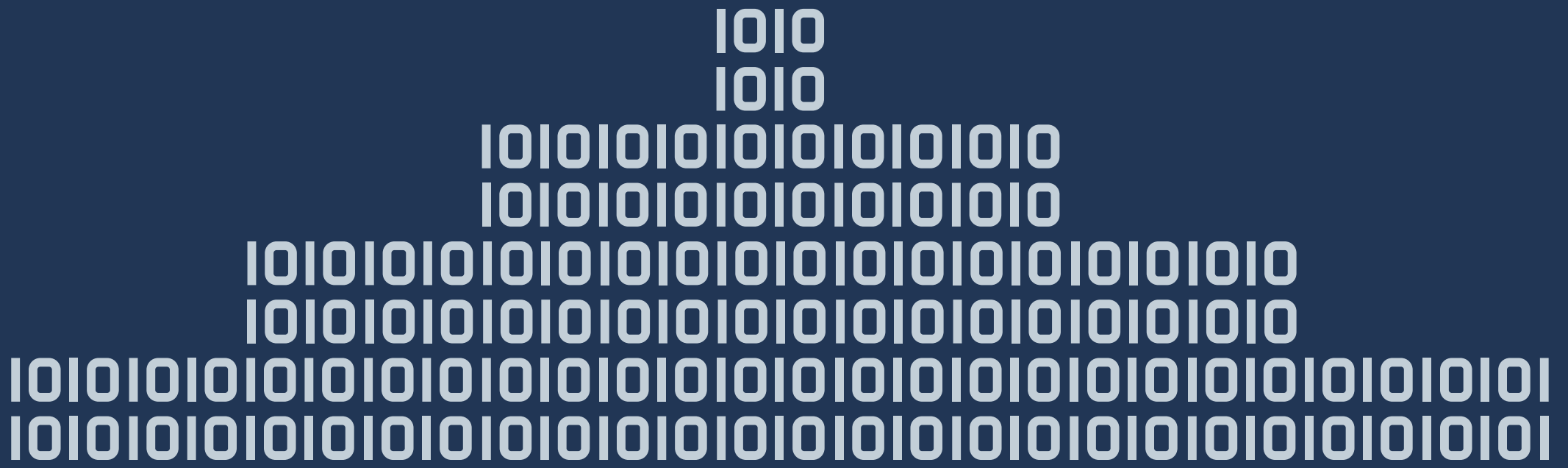
# Den Datensilos ein Ende!

