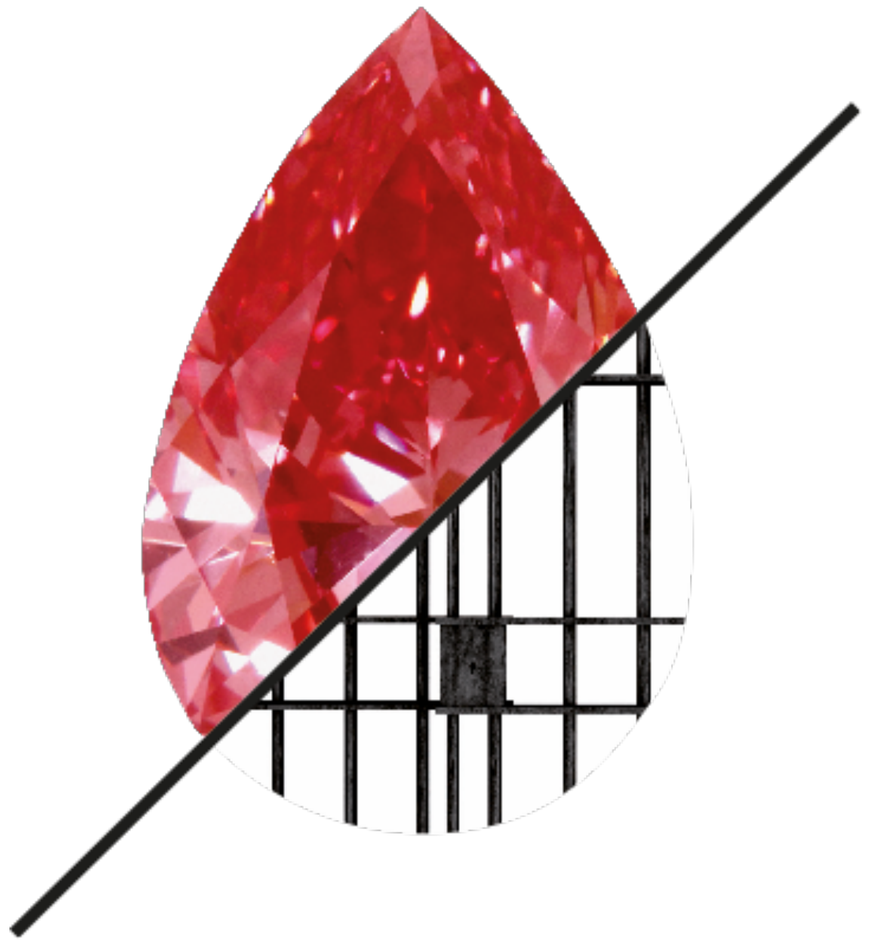
Counter Craft

Active Defence with Attack Trees & Deception



www.countercraft.eu

Active Defence & Deception

Our objectives are

1. Make the **attack** more **difficult**, from the point of view of the attacker
2. Take advantage of their **momentum**

Our objectives are

3. **Obtain** as much **information** as possible from our attacker
4. **Alert** early attack stages

The big issues

P1

Coverage

How do you ensure that attackers reach your honeypot?

Deep vs. Shallow
Internal vs. External
Breadcrumbs // SDN

P2

Plausibility

How can you make your “false” network behave like the real thing?

Emulations vs. The Real Thing
Reading network DNA

P3

N+1

Your network has to show signs of life, file changes, updates. And, as adversaries return, the depth of the illusion has to increase

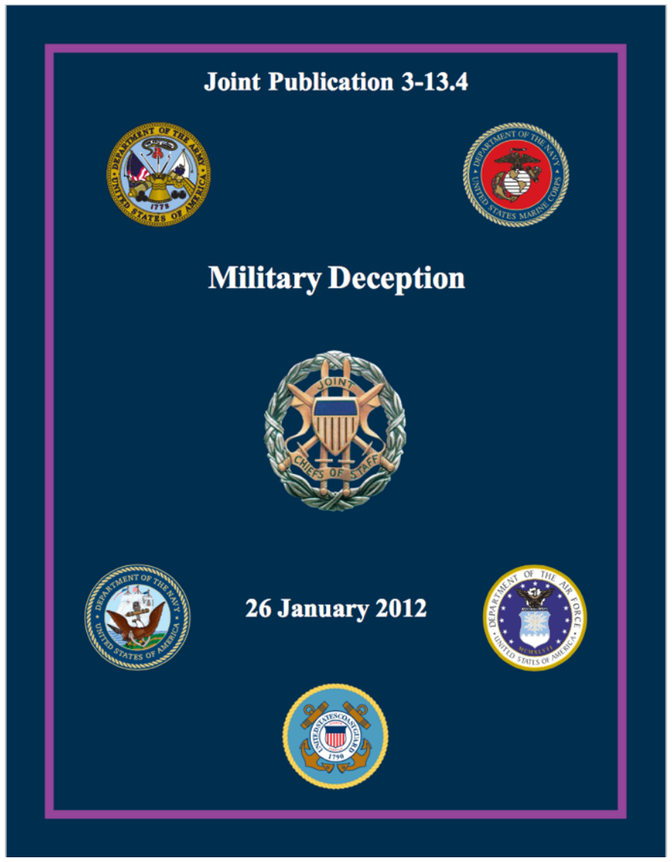
Automation (SHI)// Adaptive Exploitability // (AI algorithms?)

P4

Active Defence

How do you move form detection to concrete actions to thwart your adversaries

Super Cookies // Attribution // Offensive Capacities (Cred Theft) // Big Data Analysis



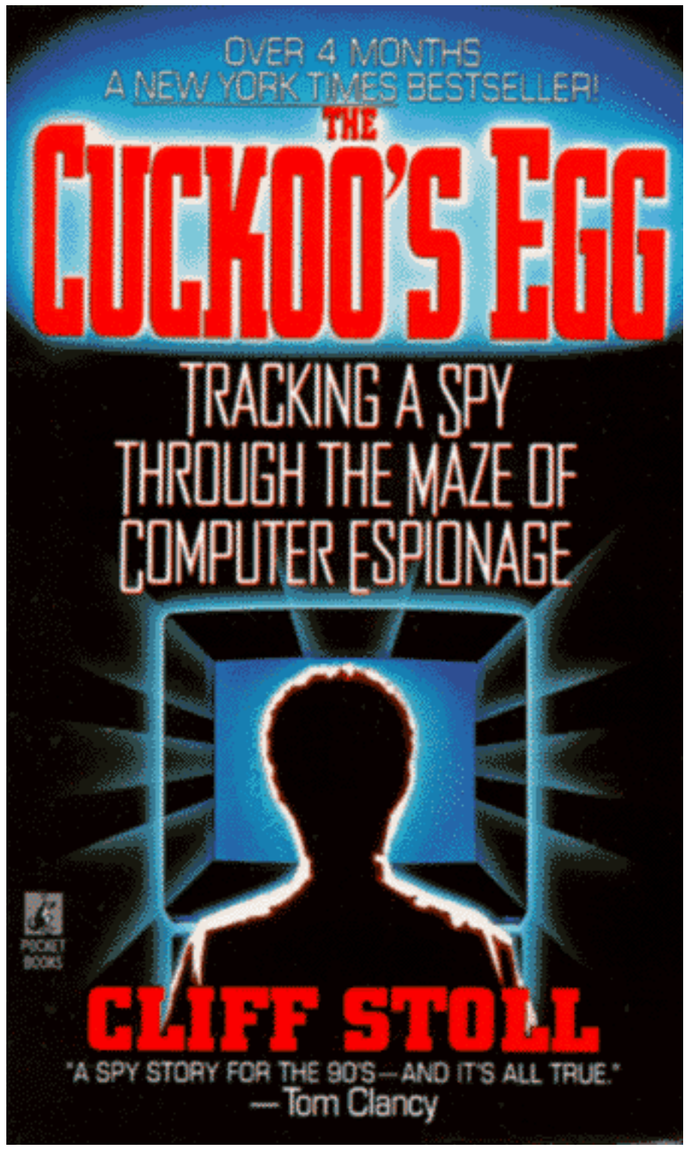
“

Military deception (MILDEC) is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

”

USA Military

“Joint Publication 3-13.4 Military Deception”, Joint Chiefs of Staff 2012



Many people's intro to infosec.

Private vs. State

How to observe the observers

Obsessive behaviour

The Cuckoo's Egg
Clifford Stoll, 1989

Counter Craft

Why did it fail?

Academic

Hobby

Silence doesn't sell

Value of Intelligence

Haroon Meer does a great job explaining it in his BlackHat preso:
https://www.youtube.com/watch?v=W7U2u-qLAB8

RESISTANCE
REPORT

How France's Macron defeated Russian hackers with one simple trap

POSTED BY: NATHAN WELLMAN MAY 7, 2017

Despite being the victim of a "massive and coordinated" hack immediately before the French election, President-elect Emmanuel Macron is currently celebrating a landslide electoral victory over the pro-Putin, rightwing nationalist Marine Le Pen.

So what did Macron's campaign do differently from Hillary Clinton's campaign, which famously suffered a similar attack, **likely from the same Russian operatives**?

