

Anatomy of a Physical Penetration Test

Recon to Reporting

Ken Smith | NavPoint Alpha

ABOUT THE SPEAKER



Ken Smith

Founder & CEO, NavPoint Alpha

Director of Solutions & Strategic Partnerships, CyberproAI

Over fifteen years in offensive security across consulting, industry, and education, building NavPoint Alpha as a purpose-built platform for physical security assessments and mission coordination.

- Former U.S. Army Signals Intelligence Operator, 5th Special Forces Group (Airborne)
- A decade teaching information security at the University of Mount Union
- Cleveland native and active mentor in the security community

BOARDS BSidesCLE | Burning River Cyber Con | eCenter@LindenPointe

CONNECT
linkedin.com/in/signalsec

SHOW OF HANDS

How many of you are, or have been, a physical penetration tester?

DISCUSSION

What problems have you encountered with physical pentests (as a tester or a client)?

WHAT WE HEAR

The Same Problems, Every Time

Different testers, different clients, the same short list. Every one of these is something this talk sets out to fix.

Inconsistent documentation

Findings reconstructed from memory, not captured as they happen

No standards

No shared frameworks for how a physical test should be run

No formal training

Skills passed down ad hoc, with few paths to build them deliberately

Loose methodologies

Company-specific, improvised approaches that vary by operator

Inconsistent reporting

Deliverables that read like war stories instead of actionable risk

Weak safety planning

Operator safety and deconfliction left to chance in the field

This Is Not a War Story Talk

The controls have standards. The testing does not.

- Physical security has mature standards: ANSI/ASIS guidance, plus physical control requirements in HIPAA, PCI DSS, and more
- What is missing is a standard for testing whether those controls actually hold
- So the testing stays improvisational: unusable deliverables, operators in danger, and a marginalized discipline



WHEN IT GOES WRONG

The Stakes Are Real

Few security disciplines can get you detained, injured, or arrested. This one can.

Armed security

Guards and K9 units, and the potential for a physical confrontation.

Scoping sets deconfliction and challenge protocols.

Law enforcement

Responding officers who have no idea an authorized test is underway.

An authorization letter and a live contact prevent an arrest.

Hazardous sites

Explosive, electrical, and industrial environments with real danger.

Restricted zones and shutdowns are mapped in advance.

Legal exposure

Operators and clients both carrying genuine liability.

Signed authorization defines exactly what is sanctioned.

> The line between an authorized assessment and a crime is airtight scoping and the authorization letter in your pocket. That is what keeps operators safe.

PHASE 1

Scoping & Rules of Engagement

What Scoping Actually Covers

Engagement Definition

- Success criteria and objectives
  what a win looks like for this engagement
- In-scope and out-of-bounds targets
  the buildings and areas that are off-limits
- Time windows and constraints
  when testing can and cannot happen
- Authorized techniques and limits
  lock picking, tailgating, forced entry

Safety & Legal

- Letter of authorization
  the document that keeps you out of jail
- Emergency contacts and abort procedures
  who to call, and when to stop
- Law enforcement notification
  whether local police are told in advance
- Who knows, and who does not
  the client's internal awareness list

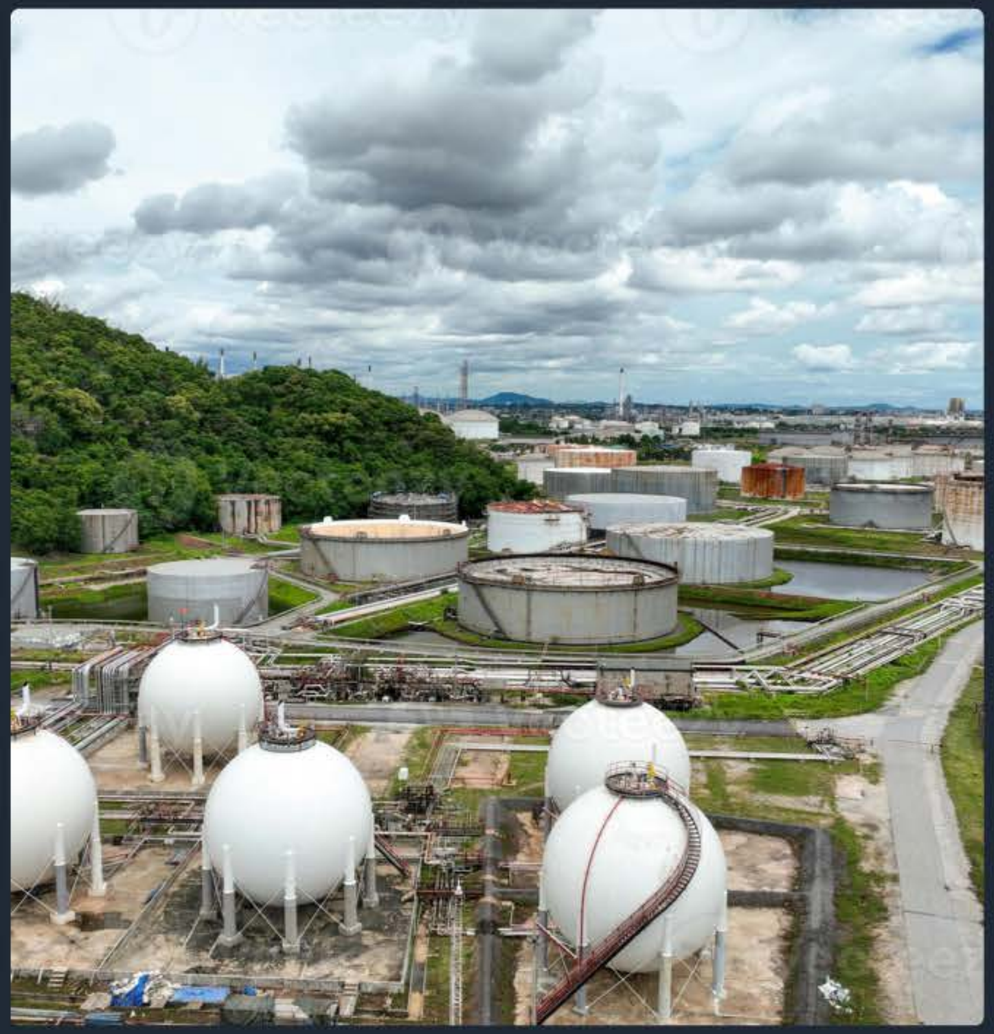
> You are potentially breaking into facilities with armed security, K9 units, and hazardous materials. Scoping is where you address the fact that this job can get you hurt, arrested, or worse.

