

Prescriptive Security Cyberbedrohungen neutralisieren, bevor sie eintreten

Einleitung

Kontext und Einordnung von Prescriptive Security

Teil 1 – Wahrnehmung

Cyber Bedrohungen
und Angriffe



Cyber Security Strategie

Cyber Bedrohungen und
Angriffe auf Ihre Organisation

Massnahmen für mehr Cyber
Security und weniger Risiken

Risiken der
Organisation



Teil 2 – Massnahmen

zur **Prävention**

zur **Reaktion** bei Angriffen

zur **Stabilisierung**

Prescriptive
Security

Security
Management

Wiederherstellung und
Verbesserung

7x24 Cyber Security Operation Center

Cyberbedrohungen und -Angriffe

Ein ständiger Wettlauf der Gegenmassnahmen

Die schwierige Frage:
Was ist das eigentliche
Ziel der Täter?

*Ich bin Creeper:
Fang mich, wenn du kannst!*

Vom Virus
als Scherz ...

*Antwort von Reaper:
Ich kann!*

Anzahl 2018
800 Mio.

... bis zum
Angriff mit KI

Anzahl 2012

Schadprogramme 100 Mio.

Spionage
Sabotage
Cyber
Crime
War
Hacktivism

Gegenmassnahmen
1970

+

+

+

2019 +

Antivirus
Programme

Mehrschichtige
Sicherheitskonzepte

Globale Reputation
& Sandboxing

Fortgeschrittene Analytik
& künstliche Intelligenz (KI)

Cybercrime als Service, ein etabliertes Geschäft

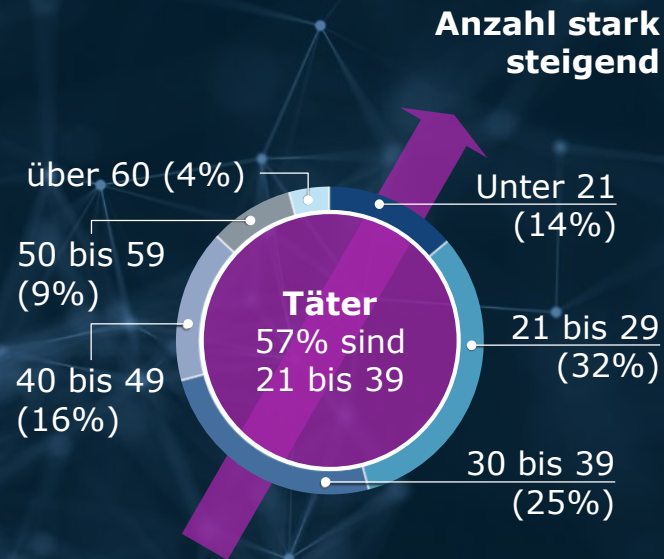
Täter benötigen keine tiefgehende technische Kenntnisse

Digitale Schwarzmärkte: Ausgangspunkt für Cybercrime

- Anfrage und Verkauf von Daten unterschiedlicher Art
- Malware Herstellung und Verteilung von Schadsoftware
- Illegale Plattformen für Handel mit Waffen, Menschen, ...
- ...

Im Auftrag des «Kunden» hergestellt. Mit Bitcoin bezahlt!

- Ransomware zur digitalen Lösegelderpressung
- Botnetze zur Massenfernsteuerung von Geräten für Angriffe
- DDoS-Angriff zur Verhinderung von Service-Verfügbarkeiten
- ...



Risiken der Organisation

Cyberbedrohungen auf Platz 2

Top 5 Risiken die Organisationen fürchten

1 Betriebsunterbruch

2 Cyberrisiken

3 «Digitaler Wandel»

