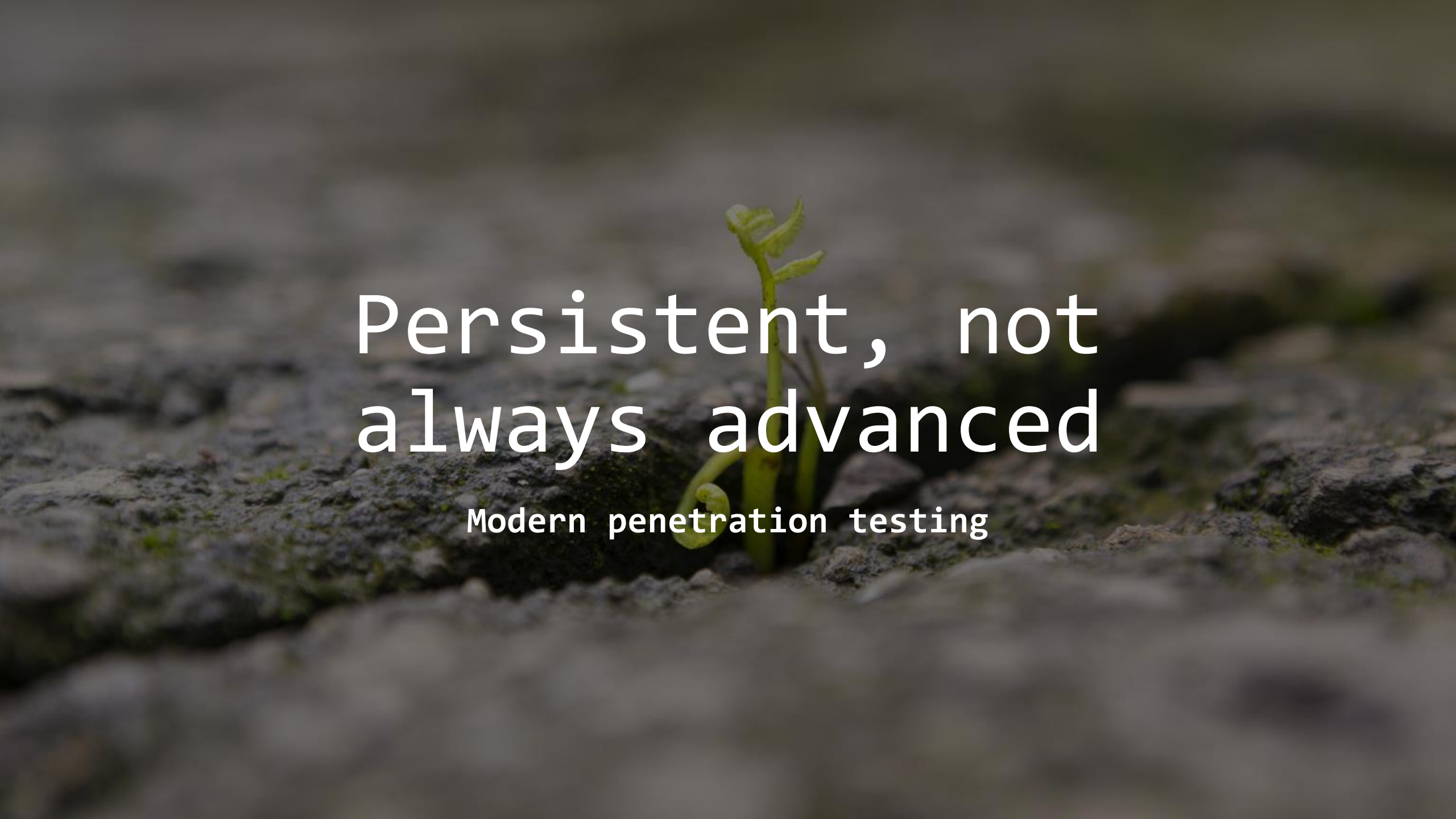

Persistent, not always advanced
Modern penetration testing

WHO AM I?

COO, Principal and Founder at River Security

Principal Instructor at SANS

Co-Author of SEC550 – Cyber Deception, Attack Detection, Disruption and Active Defense

Short summary:

I show how criminals break-in,
and I help throw them back out…

GCIH GIAC Certified Incident Handler
GPEN GIAC Certified Penetration Tester
GSLC GIAC Security Leadership
GIAC Mobile Device Security Analyst
GDAT GIAC Defending Advanced Adversaries
GCTI GIAC Cyber Threat Intelligence
GCFA GIAC Certified Forensic Analyst

RIVER SECURITY

WHY DO WE DO PENETRATION TESTING?

WHAT IS THE GOAL OF A PENETRATION TEST?
(LEGIT QUESTION)

Common problems with traditional pentests…

Receiving a Pentest

Providing a Pentest


Do Attackers Care About Scope?

Digital Footprint Assessment

Mapping Attack Surface First

- Immediate **value** by just having hackers LOOK at you
- Smaller investment up front
- Easier to guarantee that the entire (or just some) of the scope has been tested
  - Customer and Provider knows what has been left out of scope
- Find shadow IT, unmanaged data
- Bottom-up approach!

Digital Attack Surface Report

Might lead into

Penetration Test Report

Digital Footprint Report

Focus Points and Summary

Overview of Applications, status and attractiveness

Lists of leaks, vulnerabilities and everything else a customer may find useful.

Value, value, value!

How Can Testers Supply Value Sooner?

Know The Target	 Learn who the customer is, what they represent
Find Value	 Find interesting and prioritize which systems to attack
Know Themselves	 Let the customer know themselves


WHAT IS ATTACK SURFACE
MANAGEMENT?

RIVER SECURITY

HIGH LEVEL PENTEST METHODOLOGY

Reconnaissance

Discovery & Scanning

Exploitation & Verification

The road-less travelled

- How to find the roads less travelled?
- Have the best recon
  - The best recon process
  - The best wordlists
  - Continuous and always-on
- Be inspired by bug-bounty hunters
- Everyone runs automated tools
  - Innovate
  - Change
  - Win

The Digital Footprint Dilemma

- Businesses want an increased digital footprint and presence
- From a Cyber Security point of view, we want a small footprint
- Continuous Attack Surface Management helps mitigate the problem

Cyber Security Team

Organizations Direction

WHAT IS ALWAYS-ON PENTESTING?