SCOPING EXAMPLE

The Natural Gas Facility

What does scoping look like when the target has explosive infrastructure?

- Physical hazards and restricted zones
- Emergency shutdown procedures
- Operator safety protocols in the rules of engagement
- Intrinsically safe equipment only; no ignition sources
- Mandatory site escort and check-in procedures
- Evacuation routes and muster points



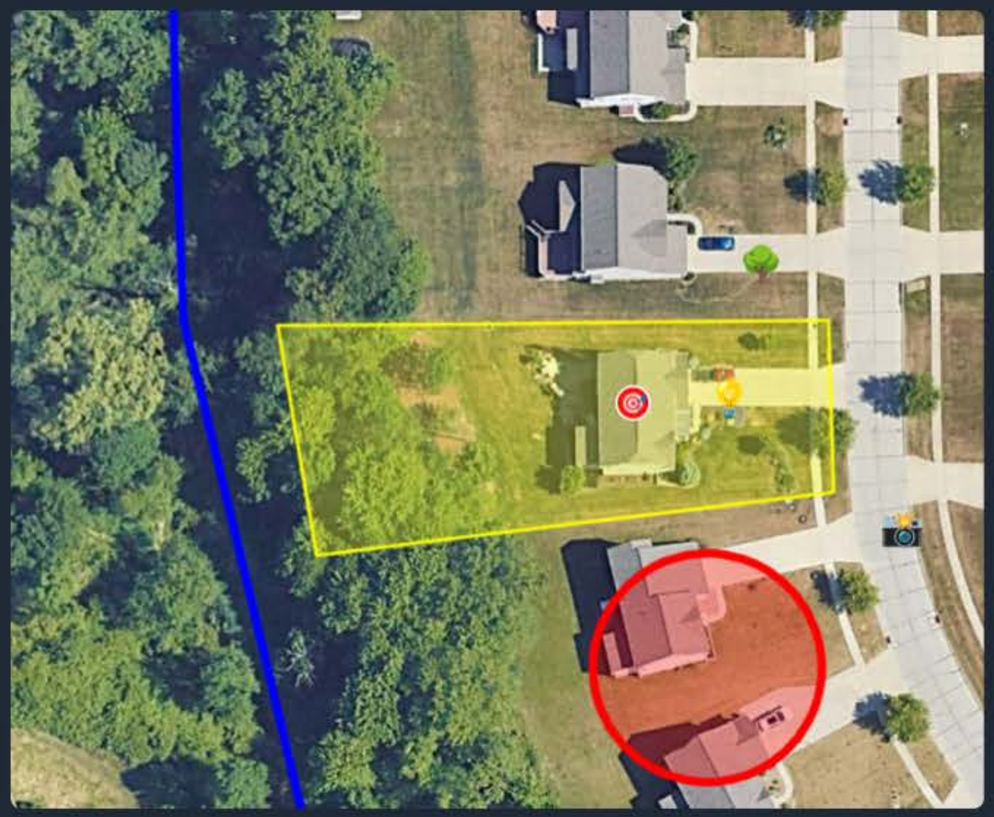
PHASE 2

Reconnaissance

The engagement is won or lost in recon.

