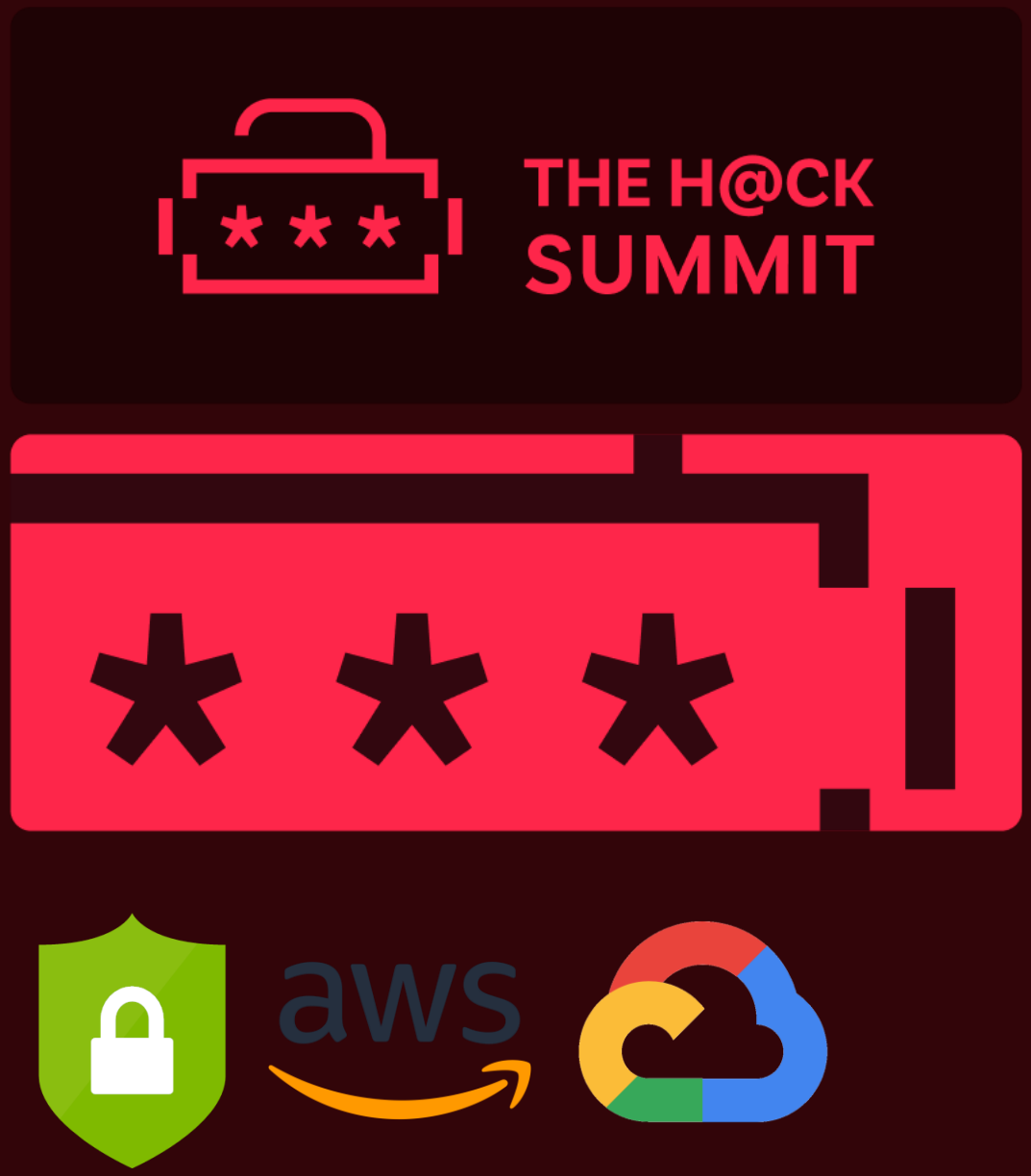
Ochrona środowisk multicloud narzędziami Microsoft

Konrad Sagała

Cloud Security Architect, Alior Bank



TROCHĘ O SOBIE

- Cloud Security Architect – Azure/M365
- Microsoft Certified Trainer since 2007
- Microsoft MVP since 2007 – M365
- Twitter - @sagus
- LinkedIn - @konradsagala
- Github - https://github.com/ksagala
- Blog – https://pepugmaster.blogspot.com
- Hobby – Podróże, Śpiew, Taniec

Agenda

- Multi-cloud security
- Native support for AWS and GCP
- CSPM capabilities for AWS and GCP
- CWP(P) capabilities for AWS and GCP

