Cybersecurity Konferenz
Frankfurt 29.04.2022

Agenda

Track 1

08:30 Uhr
Registrierung und Frühstück
09:00 Uhr
Eröffnung der Konferenz
09:10 Uhr
Cyber-Sicherheitslage in Deutschland
09:40 Uhr
Business Value Analyse an einem Kundenbeispiel
10:00 Uhr
Kaffeepause

Track 2

10:30 Uhr
Darknet: Ransomware und DDoS as a Service
11:15 Uhr
Angriffsabwehr in Echtzeit und Risikominimierung
12:00 Uhr
Mittagessen

Track 3

13:00 Uhr
Erfahrungsbericht von ProGlove
13:30 Uhr
Expertenrunde: Legacy Technologien vs. Spezialsoftware
14:15 Uhr
Zusammenfassung, Abschluss
14:30 Uhr
Rundgang Lufthansa Trainingszentrum
15:00 Uhr
Erfrischungen, Snacks und individuelle Gespräche

Referenten

Ronny Schubhart
CISO omniIT

Jens Müller
Commercial Sales Director

Dirk Althaus
Cybersecurity Sales Engineer

Abdelkader Cornelius
Technical Engineer Cybereason

Gastsprecher:

Heiko Oberleitner
Global Head of IT ProGlove

Premier Partner

Volle Transparenz

Die omnIT Experten bearbeiten proaktiv die Alarme und Informieren Sie über potenzielle Bedrohungen

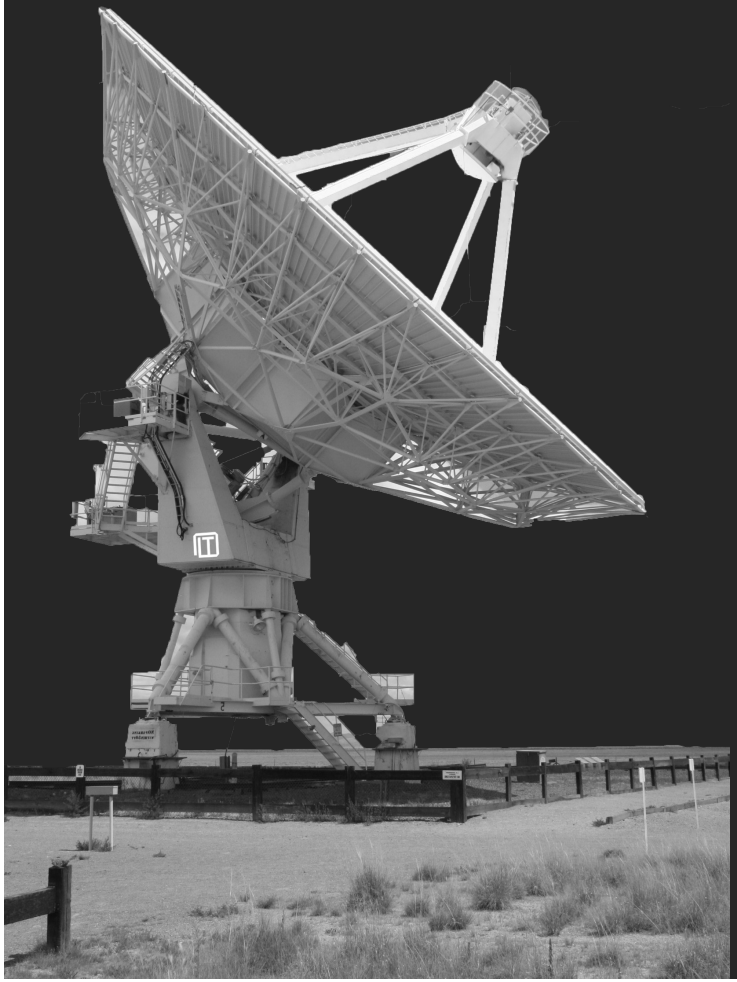
Überwachung und Erkennung

Kontinuierliche Überwachung und routinemäßige Überprüfung von Endgeräten, Servern und Netzen

Echtzeit Unterstützung

Sichere Verbindung zu infizierten Endgeräten, um die verdächtigen Dateien, Prozesse oder Verbindungen zu analysieren und zu beheben.

