pmsymposium.umd.edu

NEXT SESSION

HOW TO SUCCESSFULLY MANAGE THE PIVOT FROM DEVOPS TO DEVSECOPS

Andrew Boyle & Stephanie Jenkins

This session will be recorded.

University of Maryland
Project Management
Symposium

PROJECT MANAGEMENT
CENTER FOR EXCELLENCE
A.J. CLARK SCHOOL OF ENGINEERING
Civil & Environmental Engineering Department

How to Successfully Manage the Pivot from DevOps to DevSecOps

Andrew Boyle & Stephanie Jenkins

2022 Project Management Symposium

"We cannot ensure success, but we can deserve it" – John Adams

Agenda

15 mins

- Overview
- What is DevOps and DevSecOps & Is Injecting Sec Worth It?
- 6 Step Process to Pivot from DevOps to DevSecOps
- How to Diagnose Unbalanced 'Sec'

15 mins

- How the Project Management Construct Aligns to DevSecOps

10 mins

- Case Study
- Summary

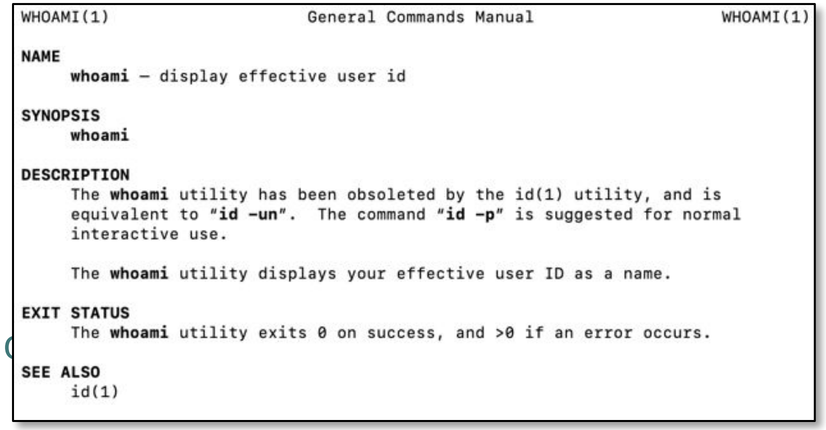
Forever!

- We All Fight 495 Traffic
- Q&A

"Experience is the name everyone gives to their mistakes"
– Oscar Wilde

Who Am I

(not the Unix command 'whoami'!)



```
WHOAMI(1)                  General Commands Manual                  WHOAMI(1)

NAME
     whoami – display effective user id

SYNOPSIS
     whoami

DESCRIPTION
     The whoami utility has been obsoleted by the id(1) utility, and is
     equivalent to "id -un".  The command "id -p" is suggested for normal
     interactive use.

     The whoami utility displays your effective user ID as a name.

EXIT STATUS
     The whoami utility exits 0 on success, and >0 if an error occurs.

SEE ALSO
     id(1)
```

Andrew 'Andy' Boyle

Distinguished Digital & Cybersecurity Technol

Booz Allen Hamilton

[AWS-CCP, AWS-SAA, CEH, CISSP, FinOps, NN/g MUXC, PMI-ACP, PMP, PRINCE2, SAFe SPC]

- 30+ years digital and cybersecurity
- Government and Fortune 100 clients
- Advocate adoption and use of standards & specifications

✉ Boyle_Andrew@bah.com

in https://www.linkedin.com/in/andrew-boyle-b74299/

"When you change the way you look at things, the things you look at change" - Max Planck

Who Am I

Stephanie Jenkins

Digital Technologist & Program Manager
Booz Allen Hamilton Principal

- 28+ years of experience supporting the Intelligence Community, Civilian Services, and Department of Defense and is a technical diversity role model across numerous geographies, including DC Metro Area and Charleston, SC.
- Technical leader with deep experience in strategic planning and project planning and control, coupled with extensive expertise in Agile-based projects, to include intelligence information systems analysis, design, and development; and DevSecOps and cloud-based Enterprise systems.
- ICAgile Certified Professional Foundation of DevOps (ICP-FDO), Certified Scaled Agile Framework (SAFe) Agilist (SA)

✉ Jenkins_Stephanie@bah.com

Quiz!

QUESTION: According to the 2022 Verizon Data Breach Investigation Report, how many cybersecurity attacks took place in 2021 against APIs?

