

ACTIVE DECEPTION FOR Red & Blue Teams

Sudarshan Pisupati
Principal Consultant - Smokescreen
[@sudartion](https://twitter.com/sudartion)

Sahir Hidayatullah
CEO - Smokescreen
[@sahirh](https://twitter.com/sahirh)



“The more you know about the past,
the better prepared you are for the future.”

Theodore Roosevelt



“Gauge your opponent’s mind
and send it in different directions.
Make him think various things,
and wonder if you will be slow
or quick.”

Miyamoto Musashi
The Book of Five Rings





“Never win by force
what can be won
with deception”

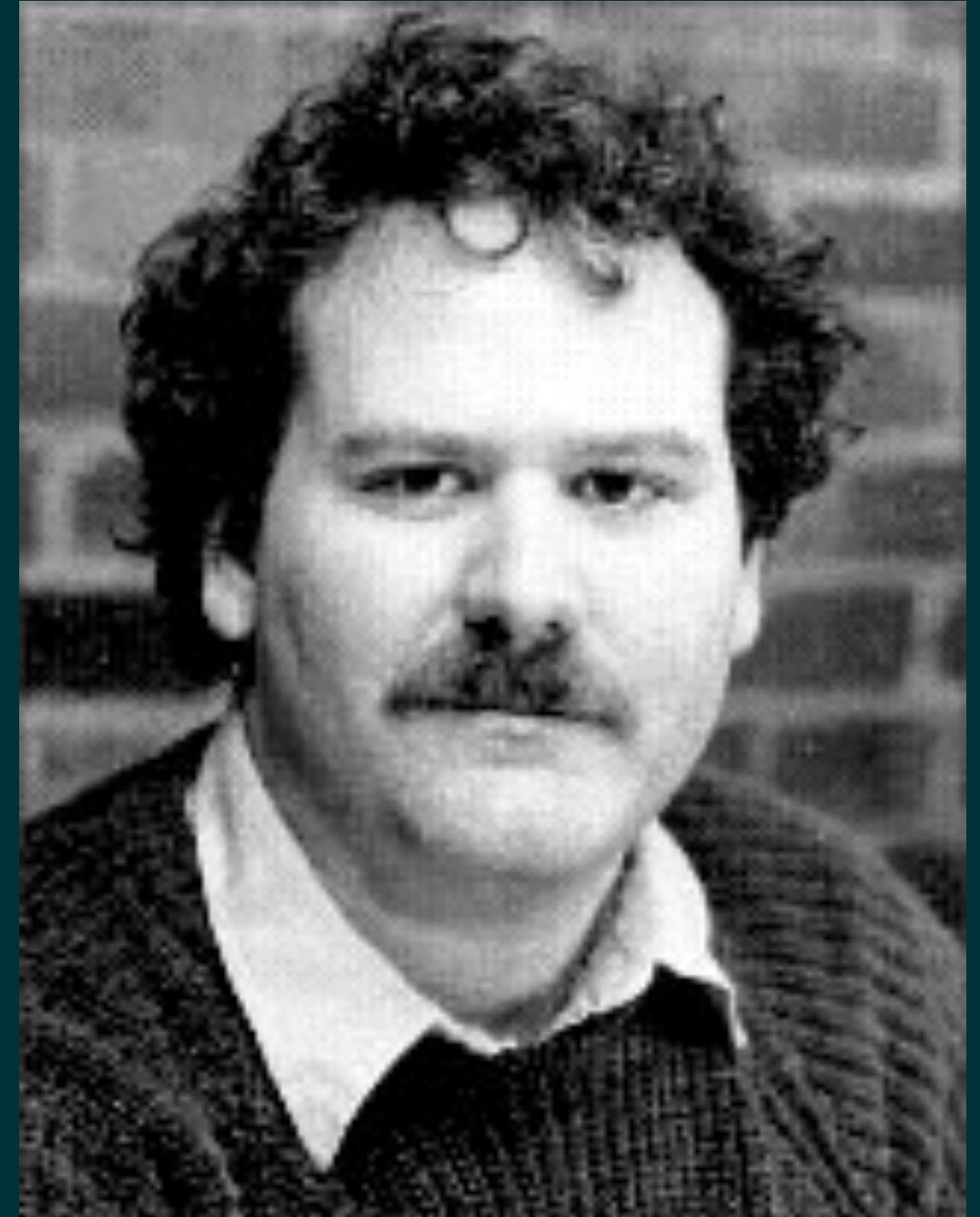
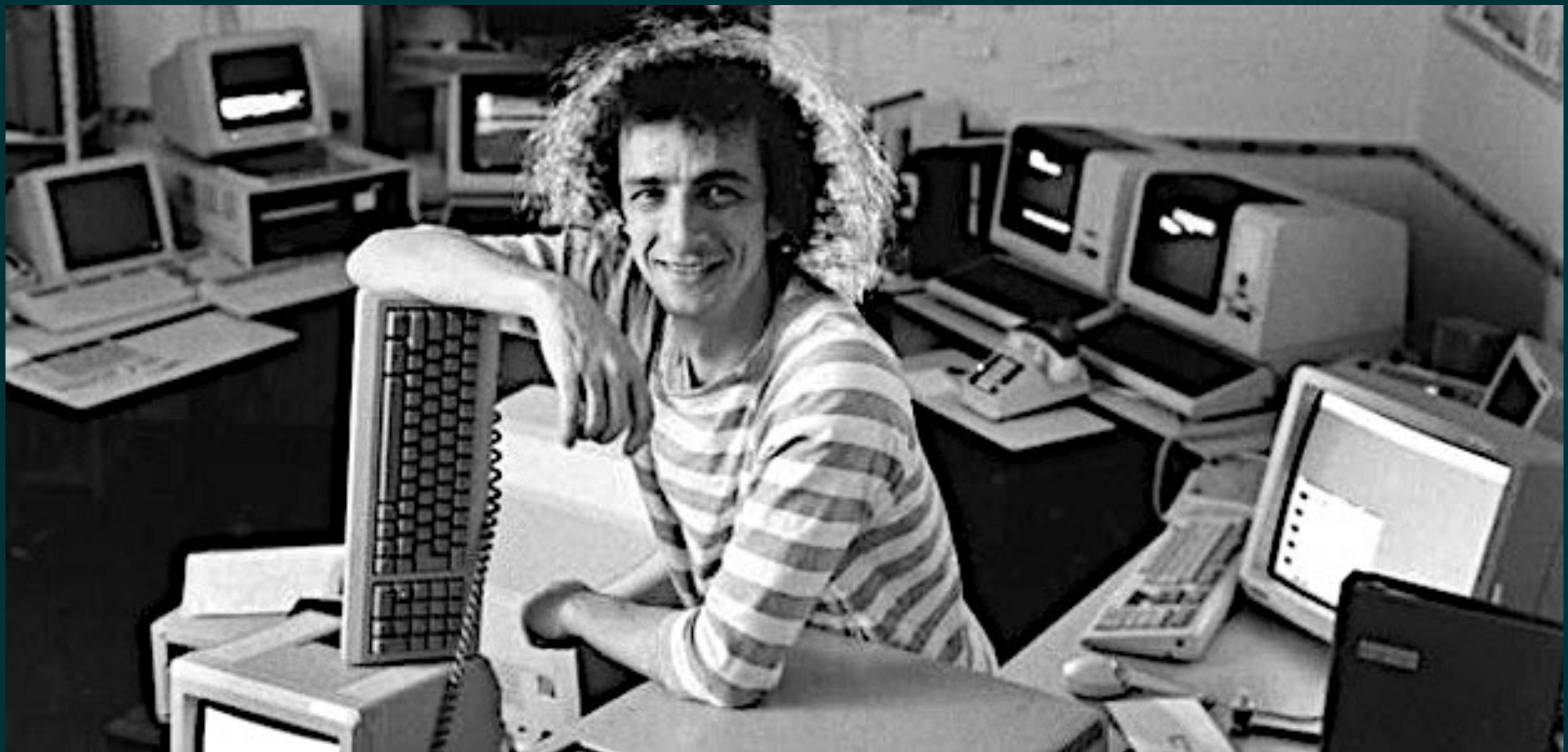
Niccolò Machiavelli,
The Discourses (paraphrased)

