ACTIVE DECEPTION FOR
Red & Blue Teams

Sudarshan Pisupati
Principal Consultant - Smokescreen
@sudartion

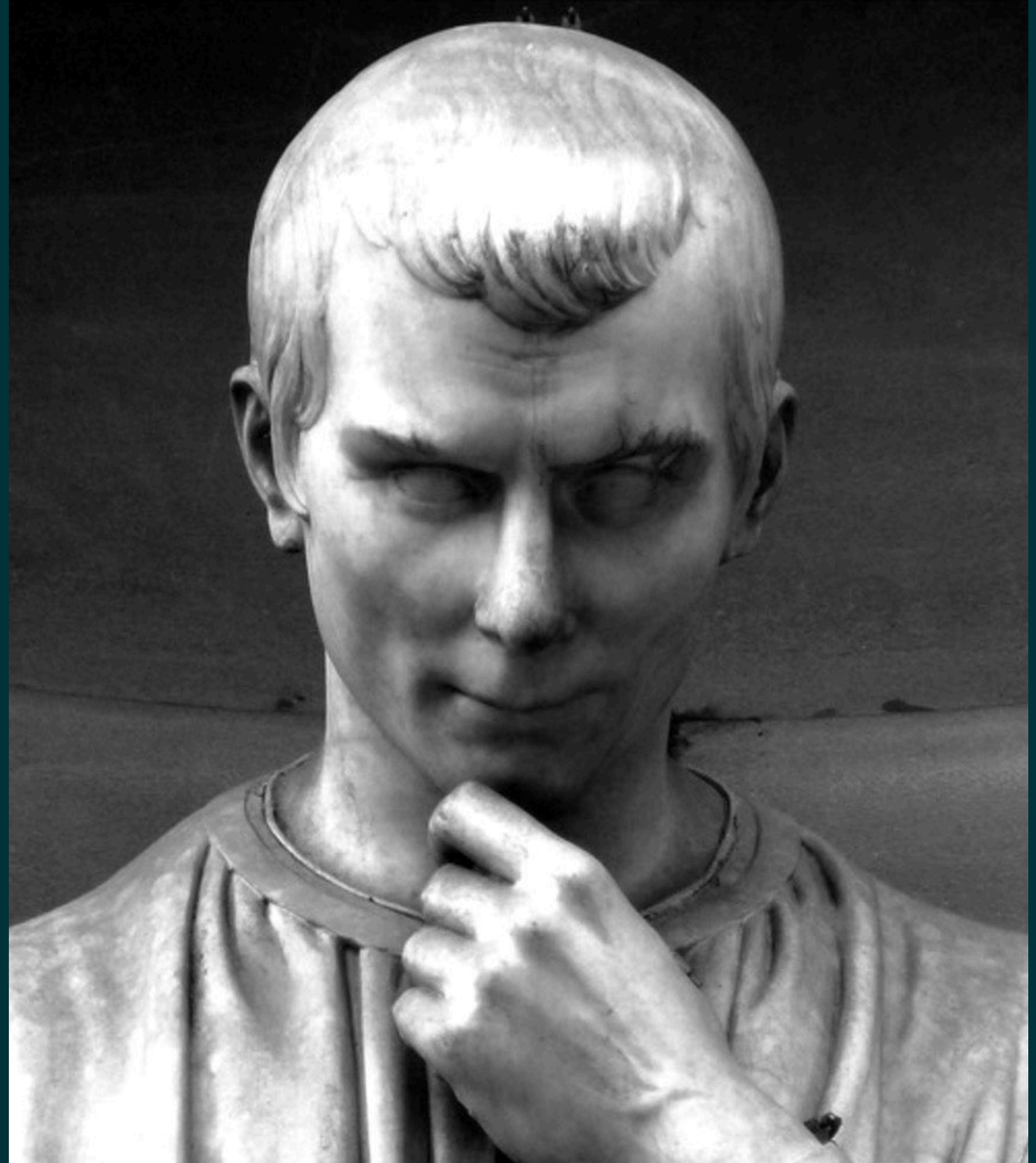
Sahir Hidayatullah
CEO - Smokescreen
@sahirh

