From the Windows to the Walls

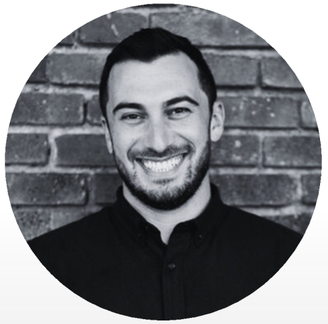
Physical Red Teaming for Security Professionals

Ana Aslanishvili & **Shawn** Abelson

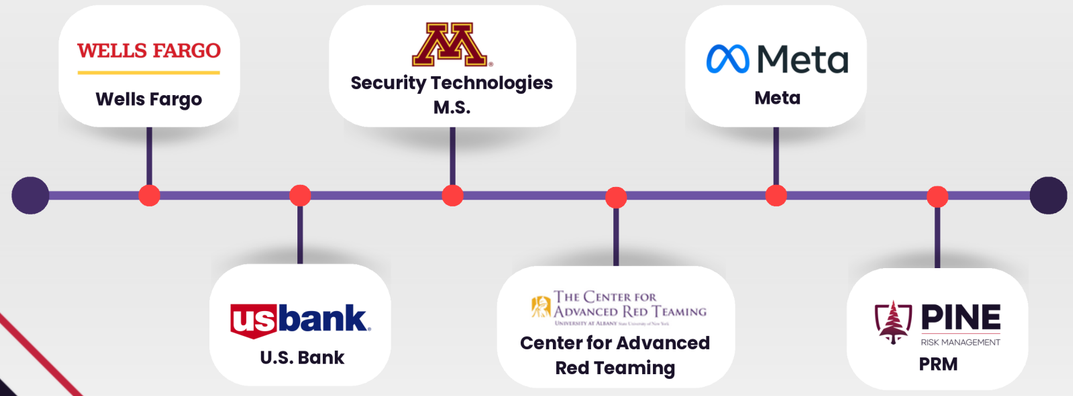
About Us

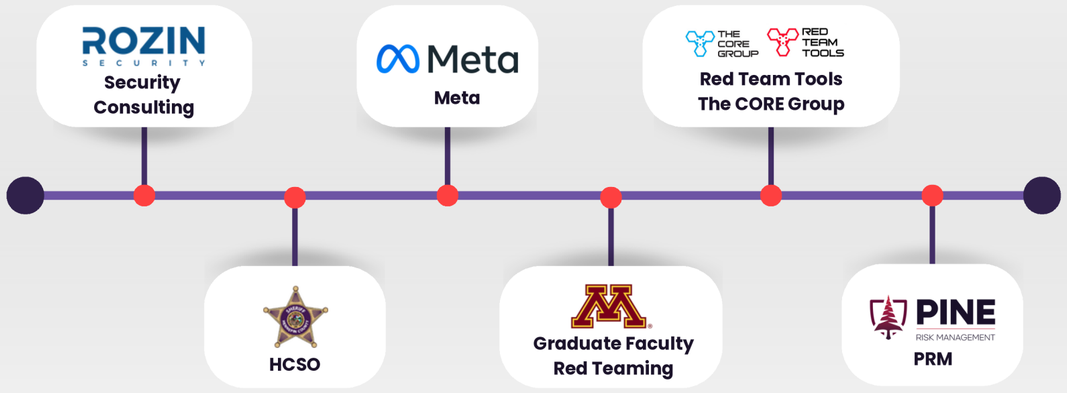
PRM: We conduct, build, and train red teams, helping organizations mature and improve security.
Meta: Started largest physical red team in Silicon Valley, hired dozens of testers, and built a team to oversee findings remediation across global office and data center footprint.

