ANATOMY OF AN APPSEC PROGRAM

OR HOW TO STOP DEPLOYING ~~SHITTY~~ SHODDY CODE TO PRODUCTION

2018 CACTUSCON

SEPTEMBER 28-29, 2018

AGENDA

BECAUSE QA SAID I NEEDED ONE

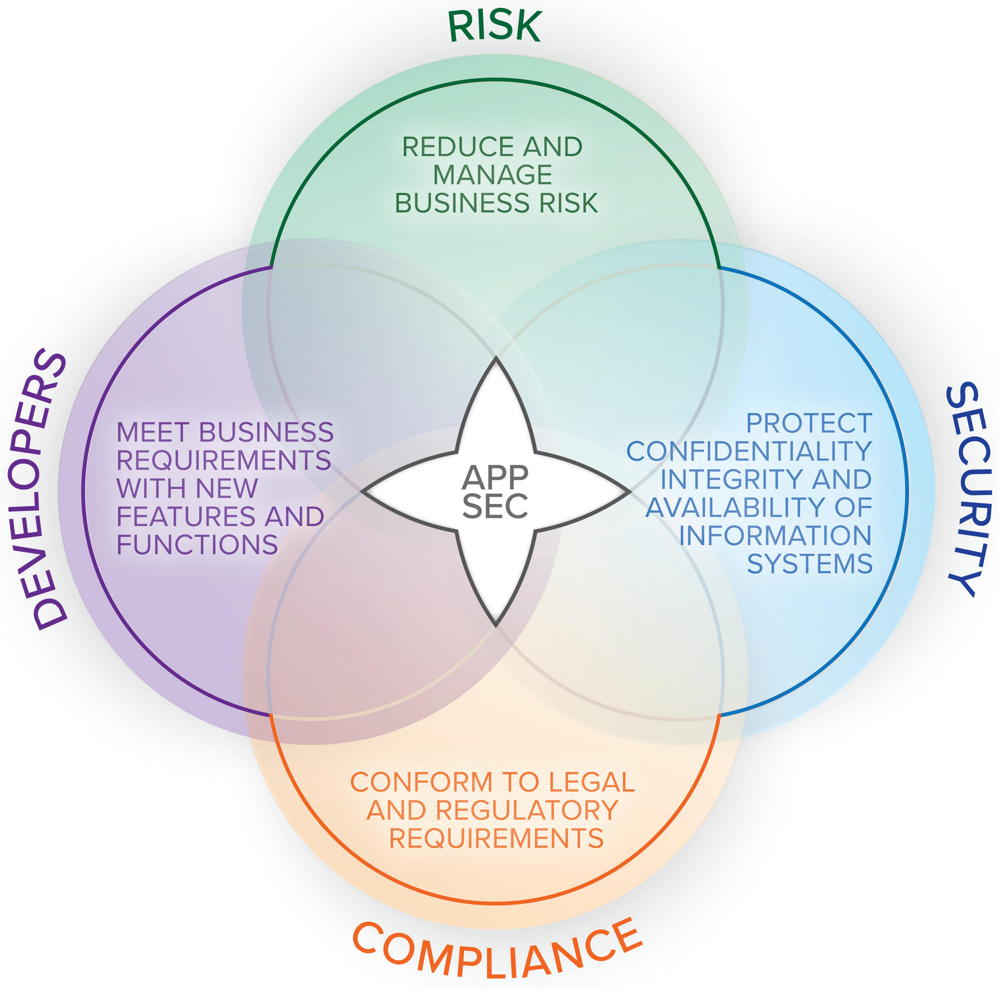
- Introductions
- The Problem (as I see it)
- The Solution (again, as I see it)
  - Finding vulnerabilities
  - Fixing things
  - Preventing vulnerabilities
  - Metrics
- Wrap-up / Q&A