Zahlen Daten Fakten



München

Hauptsitz im
#IsarValley

1 Mio.
Stunden Projekterfahrung

20+
Cloud & Security
Experten

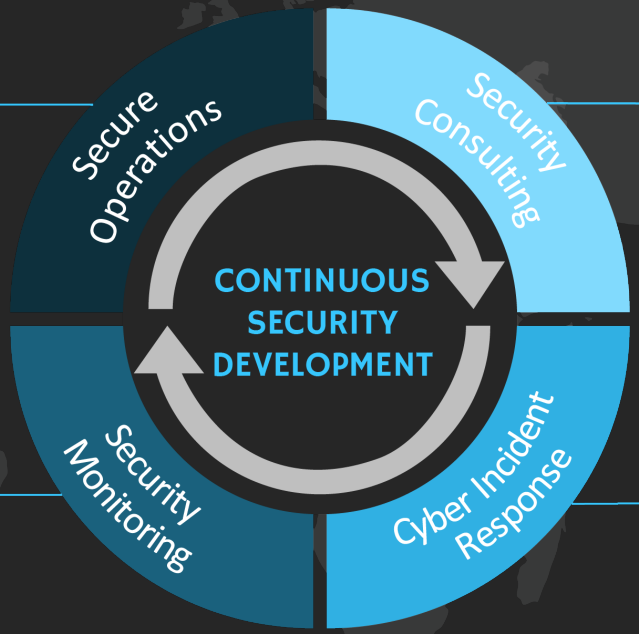
100+
Unterstützte Technologien

International
Nearshore Center

100%
Nachhaltig
Reduktion des CO2-Fußabdrucks um 70%

OUR HOLISTIC CYBER SECURITY APPROACH BASED ON AN END-TO-END DEFENSE STRATEGY

Cyber Security Defense



Secure Operations

- Firewall & NAC
- IPS/IDS
- Endpoints & Mobile Devices
- Content & Web Security
- Network, & OS Hardening
- Managed Detection & Response

Active Threat Hunting

- Managed Detection and Response
- Managed SIEM
- Vulnerability Management
- Root Cause Analysis
- Compliance Monitoring

Consulting

- Penetration Testing
- Red Team/Blue Team Assessments
- Digital Forensics
- Code Analytics
- Risk Assessments
- Cyber Security Awarness Trainings

In-depth-Analysis

- Investigation and Analysis
- Containment of the Breach
- Eradication and Remediation
- Recovery of Operations
- Improvement and optimization


cybereason
Ransomware - EDR
Jens Mueller
Commercial Account Manager
Jens.muller@cybereason.com

Allianz Risk Barometer 2022

1
↑ 44%
2021: 3 (40%)

Cyber incidents
(e.g. cyber crime, IT failure/ outage, data breaches, fines and penalties)

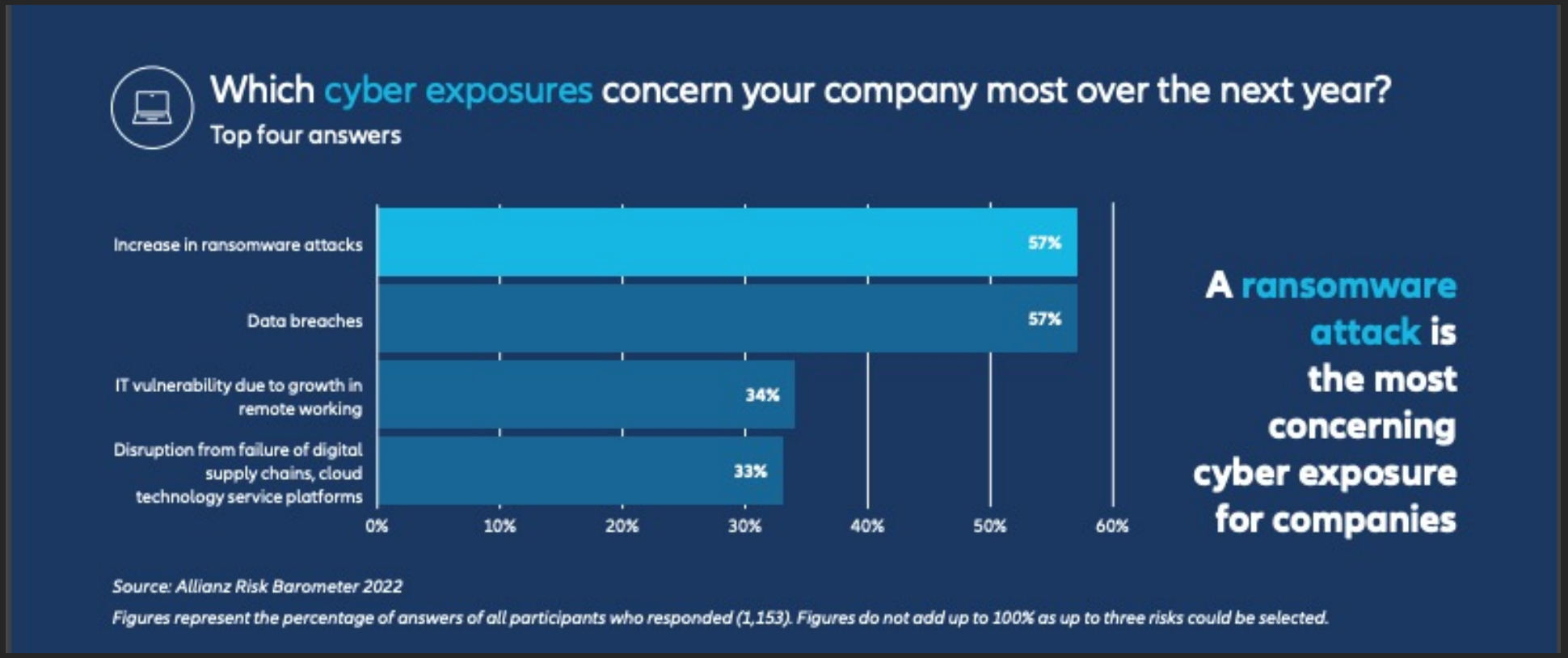
2
↓ 42%
2021: 1 (41%)

Business interruption
(incl. supply chain disruption)

