EVENT SPONSORS, THANKS!!!

GOLD

span

SuperSport

SILVER

TRIA

comminus
FOR EVERY STEP OF THE WAY, THERE'S DATA

BRONZE

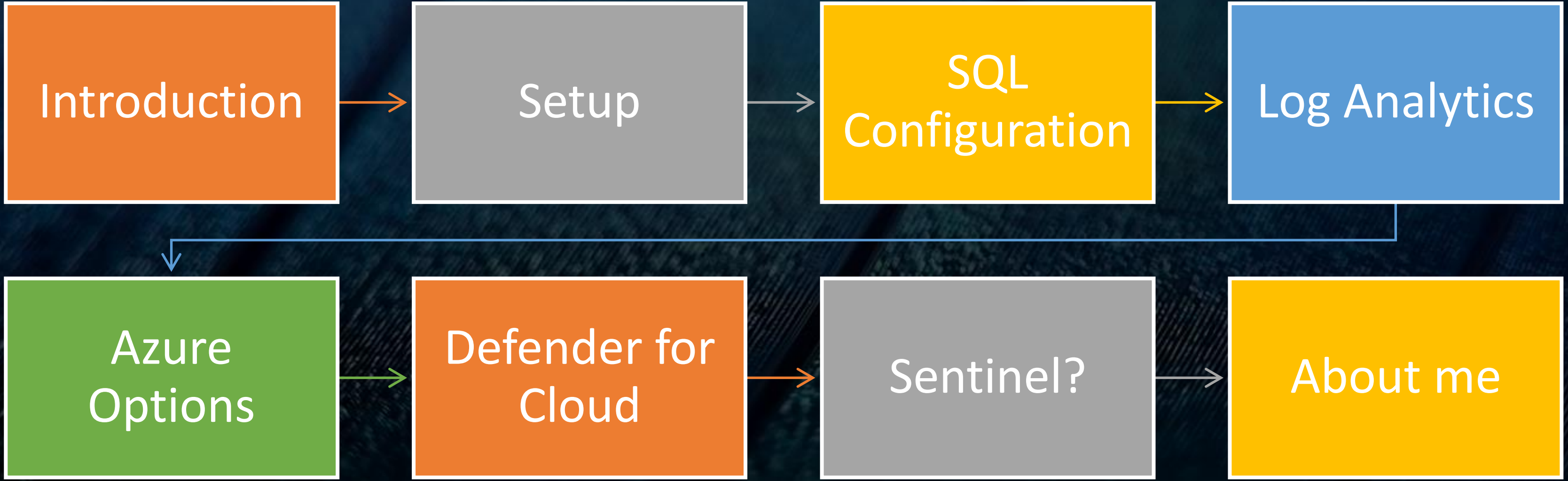
DATA SENSE
WHERE IT SPEAKS BUSINESS

infobip

WHAT ELSE CAN YOU GET FROM DEFENDER FOR SQL AND SQL AUDITS?

Ways to have all your security requirements in one place

What are we going to do today



Introduction

Setup

SQL Configuration

Log Analytics

Azure Options

Defender for Cloud

Sentinel?

About me

#intro - 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. Not a SOC Operator (☺)