Remote Reconnaissance

- OSINT and social media review
- Satellite and aerial imagery analysis
- Press coverage review
- Pretext development
- Entry point identification from remote sources



> **Repeatability:** documented processes and consistent tooling keep recon quality the same regardless of the operator, the size of the facility, or the client industry.

REMOTE RECON

The Badge in the Press Photos

Found the front and back of an employee badge in high-resolution press photography, then created derivative copies.

3
year engagement

19
facilities

All
breached



On-Site Reconnaissance

- Physical surveillance and pattern of life
- Guard patrol timing and route mapping
- Badge and access control observation
- Clothing and pretext intelligence
- Infil / exfil planning and opportunistic discovery



> Infil / exfil route planning is part of the methodology, not improvisation.

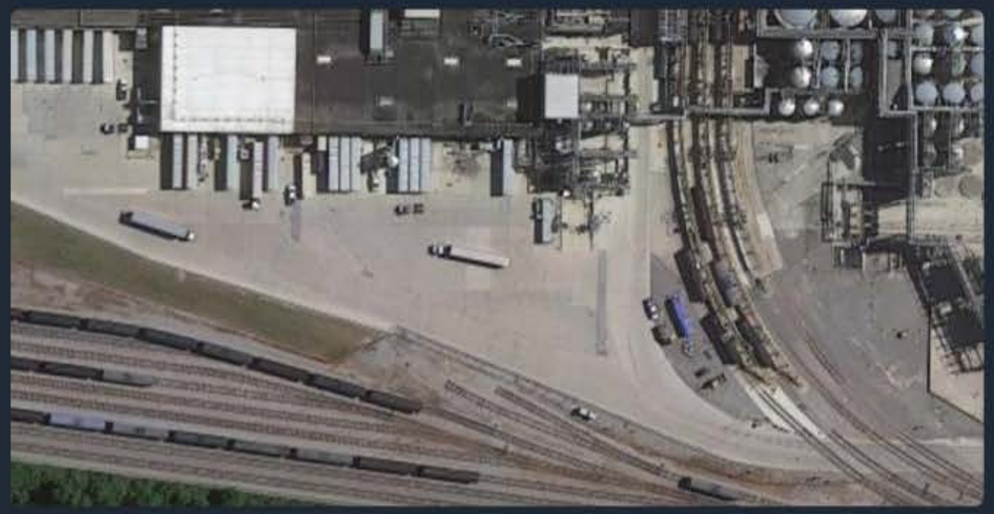
ON-SITE RECON

Under the Train

Rural manufacturing facility. Any vehicle approach would be conspicuous. Parked at a running trail two miles away and walked the railroad tracks in.

Sat under a stationary train for two hours observing an entrance door. Timed patrols, noted clothing, assessed badge usage.

Exfiltrated via the same route.





