
PCi
Security
Standards Council
®

PCI Security Standards Council

See Yourself in Cyber

Careers Beyond Hacking

Ed Adams & Luke Fletcher

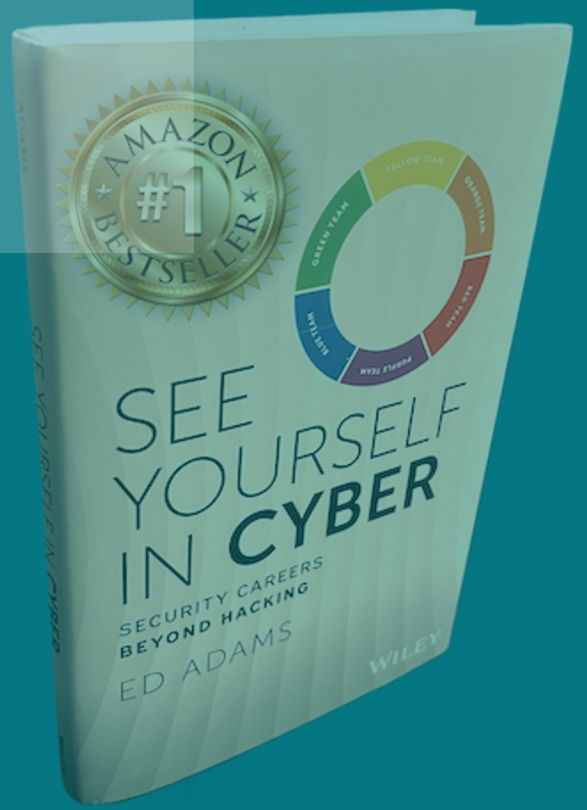
Bureau Veritas Group

About Us

Cybersecurity &
Crisis Management
Practitioners

Authors, Researchers,
& Educators

Recovering Engineers
& Public Speakers



Cybersecurity Color Wheel©

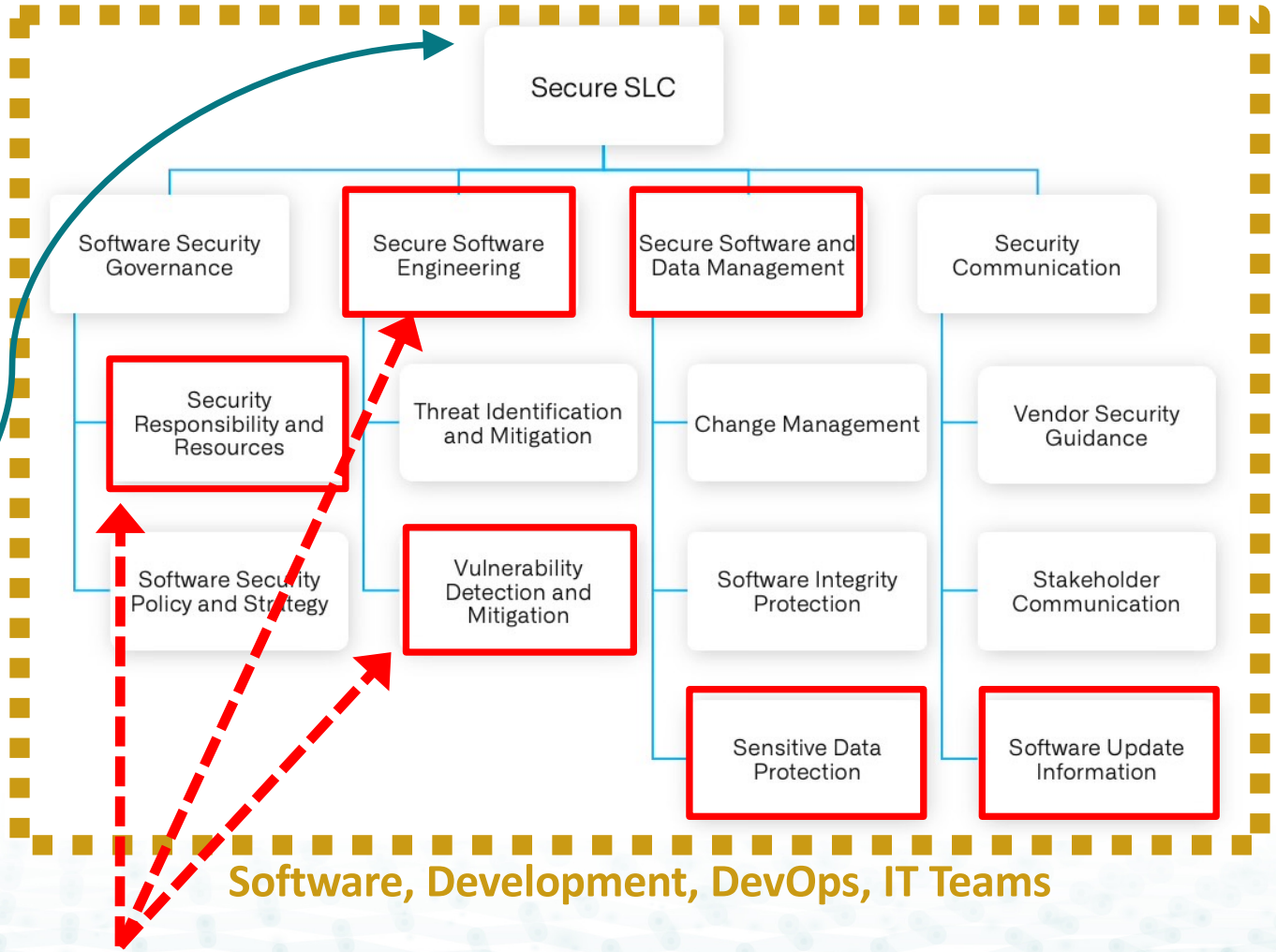
Stuck in the Middle with You

Software is Everywhere

PCI Security Standards Council

PCI Secure Software Framework & SLC

- **Minimize attack surface**
  - Identify critical software assets
  - Secure default configurations
- **Protect software assets via controls**
  - Authentication and access controls
  - Safeguard data at rest & in transit
  - Crypto to secure software assets
- **Secure software operations**
  - Track software activities
  - Detect attacks before they occur
- **Manage Secure SLC**
- **Protect account data**
  - Limit retention of authentication data
  - Protect stored cardholder data



Who's performing these activities?

Not usually the Security Team

Start with Context

- Teams already understand “quality”– leverage that
  - Call security vulnerabilities “bugs” or “defects”
  - Overlay abuse cases to use cases
  - Add security requirements when gathering functional ones

Talk to them about YOUR world, but use THEIR words

Consider all those involved in the entire Software delivery pipeline:

MANAGERS & ANALYSTS	ARCHITECTS	DEVELOPERS	ENGINEERS	IT/OPS
✓ Product	✓ System	✓ Front-end	✓ Cloud	✓ DB Admins
✓ Data	✓ Cloud	✓ Back-end	✓ Security	✓ DevOps
✓ Business	✓ Solutions	✓ UX/UI	✓ Test/QA	

