HUNT & HACKETT

OUTSMART YOUR DIGITAL ADVERSARIES

What if…

THREAT INTELLIGENCE LOST ITS SHINE?

Our time together

SUBJECTS TO COVER

- Philosophical musings
- Threat intelligence pitfalls
- Threat Intelligence led operations

A TI deja-vu

ALL OLD IS NEW AGAIN

Author: thinkstockphotos.com

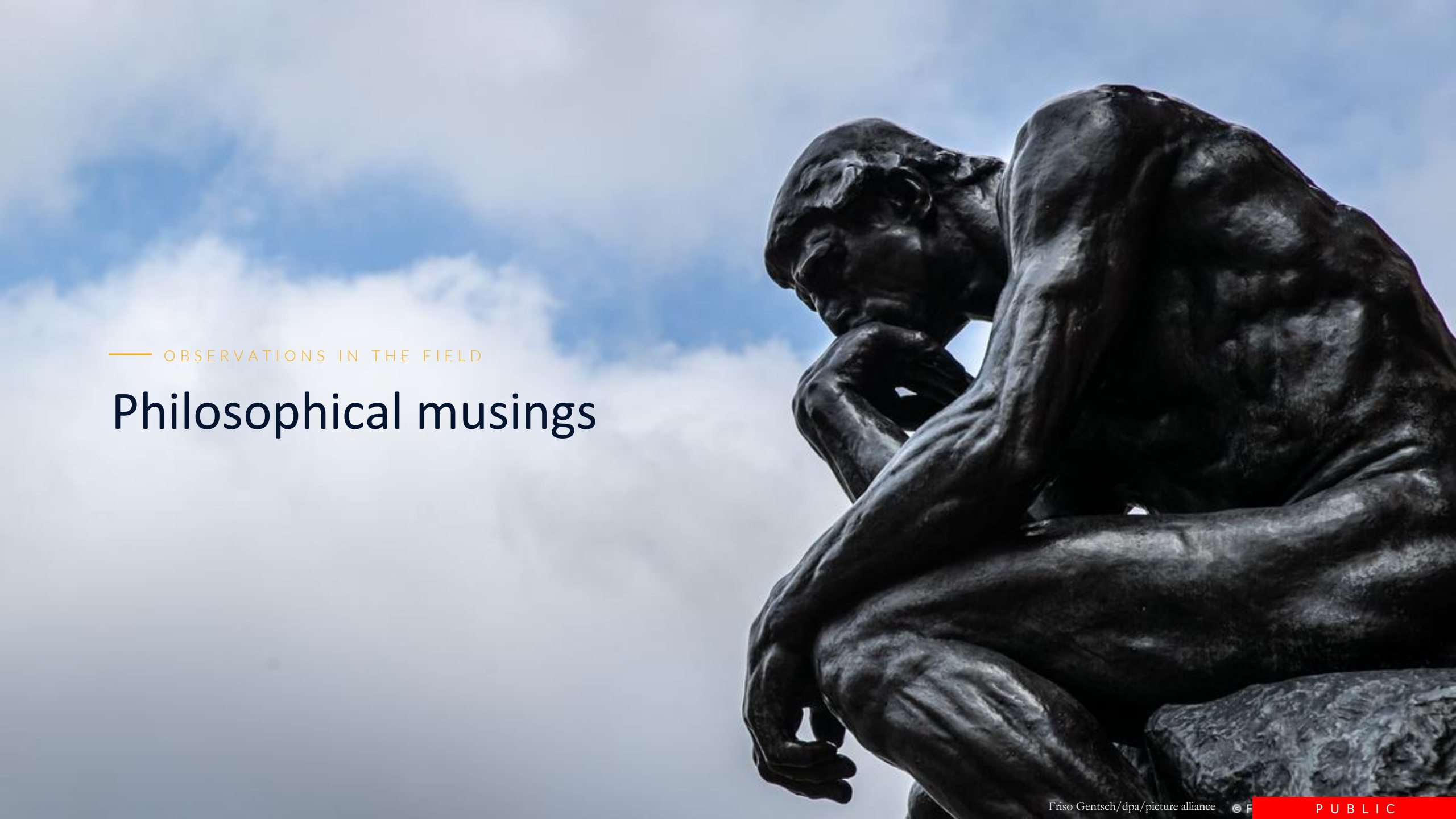
TI?

