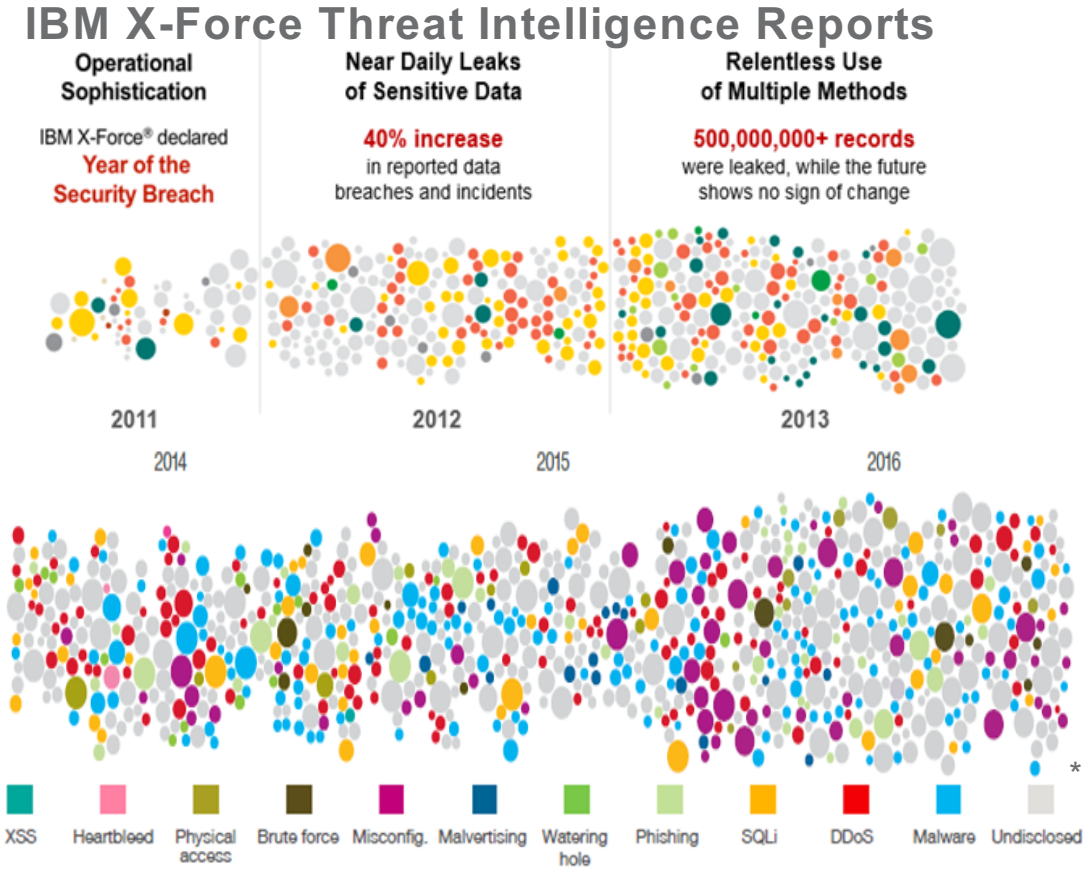
Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

IBM X-Force Data illustrates the continuing concern for the effectiveness of Security



Factoids & Insights from IBM Xforce 2017*

~ 50% of the total: undisclosed causes

~ 29% of disclosed: Web App related
~ 50% of disclosed: Software defect related

2016: Year of the Mega Breach
2016: Record number of "old" breaches disclosed
2016: Focus shift to unstructured data (such as emails + email archives, documents, source code, intellectual property, etc)

2016: DNC hacked using phishing & SQLi
2016: DDoS attacks more sophisticated

2016: Improved hashing techniques make stolen encoded passwords less valuable

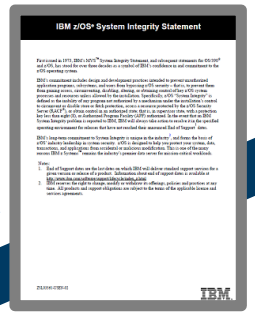
* https://www.ibm.com/security/xforce/research.html

IBM Secure Development has evolved over more than 40 years from internally defined practices with Product focus to externally aligned practices with Cloud focus.

