Who am I

- Old School gamer
- Discgolfer
- Purple teamer (mostly blue)
- Always curious (Geek)
- Father

Anders Kristiansen
Principal
Azure Security Lead
Devoteam M Cloud

What my friends say: Anders is born lucky

devoteam
M Cloud

Accelerated
Cloud Enabler
by devoteam M Cloud

Microsoft sentinel

Creative Tech for Better Change

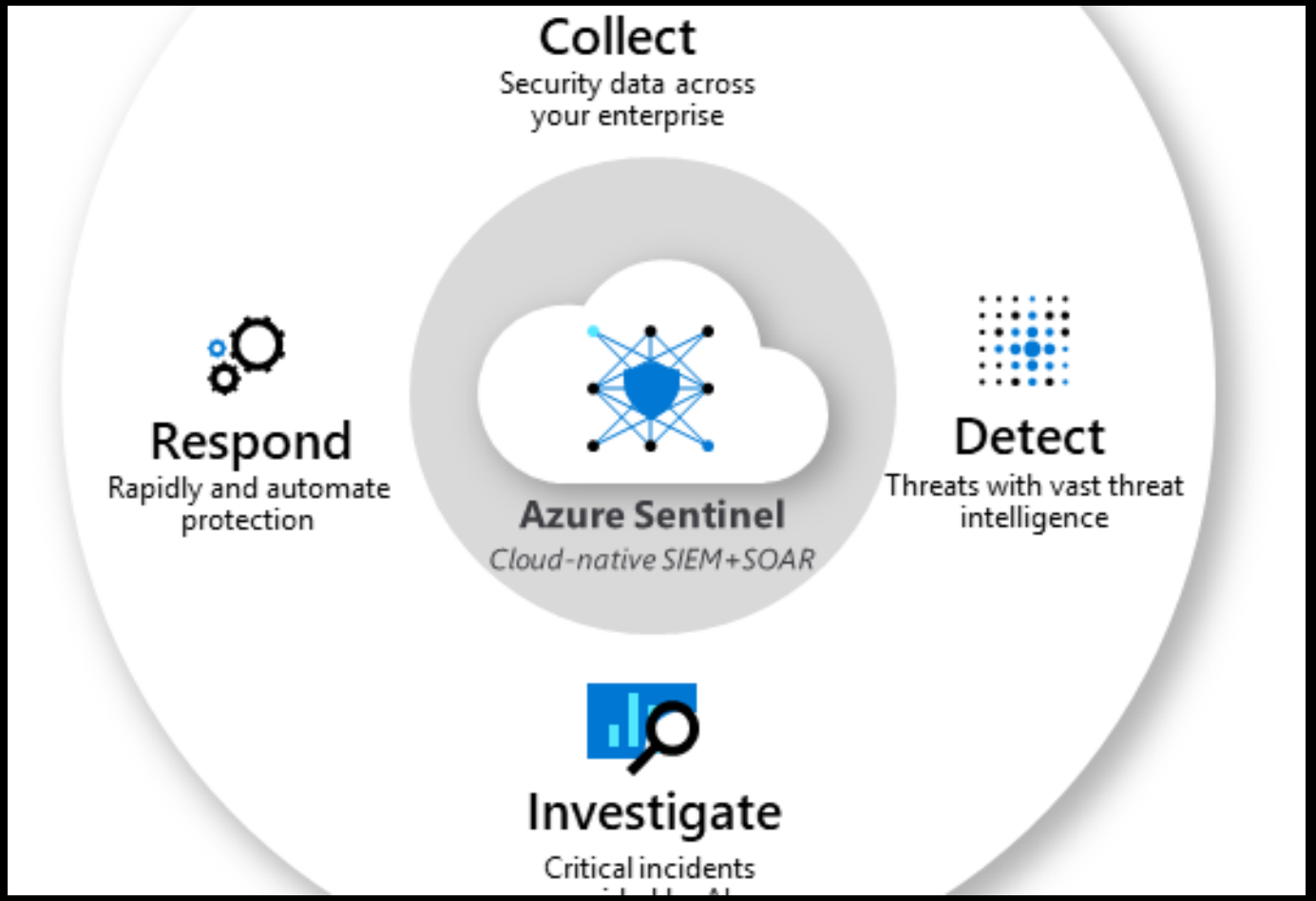