Maturity

SOC

SIEM

3rd Party Threat Intel -

Cyber Gangs

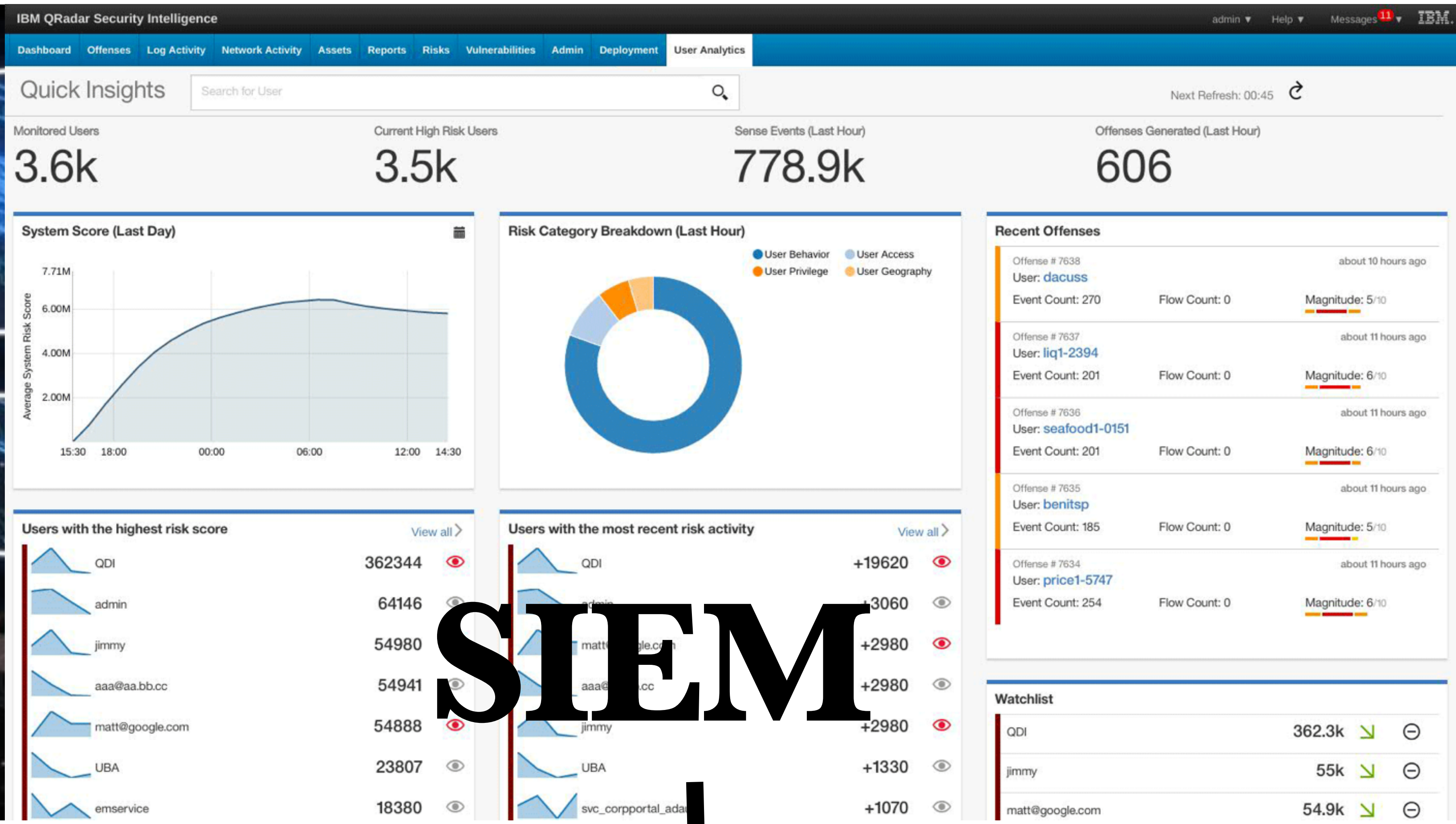
Nation State Groups

1st Party Threat Intel

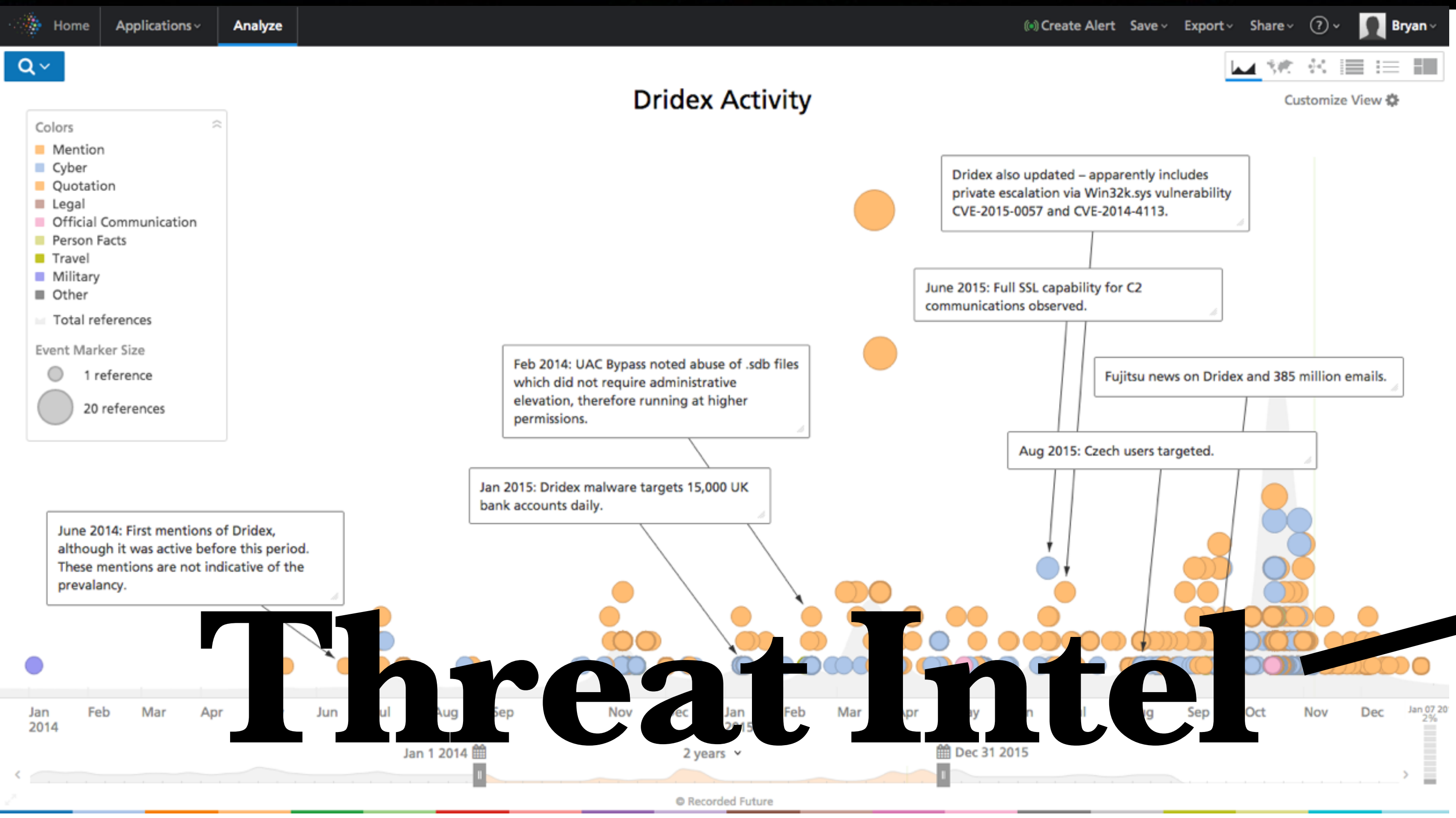
Environment Manipulation

What if?

SOC



SIEM



Threat Intel

IOCs

CounterCraft

Tons of IOCs

Trust

(threat intelligence sharing with trusted peers)

Usefulness

(threat intelligence sharing with useful peers)

