DevSecOps Days 2022 | Washington, D.C.

Graphic Recordings

October 12, 2022

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

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.

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

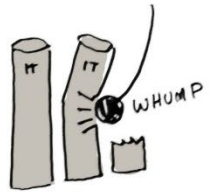
CONTINUOUS DEV IN OP ENVIRONMENT WITH NO COMPROMISE

SW-DEFINED WEAPONS ARE HERE

UBIQUITOUS CONNECTIVITY

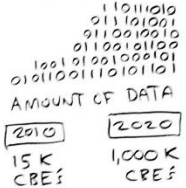
- ENABLES MOVEMENT AT SPEED & SCALE
- MAXIMIZES LEARNING
- BRINGS UNITY IN PURPOSE & MISSION

DEVSECOPS



WE LIVE IN EXPONENTIAL TIMES

NUMBER OF PHONES



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

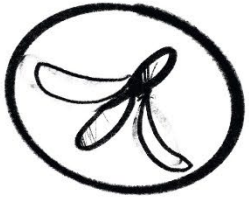
SHIFTS LEFT & SHIFTS RIGHT
PLAN/DEVELOP DEPLOY/OPERATE

DEVSECOPS REVOLUTION:

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

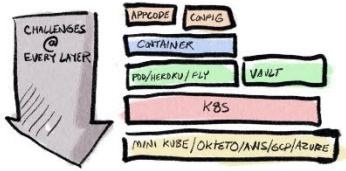
JEROEN WILLEMSEN

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



DEV SEC OPS DAYS

PROJECT SECRETS - DEMO



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

THOUGHT TO FREEZE CHALLENGES AT 25

FUN WITH AWS 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 BLAST RADIUS & EXPOSURE
- HAVE LOGGING + ALERTING

- TOKEN
- KEYS
- QR CODE

WHERE DO YOU KEEP A SECRET?
- CODE
- K8S
- CONTAINER
- ...

IF YOU HAD TO ROTATE YOUR SECRETS?

→ DO YOU KNOW WHERE THEY ARE?

SECRETS
- LAST BORROWED BY A COLLEGUE
- NOT WORKING ANY MORE

WHAT'S NEXT ?
- UI IMPROVEMENTS ARE ON THE WAY
- SECRET DETECTION
- JUICE SHOP

GET INVOLVED!

SECURITY IS AN AWESOME PRODUCT FEATURE

– Mark Hahn

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

CYBER SECURITY IS A BUSINESS PROBLEM

KIP BOYLE, "FIRE DOESN'T INNOVATE"

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

EMPLOYEES SEE IT AS PART OF THE DAILY WORK

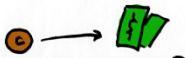
LEADERS UNDERSTAND IT IS A PRIMARY FEATURE

DESCRIBE VALUE

Evaluate value & trade-off features:

- RELATIVE VALUE
- MONETARY METHODS
- CHECKLISTS
- FRAMEWORKS

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"

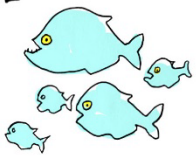
DEVSECOPS THINKING

PUT THESE CHECKLISTS INTO THE DAILY PROCESS

SECURITY IS ITERATIVE

YOU DON'T HAVE TO MITIGATE EVERYTHING ALL AT ONCE

"TAKE SMALL BITES"



FOR ITERATIVE SECURITY

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

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

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

DESIRE ★ ACTUAL

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

—DAVID SUSSMAN

HARD TO EXPLAIN HOW WE KNOW WHAT WE KNOW

WHAT IS NEEDED TO LEARN

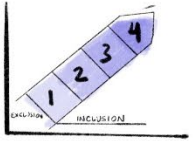
SAFETY

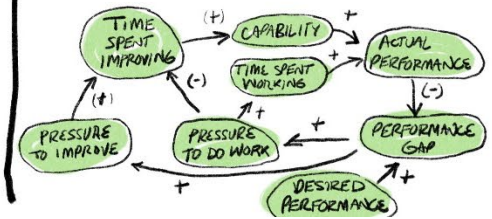
EXPERIMENTATION + REPETITION

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!