Agenda

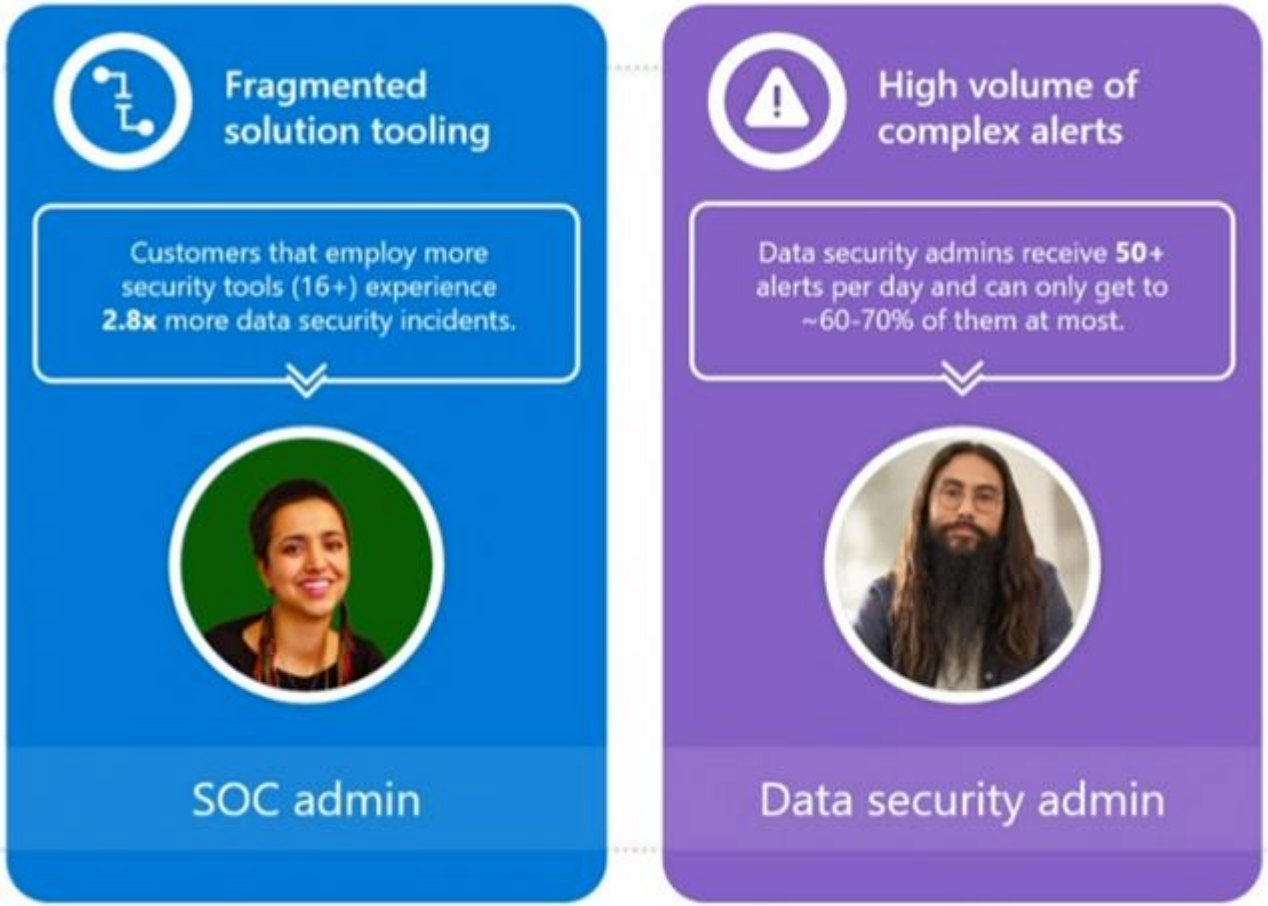
- Kort oversikt over Microsoft Sentinel
- Arkitekturen til Microsoft Sentinel
- Sentinel Case study: DataCollection Rules og betydningen av dette for kostnadskontroll og deteksjon.
- Demo av Security Pilot.
- Kostnadskontroll
- Demo/walk through: Sentinel-oppsett med GitHub som kodearkiv.
- Spørsmål

