B-SIDES 2020: A journey from DevOps to SECdevOps

Presented by Rick Payne MSc, CISSP, Security+ , BS-IST, AS-CET, AWS CSA, RHCE, RHCSA

About me

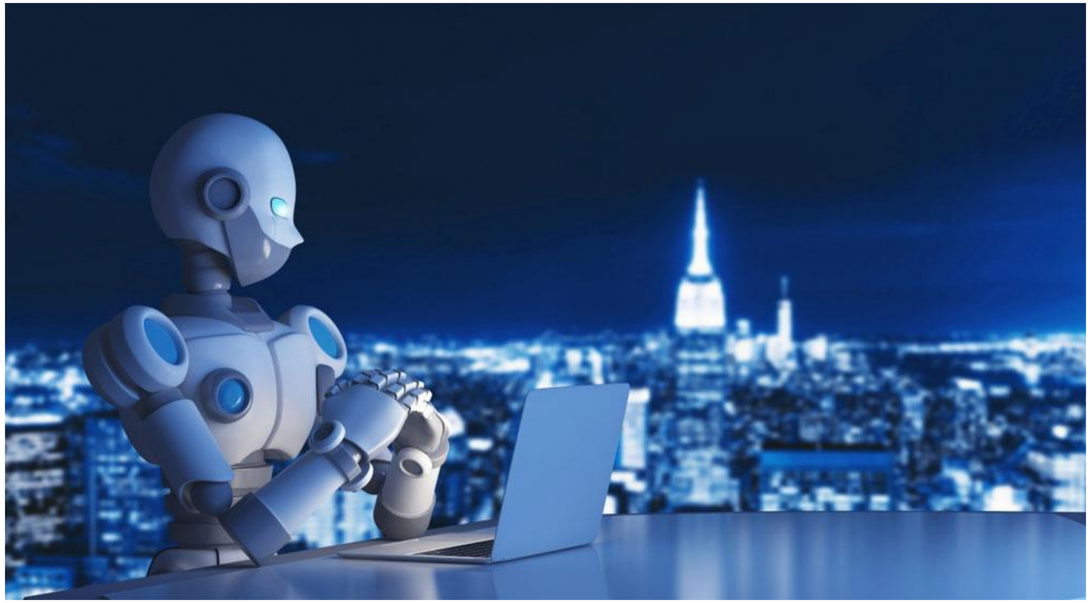
CAREER	CONF/PRES	EDUCATION
Staff Security Engineer	>35	MSc
Sr. Security Engineer		
Chief Security Officer		AWS-CSA
Security Architect		CISSP
Security Analyst I/II		BS, AA, Security+, RHCE, RHCSA
System Integration Tech I/II		
Manufacturing Test Tech I/II		AS-CET
Production Test Intern		

Presentation Goals

- Present new or current concepts & tech
- Shoot for highest content & highest quality
- Demonstrate an effective method to integrate SEC into your DevOps process via
  - People: Educate, partner with, treat like customers -> Amazon approach
    - Can become a management / people problem with disruptive automation
  - Process: Defined, embedded, speed, quality
  - Technology: Secure Automation Factory
- Impacts via metrics

2021 Stage Setting (Context)

- The digital technology is inline with the physical. E.g. Digital factories
- Build the machines that build the machines! (Elon Musk)
  - DevOps for SW delivery → Robotics Process Automation for common office tasks
- Current motto: do once, build modular, reusable tooling to automate and forget. Disruptive…labor reduction >90%, infinitely scalable

