ENGAGE YOUR ENEMY

The case for attacking the attacker

Sebastian Garcia

Stratosphere Laboratory. Czech Technical University in Prague

https://www.stratosphereips.org/

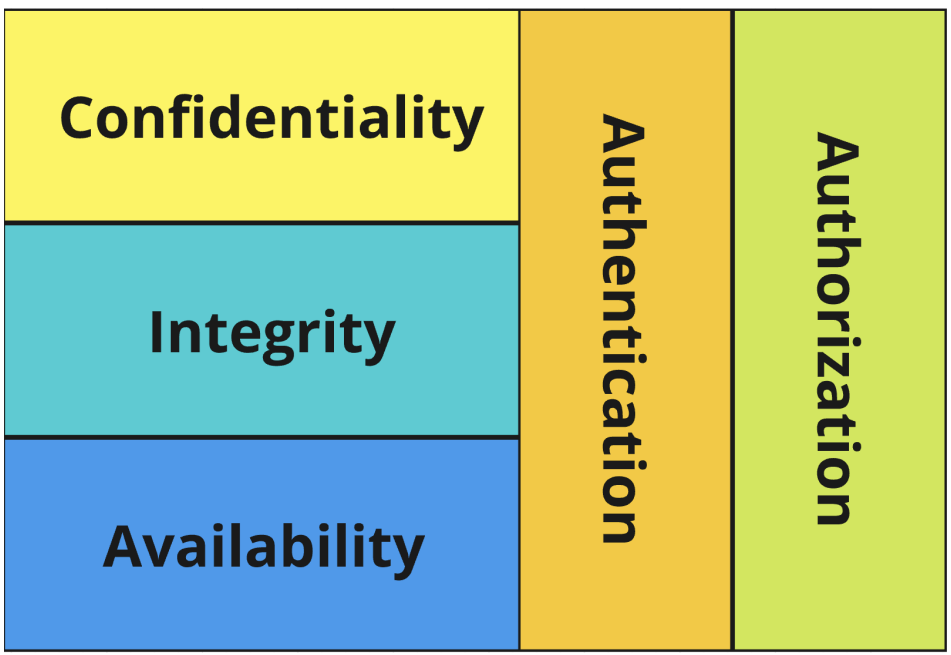
AD&D Workshop, Euro S&P, 2024

Active Defense and Deception

Active **Defense** and Deception

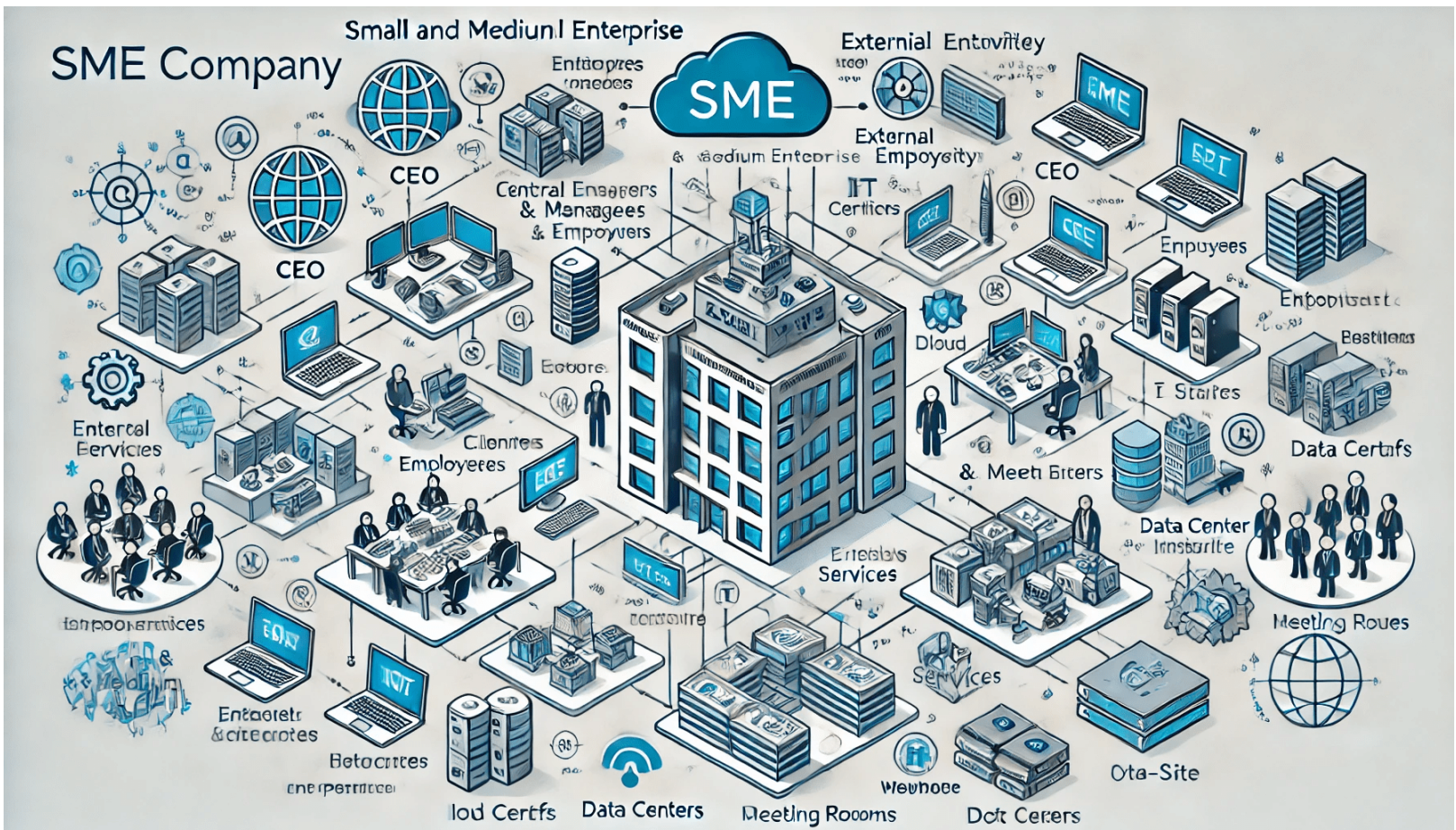
Defense

> *A multidisiplinary approach to protect your assets, values, resources, and business.*

