Empowering 💪 Cloud Security with Microsoft Sentinel, Defender for Cloud and Defender XDR

Fabian Bader, Thomas Naunheim
Cyber Security Architects @ glueckkanja AG

Sponsors

Fabian Bader | Thomas Naunheim

Cyber Security Architect @ glueckkanja AG, Microsoft MVP

Microsoft Defender for Cloud

Strengthen and manage your security posture

Security compliance management

At-scale governance & automated remediation

Attack path-based prioritization

Full visibility with agentless and agent-based scanning

Detect threats and protect your workloads

Full-stack threat protection

Vulnerability assessment & management

Automate with the tools of your choice and native integration in Microsoft Sentinel

Unify your DevOps security management

DevOps posture visibility across pipelines

Infrastructure as Code security

Code to cloud contextualization

Integrated workflows & pull request annotations

Amazon Web Services

Microsoft Azure

Google Cloud Platform

On-premises

Microsoft Defender for Cloud

Assess across DevOps lifecycle

Defender CSPM

DevOps Security

Threat protection for Azure service layer

Defender for Resource Manager

Defender for Key Vault

Defender for DNS

Defender for Cloud network-layer analytics

Threat protection for common cloud resources

Defender for Servers

Defender for (Azure) SQL

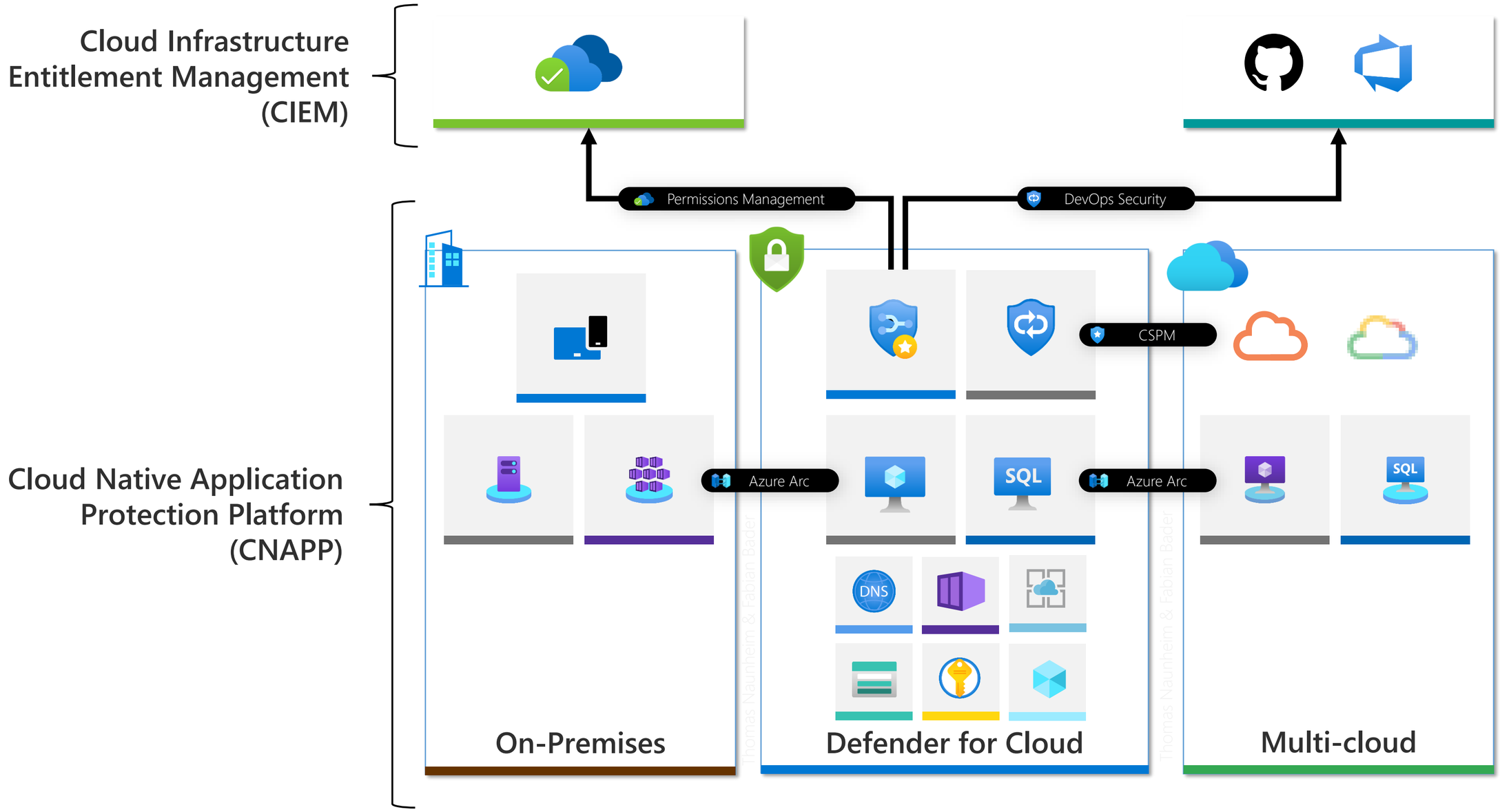
Defender for App Services

Defender for Storage

Defender for Containers

Defender for Cosmos DB

Defender for MySQL, MariaDB, PostgreSQL


Cloud Infrastructure Entitlement Management (CIEM)
Cloud Native Application Protection Platform (CNAPP)
Permissions Management
DevOps Security
CSPM
Azure Arc
Azure Arc
SQL
SQL
DNS
On-Premises
Defender for Cloud
Multi-cloud
Thomas Naunheim & Fabian Bader
Thomas Naunheim & Fabian Bader