Product Focus

Product & Service Focus

z/OS Statement of Integrity 1973



STG

SWG STG

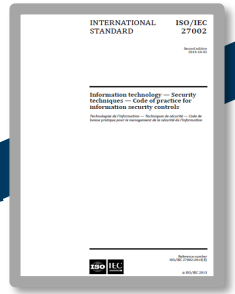
Secure Engineering Framework 2010

O-TTPS Accreditation IBM Middleware 2014

Acquisitions

Cloud SaaS SoftLayer BlueMix

Compliance & Certification to External Standards 2015 & 2016



ISO/IEC 27002:2013
Information technology Security techniques — Code of practice for information security controls

NIST SP800-53R4 (FedRAMP)
Security and Privacy Controls For Federal Information Systems and Organizations

CIO Cloud Security Policy and Implementation Standard (ISO27002)

ISO/IEC 20243:2015
Information Technology – Open Trusted Technology Provider Standard (O-TTPS)

IBM Principles for Secure Development

1. Provide security out of the box

Enable products, solutions and services to provide a reasonable and adequate level of security prior to release, and to maintain and to improve security from release to release.

2. Proactively respond to vulnerabilities & threats

Proactively identify, investigate and resolve vulnerabilities in IBM products, solutions and services, and new threats that are discovered.

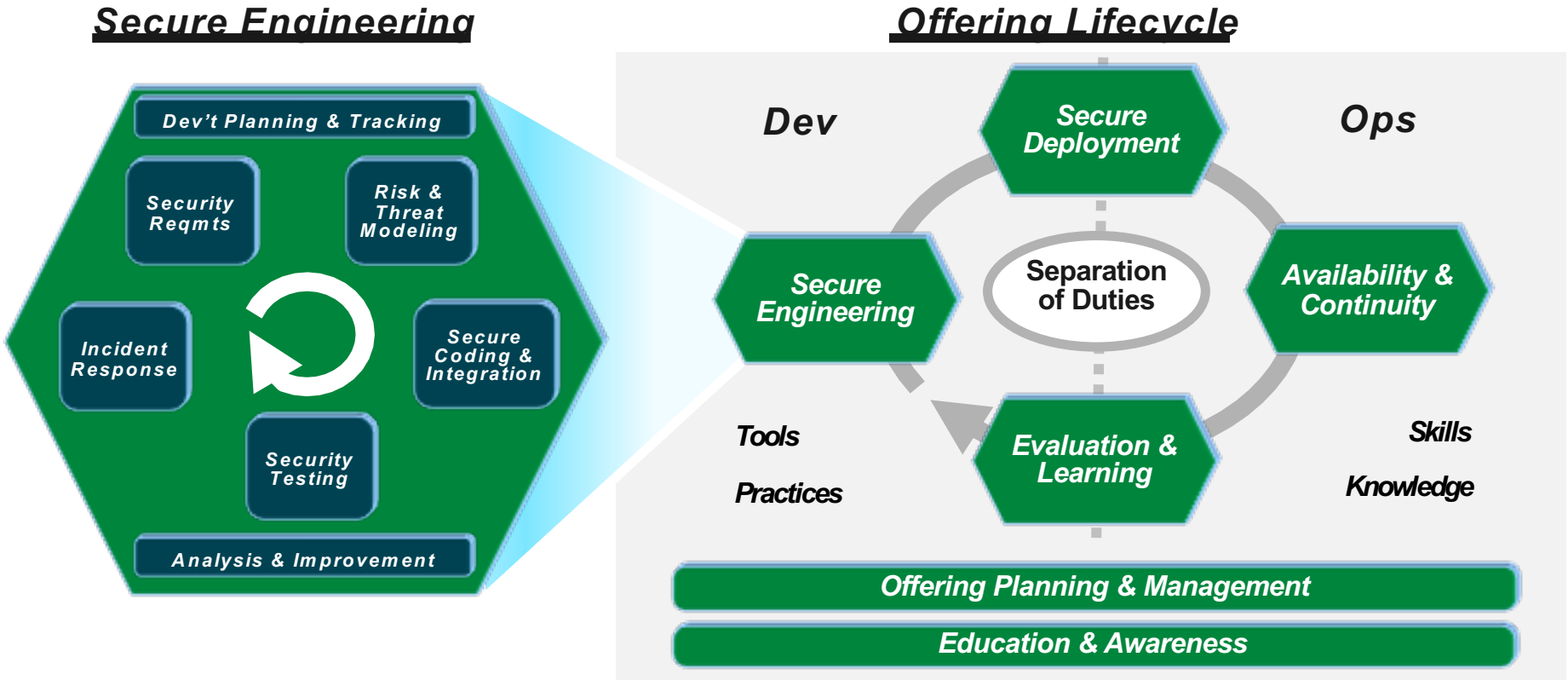
3. Protect Source Code & Intellectual Property

Establish controls to manage access to source code, and monitor and analyze patterns of behaviors in order to minimize the risk of loss or contamination of source code and development artifacts.