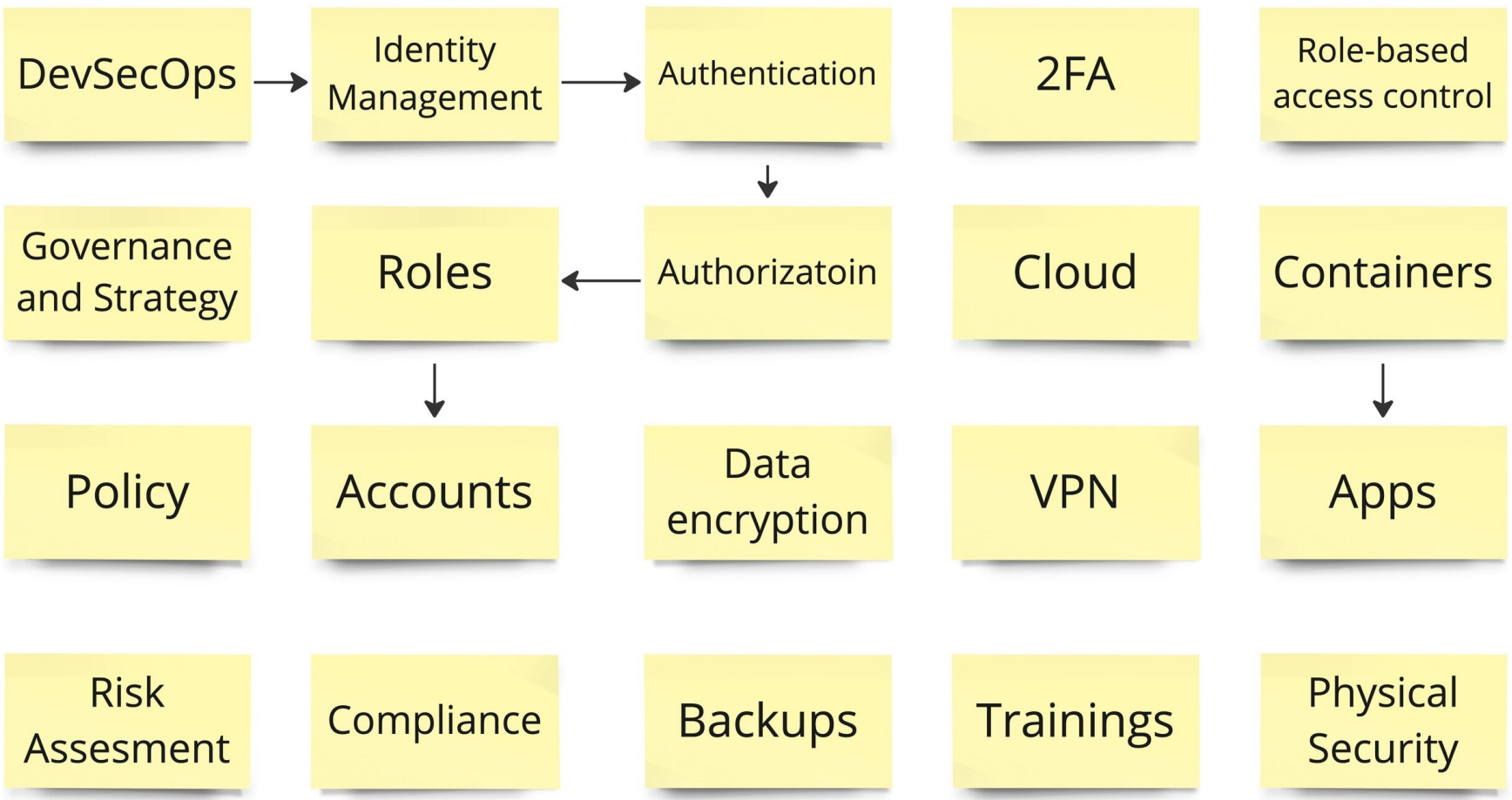


Defense

> *A multidisiplinary approach to protect your assets, values, resources, and business.*

