Alyssa

MILLER

A Pitmaster's Guide To Security Design

Conquering the Brisket and Securing your Enterprise

Hacker/Researcher

Security Advocate

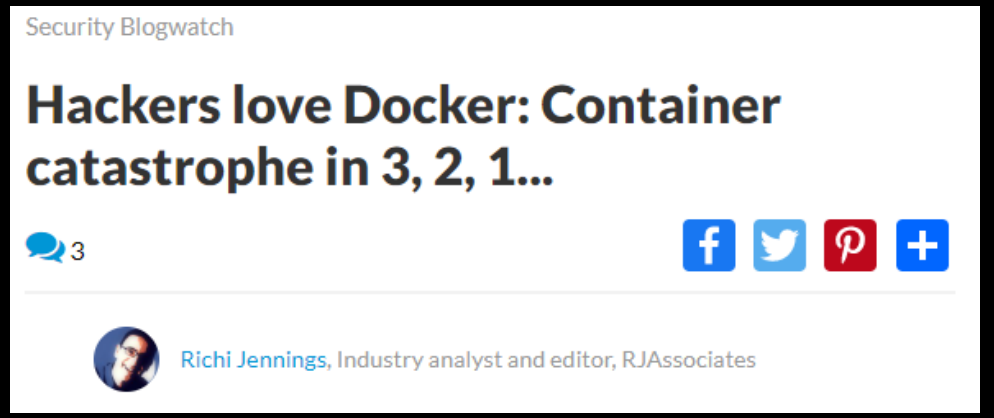
Author & Blogger

Co-Host: Uncommon Journey

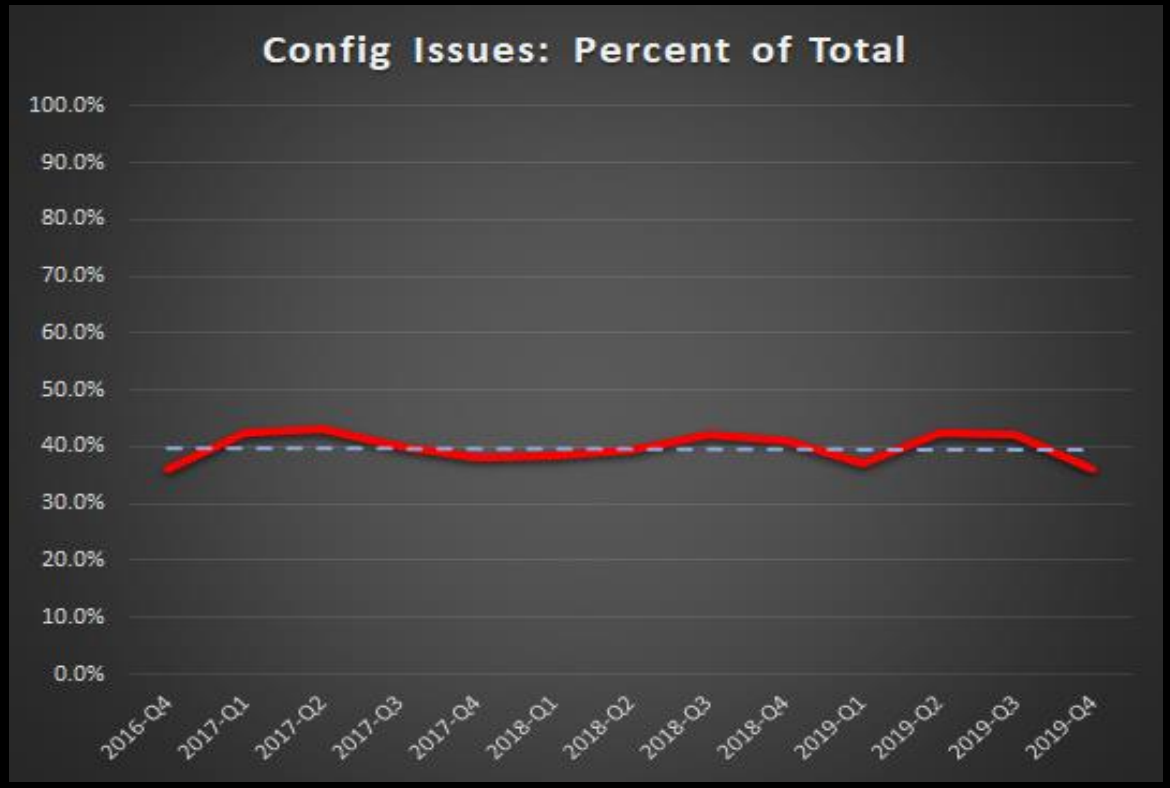
snyk


OKLAHOMA
JOE'S
Alyssa
MILLER

Breach Trends

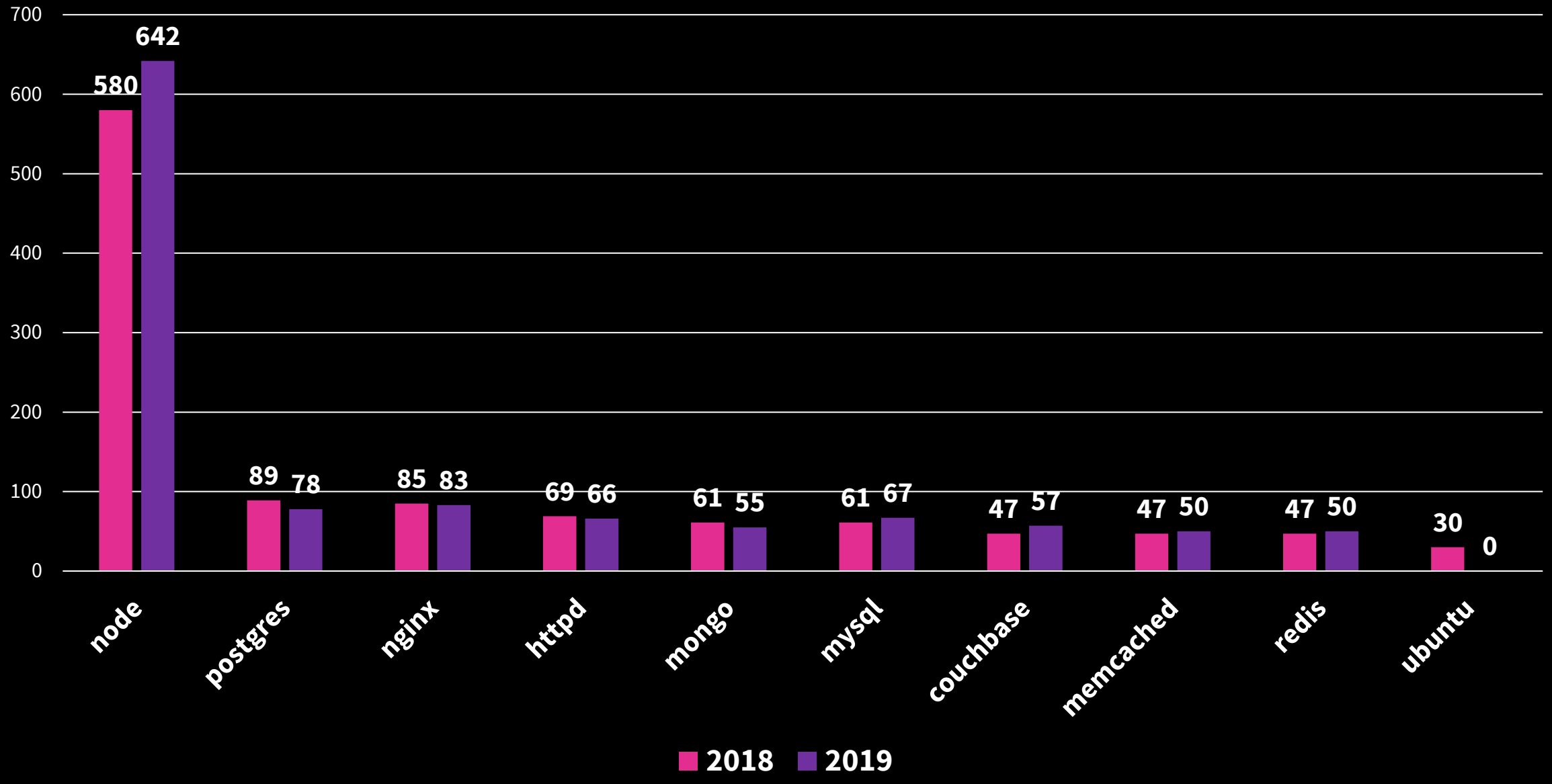


Top 5 Vulnerability Themes	
Configuration Management	**40%**
Account Management	27%
Patch Management	13%
Authentication Weaknesses	7%
Software Lifecycle	5%

