devoteam

# Security Accelerator

## Sentinel – Cloud Native SIEM

Fast track your design, deployment
and implementation

**Creative tech for Better Change**

1

# Azure Sentinel – a modern solution for modern threats

*“The are constantly attack on IT and Cloud infrastructure in all levels. If your organization didn’t observe anything, you are doing something wrong or investing in wrong security tools”*

Proactive security baseline

# evolving **security management** to match your digital transformation

## Detection

- Continuous detection of threats across a changing cloud environment
- Evaluation of resources to identify potential vulnerabilities
- End-to-end detection from cloud native resources to VM´s and endpoints

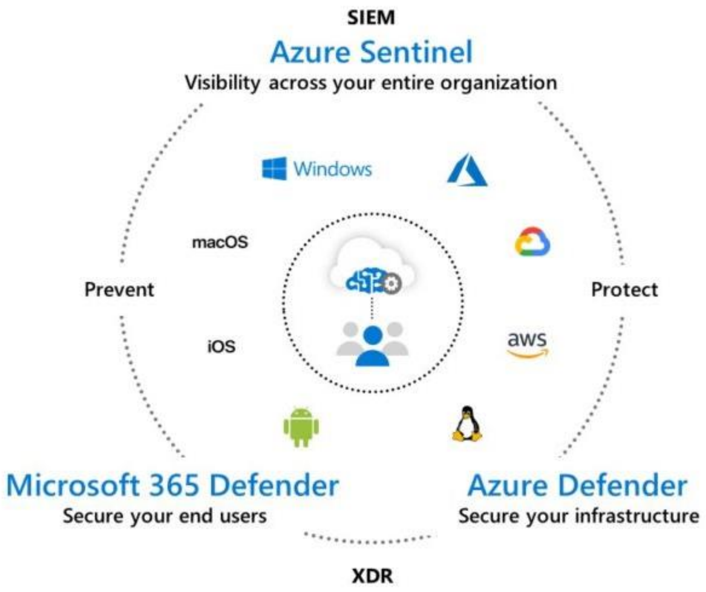
+

## Response

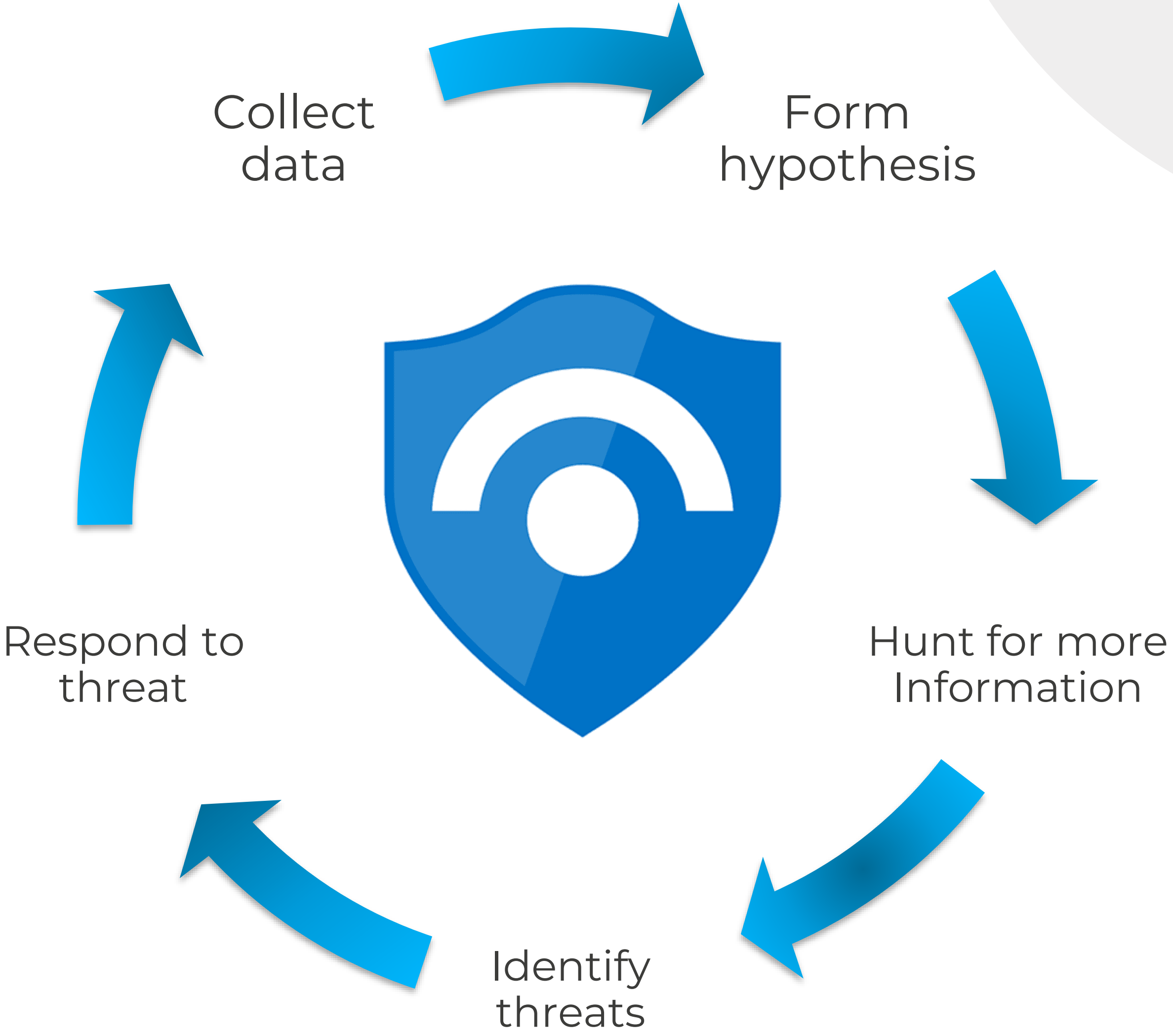
- Staff trained in cloud security and remediation of vulnerabilities and threats
- Remediation of identified events, alerts and vulnerabilities for cloud services and endpoints
- Capable of creating new code driven policies, connectors and automation

