Through a Lens Darkly

Why Seeing Yourself as the Adversaries See You is the Best Way to Understand Your Risk

SYNERCOMM IT Summit – September 2025

РОСАТОМФЛОТ

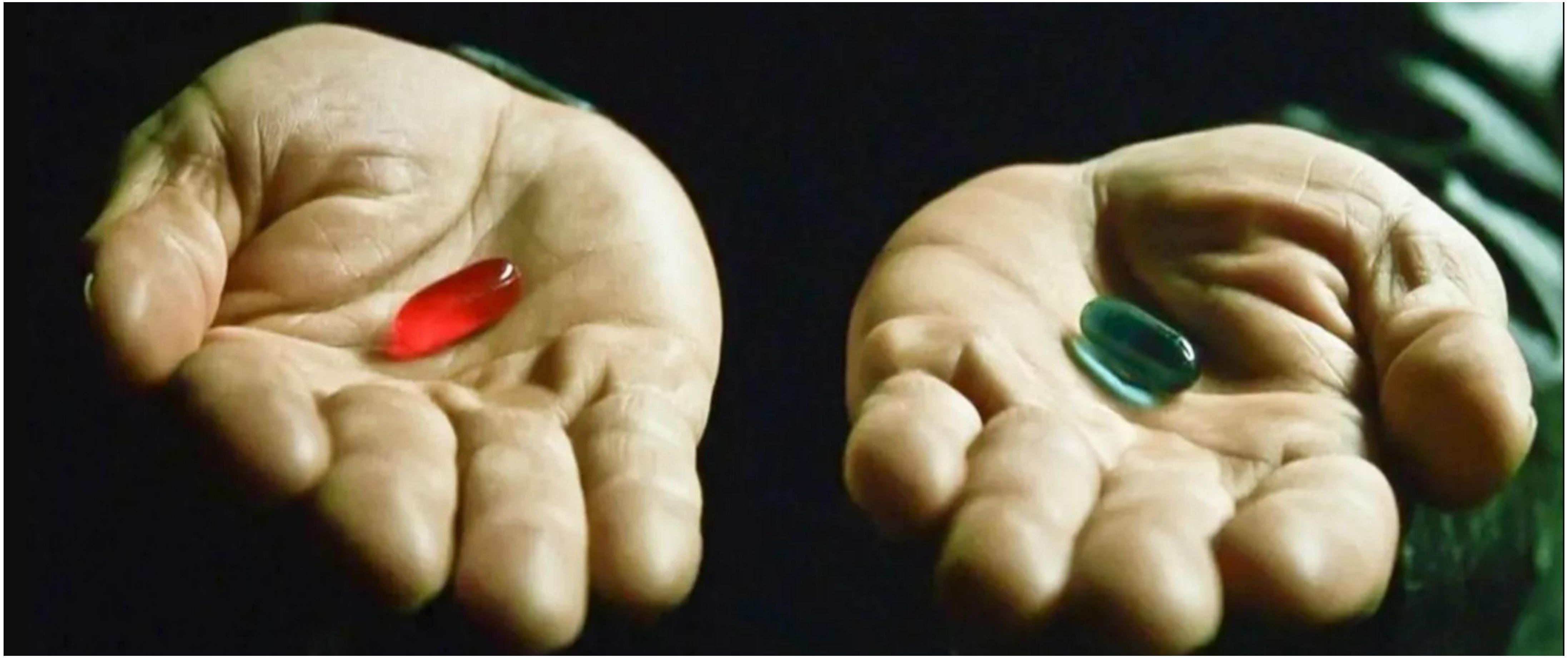
Quick show of hands

SYNERCOMM

Who’s who?

SYNERCOMM

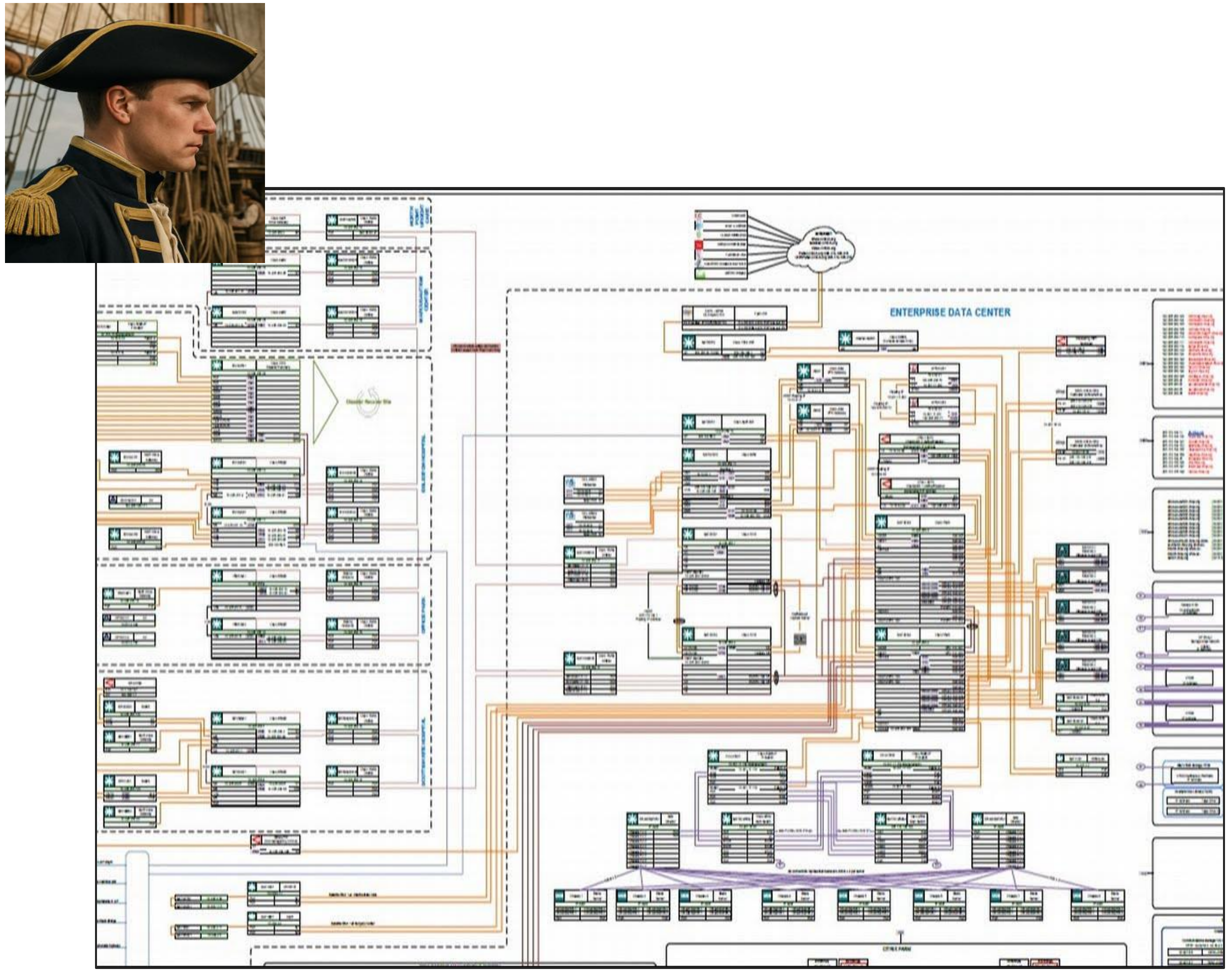
Red or Blue?



