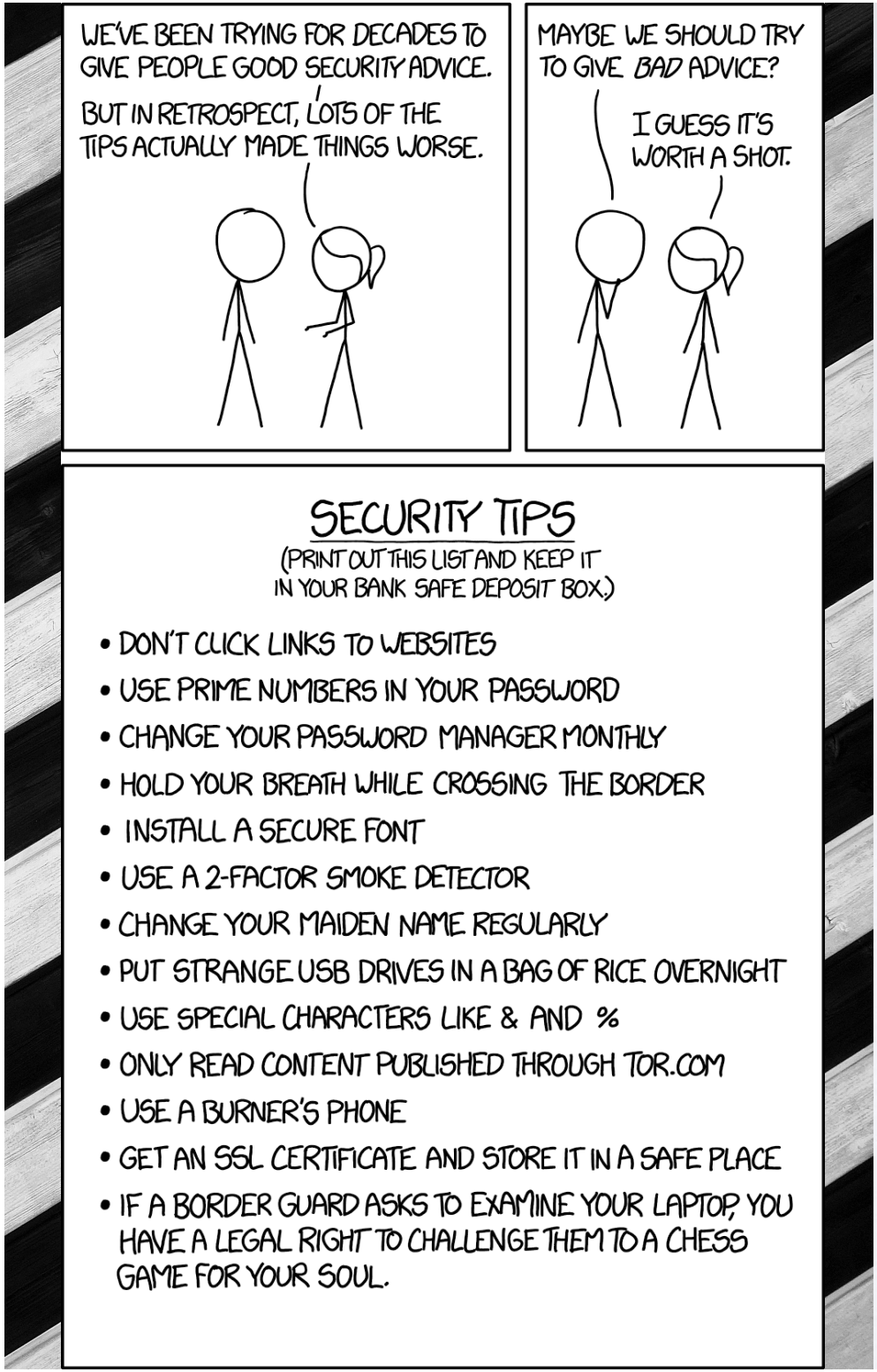
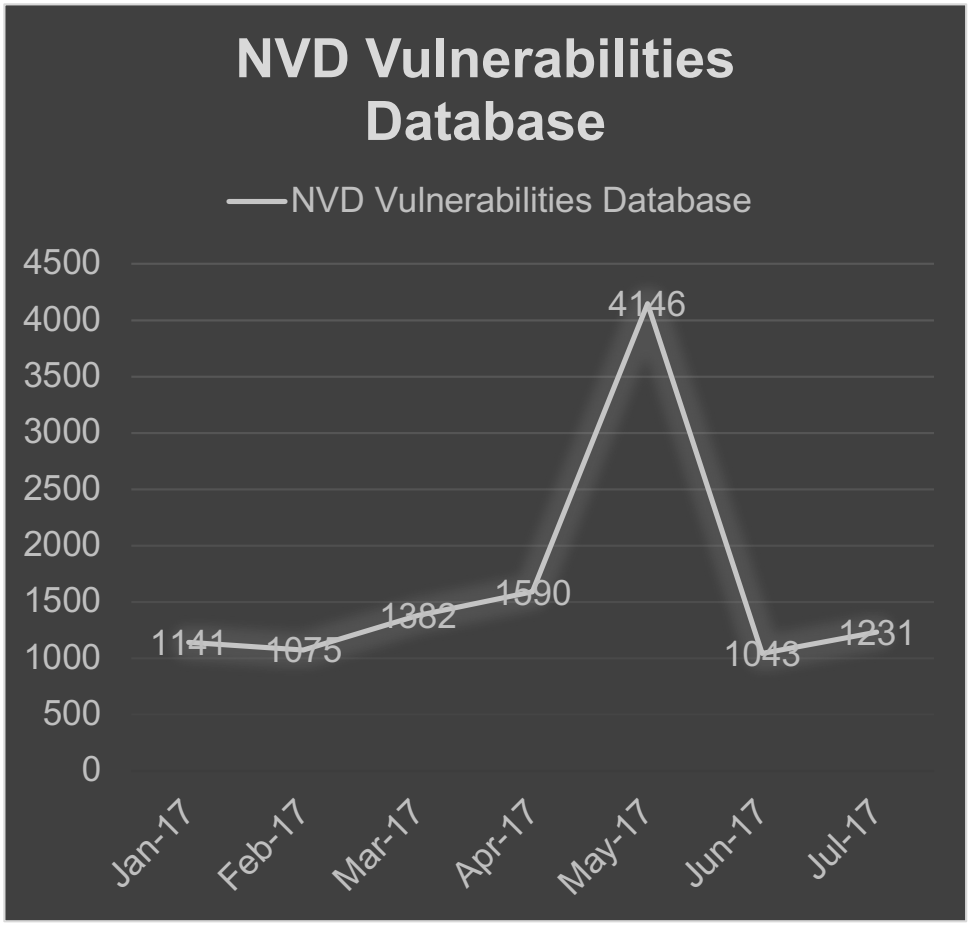


