ADDRESSING MODERN CHALLENGES IN CYBERSECURITY IN THE AI ERA

Nikos Makris, Security Sales Leader (Sales Enablement & Ops), Microsoft (CEMA)

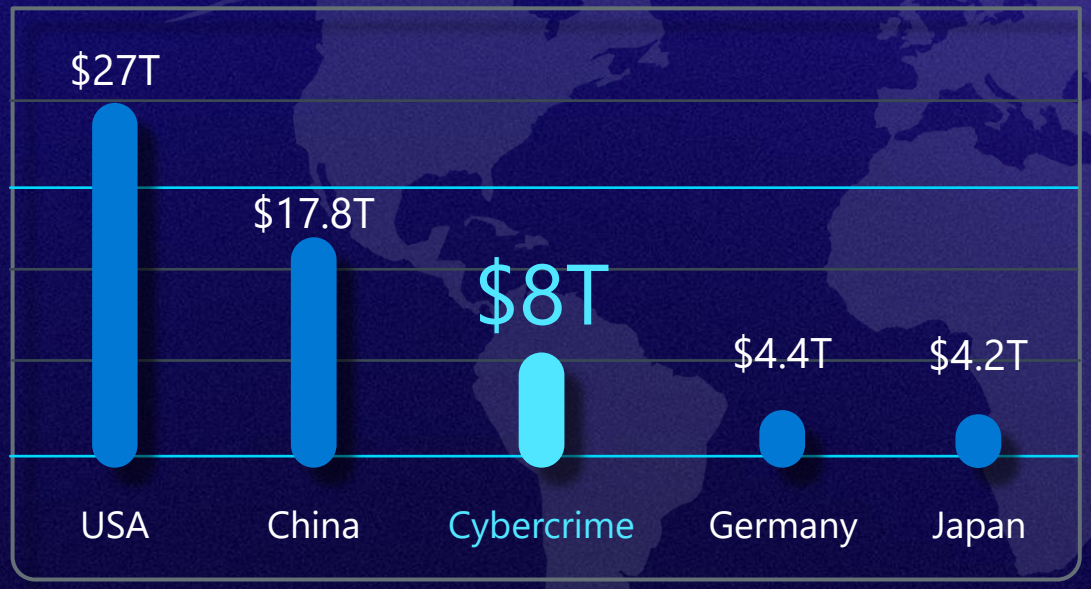
Dimitris Kalyvas, Global Channel Director

Microsoft Security

OBRELA

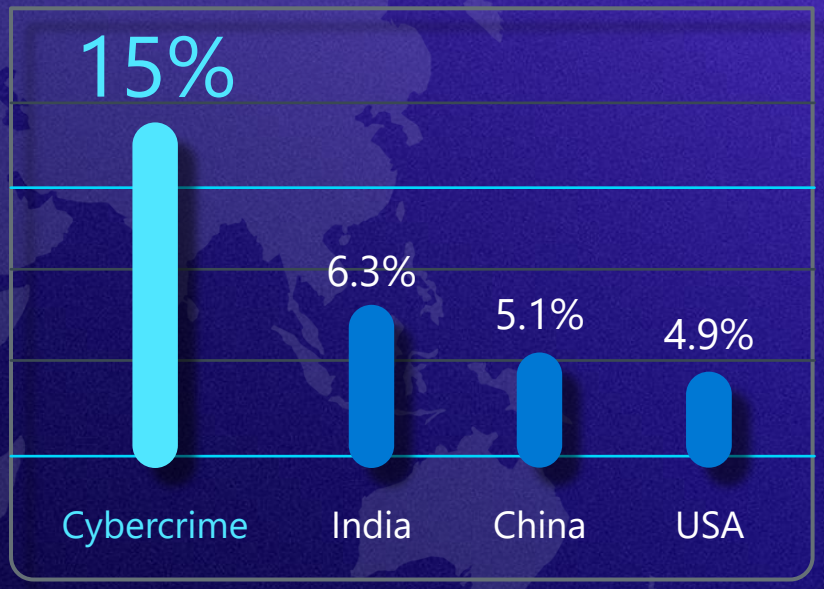
Cybercrime today equals the 3rd largest economy in the world and growing fast