A little about me (that's not on LinkedIn)

Why this matters? Role determines focus

Focus drives worldview



Let’s make this more tangible

The difference in perspective

This is my local strip mall.

What does the average person see?

SYNERCOMM

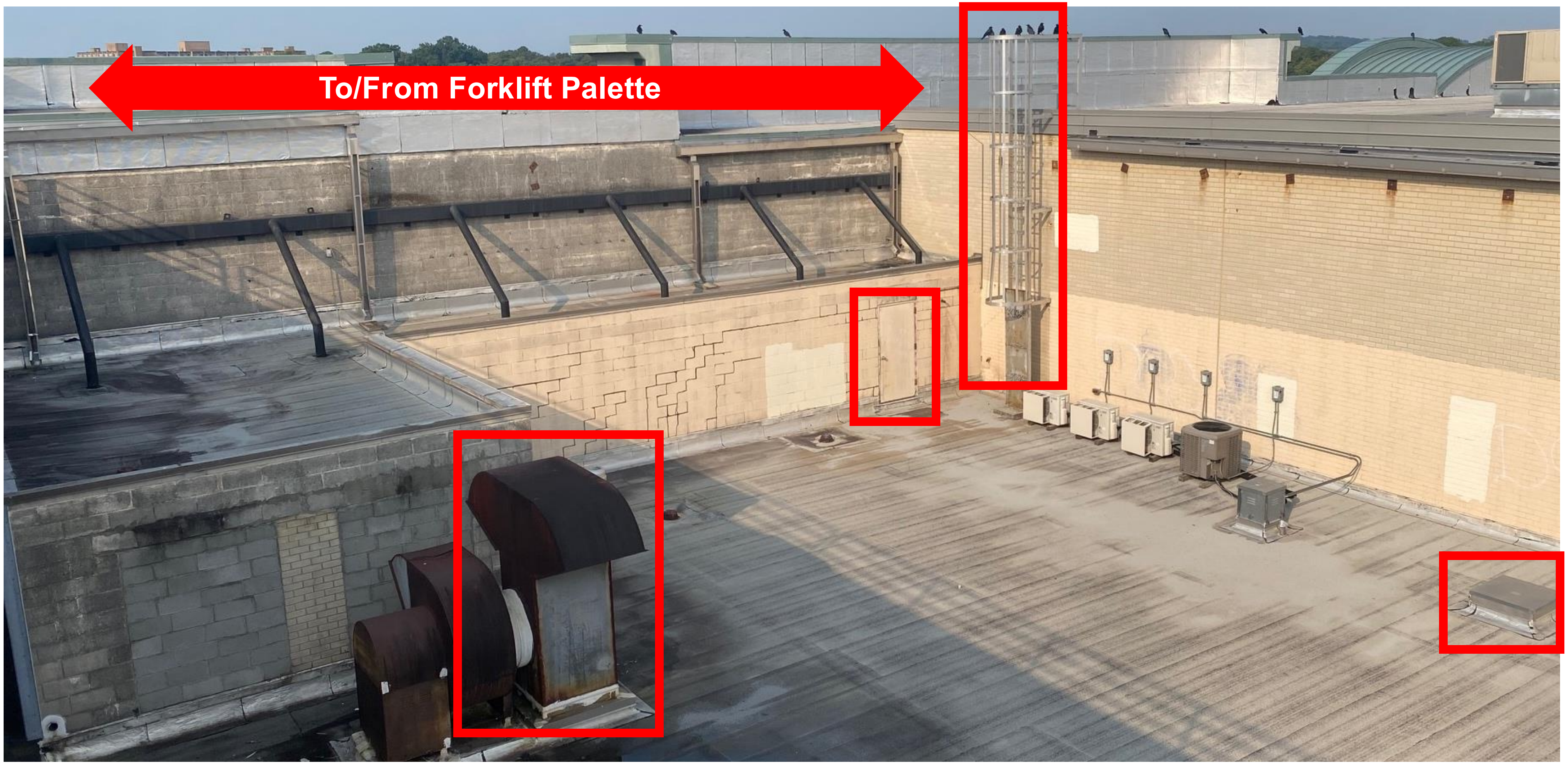
Where no one looks, no one sees

The only person here was homeless

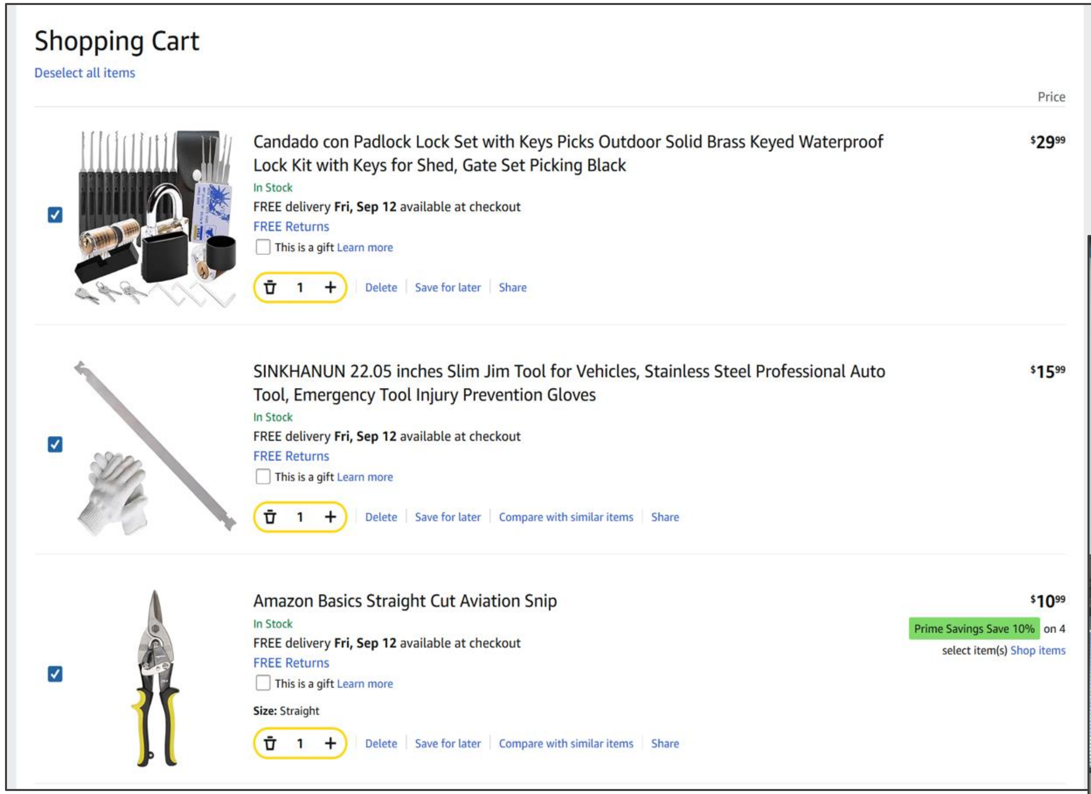
The garage has been closed for years

Go to the roof anyway – what *don't* you find?

