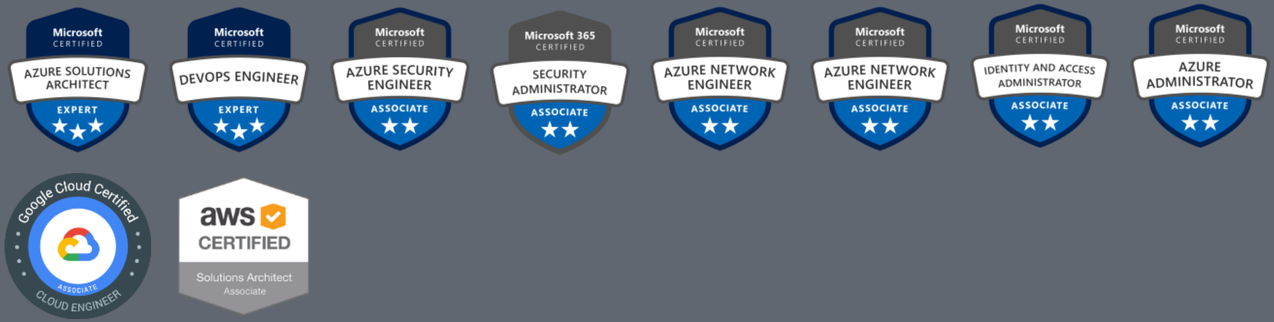
About me

Hannes Lagler-Gruener

Multi 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

New session about

Microsoft Sentinel Workbooks

Video type:	Nugget
Video category:	Level-300

Session Agenda

https://bit.ly/3gRQRqY

@HannesLagler

- Visualize you collected Data
- Use build-in or create your own
- Data Sources
- Visualization options
- Demo

Visualize you collected Data

Azure Workbooks are the modern way, to visualize your data and allow you to quickly gain insights across your data as soon as you connected a data source

Cloudblogger.at

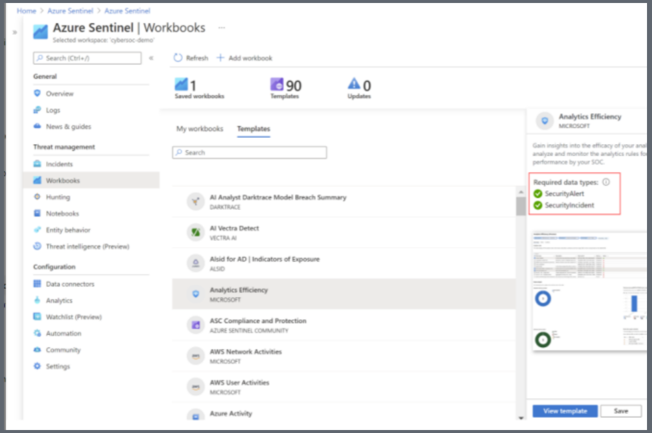
Use build-in or create your own

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

- Microsoft Sentinel has a lot of build-in Workbooks

!Keep in mind, you have to connect the data sources before.

- Or you create your own Workbooks from scratch or modify the existing workbooks.



AI Analyst Darktrace Model Breach Summary
DARKTRACE

AI Vectra Detect
VECTRA AI

Alsid for AD | Indicators of Exposure
ALSID

Analytics Efficiency
MICROSOFT

ASC Compliance and Protection
AZURE SENTINEL COMMUNITY

AWS Network Activities
MICROSOFT

AWS User Activities
MICROSOFT

Azure Activity

Analytics Efficiency
MICROSOFT

Gain insights into the efficacy of your anal
analyze and monitor the analytics rules fo
performance by your SOC.

