

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

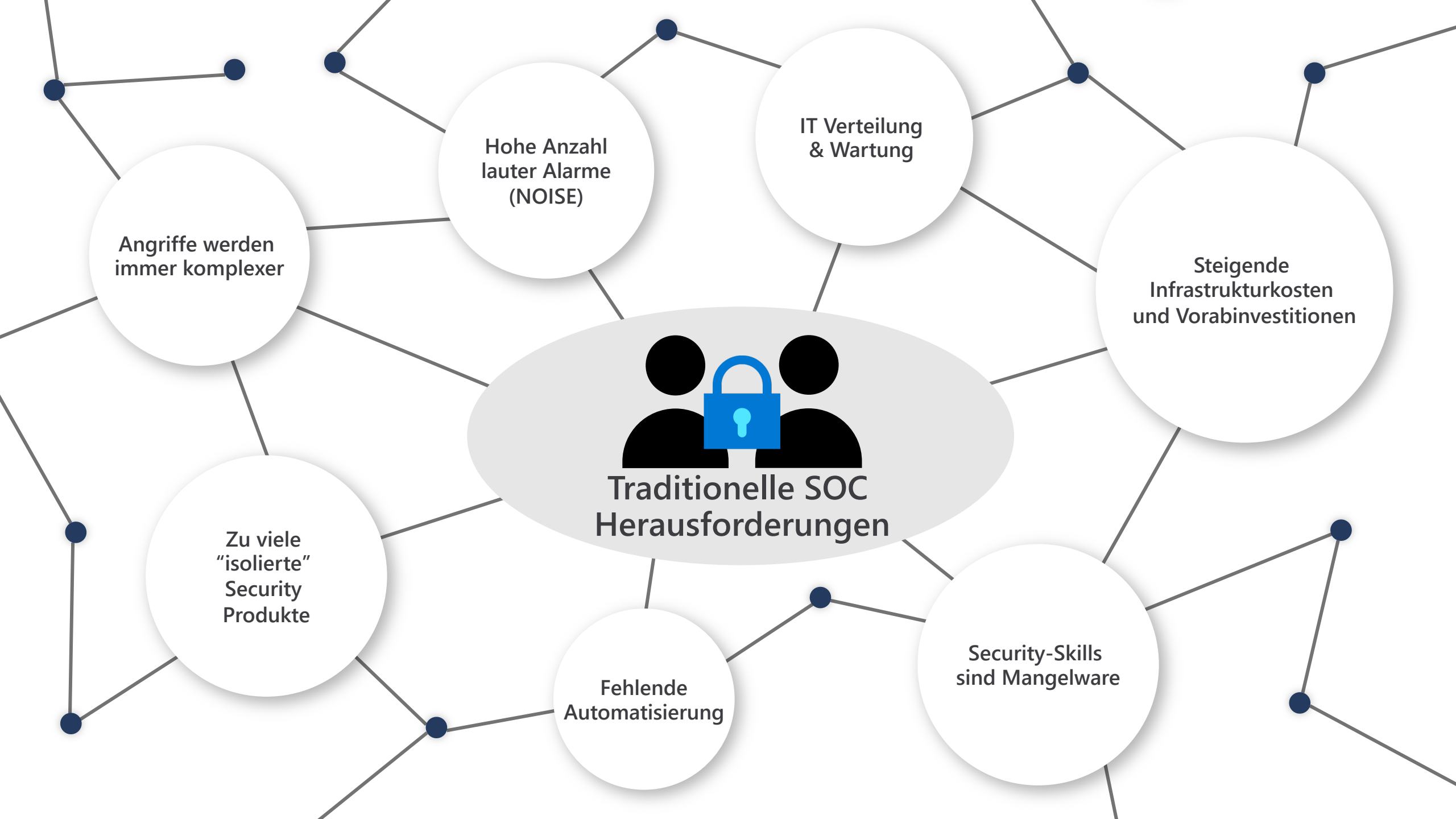
Healthcare Sector Switzerland

 **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** ?



Angriffe werden immer komplexer

Hohe Anzahl lauter Alarme (NOISE)