Ana

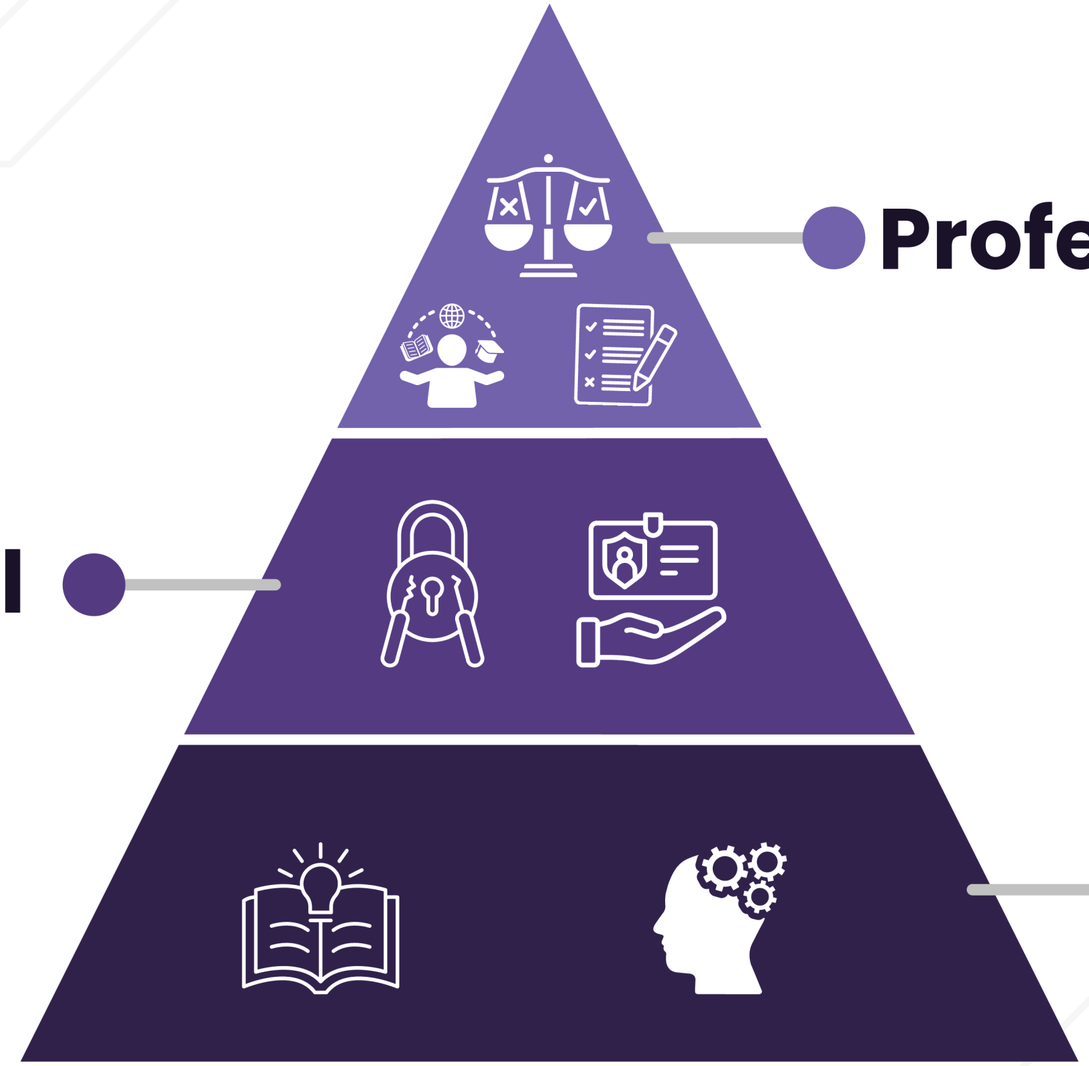


Shawn





Agenda



Professional

Technical

Foundation

What makes a good physical red teamer?

Step 1: Foundation

- The Mindset: What is red teaming?
- The basics of physical security
- Analytical Red Teaming
- Cyber Red Teaming

Step 2: Technical Skills

- Social Engineering
- OSINT
- PACS
- Bypass Techniques
  - Lockpicking

Step 3: Professional Skills

- Systems Thinking
- Ethics & Laws
- Red Teams Gone Wrong
- Managing Red Team Risk
  - Effective Scoping
- Learning from the real bad people (Effective Threat Modeling & Adversary Emulation)
- Security Frameworks, Standards, and Regulations
- Report Writing and Impactful Communication

Resources

Breaking into Red Teaming - Overview

Part 1 - Fundamentals

Part 2 - Technical Skills

Part 3 - Professional Skills

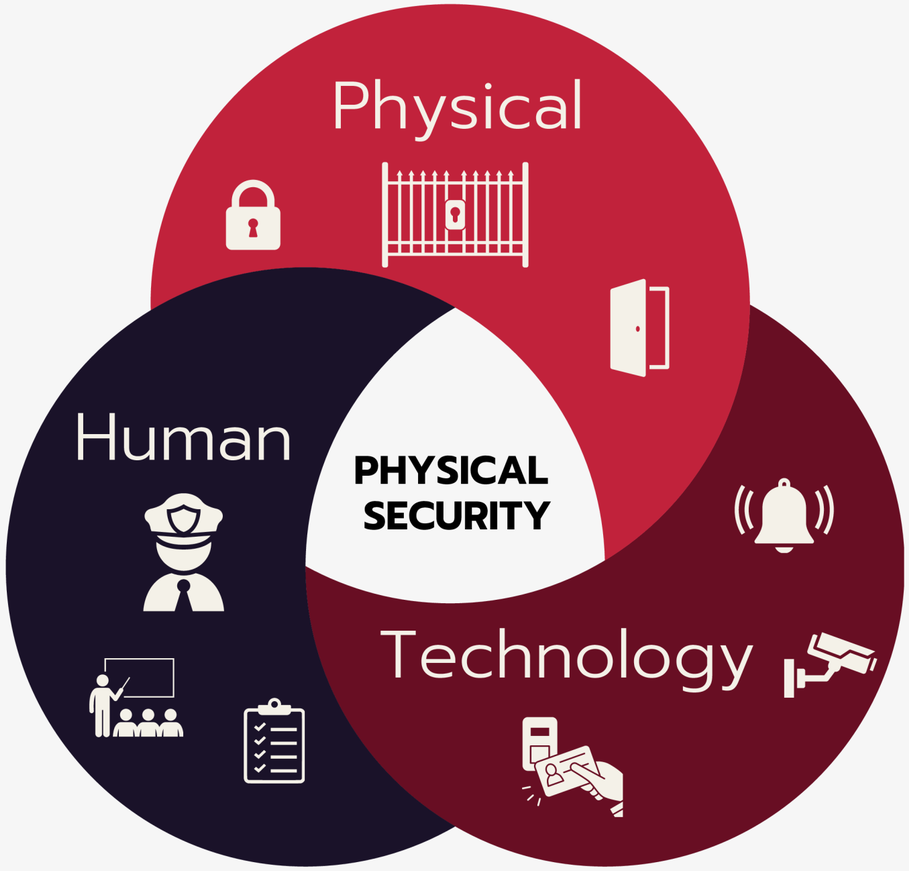
Physical Red Teaming Ethics Scenarios

STEP 1

THE FOUNDATION

Physical Security

Protecting People, Assets, and Reputation. Security measures that deny unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm.



Components of Physical Security

Physical: Doors, locks, gates, bollards, etc.