COMPLIANCE AS CODE: POLICY GOVERNED AUTOMATED SECURITY CHECKPOINTS

Nikola Vouk
@nikolavouk

David Gonzalez

Data breach frequency is exponentially increasing with a large number of new vulnerabilities ready for exploitation. For example July ’17 is at 1231…



Last Modified

Printed

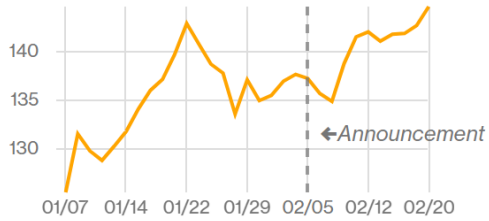
Sources: *http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/*; *https://nvd.nist.gov/*

Security breach hall of famers cross many industries

Anthem

Announced: 02/05/2015

Sources familiar with the investigation tell Bloomberg News that the details of this attack include “fingerprints” of a nation-state, and that China is the main suspect.



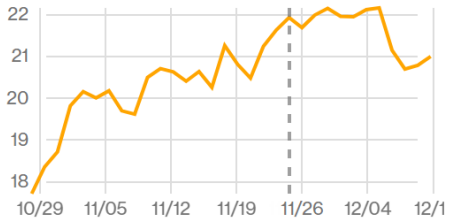
80M

Credit card numbers
Bank accounts
Social Security numbers
Proprietary information
Employee details
Email addresses
Physical addresses
Login credentials

Sony

Announced: 11/25/2014

Hackers broke into its network and exposed employment and salary records, documents and embarrassing private emails between Hollywood executives.



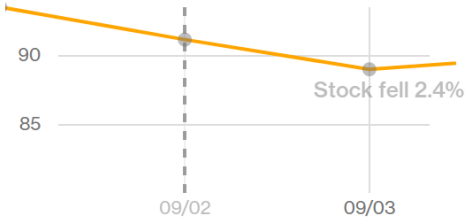
47,000

Credit card numbers
Bank accounts
Social Security numbers
Proprietary information
Employee details
Email addresses
Physical addresses
Login credentials

Home Depot

Announced: 09/02/2014

The company said 56 million payment cards had been stolen, and later disclosed 53 million e-mail addresses had also been pilfered.