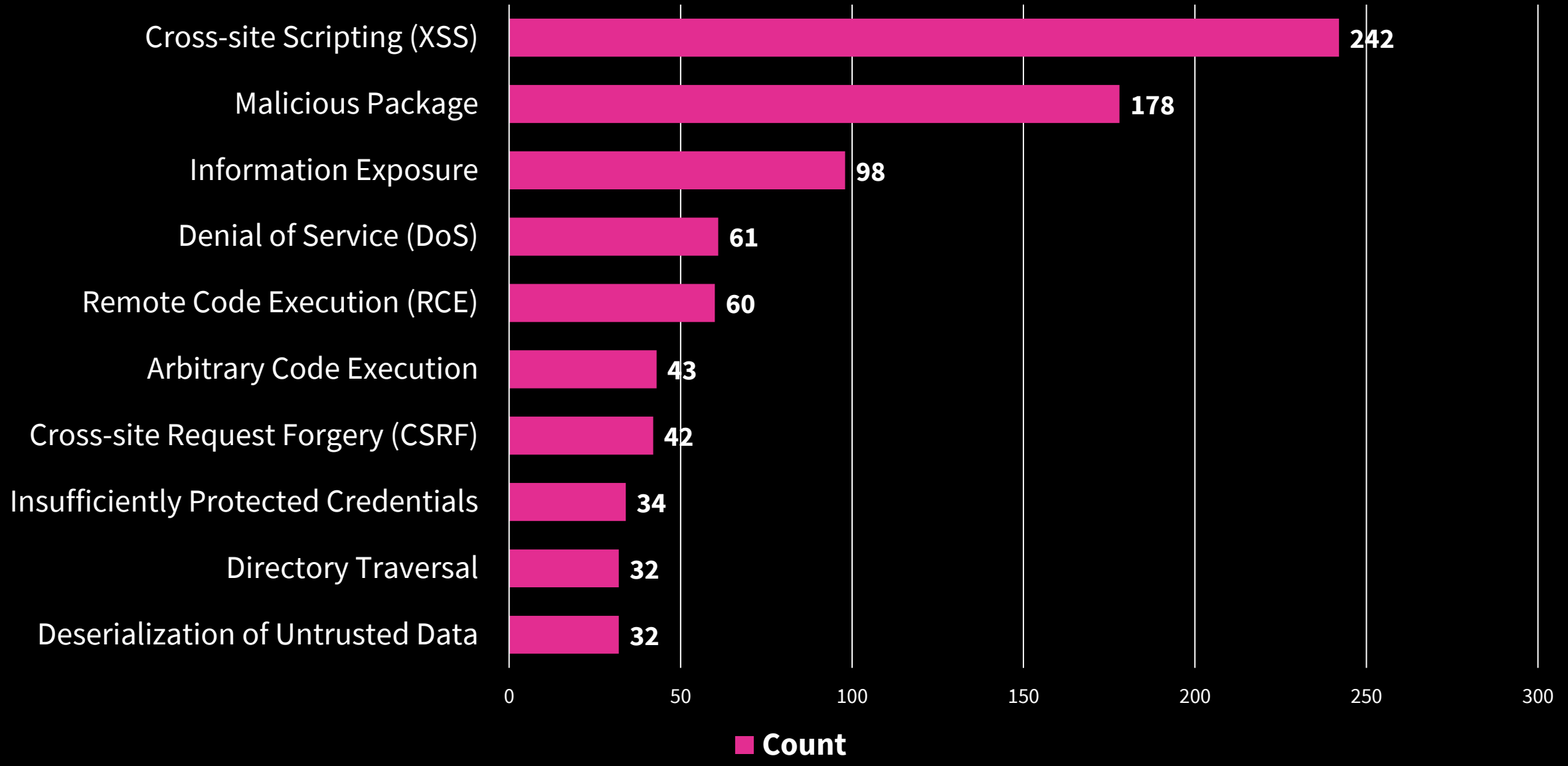


Source: CDW Information Security Assessments Practice (2017-2019)

Vulnerabilities in Official DockerHub Images



Vulnerabilities Reported in open source packages - 2019




So let’s get that brisket on and build a better security program…


Pitmaster Rule #1:
Planning and preparation
wins the day

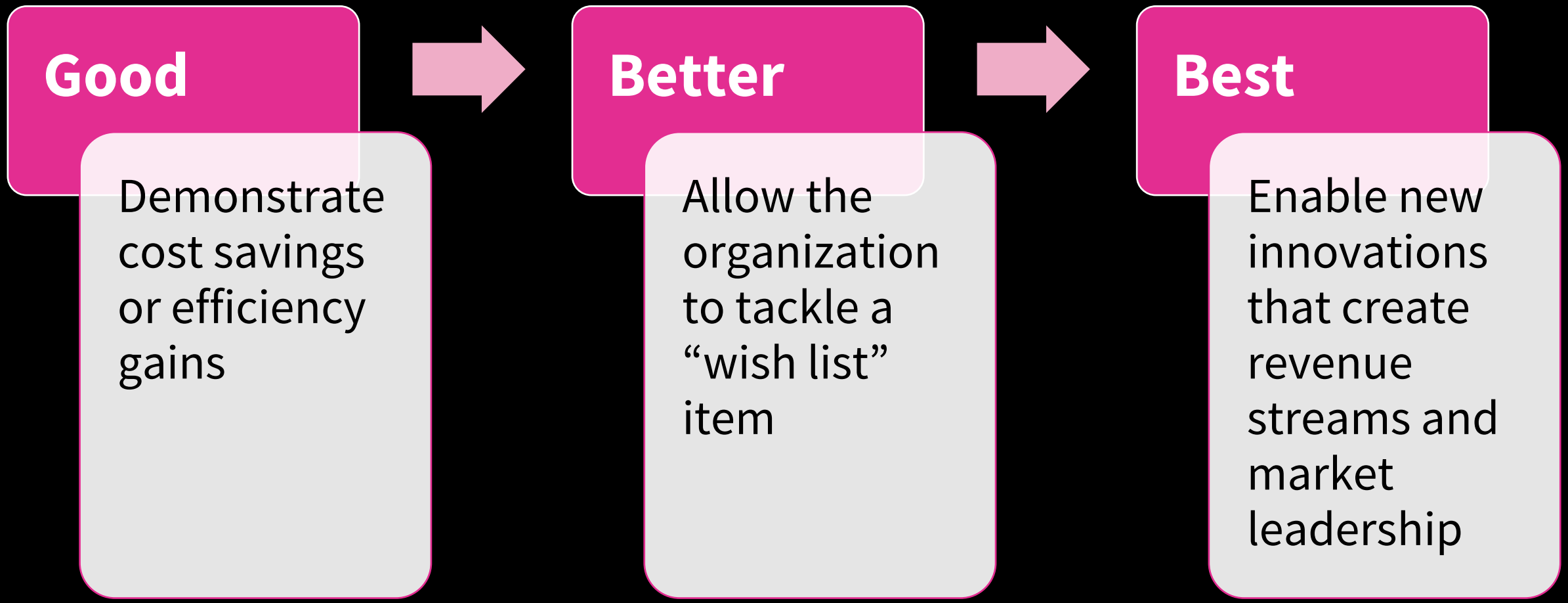
Fear,
Uncertainty,
Doubt!