Technology: PACS, CCTV, Radios, Investigative, and Intelligence tools

Human: Guards, Analysts, Managers, Awareness, Processes & Procedures

Physical Security

Physical Security Teams & Activities


Threat Management


Event Security


Travel Safety


Business Continuity


Systems and Design


Quality Assurance


GSOC


Red Team


Investigations


Intellectual Property Protection


Supply Chain Security


Security Awareness


Insider threat management


Guard-force management


Governance, Risk, and Compliance


Audit


Protective Design


Resilience


Protective Intelligence


Executive Protection

& More

Physical Security

Goals of Physical Security

Deter

Detect

Prevent
Protect / Delay

Alert

Respond

Recover

Define Red Teaming

Stress Testing:
Testing a system with the goal to improve it

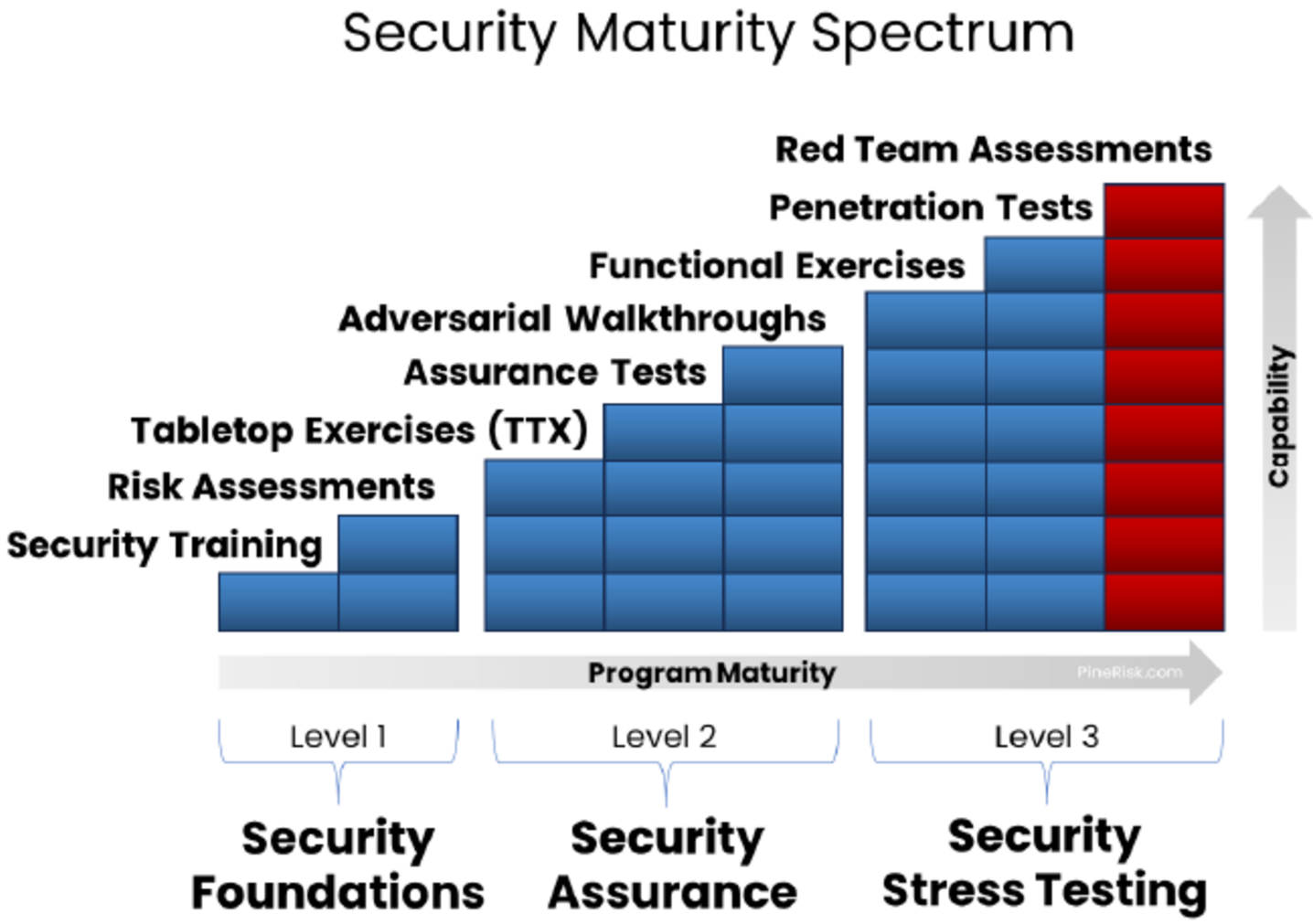
Types of Red Teams

- CYBERSECURITY
- PHYSICAL SECURITY
- AI
- ANALYTICAL RED TEAMING
- PRIVACY

Types of PhySec Assessments

- ASSET FOCUSED ASSESSMENT
- VULNERABILITY FOCUSED ASSESSMENT
- THREAT FOCUSED ASSESSMENT

Physical Red Teaming



PINE
RISK MANAGEMENT

Principles of Physical Red Teaming

UNDERCOVER

The Red Team is a Blue Team in Disguise

- Collaborate and support

SAFE TO FAIL

Red Teaming is an Exercise

- Never fire people for failures
  Systemic, Not Individual
- Blameless Lessons Learned

WHY

Do It for the Right Reasons

- No Ego

BE CREATIVE

Think outside the box

- Test the untestable
- Don’t limit yourself
- It’s your role to think of things the blue team doesn’t

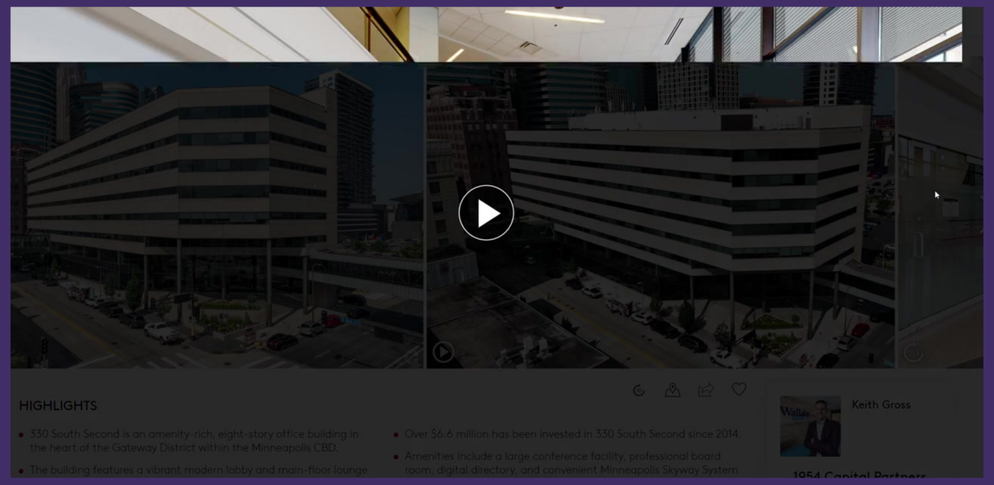
STEP 2

TECHNICAL SKILLS

OSINT for PhySec Red Teaming

Building

- **Blueprints**
  - Tax Records for Building Owner
  - Building Manager
  - Leasing Office
  - City Records, Construction Permits
- **360 Tours**
  - Leasing Agents