pyramid of pain

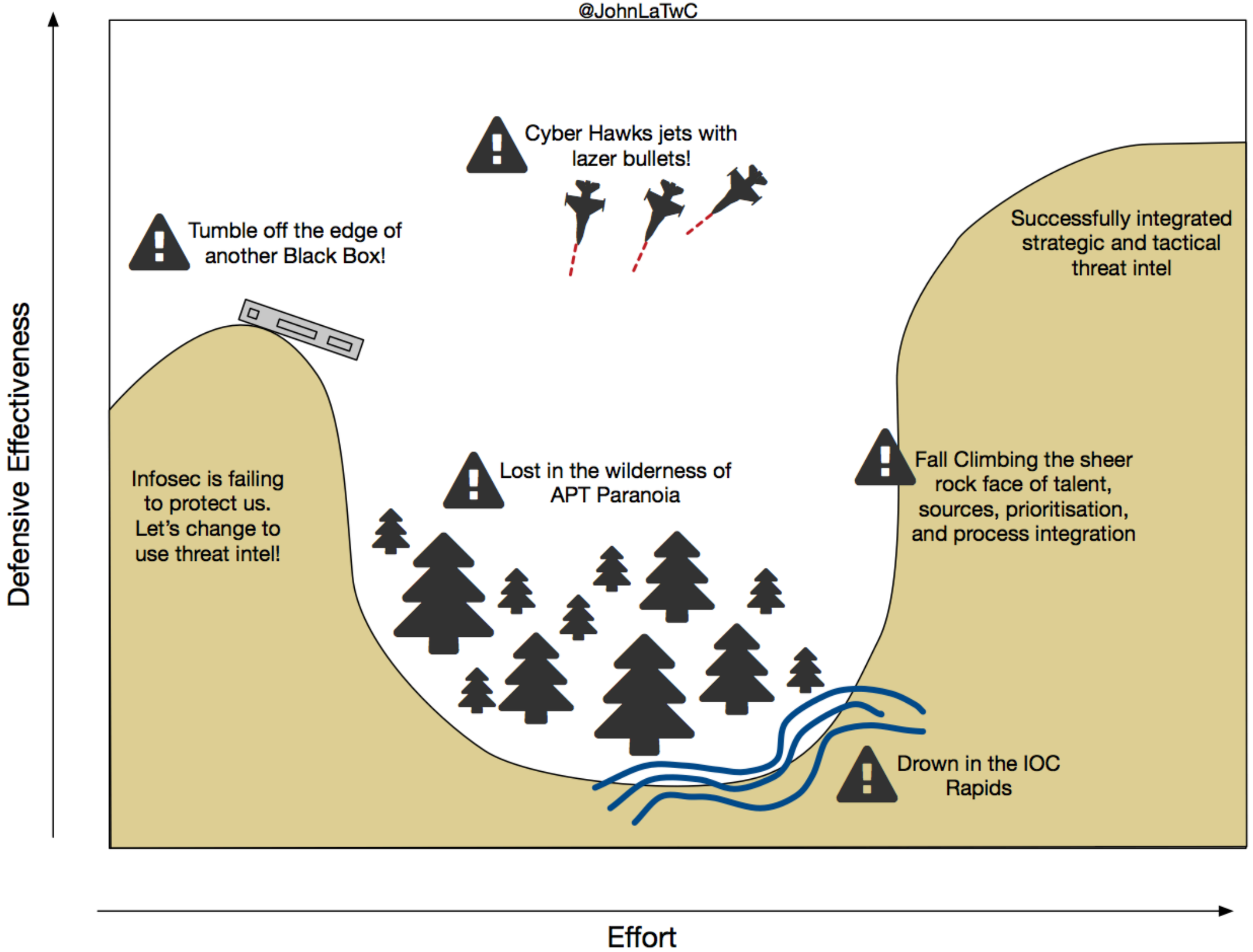
Freshness

(threat intelligence sharing with peers with live data)

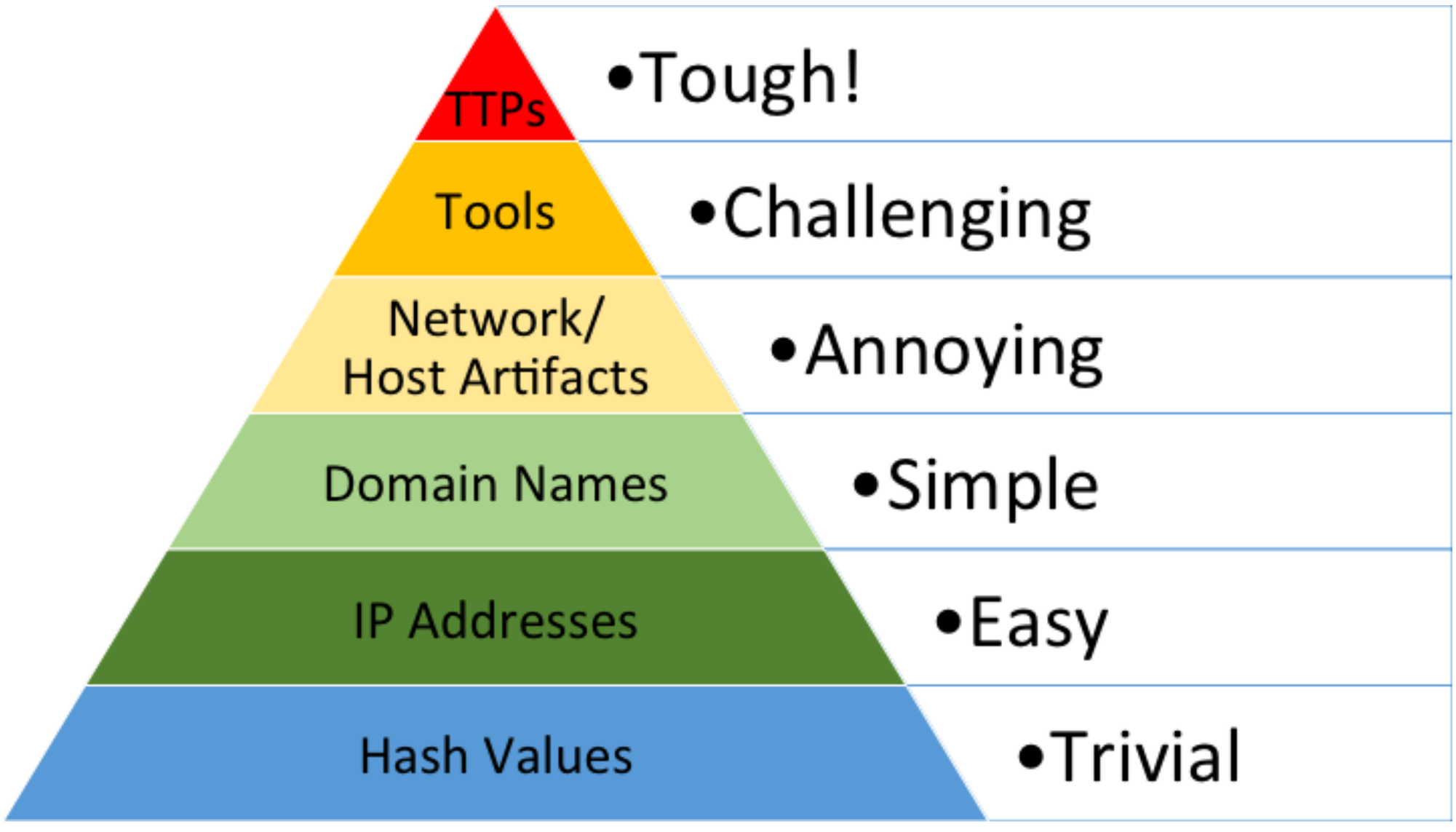
Haroon Meer does a great job explaining it in his BlackHat preso:
https://www.youtube.com/watch?v=W7U2u-qLAB8

Beware Perils in the Threat Intel Journey

thanks to John Lambert
@JohnLaTwC

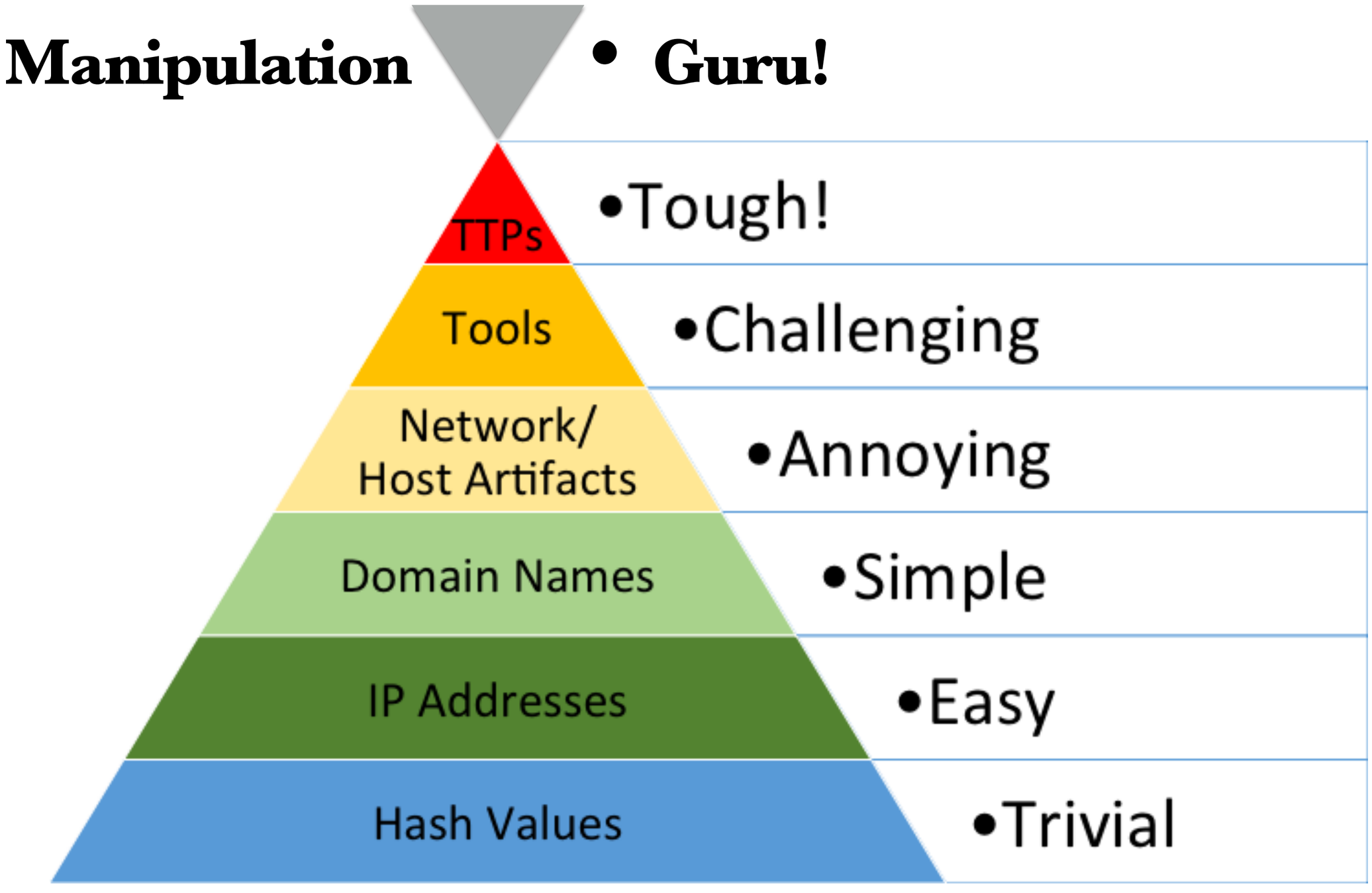


Counter Craft



David Bianco - Pyramid of Pain - Mandiant / Sqrrl / Target

Counter Craft



David Bianco - Pyramid of Pain - Mandiant / Sqrrl / Target

Counter Craft

The Pyramid of Pain shows how much pain adversaries suffer when you are able to deny them those indicators of compromise.