Discourage Action

Threats & Fear

Encourage Action

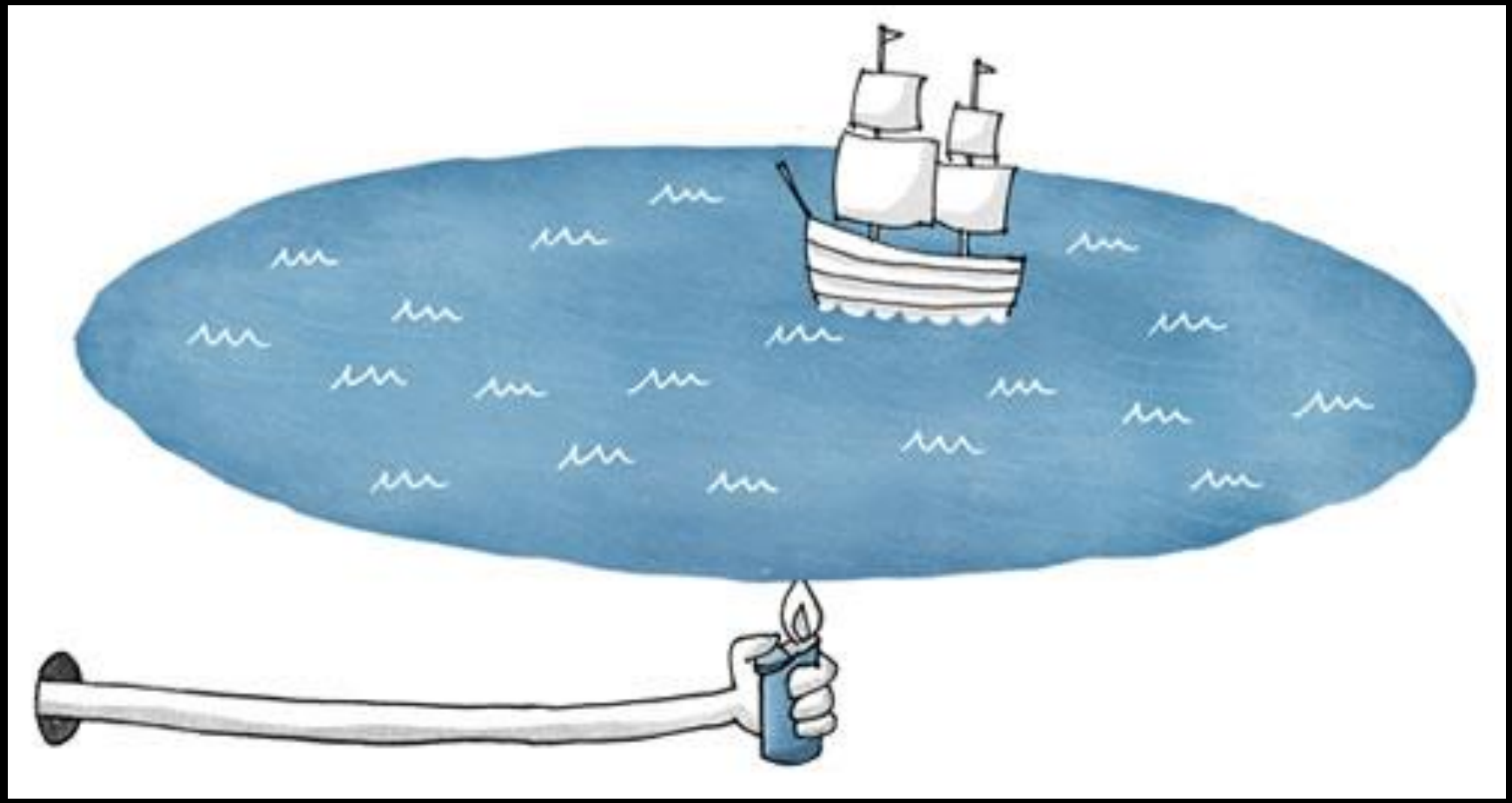
Rewards


Good
Demonstrate cost savings or efficiency gains
Better
Allow the organization to tackle a “wish list” item
Best
Enable new innovations that create revenue streams and market leadership

Talking up the chain...

