Skilpadden mot Haren – Hvordan Penetration Testing feiler

RIVER SECURITY

WHO AM I?

Principal and Founder at River Security

Principal Instructor at SANS

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

WHY DO WE DO PENTESTING?

What is the goal of a penetration test?

Common problems with traditional pentests…

Receiving a Pentest

Providing a Pentest

Procuring and Receiving a Penetration Test

As a Client

- What is the scope of the pentest?
  - You might have some idea
  - Very often clients doesn’t have the full idea of their own attack surface
- Very often wants a single application pentest
  - Testing one application vs. Testing the organizations resilience against attacks
- The client doesn’t know how hackers operate!
- Once a year approach

Providing a Penetration Test

As a Provider

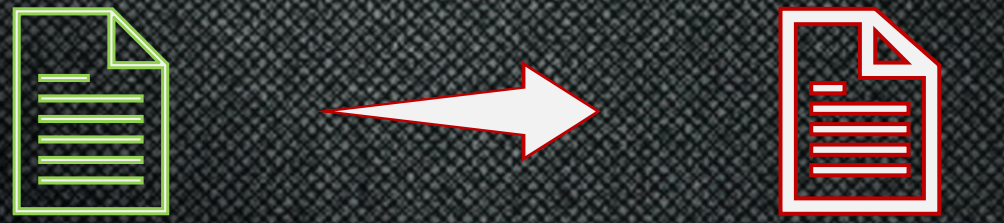
- What is the scope?
  - How do you find out?
  - The customer is likely not to know what their attack surface is
  - How much is the customer willing to invest?
- Ideally try to avoid annoying scoping meetings
- Focus on an individual application instead of real-world scenarios
- You start your work, only to be surprised by scope creep


Do Attackers Care About Scope?

Mapping Attack Surface First

Split the Penetration Test into two deliveries

- Client knows what has been left out of scope
- Easier for client to commit on having work done
- Easier to guarantee that the entire (or just some) of the scope has been tested
- Immediate value from having penetration testers first LOOK at you
- Customer gets an 3rd party understanding of their attack surface
- Easier on the Penetration Testers while they're doing work



Digital Attack Surface Report

Penetration Test Report

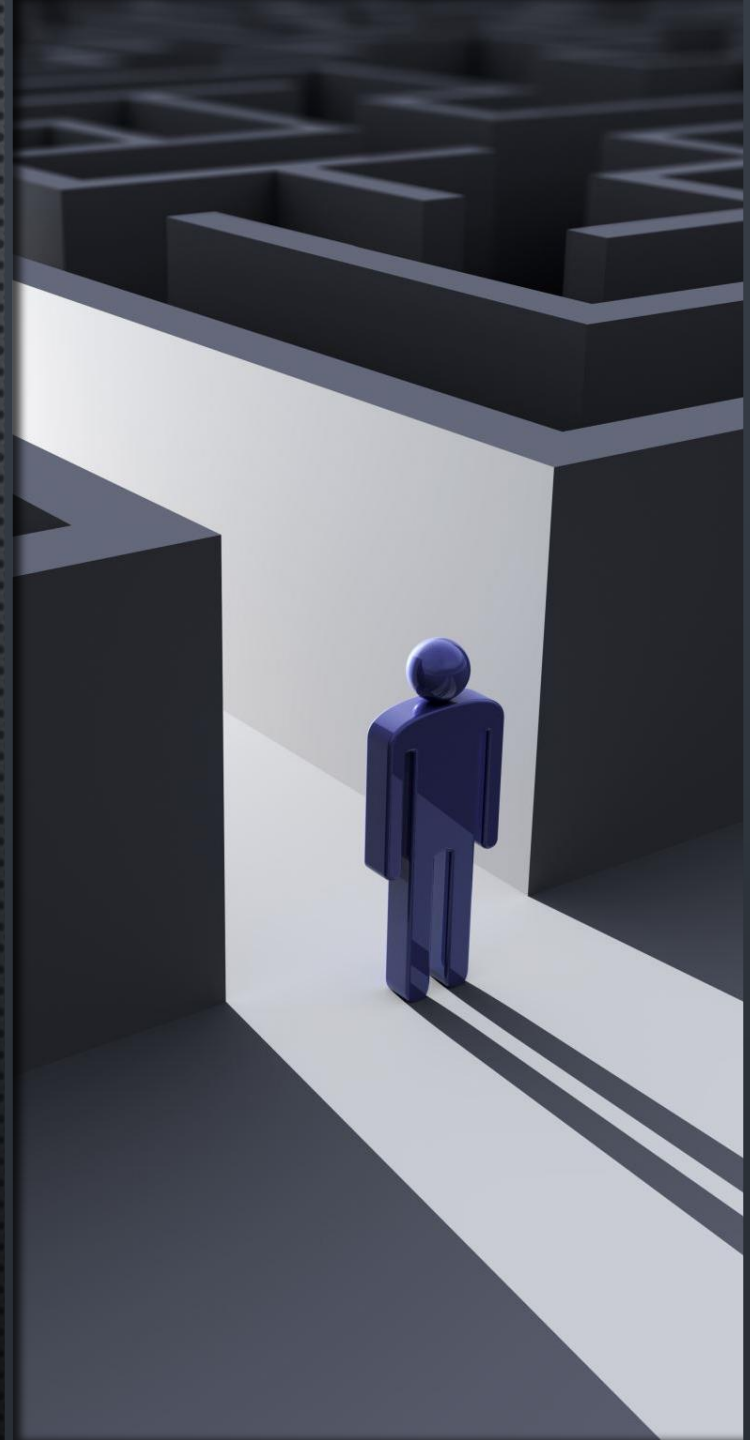
WHAT IS ATTACK SURFACE MANAGEMENT?

RIVER SECURITY

HIGH LEVEL PENTEST METHODOLOGY

ATTACK SURFACE MANAGEMENT

- Discovering OPPORTUNITIES as companies innovate and change
- Continuously doing Reconnaissance, Scanning and Discovery
- Identifying dark data and shadow IT
- Finding the paths and roads least travelled to
- Knowing the target better than they know themselves
- Discovering changes and opportunities to attack surface
- What about that door we left open?



Attackers often get in via 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

Business Innovation 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

Organizations Direction

WHAT IS ALWAYS-ON PENETRATION TESTING?