Annual GDP



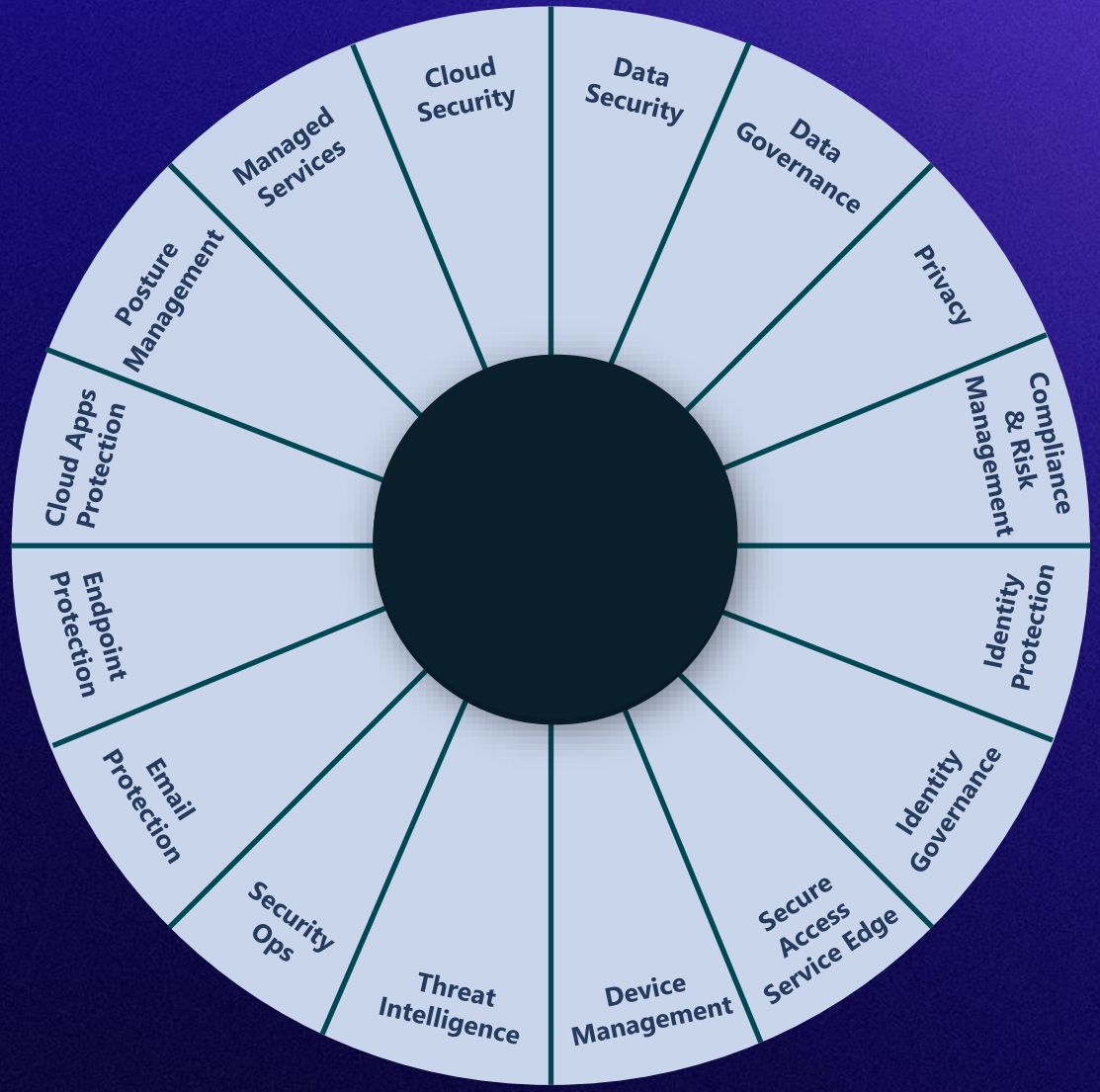
Source: Statistica

GDP annual growth rate



Source: Statistica

Approaching security from every angle