Permissions Management and Defender for Cloud capabilities

Category	Capabilities	Defender for Cloud	Permissions Management
Discover	Permissions discovery for high-risk identities (including unused identities, overprovisioned active identities, unused super identities) in Azure, AWS, and GCP	✓	✓
	Permissions Creep Index (PCI) for multicloud environments (Azure, AWS, GCP) and all identities	✓	✓
	Permissions discovery for all identities, groups in Azure, AWS, and GCP	X	✓
	Permissions usage analytics, role/policy assignments in Azure, AWS, and GCP	X	✓
	Support for Identity Providers (including AWS IAM Identity Center, Okta, Google Workspace)	X	✓

Permissions Management and Defender for Cloud capabilities

Category	Capabilities	Defender for Cloud	Permissions Management
Remediate	Automated deletion of permissions	X	✓
	Remediate identities by attaching/detaching the permissions	X	✓
	Custom role/AWS Policy generation based on activities of identities, groups, and users.	X	✓
	Permissions on demand (time-bound access) for human and workload identities via Microsoft Entra Admin Center, APIs, ServiceNow app.	X	✓
Monitor	Machine Learning-powered anomaly detections	X	✓
	Activity based, rule-based alerts	X	✓
	Context-rich forensic reports (for example, PCI history report, user entitlement and usage report)	X	✓

Live Demo
Microsoft Defender for Cloud

Microsoft Defender XDR

Microsoft Defender for Office 365

- E-Mail Protection
- Safe Link
- Safe Attachments
- Automated Investigation and Response

Microsoft Defender for Endpoint

- Next Generation Protection
- Extended Detection and Response
- Advanced Hunting
- Automated Investigation and Response

Microsoft Defender for Identity

- On-Premises Identity Protection
- Lateral Movement Detection
- Response Actions