OR JUST PENTEST FINDINGS?

- Insufficiently segmented & filtered network
- Weak passwords
- Missing patches
- Missing detection
- Insecure protocols
- Insufficient least-privilege-principle
- Insufficient hardening

OBSERVATIONS IN THE FIELD

Philosophical musings



Friso Gentsch/dpa/picture alliance

Threat Intelligence

DESIRES OF THE ~~TRENCHES~~

C-Level	Difficult to align budget allocation with risk appetite and threat landscape
CISO	Hard to demonstrate program effectiveness Limited insights leading to ad-hoc approach
Ops	Fragmented silos Technically challenging and pressured to meet deadlines

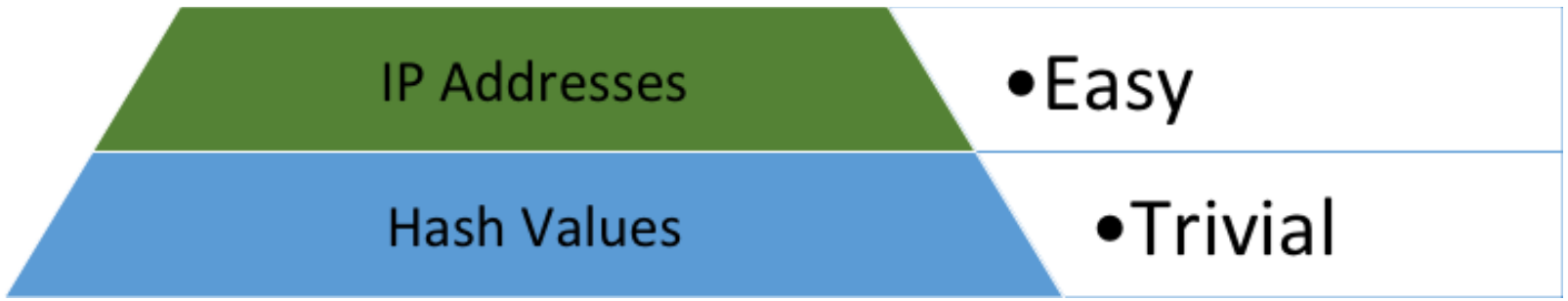
TI for inflicting pain?

CAN WE CLIMB TO THE TOP?

https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TI for inflicting pain?

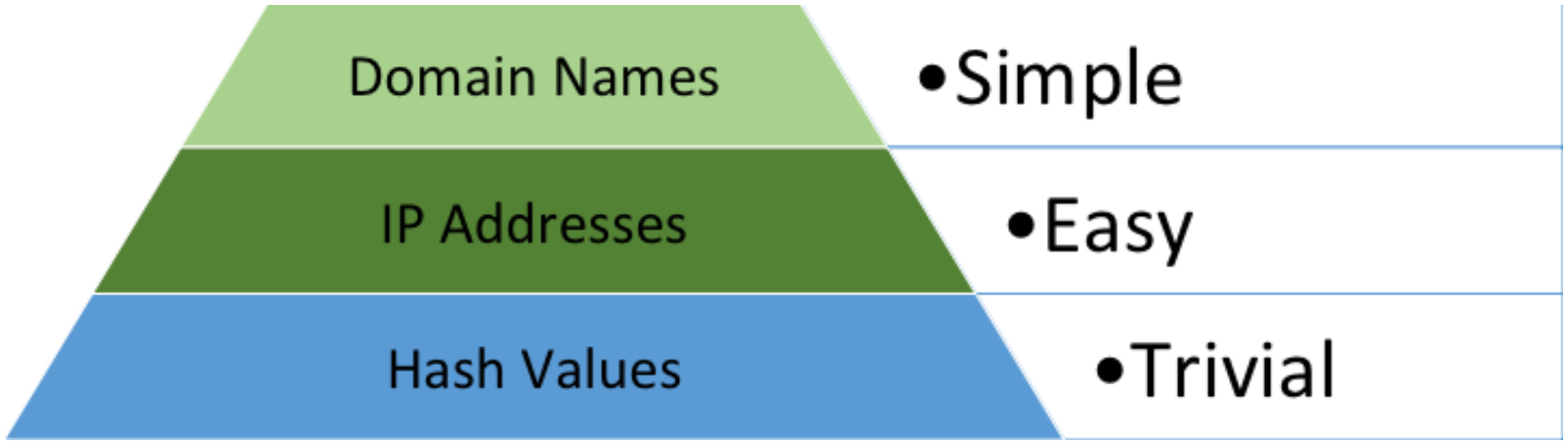
CAN WE CLIMB TO THE TOP?



https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TI for inflicting pain?

