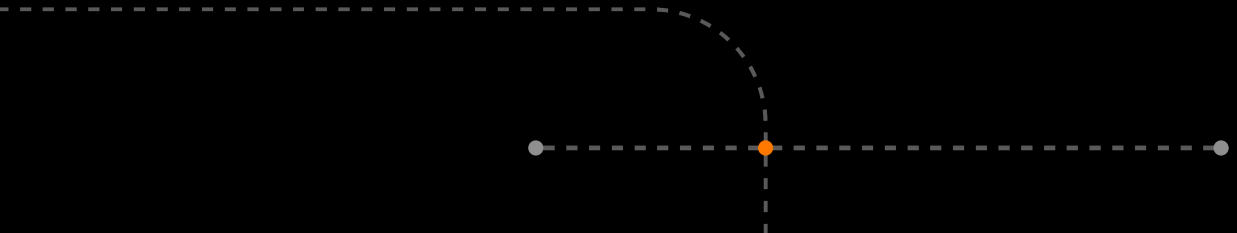
Orange
Cyberdefense

Security Maturity For All Ages

By: Leon Jacobs

Stockholm – October ‘23



orange™

👋 Hello!

Leon Jacobs
CTO Orange Cyberdefense ZA / SensePost

From South Africa 🇿🇦 ☀️
18 years IT, 13 of those in Cyber Security
Previously: Sysadmin, Tier 1 ISP, Private Bank
Open-source developer, researcher, hacker.

In short: I like to hack your stuff :)

@leonjza

SensePost Team - Research Driven Conferences & Contributions

https://sensepost.com/blog/

x : @sensepost
m: @sensepost@infosec.exchange
g : https://github.com/sensepost

Locations of operation

France

90 hackers

South Africa

29 hackers

UK

8 hackers

Belgium

6 hackers

Netherlands

7 hackers

Sweden

5 hackers

Norway

8 hackers

Denmark

2 hackers

Switzerland

21 hackers

EVERYONE HAS A PLAN
TILL THEY GET PUNCHED
IN THE MOUTH.

MIKE TYSON


FIGHT
MONKEY

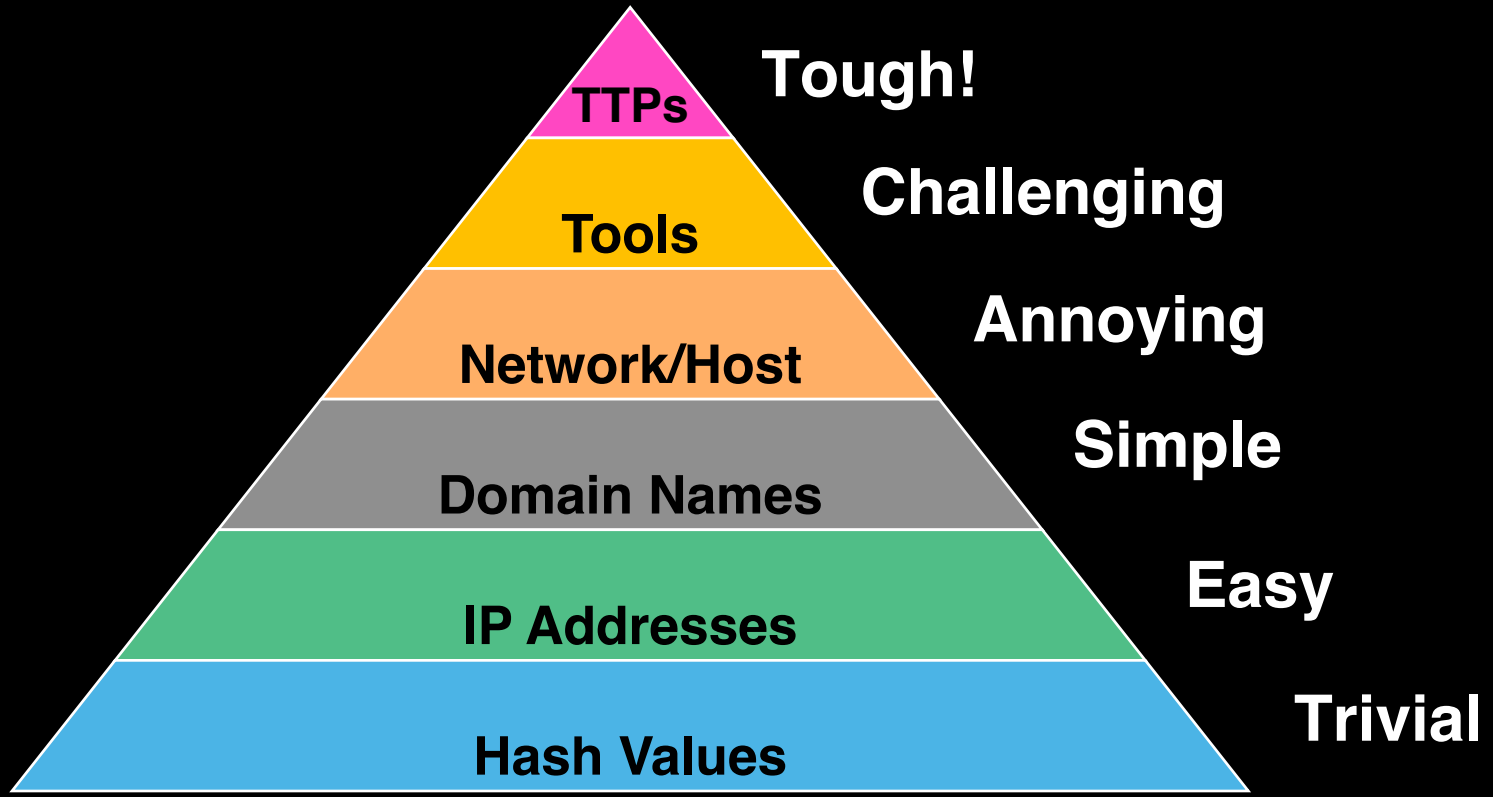
Attackers only need to be right once, defenders need to be right all the time.