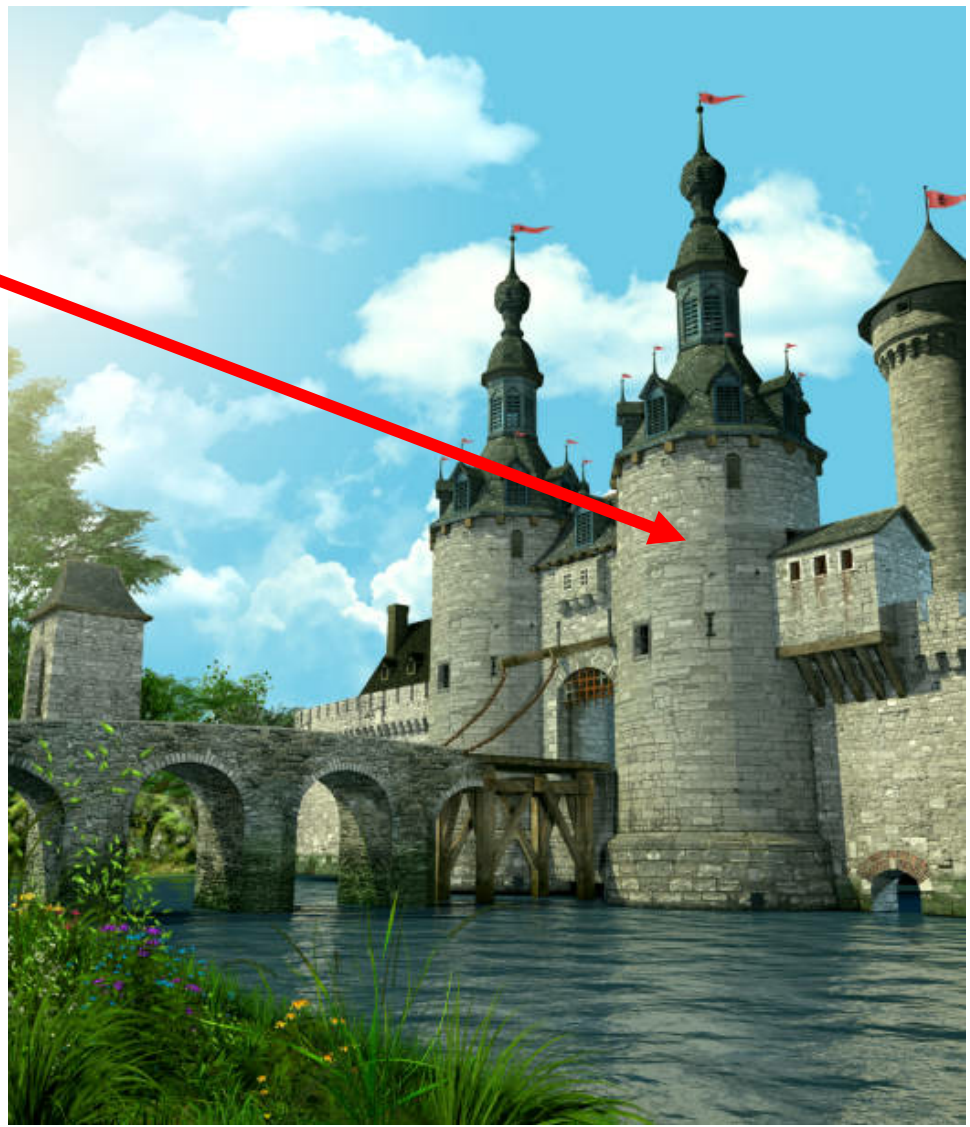


Cybersec Architecture: Passive



Cybersec Architecture: Passive

Arch Passive Defense



Cybersec Operation: Passive

Firewalls

TI

IDS

API security

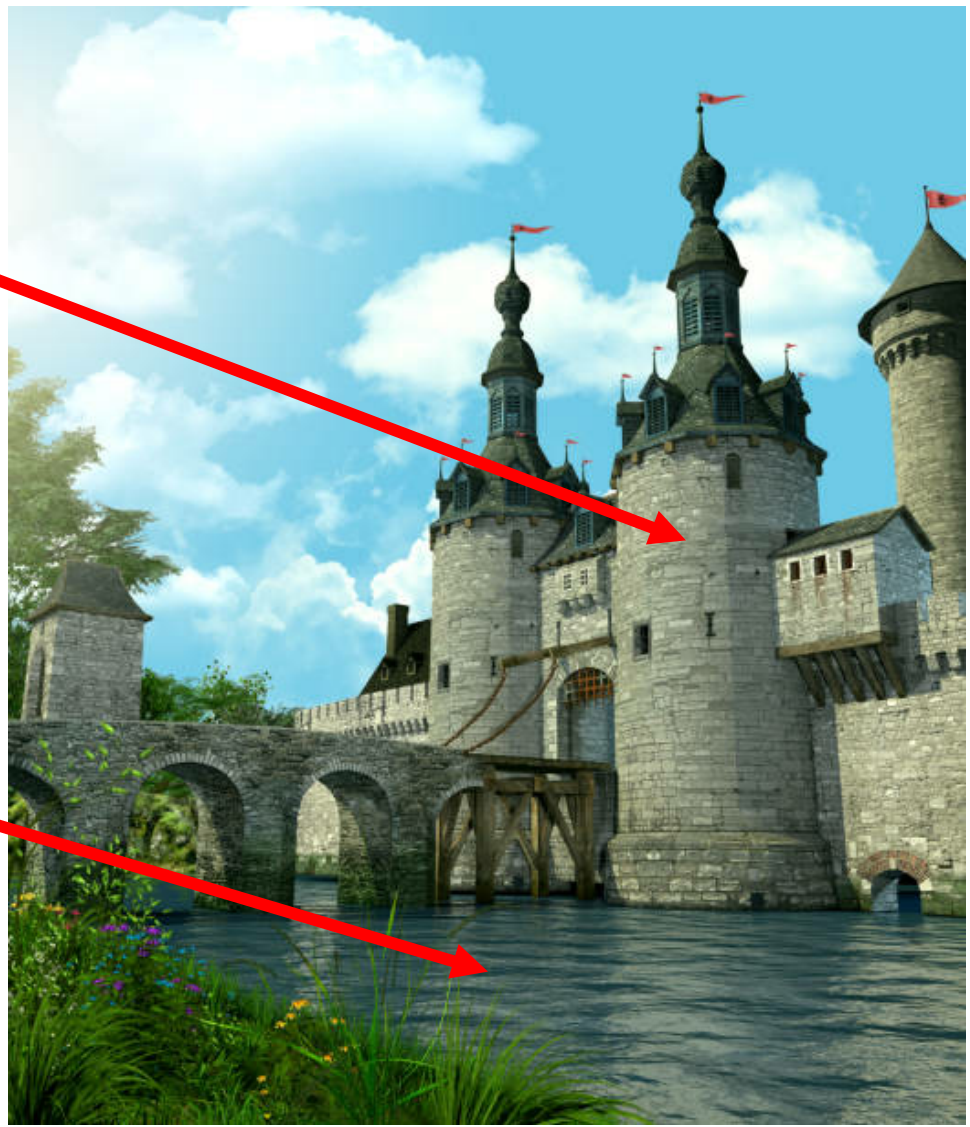
Updates

Phising simulation

SIEM

Passive Defense

Arch Passive Defense



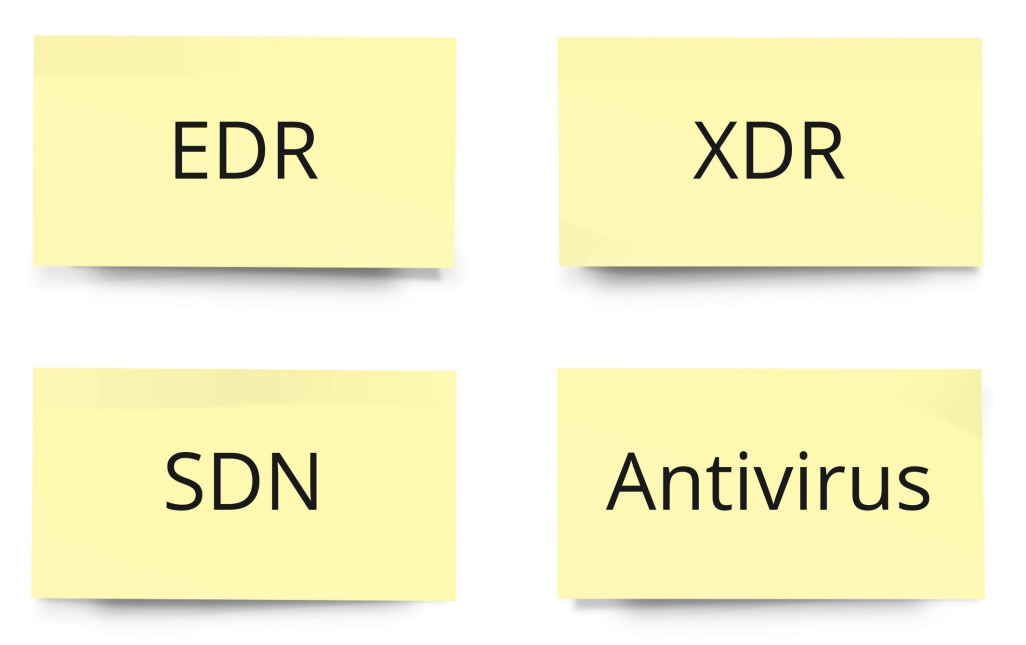
Oper Passive Defense

Active Defense and Deception

Active Defense

> *Proactive approach to protecting information systems and networks from threats. It involves taking dynamic and often aggressive measures to detect, analyze, and mitigate cyber attacks in real-time*

Active Defense



Active Defense

Active Defense

Change (a binary decision)

- A product demands to block an IP in a FW.
- SIEM blocks an account in AD.
- SIEM logouts an account in a computer.
- SIEM terminates Cloud sessions
- EDR/XDR kills a process.
- Proxy blocks URL
- Fail2ban blocks in local FW after bruteforce

Active Defense

Adapt (degrees of change. Predefined)

- Change the network bandwidth for a host.
- Change the API bandwidth access.

Active Defense

Learn (degrees of change. Learned)

- ML (AD, Classifiers)