A patchwork of siloed security tools is no longer enough

End point protection

Threat intelligence

SIEM

SOAR

XDR

Identity protection

Many organizations have 50+ cybersecurity tools

Cloud apps protection

Cloud security

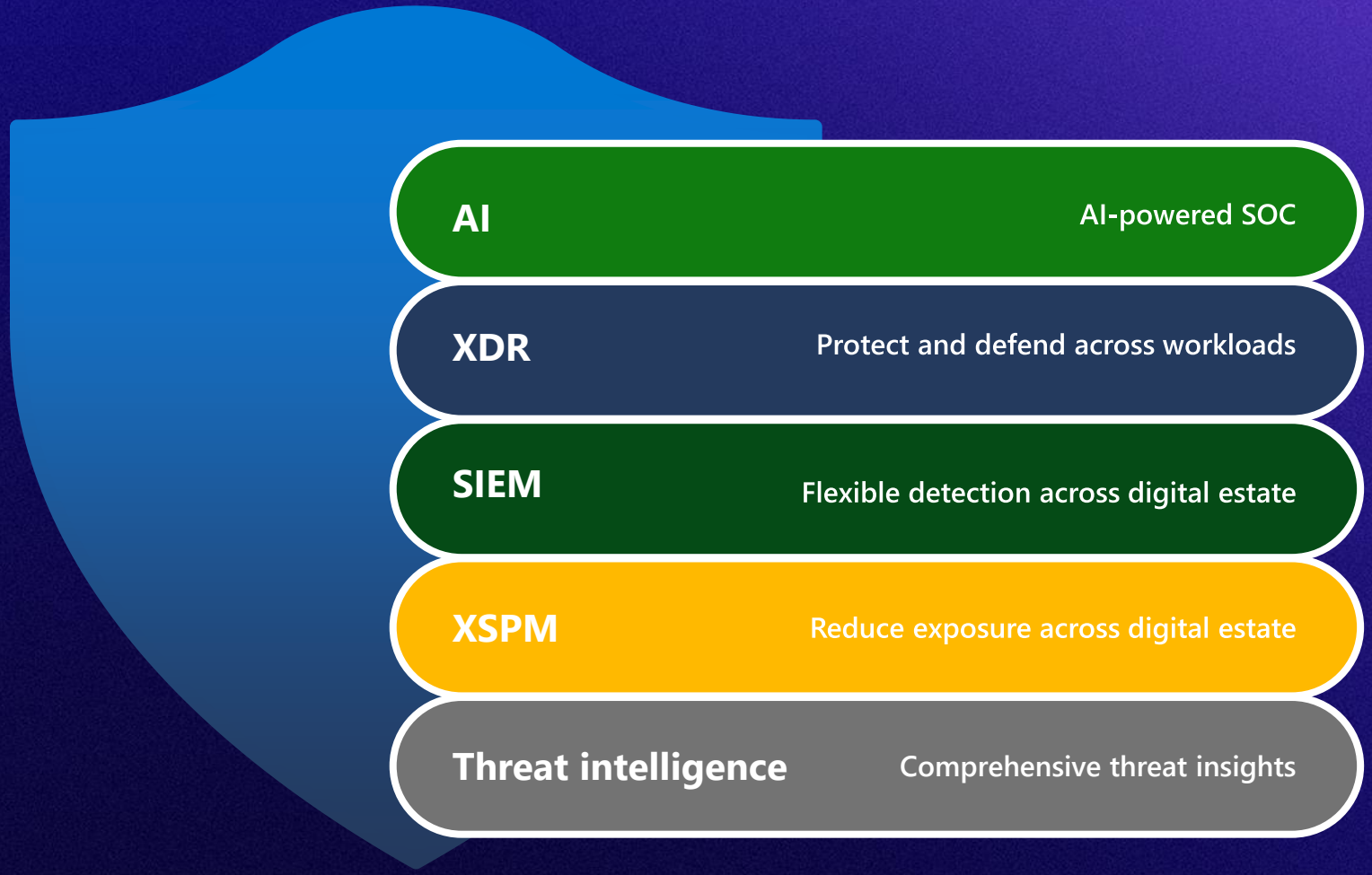
Email security

Posture management

UEBA

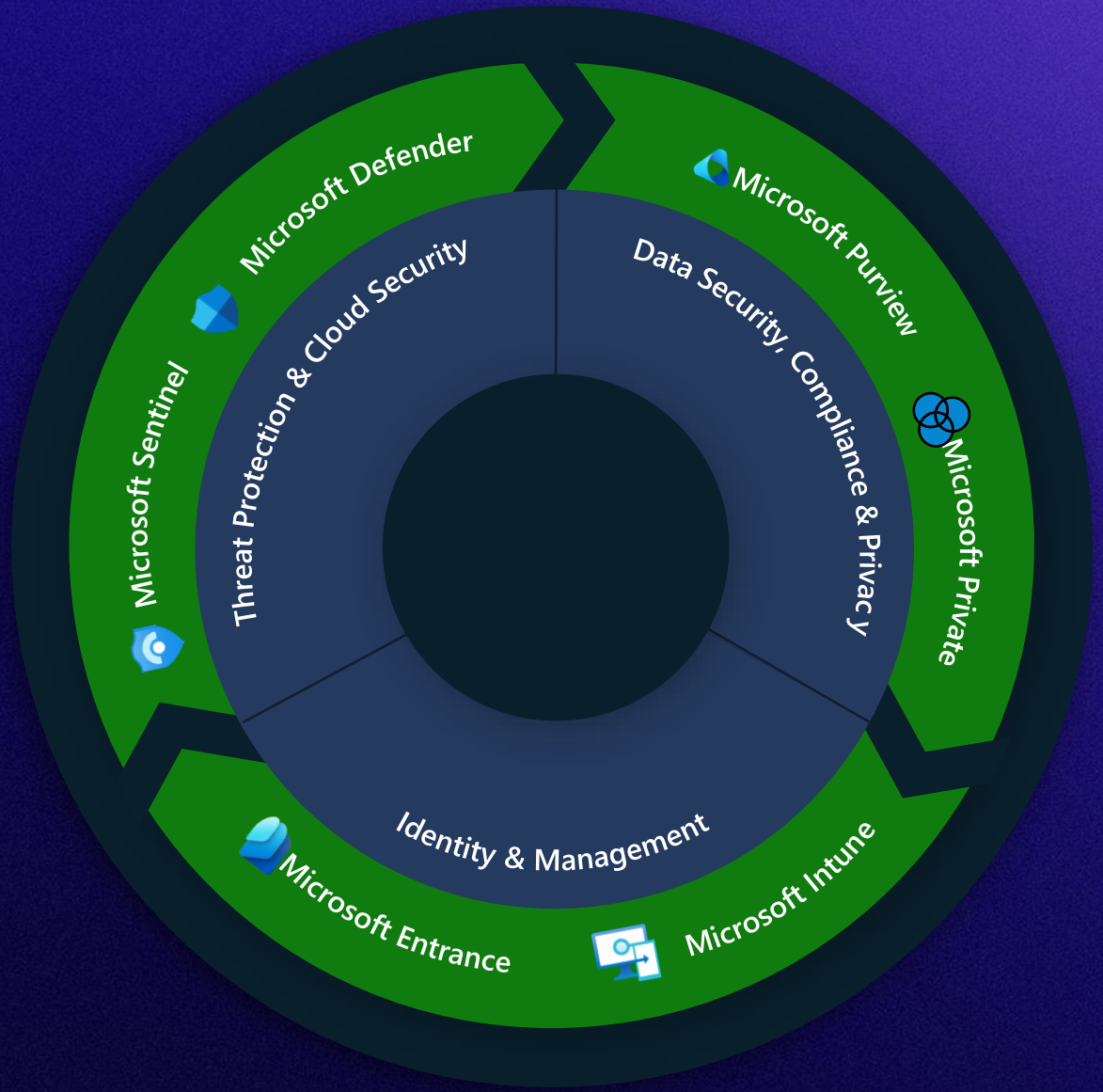
It’s time for a unified security operations platform