Pitmaster Rule #2: Low and slow, you can’t rush it

You can’t secure everything tomorrow



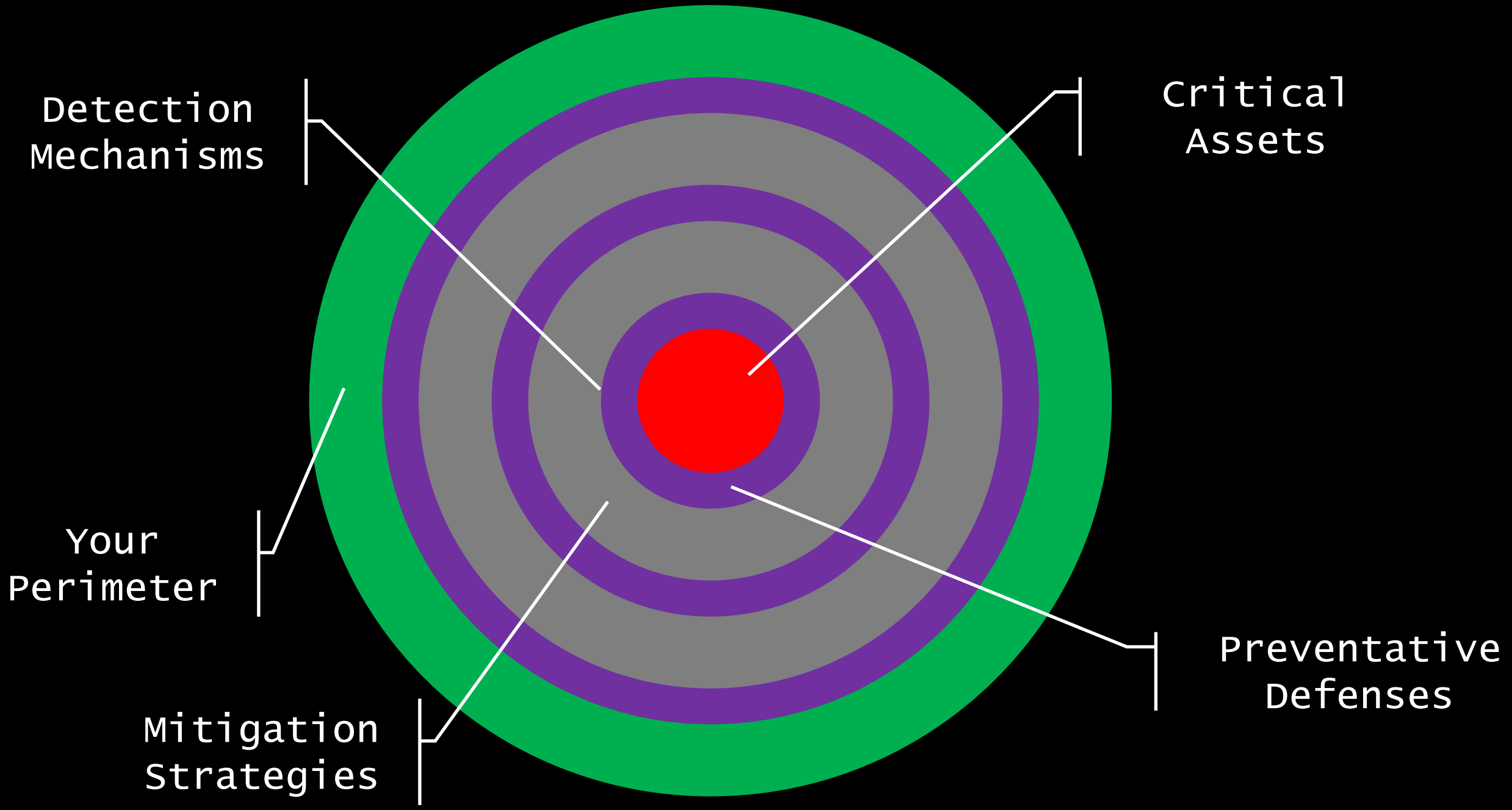
PRIVATE DATA

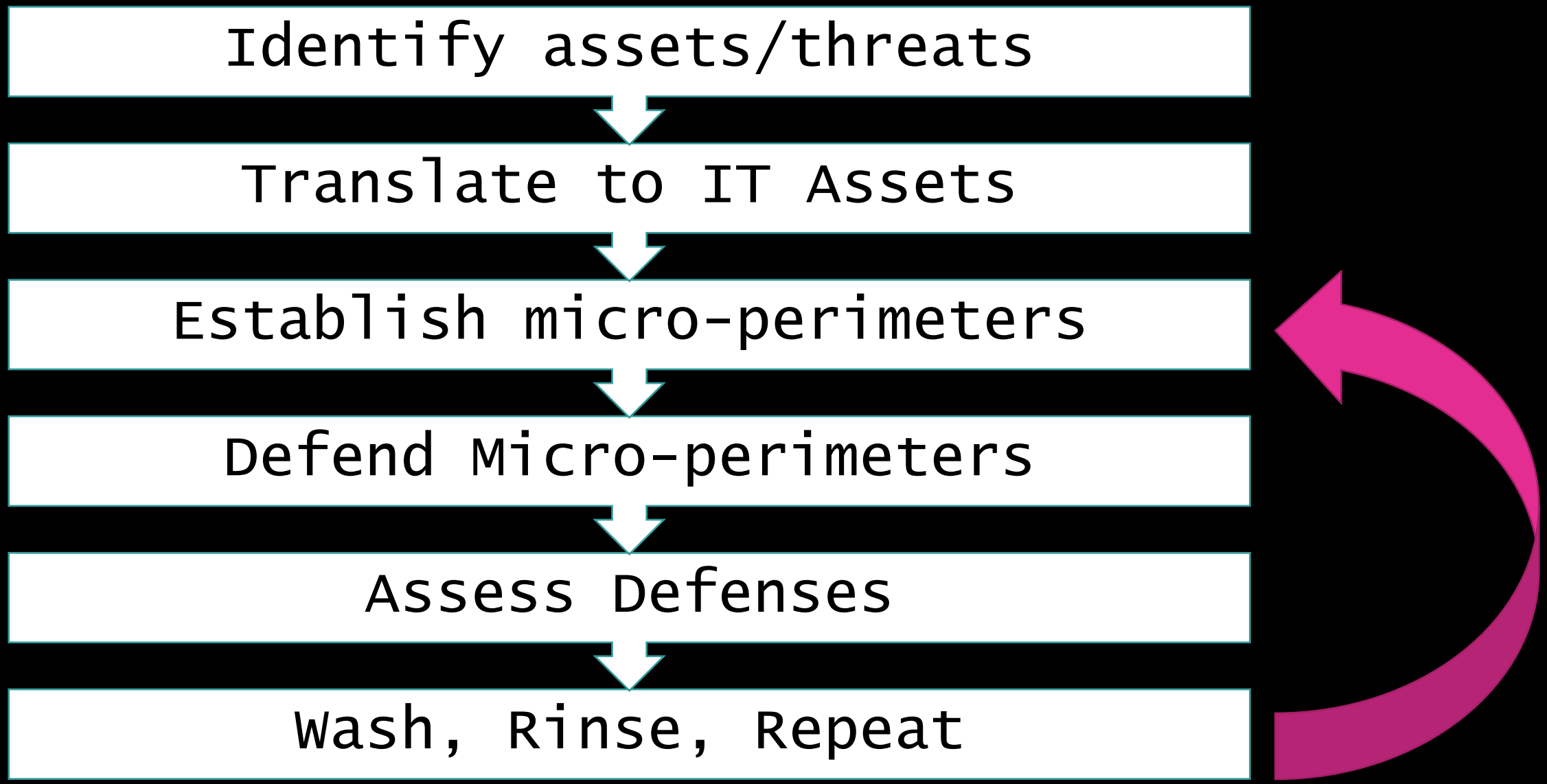
CRITICAL FUNCTIONS

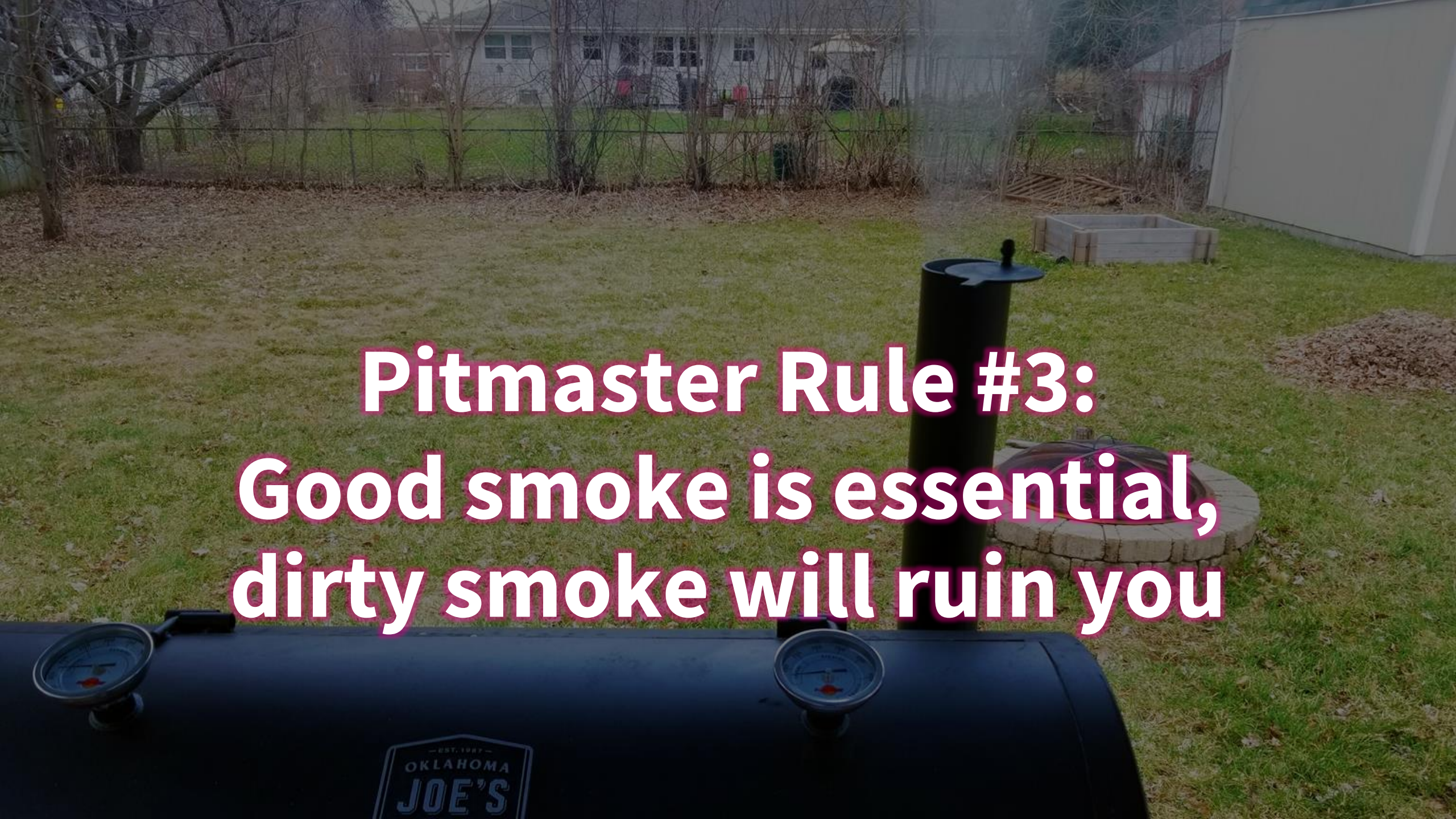
FINANCIAL ASSETS

PEOPLE ASSETS

SECRETS

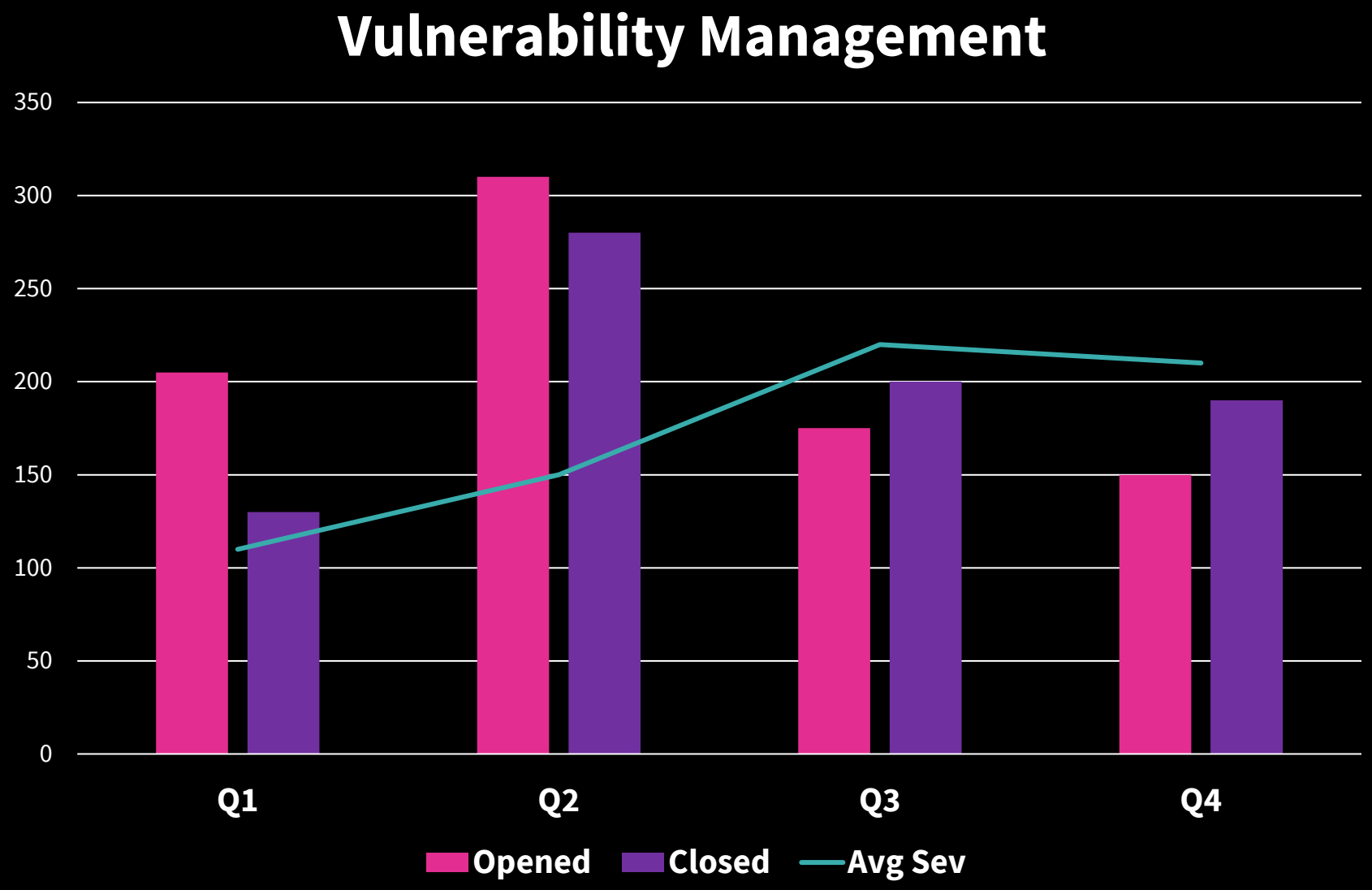

Detection Mechanisms
Critical Assets
Your Perimeter
Preventative Defenses
