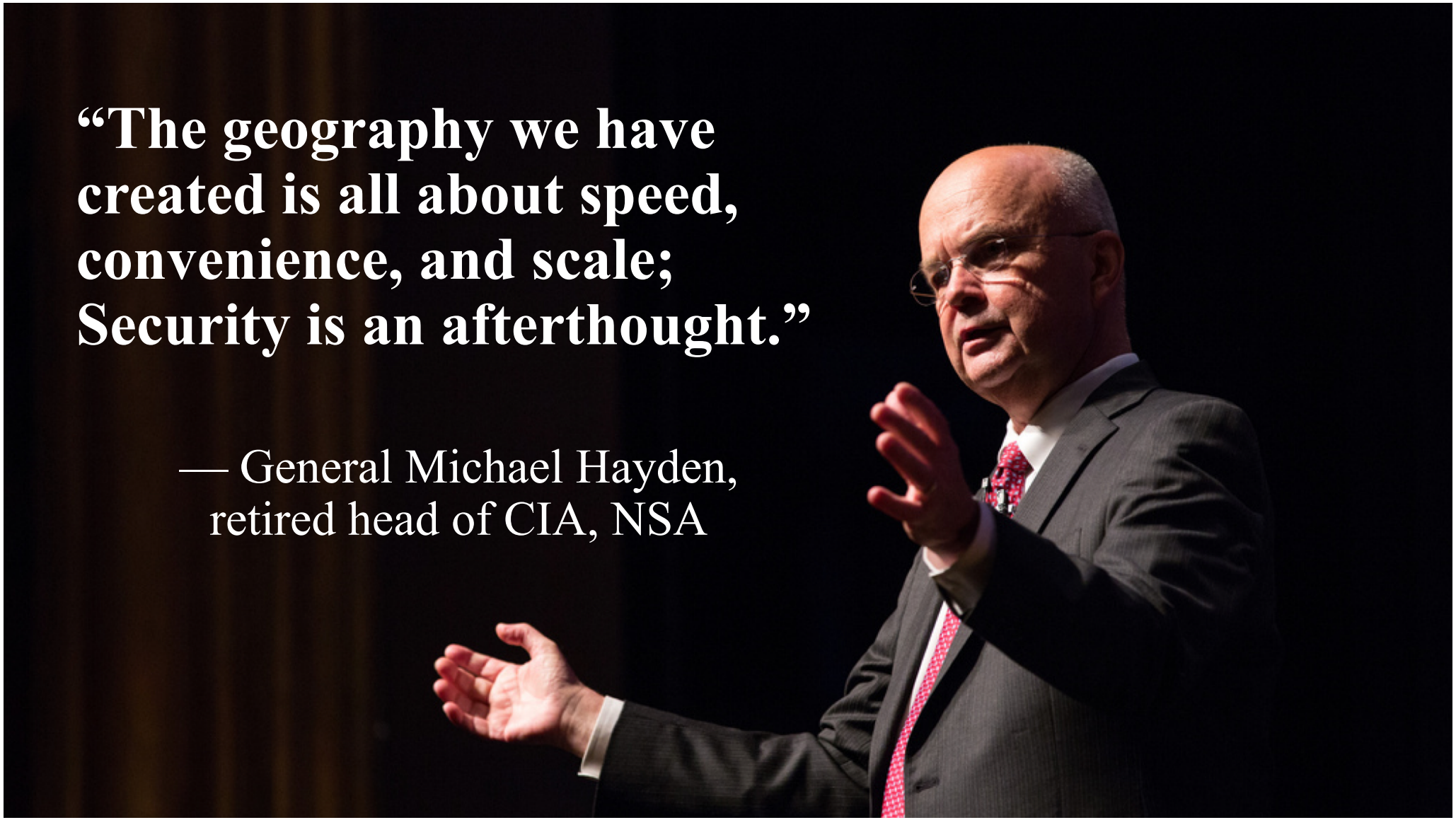
# orange is the new purple

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

verizon

aprilwright


“The geography we have created is all about speed, convenience, and scale; Security is an afterthought.”
— General Michael Hayden, retired head of CIA, NSA