Routes In & Intel Gathering

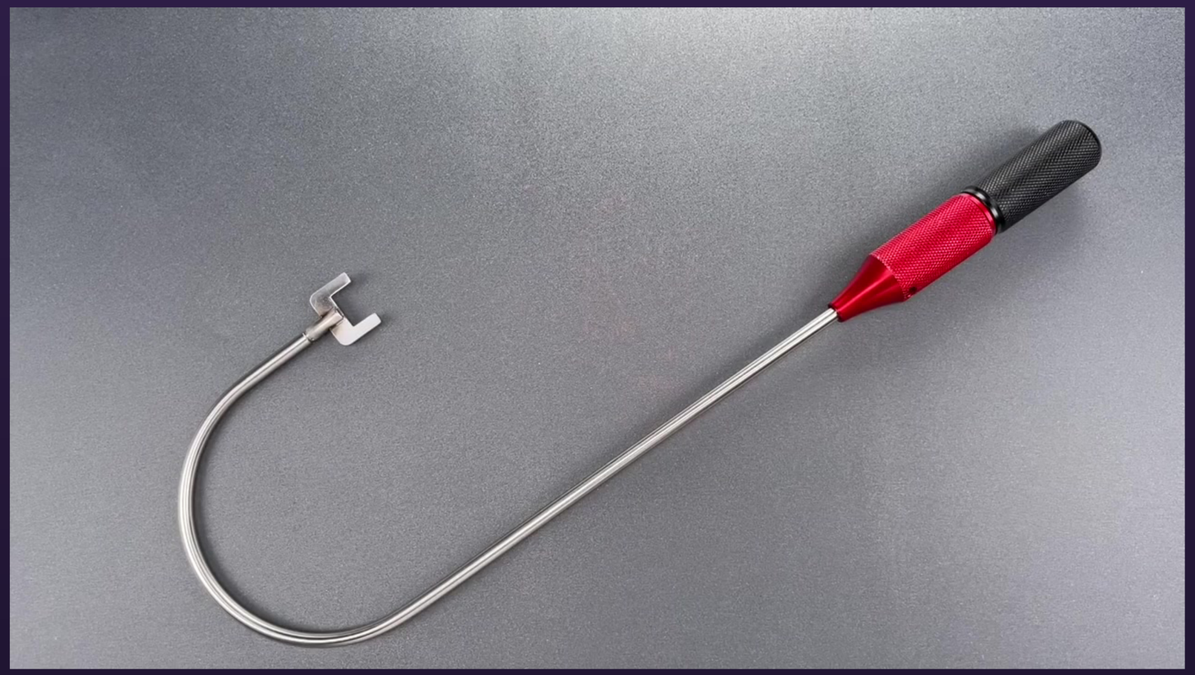
- **Find Vendors**
  - Listed on their website
  - News articles
  - Purchase orders
  - Photos
  - [Surveillance / Probing]
- **Find Co-Tenants**
- **Find Empty Floors**
- **Crime Maps**
- **Wifi (WIGLE)**
- **Complaints and Neighborhood Conversations**
- **Employees (LinkedIn)**
  - Photos, Discussions, etc.
- **Photos Inside**
  - Tags and Geolocation