  - Learn from FP.
  - Learn risk levels.
  - Learn seasonality.
- Human-in-the-loop. "Assisted"
  - Playbooks are here.

Active Defense

Share

- Sharing IoC
  - Slips IDS local P2P TI sharing [1].
  - Local IPs too.
  - Trust based, adversary-resilient.

[1] Garcia, S., Gomaa, A., & Babayeva, K. Slips, behavioral machine learning-based Python IPS

https://github.com/stratosphereips/StratosphereLinuxIPS

Active Defense

Engage

Why Active Defense?

Change

- Stops the attack, so it works.

Adapt

- A proportionate response may reduce false positives.

Learn

- A proportionate response may reduce **more** false positives.

Share

- It may stop attackers faster. They are *local* IoC.

Not Moving Target Defense?

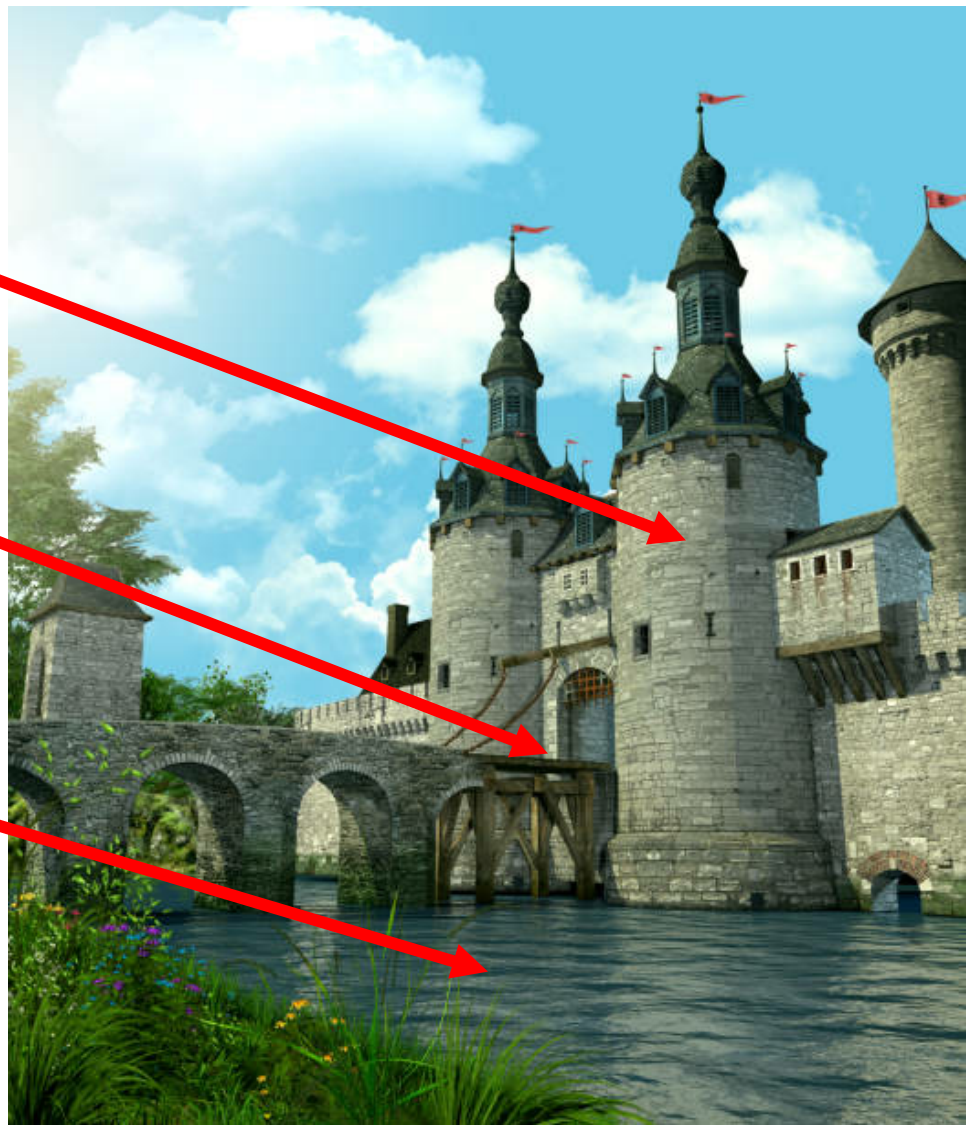
- Move the assets to confuse attackers and make them lose track of IPs, resources, etc.
  - If legit users can find the correct server, attackers also can.
  - Legitimate users/process also get lost.
- If a honeypot is found, better to move it for the next attack.
  - Production servers can not 'disappear', so the attacker knows.
- I personally don't believe it works.

