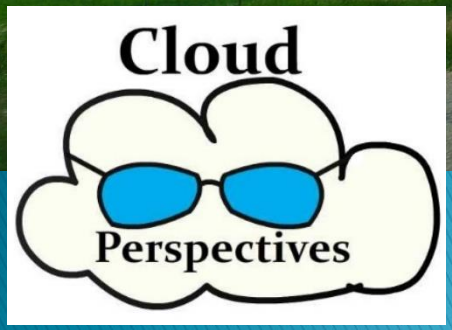
DevSecOps – Delivering Value Faster?

Metrics and Standards

Steven Woodward CCSK, CFPS, CSQA
steve@cloud-perspectives.com
613-698-5240
www.cloud-perspectives.com



DevSecOps Days – October 1 2020
Software Engineering Institute
Carnegie Mellon University

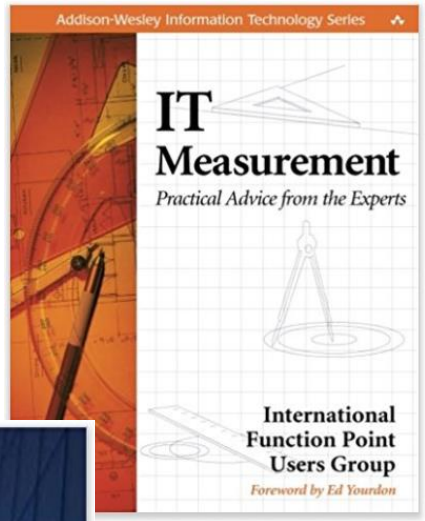
Agenda

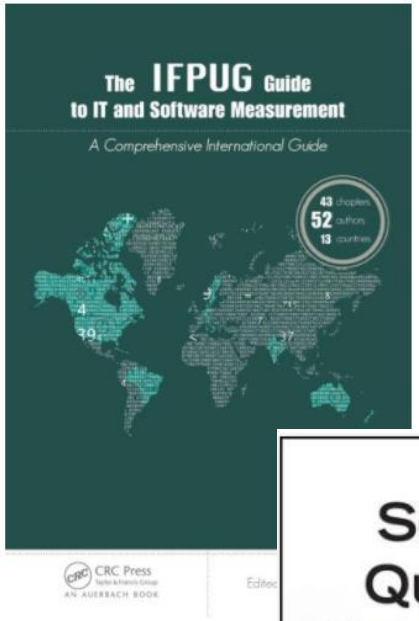
- Intro
- Context Is Everything
- Goals, Objectives, Outcomes
- Why Standardization Matters
- DevSecOps and Metrics
- Closing Perspectives and Context

