Kooy Symposium 11 april 2018

13:00 – 14:40 Beleid en visie

TIBER: aanvalssimulaties in de financiële kerninfrastructuur

Petra Hielkema
Divisiedirecteur Betalingsverkeer en Marktinfrastructuur
De Nederlandsche Bank

DeNederlandscheBank
EUROSYSTEEM

Agenda

1. **Introduction**
2. Cyber threat landscape
3. Cyber fundamentals and resilience
4. TIBER-NL: attack simulations
5. Conclusion

Agenda

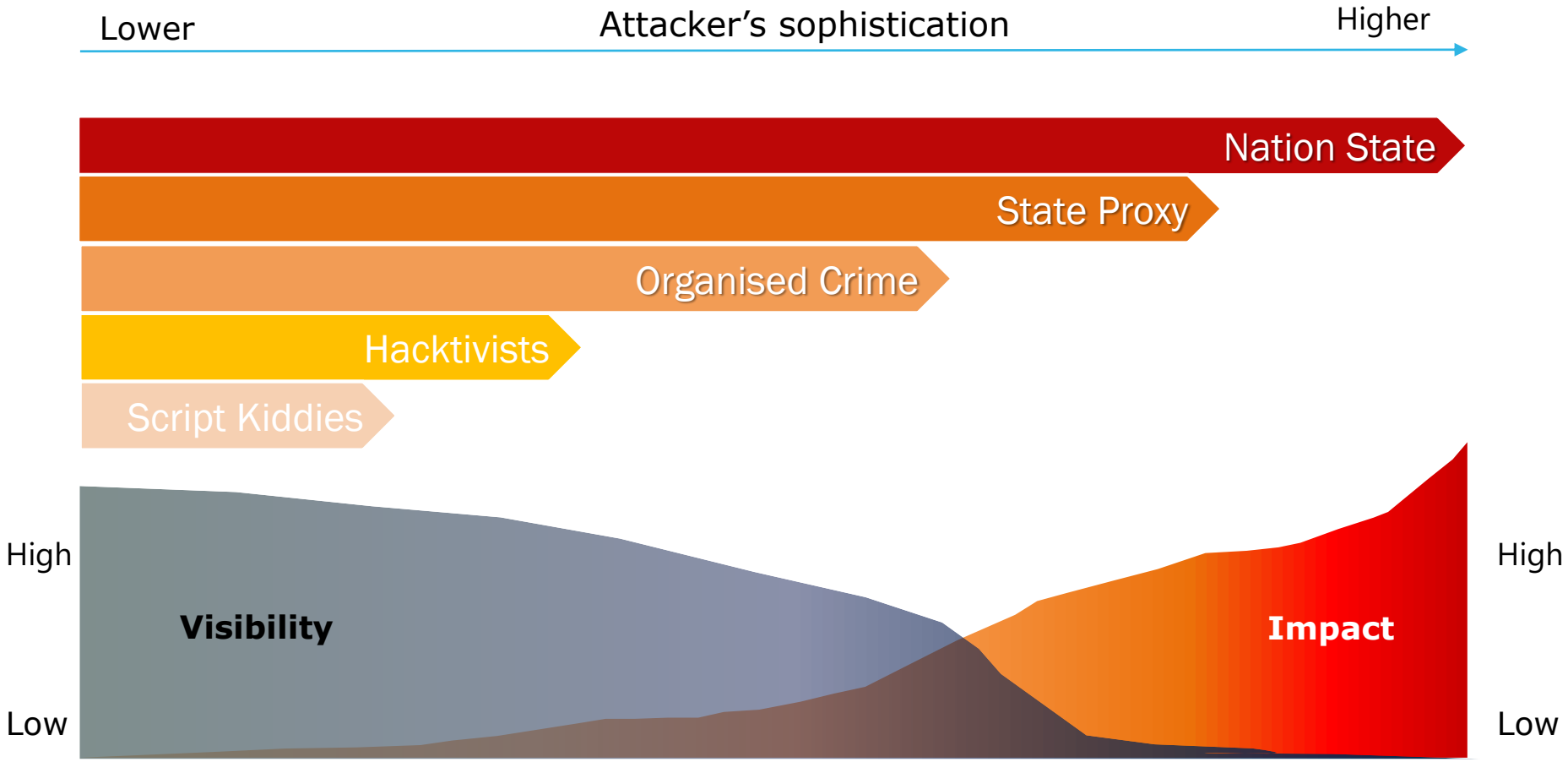
1. Introduction
2. **Cyber threat landscape**
3. Cyber fundamentals and resilience
4. TIBER-NL: attack simulations
5. Conclusion

