SIEMst du noch, oder MXDRst du schon?

Modern Security Operations - auch für Spitäler.

Information Security in Healthcare

14.06.2023 – Lorzensaal Cham (ZG)

Stefan Mathis
Director
Sales Engineering EMEA
Ontinue

Urs Achermann
Enterprise Security Executive
Healthcare Sector Switzerland
Microsoft

Anamnese - Kurze Bestandesaufnahme

- ☑ **S**ecurity **O**perations **C**enter (**SOC**) ?
- ☑ **S**ecurity **I**nformation & **E**vent **M**anagement (**SIEM**) ?
- ☑ **E**ndpoint **D**etection & **R**esponse (**EDR**) ?
- ☑ e**X**tended **D**etection & **R**esponse (**XDR**) ?

- ☑ Wer fühlt sich aktuell **gut und sicher** ?

Traditionelle SOC Herausforderungen

Hohe Anzahl lauter Alarme (NOISE)

IT Verteilung & Wartung

Angriffe werden immer komplexer

Steigende Infrastrukturkosten und Vorabinvestitionen

Zu viele “isolierte” Security Produkte

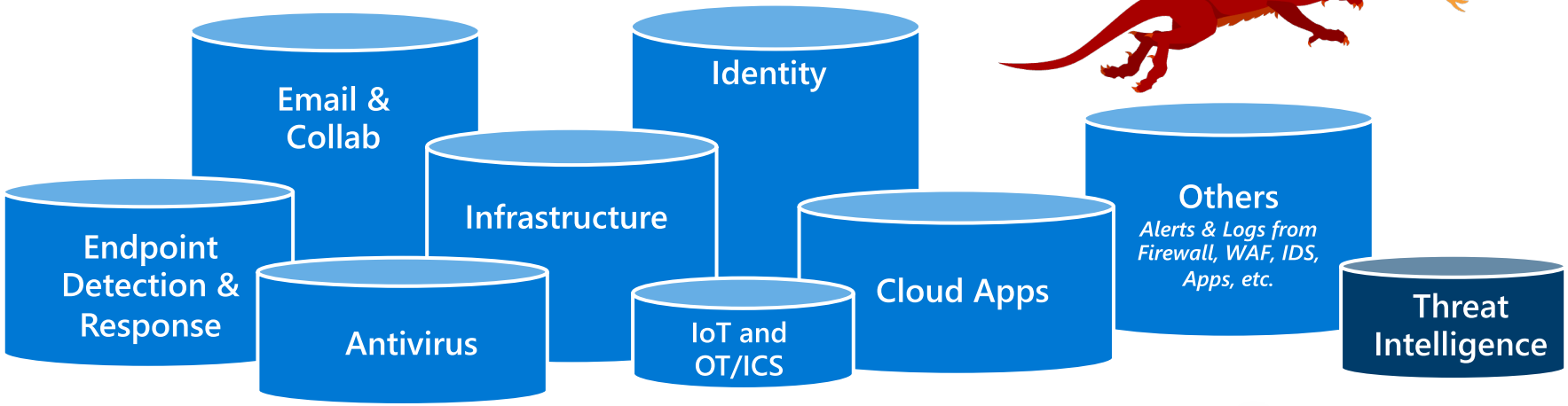
Fehlende Automatisierung

Security-Skills sind Mangelware

Silos sind der Fluch der Security Operations

Verteidiger haben Mühe, sie über Silos hinweg zu verfolgen

Angreifer bewegen sich schnell..... durch das Unternehmen

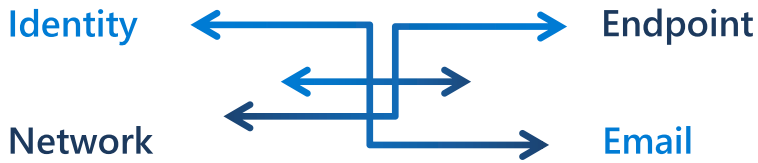


Die Integration dieser Silos ist eine Herausforderung

MAPPING HERAUSFORDERUNG
Unterschiedliche Identifiers

- Network IP address
- Computer Name
- Documents
- Device ID
- Email
- Etc.

UNTERSCHIEDLICHE ANSÄTZE & EIGENHEITEN



...

