# SOFTWARE ENGINEERING SECURITY EFFECTIVENESS

SEAN SCOTT & JOHN BENNINGHOFF

ENTERPRISE ENGINEERING

SECURITY ENGINEERING

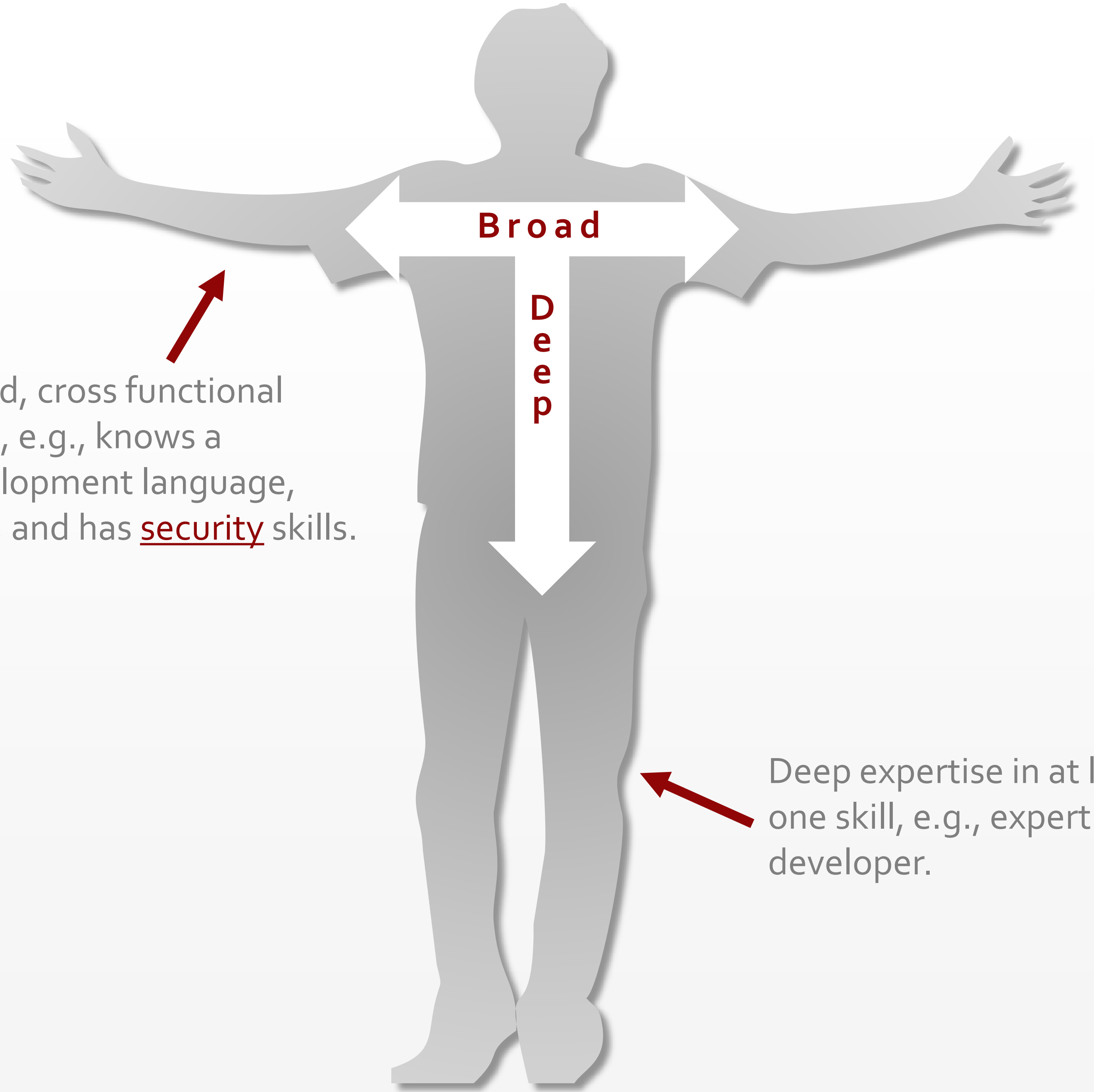
# SOFTWARE ENGINEERING SECURITY

Patterns & Practices

Secure Testing

Security Engineering

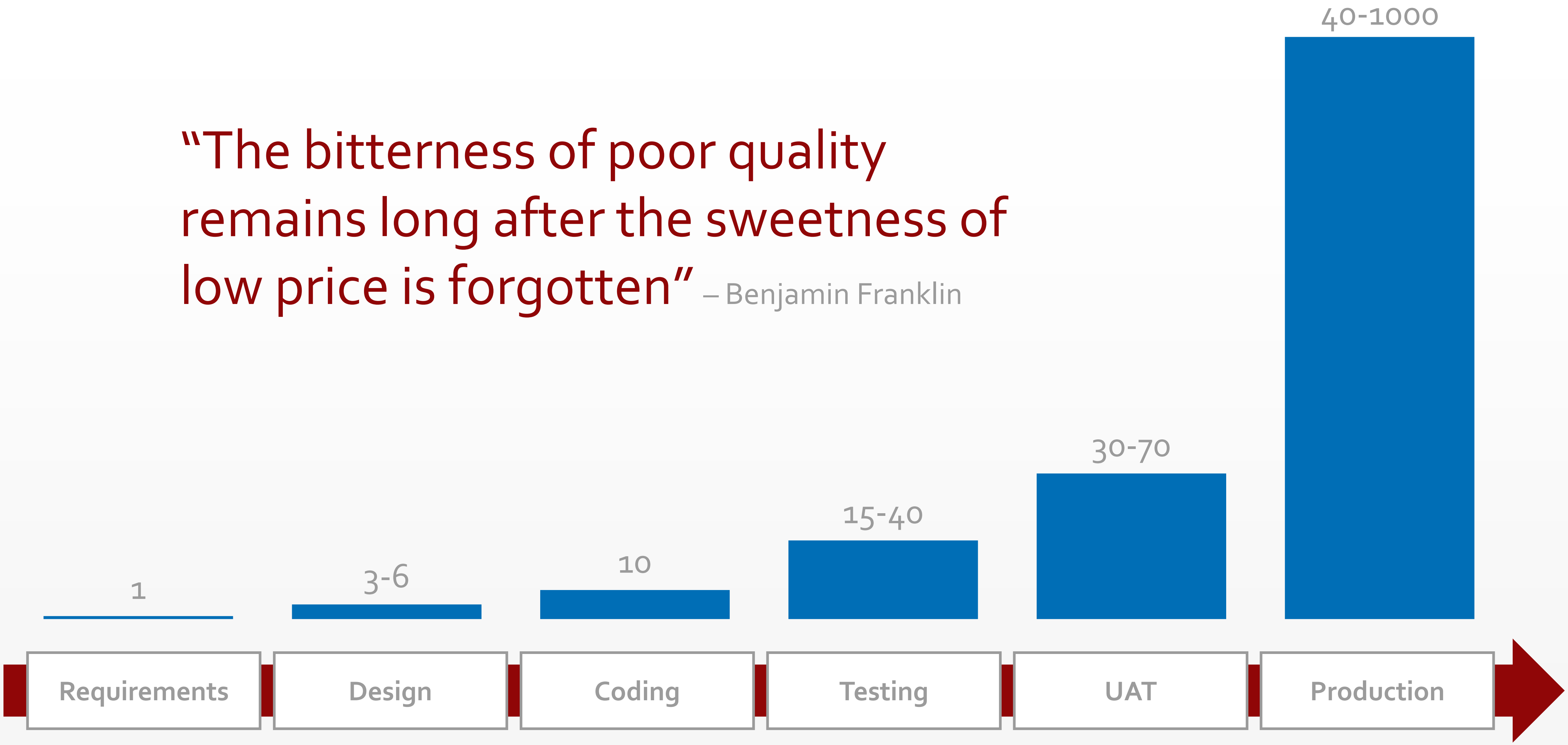
# “T”-TYPE TEAM MEMBERS



Broad, cross functional skills, e.g., knows a development language, SQL, and has security skills.

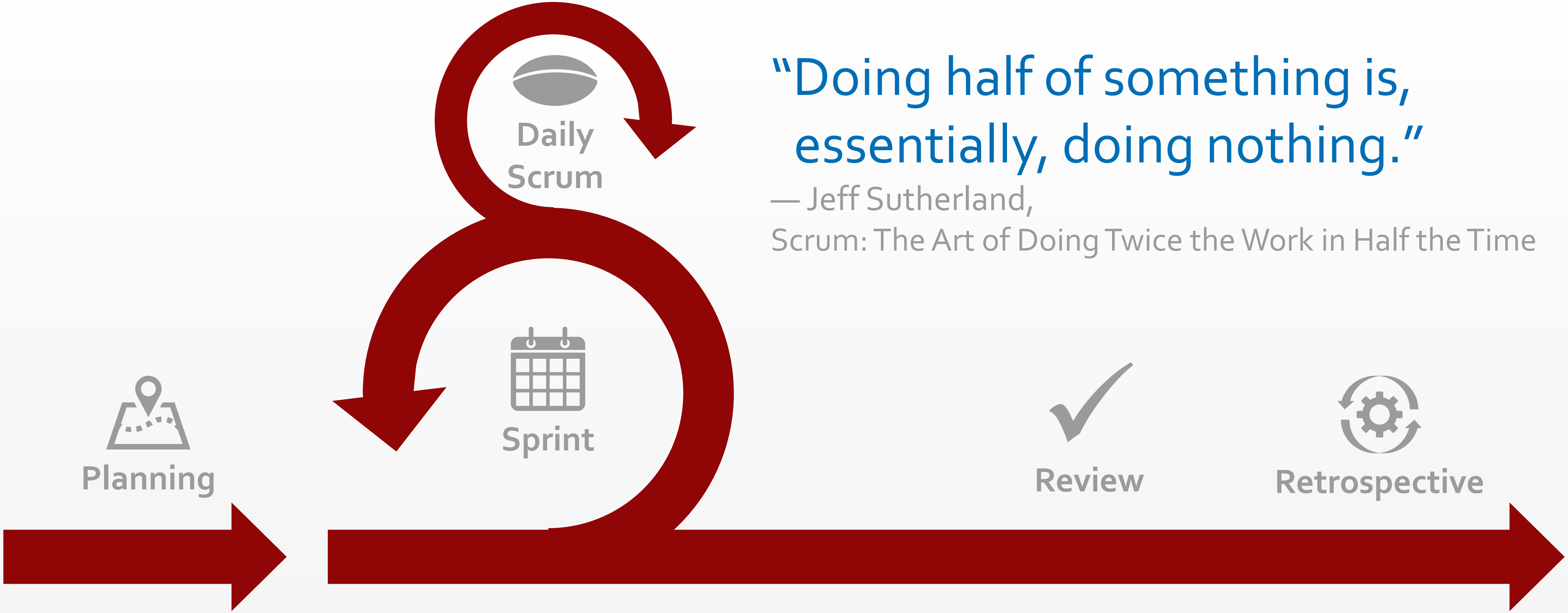
Deep expertise in at least one skill, e.g., expert level developer.

"The bitterness of poor quality remains long after the sweetness of low price is forgotten" – Benjamin Franklin



Relative cost to fix bugs found throughout the SDLC

# SCRUM EVENTS



"Doing half of something is, essentially, doing nothing."

— Jeff Sutherland,
Scrum: The Art of Doing Twice the Work in Half the Time

There is no wrong time to ask,
“How will that affect security?”
—Sean Scott

# HOW WELL ARE WE DOING?

# NULL HYPOTHESIS

The exposure to the training, coaching, and consulting services offered by the Software Engineering Security (SES) group DOES NOT influence the quality of code installed into a production environment, as measured by application security penetration testing.