RIVER SECURITY

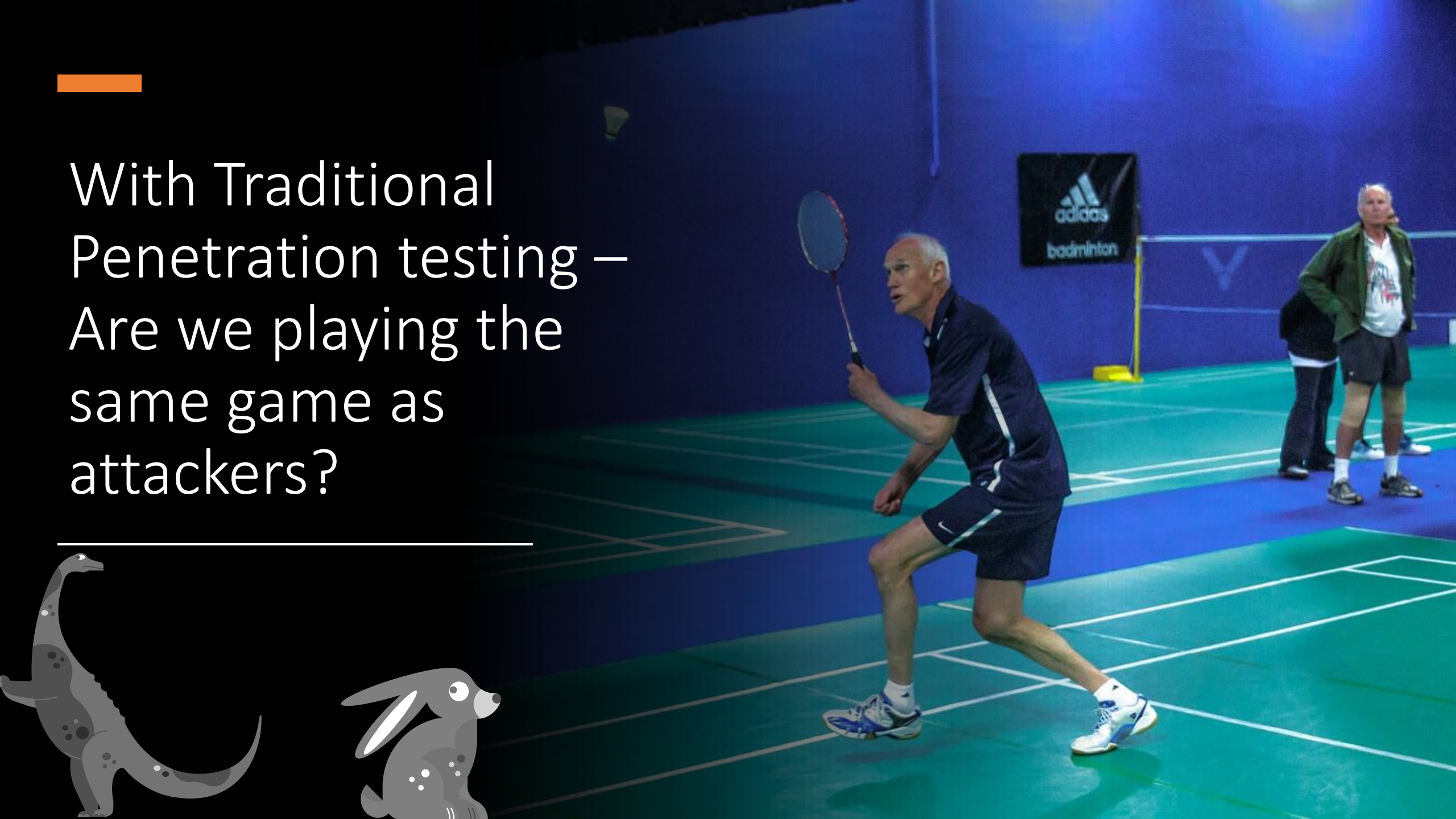
HIGH LEVEL PENTEST METHODOLOGY

Reconnaissance

Discovery & Scanning

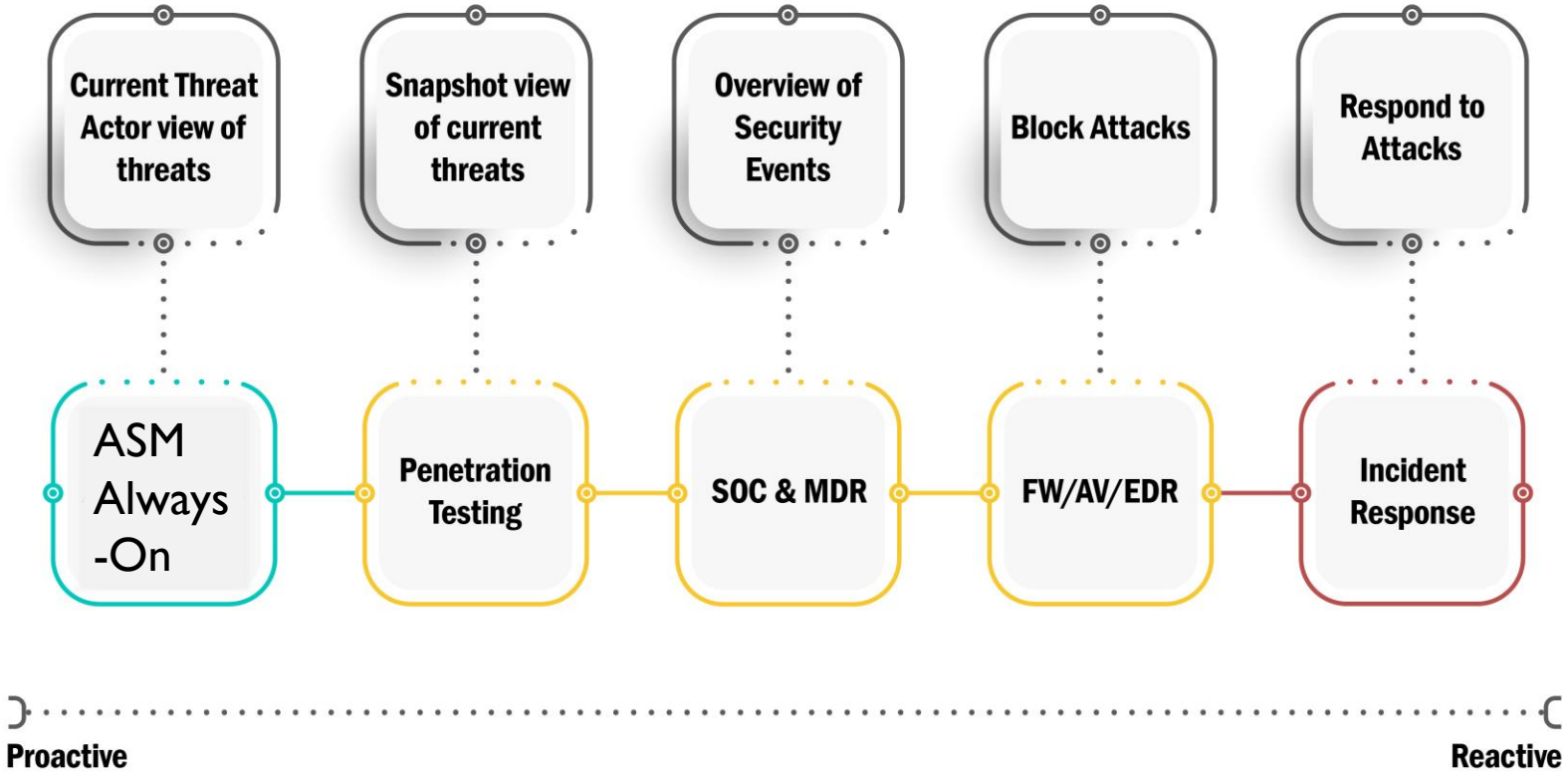
Exploitation & Verification

With Traditional Penetration testing – Are we playing the same game as attackers?

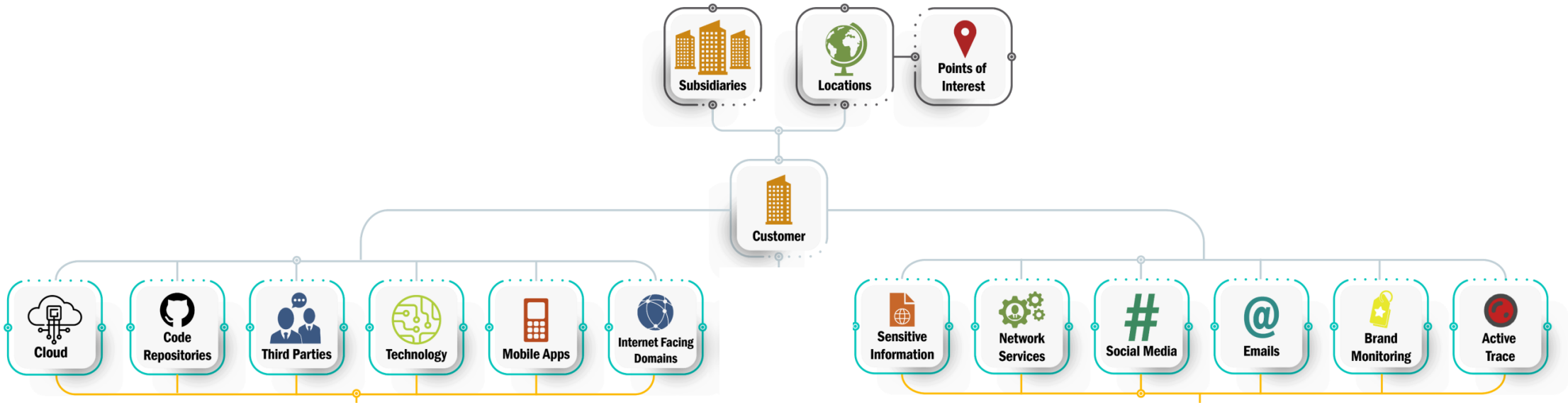



OBSERVE change to Attack Surface
DECIDE to develop working exploit and notify customer
OODA LOOPS
Beating Attackers At Their Own Game
ORIENT ourselves
Customer ACT based on recommendation