2. Cyber threat landscape

Threat levels rising

Moving upstream

2. Cyber threat landscape



Source: DNB, July 2017

DeNederlandscheBank
EUROSYSTEEM

3. The major league of adversaries

Rugbyworldcup.com 19-4-2018


AIG
AIG
AIG
AIG
AIG

Agenda

1. Introduction
2. Cyber threat landscape
3. **Cyber fundamentals and resilience**
4. TIBER-NL: attack simulations
5. Conclusion

3. Fundamentals

3. Fundamentals and resilience

Committee on Payments and Market Infrastructures

Board of the International Organization of Securities Commissions

Guidance on cyber resilience for financial market infrastructures

June 2016

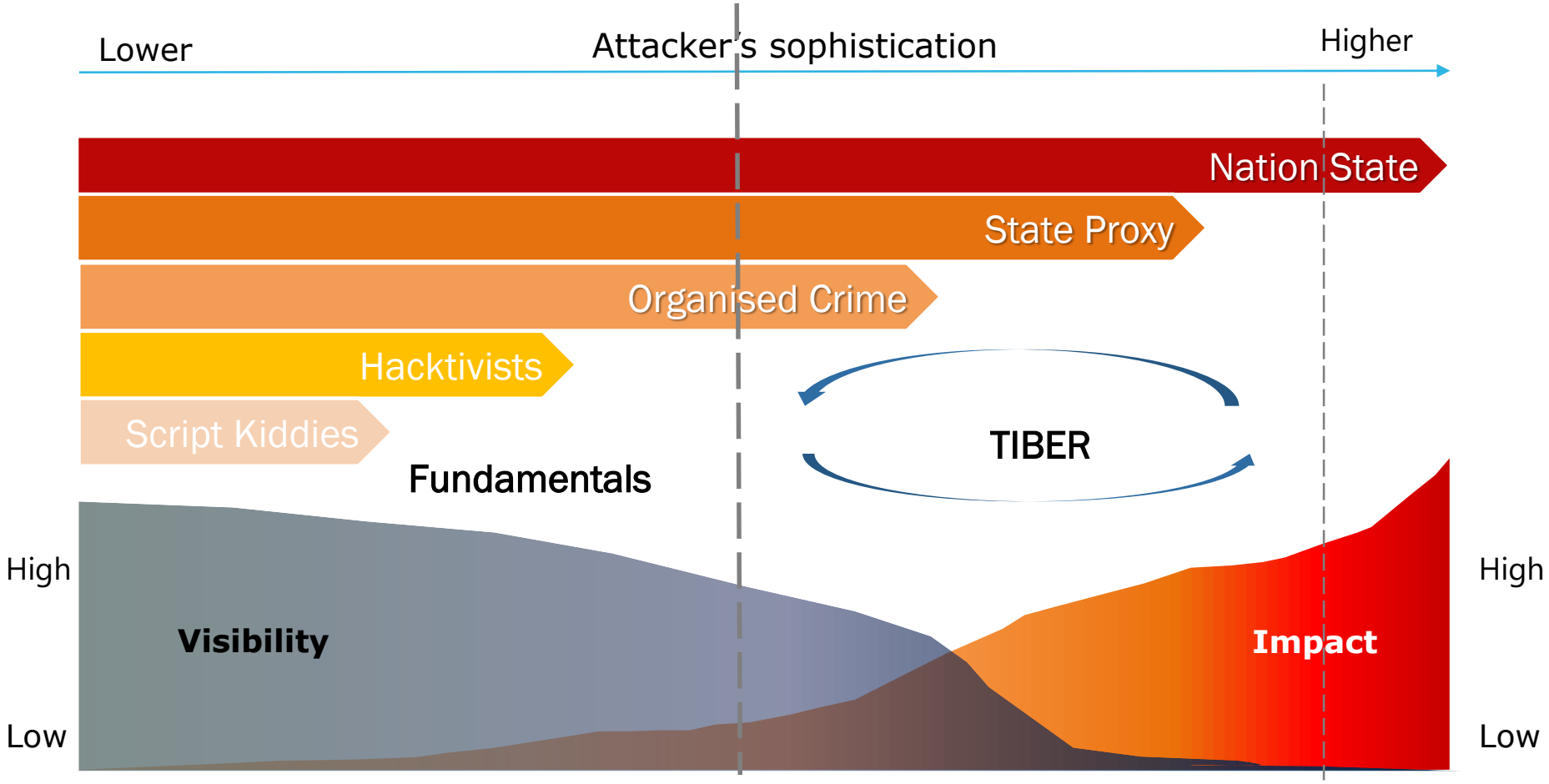
BANK FOR INTERNATIONAL SETTLEMENTS

OICU-IOSCO

Agenda

1. Introduction
2. Cyber threat landscape
3. Cyber fundamentals and resilience
4. **TIBER-NL: attack simulations**
5. Conclusion