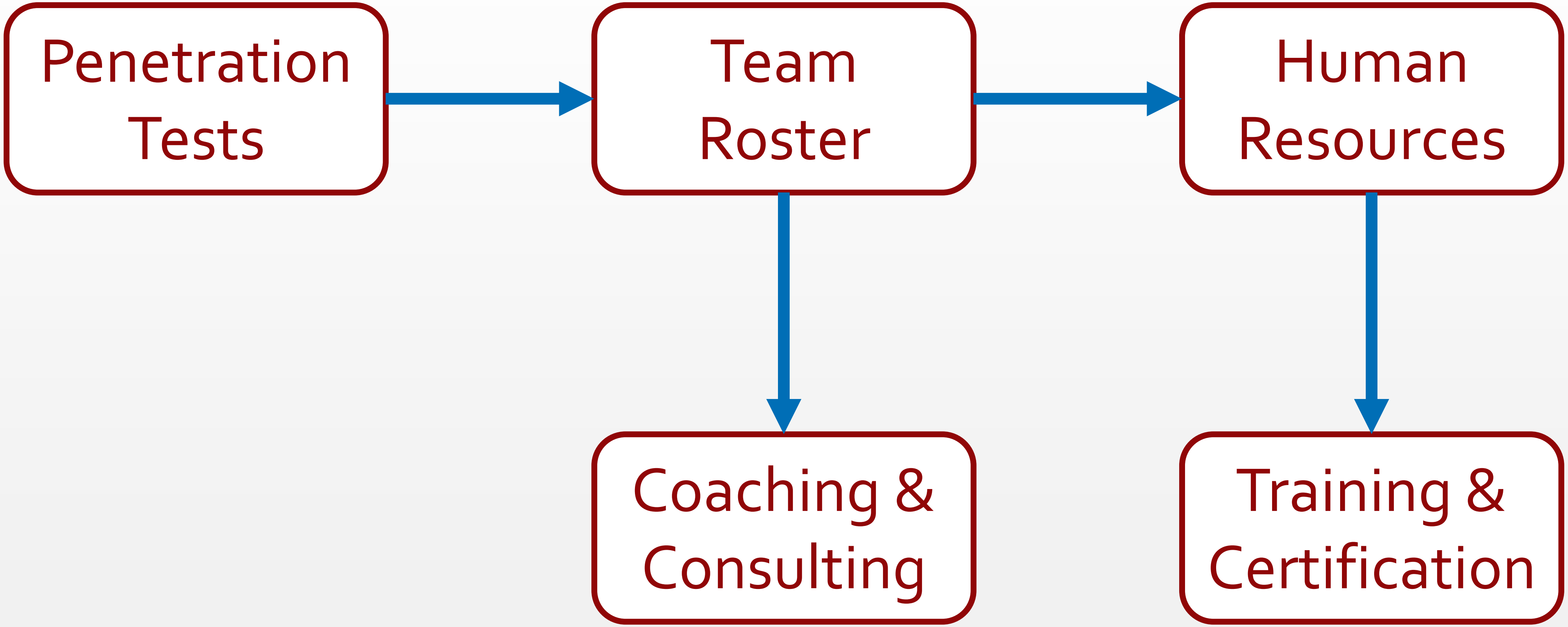
# STUDY DETAILS

retrospective comparison

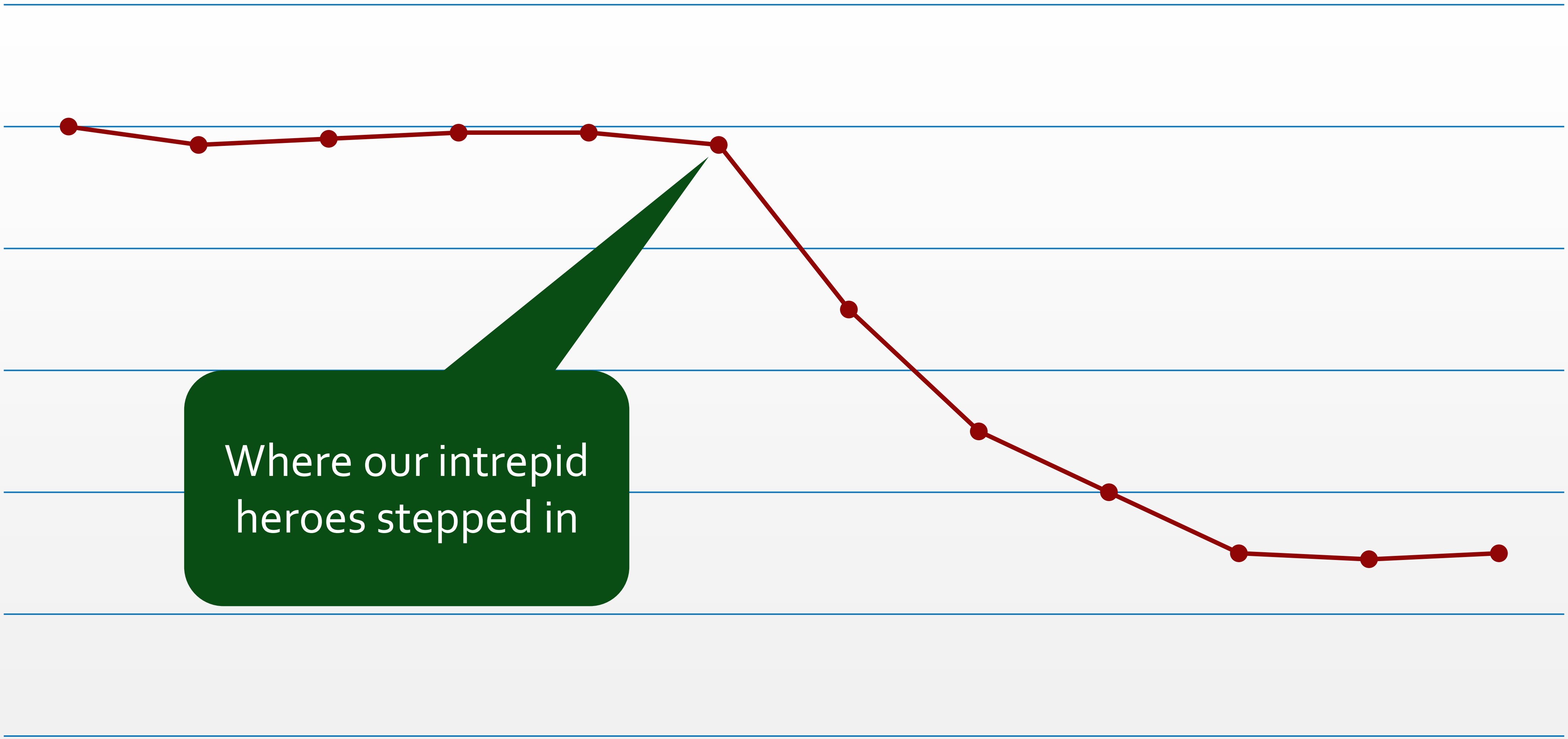
460 Teams

32 months

# EXPECTED DATA ORGANIZATION

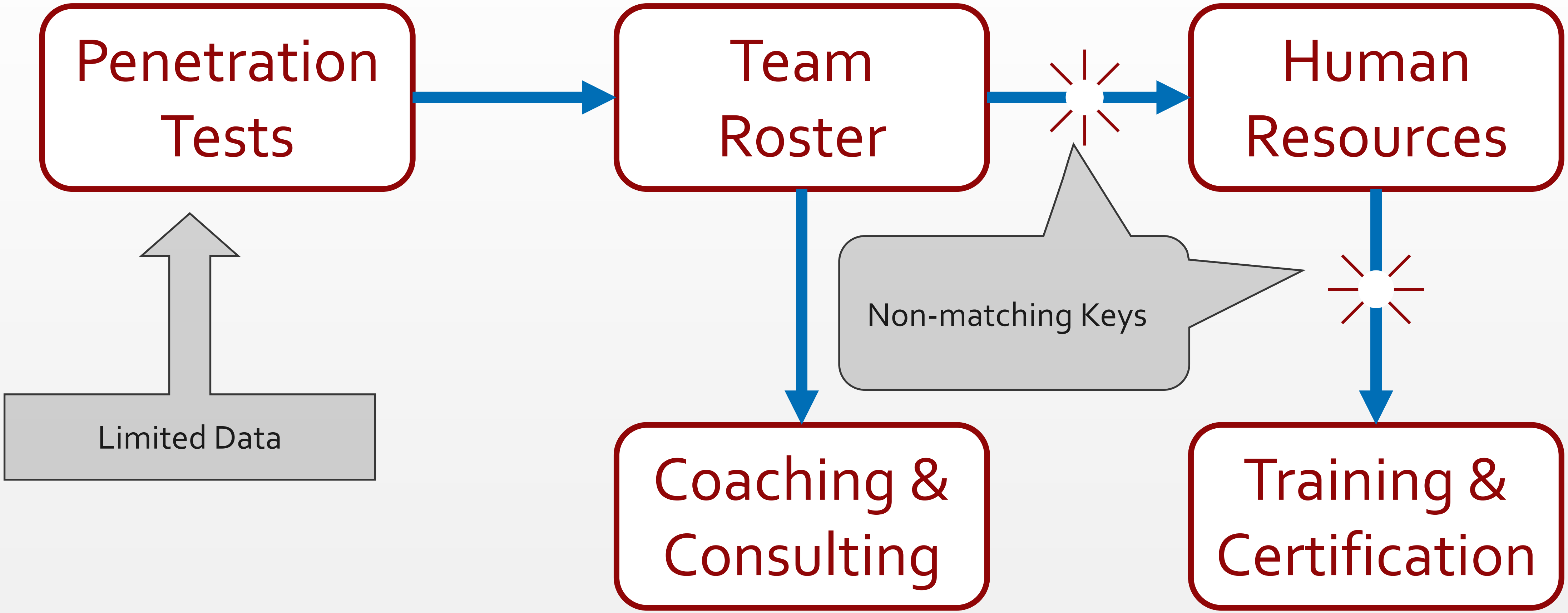


# WHAT WE HOPED TO FIND



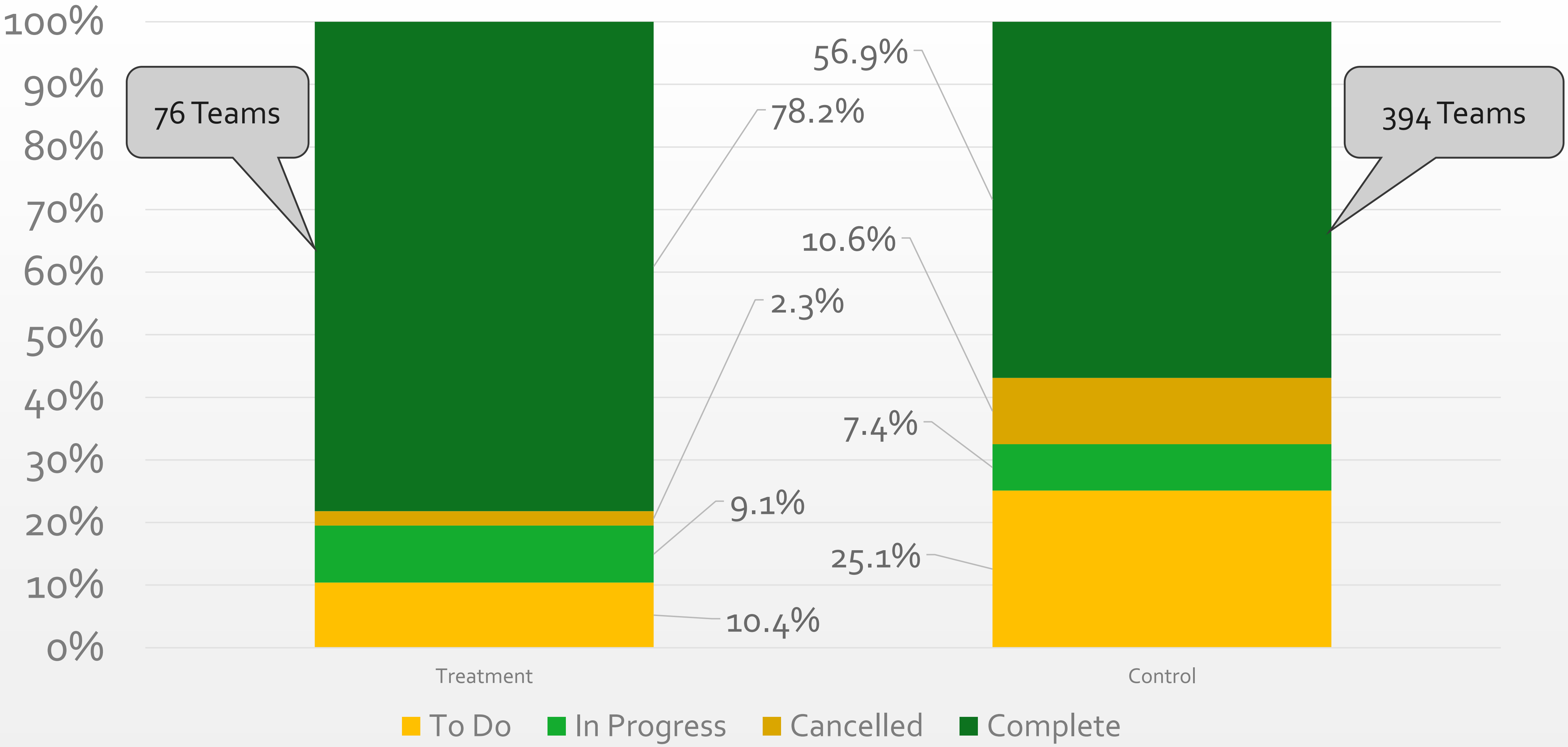
Where our intrepid heroes stepped in

# ACTUAL DATA ORGANIZATION

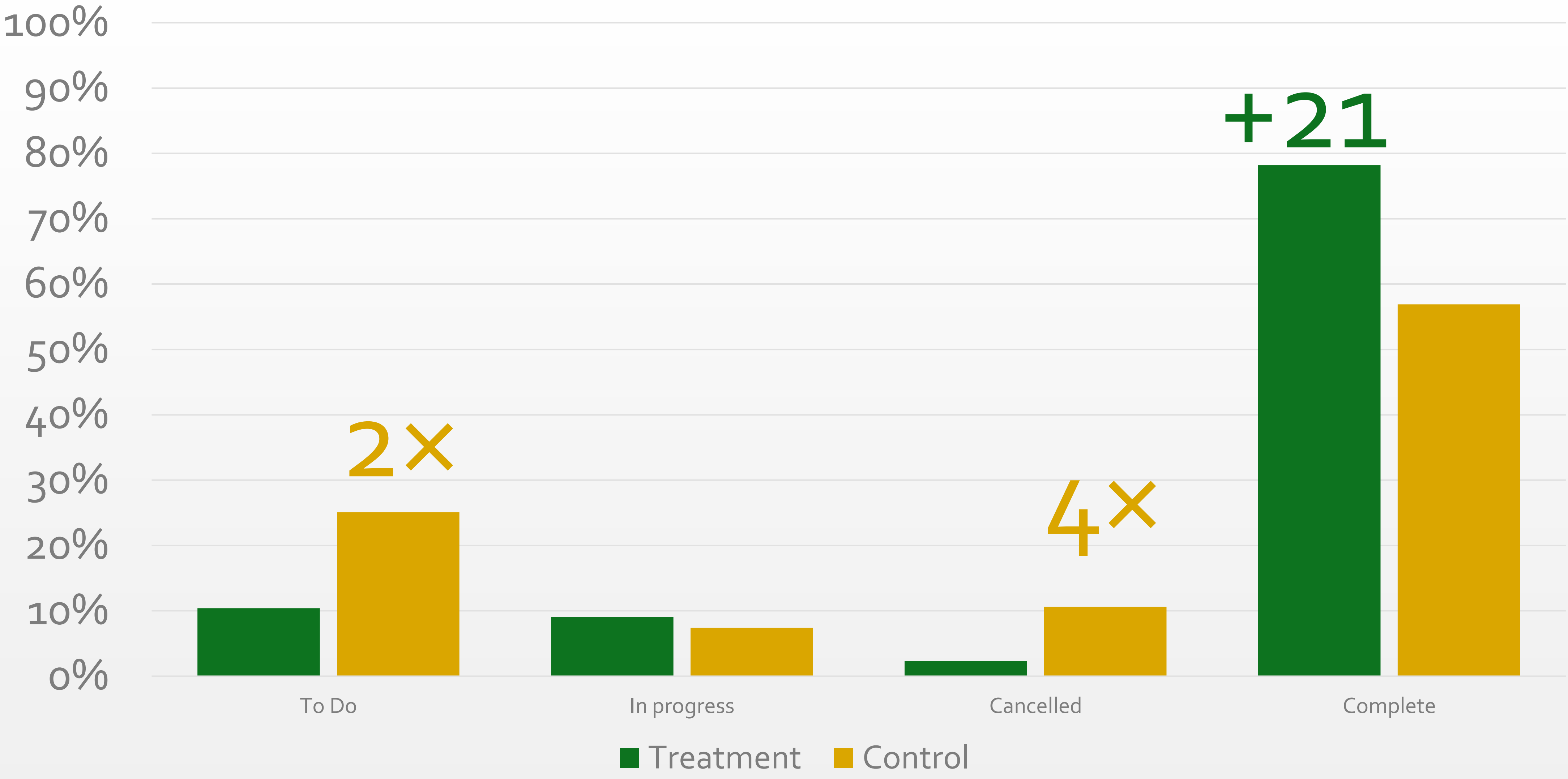


# What can the data we have tell us?

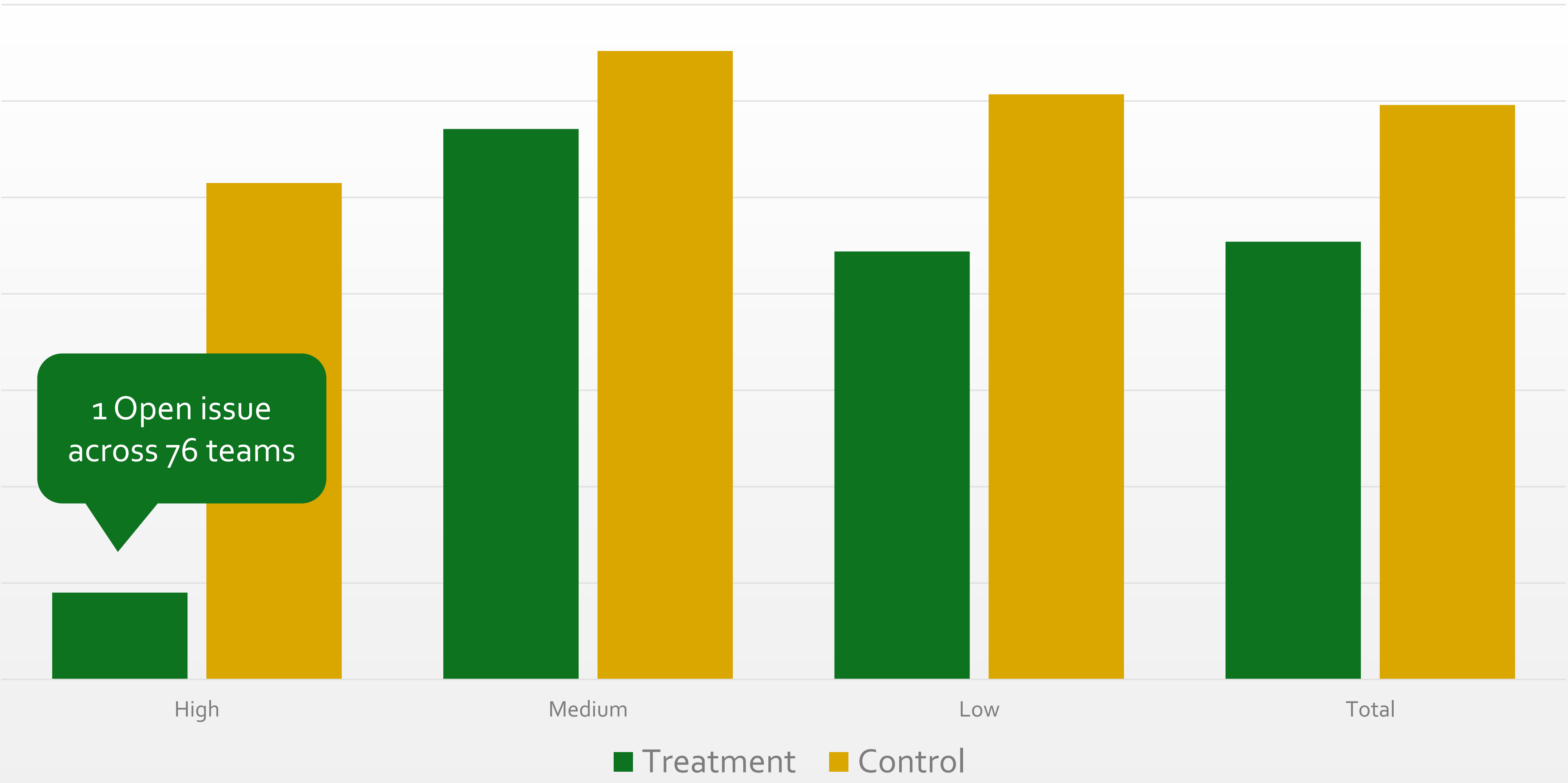
# ISSUES BY GROUP



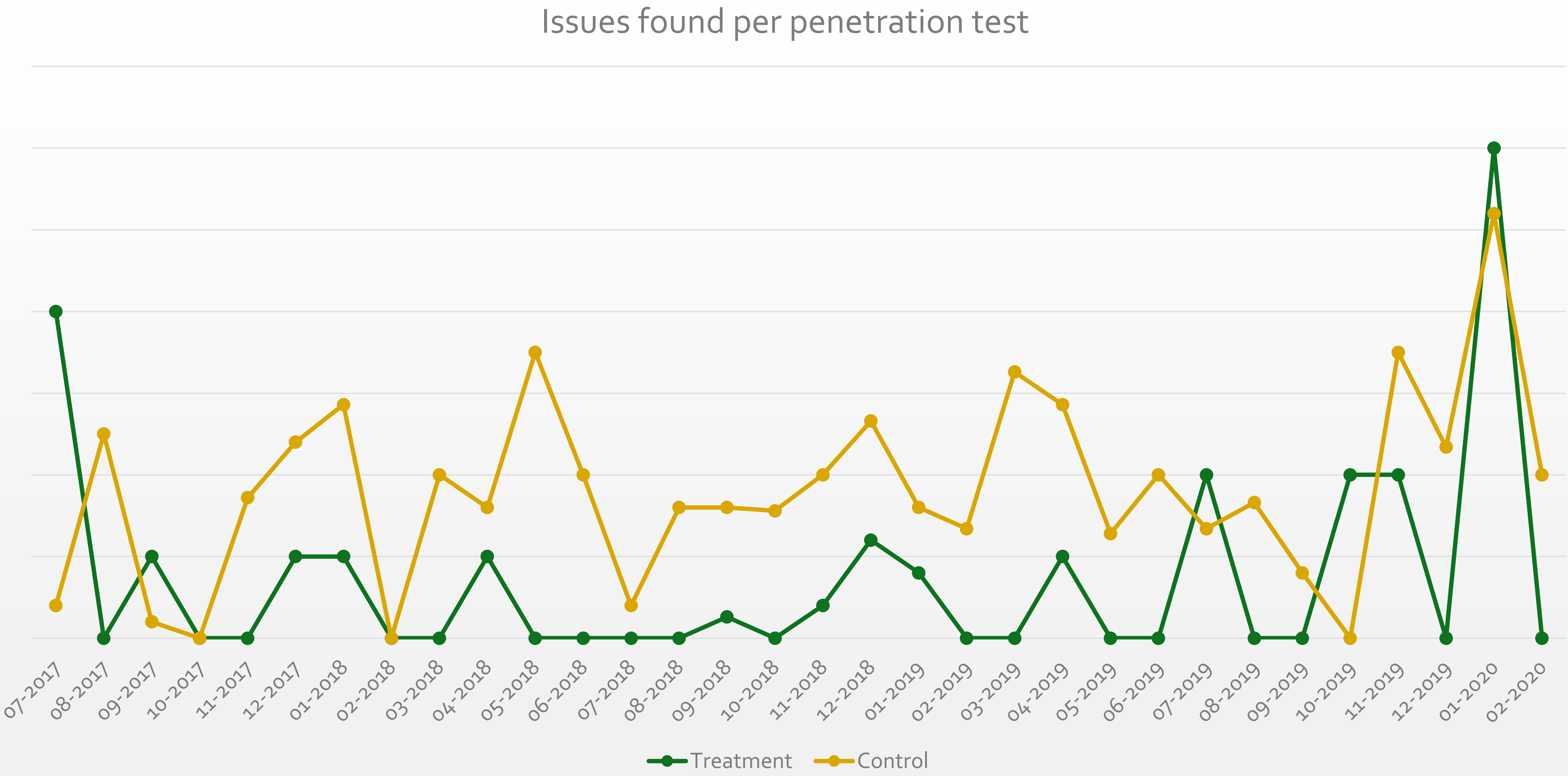
# ISSUES BY GROUP—FLIPPED



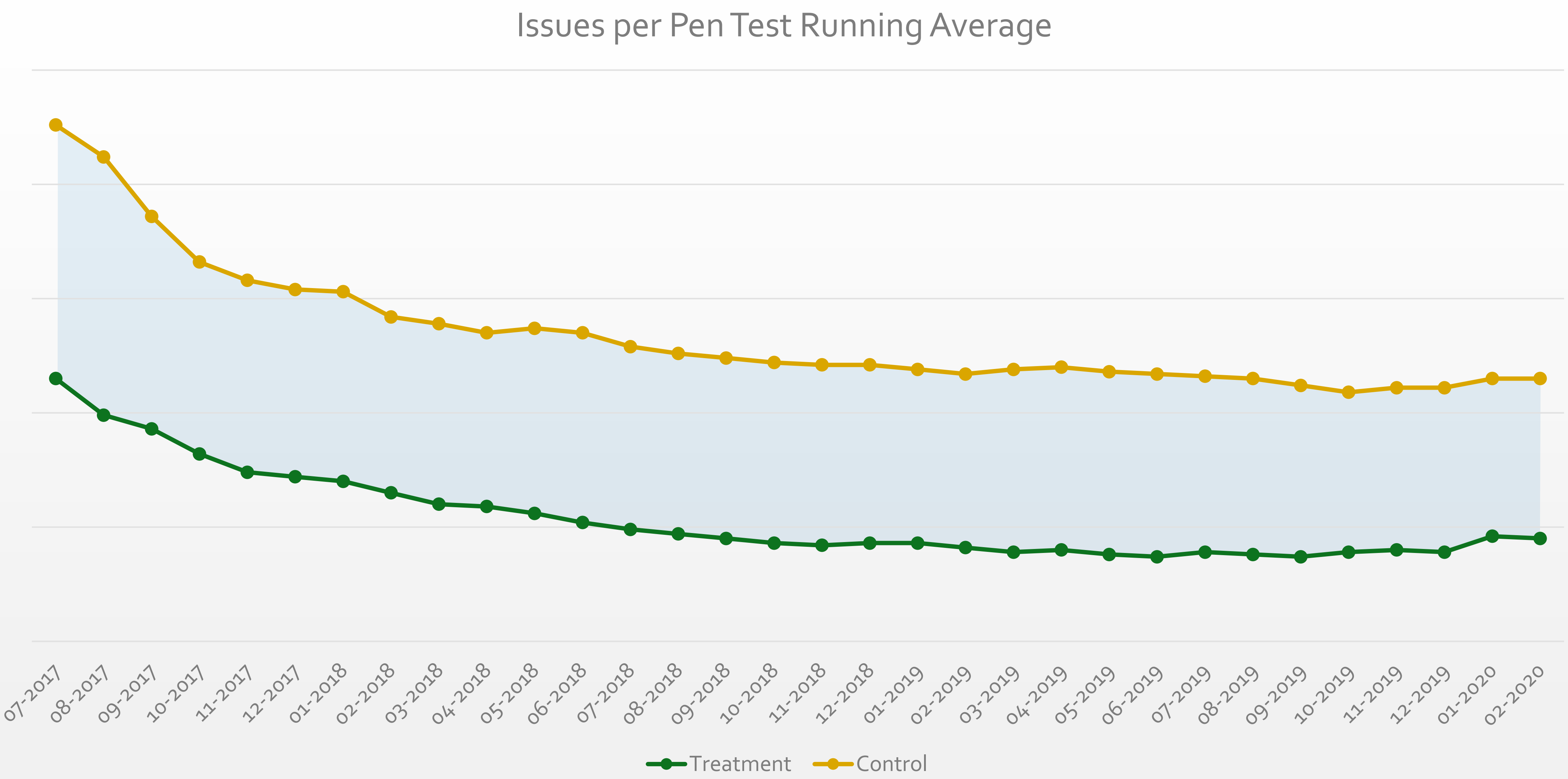
