Measuring the Whole Hole

Dr. Mark Peters

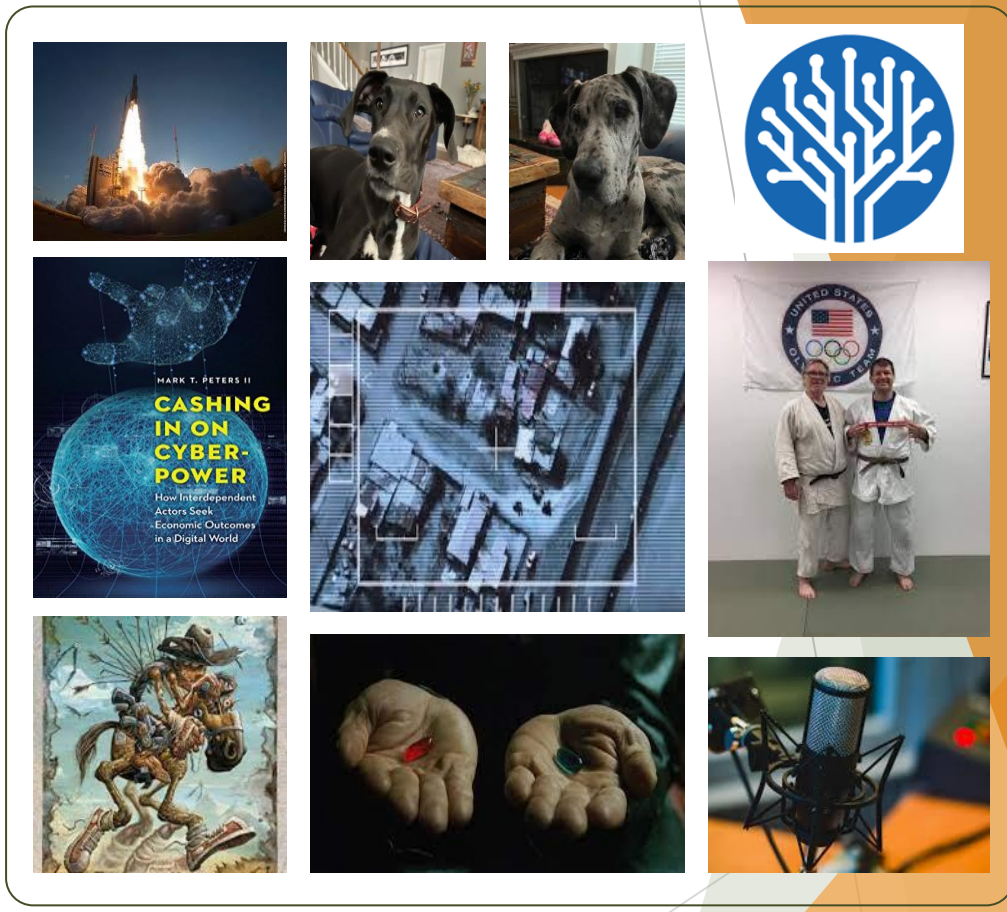
Technical Lead, Novetta

Dr. Mark Peters

Technical Lead

@tinycyber

Mark is a Technical Program Lead for Novetta, working on integrating DevOps for a US Department of Defense program. A recently converted DevOps junkie, he is a DevOps Institute Ambassador, and the US chapter chair. After a career in Air Force Intelligence, he specializes in operationalizing security issues, finding ways to bring teams together, and deliver accelerated value. In his spare time, he enjoys drawing, reading, speaking and judo as well as his two dogs, Hanna, and Watson.