Optimized analyst experience | Targeted assistance | Automated protection and remediation



End-to-end protection

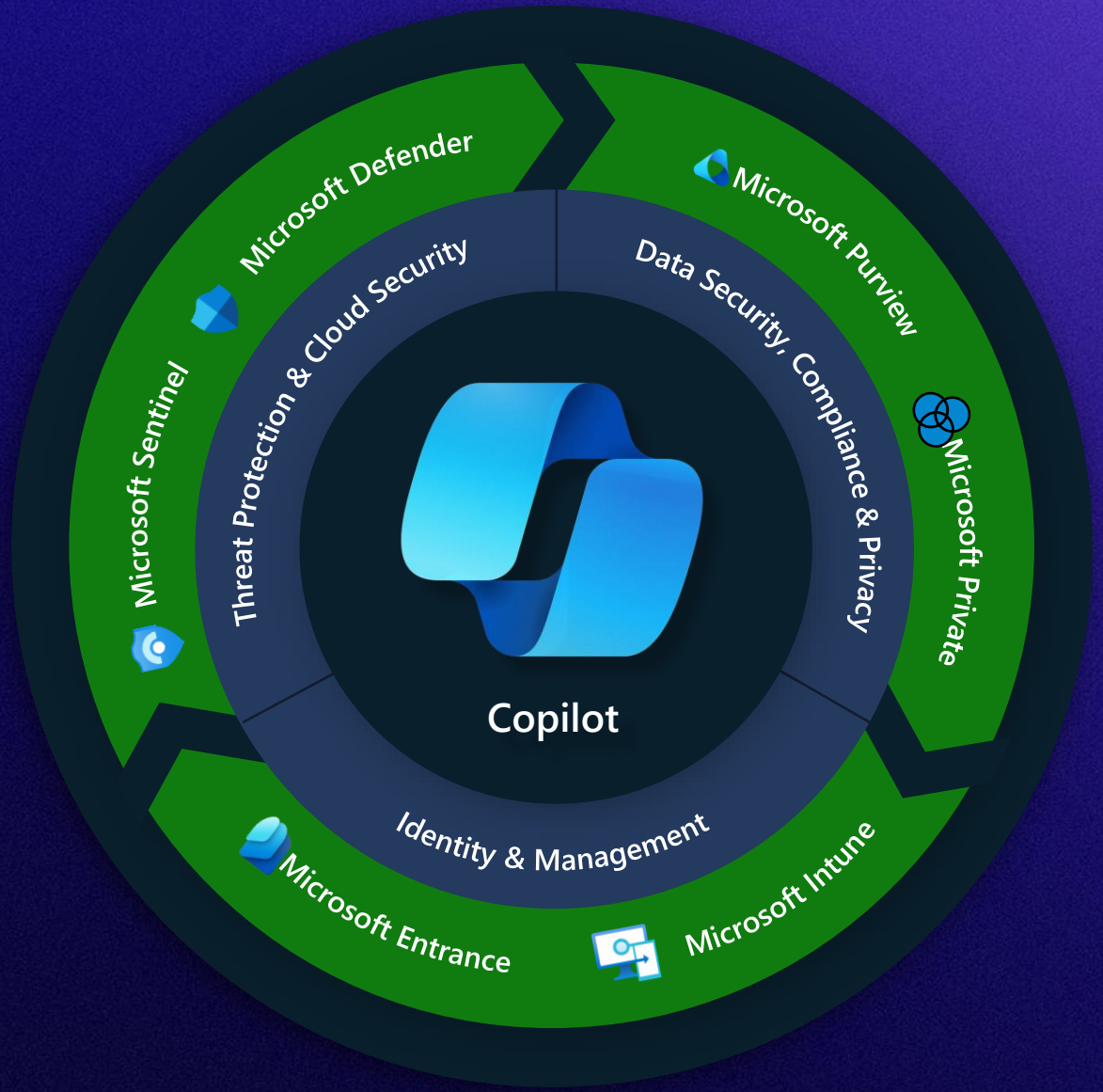
Multicloud



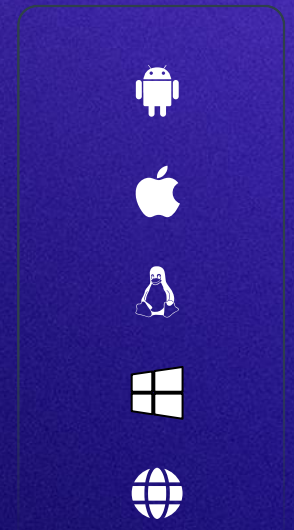
Multiplatform

Force multiplier for security

Multicloud



Multiplatform



Microsoft Copilot for Security

Defending at machine speed

> ***"It takes us three minutes to do a task that used to take at least a few hours"***