WARNING

THIS IS KINDA IMPORTANT

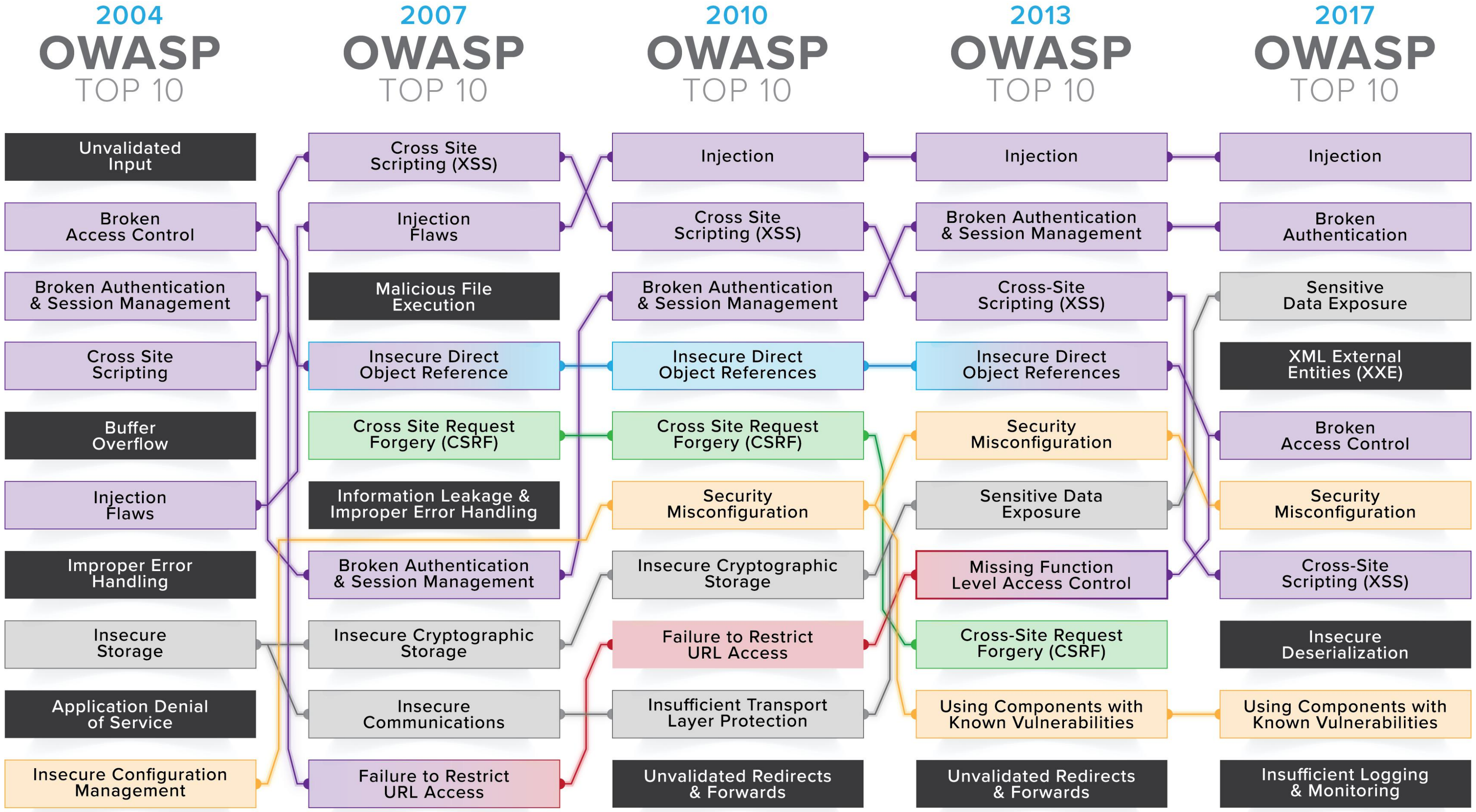
APPSEC

THE GLUE THAT STICKS SECURITY BALLS TOGETHER


RISK
REDUCE AND MANAGE BUSINESS RISK
DEVELOPERS
MEET BUSINESS REQUIREMENTS WITH NEW FEATURES AND FUNCTIONS
APP SEC
SECURITY
PROTECT CONFIDENTIALITY INTEGRITY AND AVAILABILITY OF INFORMATION SYSTEMS
CONFORM TO LEGAL AND REGULATORY REQUIREMENTS
COMPLIANCE

