$how me the Dev$ecOp$

Mark Willis, Director, Software and Mobile Security

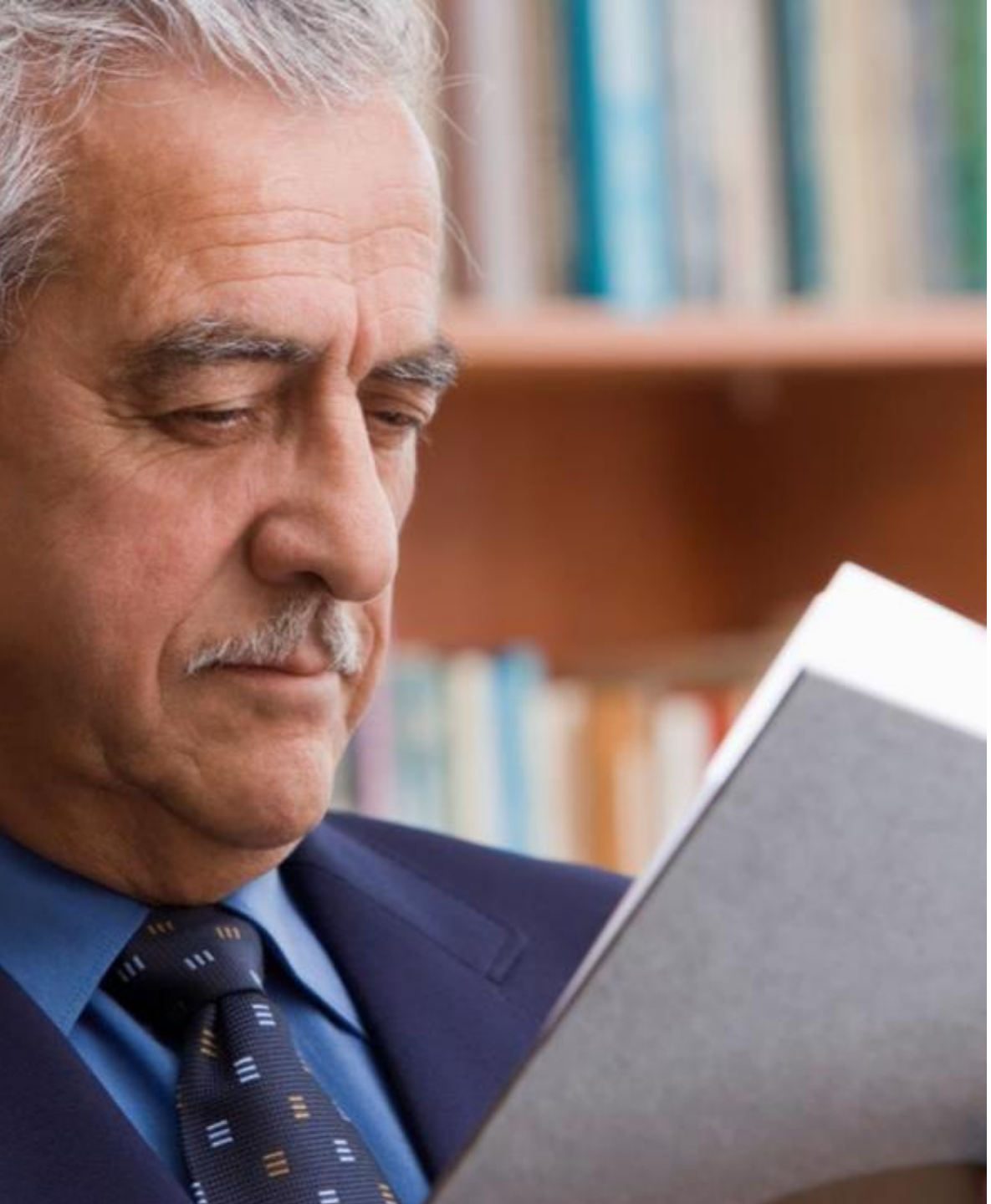
October 2018

“You build it, you run it.”

Werner Vogels

“You build it, you secure it.”

John Willis



Agenda

What is Dev$ecOp$?

- Moving from the imaginary to the real
- Quantifying the value of your DevSecOps Program

Disclaimer

This presentation is coming at you from a security vulnerability point of view but, don't worry,

This formula can be applied to all defects! ☺

Dev$ecOp$ can help you…

- Transform from cost center into a revenue center
- Determine your cost per defect (CPD)
- Build consensus across the enterprise
- Provide key decision makers options

What is Dev$ecOp$?

aetna®

What is Dev$ecOp$?