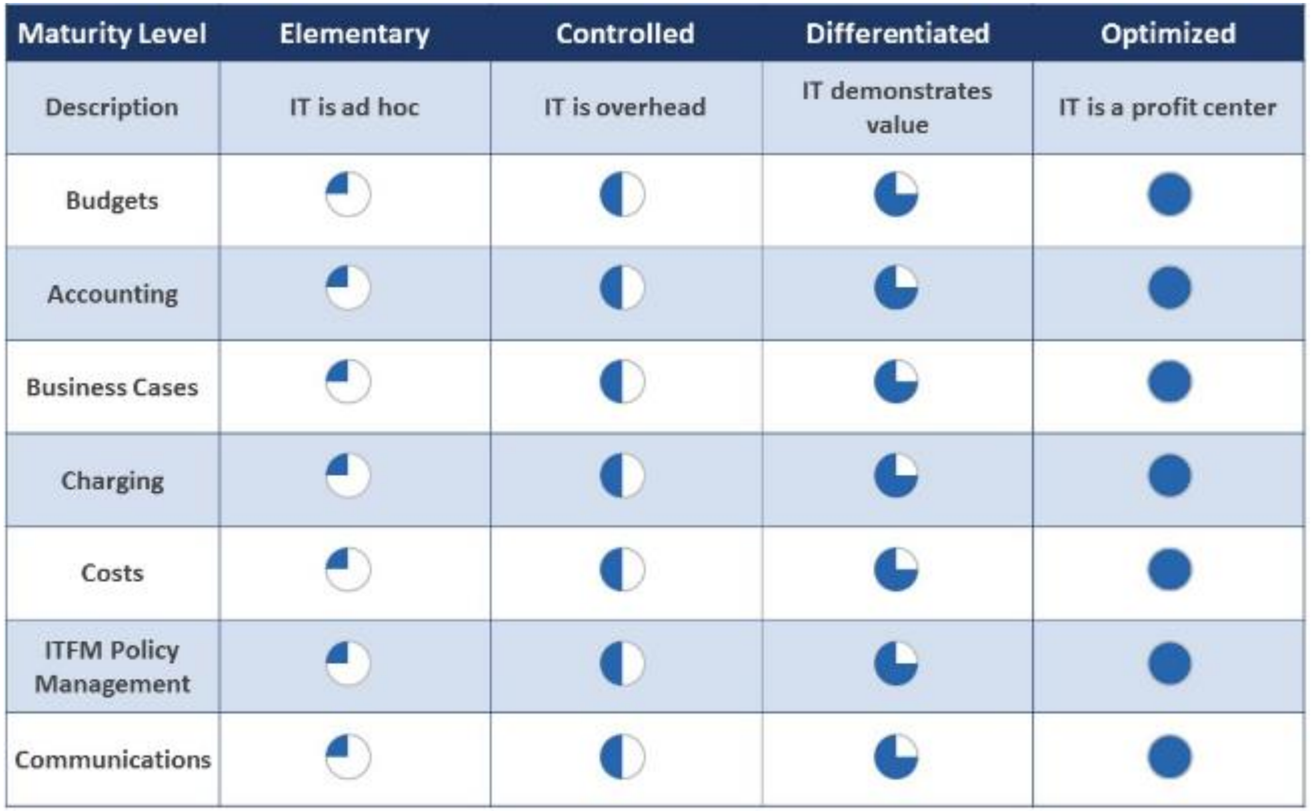


What is DevOps?

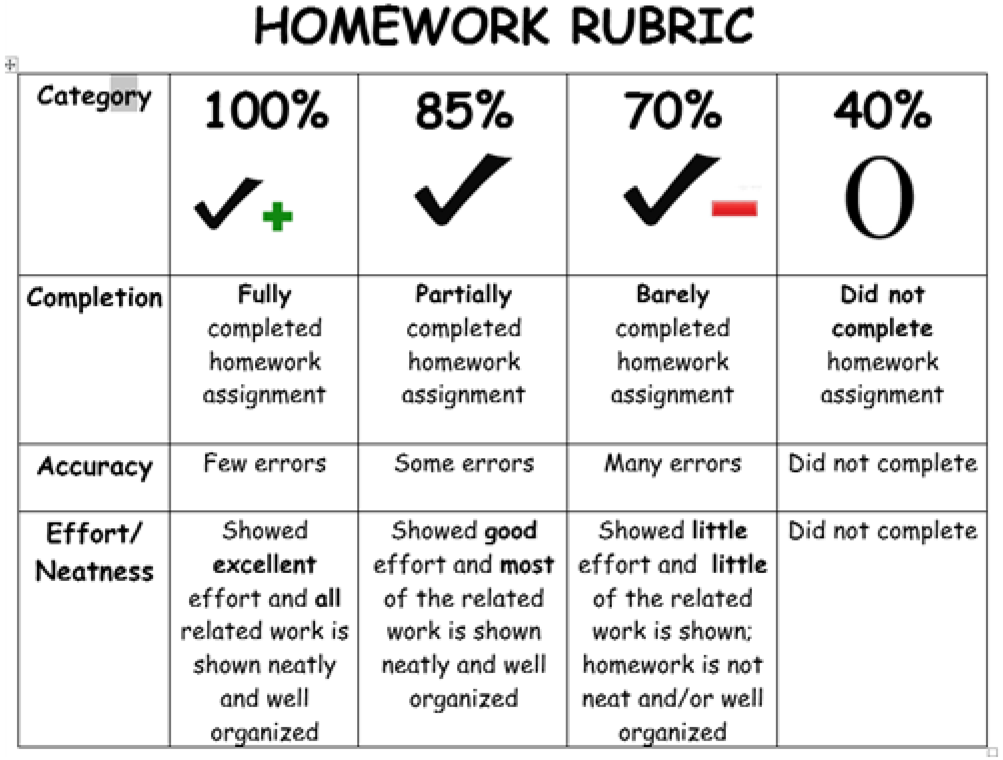
- DevOps represents a change in IT culture, focusing on rapid IT service delivery through the adoption of agile, lean practices in the context of a system-oriented approach. DevOps emphasizes people (and culture), and it seeks to improve collaboration between operations and development teams. DevOps implementations utilize technology — especially automation tools that can leverage an increasingly programmable and dynamic infrastructure from a life cycle perspective.Gartner
- First coined in 2009 because of frustrations with Dev & Ops silos