“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



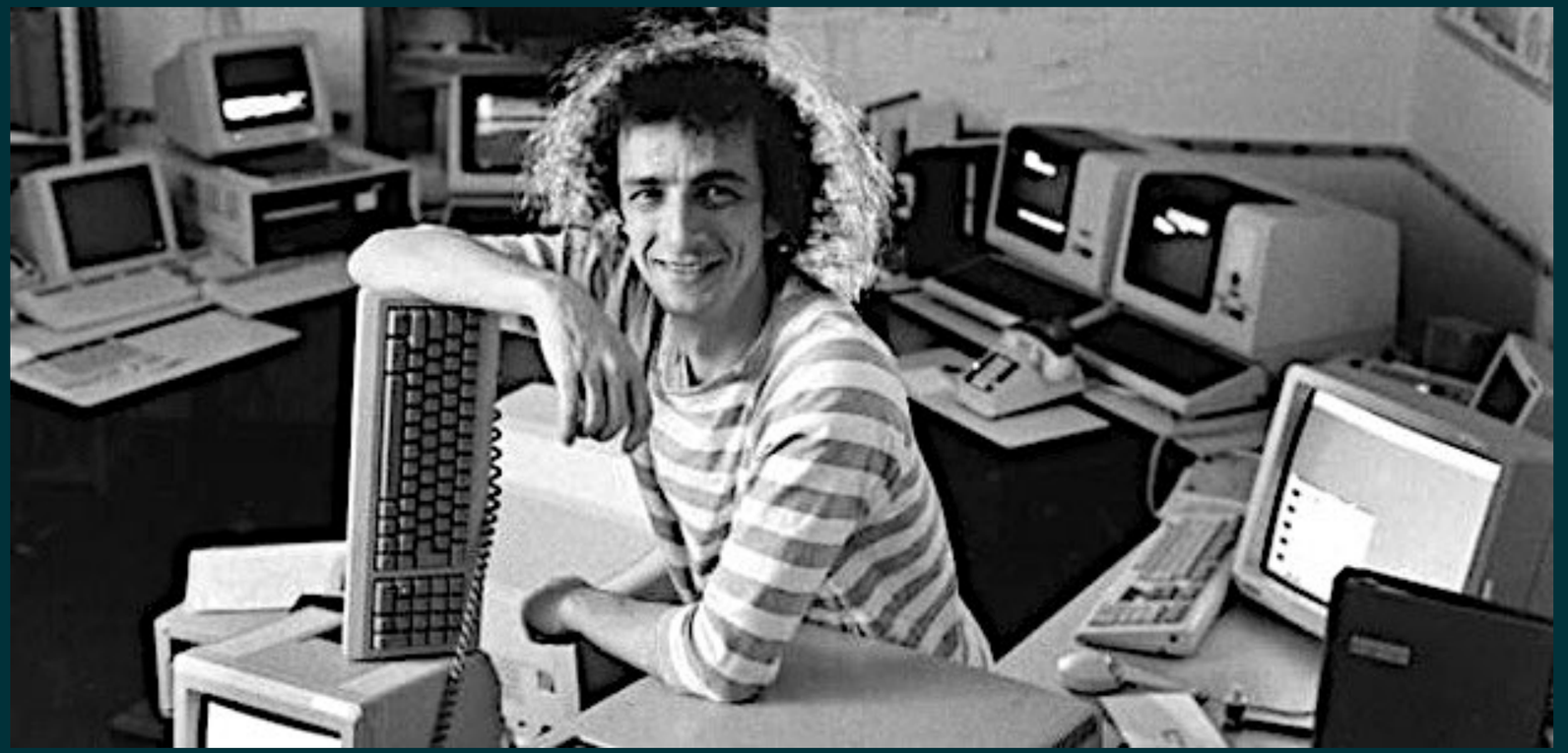
“Never win by force what can be won with deception”

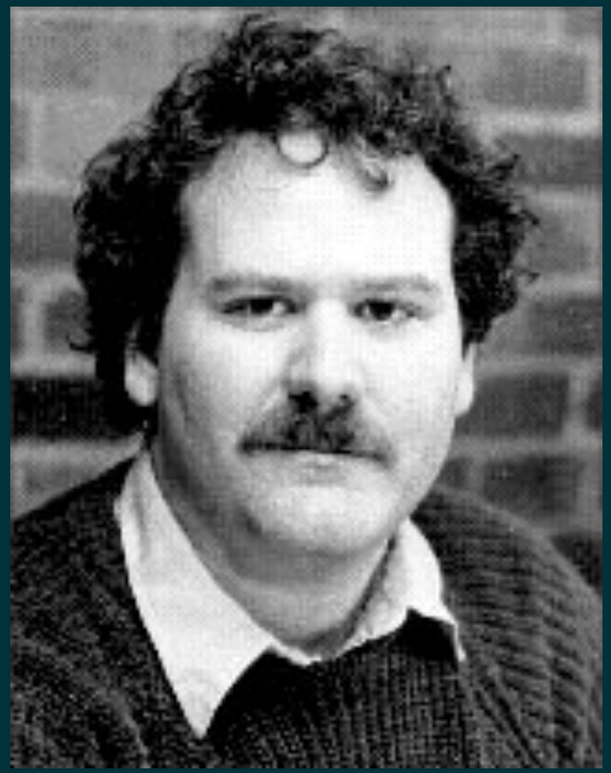
Niccolò Machiavelli,
The Discourses (paraphrased)