PINE RISK MANAGEMENT

Double Door Tools

Door Bypass Techniques

Commercial Door Hooks & J-Hook

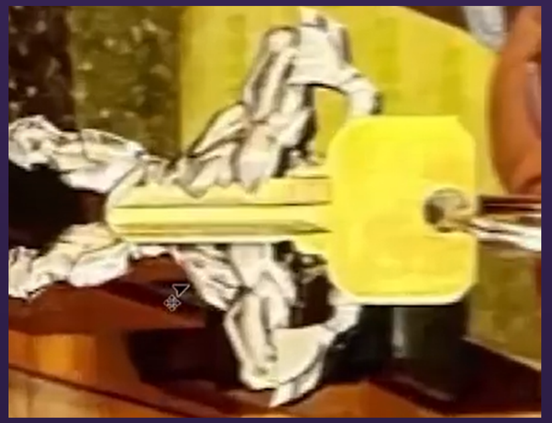


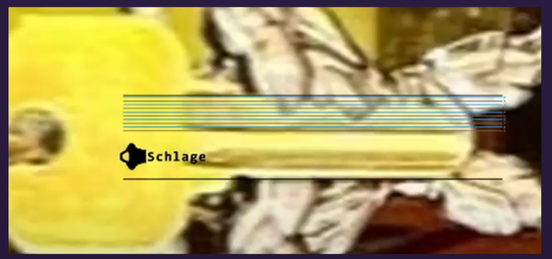
Hinge Pin and UDT

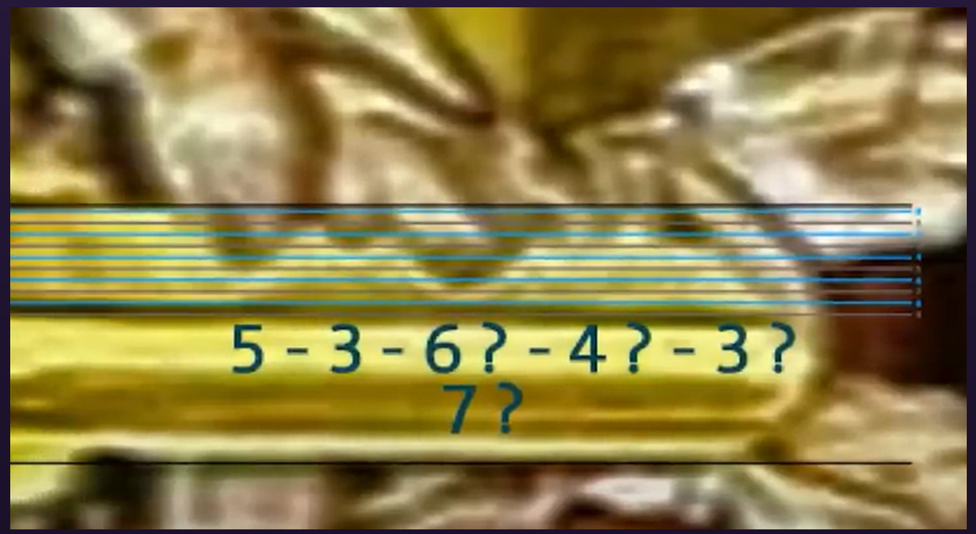
Key-Pain

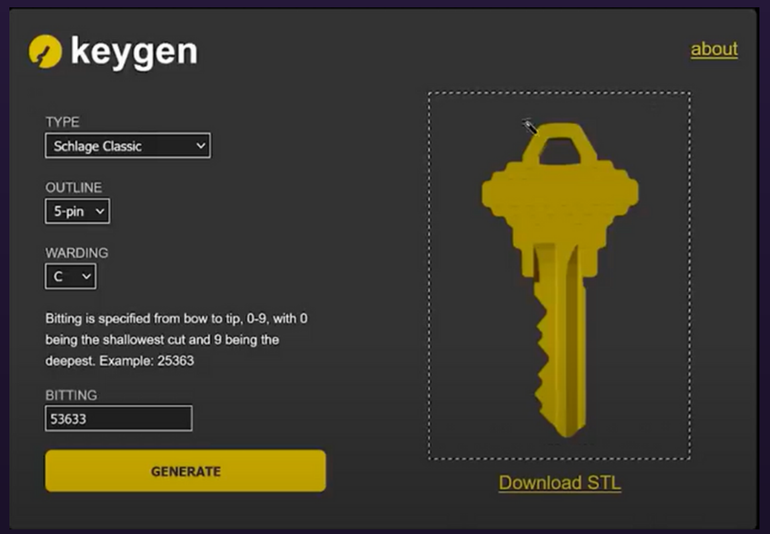

T-Pain
@TPAIN
Replying to @TeosGirlfriend6
Then what? You gonna take some cups and a chair? 😂 Thanks for the heads up tho. I just got the keys today. No way the locks are gonna be the same next week. Thanx tho
9:06 PM · May 8, 2022 · Twitterrific for iOS

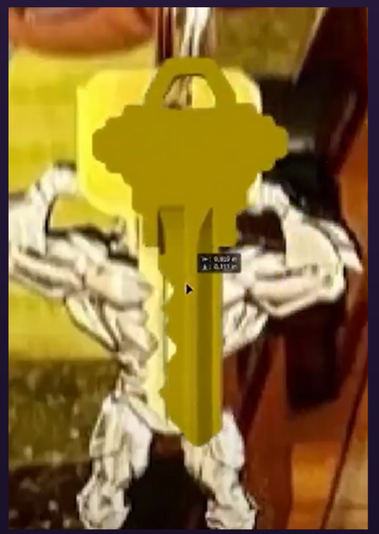

T-Pain
@TPAIN
I DID IT BOIS!!!! Im officially a restaurant owner. Got my keys today and I'm scared as shit. BUT! I can no longer ignore the paths God has set for me just because I don't understand or I'm scared. (1/4)
4:23 PM · May 8, 2022 · Twitter for iPhone
23.1K Retweets 2,340 Quote Tweets 317.5K Likes




Schlage


5-3-6?-4?-3?
7?


keygen
about
TYPE
Schlage Classic
OUTLINE
5-pin
WARDING
C
Bitting is specified from bow to tip, 0-9, with 0 being the shallowest cut and 9 being the deepest. Example: 25363
BITTING
53633
GENERATE
Download STL



Canned Air, Interception, & Badge Cloning

Social Engineering

Impersonation

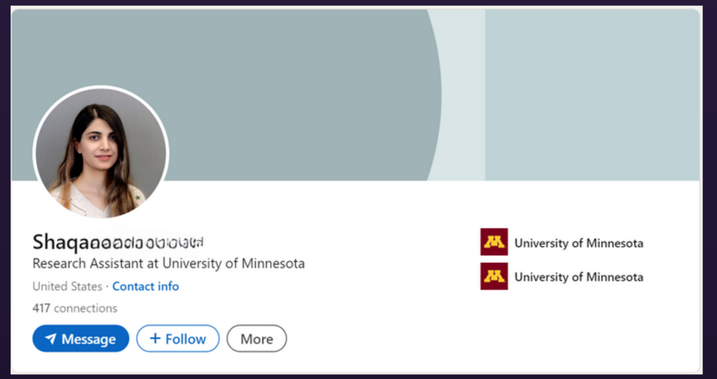
- Temporary Badge & Full Access
- Access to Restricted Areas & Material
- IT Support

