Offensive Azure Security

Sergey Chubarov

Sergey Chubarov

Ethical Hacker | Instructor

Conference speaker

https://www.linkedin.com/in/schubarov

- Microsoft MVP: Microsoft Azure
- OSCP, OSEP
- MCT, MCT Regional Lead, Microsoft 365 Certified Expert, Azure Certified Expert
- EC Council: CEH Master, ECSA Master, CEI
- CREST: CPSA, CRT

Hybrid Active Directory

Azure Virtual Machines

Web App with Azure SQL

Azure AD Connect

Azure Virtual Machines

Web App with Azure SQL

AD DS Connector account required permissions

Permission	Used for
Replicate Directory Changes Replicate Directory Changes All	Password hash sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid
Reset password	Preparation for enabling password writeback

Azure AD Connect

Azure Virtual Machines

Web App with Azure SQL

Microsoft
Active Directory

Azure AD
Connect

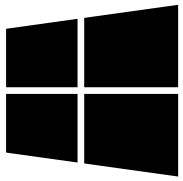
Azure Virtual Machines

Web App with Azure SQL

Microsoft
Active Directory

Azure AD
Connect

Slave-node



Master-node

Web App with Azure SQL

Microsoft
Active Directory

Azure AD
Connect

Slave-node

Master-node

Web App with Azure SQL

Microsoft Active Directory

Azure AD Connect

Slave-node

Master-node

App GW with WAF

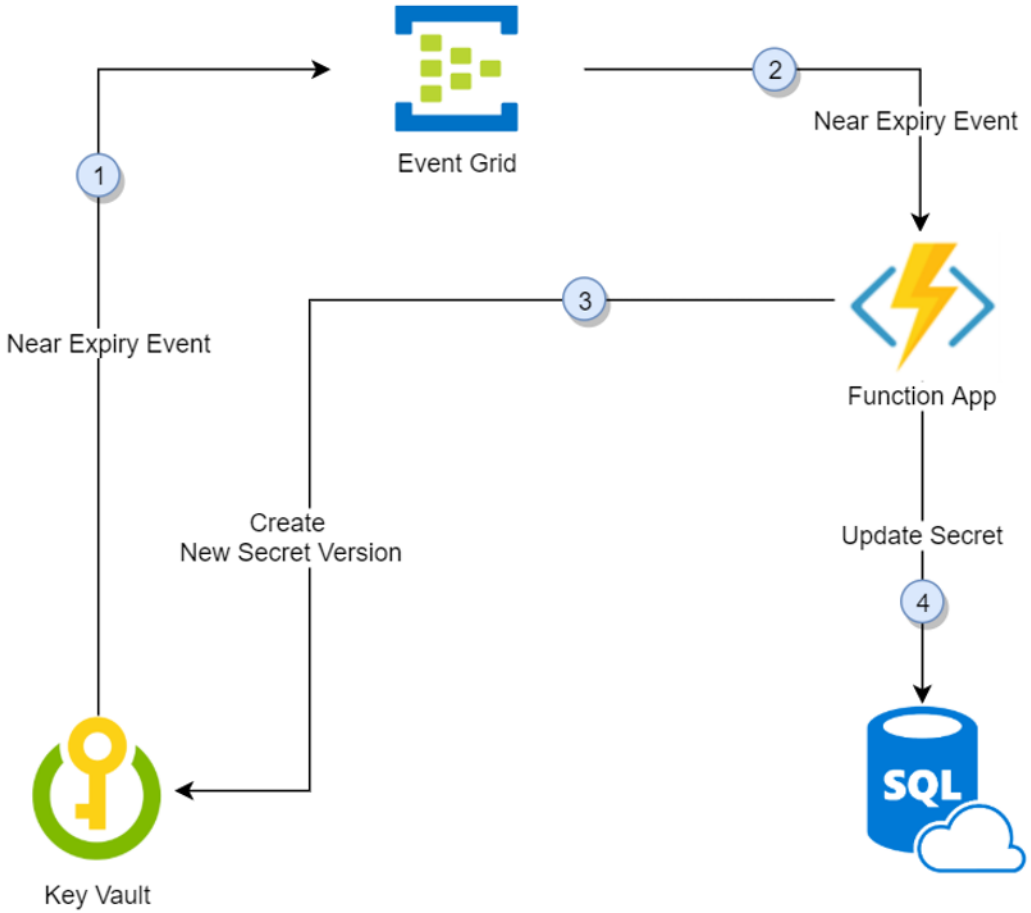
Web App

Credentials

Credentials rotation

Azure SQL Backend

AKV Secrets rotation



Microsoft Active Directory

Azure AD Connect

Slave-node

Master-node

App GW with WAF

Web App

Credentials

Credentials rotation

Azure SQL Backend

Microsoft Active Directory

Azure AD Connect

Slave-node

Master-node

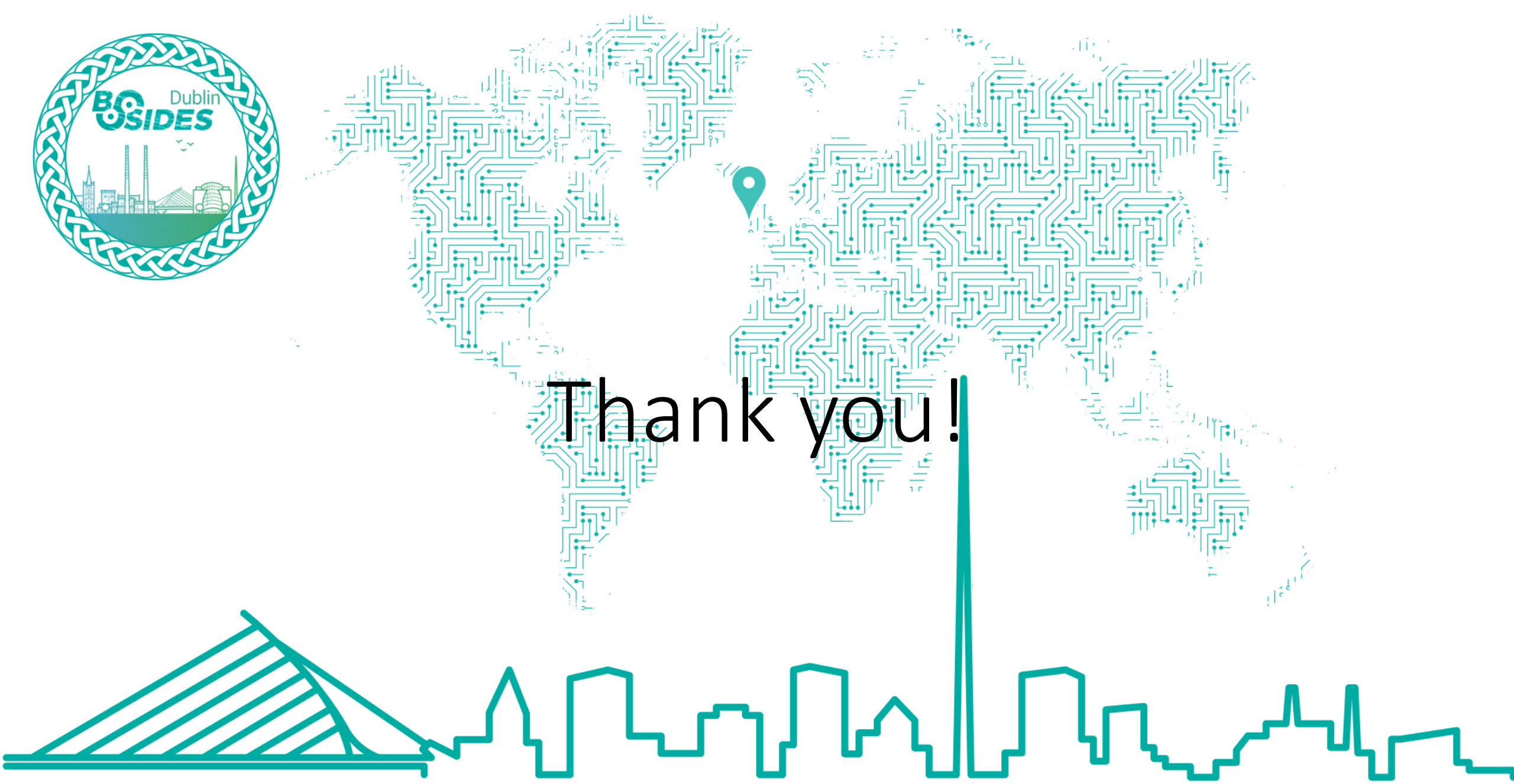
App GW with WAF

Web App

Credentials

Credentials rotation

Azure SQL Backend


Thank you!