“Never interrupt your enemy when he's making a mistake.”

Napoléon Bonaparte





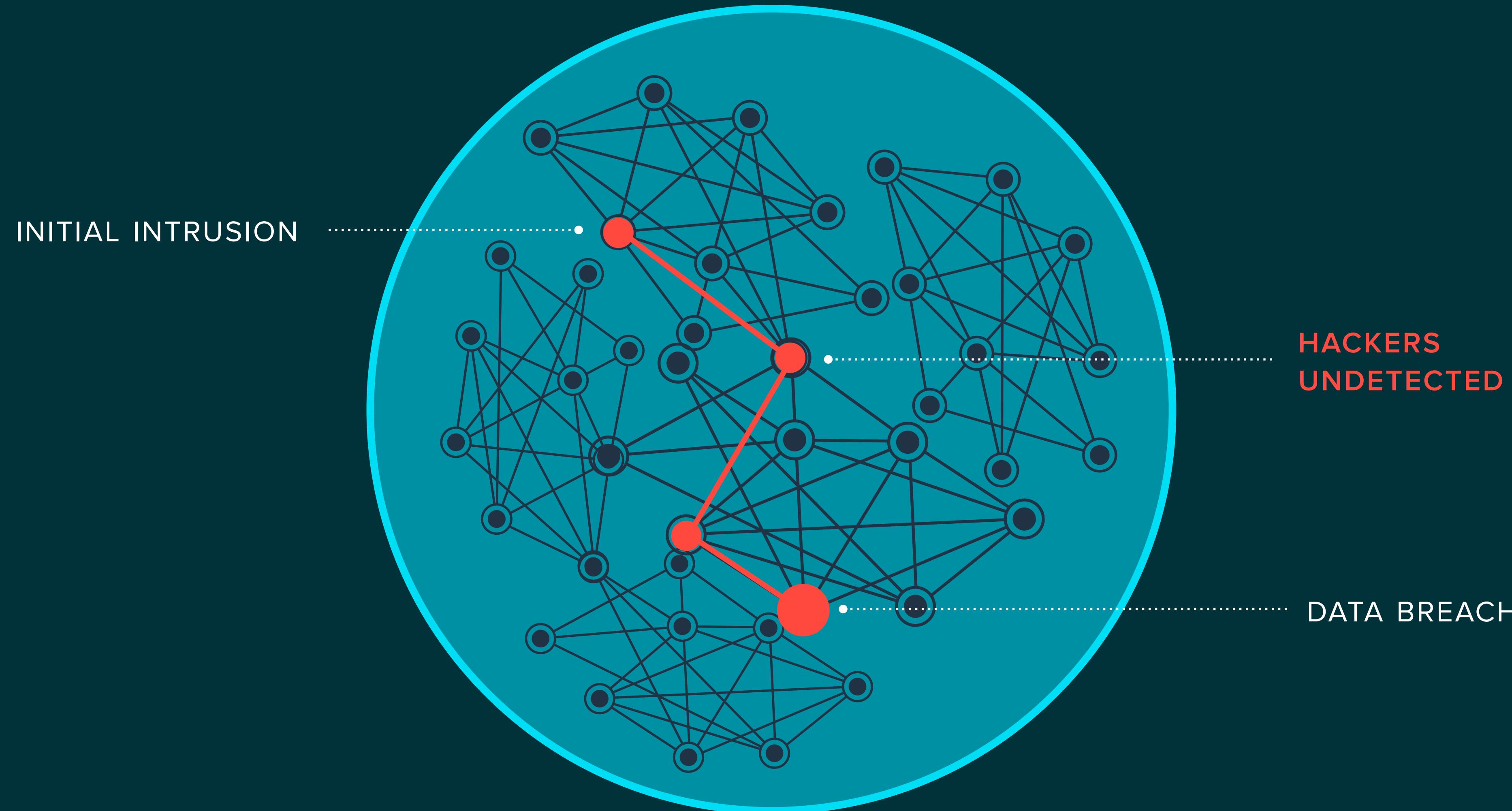


There are 3 reasons
why companies get hacked...