Attackers only need to be right once, defenders need to be right all the time.

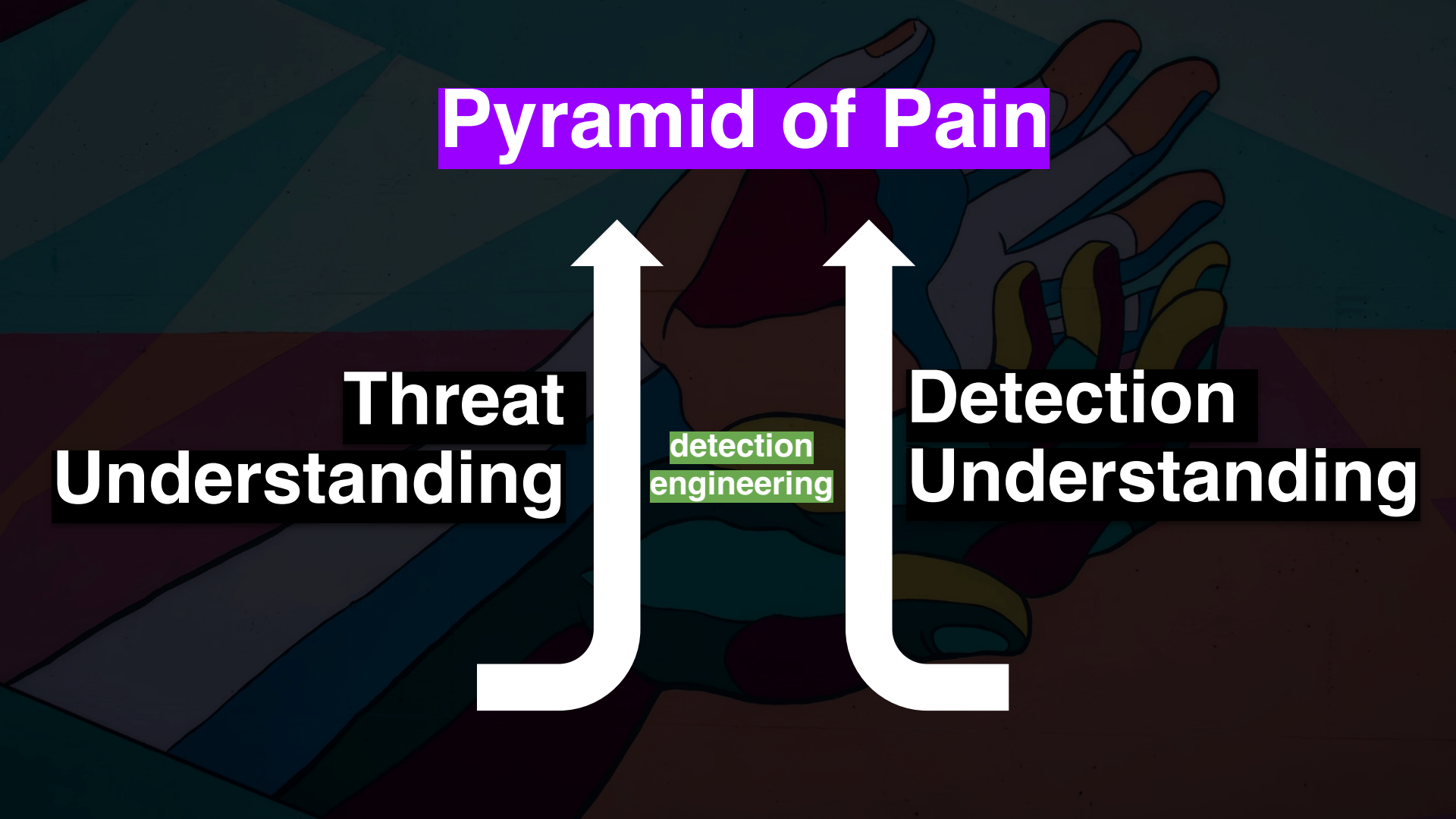
Attackers need to be right every time, defenders need to be right once.

