



Collecting PSIRT Metrics That Drive Change

Steve Hart, CISSP,
CCSP

Head of Product
Security, Research
and Development

Sallie Newton, CISSP,
PCI-P, GISP

PSIRT Lead, Research
and Development

Brian English

Product Security
Lead, Technical
Support

About SAS Institute

40+ years of analytics innovation

Solutions

- › Advanced Analytics
- › AI Solutions
- › Business Intelligence & Analytics
- › SAS & Cloud Computing
- › Customer Intelligence
- › Data Management
- › Decision Management
- › Fraud & Security Intelligence
- › Solutions for Hadoop
- › IoT Analytics Solutions
- › Performance Management
- › Personal Data Protection
- › Risk Management
- › Supply Chain Intelligence

Company Facts & Financials

Customer

Number of Countries Installed

SAS has customers in 147 countries.

Total Worldwide Customer Sites

Our software is installed at more than 83,000 business, government and university sites.

Fortune Global 1000® Customers

92 of the top 100 companies on the 2018 Fortune Global 1000® are SAS customers.

Employee

Worldwide Employees

13,939 total employees

Breakdown by Geography

United States: 6,908

World Headquarters (Cary, NC): 5,545

Canada: 312

Latin America: 491

Europe, Middle East and Africa: 3,592

Asia Pacific: 2,601

Financial

Worldwide Revenue

2018 Revenue: US\$3.27 billion

[Historical revenue data](#)

Reinvestment in R&D

2018 R&D investment: 26% of revenue

Agenda

1

Establishing a PSIRT
at SAS Institute

2

PSIRT Metrics in
Research and
Development

3

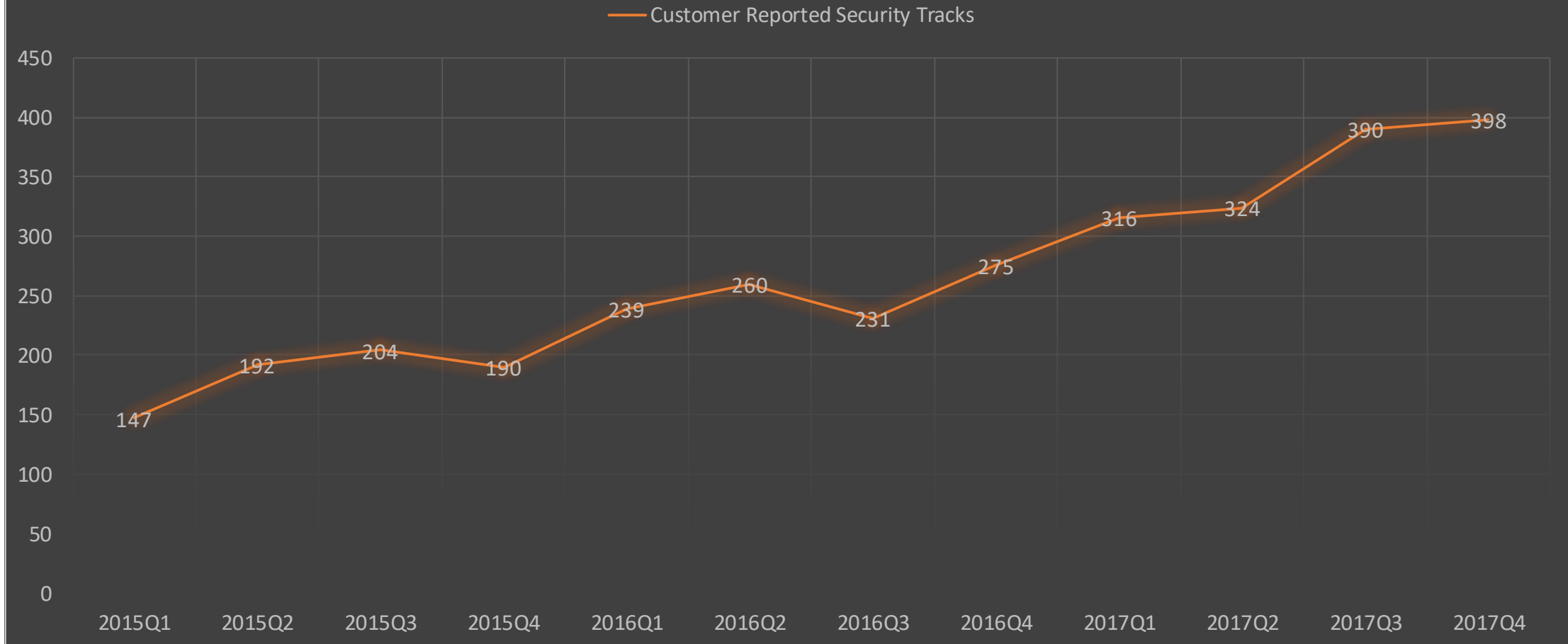
PSIRT Metrics in
Customer Support

1

Establishing a PSIRT at SAS Institute

Steve Hart, CISSP, CCSP
Head of Product Security, Research and Development

Customer Reported Security Tracks



What's happening in the industry around this same timeframe that could be driving all of this activity?