4. TIBER-NL attack simulations

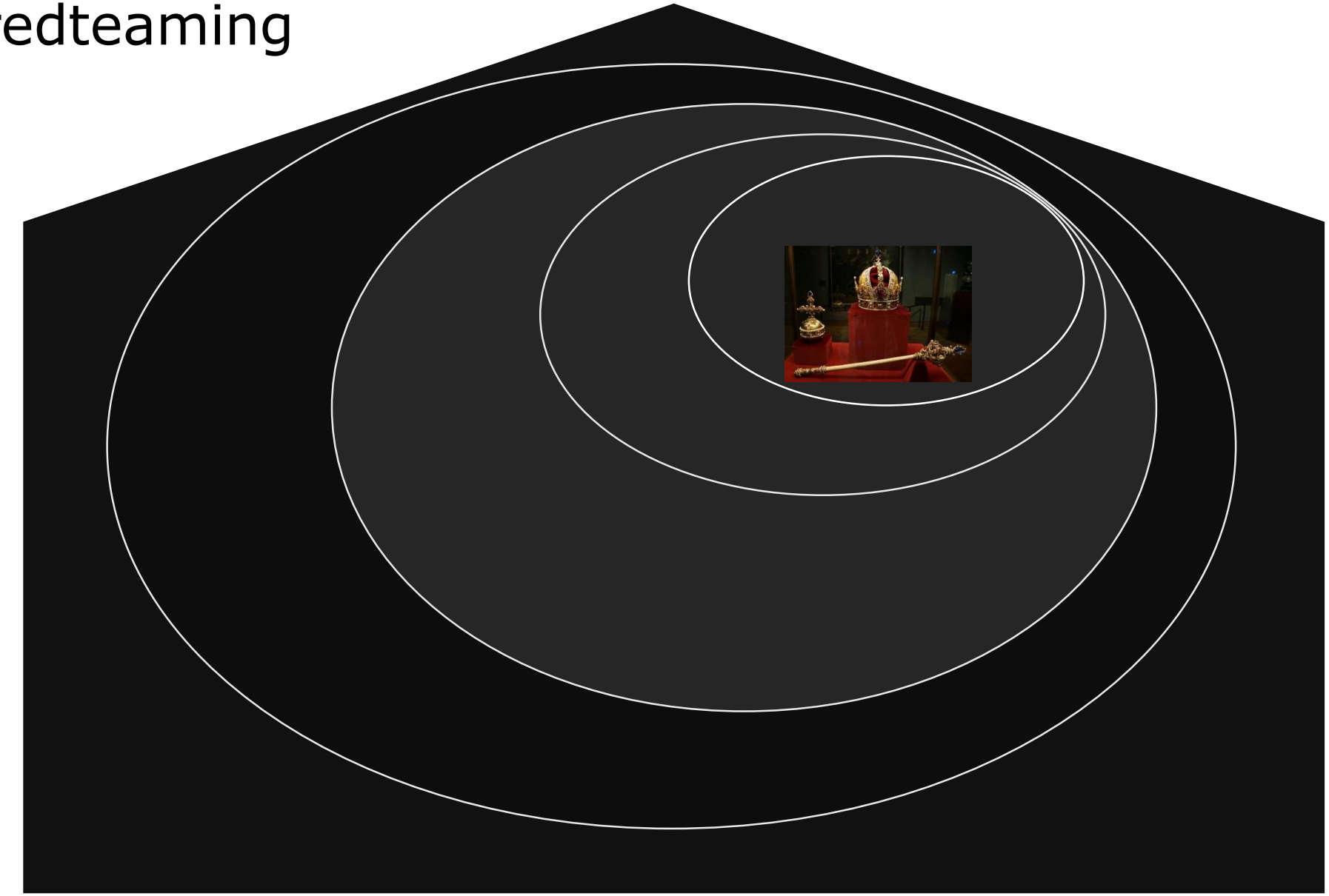


Source: DNB, July 2017