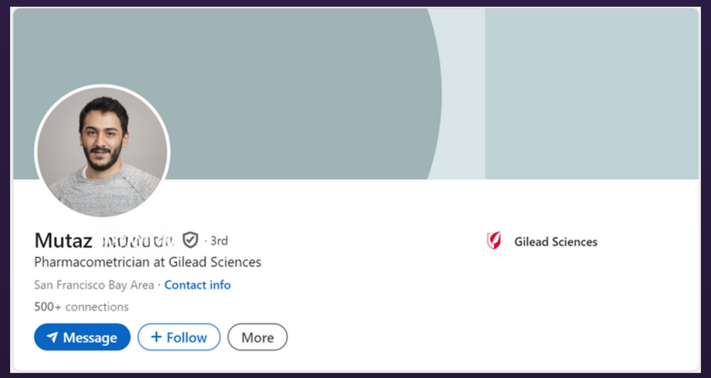
DeepPhishing

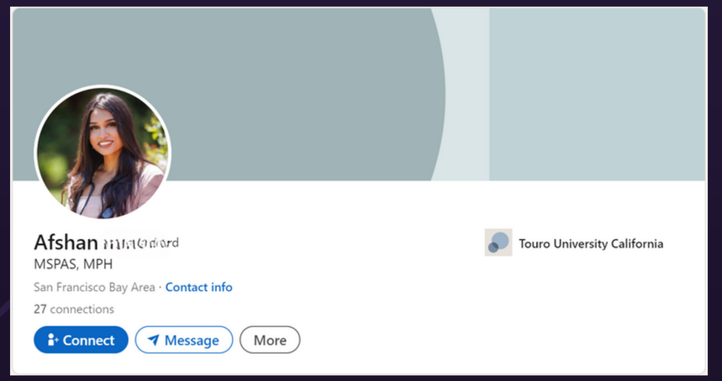
- Deepfakes
- Voice Cloning
- AI Support