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

@Socials

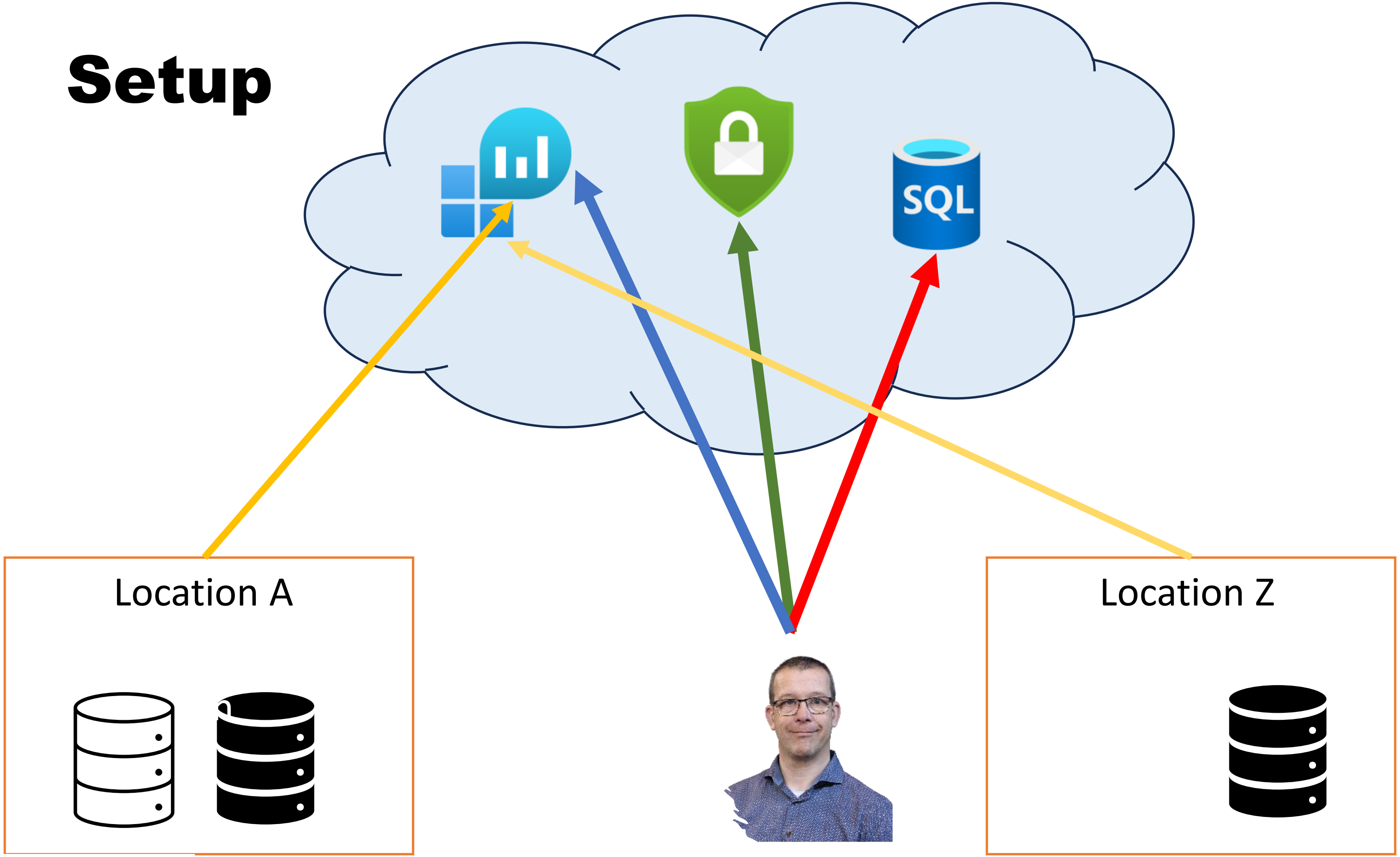
LinkedIn: https://www.linkedin.com/in/litjensr/

Bsky: roblitjens.bsky.social

Mastodon: https://dataplatform.social/@RobLitjens

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

Setup



SQL Server Configuration Changes

Creating Extended Events

Extended Events cannot write directly to the eventviewer.

Create Extended Events:
- Microsoft Learn

AZURE OPTIONS

Log Analytics

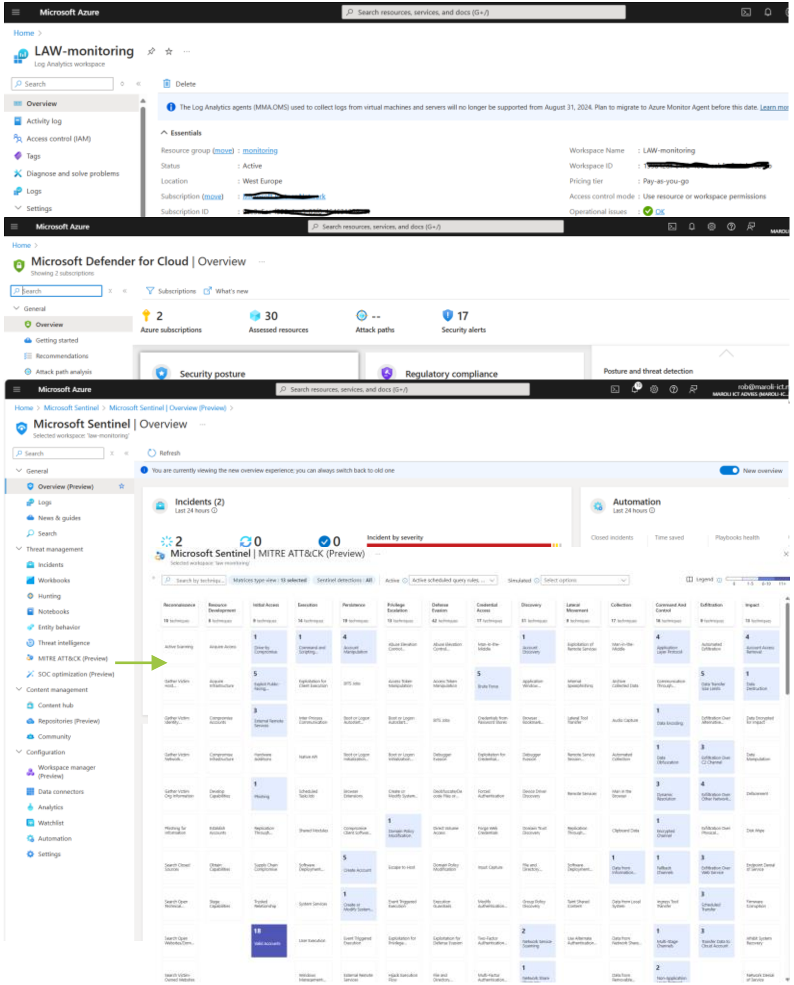
- Storing Defender Data
- Store Event Viewers
- Integration
- Alerts