109M

Credit card numbers
Bank accounts
Social Security numbers
Proprietary information
Employee details
Email addresses
Physical addresses
Login credentials

JPMorgan

Announced: 08/27/2014

The biggest U.S. bank said a data breach affected 76 million households and 7

83M

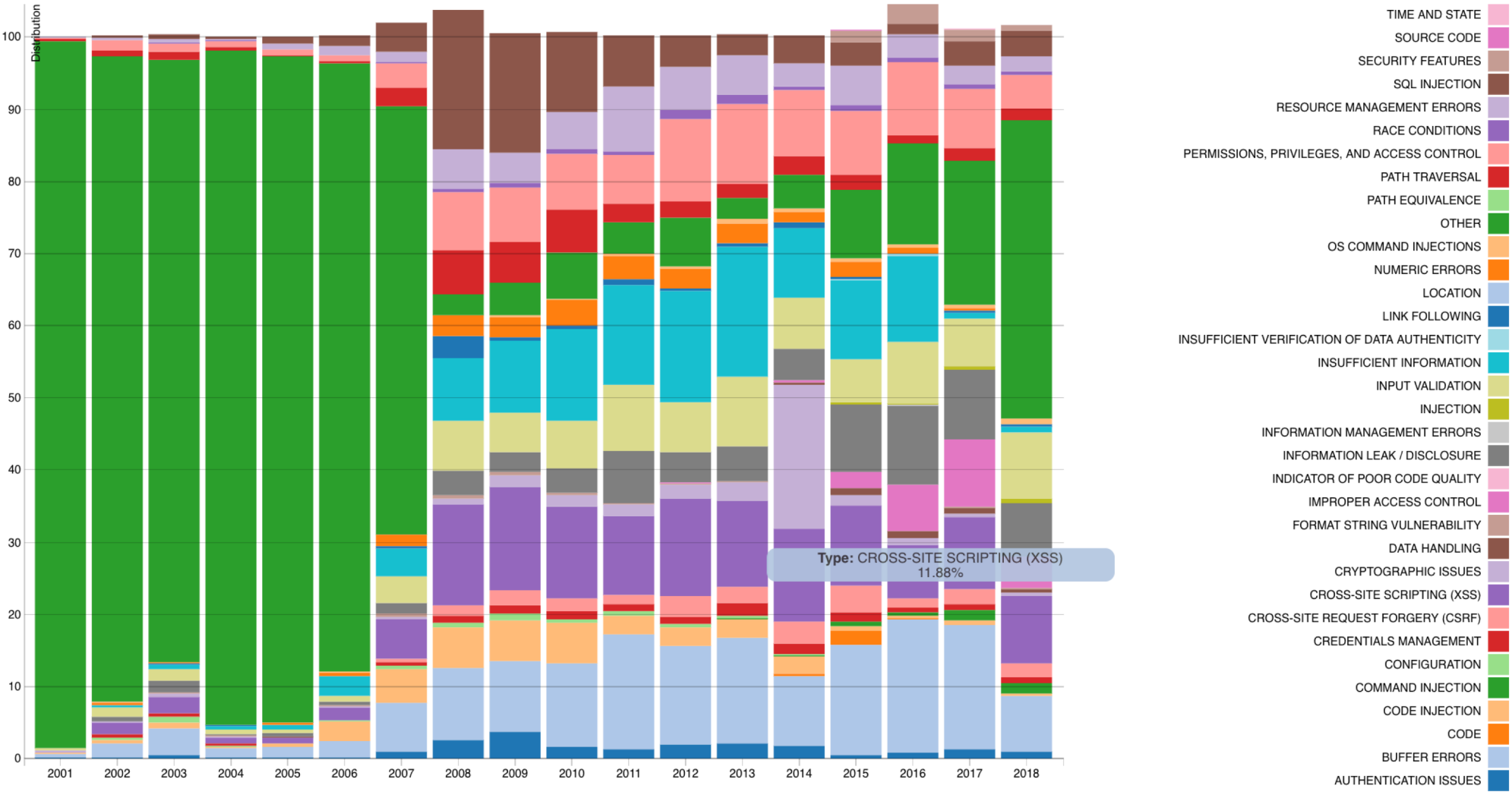
Credit card numbers
Bank accounts
Social Security numbers
Proprietary information

Last Modified

Printed

SOURCE: Source

Vulnerability types have grown in diversity



Source: https://nvd.nist.gov/vuln/visualizations/cwe-over-timehttps://nvd.nist.gov/vuln/visualizations/cwe-over-time

