$ ./test.sh

#DEFCAMP
#ORANGETEAM

https://architectsecurity.org

@aprilwright

orange is the new purple

Now featuring 27% more cats!

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

verizon

aprilwright


problemsolver
applications
knowledge
automation
complex
assessment
riskmanagement
consistent
certified
innovative
information
blueteam
preventative
leadership
evangelist
remediation
projects
creativity
assurance
defense
proactive
architecture
design
platforms
development
infosec
networks
initiatives
manager
frameworks
systems
evaluator
technical
lifecycle
safeguards
hybrid
senior
ITIL
expert
impact
security
analyst
redteam
GRC
cloud
guidance
unix
cyberz
global
author
web
enterprise
largescale
programs
shell
auditor
federal
solutions
speaker
cats
awareness
customers
planning
database
integration
operations
industry
experience
datacenter
diplomat
generalist
compliance

@AprilWright

- Generalist, polymath, security expositor
- Background: UNIX, Dev, Blue, Red, Verizon 16+ years
- Speaker: BlackHat, DerbyCon, globally
- DEFCON Groups core organizer
- Co-founder of the Boston DefCon Group

1. Certified Master’s Level Social Engineer
2. CISSP (Certified Information Systems Security Professional)
3. CSSLP (Certified Secure Software Lifecycle Professional)
4. CCSP (Certified Cloud Security Professional)
5. SSCP (Systems Security Certified Practitioner)
6. CISA (Certified Information Systems Auditor)
7. CCSK (Certificate of Cloud Security Knowledge)
8. ITIL version 3 Fundamentals
9. QualysGuard Certified Specialist
10. Vulnerability Management - Qualys
11. FedRAMP System Security Plan (SSP) 200-A
12. Oracle Certified Security Administrator
13. Oracle Certified Network Administrator
14. Oracle Certified Systems Administrator
15. CompTIA Network+
16. CompTIA Security+
17. Infra CMDB Certified Developer – EMC
18. Microsoft Certified Professional (MCP)


SDLC
is a
social
effort

We are Verizon.

Verizon delivers the promise of the digital world.

- Fortune 500 rank: #14
- $30.5 billion in second-quarter revenue (2017)
- 163,400 employees

For second-quarter 2017:

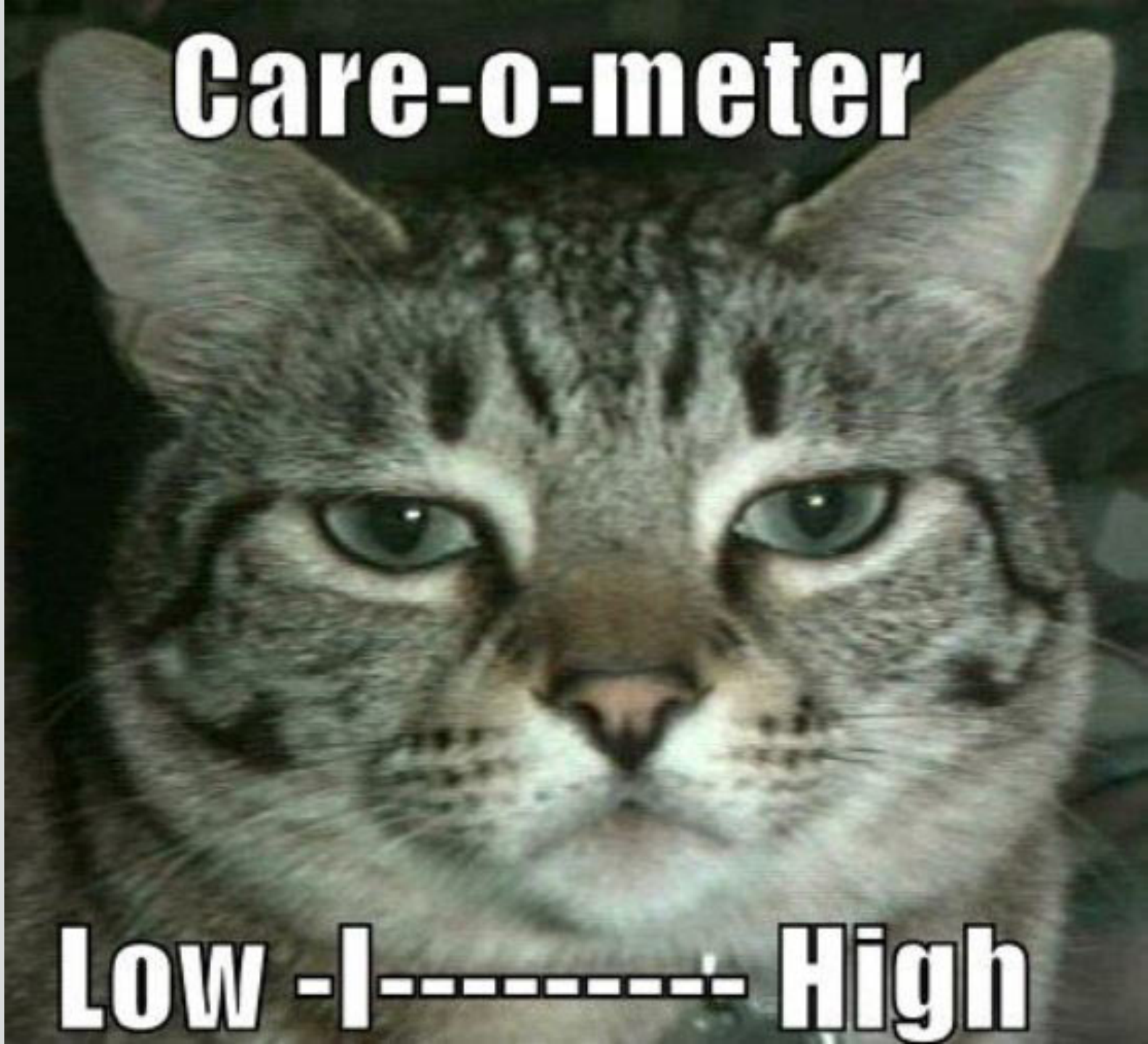
Wireless leadership
LTE covers more than 98% of U.S. population
114.5 M total retail connections
LTE Advanced covers 470 markets