IT Verteilung & Wartung

Steigende Infrastrukturkosten und Vorabinvestitionen

Traditionelle SOC Herausforderungen

Security-Skills sind Mangelware

Fehlende Automatisierung

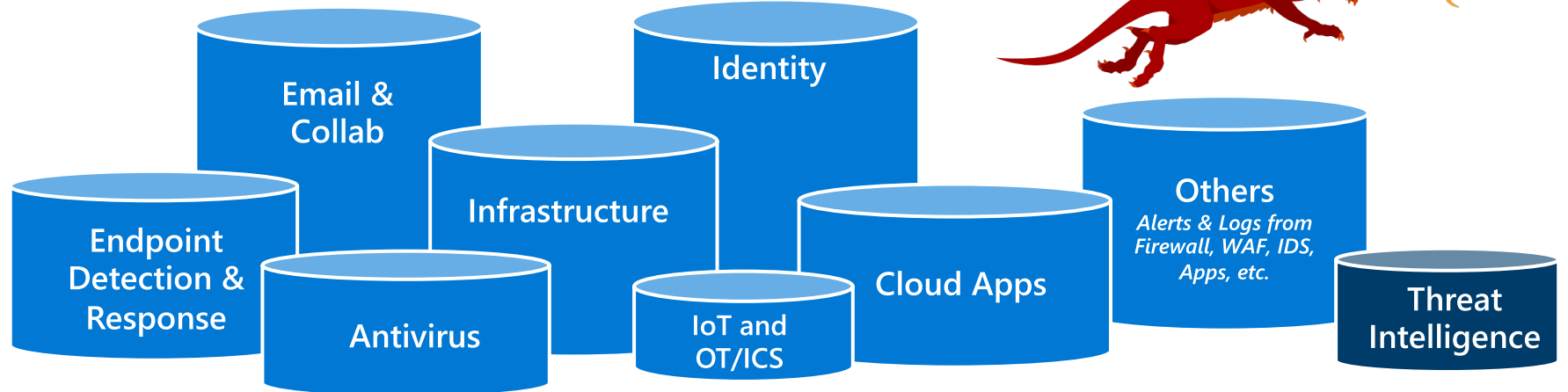
Zu viele "isolierte" Security Produkte

Silos sind der Fluch der Security Operations

Verteidiger haben Mühe, sie über Silos hinweg zu verfolgen



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



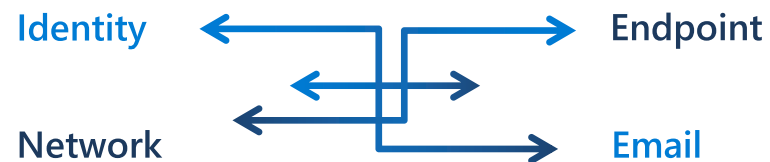
Die Integration dieser Silos ist eine Herausforderung