Oversikt av Microsoft Sentinel

-Microsoft Sentinel og dens rolle innen sikkerhetsinformasjon og hendelseshåndtering.

- Sentrale funksjoner og fordeler.

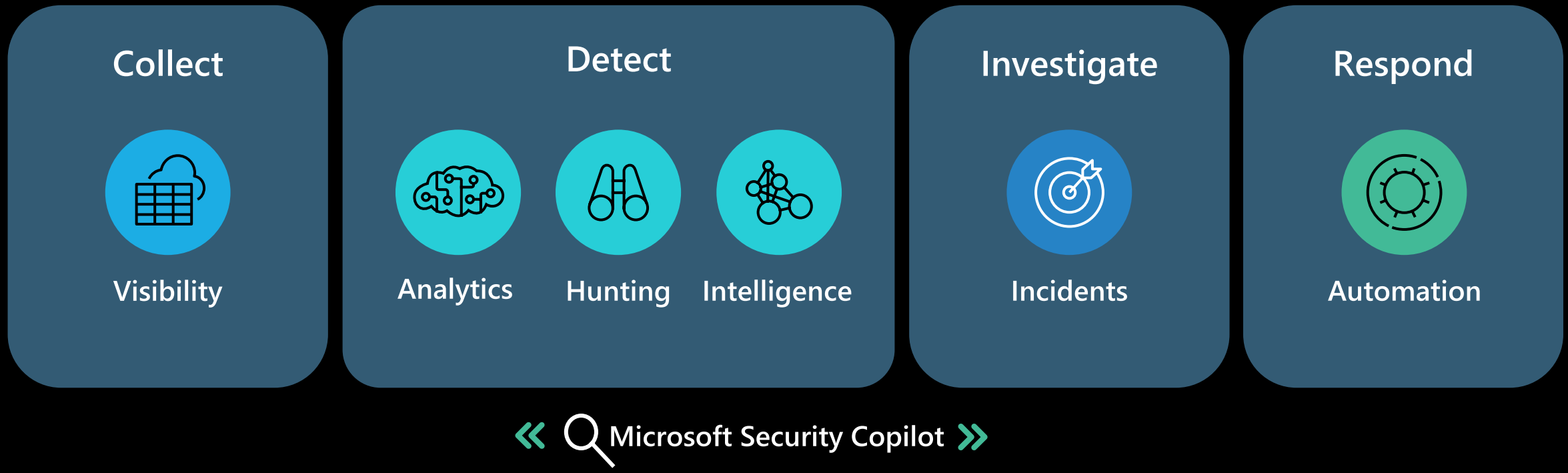


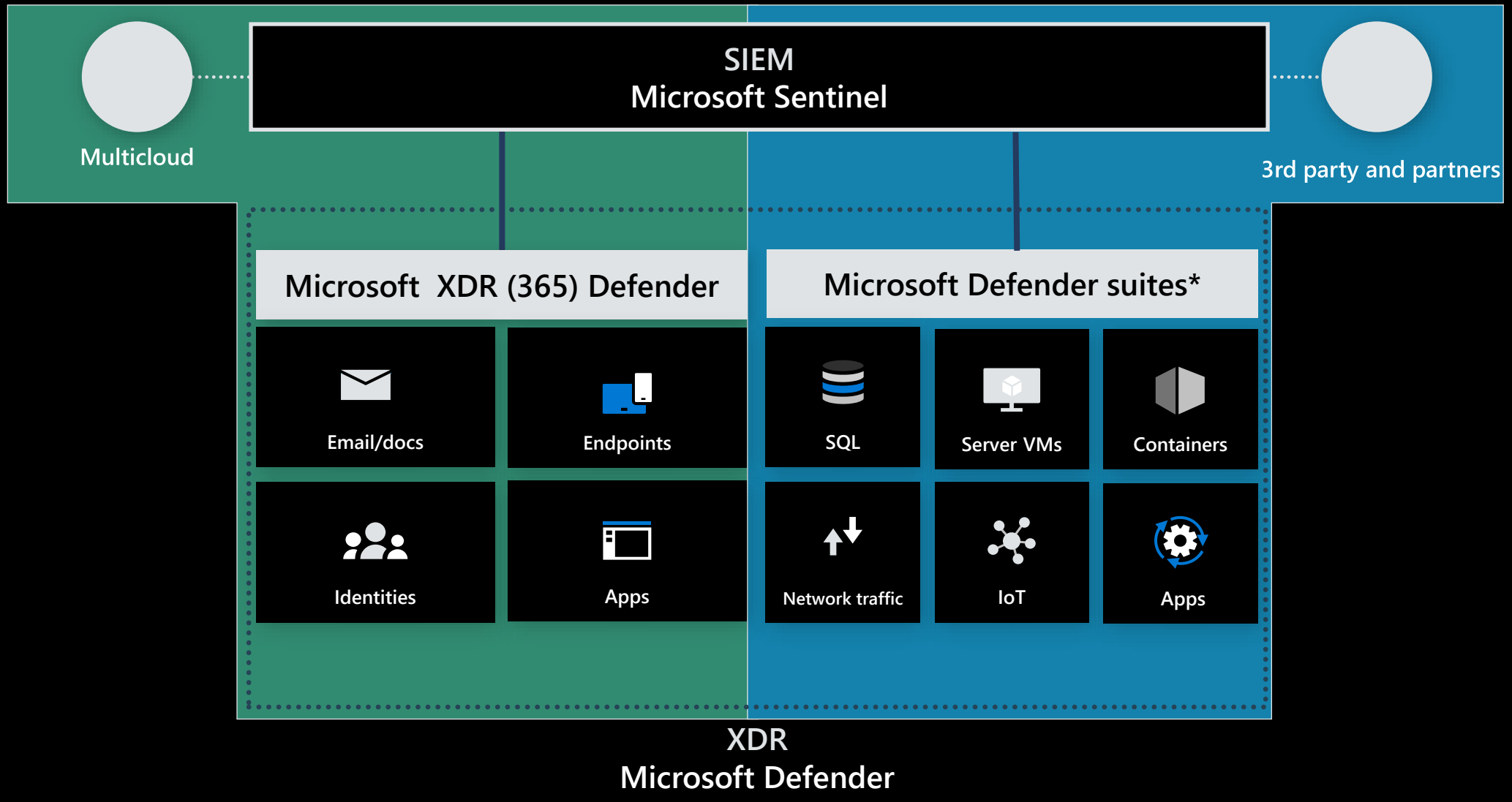