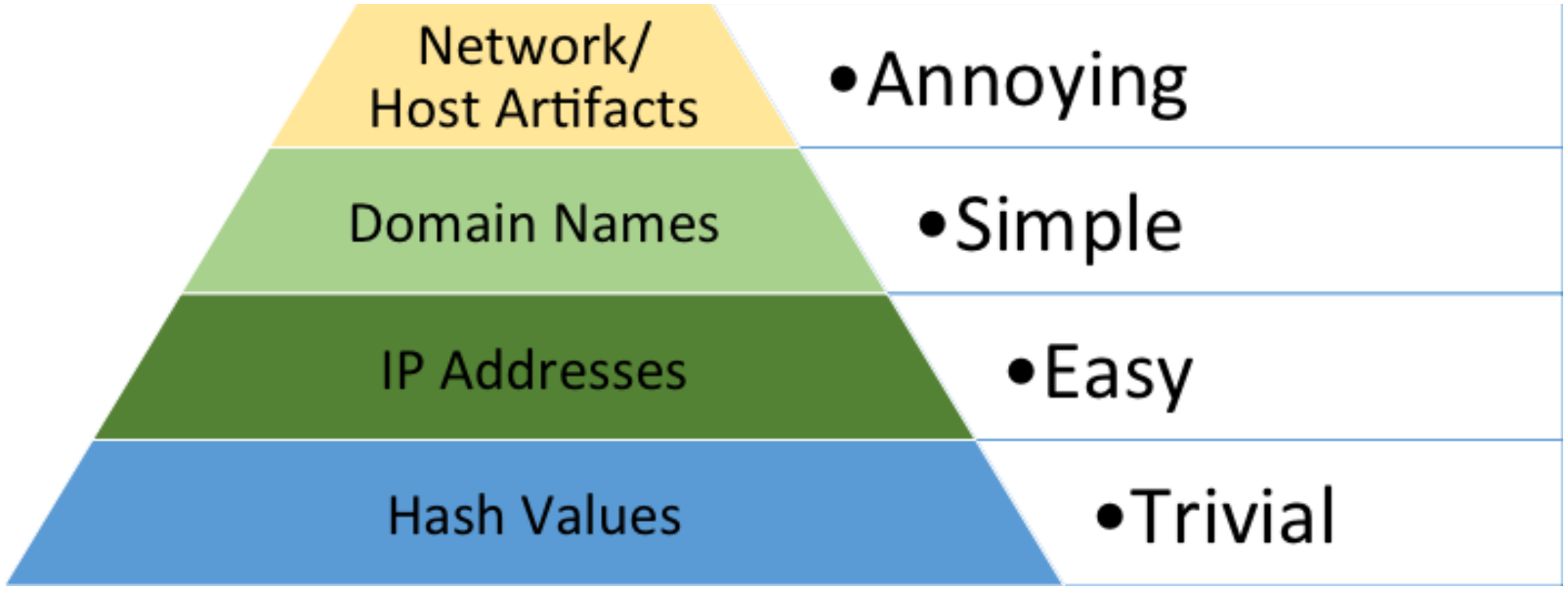
CAN WE CLIMB TO THE TOP?



https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TI for inflicting pain?

