Microsoft CERTIFIED EXPERT

Microsoft 365 Defender: Protecting Against Insider & External Attacks

Perparim Abdullahu – Cloud Security Architect | #PerparimLabs

#Microsoft365Defender #ZeroTrust #PerparimLabs

PerparimLabs

What is Microsoft 365 Defender?

- Unified defense suite
- Integrates with M365 + Azure
- Orchestrates protection & response

Defender for Endpoint

- Protects on-prem & mobile devices
- Endpoint behavior sensors
- Threat intelligence & analytics

Defender for Office 365

- Starts with **Exchange Online Protection**
- **Safe Links** & **Safe Attachments**
- P1 = protection / P2 = investigation & simulation

Defender for Identity

- Integrates with Azure AD & on-prem AD
- Real-time detection & posture assessment
- Automated response

Defender for Cloud Apps

- CASB capabilities (Cloud App Security)
- Restrict risky SaaS use (e.g., allow Dropbox Business, block Personal)
- Policy enforcement + activity monitoring

Defender Vulnerability Management

- Tracks OS & device vulnerabilities
- Supports Windows, Mac, Linux, iOS, Android
- Links to Microsoft Threat Intelligence

Entra ID Protection

- Formerly Azure AD Identity Protection
- Detects risky sign-ins & users
- Allows/block/challenge policies

Data Loss Prevention (DLP)

- Monitors sensitive data (SSN, credit cards, health data)
- Prevents sharing/leakage
- Works across Exchange, Teams, SharePoint, OneDrive, Power BI

App Governance

- Monitors OAuth-enabled apps
- Provides insights & governance
- Detects suspicious app behavior

Summary: Why Defender Suite?

- Unified protection across M365 & Azure
- Insider + external threat coverage
- AI-driven detection & automation

Call to Action (CTA)

💡 *Explore more Defender labs & security projects:*
https://perparimlabs.github.io
🤝 Connect with me on **LinkedIn**
“Follow #PerparimLabs for daily Microsoft Security insights”

#Microsoft365Defender #ZeroTrust #PerparimLabs

PerparimLabs