Microsoft Defender for Cloud Apps

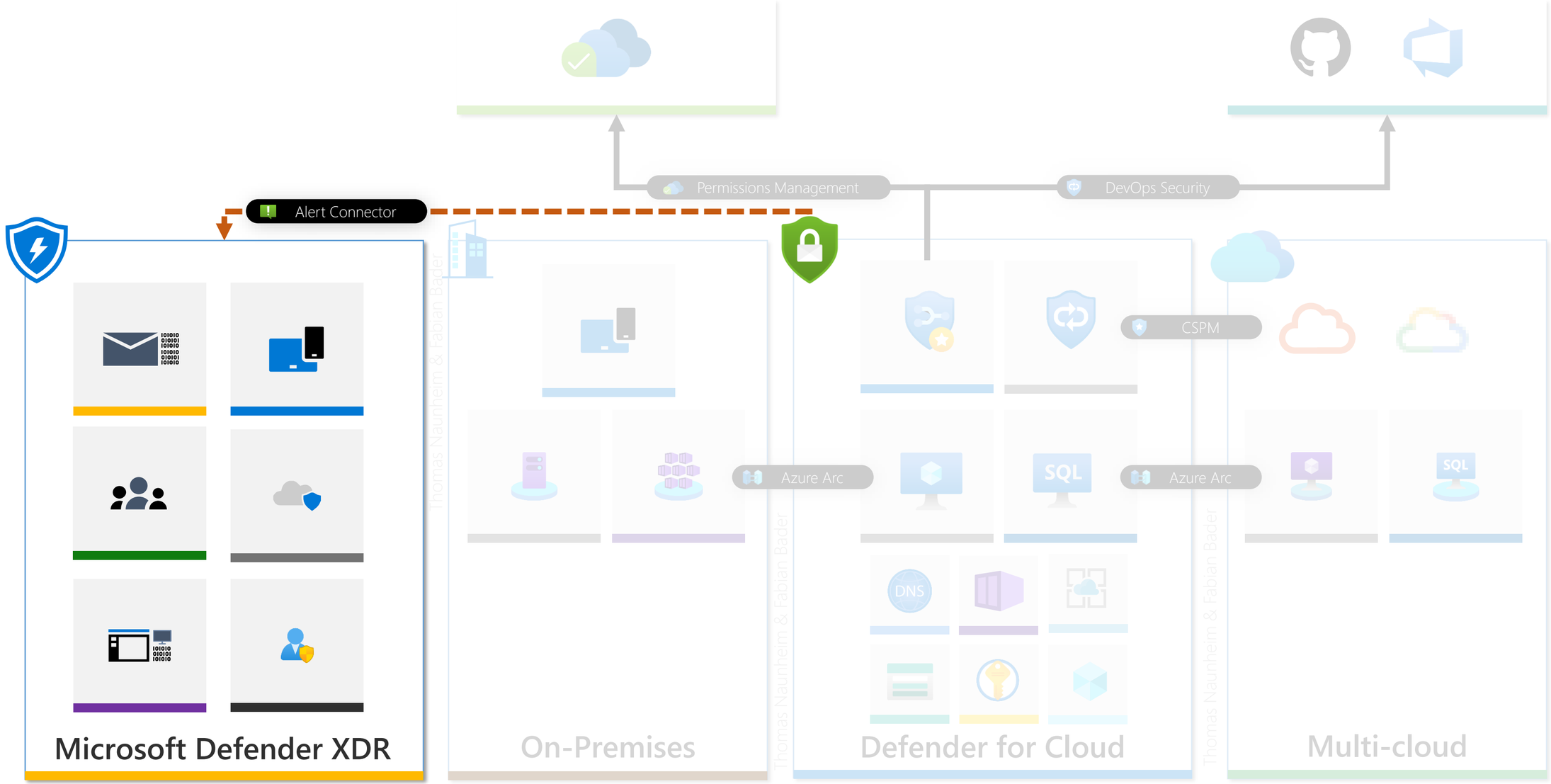
- Cloud Access Security Broker
- Protect sensitive data
- Protect 3rd party SaaS provider

Microsoft Defender Vulnerability Management

- Security baselines assessments
- Block vulnerable applications
- Network share assessment

Microsoft Entra ID Protection

- Cloud Identity Protection
- AI based anomalie detection
- Block based on Risk Level
- User based remediation


Permissions Management
DevOps Security
Alert Connector
CSPM
Azure Arc
Azure Arc
SQL
SQL
DNS
Microsoft Defender XDR
On-Premises
Defender for Cloud
Multi-cloud
Thomas Naunheim & Fabian Bader
Thomas Naunheim & Fabian Bader
Thomas Naunheim & Fabian Bader