But look what you *do* find…



Let’s talk LOE vs. ROI



Shopping Cart

Deselect all items

Price

☑ Candado con Padlock Lock Set with Keys Picks Outdoor Solid Brass Keyed Waterproof Lock Kit with Keys for Shed, Gate Set Picking Black — $29.99

In Stock

FREE delivery **Fri, Sep 12** available at checkout

FREE Returns

□ This is a gift Learn more

1 | Delete | Save for later | Share

☑ SINKHANUN 22.05 inches Slim Jim Tool for Vehicles, Stainless Steel Professional Auto Tool, Emergency Tool Injury Prevention Gloves — $15.99

In Stock

FREE delivery **Fri, Sep 12** available at checkout

FREE Returns

□ This is a gift Learn more

1 | Delete | Save for later | Compare with similar items | Share

☑ Amazon Basics Straight Cut Aviation Snip — $10.99

Prime Savings Save 10% on 4 select item(s) Shop items

In Stock

FREE delivery **Fri, Sep 12** available at checkout

FREE Returns

□ This is a gift Learn more

Size: Straight

1 | Delete | Save for later | Compare with similar items | Share

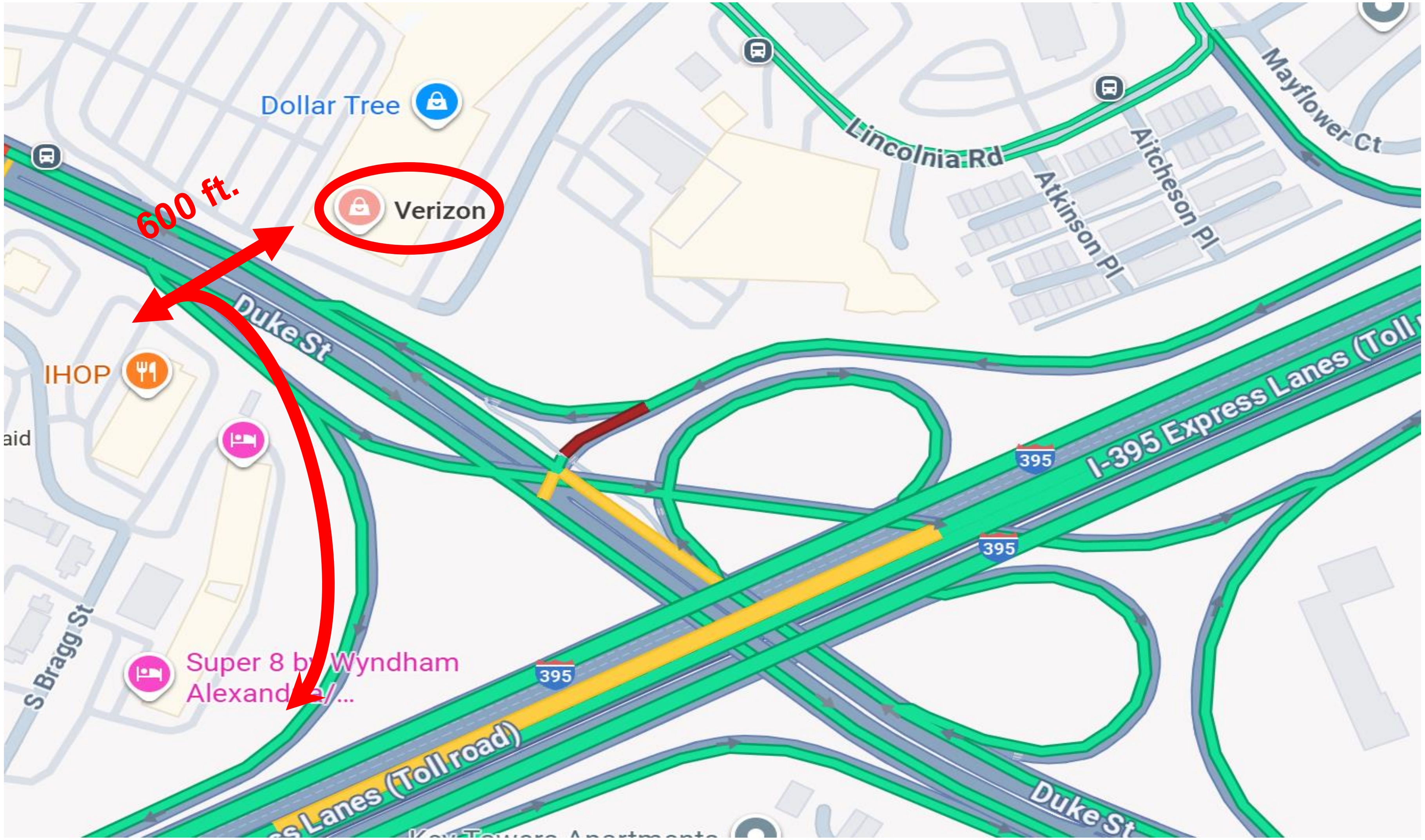
✓ Your order qualifies for FREE delivery. Choose this option at checkout.