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

Napoléon Bonaparte

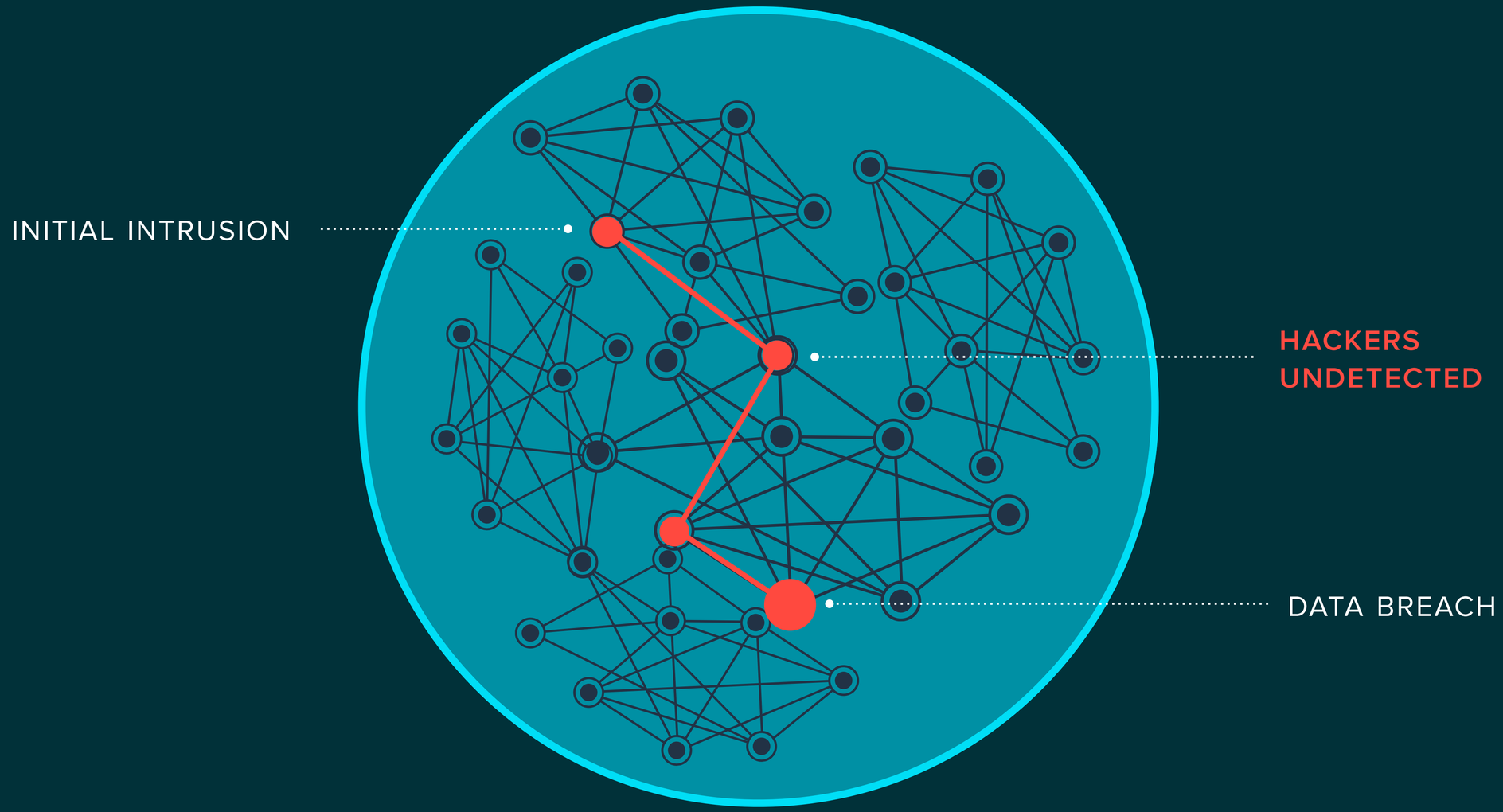

760





There are **3 reasons**
why companies get hacked...

