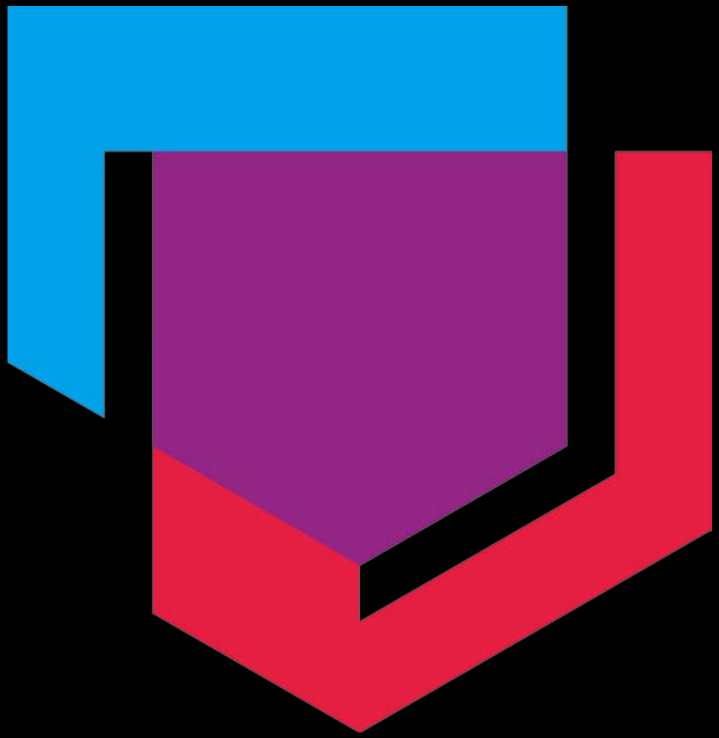
Deloitte.



FROM RED vs BLUE to RED 💜 BLUE
MITRE ATT&CKcon

Olaf Hartong & Vincent Van Mieghem

WTHAY?

VINCENT VAN MIEGHEM

RED TEAM SPECIALIST

Deloitte.

ABOUT VINCENT

- Red team operator
- Technical guy
- Focus on AV evasion techniques

- Software engineering background

HOBBIES

Computers et al.
Lifting when I get bored

@_vivami
github.com/vivami
✉ vvanmieghem@deloitte.nl

OLAF HARTONG

SPECIALIST LEADER
BLUE TEAM

Deloitte.

ABOUT OLAF

Olaf is technically responsible for the Blue Team services within Deloitte NL.

Focus on;
Incident Response, Threat Hunting, Building SOCs and Purple Teaming

Background in Tele and Data communications and Arts.

Former documentary photographer

Dad of 2 boys

HOBBIES

Photography, biking, snowboarding

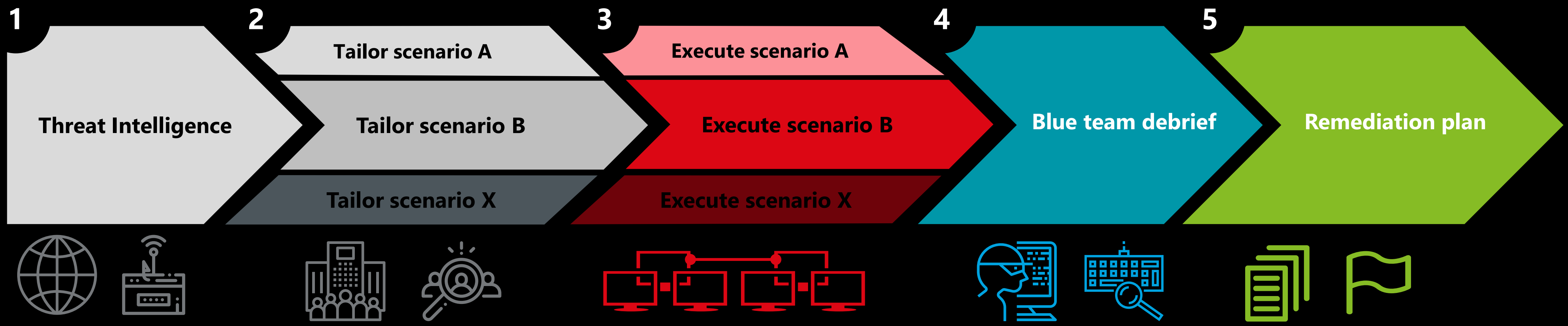
@olafhartong
github.com/olafhartong
✉ ohartong@deloitte.nl