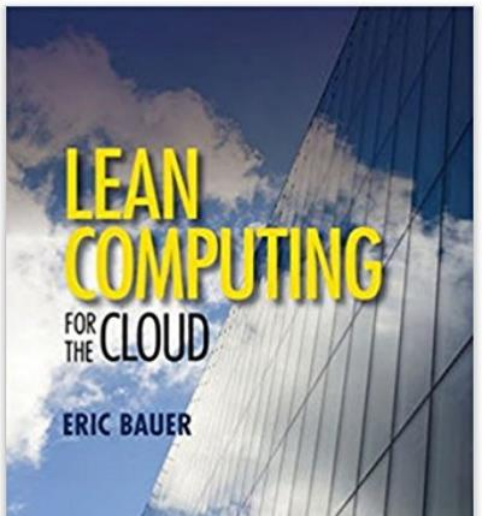
Cloud Perspectives – Steve Woodward

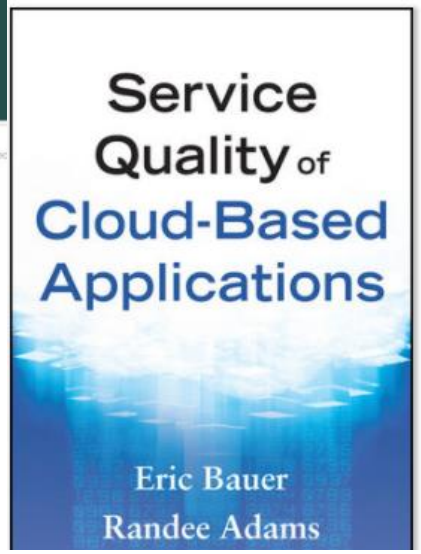
- ISO/ IEC – JTC1 Member, liaison between SC7 Systems & Software and SC38 Cloud & Distributed Systems (SLAs, Connectivity, DevOps)
- IEEE 2675 DevOps and DevSecOps
- IEEE P2302 with NIST – Cloud Federation
- IEEE 2430 – Non-Functional Sizing
- IFPUG – (software sizing) – Former Standards Chair & Director
- NIST – Lead Cloud Audit and Carrier
- Cloud Security Alliance – Standards Committee & DevSecOps & Director
- OMG CSCC – Lead Metrics, Roles, Resources
- Standards Council of Canada (Ethics, Data Governance, GDPR)
- Collaboration between various SDOs and communities

Additional Books









Agenda

- Intro
- Context Is Everything
- Goals, Objectives, Outcomes
- Why Standardization Matters
- DevSecOps and Metrics
- Closing Perspectives and Context

A Bear!… So What's Too Close?

0 – Deterrent

300 LB Bear…136 KG (estimated)

20 meters distance to bear (approx. 21 yards)

75 yards (68.58 meters) they feel disrupted

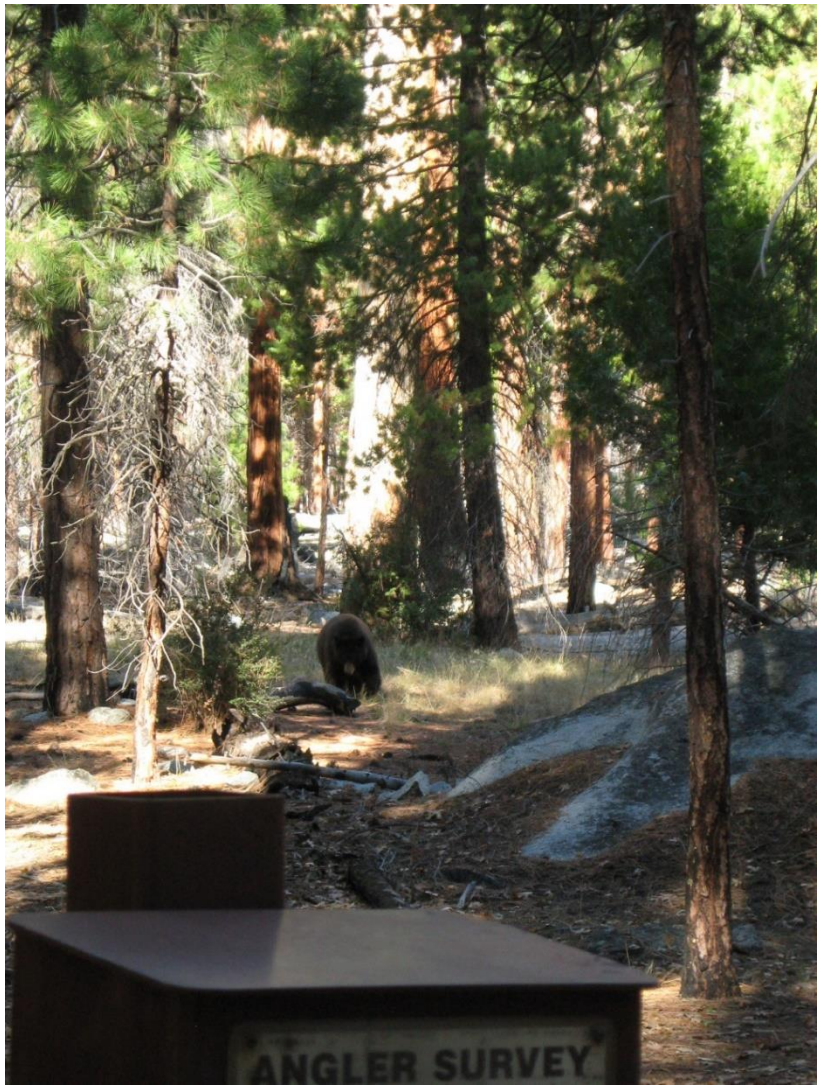
Shed 10 meters away (10 yards)