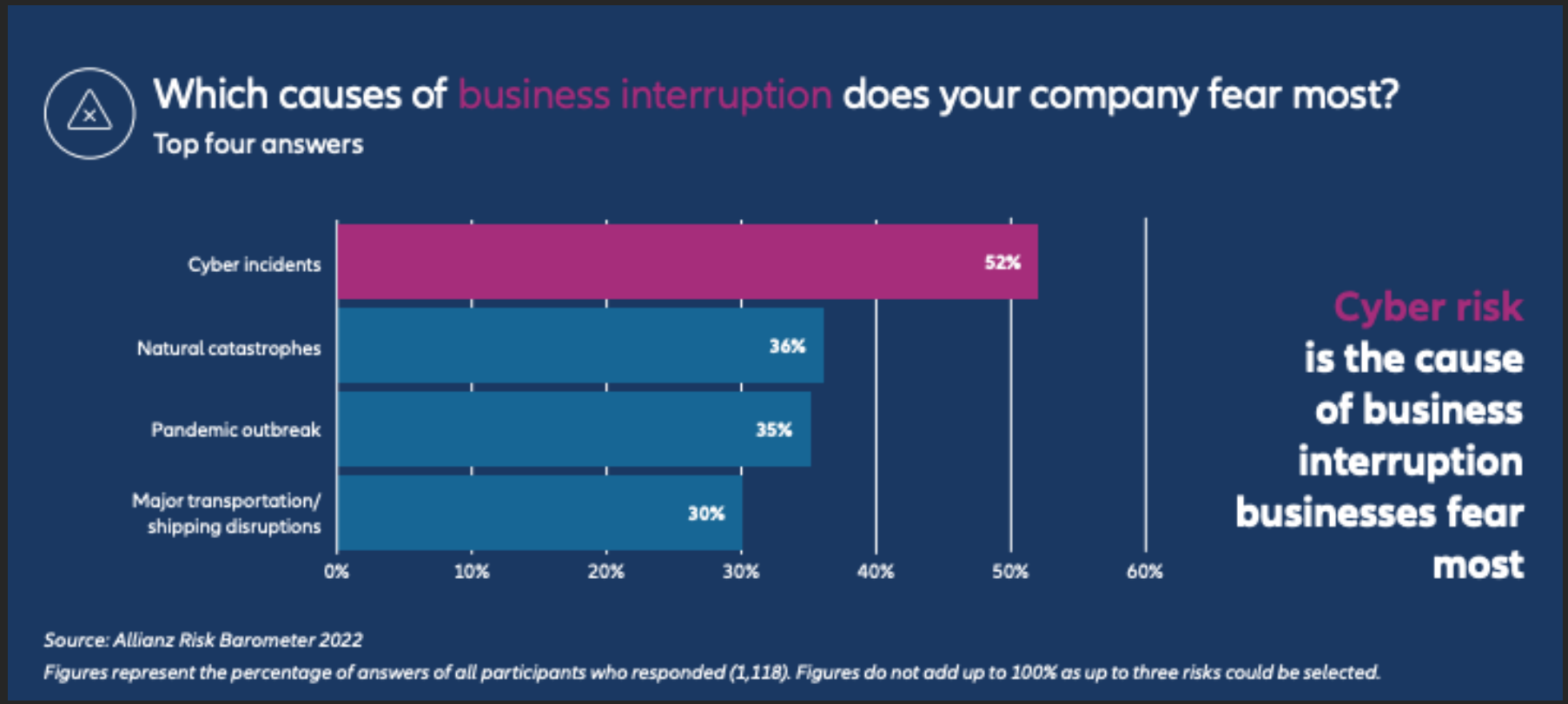
3
↑ 25%
2021: 6 (17%)

Natural catastrophes
(e.g. storm, flood, earthquake, wildfire, weather events)