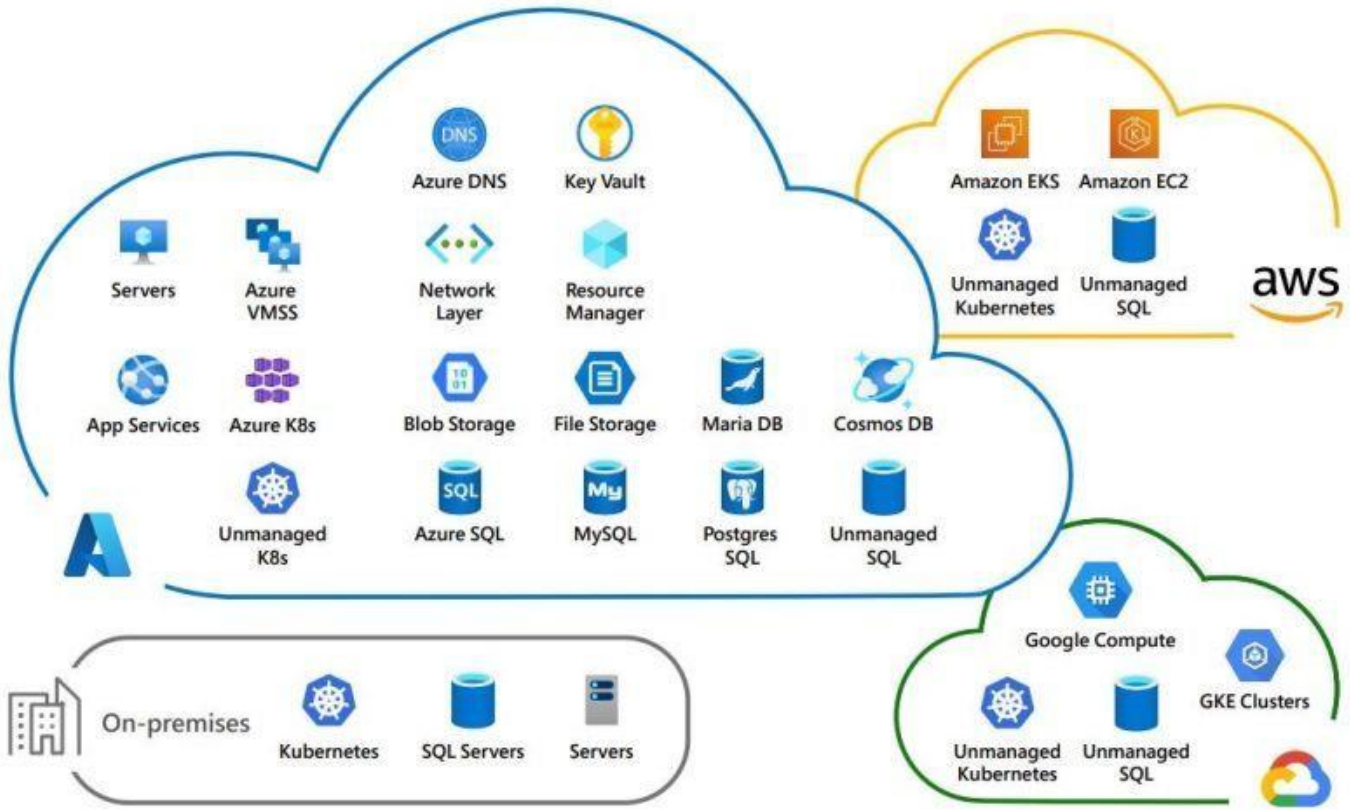
Multicloud security challenges

- Data management and compliance
- Identity and access management
- Threat detection and management
- Complexity reduction in managing multi-cloud environment


Microsoft Defender for Cloud
Unify your DevOps Security Management
Strengthen and manage your cloud security posture
Protect your cloud workloads
2
3
DevOps
CWP
CIEM
EASM
aws