Our Car 150 meters away (160 yards)

Bear can run at 22 MPH (35.4 KPH)

Estimate I can run at 15 KPH (10 MPH)

How fast can my wife run?



Agenda

- Intro
- Context Is Everything
- Goals, Objectives, Outcomes
- Why Standardization Matters
- DevSecOps and Metrics
- Closing Perspectives and Context

Goals and Outcomes – Resolution of Problems

- Slow delivery of “value” to customers
- Detected malware 8 months after it was installed
- Sensitive healthcare data of 5000 patients was stolen 6 months ago
- Customers are cancelling services
- IT spending is higher than allocated
- Business benefits/ value unrealized

Goals and Outcomes – Proactive or Technical Enabling

- Detect malware within 1 hour of deployment
- Reduce costs per feature delivered
- Reduce overall total cost of ownership
- Reduce average number of “server hops”
- Improve defect removal efficiency
- Increase user/ customer efficiency

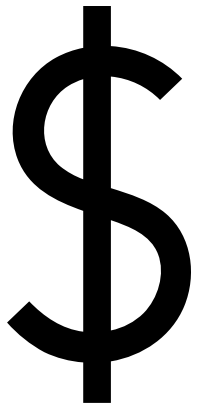
Is Faster Better?

- Rapid automation of wrong things faster
- Faster delivery of defect-prone software
- Faster delivery of unsecure software
- Faster delivery of software that doesn't satisfy user needs
- Faster delivery of the wrong software
- Faster delivery/ deployment of expensive services to operate and govern

Speed Can Kill

Agenda

- Intro
- Context Is Everything
- Goals, Objectives, Outcomes
- Why Standardization Matters
- DevSecOps and Metrics
- Closing Perspectives and Context



Comparative Analysis
(selection/ decisions)

Management
(governance)

SLAs (compliance)

Trend Analysis
(reflection)

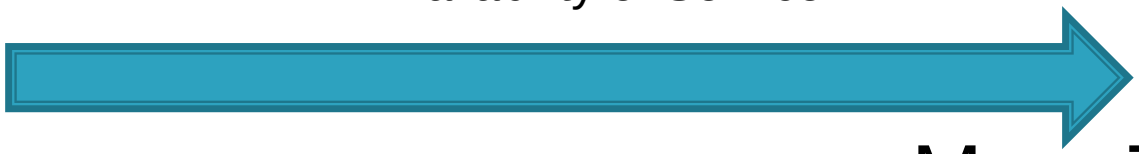
Communication

Standards Support Business and Enabling Metrics

Revenue
Expenses
Complaints Resolved
Customers Served
Average Time to Sale
Customers PII Stolen

Response Time
System Availability
TB Data Stored
Mean Time to Restore
$/ FP Developed
$/ FP Supported
Deployments/ Month
Availability of Service

Number of Server Hops
Storage Incidents
Number of Instances
Bits per Second
Availability of Network Port