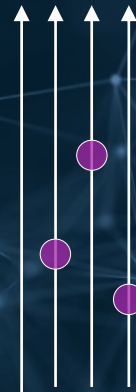
4 Naturkatastrophen

5 Fachkräftemangel

Zunahme der
Cyberbedrohungen

Ihre
Cyber
Risiken

Global



Profil der
Organisation

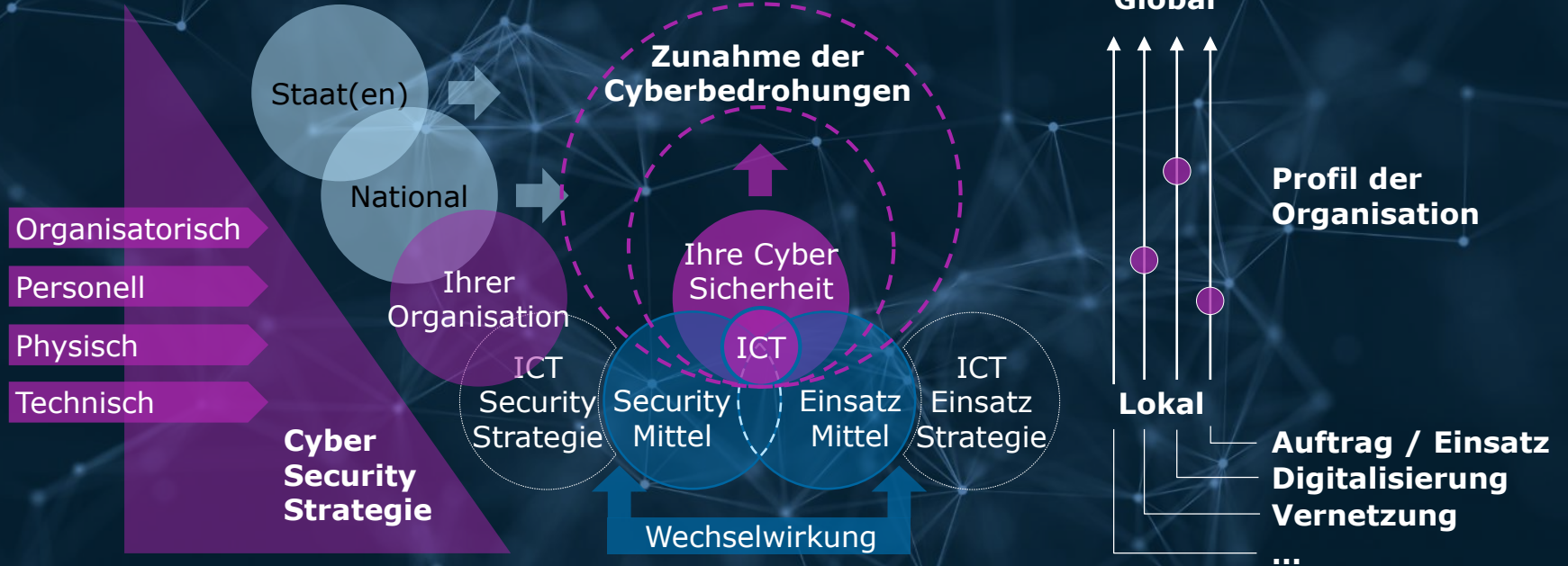
Lokal

Auftrag / Einsatz
Digitalisierung
Vernetzung
...

Cyber Security Strategie

Alle Massnahmen um Cyberrisiken zu reduzieren

Cybersicherheit ist mehr als ICT Sicherheit und betrifft alle!



Zwischenfazit

Prescriptive Security

Teil 1 – Wahrnehmung

800 Mio. Schadprogramme
2018



Cyber Security Strategie

Die schwierige Frage: Was ist das
eigentliche Ziel der Täter?