Largest all-fiber Fios network
5.7 M Fios internet and 4.7 M Fios video connections
Fios Gigabit downloads as fast as 940 Mbps and uploads as fast as 880 Mbps.

Global IP network
99% of Fortune 500 customers

Products and solutions
Innovating in entertainment, digital media, the Internet of Things and broadband service

Why is software still being built insecurely?



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

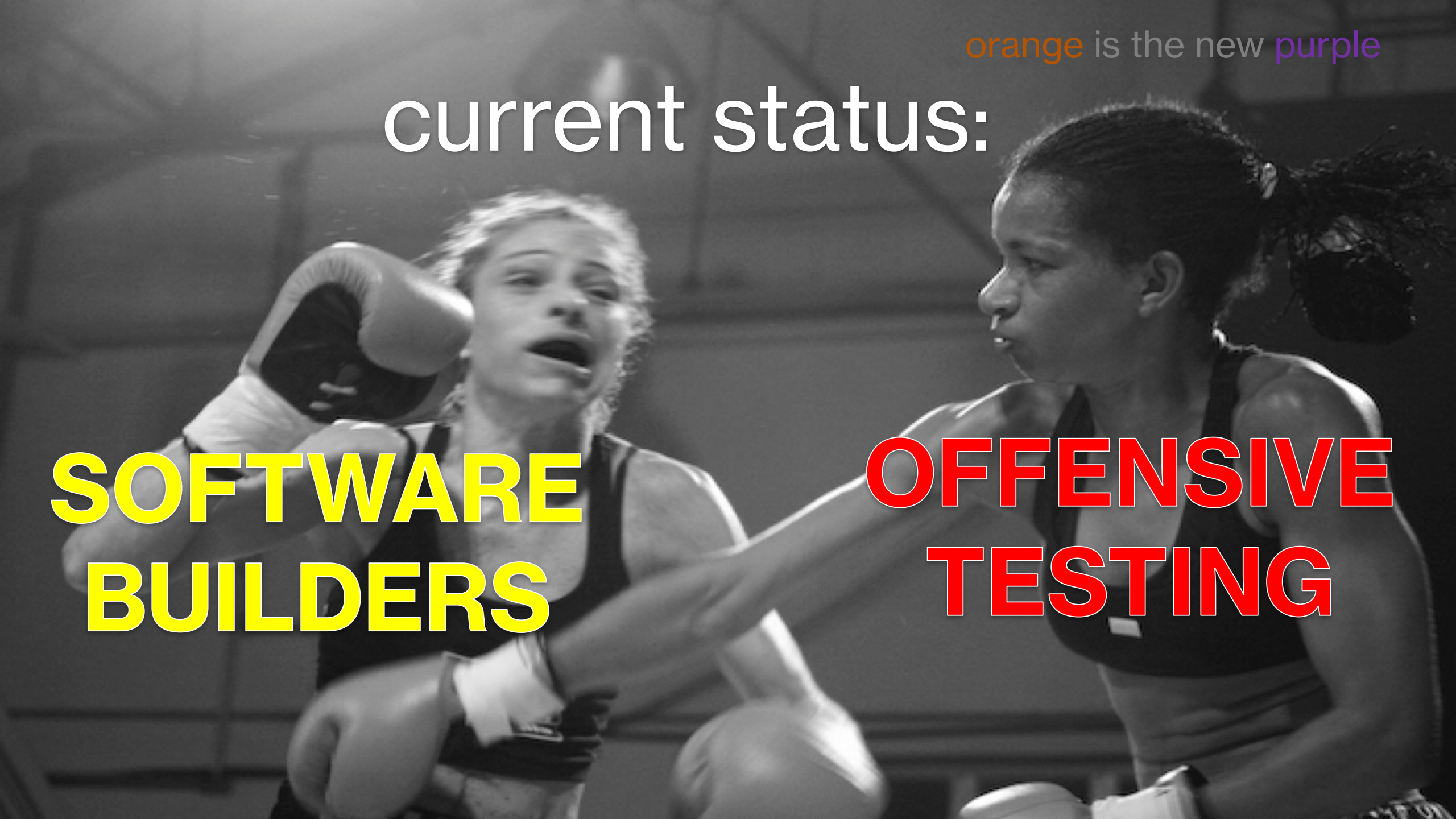
Correctness

Minimal defects

Optimization *

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

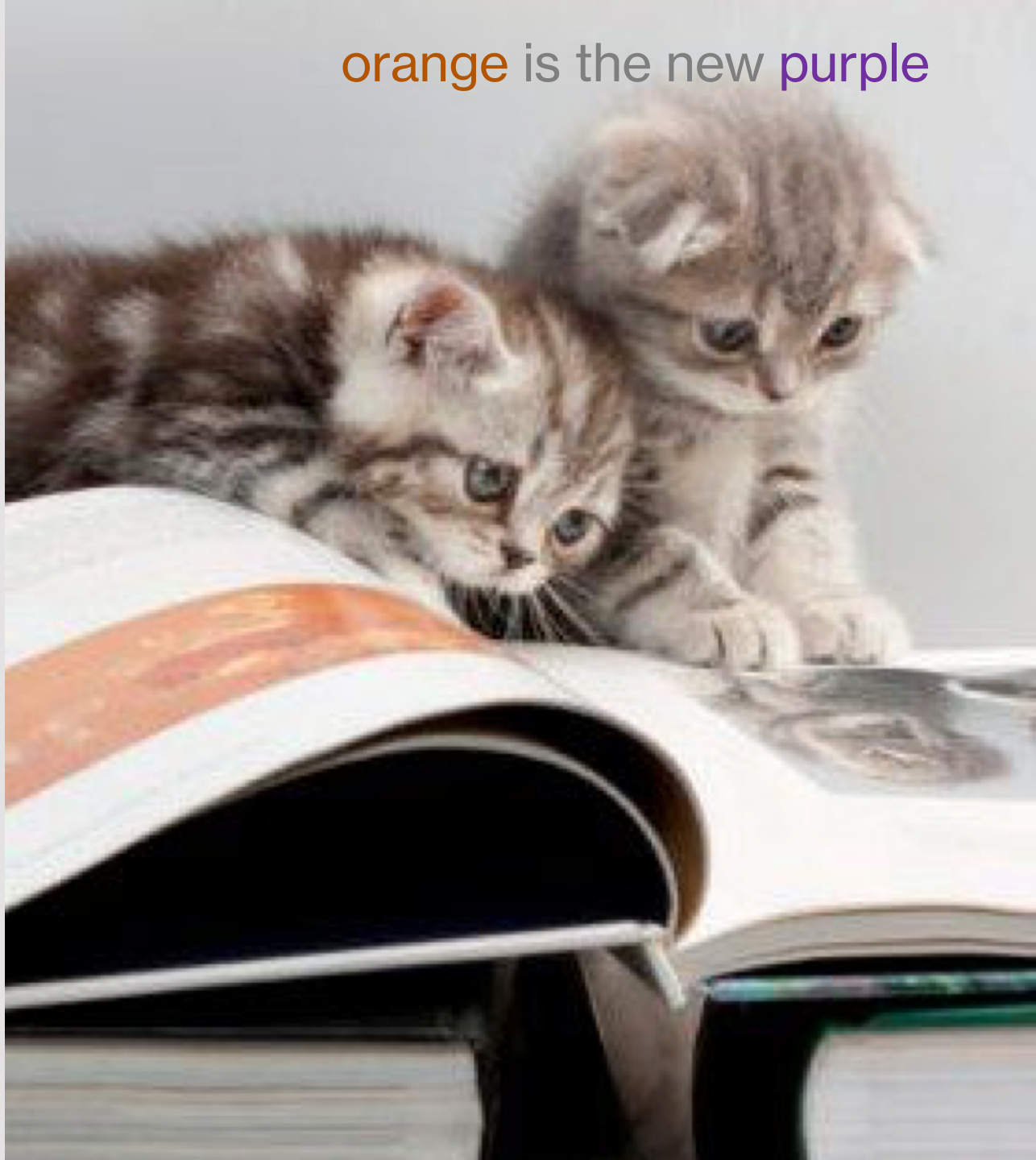
current status:



Can we overcome:

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

Can we work *together*?



Everyone contributes to the security of an organization

(we are on the same team)

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**

PICK

TWO!

NO COMPANY WANTS TO BE IN THE NEWS FOR BEING HACKED....


OMG....I'm so embarrassed


NEW
FEATURE!

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

#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!
I love the Internet...

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*

"Cost of a single data breach is over **$3.5 million**[1]

"**85** new zero-day exploits *every day*[2]

"Software vulnerabilities on COTS products are key entry point for hackers[2]"

Source: https://www.bdna.com/2014/09/02/taking-guesswork-managing-software-end-life/

1. 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2014
2. Symantec Research Labs http://www.symantec.com/connect/blogs/zero-day-world

Relays changed

1100 Started Cosine Tape (Sine

1525 Started Mult + Adder Test.

1545

Relay #7

(moth) in r

First actual case of bug

~~1655~~ 1630 arctangent started.

1700 closed down.

#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

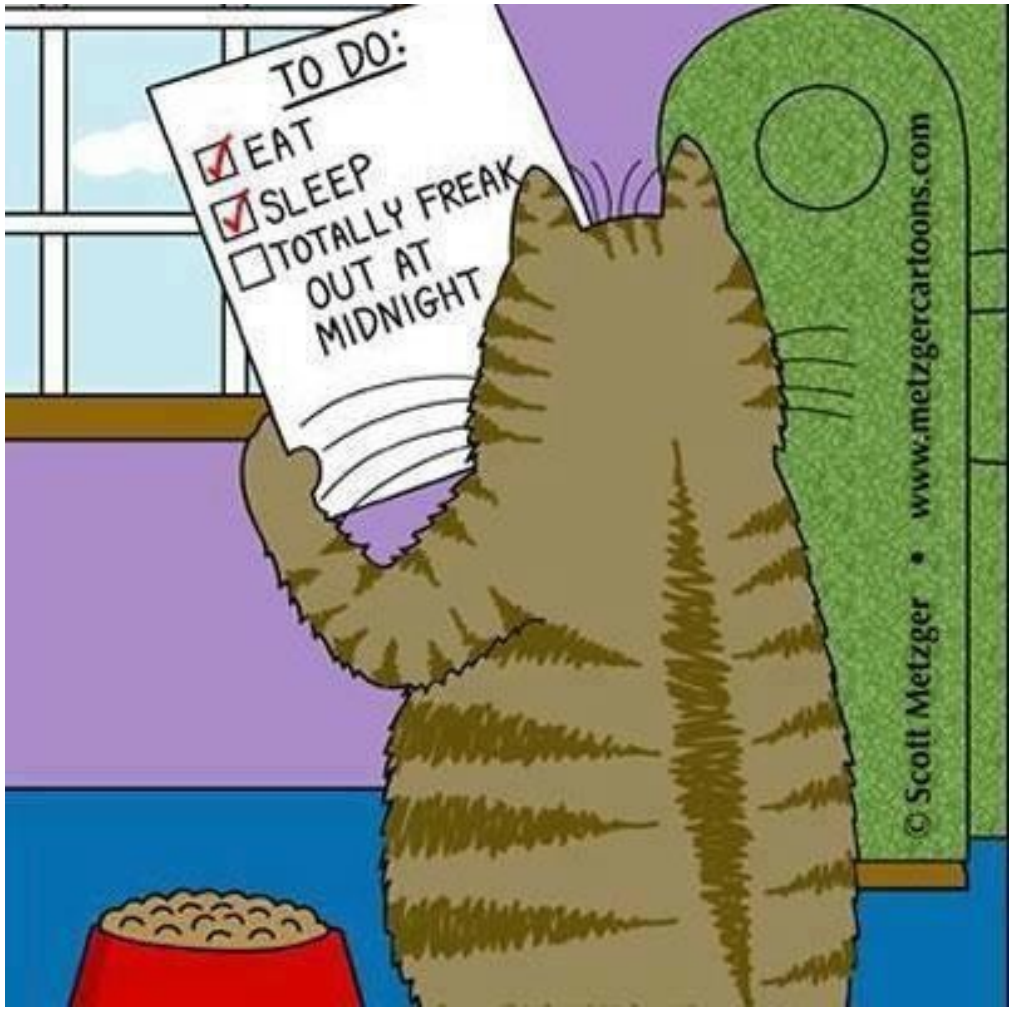
Goals:

- 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
- Better operational capabilities

Being One Team

- Use policy, process, procedures to make working together a requirement
- Security will never be an afterthought
- Informal Orange and Green teamwork
- Teach, learn & connect
- Every interaction is positive
- Be patient – security initiatives can require perseverance

Practical SDLC Security



- 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
- Store artifacts centrally for the entire life of the software
- Cloud Security Alliance has some great resources! (Even if not using ‘cloud’)

Project Managers can help you achieve your goals

- Present your checklists to the PMO as Security's "requirements for launch" or "requirements for production push"
- Work closely with PMO to set expectations
- PMO can plan security tasks in their master timeline
- Policy should mandate Security is involved as early as possible
- Explain the value of "misuse" cases (vs "use cases")
- Estimate time for each task to help with the timeline

Each SDLC phase needs a checklist

- Requirements
- Design and Architecture
- Development and Implementation
- Testing
- Post-Launch Operational Readiness

Sample Planning Phase "Requirements" Checklist

- Step One: Engage security to participate in project
- Define project scope
- Identify compliance goals and determine a compliance timeline
- Contribute Security Use Cases
- Security approval of **all** other Use Cases
- PM generates concept, timeline, budget, everyone agrees or makes changes
- **Obtain Security's approval before moving forward!**

Define and document the scope of your data for GDPR

Privacy Questionnaire

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

Security Use 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

Security Misuse Cases

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.

Sample "Design/Architecture" Phase Checklist

- Prototype design addresses both Security 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**

Your software security is only as good as the security of your vendors

Daily Mail .com — orange is the new purple

Home | U.K. | News | Sports | U.S. Showbiz | Australia | Femail | Health | Science | Mone

Latest Headlines | News | World News | Arts | Headlines | Pictures | Most read | Wires | Coupons

He's the purr-fect employee: Company in Bucharest hires a CAT as communications director.... And it earns more than a typical Romanian

- **Bossy beat off the competition of 700 other applicants for the top job**
- **The fluffy feline was appointed after the company said it was impressed by his attitude**
- **Bossy will reportedly receive a salary equivalent to £110 a month plus bonuses**

By TOM WYKE FOR MAILONLINE

PUBLISHED: 13:22 EST, 9 June 2015 | **UPDATED:** 07:45 EST, 10 June 2015

http://www.dailymail.co.uk/news/article-3117101/He-s-purr-fect-employee-Company-Bucharest-hires-CAT-communications-director-earns-typical-Romanian.html

Know your vendors

Understand them

Audit them

Perform a
gap assessment
on all vendors

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

Sample "Development/Implementation" Phase 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
- **Obtain Security's approval to proceed**

Handling the Checklists

- Tailor the checklists to each project
  - Not every control will apply
- Provide ALL checklists up-front to the PMO
- Be prepared to explain HOW to initiate each process you are requiring
- Keep track of who is responsible
- Completed = Compliance Artifacts
  - Store in a **backed-up, central** repository
  - Store for an adequate amount of time
  - Protect based on Privacy requirements

Stacking Compliances to Achieve Goals

PCI / ISO 27001 / etc.