Proactive vs. Reactive



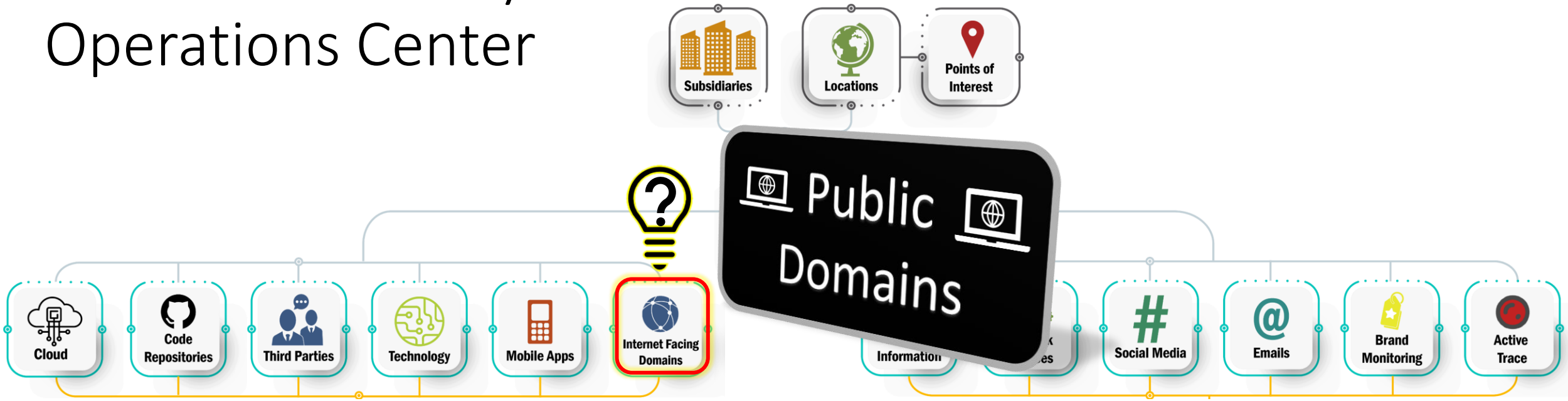
Building an **O**ffensive **S**ecurity **O**perations **C**enter



!

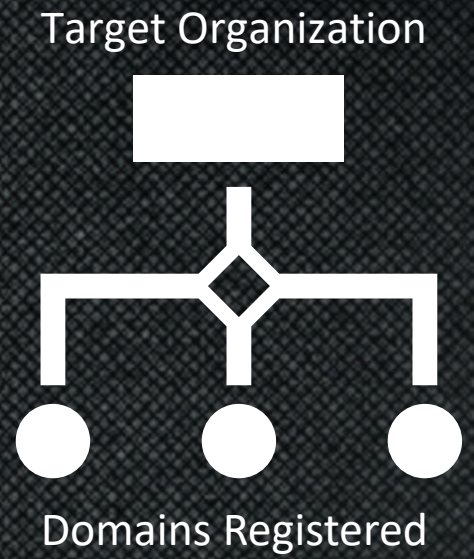
Next slides are for reference, inspiration and review

Building an Offensive Security Operations Center



Domains

- Domains is typically the focus for hunting for attack vectors
- When are new domains provisioned?
- Who registered it?
- Certificate Transparency Logs
  - Wildcard certificates
- DNS Brute Forcing
- Targeted Word Lists for finding new domains
- Malicious domains



CTL - Certificate Transparency Log

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
7914827265	2022-11-06	2022-11-06	2023-02-04	election.def.camp	election.def.camp	C=US, O=Let's Encrypt, CN=R3
7914830288	2022-11-06	2022-11-06	2023-02-04	election.def.camp	election.def.camp	C=US, O=Let's Encrypt, CN=R3
7676271998	2022-10-03	2022-10-03	2023-01-01	ladies.def.camp	ladies.def.camp	C=US, O=Let's Encrypt, CN=R3
7674466435	2022-10-03	2022-10-03	2023-01-01	ladies.def.camp	ladies.def.camp	C=US, O=Let's Encrypt, CN=R3
7676269774	2022-10-03	2022-10-03	2023-01-01	def.camp	def.camp	C=US, O=Let's Encrypt, CN=R3
7674461576	2022-10-03	2022-10-03	2023-01-01	def.camp	def.camp	C=US, O=Let's Encrypt, CN=R3
7663356094	2022-10-02	2022-10-02	2022-12-31	*.def.camp	*.def.camp def.camp	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
7629114100	2022-09-26	2022-09-26	2022-12-25	dctf.def.camp	dctf.def.camp	C=US, O=Let's Encrypt, CN=R3
7619935413	2022-09-26	2022-09-26	2022-12-25	dctf.def.camp	dctf.def.camp	C=US, O=Let's Encrypt, CN=R3
7566271182	2022-09-18	2022-09-18	2022-12-17	eventapi.def.camp	eventapi.def.camp	C=US, O=Let's Encrypt, CN=R3
7565608196	2022-09-18	2022-09-18	2022-12-17	eventapi.def.camp	eventapi.def.camp	C=US, O=Let's Encrypt, CN=R3
7566268398	2022-09-18	2022-09-18	2022-12-17	eventadmin.def.camp	eventadmin.def.camp	C=US, O=Let's Encrypt, CN=R3
7565607360	2022-09-18	2022-09-18	2022-12-17	eventadmin.def.camp	eventadmin.def.camp	C=US, O=Let's Encrypt, CN=R3
7566267956	2022-09-18	2022-09-18	2022-12-17	event.def.camp	event.def.camp	C=US, O=Let's Encrypt, CN=R3
7565606658	2022-09-18	2022-09-18	2022-12-17	event.def.camp	event.def.camp	C=US, O=Let's Encrypt, CN=R3
7266389618	2022-08-04	2022-08-04	2022-11-02	ladies.def.camp	ladies.def.camp	C=US, O=Let's Encrypt, CN=R3
7266389546	2022-08-04	2022-08-04	2022-11-02	ladies.def.camp	ladies.def.camp	C=US, O=Let's Encrypt, CN=R3
7266388688	2022-08-04	2022-08-04	2022-11-02	def.camp	def.camp	C=US, O=Let's Encrypt, CN=R3
7266385717	2022-08-04	2022-08-04	2022-11-02	def.camp	def.camp	C=US, O=Let's Encrypt, CN=R3
7261684274	2022-08-03	2022-08-03	2022-11-01	*.def.camp	*.def.camp def.camp	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
7214093039	2022-07-28	2022-07-28	2022-10-26	dctf.def.camp	dctf.def.camp	C=US, O=Let's Encrypt, CN=R3
7214164906	2022-07-28	2022-07-28	2022-10-26	dctf.def.camp	dctf.def.camp	C=US, O=Let's Encrypt, CN=R3
7162392374	2022-07-20	2022-07-20	2022-10-18	eventadmin.def.camp	eventadmin.def.camp	C=US, O=Let's Encrypt, CN=R3
7159021695	2022-07-20	2022-07-20	2022-10-18	eventadmin.def.camp	eventadmin.def.camp	C=US, O=Let's Encrypt, CN=R3

- https://transparencyreport.google.com/https/certificates
- https://certstream.calidog.io
- https://crt.sh
- https://developers.facebook.com/tools/ct/search/
- ...


chris@DESKTOP-8UENK1V: /mnt/c/Users/chris/Downloads
chris@DESKTOP-8UENK1V:/mnt/c/Users/chris/Downloads$ zcat nodomains.gz | cut -d "|" -f 3 | cut -d "/" -f 3 | sort | uniq | rev | cut -d "." -f 1,2 | rev | sort | uniq
rev: stdin: Invalid or incomplete multibyte or wide character
123hjemmeside.no
129.132
138wan.com
169.104
17mma.com
183.104
187.68
187.70
187.72
1890.no
1bakuganworld.ru
1kel.no
2009
230.17
230.26
235.104
24blogg.no
39.104
3tblogg.no
40.177
40.180
42.no
44.75
44.98
730.no
77.132
URL SHORTENERES MIGHT LEAK INFORMATION
URLTeam over at ArchiveTeam has been doing a brute force against URL Shorteners
21

