orange is the new purple

how and why to integrate software teams with red and blue teams

verizon

aprilwright

Agenda:

Terminology and concepts

Explore the current "gap" impacting software security

New ideas for bridging the divide

Ways to create change

Pragmatism about process maturity

We have different primary directives

Security's goals:

Create it securely

Maintain it properly

Prove it's protected

Document everything

Builder's goals:

Time to market

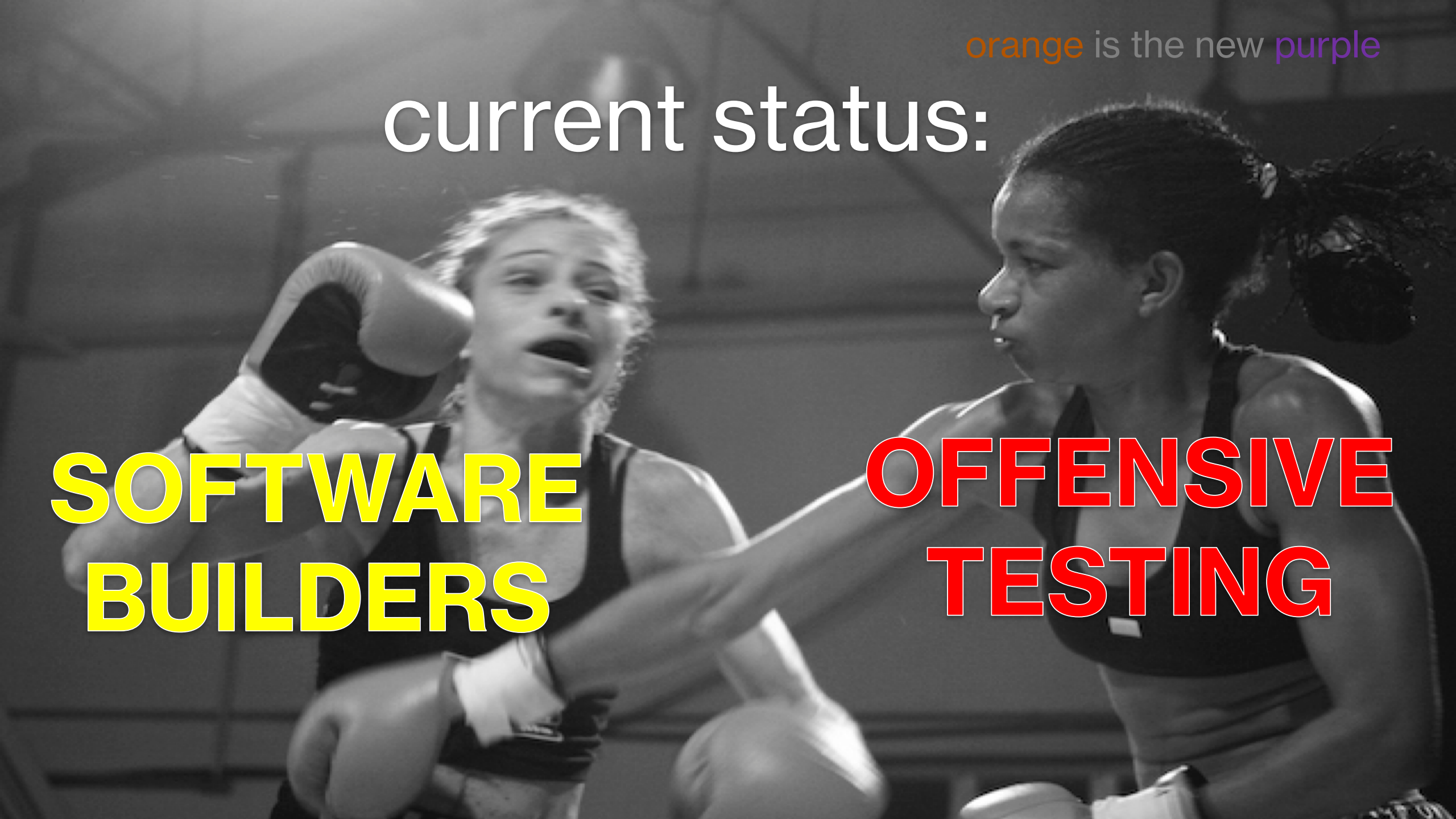
Correctness

Minimal defects

Optimization *

** (Chuck Norris writes code that optimizes itself)*

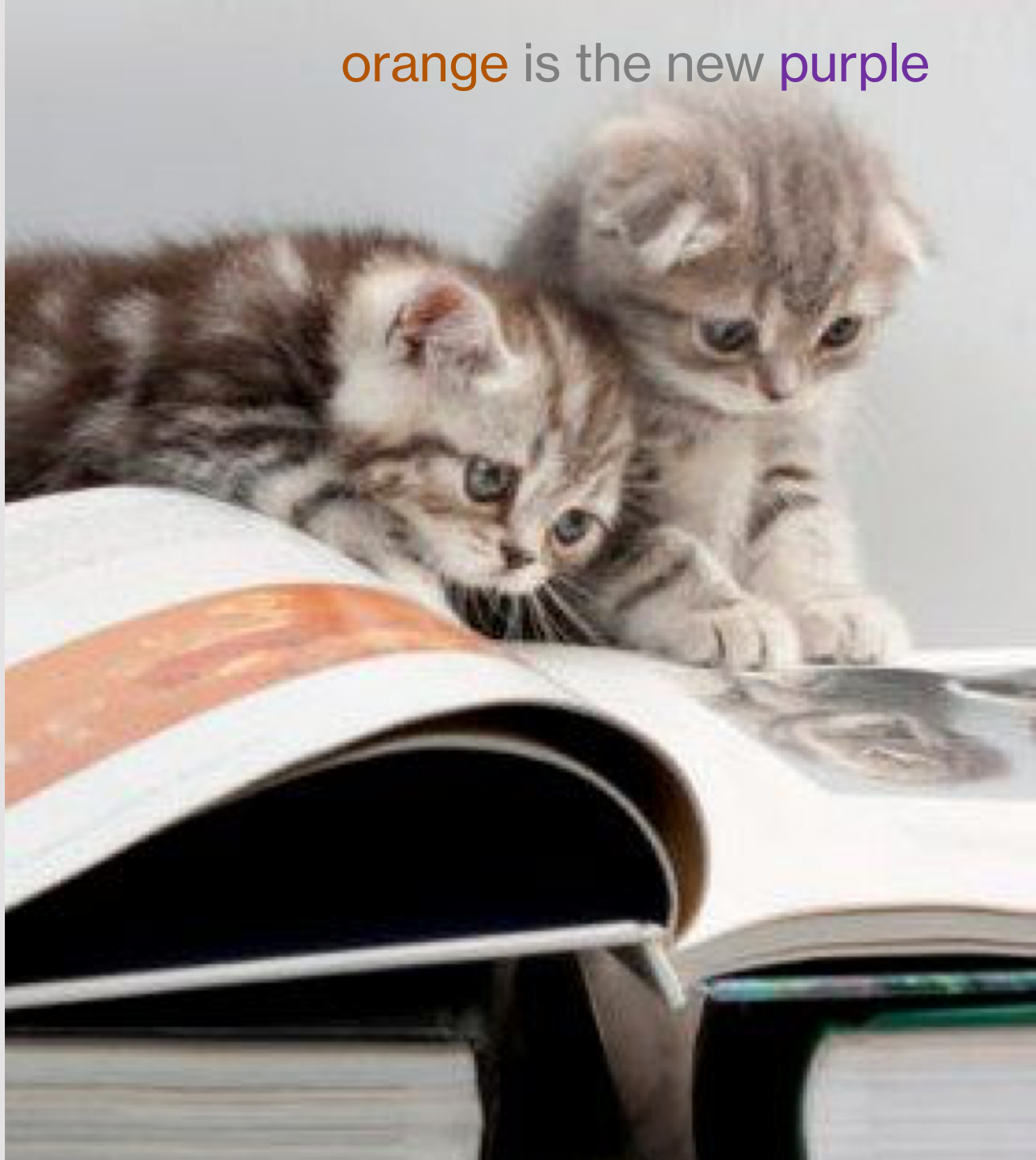
current status:



Can we overcome:

- Lack of communication?
- Non-matching goals?
- Speaking different "languages" & "jargon"?
- Siloes of knowledge?

