ITEA Test Instrumentation Workshop 2022

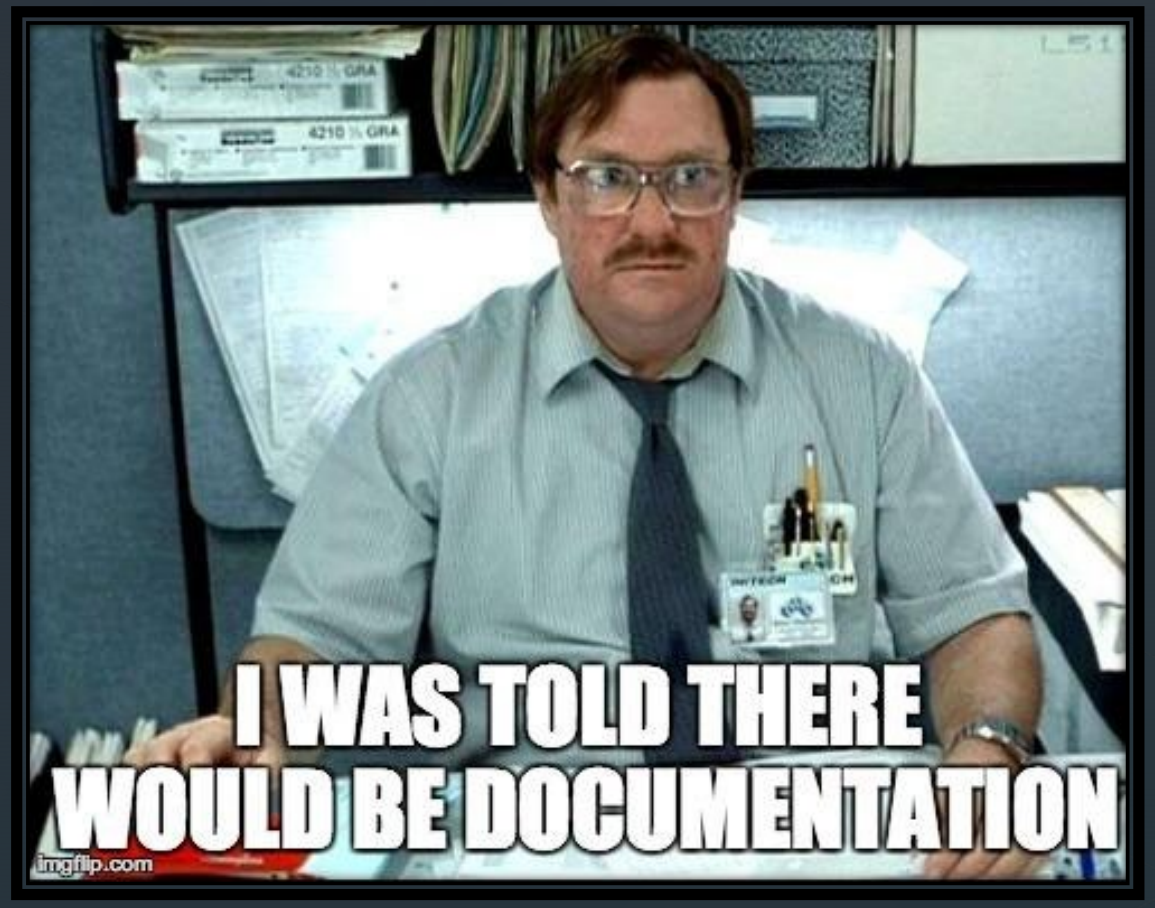
Developing a Cyber Defense Mindset

Beyond Compliance

Jason Schalow
Chief, Special Missions Flight
412th Communications Squadron
Edwards AFB

DISTRIBUTION STATEMENT A - Approved for public release; distribution is unlimited. 412TW-PA-22174

Compliance and Other Demons



The Compliance Mindset

"We've done our A&A package already, so I'm not sure why you guys are doing this."

- *Actual quote from the government ISSM of a not-to-be-named aircraft acquisition program, when the team of cyber testers trying to plan a by-law mandated pen test of his platform asked basic security questions*

(Circa A.D. 2020)

Compliance: By the Numbers

For a network with 100 Windows 10 endpoints, with 26 possible CAT 1 DISA STIGs per endpoint:

Total Possible CAT 1 Vulnerabilities	Percent Compliance	Number Remaining After Remediation
2600	95%	130
2600	99%	26
2600	99.9%	3 (if you round)

= **Every one** of your machines might be bad, or a few are REALLY bad

= Up to 25% bad endpoints

= STILL have a problem

Now, imagine you have 10,000 endpoints…
Or that you stop ignoring the 213 possible CAT II's per machine…etc.

Problem: Perfection doesn't scale well

Wait a Second!
This Heretic is Insulting my Nessus Scanner!

- *Nota Bene:*
  - I didn't mean to insult your Nessus scanner (I have one, too)
  - STIG Compliance is a good thing
  - Compliance in general is a good thing

…but…

Compliance is not Enough

…And Your Tools (Alone) will not Save You

Any of this sound familiar?

- Installed HBSS, because STIGs/A&A
  - Never look at the ePO server
- Also, turned on insane amounts of logging
  - Check them once a month, unless busy
- Bought an awesome next-gen firewall
  - Couldn't afford training/certifications
- And, of course:
  - "The vendor said all I needed was this awesome new zero-trust networking gizmo with a large recurring maintenance fee to solve all of my problems…"

Changing the Mindset: Cyber as Warfare

Does this seem relatable?