Mitigation Strategies


Identify assets/threats
Translate to IT Assets
Establish micro-perimeters
Defend Micro-perimeters
Assess Defenses
Wash, Rinse, Repeat


Pitmaster Rule #3:
Good smoke is essential,
dirty smoke will ruin you
OKLAHOMA
JOE'S

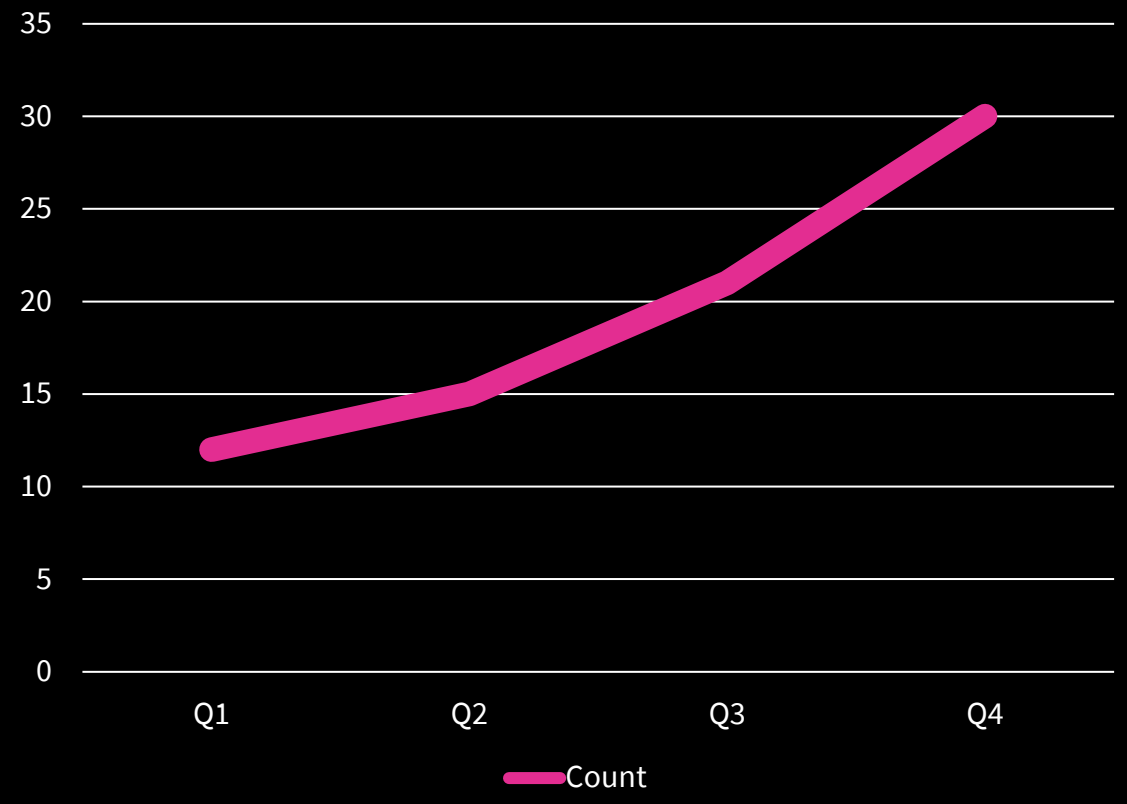

EST. 1907
OKLAHOMA
JOE'S

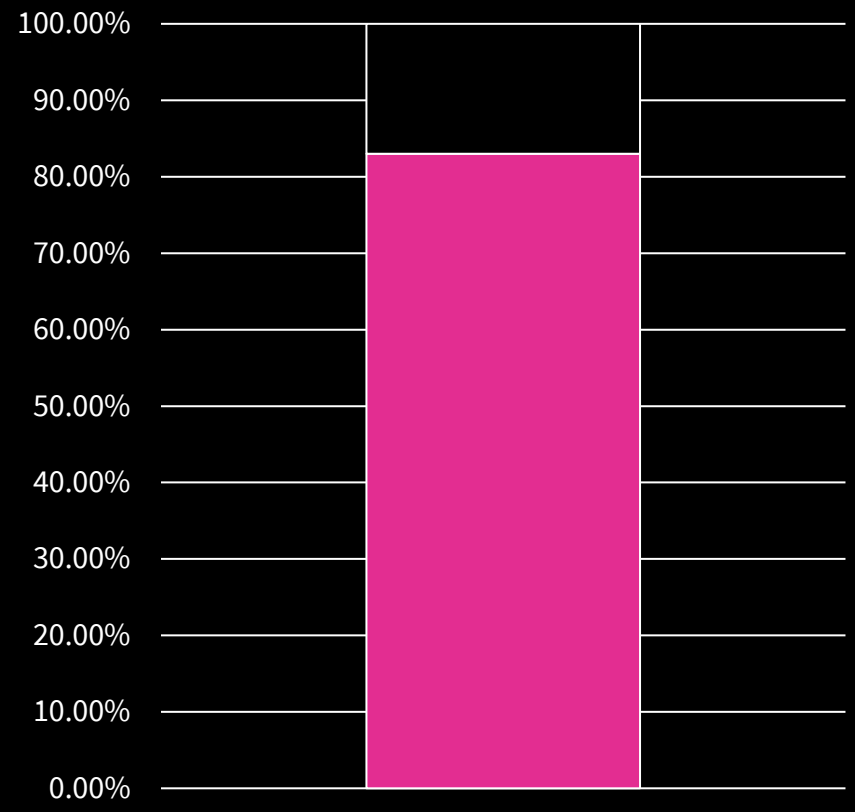
Accurate and effective metrics...