Imagine a world where you hear:

> "Hey, can anyone tell me the value of implementing a DevSecOps program?" or…
>
> "Are we really saving any money by moving to a DevSecOps program?"

- For many of us, these questions are a reality – and you've probably heard them more than once!

- So…what if you were able to say:

  "Yes, I can tell you the value of implementing a DevSecOps program….let me show you how…."

Transforming from a cost center to a revenue center

aetna®

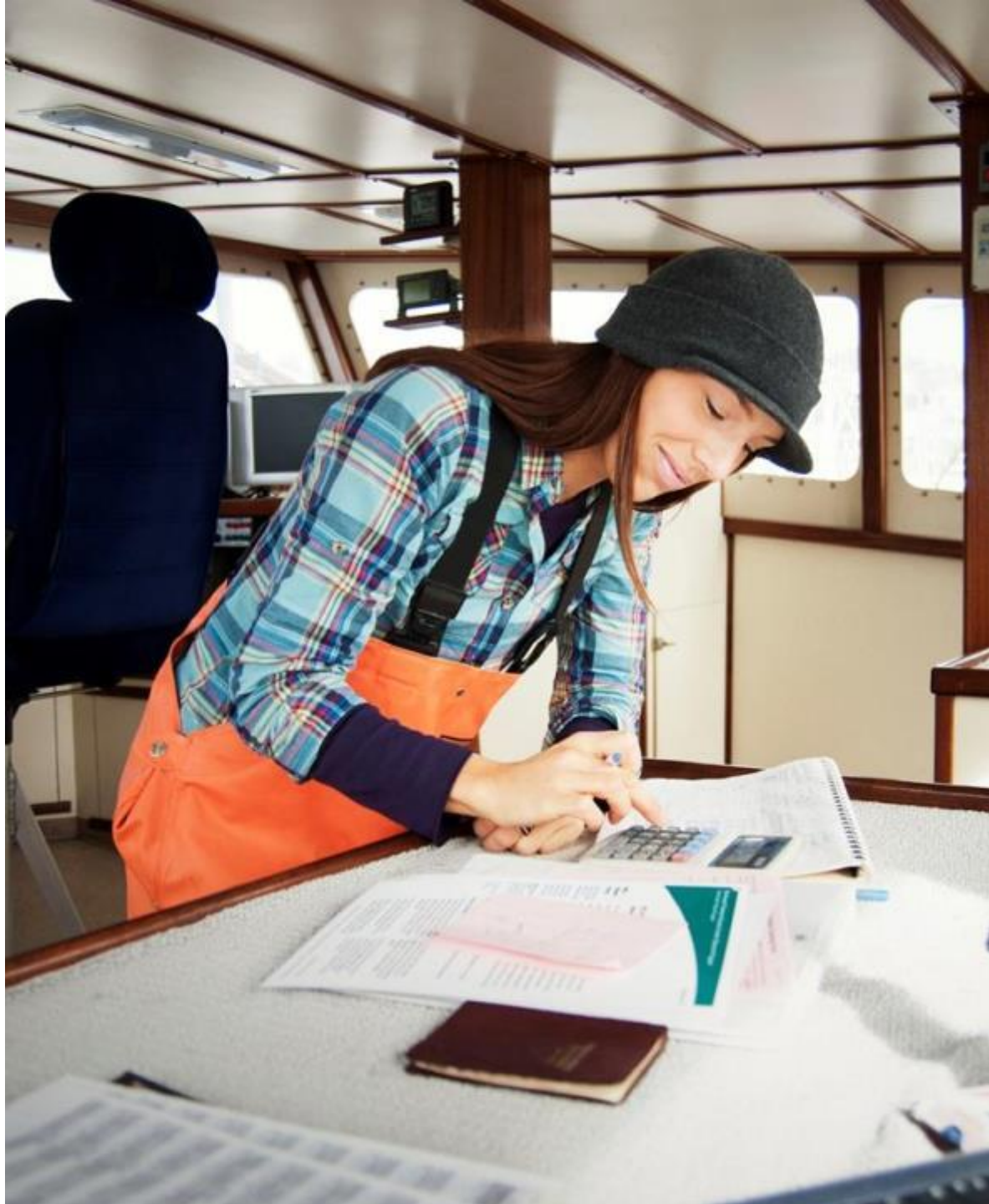
Cost center → revenue center

Measuring progress

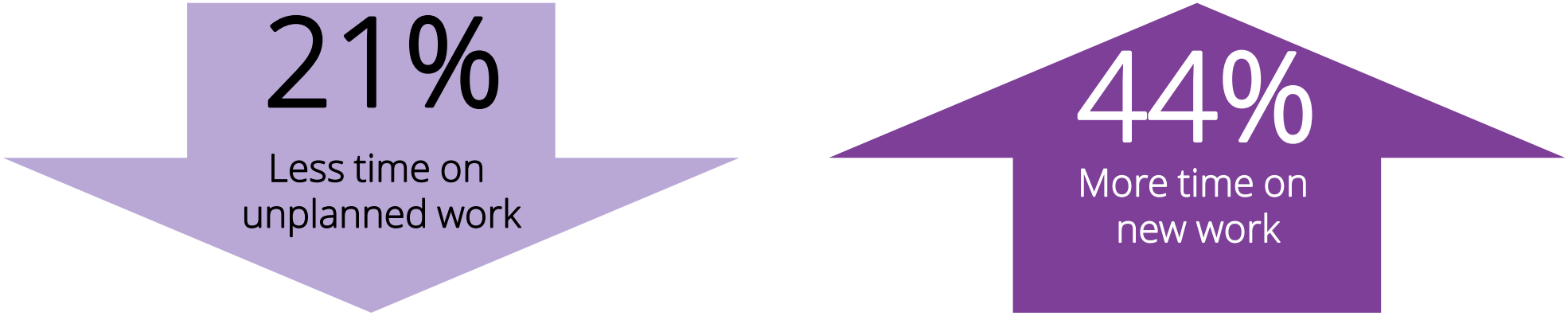
- Cost per defect consensus
  - Vital to ensure success
  - Must occur between app dev and security
- Number of defects in scope (critical and high)
- Cost per defect
- Annual (current) cost of remediation

Provides a range of estimated revenue savings

- Liberal
- Conservative
- Very conservative



Benefits of adopting a DevSecOps program



46x Improvement in deployment frequency

440x Faster lead time for changes

96x Faster mean time to recover (MTTR)

5x Lower change failure rate (1/5 as likely)

Determining the value of Dev$ecOp$

aetna®

Determining the value of Dev$ecOp$

Introducing: The Dev$ecOp$ Triad

- Application Development, Finance, & Security

Goal: Build consensus across the enterprise

Application Development

- Empathy is key, for they are the ones fixing the defects
- Lock in commitment to remediate defects

Finance

- They should be able to provide remediation costs from last year
- If not, find out how much it cost to fix all defects in 2017

Security

- Provide the best practices and tools
- Forget about the cost of tools and software
- Don’t let these costs be red herrings!

Number of defects in scope

aetna®

Number of defects in scope

The Dev$ecOp$ Triad in action:

Goal: Agreed upon number of defects in scope

Application Development

- Realistic look at what lies ahead
- Past: How many defects did we fix?
- Present: How many defects *can* we fix?

Finance