Subtotal (3 items): **$56.97**

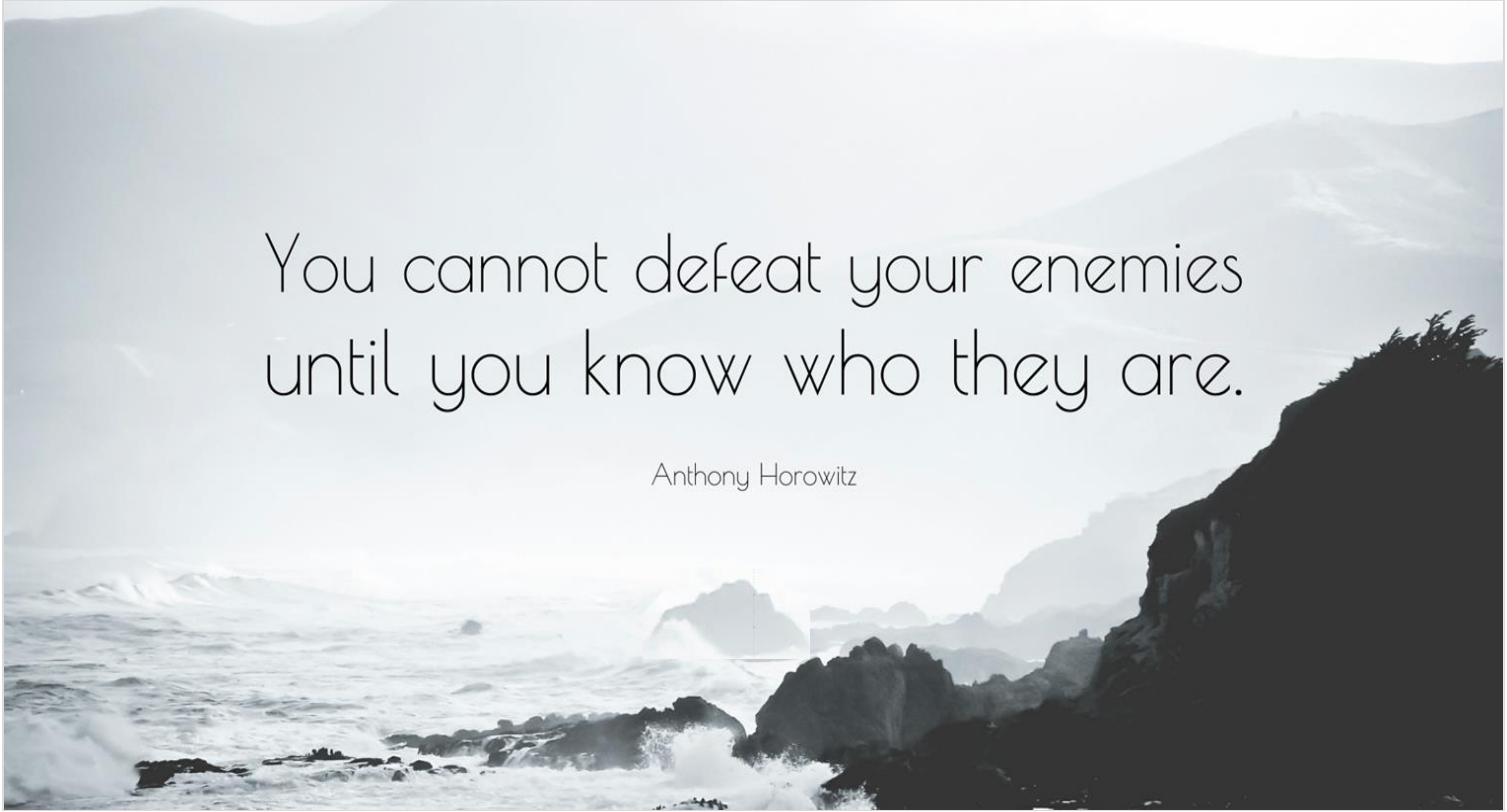
□ This order contains a gift

Proceed to checkout

Exfiltration: the shortest distance between me and “Outta here!”



To think how they think…

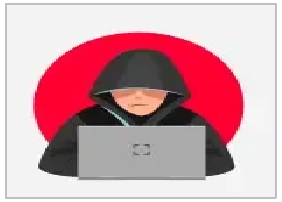


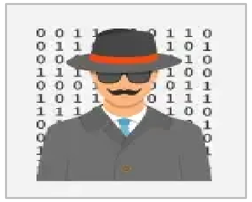
You cannot defeat your enemies until you know who they are.

Anthony Horowitz

Each type of adversary has different goals, targets & TTPs

Their goals, targets & TTPs shape *your* risk





Dimension	Hacktivists	Cybercriminals	Nation-State Actors
Primary Motivation	Ideological, political & social causes	Financial gain	Geopolitical advantage, espionage, sabotage
Target Selection	Symbolic (gov’s, firms, industries)	Opportunistic	Strategically valuable
Sophistication	Low-to-moderate; free hacker tools	Varies but moderate to high	High to untraceable
Common TTPs	Defacements, DDoS, leaks, doxxing	Phish, ransomware, cred theft, BEC	0-days, moles, LolBins, supply-chain
Resourcing	Un-/Self-funded	Profit-supported	State-backed, agency level funding
Organization	Volunteers, amateur collectives	Structured, professional businesses	Hierarchical, government-sponsored
Consequences	Embarrassment, reputational harm	Financial/operational loss, fines	NatSec risk, IP theft, kinetic conflict
Fear Factor	Aggravation, Embarrassment, $	Reputation loss, ops disruption, $$	Existential threat to firms, industries $$$
Examples	Anonymous, OpWallSt	Colonial Pipeline, Equifax, Target	SolarWinds, Stuxnet

Let’s Be Honest

Problem #1: Structural Disadvantages

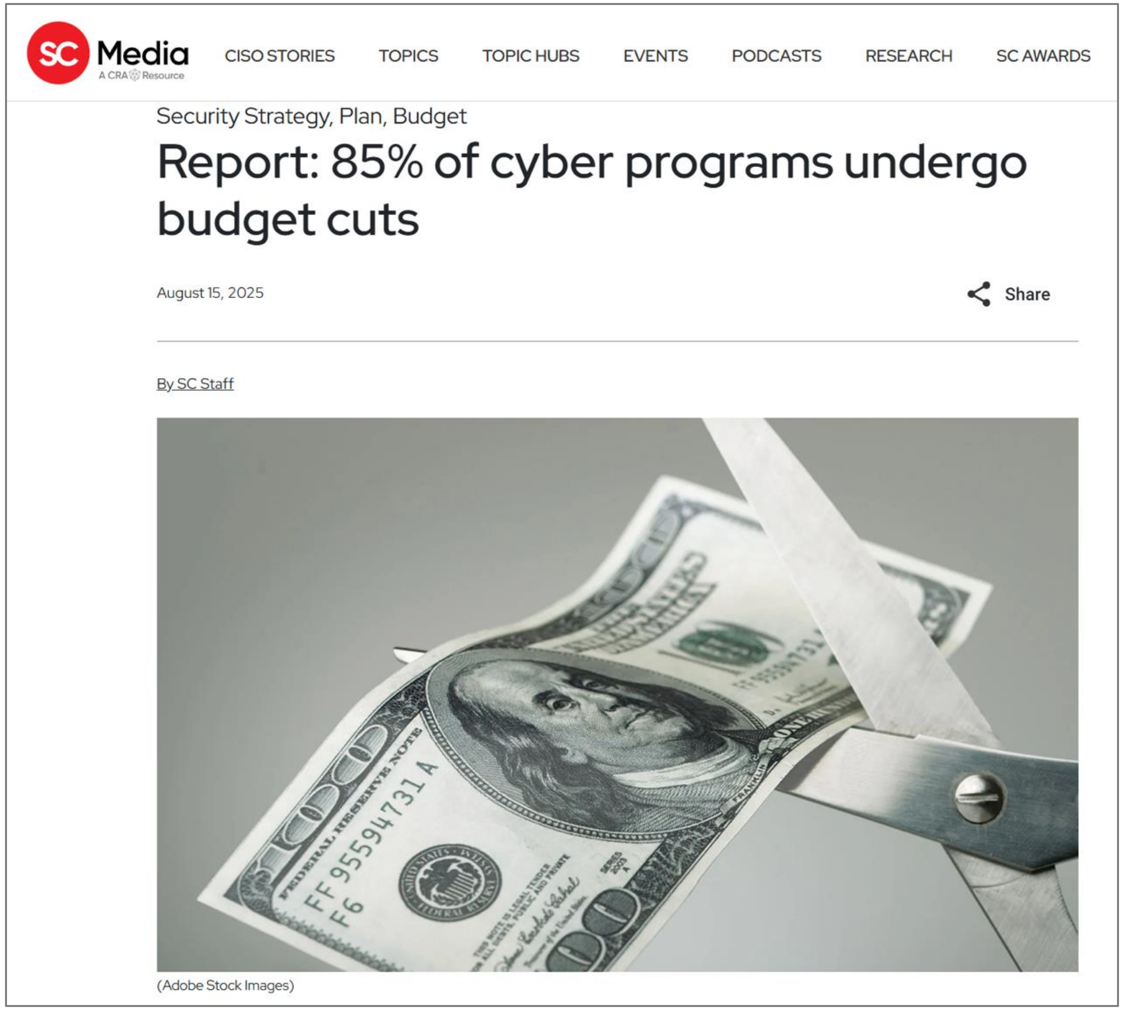
Some of what Good Guys have to worry about:

1. Operational stability/risk
2. Required Approvals
3. System interdependencies
4. Change freezes
5. BC/DR planning and rollback procedures
6. Skill shortages, holiday coverage and staffing
7. Team composition, turnover, careers and comp
8. Tooling costs, maintainability & integration
9. Fixed budgets amid expanding threats
10. Compliance (e.g. PCI; SOX; Graham-Leach-Bliley)
11. Oh, also compliance (e.g GDPR, CCPA/CCRA)
12. Then there's compliance (CMMC, NIST CSF, or maybe it's 800-53, or -171. Unless its ISO 27001?)

What Bad Guys have to worry about:

1. *Getting what they want*

Problem #2: Economics



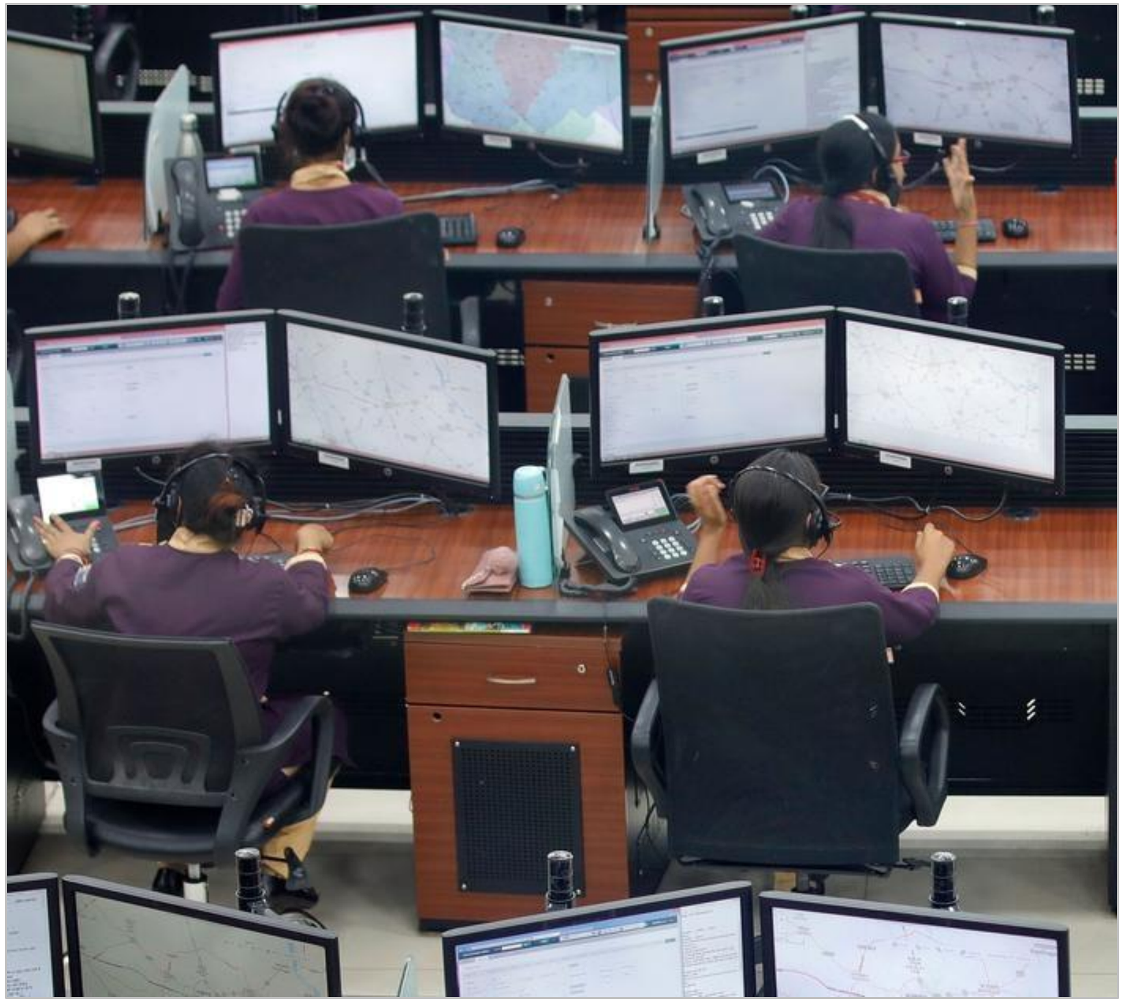
Security Strategy, Plan, Budget

Report: 85% of cyber programs undergo budget cuts

August 15, 2025

By SC Staff

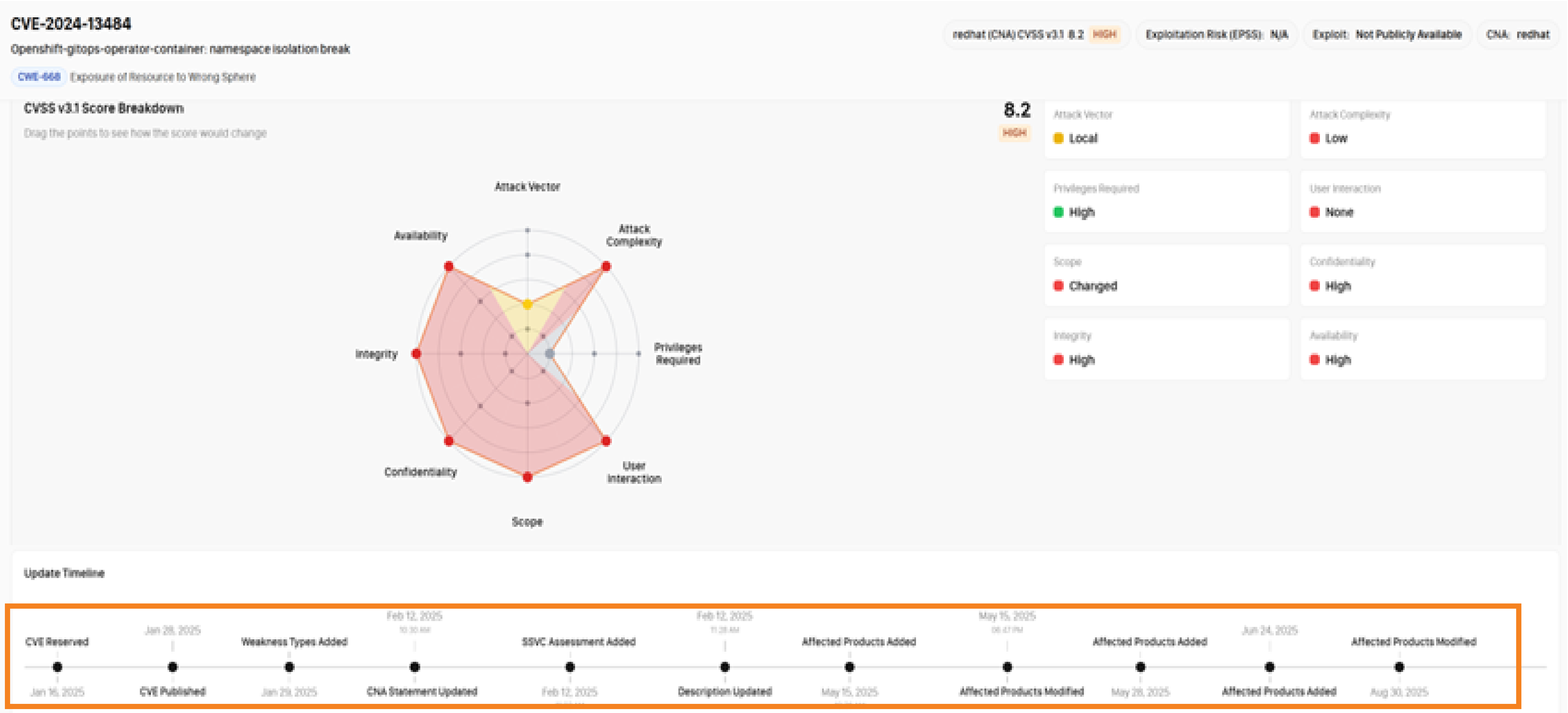
(Adobe Stock Images)