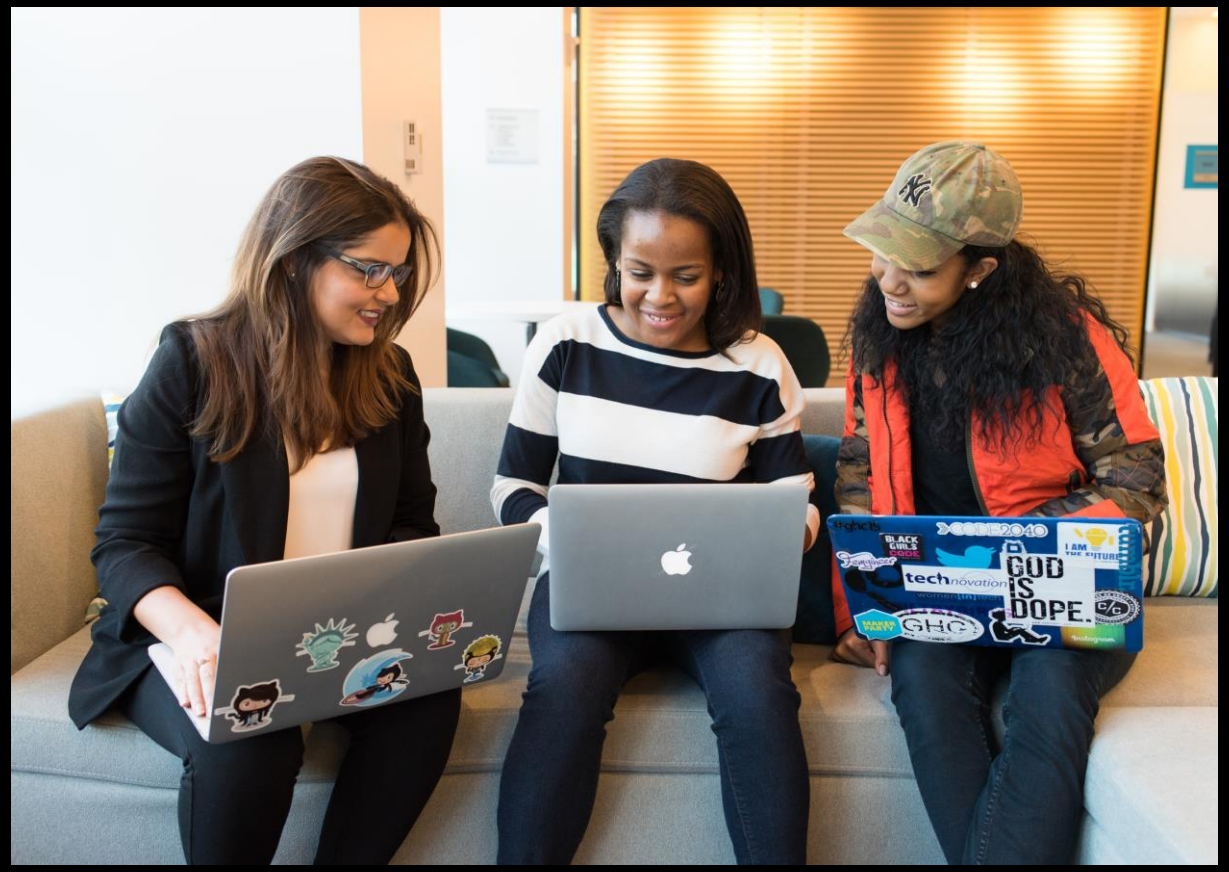
Goals...