# We have different primary directives

| Security's goals? | Builder's goals? |
| --- | --- |
| create it securely | time to market |
| maintain it properly | correctness |
| prove it’s secure | optimization |
| plan for sunsetting | minimal defects |


current
status:
orange is the new purple
DEVELOPERS
RED TEAM

# 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

aprilwright

- Infosec generalist
- Security expositor
- @Verizon

**XP**:
offensive testing, defensive sdlc, GRC, detection, df/ir, coding, soft skills, unix ops, sec ops, coding, databases, web apps, gaming, graphic design, photography…

^^ *me coding sprites*


@aprilwright

# Software challenges: Security's view

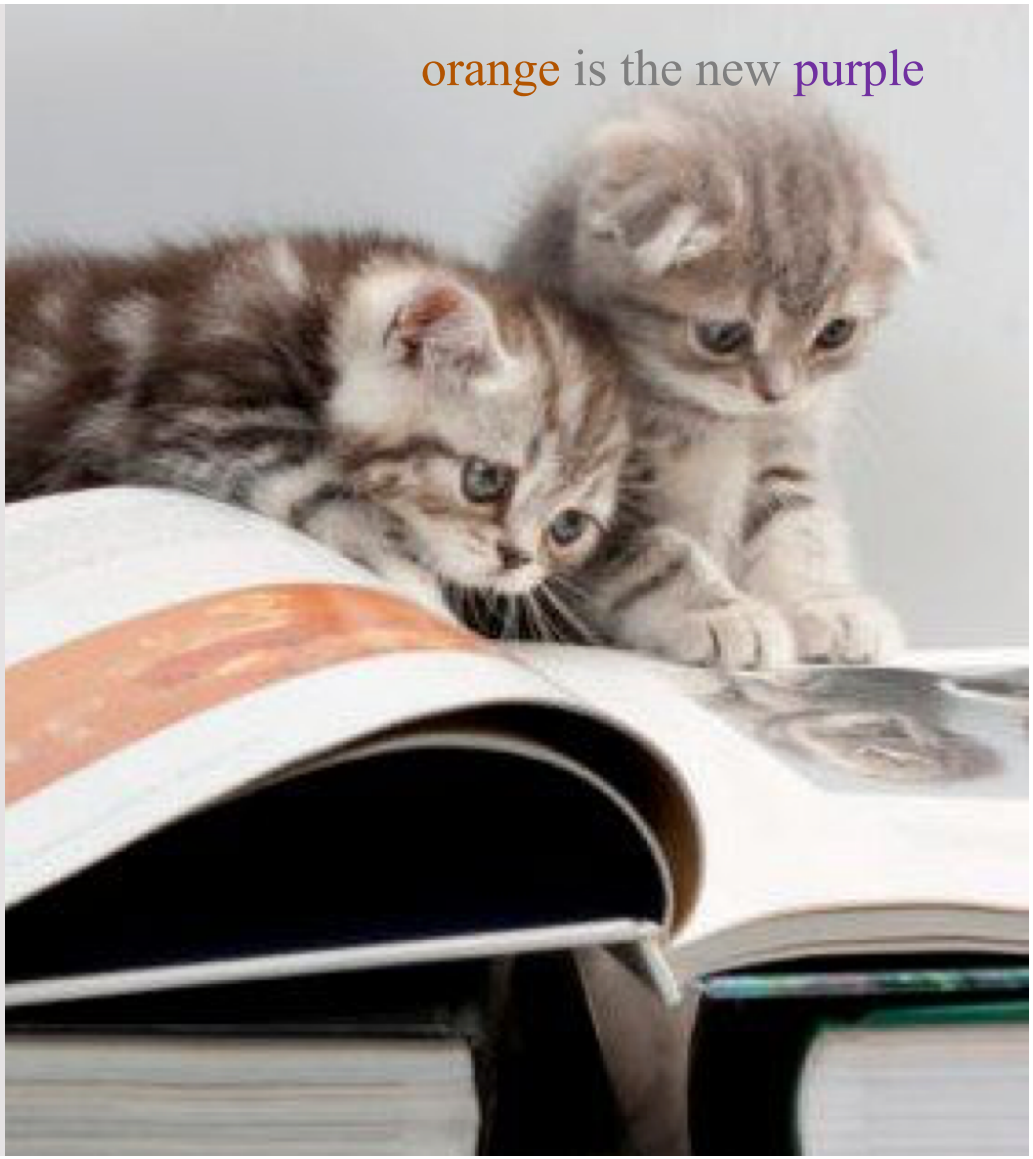
- Unknown scope of applications, libraries (Builders know this!)
- Everyone is averse to testing in production
- Why doesn't everyone just 'get it'?"
- Inability to sustain iterative release testing
- **"Organizational and communications silos between security, application development and the rest of the organization"** (starts in .edu, perpetuated in .com)

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

**Can we overcome:**

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

**Can we work *together*?**




## There is hope for creating more secure software

Builders *want* to learn about security!