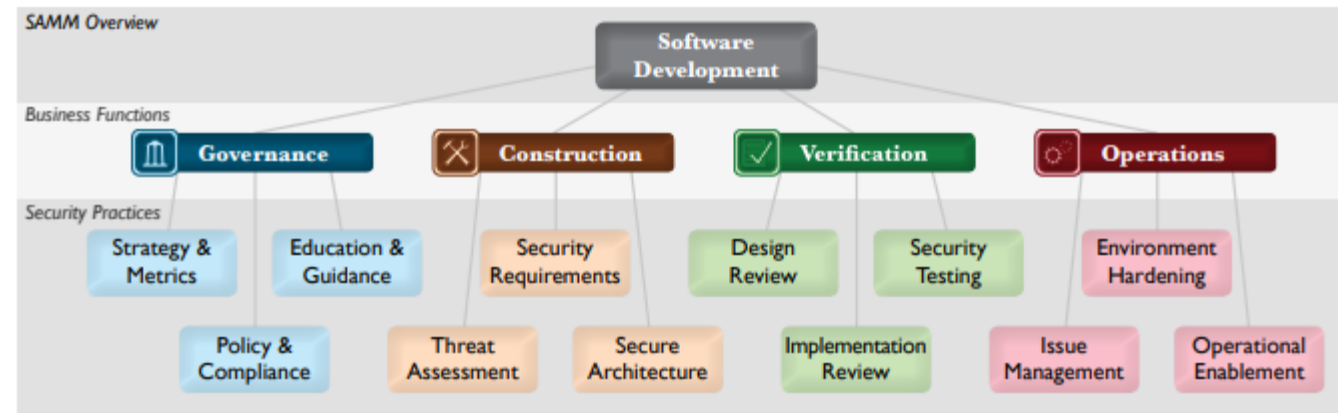
A horizontal timeline of security breaches from 2015 to 2017, enclosed in a red double-headed arrow. The breaches are: Sony Breach (heart icon), RSA Security Breach (hand with lightning bolt icon), US OPM Breach (sheep icon), Yahoo Breach (Java logo icon), Target Breach (Java logo icon), Mirai Botnet (dark blue box with white text), Adobe Breach (Adobe logo icon), eBay Breach (eBay logo icon), Petya Ransomware (Petya Ransomware logo icon), JPMC Breach (JP Morgan Chase logo icon), and Home Depot Breach (Home Depot logo icon).

Establishing PSIRT at SAS Institute

Phase 1

- 2016

- Reactive -> Proactive
- Establish a framework for how to operate
- Organize around industry standards, best practices and guidelines
 - FIRST
 - CWE
 - CVE
 - CVSS
 - OWASP
 - NIST
 - BSIMM
 - SAMM