MAPPING HERAUSFORDERUNG

Unterschiedliche Identifiers

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

UNTERSCHIEDLICHE ANSÄTZE & EIGENHEITEN











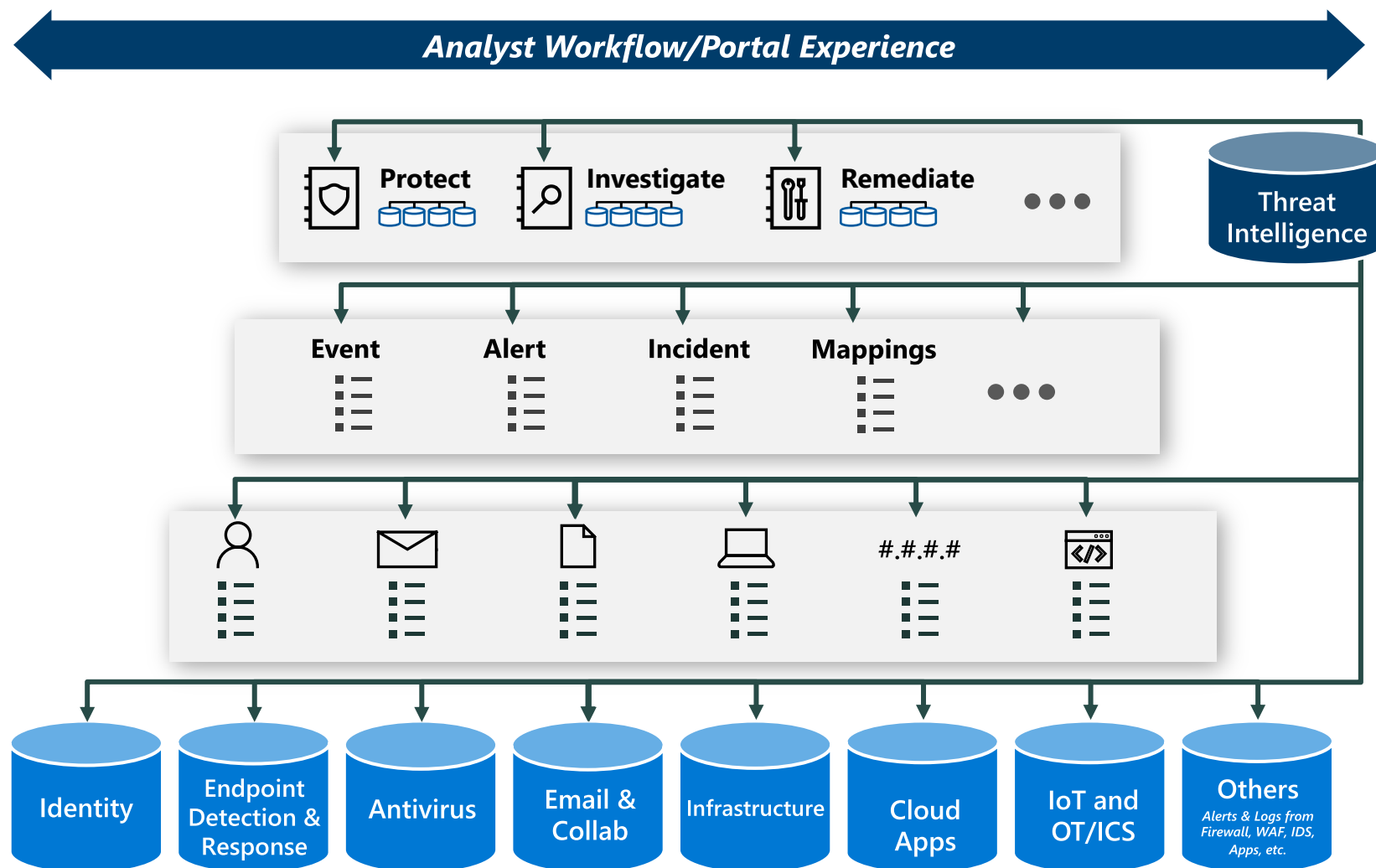
...

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



<https://aka.ms/MCRA>

Broad Enterprise View
Correlated/Unified Incident View

Case Management

Microsoft Sentinel

- Machine Learning (ML) & AI
- Behavioral Analytics (UEBA)
- Security Orchestration, Automation, and Remediation (SOAR)
- Security Data Lake
- Security Incident & Event Management (SIEM)

Align to Mission + Continuously Improve

Responsiveness - Mean Time to Acknowledge (MTTA)

Effectiveness- Mean Time to Remediate (MTTR)

Analysts and Hunters

SOAR reduces analyst effort/time per incident, increasing overall SOC capacity

Classic SIEM

ArcSightX Radar splunk > ...

API integration

Microsoft Threat Intelligence
8+ Trillion signals per day of security context & Human Expertise

Deep Insights

Actionable alerts from an XDR tool with deep knowledge of assets and ML/UEBA

Security & Network

Provide actionable security alerts, raw logs, or both

Carbon Black. Symantec
FORTINET. SOPHOS
zscaler. FIREEYE
CYBERARK. Lookout
Duo. Paloalto
Check Point
CROWDSTRIKE. Barracuda

Raw Data

Security & Activity Logs

Microsoft Defender - Extended Detection and Response (XDR)

Defender for Cloud

Servers & VMs Containers Azure app services Network traffic SQL IoT & OT ...

Microsoft 365 Defender

Defender for Identity Azure AD Identity Protection Defender for Endpoint Defender for Office 365 Defender for Cloud Apps

Infrastructure & Apps

Java JBoss HTML .NET php .NET
vmware aws windows

PaaS

...

OT & IoT

ABB Honeywell
Rockwell Automation SEL
SIEMENS YOKOGAWA
Schneider Electric

Identity & Access Management

(LDAP) Ping ...
ORACLE okta SailPoint

Endpoint & Mobile

Windows Android Apple ...

