devoteam
M Cloud

Cloud Native **SIEM** solution

Fast track your Microsoft Sentinel design, deployment and implementation

devoteam
M Cloud

Microsoft Sentinel

a modern solution for modern threats

devoteam
M Cloud

“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

devoteam M Cloud

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

Microsoft Sentinel, a Microsoft SIEM solution

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

Threat **hunting circle**

devoteam
M Cloud

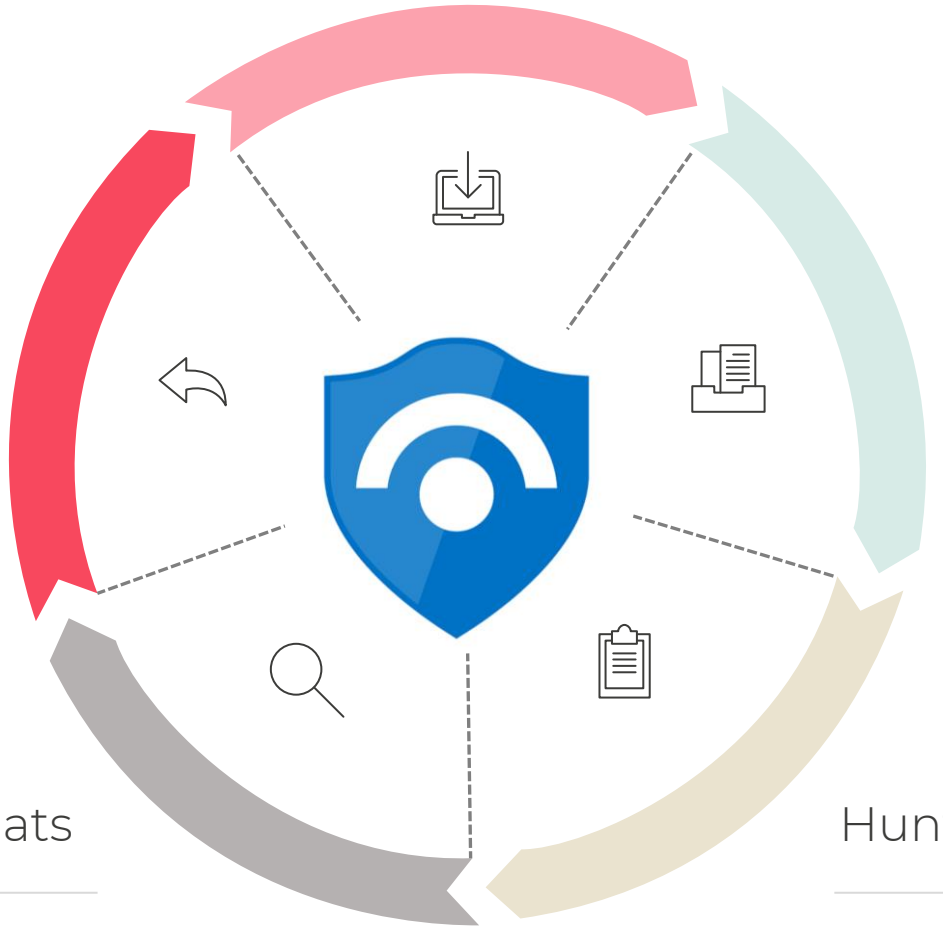
Collect data

Form hypothesis

Hunt for more Information

Identify threats

Respond to threat



devoteam
M Cloud

Setup and tune Cloud SEIM solution to the company's needs

1 › 2 › 3 › 4

Delivery **Method**

devoteam M Cloud

Phase 1
Assess

Conduct assessment and workshop with stakeholders

Key Activities

- Infrastructure assessment
- Workshop to collect business requirements
- Workshop for the current problems

Phase 2
Design

Design solution an estimate the cost

Key Activities

- Document solution design
- Estimate cost of the solution
- Get approval of the solution design

Phase 3
Implementation

Setup connectors and automate response

Key Activities

- Deploy Sentinel
- Setup solutions
- Setup connectors and playbooks and create analytic rules
- Verify setup

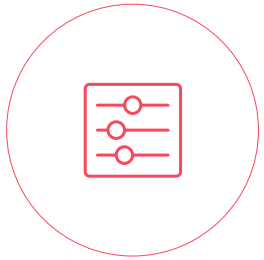
Phase 4
Tuning

Aanalyze cost and tune Alert detection

Key Activities

- Adjust alerts to reduce white noise
- Review cost
- Verify information received from different connectors

devoteam
M Cloud



Microsoft Sentinel accelerator

Empower your SOC team with a modern SEIM cloud-based solution to have proactive threat hunting and automatic response. Get your security to the next level.

Microsoft Sentinel **Accelerator**

Design and deploy your Cloud Native SIEM solutions.