Cybersicherheit ist mehr als
ICT-Sicherheit und betrifft alle

Cyber Risiken
Platz 2



Teil 2 – Massnahmen

zur **Prävention**

Prescriptive
Security

zur **Reaktion** bei Angriffen

Security
Management

zur **Stabilisierung**

Wiederherstellung und
Verbesserung

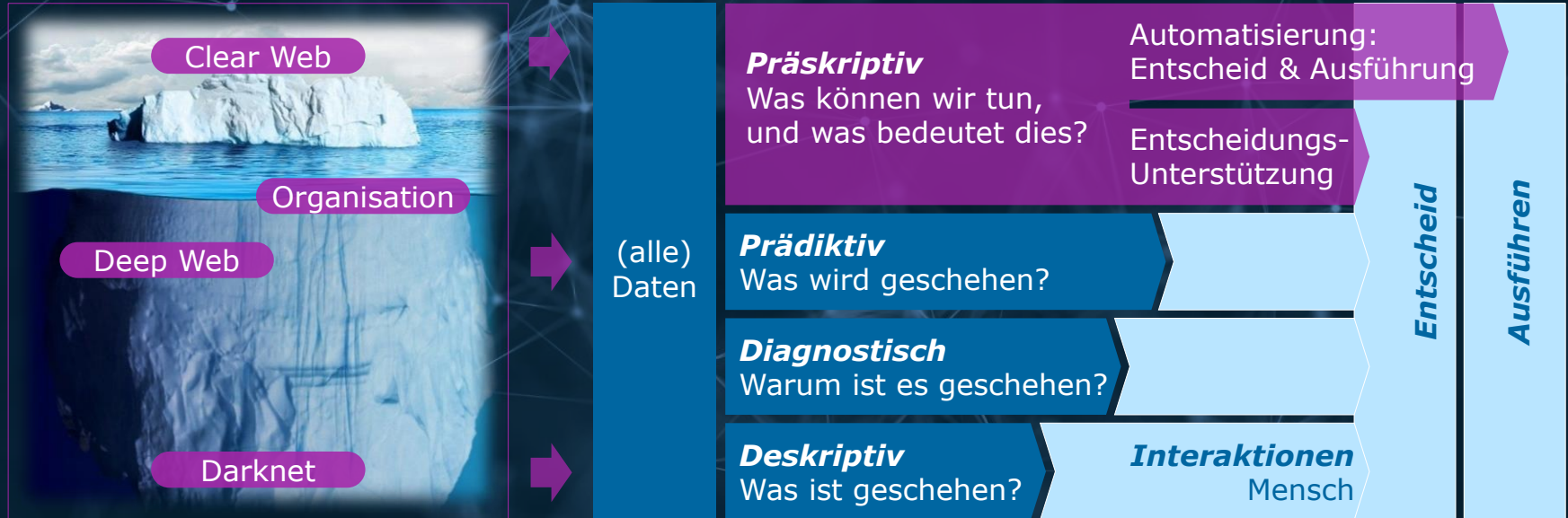
7x24 Cyber Security Operation Center

Ansatz von Prescriptive Security

Big Data + Analytik + künstliche Intelligenz (KI) + menschliche Interaktion, wenn Automation nicht möglich

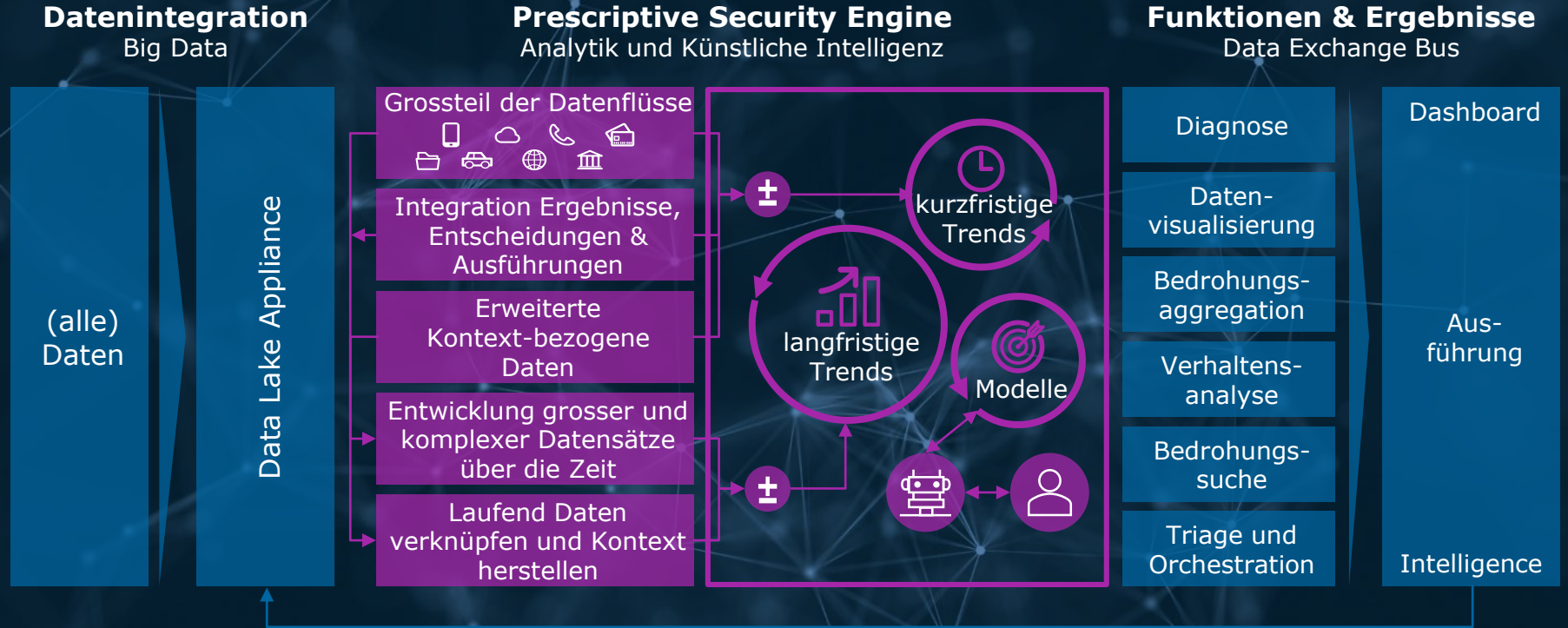
1 Nutzung (aller) Daten, um Bedrohungen zu finden