1 Low visibility



SMOKESCREEN

2 Ever changing threat landscape

3 Too many false positives

=

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

SMOKESCREEN

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

SMOKESCREEN

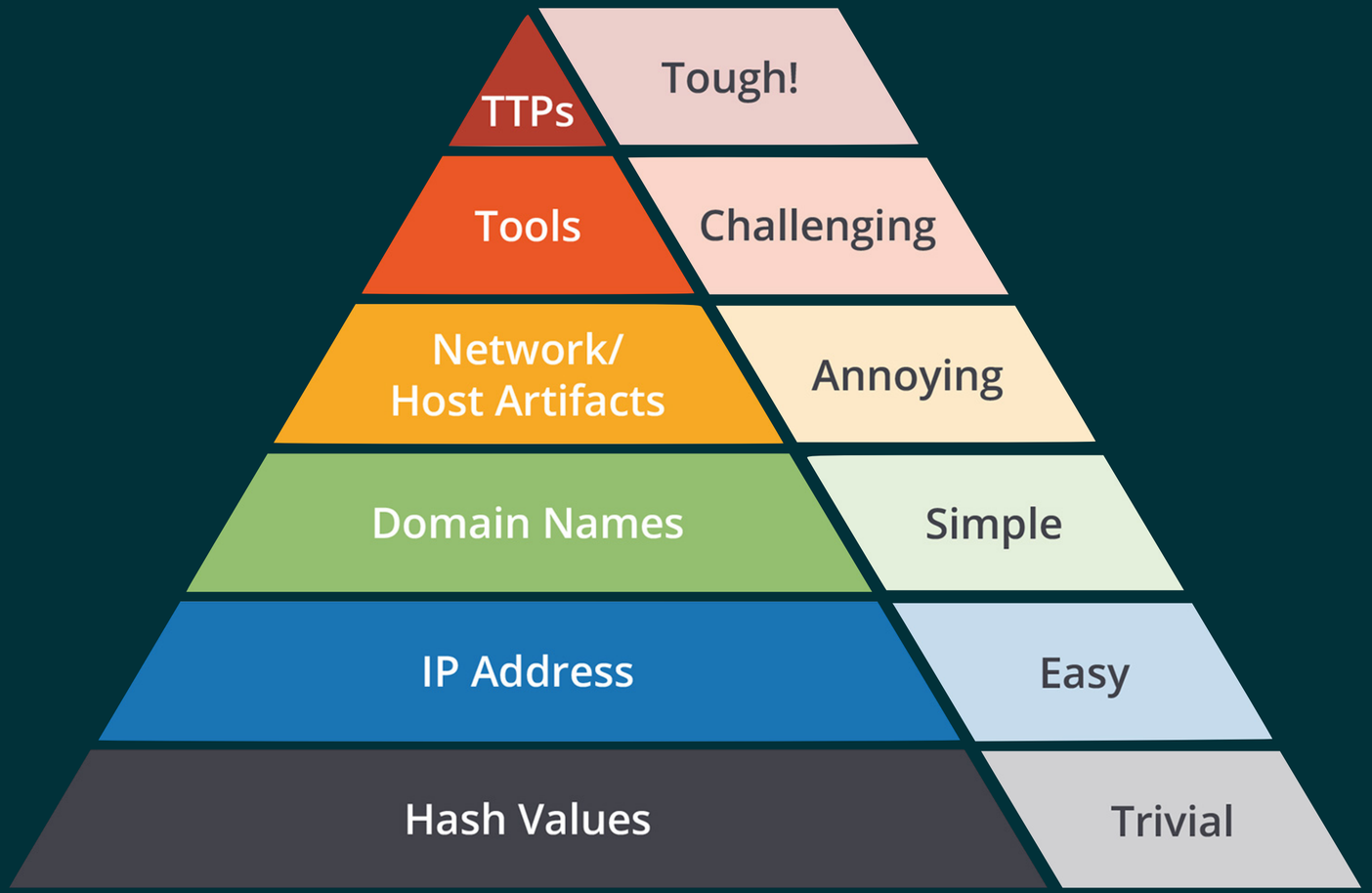
Deception Benefits

No false positives

High attacker impact

Focused on intent, not tools

The Pyramid of Pain



Source: David J. Bianco, personal blog

SMOKESCREEN