4. Align Function & Practices w/ Security Standards

Enable teams to design, build and deliver products, solutions and services that reflect the features and assurance criteria defined by international, governmental and industry recognized security standards.

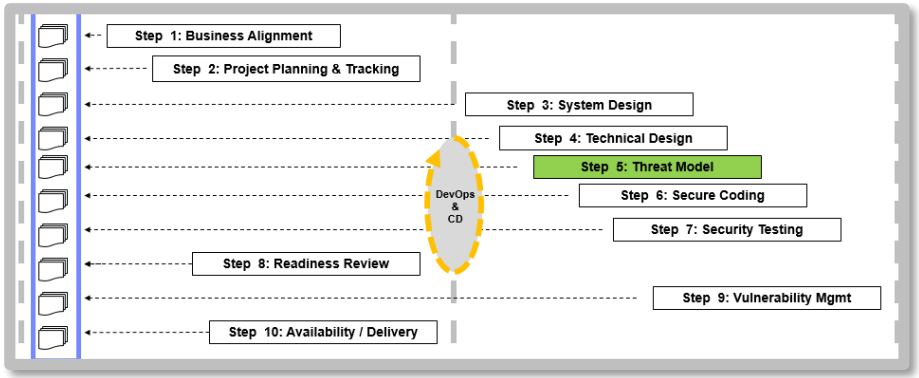
IBM Secure Development & DevOps = Secure DevOps



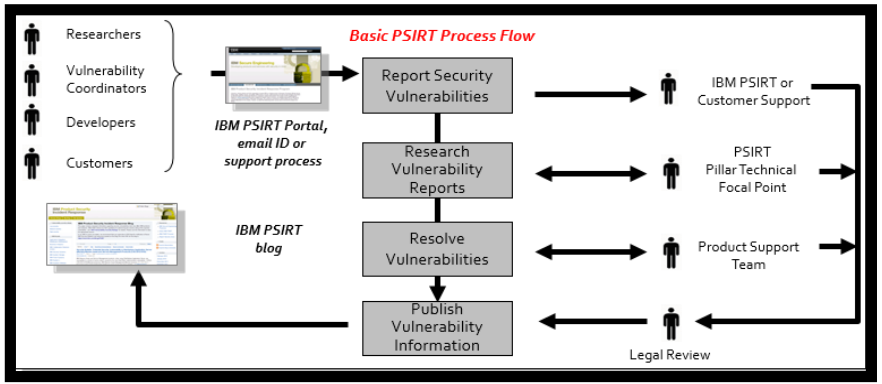
https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/devops/

IBM Secure Development is supported by key tools

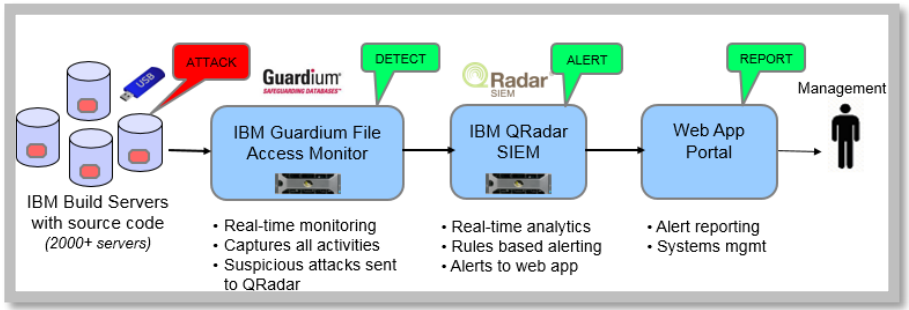
Development Tool Chain & Guidance



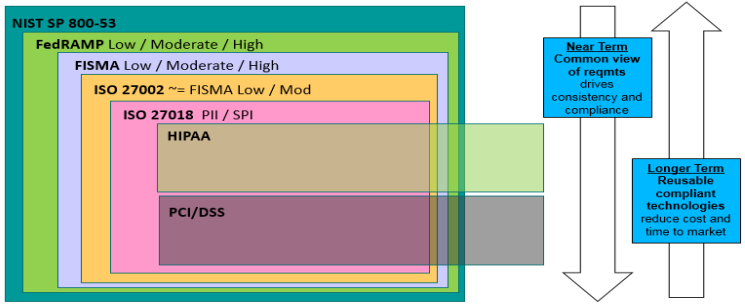
Vulnerability Mgmt & Analytics (PSIRT)