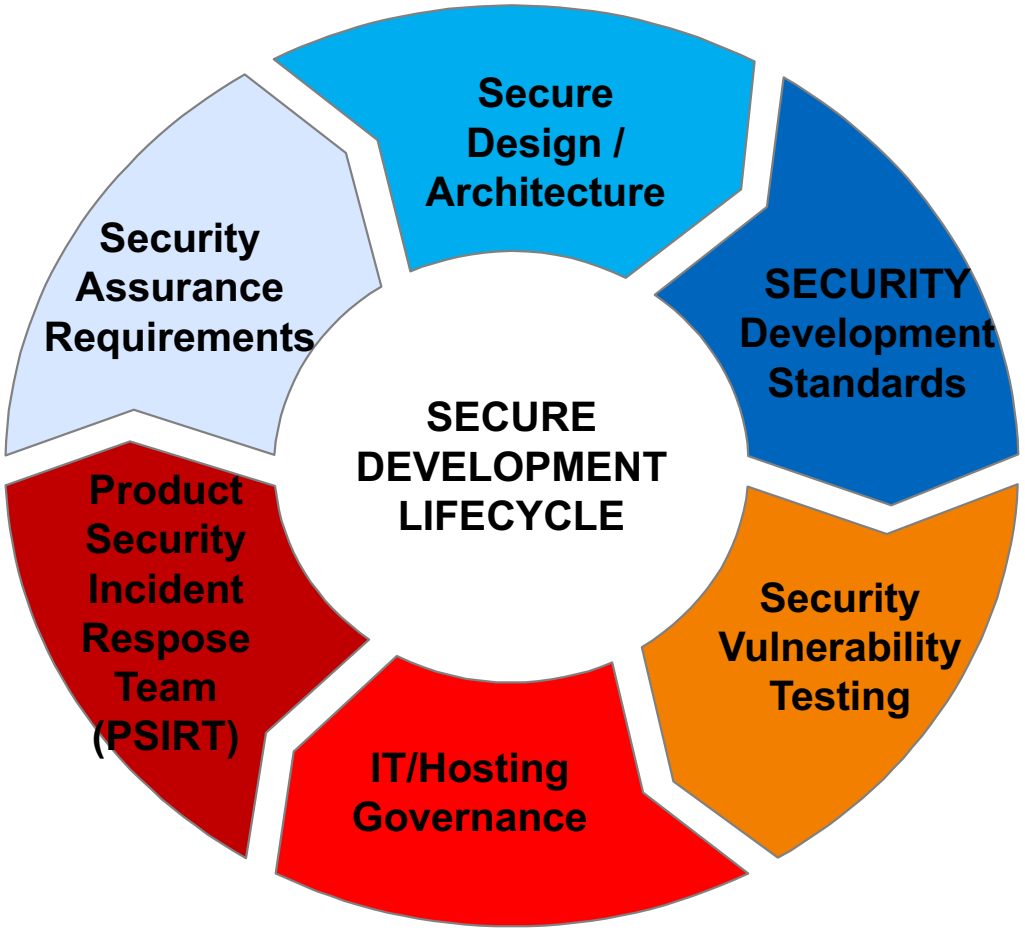
BUSINESS RISK

- REPUTATIONAL RISK
- LEGAL RISK
- FINANCIAL RISK

SOURCE: Source

DEFINING A SECURE ENGINEERING PROGRAM

- ✓Setup Standards/Policies
- ✓Roles and Responsibilities
- ✓Metrics
- ✓Education
- ✓Governance



Last Modified

Printed

SECURE SOFTWARE DEVELOPMENT LIFECYCLE

Elements of an SDLC

- Corporate Commitment
- Legal Contract Policies
- Governance
  - Release Scorecard
  - Artifact Archive
- Software Security Group
  - Security Champions
  - Security Architects
- Security Education
- Secure Architecture
  - Secure-by-design
  - Security Assurance/Threat Modeling
  - Secure Architecture Repository
- Secure Development Standards
  - Known Vulnerability Remediation
  - Critical Vulnerability Toolbox
  - Developer Guidance
- Penetration Testing
- Product Security Incident Response Team (PSIRT)
  - Vulnerability Remediation SLA
  - Support Commitment
  - Forensic Incident Support
- Third Party Certification

I. Designed to complement development

II. Evolving Set of Elements of Framework

III. Standards define 'Security Compliance for Applications'

IV. Governance to confirm assurances

Last Modified

Printed

Target Vulnerabilities

REMEDIATION OF ALL Discovered Critical SECURITY VULNERABILITIES PRIOR TO DELIVERY to Penetration Testing.