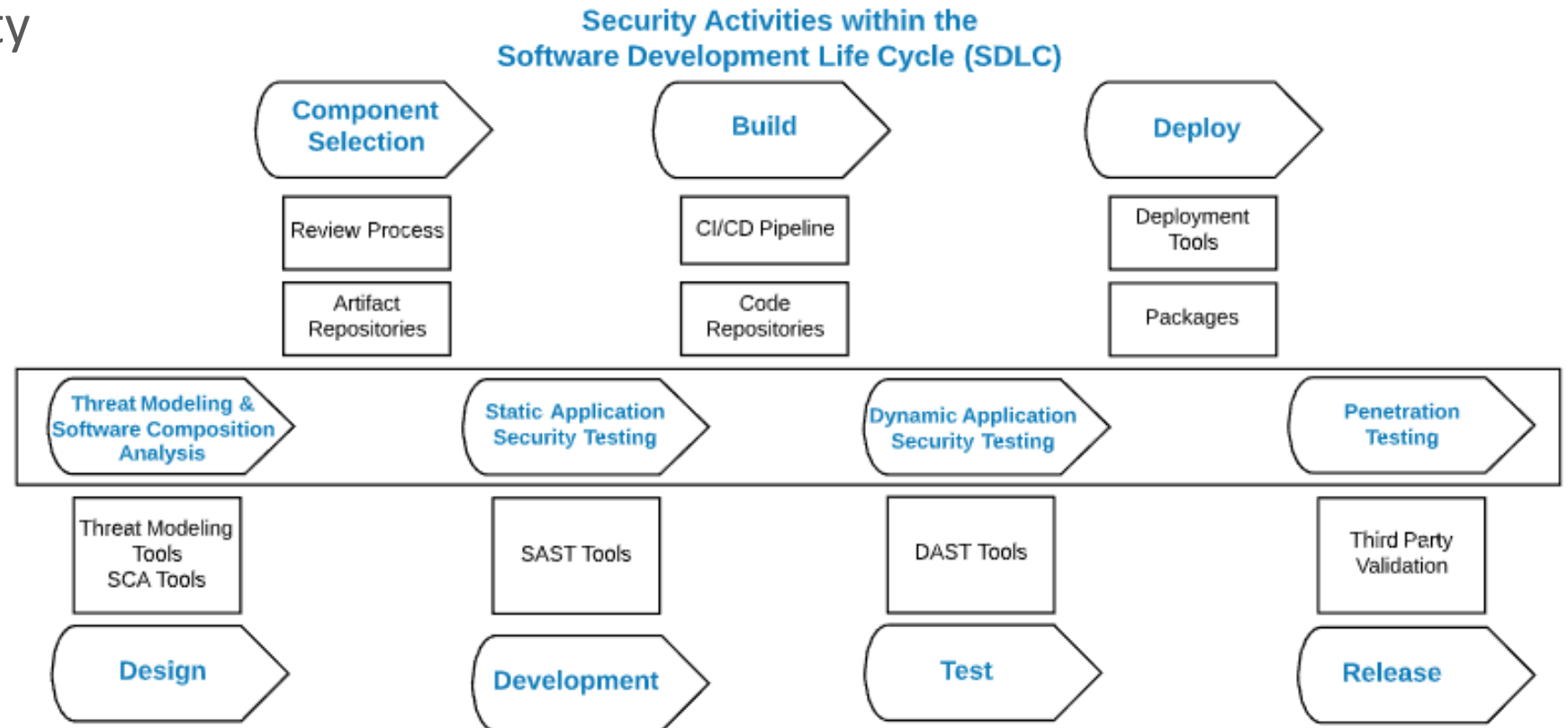


Source: <https://owasp.org/www-project-samm/>

Establishing PSIRT at SAS Institute

Phase 2

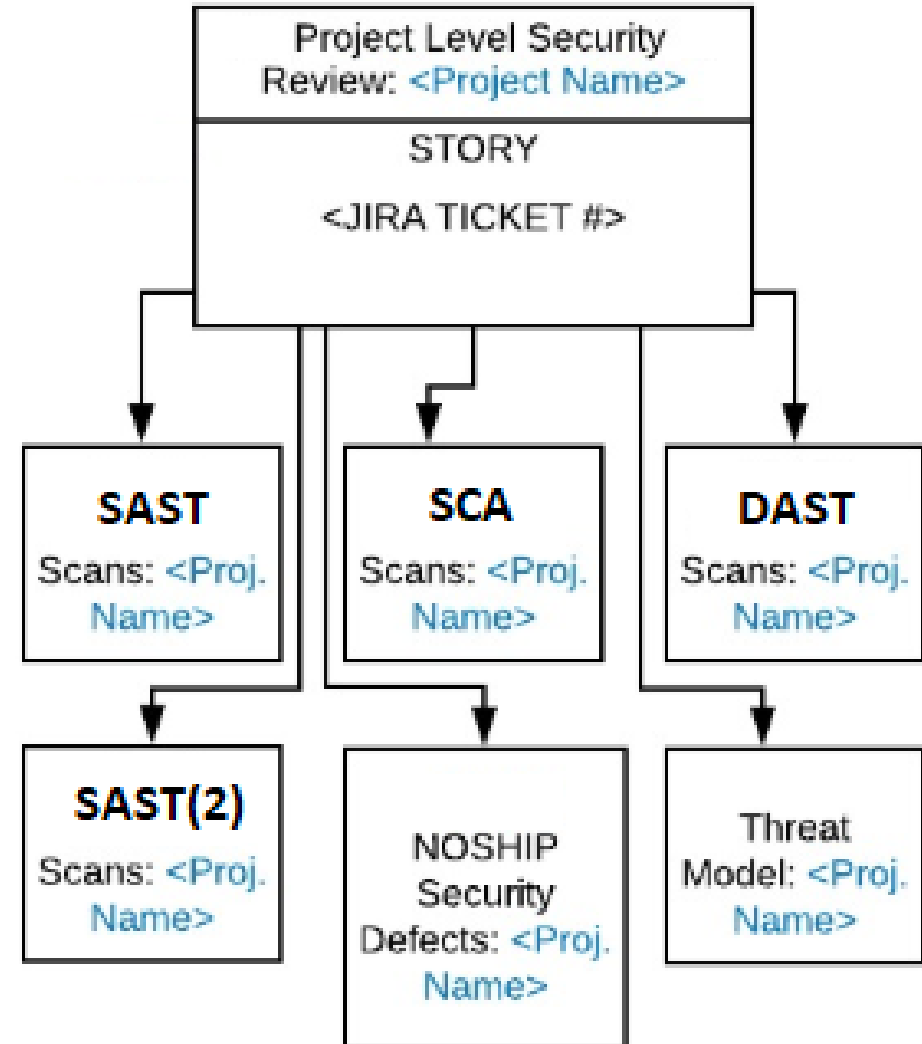
- 2017
 - Implementation of a Software Security Program
 - Roll out security tooling and guidance
 - Establish Security Champions
 - Shift Left