Can we work *together*?



 @APRILWRIGHT

InfoSec Generalist, Security Expositor @Verizon

~25 years, advanced Management and Defense, Offensive Testing, Defensive SDLC, Change, eGRC, Detection, DF/IR, Coding, Hacking, Gaming, Sec Ops (Blue Team), Soft Skills, Unix Ops, SQL, Risk, Web App Dev, Graphic Design, Photography

Software challenges: Security's view

- Unknown scope of applications, libraries (Builders know this!)
- Everyone is averse to testing in production
- Why doesn't everyone just 'get it'?
- Bugs are being remediated reactively, not proactively
- Inability to sustain iterative release testing
- **“Organizational and communications silos between security, application development and the rest of the organization”**

-- SANS: 2016 State of Application Security: Closing the **Gap**

Everyone contributes to the security of an organization

(we are on the same team)

There is hope for creating more secure software

Builders *want* to learn about security!

Security wants to share knowledge!

Organizations embrace cross-training (generally)

Because #infosec loves triads

Breakers
(Red Team)

Guardians
(Blue Team)

Builders
(Yellow Team)

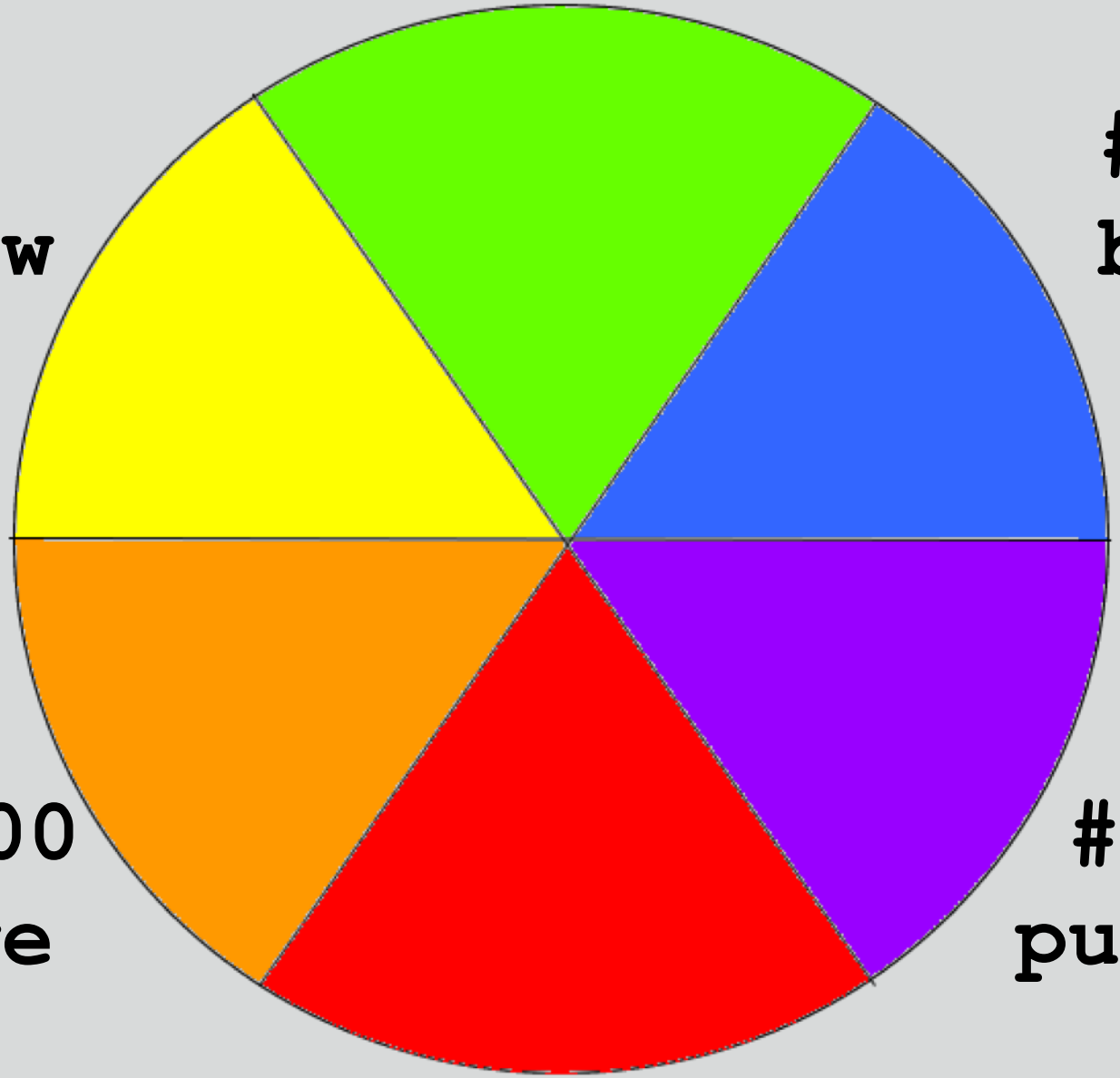
orange is the new purple

orange is the new purple

#0F0 green

#FF0 yellow

#F00 blue



#FFA500 orange

#F00 purple

#F00 red

#F00 + #00F = #800080 purple

#FF0 + #00F = #0F0 green

#FF0 + #F00 = #FFA500 orange


purple team?
security teams
working together
orange is the new purple

Introducing...

#ORANGETEAM

#GREENTEAM

^^ this is an actual photo!

Unity is strength; when there is teamwork and collaboration, wonderful things can be achieved

-- Mattie Stepanek

#ORANGETEAM (#FFA500)

Breakers + Builders

Developing a threat-mindset

- Builders benefit from current, relevant exposure to evolving security threats
- Ongoing insight into the breaker mindset
- Open-door policy between teams
- Red team finds less of the same bugs *over time*

#ORANGETEAM (#FFA500)

Goals:

- Collaboration leads to identification of related problems
- Offensive critical thinking included in builder's personal frame of "correctness" + "accuracy"
- Can avoid "misuse cases"
- Decrease in overall security bug counts *over time*

#GREENTEAM - #0F0

Guardians + Builders

Improving Defenses