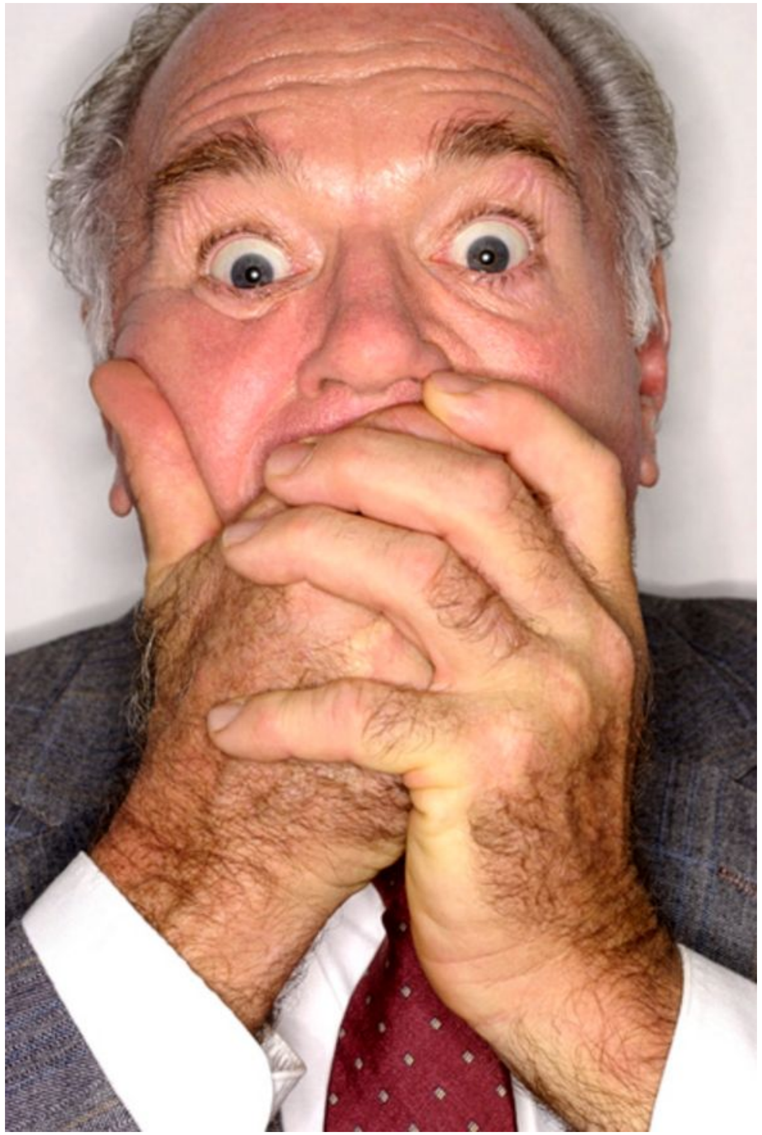
A) 1M

B) 500M

C) 7B

D) 50B

ANSWER: *C) 7 Billion!*



Overview

"The trouble with the world is that the stupid are cocksure and the intelligent are full of doubt" – Bertrand Russell

- PMBOK refined and updated to fully embrace Agile
- DevOps has led since the 2010s
- Security wasn't part of DevOps… ugh!
- DevSecOps emerged and has rapidly taken off … but not without many challenges
- Best practices & lessons learned support the DevOps to DevSecOps pivot
- PM processes can easily be tailored to support DevSecOps … but there are some landmines that you must avoid

A project without security is not a viable project – as PM Professionals we must embrace processes that improve the cybersecurity posture of all projects

“Difficulties are just things to overcome, after all”
– Sir Ernest Shackleton

Scope of Cybersecurity

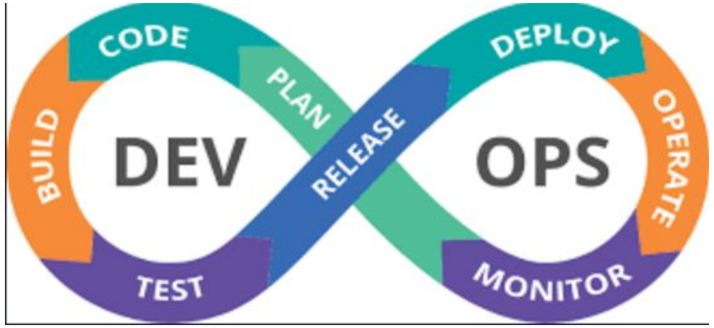
The utilization of cybersecurity is no longer a ‘*nice to have*’ – it is now a “*must have*” requirement for any trusted, modern organization of any size

"Formal education will make you a living; self-education will make you a fortune" – Jim Rohn