ref: https://attackevals.mitre-engenuity.org/enterprise/turla/

David Bianco's Pyramid of Pain



Pyramid of Pain

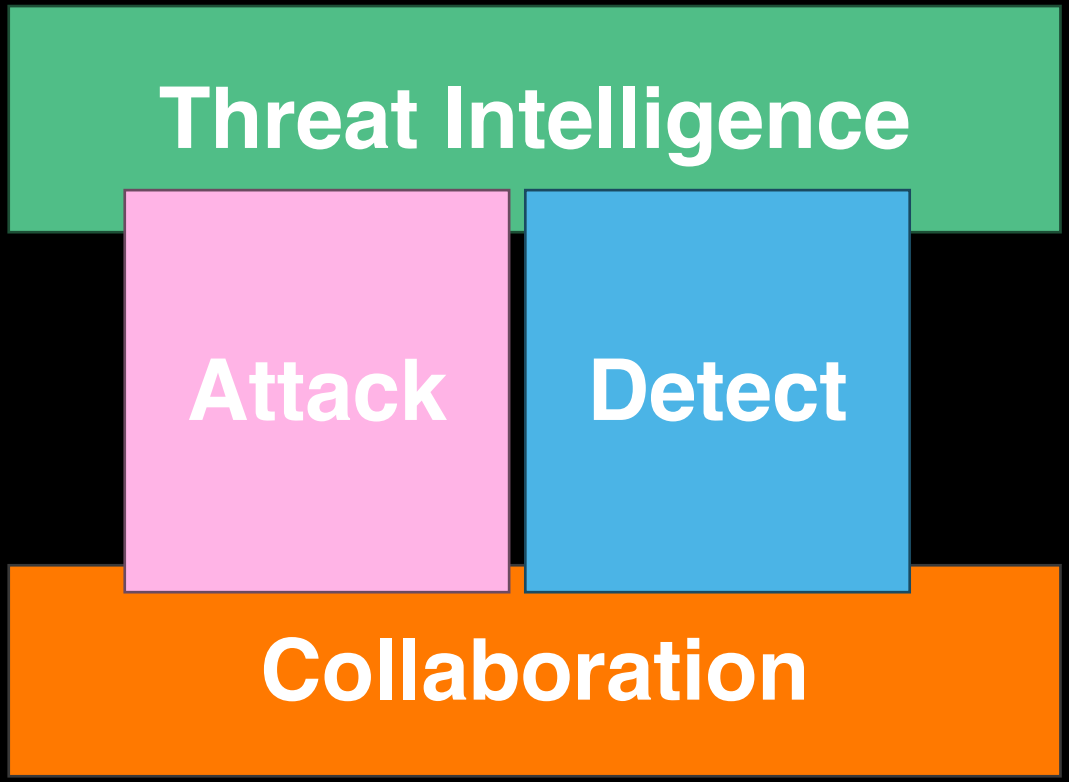


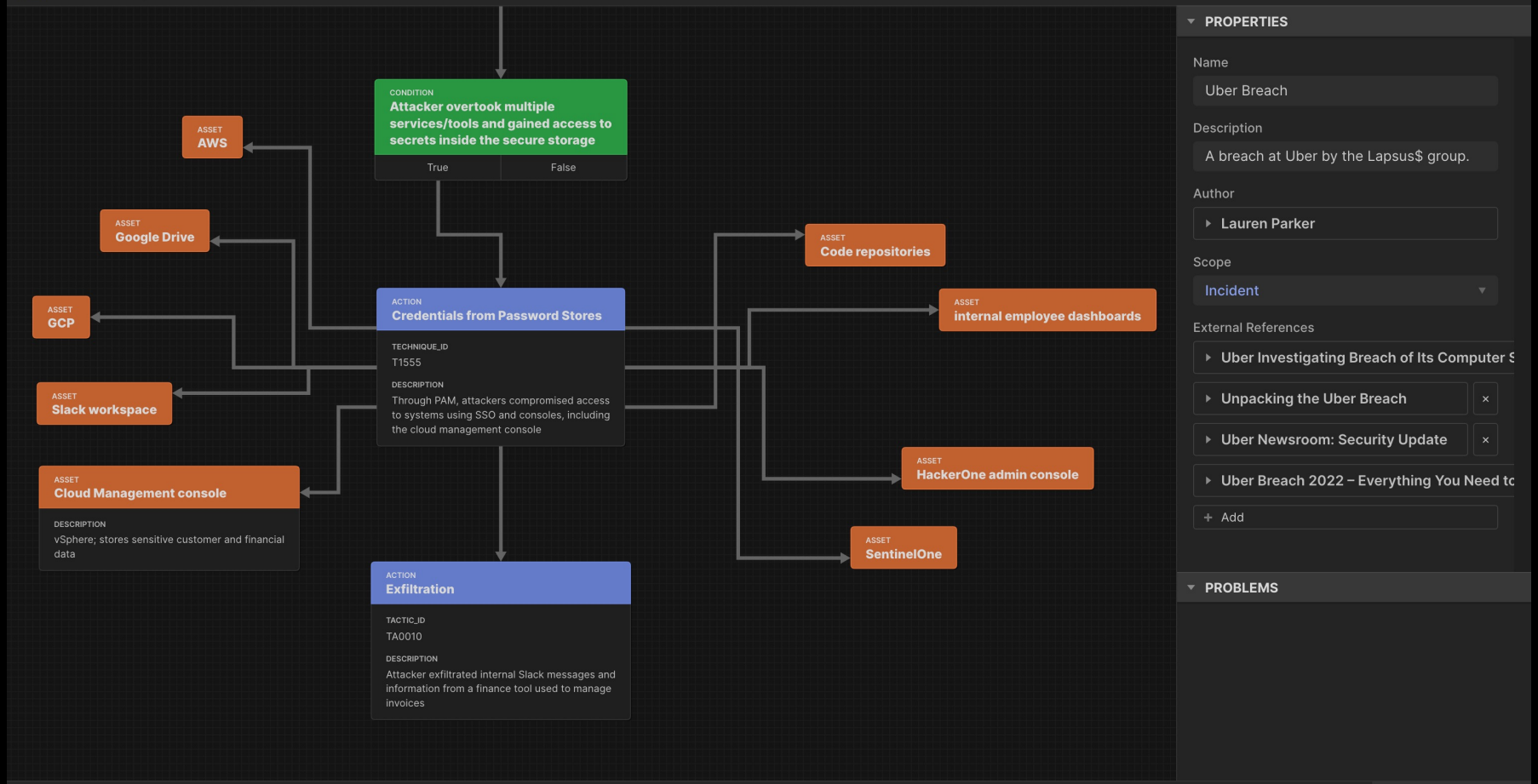

Purple Teaming

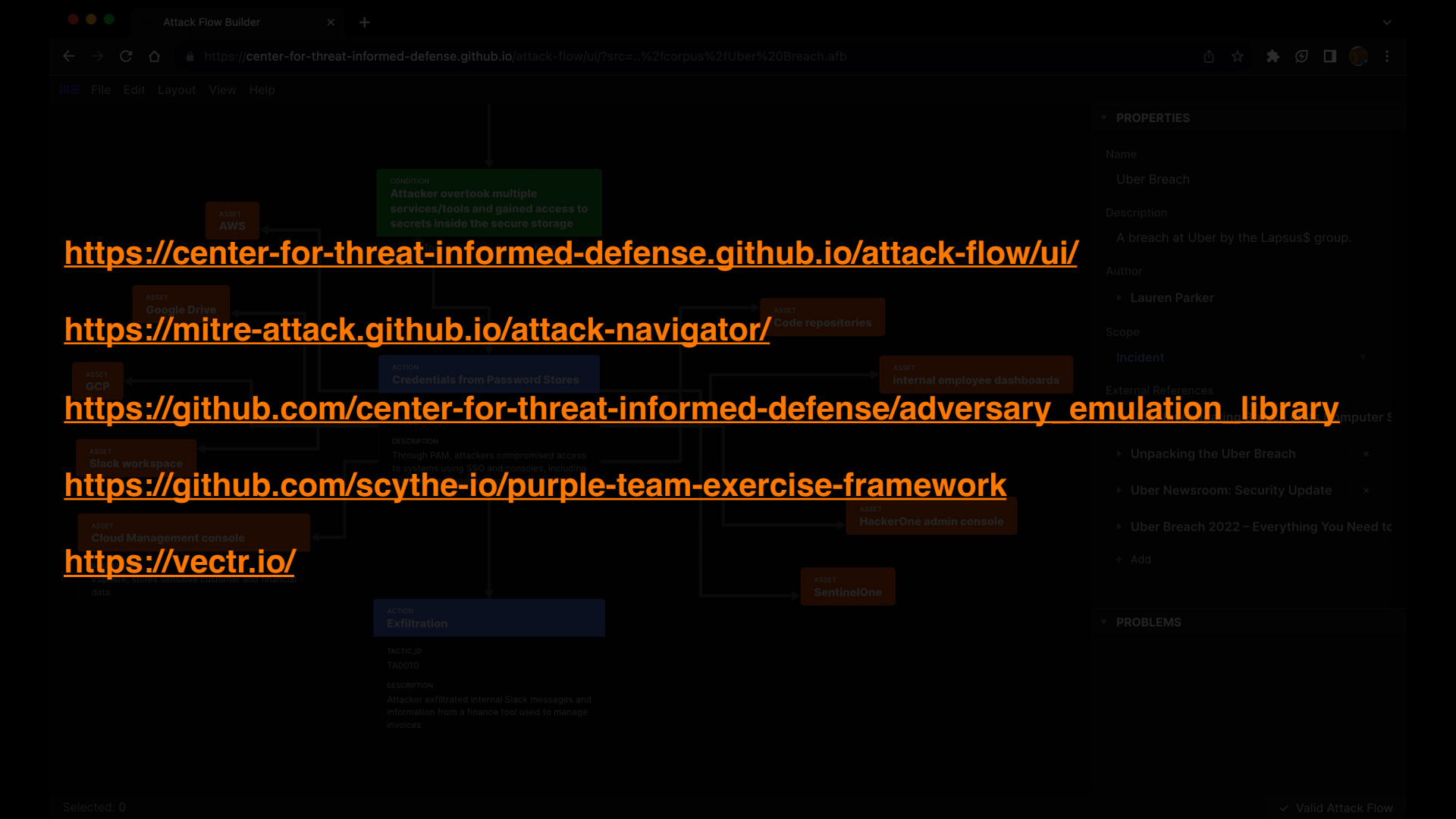
Accept that a vulnerability will be exploited, an attack will be successful and that there will be impact.

Now, test (practice) your ability to accurately detect that entire attack path.

That is purple teaming.


Threat Intelligence
Attack
Detect
Collaboration


Attack Flow Builder
https://center-for-threat-informed-defense.github.io/attack-flow/ui/?src=..%2fcorpus%2fUber%20Breach.afb
File Edit Layout View Help
CONDITION
Attacker overtook multiple services/tools and gained access to secrets inside the secure storage