Backup data

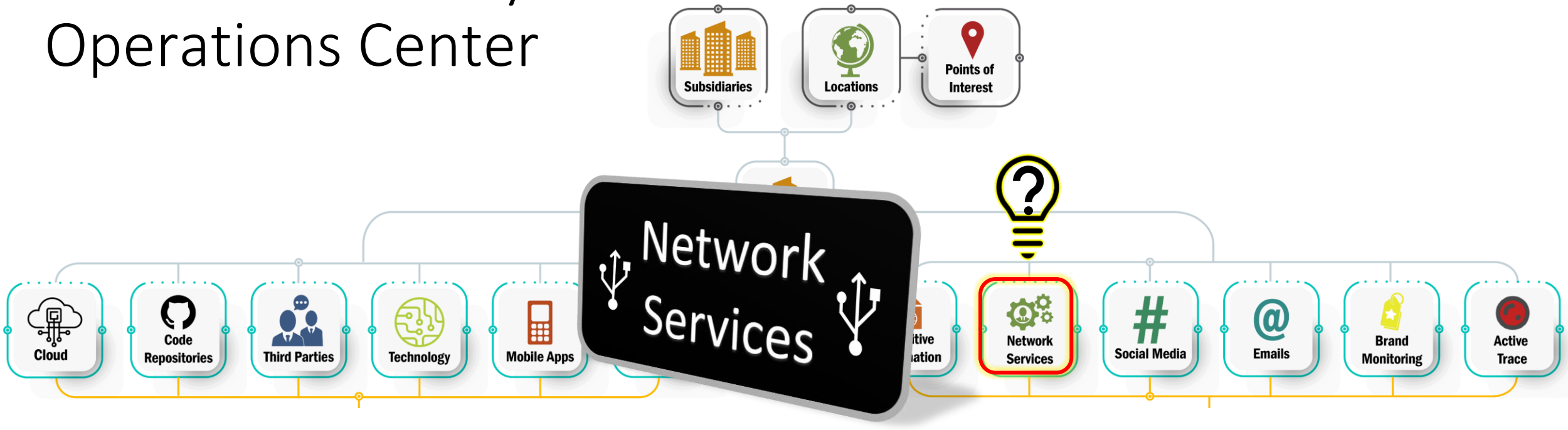
Next up in line of examples is backed up data. Many developers and IT-operators make temporary backups available online. While sharing these, it is evident that some of them have used URL shorteners to make life more convenient. This vulnerability classifies as a information leak.

Search term	Example data
{"wildcard": {"uri_path.keyword": "*.bak"}}	**uri_path** /[redacted]ca_20140924_1515.bak /mp/[redacted]moon/415.bak /blog/tag/welcome-0.bak /zh/scanresult/file/[redacted]8adcd350958547e7.bak
{"wildcard": {"uri_path.keyword":"*.sql"}}	**uri_path** /[redacted]ata-trade.sql /decibel/variant/blob/master/sql/variant.sql /dbdump.sql /[redacted]rp_main.sql /[redacted]usi.sql /[redacted]%20tempdb.sql

https://www.sans.org/blog/the-secrets-in-url-shortening-services/

Parked Domains

Building an Offensive Security Operations Center



Network Services – TCP and UDP

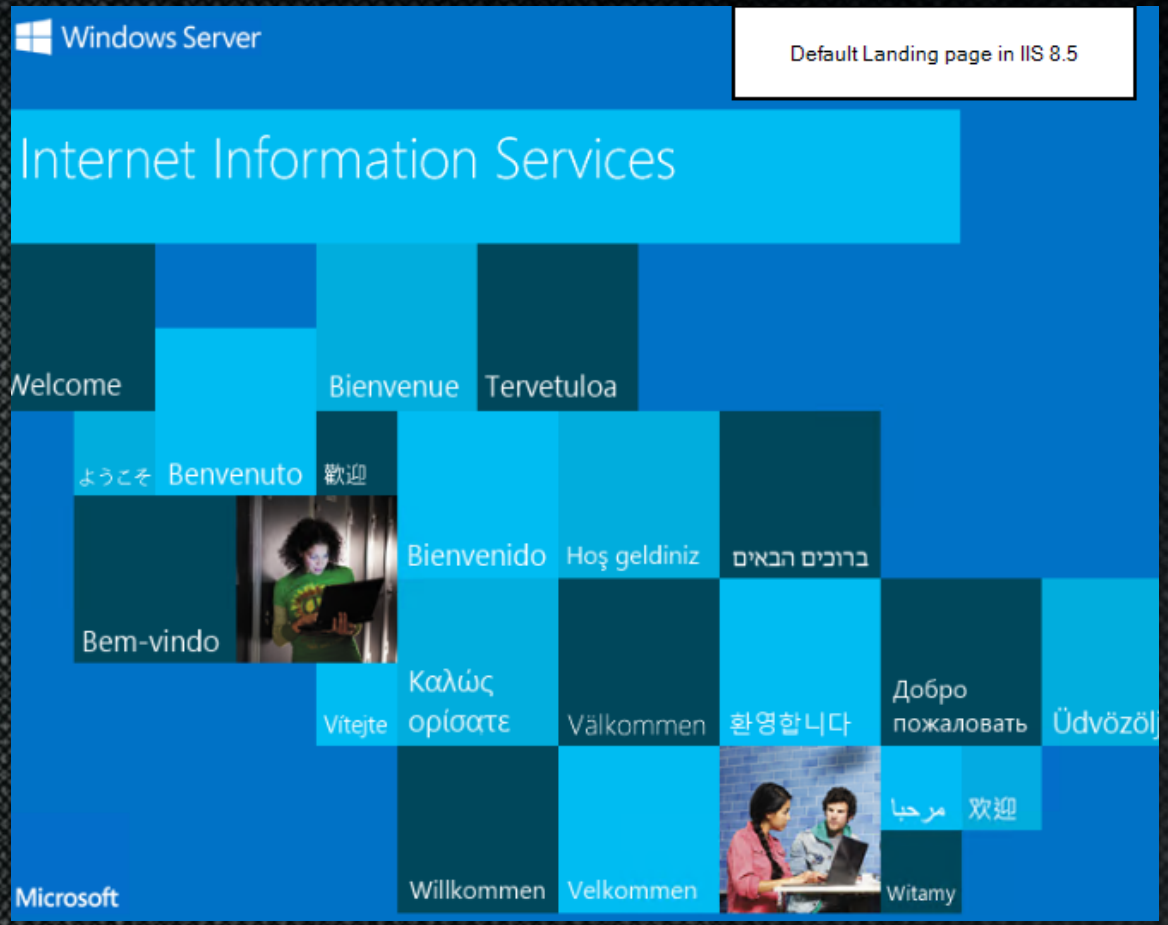
- When does a port open?
- Oscillating ports
- Service detection
- 65536 ports
  - But 90% of most common TCP ports pertain only 576 ports
- New port? New attack surface!
  - Better assess, attack and protect before anyone else…
- Scan in different configurations
  - Attackers have time, we can scan over long durations

Using trackers to expand the attack surface

```
nmap --script http-tracker_tracking.nse -p 80 -T 4  zonetransfer.me digininja.org -oA tracking

Starting Nmap 6.00 ( http://nmap.org ) at 2013-03-01 13:46 GMT
Nmap scan report for zonetransfer.me (217.147.180.162)
Host is up (0.024s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-tracker_tracking:
|   Tracking code: 7503551
|_  Page title: ZoneTransfer.me - DigiNinja

Nmap scan report for digininja.org (217.147.180.164)
Host is up (0.025s latency).
rDNS record for 217.147.180.164: www.digininja.org
PORT   STATE SERVICE
80/tcp open  http
| http-tracker_tracking:
|   Tracking code: 7503551
|_  Page title: DigiNinja

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.30 seconds
```

403/404/Splash-Pages

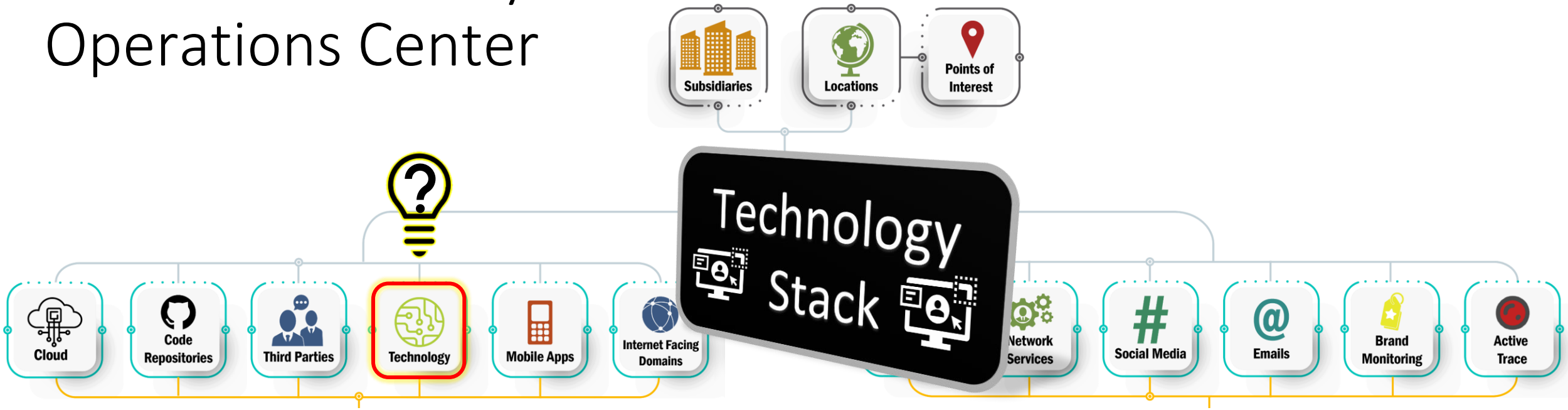
- Building great wordlists
  - CEWL is extremely useful
- DNS enumeration
- Content enumeration
- Indexed information in search engines
- VHOST enumeration
- IIS short name scanning