# AGING BY SEVERITY IN DAYS



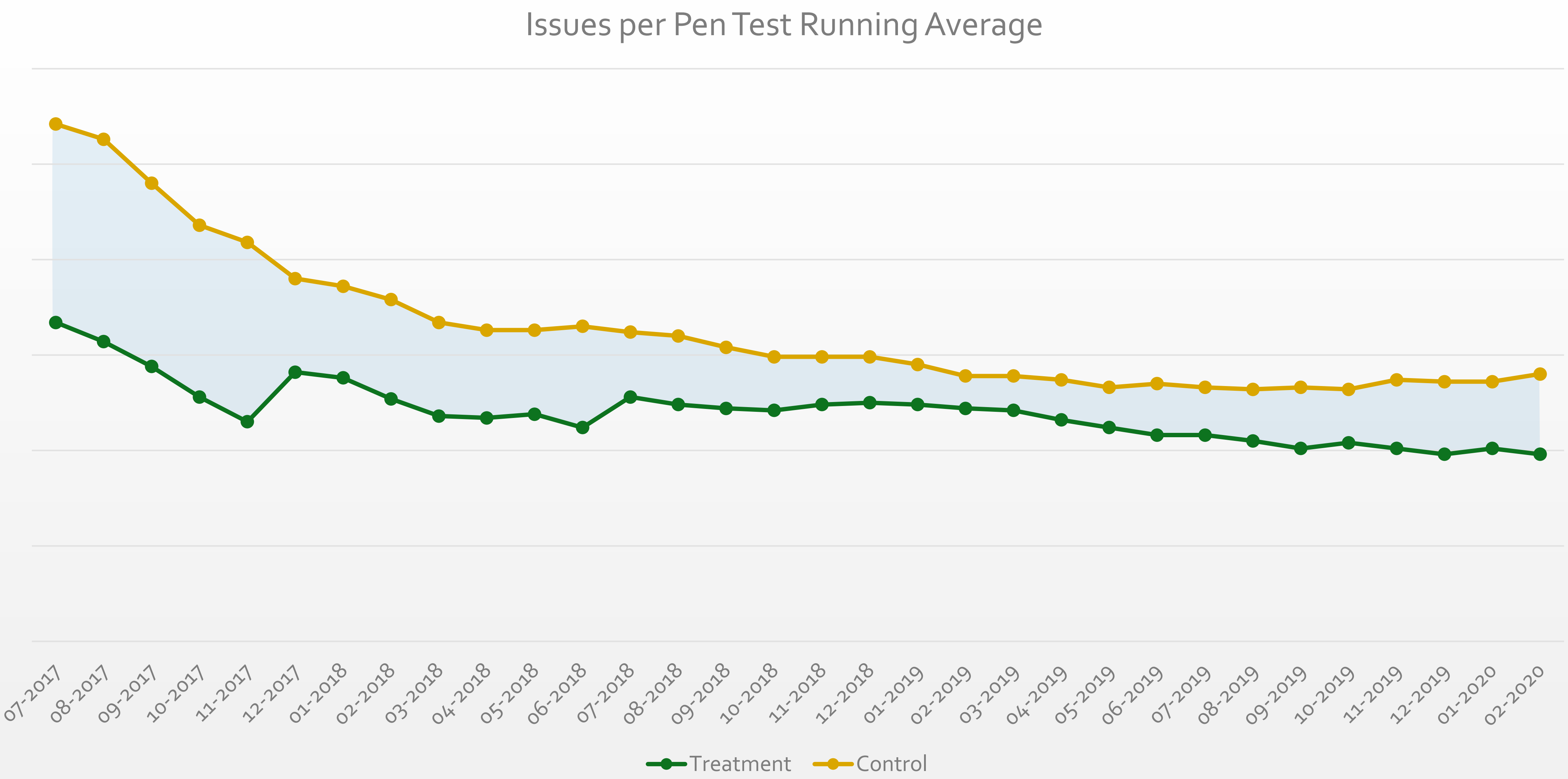
# HIGH-RISK ISSUES OVER TIME



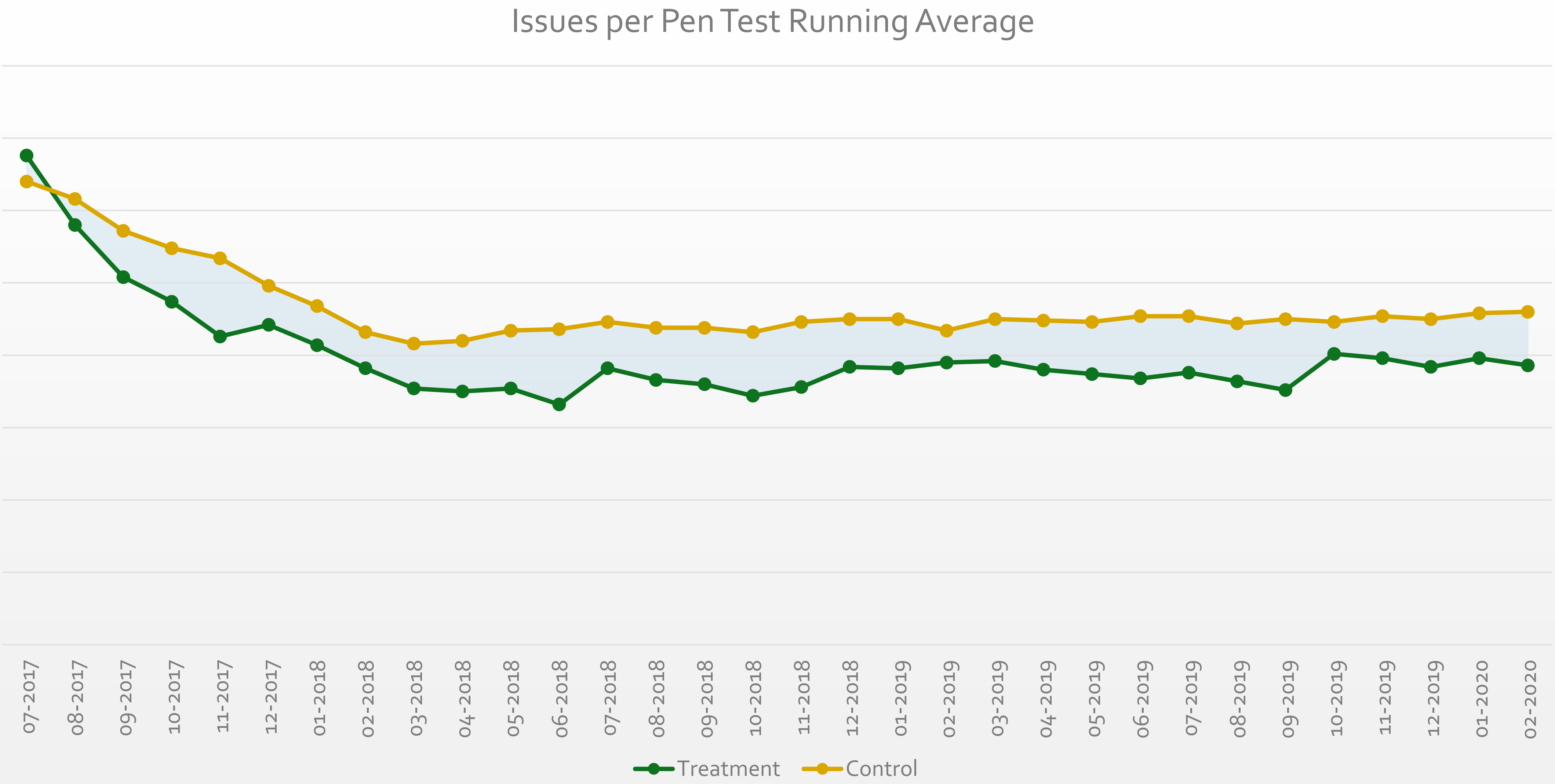
# HIGH-RISK ISSUES OVER TIME



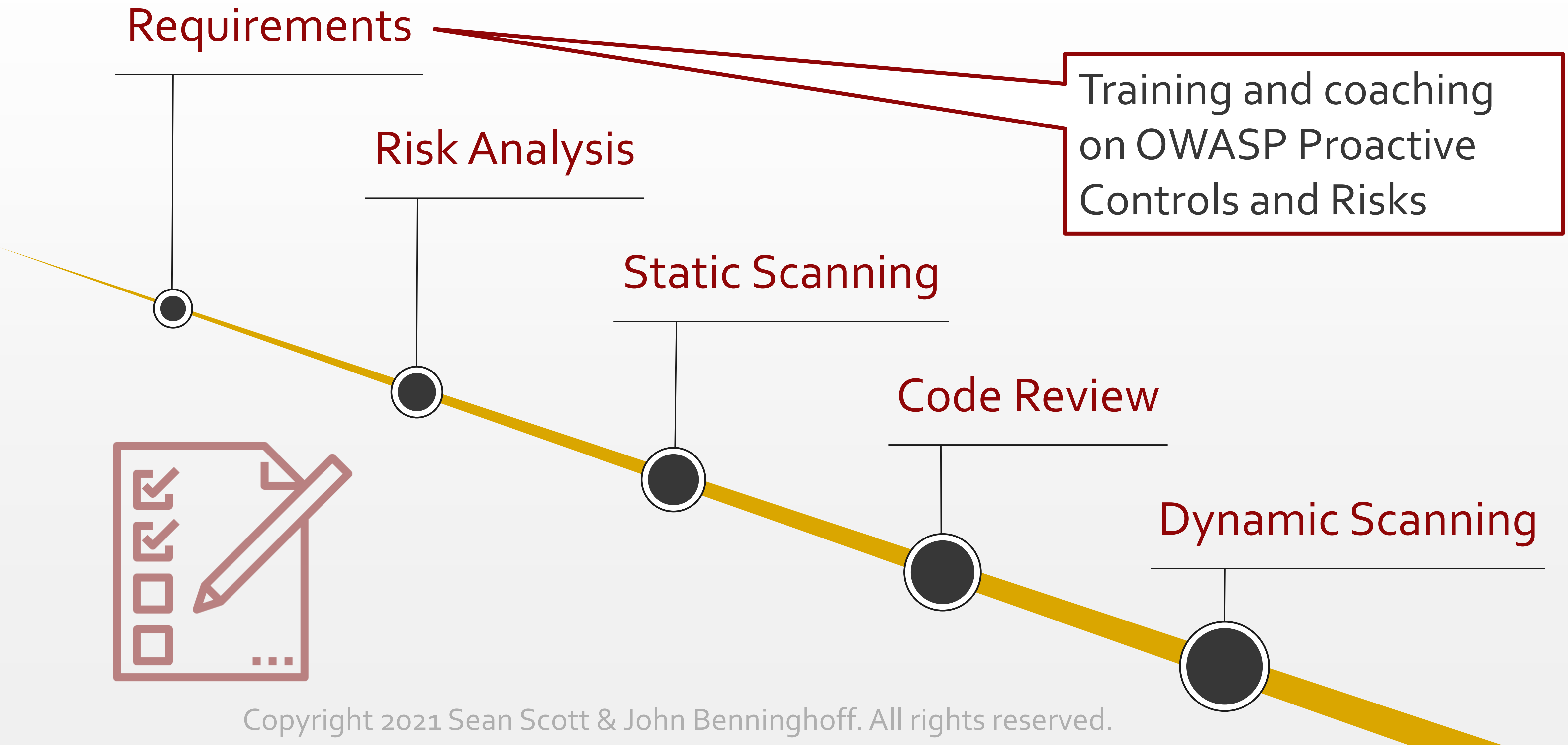
# MEDIUM-RISK ISSUES OVER TIME



# LOW-RISK ISSUES OVER TIME



# TREATMENTS



Requirements

Risk Analysis

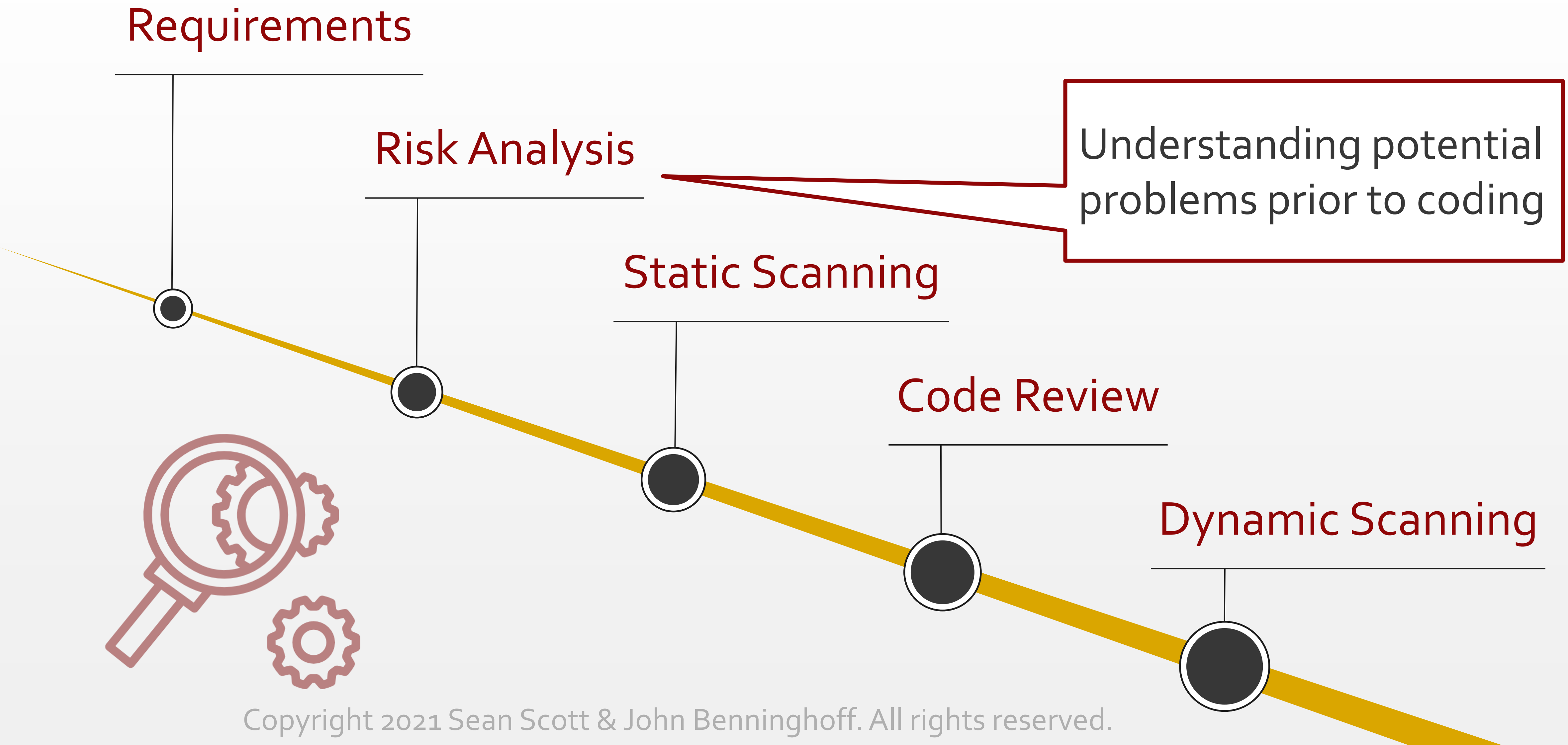
Static Scanning

Code Review

Dynamic Scanning

Training and coaching on OWASP Proactive Controls and Risks

# TREATMENTS



Requirements

Risk Analysis

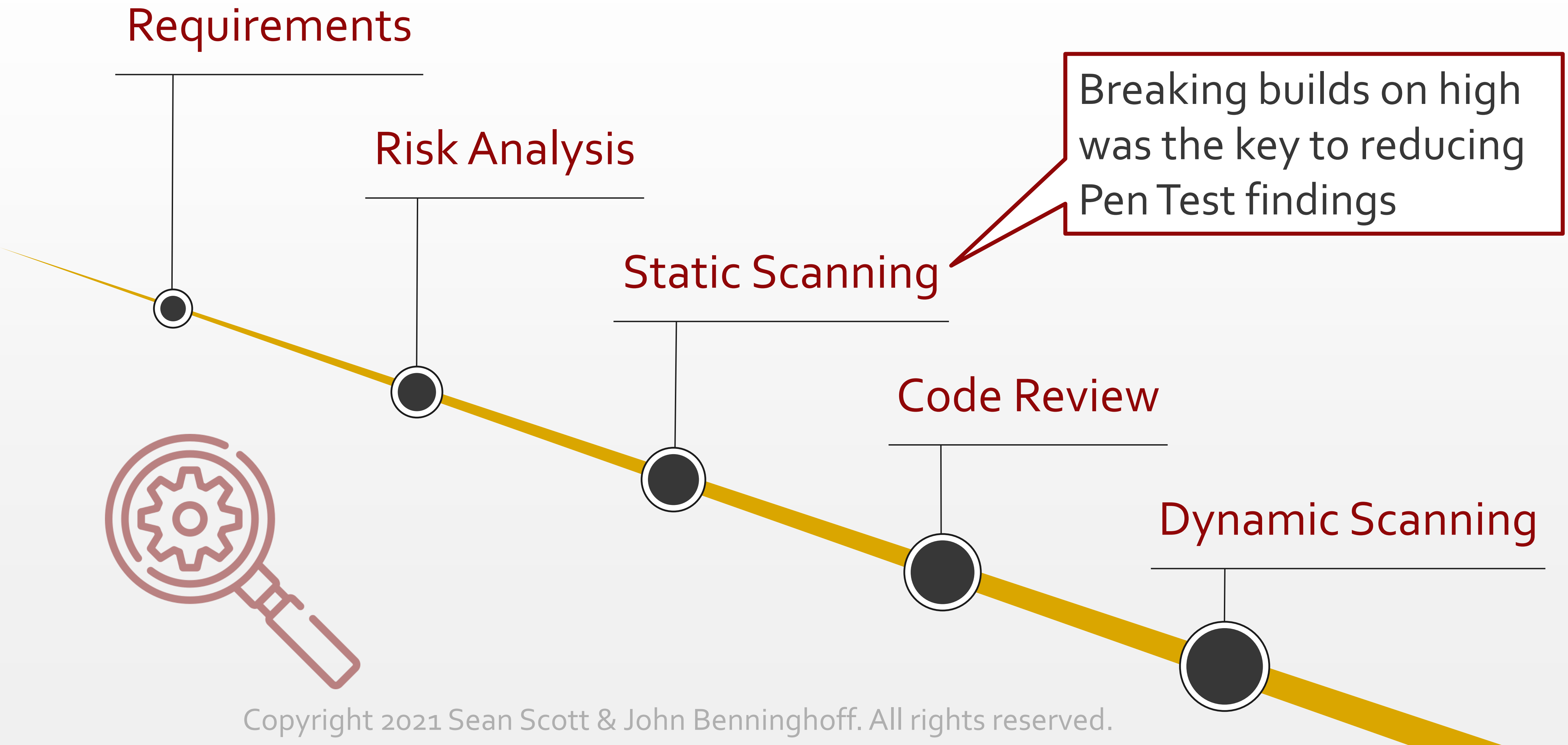
Static Scanning

Code Review

Dynamic Scanning

Understanding potential problems prior to coding

