

Graphic Recordings

October 12, 2022

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Document Markings

Copyright 2022 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM22-0929

Welcome!

DevSecOps Days 2022

Washington, D.C., October 12th



Keynote: Rise of the Software Defined Weapon:

Accurate Delivery or Lose

KYLE FOX

DOD systems
look like
COMMERCIAL systems

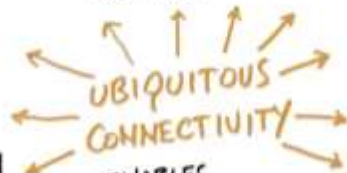


↑ SPACE-X
LEARNING
UNTIL
LAUNCH

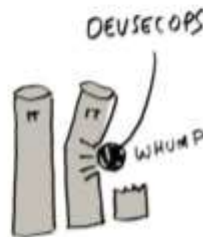
CONTINUOUS
DEV IN OP
ENVIRONMENT
WITH NO
COMPROMISE



SW-DEFINED
WEAPONS
ARE HERE



- ENABLES MOVEMENT AT SPEED & SCALE
- MAXIMIZES LEARNING
- BRINGS UNITY IN PURPOSE & MISSION



WE LIVE IN EXPONENTIAL TIMES



AMOUNT OF DATA

2010	2020
15 K CREF	1,000 K CREF

BOOM
THREATS TO EVERY ASPECT OF DELIVERY CHAIN

INTEGRATE
AUTOMATE
OPTIMIZE
DELIVERY PROCESSES

WE MUST ARCHITECT FOR SPEED

RISK-BASED APPROACH: ESTABLISH GUARDRAILS- GO FAST

PRIORITIZE DELIVERING VALUE

- Software is different from big, capital expenditures



★ RESILIENT SYSTEMS

SHIFTS LEFT & SHIFTS RIGHT
PLAN/DEVELOP DEPLOY/OPERATE

DEVSECOPS REVOLUTION:

TECHNIQUES THAT REVOLUTIONIZED IT NOW IMPACTING MANY UNIQUE ENVIRONMENTS AND PROCESSES FOR FIELDED DOD SYSTEMS

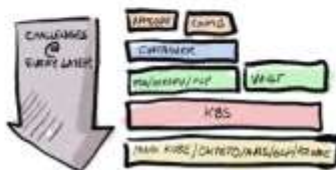


JEROEN WILLEMSSEN

LEARN HOW TO (NOT) USE SECRETS WITH OWASP WRONG SECRETS



PROJECT SECRETS - DEMO



- SIMPLER TOOLS MOST EFFECTIVE
- LOOK FOR VALUE
- SAY DOCKER BUILD TO CONSTRUCT CONTAINER



THOUGHT
TO FREEZE
CHALLENGES
AT 25

FUN WITH ANS ENVIRONMENT

- SECRET FOUND IN TERRAFORM STATE
- SEE DEMOS ON SECRETS MANAGEMENT
- "CAN I DETECT SECRETS EARLY ON?"
- DON'T JUST TRUST DEFAULTS
- NEVER HARD CODE
- ROTATE SECRETS
- REDUCE PLAYST RADIUS
 - EXPOSURE
- HAVE LOGGING + ALERTING

WHAT'S NEXT?

- UI IMPROVEMENTS ARE ON THE WAY
- SECRET DETECTION
- JUICE SHOP

GET INVOLVED!

IF YOU HAD TO
ROTATE YOUR
SECRETS?

→ DO YOU KNOW
WHERE THEY
ARE?

SECRETS

- LAST BORROWED BY A COLLEAGUE
- NOT WORKING ANYMORE



- TOKEN
- KEYS
- QR CODE

WHERE DO YOU
KEEP A SECRET?

- CODE
- K8S
- CONTAINER
- ...

SECURITY IS AN AWESOME PRODUCT FEATURE

- Mark Hahn

CYBER SECURITY IS A BUSINESS PROBLEM

KIP BOYLE, "FIRE DOESN'T INNOVATE"



EMPLOYEES SEE IT AS PART OF THE DAILY WORK	LEADERS UNDERSTAND IT IS A PRIMARY FEATURE
--	--

TEAMS WANT TO WORK ON AWESOME FEATURES, NOT SECURITY, THEY DON'T REALIZE SECURITY IS AN AWESOME FEATURE



EMPOWER TEAMS SO THEY CAN TAKE ON SECURITY AS A PRIMARY APPROACH

SECURITY IS ITERATIVE

YOU DON'T HAVE TO MITIGATE EVERYTHING ALL AT ONCE



"TAKE SMALL BITES"

FOR ITERATIVE SECURITY

- EASY WINS EARLY
- BUSINESS WINS SHOW HOW IT MITIGATES RISK (\$)

DESCRIBE VALUE

- Evaluate value & trade-off features:
- RELATIVE VALUE
 - MONETARY METHODS
 - CHECKLISTS
 - FRAMEWORKS

HIPPO NO

RELATIVE VALUATIONS CAN COME DOWN TO HIGHEST PAID PERSON'S OPINION

MONETARY METHODS

DATA BREACHES ARE EXPENSIVE!!\$!!