Instrumented Devt Servers with Analytics



Standards Assessment Advisors & Prep Tooling



Executive Dashboard is necessary for Evaluation & Learning

Risk Management Dashboard

Comparison of Issues among Workloads

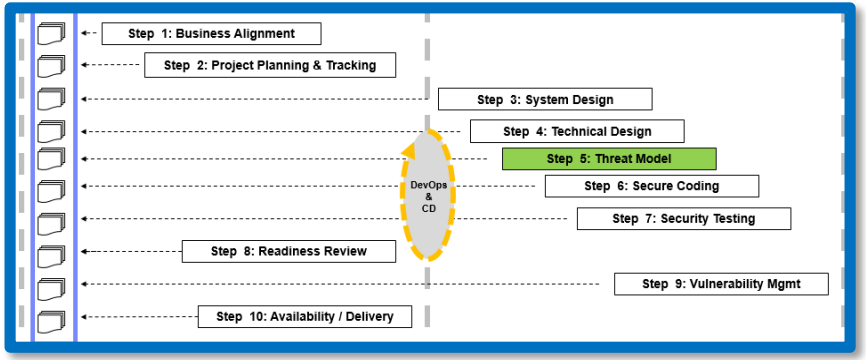
Workload Vulnerability History & Trends

In Compliance
Out-of-Compliance

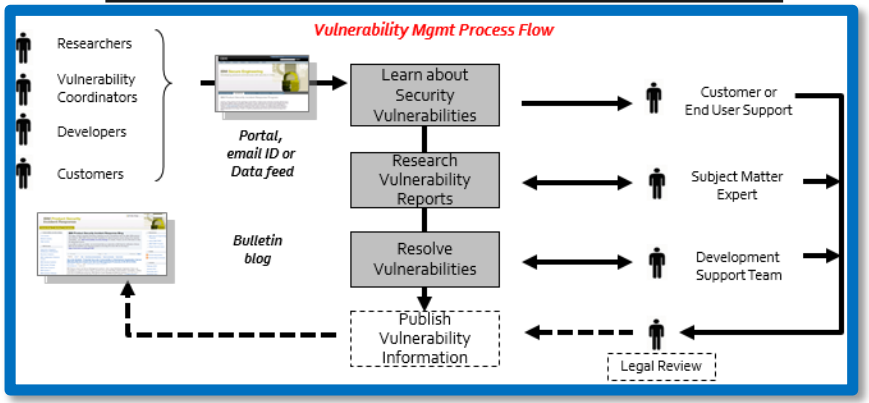
Objectives

Measurements

Secure Development Tracking Activity



Vulnerability Mgmt & Analytics (PSIRT)



Examples of Risk Management Dashboard views

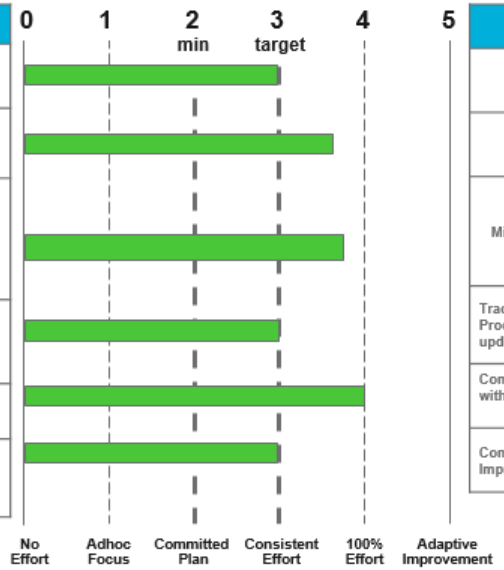
Secure Engineering Performance

Executive Summary, Secure Engineering / PSIRT / Source Code

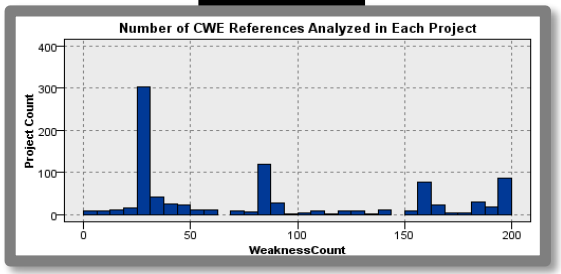
Indicator	Metrics	GAPS
Design Security In	- Threat Model guidance included on Design and Devt plans	Good Threat Model Alignment
Avoiding Vulnerabilities in Coding and Integration	- Coding & Integration addresses vulnerabilities matching Threat Model guidance	Minimal Coding and Integration Escapes