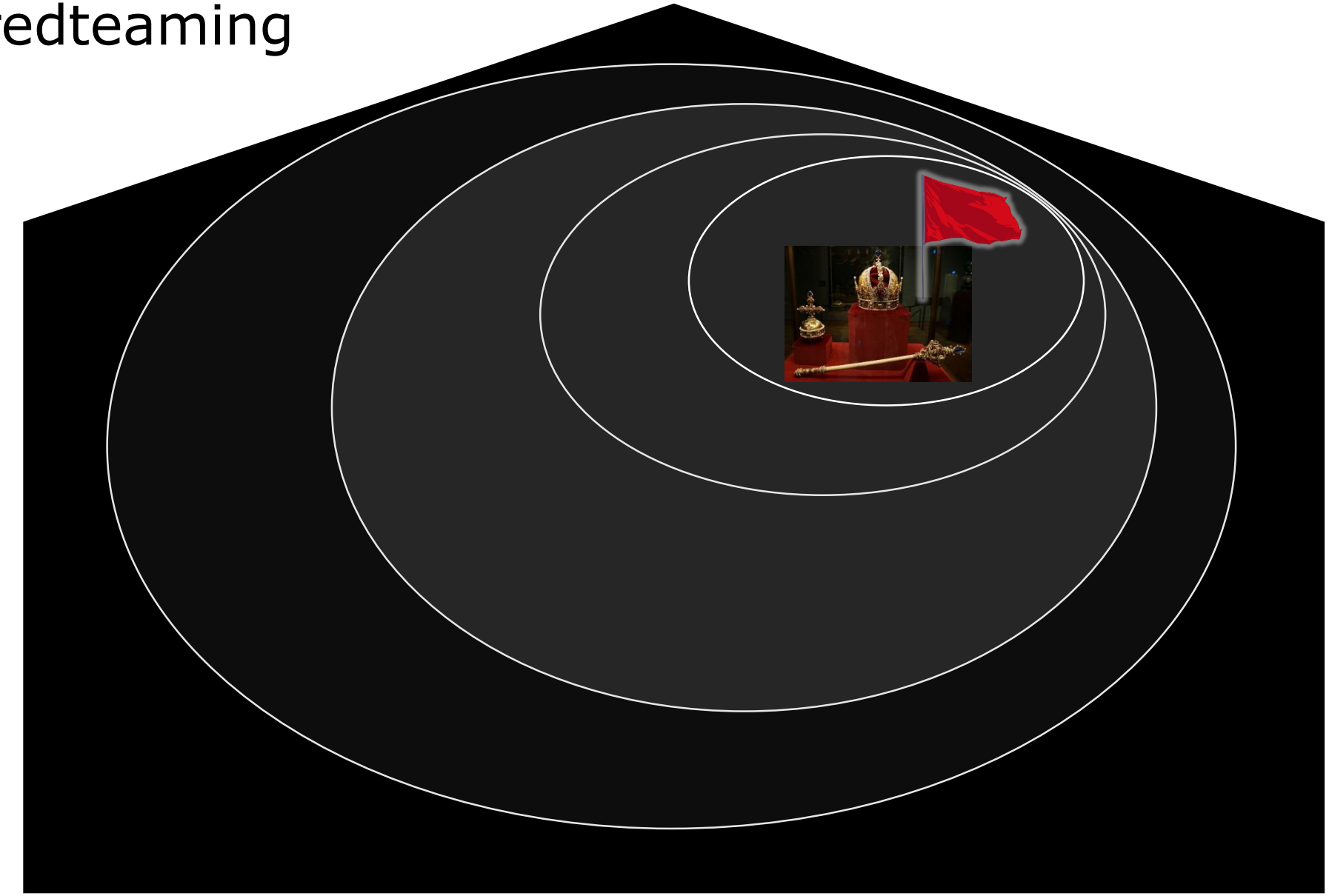
DeNederlandscheBank
EUROSYSTEEM

TIBER-NL redteaming

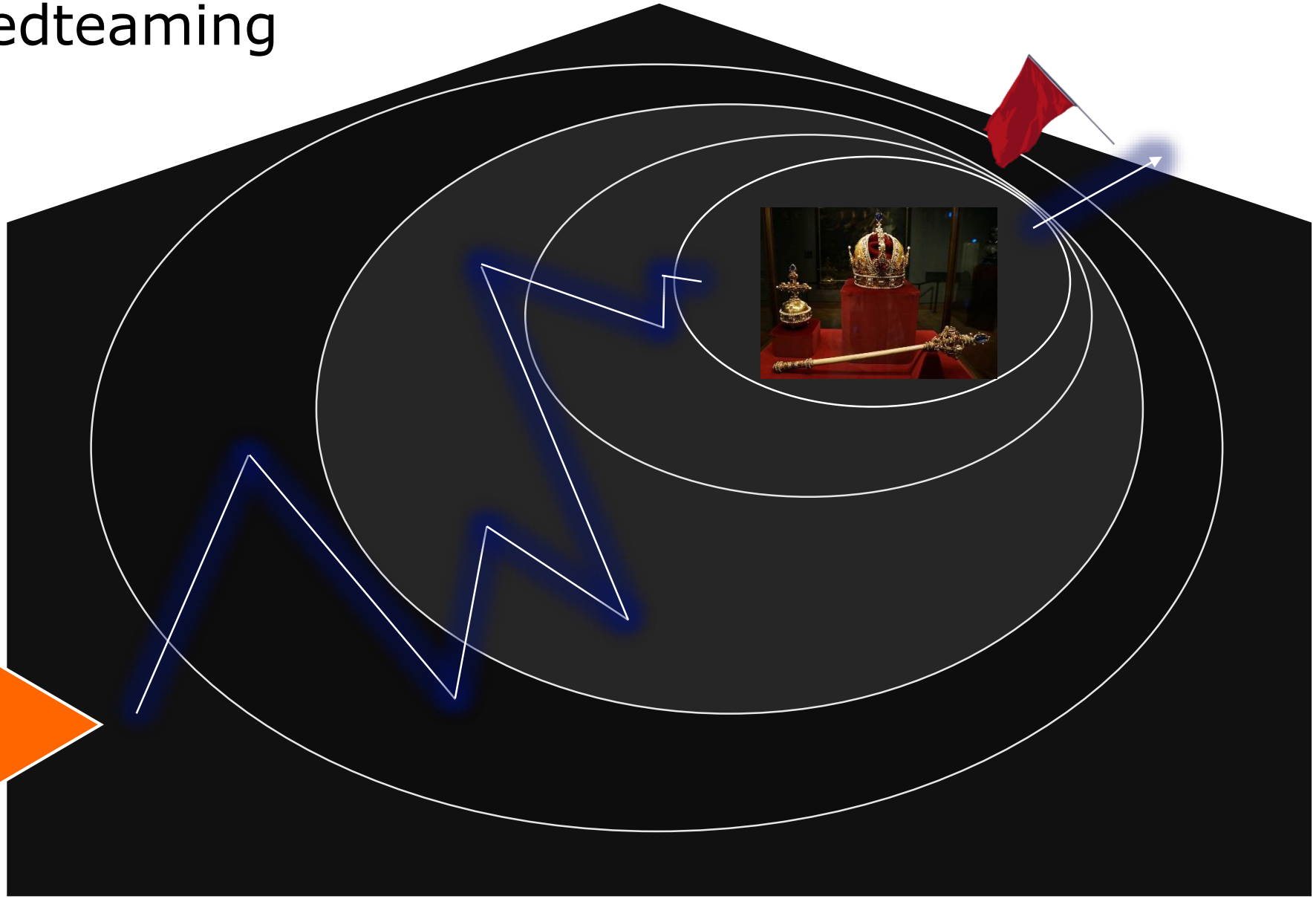
