

# Monitoring

---

# Overview

What you need to think about to be successful

Diagnostics and metrics

Log search

Alerting

# Things to Keep in Mind Regarding Azure VM Monitoring

You're free to use native tools (PerfMon, ps)

Take Azure into account when evaluating mon. solutions

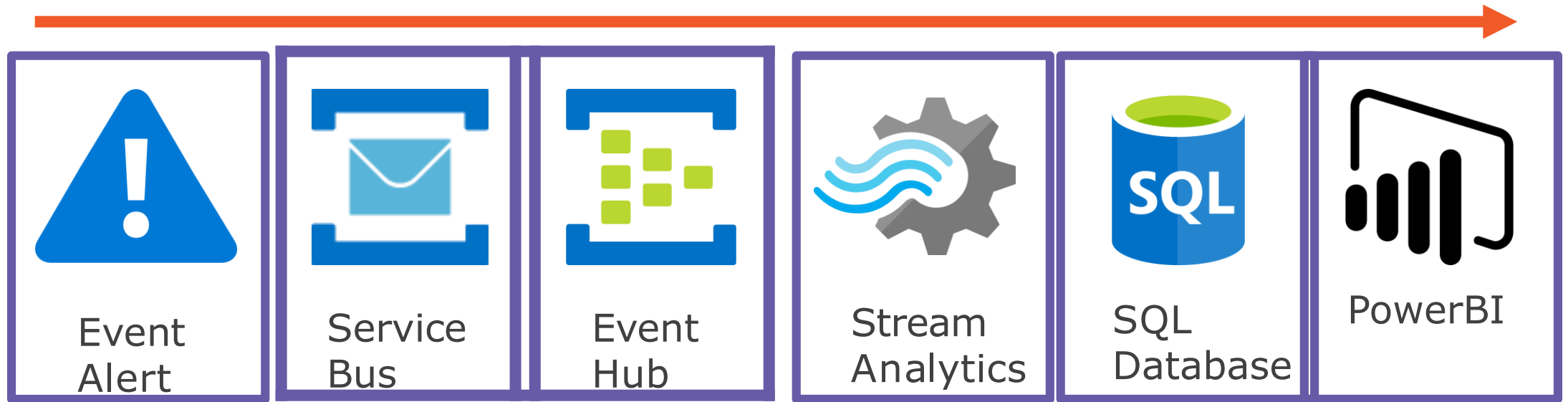
Learn about webhooks, REST, and SQL

With hybrid cloud, you can use System Center

OMS is a tightly integrated solution

Consider streaming data via Event Hub

# The Azure Event Hub Workflow



# Monitoring – A Layered Approach

## Resource level

- Internal tools
- Metrics, alert rules

## Resource Group level

- Monitor blade

## Enterprise level

- Hybrid nodes
- Log Analytics
- Azure Automation

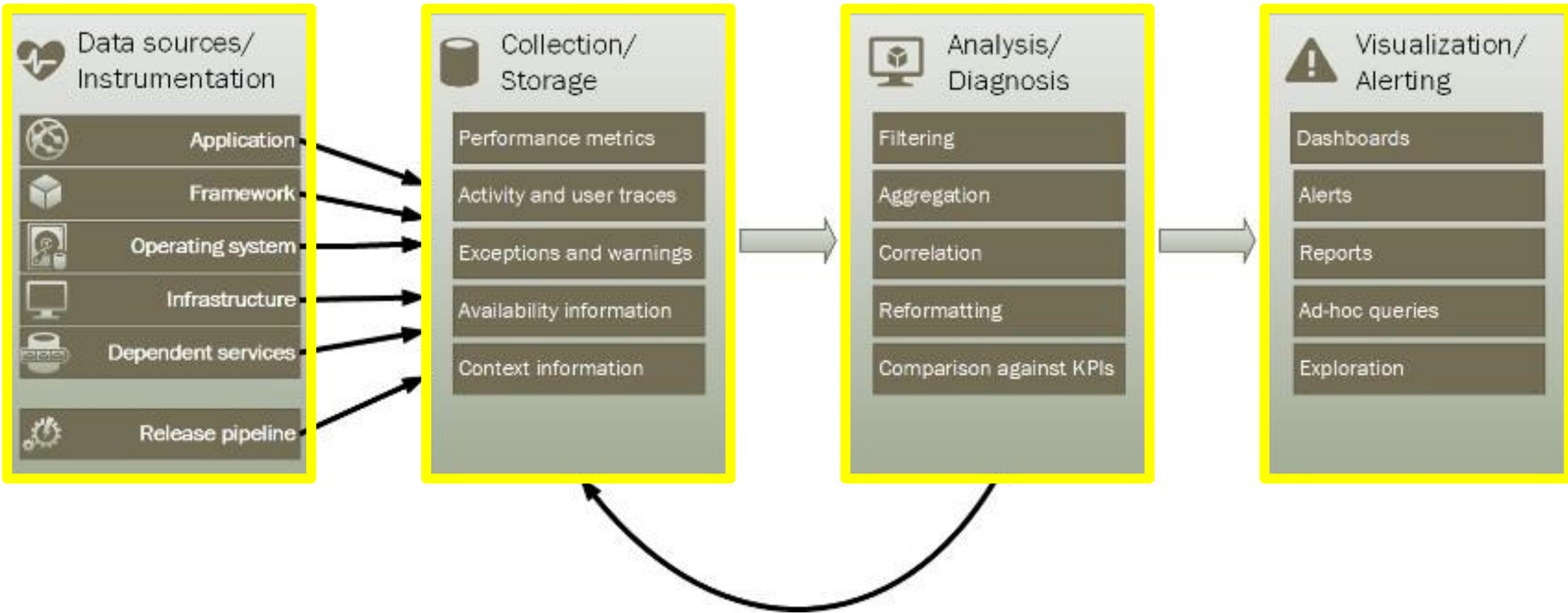
# Diagnostics and Metrics

W

# Telemetry

An automated communications process by which measurements and other data are collected at remote or inaccessible points and transmitted to receiving equipment for monitoring

# Monitoring and Diagnostics Pipeline





# Azure Diagnostics Data

## Event tracing

Configured by app  
developers

## Performance counters

The 4 traditional  
subsystems

## Event logs

You likely have  
experience here

## Application logs

Configured by app  
developers

## Azure Diagnostics logs

Table and/or blob  
storage

# Log Search

# Monitoring – Questions of Scale and Intelligence

## Log flood

- So many data sources
- How to quickly extract value?

















## Predictive analytics

- How to know what to look for?

## Automation

- Immediate remediation

# OMS Log Analytics

Pricing tier		
Get additional services with Operations Management Suite (OMS). <a href="#">Learn more</a>		