Verify Security in Development with Test Tools and Services	- No Post Devt vulnerabilities
	  - CVSS > 7.0
	  - Threat Model Vulnerabilities
	  - Source = Customer
	  - Source = 3rd Party
		Minimal Testing Escapes

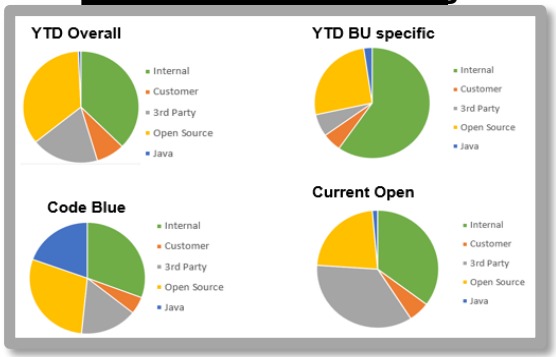
Measure and Maintain Security After Release	- PSIRT Participation with Product Remediation Plans - Post Devt vulnerabilities w/ Advisory Source = IBM	Tracking and scheduling Product, OSS & 3rd Party updates
Rapidly fix Vulnerabilities in Released Code & Services	- PSIRT Guidelines met for Sev 1, 2, 3 & 4	Completing remediation within PSIRT rules
Monitoring and Protection of IBM jewel code and source code	- % SCM & Build Servers monitored	Completing SCM & Build Improvement Plan



Threat Model Statistics



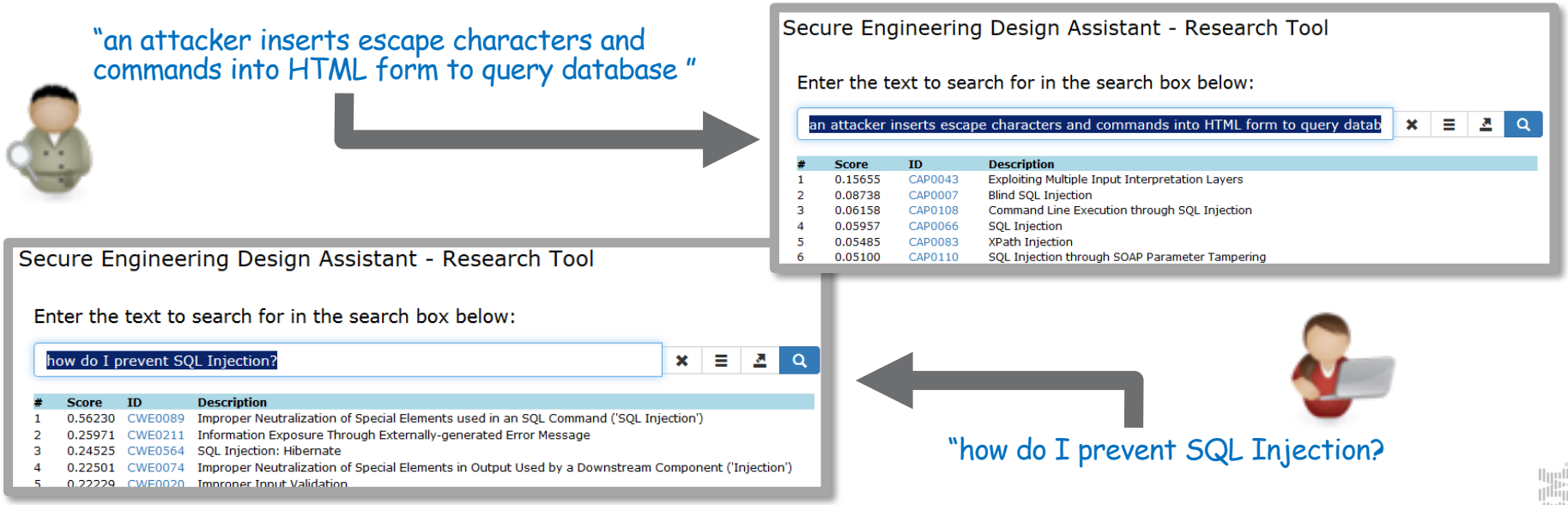
Vulnerability Remediation tracking



We are investing in tools and approaches with the goal of developing Cognitive Solutions for Secure Engineering

One of the major challenges in building an environment for Secure Development is to be able to analyze past history and apply the lessons learned to avoid revisiting past defects. This is particularly difficult to do for security defects because there are so many variations to account for.