Microsoft Defender for Cloud

Secure your hybrid-cloud and multicloud workloads



Microsoft Defender for Cloud

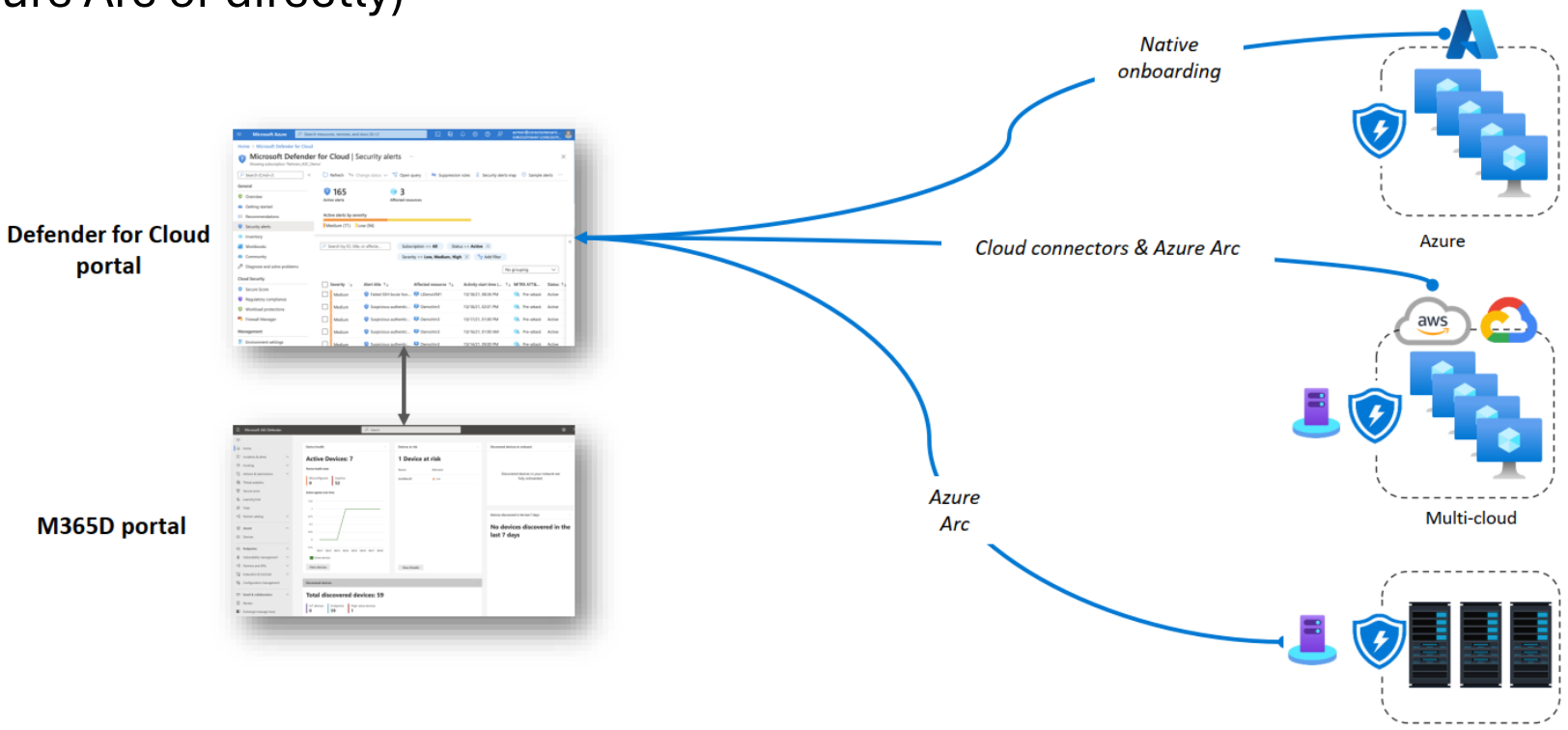
Secure your critical workloads running in AWS, Azure and Google Cloud

- Easy onboarding of AWS accounts and native support for Azure
- Assess and implement best practices for compliance and security in the cloud
- Get a bird's-eye view of your security posture and vulnerabilities across clouds with secure score
- Protect Amazon EKS and GKE clusters
- Protect GCP VM instances and AWS EC2 workloads