Azure Sentinel, a Microsoft SIEM solution

# Provides security analytics based on AI at the cloud scale for entire enterprise

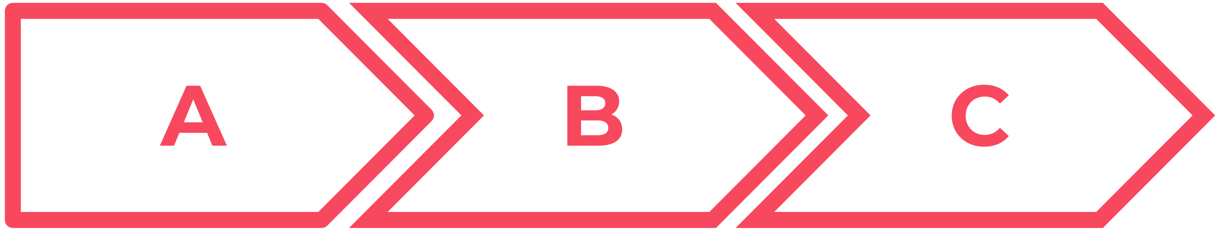


# Threat hunting circle



2

# Maturing your security posture with **3 phases**



A

B

C

# Cloud Security Deliveries

## A

### Cloud Security assessment

**Fact finding assessment**
Devoteam will conduct interviews and collect data.
The purpose is to check the current security posture of your Microsoft Tenant, both Oficce365 and Azure.

Clear prioritization of security risks on your platform.

## B

### Sentinel Accelerator

**Design, deploy and improve**
Set up Cloud-native SIEM with Sentinel. Enabling your own SOC or IT department to get full visibility on the ongoing threats towards your platform.

We will ensure multiple connectors are collecting data from relevant sources on your infrastrucure.

## C

### Managed Cloud Security

**Taking care of your SOC**
Starting or up-skilling your existing SOC and be a longer journey. Therefore, we offer the possibility for a managed service, where Devoteam Global Managed Service manage your SOC and response to threats.

Operations is running 24/7 – watching your environment.

# Sentinel Accelerator

Design and deploy your Cloud Native SIEM solutions.

devoteam

We define the connectors needed to manage the threats towards your organization. We ensure a fast-track implementation of Sentinel deployed with relevant analytics rules and playbooks, so threats are detected.

## KEY FEATURES

- Deployment of Azure Sentinel
- Connect 5 data connectors, spanning from Cloud to on-prem systems.
- Configuration of threat intelligence sources and hunting capability
- Enabling workbooks based on connectors and setup playbooks
- Provide comprehensive documentation, ensuring that your own team can continue to work with Sentinel

## ACTIVITIES

- Workshop with internal stakeholders to ensure data connectors and Sentinel opportunities are aligned
- Handover session with client, ensuring alignment on operational excellence and future roadmap

## TOOLS

- Azure Sentinel
- Sentinel Connectors

## BENEFITS

- Fast track implementation
- Cost optimization
- Transparency and visibility across resources for both users, devices, application and infrastructure
- Respond to incidents rapidly with built-in orchestration and automation of common tasks
- Detect patterns and changes from the norm as well as irregularities in your IT environment