Us = Cost Center

Them = Profit Center

Problem #3: Time Scales – Ours...



CVE-2024-13484

Openshift-gitops-operator-container: namespace isolation break

CWE-668 Exposure of Resource to Wrong Sphere

redhat (CNA) CVSS v3.1 8.2 HIGH | Exploitation Risk (EPSS): N/A | Exploit: Not Publicly Available | CNA: redhat

CVSS v3.1 Score Breakdown

Drag the points to see how the score would change

8.2 HIGH

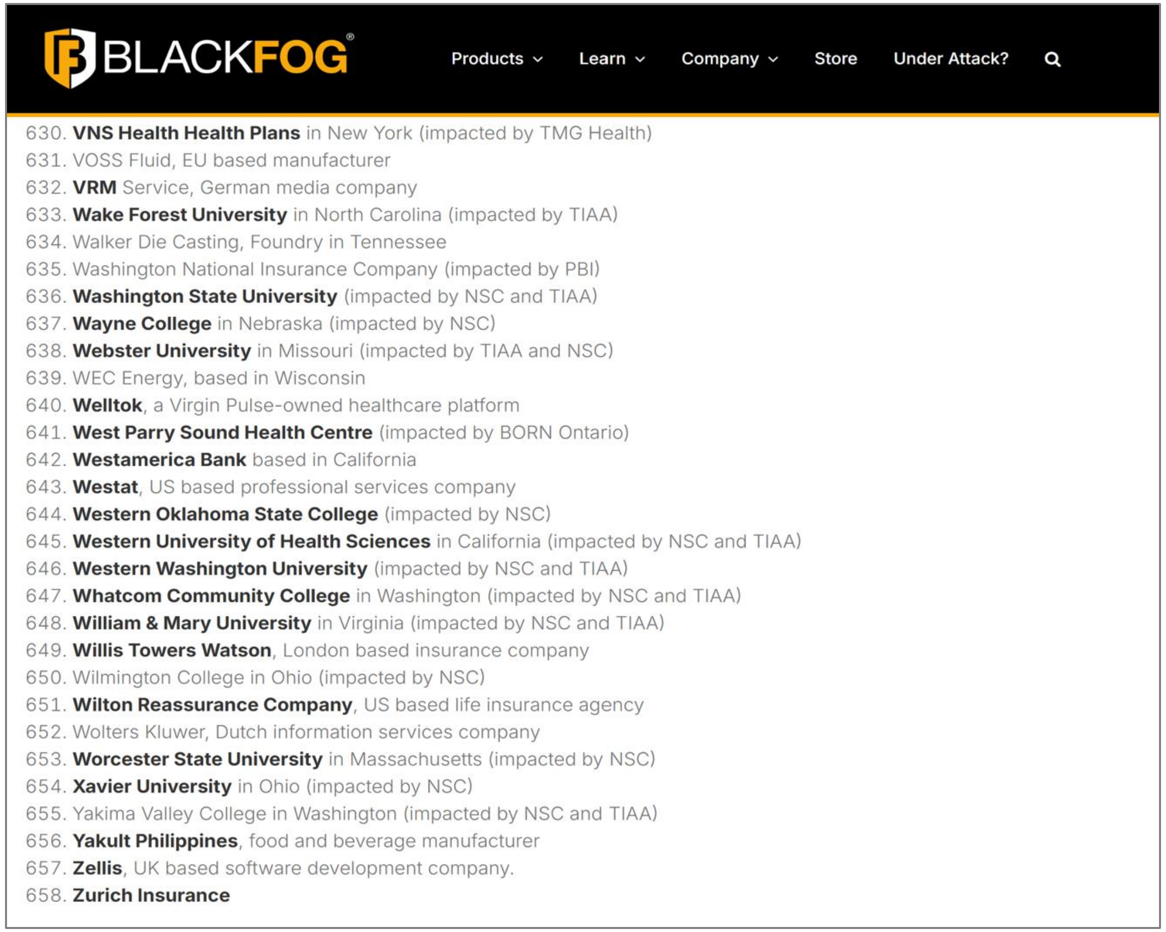
Attack Vector 🟨 Local	Attack Complexity 🟥 Low
Privileges Required 🟩 High	User Interaction 🟥 None
Scope 🟥 Changed	Confidentiality 🟥 High
Integrity 🟥 High	Availability 🟥 High

Update Timeline

- CVE Reserved – Jan 16, 2025
- CVE Published – Jan 28, 2025
- Weakness Types Added – Jan 29, 2025
- CNA Statement Updated – Feb 12, 2025 10:30 AM
- SSVC Assessment Added – Feb 12, 2025
- Description Updated – Feb 12, 2025 11:28 AM
- Affected Products Added – May 15, 2025
- Affected Products Modified – May 15, 2025 06:47 PM
- Affected Products Added – May 28, 2025
- Affected Products Added – Jun 24, 2025
- Affected Products Modified – Aug 30, 2025

