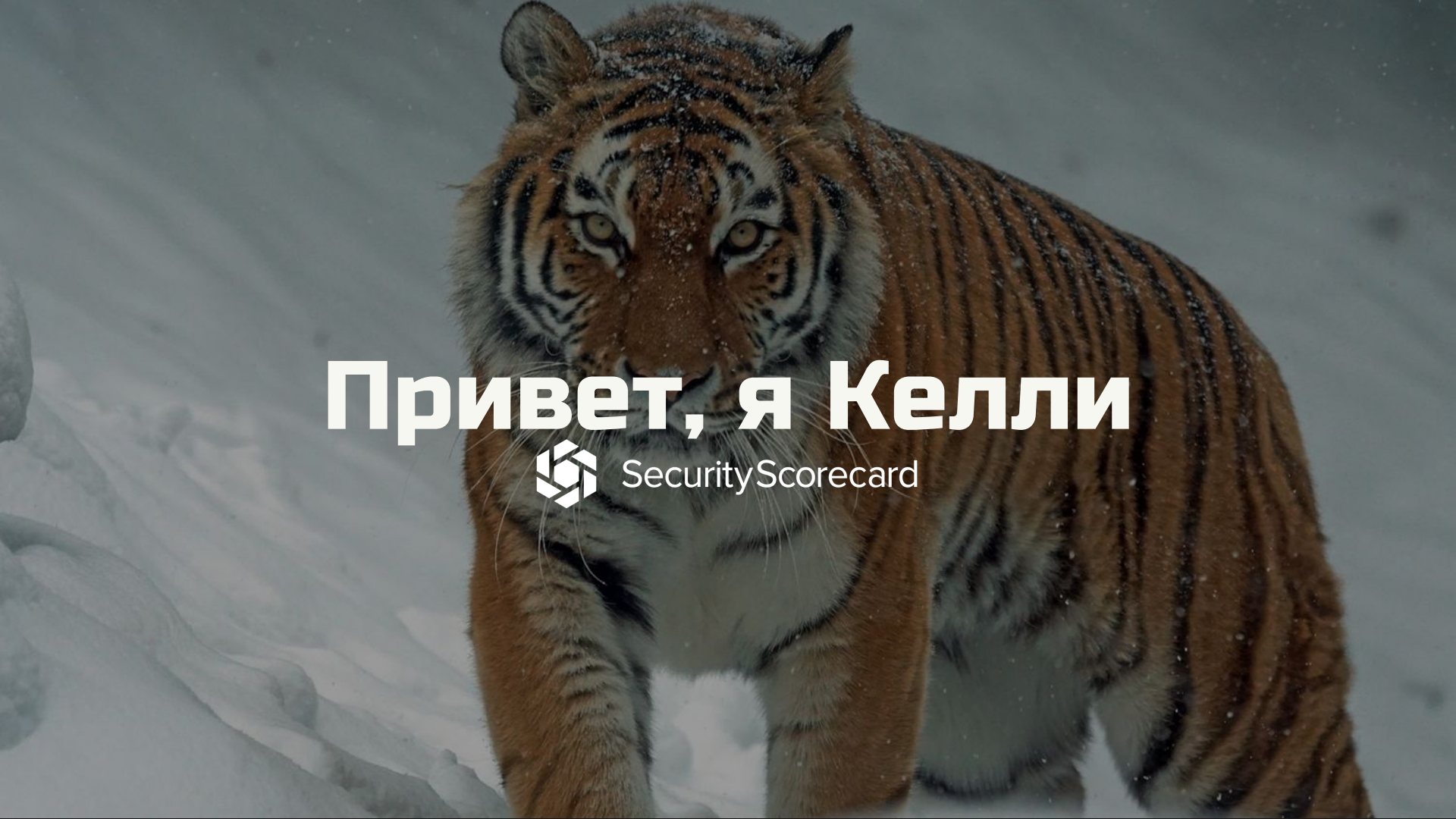
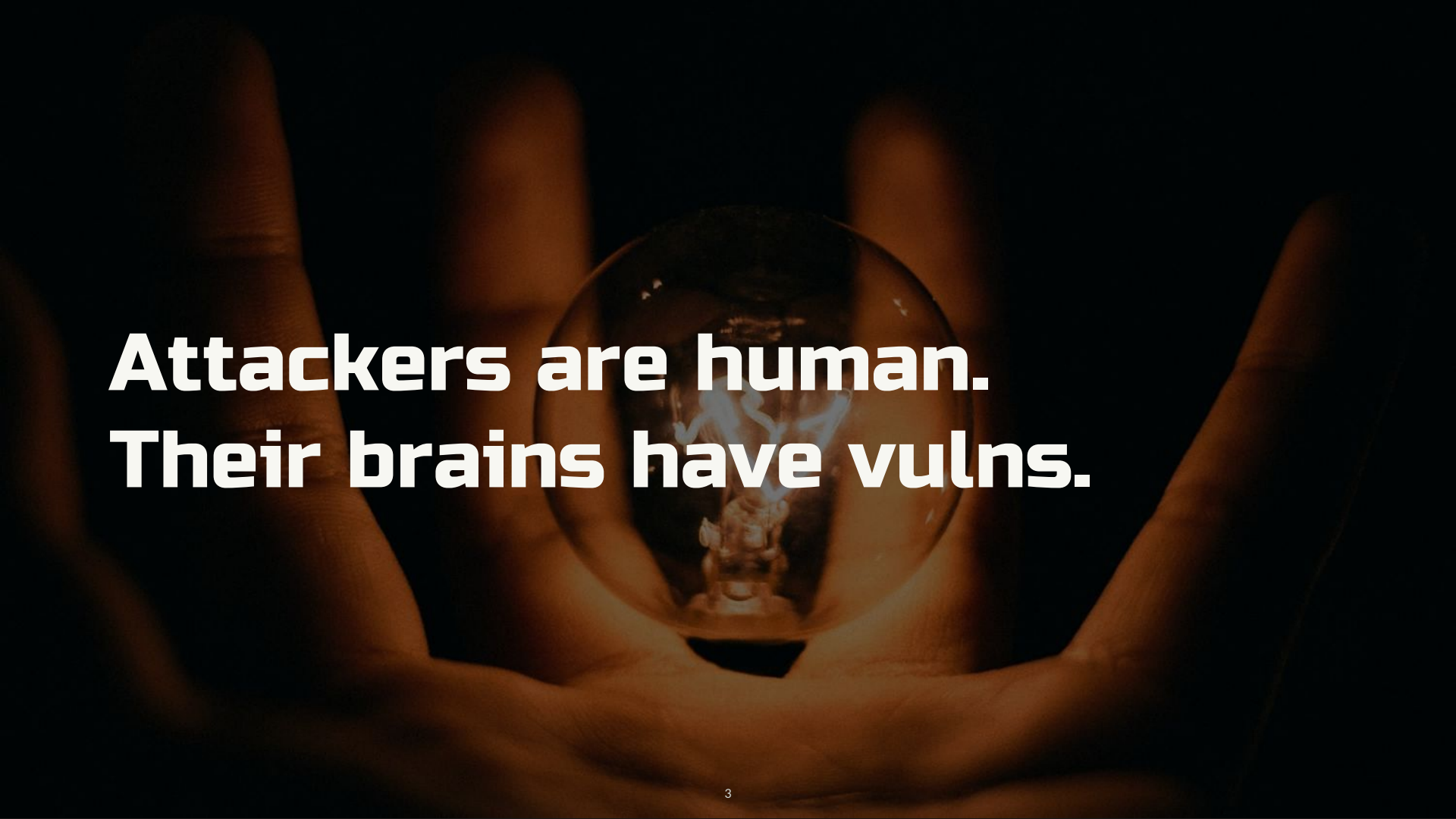
Defensive Exploitation