OUR DEFINITION OF RED TEAMING

SIMULATING A REALISTIC ADVERSARIAL ATTACK AGAINST YOUR ORGANIZATION

© 2017 North Korea's Korean Central News Agency

TI based Red Teaming (TIBER) approach



1 Threat Intelligence

2 Tailor scenario A

Tailor scenario B

Tailor scenario X

3 Execute scenario A

Execute scenario B

Execute scenario X

4 Blue team debrief

5 Remediation plan

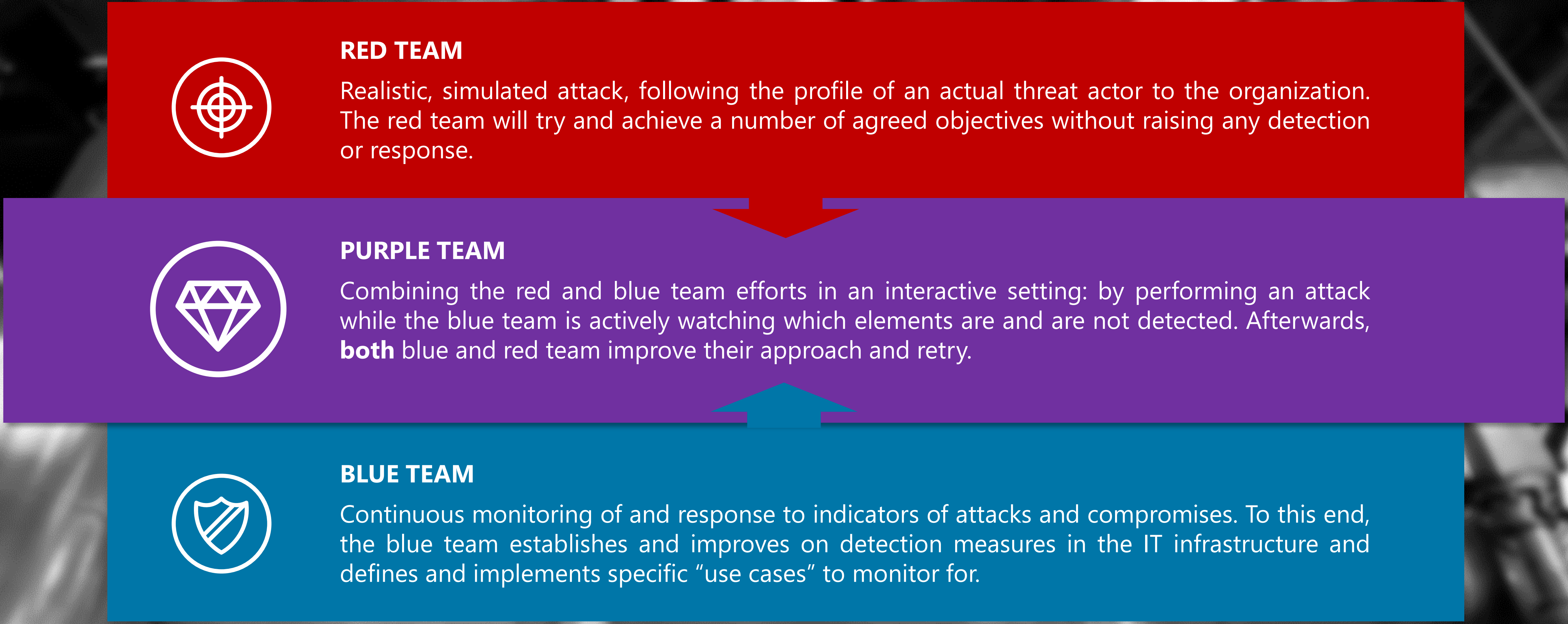
RED TEAMING PITFALLS

- CAN BE ANTAGONIZING
- BLUE TEAM CAN BE TIPPED OFF
- THE REPORT MIGHT NOT BE PUT TO GOOD USE
- YOU’RE MERELY THERE FOR COMPLIENCE REASONS
- THE BLUE TEAM LACKS THE SKILL OR KNOWLEDGE TO FOLLOW UP