Modern & SaaS Applications

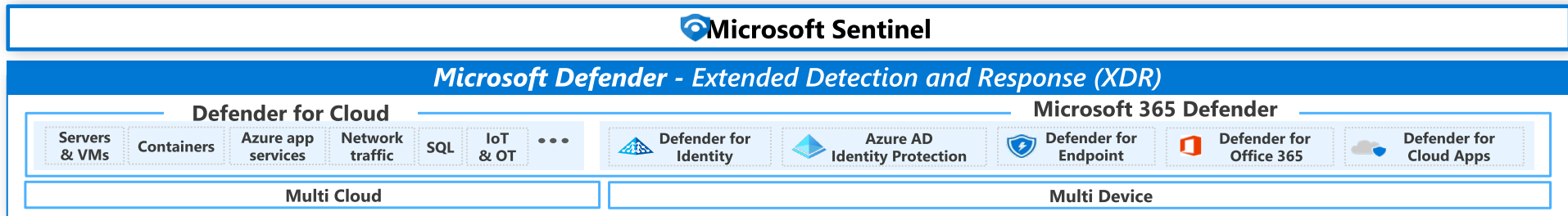
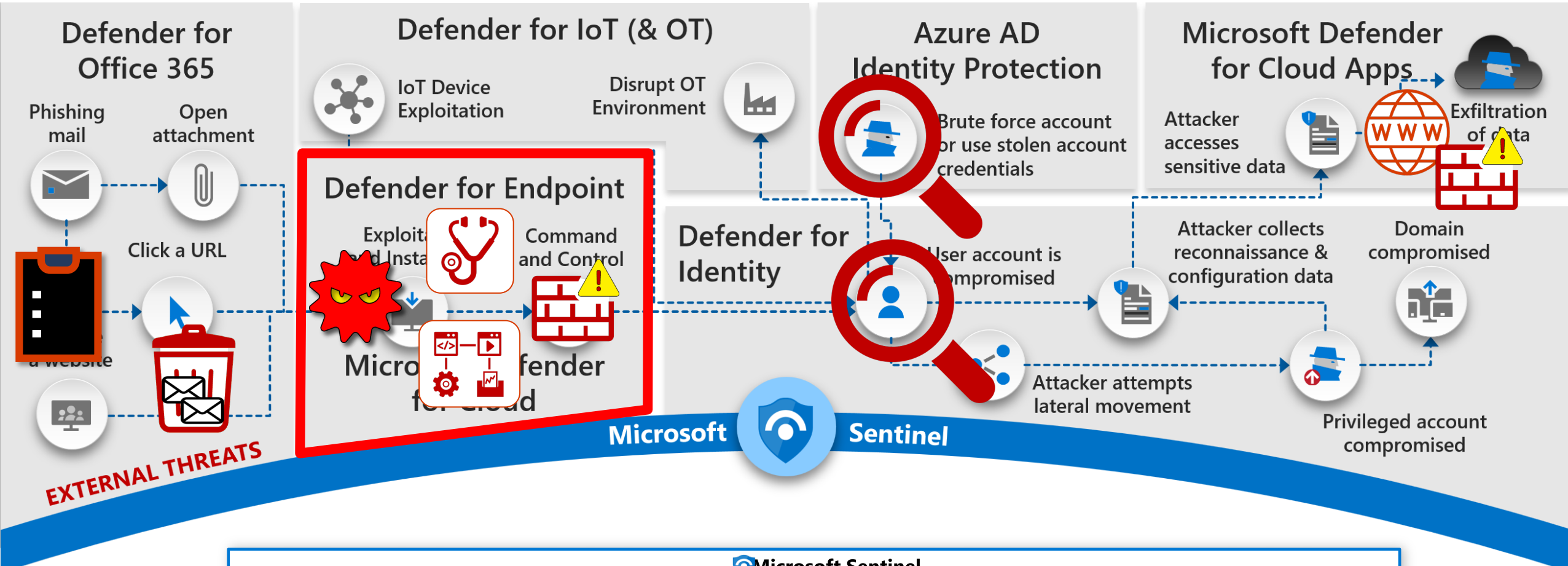
Office 365 G Salesforce box ...
OpenID Now C SAM4S ...

Information

Office Word PowerPoint Excel PDF A
ORACLE SQL Server MySQL IBM DB2 ...

Automatisierung und Austausch über die ganze Plattform innert kürzester Zeit

Bei einem (Ransomware-)Angriff zählt jede Sekunde!



Security Operations

Microsoft Reference Architecture



<https://aka.ms/MCRA>



Broad Enterprise View
Correlated/Unified Incident View

Case Management

Classic SIEM
ArcSight, Radar, Splunk, ...

