# Analiza logów systemowych w środowisku multicloud

Konrad Sagała

Cloud Security Architect




Wydarzenie organizowane przez: Fundacja Academic Partners

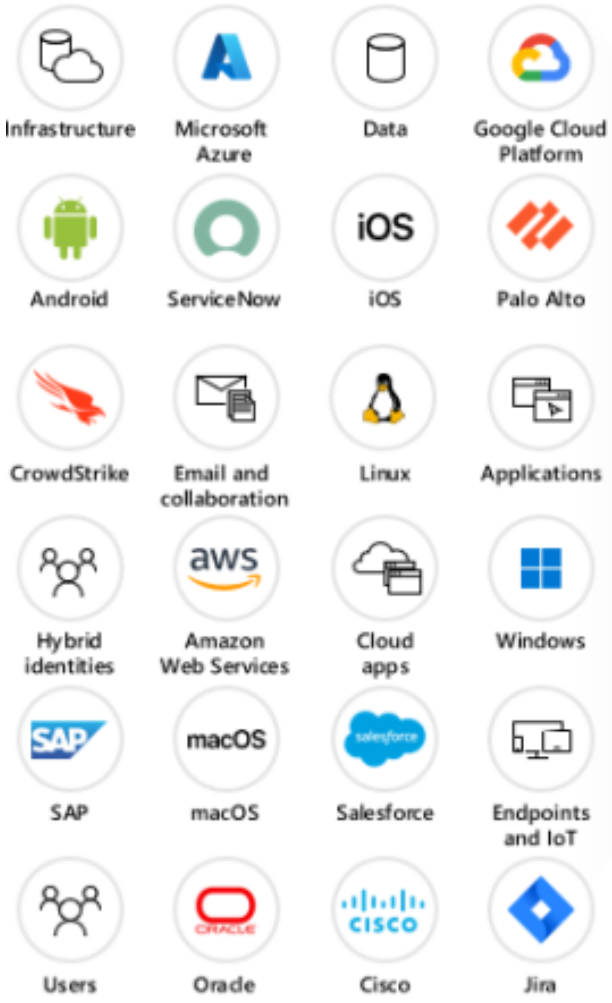
# Agenda

1. Intro
2. Data Connectors and tables
3. Log collector
4. Data Collection Rules
5. Workspace Transformation DCR

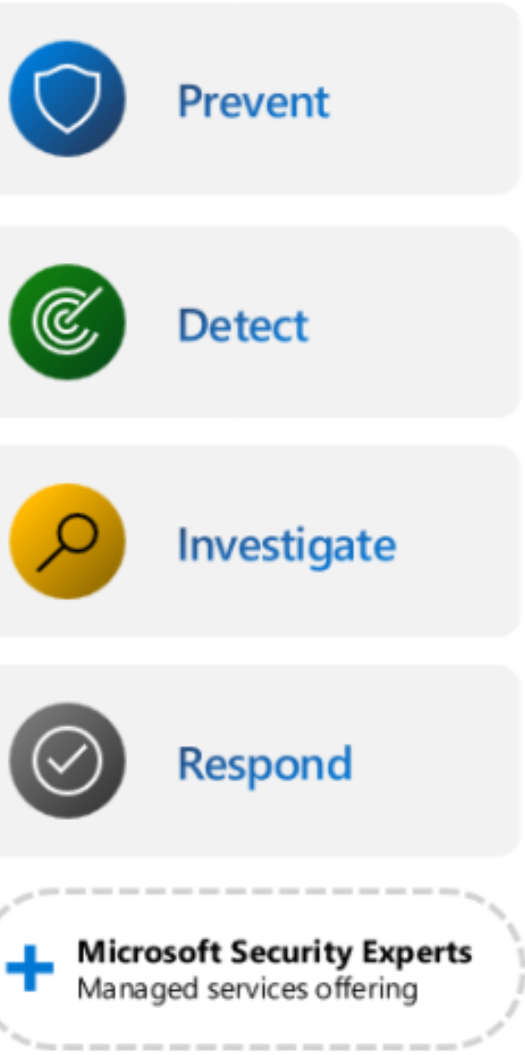
# A unified security operations platform