OWASP TOP 10

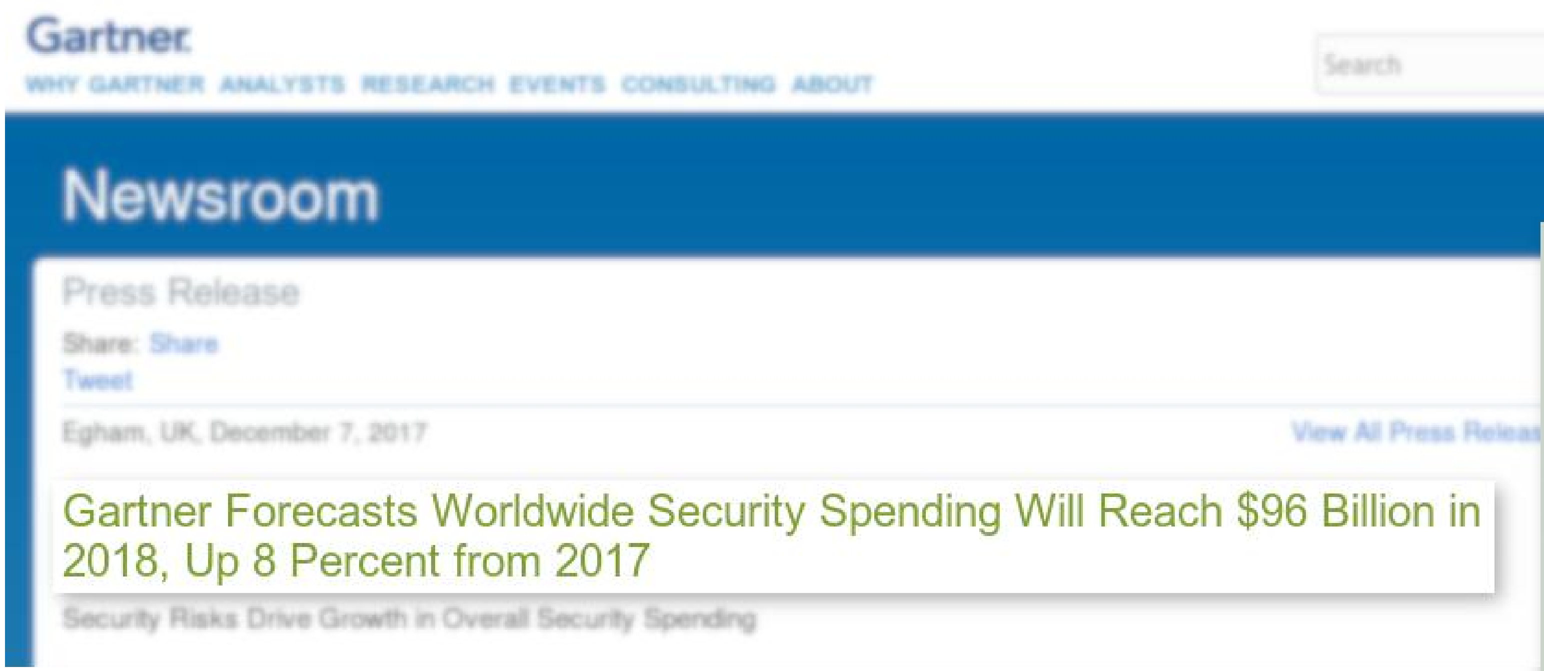
14 YEARS OF THE SAME OL' ~~SHIT~~ CRAP



2004 OWASP TOP 10	2007 OWASP TOP 10	2010 OWASP TOP 10	2013 OWASP TOP 10	2017 OWASP TOP 10
Unvalidated Input	Cross Site Scripting (XSS)	Injection	Injection	Injection
Broken Access Control	Injection Flaws	Cross Site Scripting (XSS)	Broken Authentication & Session Management	Broken Authentication
Broken Authentication & Session Management	Malicious File Execution	Broken Authentication & Session Management	Cross-Site Scripting (XSS)	Sensitive Data Exposure
Cross Site Scripting	Insecure Direct Object Reference	Insecure Direct Object References	Insecure Direct Object References	XML External Entities (XXE)
Buffer Overflow	Cross Site Request Forgery (CSRF)	Cross Site Request Forgery (CSRF)	Security Misconfiguration	Broken Access Control
Injection Flaws	Information Leakage & Improper Error Handling	Security Misconfiguration	Sensitive Data Exposure	Security Misconfiguration
Improper Error Handling	Broken Authentication & Session Management	Insecure Cryptographic Storage	Missing Function Level Access Control	Cross-Site Scripting (XSS)
Insecure Storage	Insecure Cryptographic Storage	Failure to Restrict URL Access	Cross-Site Request Forgery (CSRF)	Insecure Deserialization
Application Denial of Service	Insecure Communications	Insufficient Transport Layer Protection	Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities
Insecure Configuration Management	Failure to Restrict URL Access	Unvalidated Redirects & Forwards	Unvalidated Redirects & Forwards	Insufficient Logging & Monitoring

RIPPED FROM THE HEADLINES

BECAUSE DRAMA CREATES TENSION



Gartner

WHY GARTNER ANALYSTS RESEARCH EVENTS CONSULTING ABOUT

Search

Newsroom

Press Release

Share: Share

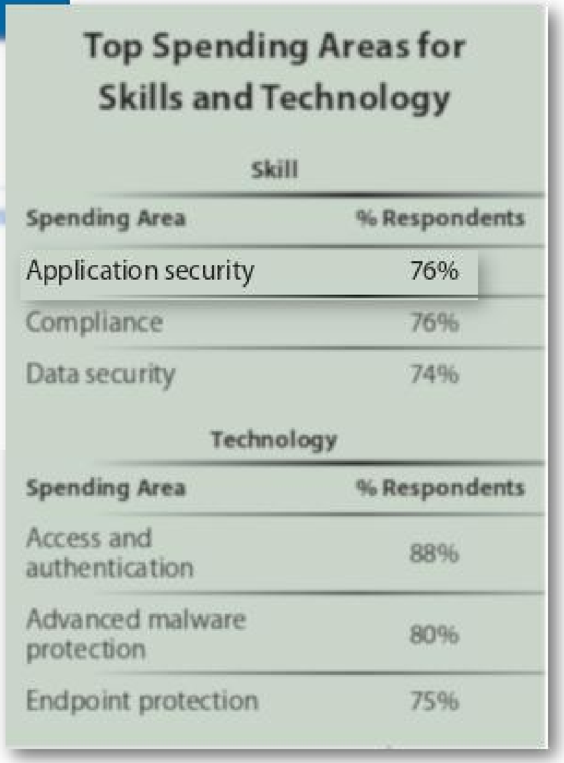
Tweet

Egham, UK, December 7, 2017

View All Press Releas

Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017

Security Risks Drive Growth in Overall Security Spending



Top Spending Areas for Skills and Technology

Skill

Spending Area	% Respondents
Application security	76%
Compliance	76%
Data security	74%

Technology

Spending Area	% Respondents
Access and authentication	88%
Advanced malware protection	80%
Endpoint protection	75%

APPLICATION SECURITY

WHAT IS THIS APPSEC YOU SPEAK OF?

IT'S SECURITY FOR APPLICATIONS

WIKIPEDIA

BECAUSE DEFINITIONS ARE AWESOME

Application security encompasses measures taken to improve the security of an application often by *finding*, *fixing*, and *preventing* security vulnerabilities.

- Wikipedia

WIKIPEDIA

BECAUSE DEFINITIONS ARE AWESOME

Application security encompasses measures taken to improve the security of an application often by *finding*, *fixing*, and *preventing* security vulnerabilities.

- Wikipedia

And then *measure* your results.