API integration

Deep Insights
Actionable alerts from an XDR tool with deep knowledge of assets and ML/UEBA

Raw Data
Security & Activity Logs

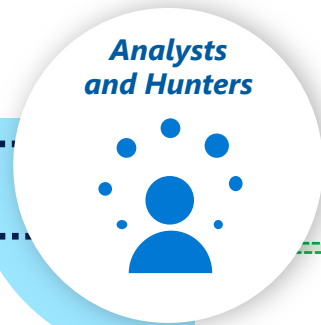
Microsoft Sentinel

- Machine Learning (ML) & AI
- Behavioral Analytics (UEBA)
- Security Orchestration, Automation, and Remediation (SOAR)
- Security Data Lake
- Security Incident & Event Management (SIEM)

Align to Mission + Continuously Improve

Responsiveness - Mean Time to Acknowledge (MTTA)

Effectiveness- Mean Time to Remediate (MTTR)



Microsoft Threat Intelligence
8+ Trillion signals per day of security context & Human Expertise

SOAR reduces analyst effort/time per incident, increasing overall SOC capacity

Managed Detection and Response Using Microsoft Security

Microsoft Defender - Extended Detection and Response (XDR)

Defender for Cloud | **Microsoft 365 Defender**

- Defender for Cloud: Servers & VMs, Containers, Azure app services, Network traffic, SQL, IoT & OT, ...
- Microsoft 365 Defender: Defender for Identity, Azure AD Identity Protection, Defender for Endpoint, Defender for Office 365, Defender for Cloud Apps

Security & Network
Provide actionable security alerts, raw logs, or both

Infrastructure & Apps
Java, JBoss, .NET, PHP, VMware, AWS, Windows, Linux, etc.

PaaS
Azure, etc.

OT & IoT
ABB, Honeywell, Rockwell Automation, Siemens, Schneider Electric, etc.

Identity & Access Management
LDAP, Ping, Okta, SailPoint, etc.

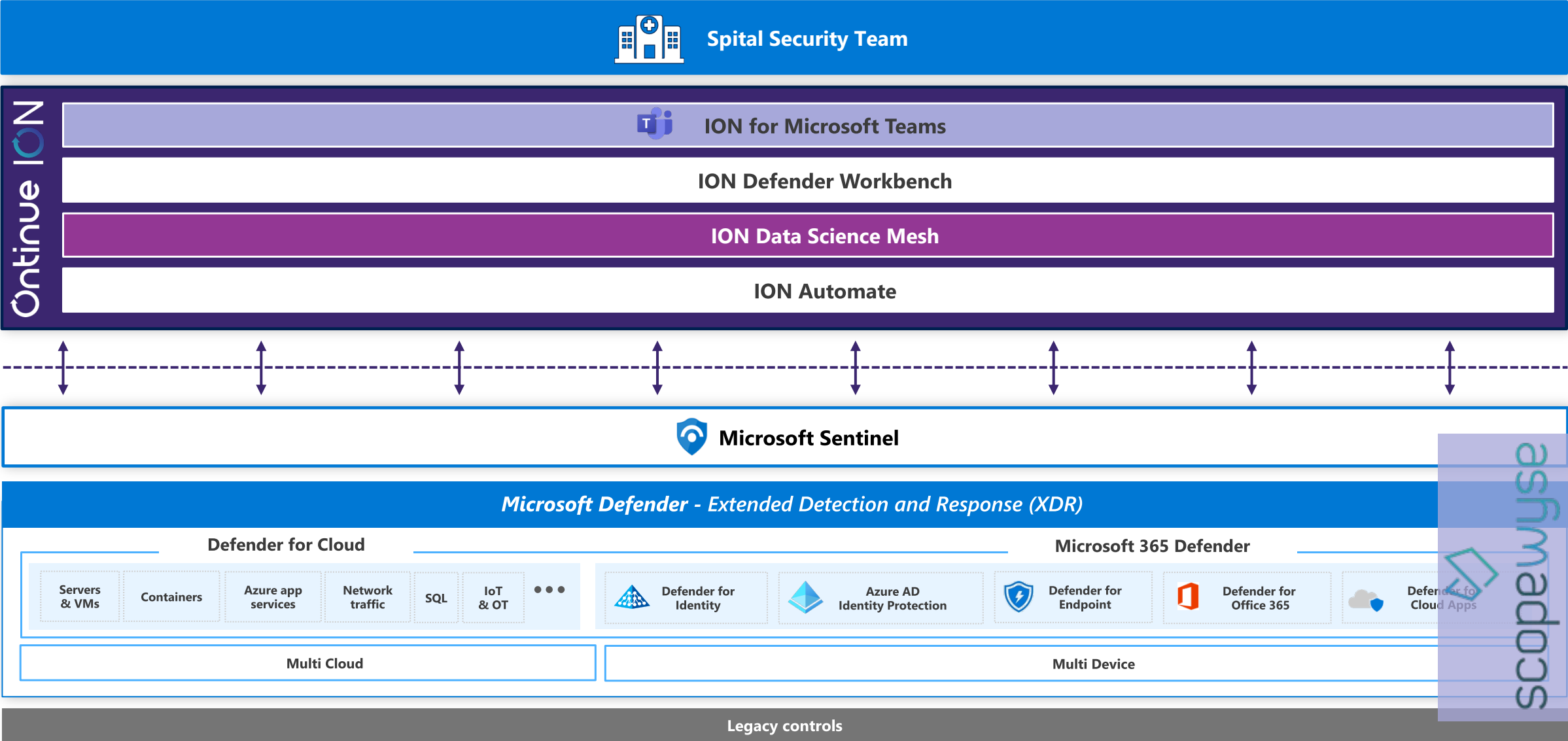
Endpoint & Mobile
Windows, Android, Apple, etc.