Short Name Scanning Example

```
PS C:\tmp\repos\IIS_shortname_Scanner> C:\Python27\python.exe .\iis_shortname_Scan.py https://[redacted]/metadatacard/
Server is vulnerable, please wait, scanning...
[+] /metadatacard/m~1.* [scan in progress]
[+] /metadatacard/me~1.*        [scan in progress]
[+] /metadatacard/met~1.*       [scan in progress]
[+] /metadatacard/meta~1.*      [scan in progress]
[+] /metadatacard/metad~1.*     [scan in progress]
[+] /metadatacard/metada~1.*    [scan in progress]
[+] /metadatacard/metada~1.z*   [scan in progress]
[+] /metadatacard/metada~1.zi*  [scan in progress]
[+] /metadatacard/metada~1.zip* [scan in progress]
[+] File /metadatacard/metada~1.zip*    [Done]
---------------------------------------------------------------
File: /metadatacard/metada~1.zip*
---------------------------------------------------------------
0 Directories, 1 Files found in total
```

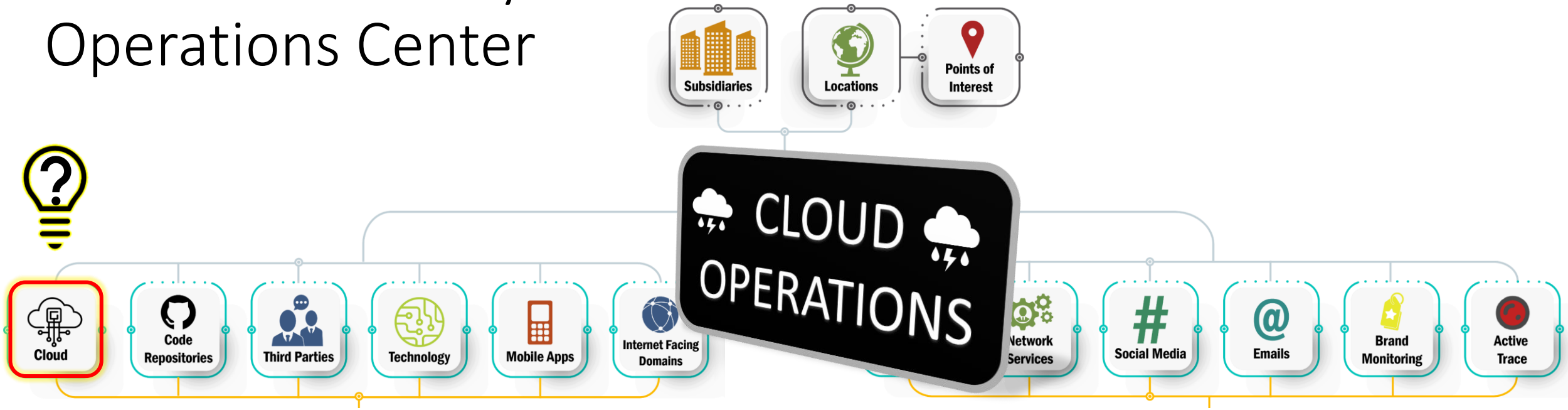
Building an Offensive Security Operations Center



Technology Stack

- Libraries might be vulnerable
  - JavaScript, dependencies, plugins, themes and more…
- Vulnerabilities
  - A vulnerability scanner finds a new vulnerability
  - Is it exploitable?
  - Can we hack the customer now?
  - Can we weaponize the CVE?
  - Local, authenticated or configuration-based vulnerabilities
- Log4j / OpenSSL / Next Big Thing happens
  - How do you react?

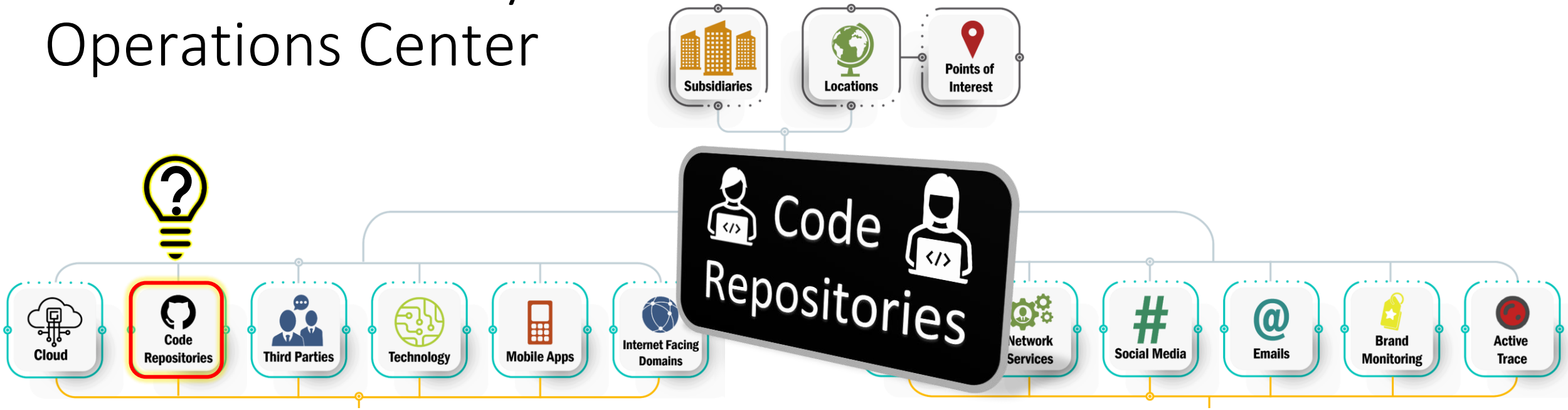
Building an Offensive Security Operations Center



Cloud Operations

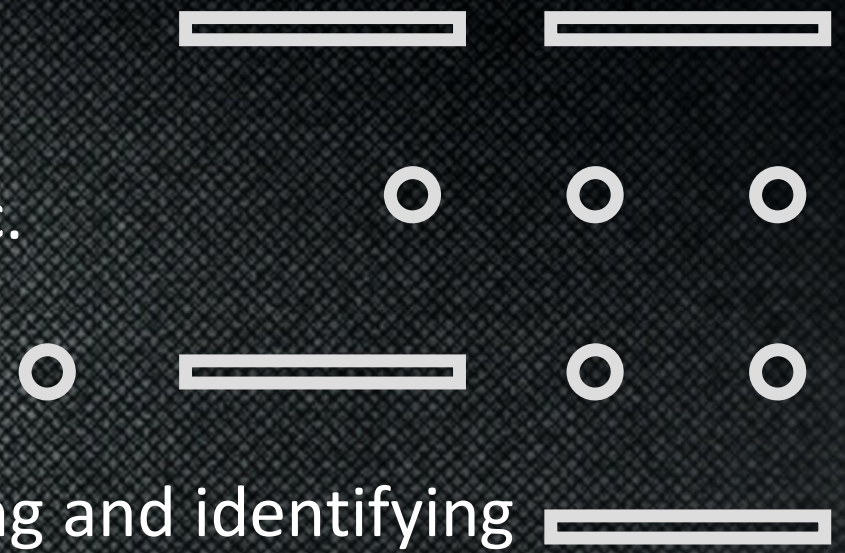
- You can scan from the outside AND inside of target customer cloud providers
  - TLS-Scan and other techniques help in attributing assets to customer
- Many OSINT sources enumerate and scan clouds
  - Check out: Grayhatwarfare.com
- Brute-force with targeted wordlists
- You can ask for an identity with list-*, describe-*, security-audit privileges
  - Scan, test and assess risk as new assets are provisioned and changed
- Anytime a customer deploy a cloud service:
  - Add it to monitoring
  - Start attacking it
  - Detect when it changes