Die Integration dieser Silos ist eine Herausforderung

Erfordert einen enormen Aufwand für die Integration

...und bei jeder Anpassung beginnt es wieder von vorne

Harmonize analyst experience
Across portals and interfaces

Write/Update Automation
Orchestrate common tasks across systems

Create/Maintain Detections
add new detections and tune existing ones

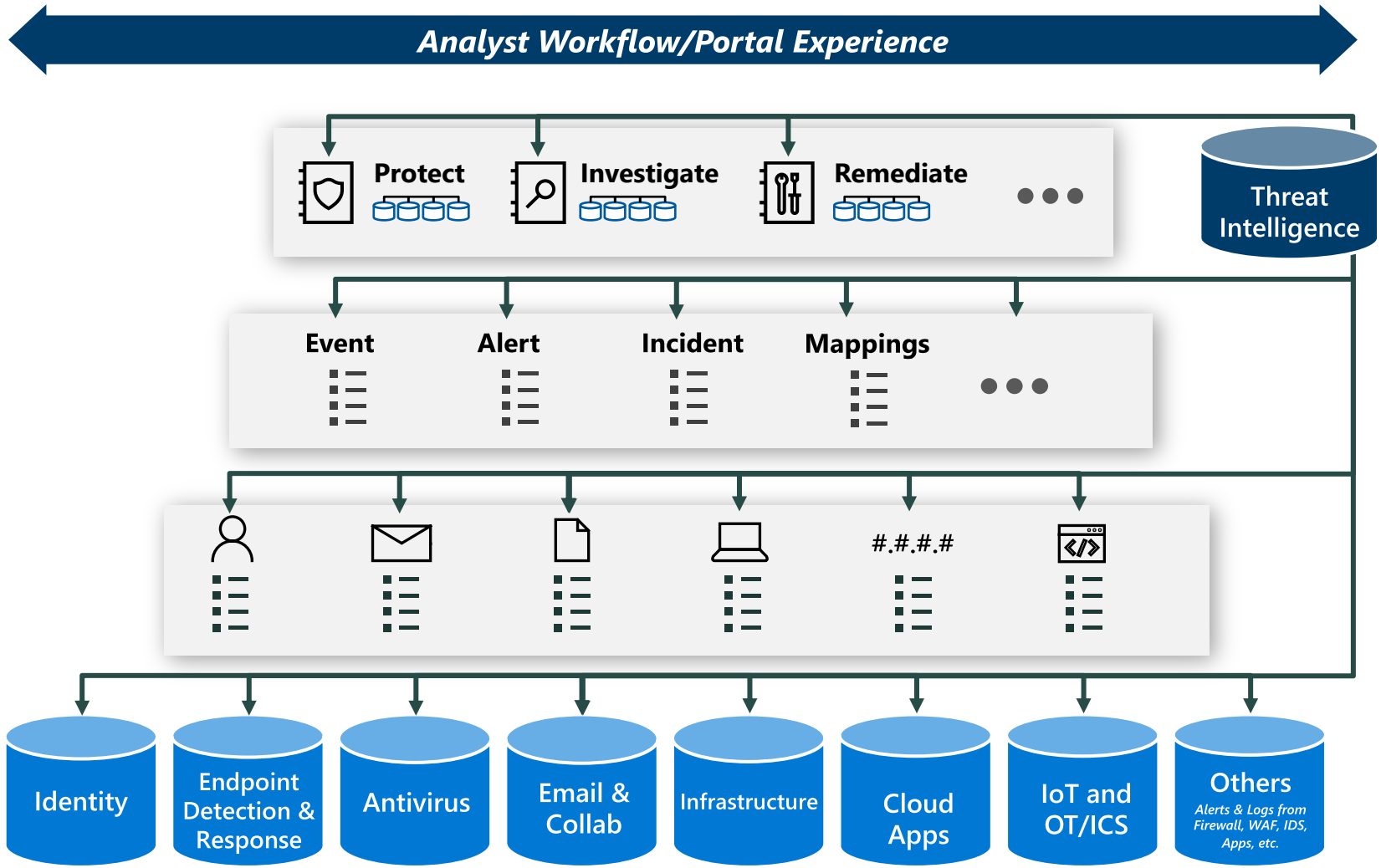
Integrate Threat Intelligence
to enrich all the different elements

Harmonize semantics & meaning
Correlation, prioritization, orchestration, etc.