Source: Ignite2023

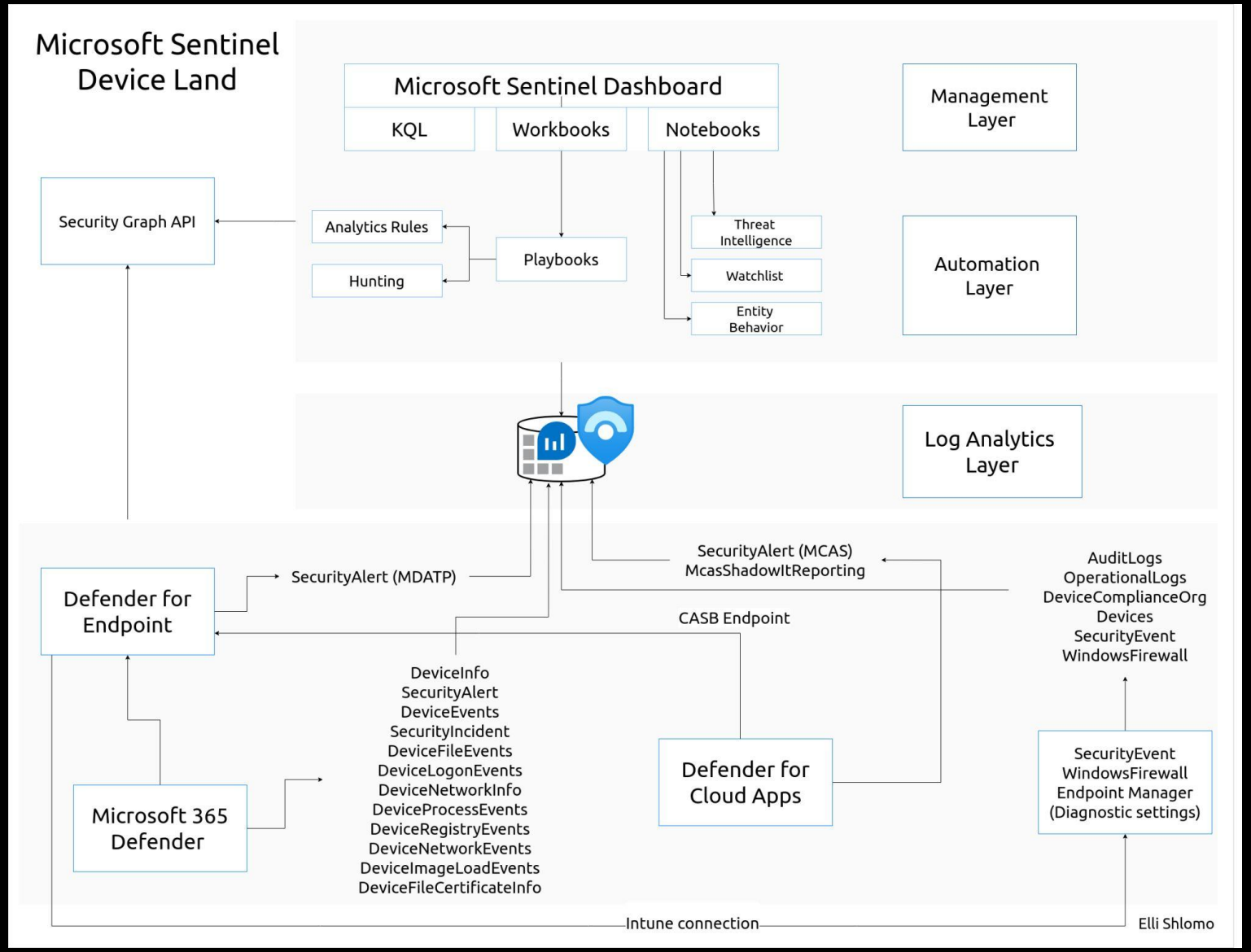
Hva skal jeg bruke min SIEM til?