- Address issues related to Forensics and Incident Response
- Tune and improve detection capability
- Gain better visibility built into important functions
- Standardize and enhance logging

#GREENTEAM - #0F0

Goals:

- Gaps in detection are closed
- Known-insecure code is more closely watched
- Improve introspection capabilities
- Thorough, standardized audit trails
- Software integrates with Security tools and automation

Practical introductory SDLC

- Start with a checklist
- Think backwards from launch
- What needs to be done?
- Who needs to be involved?
- What does Security need to see?
- Create gating conditions for each phase
- Cloud Security Alliance has great resources!
  - ...Even if you're not doing cloud, many same principles apply

Project Managers can help you achieve your goals

- Present your checklist to the PMO as "requirements for launch"
- Work closely with PMO on expectations
- PMO can plan to incorporate checklist items into the timeline
- Policy should mandate Security become engaged as early as possible
- Explain the value of "misuse" cases (vs "use cases")

Privacy Questionnaire

- Identify stakeholders
- What sensitive data will be stored?
- Where will sensitive data be stored and transmitted?
- What mitigations will be used to protect that data?
- What is the risk if the data is exposed?
- What needs to happen if there is exposure?

Each SDLC phase needs a checklist

- Requirements
- Design and Architecture
- Development and Implementation

Sample "Requirements" Checklist

- Step One: Engage security to participate in project
- Define project scope
- Identify target compliance goals and determine a compliance timeline
- Contribute security to Use Cases
- Security approval on **all** other Use Cases
- PM generates concept, timeline, budget, everyone agrees or makes changes as-needed
- **Obtain Security's approval to proceed.**

Use Cases and Misuse Cases

USE Case:

"As an admin, I need to be able to change one of our users' passwords"

Acceptance Criteria:

Administrators are able to change another user's password under the same security context/account

MISUSE Case:

"As a non-admin, I want to be able to change another user's password"

Acceptance Criteria:

Non-administrators are not able to change any other user's password.