Harmonize entity definitions
consistency across users, devices, email, IPs, etc.

Ensure tools provide APIs

Select & Implement Tools

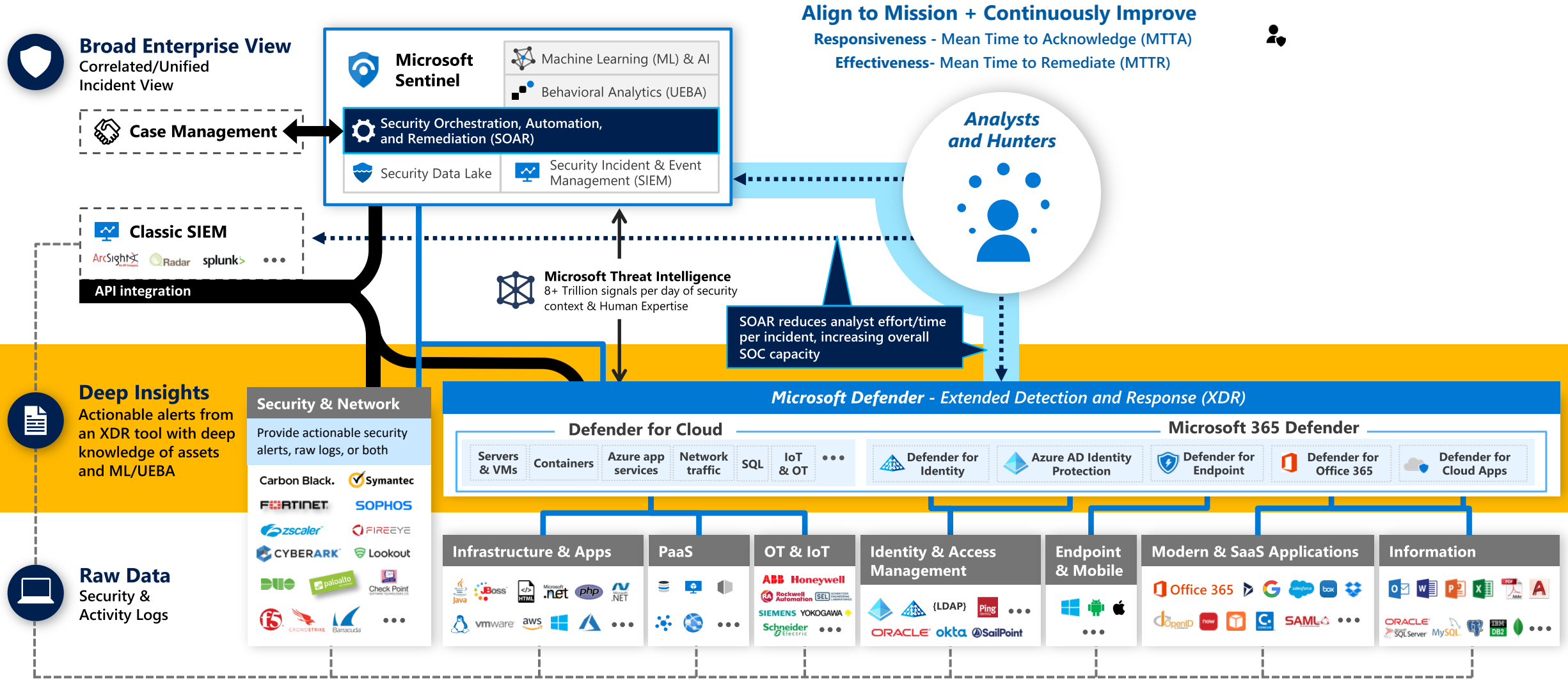


Security Operations

Microsoft Reference Architecture