- Joe

FINDING VULNS

LOOKING FOR A NEEDLE IN A STACK OF NEEDLES

FINDING VULNS

DON'T FOCUS ON TOOLS

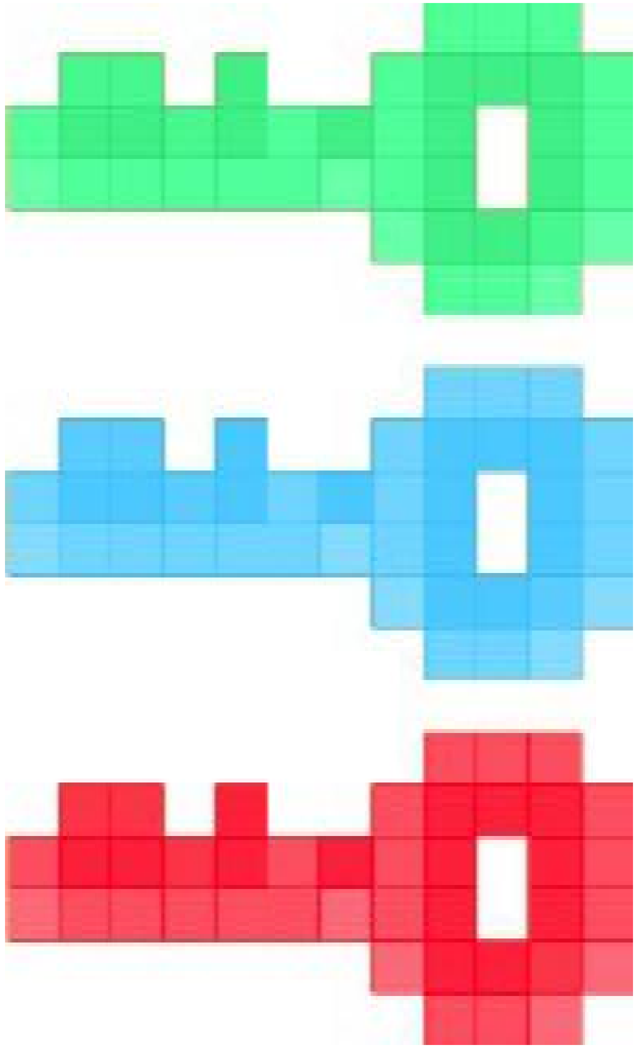
FINDING VULNS

YEAH, IT'S KINDA LIKE THAT

KEY POINTS

WRITE THIS DOWN

- Don't try to do everything at once.
- Start small and expand.
- Focus on your high-risk apps first.
- Chain together assessment methodologies.