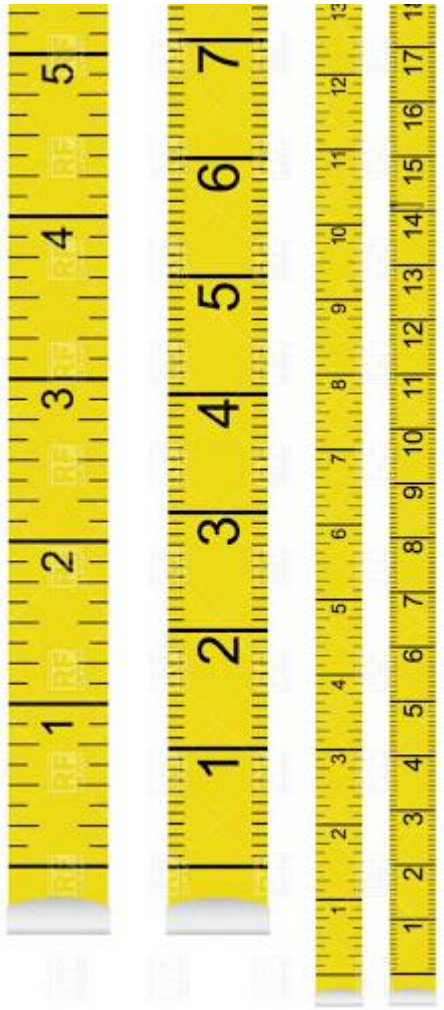
When the Security team brings you the regular scan…

Is it this hole?

Or this one?

Worse, did you just ask, what regular scan?

What does it mean to measure security?

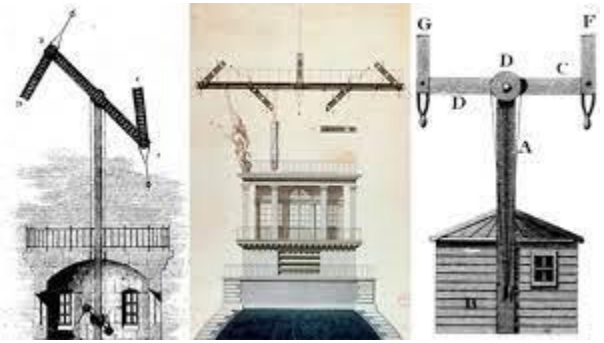


- DevOps measures actions to create feedback
- Standard measures
  - Lead time to Change
  - Deployment Frequency
  - Mean Time to Recovery
  - Change Failure Rate

- Which measurement addresses security?
  - Can’t compare measurements without security

Security Considerations

- Security exists in two phases
  - To GUARD your value
  - To SIGNAL a threat



- What do you want security to do for you?

Which holes matter?

Are you looking for a hole?

- Comparing security standards can be challenging
- Different compliance regulations use different language

	NIST RA-9 Criticality Analysis		PCI-DSS 6.1		HIPAA 164.308(a)(1)
#	Word	#	word	#	word
24	system	9	vulnerabilities	17	system
14	components	8	security	11	components
10	functions	6	system	9	functions
8	analysis	4	information	7	analysis