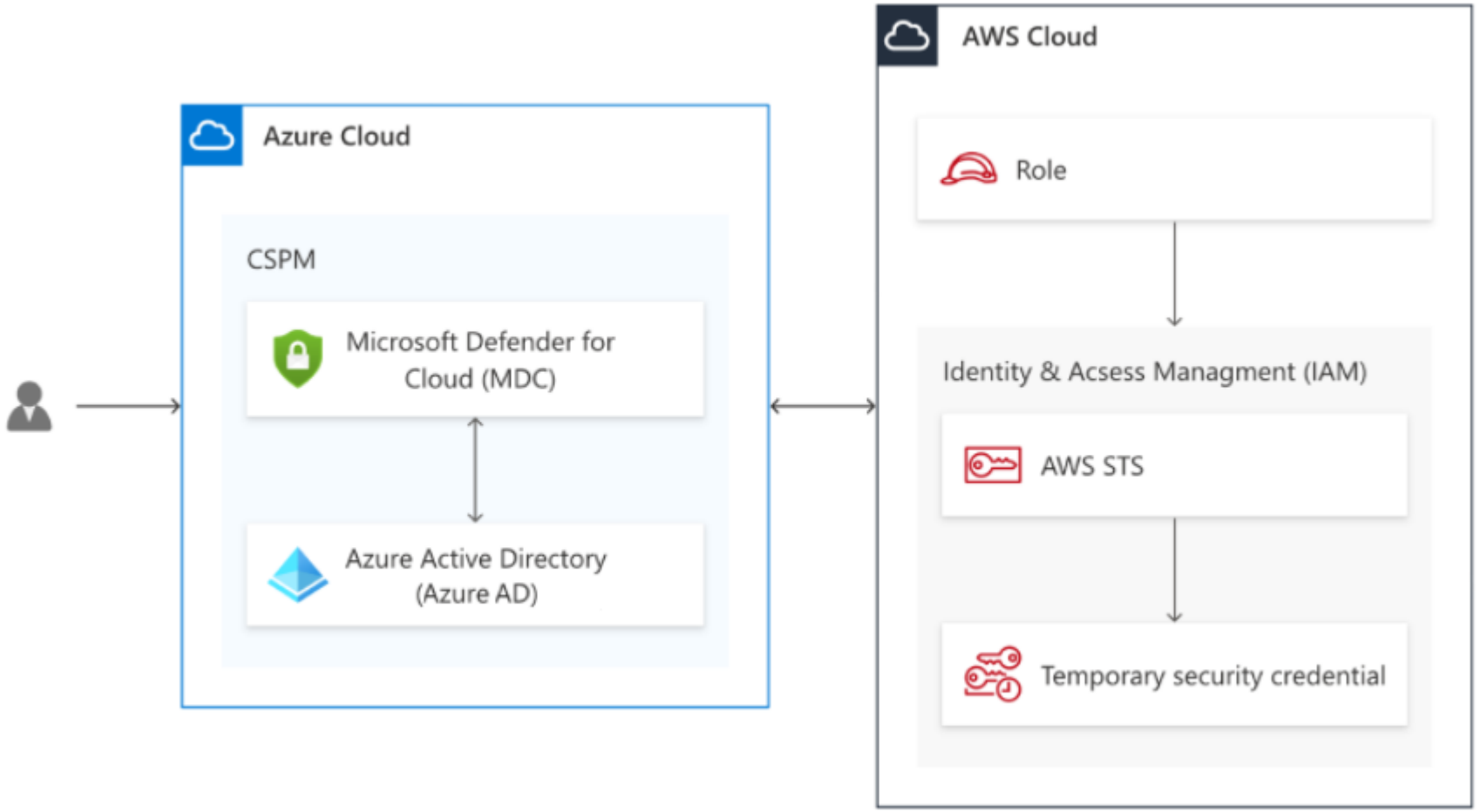
Defender for Servers in multicloud

All servers are secured the same way:

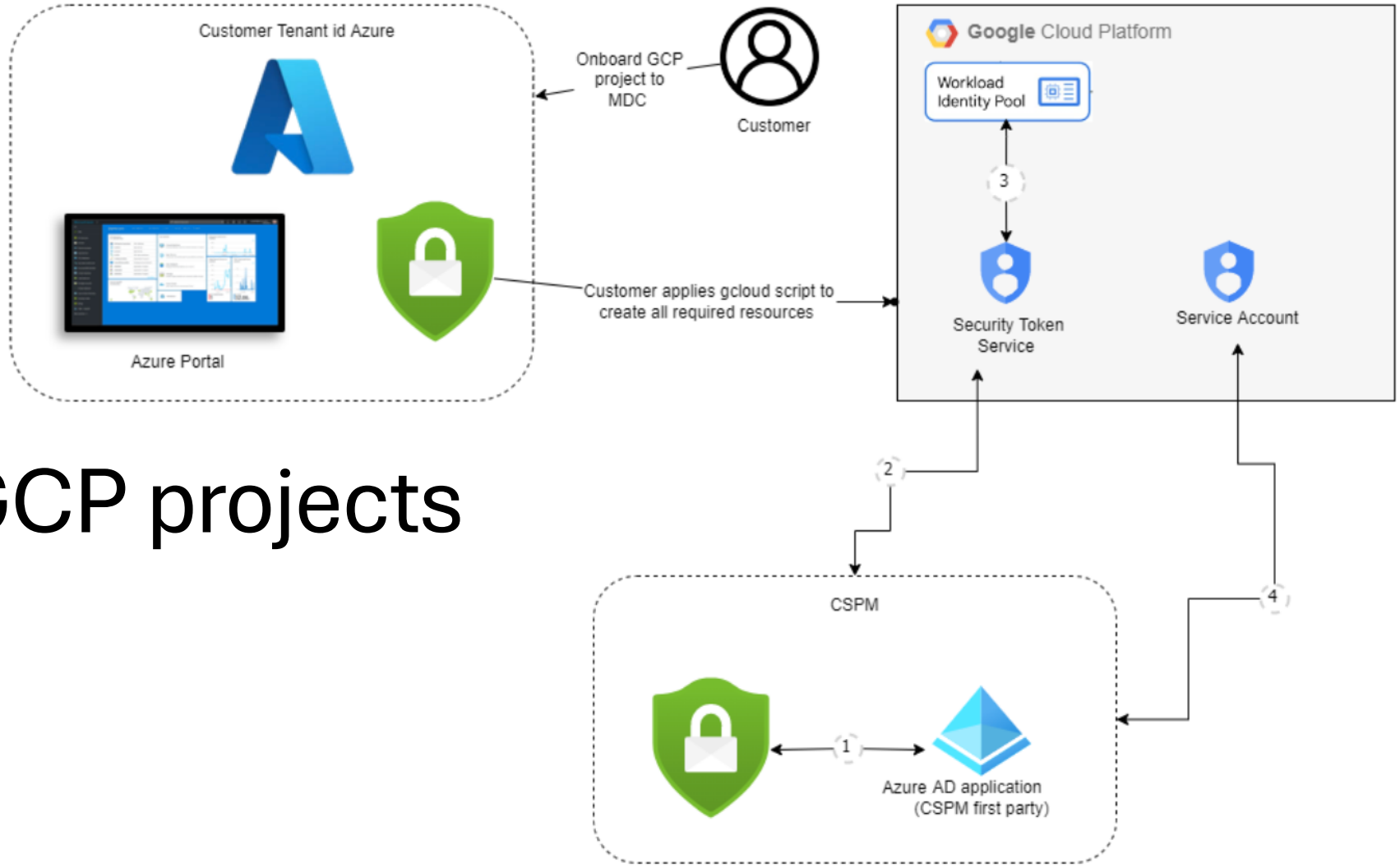
- Windows and Linux EC2 instances on AWS with Azure Arc
- Google VM instances with Azure Arc
- On-prem machines (with Azure Arc or directly)



Connecting AWS accounts



Connecting GCP projects



CSPM – security recommendations

- API based
- More than 160 out of the box recommendations for AWS
- More than 130 out of the box recommendations for GCP
- More than 30 resource types
- Regulatory compliance standards – CIS, PCI DSS, Best Practices