1

Low visibility



2 Ever changing threat landscape



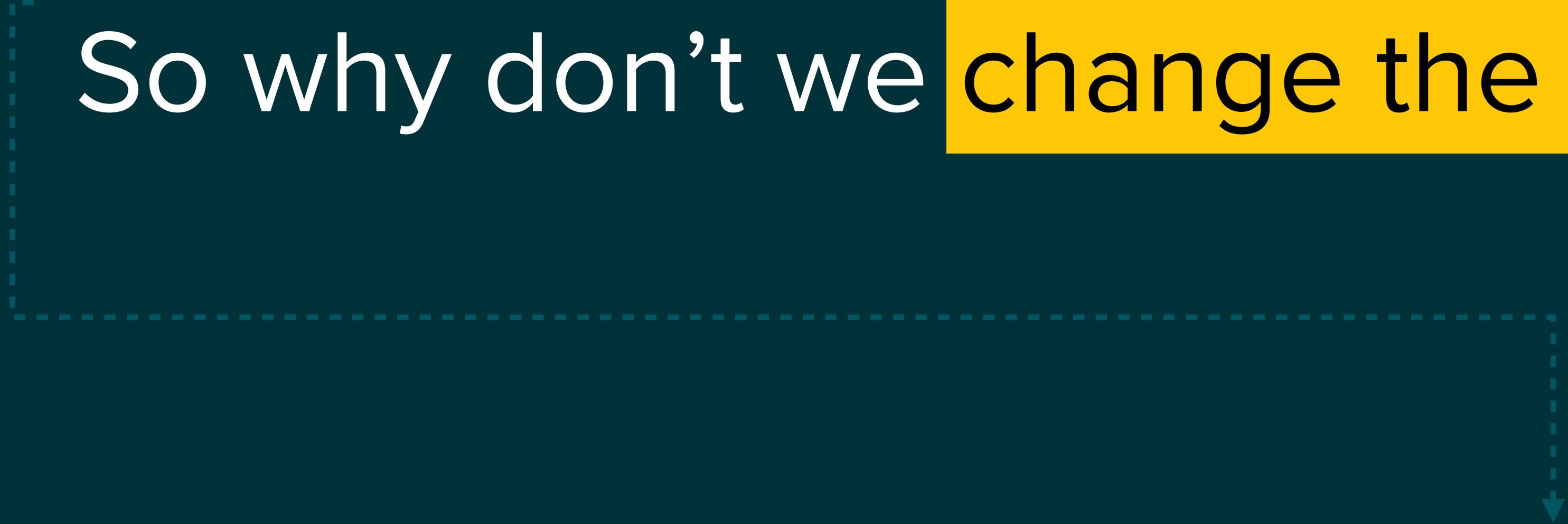
3 Too many false positives



- Event fatigue
- Data paralysis
- Missed alerts
- **Game Over**

We're losing.

So why don't we **change the game?**



Human psychology is an attacker's greatest weapon.

It's also their **greatest weakness**.