Improvement > Attainment

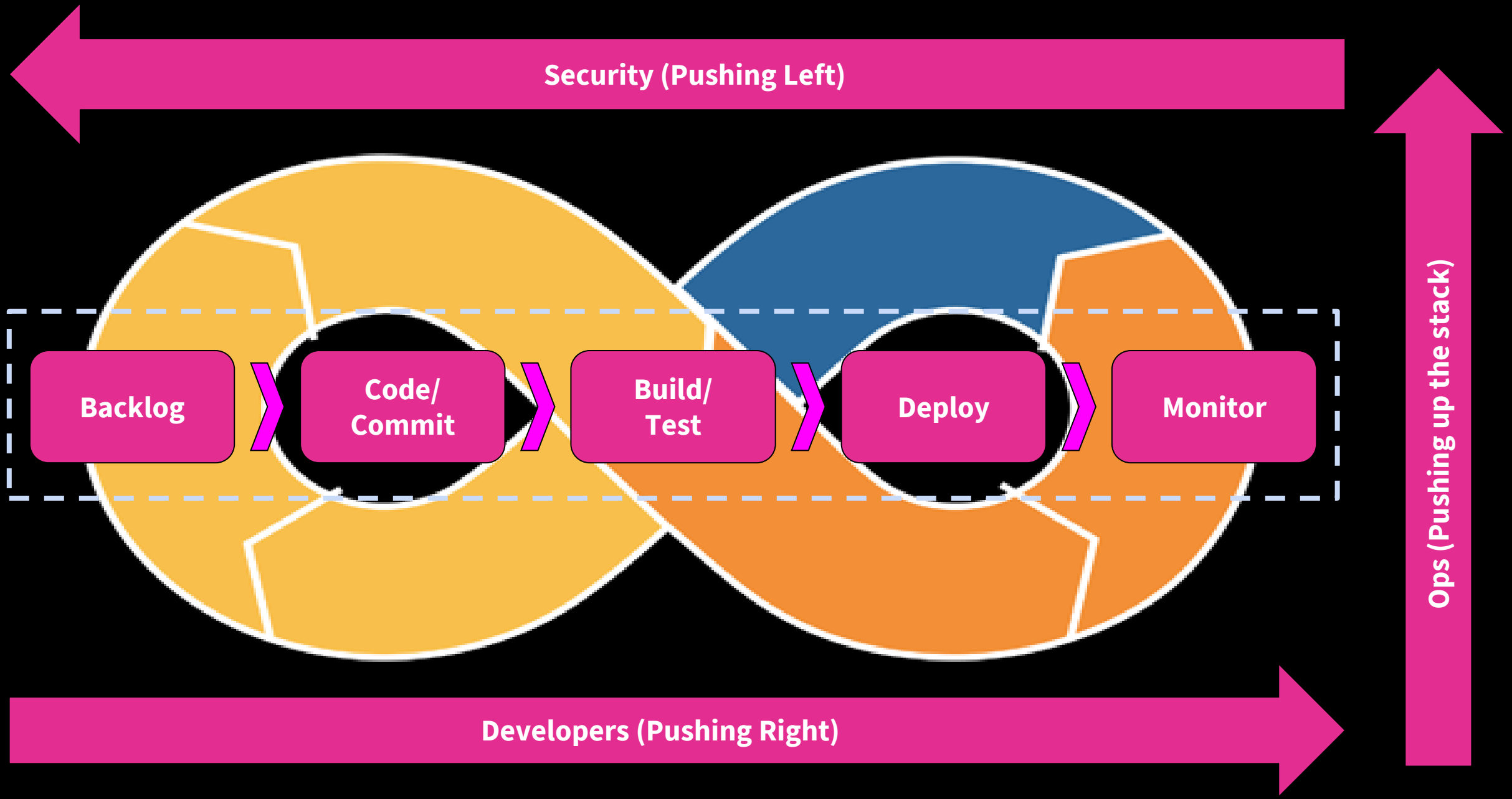




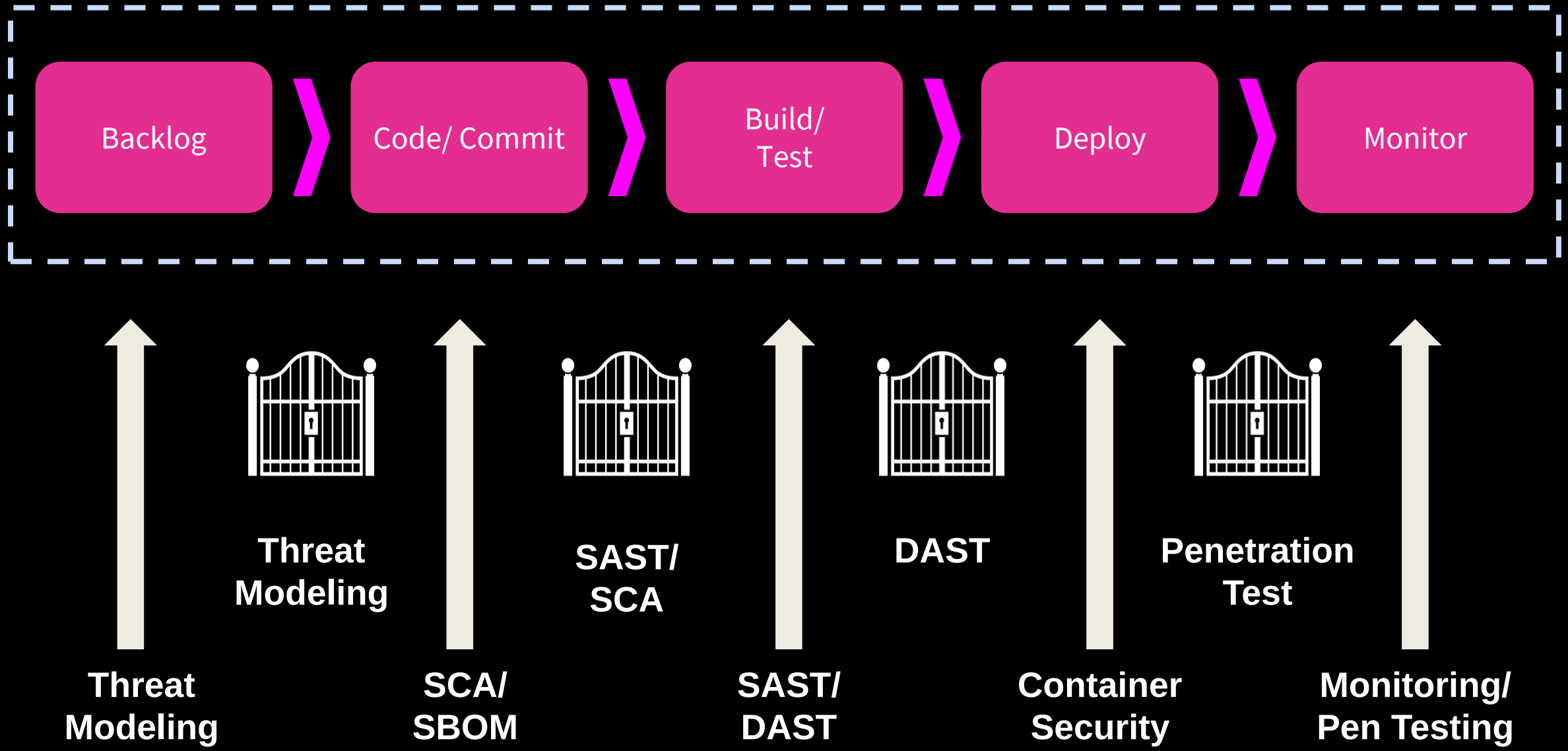
Audience...




Pitmaster Rule #4:
There is no set it and
forget it


Security (Pushing Left)
Backlog
Code/
Commit
Build/
Test
Deploy
Monitor
Ops (Pushing up the stack)
Developers (Pushing Right)

Frictionless Enablement...



