Gathering Physical OSINT

Jerod Brennen
CISSP, INFOSEC GEEK

@slandail www.slandail.net

Overview

Physical locations

Remote locations

Business relationships

Physical Reconnaissance

Gathering information about the physical locations that support the target organization's operations

Dumpster-diving and physical on premise items are out-of-scope

“Time spent in reconnaissance is seldom wasted.”

John Marsden, author

Remember the Levels of OSINT?

Three Levels of OSINT

Compliance Driven (L1)

PCI
FISMA

Best Practice (L2)

Mature Program
Customer Expectation

State Sponsored (L3)

Critical Infrastructure
Political Climate

Locations (L1)

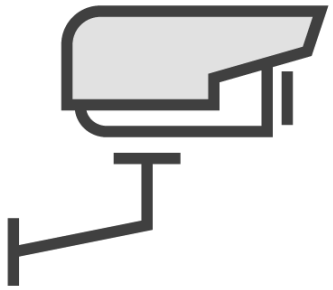
Per Location

Full Address

Ownership

Associated Records (City, Tax, Legal)

Physical Security Measures



Camera Placements

Sensors

Fences/Gates

Guard Posts

Types of Identification

Entry Points
(Employee, Supplier)

Physical Presence -> Virtual Presence

Physical Locations

IP Blocks

For Hosts/NOC

Full CIDR Notation

(Hosts & Networks)

Full DNS Listing

(All associated assets)

Full Mapping of AS

Peering Paths

CDN Provisioning

Netblock Owners

(Whois Data)

Hurricane Electric

- http://bgp.he.net/

Robtex

- https://www.robtex.net/

Internet-wide Scan Data Repository

- https://scans.io/

Censys

- https://www.censys.io/

L1 and L2

- Land/tax records
- Owner
- Shared/individual
- Time zones
- Hosts/NOC

Search Engines

- Google – https://www.google.com/
- Bing – https://www.bing.com/
- DuckDuckGo – https://duckduckgo.com/

```
“company_name” headquarters address
“company_name” branch office
“city state” county
```

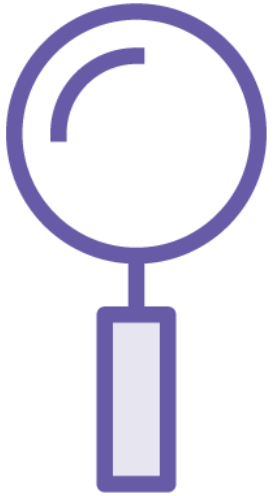
Search Engine Queries

Usage: Identify physical locations associated with the target organization

Finding Tax Records

Search for physical address

Link city to county



Conduct a property search on county auditor website

Pervasiveness (L1)

Headquarters

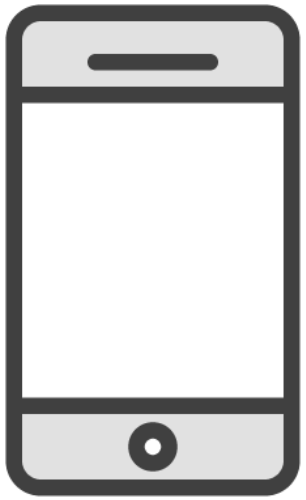
Branch/remote locations?

Security Radius

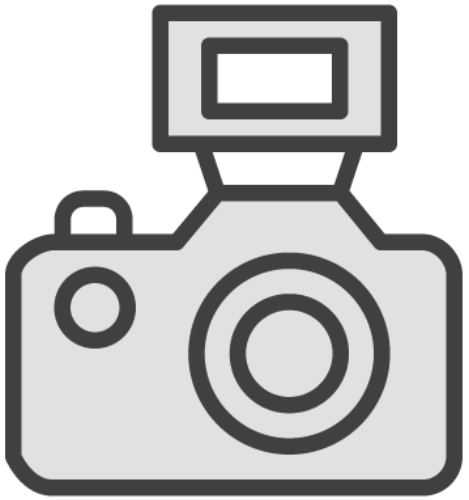
On-site Reconnaissance

In-scope or out-of-scope?

