

Moduły cyberbezpieczeństwa w Microsoft 365

Kuba Jasiński



Agenda

1. Obszary i nomenklatura
2. Moduły Microsoft 365
3. Dobór licencji i funkcjonalności

Obszary i nomenklatura

EDR

Endpoint detection and Response

Monitorowanie podejrzanych i szkodliwych działań na poziomie urządzenia końcowego

XDR

Extended Security and Response

Kompleksowy system cyberbezpieczeństwa pozwalający na wykrywanie zagrożeń i reagowanie

SIEM

Security Information and Event Management

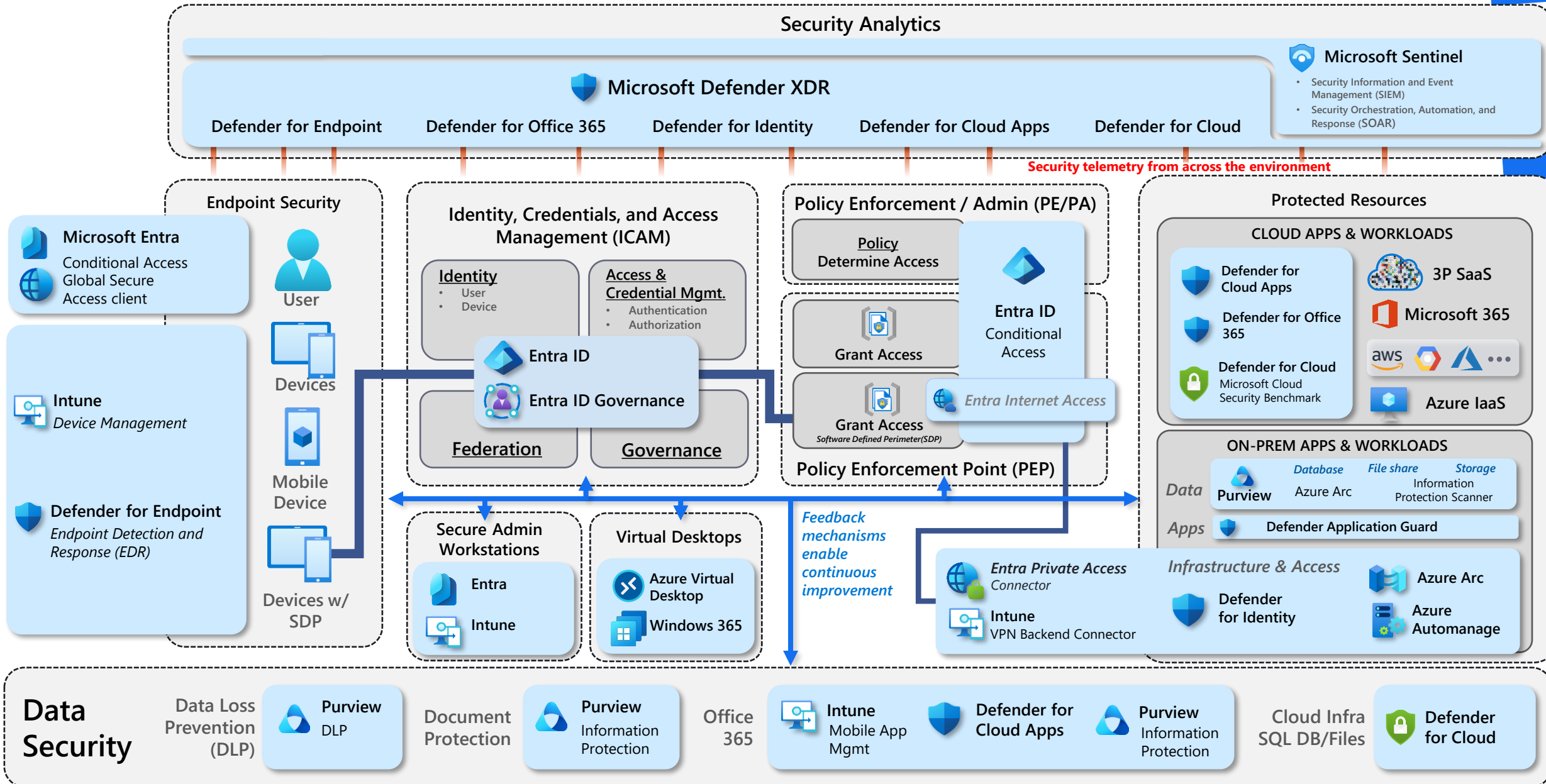
Ułatwia wykrywanie zagrożeń dla cyberbezpieczeństwa i reagowanie zanim zaszkodzą procesom biznesowym