“Prove your policies are being followed”

Corporate Policy

”Red and Yellow teams work together”

“All new products must follow SDLC”

Artifacts showing Policy is being followed = Success

Measuring Security:
start doing it right meow!

https://www.sans.org/reading-room/whitepapers/analyst/metrics-manage-application-security-program-36822

Tracking Metrics

orange is the new purple

- # of security bugs / trending
- Security bugs vs other bugs
- Severity of security bugs
- Regressions
- Reoccurrence

Important Metrics

For software security to be a priority, CxO's need to understand (from SANS):

- Improvements overall
- Improvement to availability / operational risk
- Reduction of delays to delivery
- Reduction of cost of operations
- Implemented risk reduction techniques
- Residual and unmitigated risks
- Threats to customers/company

https://www.sans.org/reading-room/whitepapers/analyst/metrics-manage-application-security-program-36822

Do not just collect data.

Find ways to use and share your metrics.

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

orange is the new purple

Elicit change with:

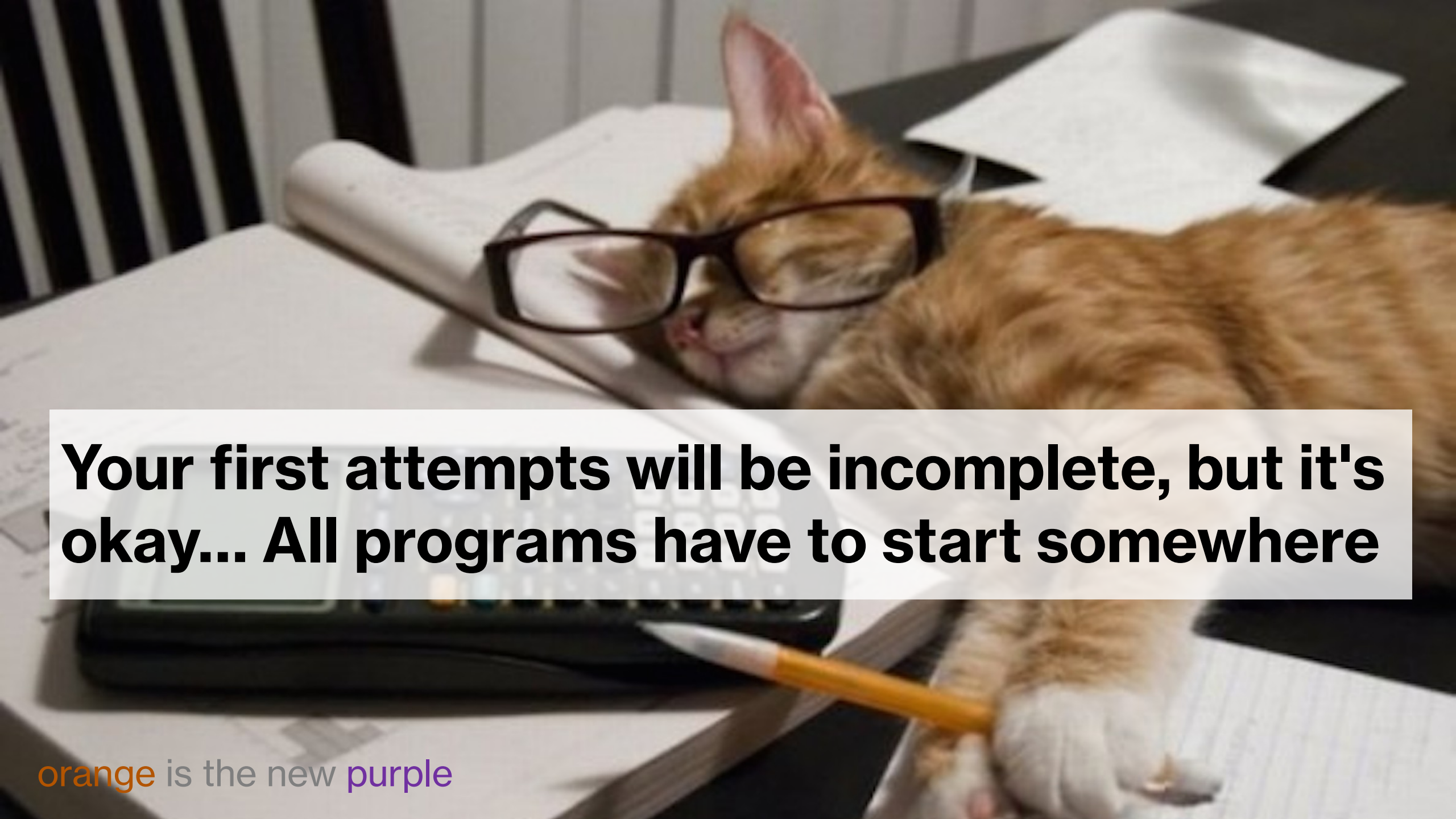