What are Maturity Models?

- Essentially, how mature is an organization at a specific objective.



Maturity Level	Elementary	Controlled	Differentiated	Optimized
Description	IT is ad hoc	IT is overhead	IT demonstrates value	IT is a profit center
Budgets	◔	◑	◕	●
Accounting	◔	◑	◕	●
Business Cases	◔	◑	◕	●
Charging	◔	◑	◕	●
Costs	◔	◑	◕	●
ITFM Policy Management	◔	◑	◕	●
Communications	◔	◑	◕	●

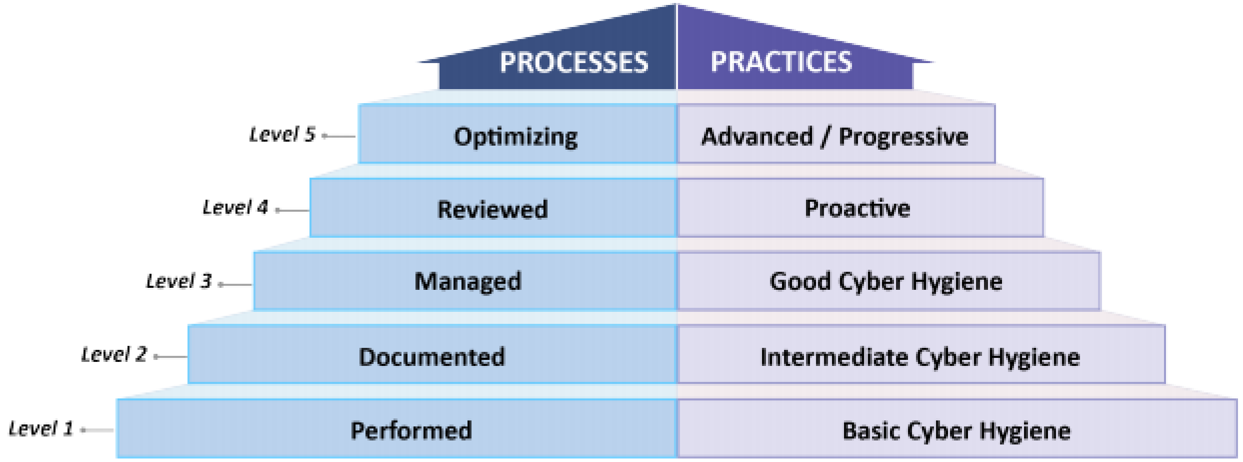


HOMEWORK RUBRIC

Category	100% ✓+	85% ✓	70% ✓−	40% O
Completion	**Fully** completed homework assignment	**Partially** completed homework assignment	**Barely** completed homework assignment	**Did not complete** homework assignment
Accuracy	Few errors	Some errors	Many errors	Did not complete
Effort/ Neatness	Showed **excellent** effort and **all** related work is shown neatly and well organized	Showed **good** effort and **most** of the related work is shown neatly and well organized	Showed **little** effort and **little** of the related work is shown; homework is not neat and/or well organized	Did not complete

What are Maturity Models?