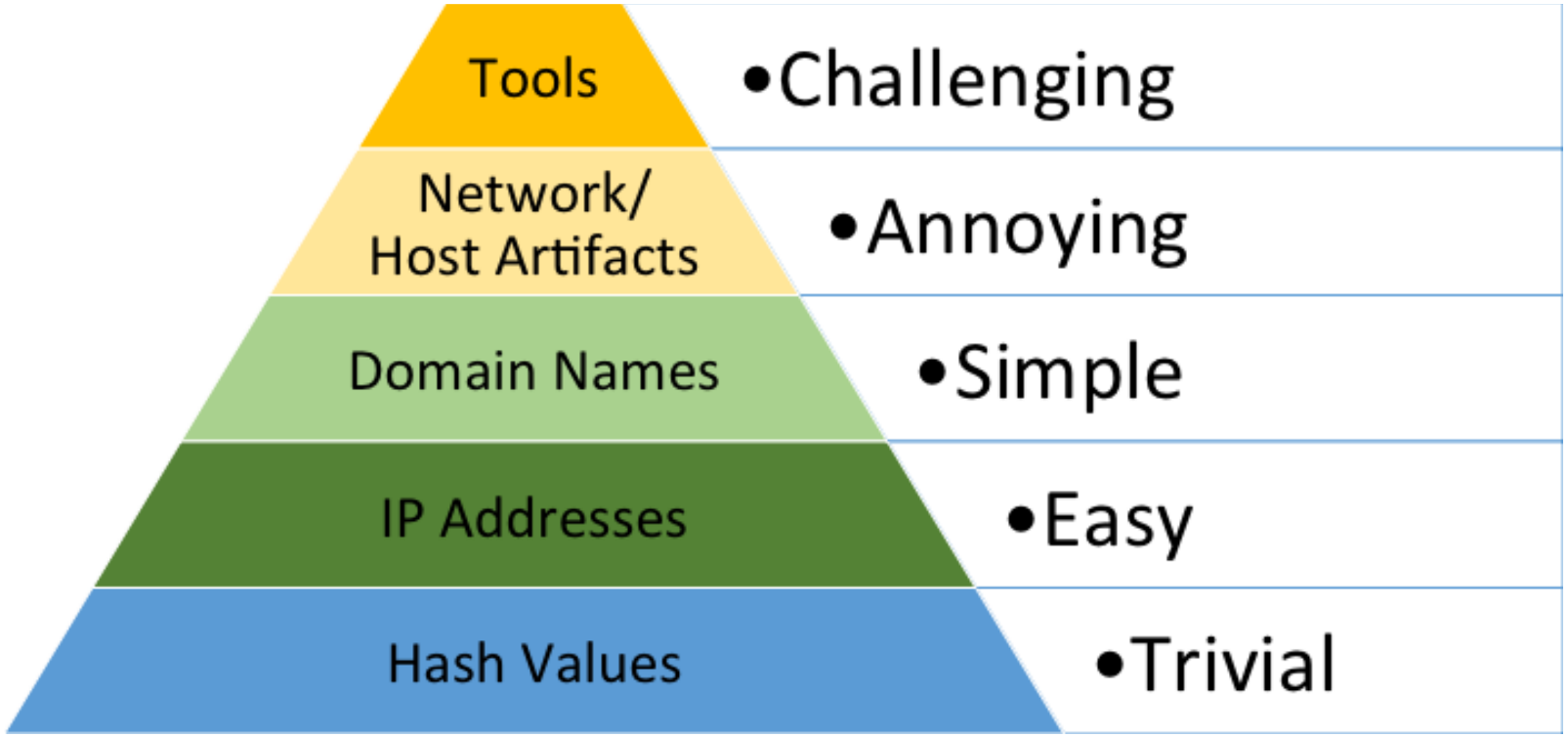
CAN WE CLIMB TO THE TOP?



https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TI for inflicting pain?