RED vs BLUE

Key to Fun
stratego
fascinating two-handed strategy game
Ages 10-Adult
Move hidden value pieces to outwit your opponent and capture his flag.
2 Players
MILTON BRADLEY Company
SPRINGFIELD, MA 01101
Made in U.S.A.
4916
STRATEGO
SEE BOX BOTTOM FOR DESCRIPTION OF GAME

RED + BLUE = PURPLE, COMBINING STRENGTHS



RED TEAM

Realistic, simulated attack, following the profile of an actual threat actor to the organization. The red team will try and achieve a number of agreed objectives without raising any detection or response.

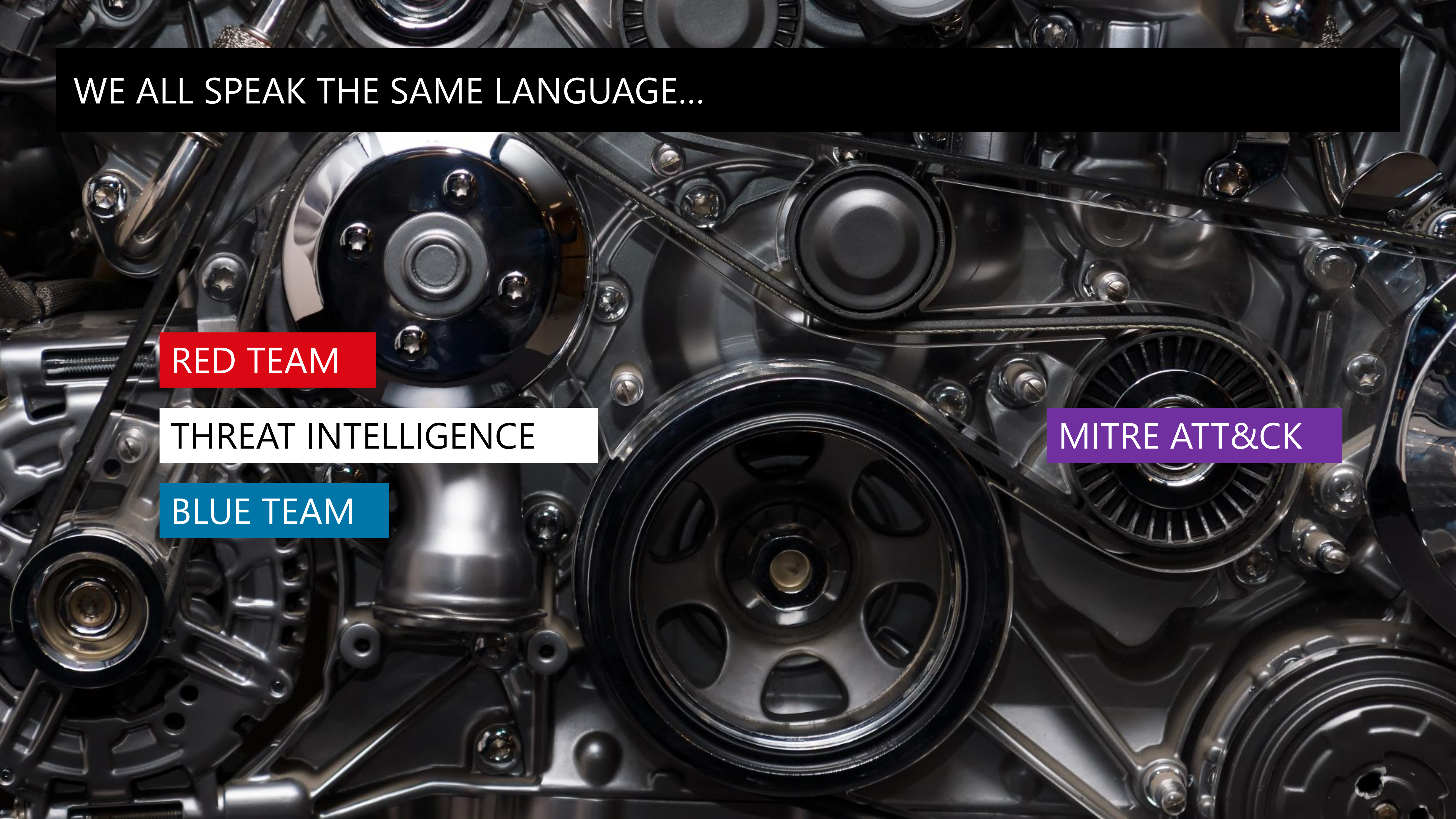
PURPLE TEAM