Business

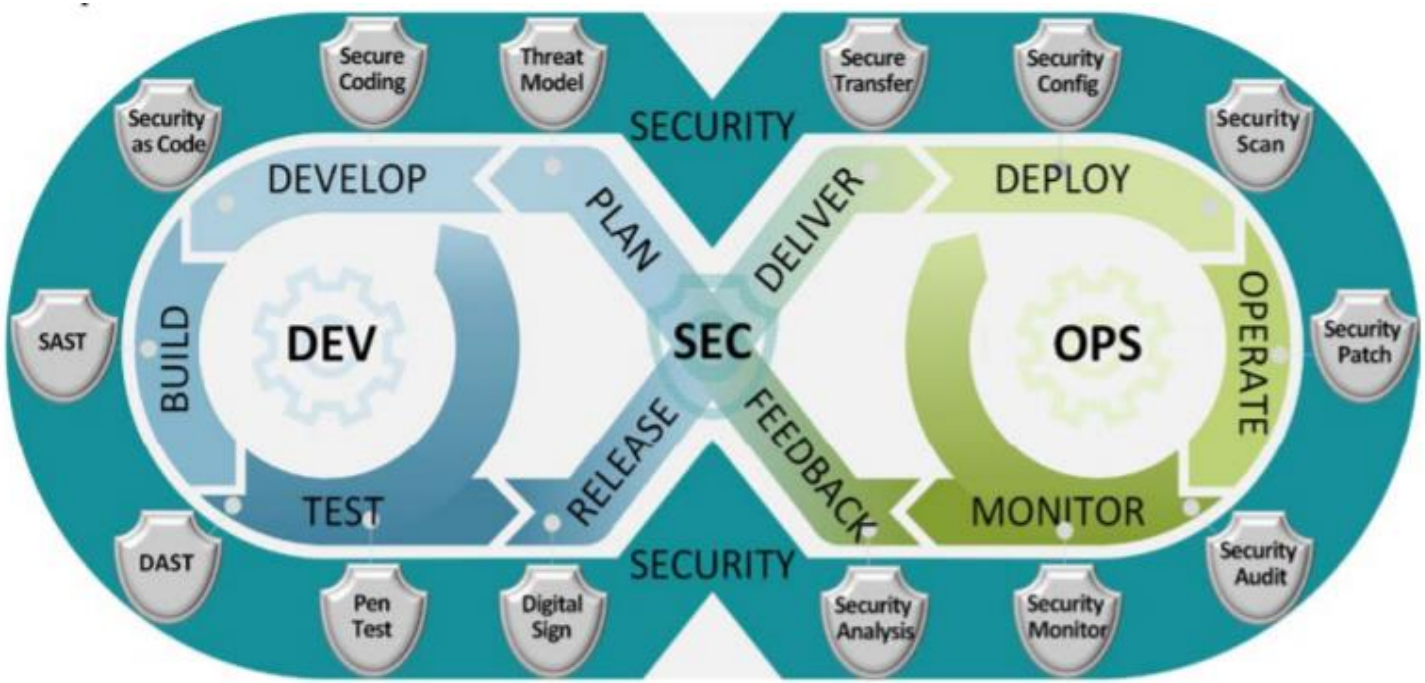
More Technical

International, Regional, Enterprise, Teams

Agenda

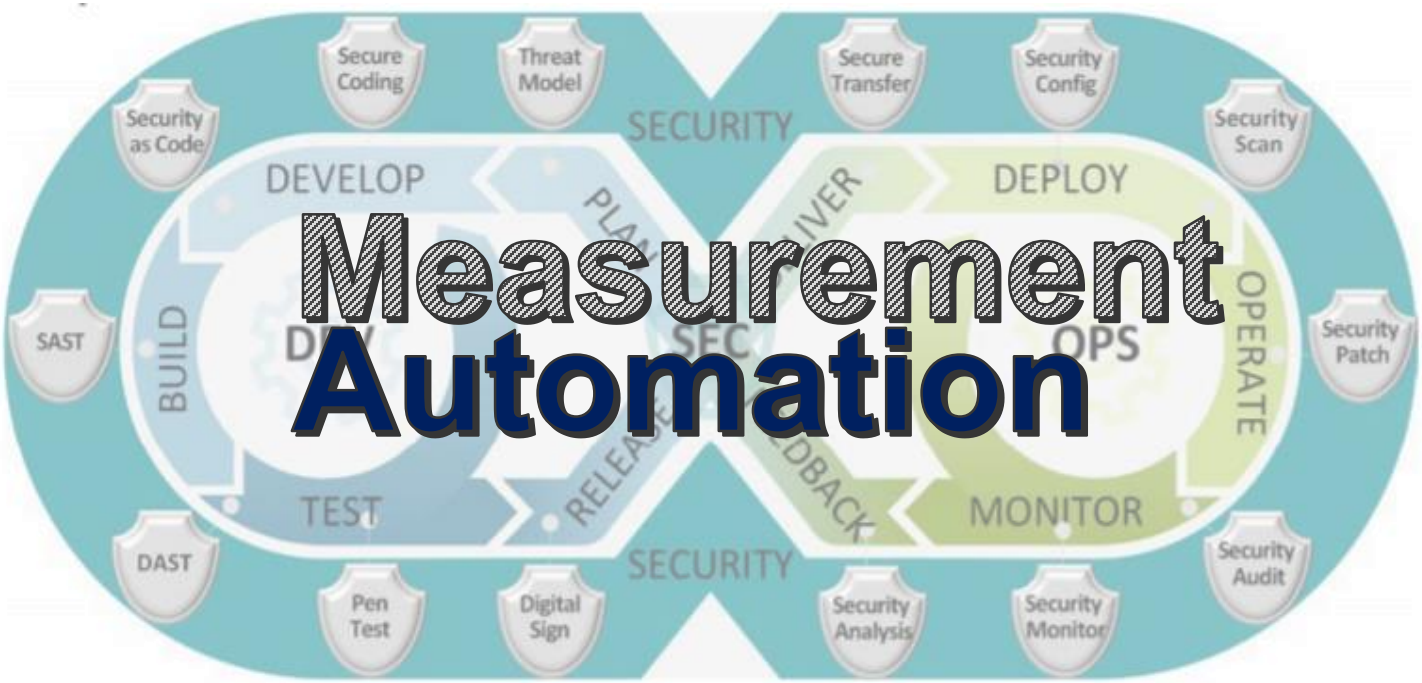
- Intro
- Context Is Everything
- Goals, Objectives, Outcomes
- Why Standardization Matters
- DevSecOps and Metrics
- Closing Perspectives and Context