it-sa 2024, zrinka.maslic@kudelskisecurity.com

Unsere Tools produzieren immer

# MEHR DATEN



KUDELSKI SECURITY

Unser Problem sind aber nicht die Daten – es sind

# DATEN-SILOS


KUDELSKI SECURITY

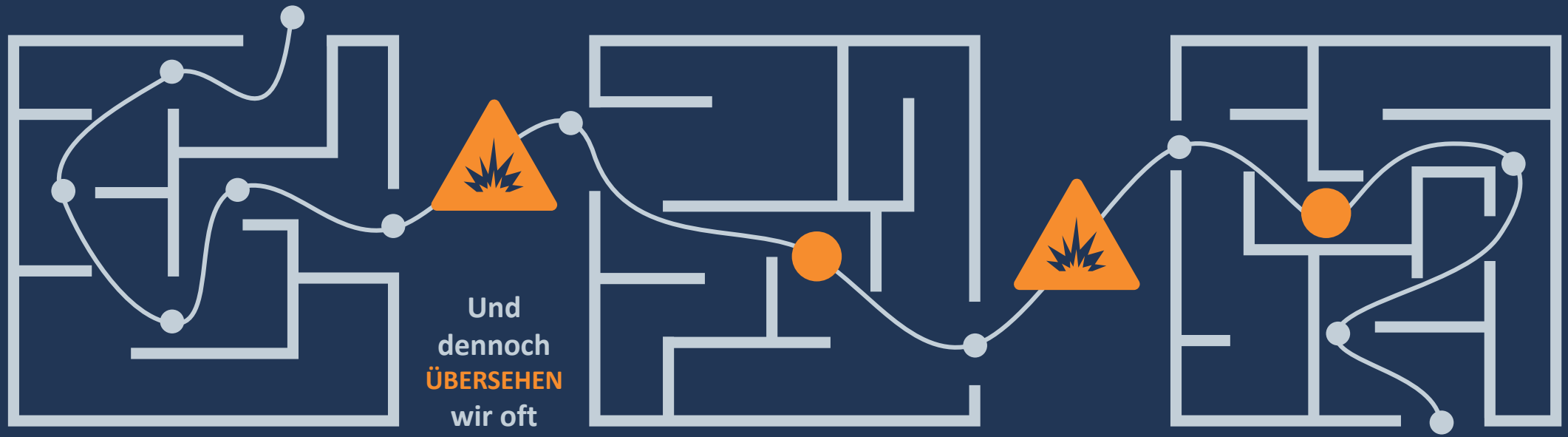
Daten-Silos (ver)brauchen

# UNSERE ZEIT

Wir verbringen immer

**MEHR ZEIT**

mit Analysieren

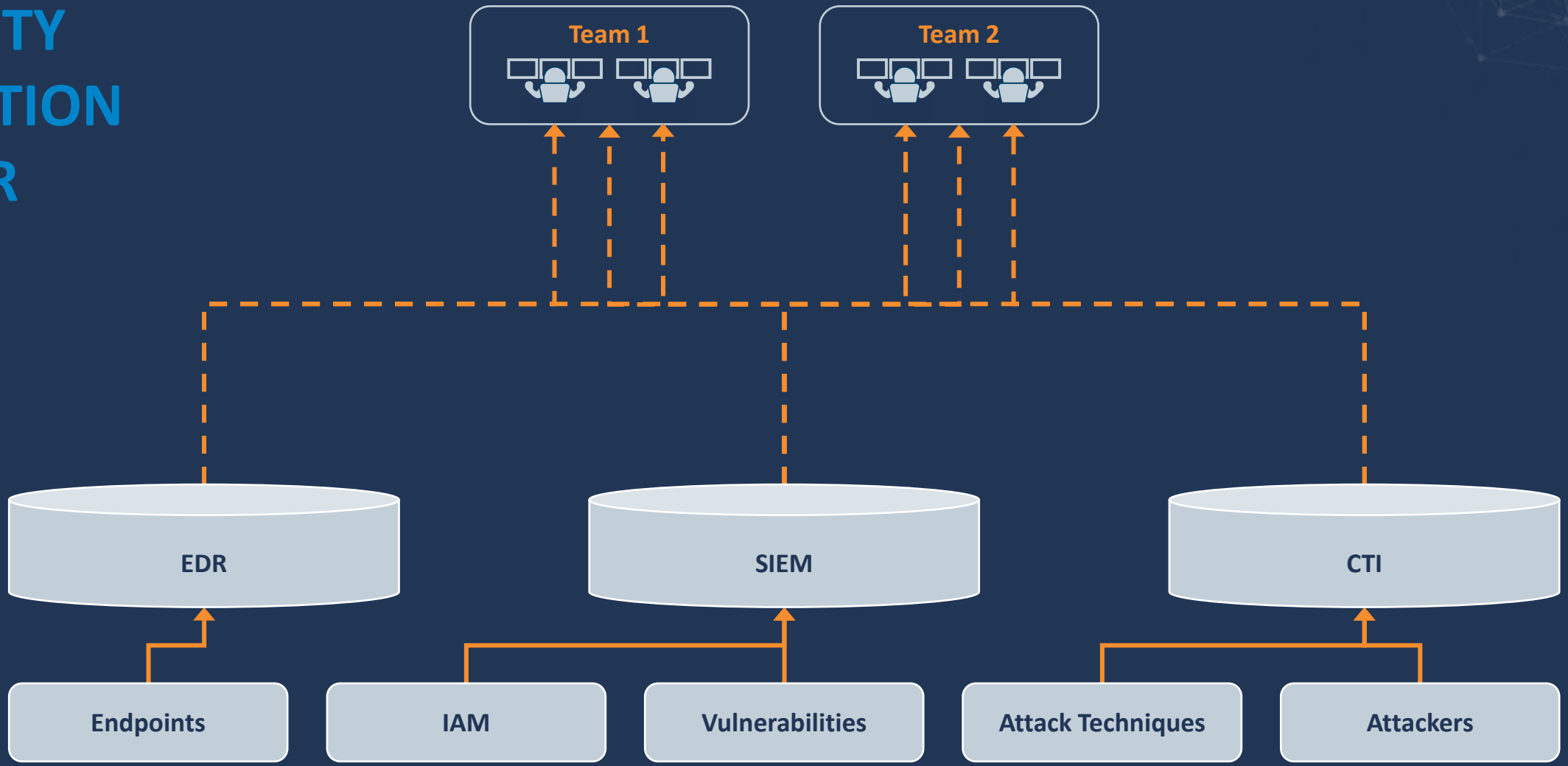


Und dennoch **ÜBERSEHEN** wir oft

**ZUSAMMENHÄNGE**

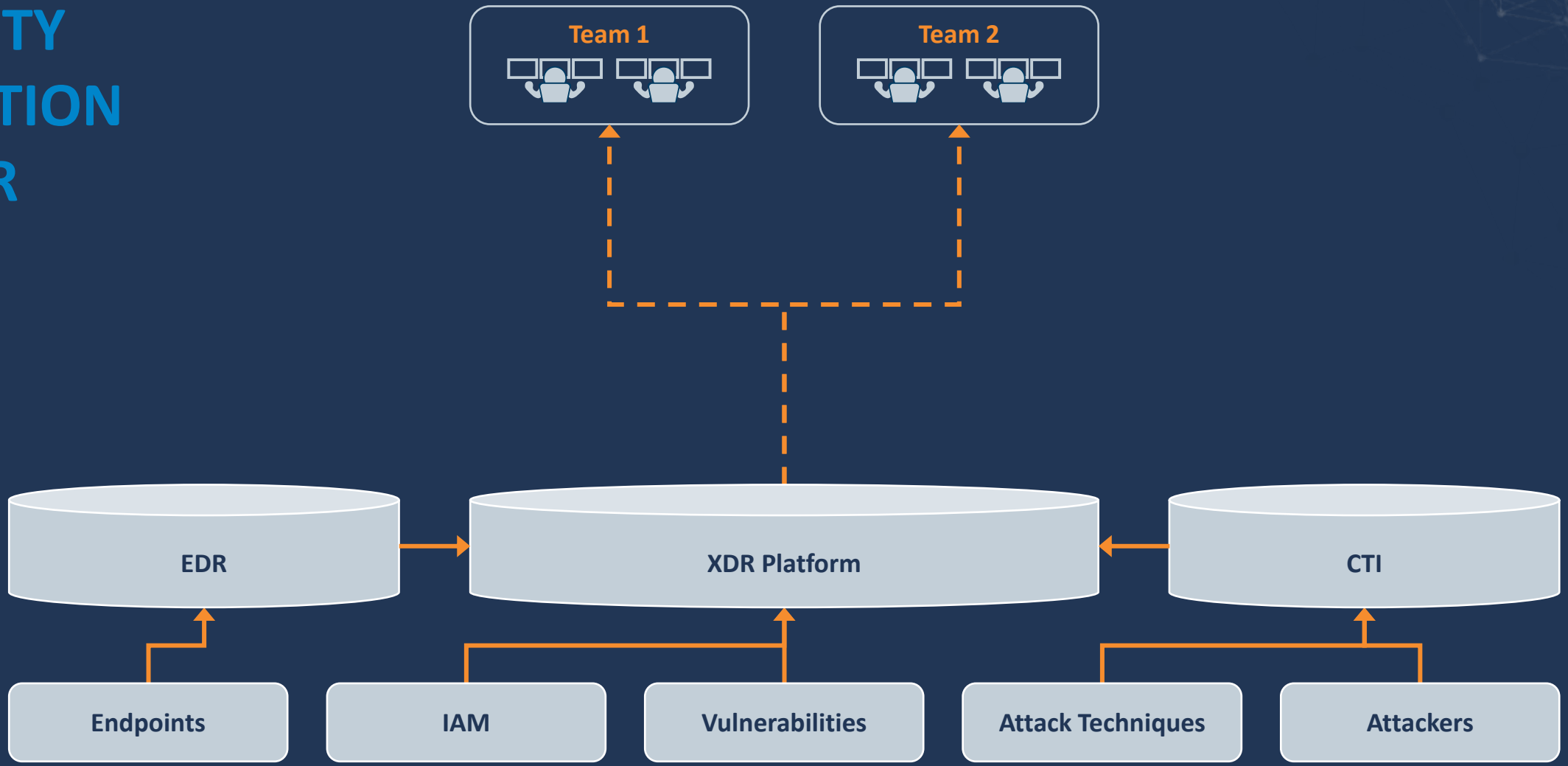
KUDELSKI SECURITY

# TRADITIONELLES SECURITY OPERATION CENTER




KUDELSKI SECURITY

