Many thanks to our BSidesKC 2019 sponsors!!!

PLATINUM

GEHA

Bitdefender

Cerner

GOLD

10-D Security
Setting a Higher Level of Excellence in Information Security & Compliance Services

APCON
Solutions for Networks

BURNS McDONNELL

netskope

red canary

VERODIN

GuidePoint SECURITY

exabeam

FORTINET

SILVER

KENNA Security

REDSIEGE

fishtech group

RAVENii
www.ravenii.com

DEPTH SECURITY

AM Cyber Inc.

VARONIS

OPTIV

SANS

ExtraHop

observe it

Additional Sponsors

CRITICALSTART

freedom bank

DEVO

pwc

Gigamon

HACKERBOXES

HAK5

SECURITY PS

Big Brothers Big Sisters.

no starch press

paloalto

NEW CONTEXT

BUILDING SECURE SOFTWARE

AUGUST JOHNSON

Who am I?

- August Johnson
- Security Architect, Netsmart Technologies

What's this talk about?

A review of **frameworks** to help

an **organization** that builds software

to **consistently** produce

more secure software

- **OWASP SAMM**
- BSIMM
- ISO 27034
- NIST SP-800-64
- Microsoft SDL

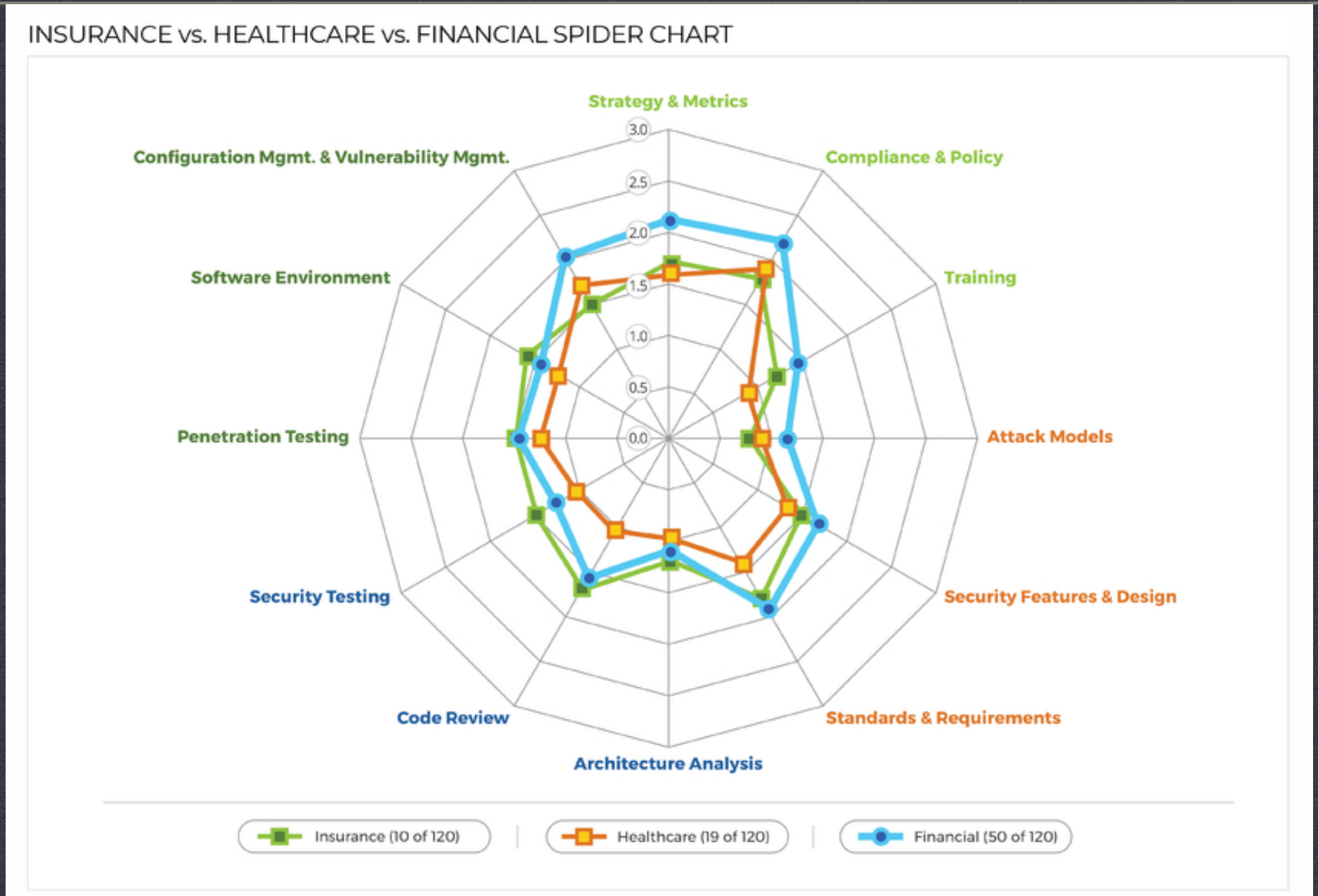
BSIMM

AN ONGOING SURVEY OF PRACTICES AMONG SOFTWARE COMPANIES

Of Organizations surveyed:

- 67% Provide awareness training.
- 40% Have an operations inventory of applications.
- 25% Identify PII data inventory.
- 21% Provide penetration testers with all available information.

- 11% Have a bug bounty program.



COOL CHARTS!

HOW OFTEN DO YOU LEGITIMATELY GET TO USE SPIDER CHARTS?

OWASP SAMM

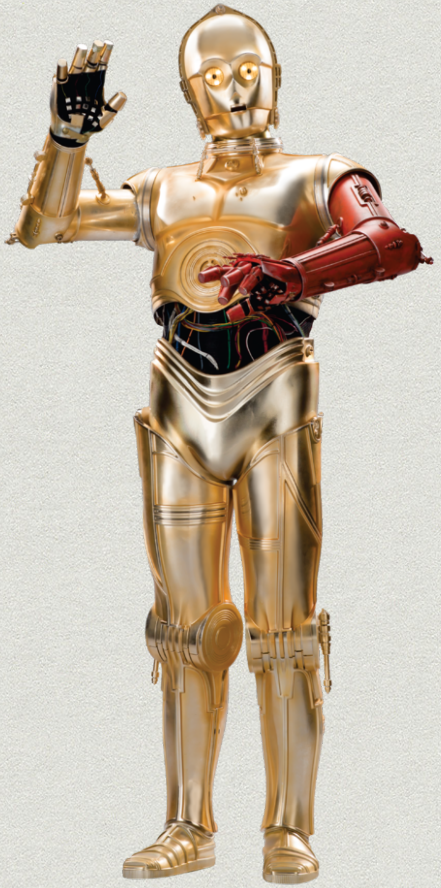
SOFTWARE ASSURANCE MATURITY MODEL (VERSION 2.0 BETA)

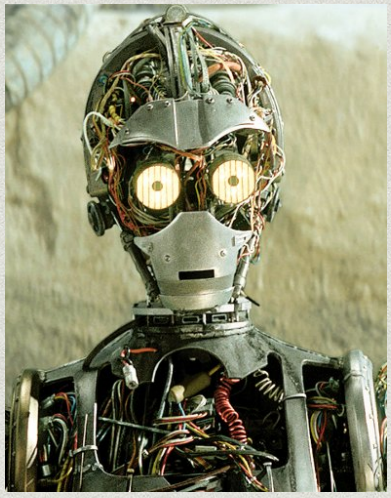
SAMM Goals

- Effective and **Measurable.**
- Provides **Actionable** paths forward**.**
- Able to work in **Versatile** environments.