Pictures, or It Didn't Happen

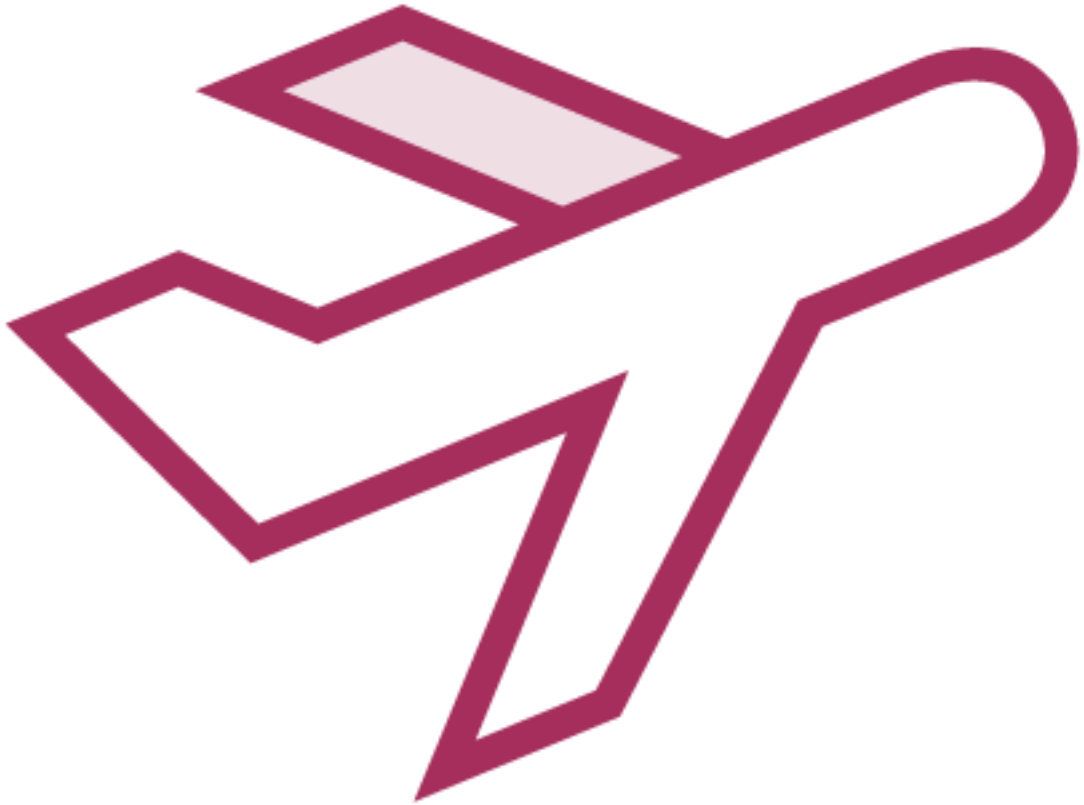


Camera Phone



DSLR

What About Drones?



Small Unmanned Aircraft Rule

Operational Limitations

Remote Pilot in Command

(Certification and Responsibilities)

Aircraft Requirements

Model Aircraft

IntelTechniques Custom Map Tool

- https://inteltechniques.com/osint/maps.html

Step 1: Enter physical address

Step 2: Copy latitude and longitude from XML to GPS location search fields

Step 3: Click submit, open 16 tabs

Relationships (L1)

Business partners

Customers

Suppliers

Rental companies

Corporate website

Search engines

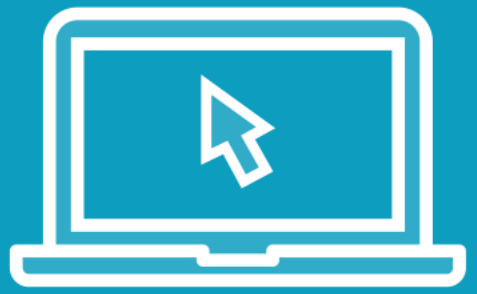
Basics

L2 and L3

- Relationships
- Shared office space
- Shared infrastructure
- Rented/leased equipment

Validate scope and rules of engagement

Demo



Bug bounty program: Indeed

- https://bugcrowd.com/indeed

Summary

- Locations
- Pervasiveness
- Relationships

On to the next module: Gathering Logical OSINT