RIVER SECURITY

HIGH LEVEL PENTEST METHODOLOGY

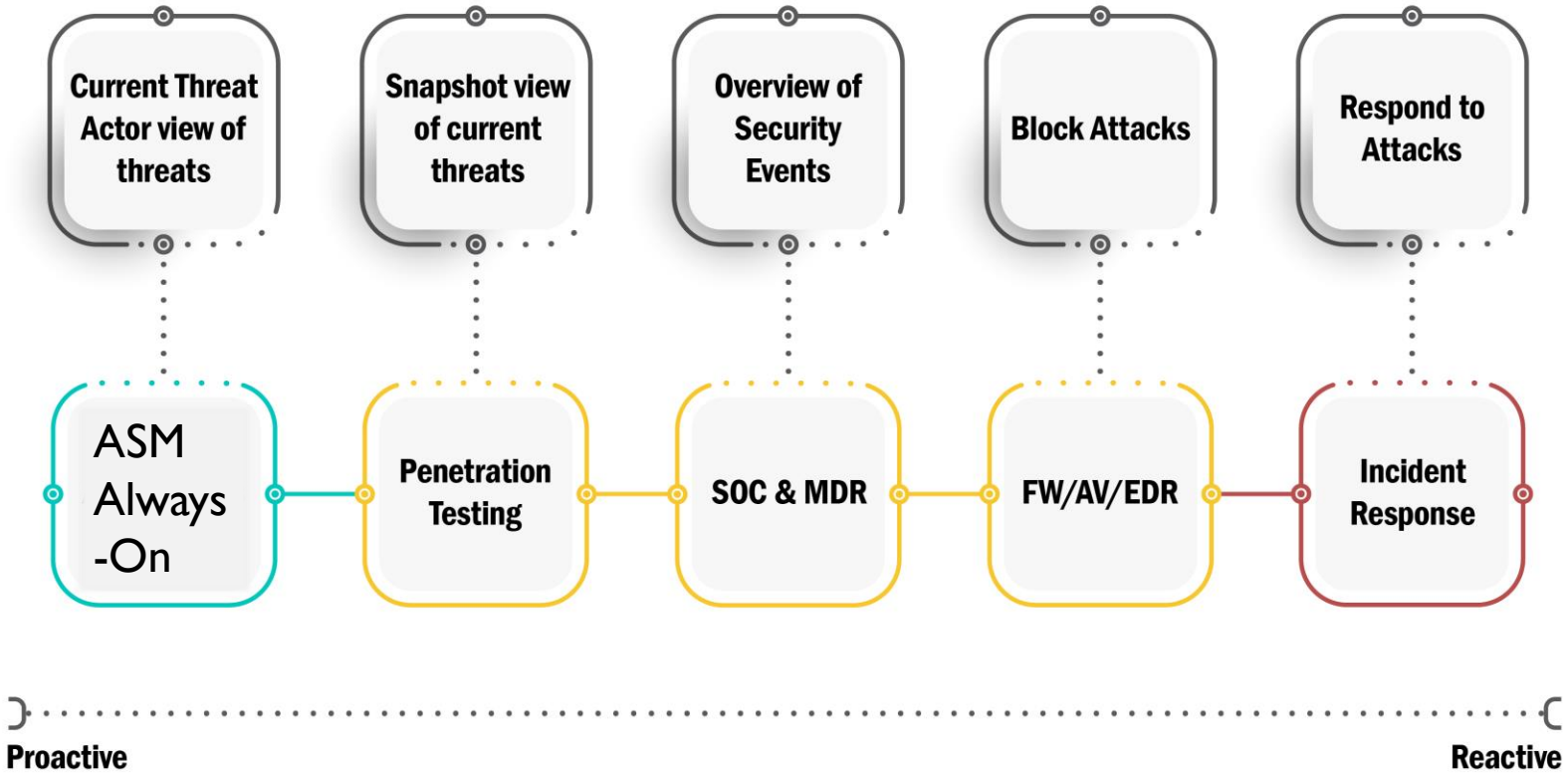
ALWAYS-ON PENETRATION TESTING

- Assessing risk, continuously and always prying on opportunities which arise
- Weaponization of CVE's
- High fidelity alerts; only alerting on what matters
- Micro engagements instead of weeklong engagements
- DevSecOps has been a thing for a while now
- Successful bug bounty hunters win because they find opportunities

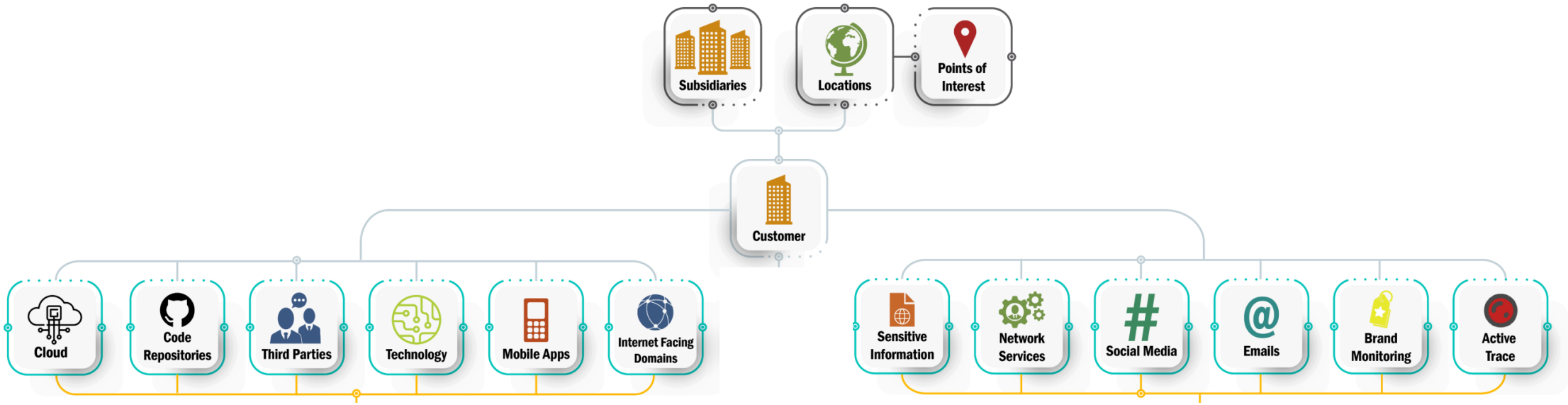
With Traditional Pentesting – Are we playing the same game as attackers?