- Empathy
- Rapport
- Policy


orange is the new purple
Security needs to be a strategic business objective


EVIL PLAN PROGRESS
0 ----------|-- 100%
ICANHASCHEEZBURGER.COM

How does it affect *them*?


orange is the new purple
IT'S ALMOST TOO EASY
made on imgur


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

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

CULTURE CHANGE DOES NOT HAPPEN OVERNIGHT

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

— General Michael Hayden,
retired head of CIA, NSA

orange is the new purple

by April Wright for DEFCAMP 2017

@aprilwright

#ORANGETEAM
#DEFCAMP

ArchitectSecurity.org

verizon

enjoy the con ☺

orange is the new purple

by April Wright for DEFCAMP 2017

@aprilwright

#ORANGETEAM
#DEFCAMP

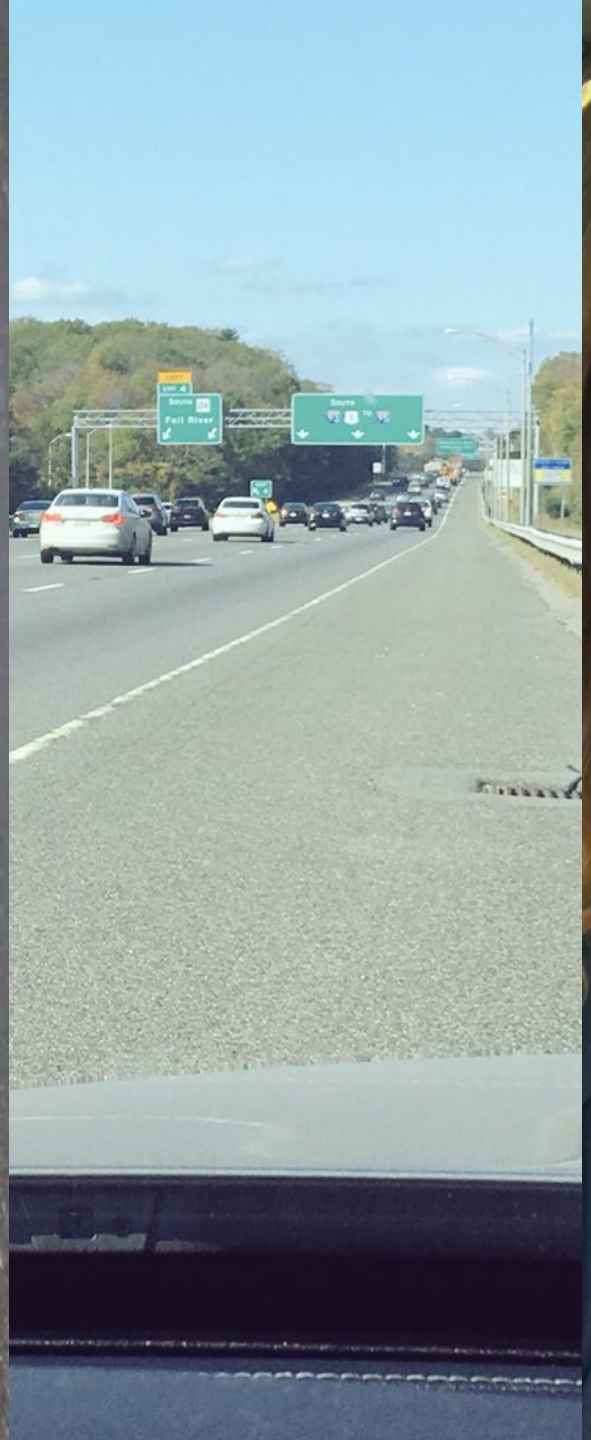
ArchitectSecurity.org

verizon

enjoy the con ☺

rm –rf ./archived_slides

<interlude>


South
Fall River

</interlude>


Under
Construction


ESC

"Cost of a single data breach is over **$3.5 million**[1]

"**85** new zero-day exploits *every day*[2]

"Software vulnerabilities on COTS products are key entry point for hackers[2]"