Deception Benefits

No false positives

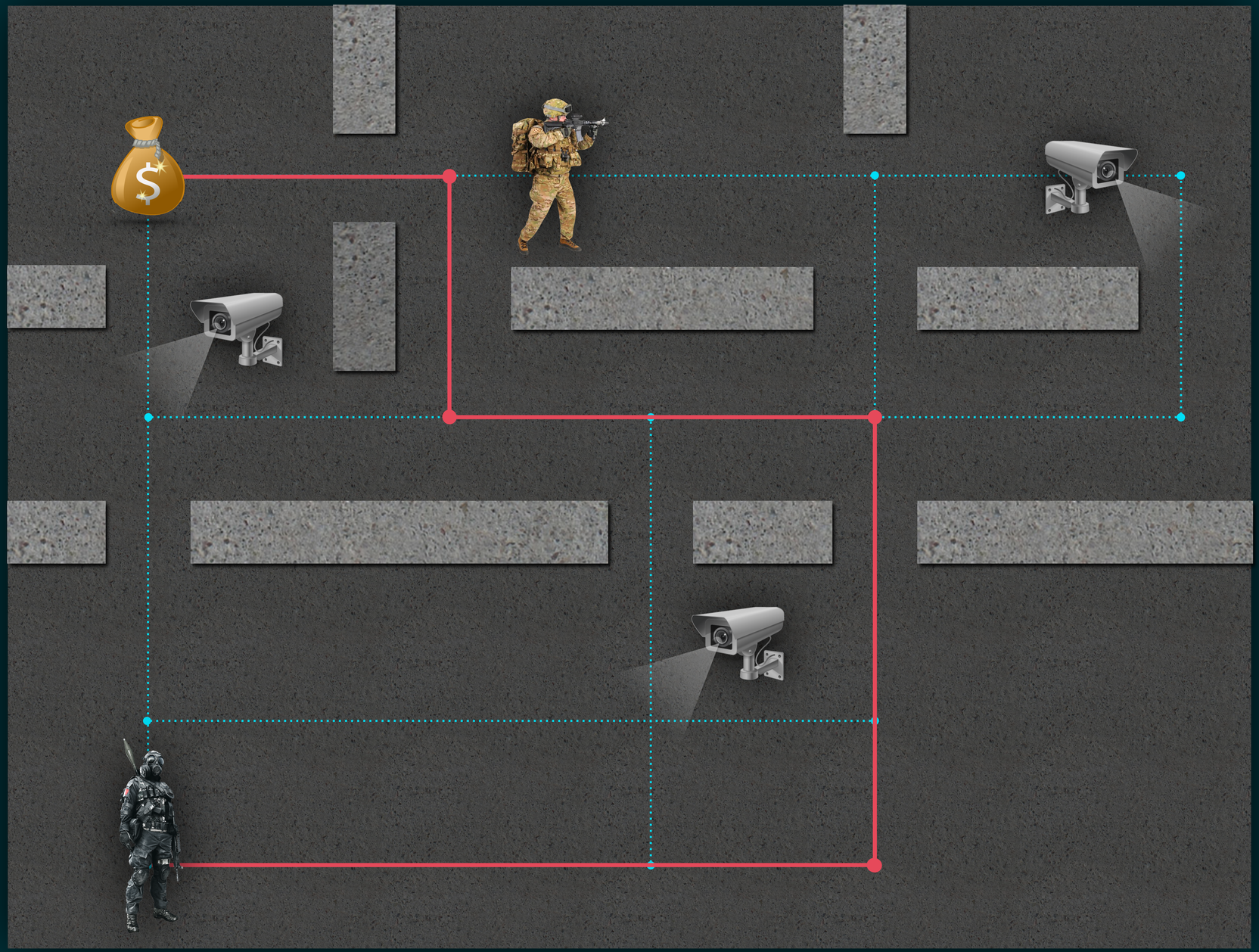
High attacker impact

Focused on intent, not tools

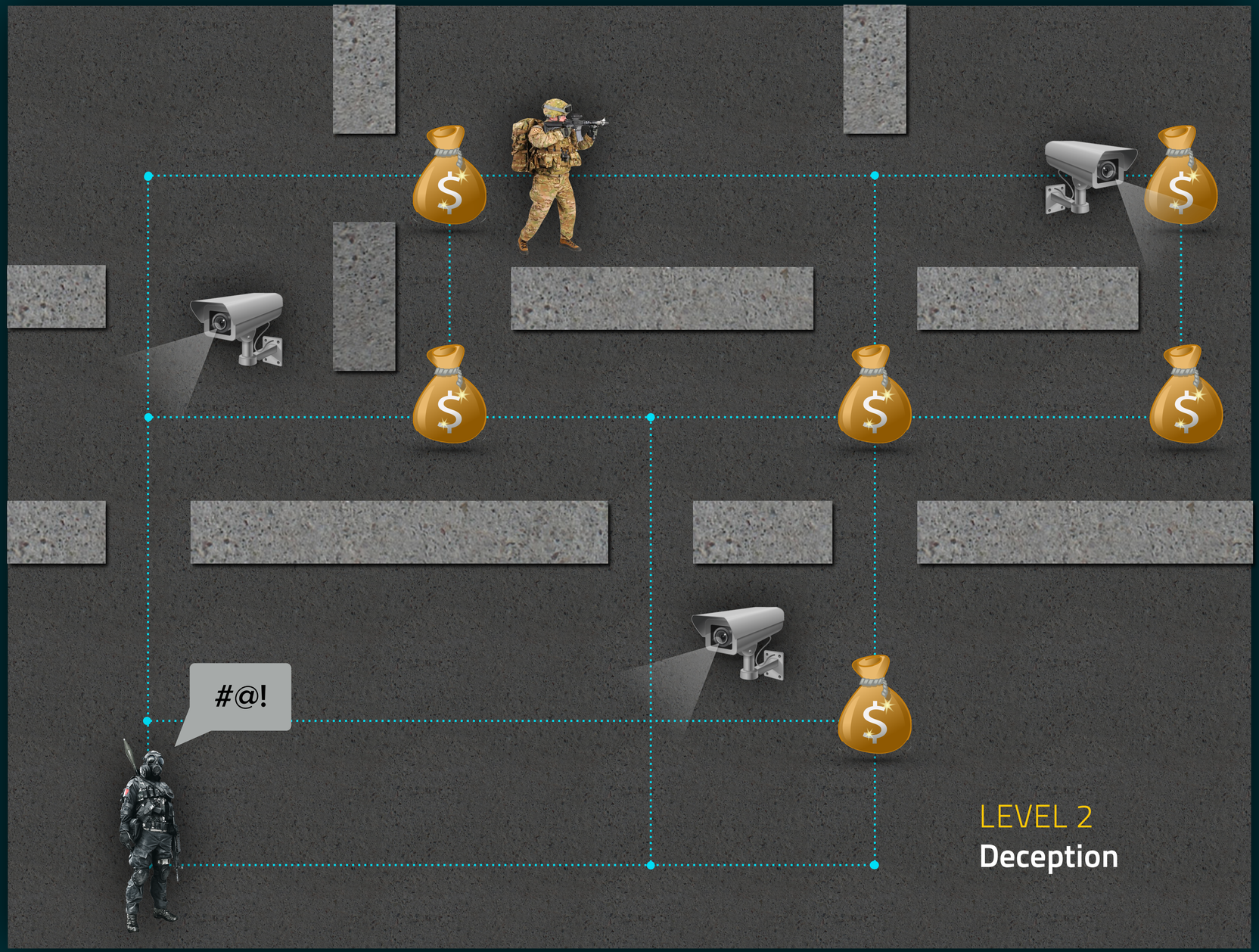
60%
of attacks
do not involve malware!