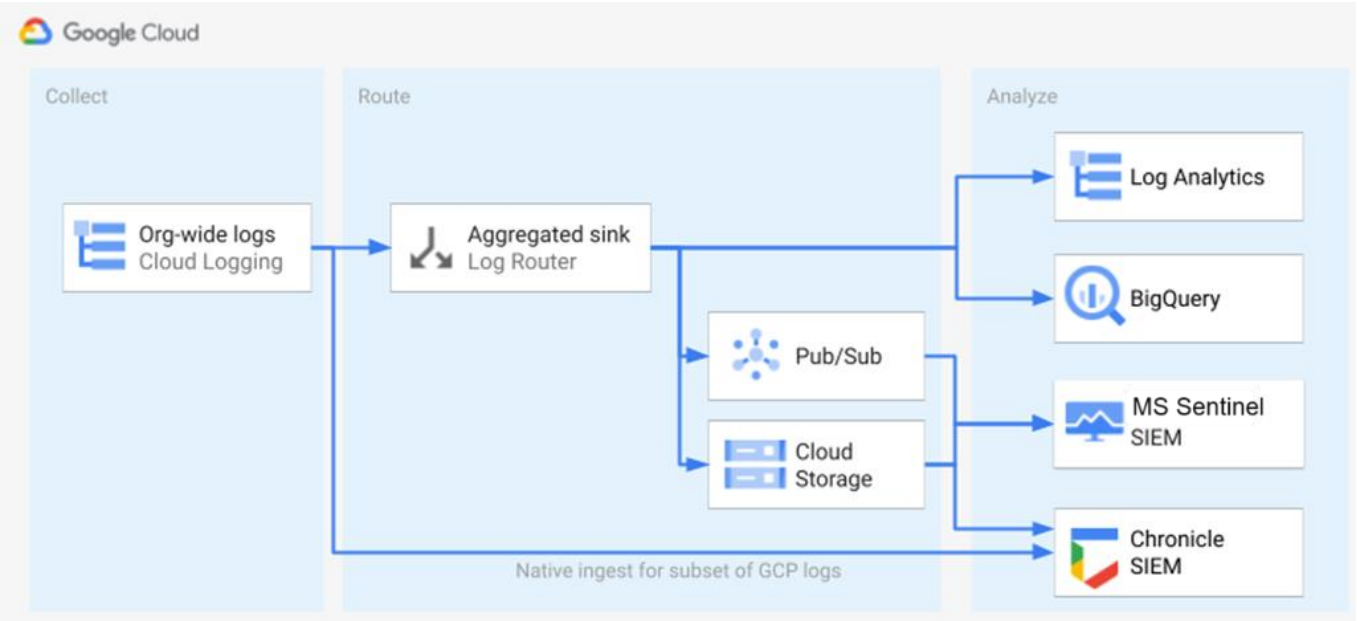
Compliance management

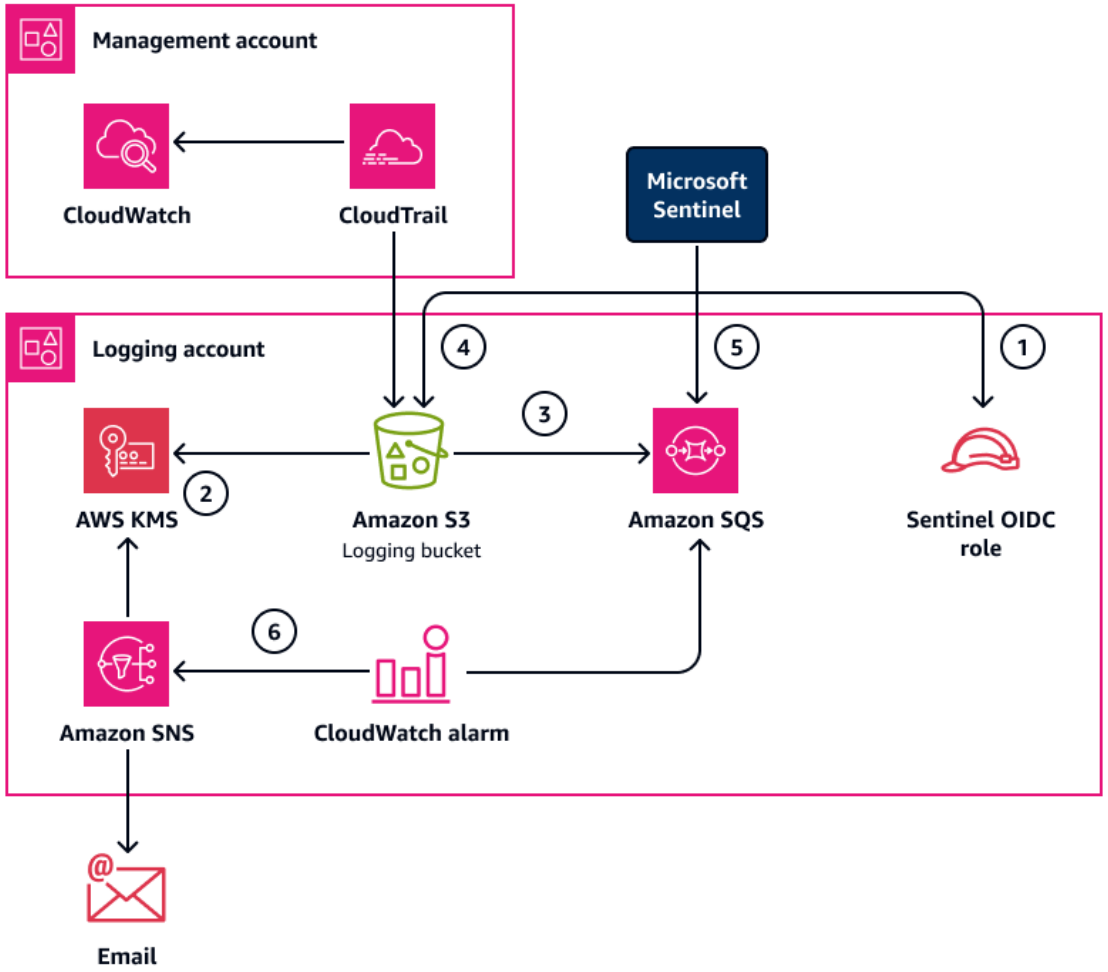
- Show compliance status, based on continuous assessments of Azure, AWS and GCP resources
- Monitor AWS and GCP resources
- Microsoft Cloud Security Benchmark monitoring enabled by default
- Mapped to the MITRE ATT&CK framework
- Support for common regulatory and compliance standards
- Reports of compliance status
- Custom recommendations possible