But we can not only deny, but **manipulate** and **interfere** with those indicators of compromise.

https://orig00.deviantart.net/64a8/f/2008/137/7/7/marionette_by_melow1.jpg

Counter Craft

Adversary manipulation

provide them with false information
make them think they are successful
show capabilities & infrastructure
divert them away from goal
waste their time and resources

Attack Trees.

Attack Trees

B. Schneier

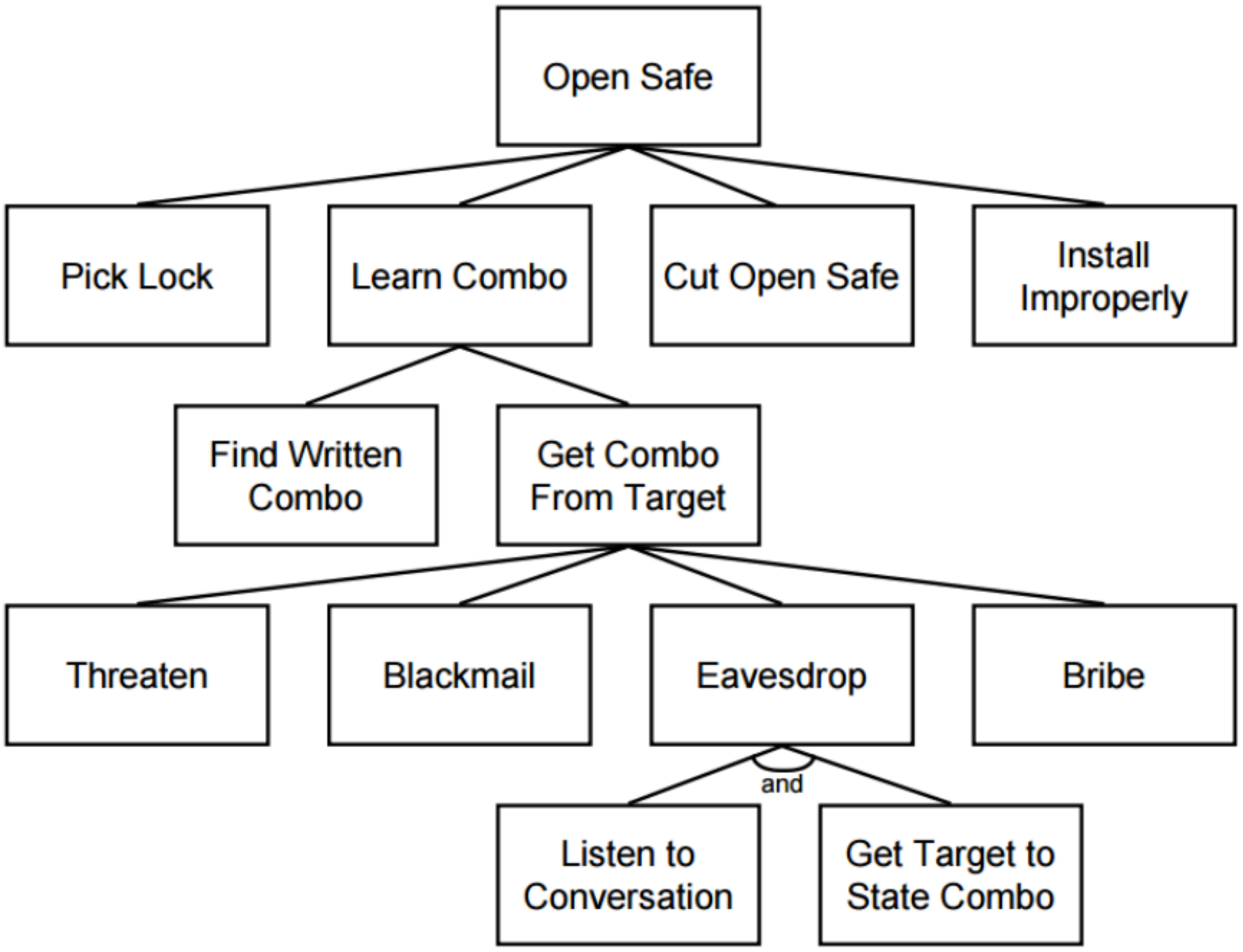
Dr. Dobb's Journal, December 1999.

Modeling security threats

By Bruce Schneier

Few people truly understand computer security, as illustrated by computer-security company marketing literature that touts "hacker proof software," "triple-DES security," and the like. In truth, unbreakable security is broken all the time, often in ways its designers never imagined. Seemingly strong cryptography gets broken, too. Attacks thought to be beyond the ability of mortal men become commonplace. And as newspapers report security bug after security bug, it becomes increasingly clear that the term "security" doesn't have meaning unless also you know things like "Secure from whom?" or "Secure for how long?"

Clearly, what we need is a way to model threats against computer systems. If we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks. And if we can understand who the attackers are -- not to mention their abilities, motivations, and goals -- maybe we can install the proper countermeasures to deal with the real threats.


Open Safe
Pick Lock
Learn Combo
Cut Open Safe
Install Improperly
Find Written Combo
Get Combo From Target
Threaten
Blackmail
Eavesdrop
Bribe
and
Listen to Conversation
Get Target to State Combo

Counter Craft

"Attack trees are conceptual diagrams describing how an asset, or target, might be attacked."

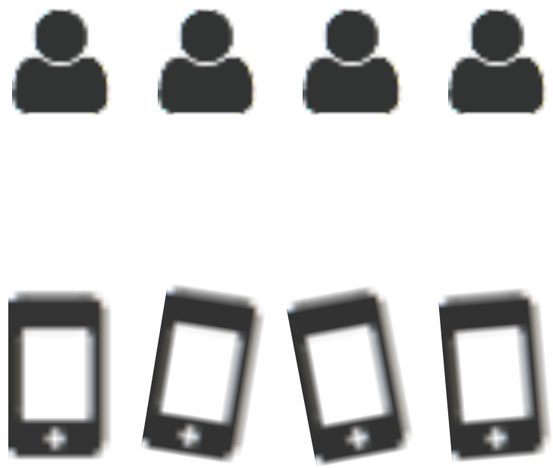
"Attack trees are conceptual diagrams **prescribing** the desired adversary lateral movement within decoy assets."

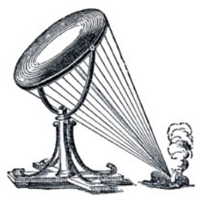
C/C

Conceptual diagrams showing how a target in a **specific scenario** can be attacked
All nodes/steps are up and running
Breadcrumbs are deployed in each node pointing to the next step
You need information from **previous steps** in order to reach the next step
Each node will gather information and TTPs from the adversary
By clustering such information we are able to generate **actionable intelligence**

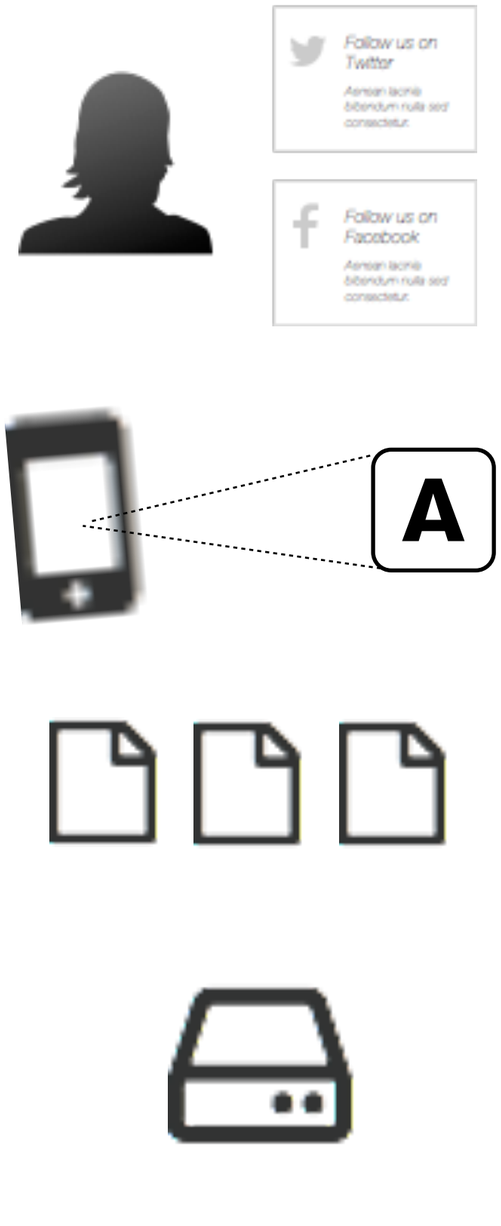
Deception Attack Trees

An organisation's typical IT assets.