Critical Security Vulnerabilities are:

- OWASP Top 10
- SANS Top 25
- ClickJacking
- Libraries with Known Vulnerabilties

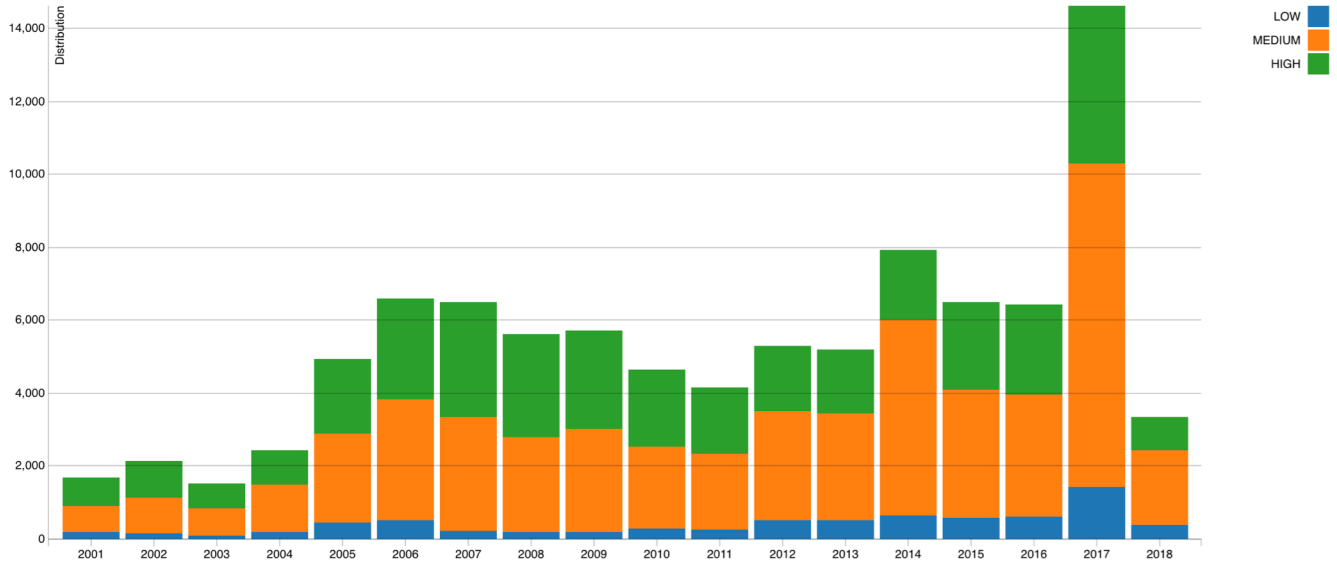
SOURCE: Source

PSIRT Remediation – Known Vulnerability Remediation

Severity	Patch/Remediate	CVSS
Critical	2 days	9.0-10.0
High	14 days	7.5 – 8.9
Medium	30 days	4.0 – 7.4
Low	60 days	0.1 – 3.9

CVSS Severity Distribution Over Time

This visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of LOW, MEDIUM and HIGH is based upon the CVSS V2 Base score. For more information on how this data was constructed please see the NVD CVSS page.