ON-SITE RECON

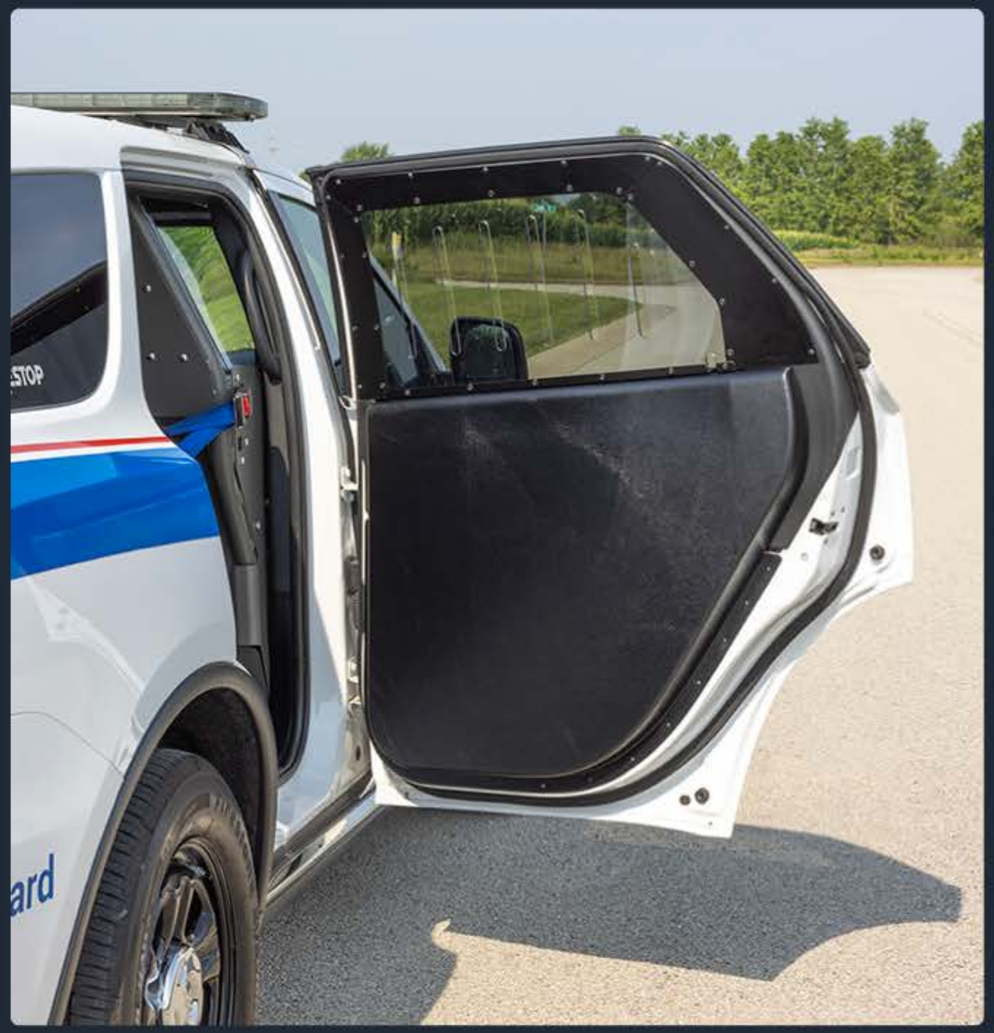
The Guard's Vehicle

Hospital campus. A guard force vehicle left unlocked.

Inside: a site map with patrol routes, a training plan, and a spare uniform.

Documented everything. Removed nothing.

> **Finding:** unsecured guard force assets exposing patrol routes, schedules, and training documentation.



PHASE 3

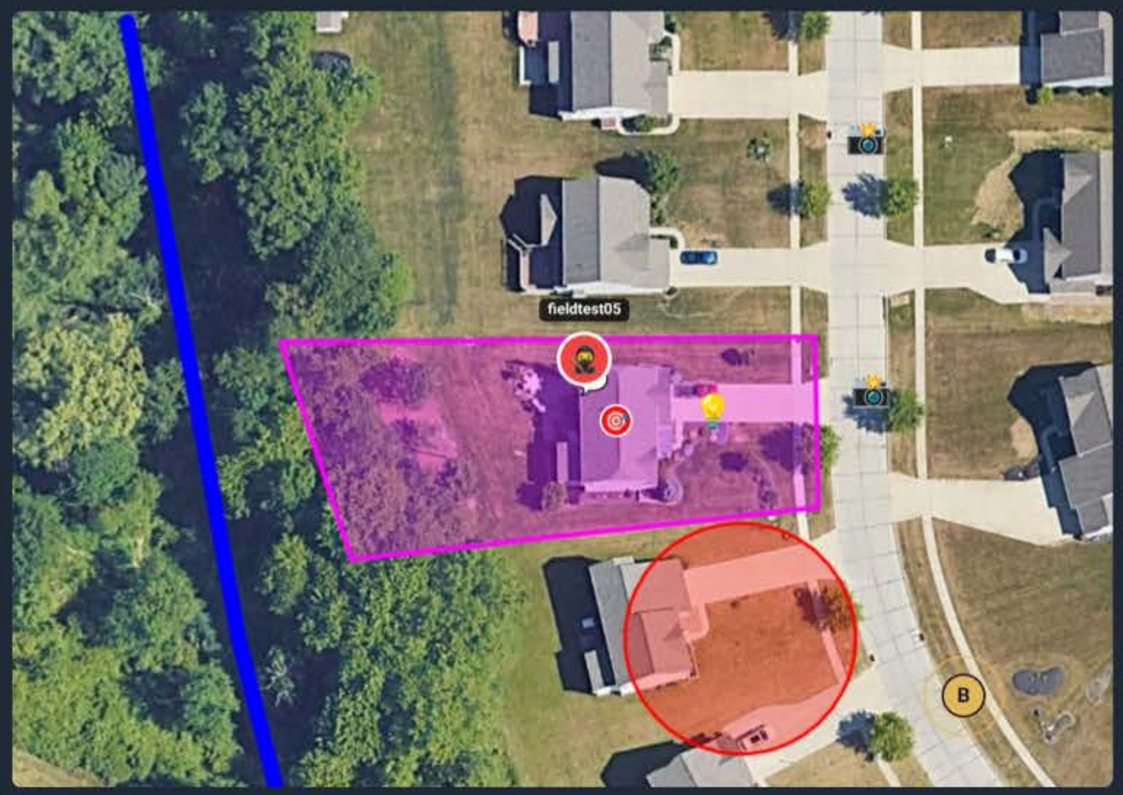
Execution

3

Execution: Discipline Over Improvisation

This is the phase people picture when they imagine physical testing. In practice it runs on discipline, not adrenaline: every move is deliberate, and every finding is captured the moment it happens.

- Objectives that define success
- Pretext selection
- Entry techniques
- Real-time documentation
- OPSEC on target
- Operator-to-command coordination
- Operator safety and abort criteria
- Knowing when to exfiltrate



> You cannot reconstruct findings from memory two weeks later and produce a credible report.

