About me

Hannes Lagler-Gruener

Cloud Innovations Expert

- https://cloudblogger.at
- https://www.linkedin.com/in/hannesl1
- @HannesLagler

https://cloudblogger.at

Welcome to a new session about

https://cloudblogger.at

Work with Azure Sentinel

Video type: Nugget

Video category: Level-300

Session Agenda

https://cloudblogger.at

- Analytics Rule
- Hunting Rule
- Playbooks
- Community

Analytics Rule

https://cloudblogger.at

- Based on Log Analytics and connected data sources
- Different types available
  - Microsoft security
  - Fusion
  - Machine learning behavioral analytics
  - Scheduled
- Create an alert, incident the ability to execute the playbook

Hunting Rule

https://cloudblogger.at

- Based on Log Analytics and connected data sources
- Manual, proaktive Investigation
- Hunting consists of several capabilities:
  - Queries
  - Bookmarks
  - Livestream

Playbooks

https://cloudblogger.at

- Based on Azure Logic App automation
- A separate trigger for sentinel available
- Automatic task creation
  - Disable account
  - Block port
  - …
- A huge number of connectors available
- Huge community

Community

https://cloudblogger.at

- Azure sentinel has an awesome community
- You can find different sources on GitHub

Switch to the Live Demo!

https://cloudblogger.at

- Create an hunting rule
- Create an livestream rule
- Create custom analytics rule
- Create an incident by analytics rule
- Add an playbook to analytics rule