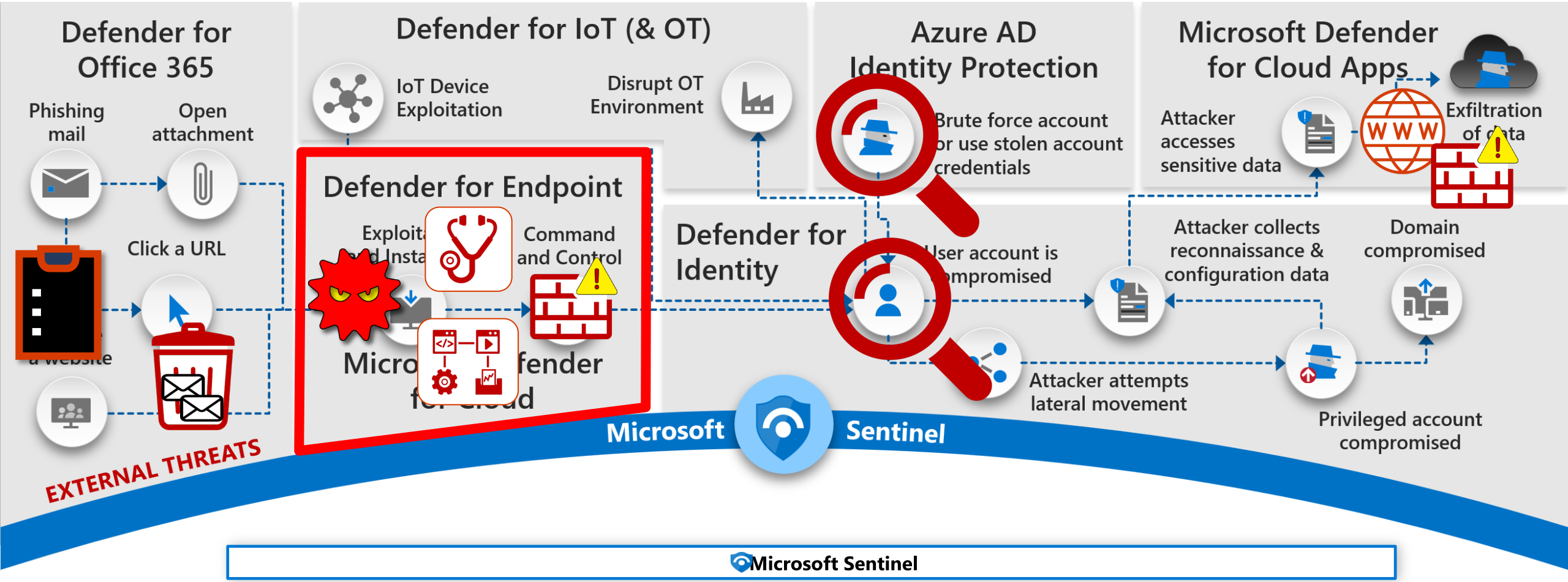
Microsoft

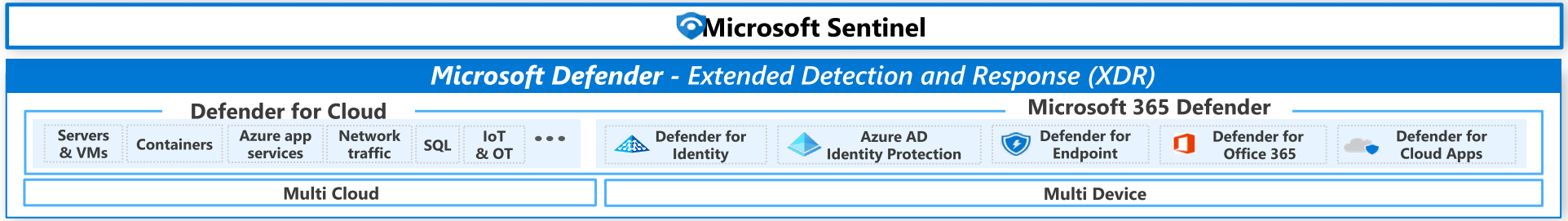
https://aka.ms/MCRA



Automatisierung und Austausch über die ganze Plattform innert kürzester Zeit

Bei einem (Ransomware-)Angriff zählt jede Sekunde!