Microsoft Sentinel in multicloud

Connectors for AWS and GCP:

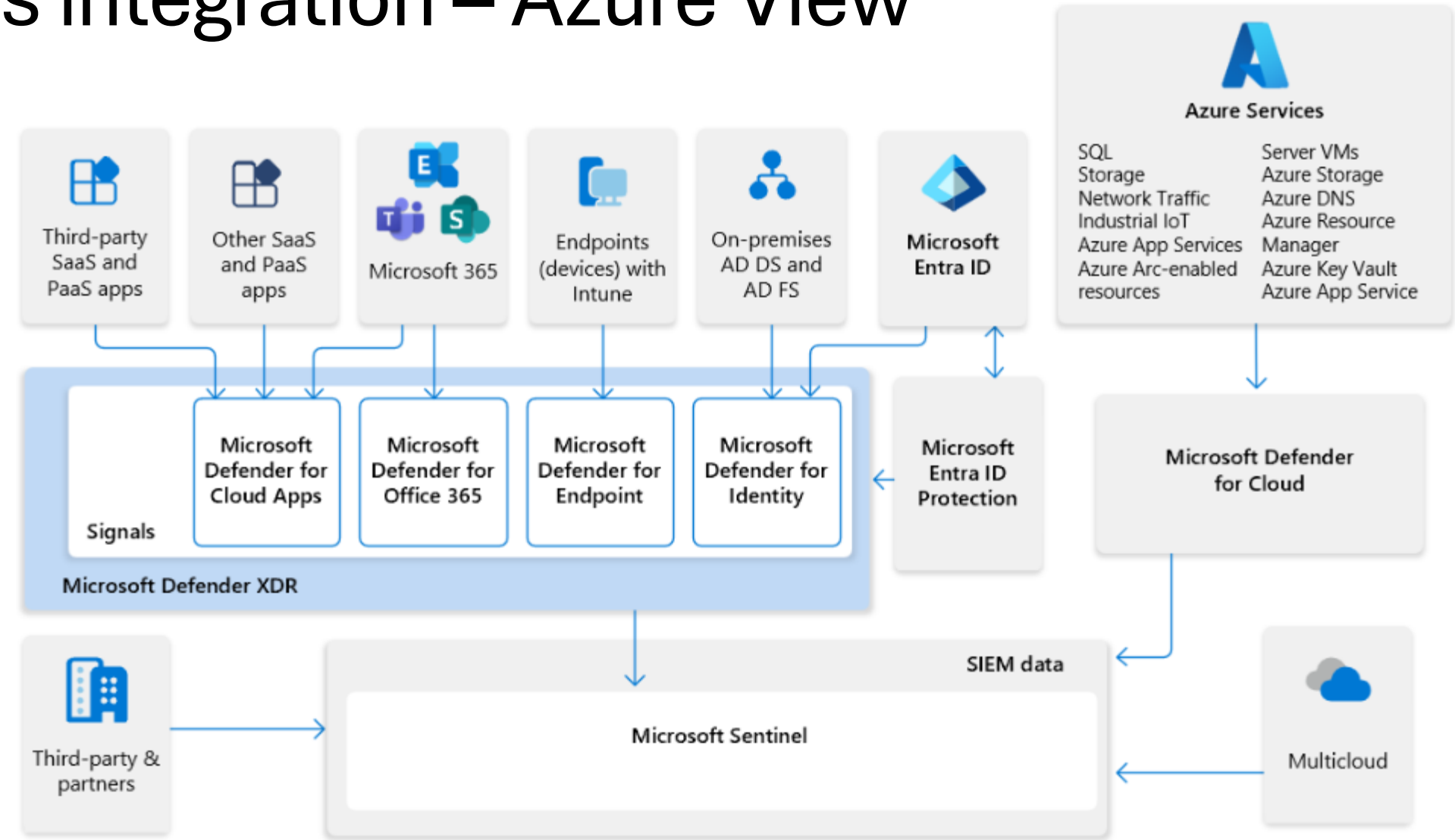
- Terraform (or Cloud Formation) code to configure integration with specific cloud