DevOps vs DevSecOps

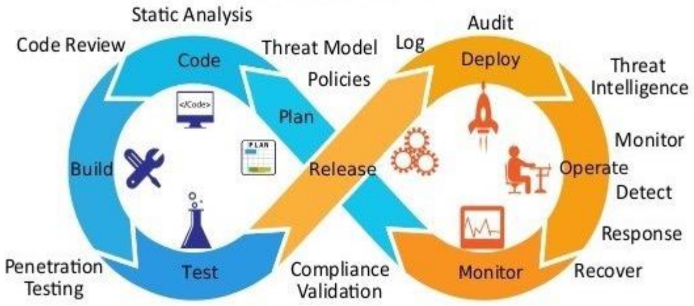
DevOps

"DevOps is the combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity" – Amazon Web Services



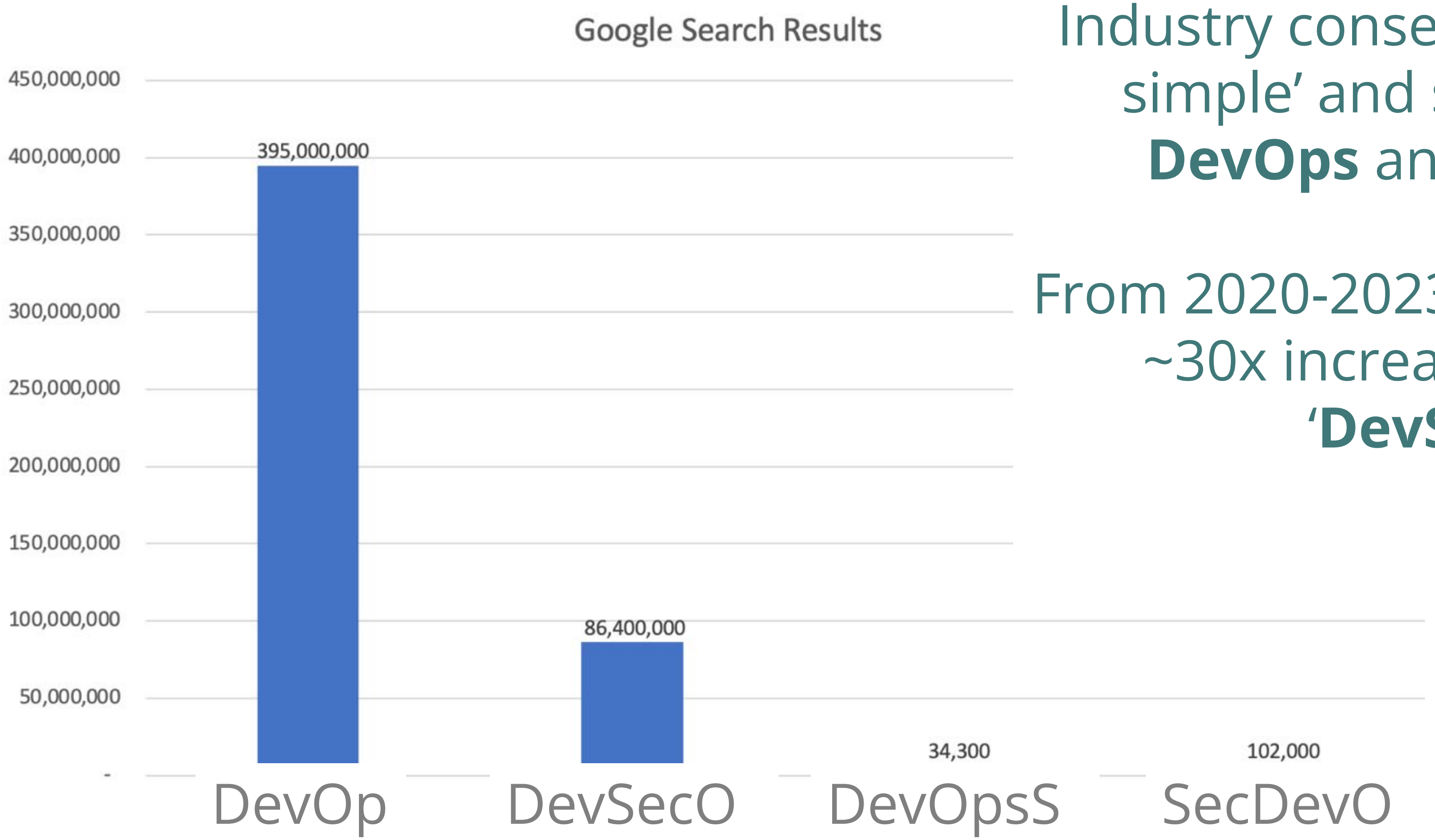
DevSecOps

"DevSecOps means thinking about app and infrastructure security from the start. It also means automating security gates to keep the DevOps workflow from slowing down" – Red Hat



"The universal aptitude to ineptitude makes any human accomplishment an incredible miracle" – Colonel John Paul Stapp

Wait, What Do We Call it?