- DoD’s Cybersecurity Maturity Model example



PROCESSES | PRACTICES

Level 5 — Optimizing | Advanced / Progressive

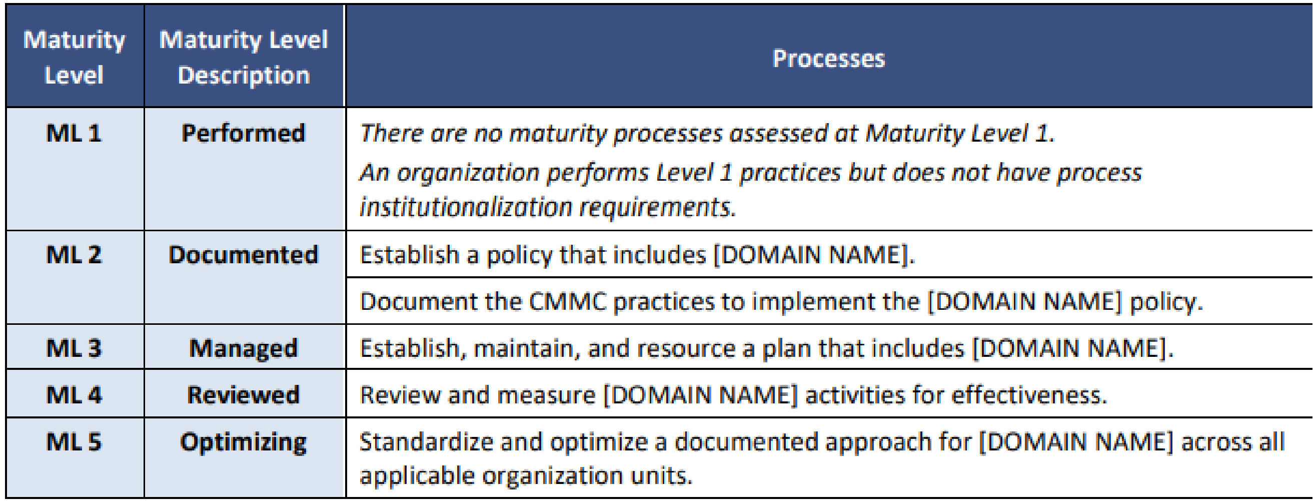
Level 4 — Reviewed | Proactive

Level 3 — Managed | Good Cyber Hygiene

Level 2 — Documented | Intermediate Cyber Hygiene

Level 1 — Performed | Basic Cyber Hygiene

Figure 2. CMMC Levels and Descriptions



Maturity Level	Maturity Level Description	Processes
ML 1	**Performed**	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	**Documented**	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	**Managed**	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	**Reviewed**	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	**Optimizing**	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

Maturity Models – DevOps -> SECdevOps

- DevOps

- DevOps without security is essentially a product pen test sandbox!
- Think about it…you can deliver all the features you'd like. But it doesn't matter if your breached
- You can't acquire or maintain any security certifications
- Applicant insight: Consider a prospective company's maturity through online research or when interviewing. This will represent the culture and shape your role while your there.
- Current company insight: Does this sound familiar? Are your peers and leadership onboard with maturing?

Maturity Models – DevOps -> SECdevOps

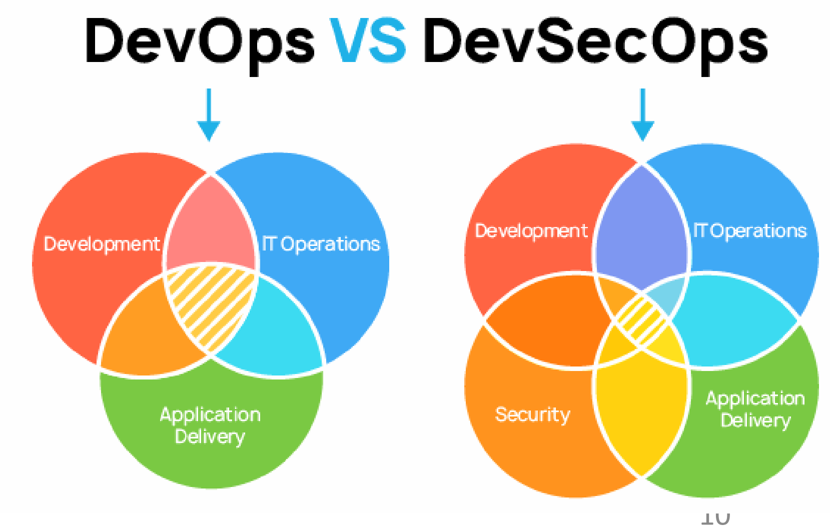
- DevOpsSec <- Shift left

- Devs & team are starting to listen to security
- As it states, security is chasing production / already released workloads
- Still political