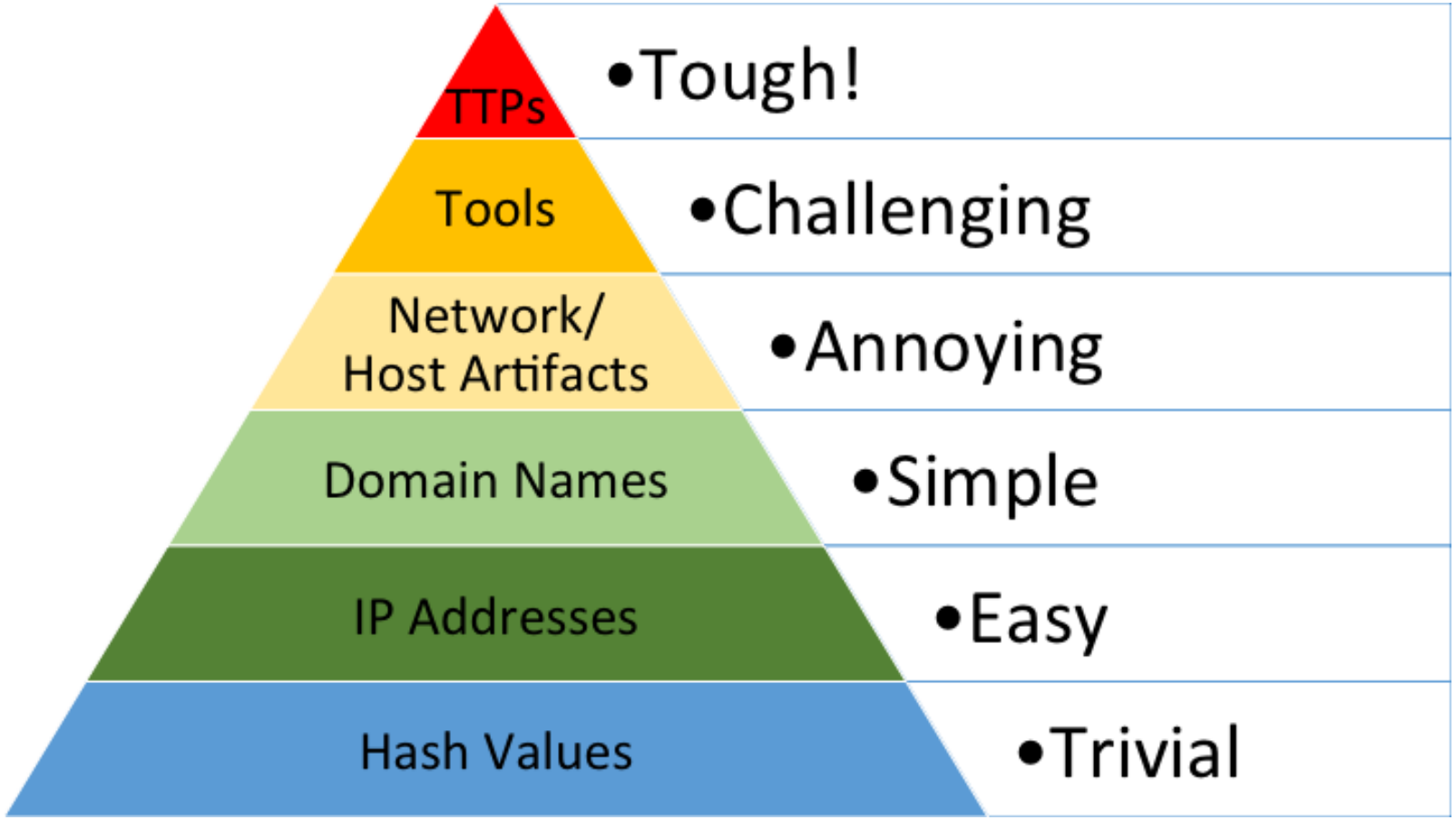
CAN WE CLIMB TO THE TOP?



https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TI for inflicting pain?

CAN WE CLIMB TO THE TOP?



https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Or maybe more for insights?

ALL INSIGHTS, INDISCRIMINATELY?