COST OF SYSTEM IS NOTHING IN COMPARISON



CHECKLIST VALUATION

GARTNER "12 THINGS TO GET RIGHT"

DEVSECOPS THINKING

PUT THESE CHECKLISTS INTO THE DAILY PROCESS



JOEL TOSI
MAKE THE WORK EASY:
CULTURE SHIFTING THROUGH LEARNING

TO CHANGE CULTURE
CHANGE THE WAY
WORK WORKS

FOCUS ON HOW TO
MAKE IT EASIER
TO LEARN

CULTURE IS
A SHADOW OF
HOW WE WORK

CAN'T JUST WORK
ON YOUR SHADOW,
HAVE TO WORK
ON YOURSELF



CAN'T ASSUME
CERTAINTY IN
A WORLD OF
COMPLEXITY

HARD TO EXPLAIN
HOW WE KNOW
WHAT WE KNOW

- COMPLEX**
- SYSTEMS VAST + DIST.
 - INTERACTIONS ARE CLOSE TO PEOPLE; PEOPLE ARE COMPLEX
 - WE'RE BUILDING THINGS THAT HAVE NEVER BEEN BUILT
 - CAN'T ASSUME CERTAINTY IN COMPLEXITY

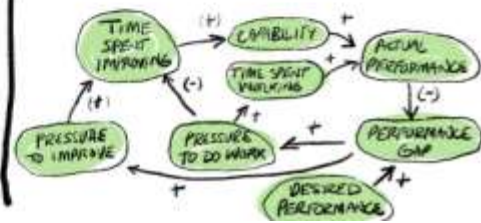
PERFORMANCE GAP



"THE DIFFERENCE BETWEEN FAILURE + LEARNING IS HOW MUCH IT COST IN EITHER YOUR EGO OR MONEY"
— DAVID SISSMAN

WHAT IS NEEDED TO LEARN
SAFETY
EXPERIMENTATION + REPEITION
CONTEXT + EXPERIENCE
SOCIAL DYNAMICS

- 1 CHALLENGER SAFETY
- 2 CONTRIBUTOR SAFETY
- 3 LEARNER SAFETY
- 4 INCLUSION SAFETY



FORGETTING CURVE—
IF YOU DON'T APPLY
KNOWLEDGE ON A
REGULAR BASIS, YOU
WILL FORGET HOW TO

STATIC THINKING FAILS
IN A DYNAMIC ENVIRONMENT

• WHEN BUILDING SOMETHING
NEW, THERE ARE NO
BEST PRACTICES, THERE
ARE EMERGING PRACTICE

LEARNING INDIVIDUALLY
IS SILLY... WE WORK
TOGETHER SO WE
SHOULD LEARN
TOGETHER!



KNOWLEDGE/CULTURE
IS NOT A THING

- CANNOT BE TRANSFERRED OR
- TALK ABOUT KNOWLEDGE CREATION NOT KNOWLEDGE TRANSFER



DJ SCHLEEN
KEYNOTE: SOFTWARE BARREL OF MONKEYS (SBOM)



OPENSOURCE STORY

- BIG VUL IN IN
 - 3AM - ARE WE @ RISK
 - CONTAINERS WERE NEW
 - SEND EXCEL SS. WITH QUESTIONS
- ↳ NOT IN USE!

WE DON'T UNDERSTANT WHAT'S INSIDE OUR SW

3RD PARTY COMPONENTS

- ARE THERE VULS IN WHAT WE USE, + WHERE ARE THEY

SBOM

- THEY CONTAIN DEPENDENCIES USED BY THE SOFTWARE, AS AN ATTEMPT TO MAP ALL THE PARTS THAT MAKE THE SYSTEM

NEED SBOM

TO KNOW WHAT IS INSIDE SOFTWARE, WHERE COMPONENTS CAME FROM + ARE THERE VULS, ASSOCIATED W/THE COMPONENTS



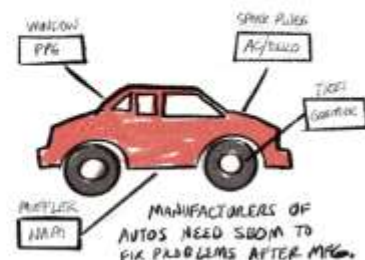
HOWEVER -
MORE TO SYSTEM HEALTH THAN JUST THE SBOM
• PROVENANCE + INTEGRITY INFO ARE MISSING