Defender for Cloud

- Incidents
- Hunting

Sentinel

- Aggregation
- Thread Hunting
- SOC



Microsoft Azure | Search resources, services, and docs (G+/)

Home >

LAW-monitoring
Log Analytics workspace

Delete

The Log Analytics agents (MMA.OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. Learn mor

Essentials

Resource group (move) : monitoring
Status : Active
Location : West Europe
Subscription (move) : [redacted]
Subscription ID : [redacted]
Workspace Name : LAW-monitoring
Workspace ID : [redacted]
Pricing tier : Pay-as-you-go
Access control mode : Use resource or workspace permissions
Operational issues : OK

Microsoft Azure | Search resources, services, and docs (G+/)

Home >

Microsoft Defender for Cloud | Overview
Showing 2 subscriptions

2 Azure subscriptions
30 Assessed resources
-- Attack paths
17 Security alerts

Security posture
Regulatory compliance
Posture and threat detection

Microsoft Azure | Search resources, services, and docs (G+/) | rob@maroli-ict.n | MAROLI ICT ADVIES (MAROLI-IC...

Home > Microsoft Sentinel > Microsoft Sentinel | Overview (Preview) >

Microsoft Sentinel | Overview
Selected workspace: 'law-monitoring'

Refresh

You are currently viewing the new overview experience; you can always switch back to old one

New overview

Incidents (2)
Last 24 hours

2 0 0

Incident by severity

Automation
Last 24 hours

Closed incidents | Time saved | Playbooks health

Microsoft Sentinel | MITRE ATT&CK (Preview)
Selected workspace: 'law-monitoring'

Search by techniqu... | Matrices type view : 13 selected | Sentinel detections : All | Active | Active scheduled query rules, ... | Simulated | Select options | Legend

Have you seen a dragon?

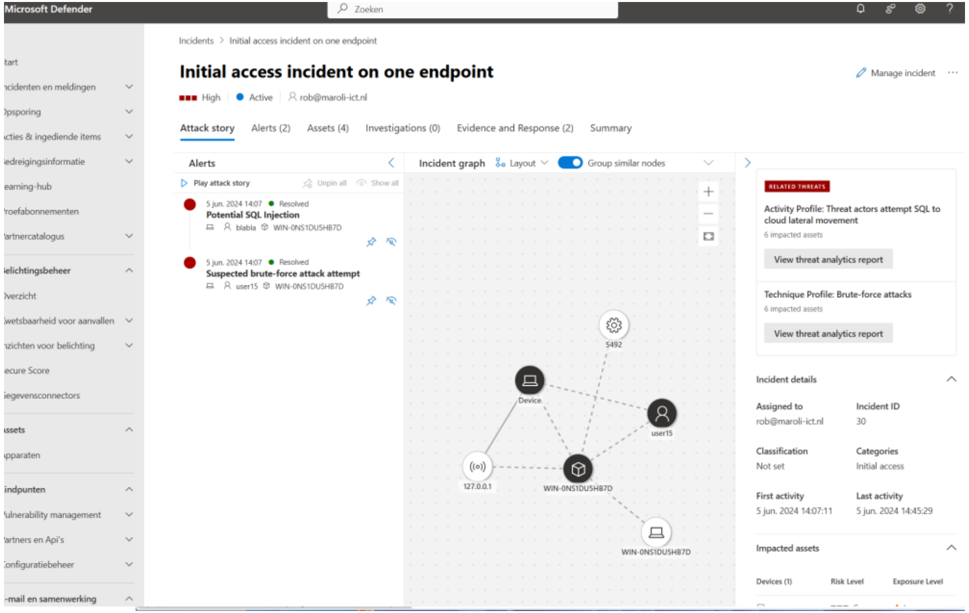
Help him!

