

Defender for SQL as part of your Defense in-depth strategy



What

... is Defense in Depth

... is the role of Defender for SQL

... is required to run Defender for SQL

... is a typical implementation

... evidence is there

... questions do you have

... about me

Defense in Depth



<https://rob-litjens.nl>

Microsoft Defender Advanced Threat Protection



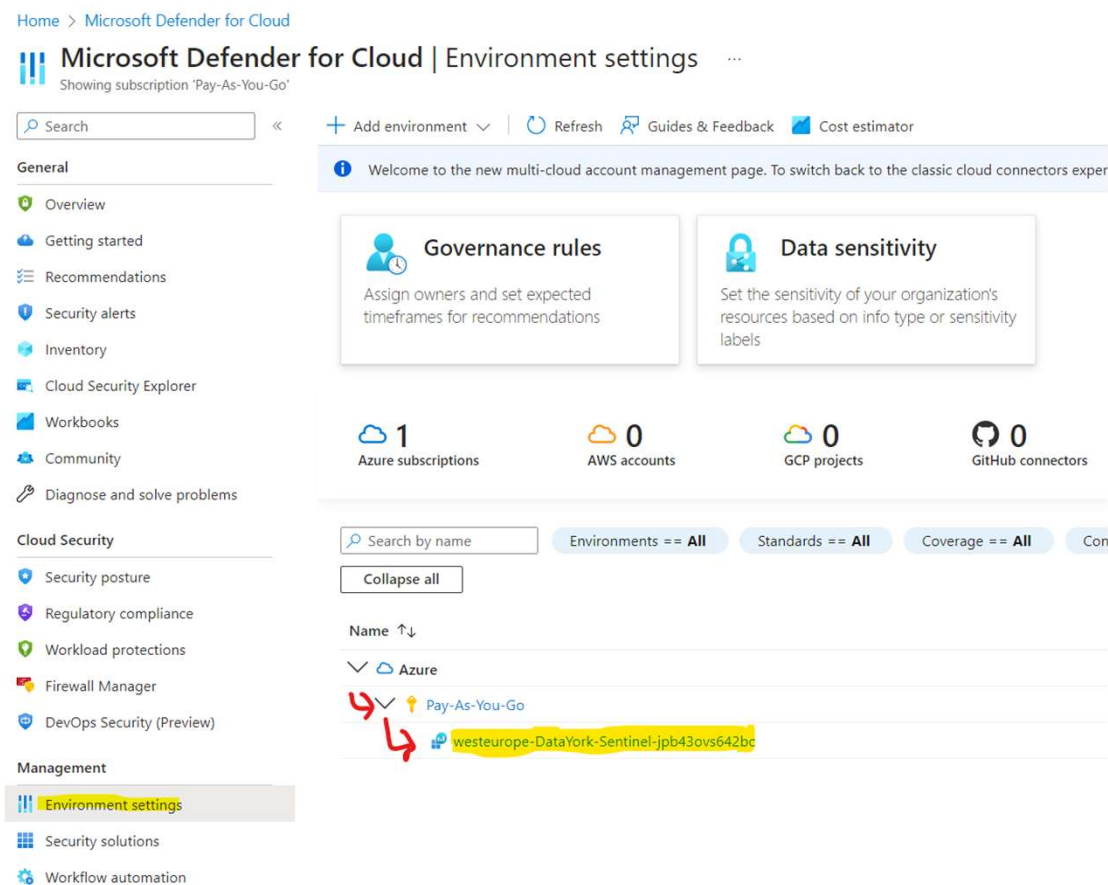
Requirements to use Defender for SQL

- Azure Tenant
 - Some Bicep knowledge
- SQL Servers
 - On premise
 - Endpoint Protection
 - Cloud
- Not supported:
 - SQL2012 and below
 - Reporting Services, Analysis Services