Problem #3: Time Scales – vs. Theirs

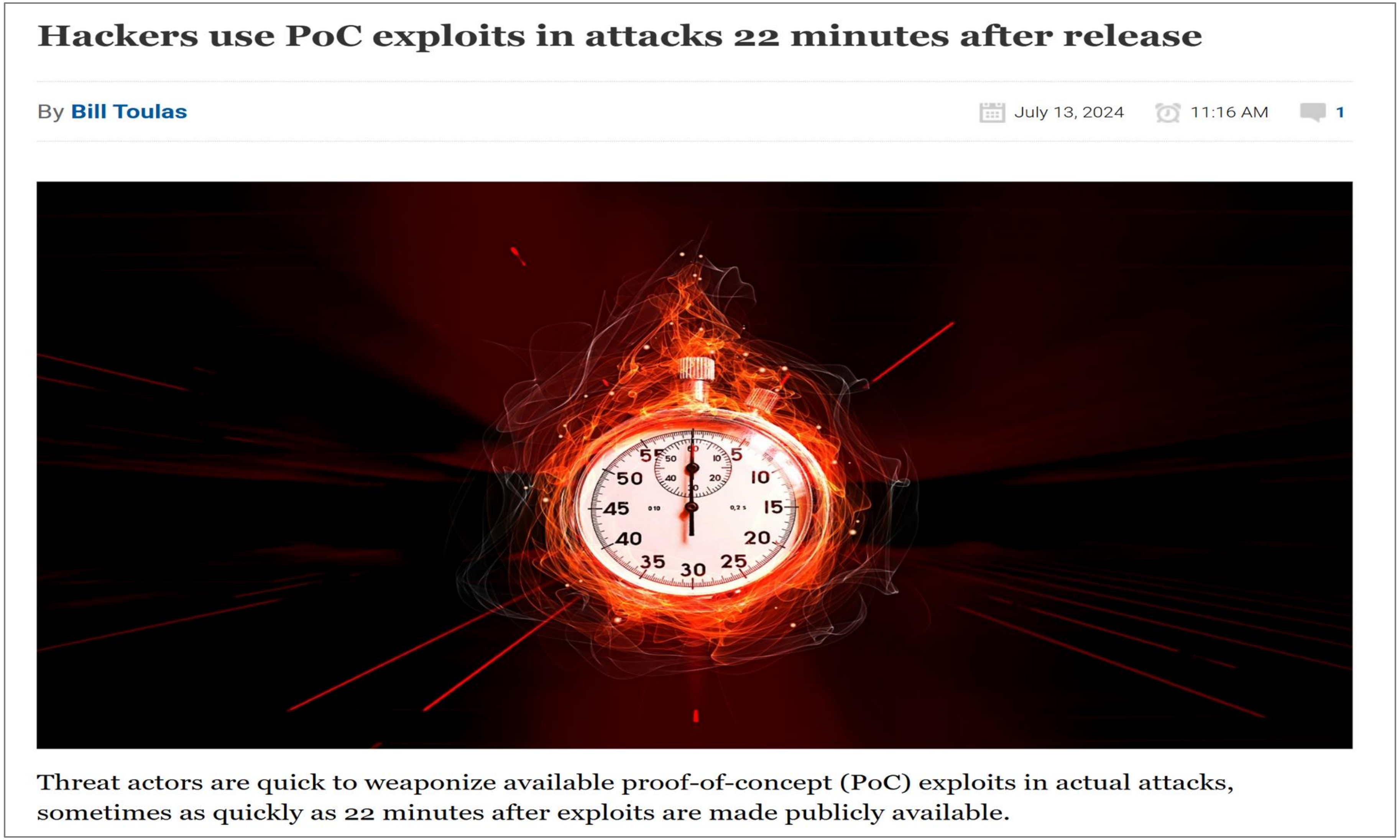
What we know about the MOVEit exploit and ransomware attacks



630. **VNS Health Health Plans** in New York (impacted by TMG Health)
631. VOSS Fluid, EU based manufacturer
632. **VRM** Service, German media company
633. **Wake Forest University** in North Carolina (impacted by TIAA)
634. Walker Die Casting, Foundry in Tennessee
635. Washington National Insurance Company (impacted by PBI)
636. **Washington State University** (impacted by NSC and TIAA)
637. **Wayne College** in Nebraska (impacted by NSC)
638. **Webster University** in Missouri (impacted by TIAA and NSC)
639. WEC Energy, based in Wisconsin
640. **Welltok**, a Virgin Pulse-owned healthcare platform
641. **West Parry Sound Health Centre** (impacted by BORN Ontario)
642. **Westamerica Bank** based in California
643. **Westat**, US based professional services company
644. **Western Oklahoma State College** (impacted by NSC)
645. **Western University of Health Sciences** in California (impacted by NSC and TIAA)
646. **Western Washington University** (impacted by NSC and TIAA)
647. **Whatcom Community College** in Washington (impacted by NSC and TIAA)
648. **William & Mary University** in Virginia (impacted by NSC and TIAA)
649. **Willis Towers Watson**, London based insurance company
650. Wilmington College in Ohio (impacted by NSC)
651. **Wilton Reassurance Company**, US based life insurance agency
652. Wolters Kluwer, Dutch information services company
653. **Worcester State University** in Massachusetts (impacted by NSC)
654. **Xavier University** in Ohio (impacted by NSC)
655. Yakima Valley College in Washington (impacted by NSC and TIAA)
656. **Yakult Philippines**, food and beverage manufacturer
657. **Zellis**, UK based software development company.
658. **Zurich Insurance**

Hackers found a MoveIT 0-day…and hit 500+ firms *at once*, three days before the flaw was *announced*, let alone patched

Problem #3: Time Scales – vs. Theirs



Hackers use PoC exploits in attacks 22 minutes after release

By **Bill Toulas** July 13, 2024 11:16 AM 1

Threat actors are quick to weaponize available proof-of-concept (PoC) exploits in actual attacks, sometimes as quickly as 22 minutes after exploits are made publicly available.

So we’ve thought about who we’re up against

Now we can talk about how they might look at you

SYNERCOMM

Example: EAS enumeration

How we might do it:

- IP address management (IPAM)
- Cloud asset management APIs
- Configuration management databases
- Web server logs
- Enterprise DNS

How they might do it:

- Passive DNS
- IP/ASN leasing and ownership hierarchy
- Certificate Transparency Logs e,g, Certstream
- OSINT tools e.g DNS dumpster, OSINT.sh etc.
- Global scanners, e.g. Shodan, Censys
- Open-Source tools, e.g. AMASS, Subfind3r etc.
- Active scanning e.g. ZMAP

Our view is IT-centric, and often focuses on completeness, structure and clarity. This is entirely logical *from our perspective*

Their view is opportunity-centric, and often focuses on exposed lowers, login pages, weak ciphers etc., entirely logical *from their perspective*

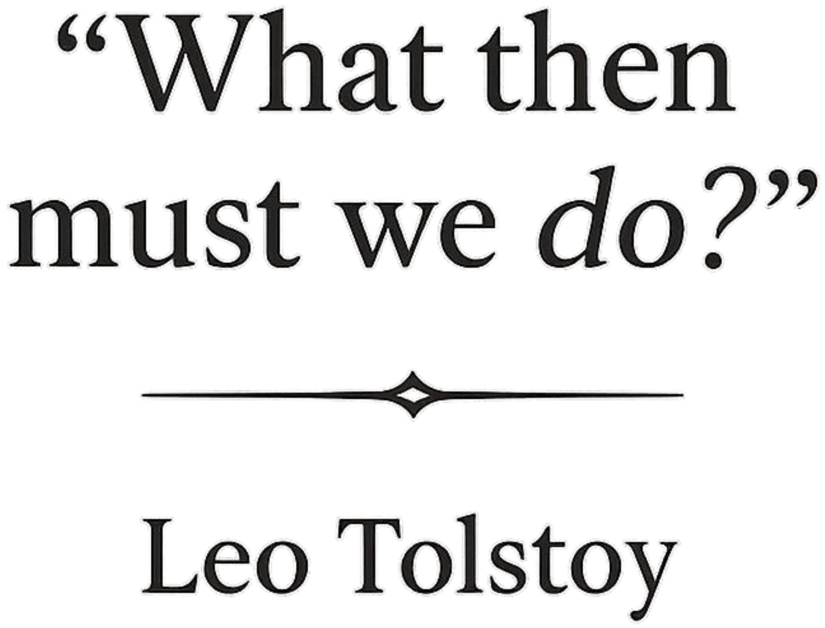
Scary story time

SYNERCOMM

A framework for how I look at my assets (both ways)