Allianz Risk Barometer 2022

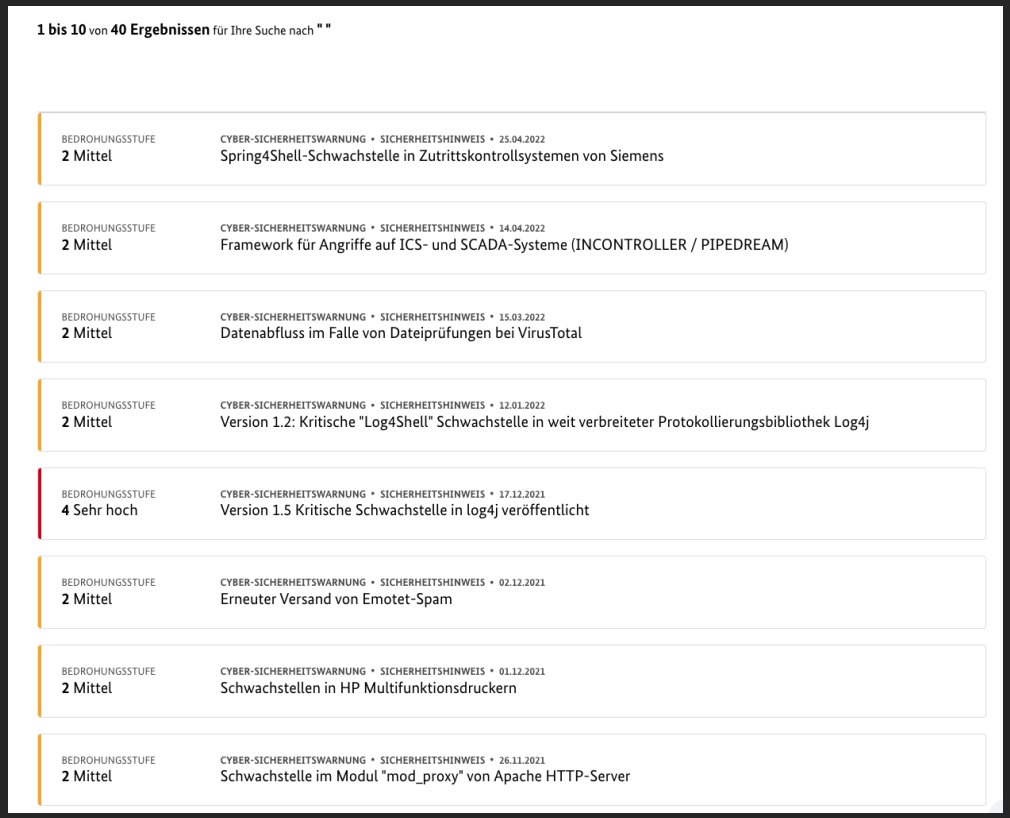


Allianz Risk Barometer 2022



Aktuelle Bedrohungen BSI

https://www.bsi.bund.de/SiteGlobals/Forms/Suche/BSI/Sicherheitswarnungen/Sicherheitswarnungen_Formular.html?cl2Categories_DocType=callforbids



1 bis 10 von **40 Ergebnissen** für Ihre Suche nach " "

BEDROHUNGSSTUFE	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • DATUM
2 Mittel	Spring4Shell-Schwachstelle in Zutrittskontrollsystemen von Siemens
2 Mittel	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 14.04.2022 Framework für Angriffe auf ICS- und SCADA-Systeme (INCONTROLLER / PIPEDREAM)
2 Mittel	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 15.03.2022 Datenabfluss im Falle von Dateiprüfungen bei VirusTotal
2 Mittel	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 12.01.2022 Version 1.2: Kritische "Log4Shell" Schwachstelle in weit verbreiteter Protokollierungsbibliothek Log4j
4 Sehr hoch	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 17.12.2021 Version 1.5 Kritische Schwachstelle in log4j veröffentlicht
2 Mittel	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 02.12.2021 Erneuter Versand von Emotet-Spam
2 Mittel	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 01.12.2021 Schwachstellen in HP Multifunktionsdruckern
2 Mittel	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 26.11.2021 Schwachstelle im Modul "mod_proxy" von Apache HTTP-Server

Informationen und Empfehlungen

Aktuelle Nachrichten und Ereignisse

- 2021: Colonial Pipeline
  Von allen Cyber- und Ransomware-Angriffen im Jahr 2021 hatte die Verletzung der Colonial Pipeline Ende April die meiste Berichterstattung.
- 2021: JBS Foods
  Eines der größten fleischverarbeitenden Unternehmen der Welt zahlt eines der größten
  Erpressungsgelder aller Zeiten
- 2021: Mediamarkt / Saturn
  Betroffen sind offenbar die Kassen- und Warenwirtschaftssysteme in den Filialen. Es seien "mehrere Windows-Server" mit einem Krypto-Virus infiziert worden, heißt in offenbar internen Dokumenten, die auf Twitter kursieren. Insgesamt seien 3100 Server
  betroffen.
- 2021:Solarwind
  Als ein IT-Überwachungssystem hat SolarWinds priviligierten Zugriff auf IT-Systeme.
  Bei diesem Angriff erhielten die Häcker Zugriff auf Tausende von SolarWinds Kunden.

Ideen und Konzepte

- Locard’s Principle
- Asymmetricher Cyberangriff
- Der Angreifer ist immer schneller als das Opfer

Aktuelle Lage in der IT

An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Report

National Cyber Awareness System > Alerts > Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

Alert (AA22-110A)

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructu

Original release date: April 20, 2022

Print Tweet Send Share

Summary

The cybersecurity authorities of the United States[1][2][3], Australia[4], Canada[5], New Zealand[6], and the United Kingdom[7][8] are releasing this joint Cybersecurity Advisory (CSA). The intent of this joint CSA is to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners.

Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the March 21, 2022, Statement by U.S. President Biden for more information). Recent Russian state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations.

Deutschland

fährdungsstufe „Orange“ aus.
ehörden bereiten sich auf den Ernstfall vor.

Heute

st befürchteten Angriffe haben
funden, das wird sich aber mit
er Lieferung schwerer Waffen
voraussichtlich ändern.

Betroffenheit

iel ist die Störung von, für die
versorgung oder wirtschaftlich
evanter Firmen auch über die
Supply Chain.

Geopolitisch

Der Angriff auf die Ukraine hat auch Auswirkungen auf die IT-Sicherheit beteiligter Staaten

Veränderungen

Die Abwehrmöglichkeit von Angriffen sinkt von Monaten auf Tage.