## Microsoft Sentinel and Defender XDR together

### 300+ data sources including:







# Log ingestion

**New Azure Monitoring Agent (AMA) replaces Log Analytics Agent (MMA)**

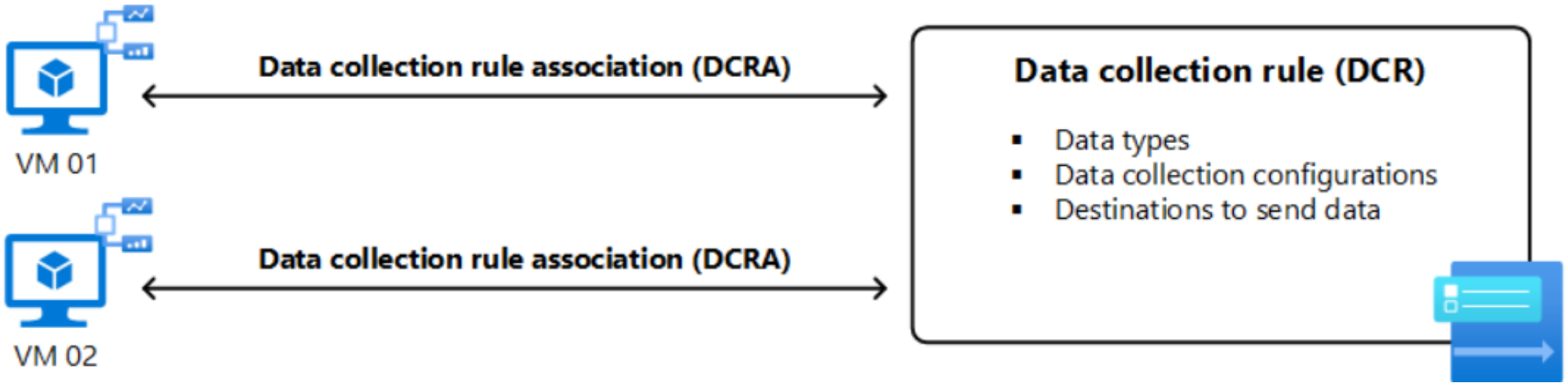
**Data Connectors:**

- **Common Event Format (CEF) via AMA**
- **Syslog via AMA**
- **Windows Security Events via AMA**

**Type of tables:**

1. **Auxiliary Logs**: 30 days of retention included; can be extended up to 12 years. $0.10 per GB.
2. **Basic Logs**: 30 days of retention included; can be extended up to 12 years. $0.50 per GB.
3. **Analytics Logs**: 31/90 days of retention included; can be extended up to 12 years. $2.30 per GB.