TODO: FIX THIS STUFF

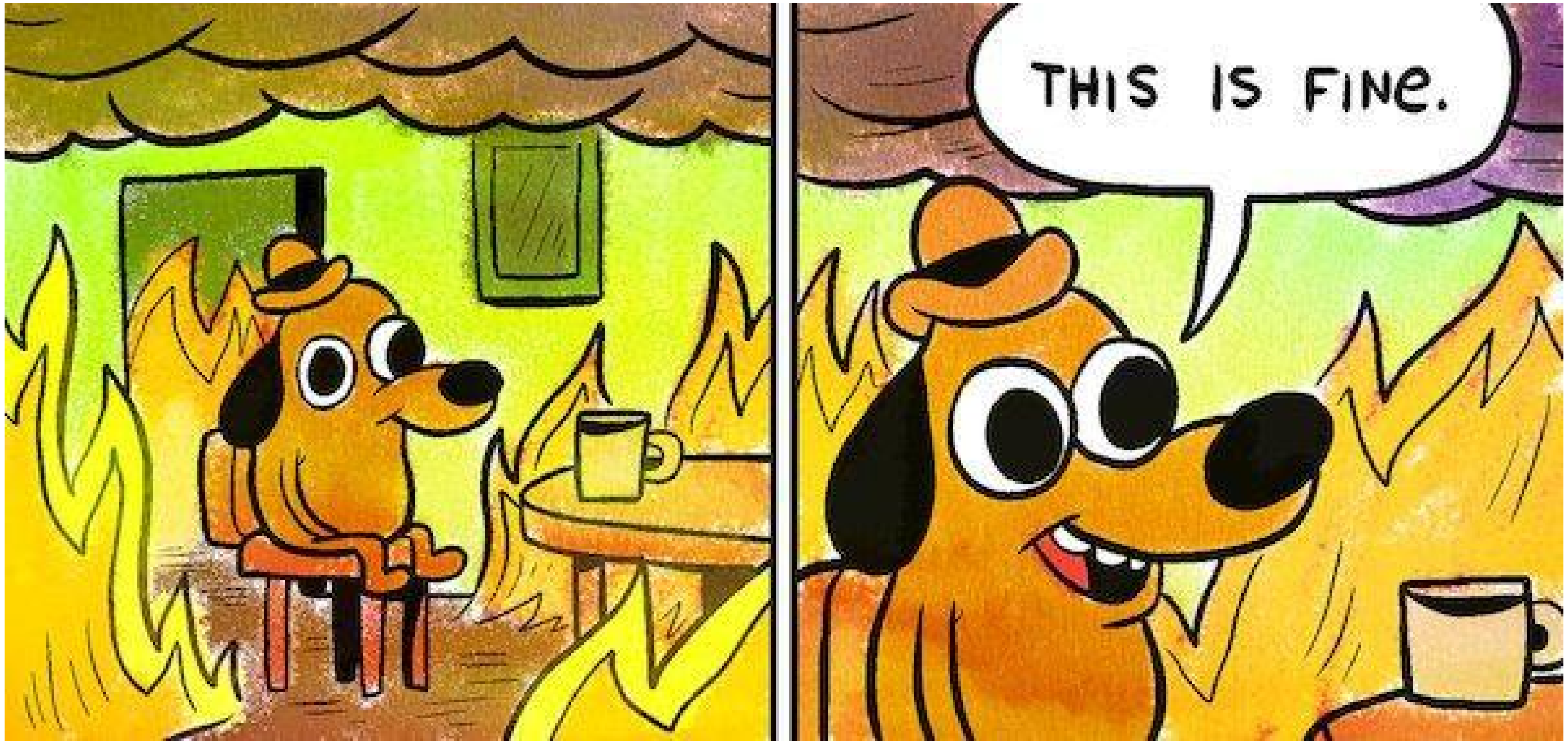
CUZ THAT'S BASICALLY THE POINT

FIXING VULNS

WITH A MEME

FIXING VULNS

WITH ANOTHER OVERUSED MEME



FALSE POSITIVES

BUT IT'S BEHIND THE FIREWALL”

```
<?php
     ...
     [omitted for brevity]
     ...

   $con = mysql_connect("localhost",$user,$pass);
   mysql_select_db("database", $con);
   $id = $_GET['id'];
   $result = mysql_query("SELECT name FROM user WHERE id=$id", $con);

   mysql_close($con);
     ...
   [omitted for brevity]
     ...

  ?>
```

FALSE POSITIVES

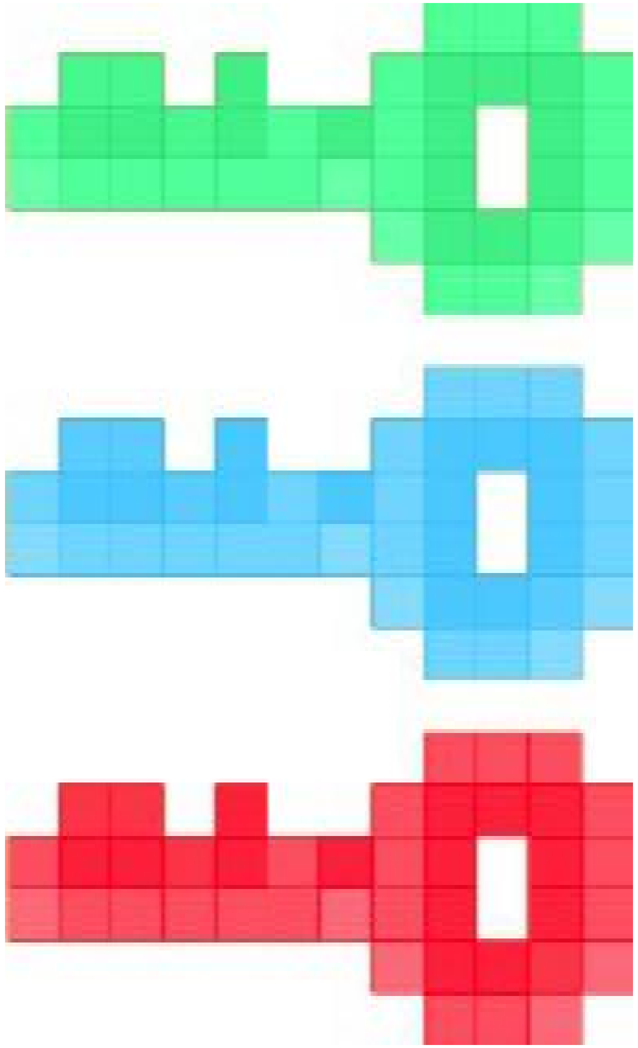
BUT IT'S BEHIND THE FIREWALL”

```
<?php
      ...
      [omitted for brevity]
      ...

   $con = mysql_connect("localhost",$user,$pass);
   mysql_select_db("database", $con);
   $id = validate($_GET['id’]; )
   $result = mysql_query("SELECT name FROM user WHERE id=$id", $con);

   mysql_close($con);
      ...
   [omitted for brevity]
      ...

  ?>
```

KEY POINTS

WRITE THIS DOWN

- Make it easy for your developers to engage in AppSec.
- Set realistic goals and expand.
- Create a security backlog and use “security sprints” each release to work it.
- As teams mature, introduce security gates.
- Have a process to handle false positives.