We have been working to apply cognitive techniques, in particular, natural language processing to help map instances of security defects (vulnerabilities) to the available catalogs of security knowledge that can drive improvements.



IBM Product Security Incident Response Team (PSIRT) – Vulnerability Management

Mission

The IBM Product Security Incident Response Team (PSIRT) is a global team that sets policies and provides guidance for IBM product teams in the receipt, investigation, communication and analytics of security vulnerability information related to IBM product offerings.

IBM PSIRT is a focal point for clients, security researchers, industry groups, government organizations and vendors to **report** potential IBM product security vulnerabilities. PSIRT provides guidance for IBM product teams in developing an appropriate response.

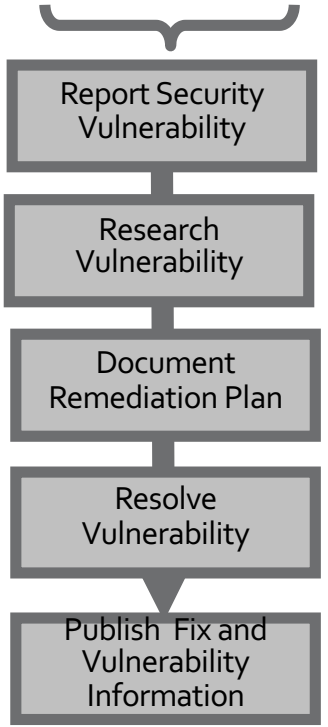
PSIRT overview

- Product Security Incident Response Team (PSIRT) is part of the Secure Engineering Framework (SEF)
- Governs handling and communication for ALL security vulnerabilities known by IBM to exist in supported code
- 1,500+ products, components, and cloud offerings tracked via PSIRT Tool, managed by 2700+ users

- ALL known security vulnerabilities documented in PSIRT Tool.
  This includes issues reported by:
  - Customer
  - Internally discovered
  - Third party reporters
  - Third party vendors
- Satisfies ISO27002 12.6.1 - Management of technical vulnerabilities
  - Participate in PSIRT
  - Receive vulnerability reports
  - Register, track and resolve vulnerabilities

