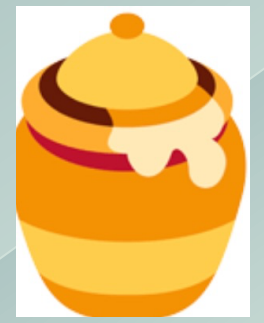
2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات

Using Free & Open Source Deception Technologies and Tools to Monitor and Protect Your Enterprise

Abdulrahman Al-Nimari, Cyber Security Advisor / Architect



Open Source and Free Deception Technologies

2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات

- ✓ Who am I ?
  - ✓ Abdulrahman Al-Nimari
  - ✓ Cyber Security Advisor, Architect, Consultant
  - ✓ 25 Years IT & Cyber Security Experience
  - ✓ Speaker : BSides, HITB, ICSC, ICAO, Arab Security Conference
  - ✓ CISSP, CISM, CCISO, PMP, GCIH, GCIA, GCUX, GREM, GSEC
  - ✓ @nimari
  - ✓ https://www.linkedin.com/in/alnimari/
  - ✓ alnimari@gmail.com
  - ✓ +966 (566) 465270

Open Source and Free Deception Technologies

2019 Arab Security Conference المؤتمر العربي لأمن المعلومات

- ✓ Agenda
  - ✓ What is Deception ?
  - ✓ Deception History
  - ✓ Why do we use deception ?
  - ✓ Deception Types
  - ✓ Cyber Kill Chain Mapping
  - ✓ Deception Implementation Best Practices
  - ✓ Sample Decoys/Breadcrumbs
  - ✓ Demo
  - ✓ Q & A
  - ✓ Resources

What is Deception ?

"The act of causing someone to accept as true or valid what is false or invalid"

Webster Dictionary

"Deception technology automates the creation of traps (decoys) and/or lures which are mixed among and within existing IT resources to provide a layer of protection to stop attackers that have penetrated the network. Traps (decoys) are IT assets that either use real licensed operating system software, or are emulations of these devices"

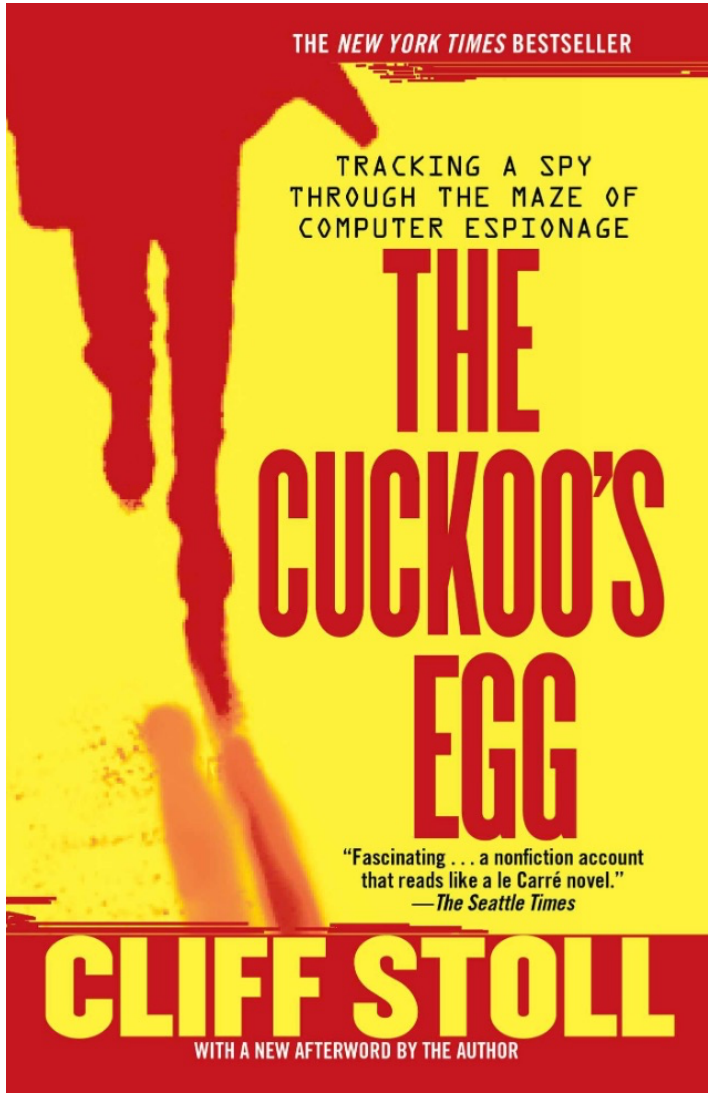
Wikipedia

Open Source and Free Deception Technologies

2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات

Telling the story of tracking a spy in 1980s :

- ✓ Stoll set up an elaborate hoax
  - ✓ Fictitious department
  - ✓ Imaginary secretary
  - ✓ Attractive files



Open Source and Free Deception Technologies

2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات

Deception in history :

"All Warfare is based on Deception. Hence when able to attack, we must seem unable; when using our force, we must seem inactive..."