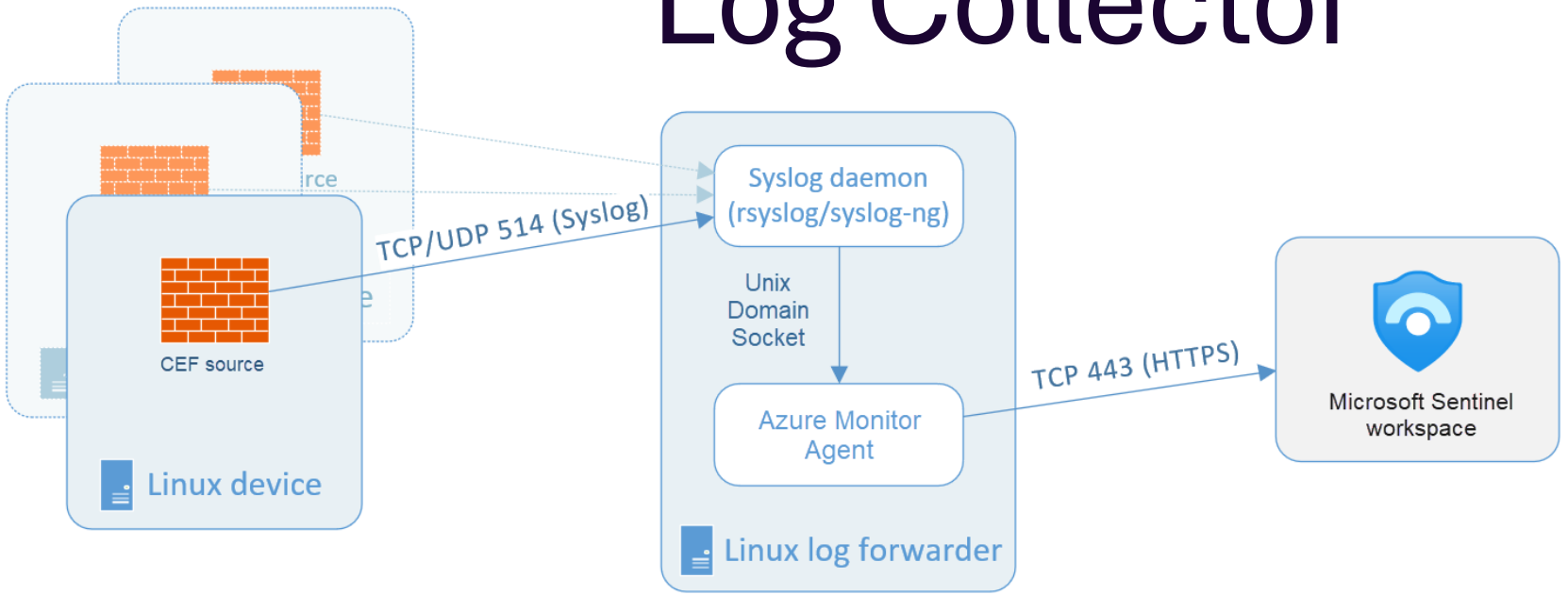
# AMA - Basic DCR from Data Connectors






Data collection rules in Azure Monitor - Azure Monitor

# Log Collector



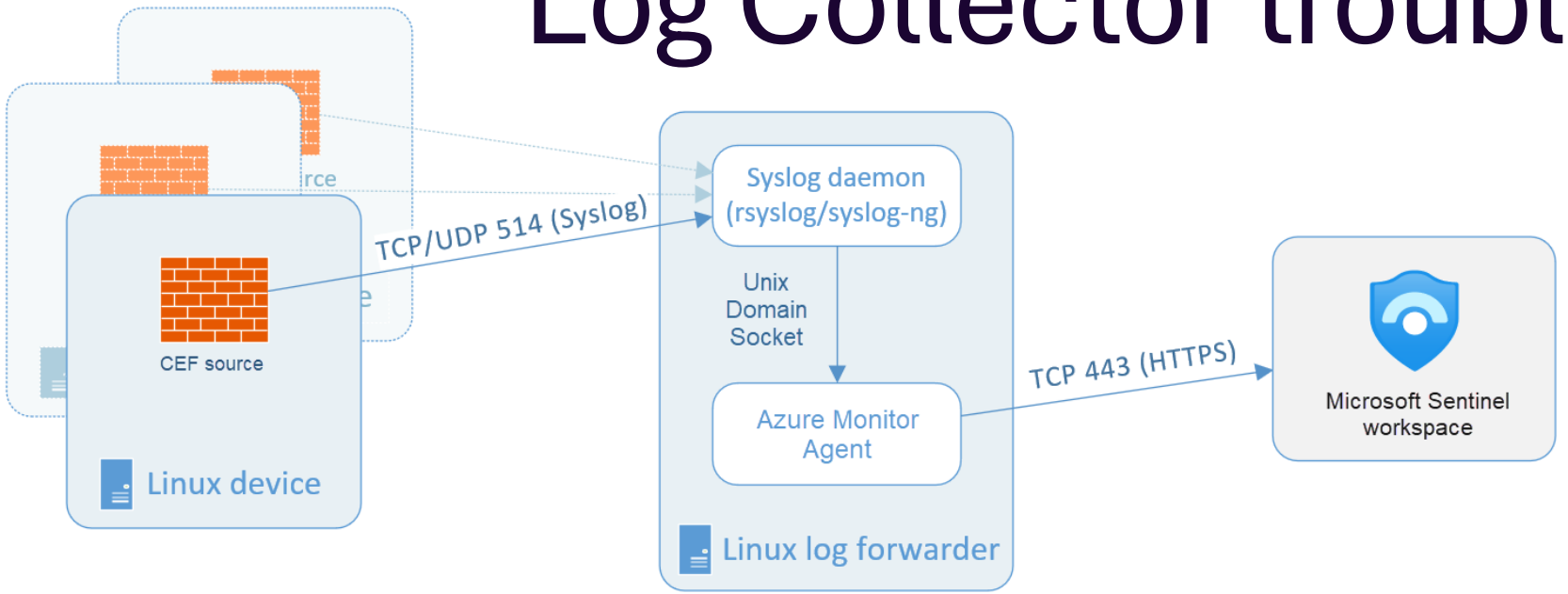

```
sudo wget -O Forwarder_AMA_installer.py
https://raw.githubusercontent.com/Azure/Azure-
Sentinel/master/DataConnectors/Syslog/Forwarder_AMA_installer.py

sudo python Forwarder_AMA_installer.py
```