Establishing PSIRT at SAS Institute

Phase 3

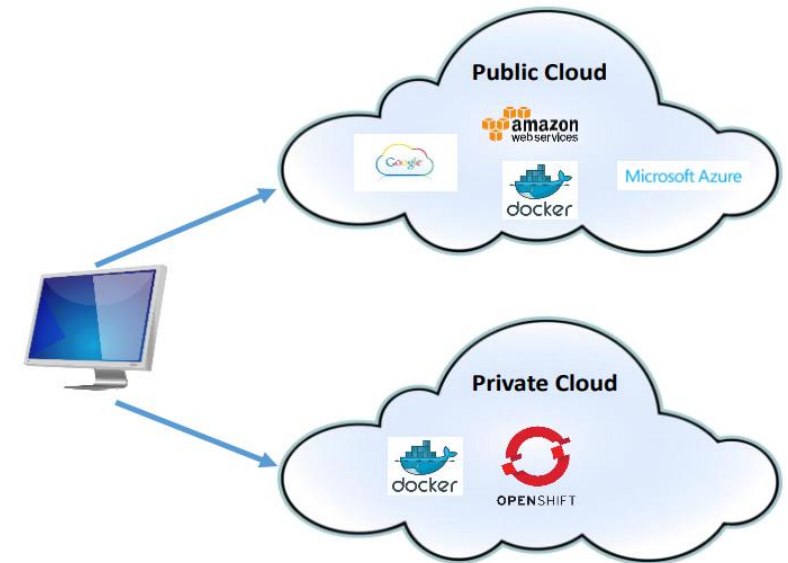
- 2018
 - 100% participation across Research & Development
 - Streamlined process
 - Collection of security artifacts tracked in project level security reviews



Establishing PSIRT at SAS Institute

Phase 4

- 2019-2020
 - Maturing and optimizing security practices
 - security architecture design review
 - secure coding developer guidance
 - internal penetration testing
 - root cause analysis
 - Automation - go faster to support CI/CD and shorten PSIRT remediation timelines
 - Expand scope to cover new technologies (Cloud-Native, Containers, K8s)
 - Build security culture
 - security open forums
 - cybersecurity month activities
 - revamp security champions program



Source: <https://communities.sas.com/t5/SAS-Communities-Library/Running-SAS-Analytics-in-a-Docker-container/ta-p/469645>

2

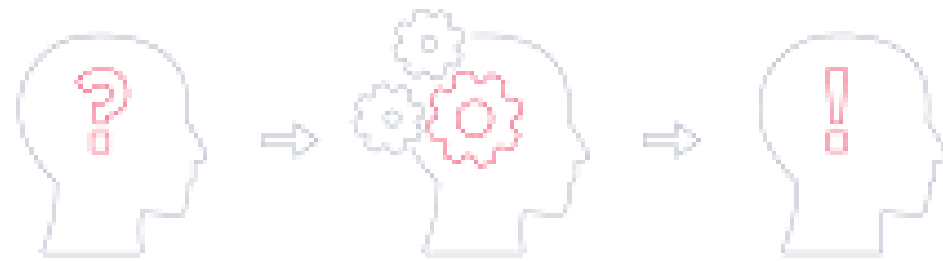
PSIRT Metrics from Research and Development

Sallie Newton, CISSP, PCI-P, GISP
PSIRT Lead, Research and Development

PSIRT Metrics from R&D

There are 5 phases to our PSIRT process:

- Vulnerability Discovery
- Vulnerability Triage
- Vulnerability Remediation
- Vulnerability Disclosure
- Post-Incident Review A.K.A



LESSONS LEARNED

PSIRT Metrics from R&D

What are
metrics?



a method of measuring something

PSIRT Metrics from R&D



Why metrics matter?