Build Momentum with Hacking

While cool, it's a means to an end

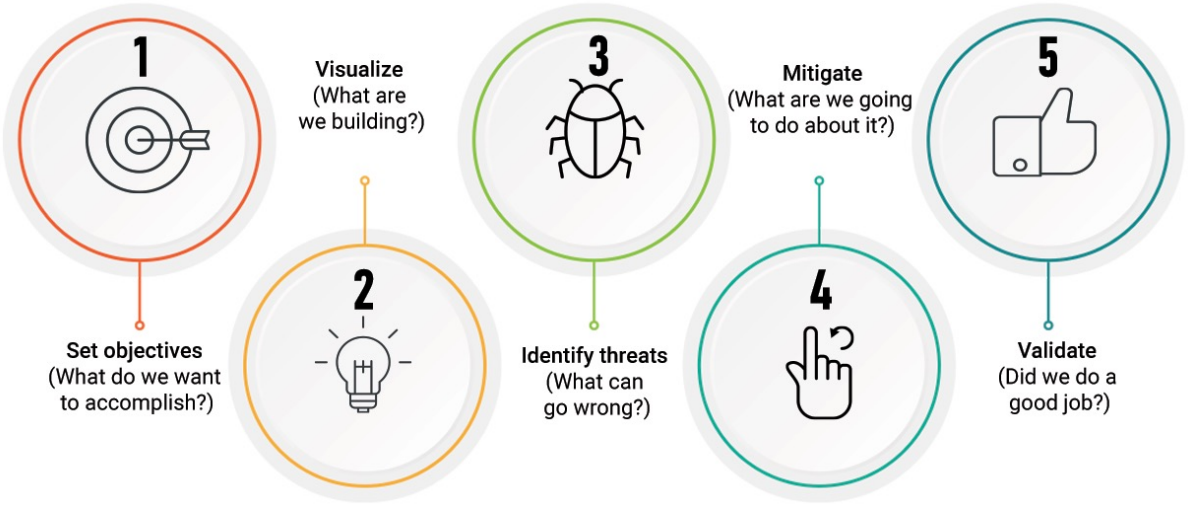
- Goal: develop an attack mentality
- You're creating Yellow Jackets not Hackers
- If your team can't find common vulnerabilities, they're…
  - likely creating them
  - not implementing proper defenses
  - struggling to remediate

"Now when I code, my first thought is, How could I hack this? What if I changed the form input here, would we reject it appropriately?

-Molly Struve, **Site Reliability Engineer**, Netflix

Start Mixing your Palette

- Start slow & small, but very focused (with focus on red)
- Invite/Challenge your teams Learn, Do, and Connect to Job
  - Pick 1 OWASP Top 10, Threat or vulnerability (e.g.SQL injection)
  - Provide easy to consume information
  - SHOW how their stuff can be broken
  - Discuss it in a collaborative forum
- You choose the medium(s) that work best for your team and culture



Help them Learn More

Or Show Them

SQL Injection

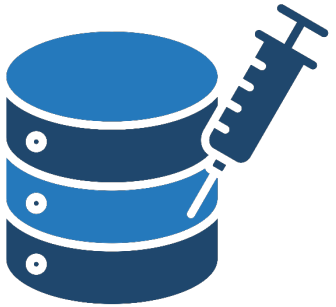
- Be giving....
- Offer a 2-minute video
- Give them context
- If you ask them to do something explain the “why?”
- Don’t like videos? Give them slides, cheat sheets, URLs, books, whatever they want