Active Defense

Arch Passive Defense

Active Defense

Oper Passive Defense



Active Defense and **Deception**

Deception

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

Merrian-Webster Dictionary. Link

> *Deliberate measures to **induce** erroneous sensemaking and subsequent behaviour within a bio-digital target set, to achieve and exploit an advantage.*

National Cyber Deception Laboratory. Link

Deception

The 23rd Headquarters Special Troops. Nicknamed “the Ghost Army.”

Members of the visual deception unit. Courtesy of Jack Masey. Link. Book

Deception

- The Ghost Army impersonated larger and more costly units.
- Copied insignias in uniforms and cars, specific officers, morse code operators typing profiles, tracks in the soil, recorded sound of larger groups, and, of course, inflatable tanks.
- The own Army believed they were real.

CyberDeception is Different

Lessons from 'kinetic' deception are nice but hard to translate. They were trying to deceive an enemy about defenses being better and larger.

CyberDeception. Why?

- Early warning systems for faster blocking.
- Minimize time to detection.
- Minimize false positives.
- Optimize resource allocation.
- Reduce cost of defense!
- Profile attackers? almost nobody does.
- Slow attacks down?
- Difficult attack.

Deception

And, do **not** to make organizations more insecure

Psychological Deception

- Opportunity to **influence** and **change** attackers:
  - Attention, Perception, Sensemaking, Expectation, Emotion, Behavior
- If told deception may be used, attackers avoid weak systems

Deception Types

- **A-type (Ambiguity)**
  - Make the attacker unsure about **all**. Defenses, actions, preparations, data.
  - A honeypot that looks ***exactly*** as the real server.
  - Attack delays the decision waiting for 'more information'.
- **M-type (Misleading)**
  - The attractiveness of the deception is larger than the real system. The attacker is **sure** the deception is the real thing.

Daniel, D. C., & Herbig, K. L. (1982). Propositions on military deception. *Journal of Strategic Studies*.

Deception Types

- **Probability honeypot**
  - Add many deception techniques so the probability of interacting with one is larger.
  - Not so much deception but a *minefield*.
- **Fake honeypot**
  - If a real server looks like a honeypot, it usually is left unattacked.
    - https://github.com/NavyTitanium/Fake-Sandbox-Artifacts
    - https://www.cyberscarecrow.com/

Deception is Uncertainty

- There can be honeypots or not.
- The honeypots can be real or not.
- The attackers may be told about the honeypots or not.
- The attackers may believe what they are told or not.

Deception Engineering

- Design of Deception Engineering [1]
  - Methods, techniques, patterns, and tools to incorporate deception.
- Why you need to think in advance?
  - **Magruder's principle:** easier to convince a target into holding on to a pre-existing belief than it is to convince a target of something it does not believe.

[1] Faveri, C. D. (2021). *Modeling Deception for Cyber Security*. NOVA University.

Deception Can go Further

AD&D 2024 Paper

Kahlhofer, M., & Rass, S. (2024). *Application Layer Cyber Deception without Developer Interaction*

Deception Can go Further

What about doing **misinformation** and **propaganda**?

Tested, with the best results obtained with a combination of **informing** the attackers about deception and **using** deception.

Ferguson-Walter, K. J. (2020). *An Empirical Assessment of the Effectiveness of Deception for Cyber Defense.*

Deception Can go Further

Can we do this on the Internet?

- Fake LinkedIn profiles of people.
- Fake questions asking to fix our "FortiGate 6000F".
- Fake internal tickets about detected attackers
- Fake versions of all our servers and services.
- Fake underground forums leaked data.
- Fake announcement "We have been hit by ransomware".

But deception is not enough

- **Limited** scope. After all, they may still be inside.
- Deception can **fail**. There are no measurements.
- Integration may **not** work. Not all blocks are effective.

Can we have...