Modern & SaaS Applications
Office 365, G Suite, Salesforce, etc.

Information
Oracle, SQL Server, MySQL, IBM DB2, etc.

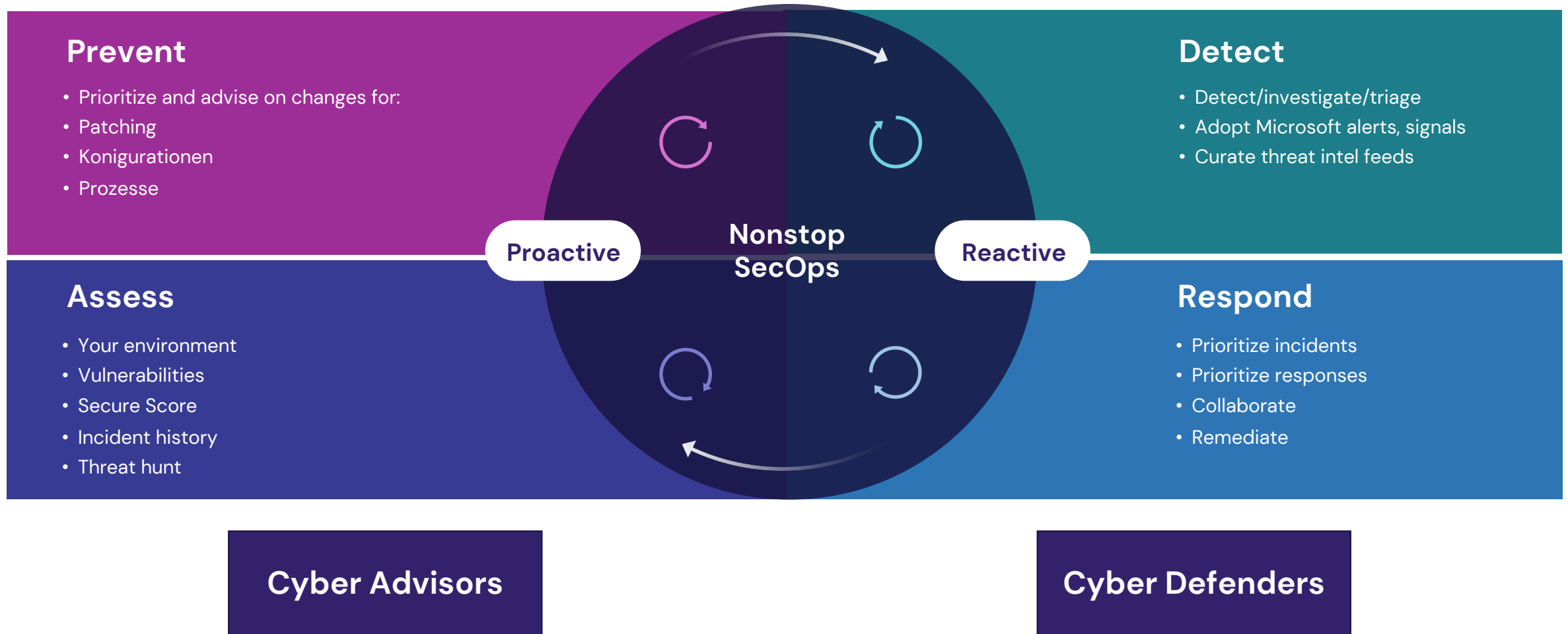
Ontinue – ION

damit Ihre bestehenden Investitionen in Microsoft-Technologien mehr bewirken können