# TREATMENTS



Requirements

Risk Analysis

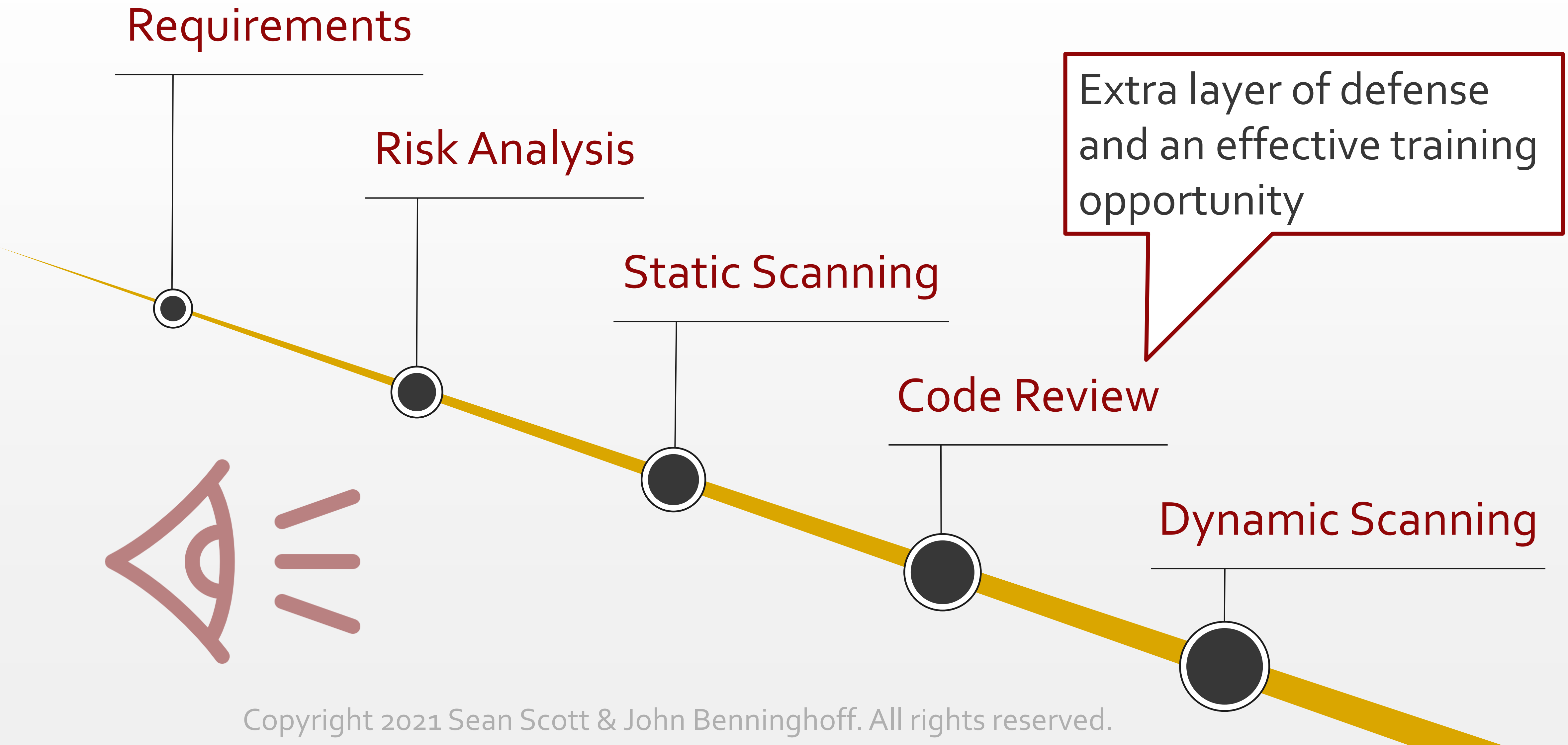
Static Scanning

Code Review

Dynamic Scanning

Breaking builds on high was the key to reducing Pen Test findings

# TREATMENTS



Requirements

Risk Analysis

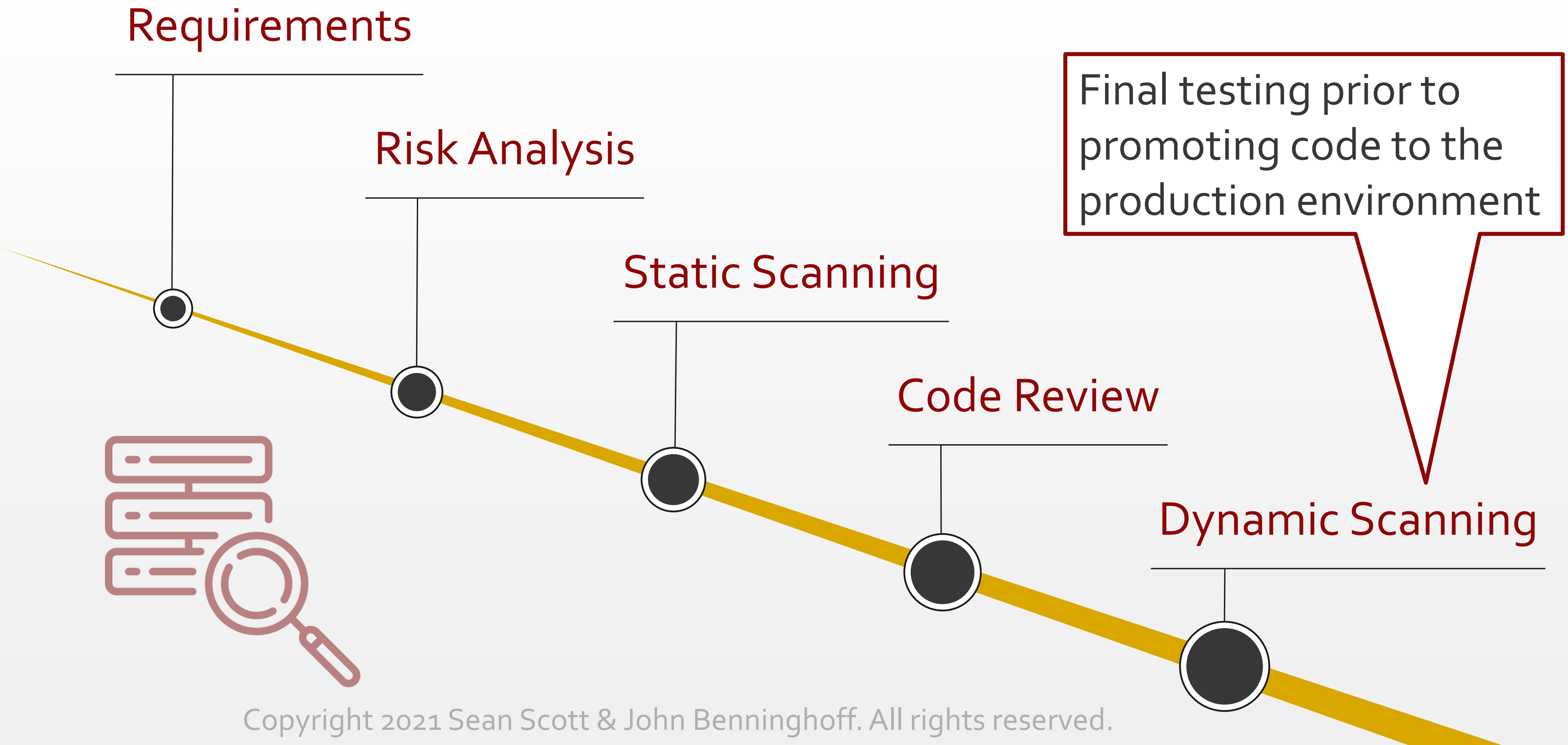
Static Scanning

Code Review

Dynamic Scanning

Extra layer of defense and an effective training opportunity

# TREATMENTS



Requirements

Risk Analysis

Static Scanning

Code Review

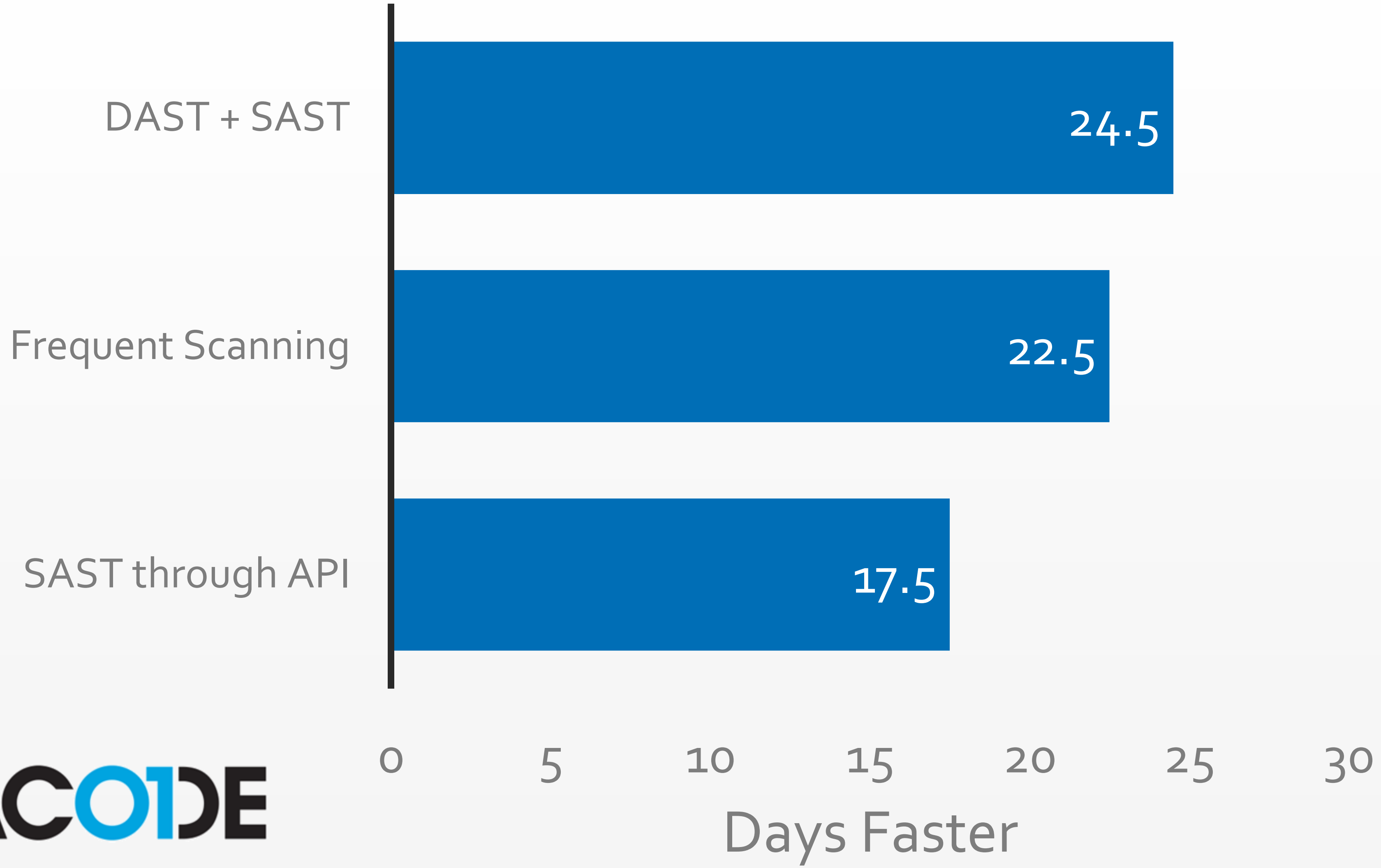
Dynamic Scanning

Final testing prior to promoting code to the production environment

VERACODE