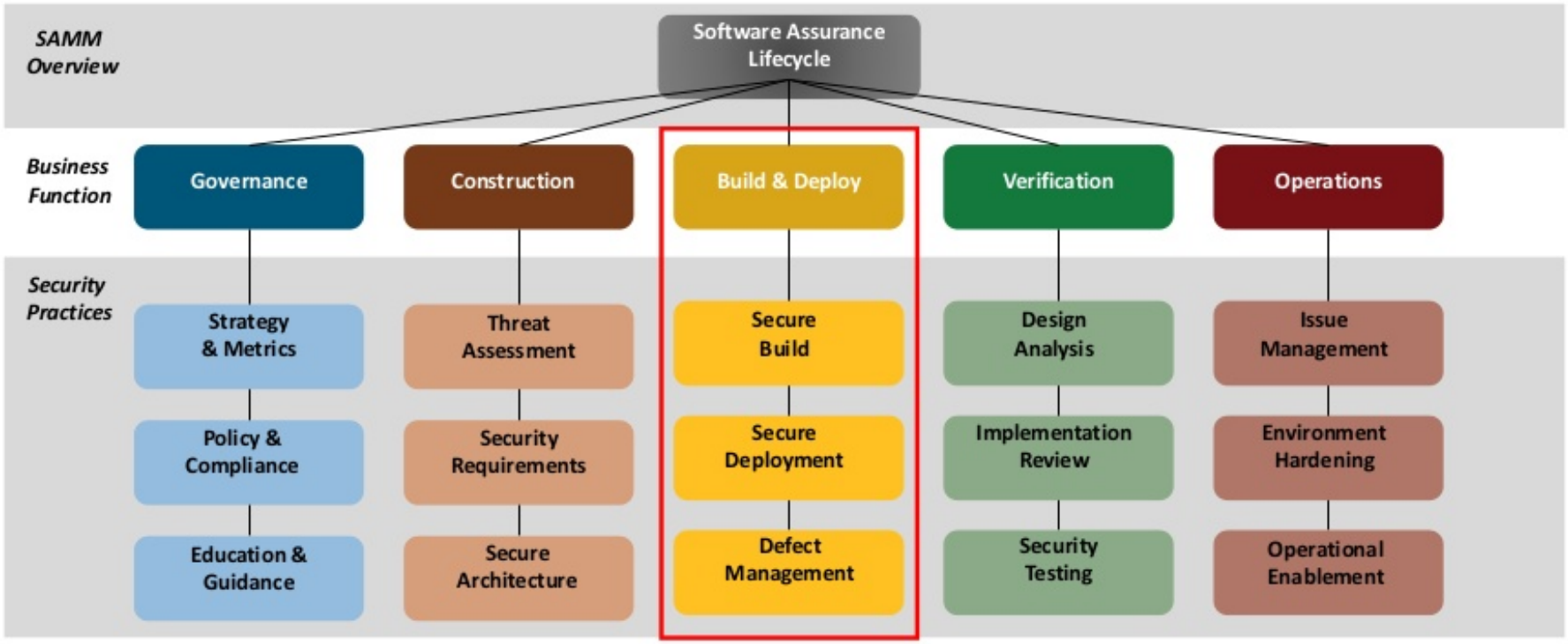
It's flexible.

- Paradigm Agnostic (**devops**, agile, waterfall)
- Customizable.
- Sliceable and diceable!





SAMM 2.0. Adjusting to devops



Deep Dive - Education and Guidance

Two Streams

- A. Training and Awareness
- B. Organization and Culture

Three maturity levels (each)