- Private preview customer

Enable response in minutes, not hours

Simplify the complex with natural language prompts and easy reporting

Catch what others miss with deeper understanding of your enterprise

Strengthen team expertise with cyber-trained generative AI

Common concerns…

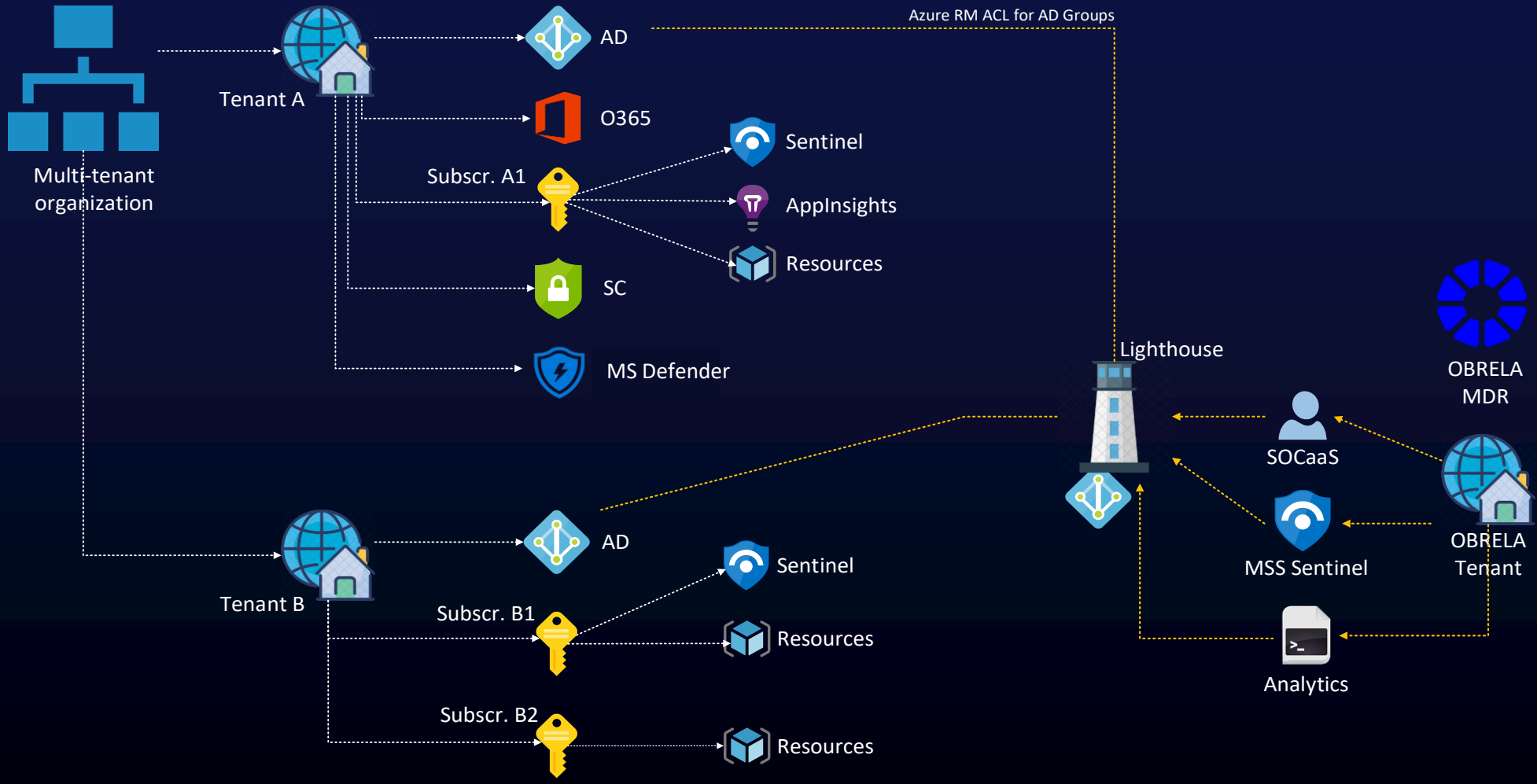
1. End-to-end security support
2. Ongoing proof of value