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

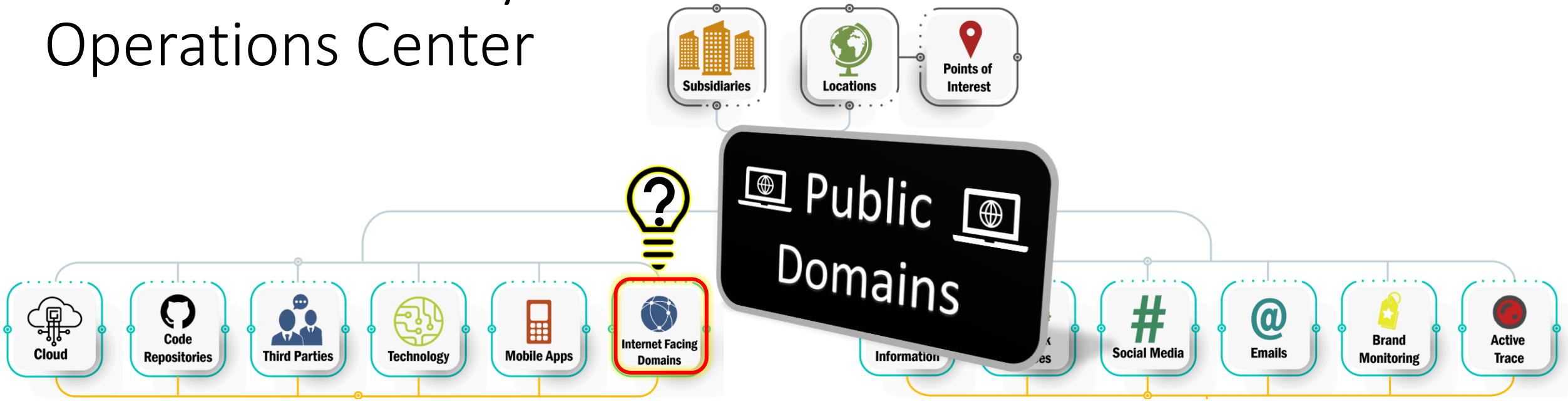
Proactive vs. Reactive



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



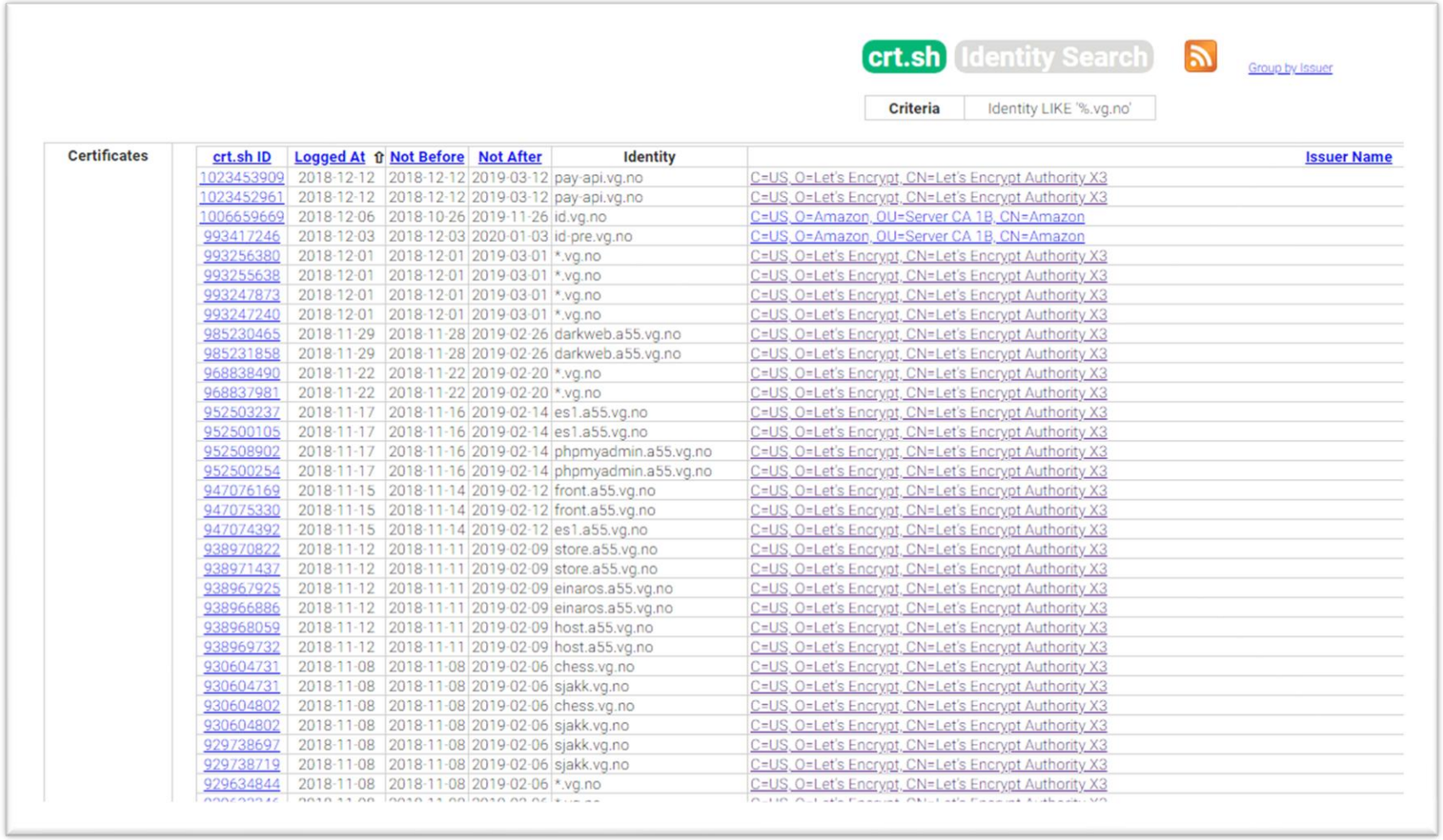
Building an Offensive Security Operations Center



Domains

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

Certificate Transparency Log



crt.sh Identity Search Group by Issuer

Criteria | Identity LIKE '%.vg.no'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Identity	Issuer Name
1023453909	2018-12-12	2018-12-12	2019-03-12	pay-api.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1023452961	2018-12-12	2018-12-12	2019-03-12	pay-api.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1006659669	2018-12-06	2018-10-26	2019-11-26	id.vg.no	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
993417246	2018-12-03	2018-12-03	2020-01-03	id-pre.vg.no	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
993256380	2018-12-01	2018-12-01	2019-03-01	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
993255638	2018-12-01	2018-12-01	2019-03-01	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
993247873	2018-12-01	2018-12-01	2019-03-01	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
993247240	2018-12-01	2018-12-01	2019-03-01	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
985230465	2018-11-29	2018-11-28	2019-02-26	darkweb.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
985231858	2018-11-29	2018-11-28	2019-02-26	darkweb.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
968838490	2018-11-22	2018-11-22	2019-02-20	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
968837981	2018-11-22	2018-11-22	2019-02-20	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
952503237	2018-11-17	2018-11-16	2019-02-14	es1.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
952500105	2018-11-17	2018-11-16	2019-02-14	es1.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
952508902	2018-11-17	2018-11-16	2019-02-14	phpmyadmin.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
952500254	2018-11-17	2018-11-16	2019-02-14	phpmyadmin.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
947076169	2018-11-15	2018-11-14	2019-02-12	front.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
947075330	2018-11-15	2018-11-14	2019-02-12	front.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
947074392	2018-11-15	2018-11-14	2019-02-12	es1.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
938970822	2018-11-12	2018-11-11	2019-02-09	store.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
938971437	2018-11-12	2018-11-11	2019-02-09	store.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
938967925	2018-11-12	2018-11-11	2019-02-09	einaros.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
938966886	2018-11-12	2018-11-11	2019-02-09	einaros.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
938968059	2018-11-12	2018-11-11	2019-02-09	host.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
938969732	2018-11-12	2018-11-11	2019-02-09	host.a55.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
930604731	2018-11-08	2018-11-08	2019-02-06	chess.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
930604731	2018-11-08	2018-11-08	2019-02-06	sjakk.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
930604802	2018-11-08	2018-11-08	2019-02-06	chess.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
930604802	2018-11-08	2018-11-08	2019-02-06	sjakk.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
929738697	2018-11-08	2018-11-08	2019-02-06	sjakk.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
929738719	2018-11-08	2018-11-08	2019-02-06	sjakk.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
929634844	2018-11-08	2018-11-08	2019-02-06	*.vg.no	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

https://transparencyreport.google.com/https/certificates

https://certstream.calidog.io

https://crt.sh


uri_lastsub_domain:test
http://test-automation[redacted]com/job/[redacted]pra%20ID%
http://test.[redacted]om/indrepetronyte?utm_campai
http://test.[redacted].com/geosweep-web/memberhome?g
http://test.[redacted]com/Jump/?v=3&i=2336&amp
URL SHORTENERS
URLTeam over at ArchiveTeam has been doing a brute force against URL Shorteners
uri_lastsub_domain.keyword:staging
staging.[redacted].org
staging-[redacted].com
staging.[redacted].com
staging.[redacted].com