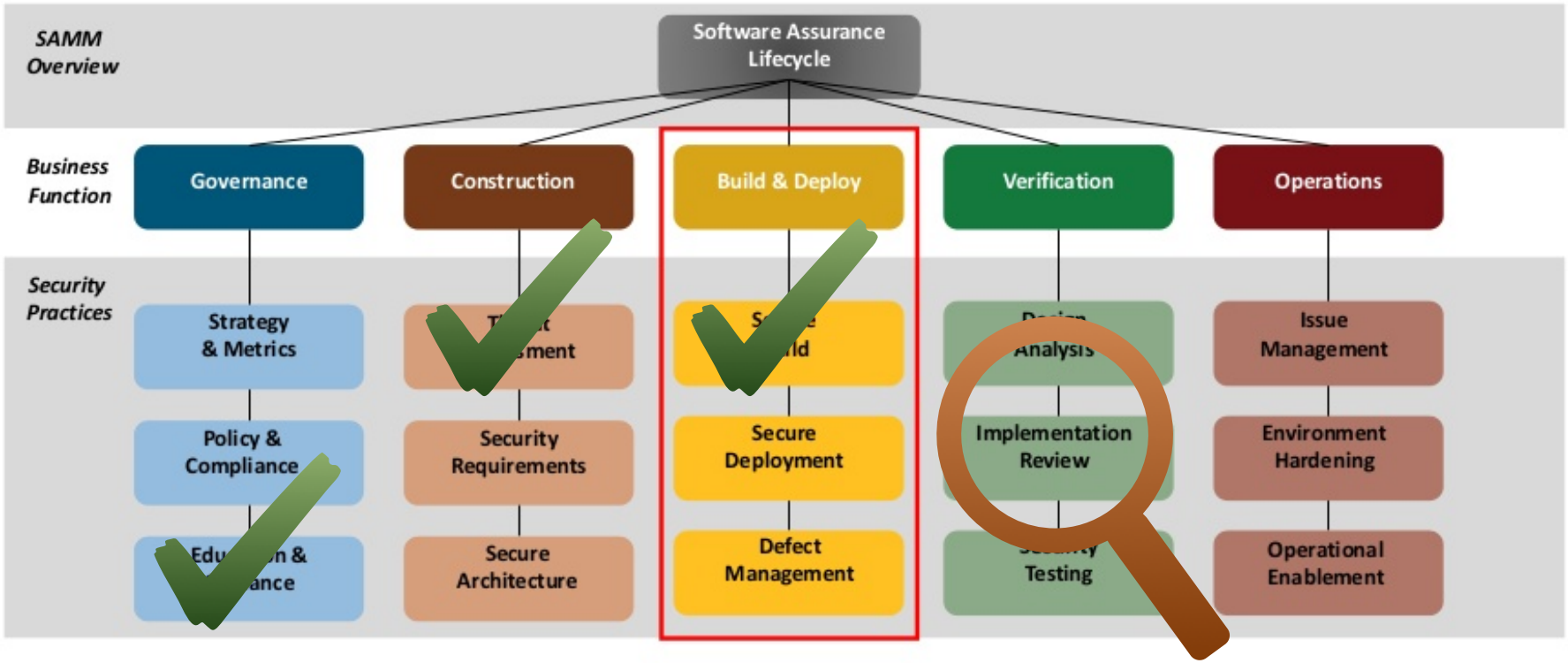
Deep Dive - Threat Assessment

	A: APPLICATION RISK PROFILE	B: THREAT MODELING
Maturity 1 - Best-effort identification of high-level threats to the organization and individual projects.	Basic assessment of the application risk.	Best effort ad-hoc threat modeling.
Maturity 2 - Standardization and enterprise-wide analysis of software-related threats within the organization.	Understand the risk for all applications in the organisation.	Standardized threat modeling.
Maturity 3 - Pro-active improvement of threat coverage throughout the organization.	Periodicly review application risk profiles.	Improve quality by automated analysis.

Deep Dive - Secure Build

- Maturity 1 - Build process is **repeatable** and **consistent**
- Maturity 2 - Build process is **optimized** and fully **integrated** into the workflow
- Maturity 3 - Build process helps **prevent** known defects from entering the production environment.