PREVENTION

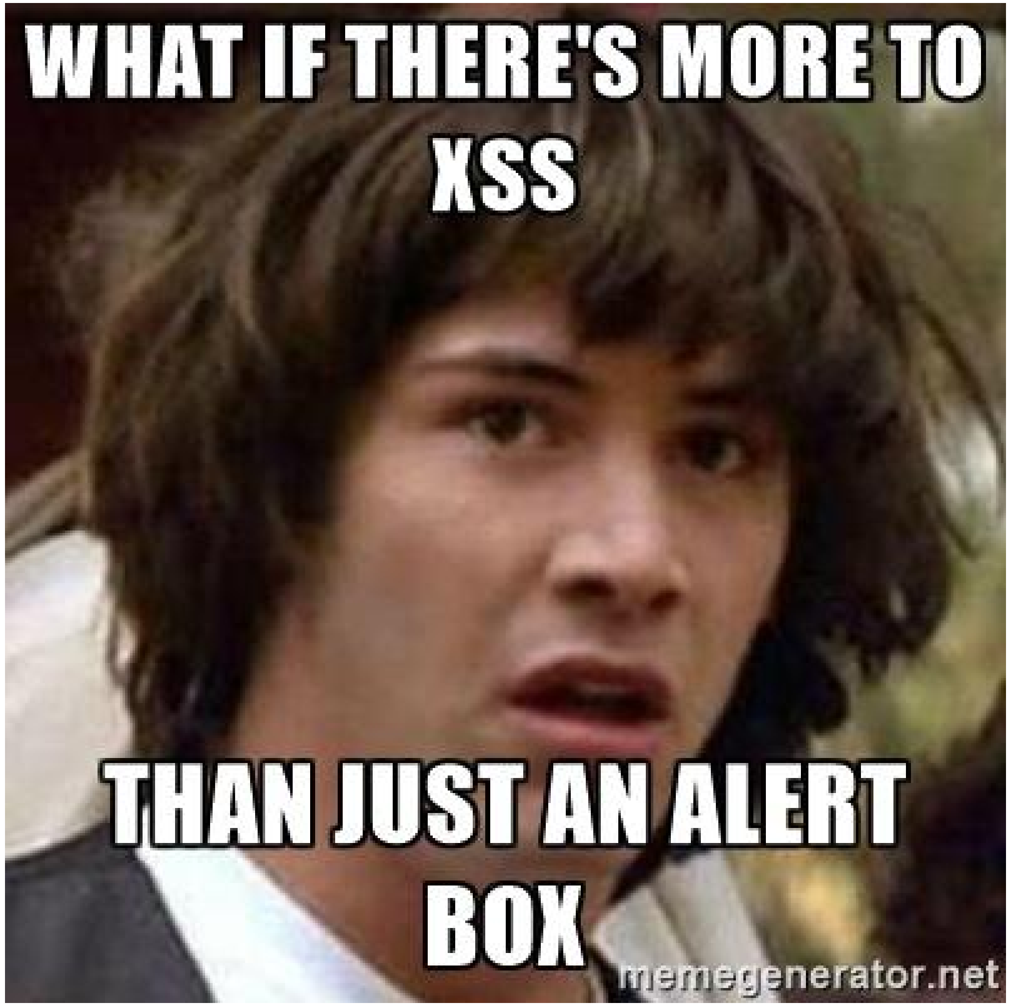
ACTUALLY GETTING BETTER

PREVENTION

MAKING DEVELOPERS BETTER

EDUCATING DEVELOPERS

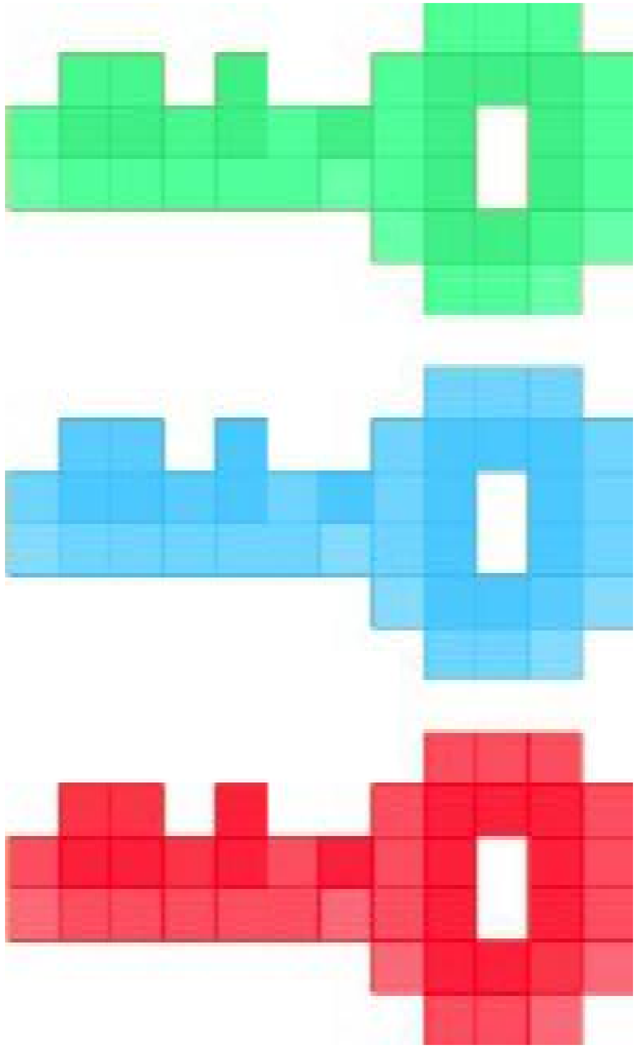
IN THE WAYS OF SECURITY



KEY POINTS

WRITE THIS DOWN

- Developers aren't security people.
- Have hands-on workshops to cover security issues.
- Walk your developers through hacking things.
- Top-down support is really critical.



METRICS

HOW TO KNOW IF IT'S WORKING

METRICS VS. STATS

WHAT'S THE DIFFERENCE?