Backup data

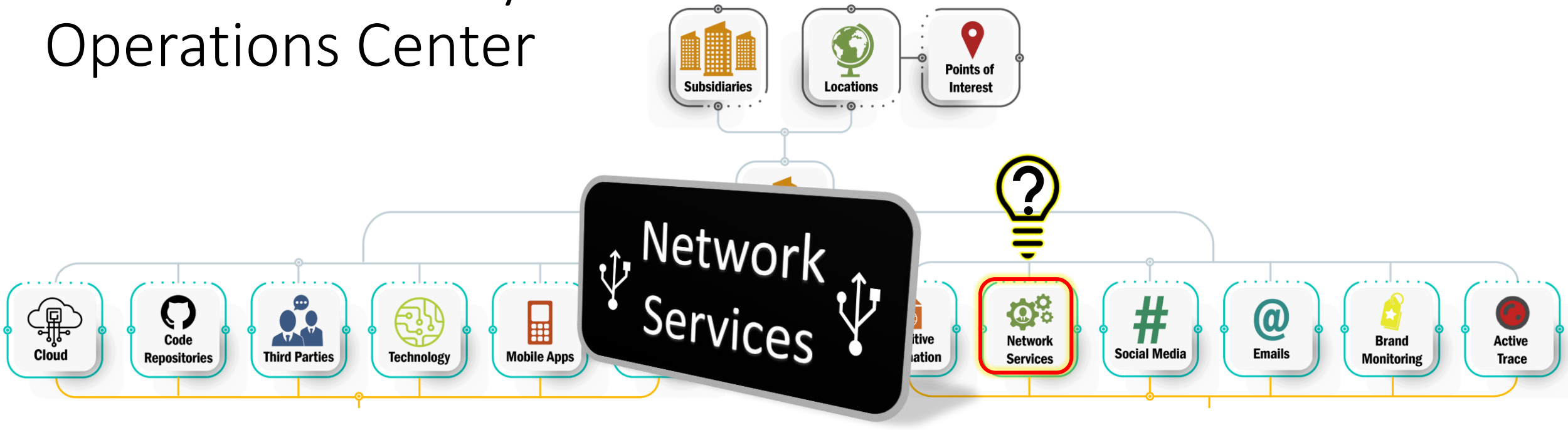
Next up in line of examples is backed up data. Many developers and IT-operators make temporary backups available online. While sharing these, it is evident that some of them have used URL shorteners to make life more convenient. This vulnerability classifies as a information leak.

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]ta-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/