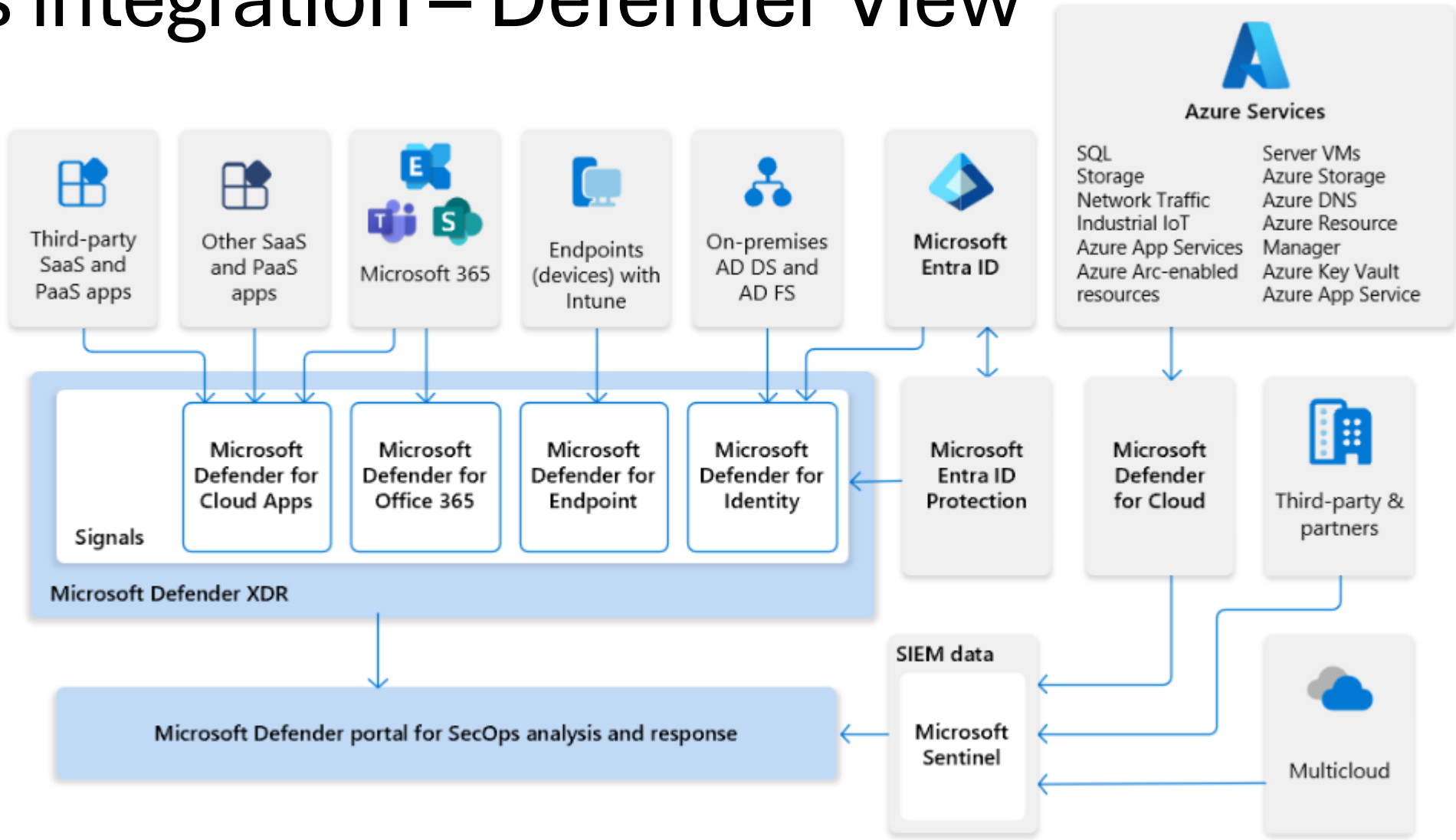
https://learn.microsoft.com/en-us/azure/sentinel/connect-aws
https://learn.microsoft.com/en-us/azure/sentinel/connect-google-cloud-platform

Tools integration – Azure View



https://learn.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration?tabs=azure-portal

Tools integration – Defender View



https://learn.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration?tabs=defender-portal

Dziękuję za oglądanie!

Pamiętaj, aby zostawić swoje pytania i oceń prezentację w poniższej sekcji.

https://thehacksummit.com/user.html#!/lecture/THS24-90f0/rate

THE H@CK SUMMIT

ACADEMIC PARTNERS