Building an Offensive Security Operations Center

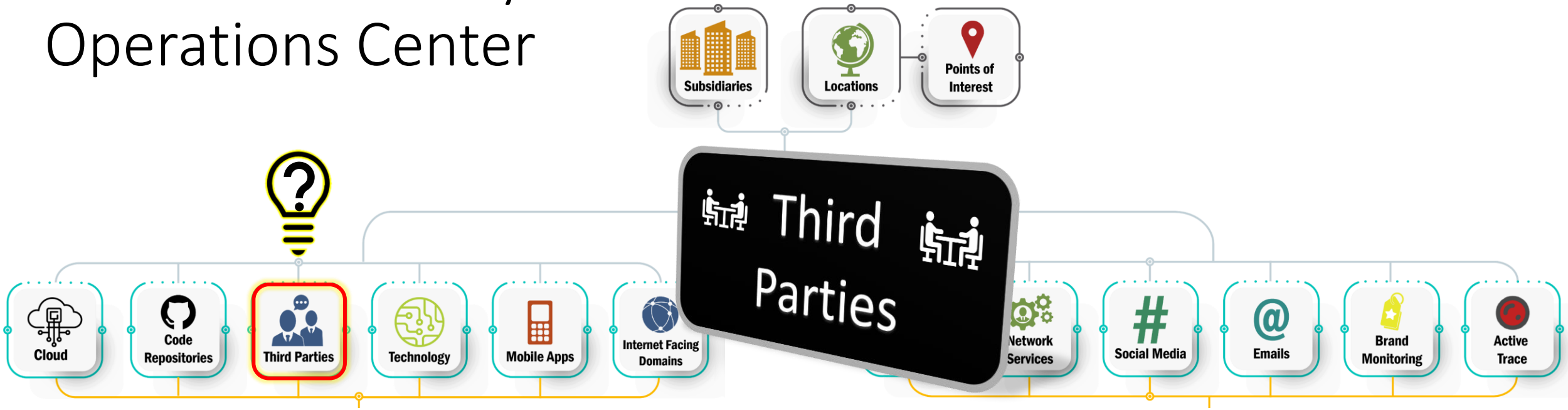


Code Repositories – They exist

- Many are public
  - Trufflehog
- Use search engines on GitHub, BitBucket, etc.
- GIST's for users on employees
  - Users private email addresses might be used
- Company "real names" are great for searching and identifying
  - Real name – Company name synonyms
    - E.g. riversecurity, rivsec, riversec
  - Can you find them attack surface when using company "real names"?



Building an Offensive Security Operations Center

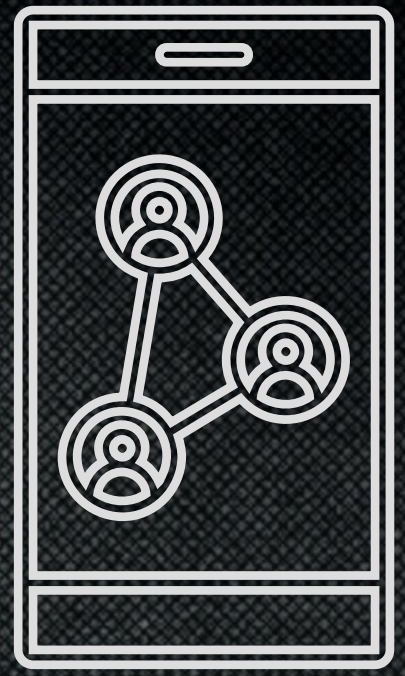


Third Parties

- Monitor Third Parties breaches and notable events
- Companies typically has a lot of SaaS
  - Does breached credentials work across them?
- Supply Chains
  - Useful for our CTI and understanding the paths towards target
- What if a third party is breached?
- Can we identify concerns when third party users are breached, possibly abusing our platform if we don’t contain it?

Building an Offensive Security Operations Center

Mobile Applications



- Typically communicates with API’s
- May have secrets embedded in them
- Contains valuable information for building:
  - Wordlists
  - Intelligence
- Monitor for new versions
  - Check delta
- Monitor for new applications
  - Detect when existing application vendors provision a new application
  - When customer name is represented in a new application

Mobile Applications

MOBILE APPLICATIONS [edit]

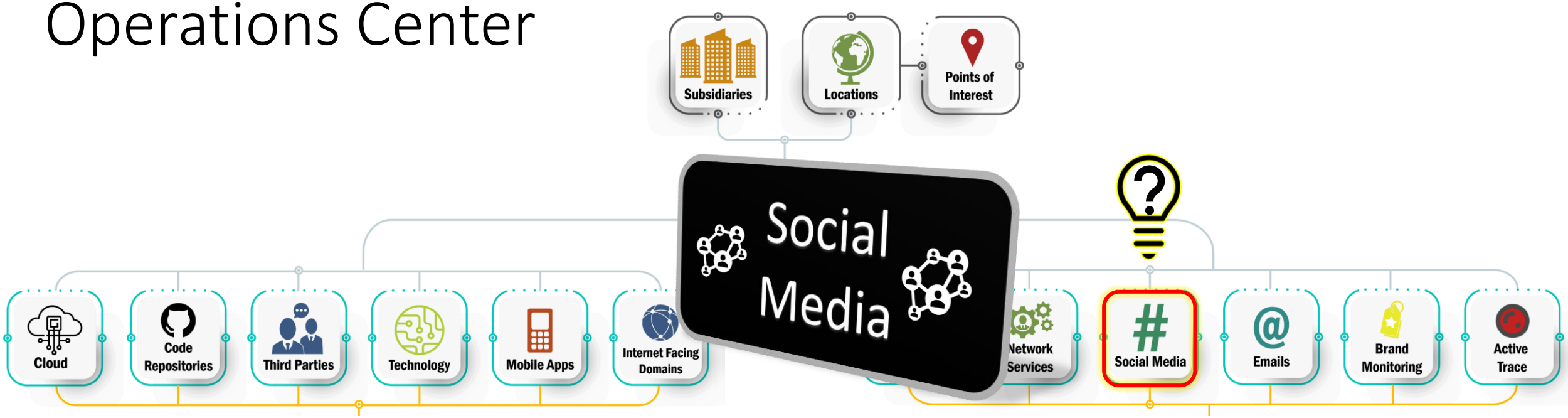
- https://theappstore.org/
- https://play.google.com/store/search
- https://appworld.blackberry.com/webstore/?countrycode=NO&lang=en
- https://www.microsoft.com
- https://android.fallible.co/

Building an Offensive Security Operations Center

Sensitive Information – i.e. Dark Data

- Google Dorking
- Automating querying through search engines
- Abusing CMS API's
- Discovering file uploads
- Leveraging OSINT
- Purchasing access to vendor API's
- Brute-forcing storage buckets, files, etc.