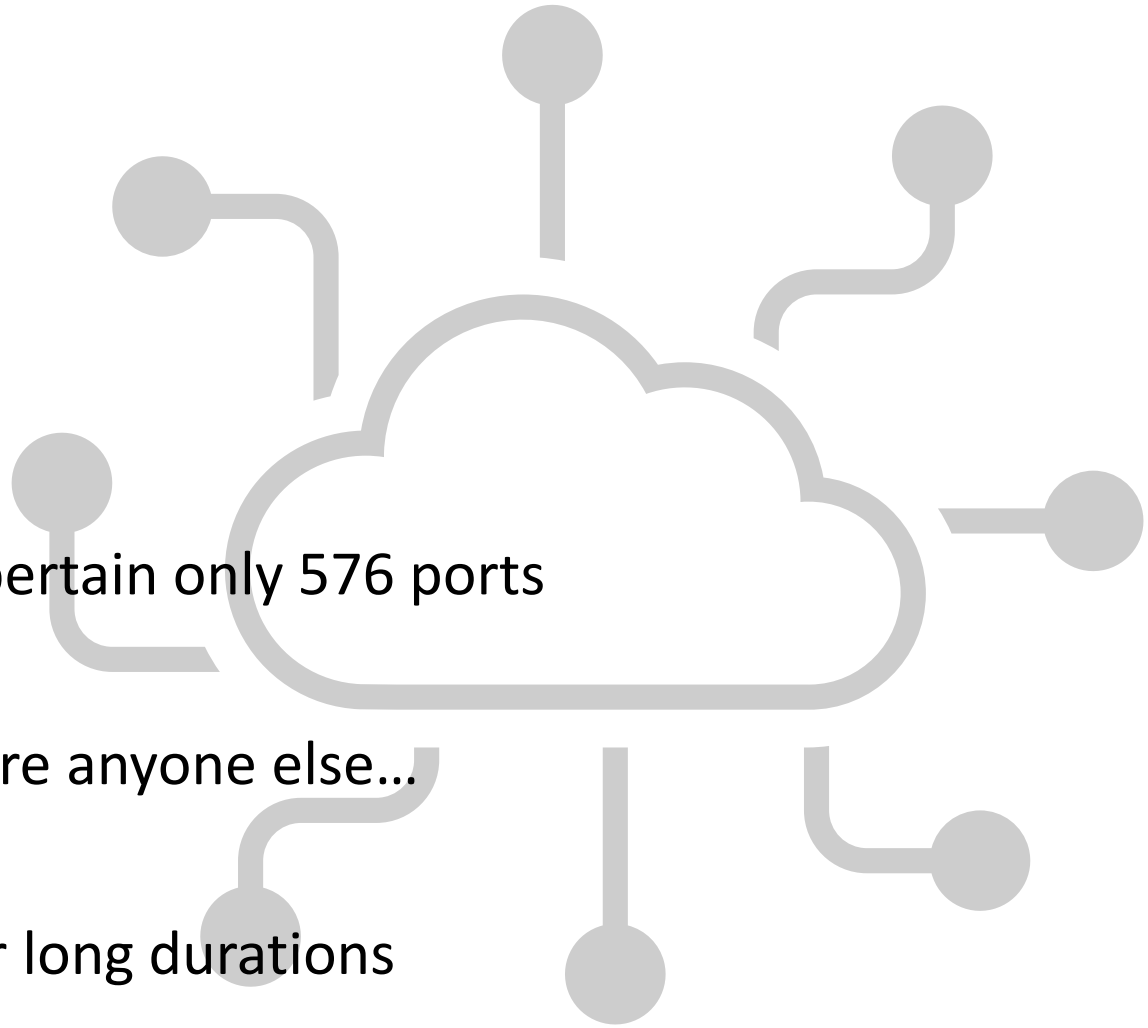
Parked Domains

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

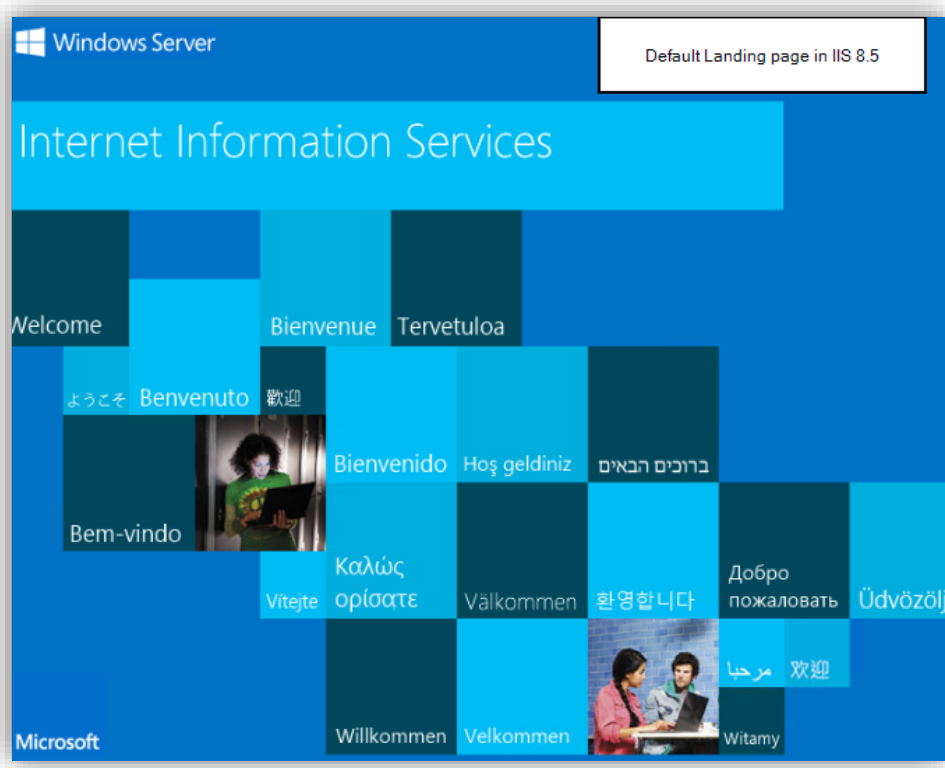


Using trackers to expand the attack surface

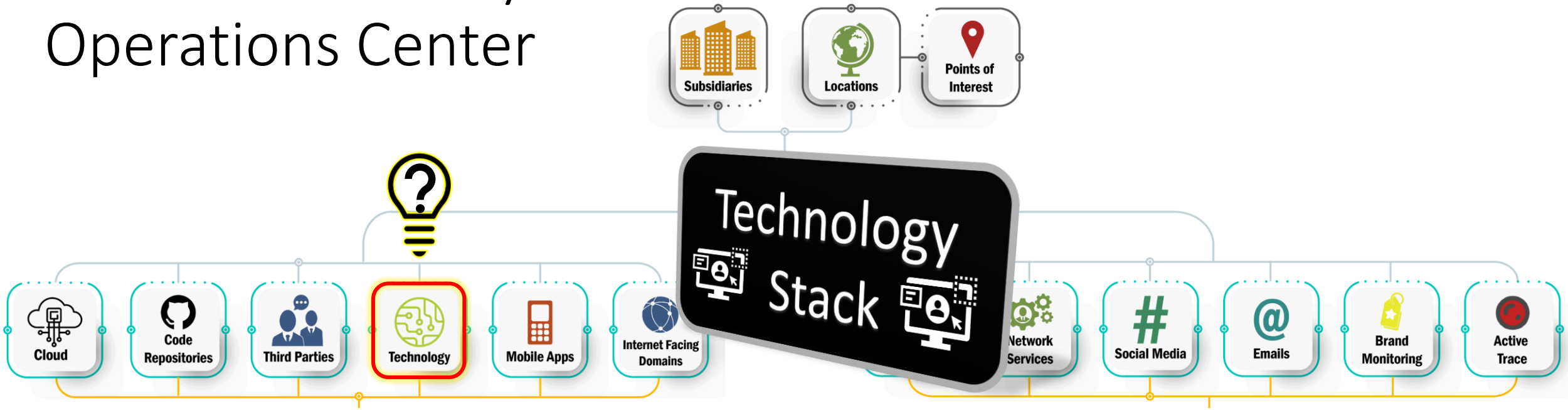
```
nmap --script http-tracker_tracking.nse -p 80 -T 4  zonetransfer.me digininja.org -oA tracking

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



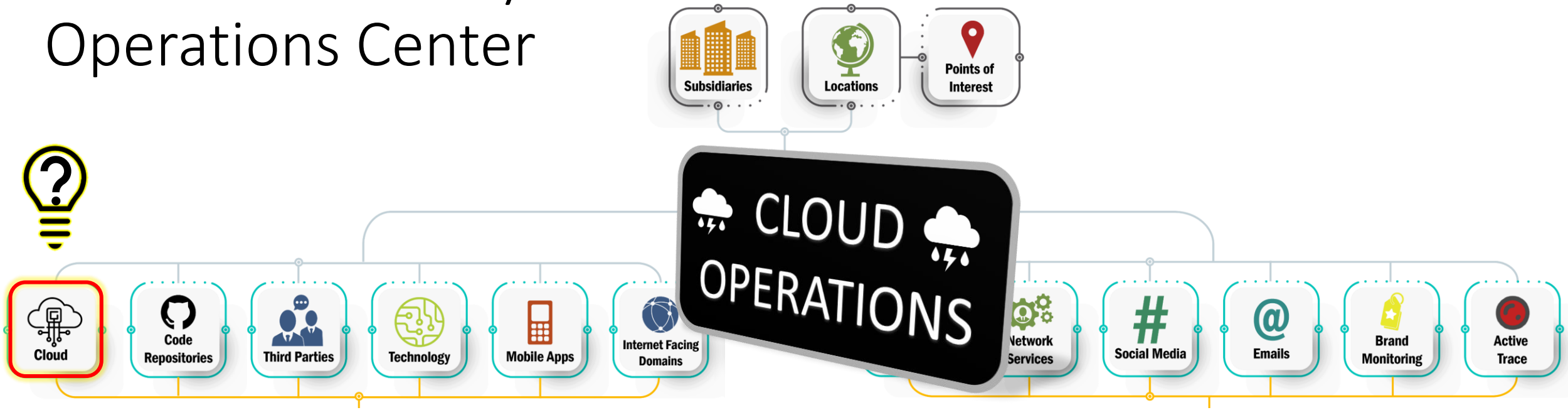
Building an Offensive Security Operations Center



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 happens
  - How do you react?

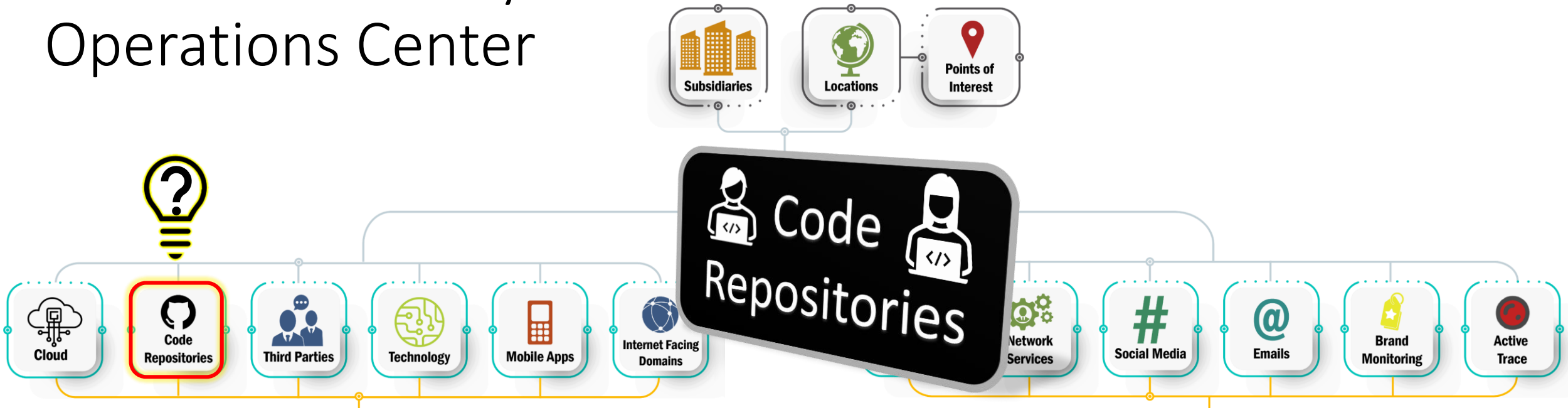
Building an Offensive Security Operations Center



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
- Several OSINT sources
- Brute-force with targeted wordlists
- You can ask for an identity with list-* 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

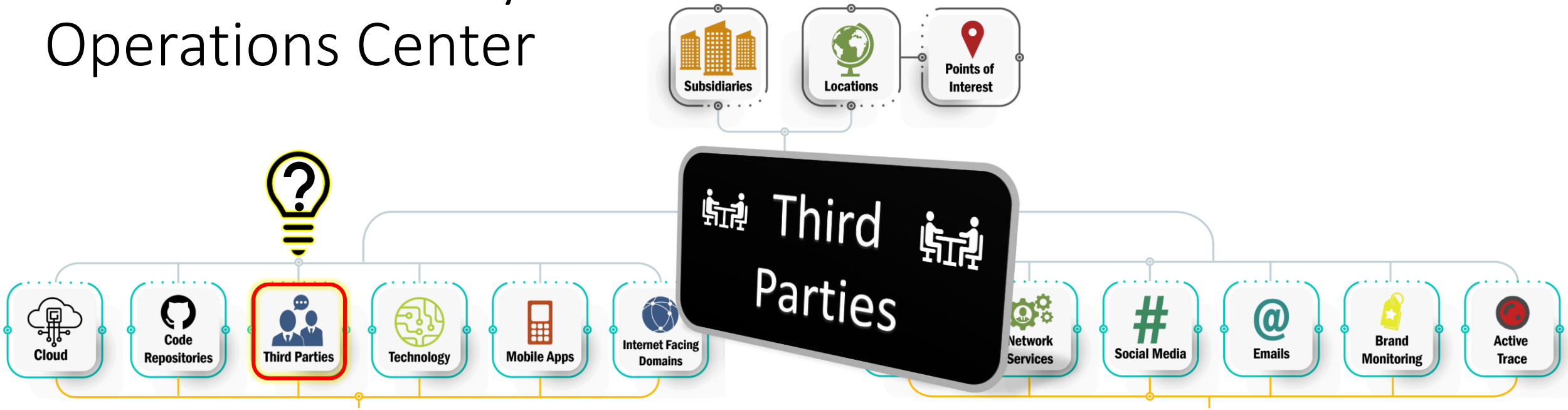
Building an Offensive Security Operations Center