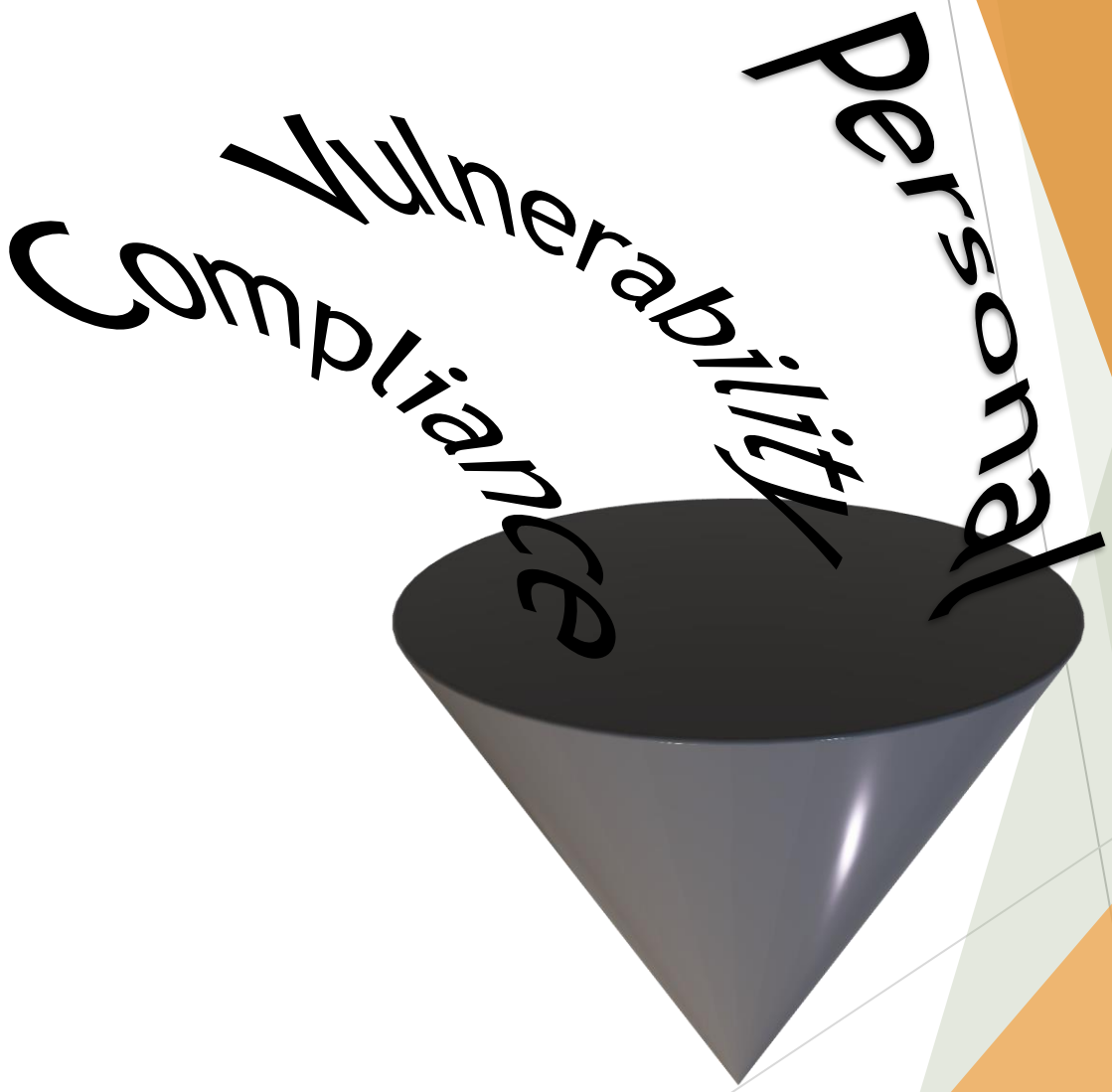
Which standard is best?

- Find the compliance standard
- Align governance across multiple levels…if necessary
- Move to defining “bad” holes
- Value question
  - Do you plan for holes?
  - Or respond to holes

	PCI_DSS	pg/score	NIST	pg/score	HIPAA	pg/score
Value (s)	15	0.11	115	0.24	3	0.03
Exchange(s)	1	0.01	69	0.14	19	0.17
Requirement (s)	443	3.19	785	1.63	233	2.03
Operational	49	0.35	133	0.28	2	0.02
norm (s)	0	0.00	0	0.00	0	0.00
Policiy (ies)	172	1.24	878	1.82	87	0.76
employee (s)	22	0.16	35	0.07	25	0.22
Management	91	0.65	597	1.24	30	0.26
technical (s)	7	0.05	57	0.12	53	0.46
Vulnerability (ies)	140	1.01	230	0.48	2	0.02
automated	20	0.14	252	0.52	2	0.02
pipeline (s)	0	0.00	7	0.01	0	0.00
vendor (s)	77	0.55	21	0.04	0	0.00
Third party (ies)	19	0.14	6	0.01	8	0.07
External	46	0.33	348	0.72	0	0.00
commercial	1	0.01	28	0.06	0	0.00
Average		0.50		0.46		0.25
Cumulative		7.94		7.37		4.03

Types of Holes

- Compliance Holes
  - Failed to meet standard
  - No policy created
- Vulnerability Holes
  - Scanned & Failed
  - New hole released
- Personal Holes
  - Failed to patch
  - Introduced vulnerability
  - Attacked by a rude person



Measuring a Compliance Hole

- Compliance creates value in market
  - Maturity levels
  - SOC 2 Evaluation
  - Authority to Operate for x time interval
- Take internal evaluation
- Requires external approval
- Generally graded as Compliant, Non-compliant