EXECUTION

The Power Cooperative

Breached the training and maintenance facility and set off an alarm. The organization reset it without ever searching the building.

We were already gone. Police brought dogs.

OPERATOR SAFETY & ABORT CRITERIA

Police deployed K9 units, a response never discussed with the client in scoping. Had the team still been on site, it becomes a serious safety incident.

OPERATOR-TO-COMMAND COORDINATION

The client point of contact was in the comms chain but never stepped in to tell responding officers this was an authorized exercise.





EXECUTION

The Research Lab: Two Layers of Failure

False tailgate at the IR beam security gates. The gates had been installed for a year and never activated. Both testers walked in unchallenged.

Then, access to the research labs themselves. The door code was **1-2-3-4**.





Layer 1: social engineering bypass plus access controls that were never enabled.

Layer 2: trivially weak access codes on the most sensitive spaces.

REAL-TIME DOCUMENTATION

Shaky, phone-in-hand video of the breach proved decisive when the security vendor later disputed our results to protect its contract.

OBJECTIVES & SCOPE

Lab staff were furious we had entered, but the executed contract and the signed letter of authorization both put the lab interiors explicitly in scope.

PHASE 4

Reporting & Remediation

The Deliverable Is the Product

Everything before this phase was in service of producing a report that drives action.

WAR STORY	ACTIONABLE FINDING
"I got in through the roof hatch."	"Unmonitored roof access lacked physical controls, intrusion detection, and surveillance coverage, exposing the administrative suite to an uncontrolled entry vector."
"I tailgated a guard through the loading dock."	"A staffed loading dock had no anti-tailgating enforcement, allowing piggyback entry behind an authorized employee."
"The server room was unlocked, so I walked right in."	"A critical server room relied on a single mechanical lock, left disengaged, with no access logging or secondary control."

