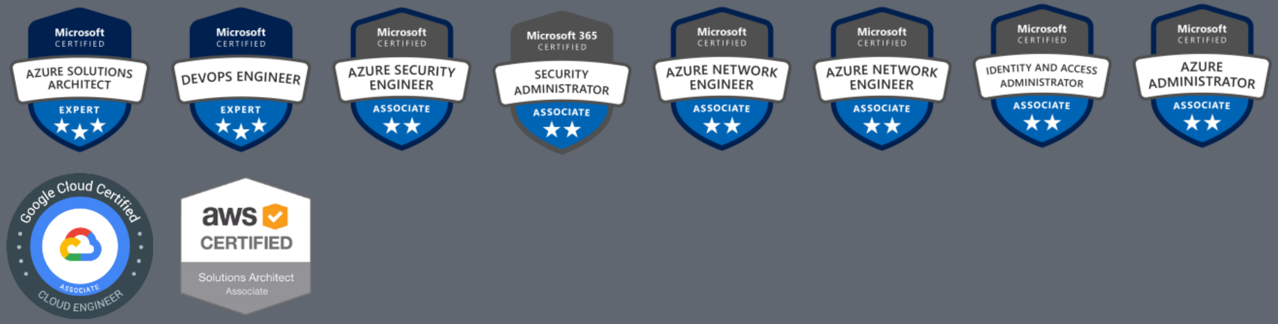
About me

Hannes Lagler-Gruener

Lead Cloud Architect

- https://bit.ly/3gRQRqY
- https://cloudblogger.at
- https://www.linkedin.com/in/hannesl1
- @HannesLagler
- https://github.com/orgs/Lagler-Gruener


Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT
Microsoft CERTIFIED DEVOPS ENGINEER EXPERT
Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE
Microsoft 365 CERTIFIED SECURITY ADMINISTRATOR ASSOCIATE
Microsoft CERTIFIED AZURE NETWORK ENGINEER ASSOCIATE
Microsoft CERTIFIED AZURE NETWORK ENGINEER ASSOCIATE
Microsoft CERTIFIED IDENTITY AND ACCESS ADMINISTRATOR ASSOCIATE
Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE
Google Cloud Certified ASSOCIATE CLOUD ENGINEER
aws CERTIFIED Solutions Architect Associate

Cloudblogger.at

New session about

https://bit.ly/3gRQRqY
@HannesLagler

Sentinel Triggers and how to use

Video type:	Nuget
Video category:	300

Session Agenda

- SOAR in Microsoft Sentinel
- Trigger types and when to use it
- Live demo

SOAR in Microsoft Sentinel

SOAR (Security Orchestration, Automation and Response) refers to the combination of three different technologies:

- security orchestration and automation
- security incident response platforms (SIRP)
- threat intelligence platforms (TIP)

We’ll cover today security orchestration and automation

Trigger types and when to use it

There are three trigger types available:

- Incident based trigger
- Entity based trigger
- Alert based trigger (deprecated effective March 2026)

Incident based trigger

This trigger type is:

- Recommended for most incident automation scenarios.
- Execute over Automation rules
- Automation rules covers:
    - When incident is created
    - When incident is updated
    - When alert is created

Entity based trigger

This trigger type is:

- Used for playbooks that need to be run manually on specific entities
- Cannot be called by **automation rules!**
- Trigger type cover the following entity types:
  - IP
  - Host
  - Account
  - URL
  - FileHash

Live Demo!

- Overview about trigger types
- Incident based trigger and automation rules Demo
- Manuell execute entity based triggers
- Playbook structure