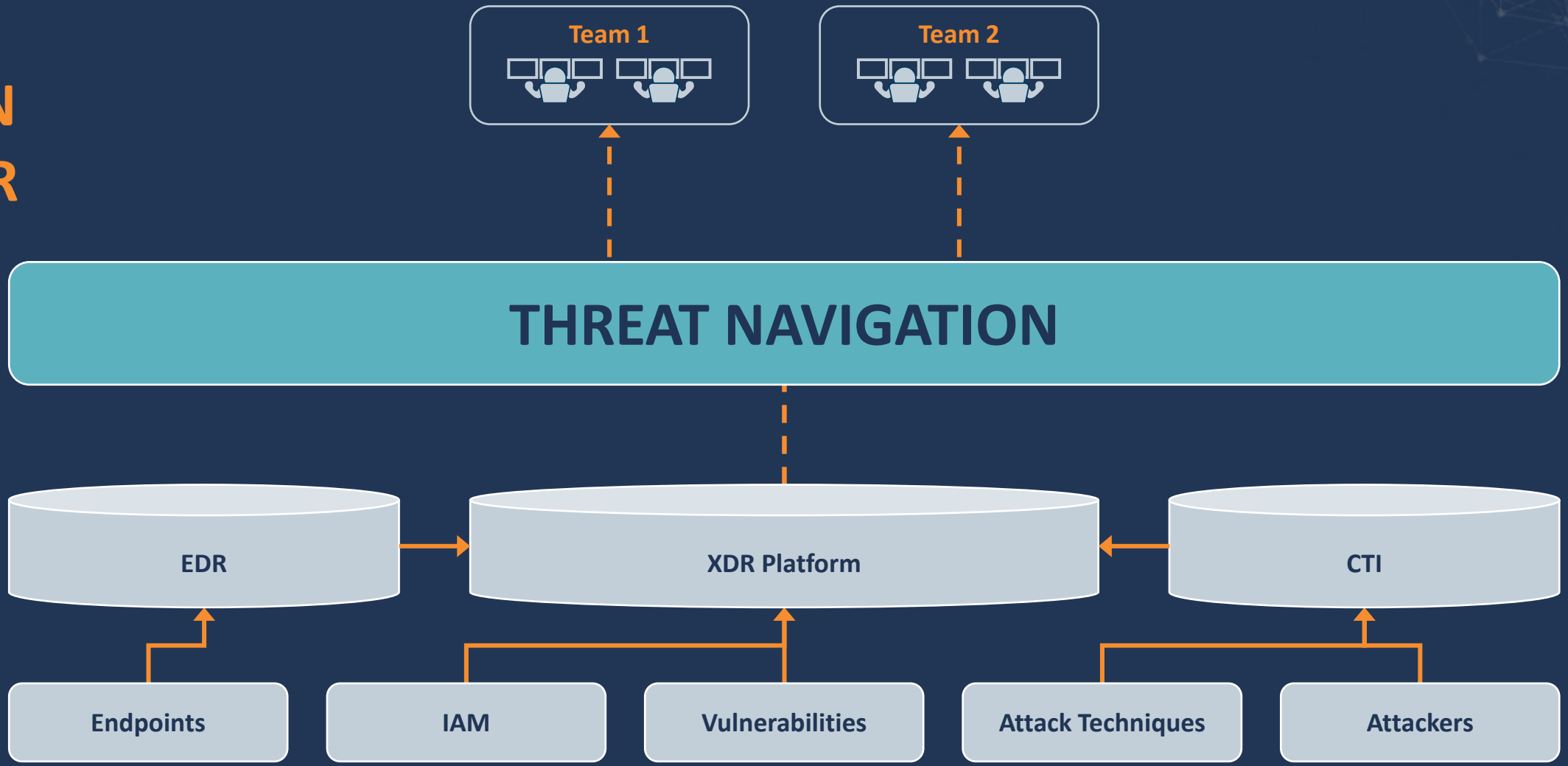
# MODERNES SECURITY OPERATION CENTER




KUDELSKI SECURITY

# KUDELSKI SECURITY

# CYBER FUSION CENTER




KUDELSKI SECURITY

# 1. ANGREIFE IDENTIFIZIEREN



KUDELSKI SECURITY

# 1. ANGREIFE IDENTIFIZIEREN

# 2. ANGRIFFS-TECHNIKEN ABLEITEN

Account Discovery | Application Window Discovery | Browser Information Discovery | Cloud Infrastructure Discovery | Cloud Service Dashboard | Cloud Service Discovery | Cloud Storage Object Discovery | Container and Resource Discovery | Debugger Evasion | Device Driver Discovery | Domain Trust Discovery | File and Directory Discovery | Group Policy Discovery | Log Enumeration | Network Service Discovery | Network Share Discovery | Network Sniffing | Password Policy Discovery | Peripheral Device Discovery | Permission Groups Discovery | Process Discovery | Query Registry | Remote System Discovery | Software Discovery | System Information Discovery | System Location Discovery | System Network Configuration Discovery | System Network Connections Discovery | System Owner/User Discovery | System Service Discovery | System Time Discovery | Virtualization/Sandbox Evasion