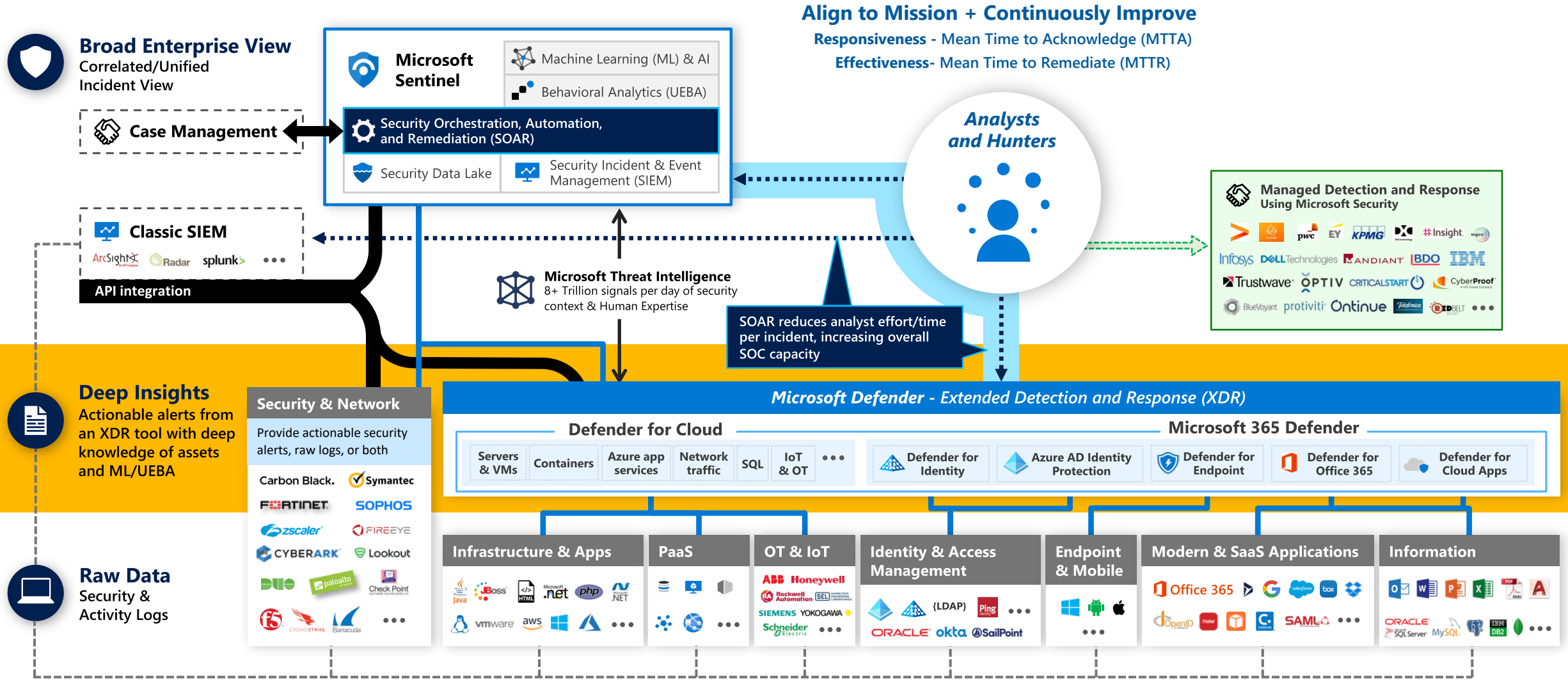


Security Operations

Microsoft Reference Architecture

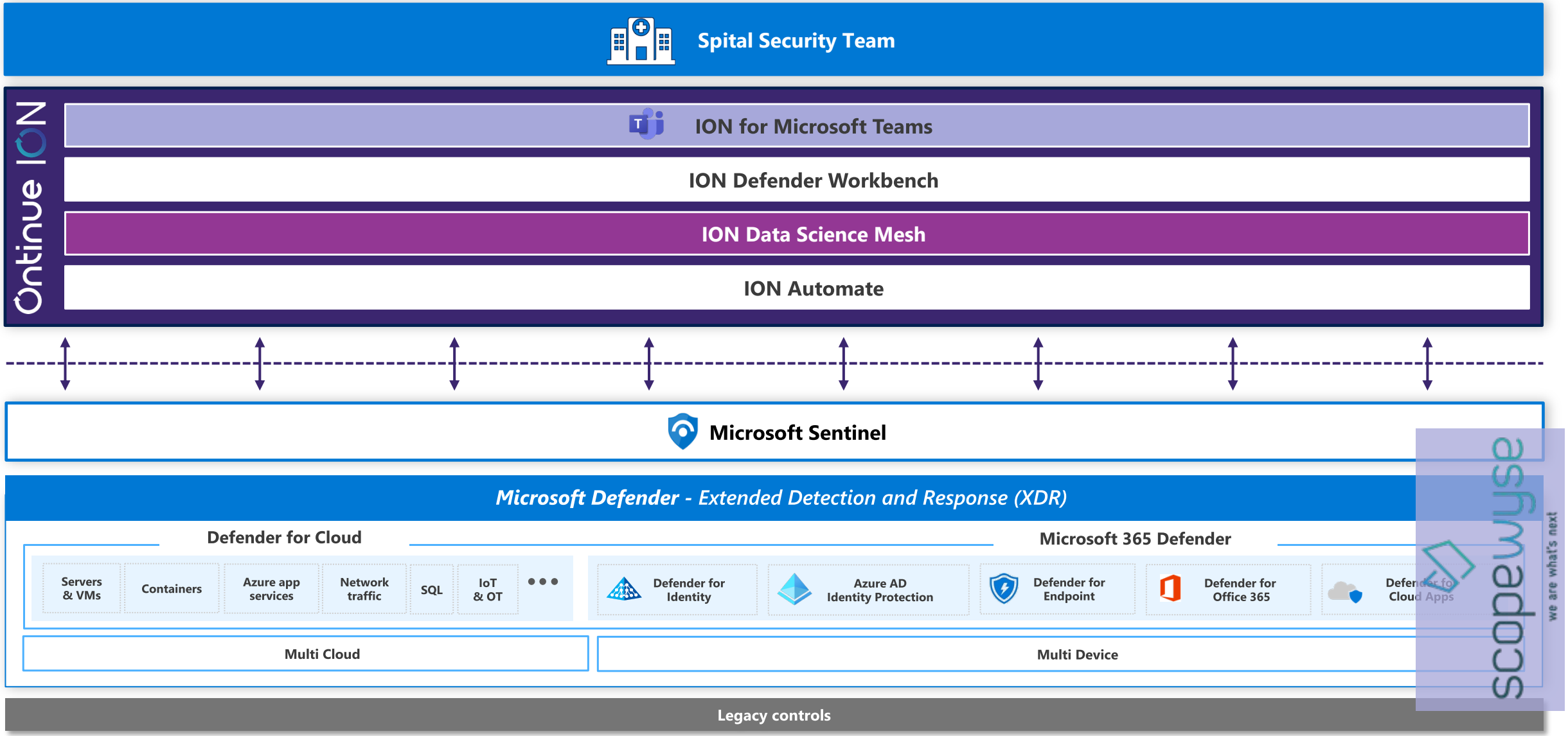
Microsoft

https://aka.ms/MCRA



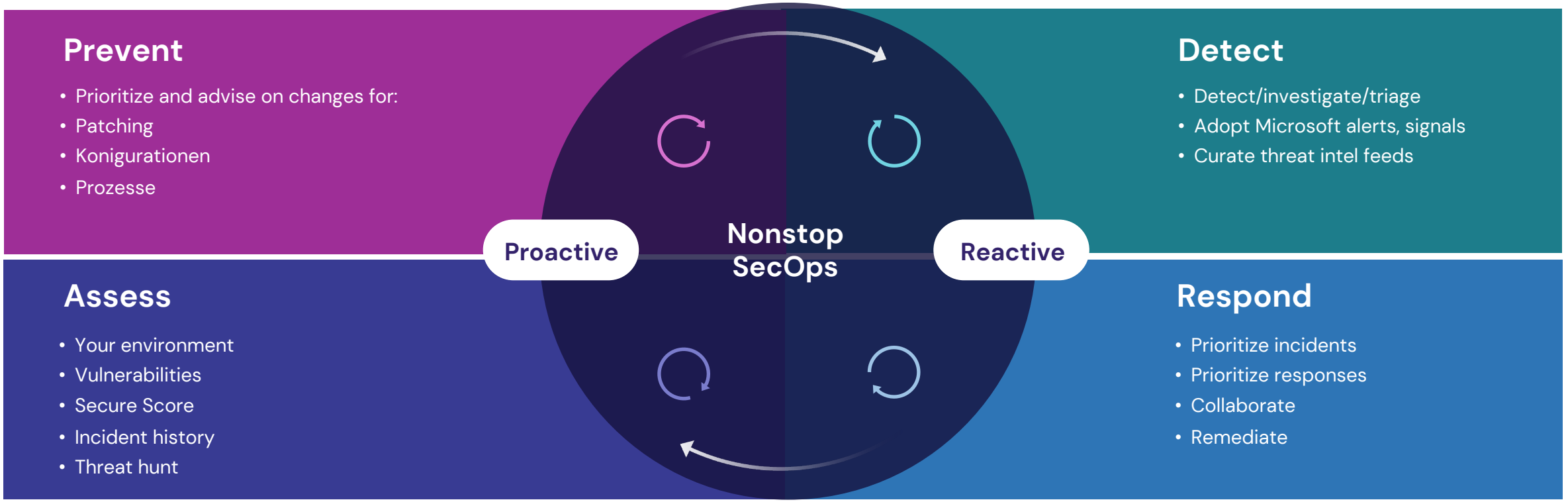
Ontinue – ION

damit Ihre bestehenden Investitionen in Microsoft-Technologien mehr bewirken können



Ontinue – Prozesse

der Mehrwert gut definierter Prozesse – Hand-in-Hand und zugeschnitten



Cyber Advisors

Cyber Defenders

Ontinue – Team

die Leute machens aus

Ontinue teams that support security operations with intelligence, automation, and engineering