SMOKESCREEN

Why does deception work?



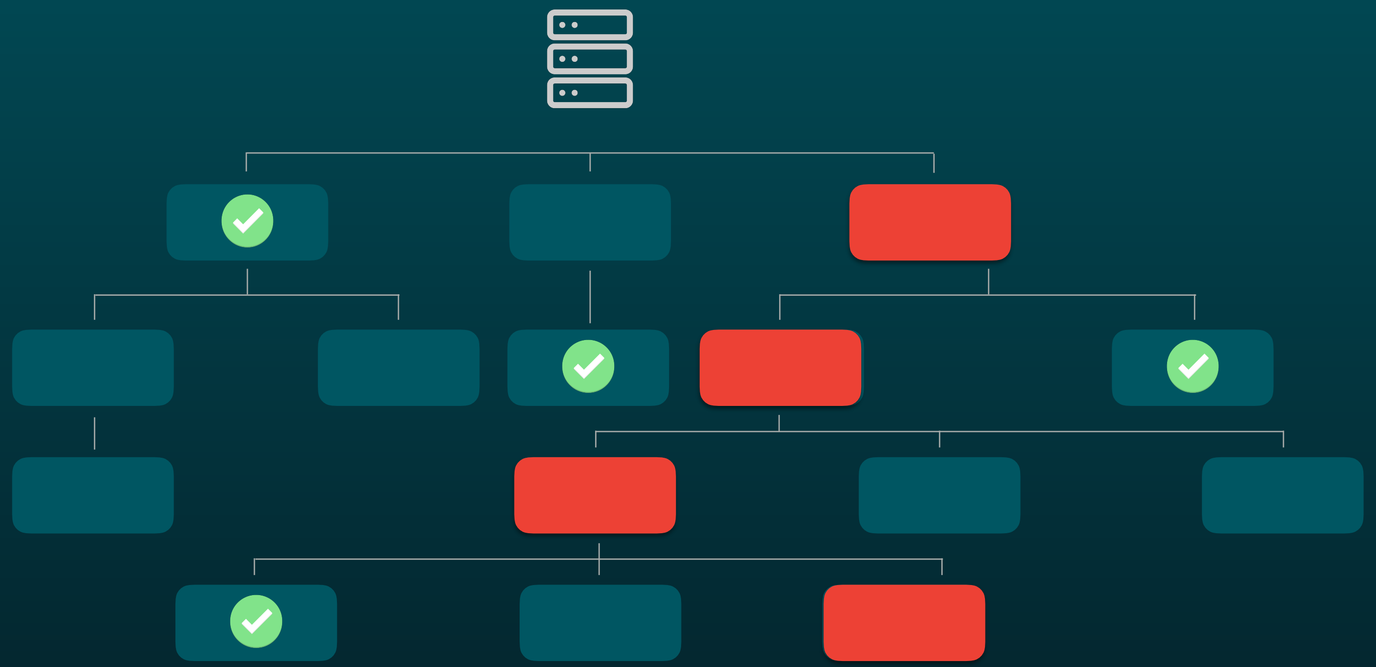
SMOKESCREEN



SMOKESCREEN

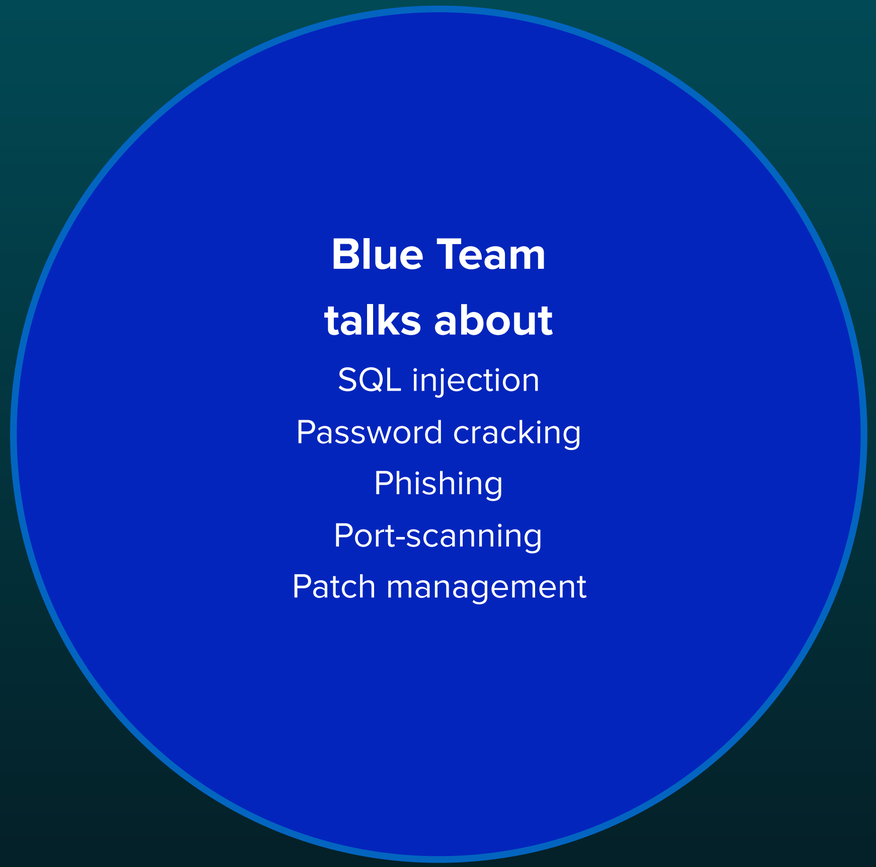
Thinking in lists v/s Thinking in graphs

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



SMOKESCREEN

Different colors, different languages...