Combining the red and blue team efforts in an interactive setting: by performing an attack while the blue team is actively watching which elements are and are not detected. Afterwards, **both** blue and red team improve their approach and retry.

BLUE TEAM

Continuous monitoring of and response to indicators of attacks and compromises. To this end, the blue team establishes and improves on detection measures in the IT infrastructure and defines and implements specific “use cases” to monitor for.

WE ALL SPEAK THE SAME LANGUAGE…



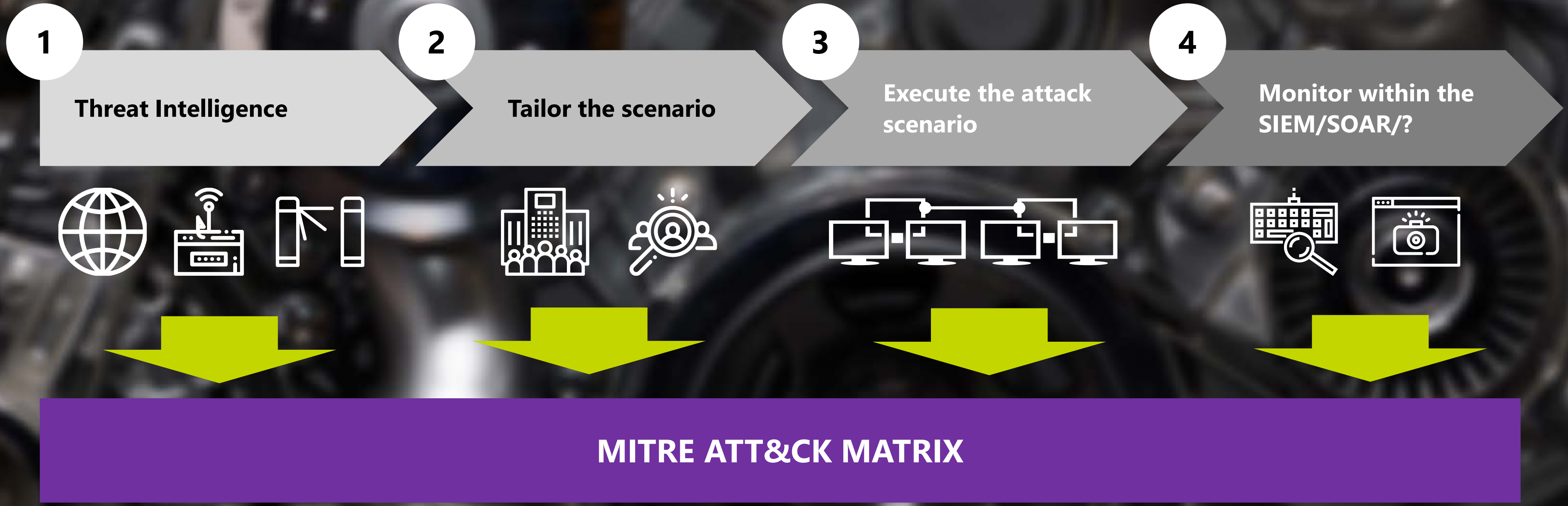
RED TEAM

THREAT INTELLIGENCE

BLUE TEAM

MITRE ATT&CK

...WE ALL SPEAK ATT&CK...