Maturity Models – DevOps -> SECdevOps

- DevSecOps <- Shift left

- Most humans are change averse. Devs are no different binding to specific versions and being overly concerned by updates e.g. patching
- Culture shift:
  - Roles: Much of the code layer abstracted, Devs can now focus on secure code and update support as Infra & Platform are invisible. Security becomes FREE!
  - Responsibilities: every piece of the puzzle has a security layer

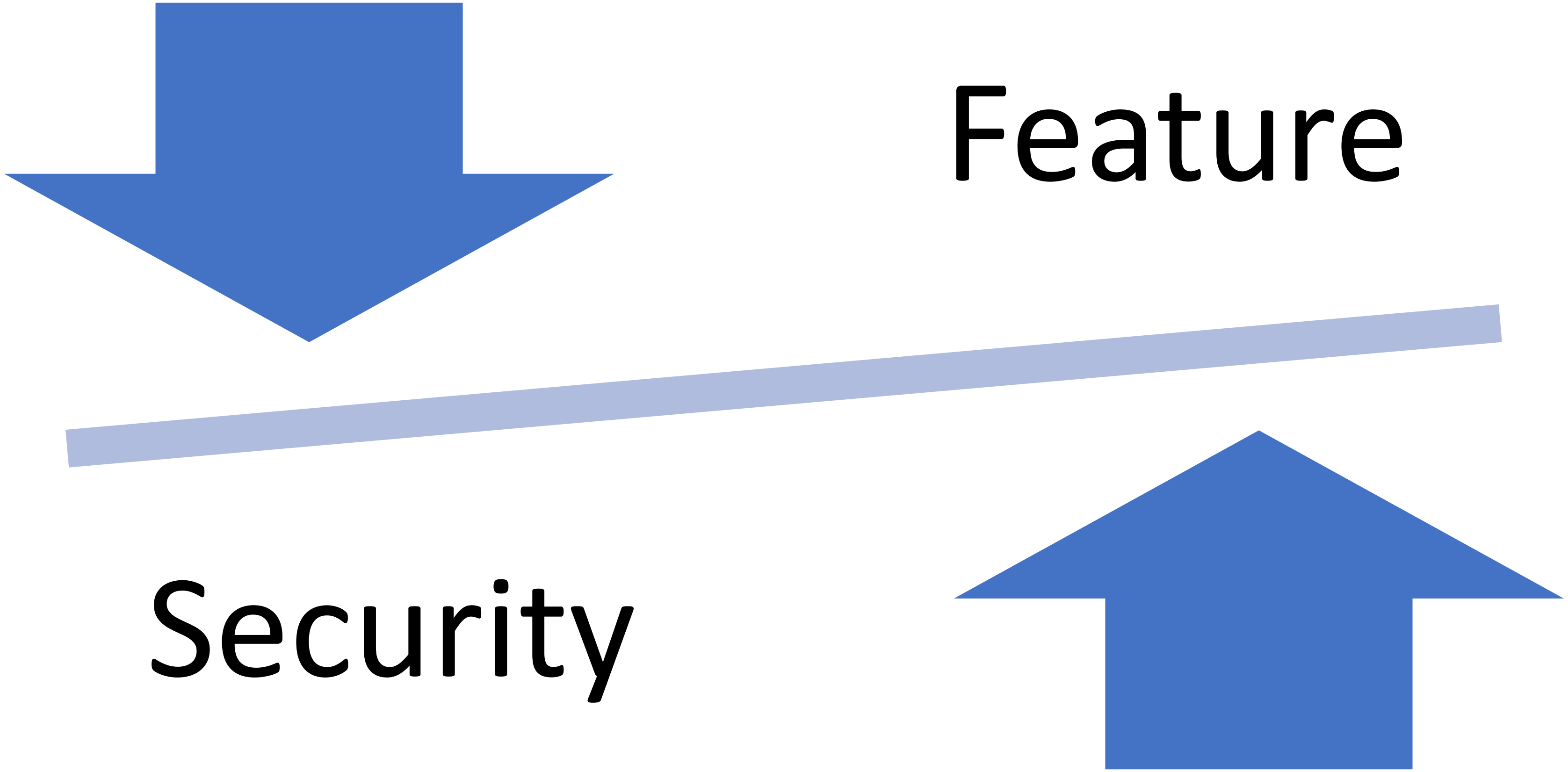


Maturity Models – DevOps -> SECdevOps

- SECdevOps

- Security is at the forefront of everything
- Project kickoffs
- Design reviews
- Security features are equally or more important than dev