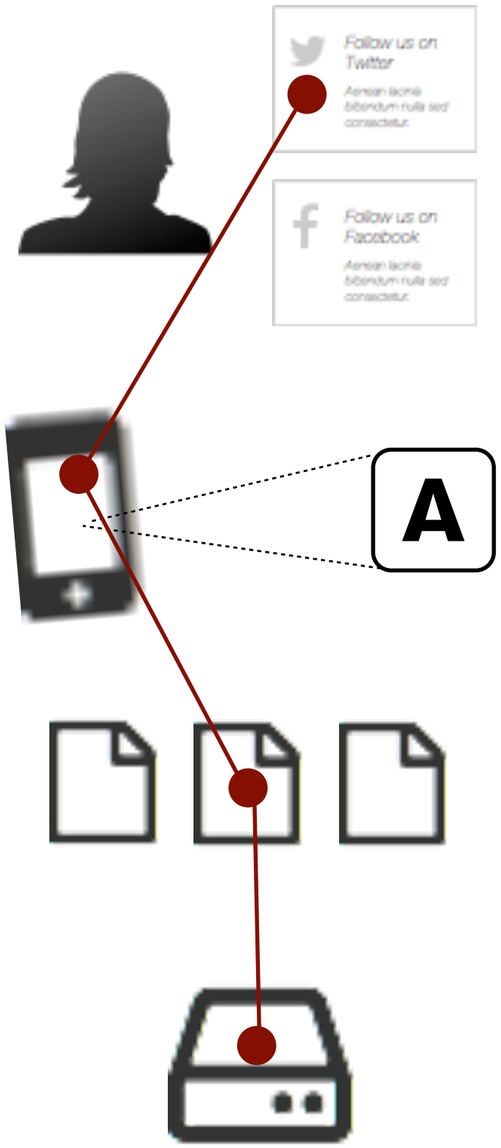




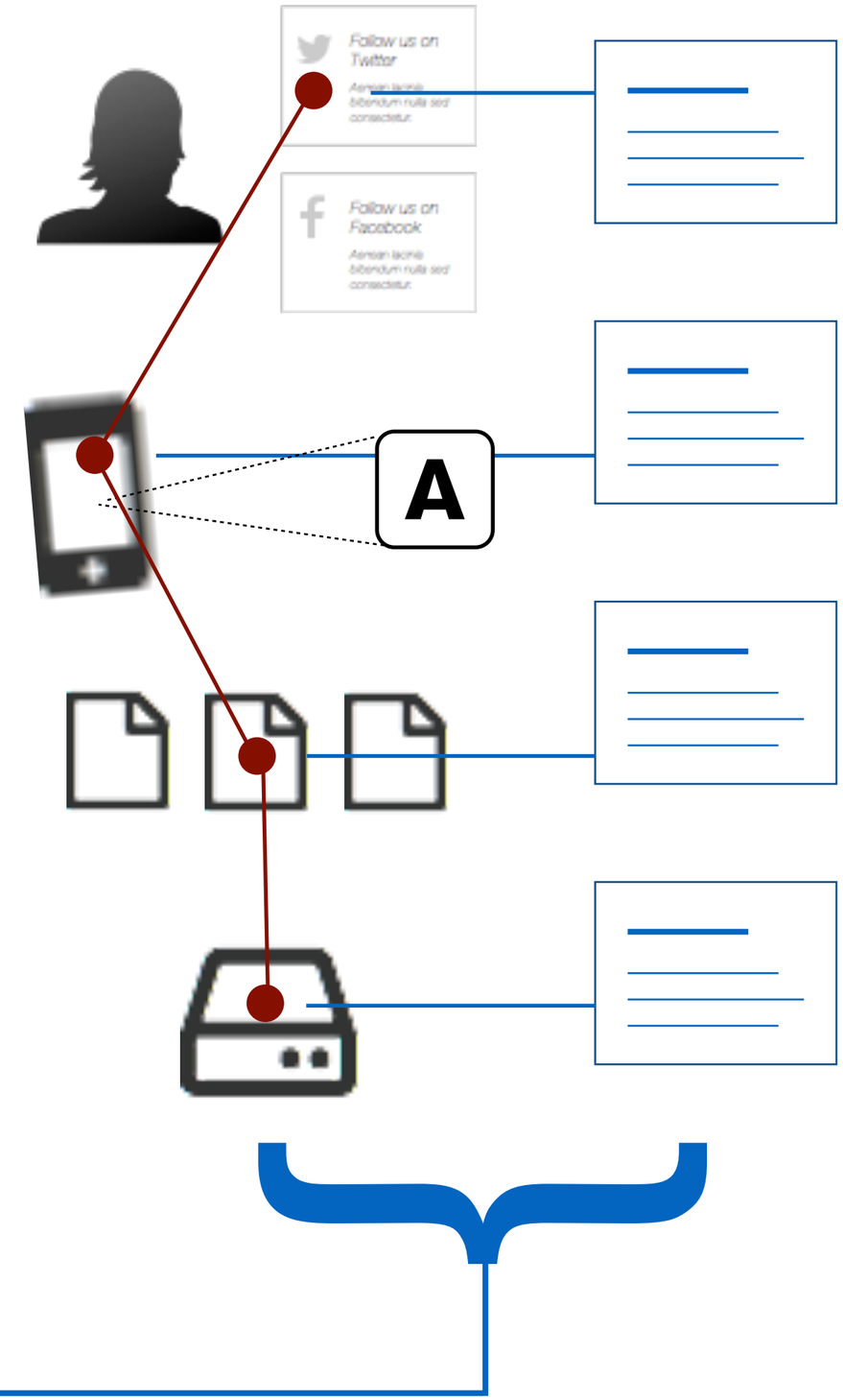
Your deception assets



Adversary's attack tree



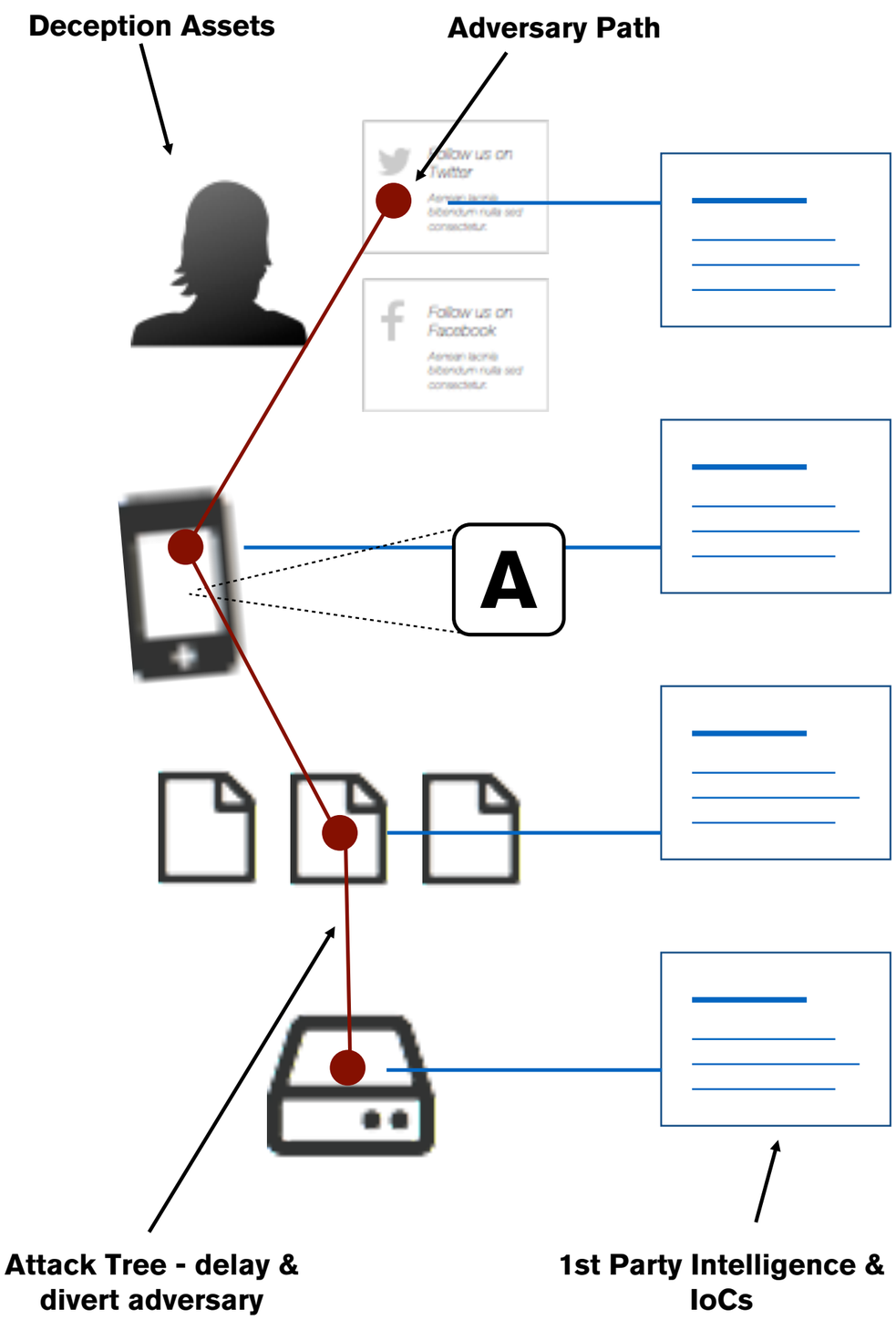
Extraction of IOC / TTP data



Get situational awareness of high risk events and threat actors that cause major impact on your digital business.