How to Pwn Your Attacker's Decision-making

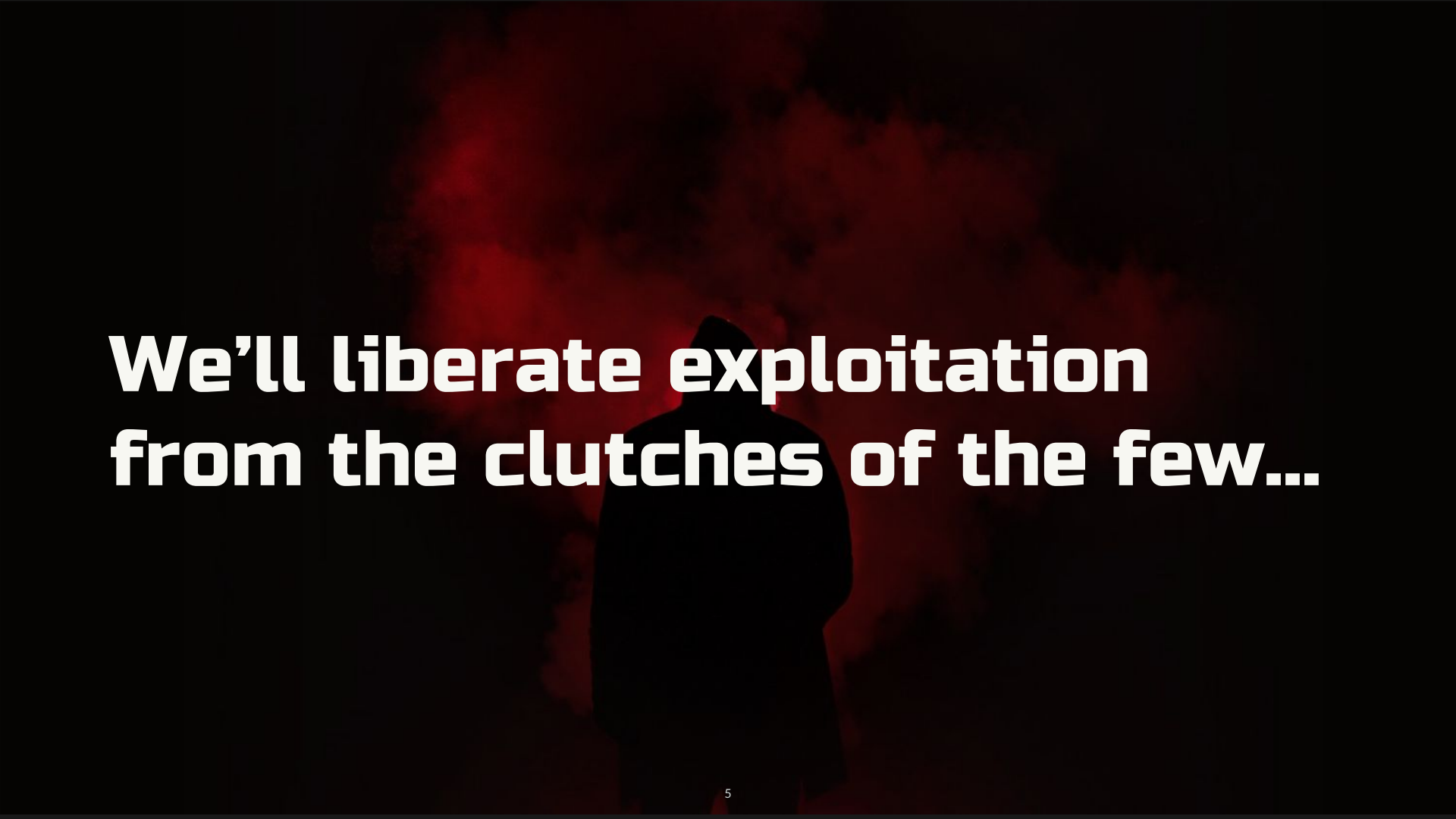
Kelly Shortridge (@swagitda_)