Sun Tzu, Art of War, 545 BC

Verizon Data Breach Investigation Report, 2019

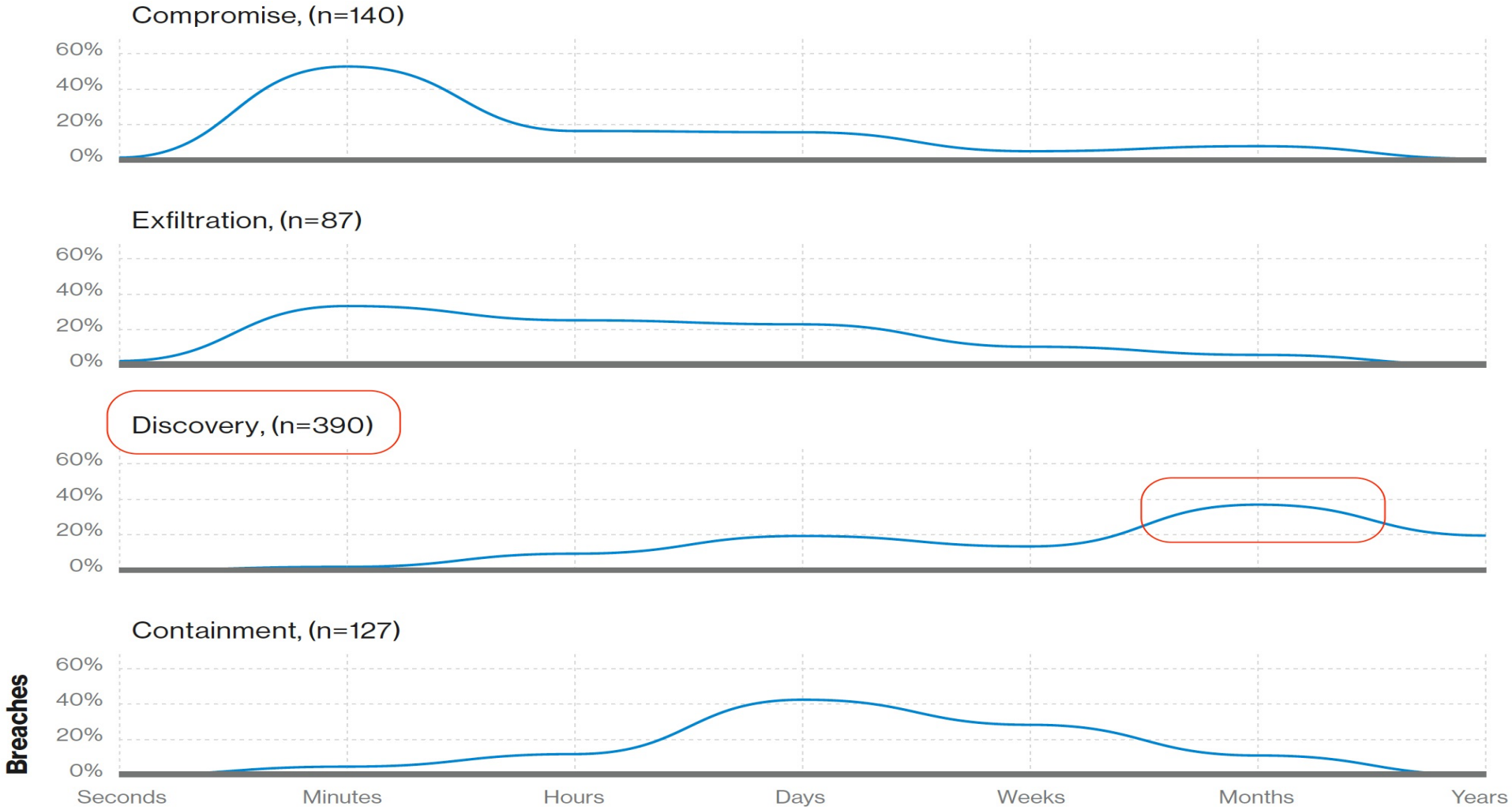
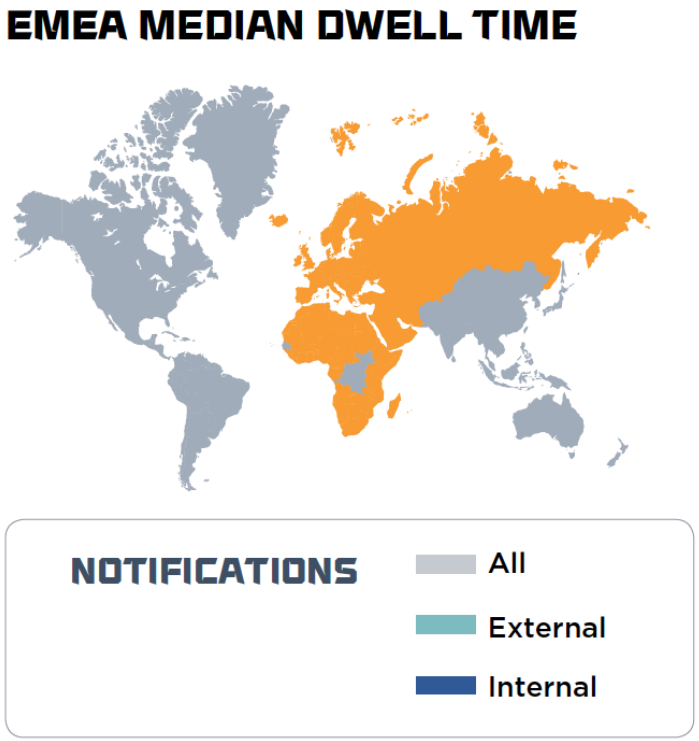
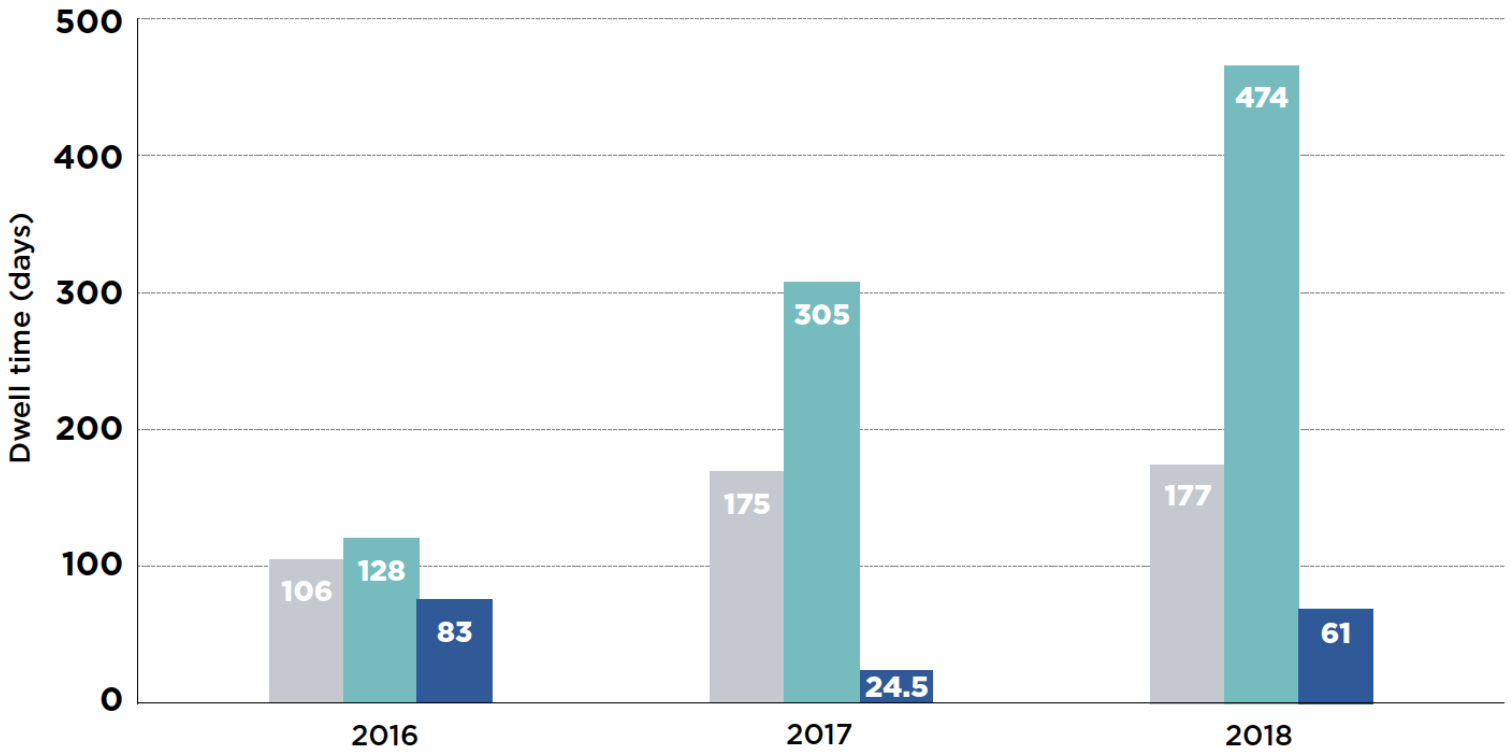