Deception Benefits

No false positives

High attacker impact

Focused on intent, not tools



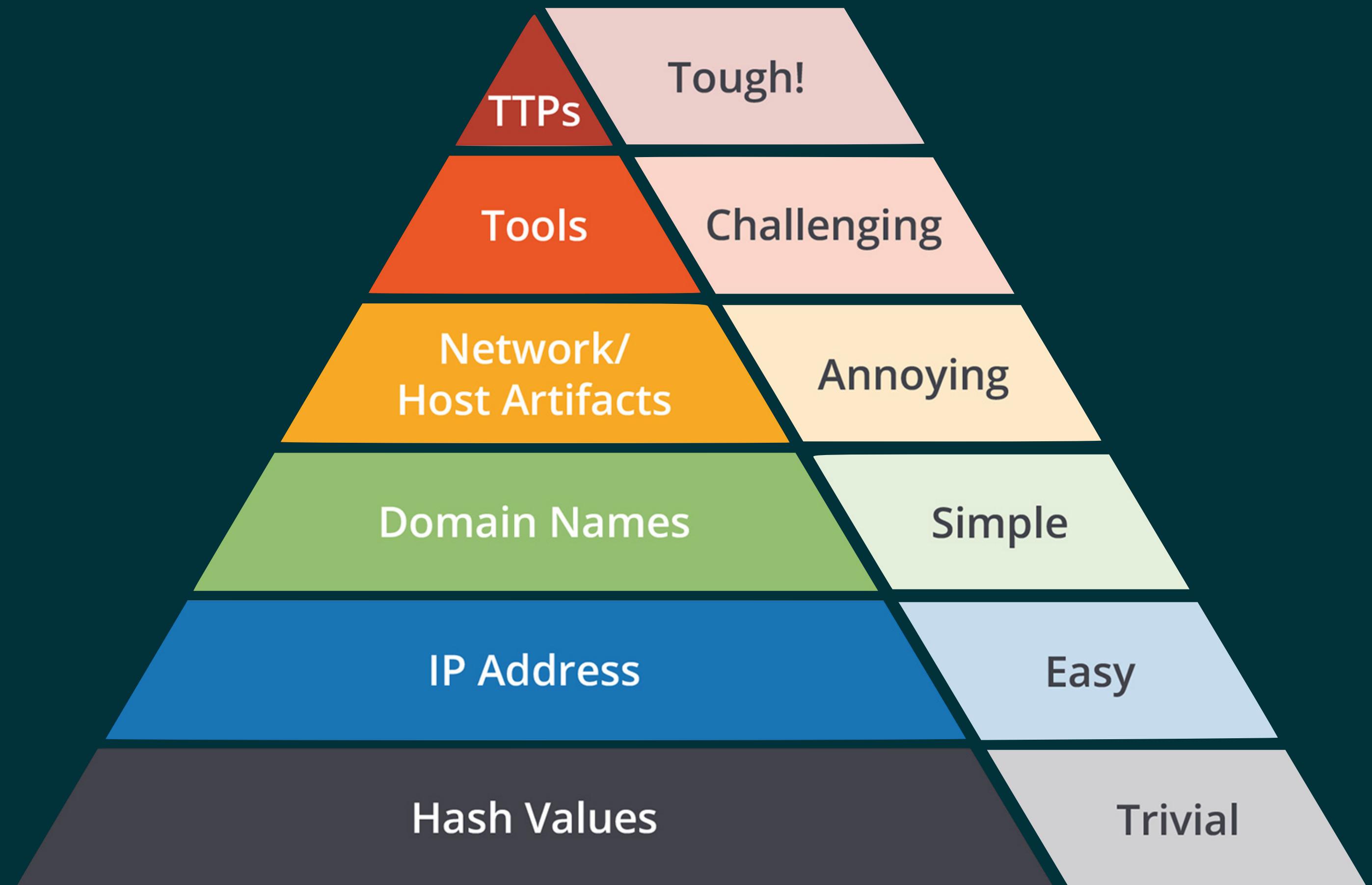
Deception Benefits

No false positives

High attacker impact

Focused on intent, not tools

The Pyramid of Pain



Source: David J. Bianco, personal blog