PSIRT Metrics from R&D

COMPLIANCE



ISO | NIST | GDPR | FedRAMP | Enterprise | FIPS

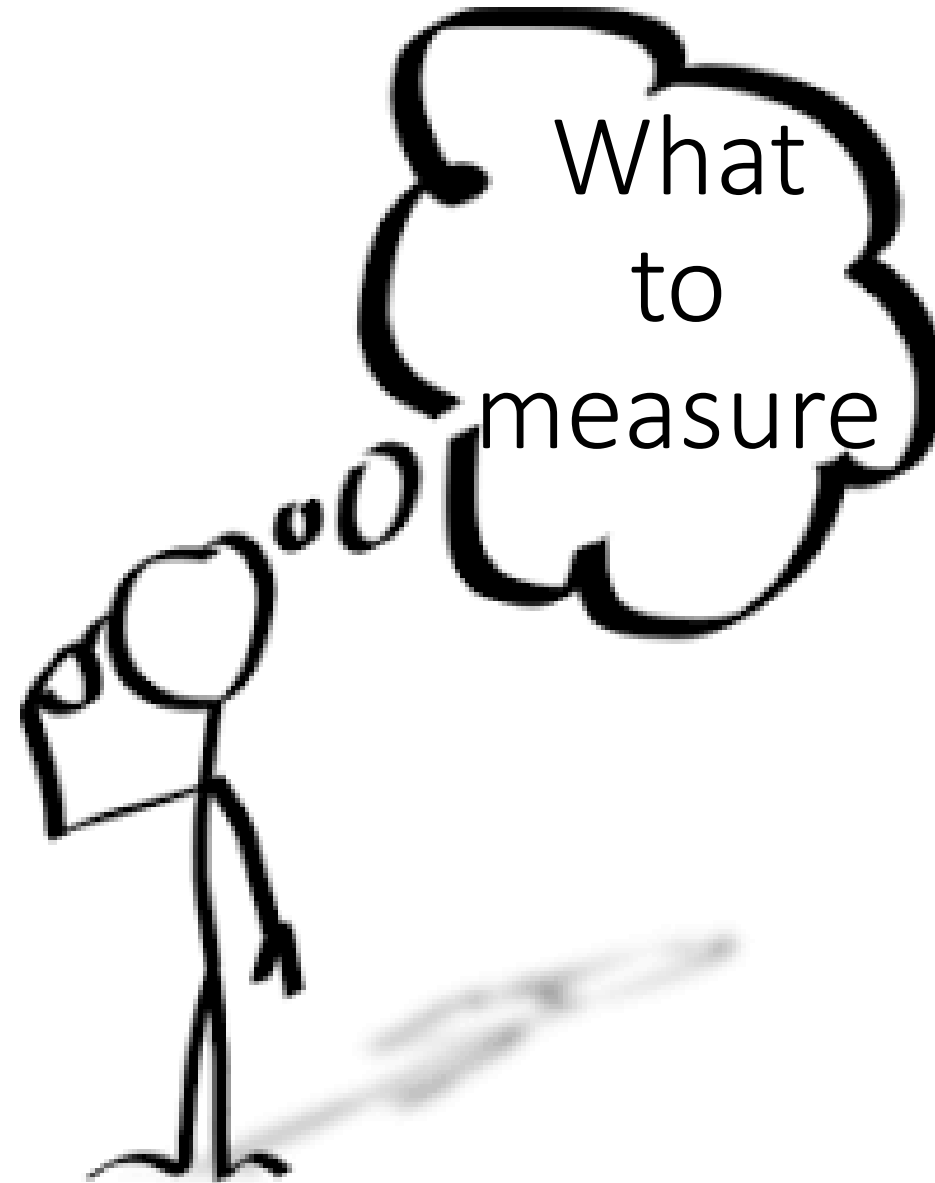
PSIRT Metrics from R&D



Vulnerability Remediation Timeline



PSIRT Metrics from R&D



PSIRT Metrics from R&D



Threat
Modeling
Metrics

PSIRT Metrics from R&D

Vulnerability
Discovery

External

Internal



PSIRT Metrics from R&D

Mitigation:
Patches
vs
Next Release

**To Patch, Or
Not To Patch**
THAT IS THE QUESTION!



?