Control Domain	CCM V3.0 Control ID	Updated Control Specification
Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.
Application & Interface Security Data Integrity	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
Application & Interface Security Data Security / Integrity	AIS-04	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.
Audit Assurance & Compliance Audit Planning	AAC-01	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.

FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	HIPAA / HITECH Act	NIST SP800-53 R3	PCI DSS v3.0
NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SC-2 NIST SP 800-53 R3 SC-4 NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6	45 CFR 164.312(e)(2)(i)	SC-2 SC-3 SC-4 SC-5 SC-6	6, 6.5
NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6		CA-1 CA-2 CA-5 CA-6	4.1.1, 4.2, 4.3
NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-3 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4)	45 CFR 164.312 (c)(1) 45 CFR 164.312 (c)(2) 45 CFR 164.312(e)(2)(i)	SI-10 SI-11 SI-2 SI-3 SI-4 SI-6 SI-7 SI-9	6.3.1 6.3.2

Tailoring the CCM

Control Specification:

Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:

- Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)
- Account credential lifecycle management from instantiation through revocation
- Account credential and/or identity store minimization or re-use when feasible
- Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)

Tailoring the CCM

Use Case:

As an Administrator, **I want to ensure that my** user account credentials are restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:

Acceptance Criteria:

- Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)
- Account credential lifecycle management from instantiation through revocation
- Account credential and/or identity store minimization or re-use when feasible
- Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)

Sample "Design/Architecture" Checklist

- Develop prototype design that addresses both Security Requirements and Functional Requirements
- Create network diagrams
- Create data flow diagrams
- Review diagrams with Security
- Incorporate Security's feedback, as-needed
- Ensure capacity is allocated for Security-related functions (e.g. SIEM server, span ports available on a switch, separate VLANs for storage and admin traffic.
- Security review for selection of vendors, supply-chain
- **Obtain Security's approval to proceed**

Perform a
gap assessment
on all vendors

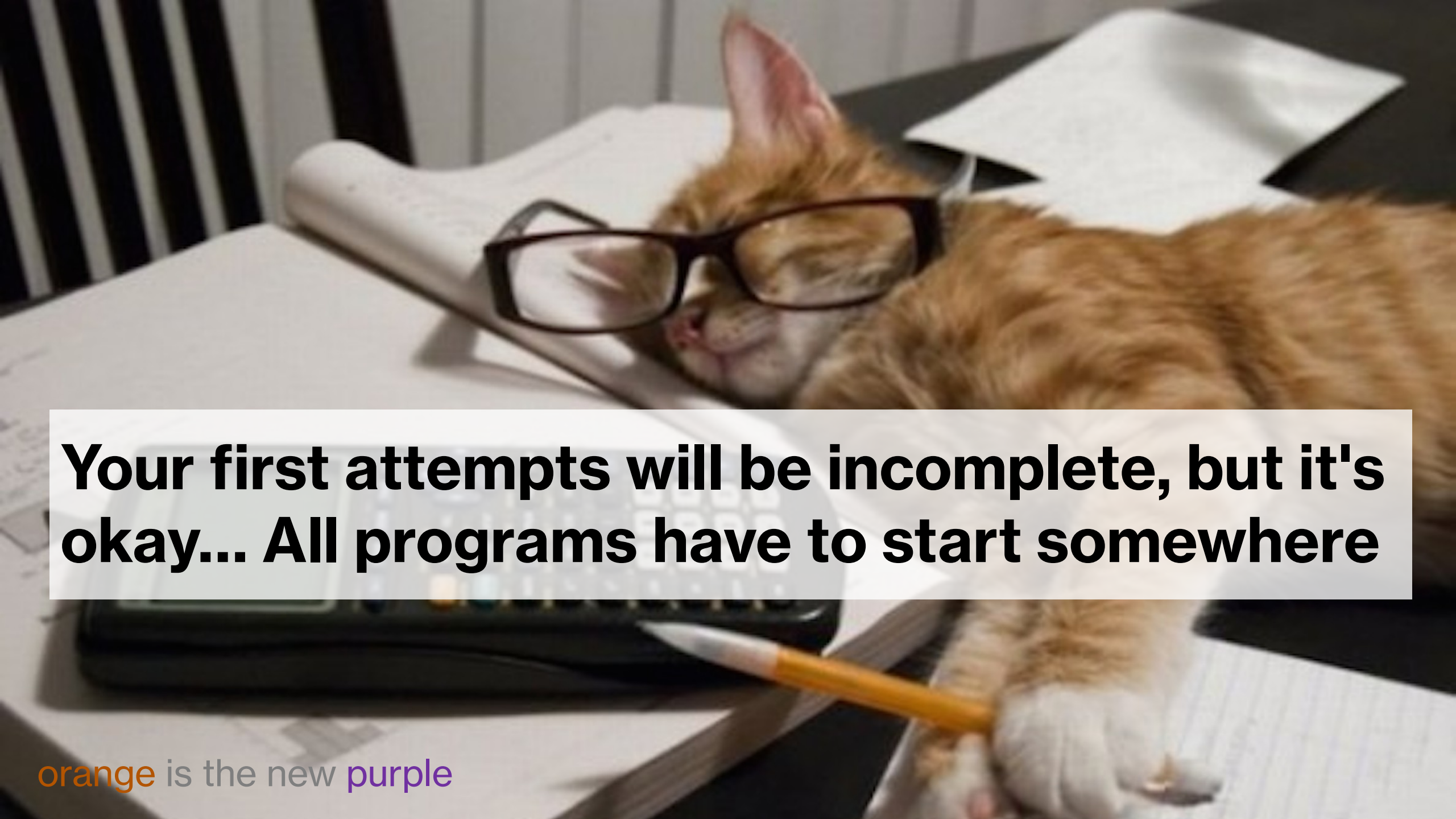
Vendor security
should be
as good as
your security
(or better)