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. River Security, 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

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]

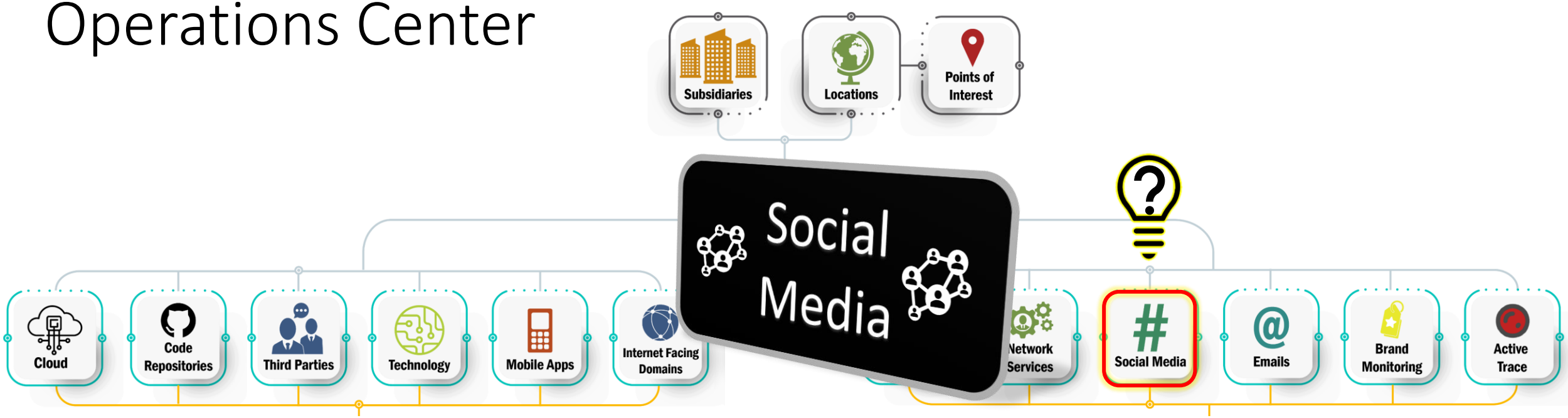
- https://theappstore.org/
- https://play.google.com/store/search
- https://appworld.blackberry.com/webstore/?countrycode=NO&lang=en
- https://www.microsoft.com
- https://android.fallible.co/

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.

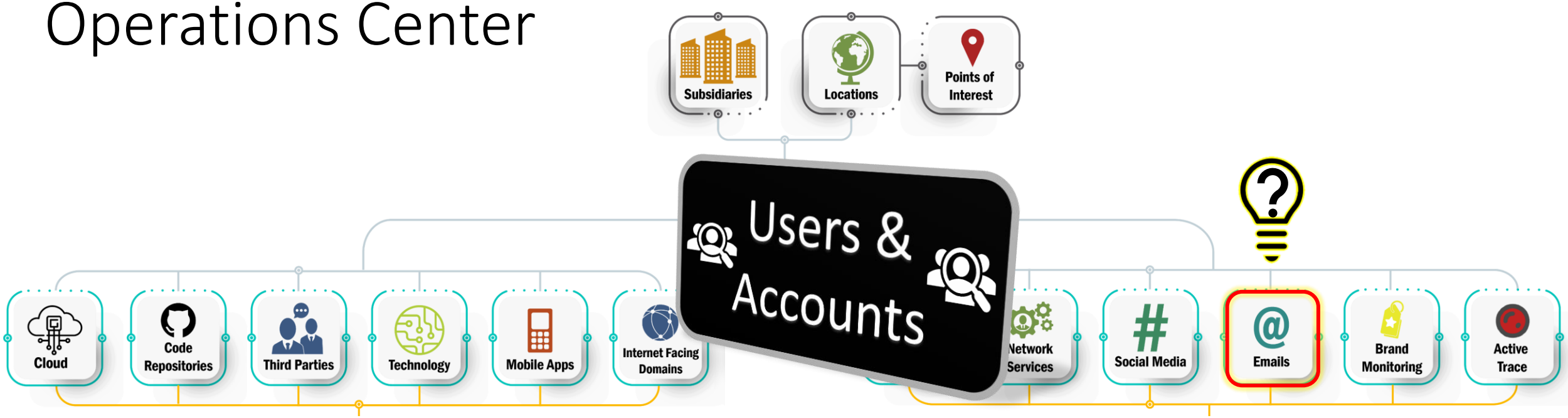
Building an Offensive Security Operations Center



Hacking Social Media and Monitoring

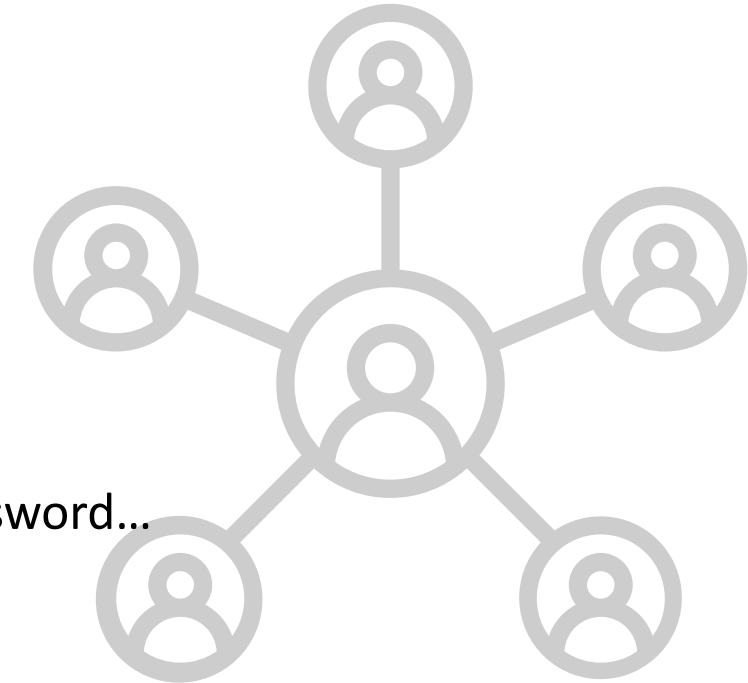
- Would your company suffer if Social Media is compromised?
- Can personal accounts be targeted to get into company accounts?
  - Credential stuffing, phishing, smishing, vishing
  - Social Engineering
- A few SoME has shared logins
  - Often stupid passwords
  - Memorable passwords which can be guessed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