PSIRT Metrics from R&D

Types of Vulnerabilities



PSIRT Metrics from R&D

SAS Top Five OWASP Vulnerabilities



PSIRT Metrics from R&D

OWASP Top 10 Vulnerabilities

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE) [NEW]
A5:2017-Broken Access Control [Merged]
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization [NEW, Community]
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

PSIRT Metrics from R&D



SAS Top 10 - 2019

- Injection
- Misconfiguration
- Broken Access Control
- Insecure Deserialization
- XSS
- Sensitive Data Exposure
- Using Components w/known vulnerabilities
- Broken Authentication

PSIRT Metrics from R&D

SAS Top 10 - 2019	
Frequency	Vulnerability
18	A9:2019 - Using Components w/known vulnerabilities
13	A5: 2019 - Broken Access Control
11	A7:2019 - XSS
7	A2:2019 - Broken Authentication
7	Other (None OWASP Top 10)
6	A1:2019 - Injection
3	A3:2019 - Sensitive Data Exposure
2	A8:2019 - Insecure Deserialization
1	A6:2019 - Misconfiguration
68	

Product Vulnerabilities
Prioritized by Frequency

PSIRT Metrics from R&D

SAS Top 5 - 2019		OWASP Top 10 - 2017
Frequency	Vulnerability	A1:2017-Injection
18	A9:2019 - Using Components w/known vulnerabilities	A2:2017-Broken Authentication
13	A5: 2019 - Broken Access Control	A3:2017-Sensitive Data Exposure
11	A7:2019 - XSS	A4:2017-XML External Entities (XXE) [NEW]
7	A2:2019 - Broken Authentication	A5:2017-Broken Access Control [Merged]
6	A1:2019 - Injection	A6:2017-Security Misconfiguration
55		A7:2017-Cross-Site Scripting (XSS)
		A8:2017-Insecure Deserialization [NEW, Community]
		A9:2017-Using Components with Known Vulnerabilities
		A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Total 55 of 68 = 81% of our vulnerabilities reside in 5 domains

PSIRT Metrics from R&D



Training, Awareness & Education

PSIRT Metrics from R&D

Module 101 - Introduction To Application

Module 150 - Protecting Sensitive

Module 460 - Integrating Security into Agile Projects [\[edit\]](#)



a blend

standards, cor
standards such as
carefully reviewed and inc
Different security metadata
classification and authentication two

the contr
of the ap
Presente
Hackers
intercept th

Three level
on product
easiest to ir
is sent from
intercept th

returned messages to the client,
files.
When errors happen, developers
obfuscation by giving generic messages. When a
level process receives the message it won't have

common forms.
Injection prevent
commands, app
using parameters

Mismatches n
files needs ca
file that a hack
seen by the ac

An [access-control matrix](#) is used to list the type of
computer function needed, by the various roles that will be
using those functions. Diagrammed, it is easy to see who
needs what. Program coding then can apply logic so that
access controls can be enforced.

PSIRT Metrics from R&D



SAS Top 5 - Training Domains

	Training Domains
1	A9:2019 - Using Components w/known vulnerabilities
2	A5: 2019 - Broken Access Control
3	A7:2019 - XSS
4	A2:2019 - Broken Authentication
5	A1:2019 - Injection