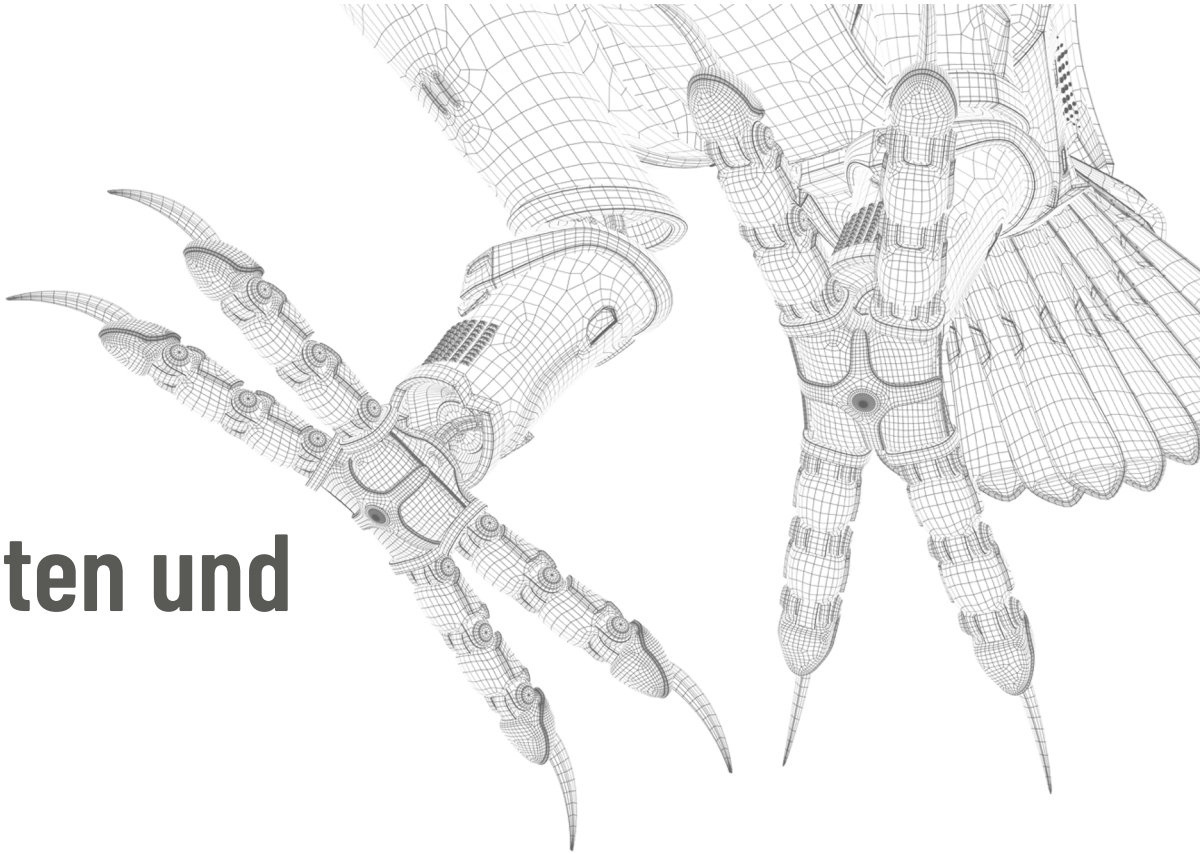
Indikatoren

Black Energy, NotPetya; Colonial Pipeline

Gegenmaßnahmen

Unmittelbare Reaktionsfähigkeit notwendig

Cybereason Möglichkeiten und Bausteine



cybereason®

Sichtbarkeit

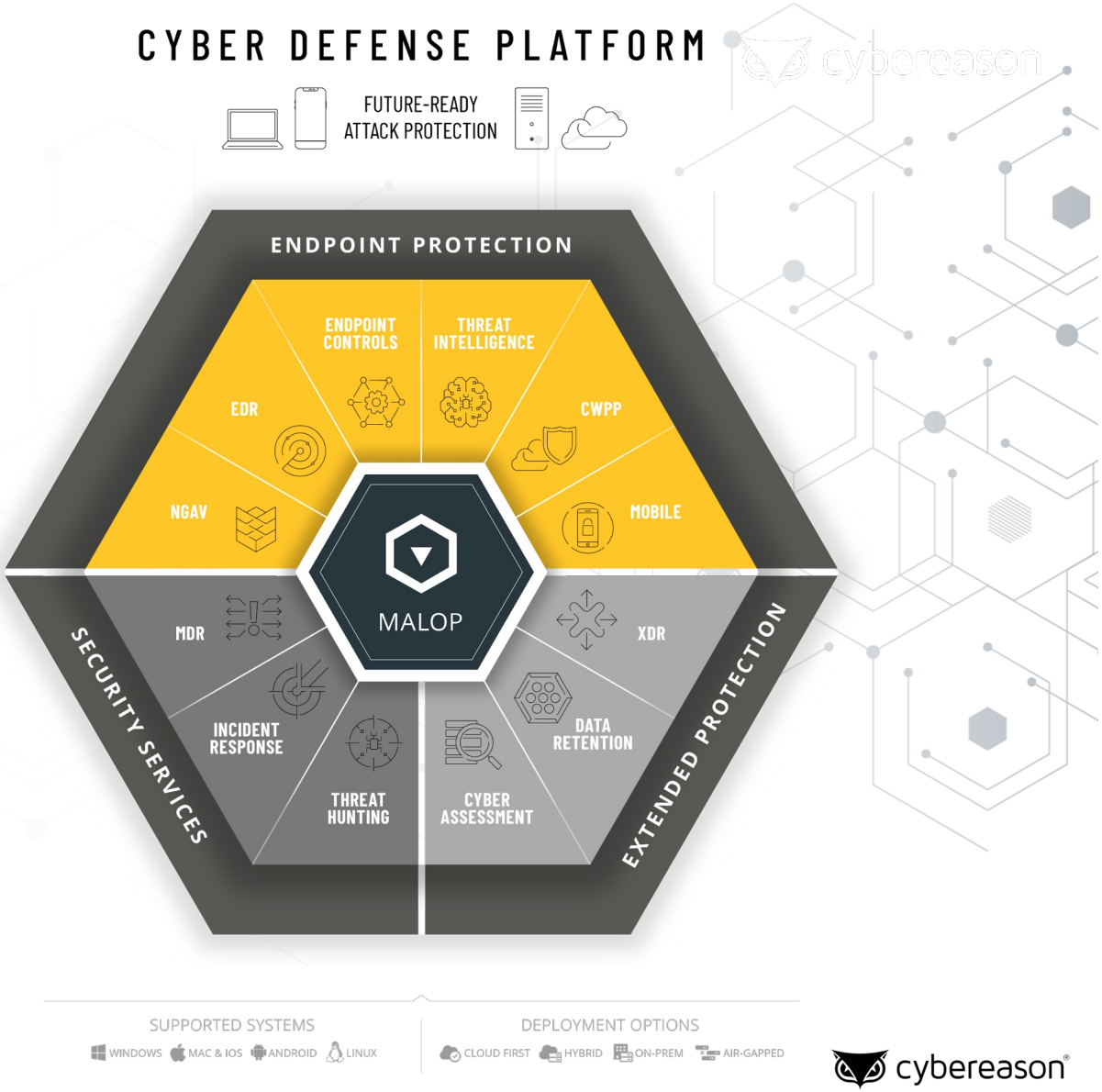
Böswillige Operationen erkennen

Geschwindigkeit

Angreifer überraschen