- What was last year's budget to fix our defects?
- What *is* the budget to fix our defects?
- Is there a budget?
- If so, can it be increased?

Security

- Commitment to tools, testing, and training
- Commitment to a super low defect density
- Defect density = # of vulns x 10k / lines of code

Annual cost of remediation

aetna®

Annual cost of remediation (ACR)

Working with the Finance team

- The key to understanding your annual cost of remediation (ACR) is identifying last year's budget to fix our defects

Working with the Application and Security teams

- How many defects were fixed last year?
- **Make a note of this #, you'll need it soon…

  And we'll call it the Number of Defects (NOD)

Cost per defect (CPD)

aetna®

Cost per defect (CPD)

Now, you can calculate your cost per defect!

- ACR from last year divided by NOD from last year
- ACR/NOV = cost per defect (CPD)

Now that you have the CPD, you can:

- Figure out what current year budget would be with the current CPD x NOD for this year
- Figure out how much Dev$ecOp$ will save (discount) your organization by presenting three levels of estimates:
  - Liberal (75% CPD discount)
  - Conservative (50% CPD discount)
  - Very Conservative (25% CPD discount)

Moving from a cost center to a revenue center

aetna®

Cost center → revenue center

Practical application of the formula in action – hypothetical situation, mileage may vary…

Status	# of apps	# of defects (NOD)	Annual cost of remediation (ACR)	Actual cost	Annual savings	Cost per defect (CPD)	Annual savings
Current model	10	100	$200,000	$200,000 (defects x current CPD)		$2,000.00	Current CPD
DevSecOps	10	100	$200,000 (findings x current CPD)	$50,000 (defects x liberal CPD)	$150,000	$500.00	Liberal
DevSecOps	10	100	$200,000 (findings x current CPD)	$100,000 (defects x conservative CPD)	$100,000	$1,000.00	Conservative
DevSecOps	10	100	$200,000 (findings x current CPD)	$150,000 (defects x very conservative CPD)	$50,000	$1,500.00	Very conservative

Thank you!

Questions?

aetna®