Figure 28. Breach timelines

FIREEYE M-Trends Report, 2019





Open Source and Free Deception Technologies

2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات

Why use deception :

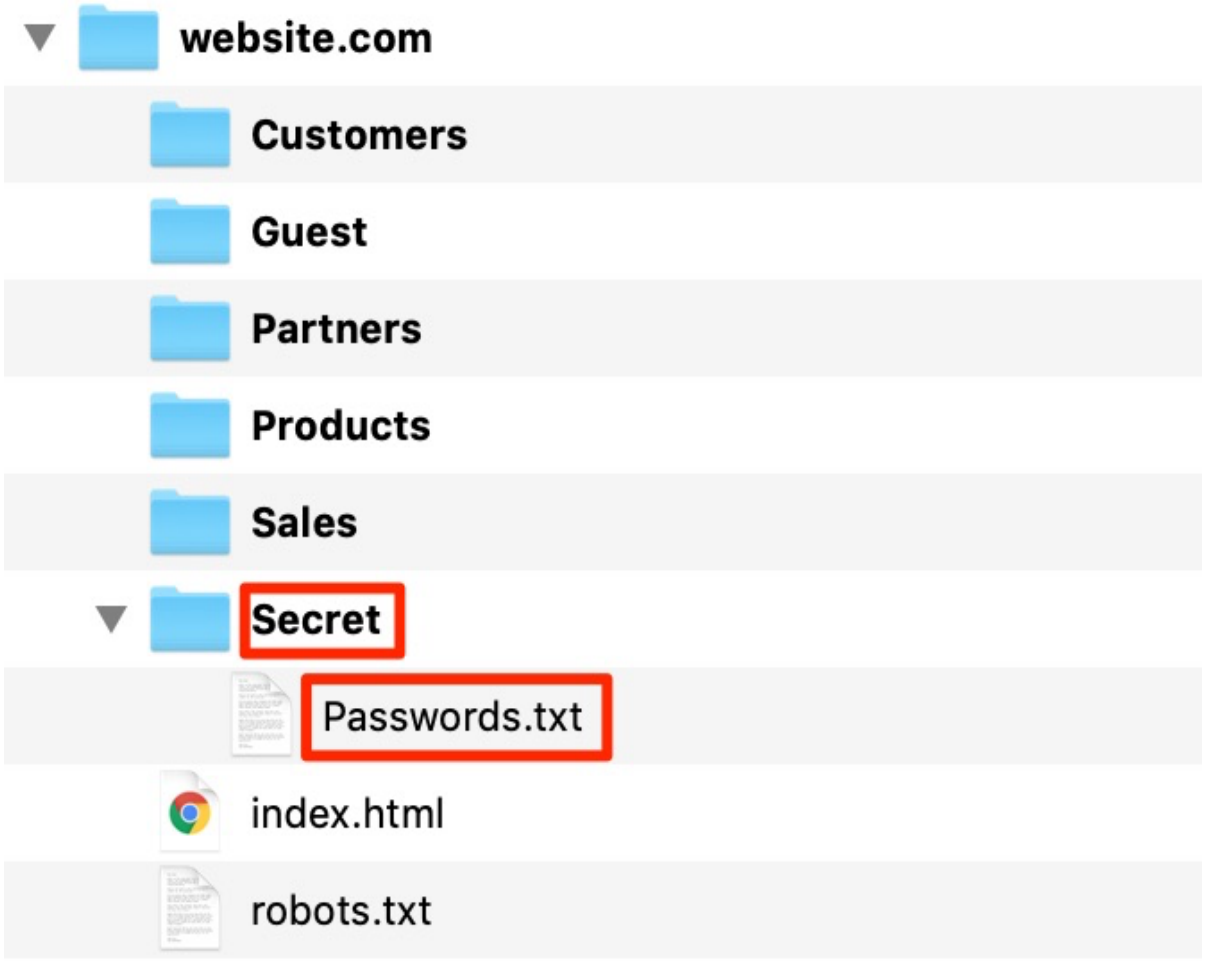
- ✓ To improve detection capabilities
- ✓ Dwell Time : Improving MTTD, MTTR
- ✓ Alerts Flood
- ✓ Too Many False Positives
- ✓ Learn Adversaries TTP
- ✓ Delay and Mislead Attackers
- ✓ Detect Zero Days & APTs
- ✓ Building Basic Threat Intel
- ✓ Detect malicious servers (using client honeypots)