Industry consensus is to 'keep it simple' and standardize on **DevOps** and **DevSecOps**

From 2020-2023 there has been a ~30x increase in usage of '**DevSecOps**'

"We have to find a way of making the important measurable, instead of making the measurable important" – Robert McNamara

Is Injecting Sec into DevOps Worth It?

- Increases software lifecycle predictability
- Automating security review processes for minimizes time-to-deploy
- Reduced downtime provides a softer cushion for unforeseen events
- Secure automation reduces mistakes and eliminates human error
- Pre-production code security tools allow vulnerabilities/bugs to be caught earlier

Quiz!

QUESTION: How much more popular is the usage of Log4j version 2.x (started in 2015) than Log4j v1.x (2001-2015)?

A) Log4j v2.x is used equally as v1.x

B) Log4j v2.x is used 2x as much as v1.x

C) Log4j v2.x is used 10x as much as v1.x

D) Log4j v2.x is used 50x as much as v1.x

ANSWER: ***Trick Question – None of the Above! Despite Log4j v1.x being 7+ years past End-of-Life (EOL), it currently has slightly more usage than v2.x***

Quiz!

QUESTION: What % of Log4j downloads from Maven Central Java application repository are old and vulnerable versions of Log4j?

A) 0%

B) 1%

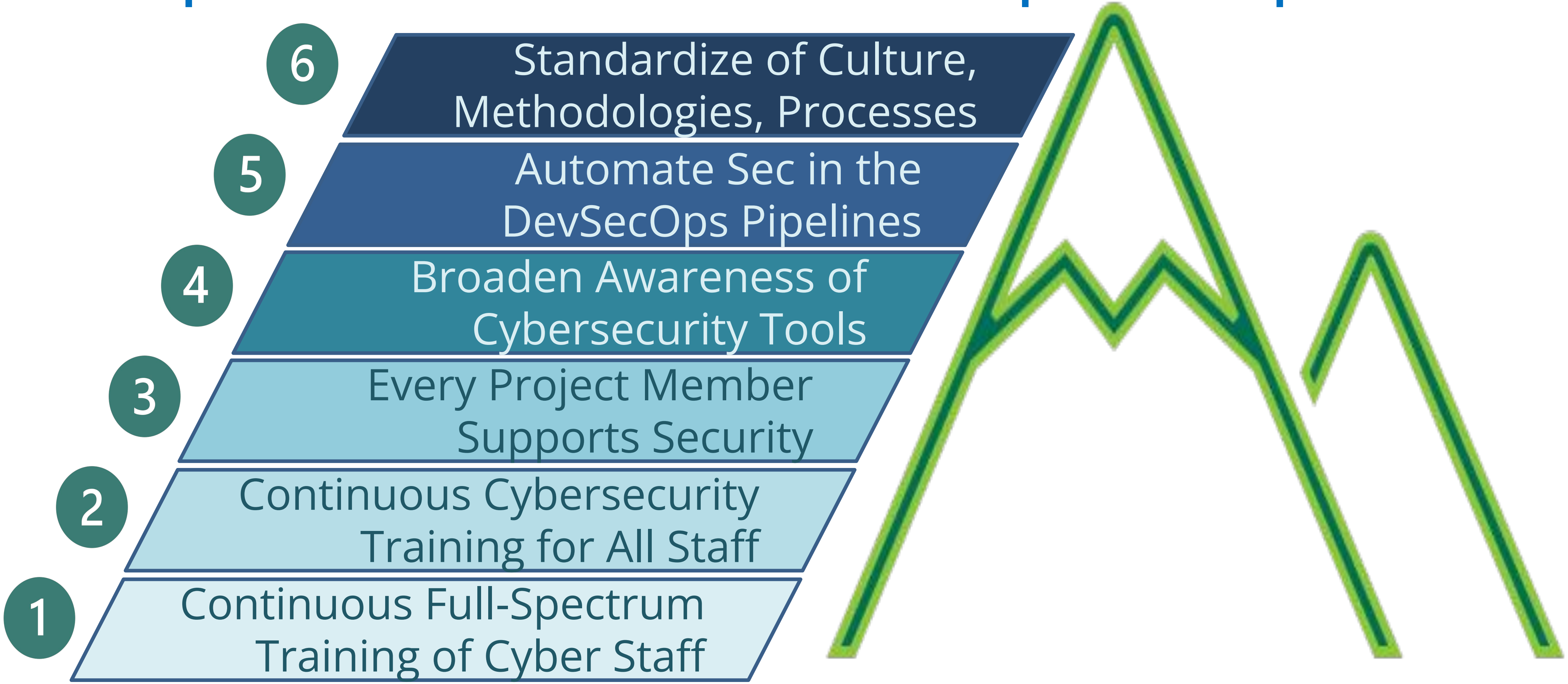
C) 2%

D) 30%

ANSWER: *D) Approximately 30% of the versions of Log4j downloaded from MJC repository are vulnerable versions of Log4j.*