PCI Security Standards Council

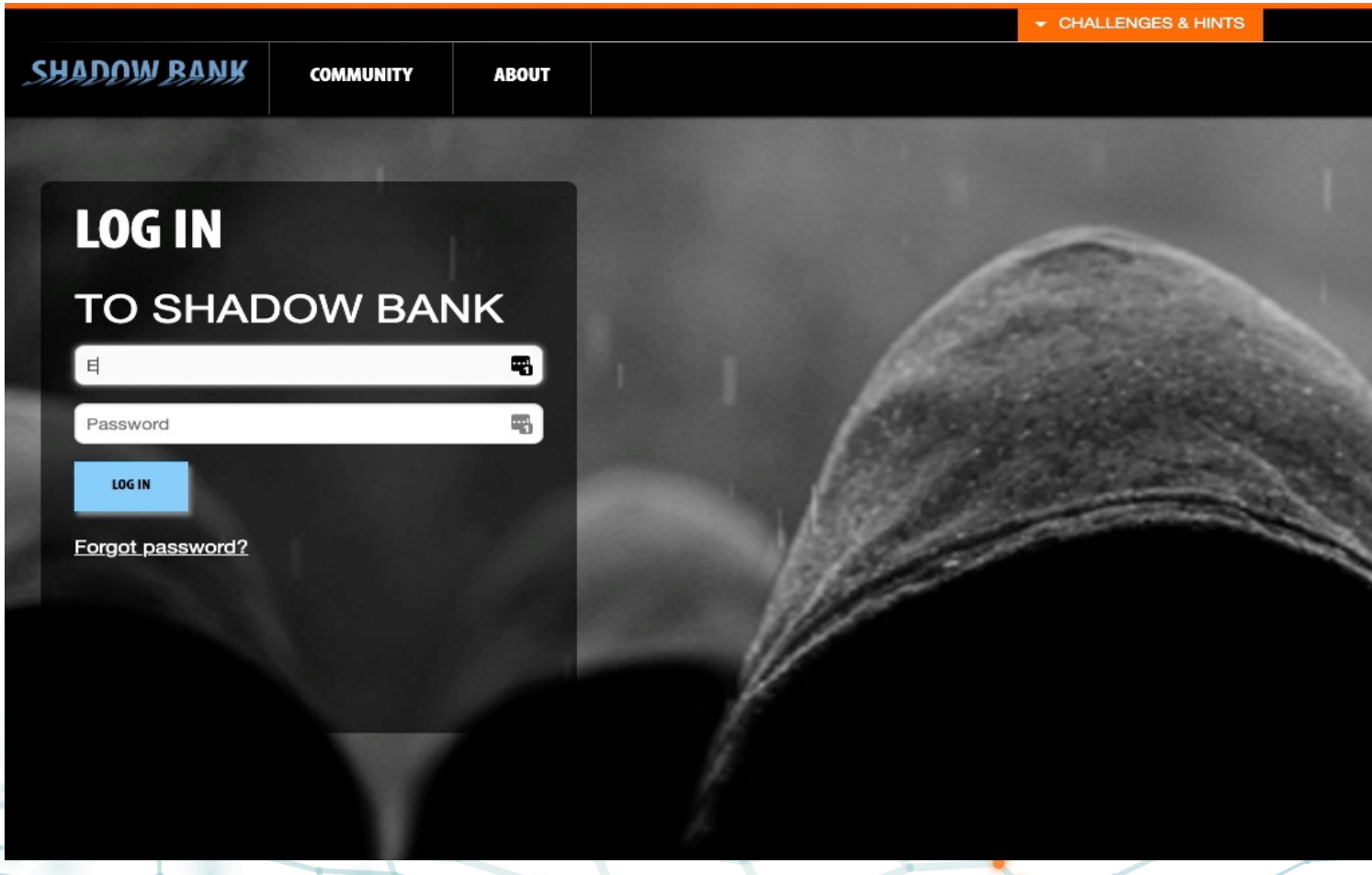
Have them Do

…show them *how* to test their stuff

SQL Injection



- Be nasty. Get a “taste for the blood.”
- Hacking lunch-and-learn
- Instead of “Implement a Zero-Trust Strategy” try… “Watch this!”…and observe the “A-ha!” moment.