Measuring a Vulnerability Hole

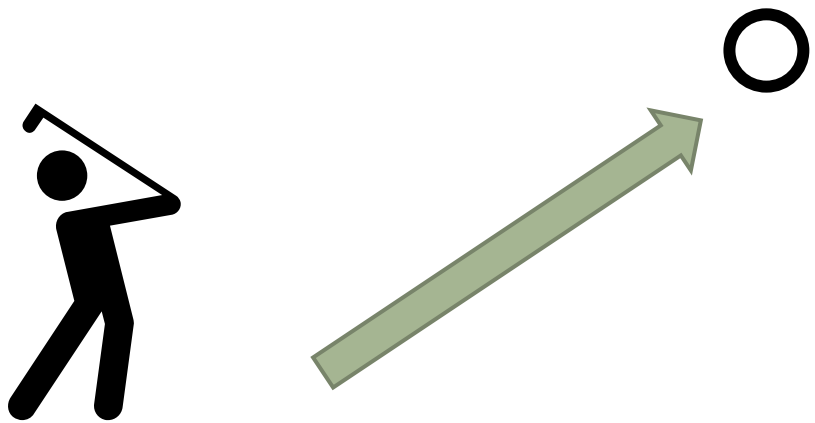
- Vulnerability – Creates value by minimizing risk
  - CVE – cve.mitre.org
  - Check software/hardware
  - Use a scanning tool (ACAS, ZAP, Anchore, Fortify
- Builds into risk equation (Risk= Threat * Vulnerability)
- Typically internal – STIG Scale
  - Low (Cat III) – Degrades protection measures
  - Medium (Cat II) Can result in loss of CIA
  - Severe (Cat 1) Direct loss of CIA EXCEPT if critical

Measuring a Personal Hole

- Personal create value across the system
- People create errors
  - Most secure system has no users
  - Intentional and unintentional errors
- Evaluated by management processes
- Constantly changing
  - New people, tools, and techniques
  - Establish process in trust

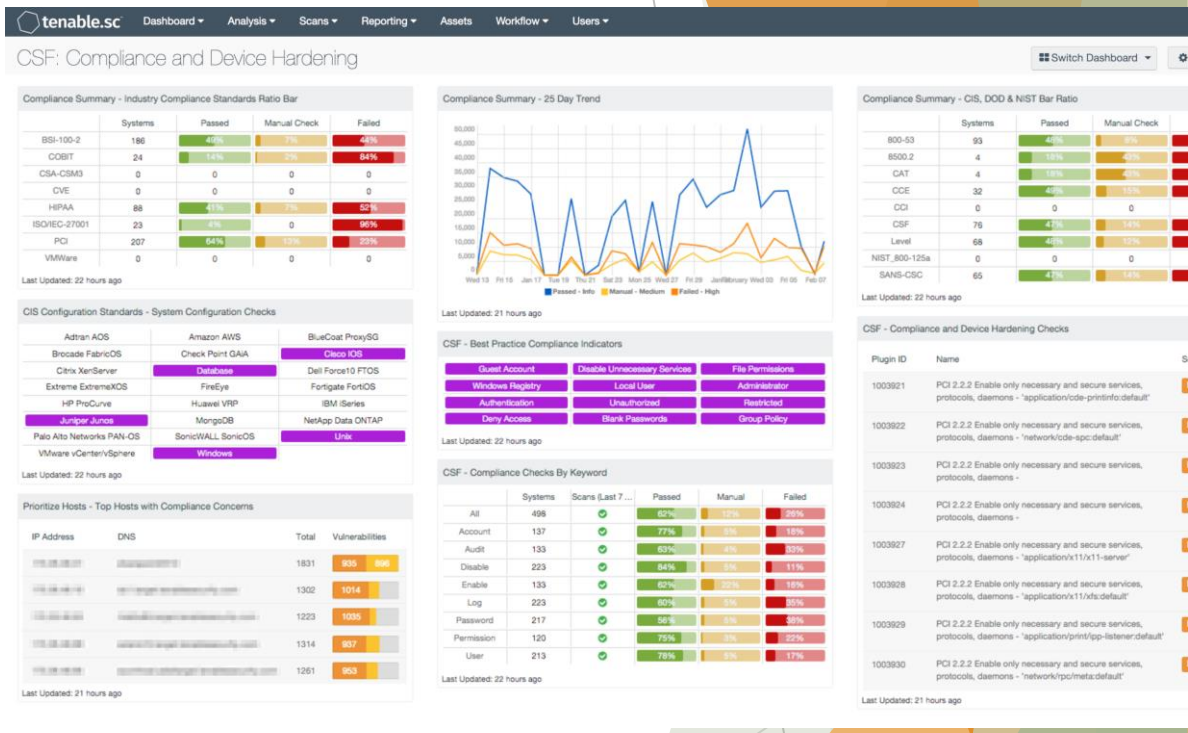
Now What?