Open Source and Free Deception Technologies

2019 Arab Security Conference المؤتمر العربي لأمن المعلومات

- ✓ Deception Types :
  - ✓ Decoys vs Breadcrumbs
    - Real Assets | Shares, Accounts
  - ✓ Low Interaction vs High Interaction
    - Emulated Services | Real VM/Hosts
  - ✓ Static vs Dynamic Deceptions
    - Easy to avoid | hard to identify
  - ✓ Internal vs External
    - inside Enterprise | in the DMZ, lots of alerts
  - ✓ Server vs Client
    - Dejavu | Thug (Detect drive by downloads)

Breadcrumbs – 1 (Attractive files in a folder in a website)

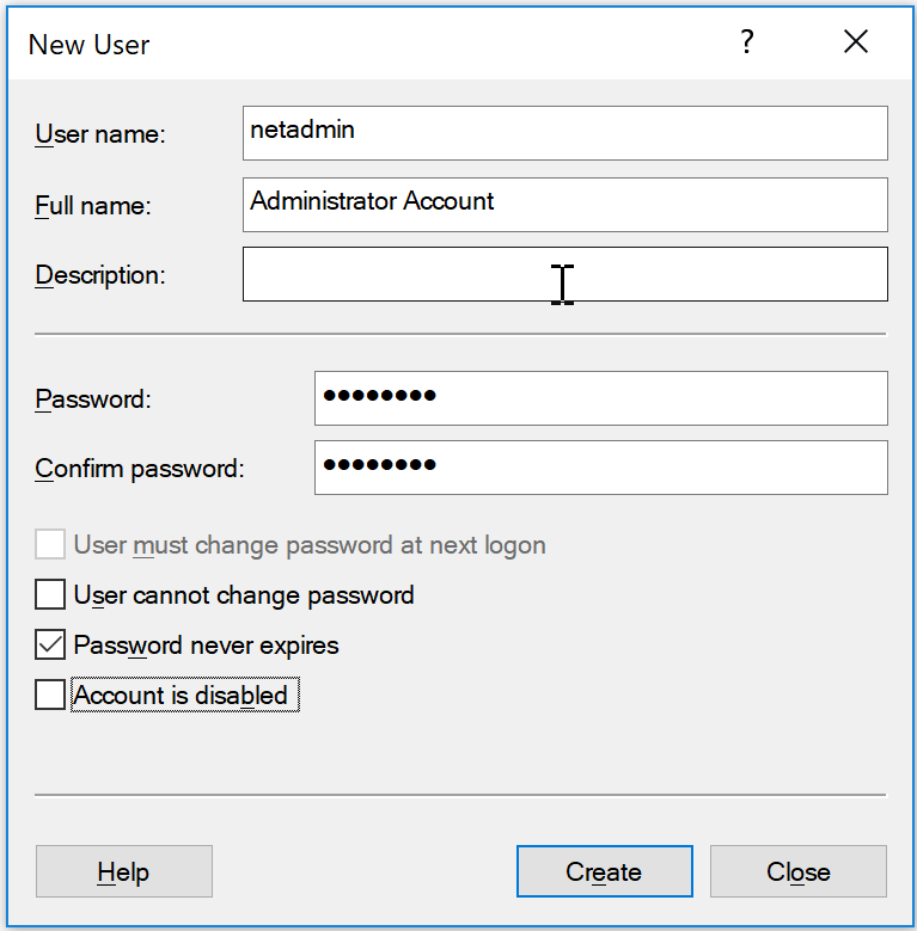


http://www.website.com/robots.txt

User-agent: *
Disallow : /Secret/

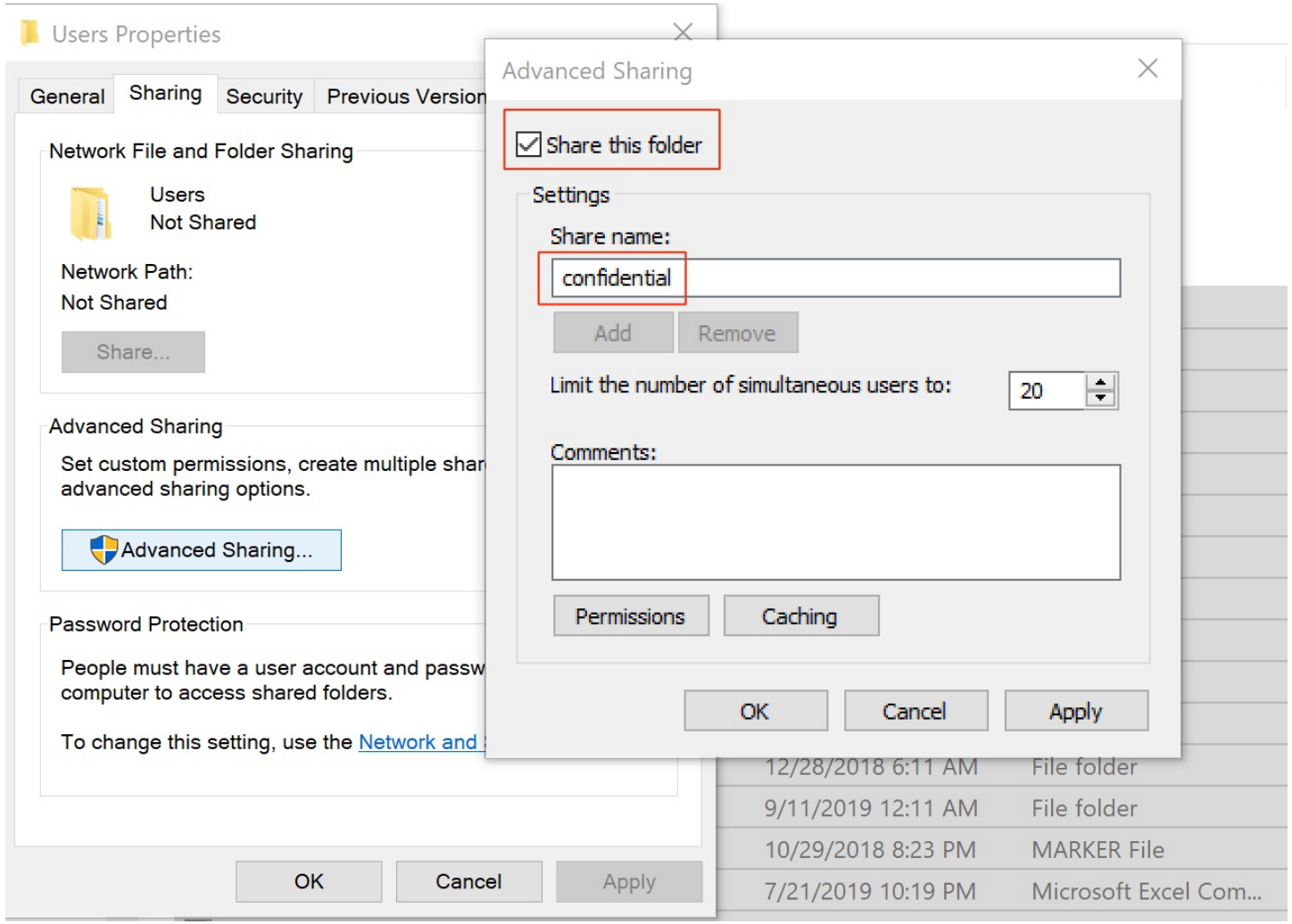
Log and Alert on access

Breadcrumbs – 2 (A user on windows AD)



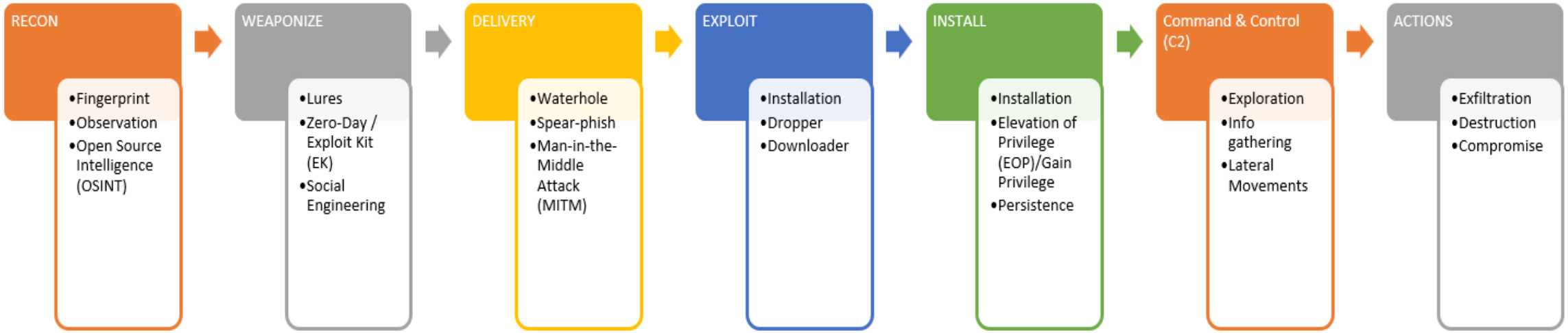
Use windows GPO to enable logging of appropriate events (Logon ..)

Breadcrumbs – 3 (a shared folder)



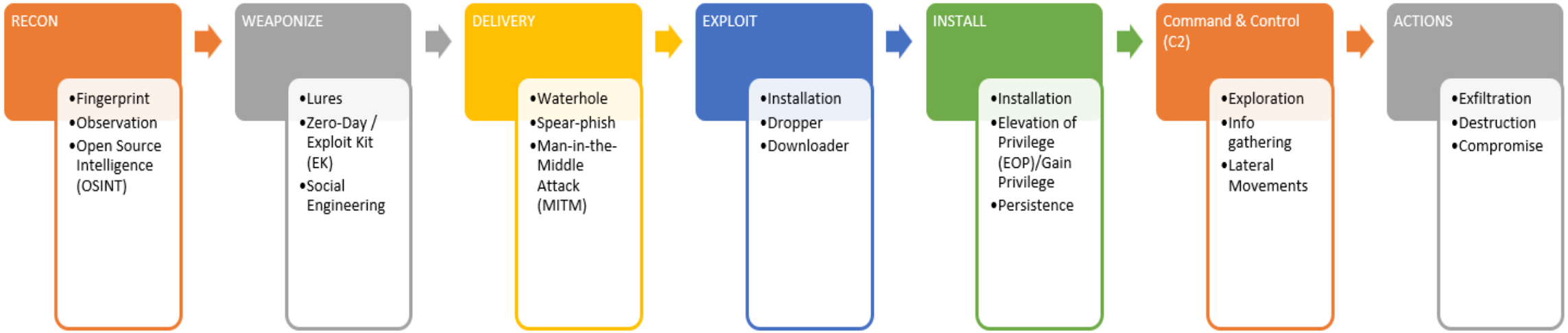
Use windows GPO to enable auditing access to the folder

Cyber Kill Chain Mapping



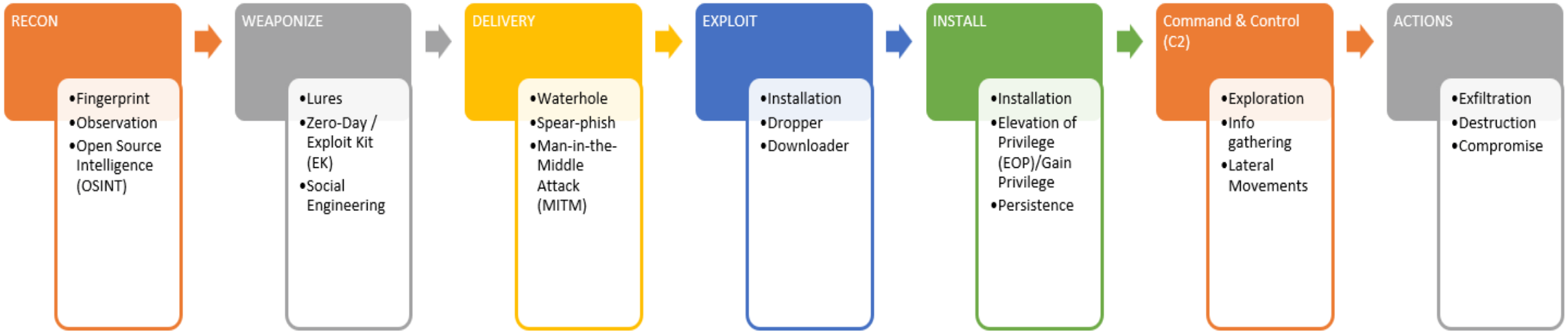
Recruitment Ads
Github Data
Meta Data
Emulated Services, IP addresses