# State of Software Security v11

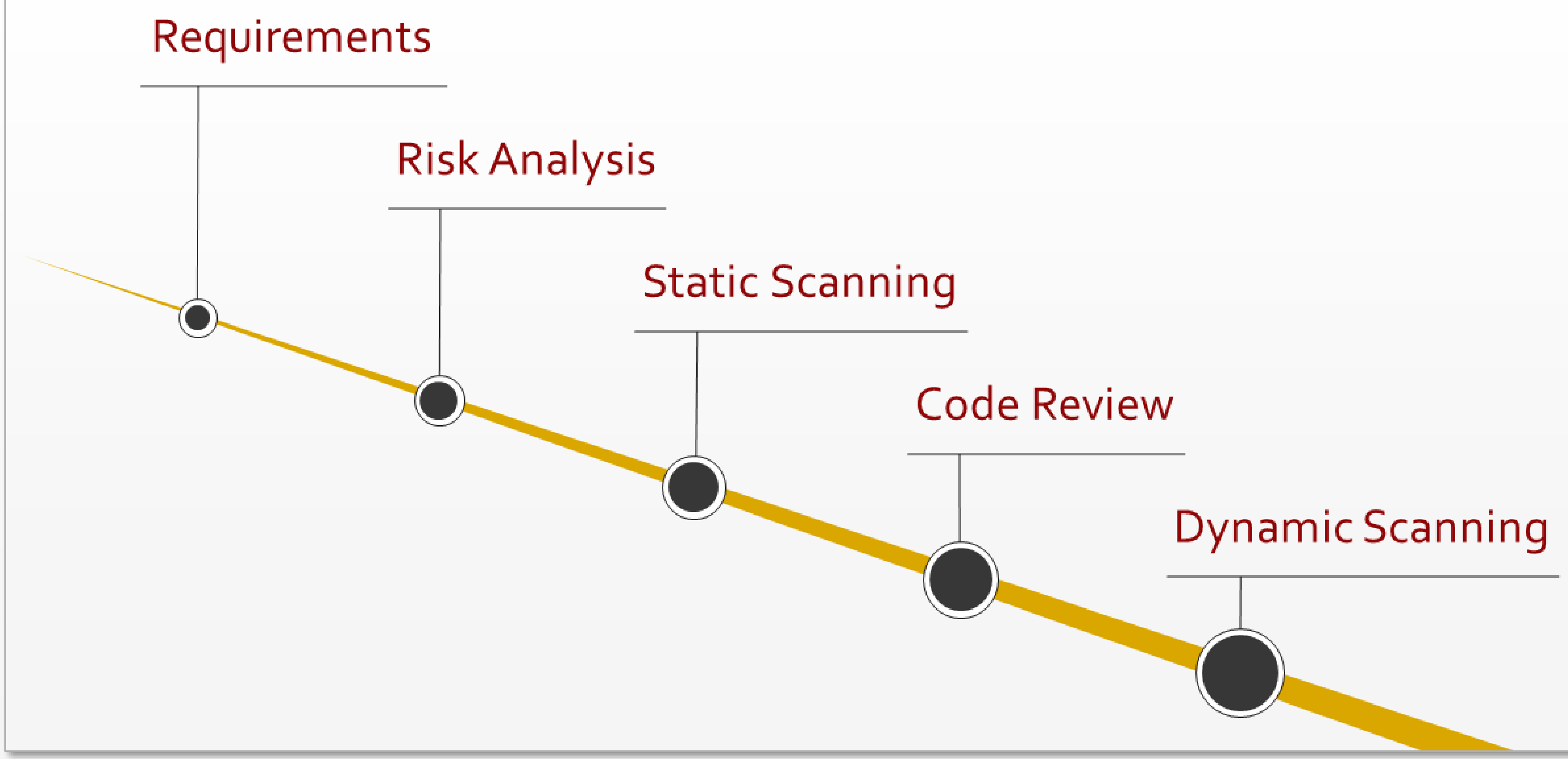
# STATE OF SECURITY REPORT



VERACODE

# SUMMARY

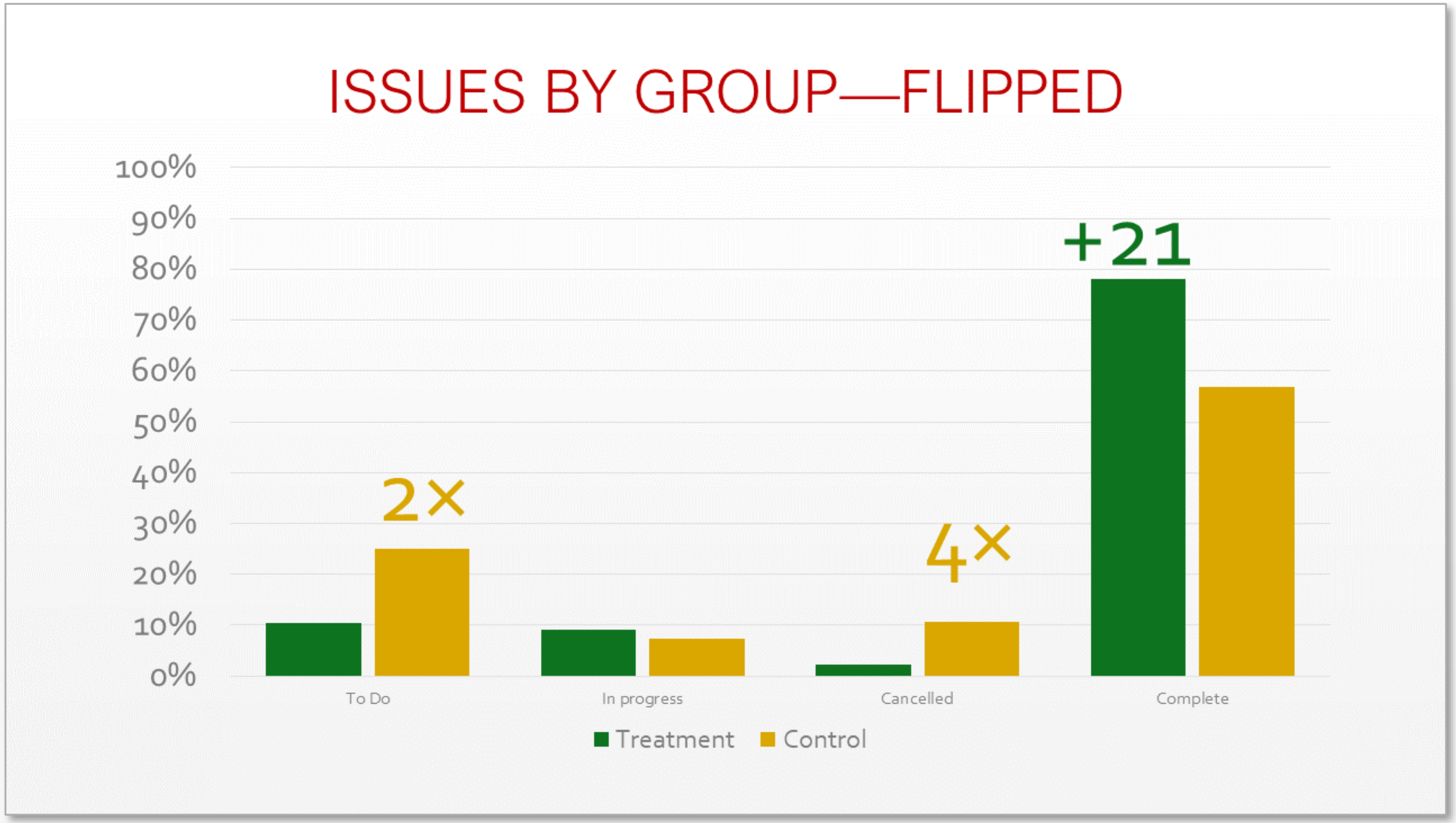
## TREATMENTS



# SUMMARY

Teams which receive coaching and training on application security topics…

Are twice as likely to be working on a security ticket and cancel tickets ¼ as often,

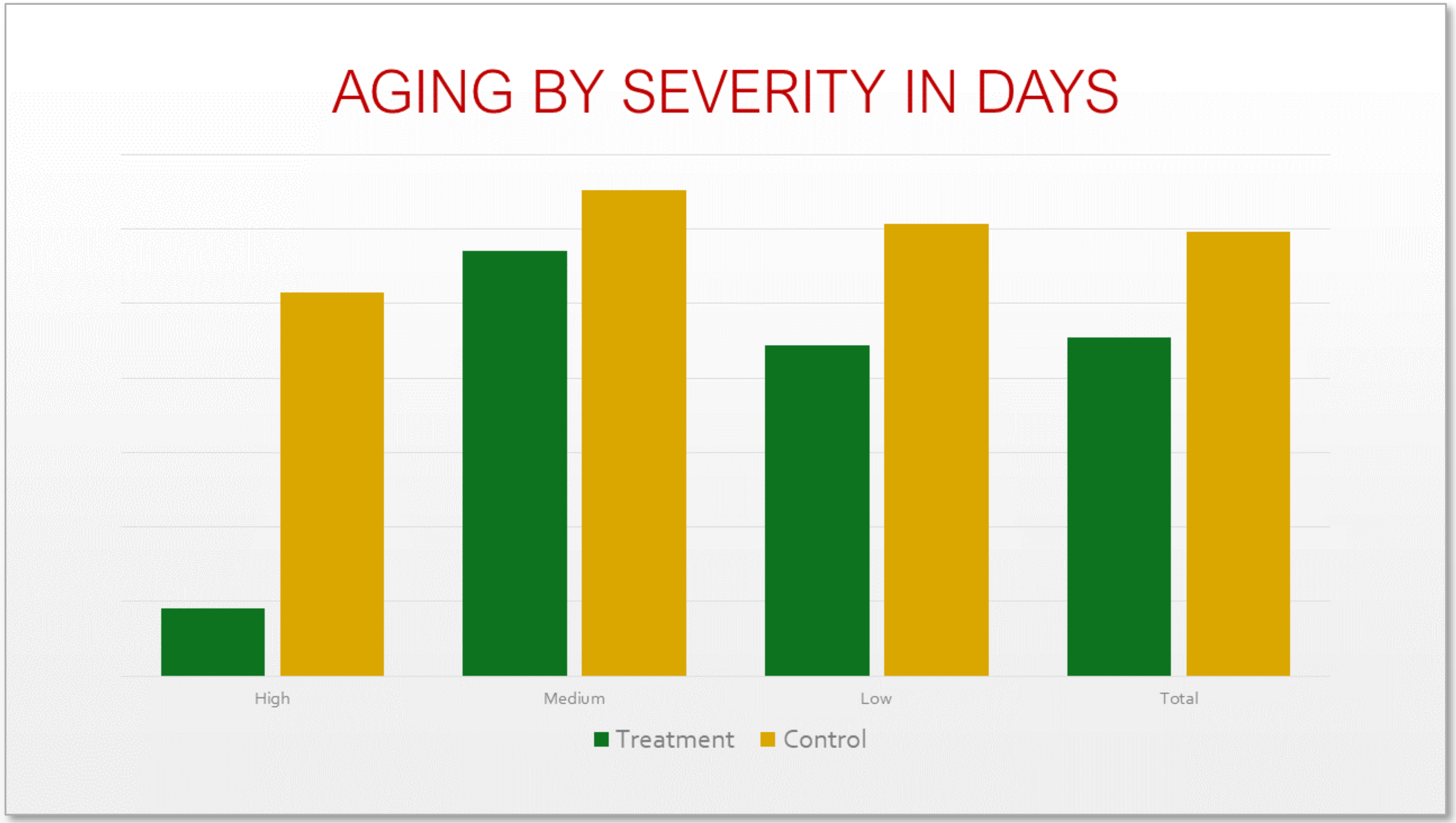


# SUMMARY

Teams which receive coaching and training on application security topics…

Are twice as likely to be working on a security ticket and cancel tickets ¼ as often,

Fix security tickets much more quickly, and,