Ontinue – Prozesse

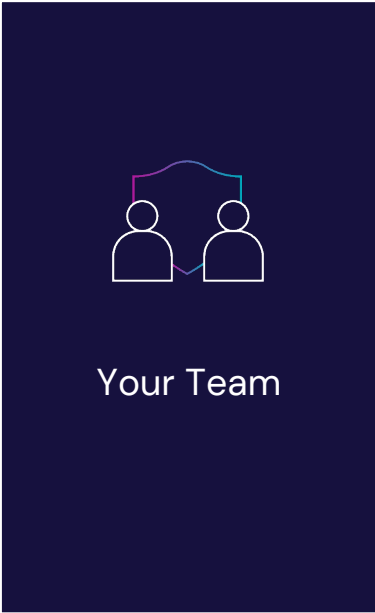
der Mehrwert gut definierter Prozesse – Hand-in-Hand und zugeschnitten



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



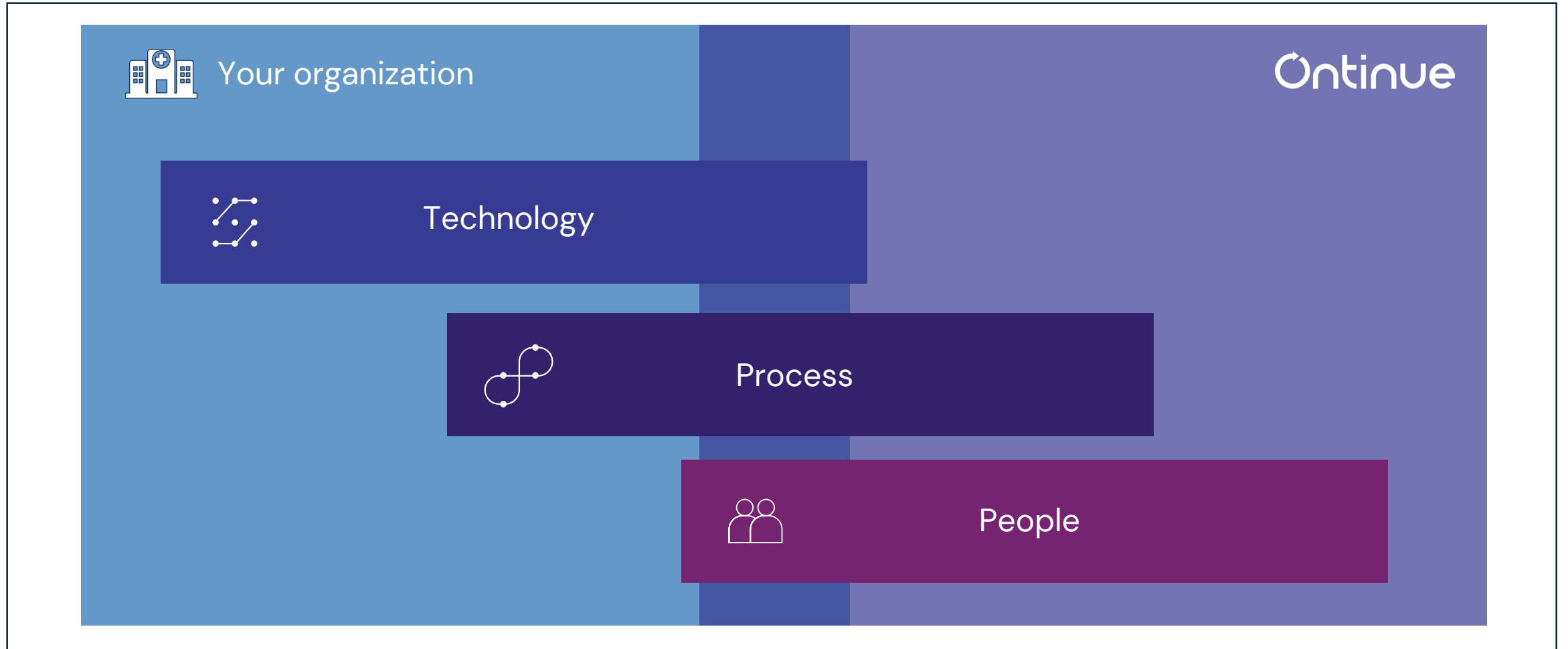
Data Science Team	Automation Team
Detection Engineering Team	Threat Intel Team