"Vision without action is a daydream. Action without vision is a nightmare"
– Japanese proverb

6 Step Process for DevSecOps Adoption



6 Standardize of Culture, Methodologies, Processes

5 Automate Sec in the DevSecOps Pipelines

4 Broaden Awareness of Cybersecurity Tools

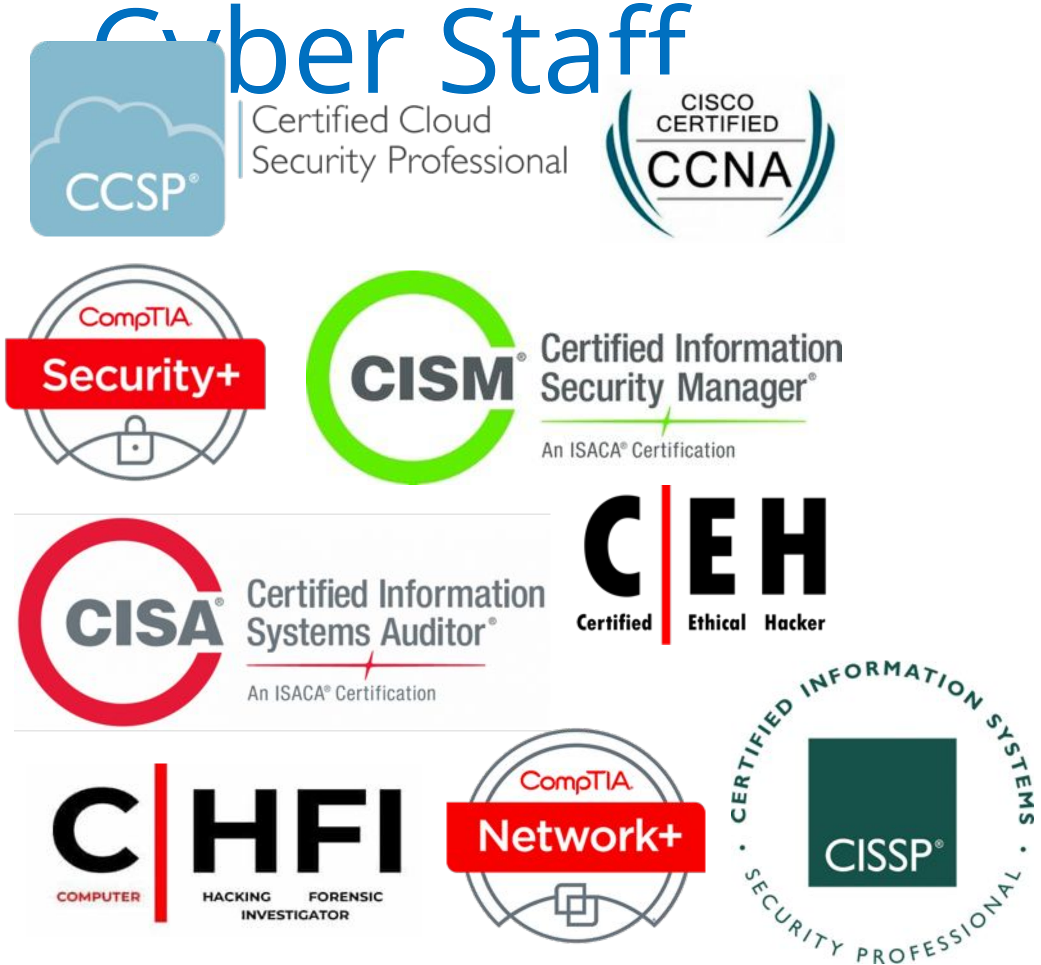
3 Every Project Member Supports Security

