MC2MC

Offensive Azure Security

Sergey Chubarov

Sergey Chubarov

Ethical Hacker | Instructor

Conference speaker

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

- Microsoft MVP: Microsoft Azure
- OSCP
- 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

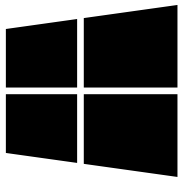
Azure Virtual Machines

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

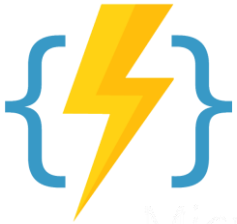
Slave-node

Master-node

App GW with WAF

Web App

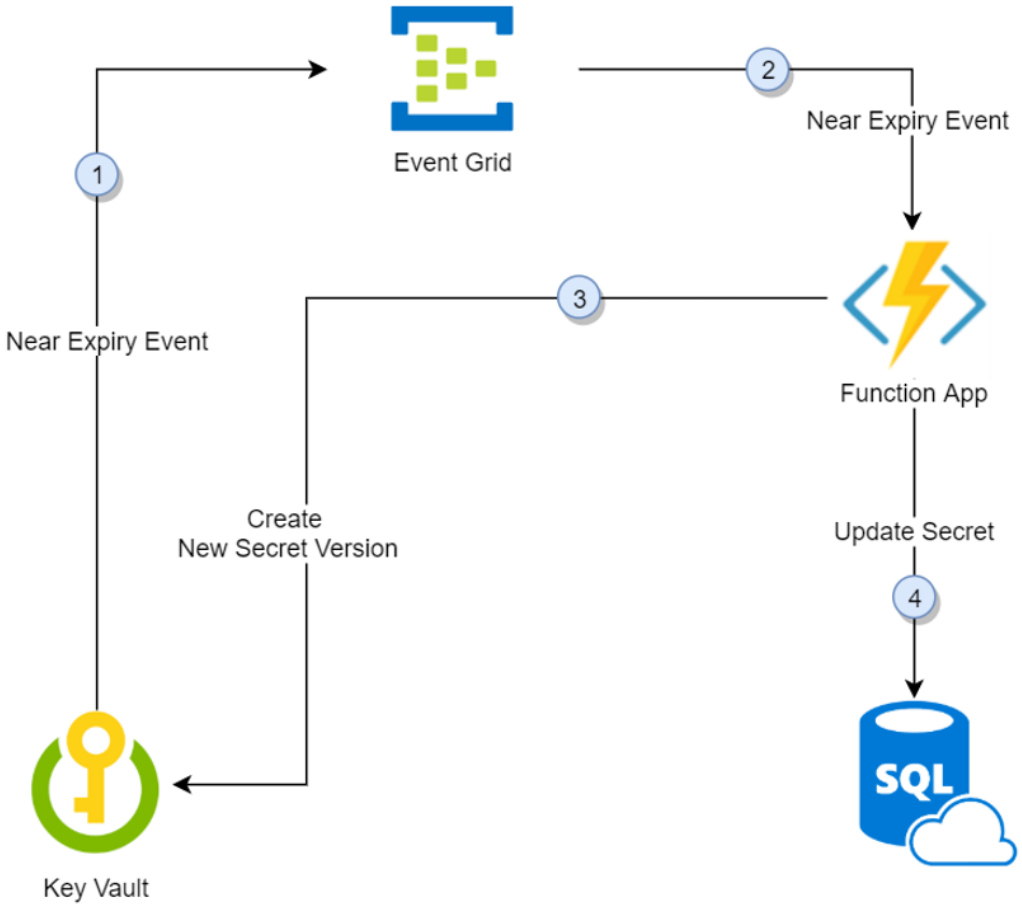
Credentials



Credentials rotation

Azure SQL Backend

AKV Secrets rotation



Microsoft Active Directory

Azure AD Connect

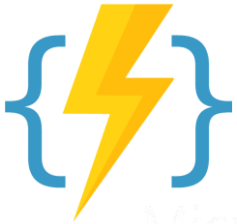
Slave-node

Master-node

App GW with WAF

Web App

Credentials



Credentials rotation

Azure SQL Backend

Microsoft Active Directory

Azure AD Connect

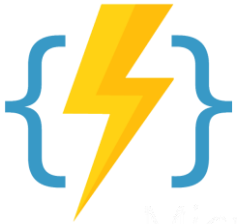
Slave-node

Master-node

App GW with WAF

Web App

Credentials



Credentials rotation

Azure SQL Backend

Mitigations

The problem	Solution
Compromising AD forest account	AD Connect is Tier 0 Principle of least privileges
Stealing cached creds	Use PAW & PoLP
Running commands against Azure VMs	Principle of least privileges
Shell upload, function modification	Disable FTP for App service and Functions
Azure SQL connectivity	Disable "Allow Azure services and resources to access this server"
Web app attacks	Web App Firewall

Join my other sessions

Offensive Azure Security
https://scottishsummit.com/ 27 Feb 2021

Hackers won't Pass - Microsoft Defender in action
https://modern-workplace.pro/ 18 Jan - 20 Jan 2021
http://microsoft365compliance.de/compliance-and-security-community-conference-2021 08 Feb 2021

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