Cyber Kill Chain Mapping



Check for Misspelled variations of he attackers registered phishing domain (comp@ny.com)

Cyber Kill Chain Mapping

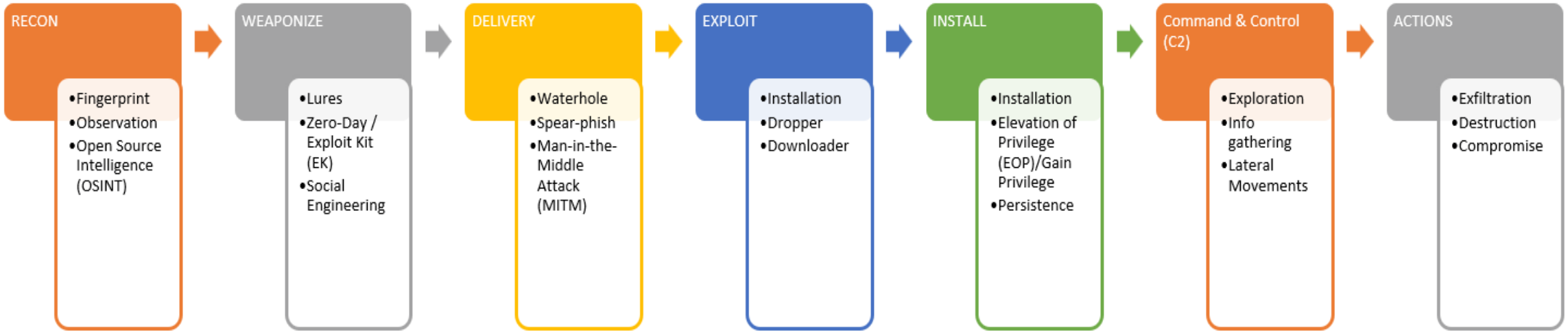


Honeypot execute code and monitor traffic.

Open Source and Free Deception Technologies

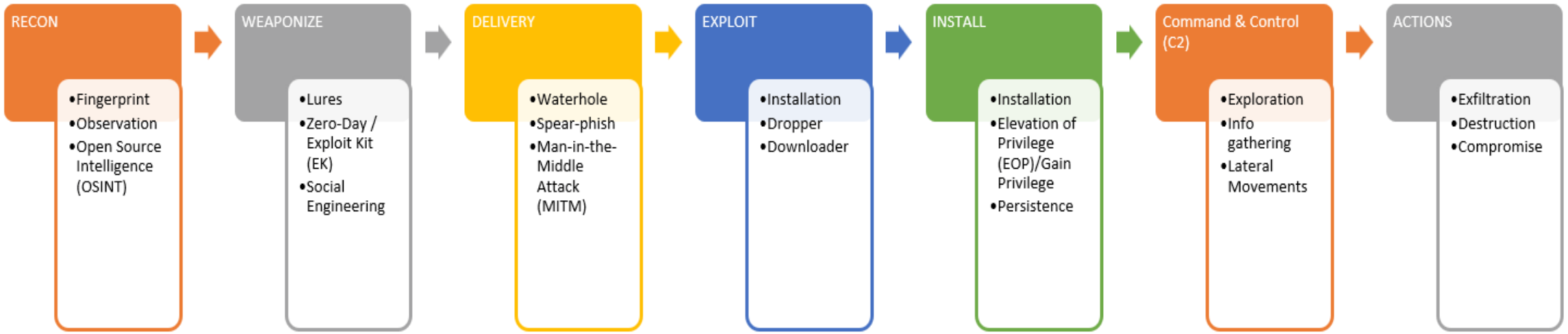
2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات

Cyber Kill Chain Mapping



Changing some system param, reg. keys : MAC address, TTL.
False success/failure error messages