2 Continuous Cybersecurity Training for All Staff

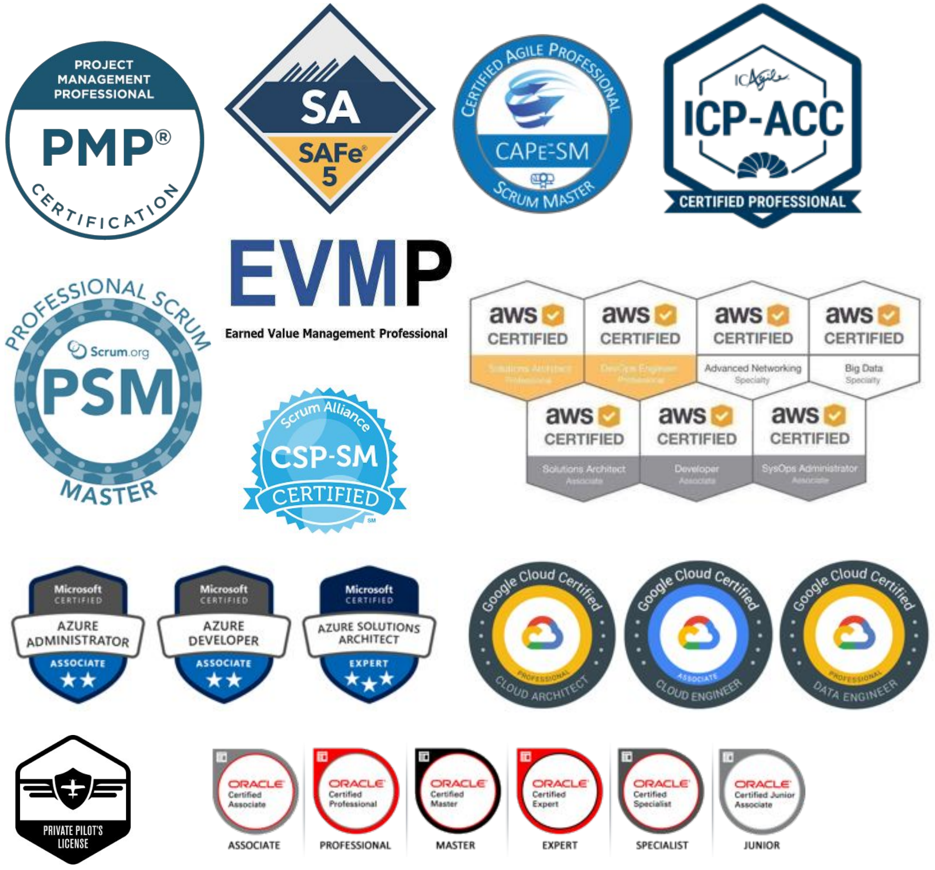
1 Continuous Full-Spectrum Training of Cyber Staff

'Live as if you were to die tomorrow. Learn as if you were to live forever" – Mahatma Gandhi

1 Continuous Full-Spectrum Training of Cyber Staff


CCSP
Certified Cloud Security Professional
CISCO CERTIFIED CCNA
CompTIA Security+
CISM Certified Information Security Manager
An ISACA Certification
CISA Certified Information Systems Auditor
An ISACA Certification
C|EH Certified Ethical Hacker
C|HFI COMPUTER HACKING FORENSIC INVESTIGATOR
CompTIA Network+
CISSP
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

+


PROJECT MANAGEMENT PROFESSIONAL PMP CERTIFICATION
SA SAFe 5
CERTIFIED AGILE PROFESSIONAL CAPE-SM SCRUM MASTER
ICAgile ICP-ACC CERTIFIED PROFESSIONAL
PROFESSIONAL SCRUM MASTER Scrum.org PSM
EVMP Earned Value Management Professional
Scrum Alliance CSP-SM CERTIFIED
aws CERTIFIED Solutions Architect Professional
aws CERTIFIED DevOps Engineer Professional
aws CERTIFIED Advanced Networking Specialty
aws CERTIFIED Big Data Specialty
aws CERTIFIED Solutions Architect Associate
aws CERTIFIED Developer Associate
aws CERTIFIED SysOps Administrator Associate
Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE
Microsoft CERTIFIED AZURE DEVELOPER ASSOCIATE
Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT
Google Cloud Certified Professional CLOUD ARCHITECT
Google Cloud Certified Associate CLOUD ENGINEER
Google Cloud Certified Professional DATA ENGINEER
PRIVATE PILOT'S LICENSE
ORACLE Certified Associate ASSOCIATE
ORACLE Certified Professional PROFESSIONAL
ORACLE Certified Master MASTER
ORACLE Certified Expert EXPERT
ORACLE Certified Specialist SPECIALIST
ORACLE Certified Junior Associate JUNIOR

"Those who have knowledge don't predict. Those who predict don't have knowledge" – Lao Tzu

2 Continuous Cybersecurity Training for All Staff

Encouraged Reading

Active Certifications Environment

Engaged Learning

Support of OTJ Engagement

"You don't lead by hitting people over the head – that's assault, not leadership" – Dwight D. Eisenhower

3 Every Project Member CAREs About Security

C COMPETENT

A AVAILABLE

R RESPONSIBLE

E EMPOWERED

Projects/organizations need a similar cybersecurity message to all staff

"Tell me and I'll forget. Show me and I may remember. Involve me and I will learn" – Benjamin Franklin

4 Broaden Awareness of Cybersecurity Tools

Share!
Build trust. Build Awareness. Make non-cyber staff interested & informed!