TIBER-NL redteaming



TIBER-NL redteaming

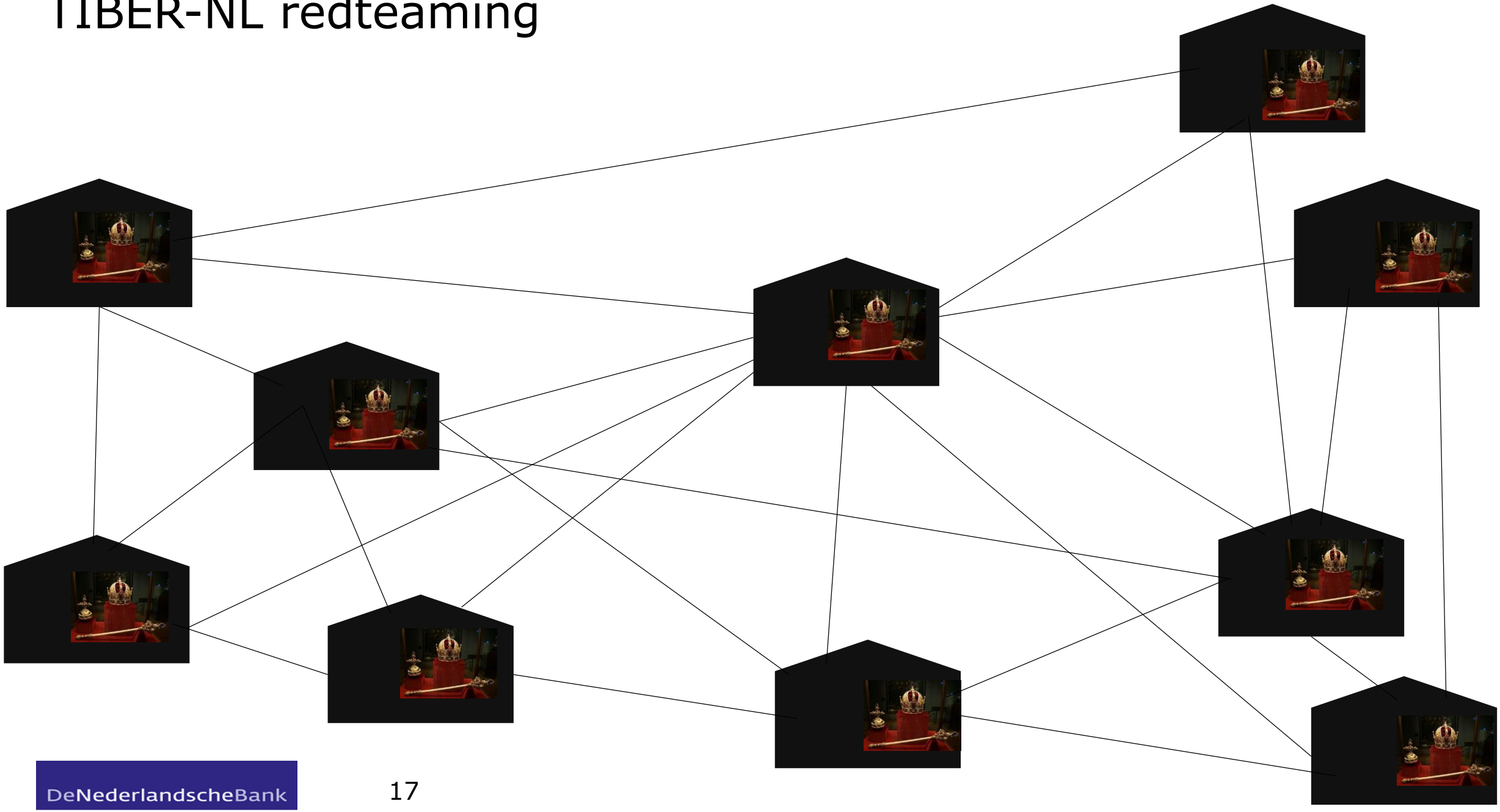