Source: https://www.bdna.com/2014/09/02/taking-guesswork-managing-software-end-life/

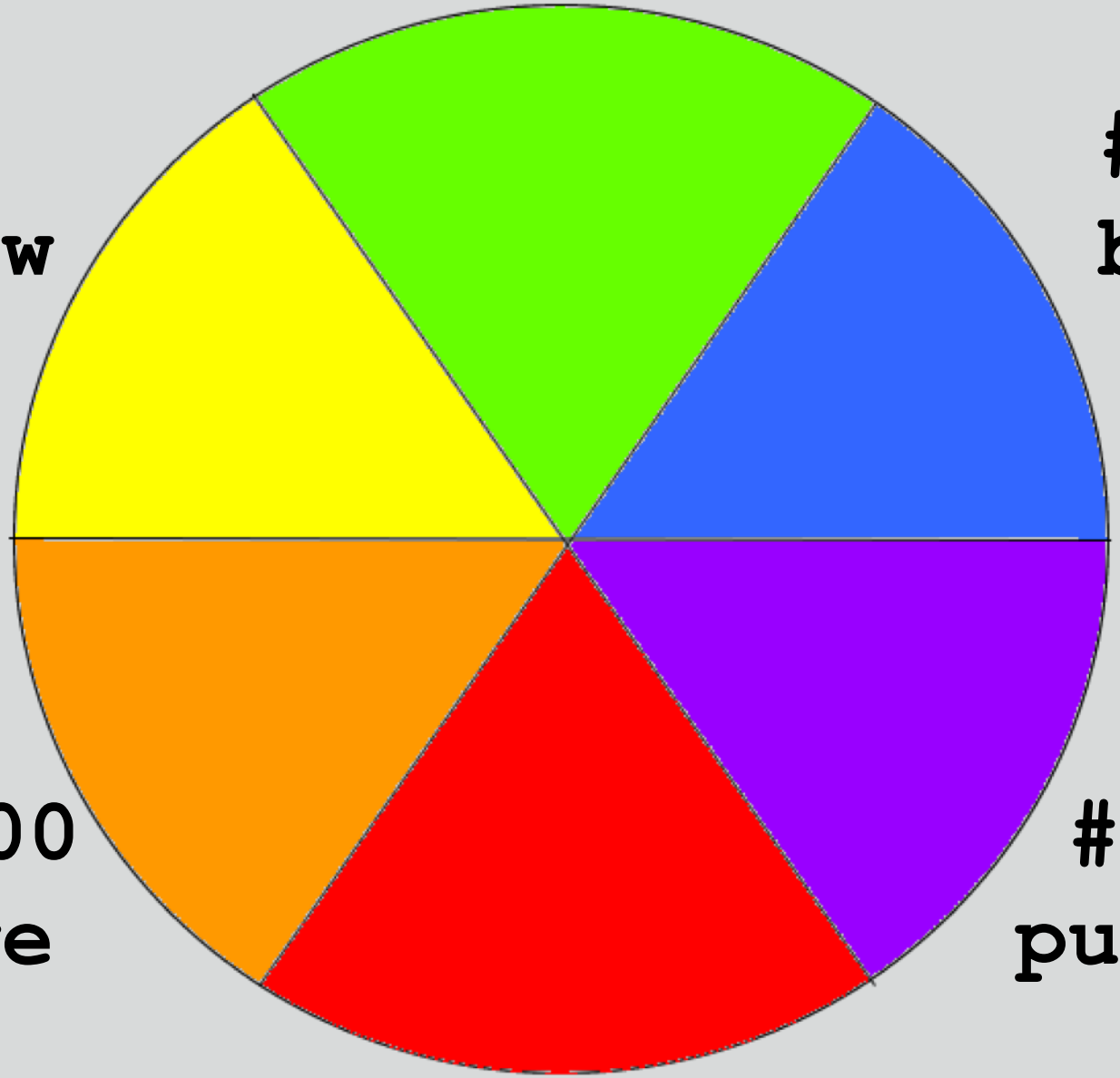
1. 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2014
2. Symantec Research Labs http://www.symantec.com/connect/blogs/zero-day-world

orange is the new purple

#0F0 green

#FF0 yellow

#F00 blue



#FFA500 orange

#F00 purple

#F00 red

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)


orange is the new purple

#ORANGETEAM
#DEFCAMP

@aprilwright

ArchitectSecurity.org