SOAR

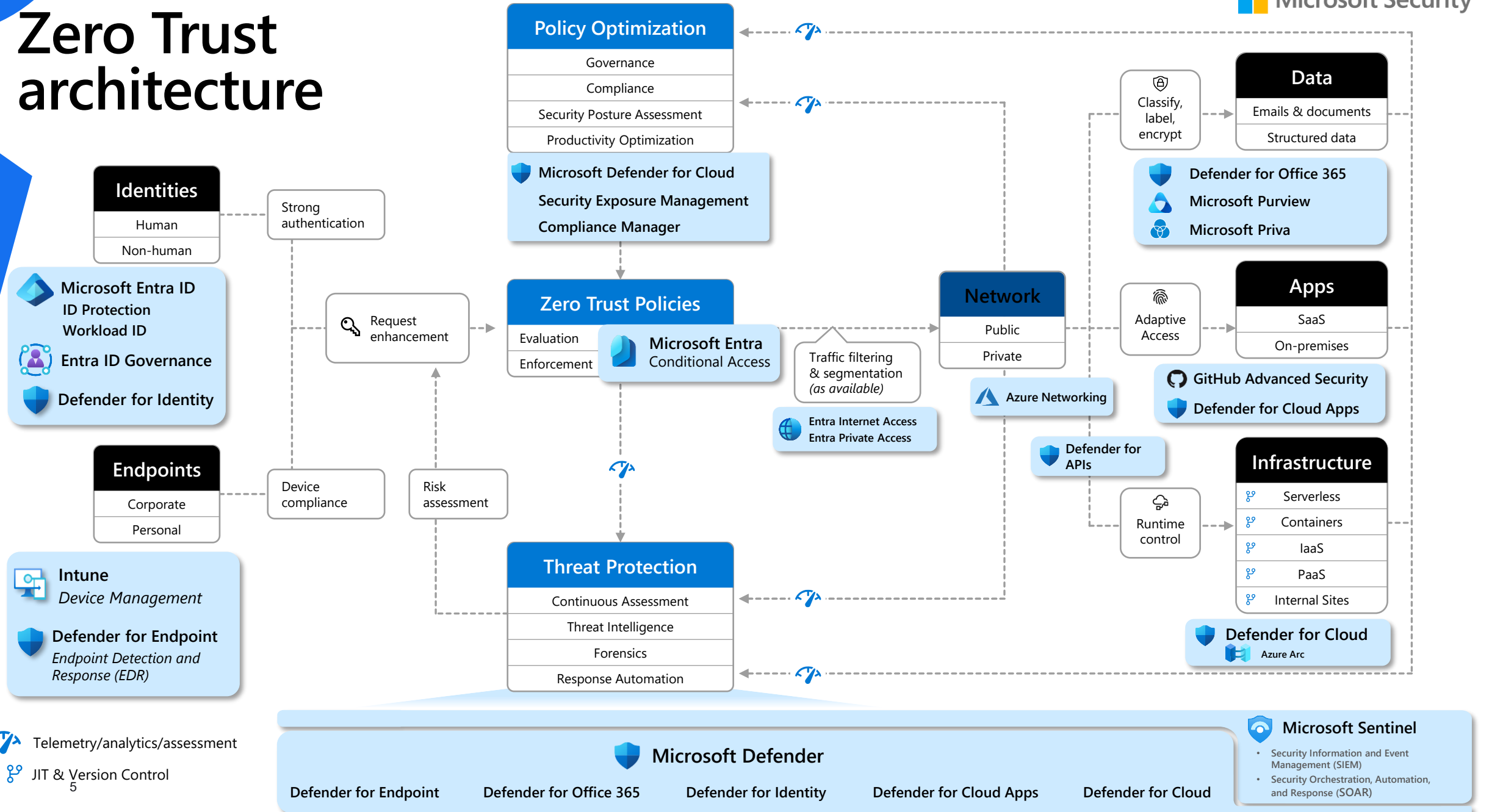
Security Orchestration and Automation Response