ZeroNights 2017


Привет, я Келли
SecurityScorecard


Attackers are human.
Their brains have vulns.

Today you'll learn how to exploit these vulns for defense


We’ll liberate exploitation
from the clutches of the few...


...into the hands of the many


How do humans think?
Tachina Lee

People predict their opponent’s moves by either “**thinking**” or “**learning**”

Thinking = modeling how opponents are likely to respond

Our brains work like volatile memory

Learning = predicting how players will act based on prior games / rounds

Humans learn through “error-reinforcement learning” (trial & error)

“**Learning rates**” = how much experiences factor into one’s decisions

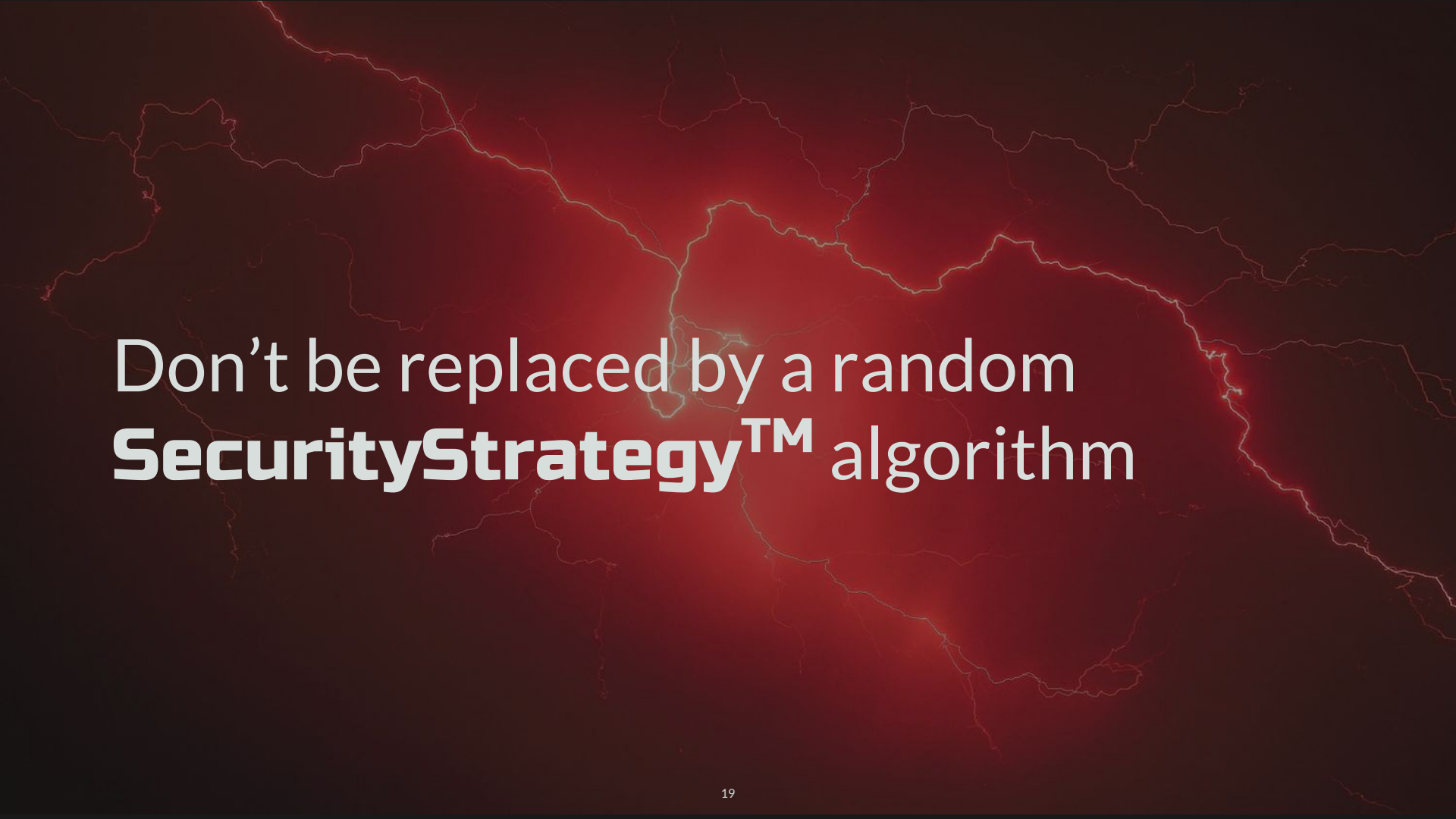
Veksler & Buchler case study:
200 “security games” to test the # of prevented attacks across 4 strategies