SAMM 2.0. Adjusting to devops



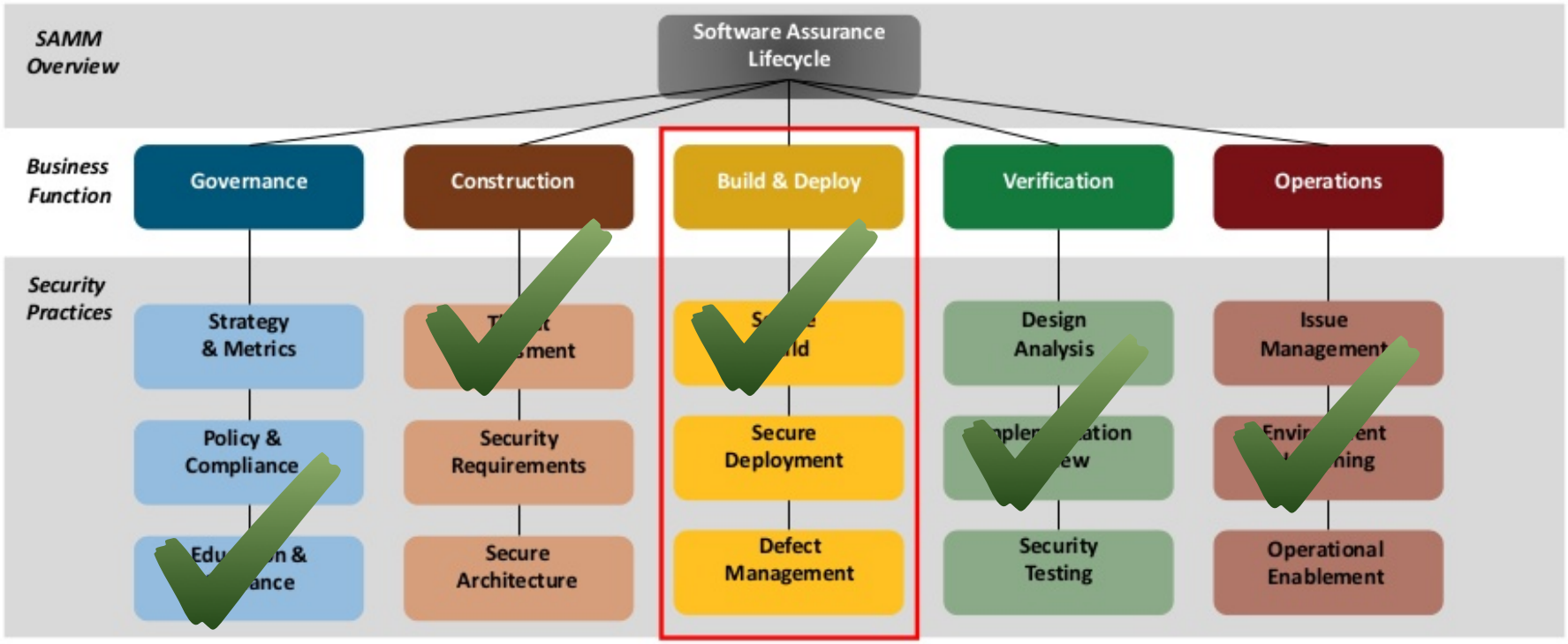
Deep Dive - Architecture Assessment
Benefits

ARCHITECTURE VALIDATION	ARCHITECTURE COMPLIANCE
Developers understand the architecture, interfaces, and how to secure them.	Assures that the compliance requirements of the architecture are met.
This activity validates the security mechanisms on the attack surface of the software and infrastructure architecture.	This activity assures that the architecture is aligned with the security requirements and best practices.
Assurance on the effectiveness of the architecture security mechanisms in terms of strategy alignment, appropriate support, and scalability.	

Deep Dive - Environment Management

- Maturity 1 - **Best-effort** patching and hardening.
- Maturity 2 - **Formal process** with baselines in place.
- Maturity 3 - Conformity with continuously improving process **enforced**.