Pretexting

- Set Up Appointments
- Information Gathering
- Initial Access







STEP 3

THE **PROFESSIONAL**

RED TEAMER

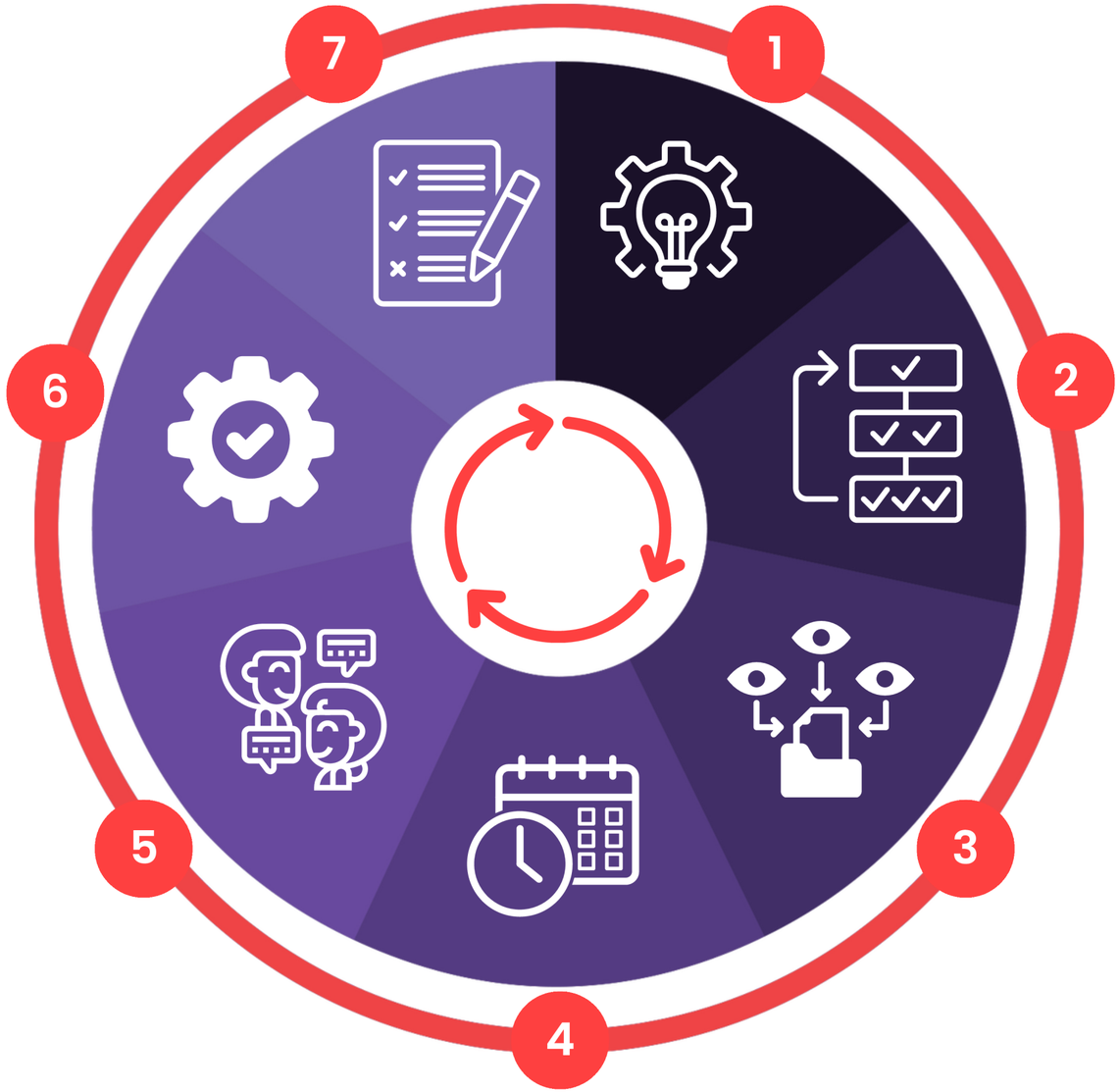
Case Study

15 v 1

Radio Thefts,
Bugs,
and Foot Chases,
Oh My

PINE
RISK MANAGEMENT

Red Team LifeCycle

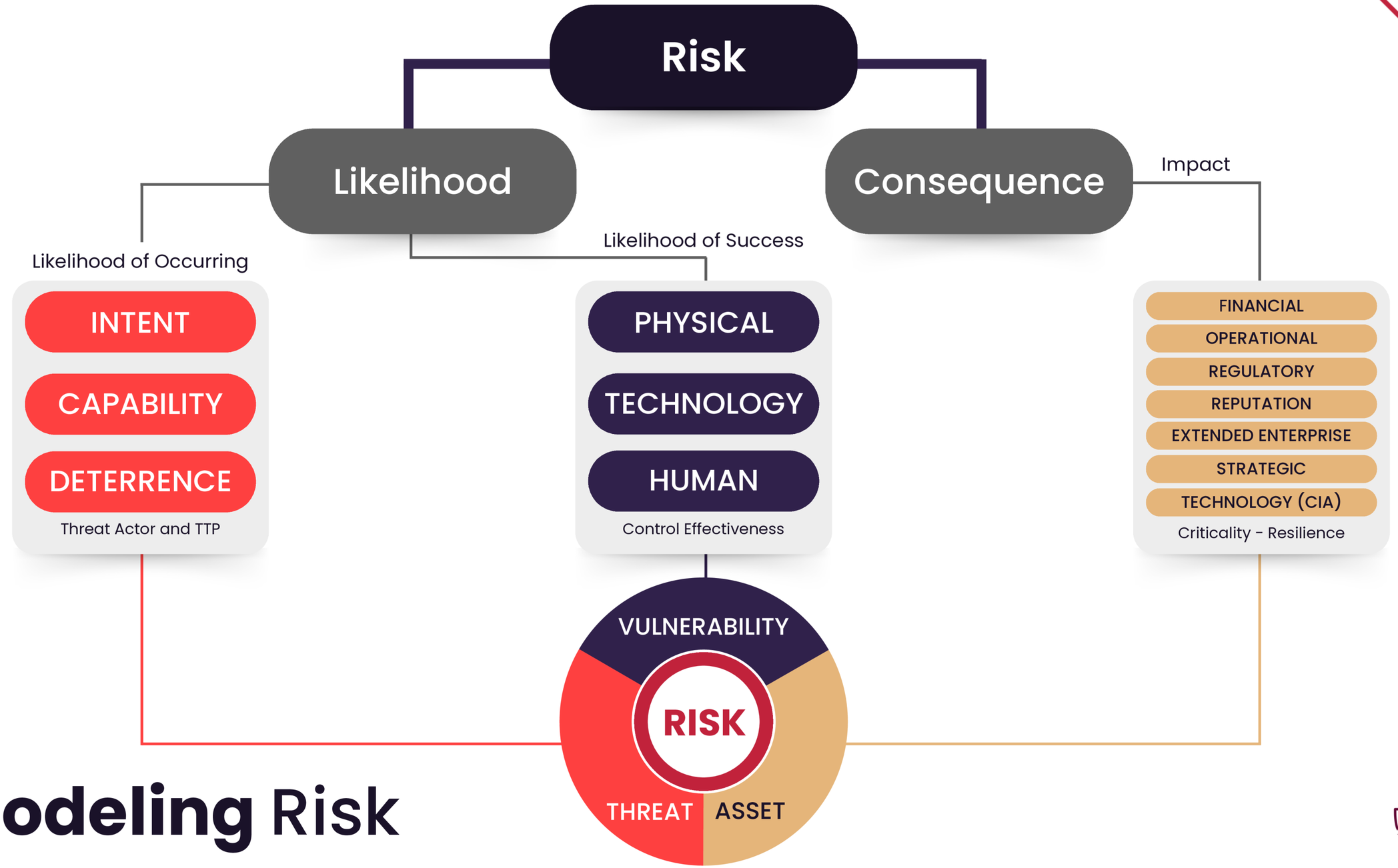


1. IDEATION
2. PRIORITIZATION
3. INTEL GATHERING
4. PLANNING
5. REHEARSAL
6. EXECUTION
7. REPORTING

remediation if you are a narc

PINE
RISK MANAGEMENT

Modeling Risk



PINE
RISK MANAGEMENT

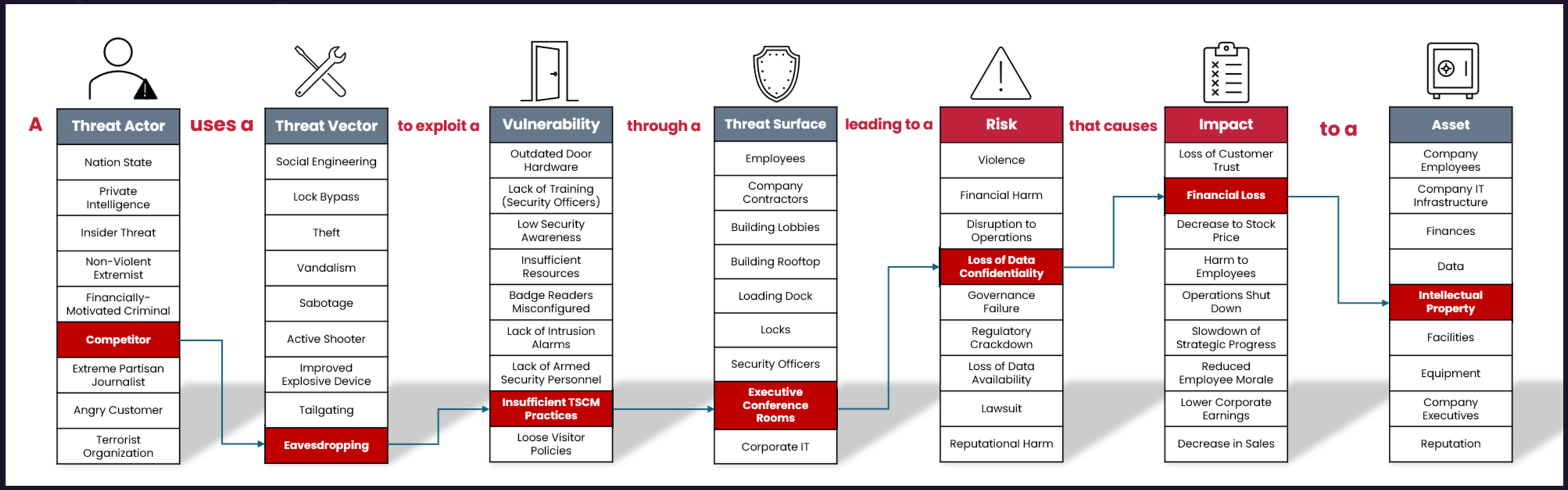
Physical Security Threat Modeling

Resource

Threat Modeling Overview

Basic Threat Modeling Visualization:

- Standard
- Long



Selling the Red Team

Camera Above Desk

$32M Truck Bomb

Bank Misconfiguration

Underwriters

Benefits of Testing Physical Security

1 **Breakdown Boundaries / Silos**
- Don’t give the adversary an advantage

2 **Holistic View of Company’s Security Risks**

3 **Unassigned Areas of Responsibility**
- Fiber-tapping
- Vendor Onboarding
- Insider Threat

4 **Increased Collaboration between Physical / Cyber**

5 **Better Assessments**

6 **Reduce Risk**

PINE
RISK MANAGEMENT

De-Risking

The goal of red teams is to reduce the risk to the organization, not to increase it. Ensure tests do not cause undue risk or disruption.

Categories or Risk:

EHS, Legal, Privacy, Compliance, GSOC, Tenant/Landlord, Firearms/Weapons, Other Risks

Key Question: Do you Notify Law Enforcement?

Authorization Confirmation:

If you get caught, how do they confirm you are authorized?

LoA, Phone Numbers, Internal Post/Page, Notification of LE

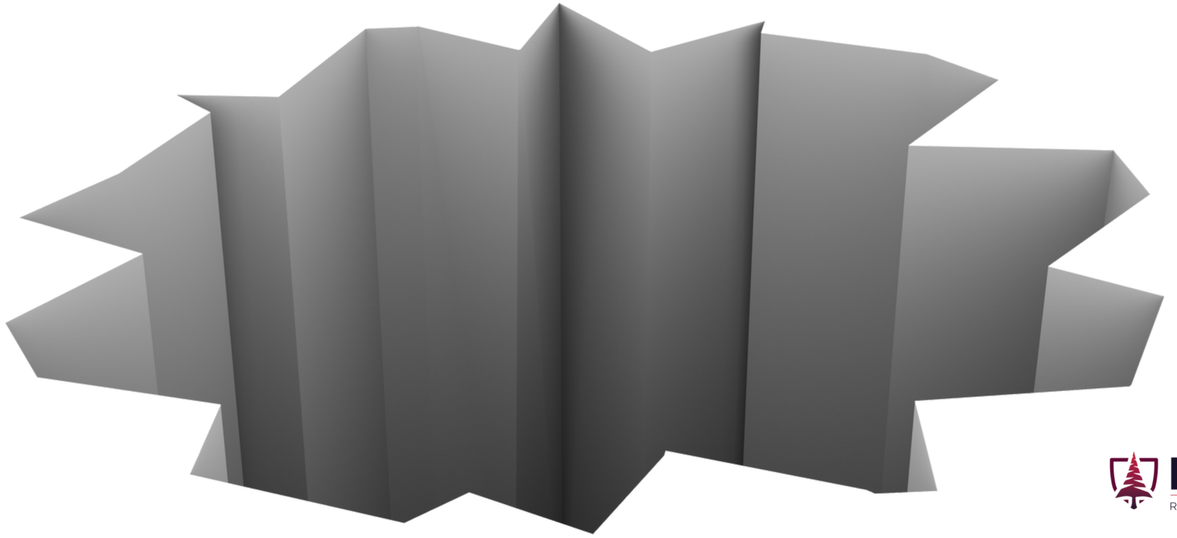
Laws: Review OpsPlan against local laws
STOPOP: When is the operation done? What are the triggers for stopping early?

PINE
RISK MANAGEMENT

Common Pitfalls

DON'T:

- Create vulnerabilities and leave them (even if the client says it's ok)
- Reach for your LoA in your back pocket while a cop points an AR15 at you
- Bring your Politics to Red Teaming
- Commit Crimes (you're authorized, or not)
- Steamroll
- Brag (Afterward or outside of reporting chain)
- Use a fake Letter of Authorization (Get out of Jail Free card)



PINE
RISK MANAGEMENT

Physical Red Teams

Gone Wrong

- Helicopter
- Long Guns
- Special Delivery
- Fire Alarms
- Steamroller
- Tel Aviv

Resource

Physical Red Team Lessons Learned

Let’s Get Physical

Seven Steps for Cyber Teams to Conduct Good Physical Assessments

TALK

Talk to the Physical Security Teams Early

UNDERSTAND

Understand their needs, strengths, known weaknesses, goals, etc.

SCOPE

Focus on objectives

DE-RISK

Get Authorization

COMMUNICATE

Before, during, and after with all parties

DEBRIEF

Show & Tell

FRAMING

Present, frame, and communicate your findings effectively. Know your audience. Technical terms don’t work, pose it in terms of risk, threat model, and threat actors. They don’t know what APTs are targeting your networks, so use the data you have to tell a compelling story.

PINE
RISK MANAGEMENT

Contribute to the Industry

Physical red teaming is immature as a profession

IF YOU WANT TO CONTRIBUTE:

Publish stories, write frameworks, give talks.

Develop tools, Open Source Them.

Learn about Physical Security:
Go to a conference, take a course, and translate it to Cybersecurity professionals.

Take effective and mature aspects of the cybersecurity and try applying them to physical security.

Resources

Locks & Leaks
locksandleaks.substack.com

Red Team Tools
www.redteamtools.com

Resources From This Talk
www.pinerisk.com/BSides

Red Team Alliance
shop.redteamalliance.com

Thank You!

Get in Touch

Text/Call: (628) 777-7475
Signal: (952) 465-4769

Shawn@PineRisk.com
Ana@PineRisk.com

Reddit.com/r/PhysicalRedTeam
Discord: ByteAbel
LinkedIn.com/Company/PineRisk

PINE
RISK MANAGEMENT