2021 CRIME TYPES

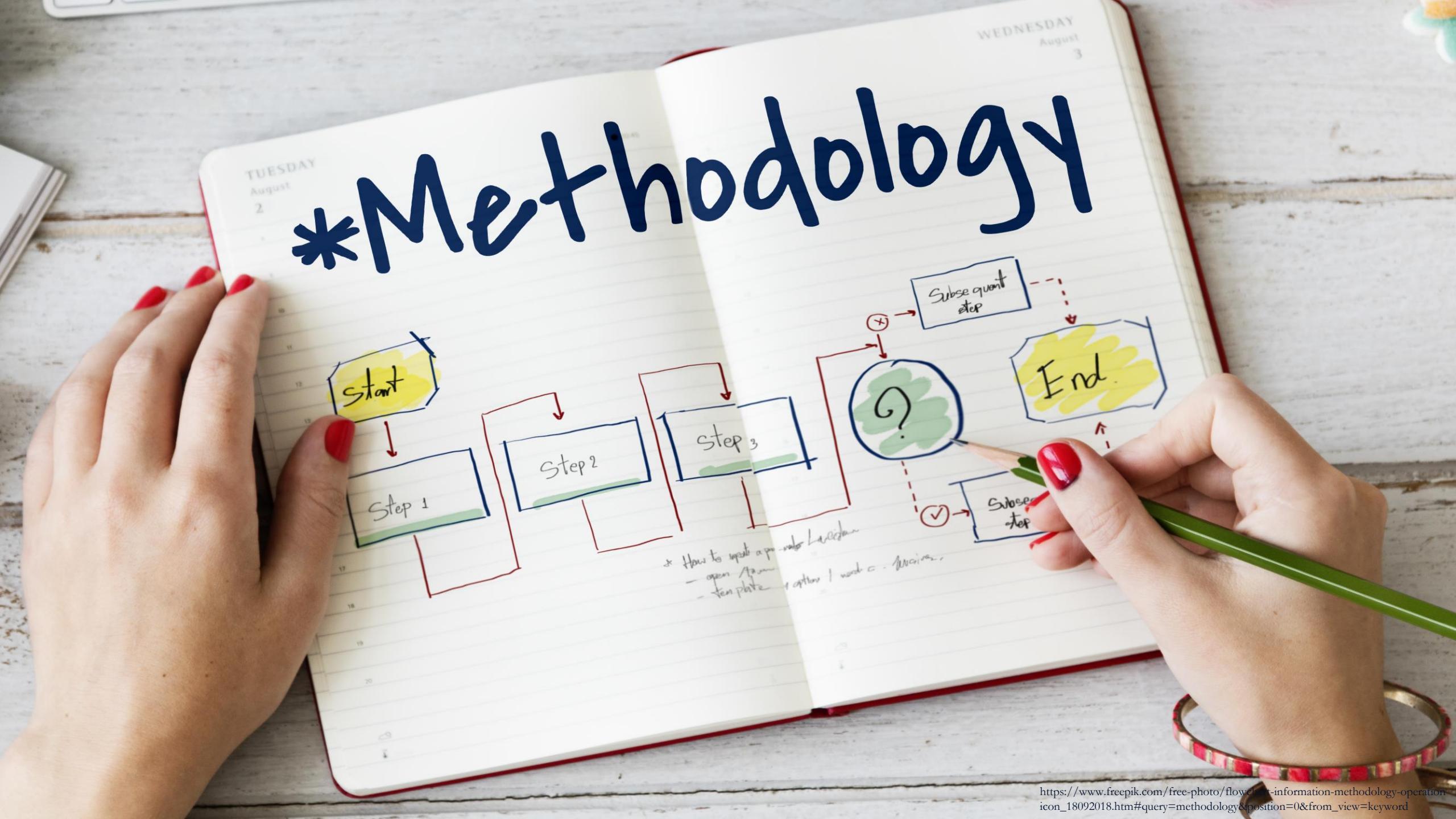
By Victim Count			
Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing/Vishing/Smishing/Pharming	323,972	Government Impersonation	11,335
Non-Payment/Non-Delivery	82,478	Advanced Fee	11,034
Personal Data Breach	51,829	Overpayment	6,108
Identity Theft	51,629	Lottery/Sweepstakes/Inheritance	5,991
Extortion	39,360	IPR/Copyright and Counterfeit	4,270
Confidence Fraud/Romance	24,299	Ransomware	3,729
Tech Support	23,903	Crimes Against Children	2,167
Investment	20,561	Corporate Data Breach	1,287
BEC/EAC	19,954	Civil Matter	1,118
Spoofing	18,522	Denial of Service/TDoS	1,104
Credit Card Fraud	16,750	Computer Intrusion	979
Employment	15,253	Malware/Scareware/Virus	810
Other	12,346	Health Care Related	578
Terrorism/Threats of Violence	12,346	Re-shipping	516
Real Estate/Rental	11,578	Gambling	395

*Descriptors**			
Social Media	36,034	Virtual Currency	34,202

https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Figure 1: ENISA Threat Landscape 2022 - Prime threats

https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends



https://www.freepik.com/free-photo/flowchart-information-methodology-operation-icon_18092018.htm#query=methodology&position=0&from_view=keyword

https://www.freepik.com/author/lembergvector

WE ALL LEARN BY FALLING

Pitfalls

Pitfalls

SHOULD YOU KNOW YOURSELF FIRST?