Building an Offensive Security Operations Center

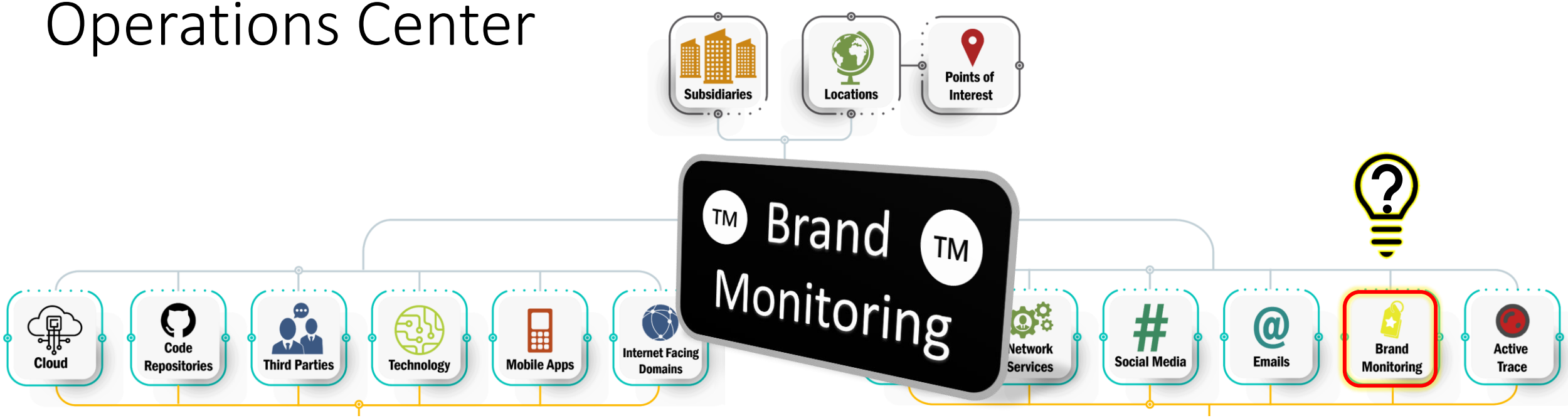


Users, Accounts and Emails

- Users have:
  - Emails
  - Usernames
  - Credentials
  - Position
- What is an email? What can it be targeted for?
  - Phishing?
  - What about password spraying?
  - How many logins does a company have? Might be a weak password…
    - They register accounts left and right
- 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
- Often all we have to do is simply **log-on** and the customer is breached

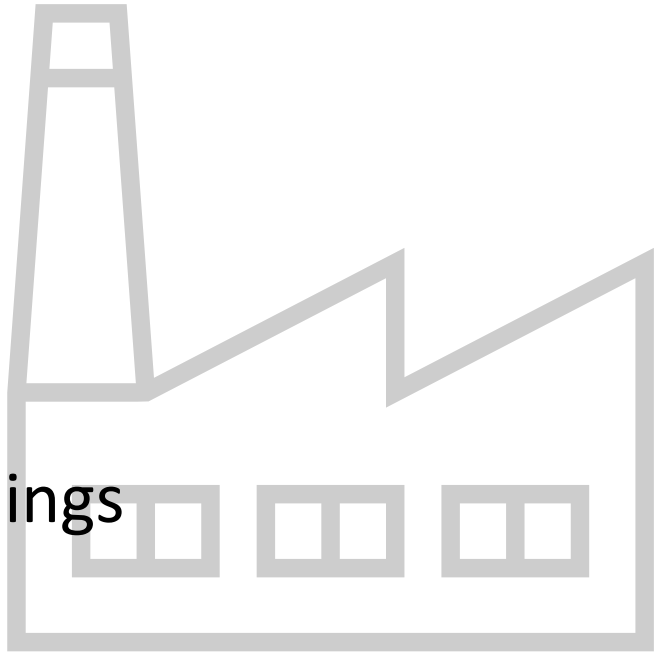


Building an Offensive Security Operations Center

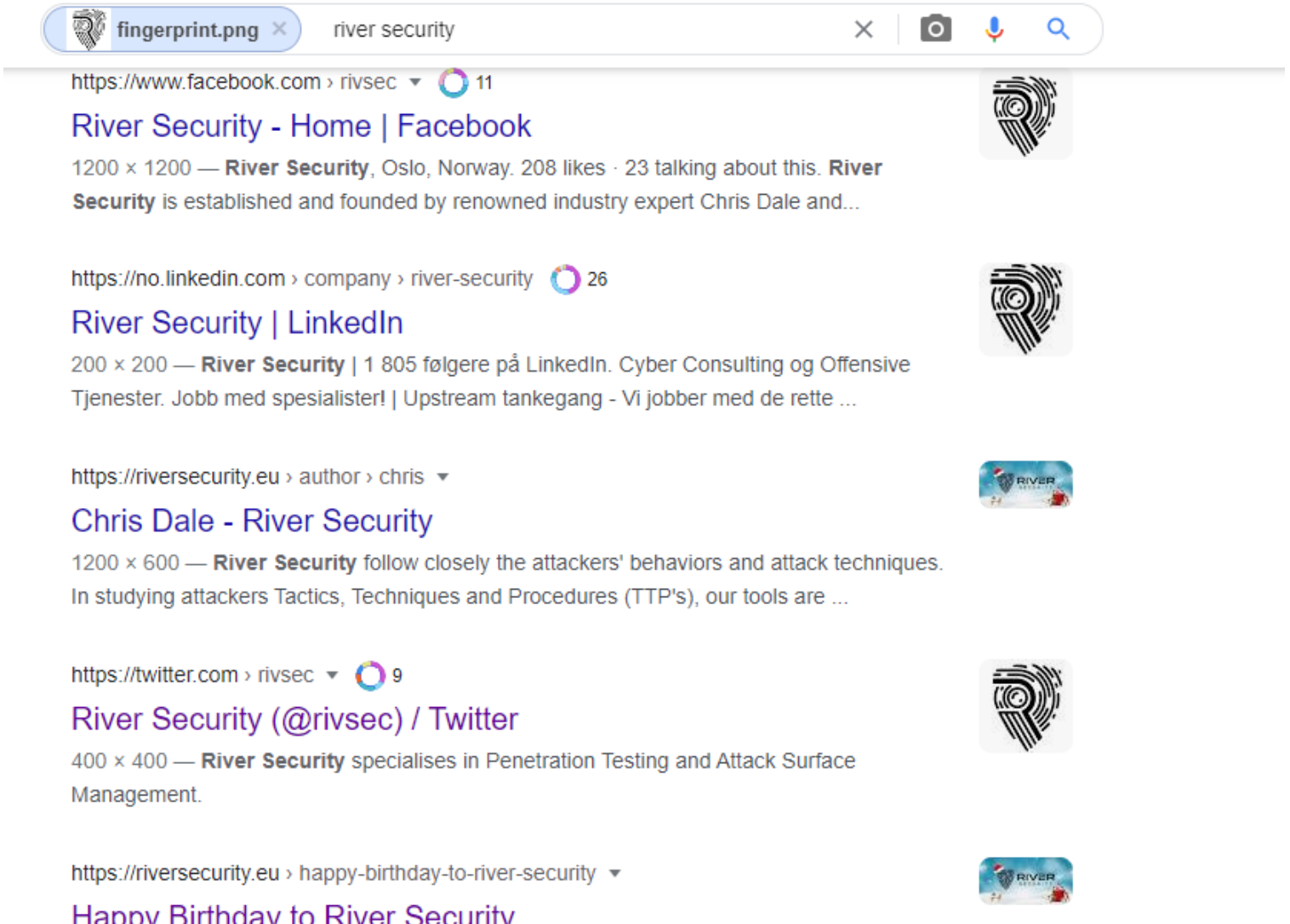


How can Offensive Services Leverage a Brand?

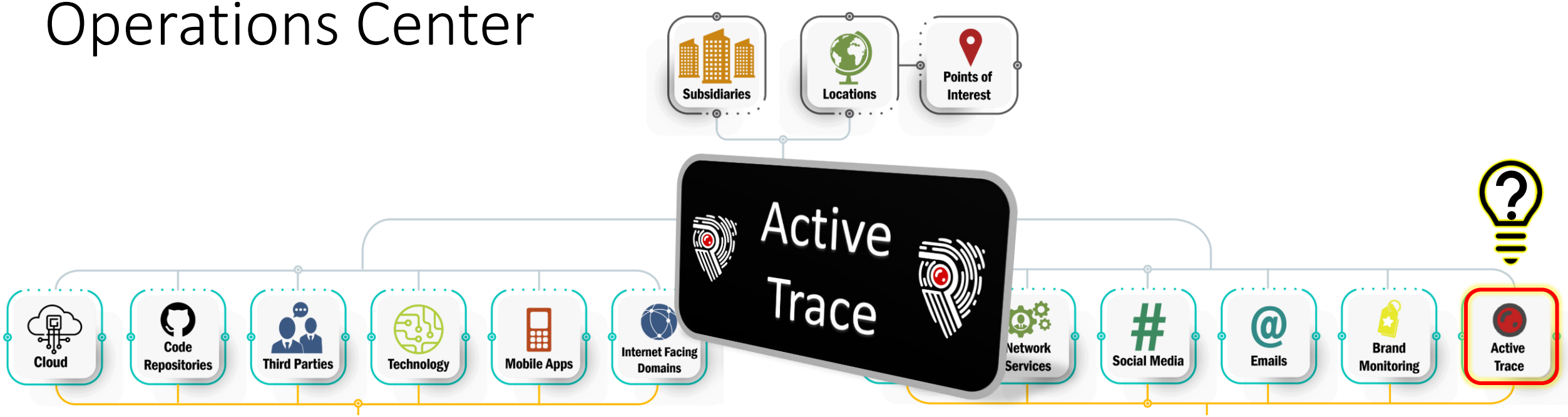
- Reverse image searching
  - Logos
  - Company specific images
- Company catch phrases and mottos
  - “Nike, just do it”
- You can automate querying for some of these things
  - It returns 1.000.000 hits, that is fine
  - But can we check and verify 1.000.001?