What happens when there is an Incident?

- You (can) get a mail or Teams Notification
- When you click on the link you will go to Defender for Cloud or Sentinel
- You can click through
- Through Defender for cloud
- Or Sentinel

- To…

- Security.microsoft.com?



Initial access incident on one endpoint

High | Active | rob@maroli-ict.nl

5 jun. 2024 14:07 ● Resolved
Potential SQL Injection
blabla WIN-0NS1DU5HB7D

5 jun. 2024 14:07 ● Resolved
Suspected brute-force attack attempt
user15 WIN-0NS1DU5HB7D

Activity Profile: Threat actors attempt SQL to cloud lateral movement
6 impacted assets

Technique Profile: Brute-force attacks
6 impacted assets

Incident details

Assigned to: rob@maroli-ict.nl
Incident ID: 30
Classification: Not set
Categories: Initial access
First activity: 5 jun. 2024 14:07:11
Last activity: 5 jun. 2024 14:45:29

Impacted assets

Devices (1)	Risk Level	Exposure Level

SSUGCRO

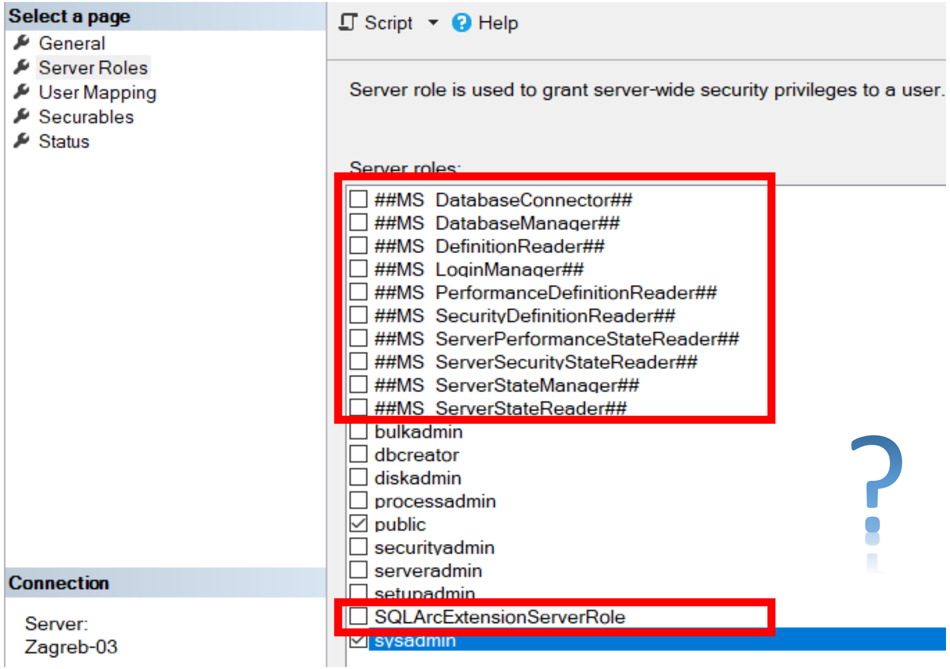
https://rob-litjens.nl

Demo

- Go through the Azure Portal
- Injection
- Shell Obfuscation
- Within the Portal
- How to combine stuff

You did an upgrade? Then your old commands still work

Fun facts



Server role is used to grant server-wide security privileges to a user.

Server roles:

- □ ##MS DatabaseConnector##
- □ ##MS DatabaseManager##
- □ ##MS DefinitionReader##
- □ ##MS LoginManager##
- □ ##MS PerformanceDefinitionReader##
- □ ##MS SecurityDefinitionReader##
- □ ##MS ServerPerformanceStateReader##
- □ ##MS ServerSecurityStateReader##
- □ ##MS ServerStateManager##
- □ ##MS ServerStateReader##
- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- □ SQLArcExtensionServerRole
- ☑ sysadmin

Connection

Server:
Zagreb-03

Questions

Defender for SQL as part of your Deense in Depth strategy

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

Mastodon: https://dataplatform.social/@RobLitjens

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

EVENT SPONSORS, THANKS!!!

GOLD

span

SuperSport

SILVER

TRIA

comminus
FOR EVERY STEP OF THE WAY, THERE'S DATA

BRONZE

DATA SENSE
WHERE IT SPEAKS BUSINESS

infobip

Session evaluation, thanks!

https://eval.datasaturdays.com/event/16636280