Use Deception Technology to create attack trees, dynamic engagement and IoC generation.

Build an active defence posture with CounterCraft as a key element of your strategy.

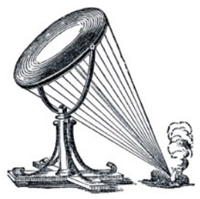


Strategic

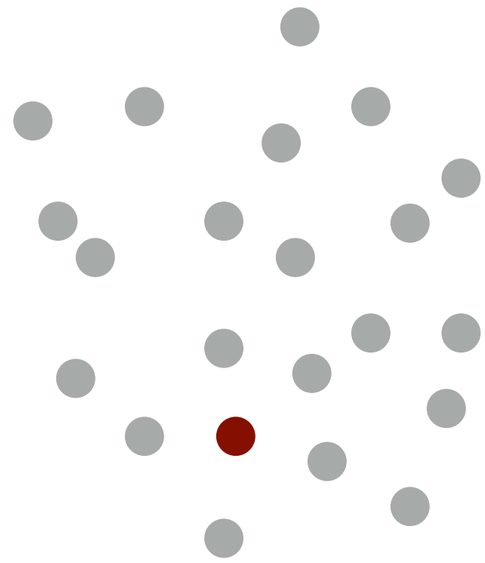
Intelligence led strategy: calculate risks to business
Increased **situational awareness** of adversaries: capability, motivations, mix of adversaries,
Test **hypotheses** about adversaries:
Gather **real evidence** of impact: communication to board

Tactical

Detection: Early on in the kill chain.
Engagement: at incident level, in real time, manipulate the information & knowledge that your adversary has access to, and affect their actions.
Control of individual threat actors: the endgame



SIEM data lake.



Better Analysis.

Deception Attack Tree.

Better Data.

Example: 1 External Recon

Adversary Attack Graph

1 external reconnaissance - Censys

2 directed brute force attack

3 document exfiltration

4 lateral movement*

5 memory analysis

6 cookie discovery

7 mobile app discovery

8 app usage

External Technical Recon

Skills 1: Brute Force

Motivation: deep Network Access

Human Check: able to parse documents

Skills 2: Memory Analysis

Reactive: System reacts to mem analysis

Social Engineering: force error

Review unique data obtained

Adversary Activity

Attacker

Fingerprinting on Shodan

189.XXX.YY Y.ZZZ

Brute Force - Hydra

Dict Attack: Troogle

App Entry / Discovery

Doc exfiltration & Opening

Time

Defender

HTTP Headers & SSL Cert Indexed by Shodan

Linux Server

Alerts on forcing

Believable Web App

Services.xlsx

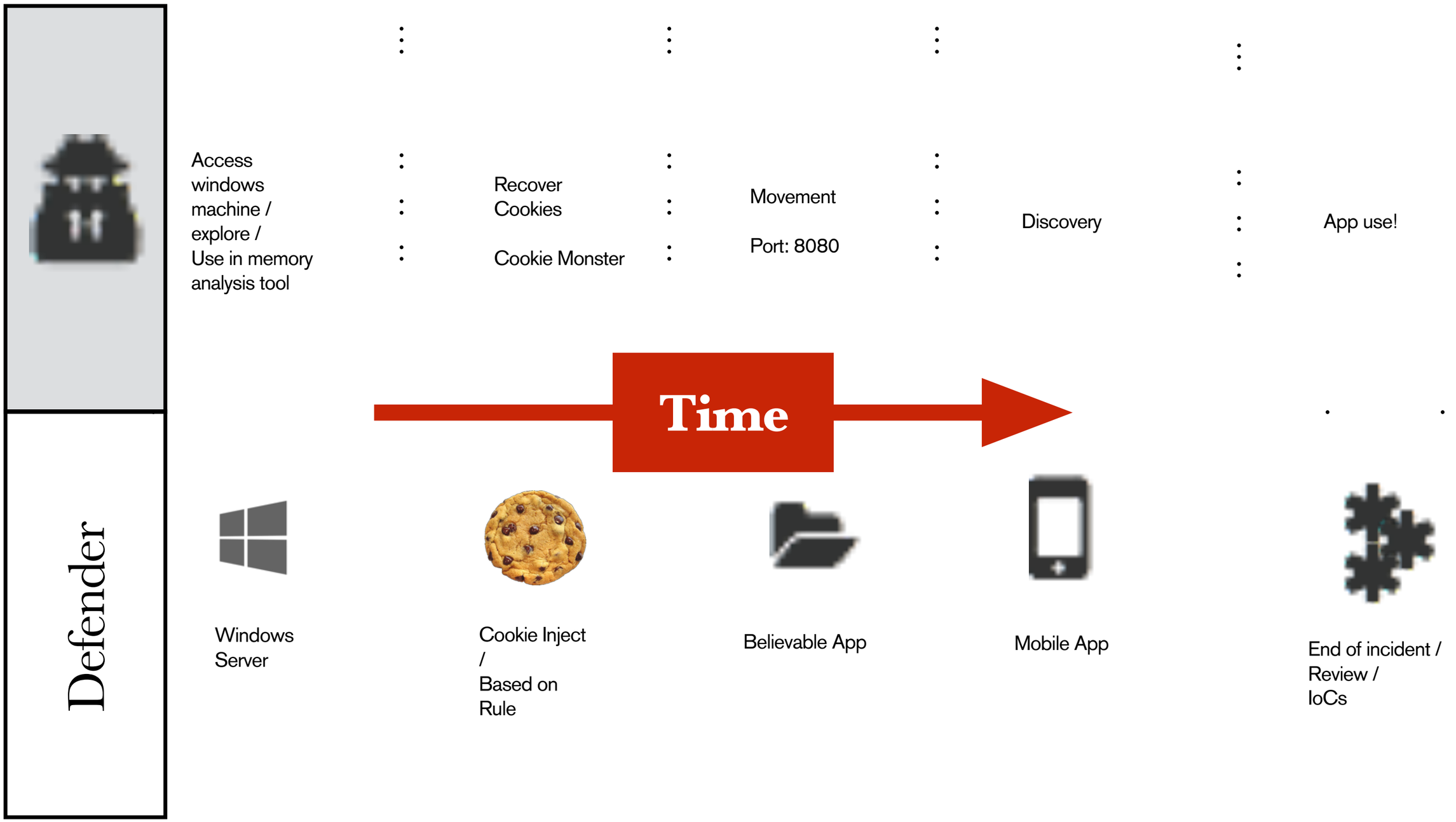
Automated / via template / upload

Review Alerts

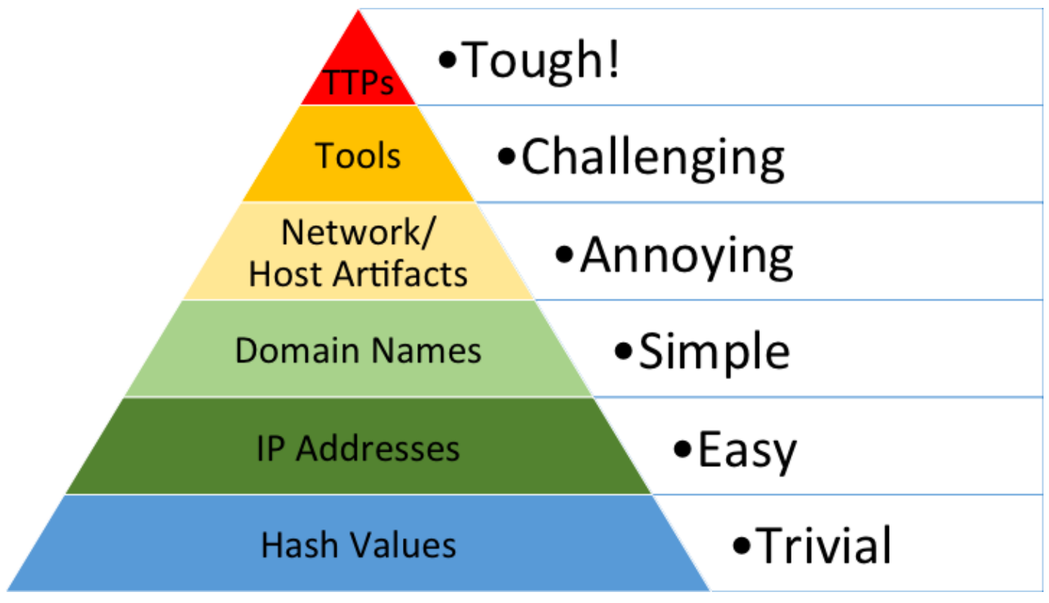
Brute Force
Access to Portal
Download doc
Opening doc