The free and standalone Log Analytics tiers are per-GB ingestion models. OMS offerings are priced per-node.		
F Free	S Standalone	O OMS
 500 MB Daily upload limit	 Unlimited Daily upload limit	 Insight + Analytics
 7 days Data retention	 31 days Data retention	 Automation + Control
 90 days Activity log	 90 days Activity log	 Security + Compliance
 500 min/month Runbooks	 10+ Management solutions	 Unlimited Daily upload limit
	 Unlimited Azure metrics	 31 days Data retention
	 Unlimited Azure diagnostics logs	 Unlimited min Runbooks
0.00 (USD)	2.30 COST PER 1GB (USD)	10.00 STARTING COST PER NODE (USD)

# OMS Insight & Analytics

## Log Analytics



## Log Search



Alerting

# The Need for an Alerting Solution

Avoiding surprises

Email, SMS

Third-party Security and  
Event Management (SIEM)

Azure integration is eminently  
possible



# Webhook

A way for an app to provide other applications with real-time information. Also called a web callback or an HTTP push API. The payload is ordinarily JSON.

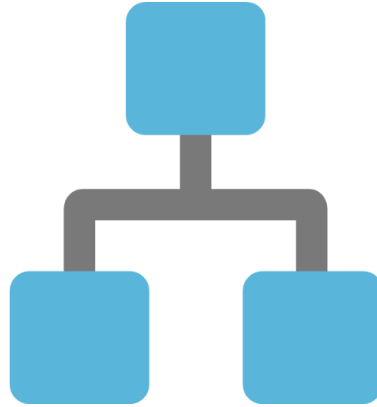


# What Can You Do with Webhooks?



## Third-Party Integrations

PageDuty, OpsGenie,  
VictorOps, Slack,  
HipChat, Campfire,  
etc...



## Script Execution Azure Automation runbooks



## SMS Text Twilio API

# Demo



1

Enable monitoring for VMs

Start with Portal

Then show PowerShell

Demo



2

# Demo



# 3

Show integration with....Datadog?

# Summary



The question now isn't how to generate actionable data

- It's what to do with the data

Take advantage of Log Analytics and the centralization and intelligence it offers

Next module: **Troubleshooting and Support**