What the Scope?

Shit my client|consultant says

Whoami /us

Luke McOmie (Pyr0)

VP of Offensive Security at Ideal Integrations

- Started in offensive security in 1994 w/HA<< (RCST)
- Founded Skytalks
- DEFCON SENIOR GOON (Retired)
- Founded and contributed to several startups, Fortune 100 companies, and federal agencies
- Published author and industry liaison
- “That guy”

Qasim Ijaz (Q)

Director of Cybersecurity at Aveanna Healthcare

Former roles

- Director of Offensive Security
- Sr. Mgr Attack Simulation at a Healthcare Org
- HIPAA/HITRUST Assessor
- Associate CISO

Instructor in after-hours

- Blackhat, BSides, OSCP Bootcamp

Agenda

- Why this talk?
- Sh* we've heard
- What we can do about this?

Why this talk?

- Past experiences as consultants and clients
- Lack of transparency (for clients / consultants)
- Sick of watching people spend money to not get value from the work that is being performed
- Language problems, bad practices, wrong focuses

It’s not in the scope…

- Over-scoping vs. Under-scoping
- Reality check (maturity and the lack of)
- Compliance vs. Security (check the box)
- Once a year vs. Continuous Assessment
- Flat networks / Hypersegmented / No networks.
- Focusing on the wrong things (PCI vs. everywhere else)
- Budgets, Lawyers, and other things that go bump in the night.

Define scope based on risk (and budget), not convenience.

Can you please disable the
<FIREWALL, EDR, Blocklist, etc.>?

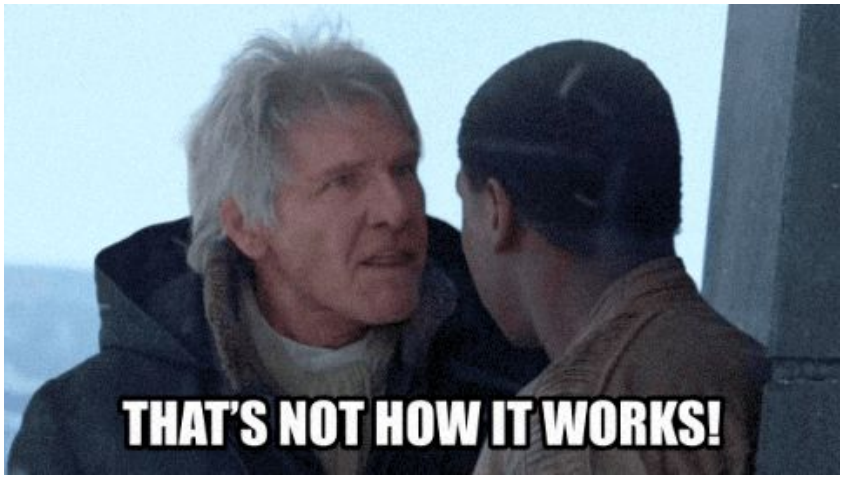
Sure! Should I also unlock the front door?

- Test Real-World conditions
- Validate defense in depth
- Compensating controls matter
- Positive measures and dumb moves
- Worried about looking good/bad?
- Stop allow listing *(at least at first)*

“We don’t need that, we already have a WAF.”

- WAF ≠ Secure Code
- All of our developers know SDLC
- Bypassing 101
- Business Logic Flaws Still Exist
- “Set it and Forget it” Fallacy
- Defense-in-Depth
- MSSP/MSP ≠ Secure, or aware, or . . .
- Nobody wants to hack us.

“Cool. So, you installed a screen door on a submarine?”



We're Not Allowed to Tell You How We Got In

- Tool confidentiality hurts customers
- Actionable Reporting **is** the Deliverable
- Knowledge Transfer is a Value-Add

The best tests teach your client how to catch or stop the attack next time.

We have MFA

- MFA ≠ Invincibility
- Real-World MFA Bypass Tactics
- Push Notification Fatigue
- Pentesting MFA Implementations

MFA is like a seatbelt—it helps, but it won’t save you if you drive straight off a cliff.

We found 850 findings, 150 are critical, and we couldn't gain access. . .

- When an "A" isn't an A. (bad work = bad results)
- Vulnerability Scanning ≠ Penetration Testing
- The false positive nightmare
- Risk ratings gone wrong
- Quality over Quantity

A real test should simulate an adversary, not a printer jam of CVEs.

Can you pentest at night?

- Attackers don't have set hours, but often prefer heavy traffic times.
- Production Impact Myths
- If One Tester Can Take You Down…
- Testing in Real Conditions
- Additional Cost
- I’m just going to go ahead and shut that down. . . .

It’ll be $50k and that’s all you need to know

- Understand what you’re buying (Pentest? Vuln scan?)
- Ask for outcomes, not just hours
- Pricing =/= value

Don’t make me dissect the SOW, be transparent!

We change our provider once a year

- Lack of intimacy and tribal knowledge
- Repeating same effort & work
- Did you even go deep?
- Fresh eyes =/= quality


OKAY. I'M HEARING
LOTS OF PROBLEMS
BUT NO SOLUTIONS!

Partner up with your consultant/client

- Collaborate on Scope
  - Make testing practical, realistic, and valuable.
- Understand Each Other's Hurdles
  - Clients have uptime concerns, consultants have testing needs - work together.
- Test Real-World Conditions
  - Don’t disable security controls, test them!
- Quality Over Quantity
  - A good test isn’t about finding 850 issues, it’s about finding the right issues.
- Security is a Journey
  - Compliance ≠ Security. Keep testing, keep improving.
- Mature Together
  - A pentest should be more than a report.
    - It should drive action and better security posture.

Thank You!

Luke McOmie

Vice President - Offensive Security at Ideal Integrations

Qasim Ijaz

Security Director in healthcare | OSCP, CRTP, CRTO, MBA