SAMM 2.0. Adjusting to devops

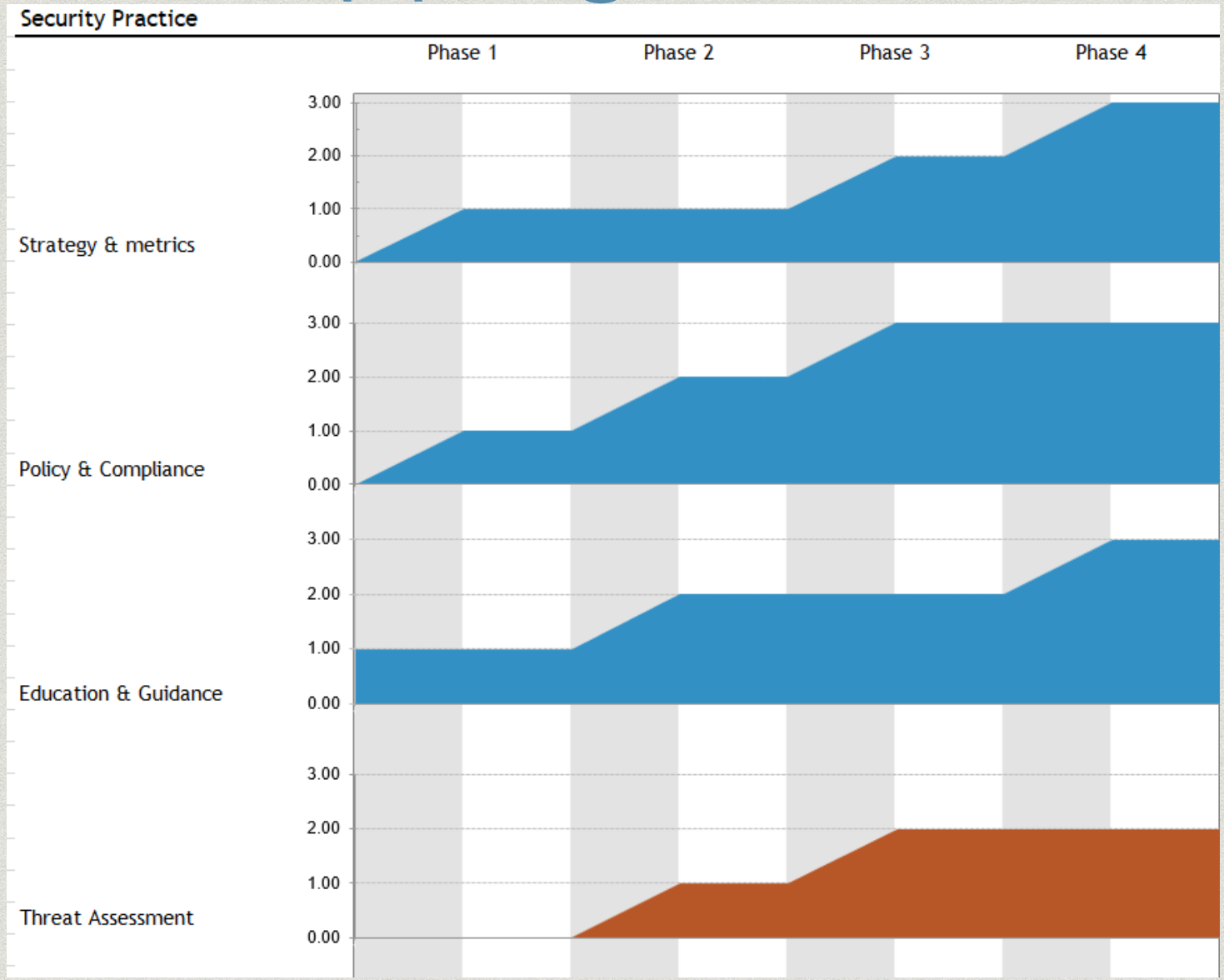


Self-Assessment

- A form you can fill out.
- A survey of sorts.
- Rates all kinds of activities at all maturity levels.

Current Maturity Score				
		Maturity		
Security Practices	Current	1	2	3
Strategy & Metrics	0.00	0.00	0.00	0.00
Policy & Compliance	1.60	0.75	0.35	0.50
Education & Guidance	0.30	0.20	0.10	0.00
Threat Assessment	0.10	0.10	0.00	0.00
Security Requirements	1.20	0.50	0.60	0.10
Secure Architecture	0.10	0.10	0.00	0.00
Design Analysis	0.00	0.00	0.00	0.00
Implementation Review	0.60	0.50	0.10	0.00
Security Testing	0.23	0.13	0.10	0.00
Issue Management	1.32	0.47	0.25	0.60
Environment Hardening	1.00	0.50	0.50	0.00
Operational Enablement	1.10	0.60	0.50	0.00

Roadmapping Tools



Setting Metrics

- Start with your self-assessment.
- BSIMM can help!
- Aim for gradual, realistic improvement.
- Re-assess after each phase.

SO FAR…

Questions?

August Johnson

august.johnson@gmail.com

keybase.io/augustjohnson

github.com/augustjohnson

augustjohnson.net

Help us get better!

Please provide feedback on…		
my talk	**the conference**	**anything else**
http://bit.ly/2019TalkEval	http://bit.ly/2019EventEval	http://bit.ly/IqT6zt