Zestaw usług automatyzujących reagowanie na zagrożenia w oparciu o przygotowane mechanizmy i plany

Obszary i nomenklatura - MCRA



Zero Trust architecture



Telemetry/analytics/assessment

JIT & Version Control

Microsoft security capability mapping

Which roles typically use which capabilities

April 2025 – <https://aka.ms/MCR>



Access Control

Establish Zero Trust access model to modern and legacy assets using identity & network controls

Microsoft Entra

Identity Admin, Identity Architect, Identity Security

- **Entra ID (Formerly Azure AD)**
 - Multifactor Authentication
 - Conditional Access
 - Application Proxy
 - External Identities / B2B & B2C
 - Internet/Private Access
 - Identity Governance
 - and more..
- **Windows Hello for Business**
- **Microsoft 365 Defender**
 - Microsoft Defender for Identity
 - Microsoft Defender for Cloud Apps
- **Microsoft 365 Lighthouse** [multi-tenant]
- **Azure Lighthouse**
- **Azure Bastion**
- *Azure Administrative Model*
 - Portal, Management Groups, Subscriptions
 - Azure RBAC & ABAC

Network Security

- **Azure Firewall**
- **Azure Firewall Manager**
- **Azure DDoS**
- **Azure Web Application Firewall**
- *Azure Networking Design*
 - Virtual Network, NSG, ASG, VPN, etc.
 - PrivateLink / Private EndPoint

Endpoint / Device Admin

- **Microsoft Intune**
 - Configuration Management
- **Microsoft Defender for Endpoint**



Security Operations

Detect, Respond, and Recover from attacks; Hunt for hidden threats; share threat intelligence broadly

Incident preparation

Microsoft Defender

Security Operations Analyst

Microsoft Defender XDR

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Entra Identity Protection
- **Microsoft Defender for Cloud**
 - Microsoft Defender for DevOps
 - Microsoft Defender for Servers
 - Microsoft Defender for Storage
 - Microsoft Defender for SQL
 - Microsoft Defender for Containers
 - Microsoft Defender for App Service
 - Microsoft Defender for APIs
 - Microsoft Defender for Key Vault
 - Microsoft Defender for DNS
 - Microsoft Defender for open-source relational databases
 - Microsoft Defender for Azure Cosmos DB
- **Microsoft Security Copilot**
- **Microsoft Sentinel**
- **Microsoft Security Experts**
- *Microsoft Incident Response Detection and Response Team (DART)*

Threat intelligence Analyst

- **Microsoft Defender Threat Intelligence (Defender TI)**
- **Microsoft Sentinel**



Security Governance

Protect sensitive data and systems. Continuously discover, classify & secure assets

Security architecture

- *Microsoft Cybersecurity Reference Architecture*
<https://aka.ms/MCRA>

Posture management, Policy and standards, Compliance management

- **Microsoft Defender for Cloud**
 - Secure Score
 - Compliance Dashboard
 - Azure Security Benchmark
- **Azure Blueprints**
- **Azure Policy**
- **Microsoft Defender External Attack Surface Management (MD-EASM)**
 - Azure Administrative Model
 - Portal, Management Groups, Subscriptions
 - Azure RBAC & ABAC
- **Microsoft Purview**
 - Compliance manager

Data security

- **Microsoft Purview**
 - Information Protection
 - Data Loss Prevention
- **Microsoft 365 Defender**
 - Microsoft Defender for Cloud Apps

People security

- **Attack Simulator**
- **Insider Risk Management**

Privacy Manager

- **Microsoft Priva**



Asset Protection

Continuously Identify, measure, and manage security posture to reduce risk & maintain compliance

Infrastructure and endpoint security, IT Ops, DevOps

- **Microsoft Defender for Cloud** (including Azure Arc)
- **Azure Blueprints**
- **Azure Policy**
- **Azure Firewall**
- **Azure Monitor**
- **Azure Web Application Firewall**
- **Azure DDoS**
- **Azure Backup and Site Recovery**
 - *Azure Networking Design*
 - Virtual Network, NSG, ASG, VPN, etc.
 - PrivateLink / Private EndPoint
 - Azure Resource Locks

OT and IoT Security

- **Microsoft Defender for IoT (& OT)**
- **Azure Sphere**



Innovation Security

Integrate Security into DevSecOps processes. Align security, development, and operations practices.