Ontinue teams responsible for day-to-day security operations

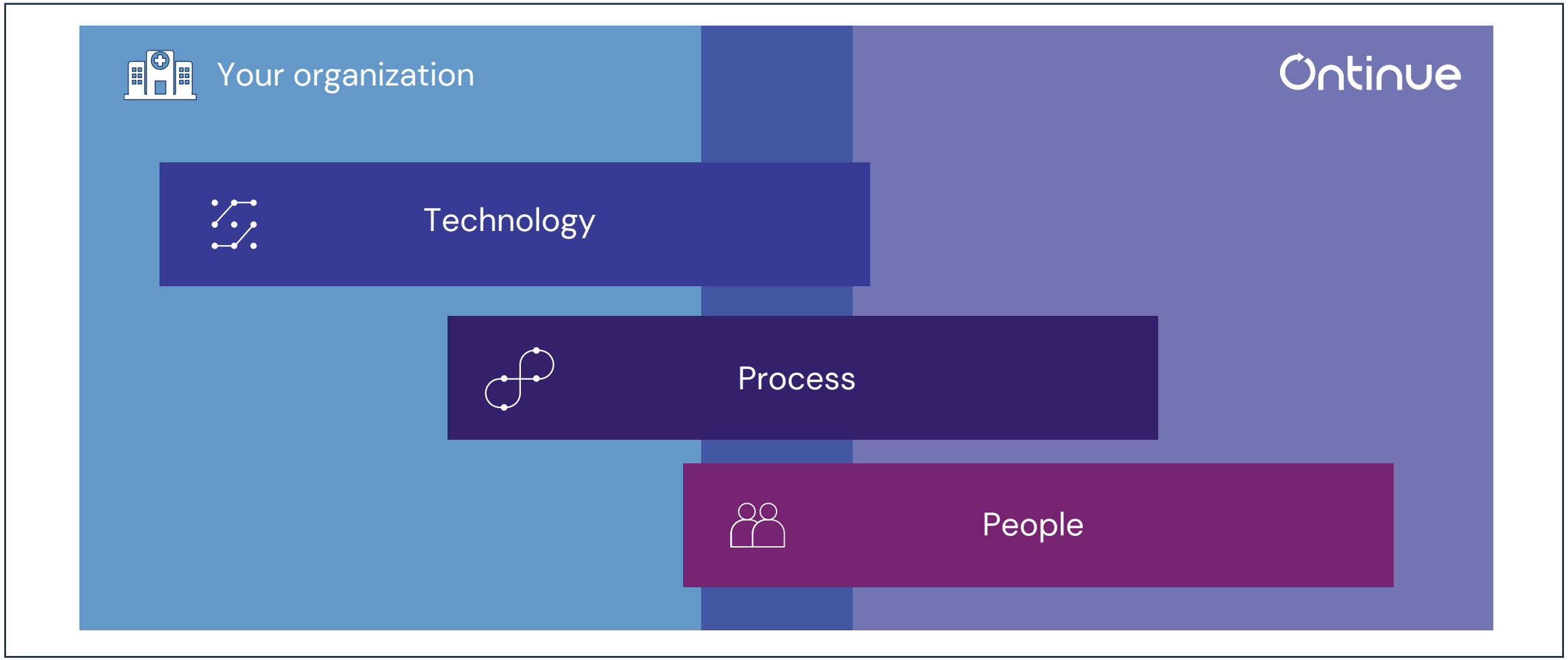
Your Team

- Data Science Team
- Automation Team
- Detection Engineering Team
- Threat Intel Team
- Cyber Advisors
- Cyber Defenders
- Threat Hunters
- Vulnerability Analysts