Fixed strategy: 10% - 25% of attacks prevented

Game Theory strategy: 50% of attacks prevented

Random strategy: 49.6% of attacks prevented

Cognitive Modelling strategy: 61% - 77% of attacks prevented


Don’t be replaced by a random
SecurityStrategy™ algorithm

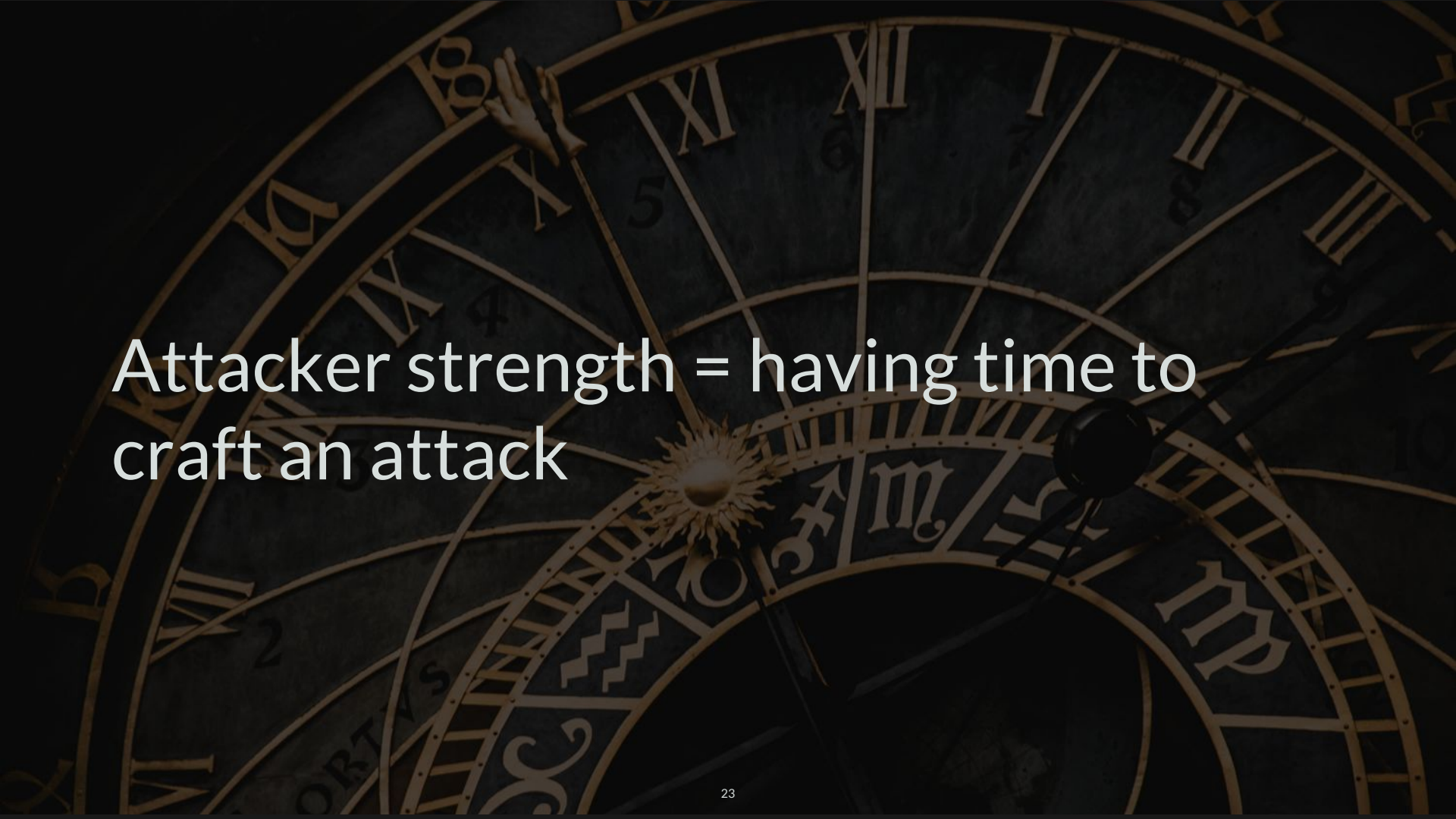

How to Pwn Attackers

Perceptual SWOT Analysis

Scott Webb

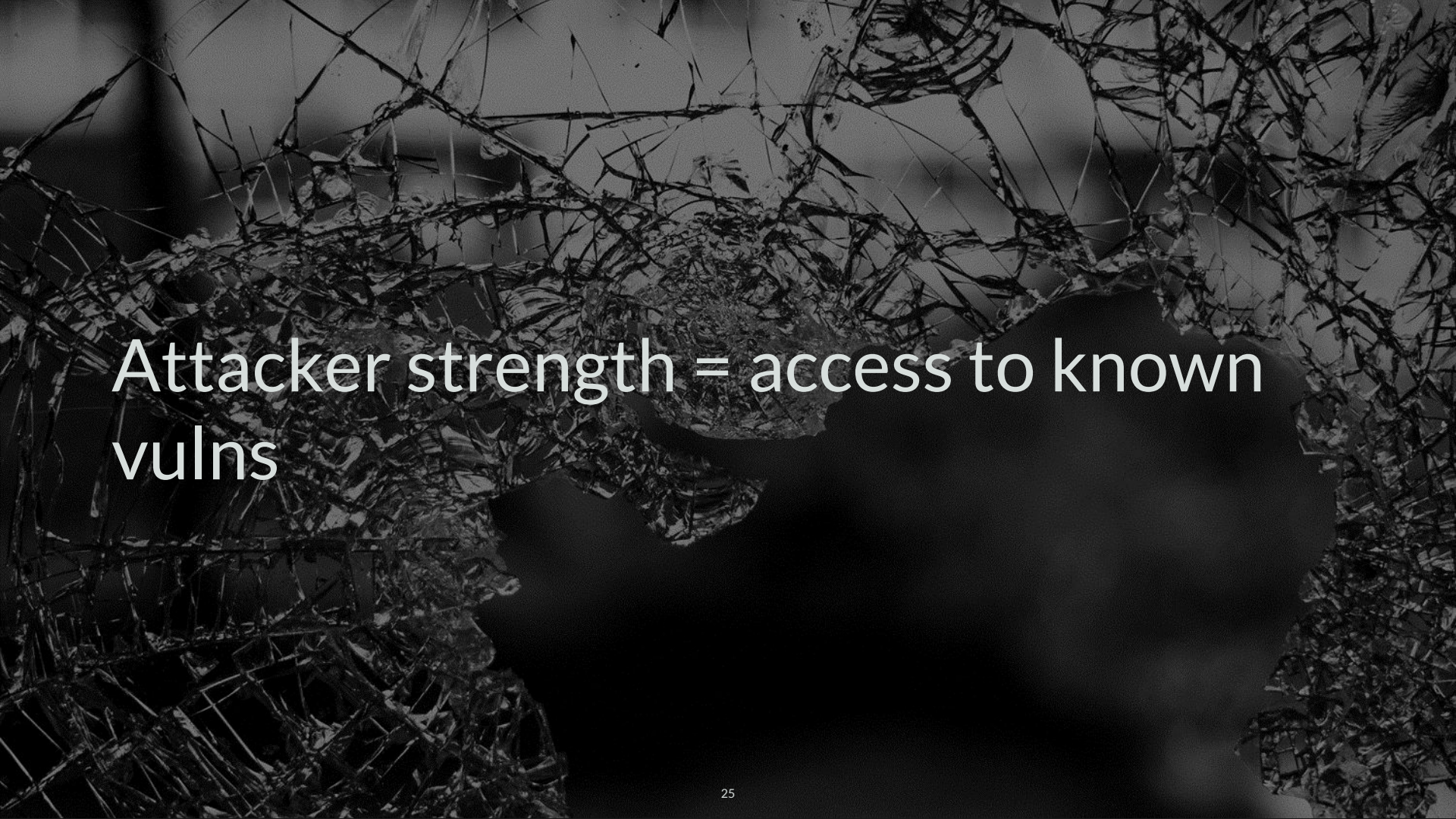
How can strengths be weaknesses?

How can weaknesses be strengths?