DEV SEC OPS DAYS

BEST TIME TO PLANT THE TREE IS NOW

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)

DEV SEC OPS DAYS

OPENSSL 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

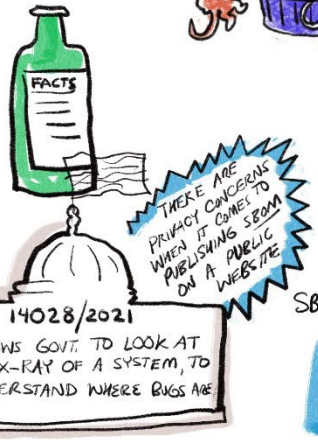
- ARE THERE VULS IN WHAT WE USE, + WHERE ARE THEY

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

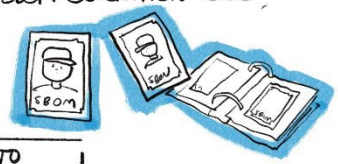


HOWEVER —

MORE TO SYSTEM HEALTH THAN JUST THE SBOM

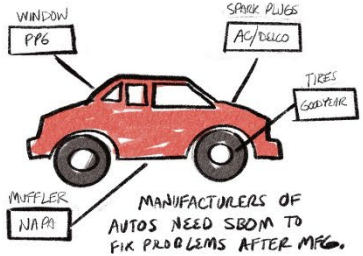
- PROVENANCE + INTEGRITY INFO ARE MISSING

SBOM GENERATION TOOL



SBOM USABILITY ISSUES

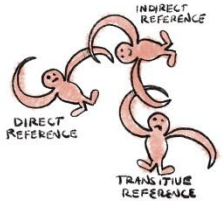
- SEVERAL STANDARDS + FORMATS, NOT EASILY UNDERSTOOD BY NON-TECH PEOPLE
- ★ GOOD IDEA IS TO BUILD SBOM GENERATE FUNCTIONALITY INTO YOUR RELEASES



MINIMUM ELEMENTS TO INCLUDE IN A REPORT:

- SUPPLIER NAME
- COMPONENT NAME
- VERSION of COMPONENT
- OTHER UNIQUE IDENTIFIERS
- DEPENDENCIES
- REPORT AUTHOR
- REPORT TIMESTAMP

BARREL OF MONKEYS



ESCAPING UNICORN CULTURE

ALEX CROSS

FANTASTIC ENGINEERS AND WHERE TO FIND THEM

THE HYPE TALENTED INDISCIPLINARY EXPERT WHO CAN HANDLE ANYTHING PRECIOUS, RARE CANNOT BE DUPLICATED

DON'T BUILD YOUR DEVSECOPS CAPABILTY ON UNICORNS

ARCHITECT YOUR TEAMS AS YOU WOULD A SYSTEM

- COHESIVE
- RESILIENT
- LOOSELY COUPLED

AVOID SECURITY UNICORNS, ENABLE SECURITY CHAMPIONS

T-shaped Peoples

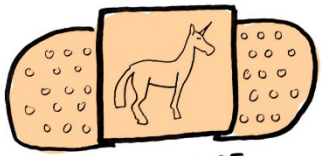
Deep Skills in one area

Pi-shaped People

Deep Skills in several areas

Blob-shaped People

Form to fit Needs



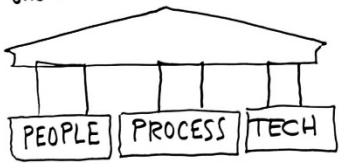
EASIER TO USE UNICORNS THAN TO MAKE REQUIRED CHANGES

ROLE MAPPING

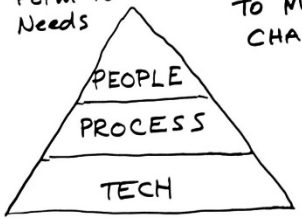
BALANCE ROLES ACROSS TEAM FAIRLY

IF YOU HAVE A UNICORN:

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



PERCEPTION



REALITY

UNICORNS ARE:

- EXPENSIVE
- HARD TO KEEP
- HARD TO FIND
- HARD TO PLACE
- HARD TO TRAIN
- PERPUATING CHAOS

VISHY MAHADEVAN

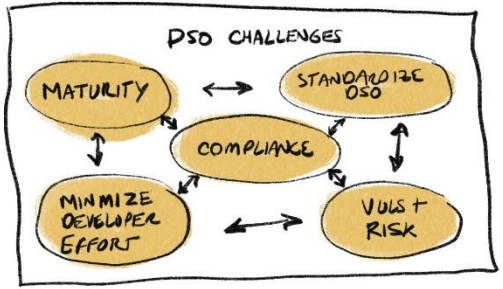
THE ART OF ENABLING ENGINEERING EXCELLENCE AND DEVSECOPS

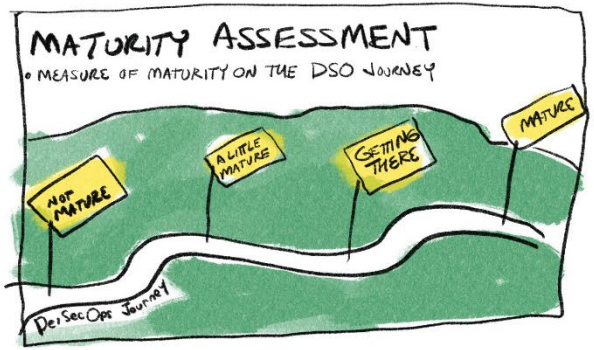
DEV SEC OPS DAYS

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



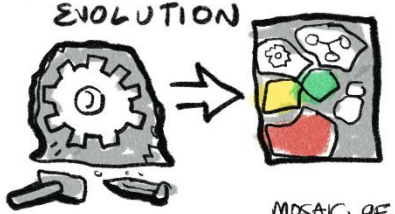


LEADER CHALLENGES TODAY

- 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

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.

SOFTWARE TRANSPARENCY:

SECURING THE DIGITAL SUPPLY CHAIN

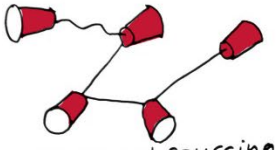
CHRIS HUGHES

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

SCAN THOSE CONTAINERS THROUGH OUT LIFE CYCLE

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

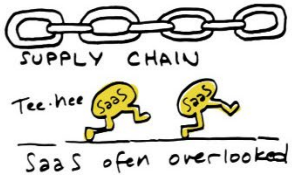
GOOD
- SECURITY
- AUTOMATION
- RELEASES

BAD
- INTEGRATION COMPLEXITY
- COMPROMISED COMPONENTS
- COMPROMISED RELEASES

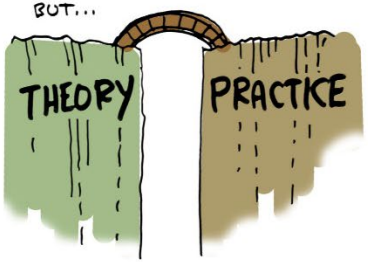
KUBERNETES AND CONTAINERS —

Common Helm Charts have insecure configs.

SCAN YOUR INFRASTRUCTURE AS CODE



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

HIGHMARK JOURNEY

- FORMERLY HAD TRADITIONAL SECURITY DEV. PROCESS
- LEARNED COMMON OBSTACLES FROM AN ASSESSMENT
  - COMMON ISSUES IC 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 DSO
- UNIVERSAL ADOPTION WAS IMPLEMENTED

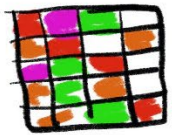
LEADERSHIP SHOULD

- 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



FAIR METHOD

- SPEAK SAME LANGUAGE OVER ENTEPRISE
- 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 AUTHORITATIVE 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