Basic PSIRT Process Flow

- 3rd party reporters and OSS
- IBMers (internally discovered)
- Customers

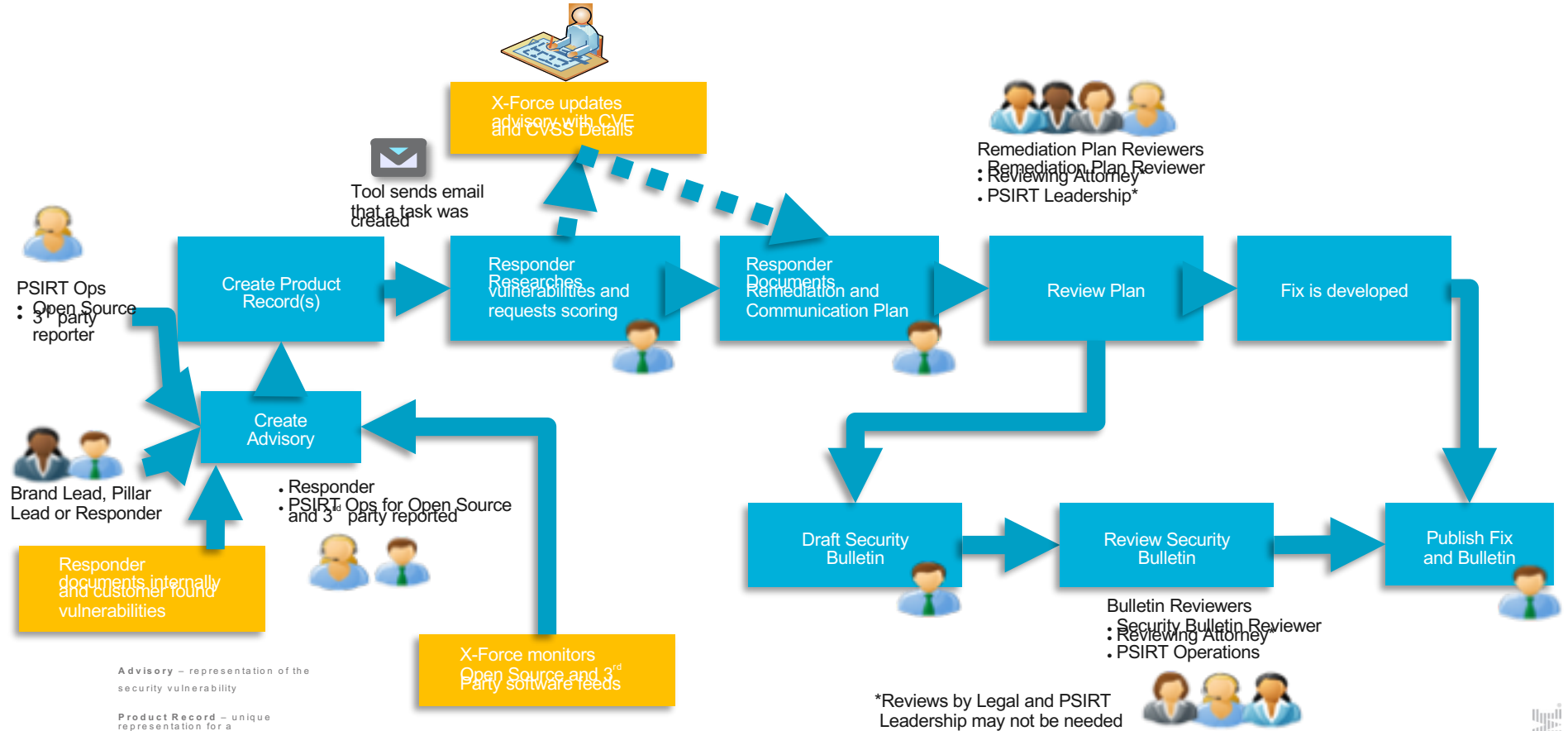


PSIRT communication

- IBM does not publically disclose or confirm security vulnerabilities until IBM has conducted an analysis and issued fixes and/or mitigations
- Methods to communicate security vulnerability information
  - Public communication via Security Bulletin
    - IBM Support Portal
    - IBM PSIRT Blog
    - Subscription or push notifications My Notifications
  - Targeted communication such as z Systems Security Portal and cloud offerings

- Security Bulletins similar to Common Vulnerability Reporting Framework (CVRF)
  - Common Vulnerabilities and Exposures (CVE) common identifier
  - Common Vulnerability Scoring System (CVSS) for communicating the impact
    - Industry open standard for assessing the severity or impact
    - Numeric measure that represents how much concern or attention the vulnerability warrants

Simple scenario PSIRT process workflow



Advisory – representation of the security vulnerability

Product Record – unique representation for a product/offering/component potentially affected

The IBM open technology approval process

Business Guidelines: Each operating unit (divisional or geographical) is responsible for ensuring that its activities comply with the cross IBM Open Source Review Process.

The process ensures business, technical, legal and licensing objectives

Business & Strategic: OSS Use or Standards Participation

Review group (OSSC or STSC) --
- Assesses strategic alignment with business and technical direction
- Recommend approval or actions required for approval
- Identify – License, package, control preferences