DevSecOps – Reference Architecture



Based on the United States DoD – Enterprise DevSecOps Reference Design

DevSecOps – Reference Architecture

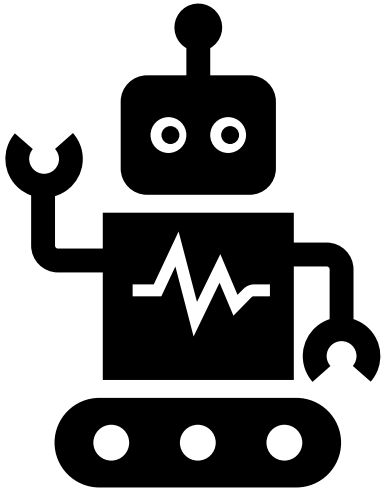


Based on the United States DoD – Enterprise DevSecOps Reference Design

Alert and Trigger

- Alert

- Trigger



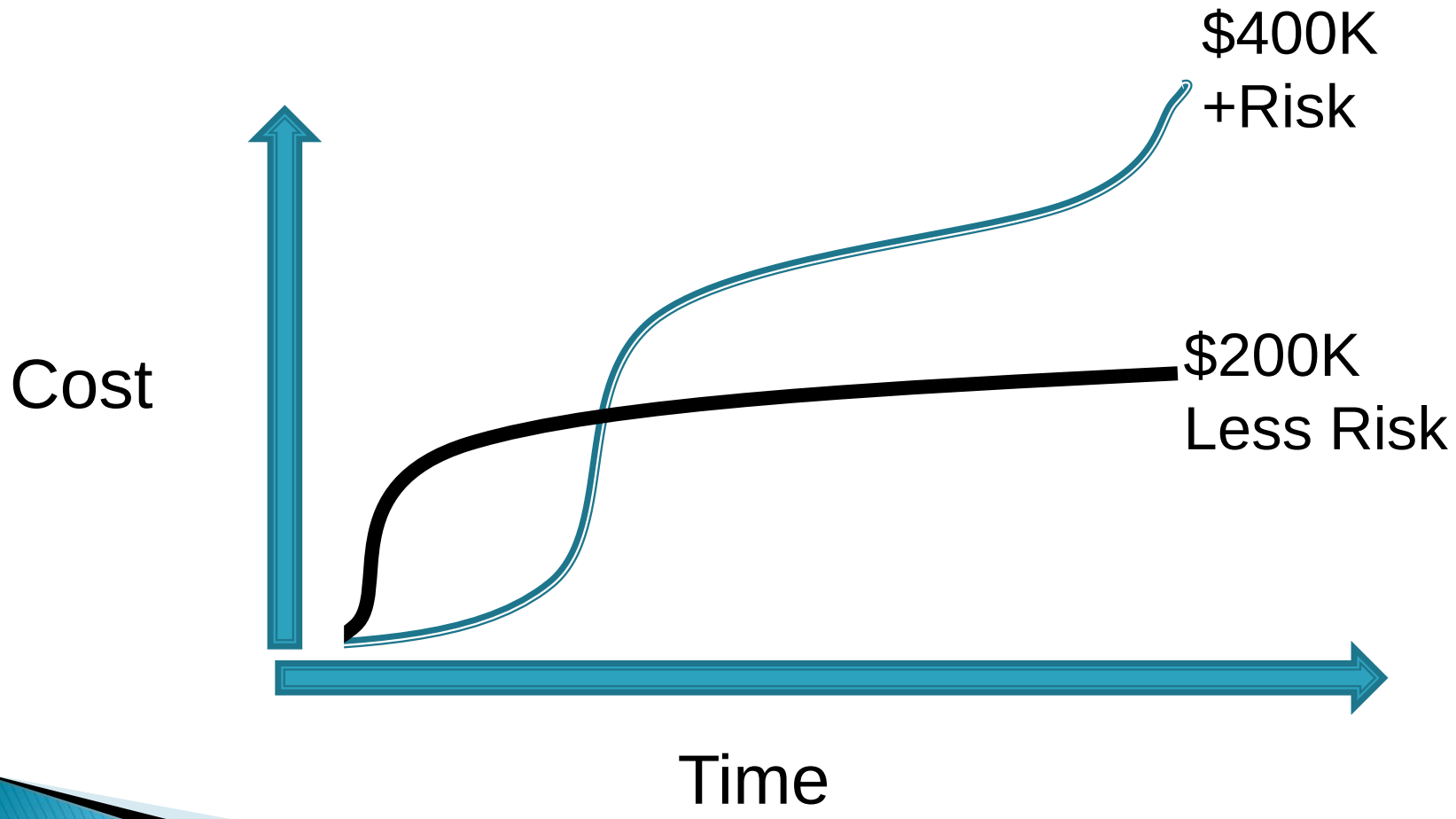
Agenda

- Intro
- Context Is Everything
- Goals, Objectives, Outcomes
- Why Standardization Matters
- DevSecOps and Metrics
- Closing Perspectives and Context