- If we really are at war (cold, warm, hot or otherwise) in Cyberspace, then we need to think differently
- Traditional warfare wisdom can help us modify our mindset and become more agile in our defense

We'll try to apply some traditional military wisdom to our cyber domain to get us out of our 'mental trap'

#1: Perfect really is the enemy…

- Your security will never be perfect, because this is all harder than it looks!
- If you think it is good enough, you are already wrong
- Frameworks like SOC-CMM can help you assess you maturity
  - **Just don't get depressed at where you are!**

"**Activity in war** is movement in a resistant medium. Just as a man in water is unable to perform with ease and regularity the most natural and simplest movement, that of walking, so in war, with ordinary powers, one cannot keep even the line of mediocrity."

Carl von Clausewitz
On War, Book 1 Chapter 7

Friction isn't failure; it is a fact of life
You will never be 100% ready or 100% 'mature' in your cyber defense

#2: The enemy gets a vote, so you should ask what it is…

"**Success in warfare** is gained by carefully accommodating ourselves to the enemy's purpose."

Sun Tzu
Art of War, Chapter 11, #60

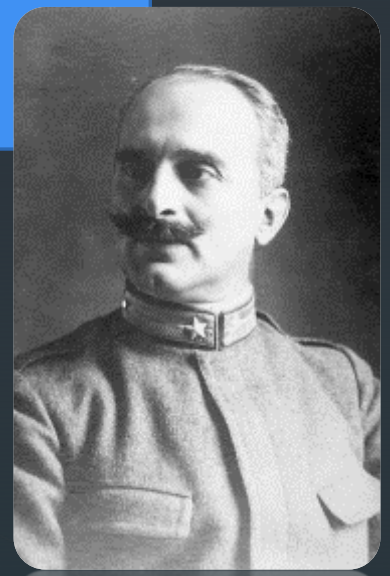
- Threat intelligence and penetration testing are critical skills NOW, not when you become more mature, advanced, etc.
- **Do them…even if you are bad at them!**
- MITRE ATT&CK is your friend, get to know it
  - Along with 'InfoSec Twitter', etc.

You can't do everything; understanding your potential adversaries allows you to focus on what's important

#3: Understand the adversary's TTPs, and how to detect them…

"**The form** of any war—and it is the form which is of primary interest to men of war—depends upon the technical means of war available."

Giulio Douhet
The Command of the Air, Ch. 1



- Once you understand the adversary's TTPS, map them to detention methods
  - MITRE D3FEND is a good resource
- Understand your gaps:
  - What can you see?
  - What can prevent?
  - Where are you potentially blind?
  - **What can you hunt for?**

Understanding the capabilities you have, and the capabilities you need will prevent wasting time on 'shiny objects'

#4: Know your mission and terrain and defend the critical points…

"**The most** fertile areas always attracted the strongest attack, and therefore required the strongest defense; and between the fertile and infertile areas it was possible to draw a line which for strategical purposes was definite and consistent."

Sir Julian Corbett
Some Principles of Maritime Strategy, Ch. 4

- Defend you mission, not your systems
  - **A device is only as important as the role it is *currently playing* in the mission**
- Not everything is equally important
  - A CAT III vulnerability in a critical system may be more important than a CAT I is a non-critical system

If you can't protect everything, identify the critical elements to the mission at any given time

#5: Make the adversary's job hard…

"**Conflict** can be viewed as repeated cycles of **observing, orienting, deciding and acting** by both sides, and also, I might add, at all levels. The adversary that can move through these cycles faster gains an inestimable advantage by **disrupting his enemy's ability to respond effectively**."

John Boyd
Testimony before the House Armed Services Committee

- You can't stop a persistent adversary
  - But you can increase their requirements and make their job difficult
- Your ability to effectively orient yourself is the key to operating faster than the enemy
  - **Focus less on closing the gates and more on manning the watchtowers**
  - If you aren't checking logs, have an IDS (that you monitor), performing 'hunt' mission etc. you won't know when the adversary succeeds

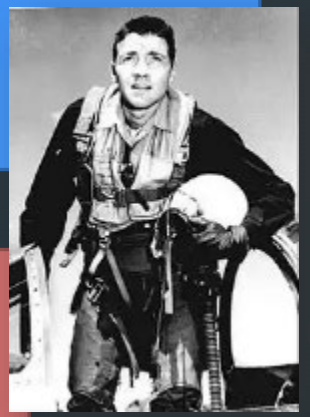
Monitoring your systems and networks is not an advanced skill, but a basic requirement

#6: Your people are the only technical advantage you have…

- The adversary can match (and exceed) all of your hardware and software resources
  - An Advanced Persistent Threat will know your technology and figure out how to defeat it
- It's the quality of your humans that determines the outcome of the fight
  - Invest as much in training as you do in hardware
  - **Encourage innovation rather than slavish compliance**

"**People,** ideas, hardware—in that order."

John Boyd
Quoted in: Boyd: The Fighter Pilot Who Changed the Art of War



Cyber warfare is ultimately a fight between humans

#7: Know what tools you have, and what tools you need…

"**You should not** have any special fondness for a particular weapon, or anything else, for that matter. Too much is the same as not enough. Without imitating anyone else, you should have as much weaponry as suits you."

Miyamoto Musashi
The Book of Five Rings

- You already have more tools than you realize…learn how to use them
  - **Anyone who has spent any time doing digital forensics can tell you: you already have a lot of data!**
  - The trick is leveraging it appropriately
  - Again, training! (and practice!)
- Only invest in weapons you have time to learn and train to use effectively
  - Work on those playbooks (or borrow/steal them!)

Let the IT folks be obsessed with gadgets; a cyber defender's job is to win the fight

Take-aways

- Mindset change is critical to success
- Compliance is good, but not good enough
- Don’t expect perfection; do it anyway
- Know your threats, know their TTPs, know how to detect them
- Know your mission and terrain
- Focus on people over tools
- **Make the adversary have a really bad day**