  - Is it easy? Is it doable?



Reverse Image Searching



Building an Offensive Security Operations Center



Active Trace

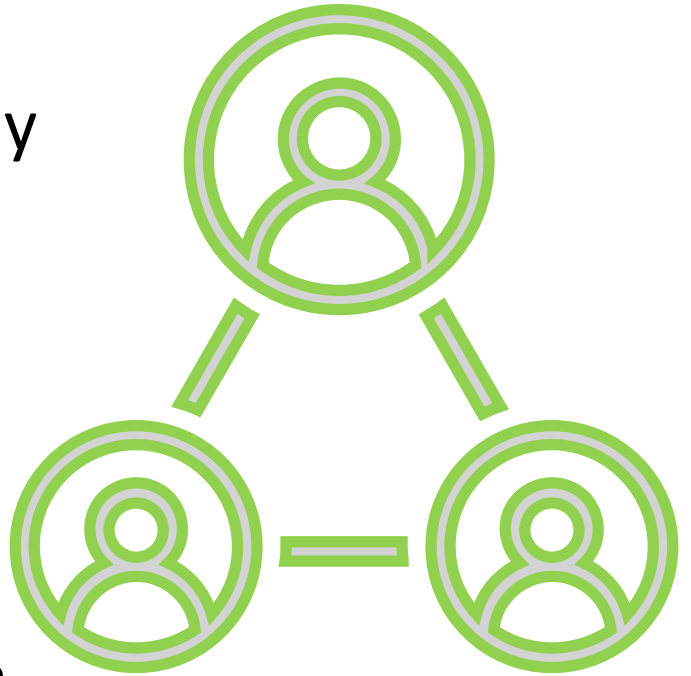
- Deception Element
- Can we embed code which triggers when a website has been cloned?
- SVG with callbacks when used outside of scope
- JavaScript which only returns when website runs outside of original domain
- It doesn’t have to be complex, but could get the job done

Alert: Website https://riversecurity.eu/ is calling back from http://riversecurity.eu-no.com

How our **O**ffensive-**SOC** operates

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 really 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 – WHERE DOES ALWAYS-ON PENETESTING SUPPORT?

- 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

Thank You For Your Attention!

https://into.bio/chrisdale

Twitter – https://twitter.com/ChrisADale

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

Stopping Threat Actors – https://riversecurity.eu

WE'RE HIRING!