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.

devoteam M Cloud

Scope

- Deployment of Microsoft 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

Process

- Workshop with internal stakeholders to ensure data connectors and Sentinel opportunities are aligned
- Design the solution according to the company needs
- Implementation and tuning, to reduce cost and white noise
- Handover session with client, ensuring alignment on operational excellence and future roadmap

Outcome

- Documentation and handover session
- Transparency and visibility across resources for both users, devices, application and infrastructure
- Automated response to common tasks
- Dashboards to detect patterns and changes from the norm as well as irregularities in your IT environment

Duration

- Estimated 3 weeks, provided required permissions and relevant stakeholders are available

Price

- From 70.000 DKK

devoteam
M Cloud

Who are **Devoteam**

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

devoteam M Cloud

Sized for agility and trust

Gold Microsoft Partner

Azure Expert MSP

+ 125 M€ Revenue

+ 1000 Experts

+ 1950 Certification

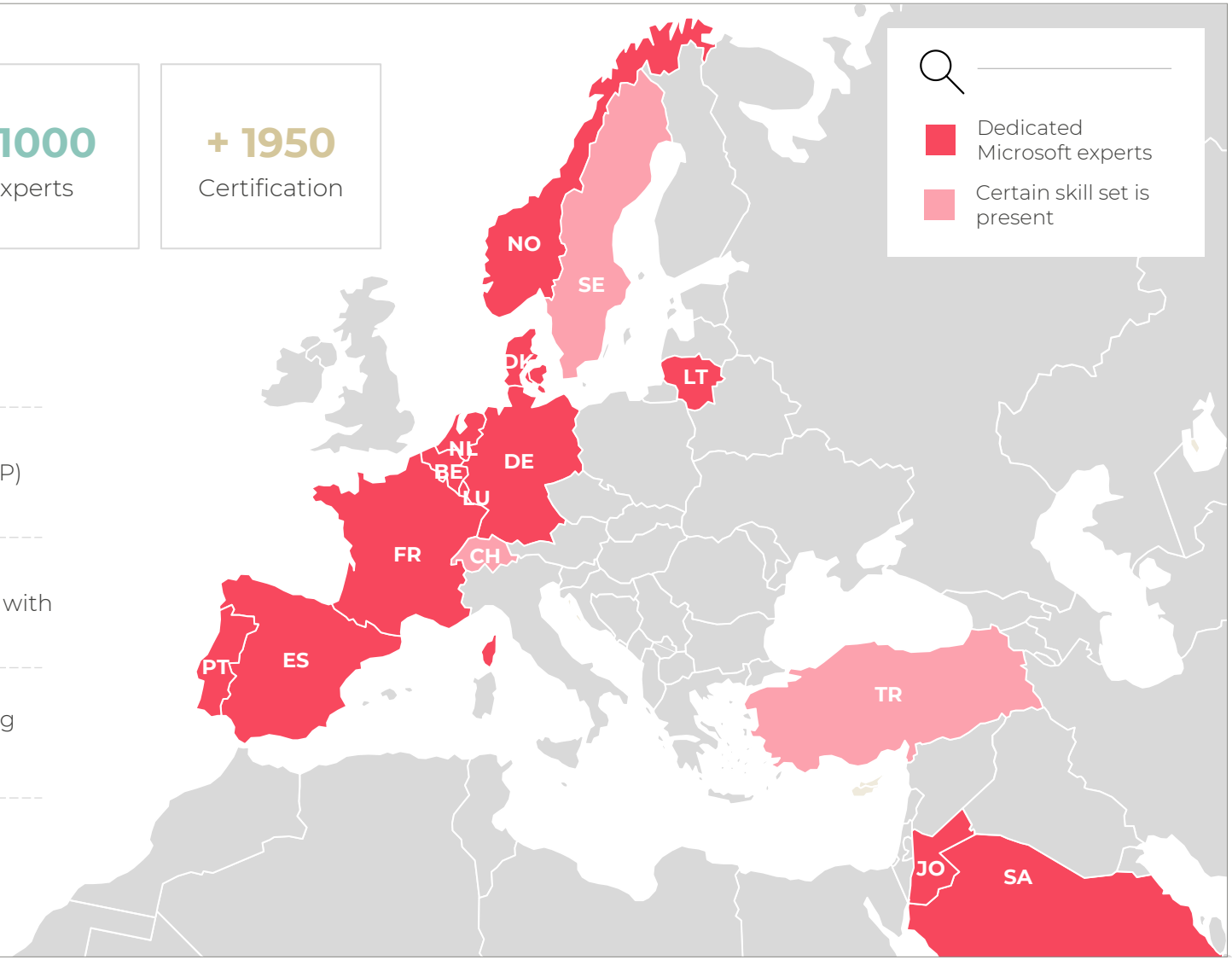
Our expertise

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



devoteam
M Cloud

Thank **you.**