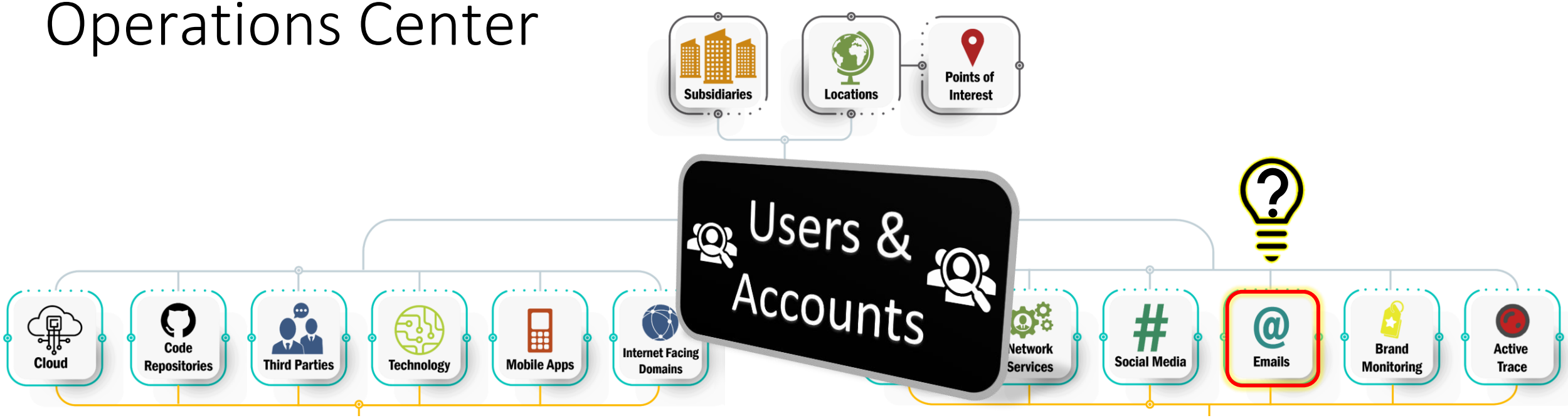
Building an Offensive Security Operations Center



Hacking Social Media and Monitoring

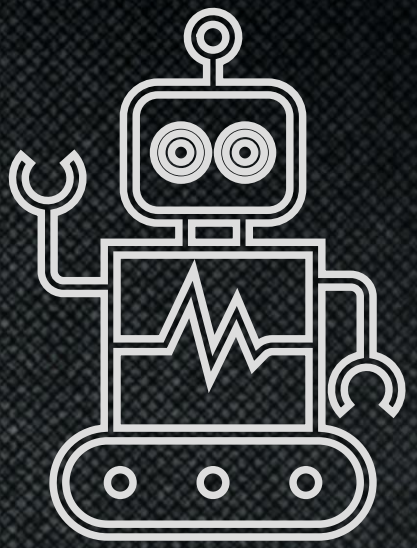
- Would your company suffer if Social Media is compromised?
- Can personal accounts be targeted to get into company accounts?
  - Credential stuffing, phishing, smishing, vishing
  - Social Engineering
- A few SoME has shared logins
  - Often stupid passwords
  - Memorable passwords which can be guessed
- Identify SoME accounts and do sentiment monitoring
  - AI/ML helps in this aspect

Building an Offensive Security Operations Center

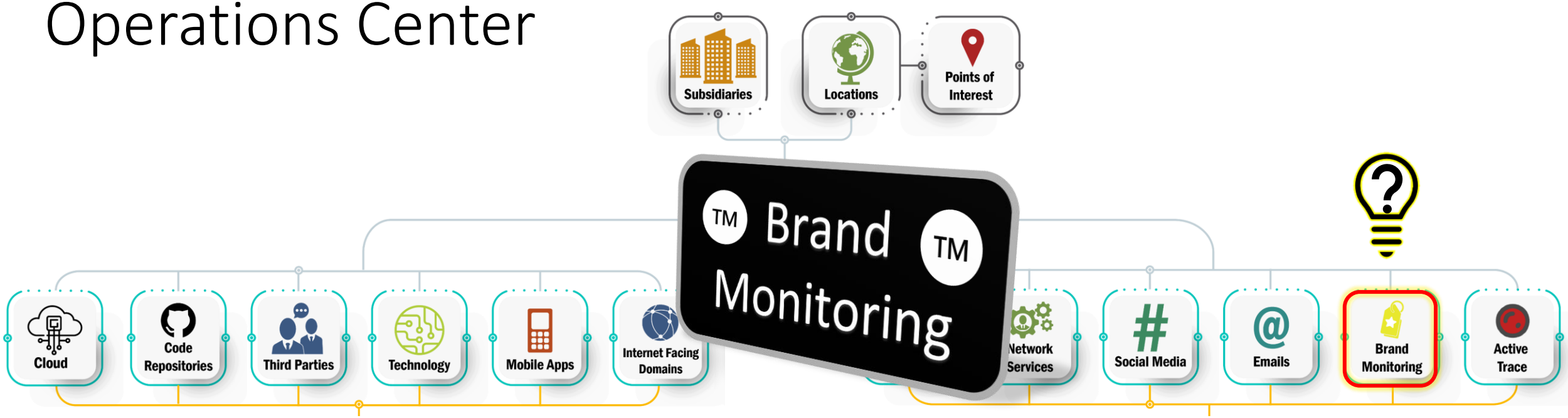


Users, Accounts and Emails

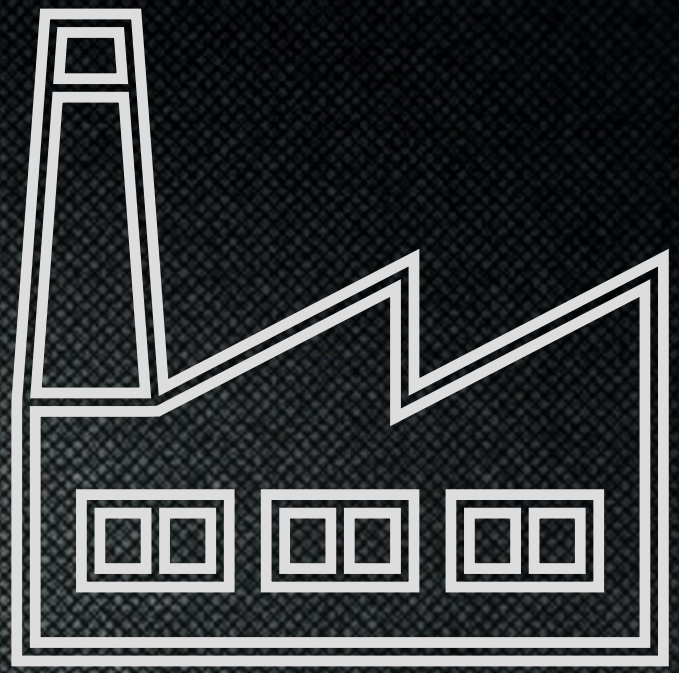
- Often all we have to do is simply **log-on** and the customer is breached
- What is an email? What can it be targeted for?
  - Phishing?
  - What about password spraying?
    - Email is often a username
  - How many logins does a company have?
    - Might be a weak password…
    - They register accounts left and right
    - Guest accounts in target tenant (e.g. Azure AD)
- When a system is compromised, credentials are leaked
  - Credential stuffing
- Every week we have multiple reports through CTI about compromised systems
  - We do our best to get a hold of the databases and credentials