Ende til ende løsning for sikkerhets operasjoner

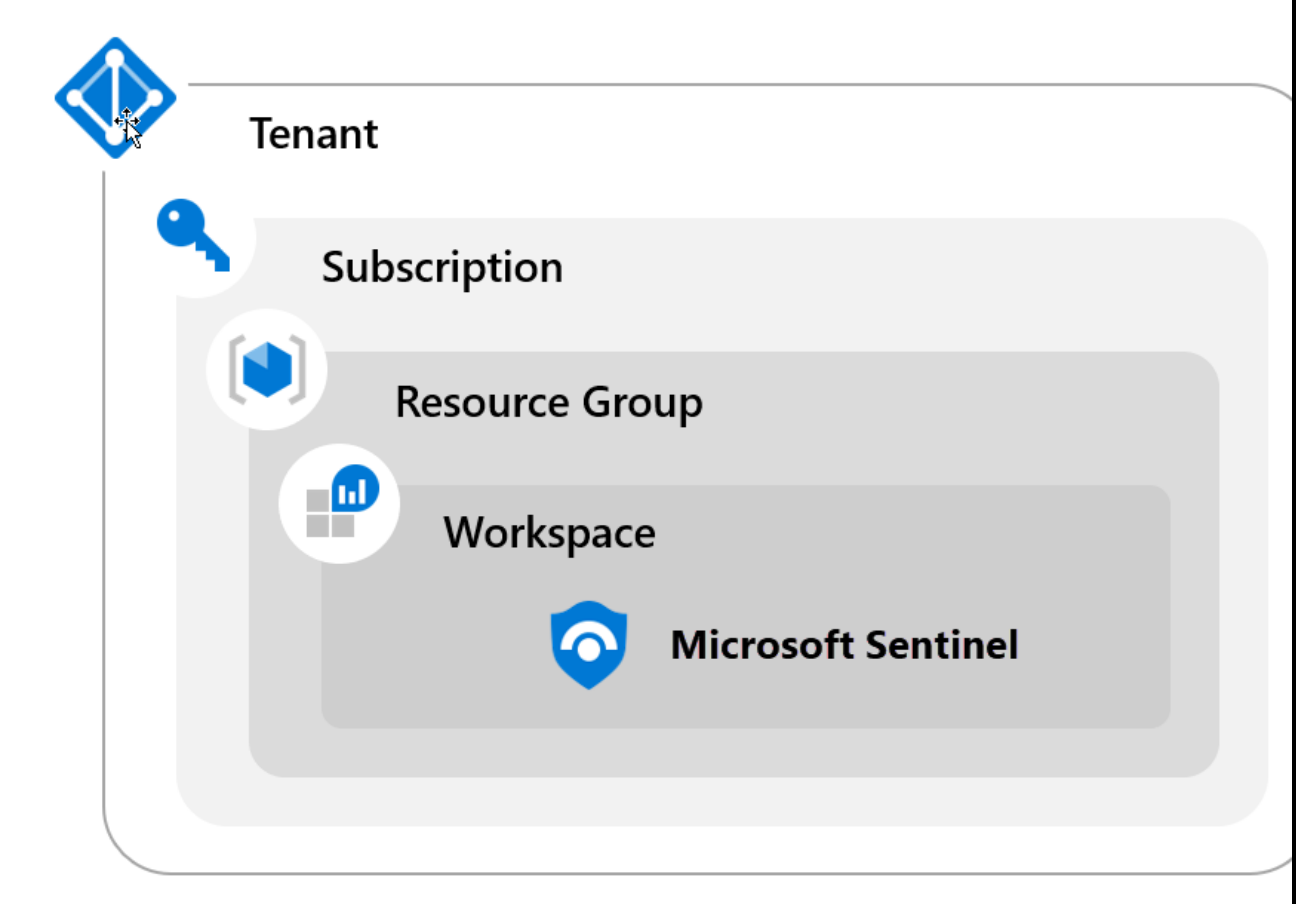



SIEM
Microsoft Sentinel
Multicloud
3rd party and partners
Microsoft XDR (365) Defender
Microsoft Defender suites*
Email/docs
Endpoints
SQL
Server VMs
Containers
Identities
Apps
Network traffic
IoT
Apps
XDR
Microsoft Defender