Sample "Development/Implementation" Checklist

- Users created within the Application for authenticated penetration testing
- SNMP traps setup, Logging to centralized SIEM
- Secure Baseline is used for all O/S and supporting applications
- Procedural and Process documentation is created
- A patch management process and procedure is created
- Monitoring and related Access Control Lists are put in place
- NIDS, HIDS, HIPS are configured and tested
- Vulnerability scanning and Internal Pen Testing have been performed
- Remediation has occurred, based on Testing

Handling the Checklists

- Provide ALL checklists up-front to the PMO
- Be prepared to explain HOW to initiate each process you are requiring
- Completed checklists are Compliance Artifacts
  - Store in a backed-up repository
  - Store for an adequate amount of time
  - Protect based on Privacy requirements
- Tailor the checklists to each project – not every control will apply


Your first attempts will be incomplete, but it's okay... All programs have to start somewhere

CULTURE CHANGE DOES NOT HAPPEN OVERNIGHT

Initiate change, be patient

- Solidify your goals with organizational policy (it all starts there!)
- Foster a "one team" mentality (it is *not* "us vs. them")
- Facilitate frequent opportunities for communication
- Eliminate obstacles to sharing (collaborative systems, politics)
- Allocate time for ongoing, practical interaction and training
- Positive reinforcement for software builders' good choices

Gaining management buy-in

- Objectively gathered Metrics / Statistics are influential
- We need to communicate risks:
  - Bug found in requirements phase may cost $1 to fix. Same bug may cost $5 during design, $50 during development, $500 during testing, and $Millions if found by an attacker
  - Harm to the brand
  - Legal implications
- Risk Management Program results and scoring

“The geography we have created is all about speed, convenience, and scale; Security is an afterthought.”

— General Michael Hayden,
retired head of CIA, NSA

Remember...

- Security should never be an afterthought
- Application builders and defenders should be a team
- Orange and Green teams do not need to be formal activities
- Teach, learn & connect with each other
- Make every interaction as positive as possible
- Use policy, process, procedures to formalize requirement
- Be patient – security initiatives can require perseverance

#ORANGETEAM

ArchitectSecurity.org

aprilwright

Please provide feedback to BlackHat for this session! ☺

orange is the new purple

by
april wright
BlackHat
2017
#bhusa

verizon

enjoy
the
con
☺