A Common Language for Findings

FORTRESS Framework

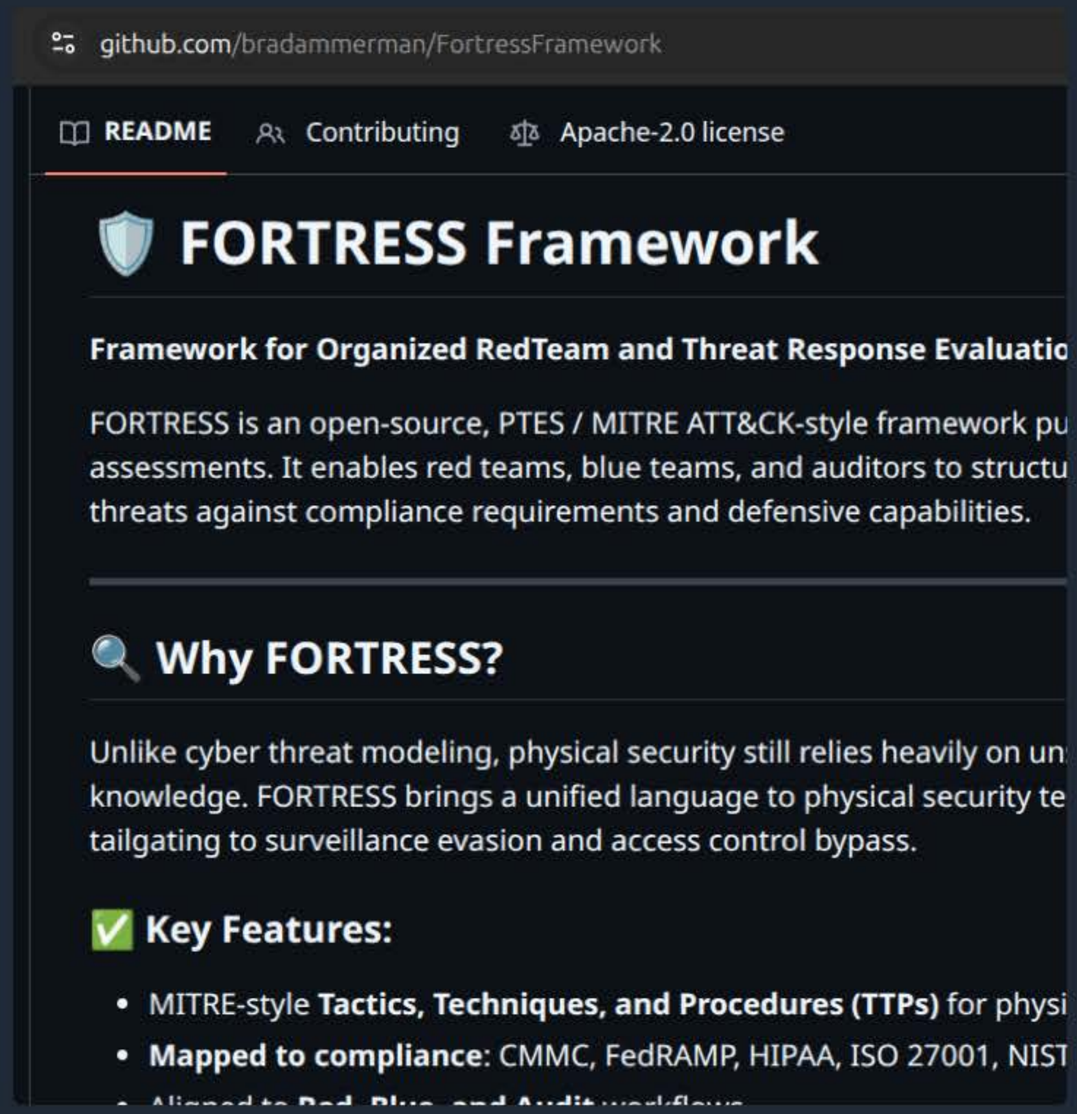
Created by Brad Ammerman

236+ physical security controls

60+ mapped compliance frameworks

"The PTES equivalent for physical security."

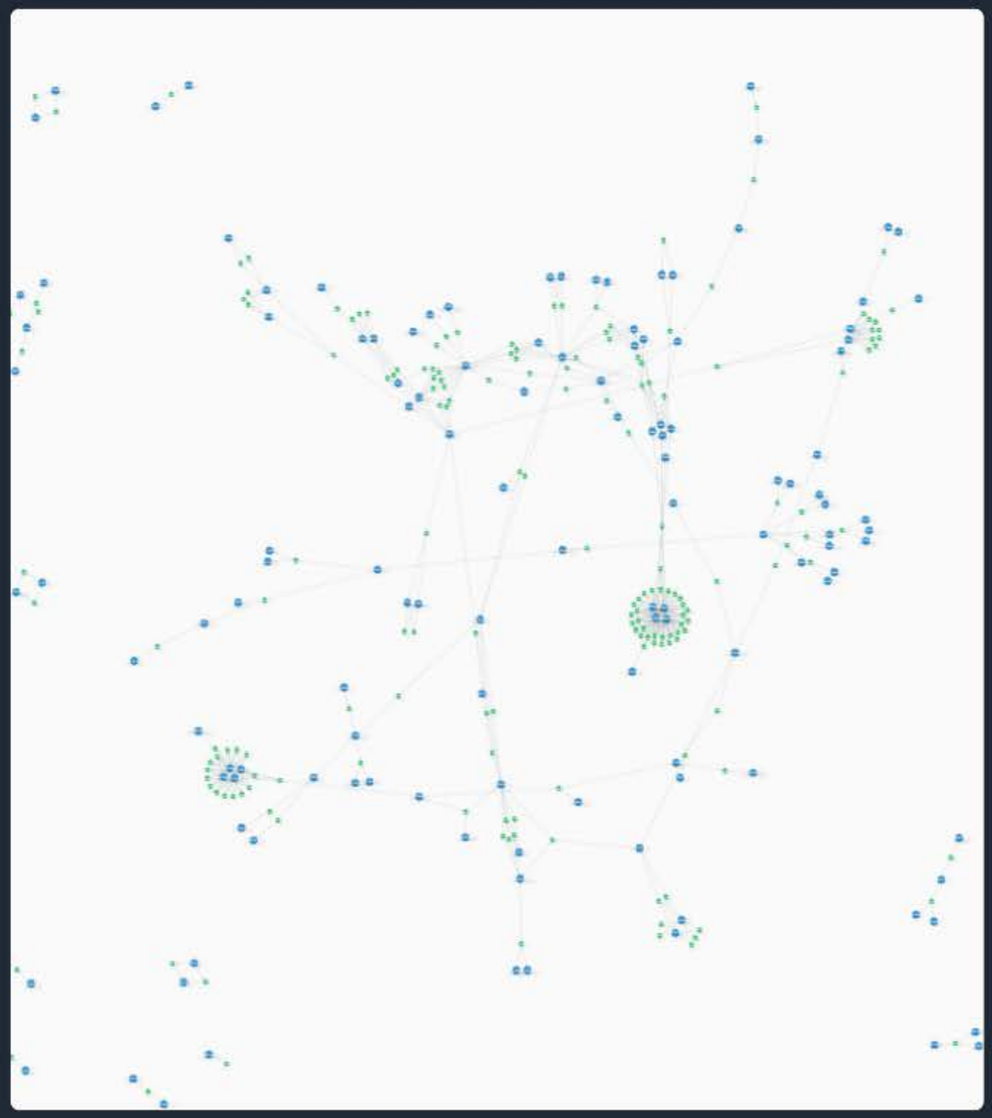
`fortressframework.com`



Mapping Findings to What Clients Care About

- Map every finding to controls and compliance frameworks
- Executive summaries tied to business risk
- Tactical and strategic recommendations
- Longitudinal tracking of remediation
- Standardized templates for repeatable, comparable reports