Sentinel Arkitektur



Eksempel: Singel workspace

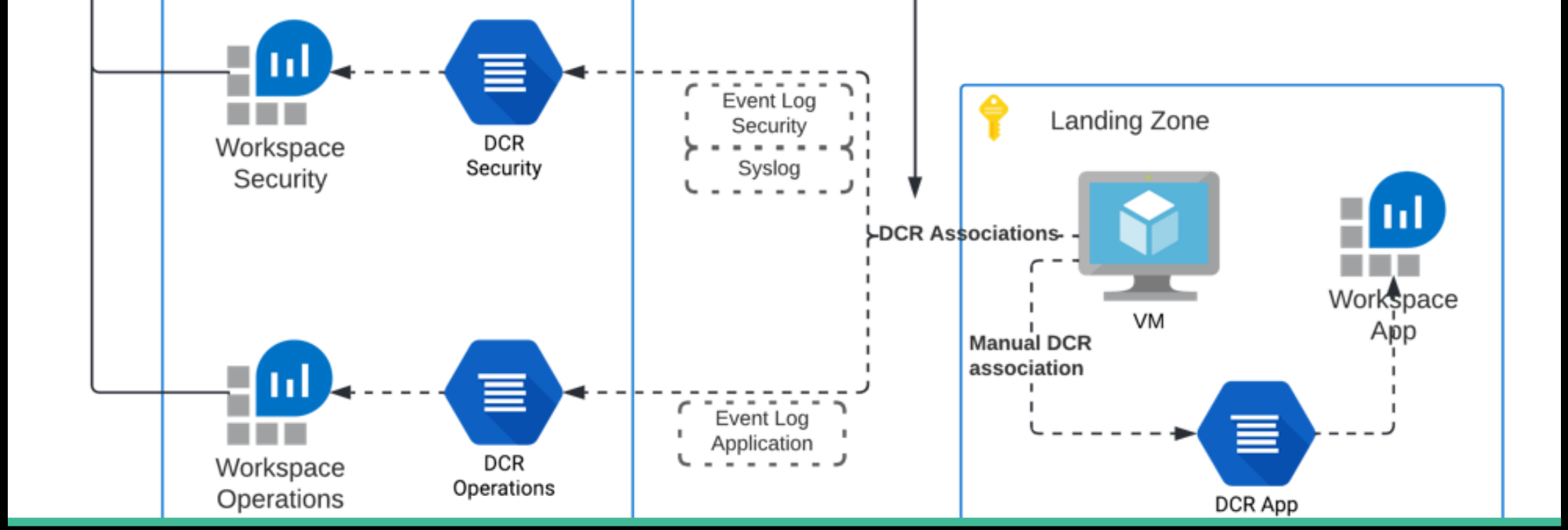


Fordeler:

- Single Pane of Glass
- Lettere query all info
- Log Analytics RBAC for data plane access
- Sentinel RBAC for sentinel

Ulemper:

- kostnad (cross region / opslogs)
- Kan by på data governance krav.



Fordeler:

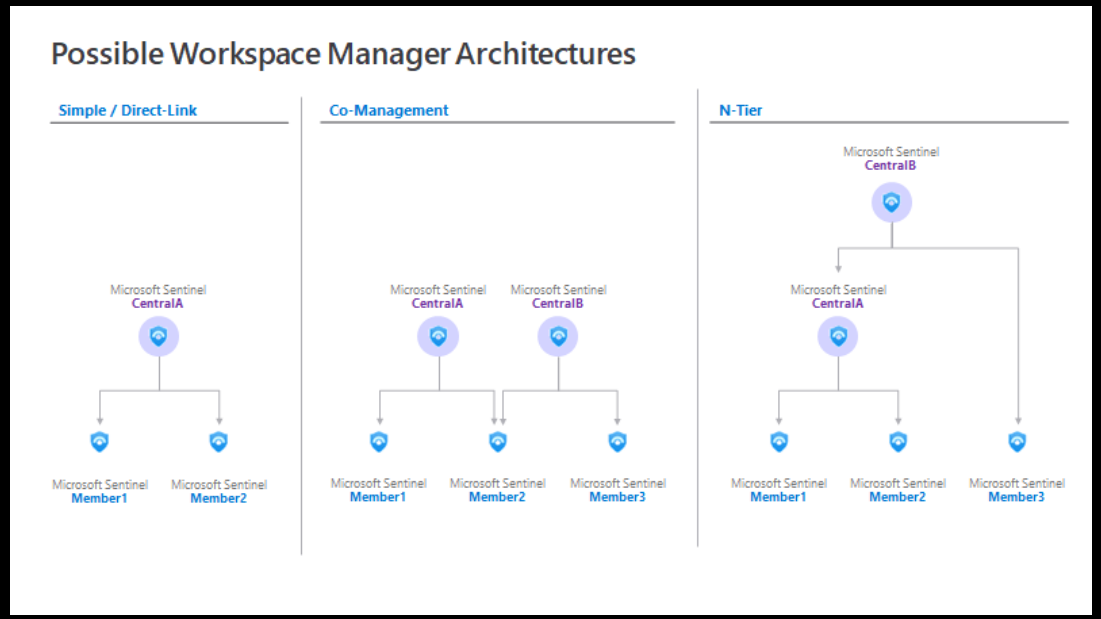
- kostnads besparende
- Kan delegere ansvar basert på rolle
- Kan logge mer operasjonell data I opslog*