Cyber Advisors	Cyber Defenders
Threat Hunters	Vulnerability Analysts

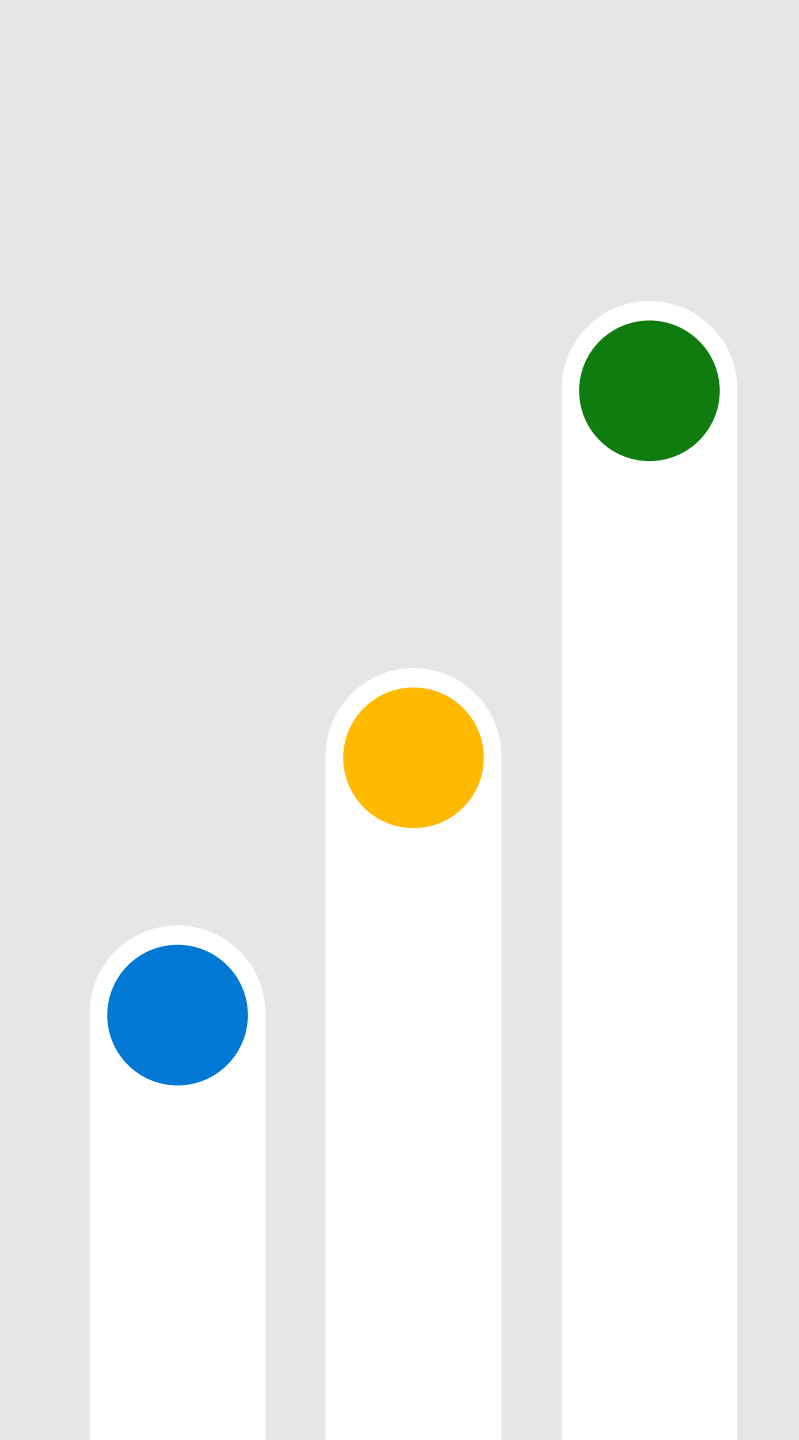
ION Cyber Defense Center

Security ist ein Team sport

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