Application security and DevSecOps

- (Same as Infrastructure Roles)
- **GitHub Advanced Security**
- *Azure DevOps Security*

Moduły Microsoft 365



Microsoft 365 Licensing



Office 365

Aplikacje do pracy biurowej oraz zespołowej

Enterprise Mobility + Security

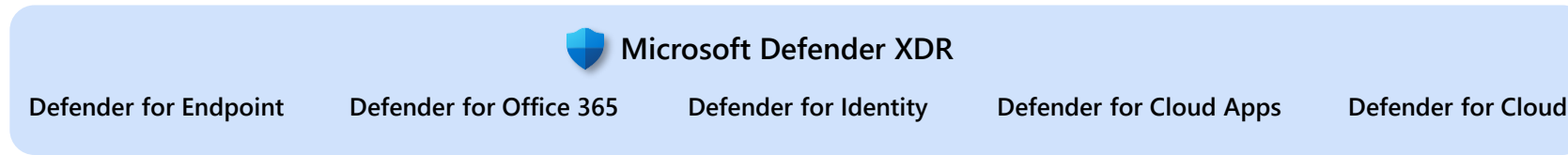
Zarządzanie tożsamością, dostęпами, urządzeniami w organizacji

Windows

Aktualizacje, upgrades, dodatkowe funkcjonalności dodawane do OS

Elementy Microsoft 365 – Produkt vs Licencja vs Plan

Platforma do zarządzania



- Plan 1
- Plan 2
- Business

- Plan 1
- Plan 2

- 1 SKU

- 1 SKU
- + App Governance Addon

Licencjonowane przez Azure PAYG

Dobór licencji i funkcjonalności

1. „Potrzebuję zabezpieczyć się przed utratą danych...”

Identyfikacja produktu pod potrzebę – **Microsoft Purview**

Rozpoznanie licencji obejmujących wskazany obszar – **Data Loss Prevention**

Dobór planu – **Office 365 Data Loss Prevention** lub upgrade do **Business Premium+**

2. „Chcę kompleksowo zabezpieczyć organizację, w której korzystamy z danych aplikacji Microsoft oraz rozwiązań innych dostawców...”

Identyfikacja produktu – **Microsoft XDR**

Rozpoznanie licencji – **Microsoft Defender for Office, Endpoint, Identity...**

Dobór planu – w zależności od posiadanych licencji i wykorzystywanych aplikacji:

- **Business Premium + Defender for Identity,**
- **M365 E3**
- **Pojedyncze licencje Defender for Office p1, Endpoint p1, Identity...**

Defender & Purview Suites

Microsoft Defender Suite for Microsoft 365 Business Premium

Bring Microsoft 365 E5 advanced security to your business at an affordable price, for up to 300 users.

Microsoft Purview Suite for Microsoft 365 Business Premium

Bring Microsoft 365 E5 data security, compliance, and governance to your business at an affordable price, for up to 300 users.

Microsoft Defender and Purview Suites for Microsoft 365 Business Premium

Bring Microsoft 365 E5 advanced threat protection, data security, and compliance to your business for up to 300 users.

- Microsoft 365 E5 Compliance staje się **Microsoft Purview Suite**
- Microsoft 365 E5 Security staje się **Microsoft Defender Suite**
- **Defender i Purview Suites** są dostępne dla pakietów E3, A3, F3, oraz **Business Premium**

Dostępny bundle w niższej cenie!

A photograph of a modern office environment. In the foreground, a man with a beard and a checkered shirt is seated at a desk, looking at a computer monitor. The monitor displays a dashboard with various charts and graphs. In the background, other office workers are visible at their desks. A large blue circular graphic is overlaid on the right side of the image.

Dziękuję!