- Bring the measurements together
- Compare & evaluate holes
- Develop a patching strategy



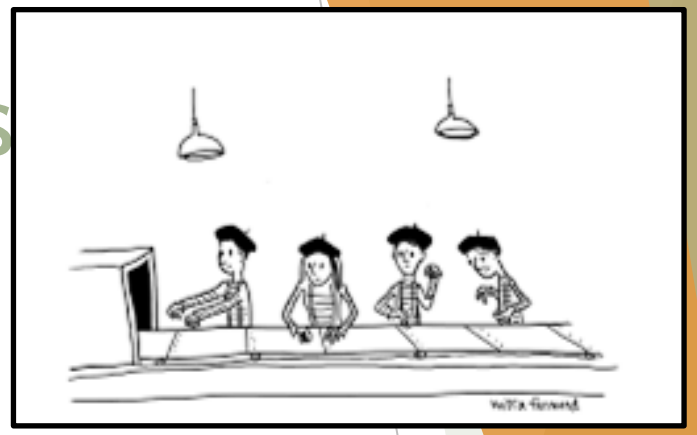
Dashboards shortcut security discussions

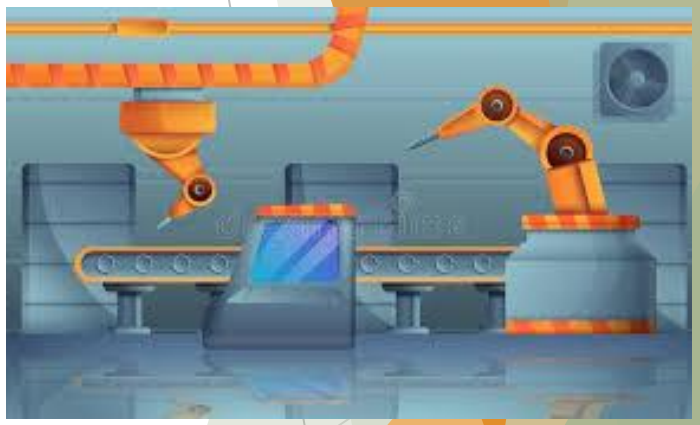
- Enhanced visibility improves flow
- Observability creates awareness
  - Metrics
  - Logs
  - Traces
- Value question
  - What do you learn from dashboard?
  - How does it create action?



Manual vs automated assessments

- Manual
  - Human-based, Usually labor-intensive
  - Verifies completion of desired task
- Automated
  - Machine based, possible ML
  - Large data volumes
  - Possible trust issues
- Cooperative
  - Combine Automation & Human
  - Best of both options





+

How do you know what you know?

- How do you know?
- If true, what comes next?
- Are the premises true?
- Do conclusions follow premises?
- What arguments are needed for premises to be true?
- Compare apples to apples not oranges to elephants

- Dashboards do not equal awareness

≠

≠

Patching Strategy

- Feedback from measurement creates experiment
  - What solutions fill which holes?
  - Which hole is most important?
  - Do I measure success as less hole or no hole?

Takeaways

- Determine which measurement standard is in play
- Link measurements to value
- Holes change over time
  - Decision creates error, indecision creates disaster
  - Continuous monitoring better than interval measurements

Good luck finding and fixing your holes!

Measuring the Whole Hole

Dr. Mark Peters

Novetta, Technical Lead

@Tinycyber LI: in/tinycyber/ Github: @TinyCyber