Step-by-Step Guide for Deploying a Syslog Collector to ingest into Microsoft Sentinel – RYAN PERRIN

# Log Collector troubleshooting




logger -p local4.warn -P 514 -n 127.0.0.1 --rfc3164 -t CEF "0|Mock-test|MOCK|common=event-format-test|end|TRAFFIC|1|rt=$common=event-formatted-receive_time”

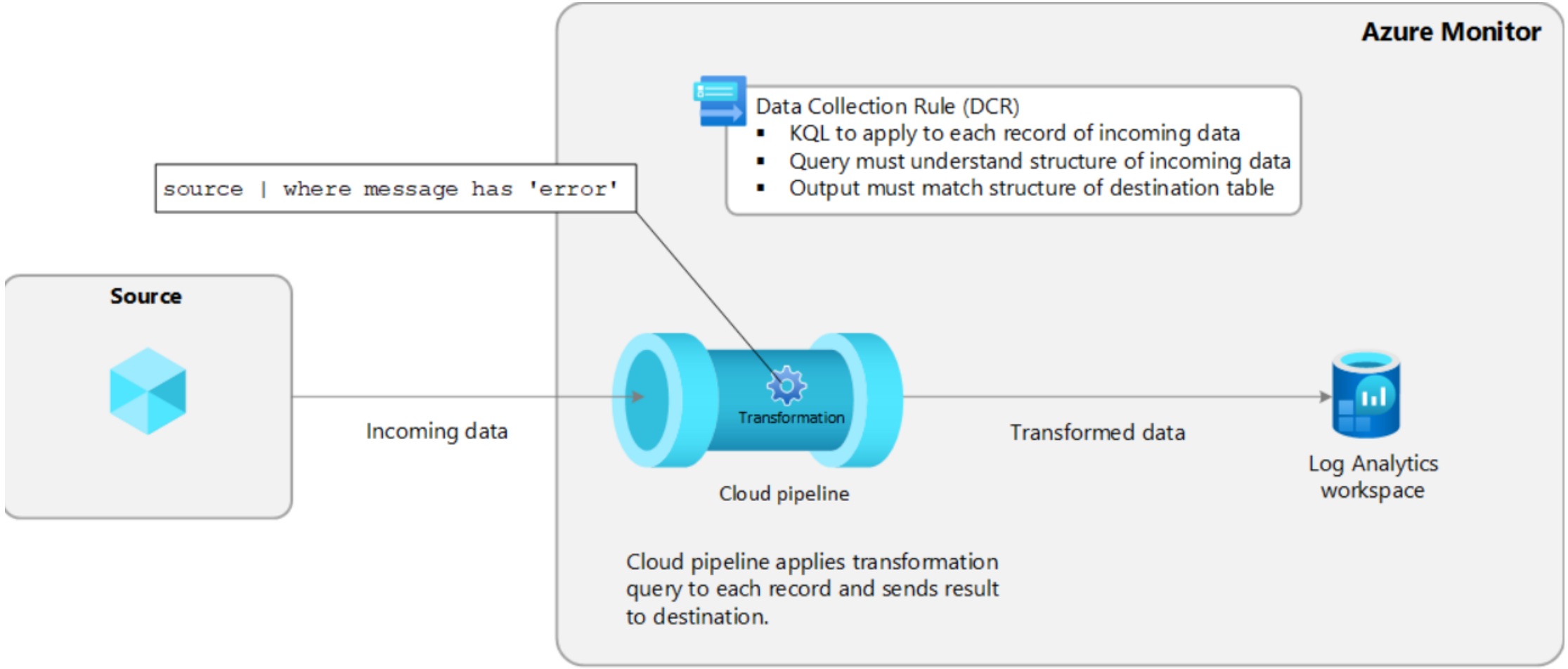
sudo wget -O Sentinel_AMA_troubleshoot.py https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/Syslog/Sentinel_AMA_troubleshoot.py