## OUR APPROACH

- Identify relevant data connectors together with customers' stakeholders
- Delivering a scalable design
- Deploy and implement the agreed solution
- Provides documentation and handover session, so customer is ready to run Sentinel
- Fine tuning deployed rules after collecting production data

Gold Microsoft Partner Microsoft

Azure Expert MSP

3

# Devoteam M Cloud Managed Cloud Security

24/7 operation with best practices

What is Managed Cloud Security

# what you can expect from our **Managed Cloud Security** service

## Platform

- Leverage Defender for Cloud to achieve Cloud Security Posture Management and Cloud Workload Protection
- Cross cloud tooling supporting engage on-premises and multicloud (Azure, AWS and GCP
- Continually assess security posture for progress and react to recommendations and alerts

## SIEM

- Central collection of logs across cloud and on-premises sources
- Utilize Advanced Security Information Model (ASIM) security content
- Collection and correlation of Microsoft 365 sources and events
- Implementation of global frameworks such as MITRE ATT&CK

## SOAR

- Advanced orchestration fueled by Microsoft, opensource and Devoteam
- Access to hundreds of connectors from Microsoft and 3rd part suppliers
- Creation of custom connectors for customer specific needs
- 24x7 monitoring, investigation and remediation team

Managed Detection and Response

# Devoteam Managed Cloud Security

key figures

< 30 min
guaranteed response

95%
service levels

>30
certifications

74%
automated response

365
access to analytics

24x7
active operations

3
spoken languages

19
supporting countries

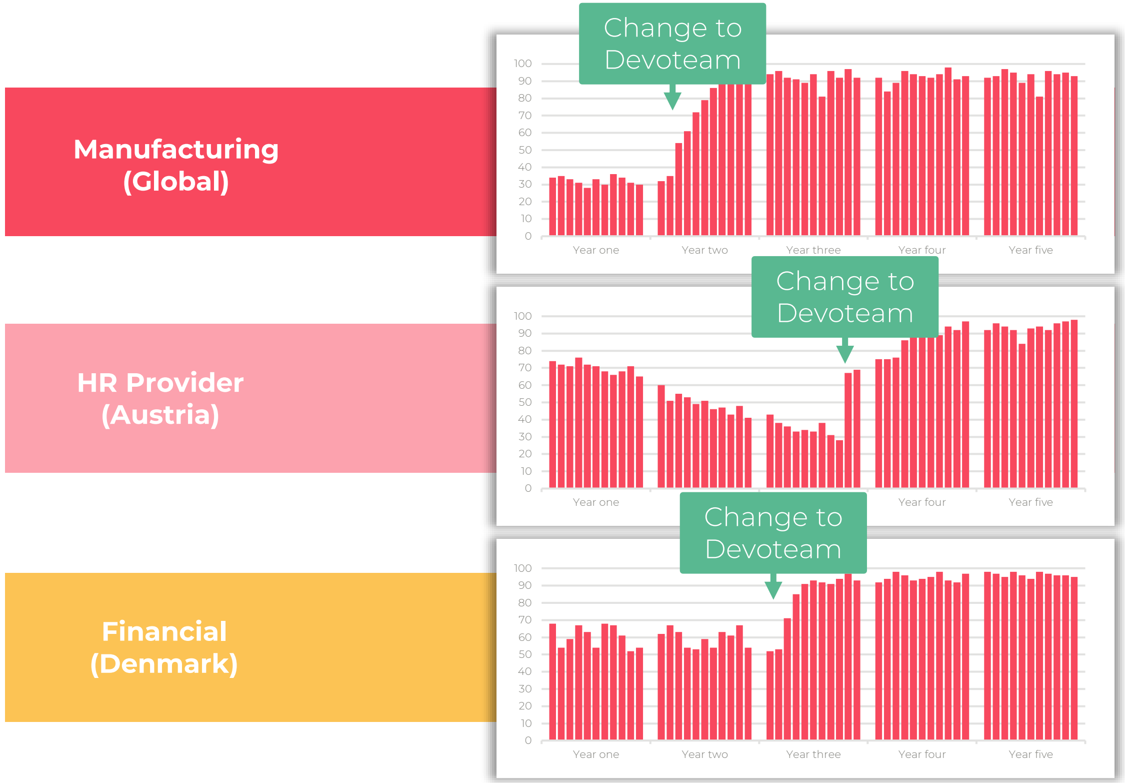
**Security posture increase**

# driving **security excellence** to the next level

- Reduce reaction time via automation
- Prioritized remediation efforts
- Leverage global standards
- Cloud native SOAR transparency
- **Customer owned | partner driven**