Defender Assets / Alerts

Adversary Activity



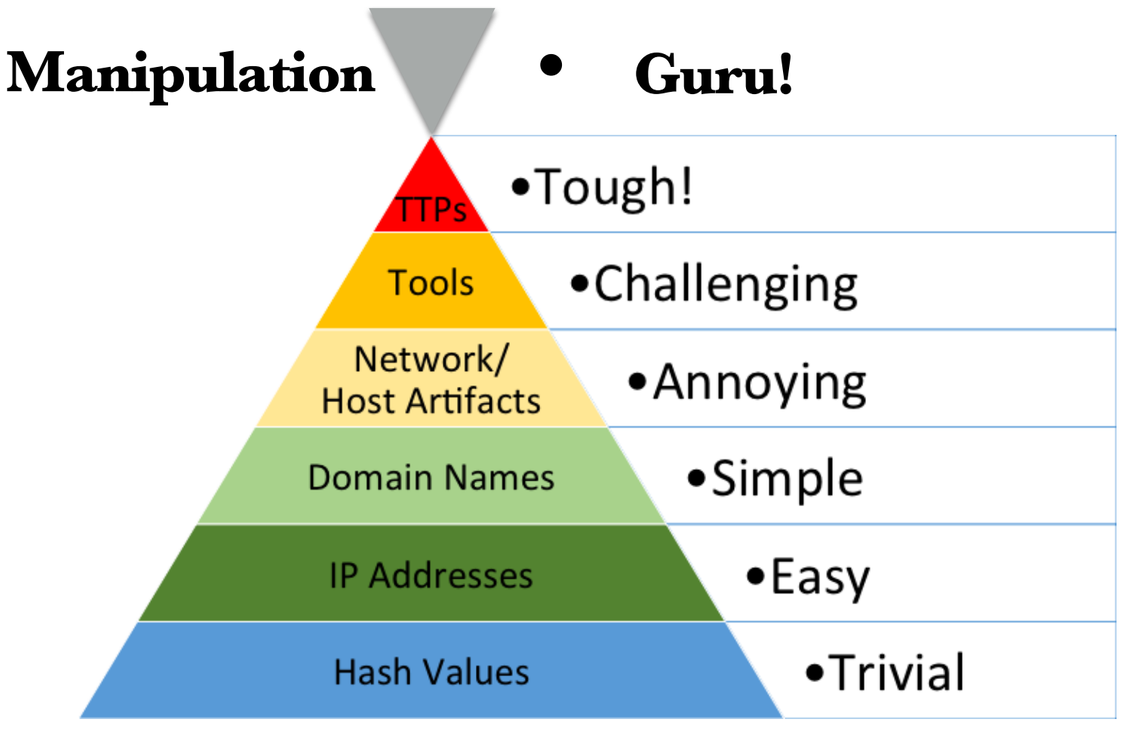
Defender Assets / Alerts



TTPs - In memory attacks
Tools - Cookie Extractors
Host Artifacts - Files, dir structure
Domain Names -
IP Addresses - User Agents
File Hashes - of tools used

External Recon Results

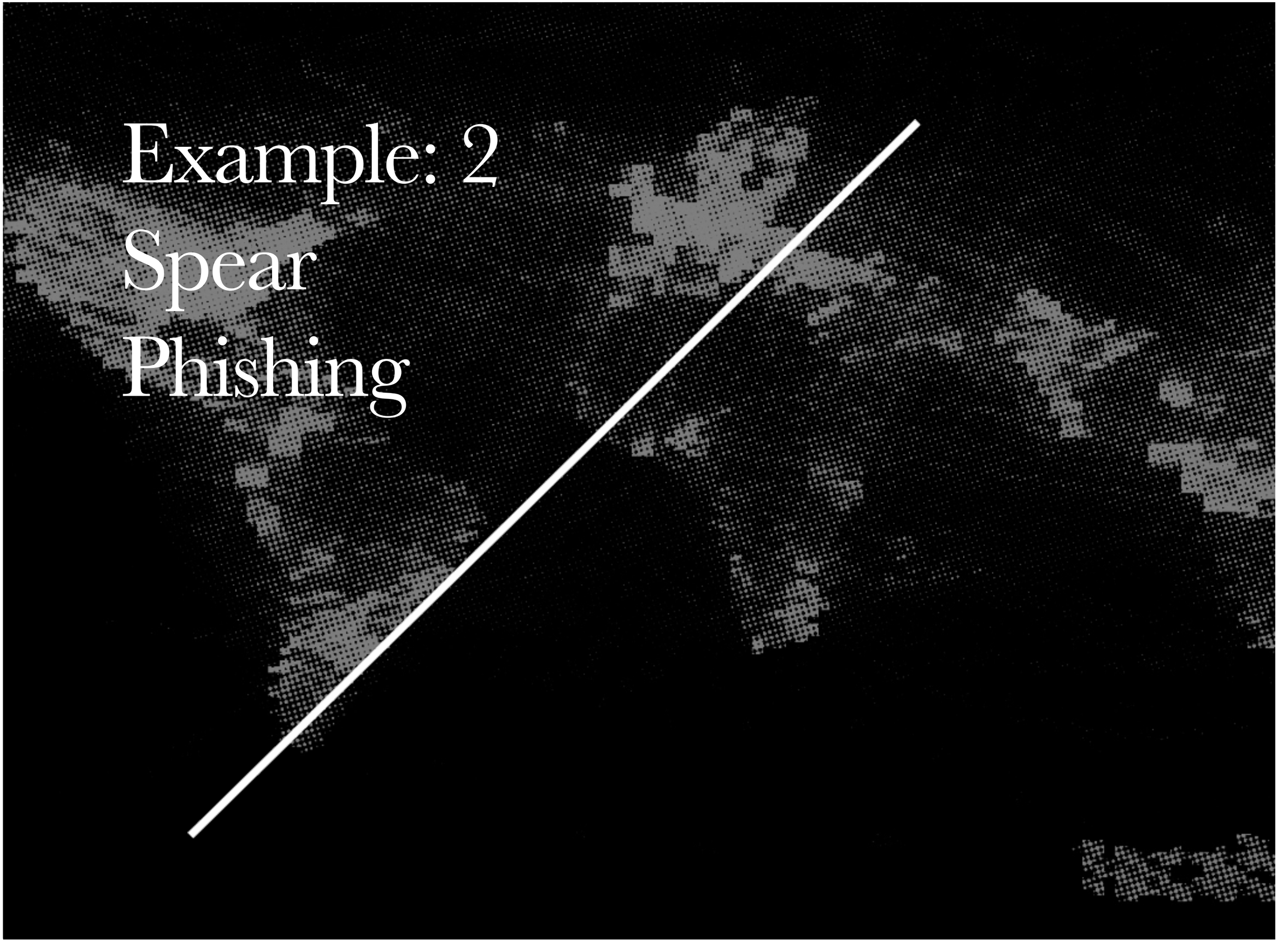
c/c



TTPs - In memory attacks
Tools - Cookie Extractors
Host Artifacts - Files, dir structure
Domain Names -
IP Addresses - User Agents
File Hashes - of tools used

External Recon Results

Example: 2
Spear Phishing

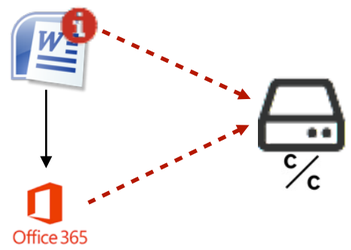


Counter Craft

Two approaches

1. Malware or Phishing Incident
2. Malware - long term sandbox
3. Phishing - inject other domain deception asset
4. lateral movement*

Adversary “finds” documents / credentials

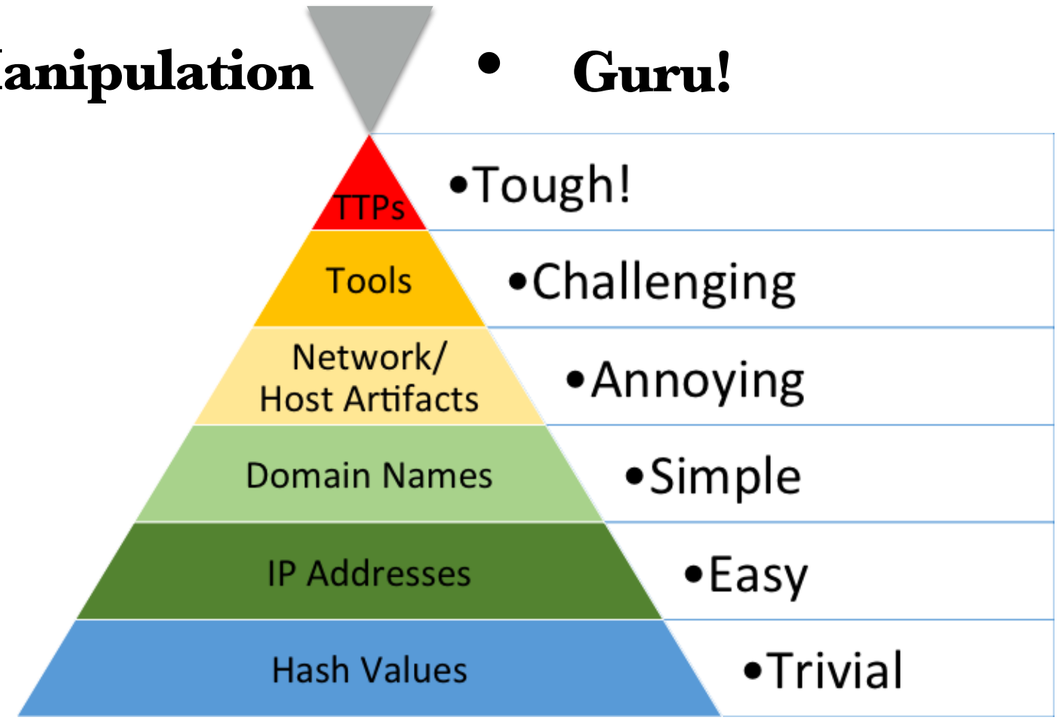


Both document & platform report back to C/C

C/C

c/c

Manipulation • **Guru!**

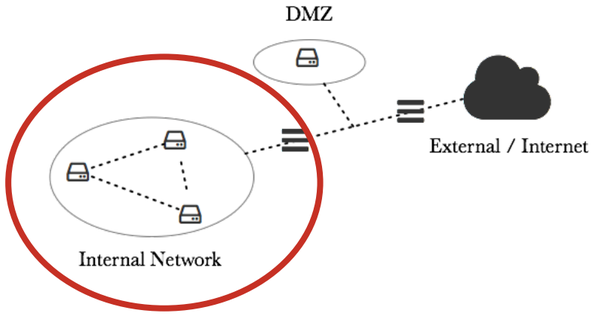


TTPs - Targeted; Use Creds; Motive
Tools - Infection Vector; Exploits
Host Artifacts - Files, dir structure; C2
Domain Names - Phishing Infr.
IP Addresses - User Agents
File Hashes - Dropper