<https://rob-litjens.nl>

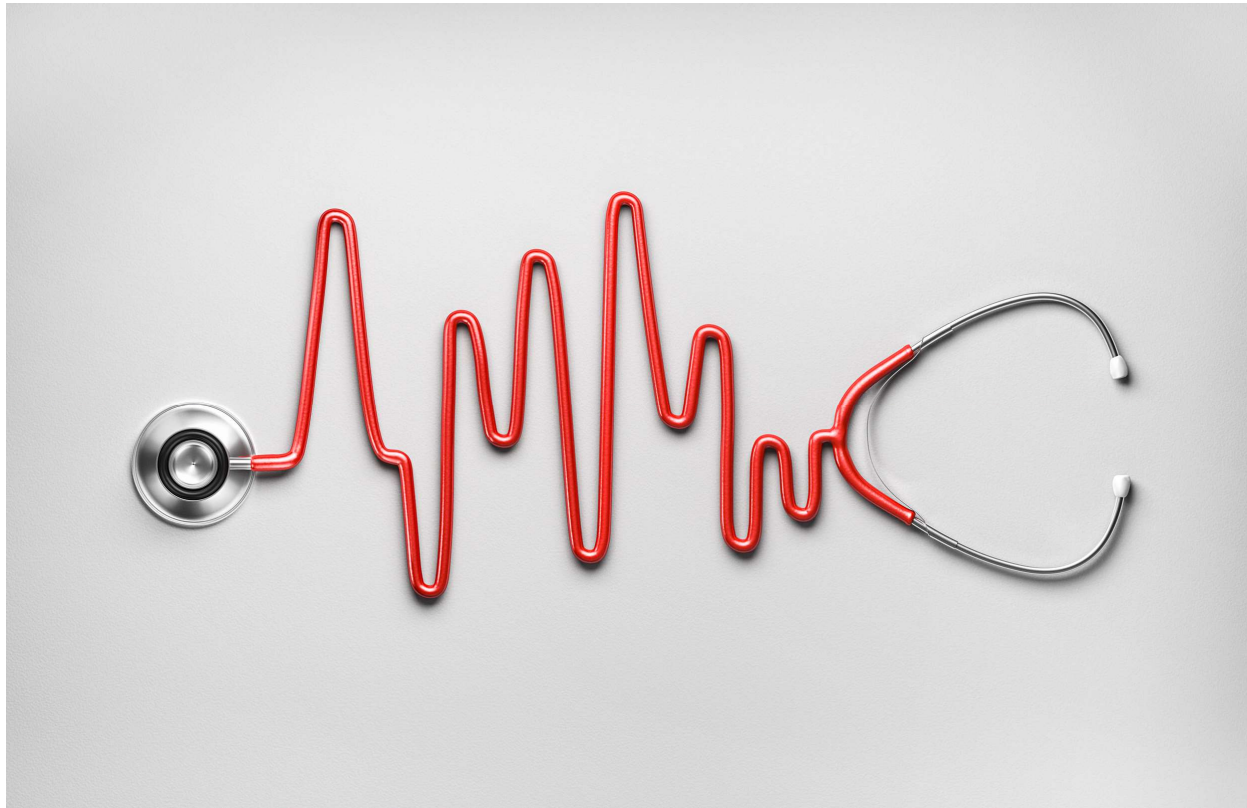
The implementation

- Connect to your tenant
- Implement:
 - A subscription
 - Resource Group
 - A Log Analytics Workspace
- Configure Workspace
- Configure Client



<https://rob-litjens.nl>

Demo Implementation



<https://rob-litjens.nl>

Done so far

Setup Azure

Setup Log Analytics Workspace

Setup Client

But...

We need proof it is working

<https://rob-litjens.nl>

Evidence

HIGH SEVERITY

Microsoft Defender for Cloud has detected suspicious activity in your resource



Suspected brute-force attack attempt

Brute-force attack is a common attack technique for finding valid credentials to the database. By submitting many users/passwords combinations, an attacker can guess a correct one. Once obtained, an attacker can have full access to the database. While this specific alert doesn't indicate a successful brute-force, it is advised to take safety measures to protect your resource against this attack. To investigate this suspected brute-force attempt, review its origin (based on the application name and IP/Location), and try to find out whether it's recognized to you, or suspicious. If you believe this to be an attack on your database, use firewall rules to limit the access to your resource, and make sure you use strong passwords and not well known user names. Also, consider using only AAD authentication to further enhance your security posture.

June 23, 2023 18:37 UTC



Affected On Prem Machine:
TOBO-SQL2019



Detected by
Microsoft

<https://rob-litjens.nl>

Questions



**Defender for SQL as
part of your Deense
in Depth strategy**

<https://rob-litjens.nl>

About me

Rob Litjens

SQL Server Automation Engineer at Financial Institute

Working with SQL since ages (version 6.0), automating since then. Interested in Data Protection and Security, audits and auditing.

Personal interests: Mountainbiking, traveling and work (not always on 😊)

@Socials

LinkedIn: <https://www.linkedin.com/in/litjensr/>

Bsky: [roblitjens.bsky.social](https://bsky.social/roblitjens)

Mastodon: <https://dataplatfom.social/@RobLitjens>

Blog: <https://www.rob-litjens.nl>