Security wants to share knowledge!

Organizations embrace cross-training (generally)

orange is the new purple

# Everyone contributes to the security of an organization

( we are on the same team )

# Because #infosec loves triads

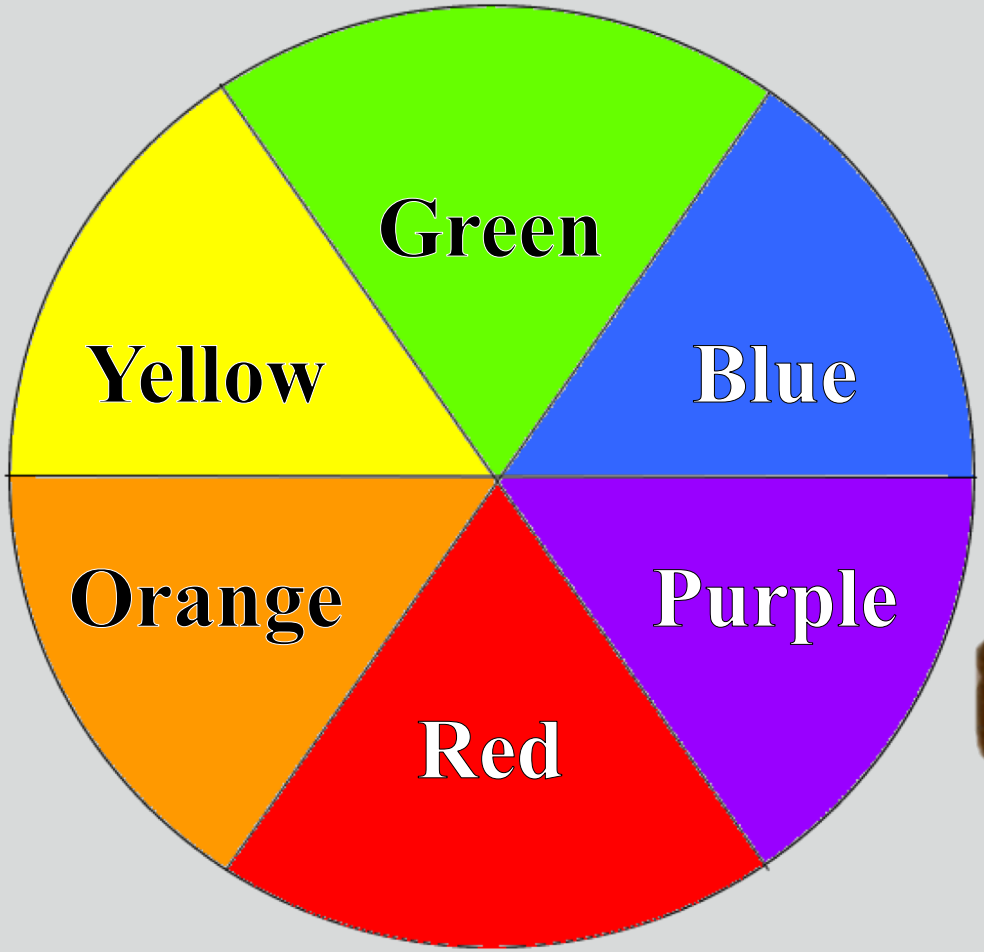
**Breakers**
(Red Team)