2 Nutzung fortgeschrittene Analytik + Künstliche Intelligenz (KI)



Funktionsweise Prescriptive Security

Eine End-to-End Betrachtung



Prescriptive Security – Ergebnisbeispiel 1

Cybercrime im weiteren Sinne



SIG Sauer P226 AL SO DAO, Kal. 9mmP

New and unused and unregistered!
Ammo can only be purchased if you also buy the

Product	Price	Quantity
SIG Sauer P226 AL SO DAO, Kal. 9mmP	790 EUR = 0.112 €	1 x Buy now



Black List Cyber Kahilafah: United States Government And Military - The Head Of The Crusader Coalition - Phone Numbers and Location Information Leaked Peace Be Upon The One Who Fights Towards the Islamic State and your bombing campaign against the muslims, know that we are recording your every move, we have your names and addresses, we are in your email and passing on your personal information to the soldiers of the khilafah, who soon will be in your lands! "So wait; we too are waiting" - Islamic State Hacking Division Full Name: [redacted] City / State Zip Code Phone / Cell [redacted] Colorado Spring [redacted] Hunter 200th MMC - US Army [redacted] [redacted] SCHOFIELD BARRA 96857 80865625 [redacted] APO 9459 1.14416E-13 EMIN [redacted] B42455E325A4EFA6 ADANA [redacted] Hood [redacted] [redacted] region5 APO [redacted] Washington 20005 [redacted] Foundation [redacted] washington 20005 [redacted] WASHINGTON 20005 202 [redacted]

Prescriptive Security – Ergebnisbeispiel 2

Cybercrime im engeren Sinne

Angebot gestohlener Login-Daten

Erweiterte Analyse

Präventive Handlung

Täter nutzt die Login Daten

2

Nutzerverhalten

Zielsystem sperrt den Zugang

Anweisung des Zielsystems

Entscheidung automatisiert

Prescriptive Security findet die Bedrohung

1

Email mit Login Daten abgefangen

Darknet

Alert/Stream	Deep + Dark Webs	Results	Domains	Emails with password or hash
Semantic Scope (keyword)				
@ [redacted] ch	26	3	2	
@ [redacted] ch	154	14	13	
@ [redacted] ch	22	3	0	

Timeline: 1994, 1999, 2004, 2008

Alerts: 23/07, 07/07, 09/07

Zusammenfassung Prescriptive Security

Was können wir tun, um Cyberbedrohungen zu neutralisieren, bevor sie eintreten?

1 Nutzung (aller) Daten, um Bedrohungen zu finden



2 Aufbau der Prescriptive Security Fähigkeiten

Spezialisten Teams & Tools

Kommunikationsplattform

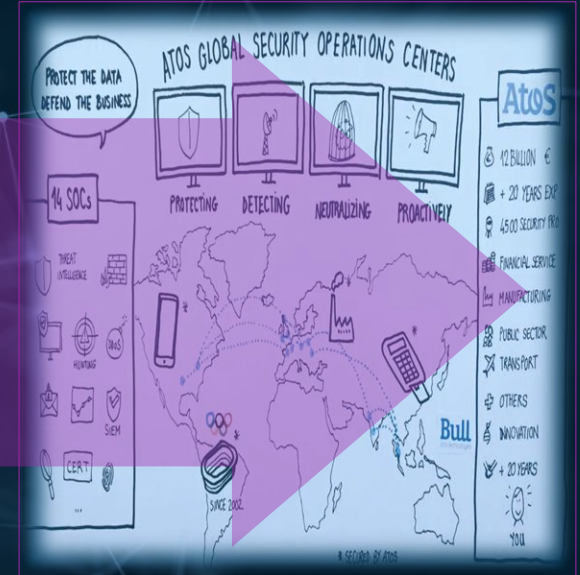
Entscheidungsalgorithmen

Fortgeschrittene Analytik + KI

Echtzeit Datenanalyse

Supercomputing-Infrastruktur

3 Etablierung im 7x24 Cyber Security Operation Center



▶ mehr ...

Wir danken Ihnen für Ihr Interesse
und freuen uns auf Ihren Besuch am Stand



Jürg Scheidegger
Senior Management Consultant

juerg.scheidegger@atos.net
+41 79 794 63 59



Patrik Bengtsson
Senior Cyber Security Consultant

patrik.bengtsson@atos.net
+41 78 691 04 22