Building an Offensive Security Operations Center

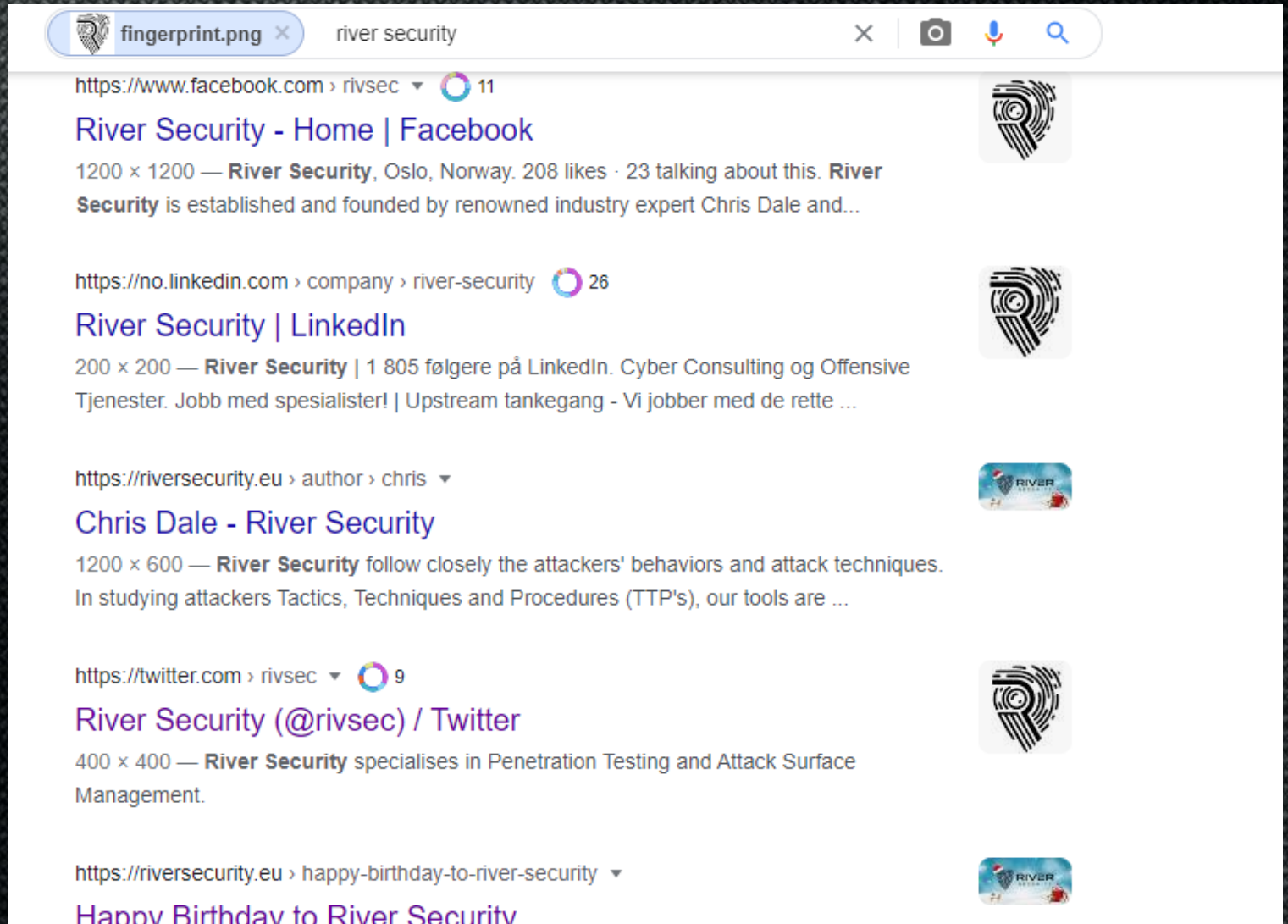


Leverage The Brand

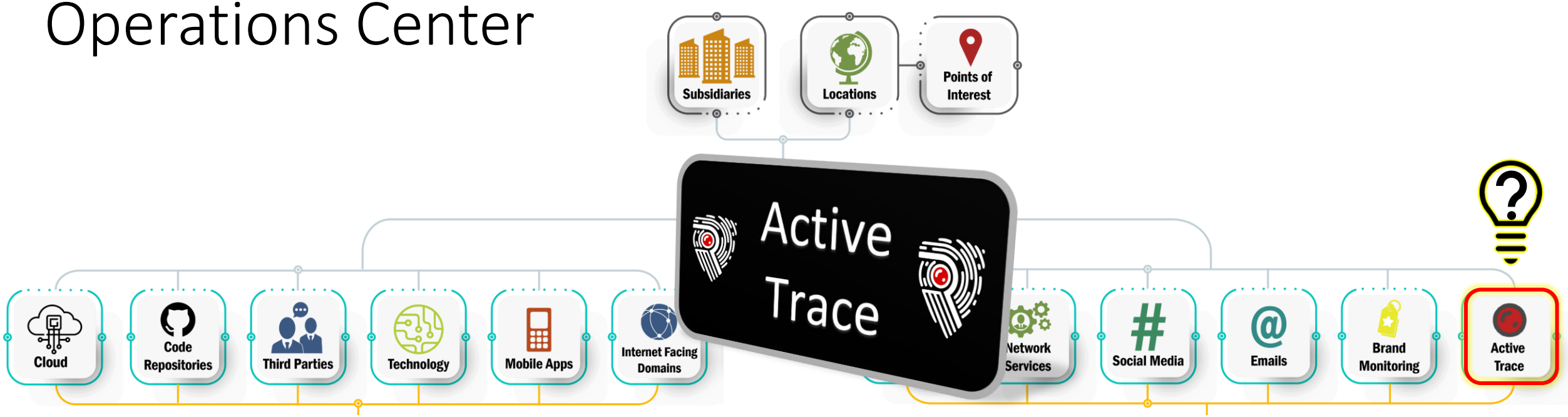


- Reverse image searching
  - Logos
  - Company specific images
- Company catch phrases and mottos
  - “Nike, just do it”
- You can automate querying for some of these things
  - It returns 1.000.000 hits, that is fine
  - But can we check and verify 1.000.001?
  - Is it easy? Is it doable?

Reverse Image Searching



Building an Offensive Security Operations Center

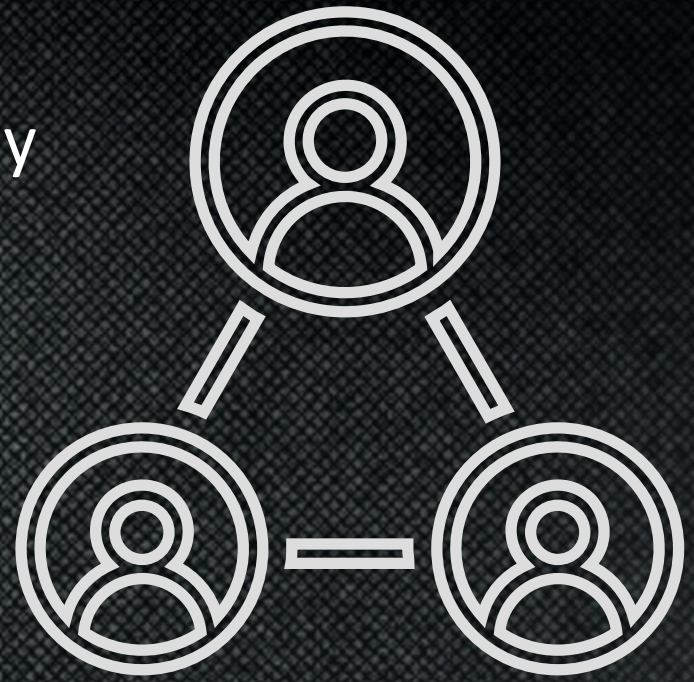


Active Trace – Adding Deception

- We can embed code which triggers when a code has been cloned
- SVG with callbacks
- JavaScript which only returns when website runs outside of original domain
- It doesn't have to be complex, but it adds to pro-activeness

Reporting

- Do we want yet another dashboard?
- Most organizations can consume from API's today
  - I.e., a defensive SOC
- Human to human interaction is valuable
  - It provides knowledge transfer
  - Collaboration stimulates solutions
- What we suggest and practice:
  - Report where customers can process the information
  - Make API's and data accessible
  - Adapt and innovate



CIS TOP 18

- **CIS 1: Inventory and Control of Enterprise Assets**
- **CIS 2: Inventory and Control of Software Assets**
- **CIS 3: Data Protection**
- **CIS 4: Secure Configuration of Enterprise Assets and Software**
- CIS 5: Account Management
- **CIS 7: Continuous Vulnerability Management**
- **CIS 12: Network Infrastructure Management**
- CIS 13 Network Monitoring and Defense
- CIS 14: Security Awareness and Skills Training
- CIS 15: Service Provider Management
- **CIS 16: Application Software Security**
- **CIS 18: Penetration Testing**

NSM CORE PRINCIPALS FOR INFORMATION SECURITY

- **1. Identify and Map**
- **1.1 Map governance, deliveries, supply chain, and supporting systems**
- **1.2 Map assets and software**
- 1.3 Map users and need for access and privileges
- **Protect and Maintain**
- 2.1 Maintain security in procurement and development processes
- **2.2 Establish a secure IT infrastructure**
- **2.3 Ensure a secure configuration**
- **2.4 Protect the organizations networks**
- 2.5 Control the flow of data
- **2.6 Ensure control of identities and accesses**
- **2.7 Protect data at rest and data in transit**
- **2.8 Protect email and browser**
- 2.9 Establish routes and skill to recover data
- **2.10 Integrate security into processes for Change Management**
- **Detect**
- **3.1 Detect and remove known vulnerabilities and threats**
- **3.2 Establish security monitoring**
- 3.3 Analyze data from security monitoring
- **3.4 Perform penetration tests**
- **Handle and restore**
- 4.1 Prepare the business for handling incident response
- 4.2 Evaluate and categorize incidents
- 4.3 Control and handle incidents
- 4.4 Evaluate and learn from incidents

Cyber Warfare vs. Traditional Warfare

"Know yourself, know your enemy, you will not fear the result of a hundred battles"
Sun Tzu, The Art of War

APT – Advanced Persistent Threat

Does not have to be advanced, just persistent

Thank You For Your Attention!

https://into.bio/chrisdale & https://into.bio/rivsec

Download slides here!

Twitter – https://twitter.com/ChrisADale

LinkedIn – https://www.linkedin.com/in/chrisad/

Fighting Cyber Crime – https://riversecurity.eu