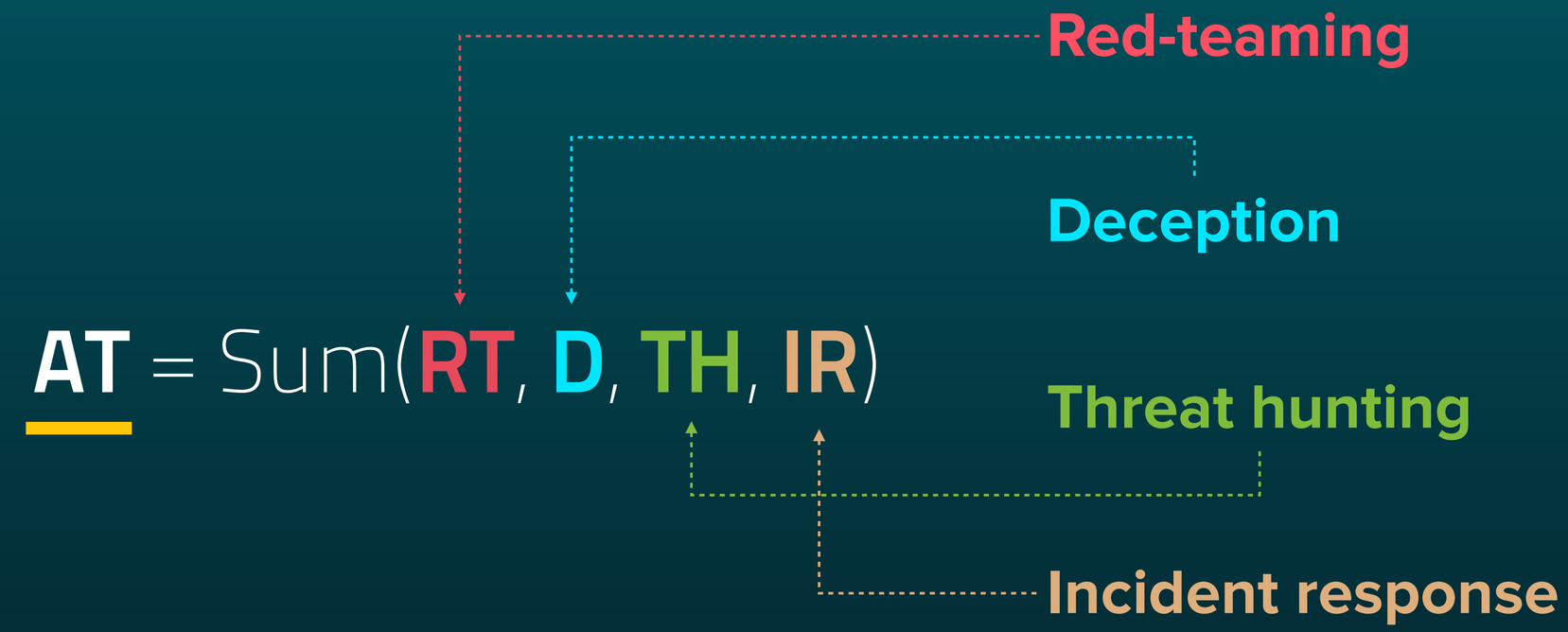
SMOKESCREEN

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



SMOKESCREEN

Good deception blankets the kill chain

RECONNAISSANCE

EXPLOITATION

PRIVILEGE ESCALATION

LATERAL MOVEMENT

DATA EXFILTRATION

Internet Assets

People

Application Credentials

Active Directory Objects

Applications

Servers

Endpoints

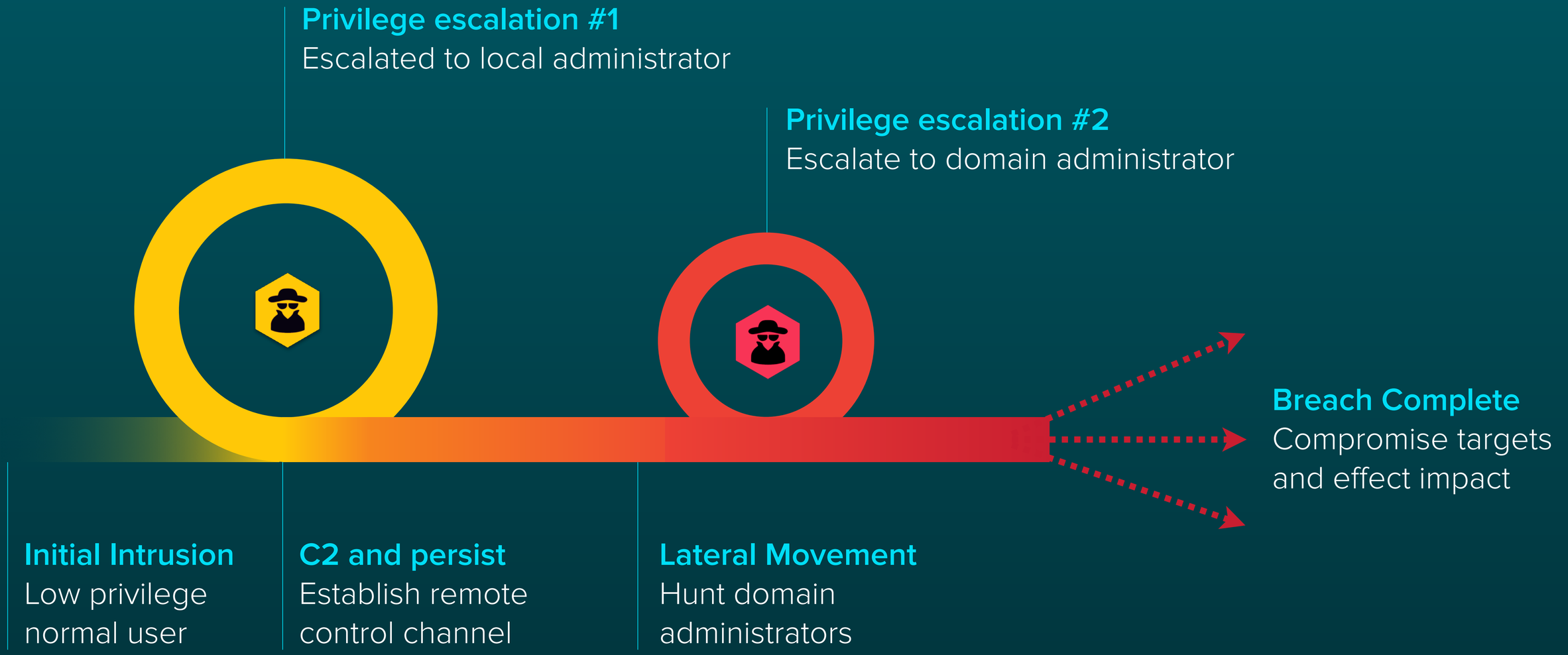
Network Traffic

Files

SMOKESCREEN


YOU THINK THAT'S AIR
YOU'RE BREATHING?

Chronology of an Attack - “The Double Cycle Pattern”



SMOKESCREEN

SMOKESCREEN

WE CAN NOW TAKE QUESTIONS!

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