Situational Awareness Improves Decision Making

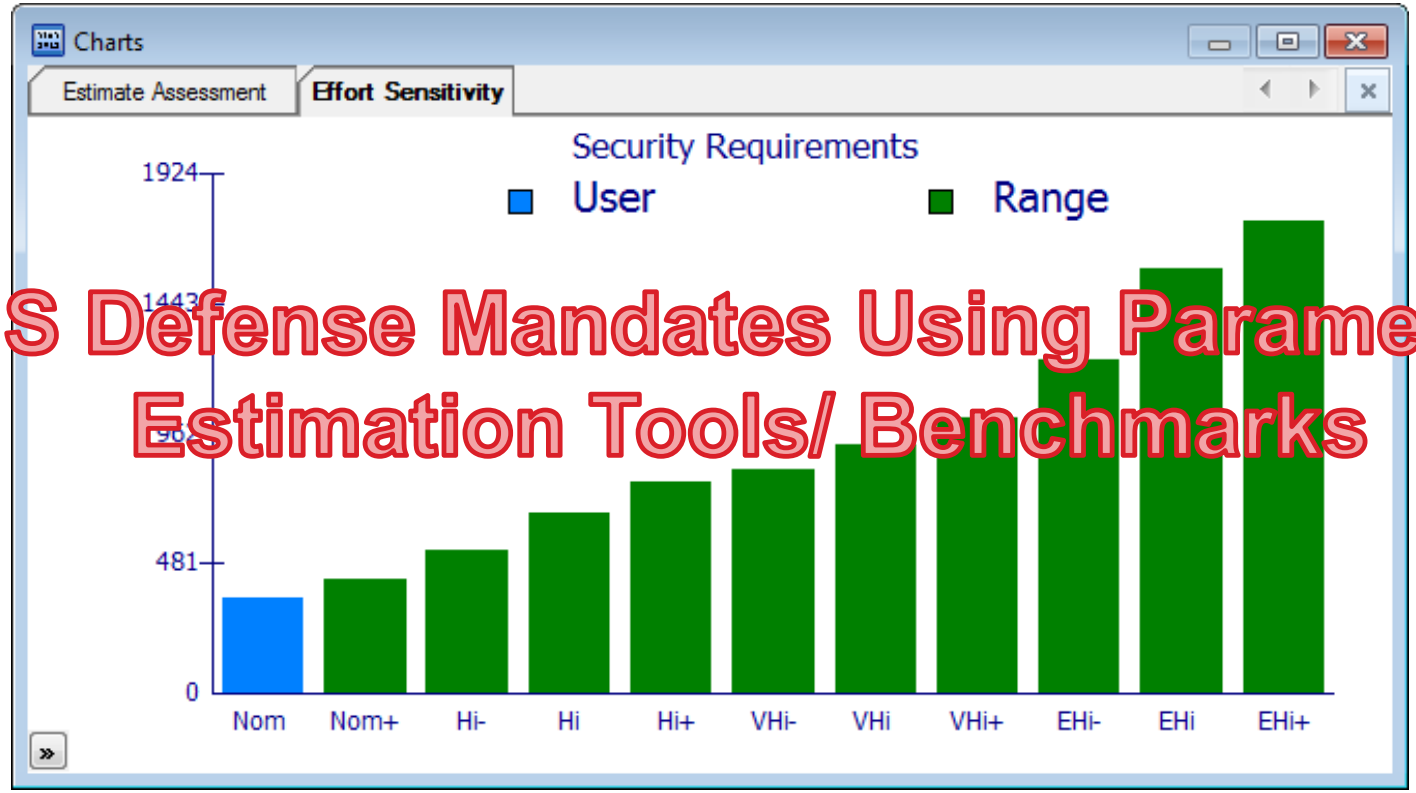
Right Automation at the Right Time

Collaborate – Get the Right Team Composition Early!



Higher Security Resiliency Levels Require Adequate Funding

- Building secured software is costly…
- Cost of breaches can be much worse



US Defense Mandates Using Parametric Estimation Tools/ Benchmarks

Based on Galorath SEER-SEM Parametric Estimation Model

Funding DevSecOps

- IDC Scalar Security Study 2019
  - Average cost per organization responding to and recovering from cyber-security incidents?
  - $4.8 to $5.8 Million Dollars
  - Average organization attacked 440 times per year

- Competent DevSecOps – Can reduce costs and risks for development and support

A Few Keys For Success

- Don’t Measure to Measure
- Recognize what you measure impacts behavior (positive or negative)
- Check for abuse
- Standardize so precision is fit for purpose
- Educate through supply chain
- Incremental and value focus

The Future is Driven From Metrics

- Driverless cars
- IoT
- Artificial Intelligence
- Microservices
- Analytics/Big Data
- Blockchain (distributed ledgers)

Governing, Monitoring and Executing

Thank You & Questions

- steve@cloud-perspectives.com
- Twitter: @woodwardsystems or @cloudsimplify
- www.cloud-perspectives.com
- 613-698-5240