**Guardians**
(Blue Team)

**Builders**
(Yellow Team)

orange is the new purple

orange is the new purple



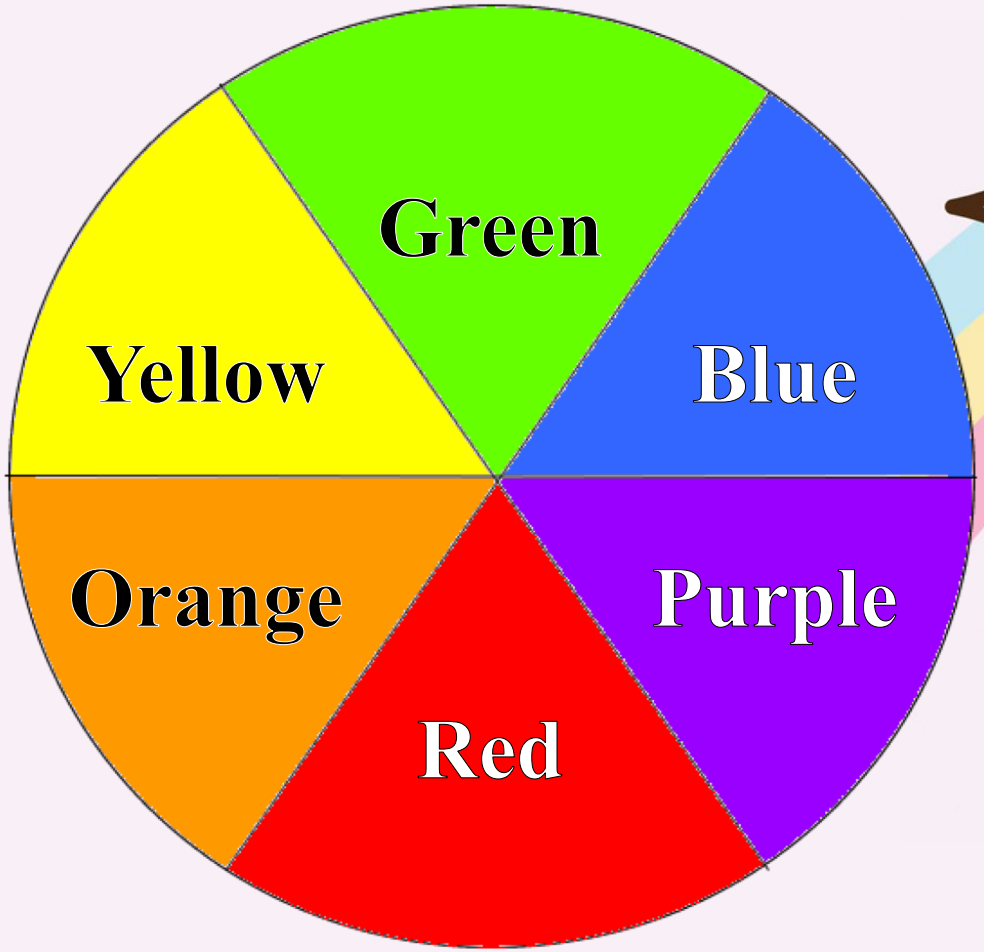


#F00 + #00F = #800080 purple

#FF0 + #00F = #0F0 green

#FF0 + #F00 = #FFA500 orange

orange is the new purple





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

orange is the new purple

# Introducing…

**#ORANGETEAM**

**#GREENTEAM**

**#ORANGETEAM (#0F0)**

**Focus: Developing a threat-mindset via Red Team**

- 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 (#0F0)**

**Goals**:

- Discussions lead to other, related problems
- Offensive critical thinking included in builder's personal frame of "correctness" + "accuracy"
- Can avoid "misuse cases" (these are so fun!)
- Decrease in overall security bug counts *over time*

**#GREENTEAM - #0F0**

**Focus: improving forensics + incident response**

- Tune and improve detection capability
  - e.g. Enhanced logging
- More visibility built into important functions
  - Functional introspection
- Integrate software with security automation

**#GREENTEAM - #0F0**

**Goals:**

- Gaps in detection get addressed
- Known-insecure code can be risk-evaluated
- Improved introspection capabilities
- Thorough, standardized audit trails


orange is the new
CULTURE CHANGE DOES NOT HAPPEN OVERNIGH T

# Initiate change, be patient

- Solidify your goals with organizational policy (it all starts there!)
- Start molding a "one team" mentality (it's 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

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

-- Mattie Stepanek

# "BlackHat Soundbytes"

- Security should never be an afterthought
- Software builders and defenders should be a team
- Methodology does not need to be formal
- Teach, learn & connect with each other
- Make every interaction positive, not just negative
- Add cross-team interactions to policy, process, procedure to formalize requirement to do so
- Be patient – security initiatives can require perseverance

aprilwright

#ORANGETEAM

**Please provide feedback to BlackHat for this session! ☺**

# orange is the new purple

by
april wright
BlackHat
2017
#bhusa


enjoy
the
con
☺