TIBER-NL redteaming



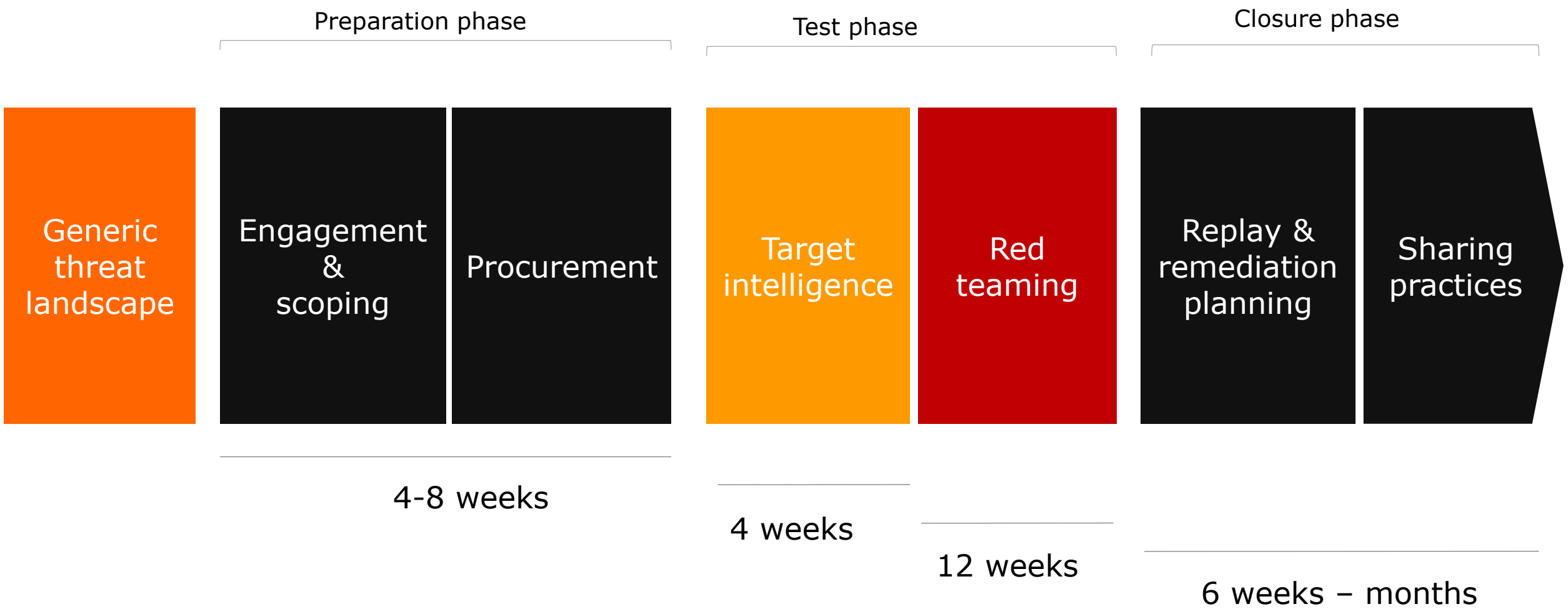
1. Reconnaissance
2. Get in
3. Get through
4. Get out