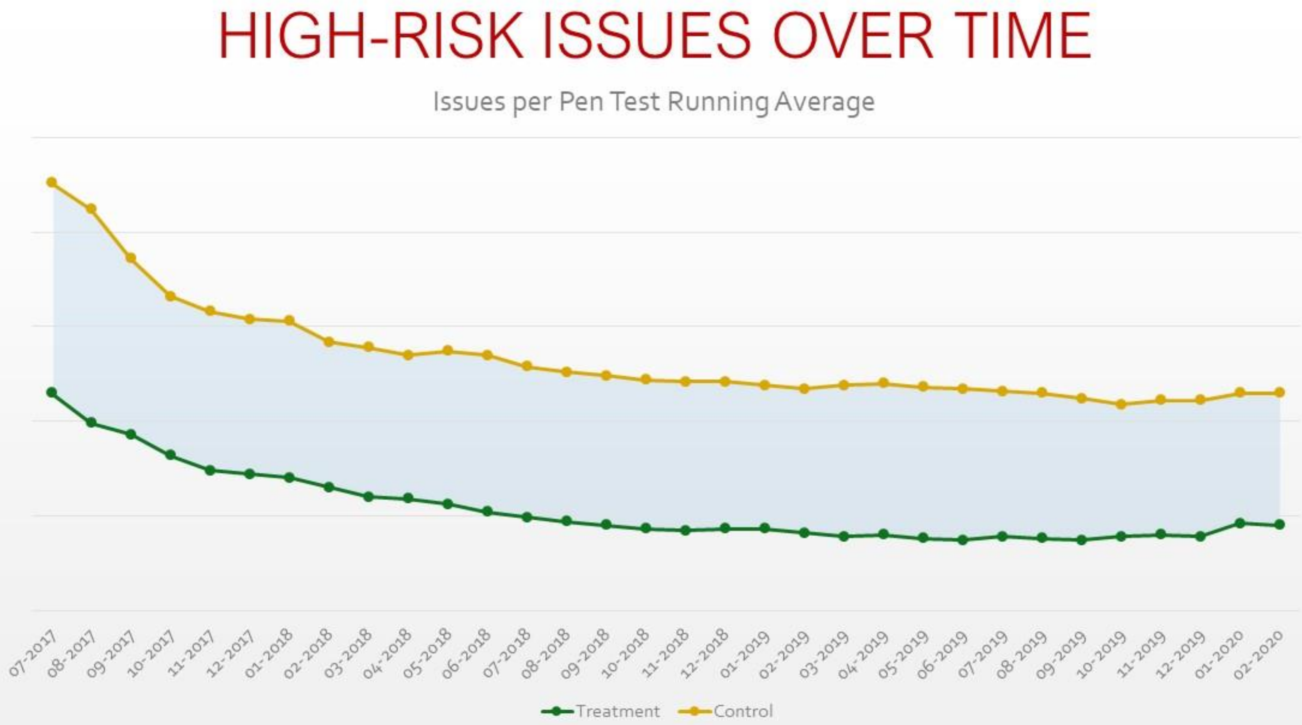
# SUMMARY

Teams which receive coaching and training on application security topics…

Are twice as likely to be working on a security ticket and cancel tickets ¼ as often,

Fix security tickets much more quickly, and,

Have fewer security bugs found during pen testing.



# STATISTICS

## High-impact vs. Control

T-test significance level: **0.000212**,

Control group (M=.91, SD=.57)

Treatment group (M=.37, SD=.65, t(31)=3.174, p<.05).

## High- + Medium-impact vs. Control

T-test significance level: **0.010504**

Control group (M=2.06, SD=1.07)

Treatment group (M=1.23, SD=1.39, t(31)=5.01, p<.05).