Deception Benefits

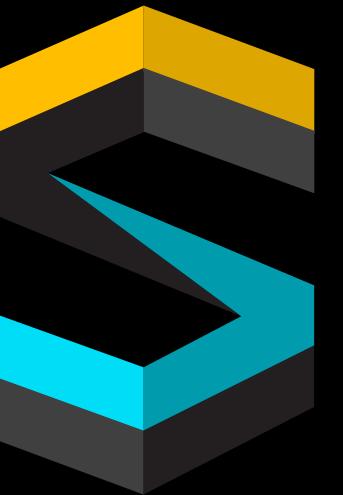
No false positives

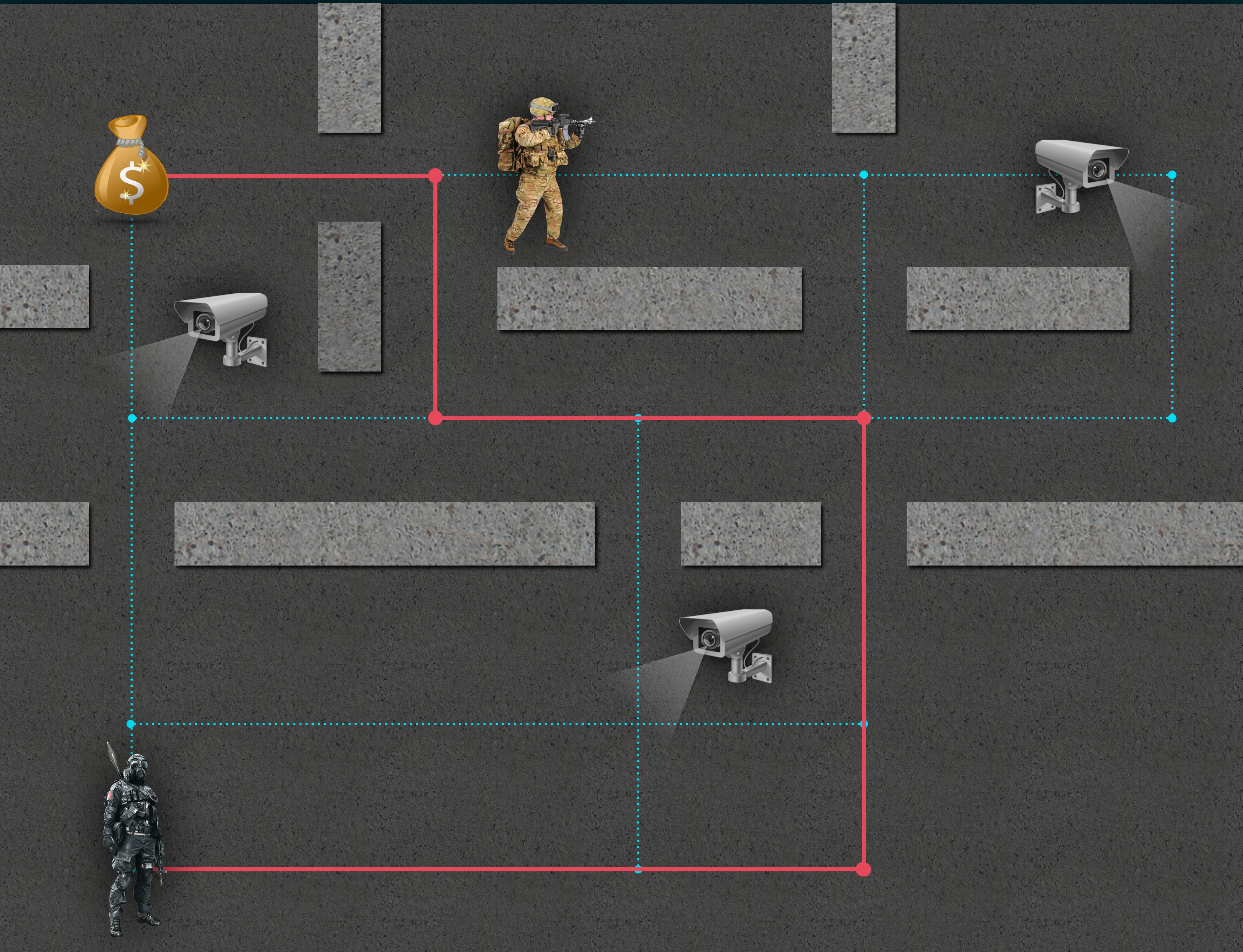
High attacker impact

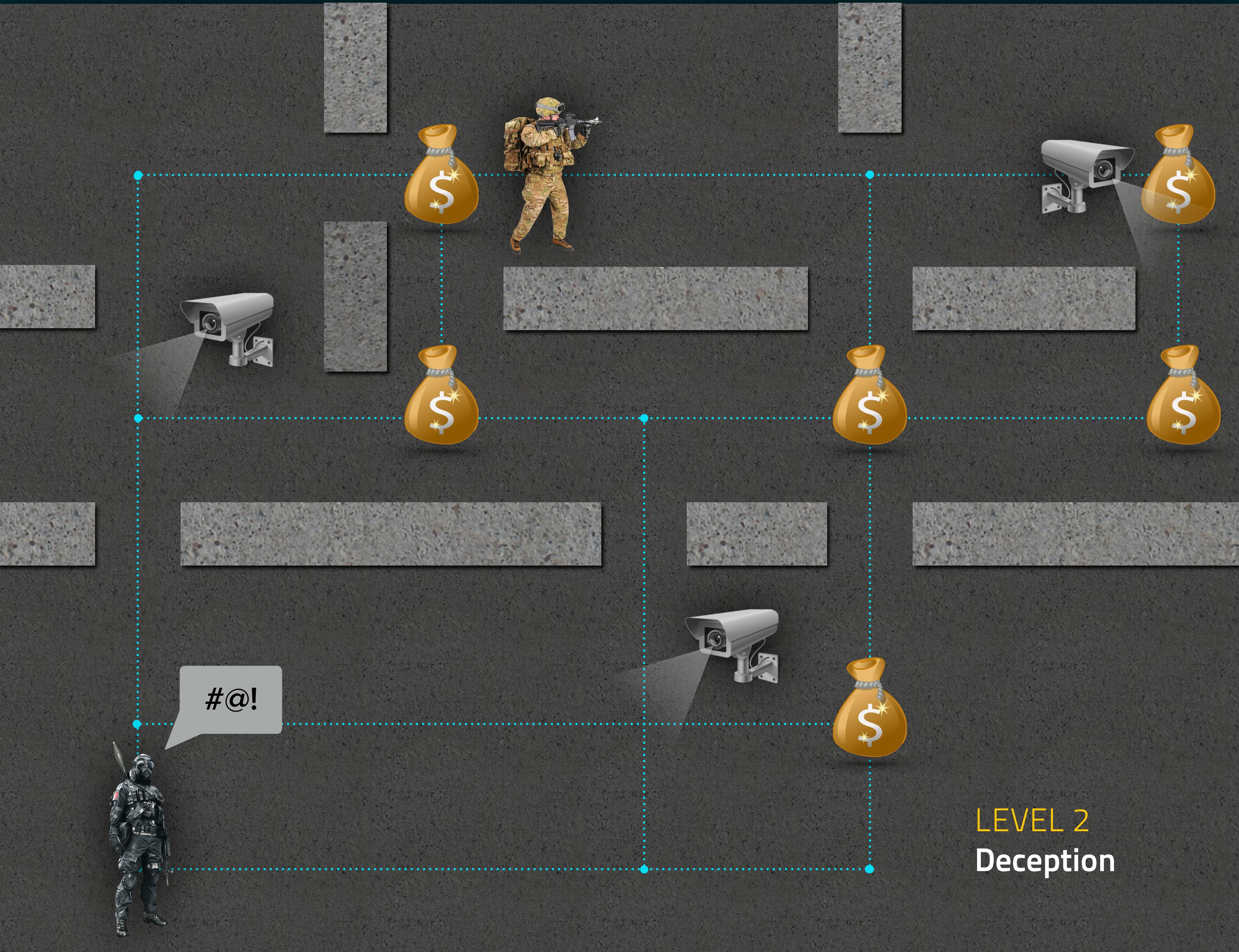
Focused on intent, not tools

60%
of attacks
do not involve malware!

Why does deception work?