TIBER-NL redteaming

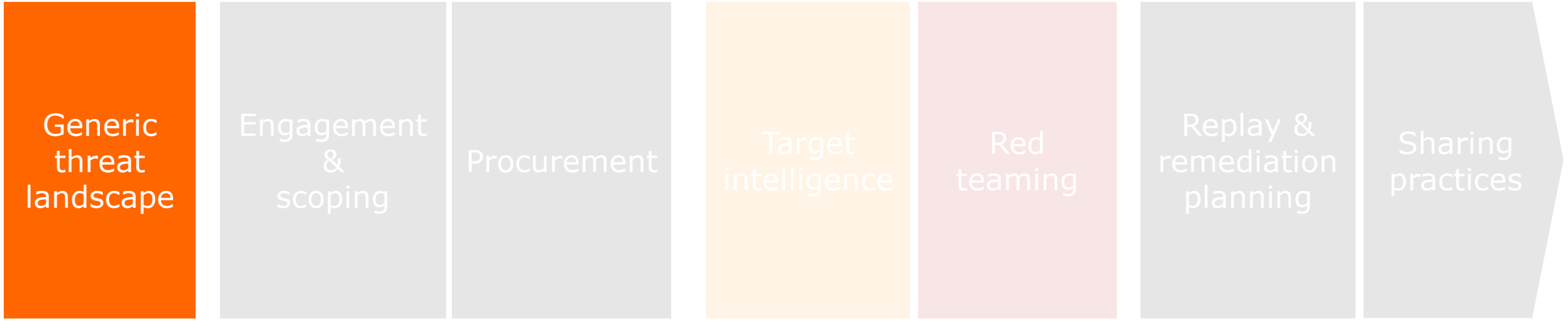


DeNederlandscheBank
EUROSYSTEEM

TIBER-NL


Preparation phase
Test phase
Closure phase
Generic threat landscape
Engagement & scoping
Procurement
Target intelligence
Red teaming
Replay & remediation planning
Sharing practices
4-8 weeks
4 weeks
12 weeks
6 weeks – months

TIBER-NL



Generic threat intelligence

NL financial critical infrastructure, divided in: Retail banking, Wholesale, Clearing and settlement, Stock exchange

TIBER-NL

Critical economic functions, selected key systems and services

Potential compromise actions

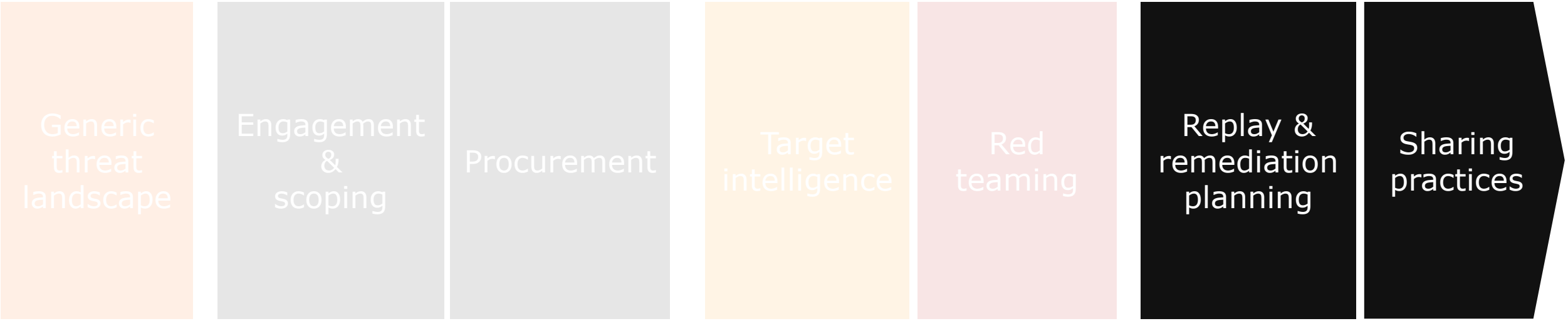
Highest standards TI and RT (procurement)