KUDELSKI SECURITY

1. ANGREIFE IDENTIFIZIEREN

2. ANGRIFFS-TECHNIKEN ABLEITEN

3. SECURITY-LOGS BESCHAFFEN

Account Discovery | Application Window Discovery | Browser Information Discovery | Cloud Infrastructure Discovery | Cloud Service Dashboard | Cloud Service Discovery | Cloud Storage Object Discovery | Container and Resource Discovery | Debugger Evasion | Device Driver Discovery | Domain Trust Discovery | File and Directory Discovery | Group Policy Discovery | Log Enumeration | Network Service Discovery | Network Share Discovery | Network Sniffing | Password Policy Discovery | Peripheral Device Discovery | Permission Groups Discovery | Process Discovery | Query Registry | Remote System Discovery | Software Discovery | System Information Discovery | System Location Discovery | System Network Configuration Discovery | System Network Connections Discovery | System Owner/User Discovery | System Service Discovery | System Time Discovery | Virtualization/Sandbox Evasion

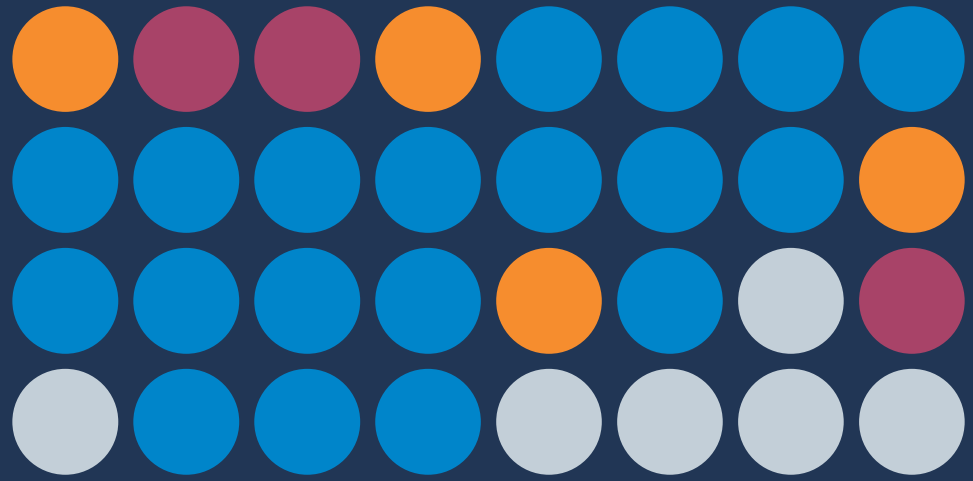
KUDELSKI SECURITY

1. ANGREIFE IDENTIFIZIEREN

2. ANGRIFFS-TECHNIKEN ABLEITEN

3. SECURITY-LOGS BESCHAFFEN

4. PATCHING PRIORISIEREN



Account Discovery | Application Window Discovery | Browser Information Discovery | Cloud Infrastructure Discovery | Cloud Service Dashboard | Cloud Service Discovery | Cloud Storage Object Discovery | Container and Resource Discovery | Debugger Evasion | Device Driver Discovery | Domain Trust Discovery | File and Directory Discovery | Group Policy Discovery | Log Enumeration | Network Service Discovery | Network Share Discovery | Network Sniffing | Password Policy Discovery | Peripheral Device Discovery | Permission Groups Discovery | Process Discovery | Query Registry | Remote System Discovery | Software Discovery | System Information Discovery | System Location Discovery | System Network Configuration Discovery | System Network Connections Discovery | System Owner/User Discovery | System Service Discovery | System Time Discovery | Virtualization/Sandbox Evasion

KUDELSKI SECURITY

# Daten-Silos sind am ENDE.

# Risikobasiertes, kontinuierliches Exposure & Threat Management ist da!

KUDELSKI SECURITY

KUDELSKI SECURITY


## Zrinka MASLIC

Solution Architect

zrinka.maslic@kudelskisecurity.com
www.kudelskisecurity.com