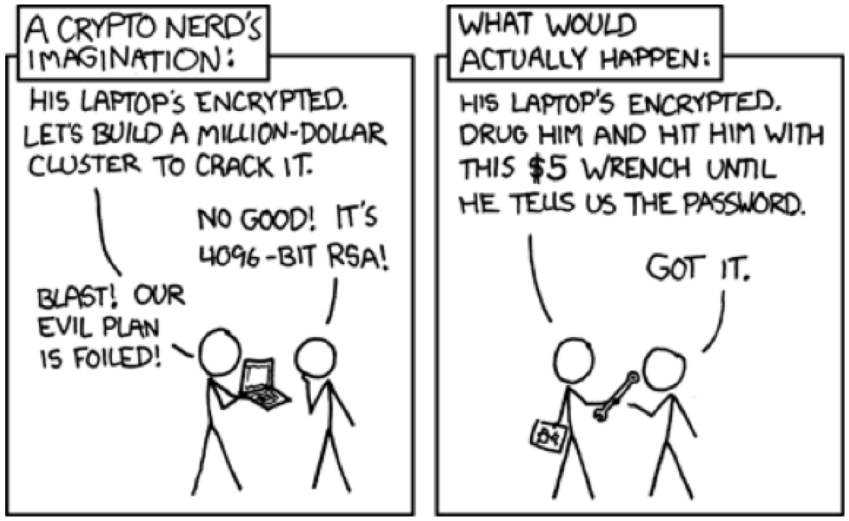


Last Modified

Printed

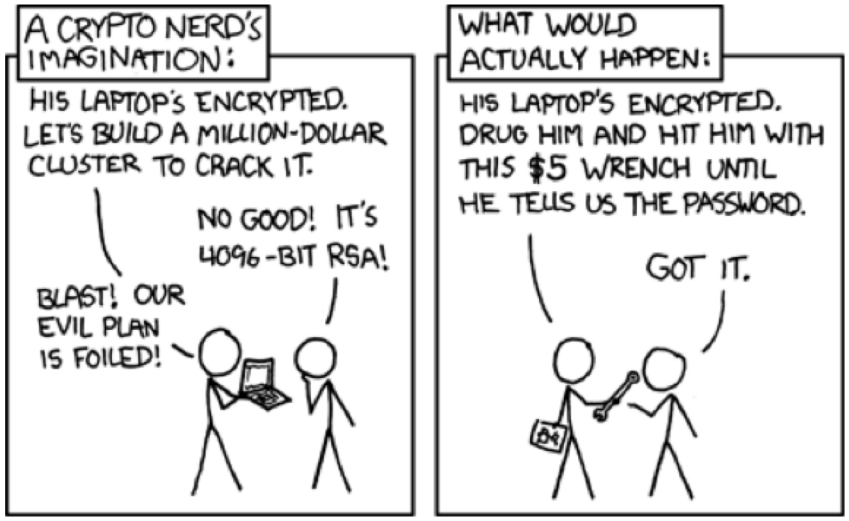
PEN TESTING

Severity	Policy
Critical	Must Remediate
High	Must Remediate
Medium	Must Remediate
Low	Must Remediate

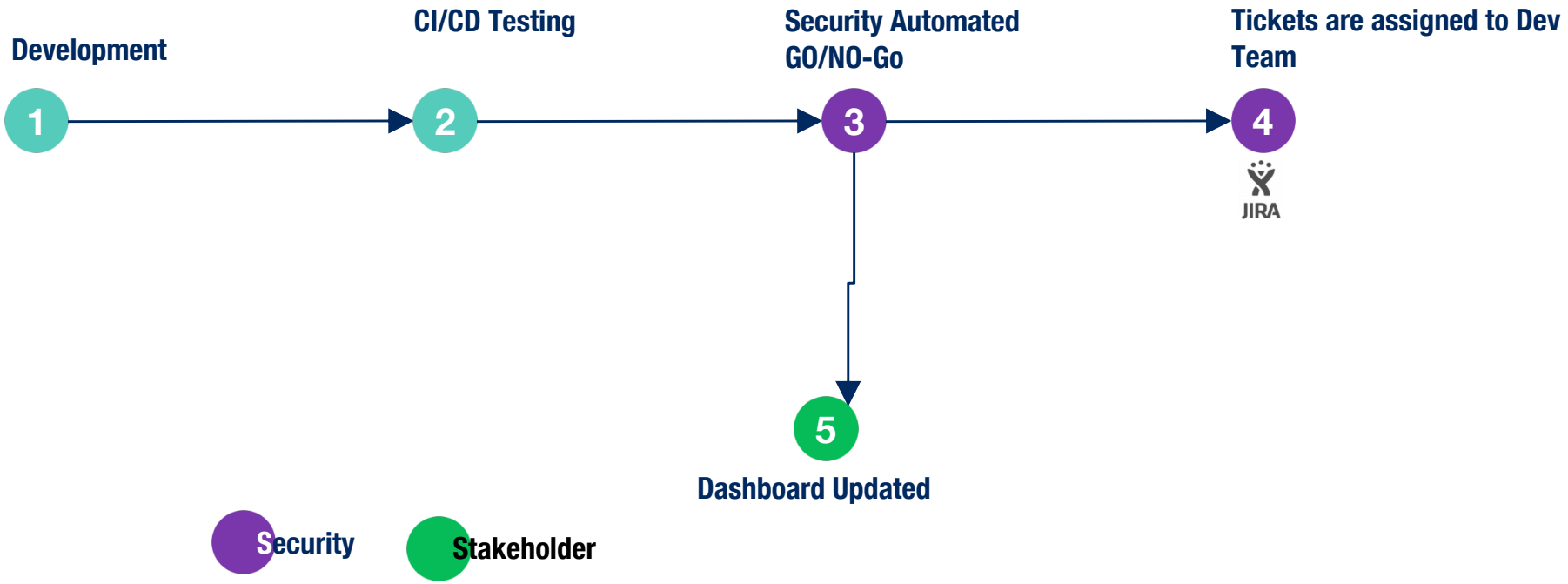


PEN TESTING

Severity	Policy
Critical	Must Remediate
High	Must Remediate
Medium	Not Required
Low	Not Required