3. A safe and rapid migration & modernization

© Copyright Microsoft Corporation. All rights reserved

OUR JOURNEY WITH MICROSOFT

OBRELA

MDR CLOUD INTEGRATION METHODOLOGY



OBRELA

AI ENHANCED SECURITY OPERATIONS

PROCESS

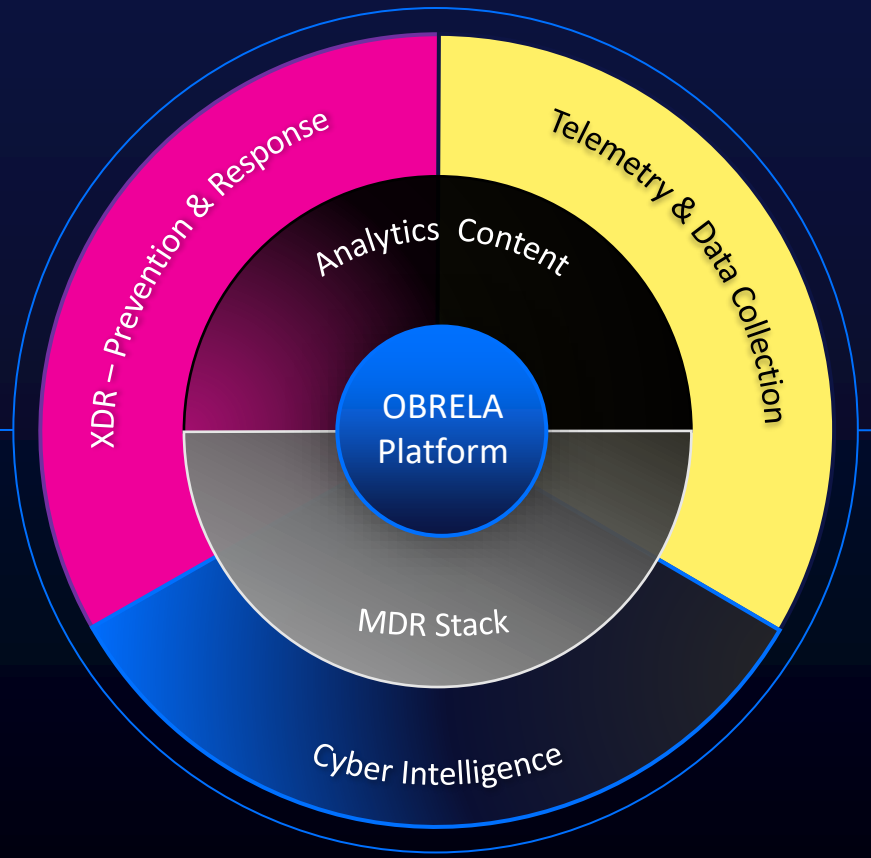
Threat Hunting
- Kill Chain Analysis
- What-if Analysis
- Incident Discovery
- Threat Intelligence Mapping with Customer Environment