sudo python Sentinel_AMA_troubleshoot.py --cef



Ingest syslog and CEF messages to Microsoft Sentinel - AMA | Microsoft Learn

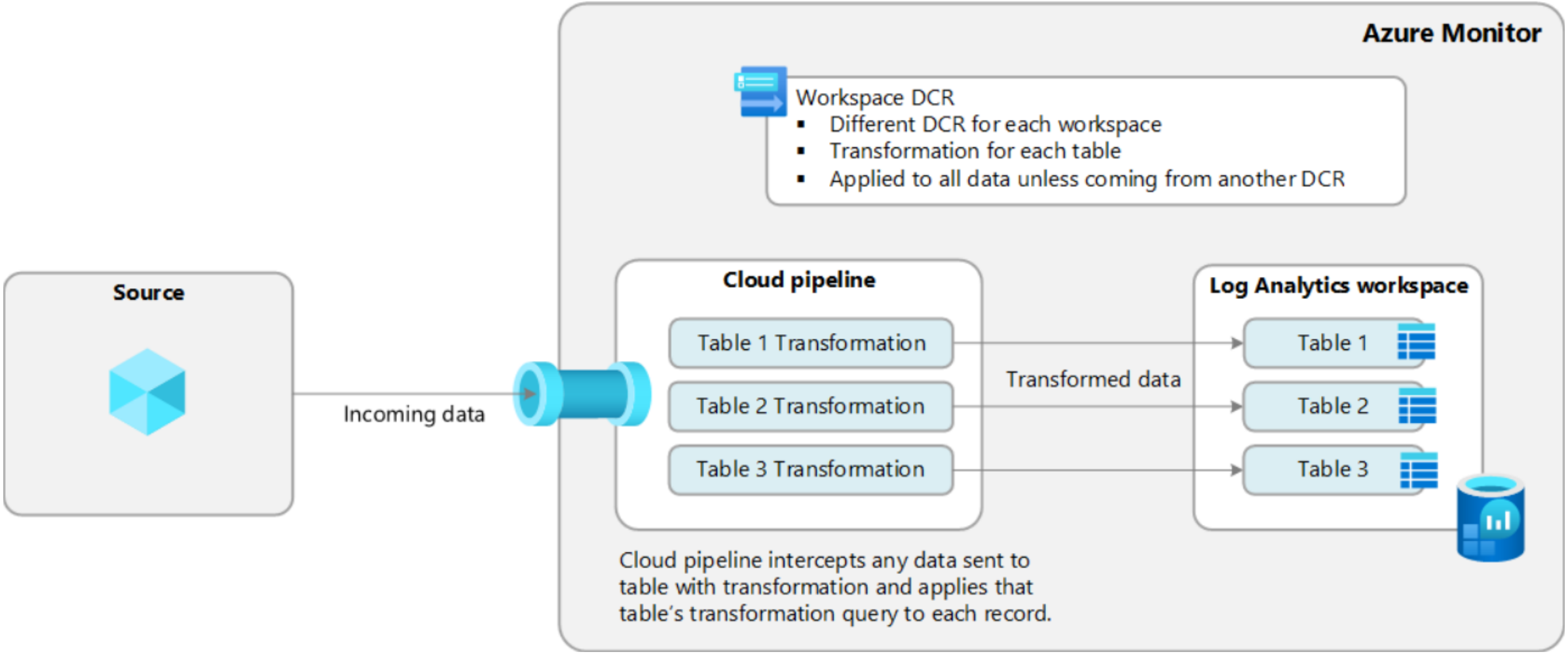
# Transformations






[Tables that support ingestion-time transformations in Azure Monitor Logs]

# Workspace transformations DCR






Transformations in Azure Monitor

# Vertical vs Horizontal filtering

Vertical filtering example (removing columns):
Source
| project-away RawData

Horizontal filterling example (removing rows):
Source
| where severity == "Critical"

Data Collection Rule - Vertical vs Horizontal Filtering
Sample transformations in Azure Monitor - Azure Monitor

# More info about transformation DCR

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/tutorial-workspace-transformations-portal

https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-transformations-samples

https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-transformations-create?tabs=portal

# Dziękuję za oglądanie!

Pamiętaj, aby zostawić swoje pytania i oceń prezentację w poniższej sekcji.

WDI WARSZAWSKIE DNI INFORMATYKI

Prelekcja wybrana w wyniku selekcji przez Radę Programową złożoną z uznanych liderów obszaru IT oraz Data Science.

Warszawa,
04.04.2025 - 05.04.2025

OFICJALNA PRELEKCJA WARSZAWSKICH DNI INFORMATYKI

ACADEMIC PARTNERS

# Feedback

## Zeskanuj kod i zostaw swoją opinię

WARSZAWSKIE DNI INFORMATYKI

Analiza logów systemowych w środowisku multicloud

Konrad Sagała

https://warszawskiedniinformatyki.pl/user.html#!/lecture/WDI25-72b1/rate