STATISTIC: A fact or piece of data from a study of a large quantity of numerical data

METRICS: Standards of measurement by which performance, progress, or quality of a plan, process, or product can be assessed

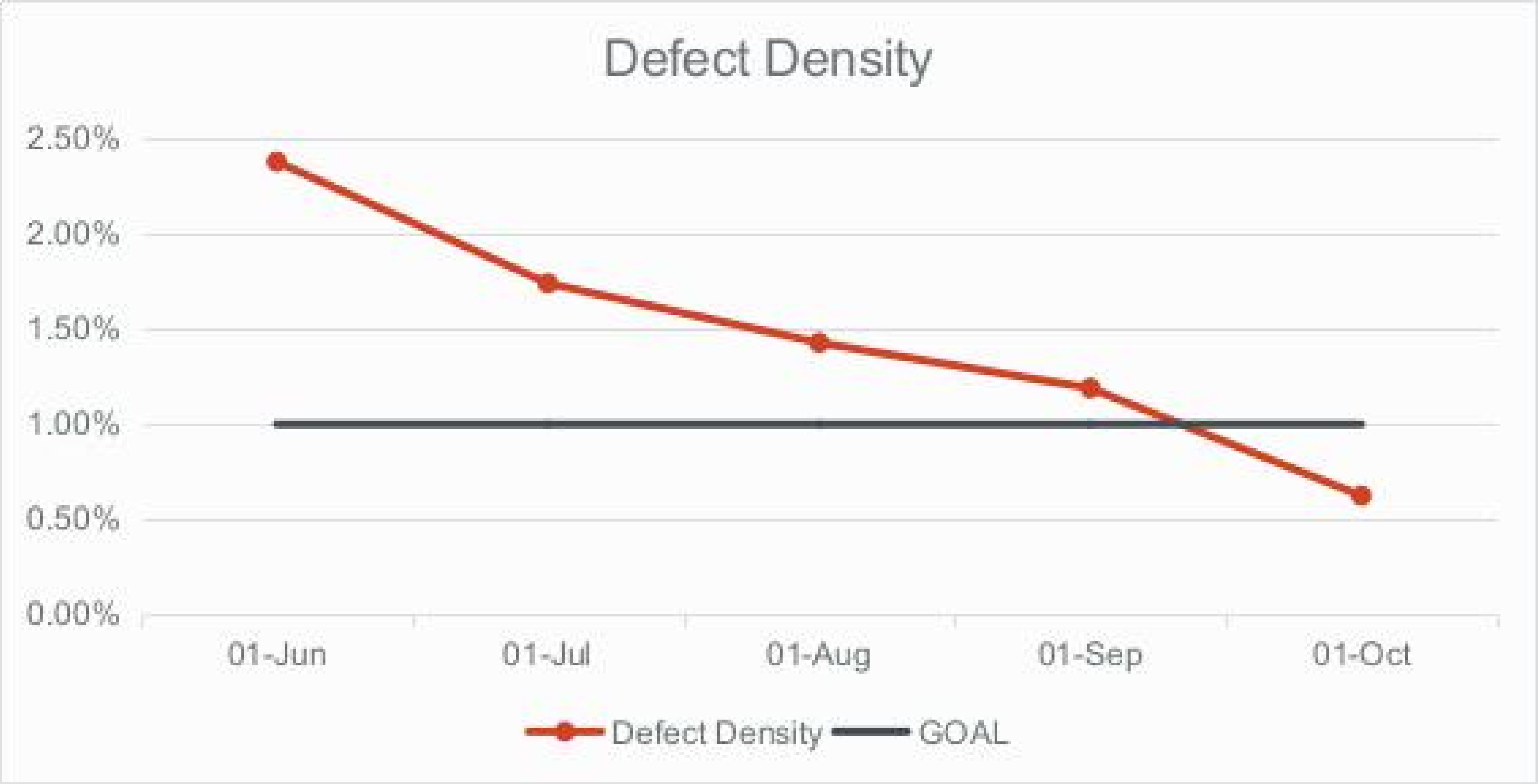
APPSEC METRICS

AN EXAMPLE

GOAL	QUESTION	MEASURE	METRIC
Less than 1% security defect rate	How many vulns are there? How many lines of code?	Number of vulns Number of LoC	Security Defect Density – number of vulns/1000 lines of code, plotted over time with the target waterline