**↑42%**

**Higher security posture score**



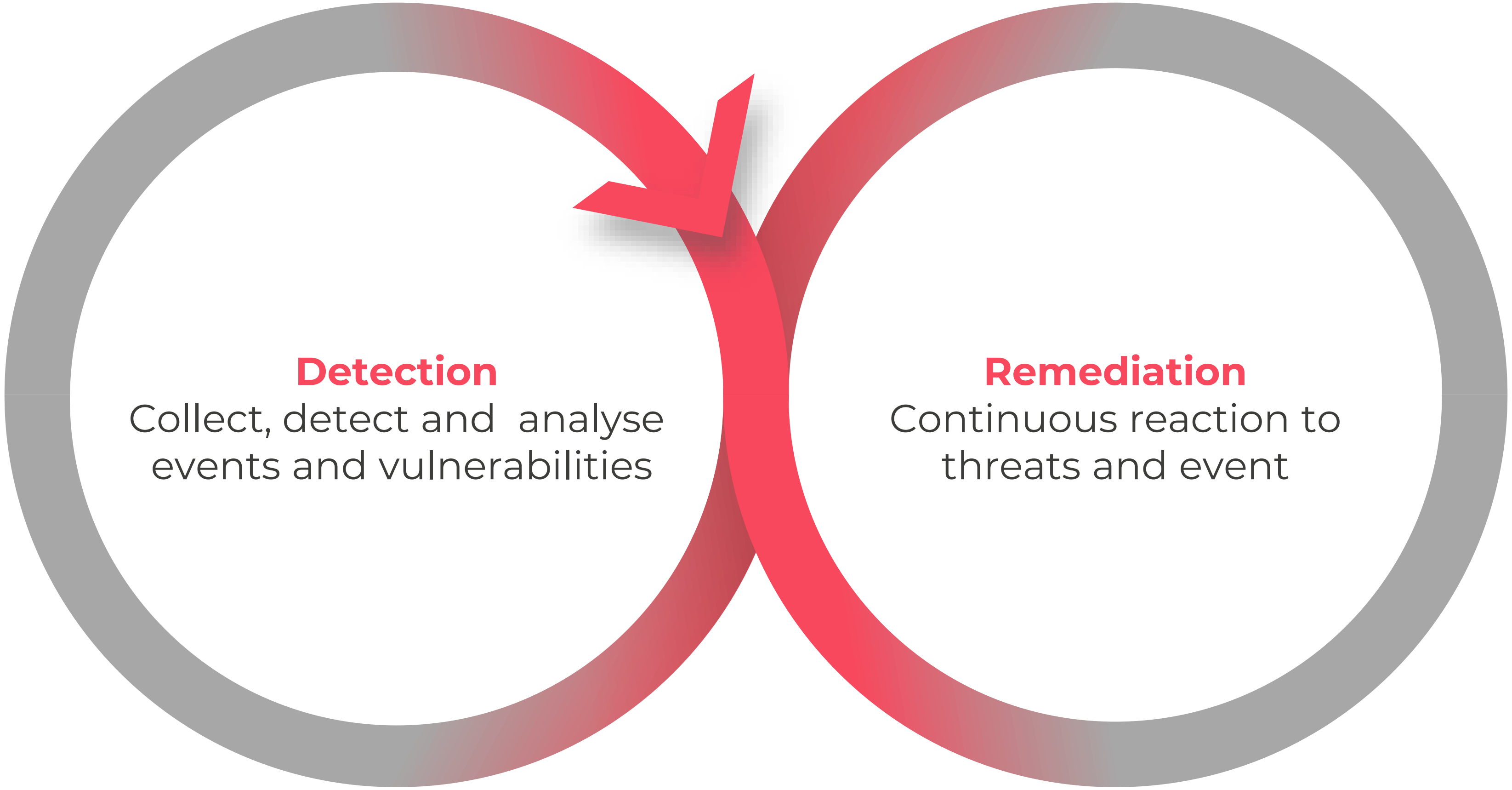
**Manufacturing (Global)**

**HR Provider (Austria)**

**Financial (Denmark)**

Our security lifecycle

# From detection to remediation **and over again**



**Detection**
Collect, detect and  analyse events and vulnerabilities

**Remediation**
Continuous reaction to threats and event

# 4

## Who are Devoteam

# Devoteam M Cloud: **a preferred partner in EMEA**

**Sized for agility and trust**

Gold
Microsoft
Partner
Microsoft

Azure
Expert
MSP

| | |
|---|---|
| + 125 M€ | Revenue |
| + 1000 | Experts |
| + 1950 | Certifications |