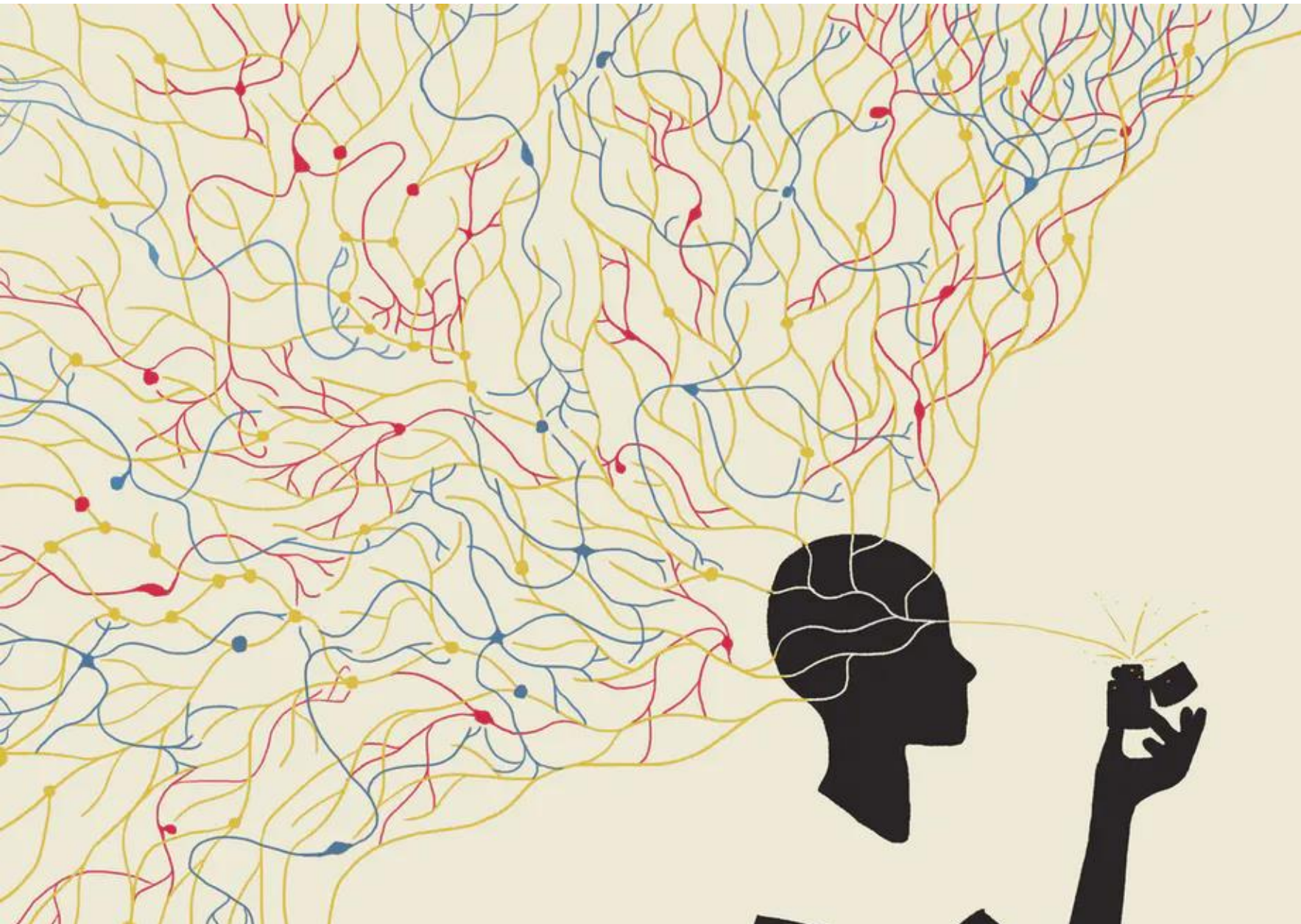
PSIRT Metrics from R&D

Guidance - Top Five Testing Recommendations

SAS Top 5 - Testing Domains	
1	A9:2019 - Using Components w/known vulnerabilities
2	A5: 2019 - Broken Access Control
3	A7:2019 - XSS
4	A2:2019 - Broken Authentication
5	A1:2019 - Injection



PSIRT Metrics from R&D



Support Security
and Compliance
Decisions with
Metrics

3

PSIRT Metrics from Customer Support

Brian English
Product Security Lead, Technical Support

PSIRT Metrics from Customer Support

What can be learned from Customer Support Data?

- **Measure cost and manpower required to address customer reported security vulnerabilities.**
- **Scope PSIRT staffing needs in both customer support and R&D.**
- **Identify security metrics by**
 - Customer
 - Country
 - Software release
 - Software products/solutions
- **Identify pace of incoming security tracks vs. outgoing security patches.**

PSIRT Metrics in Customer Support

Collecting Customer Support Data

This relationship is solved.

Request - Question: Security findings in SASFM

Product: SAS Fraud Management
Topic: security inquiry
Subtopic:
Product Release: 4.4_M1
SAS Release: 9.4 TS1M5
Platform: linux x64
Platform Release: RHEL 7 x64

SLA Expiration Date:
Hot Potato: Target
Priority: Medium
Team: fraud mgmt

Primary Owner

Brian English
SAS United States
0001000121
+1 (919) 531-4154
brian.english@sas.com

Secondary Owner

- Ticket metadata added to identify security inquiries and incidents
- Other metadata allows granular reporting on issues

PSIRT Metrics in Customer Support

Interpreting Customer Support data

SAS® Visual Analytics - Explore and Visualize

PSIRT Track Summary

PSIRT Track Count by Customer Name | PSIRT Track Count by Country | PSIRT Track Count by Release | Top 15 Products

PSIRT Track Count by Customer Name

	^ 2020	∨ Q1	^ 2019	∨ Q1	∨ Q2	∨ Q3	∨ Q4	∨ 2018	∨ 2017	∨ 2016	∨ 2015
	Track Count	Track Count	Track Count	Track Count	Track Count	Track Count	Track Count	Track Count	Track Count	Track Count	Track Count
Total	184	184	1,200	291	371	297	241	1,514	1,428	1,005	733
	9	9	20	3	4	5	8	100	123	97	63

- Values represent number of customer inquiries, not necessarily product vulnerabilities
- Broken out by year/quarter
- Separated into tables featuring Customer Name, Country, Product Release, and Top Products

PSIRT Metrics in Customer Support

Interpreting Customer Support data

PSIRT Track Count by Customer Name : PSIRT Track Count by Country PSIRT Track Count by Release

	^ 2020	∨ Q1	^ 2019	∨ Q1	∨ Q1
	Track Count	Track Count	Track Count	Track Count	Track Co
Total	184	184	1,200	291	
IBM Business Partner	9	9	20	3	
IBM Business Partner (India)	7	7	24	2	
Business Information Systems Ltd	6	6	25	4	
Walter Corp	6	6	30	4	
IBM Business Partner	5	5	10	1	