Big Picture
What role do each of the tools play? Why are they needed?

Configurations
Share not only what the tool can do, but what it is configured to do

Outputs and Impacts
How are the outputs used? What are the thresholds? Why thresholds?

Limited Distro
Some tool outputs (vulnerabilities) may be too sensitive to share

Be like Missouri!

'Show Me'

All organization and project staff must have at least some awareness off, at the very least, the general capabilities of the tools used in cyber security….

In many cases cyber security staff treat the tools as 'secrets in their ivory tower'…

Not sharing erodes the necessary trust across Dev, Sec, and Ops

sonarqube

MICRO FOCUS Fortify

VERACODE

coverity

"it is not from the benevolence of the butcher, the newer, or the baker that we expect our dinner, but from their regard to their own self interest" – Adam Smith

5 Automated Sec in the DevSecOps Pipeline

Google
50/day/product

Capital One
50/day/product

amazon
Every 11.7 seconds

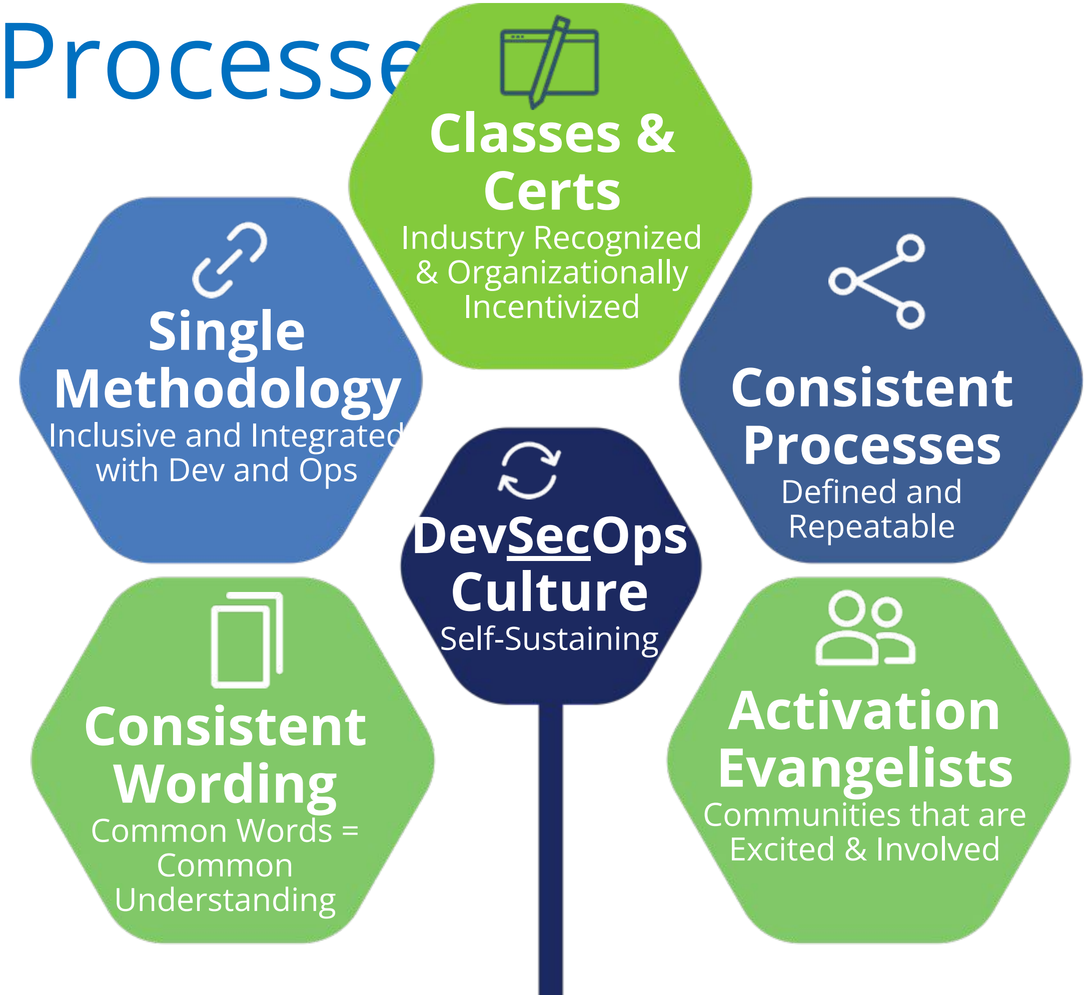
NETFLIX
100+ per day

f
100M LOC /day

Etsy
50/day

"The first step towards getting somewhere is to decide that you are not going to stay where you are" – J.P. Morgan