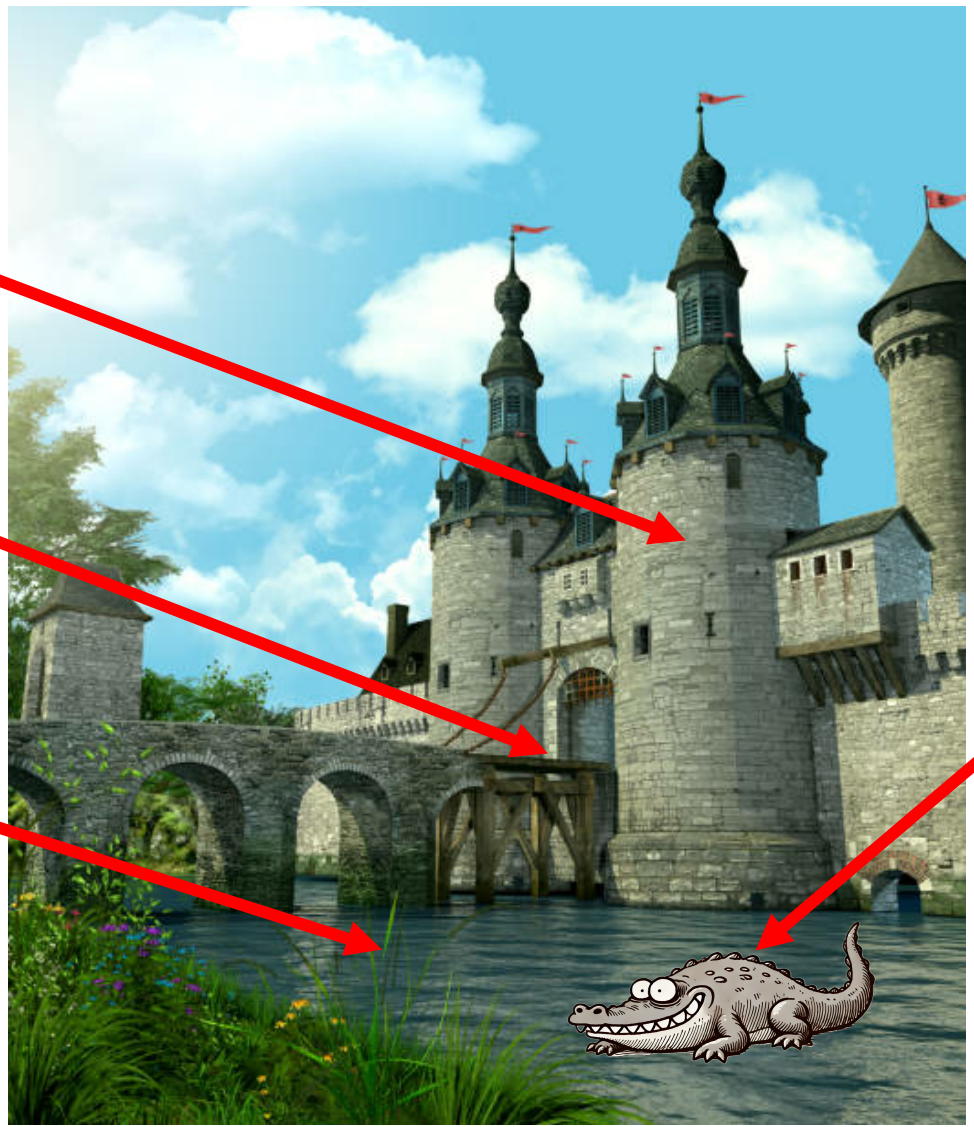
- Enhanced Threat Intelligence.
- Measure response capabilities.
- Profile the proficiency of the attacker.
- Faster resolution of FP. AKA 'the phone test.'
- Better misdirect their attention.

Active Defense and Deception and **Engaging**

Engaging

> *To have contact and actively disrupt the operation of your attacker.*

Engaging



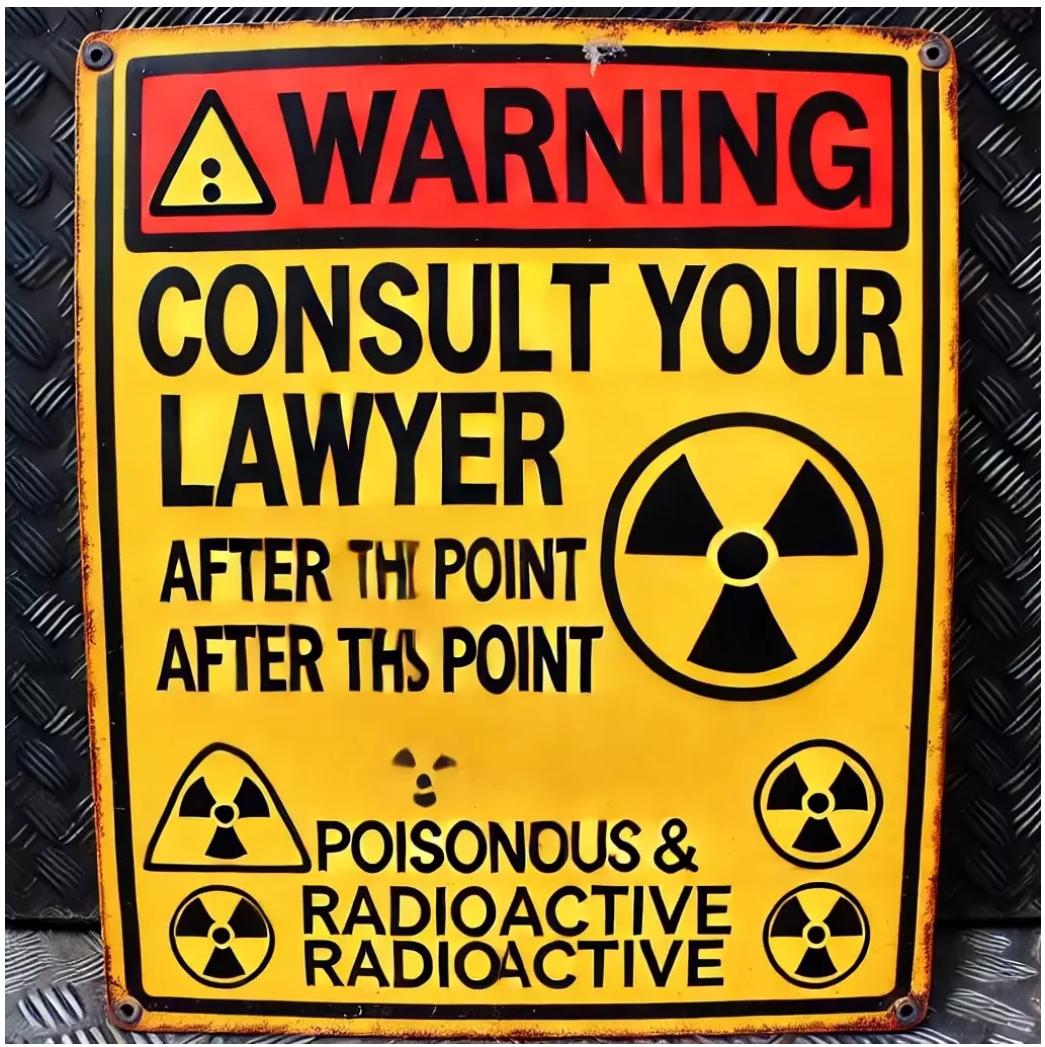
Arch Passive Defense

Active Defense

Oper Passive Defense

Engaging

Engaging


WARNING
CONSULT YOUR
LAWYER
AFTER THI POINT
AFTER THIS POINT
POISONOUS &
RADIOACTIVE
RADIOACTIVE

Engaging. Not new.