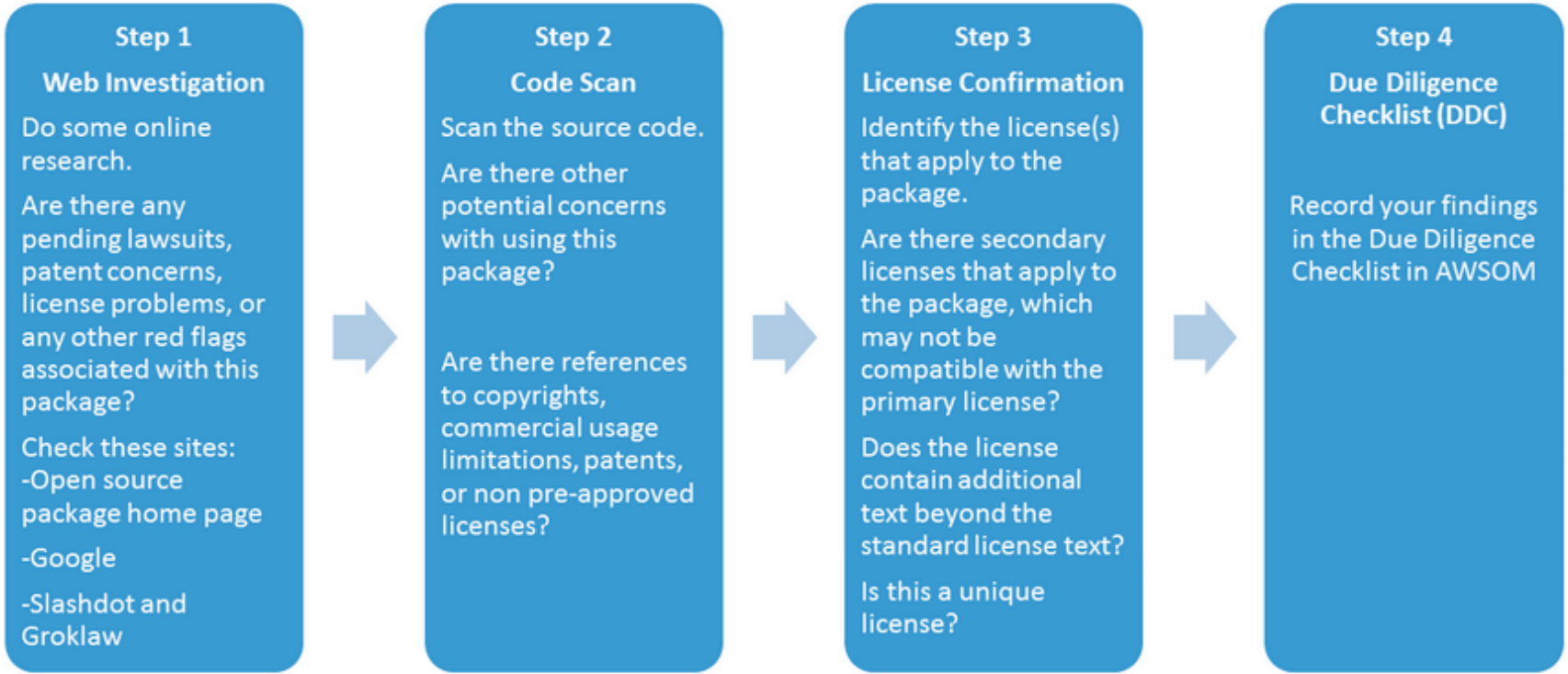
Legal (OSS & Standards)
- Review participation documents for legal risks
- Advise OSSC or SAR leadership regarding acceptability of terms
- Lead or support Agreemnt s or change s
- Ensure IBM participants understand terms
- Identify education needs

Business & Strategic: OSS Contribution or Standards Initiation

Review group (OSSC or STSC) + VP Open Tech
- Assesses strategic alignment with solutions and technical direction
- Recommend approval or redirection
- Identify Business / Strategic issues and required additional reviews

Open Source Core Team and IP Licensing staff
- Process owners
- Review proposals for revenue or license/strategy/code impacts
- Guide / consult identified changes
- Provide check and balance between legal and business
- Recommend approval / disapproval OSSC

All Open Source Package must be approved before use in IBM Products and Services. The review process considers Licensing and other Issues



Secure Engineering Guidance for Open Source

For each Open Source component used:

1. Select an approved version for which no vulnerabilities are reported, or minimally, one with no issues that affect the product or introduce a vulnerability into customer environment.
   - Check OSS project site and release notes
   - Search vulnerability sites (XForce, OSVDB, CVEdetails, NIST NVD, Security Focus)
   - Scan with appropriate scanner (OWASP Dependency Checker, etc.)
2. Obtain files only from approved internal locations.
3. Include the component in the product's threat modeling and system verification testing.
4. Subscribe to each relevant security notification list. Check project site frequently for issues and notify PSIRT if any are reported.
5. Ensure each package is included in Cert. of Originality (including version info).
6. Update bundling and/or usage dependency info as appropriate (including version info).

Notices and Disclaimers

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law

Notices and Disclaimers Con’t.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM’s products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services ®, Global Technology Services ®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli®, Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.