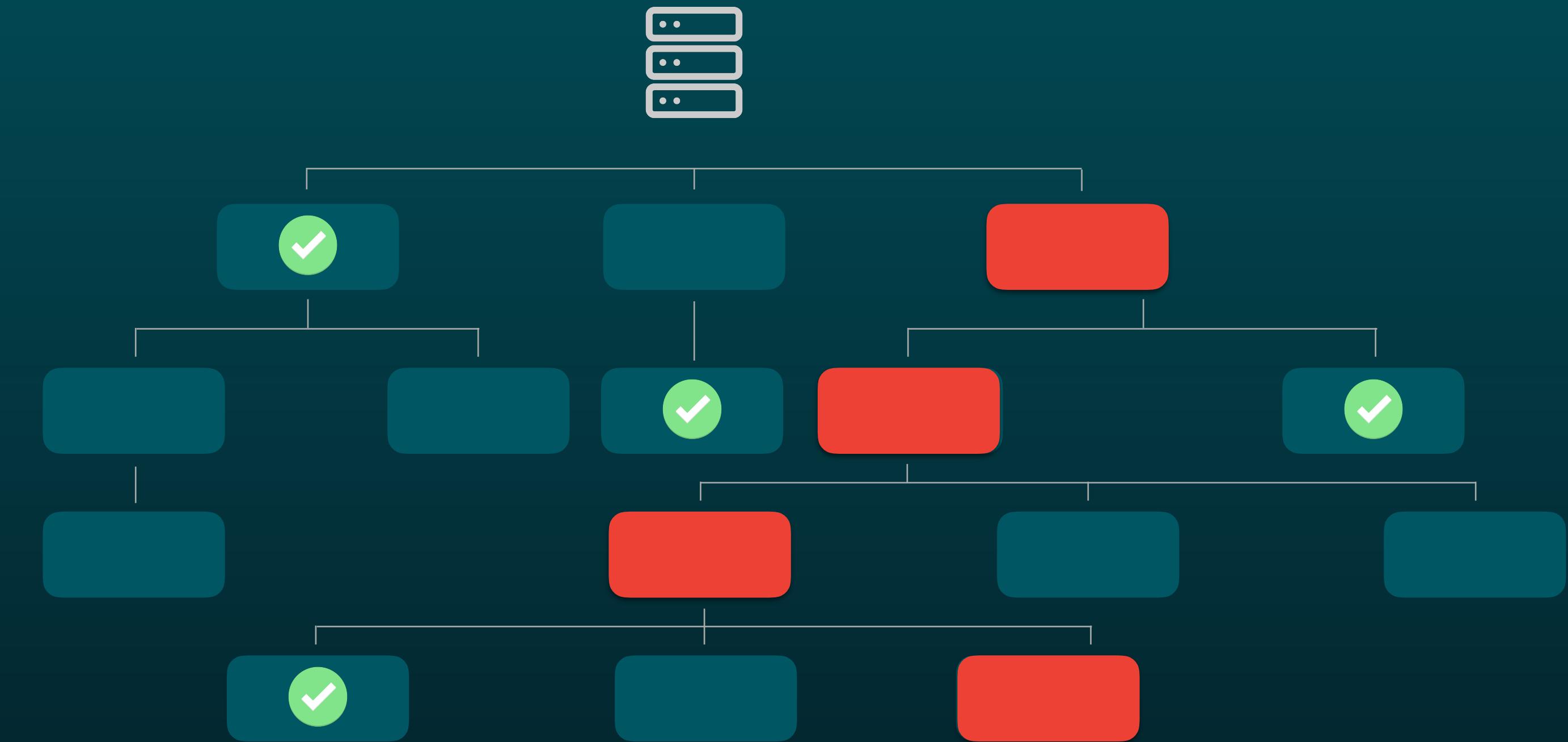




LEVEL 2
Deception

Thinking in lists v/s Thinking in graphs

- ✓ Next-gen firewall
- ✓ Sandboxing
- ✓ Two-factor authentication
- ✓ DAST / SAST
- ✓ Network analytics
- ✓ Endpoint detection and response



Different colors, different languages...

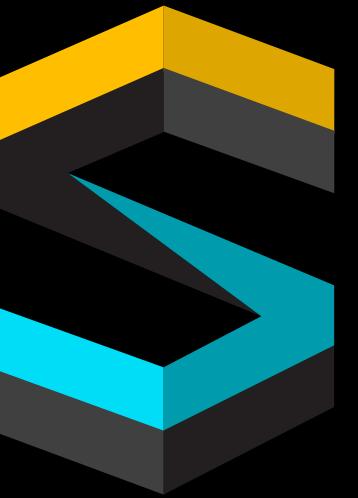
Blue Team talks about

- SQL injection
- Password cracking
- Phishing
- Port-scanning
- Patch management

Red Team talks About

- Squiblydoo
- AS-REP roasting
- Hot potato attacks
- SPN enumeration
- LocalAccountTokenFilterPolicy
- Unquoted service paths
- Process hollowing
- OLE embedded phishing
- LLMNR poisoning
- Bloodhound / user hunting
- DLL side loading
- GPP exploitation
- Time-stomping

Wait a minute, how is
deception different from...



Honeypots...