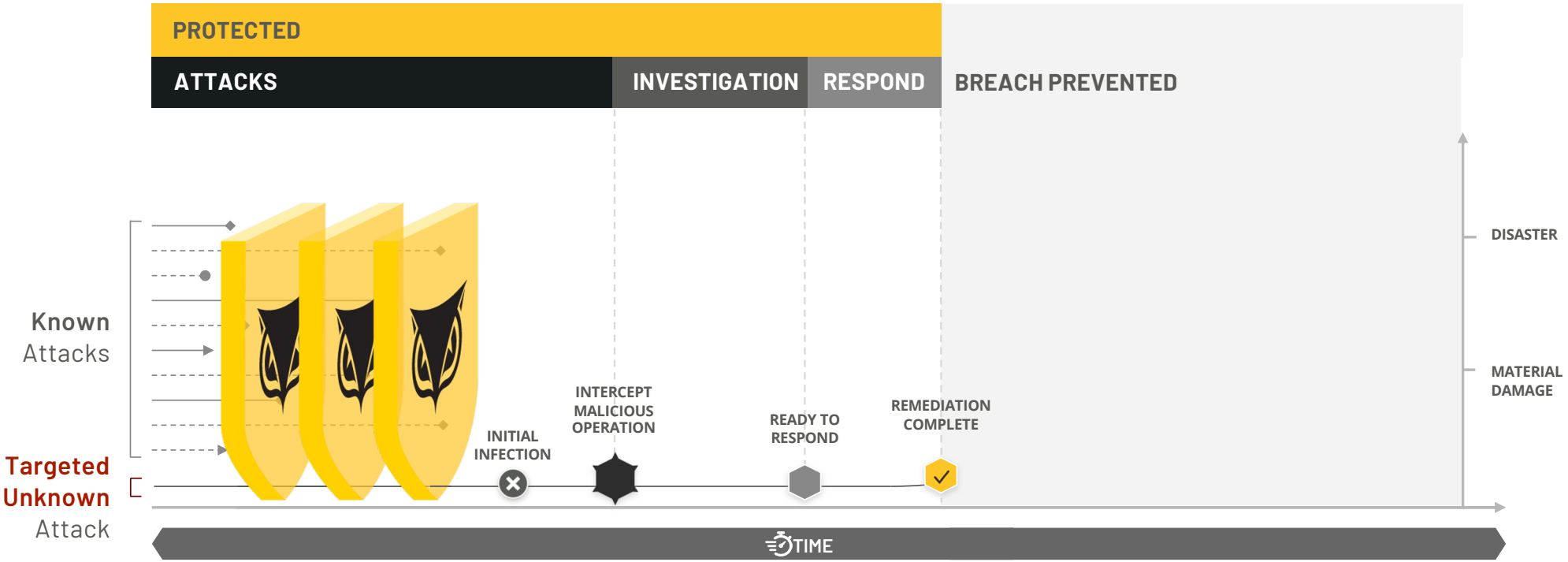
Prezision

Angriffe beenden



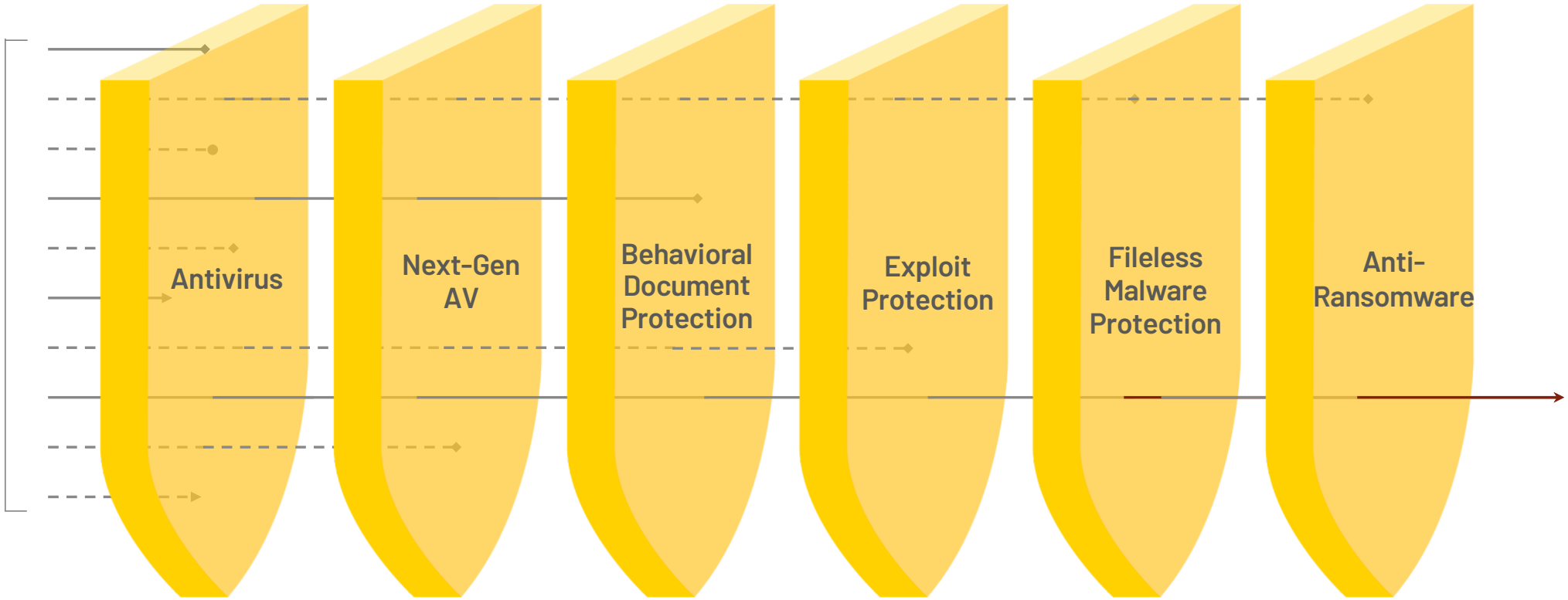
OPERATION-CENTRIC SECURITY

The Ideal State



cybereason®

MULTI-LAYERED PREVENTION



cybereason

CYBEREASON DIFFERENTIATORS

Nutzen Sie alle Ihre Daten

Die Qualität Ihres Schutzes hängt von der Qualität Ihrer Daten ab