Attacker strength = having time to craft an attack


Leverage that “strength” with
strategies leading down rabbit holes


Attacker strength = access to known vulns

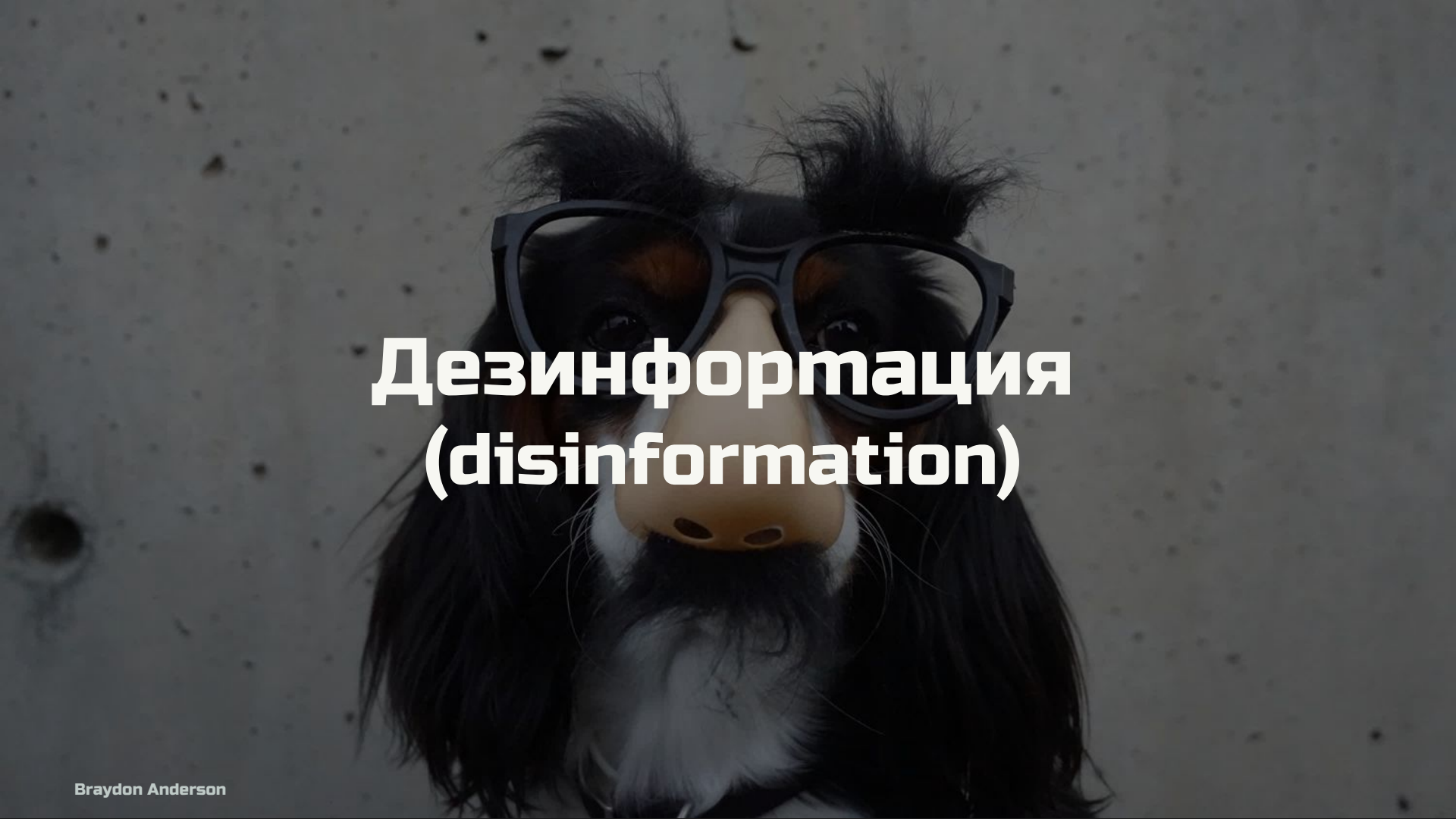

Confuse them with fake architecture
for uncertainty around your systems


Learning Exploitation

Info asymmetry exploitation:
Disrupt the attacker’s learning process

Learning rate exploitation:
Introduce unreliability and pre-empt attacker moves

Exploit the fact that
you understand the local environment