6 Standardize of Culture, Methodologies, Processe


Classes & Certs
Industry Recognized & Organizationally Incentivized
Single Methodology
Inclusive and Integrated with Dev and Ops
Consistent Processes
Defined and Repeatable
DevSecOps Culture
Self-Sustaining
Consistent Wording
Common Words = Common Understanding
Activation Evangelists
Communities that are Excited & Involved

- Always use 'DevSecOps' (stop using 'DevOps')'; drive this adoption across your organization
- Security should never be a bolt-on, and neither should 'Sec'; ensure Sec processes are comparable to the quality and quantity of the Dev and Ops (as well as fully integrated)
- Become an evangelist of DevSecOps - PMs need to lead the culture change that everyone needs to embrace cybersecurity
- Encourage staff to get involved in DevSecOps
- Instill a culture of equality across Dev, Sec, and Ops - DevSecOps is only as strong as the weakest link

“Life was simple before World War II. After that we had systems”
– Grace Hopper

How to Diagnose Unbalanced ‘Sec’

Do you identify any of these in your organization?

- Unequal culture
- Lack of mutual respect
- Not ‘at the table’ for project-wide decisions
- Unequal understandings of the fundamentals of Dev, Sec, and Ops across Dev, Sec, and Ops staff

Probably the Situation Today …

	Dev Staff	Sec Staff	Ops Staff
Knowledge of Dev	●	◔	◑
Knowledge of Sec	◔	●	◔
Knowledge of Ops	◑	◔	●

Objective State for the Future …

	Dev Staff	Sec Staff	Ops Staff
Knowledge of Dev	●	◕	◕
Knowledge of Sec	◕	●	◕
Knowledge of Ops	◕	◕	●

How the PM Construct Aligns to DevSecOps

How can Program Managers make DevSecOps programs effective?

Integrate automated testing into the pipeline

Integrate security testing into workflows

Automated deployment

Infrastructure as Code (IaC)

Continuous monitoring

Train engineers in Secure DevOps

www.aquasec.com

"Success is not final; failure is not fatal: it is the courage to continue that counts" – Winston Churchill

Case Study 1

PROJECT: On-going project had some cyber security issues (actual as well as potential) due to Dev and Ops not understanding Sec domain.

- **BEST PRACTICE**: Set-up a custom on-site CISSP class for Dev & Ops based around project schedule/demands and helped form study groups.
- **RESULT**: Not only did the 15 staff learn cyber security, but that knowledge rippled throughout the project.

“Never let success get to your head, and never let failure get to your heart” – Meredith Kessler

Case Study 2

PROJECT: Project failed to meet deadlines. Cybersecurity lead was the bottleneck as they practiced ‘risk avoidance’; prior cybersecurity lead fired after being held at-fault. Coordinated cross-functional meetings to reset risk expectations.

- **LESSON LEARNED**: Dev, Sec, and Ops must not only appreciate the other domains and recognize the different risk perceptions.
- **RESULT**: Executive perceptions shifted to cybersecurity being a ‘when not if’ situation. Increased cybersecurity resources and clearly defined risk expectations.

"The great myth of our times is that technology is communication"
– Libby Larson

Summary

- **Project Management Mindset**: As Project Management Professionals, we need to shift security left to apply security fixes as early as possible in every phase of the software development; it is less expensive to do so.
- **We Can (and MUST) Do This**: DevSecOps extends the DevOps culture to include improving the effectiveness of security processes, shortening the length of test cycles, and ultimately aids in increasing software quality.
- **Train, Train, Train**: Educating your staff is a huge key to pivoting successfully.

"Computers are useless. They can only give you answers"
– Pablo Picasso

Questions
?

Andrew Boyle
Booz | Allen | Hamilton

Boyle_Andrew@bah.com

https://www.linkedin.com/in/andrew-boyle-b74299/

Stephanie Jenkins
Booz | Allen | Hamilton

Jenkins_Stephanie@bah.com

Evaluate Session