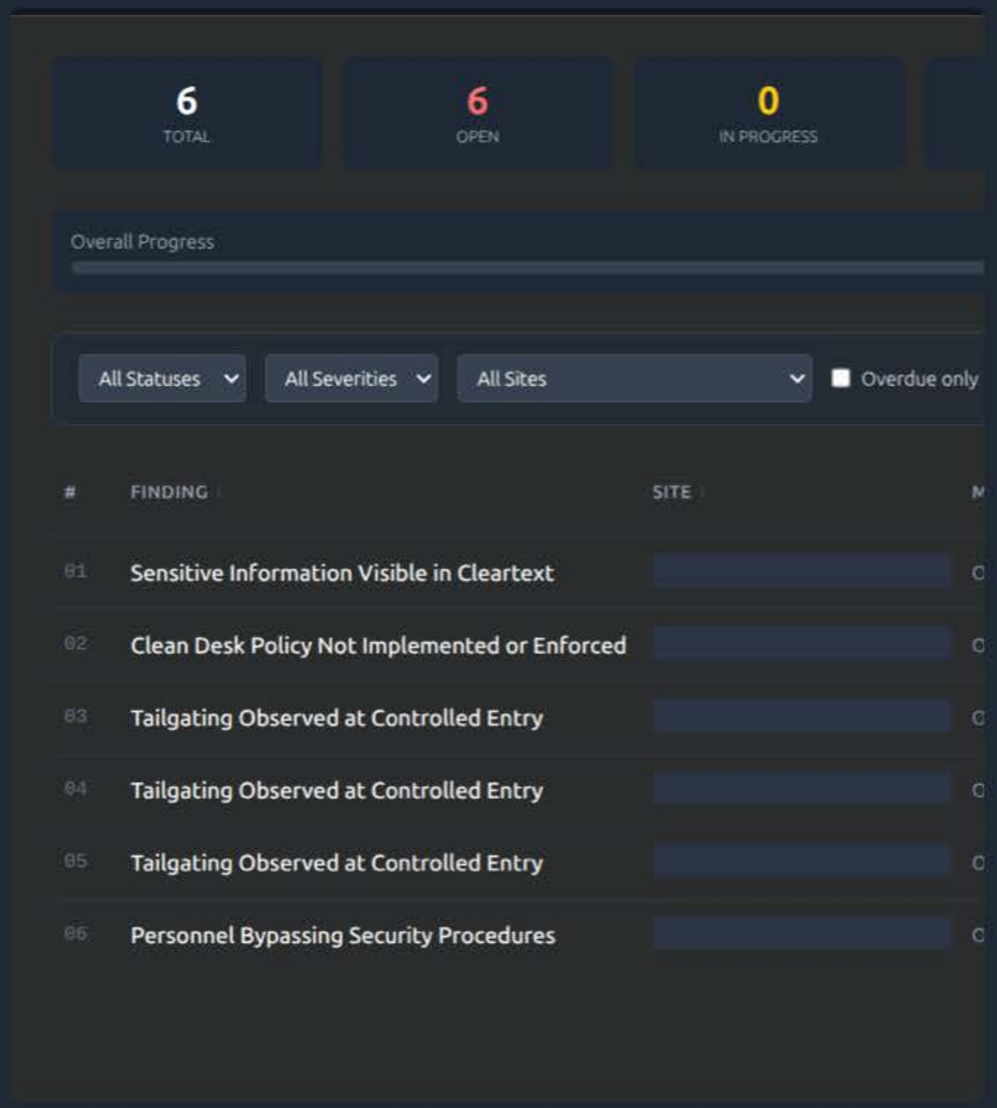
Common language: findings map through the framework into the standards clients answer to, from FedRAMP and HIPAA to PCI DSS, ISO 27001, and NIST 800-53.



The Long Game: Tracking Remediation Over Time

The badge engagement ran three years across 19 facilities. Longitudinal data shows remediation progress, or the lack of it.

The report is not a one-time event. It is the beginning of a security improvement program.



CASE STUDY

The Midwest Facility

One engagement, every phase, from scoping to remediation.

CASE STUDY · THE MIDWEST FACILITY

Scoping

- One site within a larger, multi-facility program
- Two factory floors, office space, and a cafeteria
- The major employer in the area
- 24-hour floor operations; offices staffed daytime only