OPERATION-CENTRIC: THE MALOP™

Sie haben keine Zeit, durch einen Ozean von Warnungen zu schwimmen, um diejenige zu finden, die wichtig ist

FUTURE-READY ATTACK PROTECTION

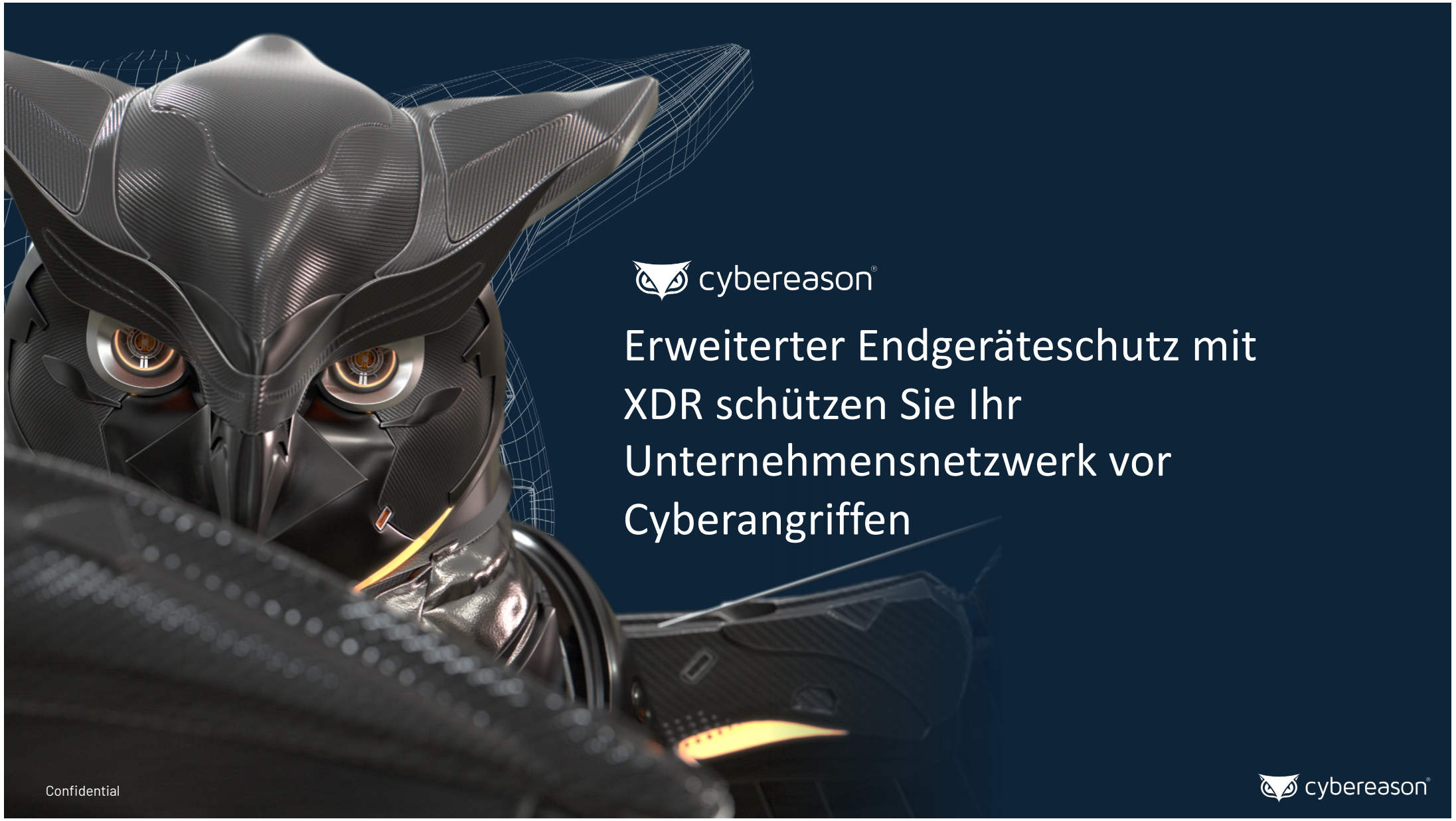
Schützen Sie die Endpunkte von heute und sichern Sie das Unternehmen für morgen zukunftssicher