- Engaging has been happening for a long time
  - 2005 Book "Aggressive Network Self-defense". Link
  - 2013 Conversation "The Ethics of Hacking Back: Cybersecurity and Active Network Defense". Link.
  - 2013 Book "Offensive Countermeasures. The art of active defense" John Strand/Paul Asadoorian. Link
  - 2015 News "Should Companies Strike Back at Hackers?". Tripwire. Link

The Rise of Engaging

2019. US **Active Cyber Defense Certainty Act (ACDC)**

The Rise of Engaging

2019. US **Active Cyber Defense Certainty Act (ACDC)**

- Aimed to **allow** companies to engage in "**active** cyber defense measures" to trace and stop cyber attackers:
  - Only qualified defenders with a high confidence in the attacker's **identity** can engage.
  - Companies **must** inform the FBI
  - **Allowed to** identify attackers, disrupt attacks, and monitor attackers
  - **Prohibited** to destroy data or cause significant harm to others.

Luckily, **never** approved. Link

The Rise of Engaging

2019. **National Cyber Deception Laboratory**, UK

*"(...) a new government-backed national laboratory for cyber deception that aims to actively **"take the fight to network attackers"** rather than rely on passive measures to block incoming digital offensives."*

Link

It was 'mysteriously' left to expire... Sure.

The Rise of Engaging

- **Engage MITRE. 2022.** https://engage.mitre.org/
  - *"assist defenders in understanding the intricacies of adversary engagement strategies and technologies."*

Wait… global adversaries?

MITRE | Engage™

WHAT IS ADVERSARY ENGAGEMENT?

Adversary engagement is the combination of denial and deception to increase the cost and decrease the value of your adversary's cyber operations. Adversary engagement goals can be any combination of the following: to detect adversaries on the network, to elicit intelligence to learn about adversaries, or to affect adversaries by raising the cost and lowering the value of their cyber operations.

OVERVIEW

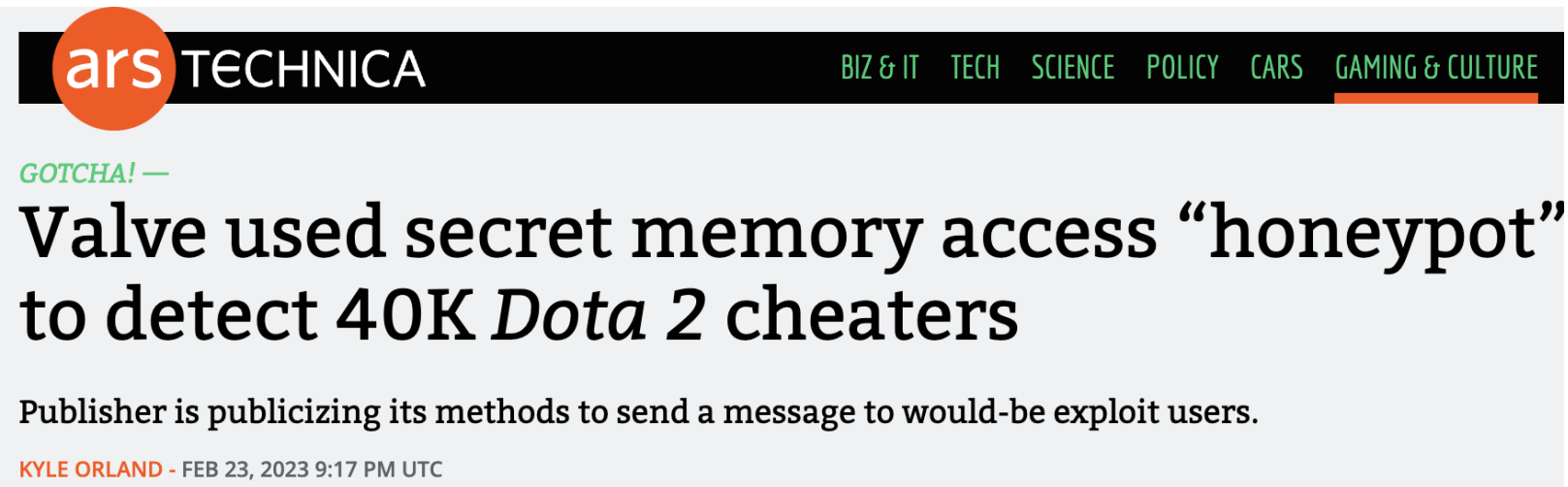
Cyber defense has traditionally focused on the use of defense-in-depth technologies to deny an adversary access to an organization's networks or cyber assets. In this paradigm, any time the adversary can exploit a network vulnerability to access a new system or exfiltrate a piece of data from the network, they win. However, when a defender introduces deceptive artifacts and systems, they increase the ambiguity for the adversary. Is the system they just accessed legitimate? Is the piece of data they just stole real? These questions drive up the cost and drive down the value of the adversary's cyber operations.

Adversary Engagement is a combination of cyber denial and deception activities to interact with cyber adversaries to achieve the defender's goals. When paired with defense-in-depth technologies, adversary engagement allows defenders to proactively interact with cyber adversaries to achieve the defender's strategic goals.