Phishing Results

Example: 3 Internal Lateral Movement

Internal Lateral Movement



Lateral Movement

3rd parties have infiltrated endpoints in the network. By leaving a trail of massively distributed breadcrumbs (20K+) we can lead them to our deception assets, and detect & study them.

Nation State Actors

Cyber Criminal Gang
Competitors

Rogue Employee
Politically Motivated Activists

Cyber Delinquents

Detection & study of the lateral movement of an adversary

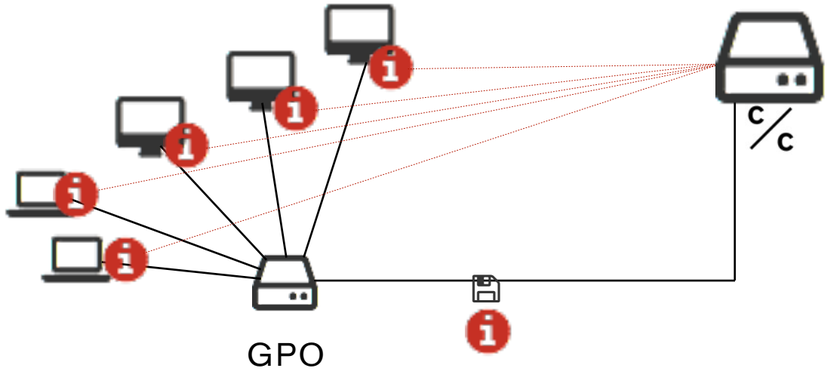
1.

Attack Tree

1. Adversary compromises endpoint.
2. Adversary searches for trails left behind by authorised users like browser histories and log files.
3. Adversary follows “decoy” data to one of our instrumented high interaction honeypots.

2.

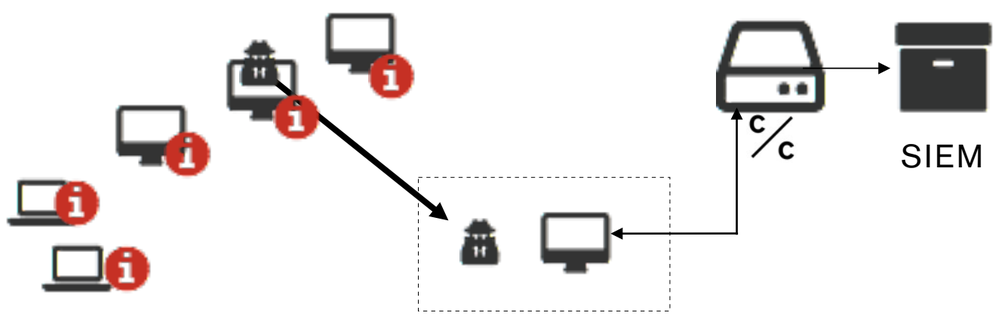
Breadcrumb Distribution



We distribute a large number of varied breadcrumbs to endpoints, at scale. These beacon back to our server to ensure they are installed and fresh.

3.

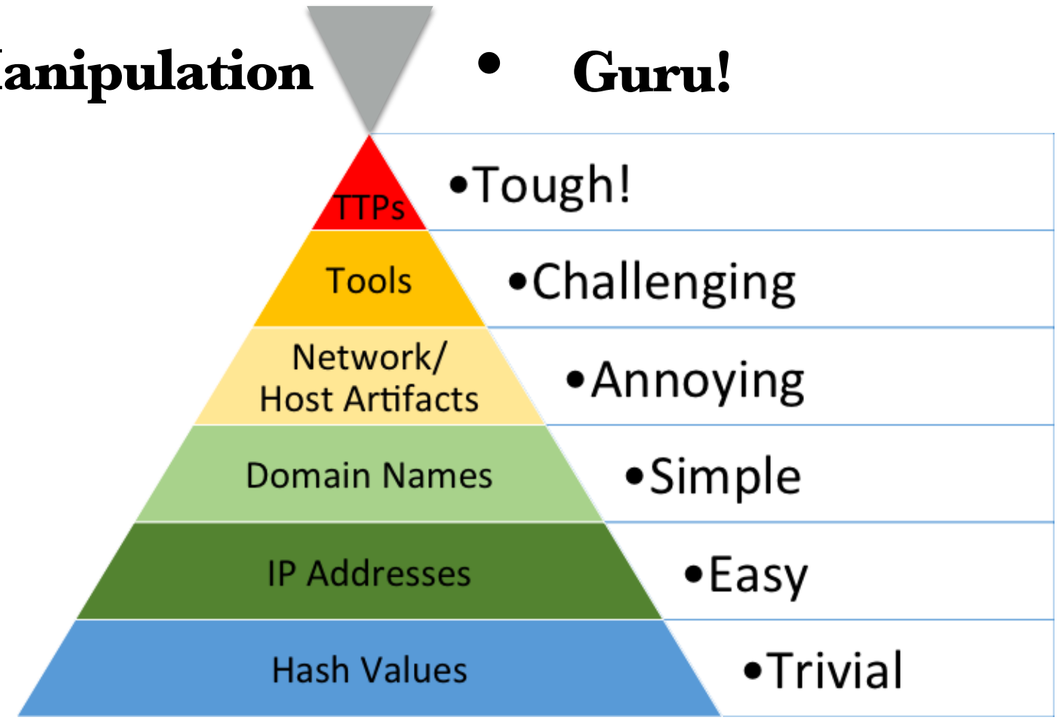
Deception Environment



The adversary interacts with our deception environment firing off alerts to SIEM

c/c

Manipulation • **Guru!**



TTPs - Red Team; Motives;
Tools - Scanning Software,
Host Artifacts - Files, dir structure; C2
Domain Names -
IP Addresses - Internal IPs
File Hashes -

Phishing Results

Conclusions.

Counter Craft

What did we see?

Active Defence & Deception

Attack Trees

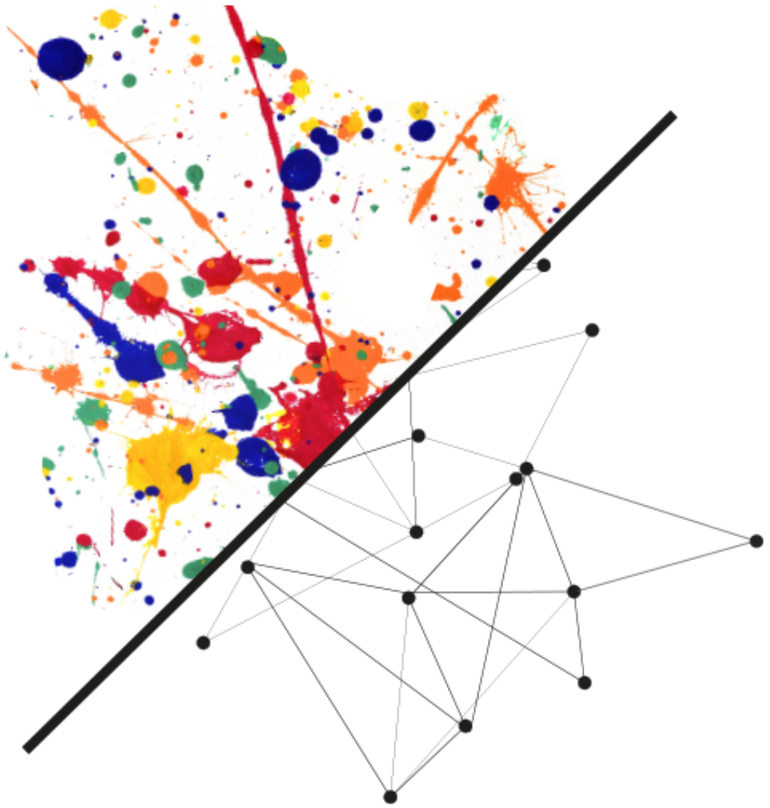
Examples

Conclusions

Take- aways

- 3rd party threat intelligence powerful but not easily actionable
- Combine that 3rd party with 1st party threat intel
- Move up the pain triangle of IOCs
- IR and Threat Intelligence teams can use deception in many use cases
- Stop managing incidents and start managing adversaries

Counter
Craft



David Barroso
Founder
CEO
dbarroso@countercraft.eu

www.countercraft.eu
craft@countercraft.eu