SBOM GENERATION TOOL

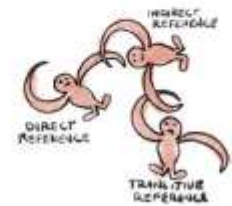


SBOM USABILITY ISSUES
• SEVERAL STANDARDS + FORMATS, NOT EASILY UNDERSTOOD BY NON-TECH PEOPLE
★ GOOD IDEA IS TO BUILD SBOM GENERATE FUNCTIONALITY INTO YOUR RELEASES



- MINIMUM ELEMENTS TO INCLUDE IN A REPORT:
- SUPPLIER NAME
 - COMPONENT NAME
 - VERSION + COMPONENT
 - OTHER UNIQUE IDENTIFIERS
 - DEPENDENCIES
 - REPORT AUTHOR
 - REPORT TIMESTAMP

BARREL OF MONKEYS



ESCAPING UNICORN CULTURE



ALEX CROSS

THE HYPER-TALENTED
INDISCIPLINARY
GURU WHO CAN
HANDLE ANYTHING
PRECIOUS, RARE
CANNOT BE DUPLICATED



AVOID SECURITY UNICORNS, ENABLE SECURITY CHAMPIONS

ARCHITECT YOUR TEAMS AS YOU WOULD A SYSTEM

FANTASTIC ENGINEERS AND WHERE TO FIND THEM

DON'T BUILD YOUR DEVSECOPS CAPABILITY ON UNICORNS

ROLE MAPPING
BALANCE ROLES ACROSS TEAM FAIRLY



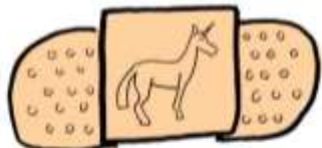
T-shaped People
Deep Skills in one area



Pi-shaped People
Deep Skills in several areas



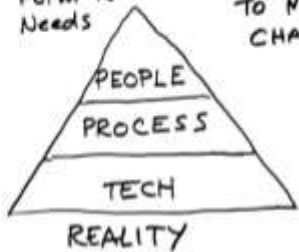
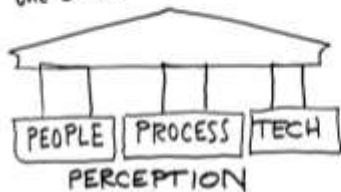
Blob-shaped People
Form to fit Needs



EASIER TO USE UNICORNS THAN TO MAKE REQUIRED CHANGES

IF YOU HAVE A UNICORN!

- USE CAREFULLY
- ASSIGN SHORT-TERM ROLES
- APPLY SAME STRATEGIC ROLES
- PREPARE FOR BACKLASH AS THE CONSTRAINTS KICK IN



UNICORNS ARE:
- EXPENSIVE
- HARD TO KEEP
- HARD TO FIND
- HARD TO PLACE
- HARD TO TRAIN
- PERPETUATING CHAOS



VISHY MAHADEVAN
THE ART OF ENABLING ENGINEERING
EXCELLENCE AND DEVSECOPS

KEY DSO CHALLENGES FOR SECURITY LEADERS:
MATURITY, MINIMIZING DEVELOPER EFFORT, COMPLIANCE, STANDARDIZATION AND VULNERABILITIES/RISK

MOST ORGS INVEST IN TOOLS TO IMPROVE
WHAT IF... WE REMOVE COMPLEXITY + PROVIDE INSIGHT



USE OF METRICS + MONITORING:
MAXIMIZED DATA COLLECTION FOR ASSESSMENT OF PROJECT PERFORMANCE

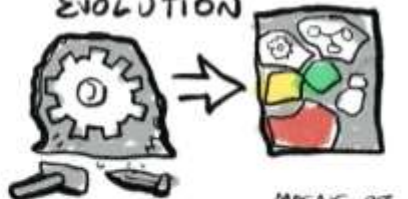
SHIFT SECURITY, WHILE GETTING NEAR REAL-TIME VISIBILITY + GOVERNANCE OF THE STAGE GATES IN THE LIFECYCLE OF SOFTWARE DELIVERY.