Threat Intelligence
- New Threats Discovery
- IOC Collection
- Targeted Intelligence
- Collective Intelligence
- Cyber Adversary Characterization

Risk Management
- Vulnerability
- Asset
- Incident
- Policy
- Vendor Security
- Privacy
- Compliance
- Reporting

Cyber Ops
- Rules of Engagement
- Case Management
- Intelligence Analysis
- 24/7/365 Monitoring
- Incident Response
- Client Onboarding

Platform & Content Management
- IR Playbooks
- Alert Management
- Continuous Improvement
- HardCore Content Development
- Integration & Connectors Development



PEOPLE

Service Management
- Service Delivery Manager

SOC Operations
- L1/L2 Analysts
- SOC Officers

Blue Team Support
- Threat Intelligence Experts
- Threat Detection & Response Experts

Threat Hunting & Incident Response
- Threat Hunters
- CSIRT

Devops
- Security Engineers
- Data Engineers
- Content Developers
- Network/System Engineers

Customer / Partner
- Customer Side Security Team
- Partner Security Team

OBRELA

ACTUAL CASE SCENARIO | Energy Company

The Company Need

- *Seeking partner to provide MDR Services*
- *Challenges in IT and OT environments*
- *New operating model after COVID19*
- *Broad networks surface and multiple locations*
- *GDPR & NIS Compliance*
- *Customer aimed to:*
  - *Reduce Likelihood and/or impact of security incidents through early identification and mitigation*
  - *Optimise operational cost to monitor security events*
  - *Maintain a secure operating environment and integrity of data*
  - *To achieve objectives, Obrela partnered with customer providing MDR services which took advantage of their existing investments.*

Solution Selected

- *Combine MS Defender 365, MS Defender for IoT, MS Defender for Identity and MS Defender for Cloud Apps to achieve holistic visibility.*
- *Solution proposed for RFP response.*
- *Obrela MDR integration with Sentinel incorporating:*
  - *MS Defender 365 and Defender for IoT*
  - *MS Defender for Identity*
  - *MS Defender for Cloud Apps*
- *Obrela MDR services including:*
  - *24x7x365 SOC Services*
  - *Threat Hunting*
  - *Incident Response Support*

The Gain

- *Single service monitoring OT, IT and Identity solutions.*
- *Augmented customer security capability with support of Obrela team.*
- *Increased fidelity of alerts through Obrela HardCORE content using Lighthouse.*
- *A scalable cloud-based solution integrating the customers IT and OT environments.*
- *Repeatable Solution.*

OBRELA

OUR MISSION

WE KEEP YOUR BUSINESS IN BUSINESS

Copyright © 2023, OSI. All rights reserved.

OBRELA

OBRELA

Microsoft Security

THANK YOU

London | Athens | Dubai | Frankfurt | Riyadh

www.obrela.com