"Adversary Engagement operations provide opportunities for defenders to demonstrate tools, test hypotheses, and improve their threat models, all with the added benefit of negatively impacting the adversary."

Gabby Raymond, Adversary Engagement Capability Area Lead, MITRE

Engaging Cases



Link

Engaging Cases

South Korean telecom company attacks customers with malware — over 600,000 torrent users report missing files, strange folders, and disabled PCs

News By Jowi Morales published 26 June 2024

Link

Engaging Tools

- Fake exploits to surveil attackers. Link.
- Beef. Exploit browsers. Link
- Tarpit style
  - The infinite webpage. Consume browser mem. Link.
  - PHP-Tarpit. Redirection and content. Link
  - LaBrea. TCP tarpit. Link.
  - Endlessh. TCP tarpit. Link.

Engaging Tools

- Rubberglue. Mirror trafick back to attacker. Link.
- WebLabyrinth. Bogus web-page links. Link.
- Fing blocks new WiFi clients. ARP poisoning. Link.
- SET. Attack web clients. Link.
- HoneyBadger. Attack web clients to get their IP.
  - Exploits + honeytokens + search your local images + iTunes backup. Link. Link. Video

Engaging. Locally

- Local attackers are inside your network.
- **Your** network.
- Legal differences.
- Many more options.
- Much more control.
- Much more risk.
- Much more need.

Engaging Ideas

- ARP poisoning. Multiple sources.
- Terminal injection

- Copy data changing
- WiFi logout of attacking devices
- DoS the computer. Give **more** bandwidth!

Engaging Ideas

- DNS Spoofing. Change the IP of the domains
- Block MAC address in network/WiFi/DHCP

Engaging Ideas

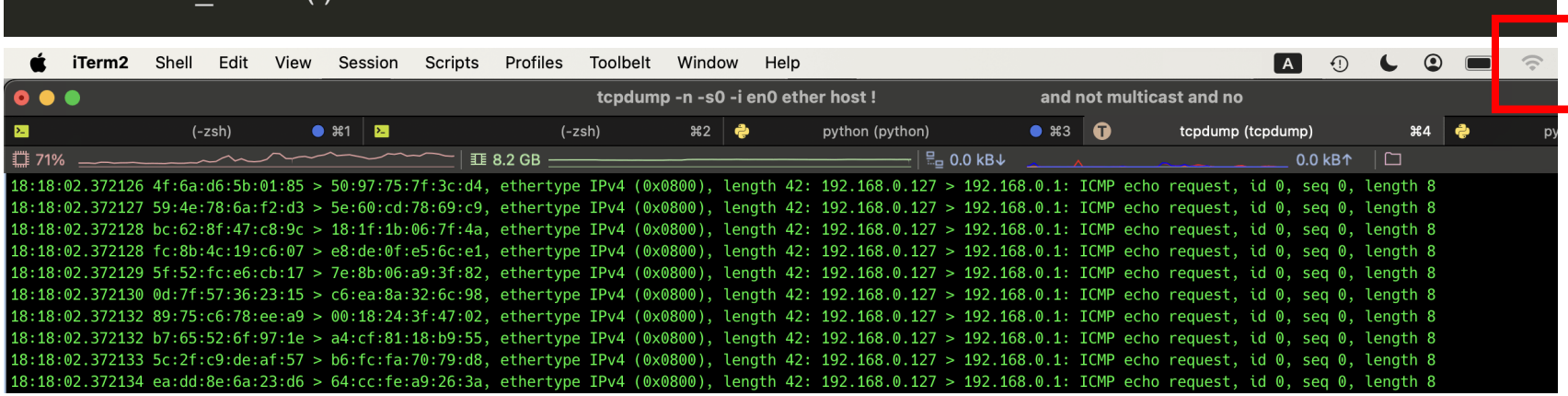
- MAC Spoofing DoS

```python
from scapy.all import *

# Define the network interface
interface = "eth0"

# Generate and send packets with random MAC addresses
def mac_flood():
    while True:
        pkt = Ether(src=RandMAC(), dst=RandMAC()) / IP(dst="192.168.1.1") / ICMP()
        sendp(pkt, iface=interface, verbose=False)

if __name__ == "__main__":
    mac_flood()
```



Engaging Ideas

- What about scanning the ports of all new computers appearing in the network?

```
import os, json, logging
from scapy.all import sniff, ARP
import subprocess
logging.basicConfig(filename='network_scan.log', level=logging.INFO,
                    format='%(asctime)s - %(message)s')
KNOWN_COMPUTERS_FILE = 'known_computers.json'
if os.path.exists(KNOWN_COMPUTERS_FILE):
    with open(KNOWN_COMPUTERS_FILE, 'r') as f:
        known_computers = json.load(f)
else:
    known_computers = {}
def save_known_computers():
    with open(KNOWN_COMPUTERS_FILE, 'w') as f:
        json.dump(known_computers, f)
def scan_host(ip):
    logging.info(f"Scanning new host: {ip}")
    result = subprocess.run(["nmap", "-p-", ip], capture_output=True,
text=True)
    logging.info(result.stdout)
def process_arp_packet(packet):
    if packet.haslayer(ARP) and packet[ARP].op in (1, 2):
        mac, ip = packet[ARP].hwsrc, packet[ARP].psrc
        if mac not in known_computers:
            known_computers[mac] = ip
            scan_host(ip)
            save_known_computers()
print("Starting ARP packet sniffing...")
sniff(filter="arp", prn=process_arp_packet, store=0)
```

Conclusion

Engaging attackers in your local network can give an **advantage** to your **protection** by keeping the attackers **busy**, forcing their **mistakes**, and leaving more **traces** behind.

But we need you to advance and help understand how deception works.

We need to find the limits of technical active defense and psychological cyberdeception to better engage attackers.


HONEY
HONEY
HONEY
WE NEED YOU
TO IMPROVE
HONEYPOTS

Thanks!

Sebastian Garcia

https://www.stratosphereips.org/

https://infosec.exchange/deck/@eldraco

@eldraco

https://www.linkedin.com/in/sebagarcia/