Maturity Models – DevOps -> SECdevOps

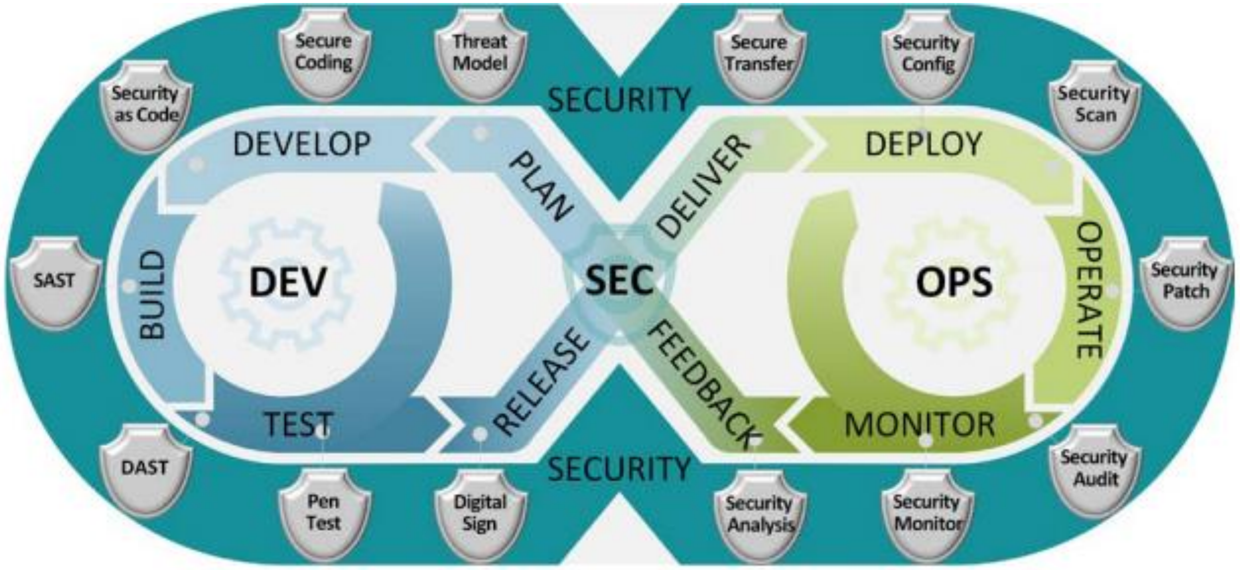


Feature

Security

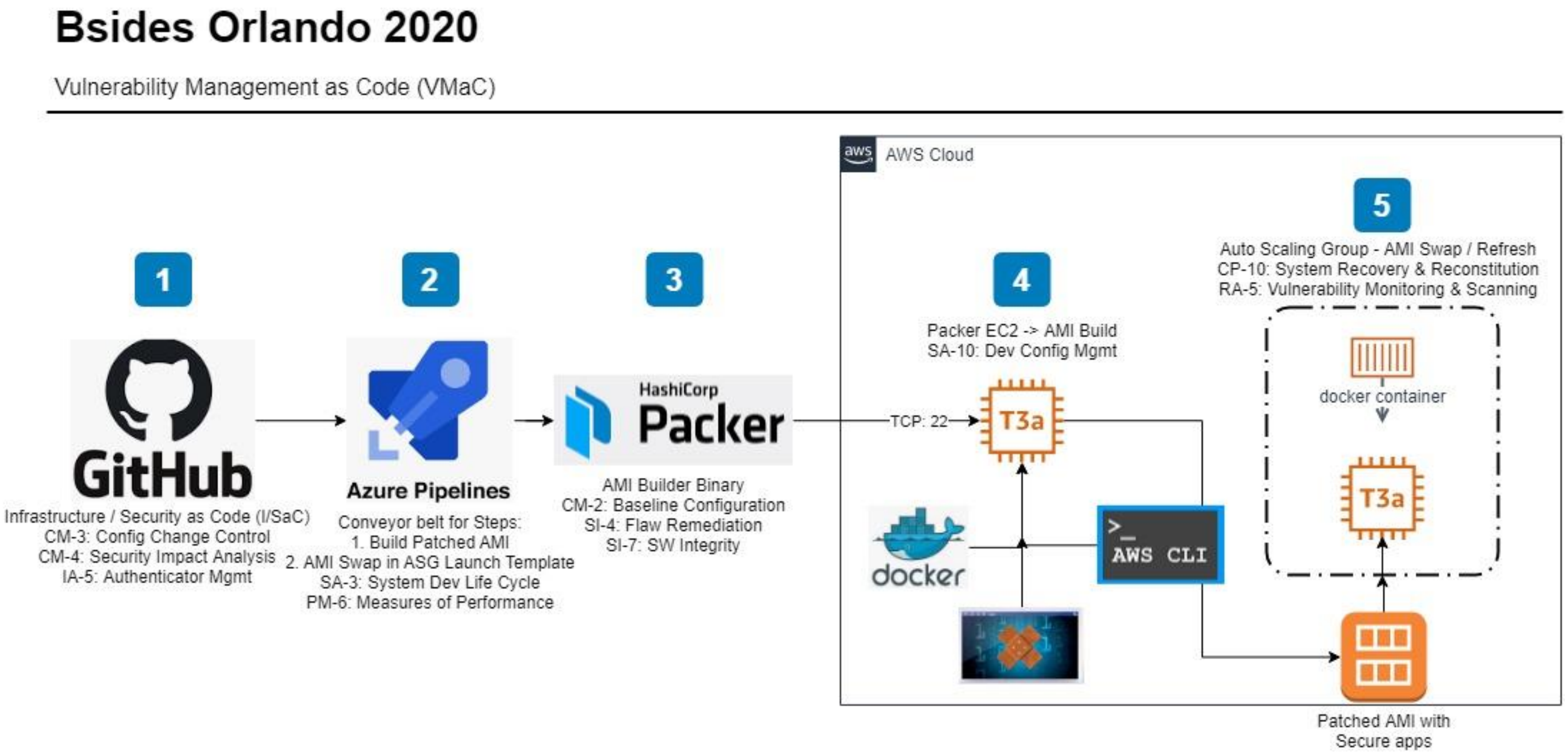
Maturity Models – DevOps -> SECdevOps

- DevSecOps is a software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of software development: plan, develop, build, test, release, deliver, deploy, operate, and monitor.[DoD]



Lightweight, Conceptual Demo

- Vulnerability Management as Code (VMaC) solution overview



Bsides Orlando 2020

Vulnerability Management as Code (VMaC)

1. GitHub

Infrastructure / Security as Code (I/SaC)
CM-3: Config Change Control
CM-4: Security Impact Analysis
IA-5: Authenticator Mgmt

2. Azure Pipelines

Conveyor belt for Steps:
1. Build Patched AMI
2. AMI Swap in ASG Launch Template
SA-3: System Dev Life Cycle
PM-6: Measures of Performance

3. HashiCorp Packer

AMI Builder Binary
CM-2: Baseline Configuration
SI-4: Flaw Remediation
SI-7: SW Integrity

4.

Packer EC2 -> AMI Build
SA-10: Dev Config Mgmt

5.

Auto Scaling Group - AMI Swap / Refresh
CP-10: System Recovery & Reconstitution
RA-5: Vulnerability Monitoring & Scanning

Patched AMI with
Secure apps

Lightweight, Conceptual Demo

- Draw.io solution
- My app is docker running a website
  - Security change review on GitHub Pull Request (PR) that updates the website – Shift waaaay left
- DevOps’ing -> Pushed to the next release! ☺
  - Easy to not follow secure credential usage
    - https://learn.hashicorp.com/tutorials/packer/getting-started-build-image
  - Principle of Least-Privilege (PoLP) – IAM Role
  - Unnecessary exposure – Critical workload production facing (VPN + Dockerfile)
- AzDO
  - PR Trigger via code update
  - Packer Build
    - Secure 3rd party software
    - Patch on build for Linux. Windows are mainly 1 per month @ patch Tuesday +1d
  - ASG update
  - ASG “instance refresh”

- If there’s demand, I’ll build and publish a step-by-step guide.

Last but not least, take care of yourself!

Q&A / References

- GitHub - https://github.com/rickpayne929/presentations
- Track 2 YouTube - https://www.youtube.com/watch?v=H5R7MpAjdv8
- DoD Cybersecurity Maturity Model Certification (CMMC) - https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf
- DoD DevSecOps Reference Design - https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583