APPSEC METRICS

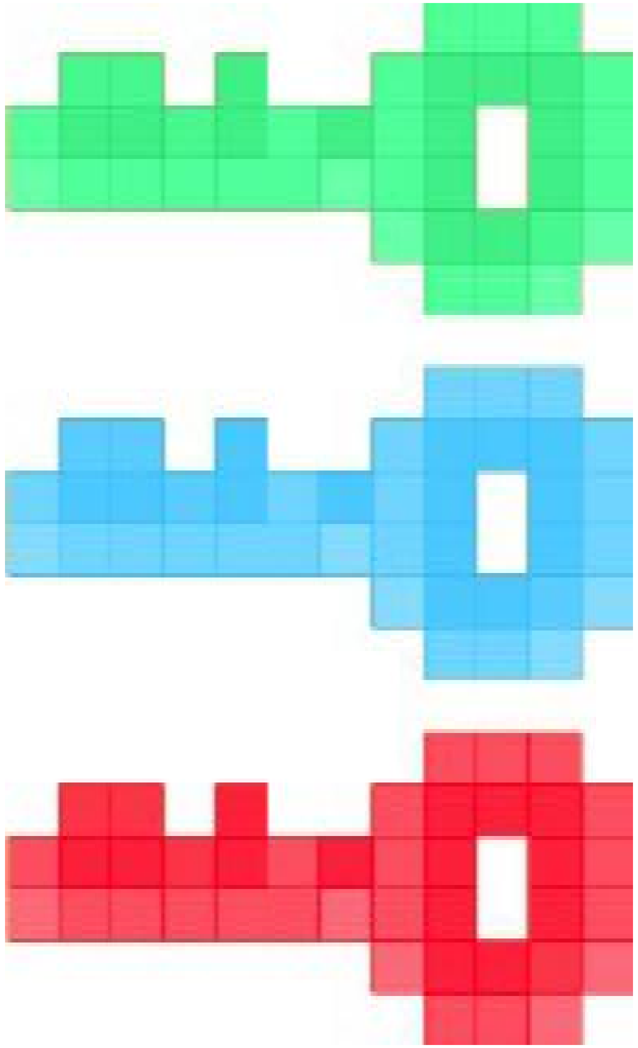
AN EXAMPLE



KEY POINTS

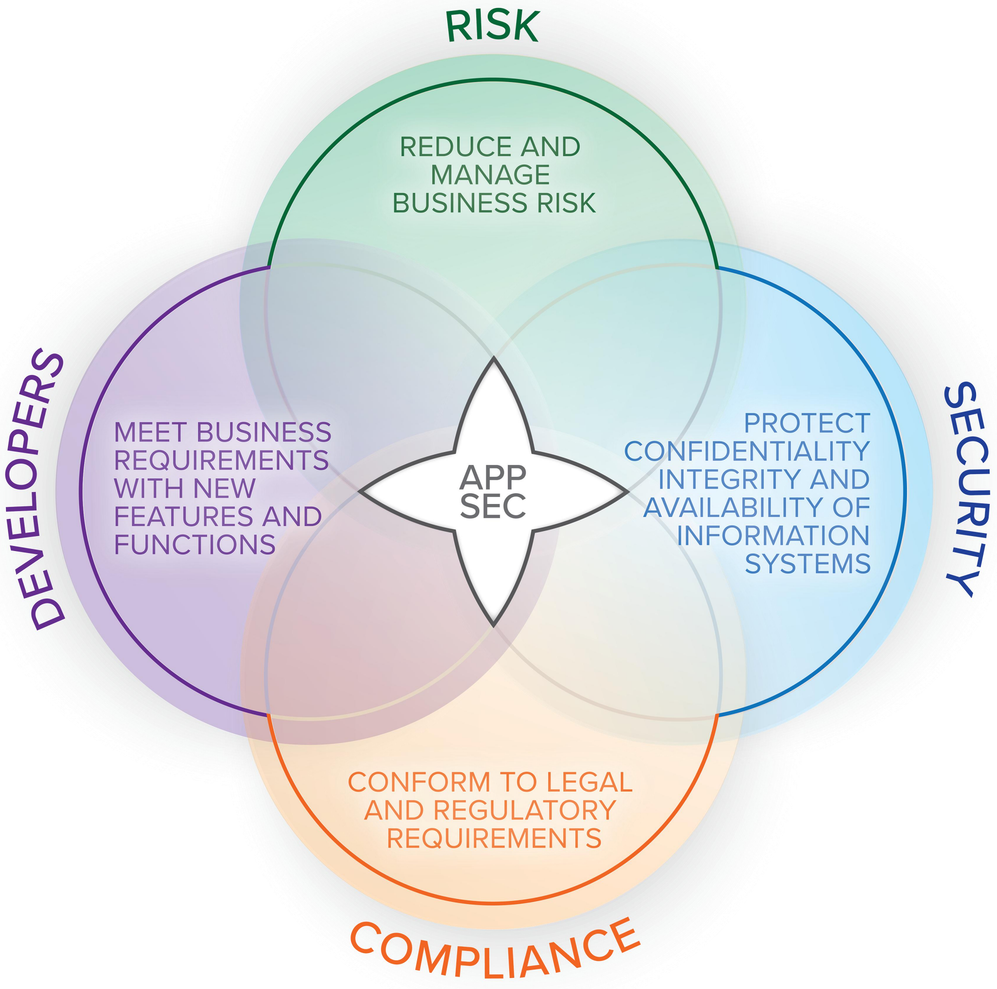
WRITE THIS DOWN

- Use the G-Q-M method for metrics.
- Choose meaningful metrics.
- Evaluate against a defined framework.
- This is how you demonstrate value.



APPSEC

THE GLUE THAT STICKS SECURITY BALLS TOGETHER



RISK

REDUCE AND MANAGE BUSINESS RISK

DEVELOPERS

MEET BUSINESS REQUIREMENTS WITH NEW FEATURES AND FUNCTIONS

APP SEC

SECURITY

PROTECT CONFIDENTIALITY INTEGRITY AND AVAILABILITY OF INFORMATION SYSTEMS

CONFORM TO LEGAL AND REGULATORY REQUIREMENTS

COMPLIANCE

WE'RE HIRING

VISIT US ONLINE TO FIND OUT MORE

www.BishopFox.com

Careers@BishopFox.com

THANK YOU

2018

cactuscon