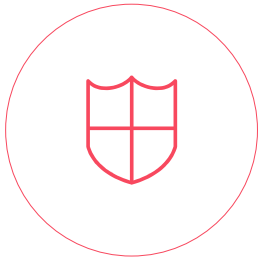




# Microsoft **Defender 365**

Enterprise defense suite





# Microsoft Threat Protection

MS Defender 365 employs AI and automation that support your SOC team in their daily tasks of detecting attacks and remediation on affected assets.



**Security**, at all levels, should be correlated with business priorities, IT initiatives and risks the organization can accept.

Security should feel like a natural part of the business. Business should feel like a natural part of security.



Endpoints



Identities



Cloud apps



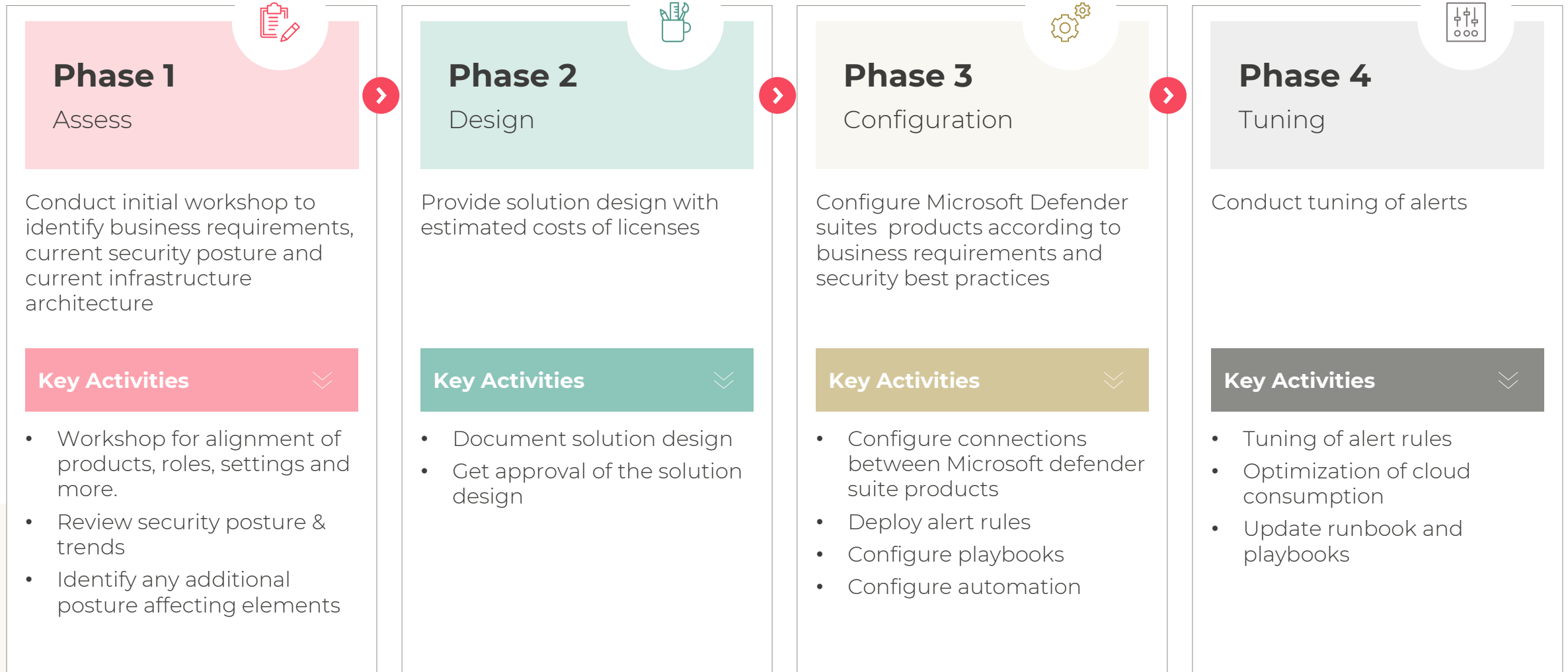
E-mails  
and documents



---

# **Tune XDR solution** according to your needs

# Delivery Method



# Defender 365



## Product scope



### Defender for Identity

#### Features

- Reduce the attack surface
- Identity configuration
- Privileged access
- Manage and update sensor



### Defender for Office 365

#### Features

- Preset Policies
- Configuration Analyzer
- Review message overrides
- Automate investigation and response



### Defender for Endpoint

#### Features

- Attack surface reduction config
- AV scanning
- Tamper Protection
- Intune configuration
- Network protection
- Reporting and alerts
- Shadow IT Discovery



### Defender for cloud app

#### Features

- Cloud governance policies
- Manage OAuth apps policy
- Data exposure policies
- Tune Anomaly policies
- Microsoft Purview integration \*



### Azure AD Identity protection

#### Features

- Alerts overview
- Automated threat response



### Data Loss Prevention \*

#### Features

- Meet compliance requirements
- Protect sensitive data on endpoints

Security baselines

Identity controls

Integration across  
suite kit

Governance and data  
protection

Response  
automation

\* will be enabled if the customer already has Microsoft Purview in use



## Cross-product overview

To better understand security alerts SOC team should have a good overview across endpoints, network and identities



# Microsoft Defender 365

Microsoft Defender 365 is a cloud-based enterprise defense solution, that helps to cover all layers of the infrastructure and data for easier and faster response to cyberattacks.