- Identify customers and sectors most concerned about product security, or most active in security auditing
- Valuable to Sales/Marketing and Product Management

PSIRT Metrics in Customer Support

Interpreting Customer Support data

PSIRT Track Count by Customer Name PSIRT Track Count by Country PSIRT

	∨ 2020	∧ 2019	∨ Q1	∨ Q2
	Track Count	Track Count ▼	Track Count	Track Count
Total	184	1,200	291	371
United States	72	338	73	111
Canada	21	150	38	38
Europe	12	115	27	43
Asia/Pacific	15	98	17	41
Australia	10	82	25	22
South America	4	44	12	14
Other	5	38	7	9
India	5	35	11	10
Japan	5	28	6	13

- Track workload for Customer Support in various regions
- Identify possible staffing needs

PSIRT Metrics in Customer Support

Interpreting Customer Support data

PSIRT Track Count by Customer Name PSIRT Track Count by Country PSIRT Track Count by Release

	∨ 2020	∧ 2019	∨ Q1	∨ Q2	∨ Q3	∨ Q4	∨
	Track Count	Track Count ▼	Track Count	Track Count	Track Count	Track Count	Track
Total	184	1,200	291	371	297	241	
9.4 TS1M3	43	281	76	85	82	38	
9.4 TS1M5	41	228	64	78	53	33	
9.4 TS1M4	11	199	59	61	43	36	
9.4 TS1M6	44	114	7	29	31	47	
Viya 3.4	12	98	17	32	20	29	
9.4 TS1M2	7	94	21	28	25	20	
9.3 TS1M2	2	59	17	13	16	13	
(missing)	7	43	5	18	9	11	
Viya 3.3	1	25	2	14	9	.	

- Customers staying on old software versions
- More vulnerabilities in older versions
- Fewer vulnerabilities in new versions

PSIRT Metrics in Customer Support

Interpreting Customer Support data

Product	Track Count ▼
SAS Web Server	1,098
Base SAS	632
...	520
...	393
...	266
...	232

- Products and components commonly targeted by scans (Apache, OpenSSL)
- Products that encompass many components
- Specific products that are targeted to certain customer sectors
- Products that simply have more vulnerabilities

PSIRT Metrics in Customer Support

What do customer reported problems mean for R&D?

Q1 2020 Summary: 12 Hot Fixes released addressing 15 Security Defects (10 unique)

February 2020 - 5 Hot Fixes released addressing 8 Security Defects (6 unique)

F1E007	02 / 25 / 20	Base SAS 9.4_M6 (18w47)	S1516964 - SAS/Share libname third
Viya	02 / 21 / 20		S1455702 - CRP : Stored XSS via Da
C2L008	02 / 21 / 20	SAS Studio 3.71 (17w47)	S1557661 - CRP : XSS in signout.jsp S1558010 - CRP : Velocity template in
Viya	02 / 18 / 20	SAS Viya 3.5 for Linux	S1520172 - CRP : SASGraphBuilder s
D8F004	02 / 10 / 20	SAS Studio 3.8 (18w47)	S1527677 - Information Disclosure th S1557661 - CRP : XSS in signout.jsp S1558010 - CRP : Velocity template in

January 2020 - 7 Hot Fixes released addressing 7 Security Defects (4 unique)

F6R002	01 / 30 / 20	SAS Fraud Management 6.1 (19w25)	S1554388 - CRP : XSS in the Alert se
D9T067	01 / 30 / 20	Base SAS 9.4_M6 (18w47)	S1548101 - CRP PERFORMANCE: H
B6T011	01 / 22 / 20	SAS Management Console 9.4_M5 (17w38)	S1542451 - CRP : Communications b

- Identify resources and cost associated with Product Security fixes
- Establish association between customer inquiries and bug fixes

PSIRT Metrics in Customer Support

What Next?

- The missing link... bridge the gap between the customer tracking system and our R&D defects/jira system.
- As we upgrade or transition to new tools, ensure data model improvements are considered in the design to aid the collection and quality of metrics.

Driving Change

What did we learn from all this?

1. Start with tracking security defects
2. Score all security defects honestly
3. Use a well known maturity model to help guide you (e.g. SAMM)
4. Identify trends and patterns in your PSIRT data
5. Prioritize, you can't fix everything all at once
6. Utilize free resources for vulnerability data (e.g. NVD, OWASP)
7. Let security tools do some of the heavy lifting (e.g. SAST, DAST, SCA)
8. Threat Modeling can be very powerful once understood
9. Continuous professional education is extremely important
10. Regular update meetings with leadership (e.g. quarterly)



Questions