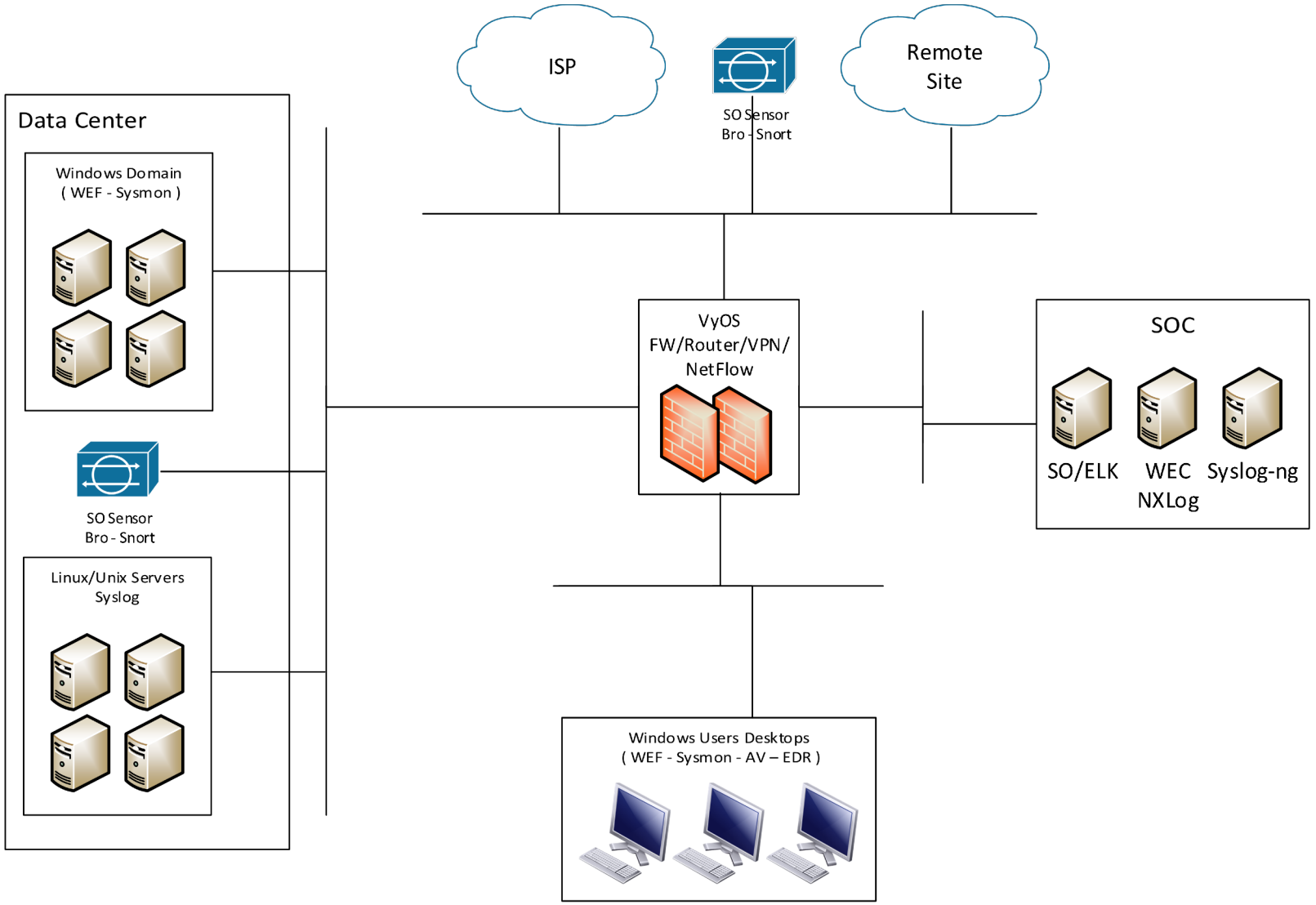
Cyber Kill Chain Mapping



Observe attacker movements and collect intelligence on TTPs

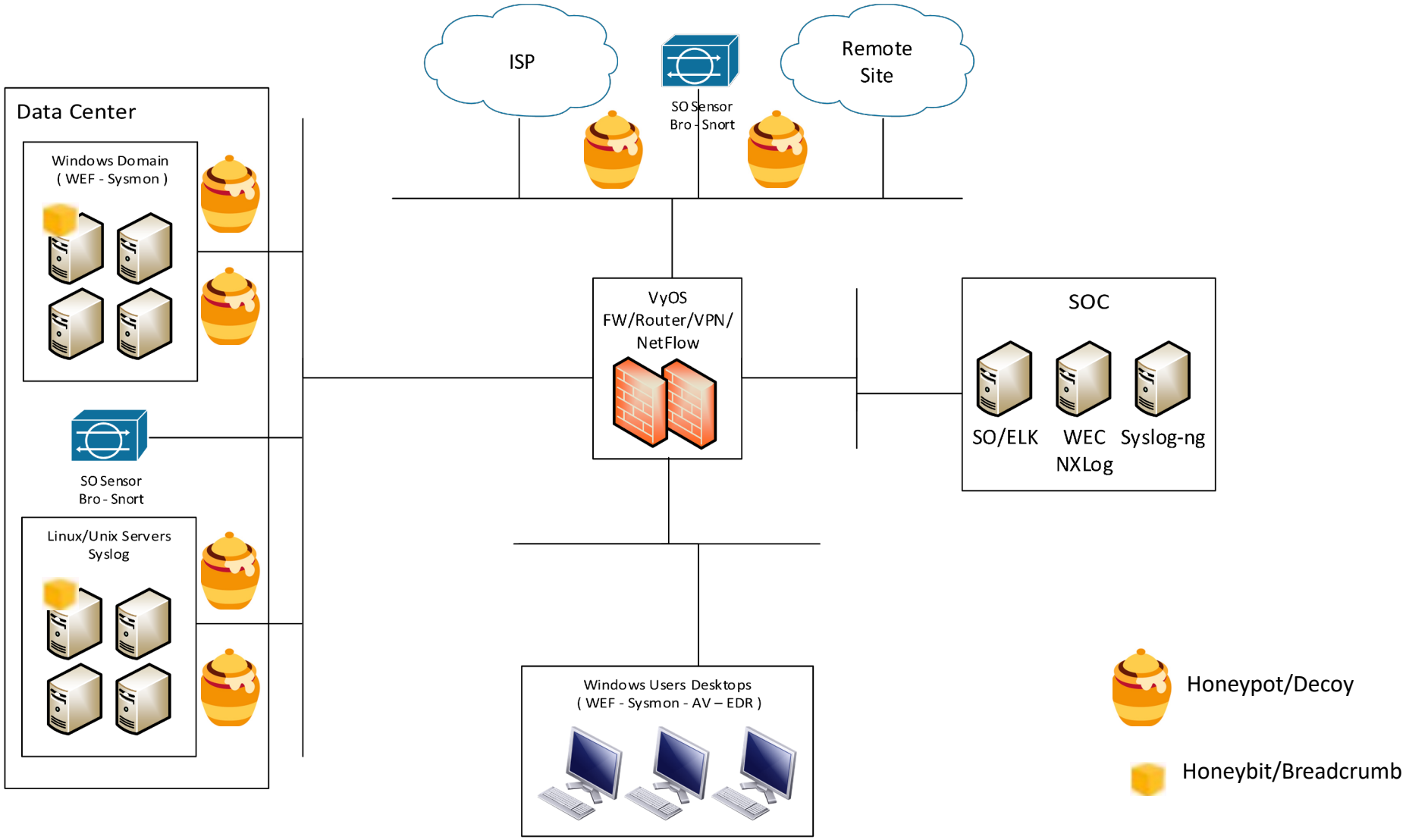
Open Source and Free Deception Technologies

2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات



Open Source and Free Deception Technologies

2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات



Open Source and Free Deception Technologies

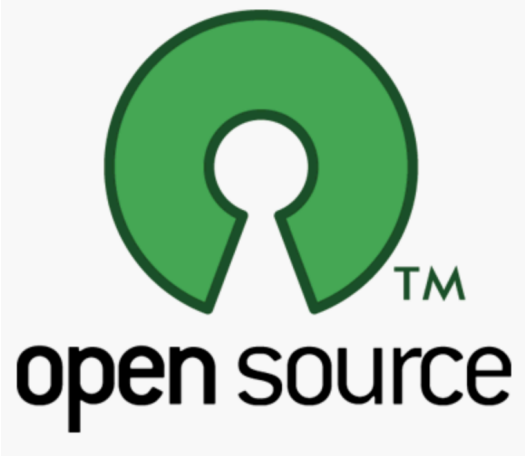
2019 Arab Security Conference المؤتمر العربي لأمن المعلومات