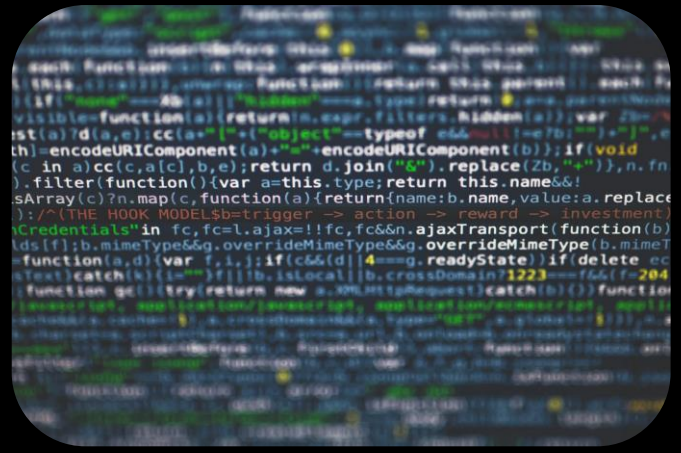
Meet them where they live…

Walk-a-Mile In Their Shoes

Job shadow / Dev, Sec, and Ops / Build empathy

Mutual Engagement

Connect Daily Activities Across Disciplines



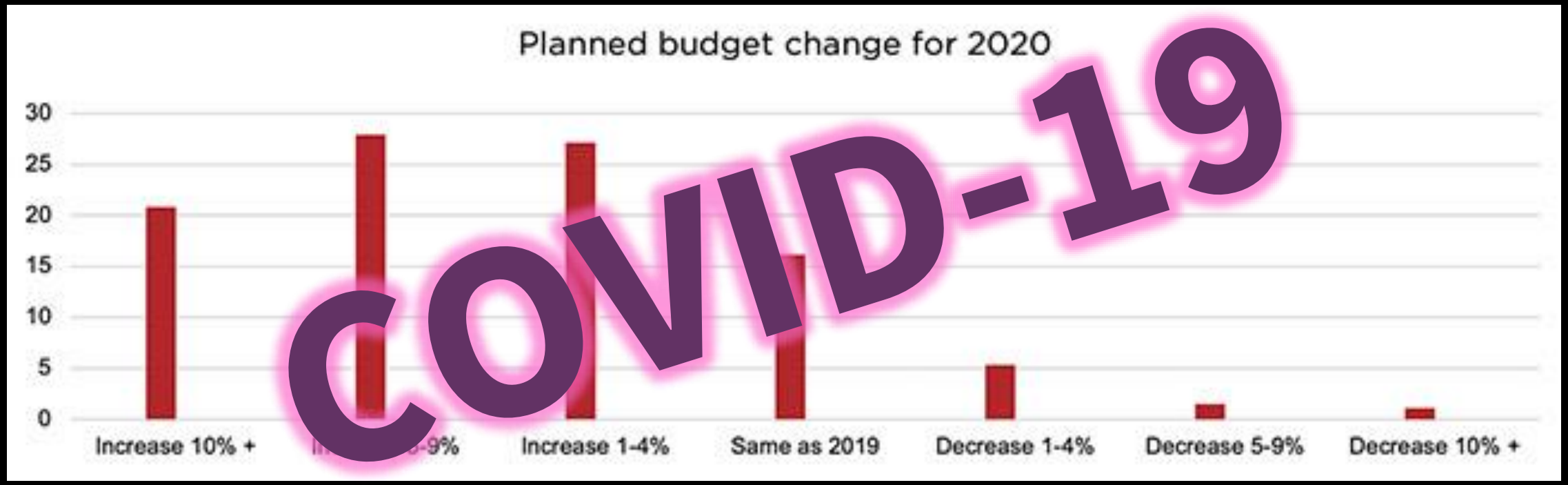
Pave the Road

Automation / Tool Selection / Accountable Trust

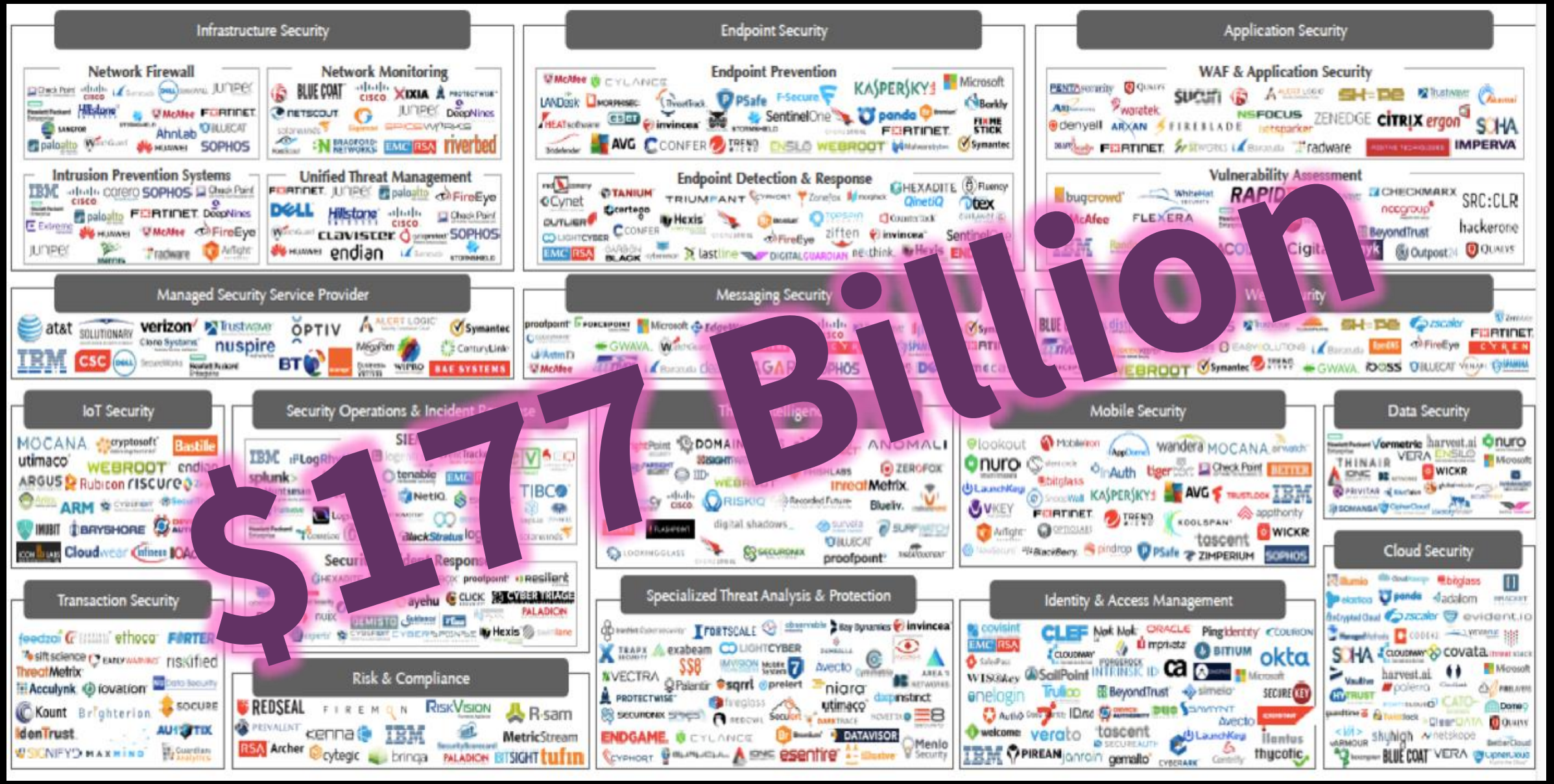
Pitmaster Rule #5: Know your tools, abilities, and limitations


OKLAHOMA
JOE'S
Alyssa
MILLER

Security Budgets for 2020...



Source: Fireeye - https://www.helpnetsecurity.com/2019/11/06/cybersecurity-budgets-2020/


Infrastructure Security
Network Firewall
Network Monitoring
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Messaging Security
IoT Security
Security Operations & Incident
Mobile Security
Data Security
Transaction Security
Risk & Compliance
Specialized Threat Analysis & Protection
Identity & Access Management
Cloud Security
$17 Billion

60+ Tools in use

35% Tools overlap

80% Underutilized

Source: https://www.msspalert.com/cybersecurity-research/fireeye-mandiant-report-2020/

Bring it all together…

1. Planning and preparation wins the day
2. Low and Slow, you can’t rush it
3. Good smoke is essential, dirty smoke will ruin you
4. There is no set it and forget it
5. Know your tools, abilities, and limitations

1. Win executive sponsorship by driving business value
2. You can’t secure everything tomorrow
3. Your program will fail if you can’t measure it effectively
4. Build a culture of enablement and accountability
5. Maximize existing tools, don’t chase fads


Bon Appetit...

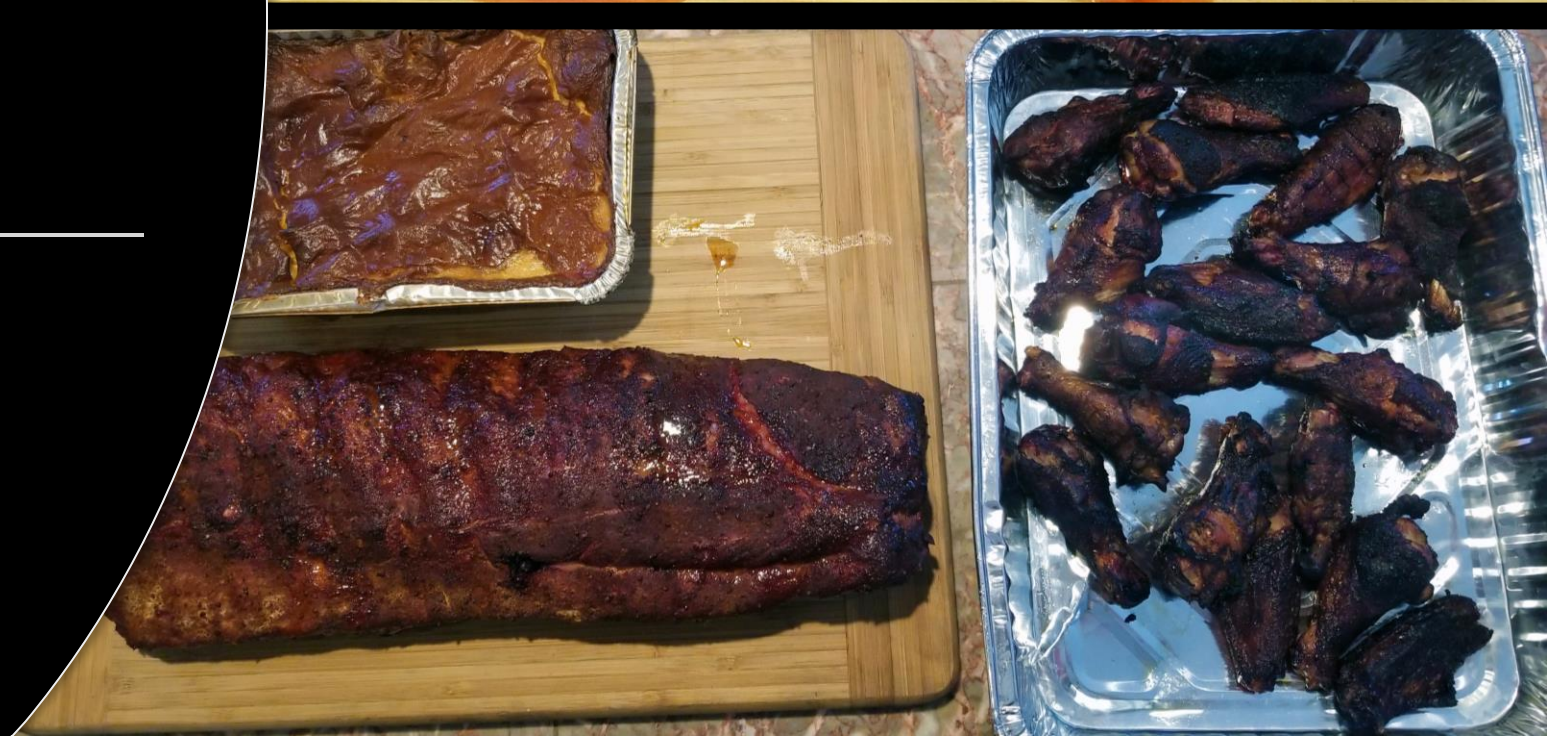
All things tasty...

https://github.com/r4v1np1nk/HackersKitchen

https://barbecon.com/

#HackerBBQ

#HackersKitchen



@AlyssaM_Infosec

/in/alyssam-infosec

https://alyssasec.com

Thank You

Alyssa

MILLER