PCI Security Standards Council

Connect to their Job

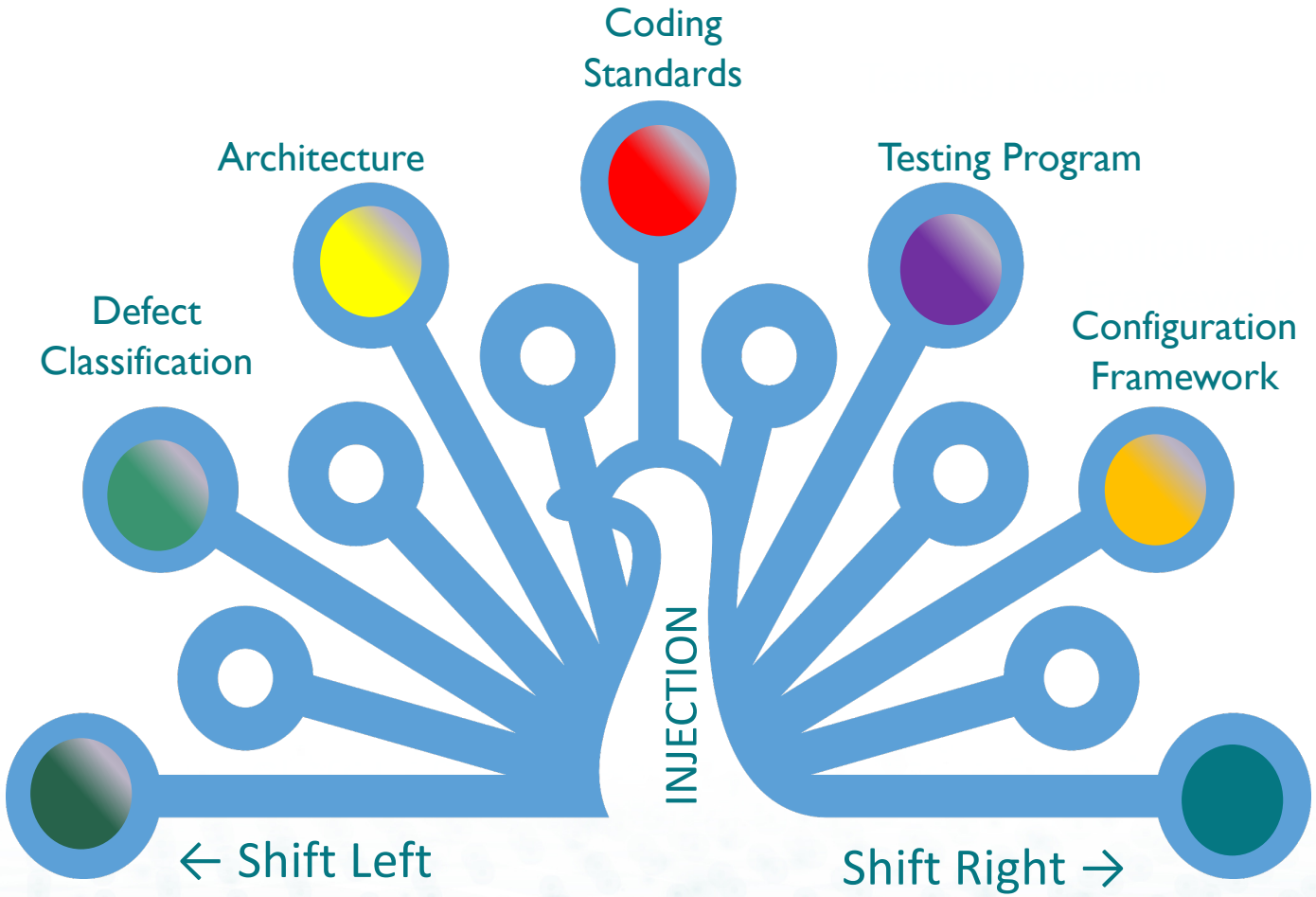
Be Open

- Invite a conversation
- Lead a workshop
- Use analogies
- Talk threat modeling without saying “threat modeling” ☺

Security is like a Peacock

- For each SDLC phase (Yellow's world)
  - Security overlays
  - Job activities
  - Discussions
  - Value-add to other teams
  - Better quality
  - Happier teams