## Our expertise

- 16 Gold competencies
- 9 Advanced specializations:

Change & Adoption
Low Code Development
Threat Protection

Windows and SQL migration
Calling for Teams
Application Modernisation

Kubernetes on Azure
Meetings and Rooms for Teams
Teamwork Deployment

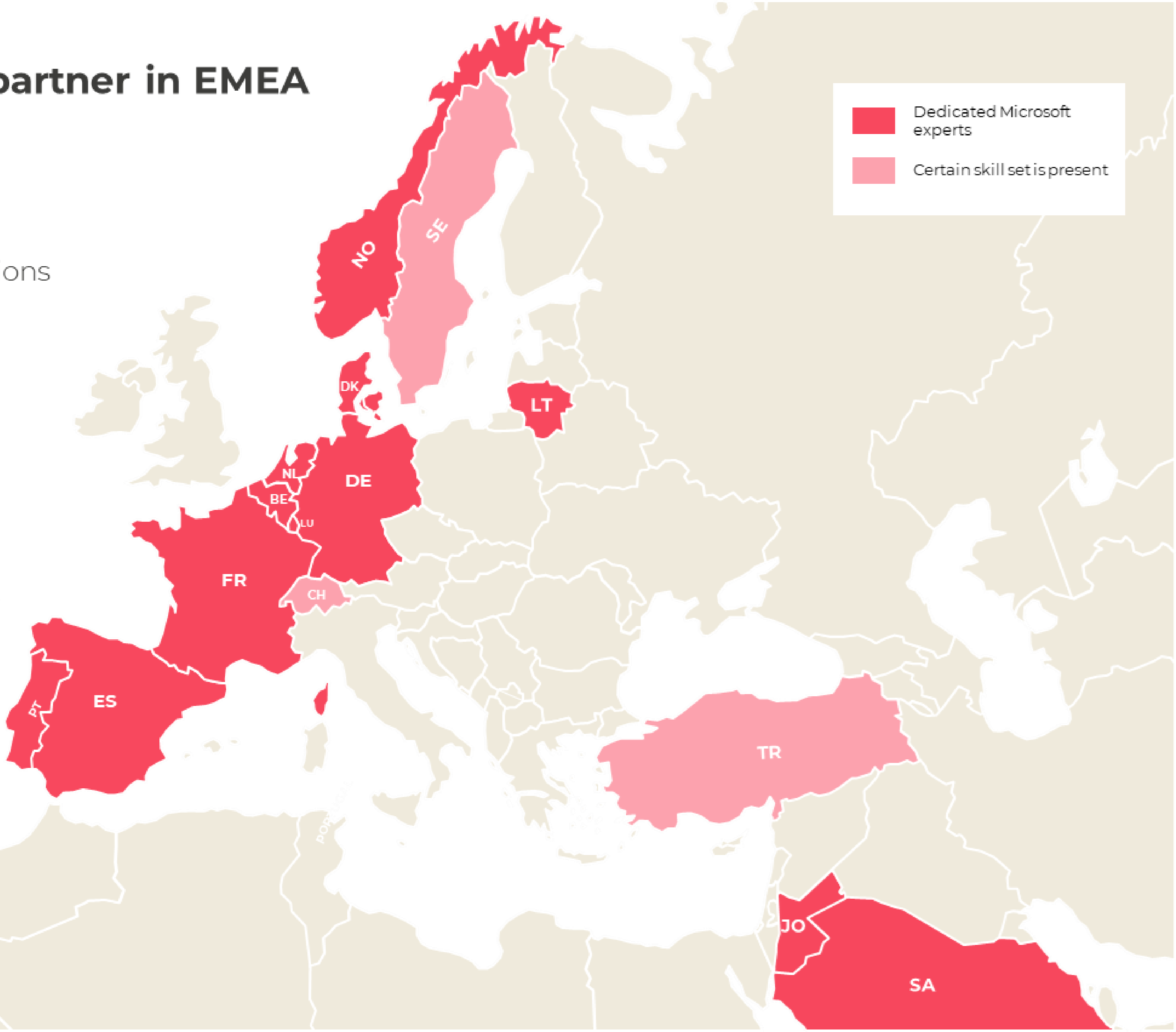
✓ FastTrack Ready

✓ Direct Reseller (CSP)

✓ Cloud and Hybrid Managed Services *with own IP*

✓ Authorized Training Partner

2019-2021
Partner of the Year Award



Creative tech for Better Change

# Thank you