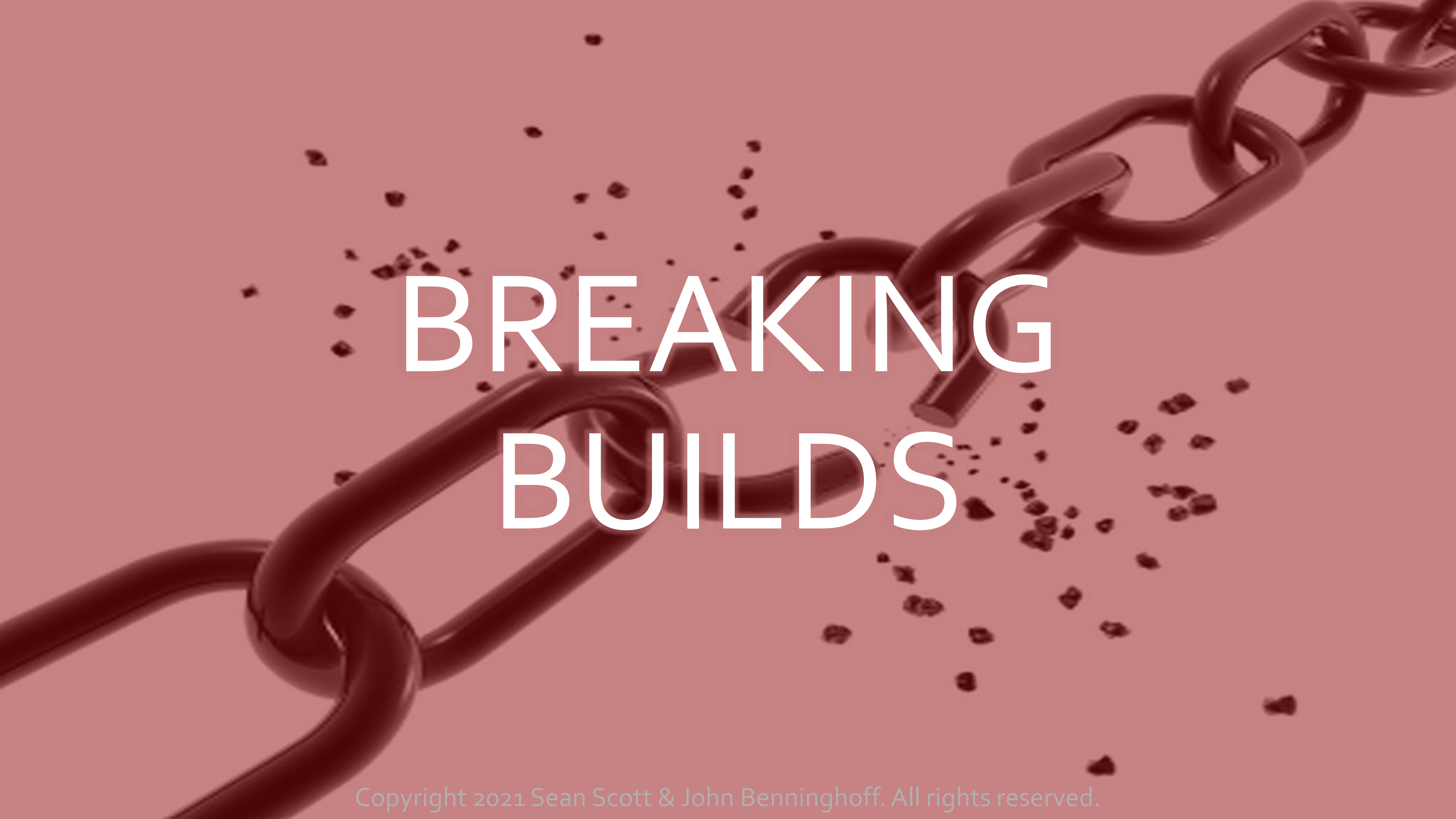
# CONCLUSIONS & RECOMMENDATIONS

OWASP

Champions

Opt-in

Break builds

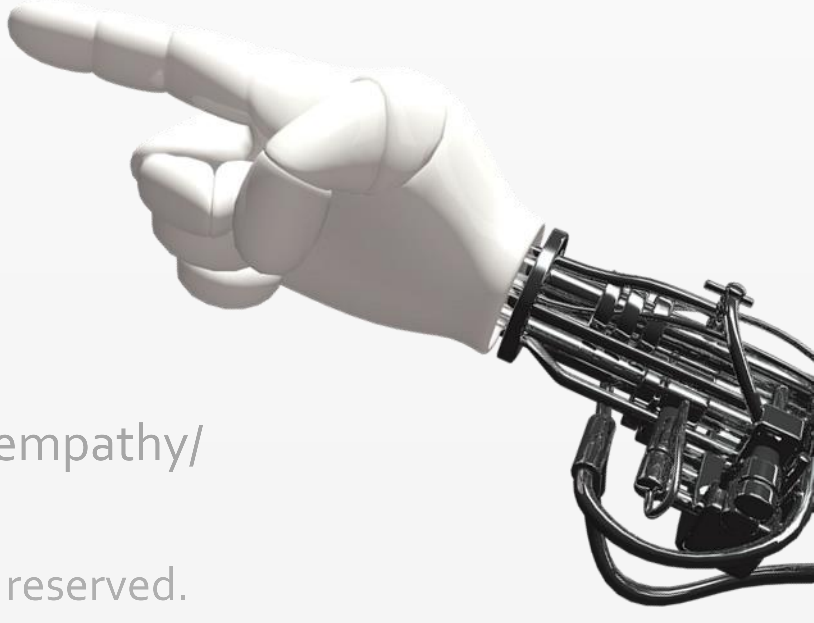


# BREAKING BUILDS

# ROBOT PEDANTRY, HUMAN EMPATHY

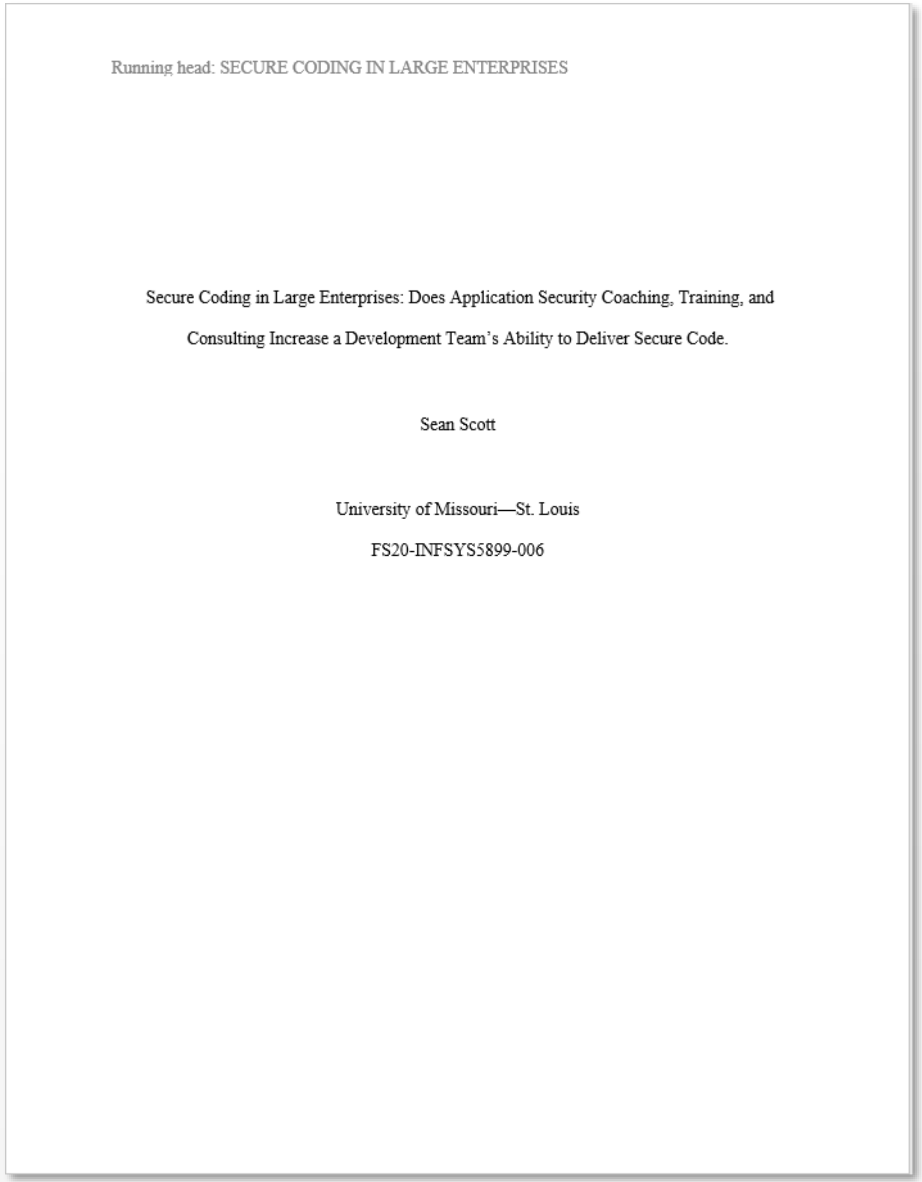
"Seek on your project to automate and codify as much as you possibly can while remembering that the human touch is still necessary"

—Mike McQuaid



https://mikemcquaid.com/2018/06/05/robot-pedantry-human-empathy/

# ACADEMIC PAPER



Running head: SECURE CODING IN LARGE ENTERPRISES

Secure Coding in Large Enterprises: Does Application Security Coaching, Training, and Consulting Increase a Development Team's Ability to Deliver Secure Code.

Sean Scott

University of Missouri—St. Louis

FS20-INFSYS5899-006

To be submitted for peer review and publishing in fourth quarter of 2021

seantscott.com

# WHAT SAFETY SCIENCE TAUGHT ME ABOUT INFORMATION RISK

## ASSUMPTIONS BACKED BY ACCEPTED THEORY

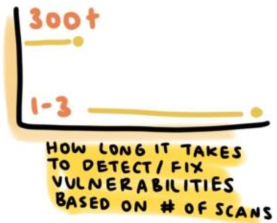
1 ORGANIZATIONS ARE SOCIOTECHNICAL SYSTEM

2 ALL FAILURES ARE SYSTEMS FAILURE

FROM SAFETY TO WORKING SAFELY

1 RESILIENCE IMPROVES THROUGH PERFORMANCE

2 SECURITY PERFORMANCE IS CORRELATED WITH GENERAL PERFORMANCE

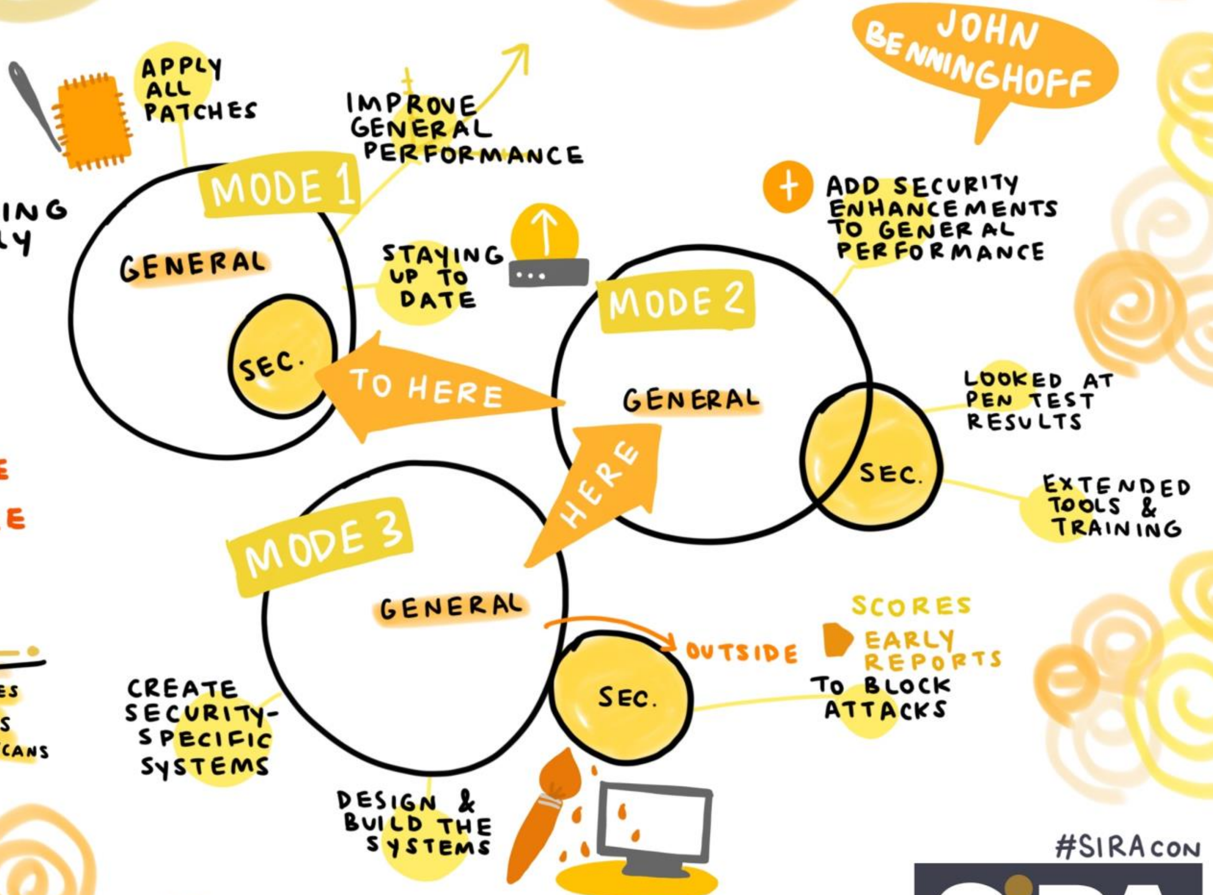


## ARGUMENTS FOR A NEW MODEL

3 THERE ARE 3 MODES OF SECURITY PERFORMANCE

GENERAL PERFORMANCE
SECURITY PERFORMANCE

JOHN BENNINGHOFF


APPLY ALL PATCHES
IMPROVE GENERAL PERFORMANCE
MODE 1
GENERAL
SEC.
STAYING UP TO DATE
TO HERE
+ ADD SECURITY ENHANCEMENTS TO GENERAL PERFORMANCE
MODE 2
GENERAL
SEC.
LOOKED AT PEN TEST RESULTS
EXTENDED TOOLS & TRAINING
HERE
MODE 3
GENERAL
SEC.
OUTSIDE
SCORES
EARLY REPORTS
TO BLOCK ATTACKS
CREATE SECURITY-SPECIFIC SYSTEMS
DESIGN & BUILD THE SYSTEMS