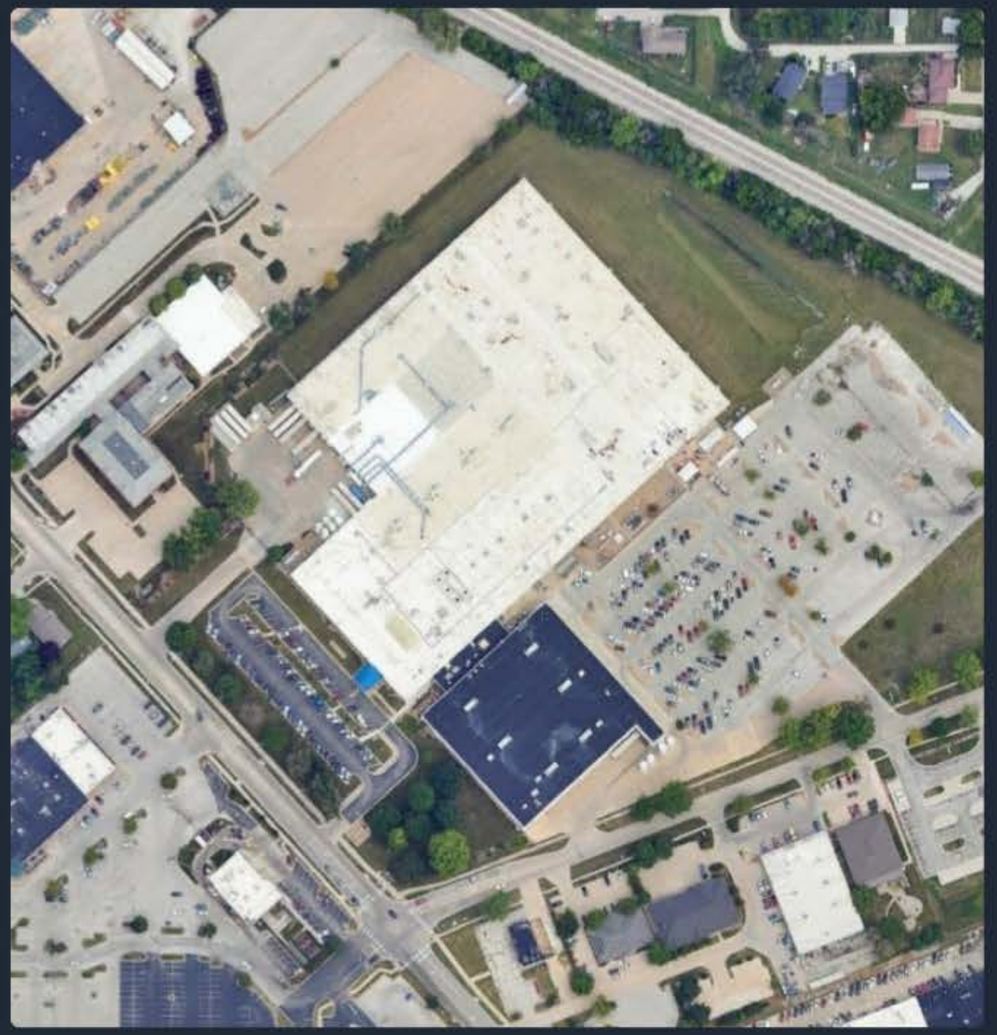


CASE STUDY · THE MIDWEST FACILITY

Remote Recon

- Mapped entrances, exits, and spoofable employees
- Google Maps proved very useful for IMINT
- Built a pretext: corporate inspectors auditing wireless and hardware tags





CASE STUDY · THE MIDWEST FACILITY

On-Site Recon

- Bought branded work clothing secondhand at Goodwill
- The major local employer, so even branded clipboards turned up
- Exposed I-beams ran vertically around the outer wall of the factory space, spaced about 50 feet apart
  - Not visible on Maps or StreetView
  - A reminder not to just dive in on remote recon alone



CASE STUDY · THE MIDWEST FACILITY

Execution: The Front Door

- **First attempt:** front-door breach as "wireless assessment" inspectors
- Tailgated in behind an employee at the main entrance
- No directory photos; a known name plus a prepared ID carried it
- Dressed the part of a corporate employee: branded attire and clipboard from on-site recon
- Both factory floors breached



CASE STUDY · THE MIDWEST FACILITY

Execution: The Roof

- **Second attempt:** failed when a tailgate attempt was caught at the interior door between office and lunch room
- The consultant extracted himself without surrendering the letter
- **Third attempt:** shimmied up one of those I-beams and walked the roof path mapped in remote recon
- Dropped through the roof hatch straight into the office space



CASE STUDY · THE MIDWEST FACILITY

Reporting & Remediation

- No compliance box-checking; the program was driven by real risk, agreed up front
- The real value: findings tied to trends across every facility, good and bad

Repeatability: standardized report templates kept every facility consistent and comparable, turning one engagement into a program-wide trend line.



Raising the Bar

- Repeatable methodology & tooling
- Real-time documentation
- Defensible reporting
- Operator safety

These are what separate a professional engagement from a break-in with a statement of work.

Thank You

CONNECT ON LINKEDIN

linkedin.com/in/signalsec

CONTACT

Ken Smith · ken@navpointalpha.com

EXPLORE & SUPPORT THE COMMUNITY

NavPoint Alpha · navpointalpha.com

FORTRESS Framework · fortressframework.com Brad Ammerman

BSidesCLE · bsidescle.com

Burning River CyberCon · burningrivercybercon.com