RECON DONE RIGHT

A GUIDE TO A SUCCESSFUL PHYSICAL

PRESENTED BY ZLATA PAVLOVA & ROB CURTINSEUFERT

LAYER 8 CONFERENCE, OCTOBER 8, 2021

PRESENTED BY:

Rob CurtinSeufert,
Director Of Services, InGuardians
@curtinseufert

Zlata Pavlova,
SM and Marketing Coordinator, InGuardians
@3latka_

DISCLAIMER

This works for us. You may need to make some adjustments, depending on your situation and your style of work.

Rob spent years in the US Army, working in various long range reconnaissance units

Z is Russian, you just don’t mess with Russians.

OVERVIEW

- Definition
- Phase 1. Pre-engagement Intel gathering (OSINT)
- Phase 2. Establishing a pattern of life
- Phase 3. Analysis and Planning
- Phase 4. Breach
- Phase 5. Site Exploitation (SSE) and exfil
- Conclusion

DEFINITION

Reconnaissance (military) - observation of a region to locate an enemy or ascertain strategic features.

Reconnaissance (infosec) - gathering all of the information about the client (aka target) prior to the engagement.

The main goal of recon - is to covertly collect data about the target. Sources include OSINT, SE, digital or physical monitoring.

PHASE 1. PRE-ENGAGEMENT INTEL GATHERING (OSINT)

- OSINT is your best friend for any physical or SE engagement!
- Approach and resources used varies based on the target and the objective.
- Multiple sources should be used to gather better intel, verify, get better results.
- Manual search is time consuming but could provide better results.
- Divide the responsibilities – more time efficient

PHASE 1. PRE-ENGAGEMENT INTEL GATHERING (OSINT)

Location:

- Identify Target's location and surrounding area
- Identify Access points (doors, gates, windows, etc)
- Identify CCTVs
- Visible Physical Security Controls (RFID readers next to entrance doors)

Resources:

- Google Maps, Google Earth, Street View
- Bing Maps
- Company filings, gov. records (EDGAR)
- Melissa.com - Verify address, lookup carrier routes
- Google Photos, Yelp, geo tags on social media

PHASE 1: PRE-ENGAGEMENT INTEL GATHERING

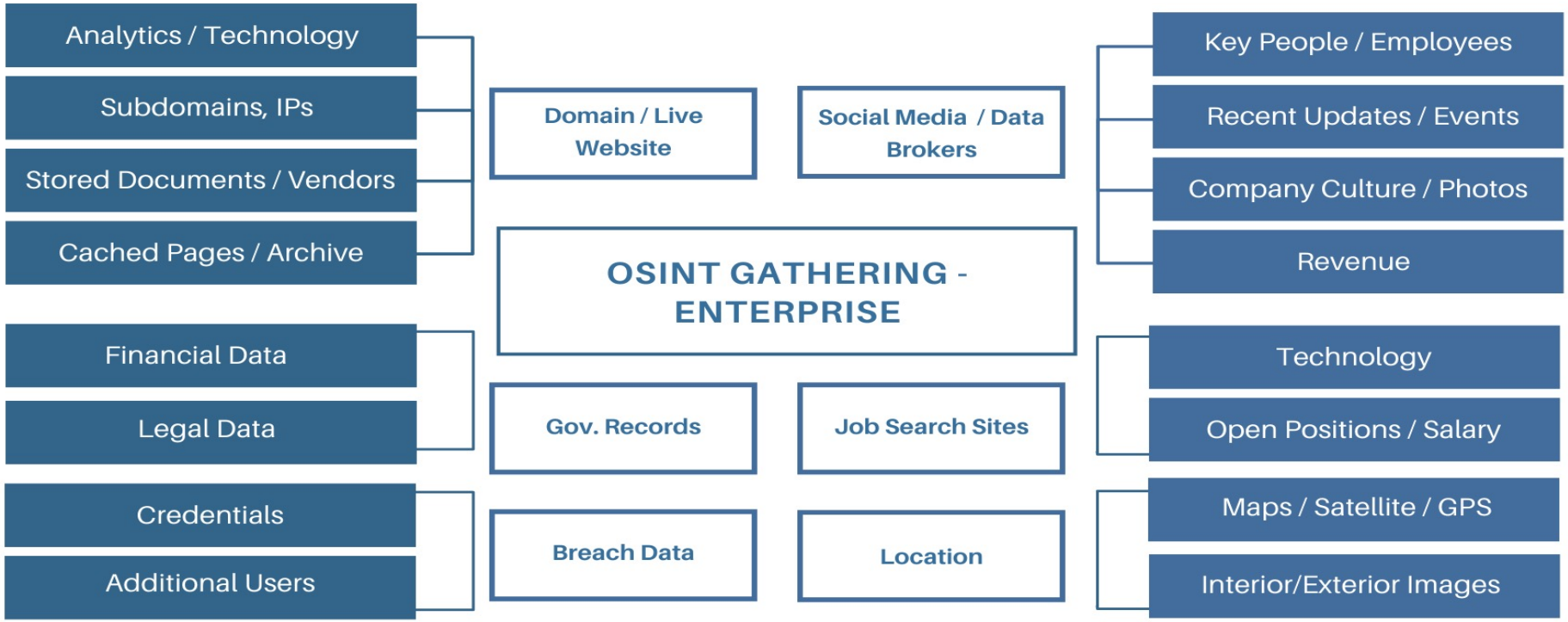
Job Postings:

- Schedule / Shift Changes
- Guards
- Open positions / in-person interview schedule
- Reviews from former & current employees

Other resources:

- LinkedIn (employees, company's events, updates, etc.)
- Facebook pages
- Instagram (geo tagged photos, badges)
- Yelp
- YouTube
- Press

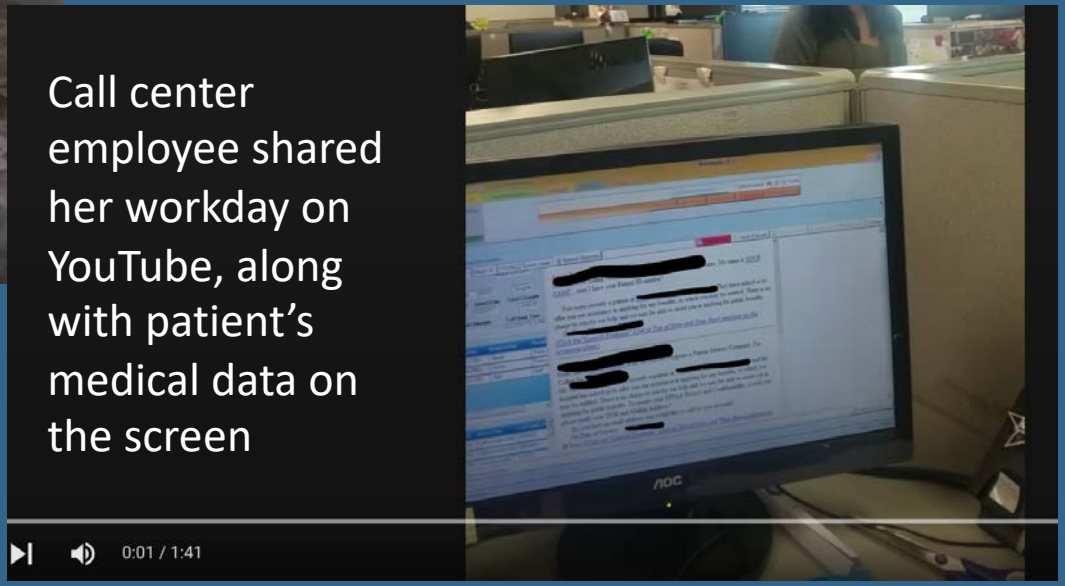
PHASE 1. PRE-ENGAGEMENT INTEL GATHERING (OSINT)



PHASE 1. EXAMPLES

Blueprints of the building, posted on company's Google page

Call center employee shared her workday on YouTube, along with patient's medical data on the screen



PHASE 2: ESTABLISHING THE PATTERN OF LIFE

Why:

- Validate the OSINT collected (maps, shift changes, etc.)
- Develop the initial attack path
- Get familiar with surroundings in real life
- Visual representation is the best

How:

- Drive by the parking lot – do cars ever leave? When?
- Surrounding businesses - hours of operation, traffic, etc.
- Security Patrol
- Employees' hangout areas (smoking areas)
- Terrain Analysis
- Lights
- CCTVs coverage

PHASE 2: ESTABLISHING THE PATTERN OF LIFE

Tools:

- PRINT OUT A MAP!
- DSLR camera with a decent zoom and the ability to take good shots in poor lighting
- Take lots of notes
- Do not bring your breach kit!

Image source: https://www.optactical.com/

PHASE 3: ANALYSIS AND PLANNING

THE MOST IMPORTANT PHASE!

5 Ps' Prior Planning Prevents Poor Performance

- Multiple ingress plotted
- Multiple breach points ID'd
- Establish time frames for each point
- Exit strategies and rendezvous points in case separated
- Communication plan with partner and PM, and client's point of contact
- Bug out words
- EQUIPMENT CHECKS!

Things to remember:

- Always plan for "what if"
- Rehearsal
- Stick to the plan!

PHASE 4: BREACH

- **Get out of the jail card!**
- Bring your gear
- Know your plan and stick to it
- Stick to the time frame
- Know when to get out
- Car keys ☺

PHASE 5: SITE EXPLOITATION

- Hit your objectives and get out
- Stick to the plan!

CONCLUSION

- Good OSINT = higher success rate
- Proper documentation / Report
- Communication is important every step of the way
- **Multiple scenarios - always plan for “what if”**

- Get out of jail card
- Gear check
- Proper Attire
- **Rehearsal**

- **Stick to the plan!**
- **Stick to the time frame!**
- Know when to disengage
- Don’t be Leroy!

90%

Intel Gathering
Pattern of Life
Analysis and Planning

10%

Breach
Site Exploitation

DON’T BE LEROY!

QUESTIONS?

THANK YOU!