1 Threat Intelligence

2 Tailor the scenario

3 Execute the attack scenario

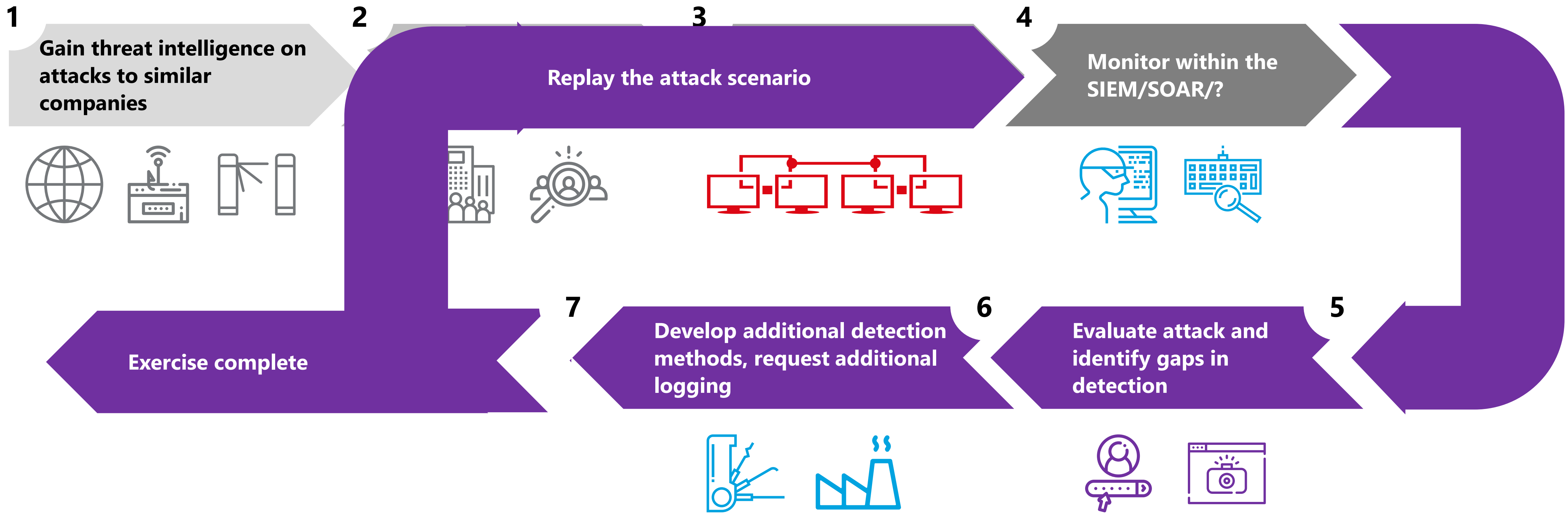
4 Monitor within the SIEM/SOAR/?

MITRE ATT&CK MATRIX

…SO WE DON’T END UP LIKE THIS

© Disney, All Rights Reserved, Muppets

TIBER STYLE PURPLE TEAMING



1

Gain threat intelligence on attacks to similar companies

2

3

Replay the attack scenario

4

Monitor within the SIEM/SOAR/?

5

Evaluate attack and identify gaps in detection

6

Develop additional detection methods, request additional logging

7

Exercise complete

OPEN SKIES

WHAT TRACES DO I LEAVE?

HOW DOES A RED TEAM THINK?

CAN I ADOPT MY TTP’S TO FALL OFF THE RADAR?

FOCUS DETECTION BASED ON ATT&CK

SKILL/KNOWLEDGE BOOST FOR BOTH TEAMS

QUESTIONS?

Deloitte.