TIBER-NL

Institution's attack surface: People, process and technology
- In
- Through/Out

+ Scenario X

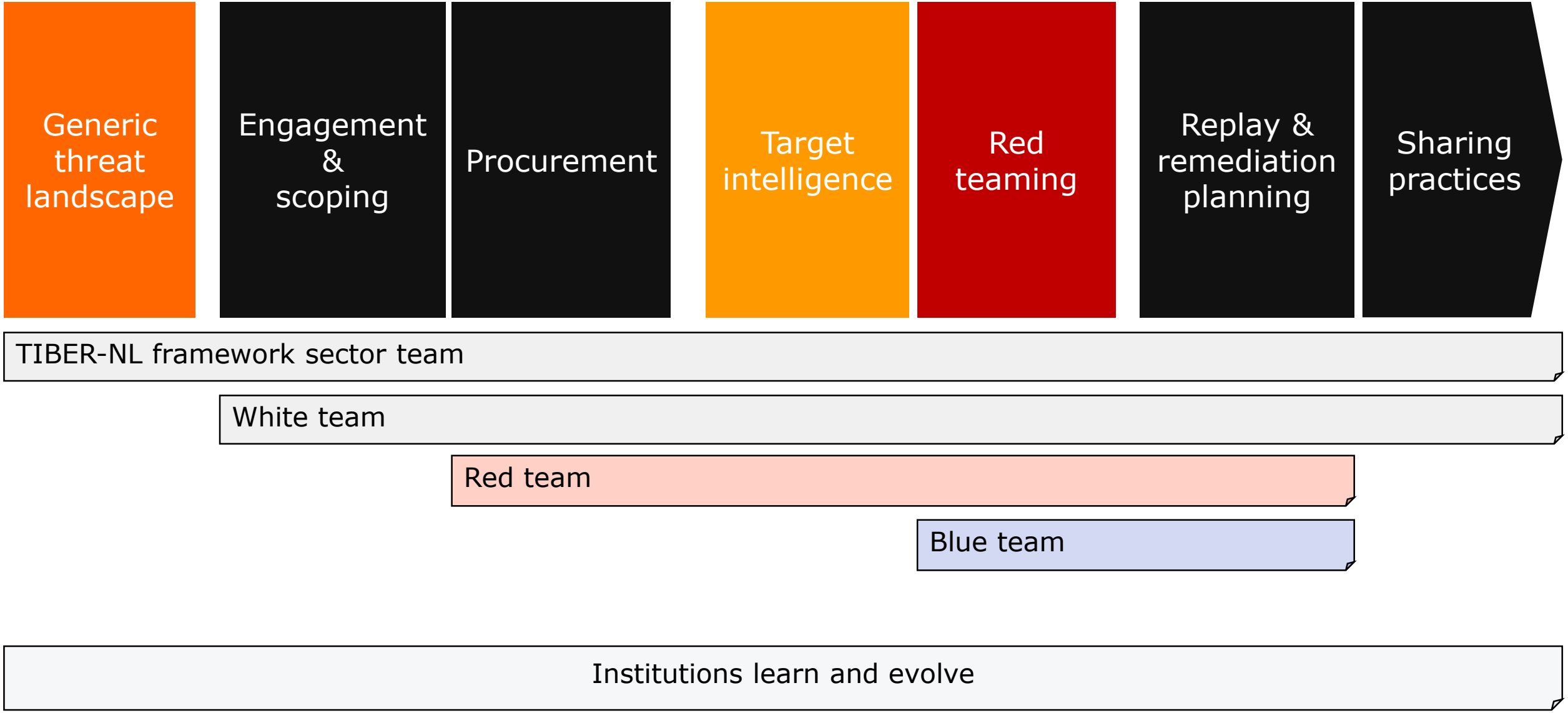
TIBER-NL



Replay (red and blue team, purple teaming)
Remediation

Learning experience by institution self
Sharing good practices with TIBER-NL participants

TIBER-NL:framework roles and involvement



Agenda

1. Introduction
2. Cyber threat landscape
3. Cyber fundamentals and resilience
4. TIBER-NL: attack simulations
5. **Conclusion**

Redteaming: the world from a different perspective

Thank you

Petra Hielkema

Division Director Payments and Market Infrastructures
Dutch Central Bank

p.e.hielkema@dnb.nl

Useful links

CPMI-IOSCO guidance on cyber resilience for financial market infrastructures

https://www.bis.org/cpmi/publ/d146.pdf


Committee on Payments and Market Infrastructures

Board of the International Organization of Securities Commissions

Guidance on cyber resilience for financial market infrastructures

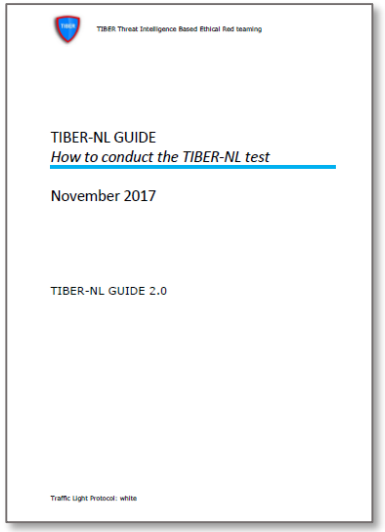
June 2016

BANK FOR INTERNATIONAL SETTLEMENTS

OICU-IOSCO

TIBER-NL guide

https://www.dnb.nl/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365455.pdf?2018032811


TIBER Threat Intelligence Based Ethical Red teaming

TIBER-NL GUIDE

How to conduct the TIBER-NL test

November 2017

TIBER-NL GUIDE 2.0

Traffic Light Protocol: white