Honeypots

- Attract attacks
- Public facing
- Vulnerable
- Network focused
- Low signal / noise ratio
- Poor realism
- Not scalable
- Useful for research



$$\underline{AT} = \text{Sum}(RT, D, TH, IR)$$

Red-teaming

Deception

Threat hunting

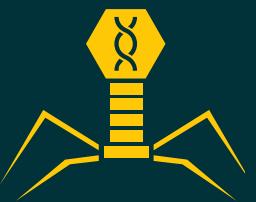
Incident response

Good deception blankets the kill chain



RECONNAISSANCE

Internet Assets



EXPLOITATION

People

Application Credentials



PRIVILEGE ESCALATION

Active Directory Objects

Applications



LATERAL MOVEMENT

Servers

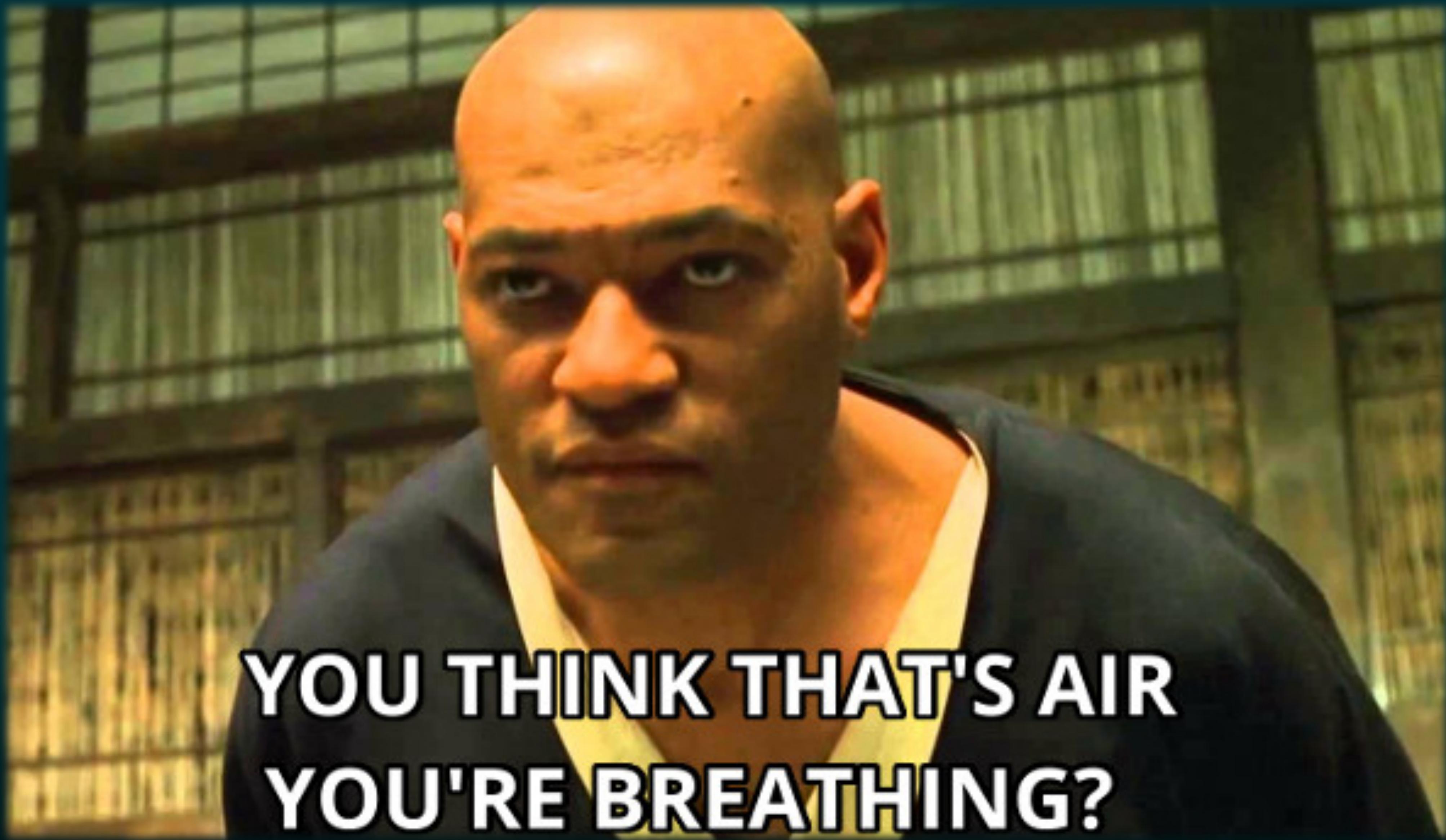
Endpoints



DATA EXFILTRATION

Network Traffic

Files



**YOU THINK THAT'S AIR
YOU'RE BREATHING?**

Chronology of an Attack - “The Double Cycle Pattern”



Initial Intrusion
Low privilege
normal user



C2 and persist
Establish remote
control channel



Lateral Movement
Hunt domain
administrators

Privilege escalation #1
Escalated to local administrator

Privilege escalation #2
Escalate to domain administrator

Breach Complete
Compromise targets
and effect impact



SMOKESCREEN

WE CAN NOW TAKE QUESTIONS!

sahirh@smokescreen.io | www.smokescreen.io | @sahirh