better than attackers


Дезинформация
(disinformation)
Braydon Anderson

Defenders have information their adversaries need to intercept

Hide or falsify data on the legitimate system side

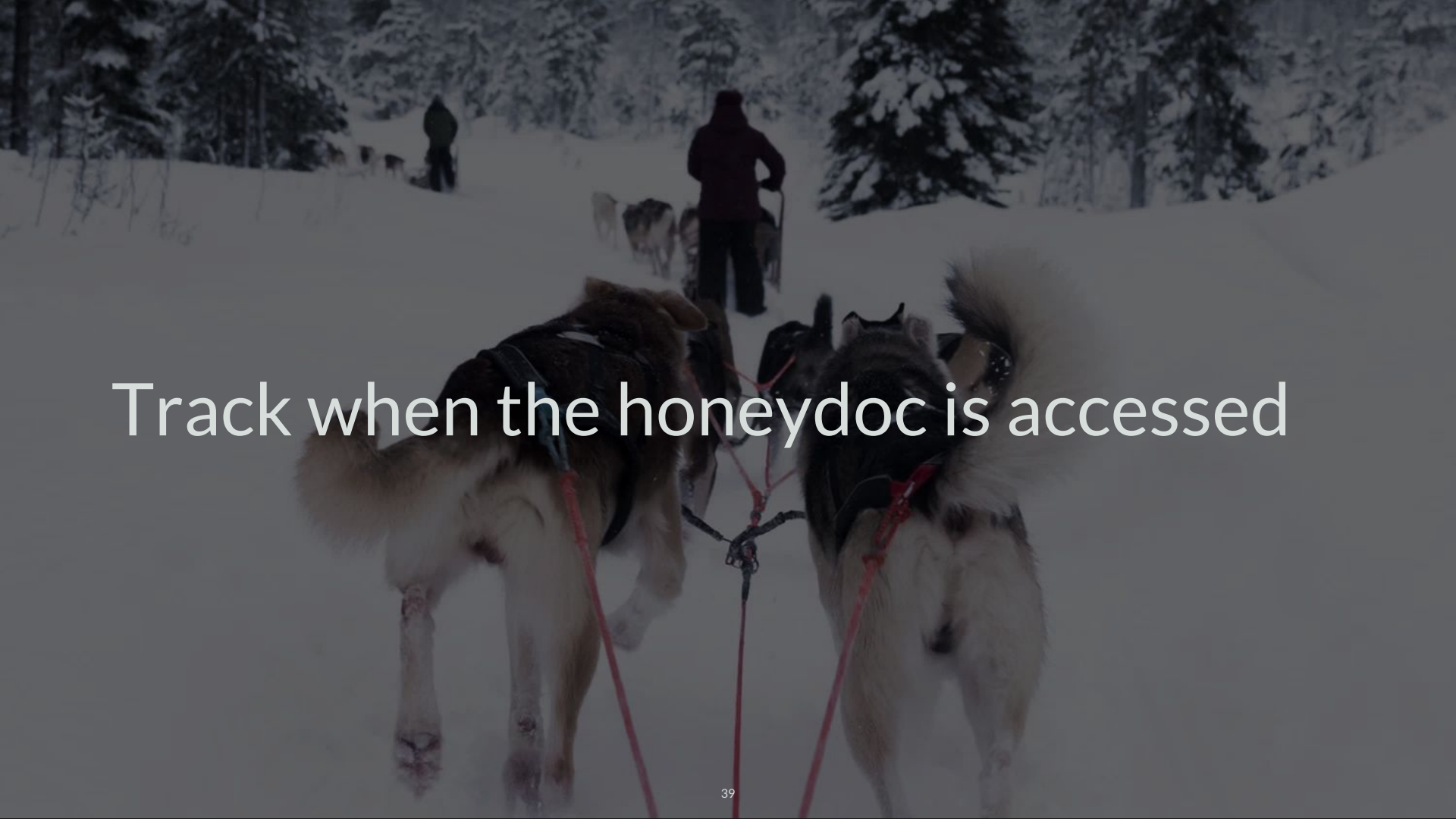
Remove the attacker's scientific method so they can't test hypotheses

Create honeytokens that look legit & would be useful in attacker recon

Example: Create custom email rejection messages

Then, create a honeydoc for violation of the “Rivia Policy”