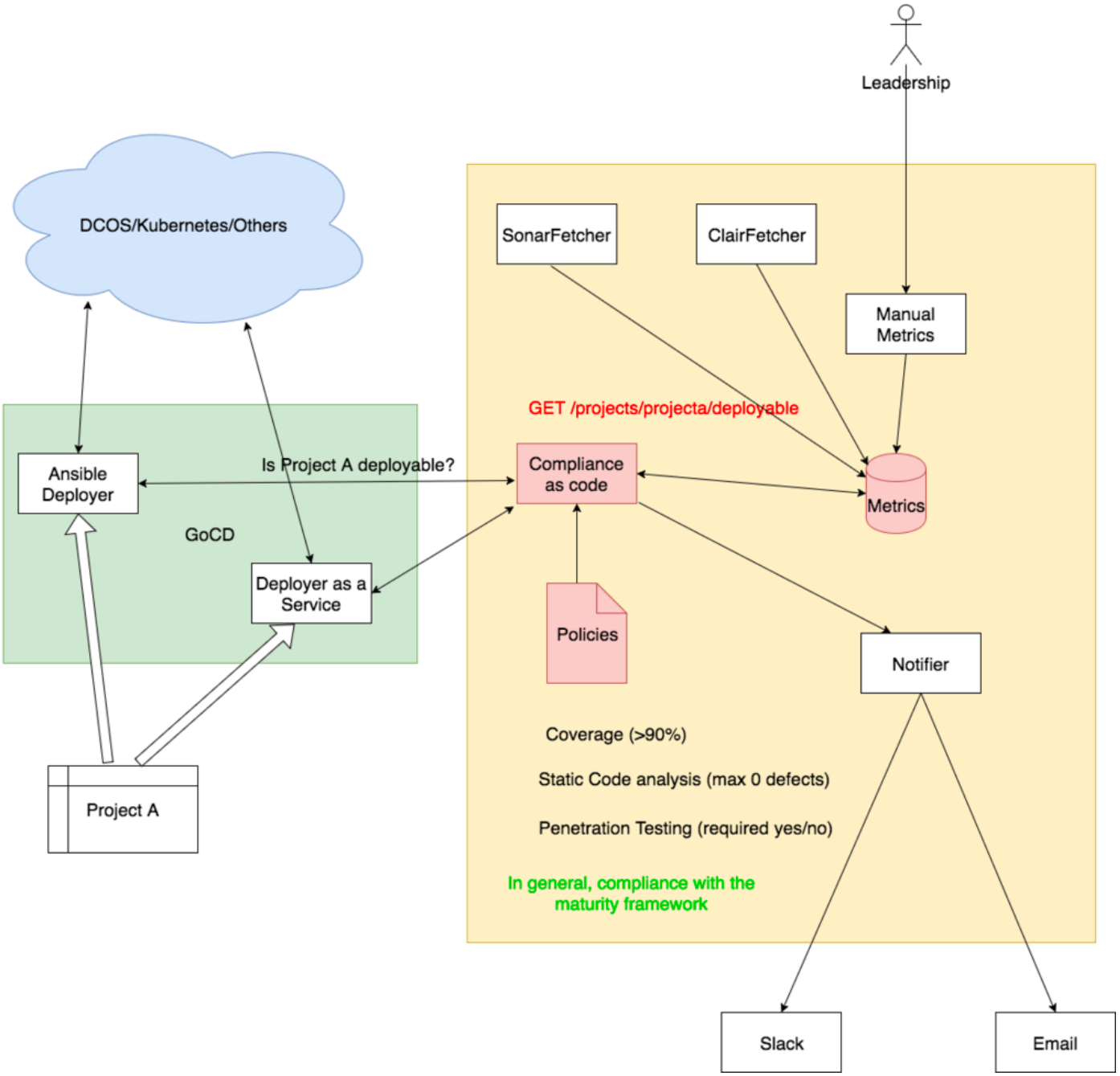


Governance Workflow



Last Modified

Printed



Last Modified

Printed

Create Arbitrary Policy on results from unique data source values

```
metrics "coverage" {
  mandatory = true
  min {
    value = 90.0
    units = "percentage"
  }
}

metrics "clair_errors" {
  max {
    value = 10.0
    units = "items"
  }
}

metrics "static_code_analysis_errors" {
  max {
    value = 0.0
    units = "items"
  }
}
```

Policy Definition – Standards to measure compliance

Domain Specific Language

Metric Names	Arbitrary Text matching data types from Unique data source
Operators	Max Min Range
Units	Floats