Strategic

- How do you measure the impact of TI on your security posture?
- What is your own maturity, what type of TI can you handle?

Tactical

- What are your requirements?
- Are you aware of TI limitations?

Operational

- Decay time / timeliness
- Accuracy / feedback loop

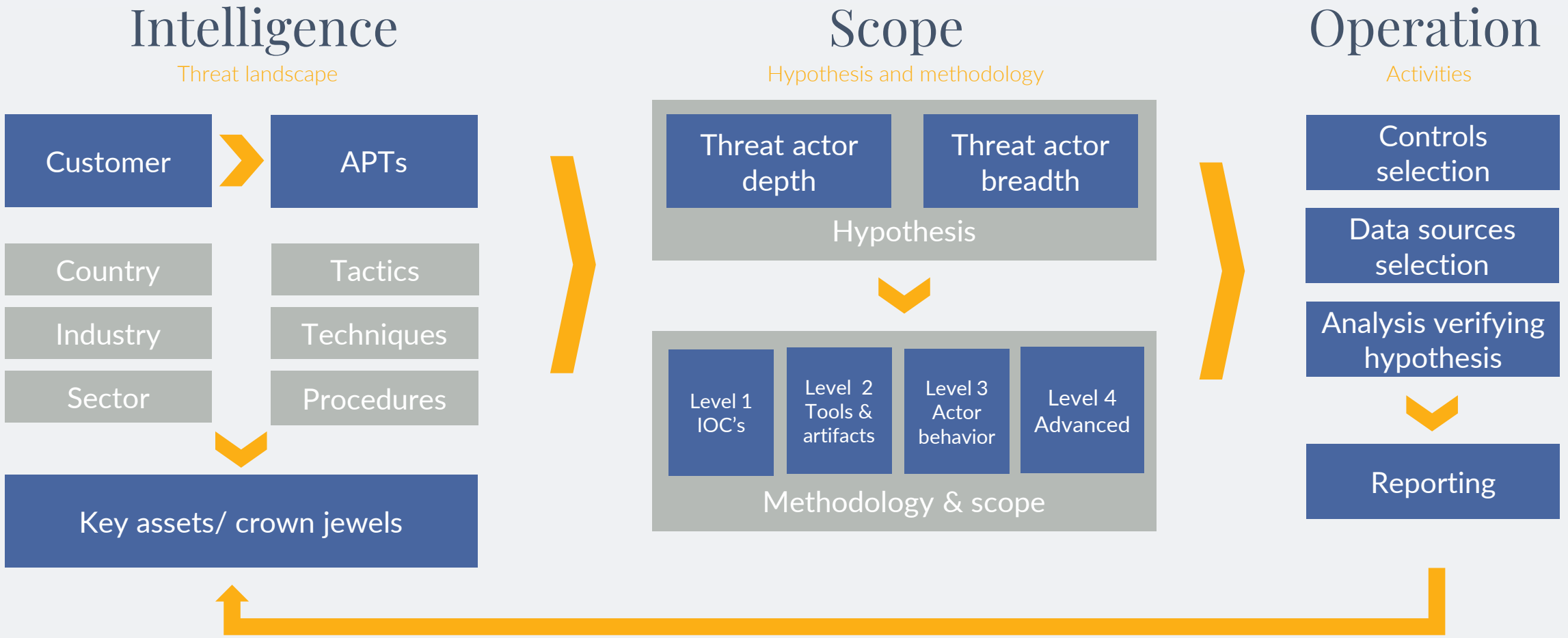
OPERATIONAL POSSIBILITIES

Applying Threat Intelligence

https://www.netsuite.com/portal/resource/articles/inventory-management/manufacturing-operations.shtml

Hunt & Hackett approach

ALIGNING SECURITY CONTROLS & DETECTION WITH THE THREATLANDSCAPE



Offensive

Relevance of threat actor

Relevance of scenario

Understanding of current entity capabilities

Understanding of TI limitations

Execution of scenario

Data generation of scenario

Defensive

Relevance of threat actor

Relevance of business risks

Understanding of current entity capabilities

Understanding of TI limitations

Prioritization of tasks

Data source / control selection

Update of threat understanding

HUNT & HACKETT

OUTSMART YOUR DIGITAL ADVERSARIES

PUBLIC