LEADER CHALLENGES TODAY

- PRODUCTIVITY-DEVELOPER
- VELOCITY
- CODE QUALITY
- SECURITY

CHALLENGE TO FIND A RELIABLE DEVSECOPS PROCESS, BUT CAN IT BE AUTOMATED?
COLLECT DATA AND FIND INSIGHTS FROM IT, LEADING TO SOLUTIONS

SOFTWARE DEVELOPMENT EVOLUTION



CUSTOM DEVELOPMENT

MOSAIC OF TOOLS AND CAPABILITIES

ENGINEERING EXCELLENCE:
BEST PRACTICES TO CRAFT ALLIED TO BENCHMARKING FOR CONTINUOUS EVALUATION AND IMPROVEMENT

SOFTWARE TRANSPARENCY:

SECURING THE DIGITAL SUPPLY CHAIN

CHRIS HUGHES

OPEN SOURCE SOFTWARE


Good -

- EXPEDITES INNOVATION
- CREATES ROBUST COMMUNITY AND ECOSYSTEM

BAD

- 60-80% OF SOFTWARE IS COMPRISED OF OSS
- SOFTWARE SUPPLY CHAIN ATTACKS ARE ON THE RISE
- MANY PROJECTS SUPPORTED BY UNPAID VOLUNTEERS
- LACK OF VISIBILITY AT THE COMPONENT LEVEL



(C-SCRM) 



OSS Crowd sourcing

SHIFT LEFT
TO CATCH BUGS EARLY



DUE TO A LACK OF UNIFIED
CI/CD CLEANSING STANDARDS,
VULNERABILITIES CAN PROPAGATE
DOWN A SUPPLY CHAIN

* CIDER SECURITY TOP 10 LIST

* SLSA DEV

- PREVENT TAMPERING
- IMPROVE INTEGRITY
- SECURE PACKAGE

CI/CD PIPELINES

GOOD

- SECURITY
- AUTOMATION
- RELEASES

BAD

- INTEGRATION COMPLEXITY
- COMPROMISED COMPONENTS
- COMPROMISED RELEASES



SCAN THOSE
CONTAINERS
THROUGHOUT
LIFE CYCLE

KUBERNETES AND CONTAINERS

Common Helm Charts
have insecure configs.

**SCAN YOUR
INFRASTRUCTURE
AS CODE**

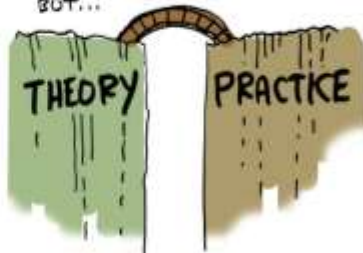


SUPPLY CHAIN



SaaS often overlooked

NO SHORTAGE OF GUIDANCE,
BUT...





JASON MARTIN
MINIMUM VIABLE SECURITY:
HOW TO GET STARTED

HIGHMARK
2ND
LARGEST IN NATION

SECURE SW DEV OBSTACLES

- WRITING CODE IS HARD
- LACK OF SECURITY SKILLS
- LEGACY SW
- CAN'T JUST RELY ON BEST PRAC.
- LACK OF FOCUS ON RISKS & LACK OF AUDIT/CONTROL POINTS

FAIR METHOD

- SPEAK SAME LANGUAGE OVER ENTERPRISE
- DOES NOT BREAK RAPID DELIVERY MODEL

DEV
SEC
OPS
DAYS

SIMPLIFY THESE SECURITY PROBLEMS:

OBJECTIVE - IS IT SECURE/SECURABLE

TASK - DOCUMENTATION OF CONTROL OBJECTIVES, IDENTIFICATION OF INTERDEPENDENCIES + RECORDS, ESTABLISHMENT OF AUTHORITY APP DATA, DELIVERABLES

A SCORECARD KEEPER TRACK OF HOW VULNERABLE YOUR SW IS PER FUNCTIONAL AREA

"MVS SCORECARD IS A NICE WAY TO START THE DSO IMPLEMENTATION,"
— HASAN YASAIT

RACI CHARTS ARE ALSO ANOTHER GOOD INSTRUMENT TO MAP RESPONSIBILITIES + AWARENESS ACROSS THE ORGANIZATION



HIGHMARK JOURNEY

- FORMERLY HAD TRADITIONAL SECURITY DEV. PROCESS
- LEARNED COMMON OBSTACLES FROM AN ASSESSMENT
 - COMMON ISSUES i.e. VUL NOT RESOLVED
- LEARNED A HIGH VALUE TO BE PLACED ON ALL PARTS OF THE SW PROCESS
- ASSESSMENT MADE A STRONG CASE FOR CHANGE. AREAS AT THE TIME WERE ALREADY STARTING DSD
- UNIVERSAL ADOPTION WAS IMPLEMENTED

LEADERSHIP SHOULD

- ENCOURAGE AN ENVIRONMENT WHERE SECURITY IS IMPORTANT AT EVERY STAGE
- HIGHER UP FRONT COSTS, BUT COULD SAVE MONEY IN THE LONG RUN

97% COMMERCIAL CODE HAS OS CODE

81% CODE BASES CONTAIN OUTDATED OS

62% BREACHES COME FROM SW COMPONENT