Required data types: ⓘ
✓ SecurityAlert
✓ SecurityIncident

Data Sources

There are different data sources available

- **Log** > Collected data from data connectors
- **Metrics** > Get information from different Azure resources
- **Resource Graph** > Metadata from Azure resources
- **Azure Resource Manager** > Azure REST operations
- **Azure Data Explorer** > Query clusters with KQL
- **Workload health** > Monitor performance of IaaS resources

Data Sources (continue)

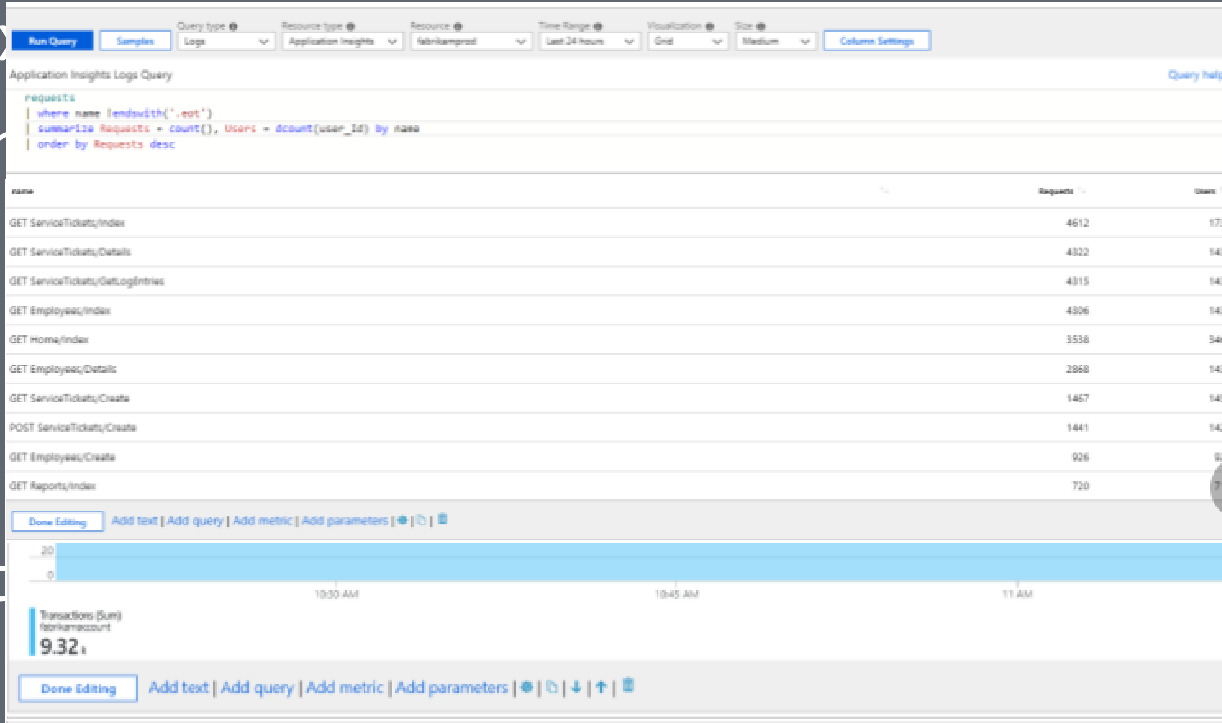
There are different data sources available

- **Azure resource health** >Get health of Azure resources
- **Change Analysis** > Query Application Change Analysis
- **JSON** > Query static JSON content (often used for parameters)
- **Alerts** > Visualize active Alerts in Azure
- **Custom endpoint** > Get data from external sources

Visualization options

There are different visualization options available

- **Text >** allow to include tex
- **Chart** > There are differen
    - Log
    - Time-series
    - Categorical bar
    - Pie charts
    - Metric charts
- Grid > There are different
    - Log-based
    - Simple


Run Query
Samples
Column Settings
Query help
Done Editing
Add text | Add query | Add metric | Add parameters
20
0
10:30 AM
10:45 AM
11 AM
Done Editing
Add text | Add query | Add metric | Add parameters