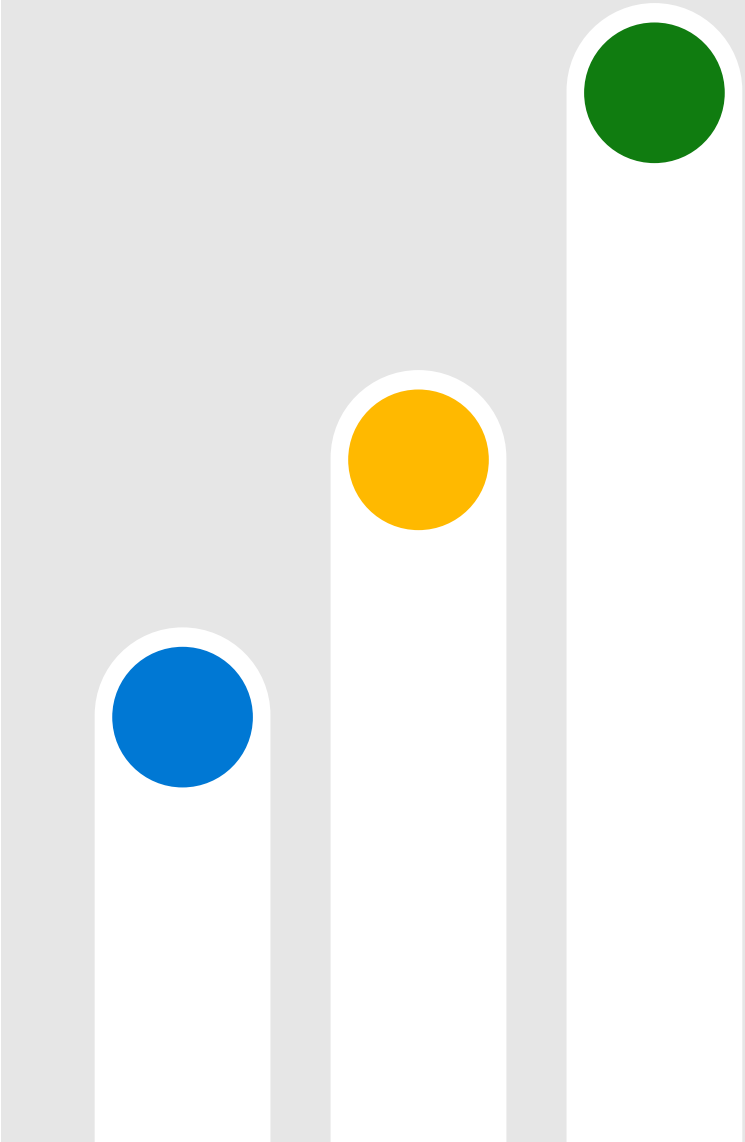
ION Cyber Defense Center

Security ist ein Teamsport

Zusammen sind wir stark und effizient



Demo



Thank you!

Steve Mathis

Director,
Sales Engineering EMEA

Ontinue

smathis@ontinue.com

Urs Achermann

Enterprise Security Executive

Microsoft

urs.achermann@microsoft.com