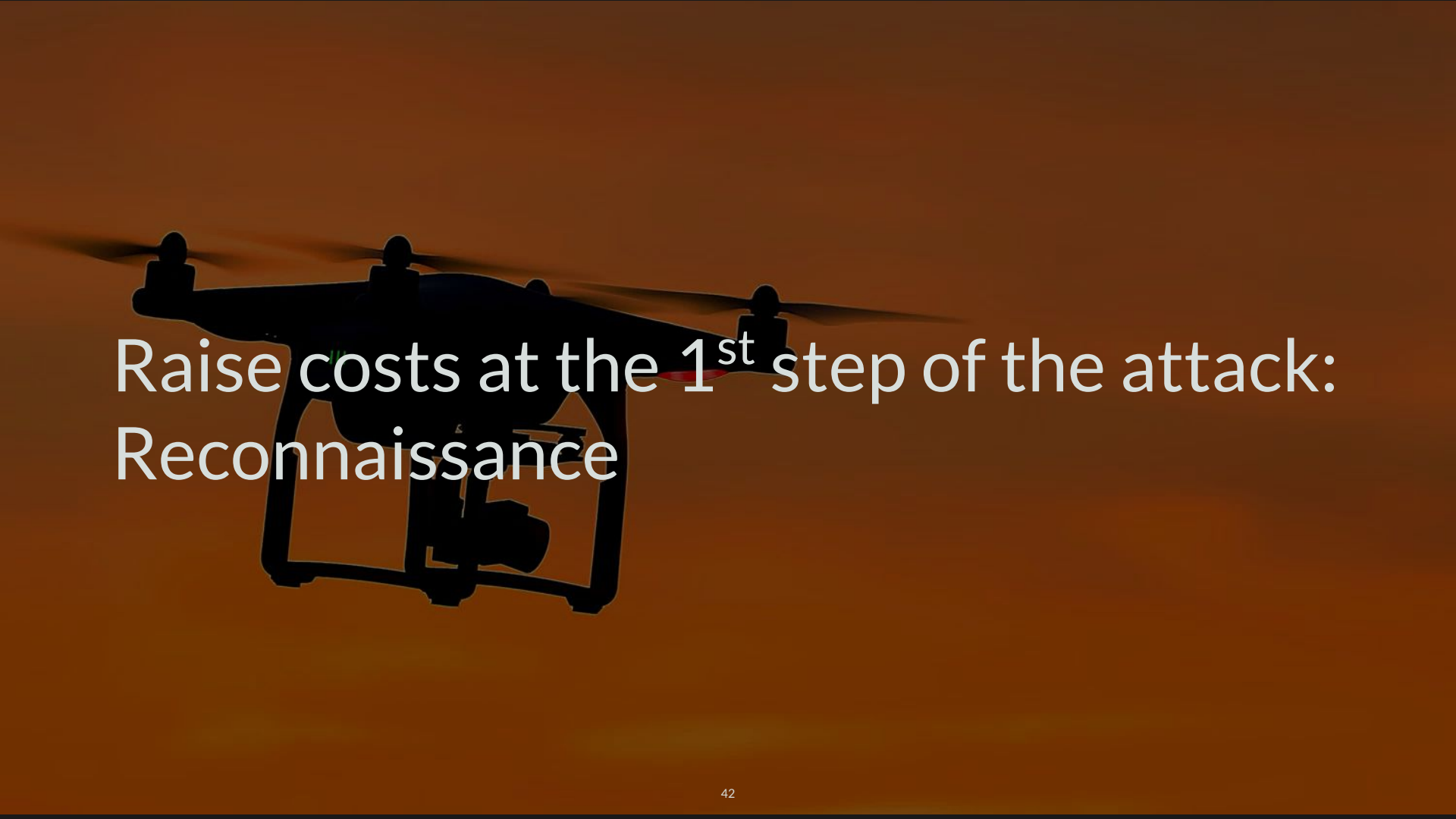
Respond to suspicious emails with, “You’ve violated the Rivia policy 21a”



Track when the honeydoc is accessed


Маскировка
(deception)
Candice Seplow

Non-determinism: different behaviors at different times



Raise costs at the 1st step of the attack: Reconnaissance

Make the attacker uncertain of your defensive profile and environment

Attackers now design malware to be VM-aware

Good: Make everything look like a malware analyst's sandbox

Better: Look like a different malware analyst's sandbox each time


Put wolfskins on the sheep

Mix & match superficially sketchy-looking artifacts on normal systems

Emulate virtual artifacts onto physical machines

https://github.com/fr0gger/RocProtect-V1

VMwareServices.exe
VBoxService.exe
Vmwaretray.exe
VMSrvc.exe
vboxtray.exe
ollydbg.exe
wireshark.exe
fiddler.exe

\\\\.\\pipe\\cuckoo
cuckoomon.dll
dbghelp.dll

Mac addresses:
"00:0C:29", "00:1C:14",
"00:50:56", "00:05:69"

system32\drivers\VBoxGuest.sys
system32\drivers\VBoxMouse.sys

HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions

C:\cuckoo, C:\IDA
Program Files\Vmware

Make the IsDebuggerPresent function call always return non-zero

Create fake versions of driver objects like \\.\NTICE and \\.\SyserDbgMsg

Set KdDebuggerEnabled to 0x03

Load DLLs from AV engines using a Windows loader with a forwarder DLL

ex64.sys (Symantec)
McAVSCV.DLL (McAfee)
SAUConfigDLL.dll (Sophos)
cbk7.sys (Carbon Black)
cymemdef.dll (Cylance)
CSAgent.sys (Crowdstrike)

Deploy lightest weight hypervisor possible for added “wolfskin”

https://github.com/asamy/ksm
https://github.com/ionescu007/SimpleVisor
https://github.com/Bareflank/hypervisor

Conclusion

Start with a perceptive SWOT analysis to gain perspective

Use info asymmetry & learning rate exploitation to beleaguer your adversaries

Дезинформация и маскировка

Worst case, random strategies are just as good as game theory


Клин клином вышибают
(fight fire with fire)

@swagitda_

/in/kellyshortridge

kelly@greywire.net

Suggested reading

- “Know Your Enemy: Applying Cognitive Modeling in the Security Domain,” Veksler, Buchler
- “Know Your Adversary: Insights for a Better Adversarial Behavioral Model,” Abbasi, et al.
- “Deterrence and Risk Preferences in Sequential Attacker–Defender Games with Continuous Efforts,” Payappalli, Zhuang, Jose
- “Improving Learning and Adaptation in Security Games by Exploiting Information Asymmetry,” He, Dai, Ning
- “Behavioral theories and the neurophysiology of reward,” Schultz
- “Evolutionary Security,” and “Measuring Security,” Dan Geer