Query type	Resource type	Resource	Time Range	Visualization	Size
Logs	Application Insights	fabrikamprod	Last 24 hours	Grid	Medium

Application Insights Logs Query

```
requests
| where name !endswith('.eot')
| summarize Requests = count(), Users = dcount(user_Id) by name
| order by Requests desc
```

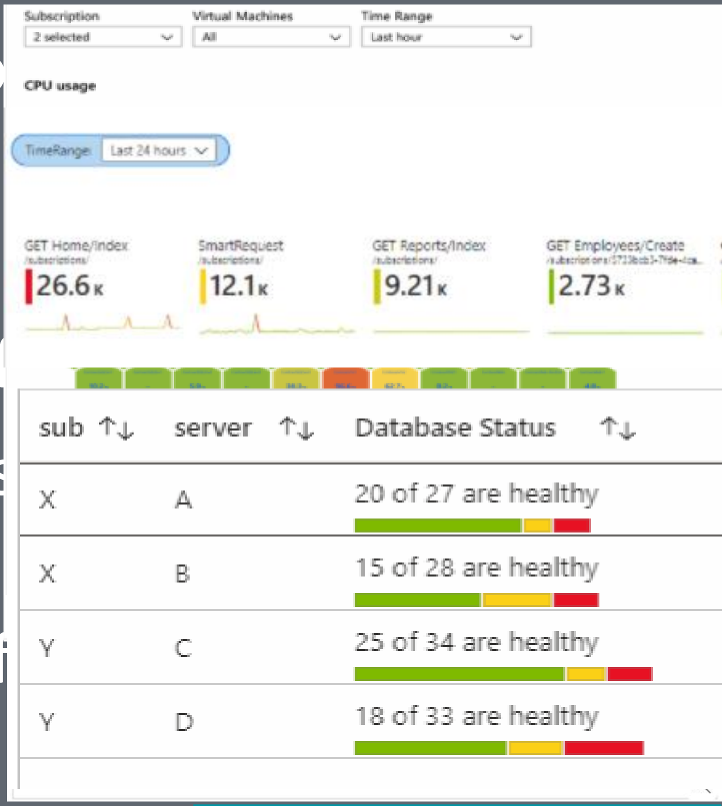
name	Requests	Users
GET ServiceTickets/Index	4612	17
GET ServiceTickets/Details	4322	14
GET ServiceTickets/GetLogEntries	4315	14
GET Employees/Index	4306	14
GET Home/Index	3538	34
GET Employees/Details	2868	14
GET ServiceTickets/Create	1467	14
POST ServiceTickets/Create	1441	14
GET Employees/Create	926	9
GET Reports/Index	720	7

Transactions (Sum)
fabrikamaccount
9.32 k

Visualization options (continue)

There are different visualization options available

- **Tile >** to present summary data in workbo
- **Tree** > allow some rows to be expandable
  level for a drill-down experience
- **Graph** > visualizing graphs based on data f
- **Map** > visualization aids in pin-pointing iss
  specific regions
- **Honey comb** > allow high density views of
  categories
- **Composite bar** > allows rendering data using
  composite bar



Subscription: 2 selected
Virtual Machines: All
Time Range: Last hour

CPU usage

TimeRange: Last 24 hours

GET Home/Index /subscriptions/ 26.6K

SmartRequest /subscriptions/ 12.1K

GET Reports/Index /subscriptions/ 9.21K

GET Employees/Create /subscriptions/5733bcb3-7f4e-4ca... 2.73K

sub ↑↓	server ↑↓	Database Status ↑↓
X	A	20 of 27 are healthy
X	B	15 of 28 are healthy
Y	C	25 of 34 are healthy
Y	D	18 of 33 are healthy

Switch to the Live Demo!

https://bit.ly/3gRQRqY

@HannesLagler

- Design a workbook from scratch
- Implement different visualizations
- (Advanced) Implement a Graph visualization
- Use Azure Actions in workbooks