Live Demo
Microsoft Defender XDR

Microsoft Sentinel

Scalable and open architecture

Cloud scaling

Third-Party data sources using API, Syslog and CEF

Native integration with MDE and MDC

DevSecOps support

Advanced Analytics Capabilities

Kusto Query Language

Community content

Content Hub for advanced integrations

Custom and template-based Analytics Rules

Workbooks

Watchlists for persistent data

Threat indicators

Jupyter notebooks

Incident and Threat Management

Built-In Threat Hunting

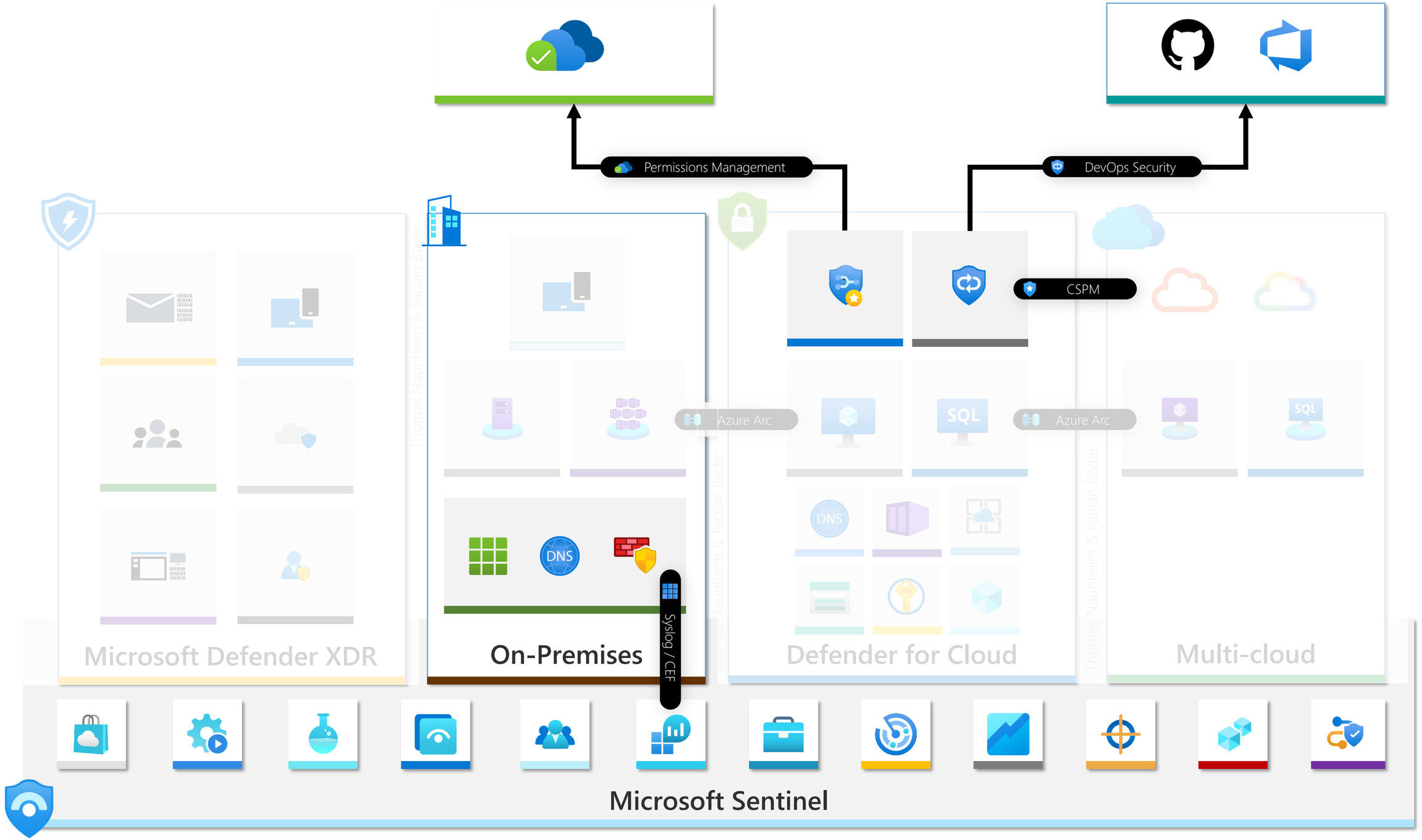
Azure Machine Learning

MITRE ATT&CK dashboard

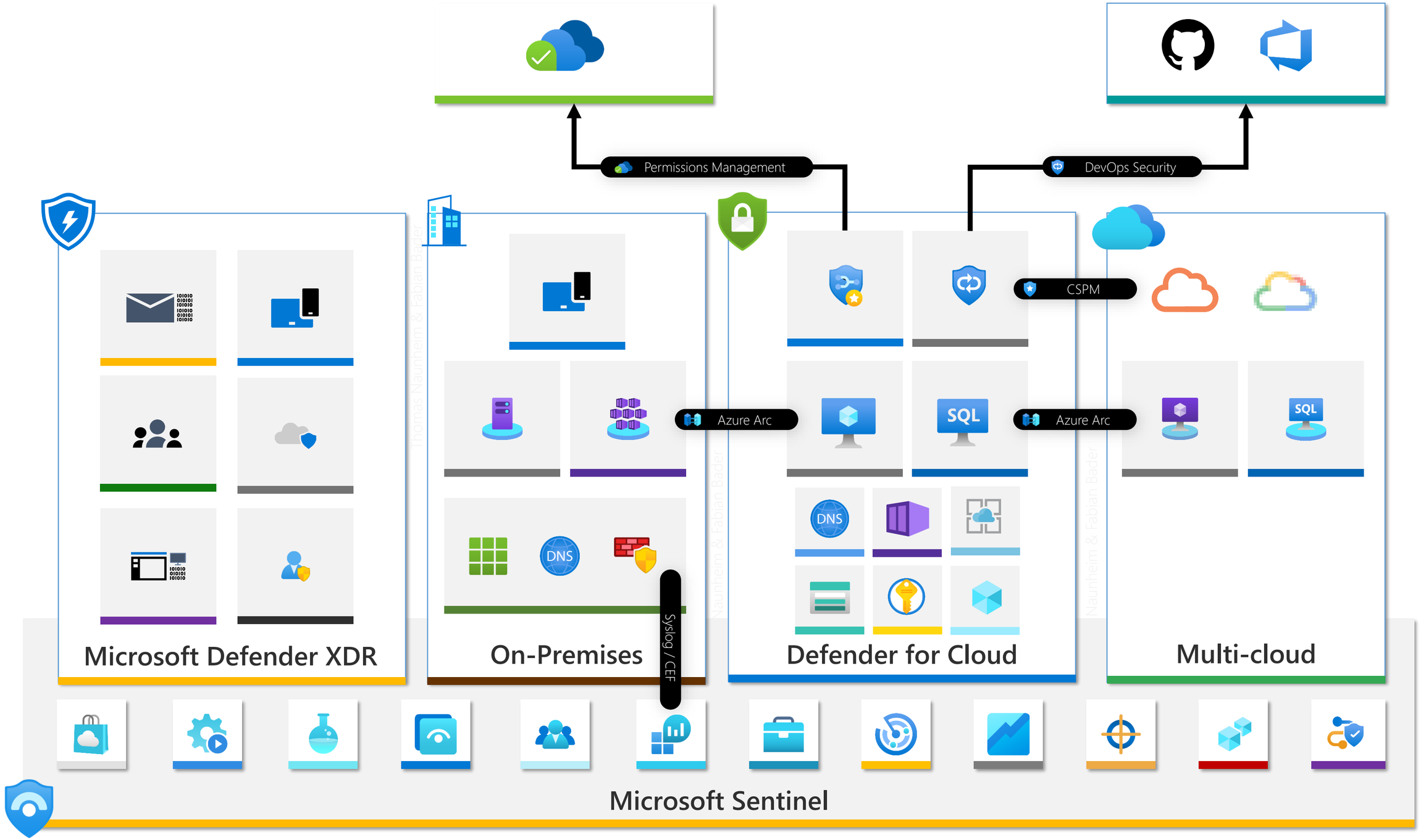
User and entity behavior analytics

Automated response using playbooks

Incident correlation and management


Permissions Management
DevOps Security
CSPM
Azure Arc
Azure Arc
SQL
SQL
DNS
DNS
Syslog / CEF
Microsoft Defender XDR
On-Premises
Defender for Cloud
Multi-cloud
Microsoft Sentinel
Thomas Naunheim & Fabian Bader
Thomas Naunheim & Fabian Bader
Thomas Naunheim & Fabian Bader

Live Demo
Microsoft Sentinel


Permissions Management
DevOps Security
CSPM
Azure Arc
Azure Arc
SQL
SQL
DNS
DNS
Syslog / CEF
Microsoft Defender XDR
On-Premises
Defender for Cloud
Multi-cloud
Microsoft Sentinel
Thomas Naunheim & Fabian Bader
Thomas Naunheim & Fabian Bader
Thomas Naunheim & Fabian Bader

One more thing…

Demo

Unified Security Operations Platform with Microsoft Sentinel and Defender XDR

Vielen Dank für‘s Zuhören!