Verhindern Sie automatisch Angriffe

Die integrierte automatische Korrektur reduziert die MTTR von Tage auf Stunden

Verhaltensbasierte Erkennung

Fangen Sie Angreifer anhand ihres Verhaltens, nicht nur anhand ihrer Hashes



cybereason®

Erweiterter Endgeräteschutz mit XDR schützen Sie Ihr Unternehmensnetzwerk vor Cyberangriffen

cybereason®

Was ist Advanced XDR ?

Vorteile Advanced XDR

Warum ist Advanced XDR wichtig für moderne Sicherheit ?

Warum haben die Angreifer einen Vorteil ?

Isolierte Einzellösungen sind teuer und haben begrenzte Visibilität

RISK: Bereiche mit ”Null” oder ineffektiver Abdeckung

Die Untersuchung von Warnungen erfordert vielfältiges und erfahrenes Fachwissen

RISK: Faktor Mensch, Fachwissen, Personalmangel

Begrenzte und langsame Reaktion der Verteidiger

RISK: Eingeschränkte Incident Control (z.B. bei Datendiebstahl oder Ransomware)

cybereason

Was können Sie von XDR erwarten

INTEGRATION in meine sich entwickelnde nicht homogene

Infrastruktur

Hilfe um **ADVANCED ATTACKS zu finden und zu Untersuchen.**

Verbessern Sie Ihre **INCIDENT RESPONSE Geschwindigkeit & Genauigkeit.**

cybereason®

Cybereason XDR powered by Google Chronicle

Angriffe voraussagen, verstehen und mit einer ganzheitlichen Sicht beenden.

1 detect | **5** triage | **30** respond

GANZHEITLICHER SCHUTZ

- Schützen Sie Benutzer und Assets vor Ransomware und Top-Angriffen
- 100% Schutz in MITRE ATT&CK Evaluation
- Entwickelt für Skalierbarkeit und Geschwindigkeit

10X SCHNELLERE INCIDENT RESPONSE

- Geführte Reaktion im gesamten Netzwerk
- Automatisierte Suche und Reaktion im Petabyte Bereich
- Branchenführende SLAs für Erkennung, Einstufung und Reaktion

ANGRIFFSVERHALTEN VORHERSEHEN

- XDR, das zukunftige Angriffe und Risikobereiche vorhersagt
- Überprüfen Sie Ihre SOC Effizienz und verbessern Sie Ihre Reaktionszeit

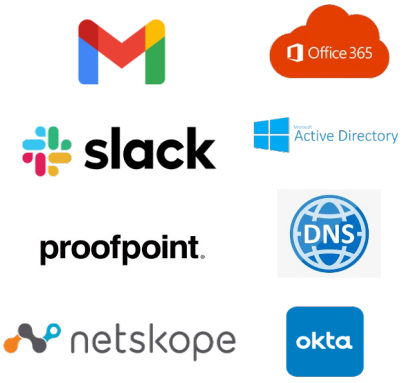
cybereason

XDR Use-Cases

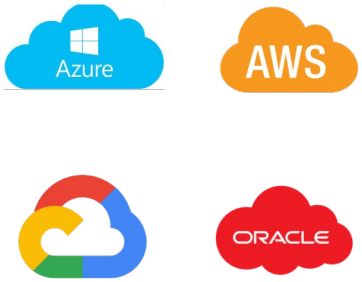
End Cyber Attacks Anywhere

ENDPOINT

WORKSPACE & IDENTITY



CLOUD



NETWORK

cybereason

Q&A