True
False
ASSET
AWS
ASSET
Google Drive
ASSET
GCP
ASSET
Slack workspace
ACTION
Credentials from Password Stores
TECHNIQUE_ID
T1555
DESCRIPTION
Through PAM, attackers compromised access to systems using SSO and consoles, including the cloud management console
ASSET
Code repositories
ASSET
internal employee dashboards
ASSET
HackerOne admin console
ASSET
SentinelOne
ASSET
Cloud Management console
DESCRIPTION
vSphere; stores sensitive customer and financial data
ACTION
Exfiltration
TACTIC_ID
TA0010
DESCRIPTION
Attacker exfiltrated internal Slack messages and information from a finance tool used to manage invoices
PROPERTIES
Name
Uber Breach
Description
A breach at Uber by the Lapsus$ group.
Author
Lauren Parker
Scope
Incident
External References
Uber Investigating Breach of Its Computer S
Unpacking the Uber Breach
Uber Newsroom: Security Update
Uber Breach 2022 – Everything You Need to
Add
PROBLEMS
Selected: 0
Valid Attack Flow



https://center-for-threat-informed-defense.github.io/attack-flow/ui/

https://mitre-attack.github.io/attack-navigator/

https://github.com/center-for-threat-informed-defense/adversary_emulation_library

https://github.com/scythe-io/purple-team-exercise-framework

https://vectr.io/

Help your team turn response into instinct.

Orange
Cyberdefense

Thank You

Leon Jacobs

e: leon@orangecyberdefense.com

x: @leonjza m: @leonjza@infosec.exchange

orangecyberdefense.com

orange™