This *IS* the embodiment of the
PCI Secure Software Framework & SLC



PCI Security Standards Council

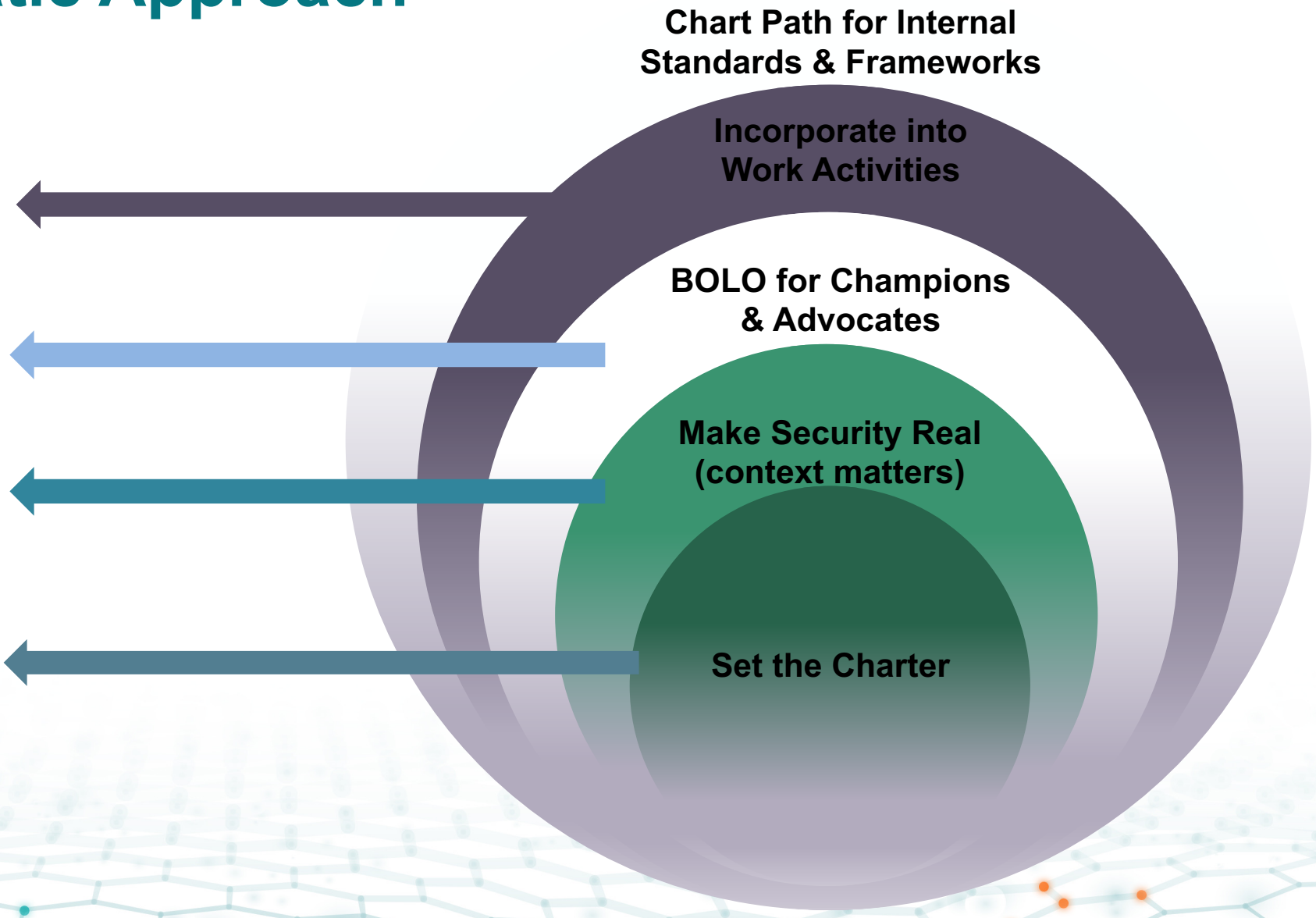
It Takes a Pragmatic Approach

Peer reviews, configuration reviews, etc.

Instant Credibility with IT Teams

Get teams thinking (and excited) about security

Management Support



Proof Points

We can now implement defenses, expedite features, and improve resiliency”

Trupti Shakalrar
AppSec Director, Illumio

“Our belt program allowed engineers to diagnose & remediate vulnerabilities fast”

- Alex Rueben
Chief of Staff, Cyber Security, Citrix

“Hands-on hacking opened our teams eyes”

- Satish Janardhanan
Co-head AppSec, Acccenture

“Security champions in a product team is really valuable”

- Alex DeDonker
Program Manager, Microsoft

CITRIX

Microsoft

illumio

accenture

PCI Security Standards Council

SECURITY INNOVATION

Thank You

Questions?

www.edtalks.io

getsec.in/PonemonReport

PCI Security Standards Council


PCi
Security
Standards Council
®