With Defender 365 your SOC team has access to investigate the whole story of the attack across product alerts, behaviors and context.



## Scope



- MS Defender for Identity
- MS Defender for Office 365
- MS Defender for Cloud apps
- MS Defender for Endpoint
- Azure active Directory Identity Protection
- Data Loss Prevention \*



## Process



- Assess current infrastructure and identify business requirements
- Design solution and estimate cost
- Configuration and implementation according to business requirements
- Tuning of alerts and cost optimization



## Outcome



- Protect endpoints
- Protect identities
- Protect data
- Protect workloads
- Automate responses to common attacks



## Duration



- Estimated 6-10 weeks, provided required permissions and relevant stakeholders are available



## Price



- Depends on the company size





---

# Who are **Devoteam**

# Devoteam M Cloud: a preferred partner in EMEA



## Sized for agility and trust

Gold  
Microsoft  
Partner

Azure  
Expert  
MSP

+ 125 M€  
Revenue

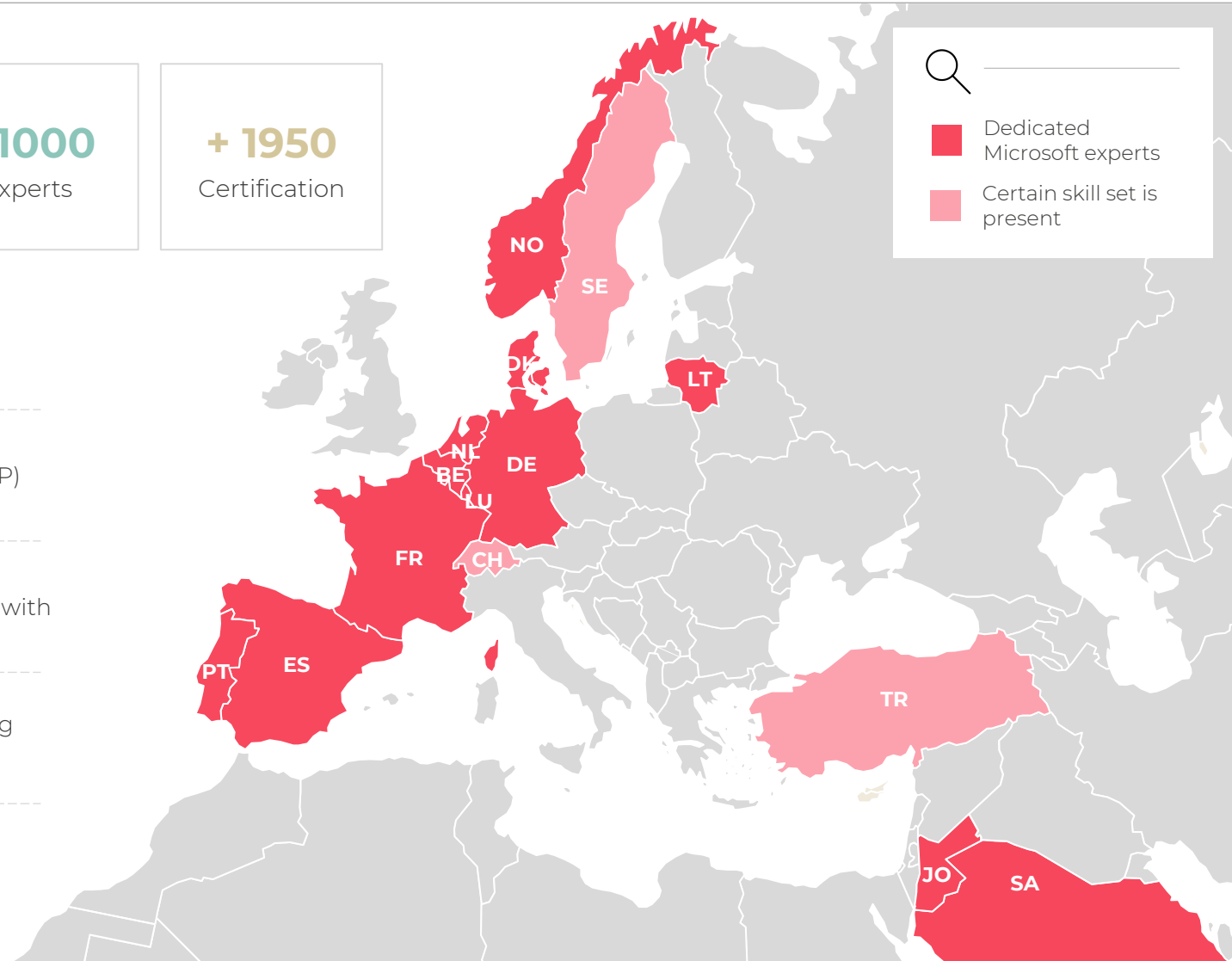
+ 1000  
Experts

+ 1950  
Certification

## Our expertise

- 16 Gold** competencies
- 9 Advanced** specializations:
  - Change & Adoption
  - LowCode Development
  - Threat Protection
  - Windows and SQL migration
  - Calling for Teams
  - Application Modernisation
  - Kubernetes on Azure
  - Meetings and Rooms for Teams
  - Teamwork Deployment

- FastTrack Ready
- Direct Reseller (CSP)
- Cloud and Hybrid Managed Services with own IP
- Authorized Training Partner
- 2019-2021 Partner of the Year Award





# Thank **you.**

---