COMPLIANCE AS CODE

Dashboard

Real Time Feed

More Info

Sonarqube Status Deployable

test

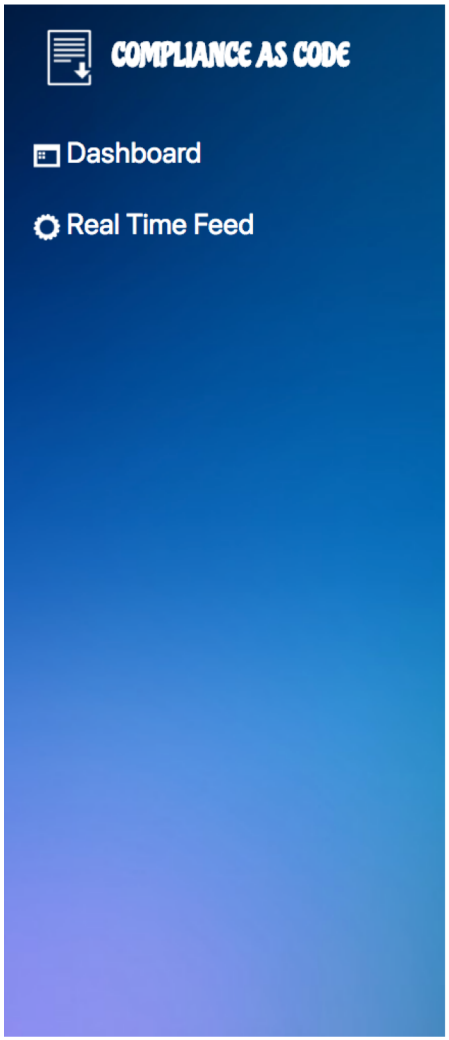
Product Owner: Owner McMahon
Technical Lead: Techie McGowen
UX Lead : Someone Notustington

More Info

Sonarqube Status Deployable

com.mckinsey.clientnews:cn-jobs

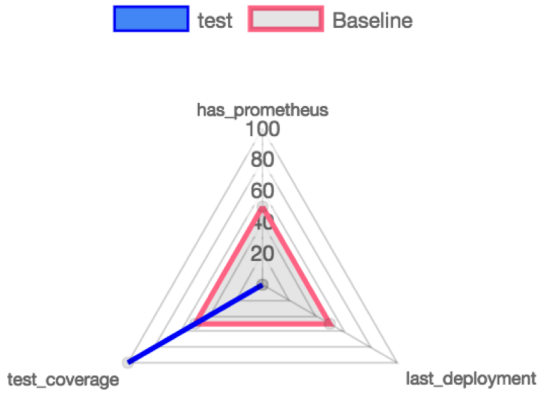
Product Owner: -
Technical Lead: -
UX Lead : -


COMPLIANCE AS CODE
Dashboard
Real Time Feed
Deployment Feed
Project test has evaluated successfuly for deployment 2018-04-10T16:26:11Z
Project nsm has failed evaluation for deployment at 2018-04-10T16:26:05Z
Project test has evaluated successfuly for deployment 2018-04-10T16:25:58Z
Project test has failed evaluation for deployment at 2018-04-10T16:25:43Z
Project test has failed evaluation for deployment at 2018-04-10T16:24:59Z
Project test has evaluated successfuly for deployment 2018-04-10T16:24:20Z
Project test has failed evaluation for deployment at 2018-04-10T16:18:39Z
Project test has evaluated successfuly for deployment 2018-04-10T16:18:31Z

COMPLIANCE AS CODE

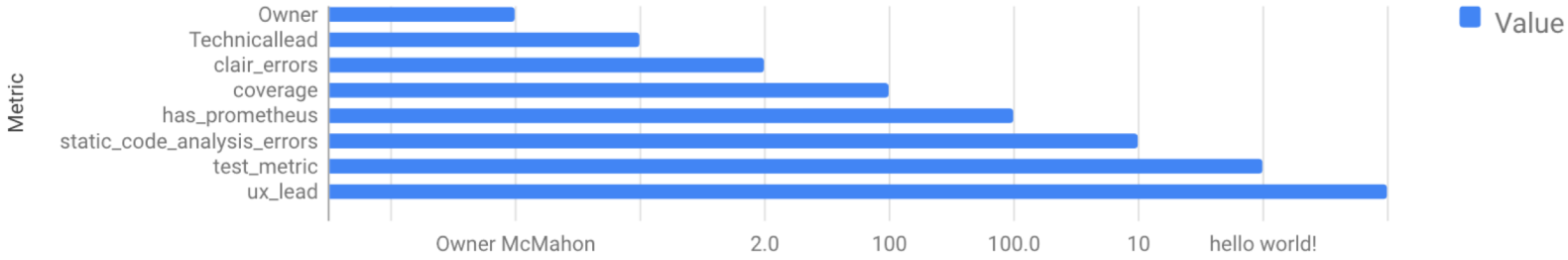
- Dashboard
- Real Time Feed

Project Maturity



More Data

DevOps Metrics



Thank you

Nikola Vouk
nikvouk@gmail.com

David Gonzalez
dagonza1983@gmail.com