@mindseyeccf MIND'S EYE CREATIVE

#SIRACON

datto

SIRA DATA > DOGMA

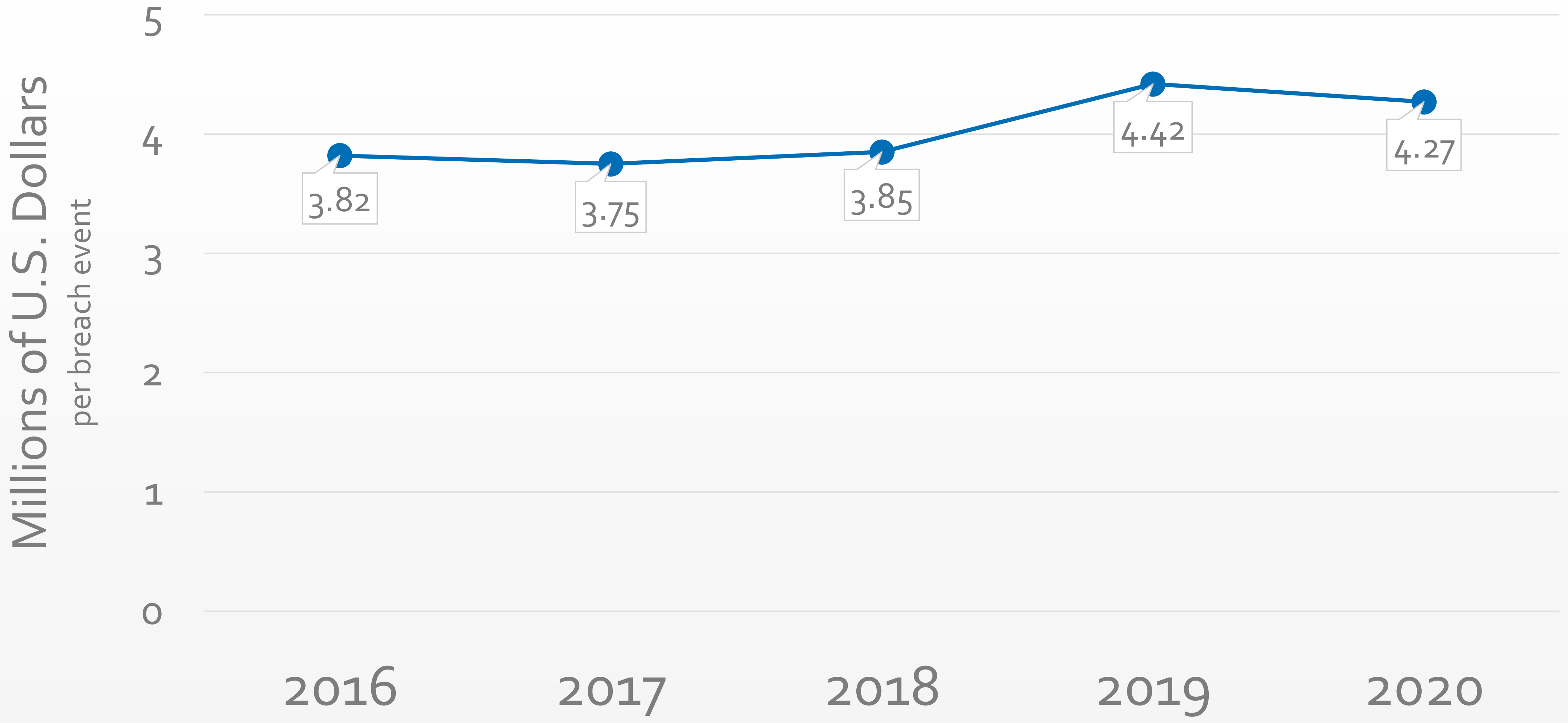
linkedin.com/in/seantscott
conference@seantscott.com
seantscott.com

linkedin.com/in/jbenninghoff
twitter: @jbenninghoff
information-safety.org

# APPENDIX

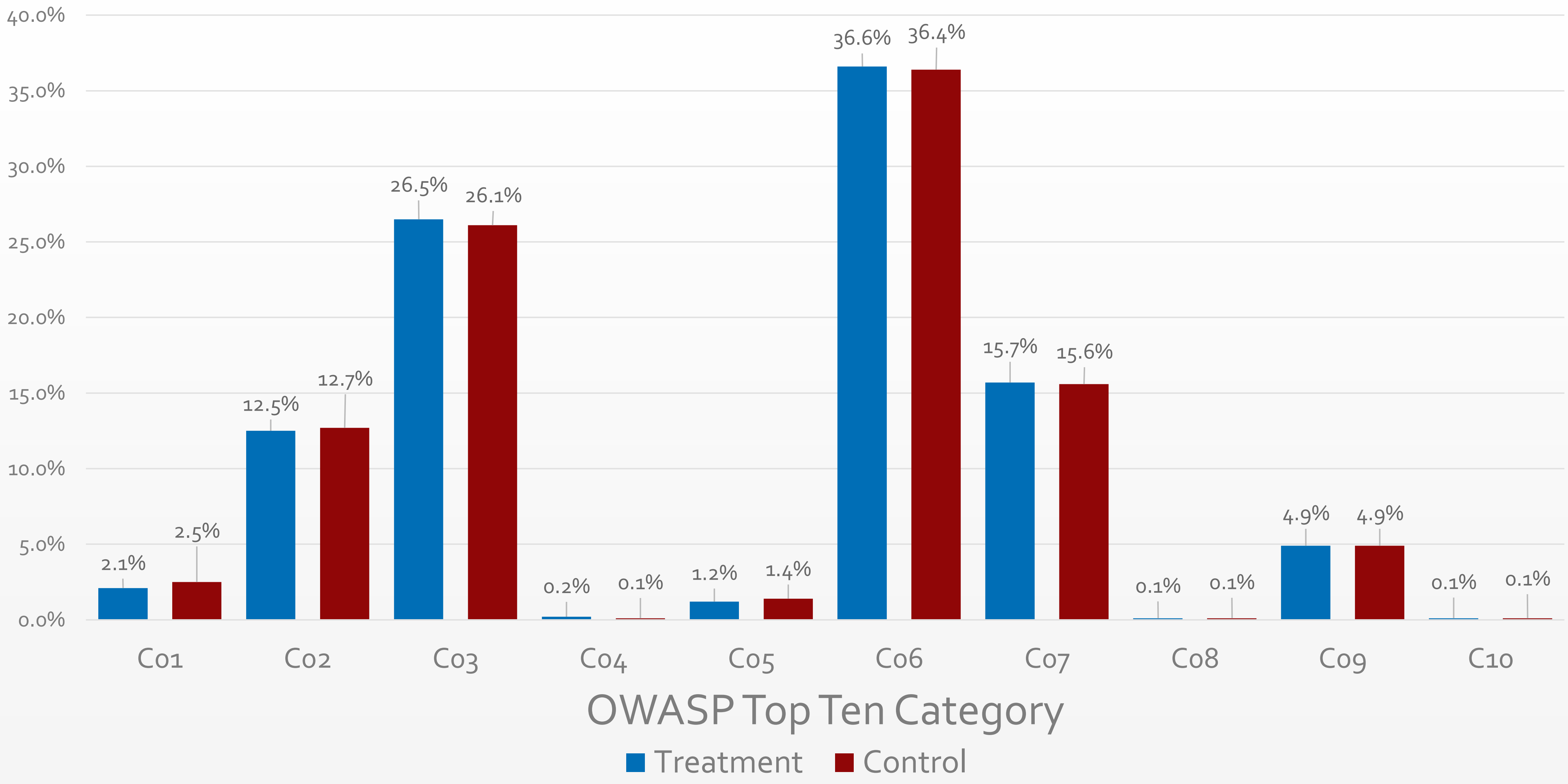
More information for the curious…

# COST OF DATA BREACHES BY MALICIOUS ATTACK

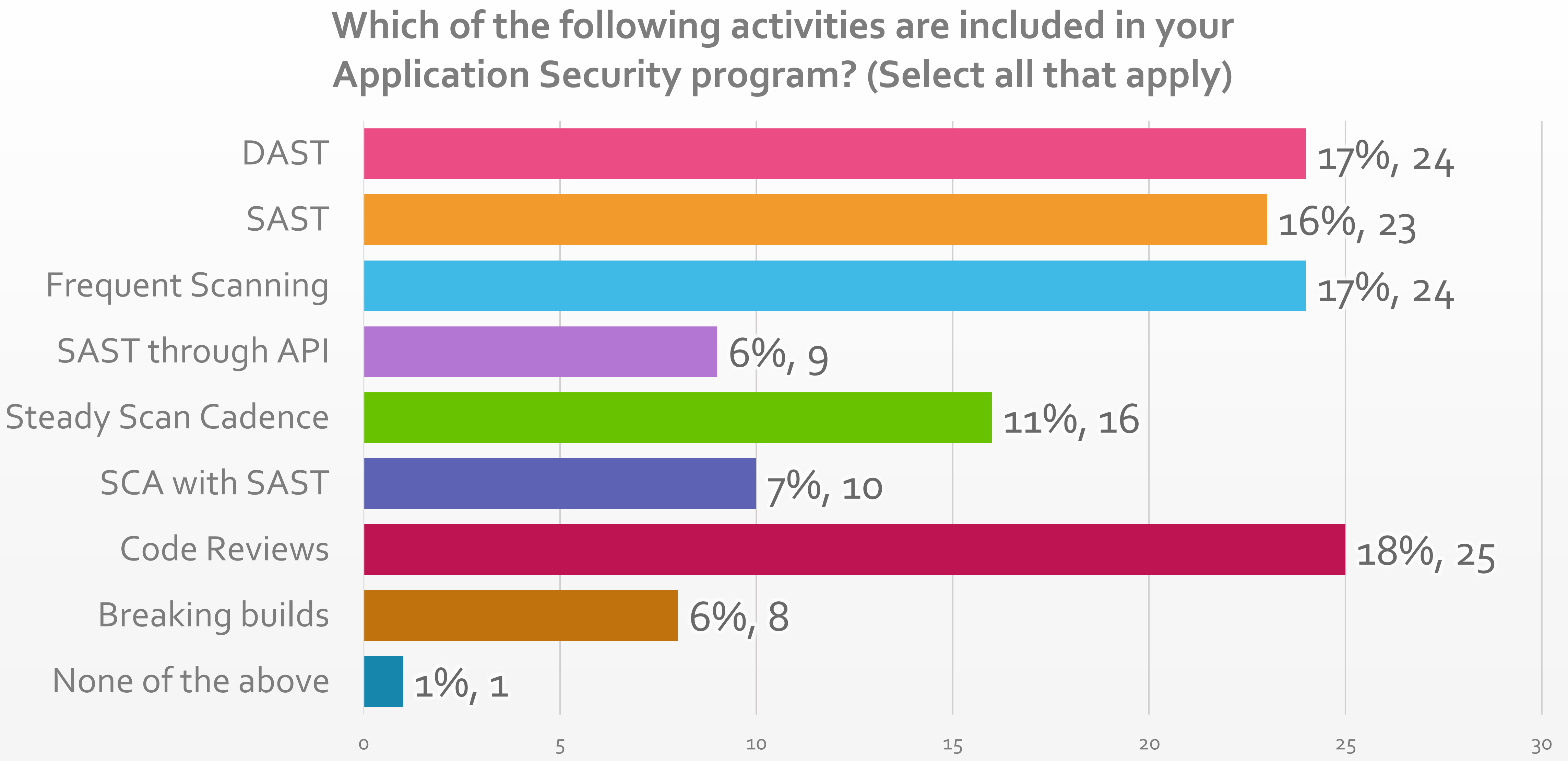


Cost of Data Breach Report 2020, IBM

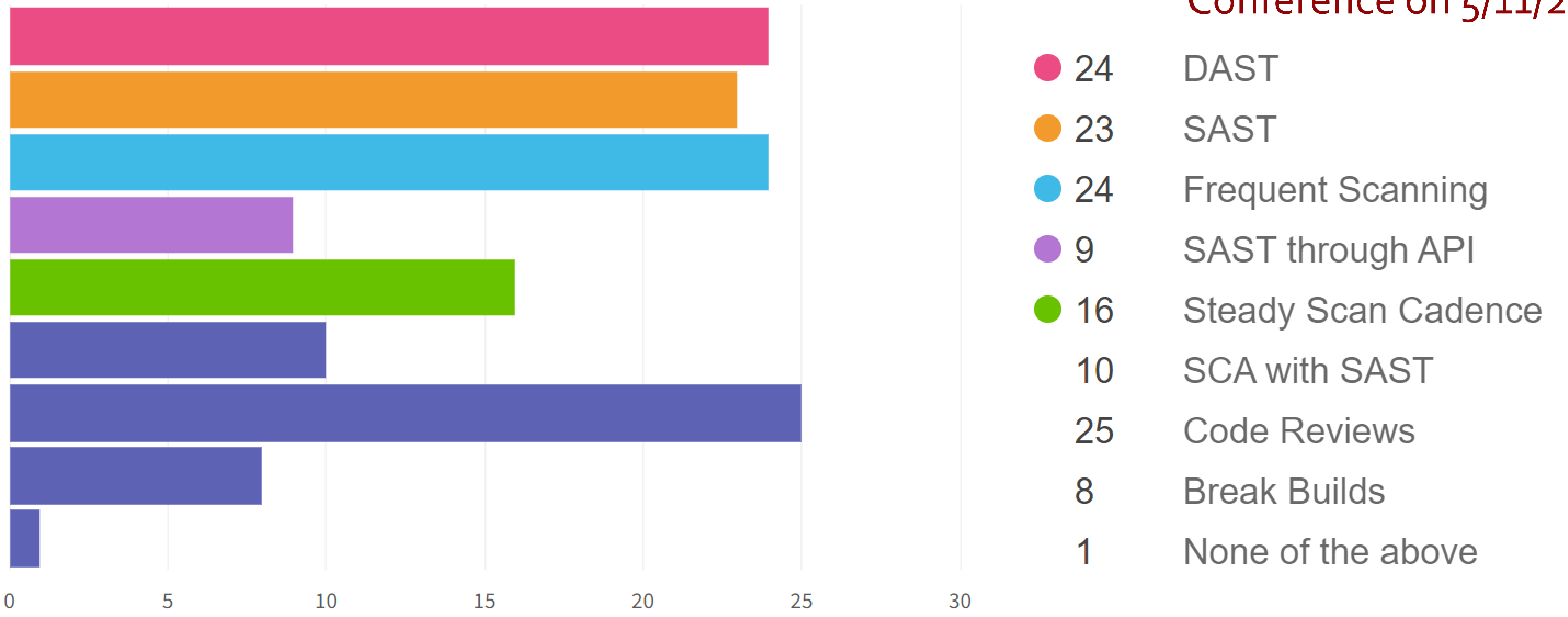
# OWASP CATEGORIZATION BY GROUP



# Secure360 5/11/2021



# Which of the following activities are included in your Application Security program? (Select all that apply)



(Data from the Secure360 Conference on 5/11/2021)