Deception Best Practices :

- ✓ Have visibility of your enterprise
- ✓ Have a mature security program before attempting deception
- ✓ Build objectives - Identify Devices/Services to be mimicked
- ✓ Understanding the Cyber Kill Chain
- ✓ Keep it a secret
- ✓ Make it look real
- ✓ Log, Alert and Respond

Open Source Deception Tools

- ✓ Full OS / Solution
  - ✓ ADHD (Active Defense Harbinger Distribution)
  - ✓ DejaVU
  - ✓ T-POT
- ✓ Honeypots / Honeytokens / Breadcrumbs
  - ✓ HoneyPy, low interaction, plugins, logging
  - ✓ Cowrie, SSH and Telnet honeypot, detect BF
  - ✓ Honeybits, Create Honeytokens across enterprise
- ✓ Client Honeypots
  - ✓ Thug, detect drive by downloads



Open Source and Free Deception Technologies

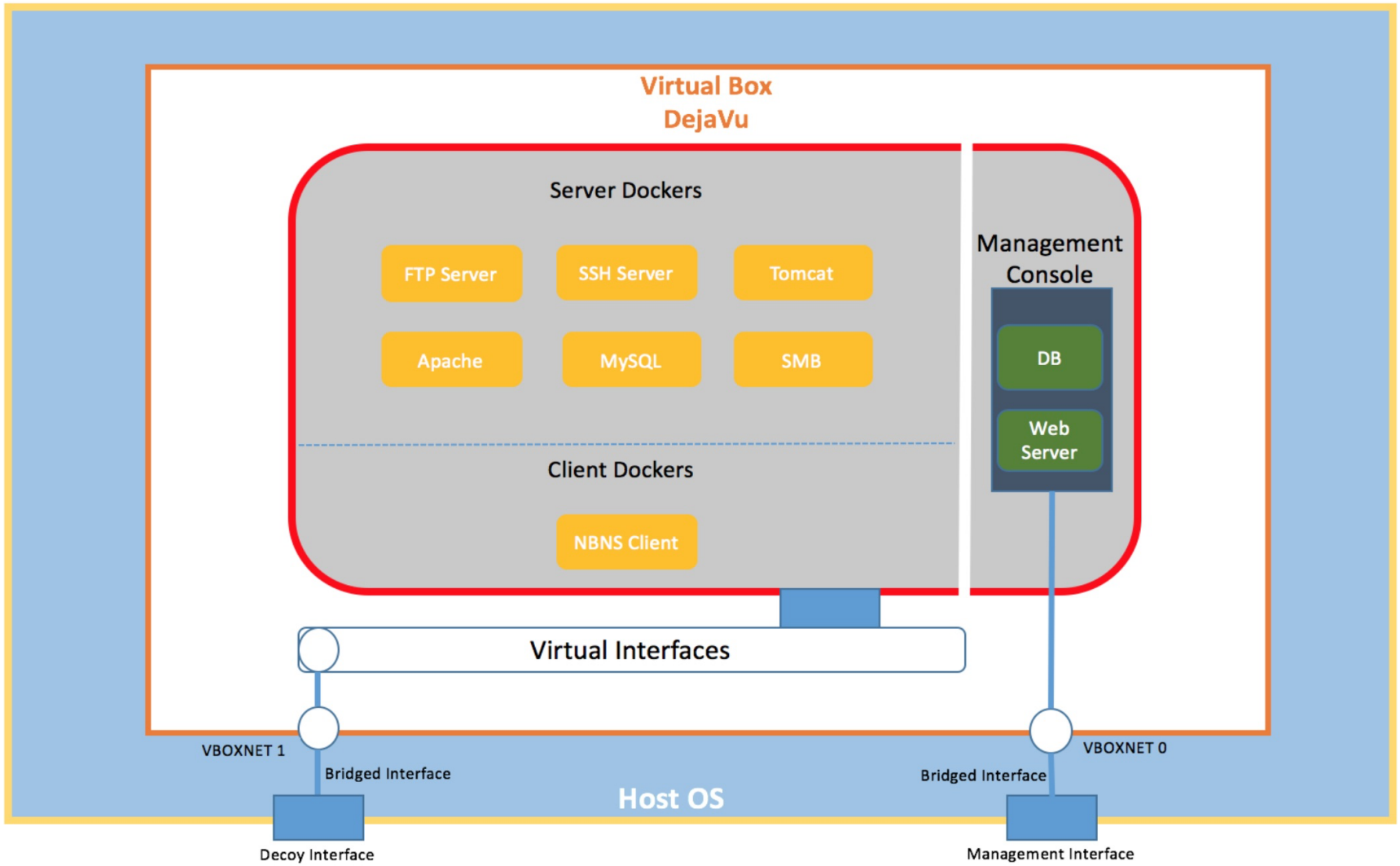
2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات

Demo

Open Source and Free Deception Technologies

2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات

DejaVU Deception Framework



https://github.com/bhdresh/Dejavu

Resources

https://en.wikipedia.org/wiki/Deception_technology
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
https://moretip.com/dejavu-open-source-deception-framework/
https://www.honeynet.org/project
https://github.com/dtag-dev-sec/tpotce
https://github.com/bhdresh/Dejavu
https://www.youtube.com/watch?v=Cf_XXmRLnRQ&index=39&list=PLLWzQe8KOh5nHbxFsxHEU3o50ykuv6gaC
https://github.com/0x4D31/honeybits
https://www.smokescreen.io/7-deadly-sins-how-to-fail-at-implementing-deception-technology/
https://www.blackhillsinfosec.com/projects/adhd/

Open Source and Free Deception Technologies

2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات

Your Q & A

Open Source and Free Deception Technologies

2019
Arab Security Conference
المؤتمر العربي لأمن المعلومات

Thank You