The Question I Ask	What It Tells Me (Assuming the role of Attacker)	Why I Care (As the defender assessing risk)
Who am "I" in this scenario?	My goals, motivations, and therefore likely targets	Can inform my view of adversary sophistication, likely TTPs, Initial Access vectors and point to likely at-risk systems & data
What kind of asset is it?	Does the tech match either my targets of interest and/or my skills, toolset and knowledge, aka "Should/can I hit this?"	Everyone has finite resources, and work must be prioritized; my potential attacker may bias toward certain systems; use that intel & stack rank risk remediation work
Where do I think it's located?	Geography, ISP, physical owner etc. may influence my interest level, e.g. familiarity with security controls, insider access, DAB offers, likelihood of prosecution etc.	Security maturity almost always varies by location (by cloud, by data center, by country, facility or office) etc. Risk ranking drives intelligent prioritization
How important might it be?	Whatever says "more important" – naming conventions, login access, payment-related or core to customer journeys – says "worth more to ransom, hurts more if I break it."	Prioritizing importance to the business is obvious; What's not is whether *your* view of the importance aligns to what the attacker can observe and the likely conclusions THEY draw
How valuable is the stuff inside?	This is not quite the same as above; Importance to the victim is one axis of importance; market/sale value of data is another, and is distinct	Once again, attacker profile is key here; ATPs and hacktivists may be content to break things; criminals want to monetize; NOT the same priorities
What observable controls protect it?	The more layers of defense I can observe, the faster I will pivot to lower LOE options	My most valuable assets may be well-layered and protected; less hardened targets may be down my list, but high on the attackers; this leads to misaligned prioritization

The Big Question



“What then must we *do*?”

Leo Tolstoy

Use our new perspective to rebalance the scales

Problem #1: Structural Disadvantages

Problem: Bue Teams with too much to deal with

Options: Enlist " good bad guys"

1. Build a red team (in house, offshore etc.)
2. Hire outside pen-testers
3. Run TTX's and Attack Simulations
4. Script automated control validation tests
5. Start a VDP or Bug Bounty Program
6. Build and attack a "digital twin" or cyber range
7. Deploy honeypots and lures and hold CTFs

Problem #2: Economics

Problem: We're a cost center, they make profit

Options: Show sources of value that aren't all ROI

1. Threat Detection & IR KPIs –improved operational performance
2. Attacks stopped with loss estimates from similar/peer failures (e.g. MGM)
3. Fuse cyber and anti-fraud use cases to show revenue protection or recovery
4. Peer/industry benchmarking
5. Litigation-proofing
6. Compliance adherence/audit risk
7. Diligence preparedness for funding or M&A

Problem #3: Time Scales

Problem: Disciplined Ops vs. Smash & Grab

My view: This one is not easy, but it is simple

I believe there is only one way to compete on this field. You *must* invest in attacking your own estate, as hard and as often as you can afford.

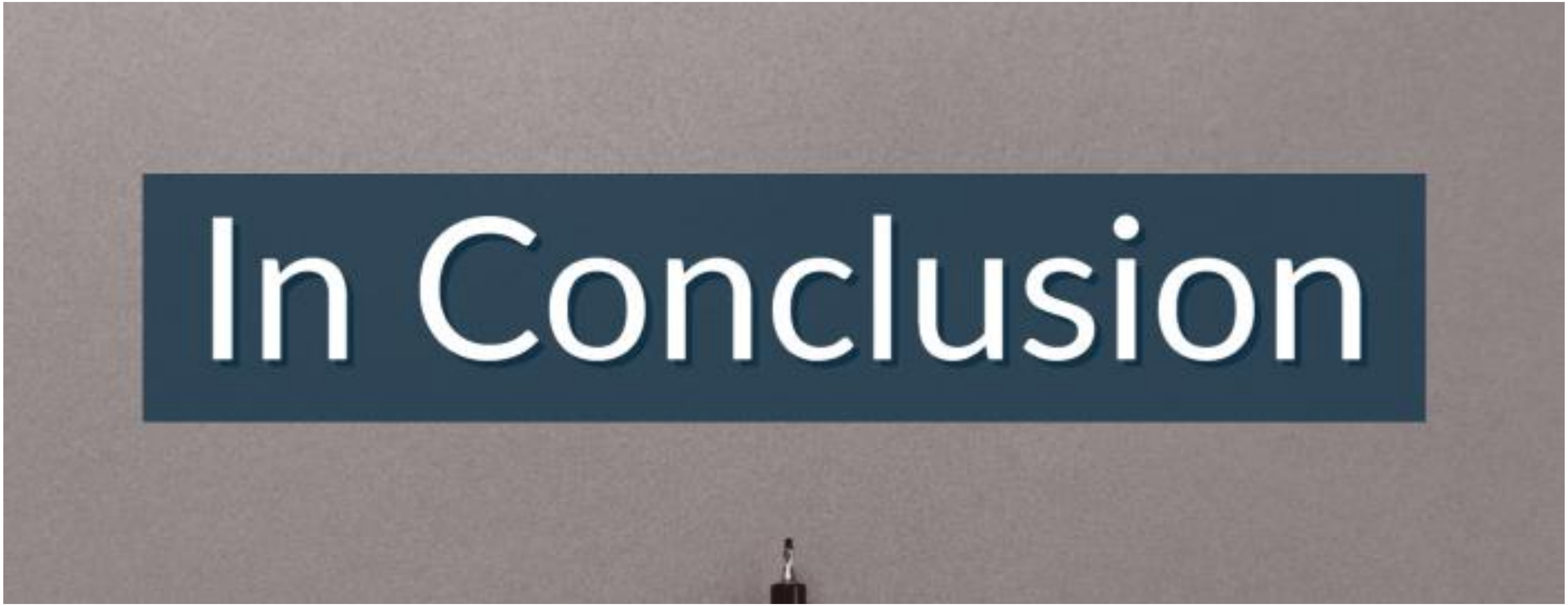
1. Periodic, human-driven ***"gloves off"*** *testing*

2. Attack plans for ***business logic exploitation***, not just technical vulnerabilities and control gaps

3. ***Continuous, aggressive, automated*** probing of your external attack surface

4. RCA metrics on findings; find the weak spots in your SDLC and ***call out recurring problems***

Wrap Up



Downloadable Matrix Pages at opensourcery.io/blog/synercomm

Has this changed your view? Let me know

Thank you!