Ulemper:

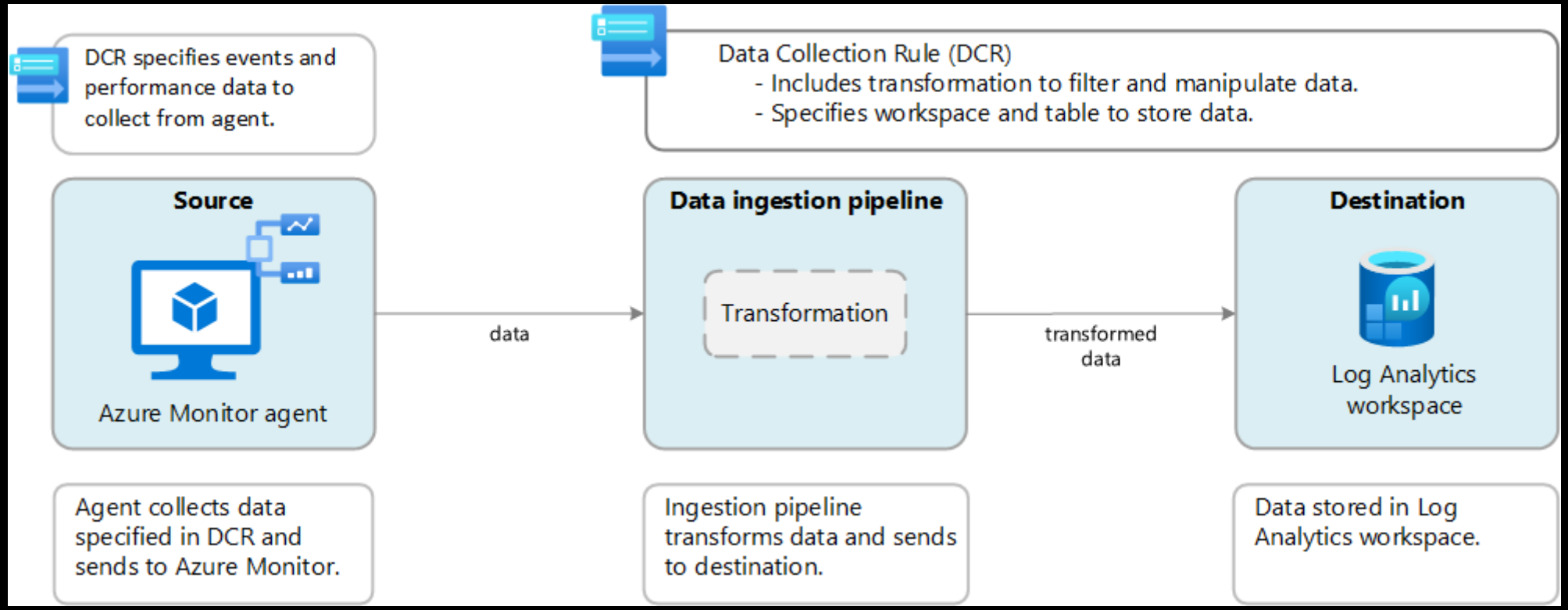
- Mer kompleks med azure policy, DCR.
- cross query
- Kan bli vanskelig bestemme seg for hvilke logger som skal hvor.

Workspace manager (preview)

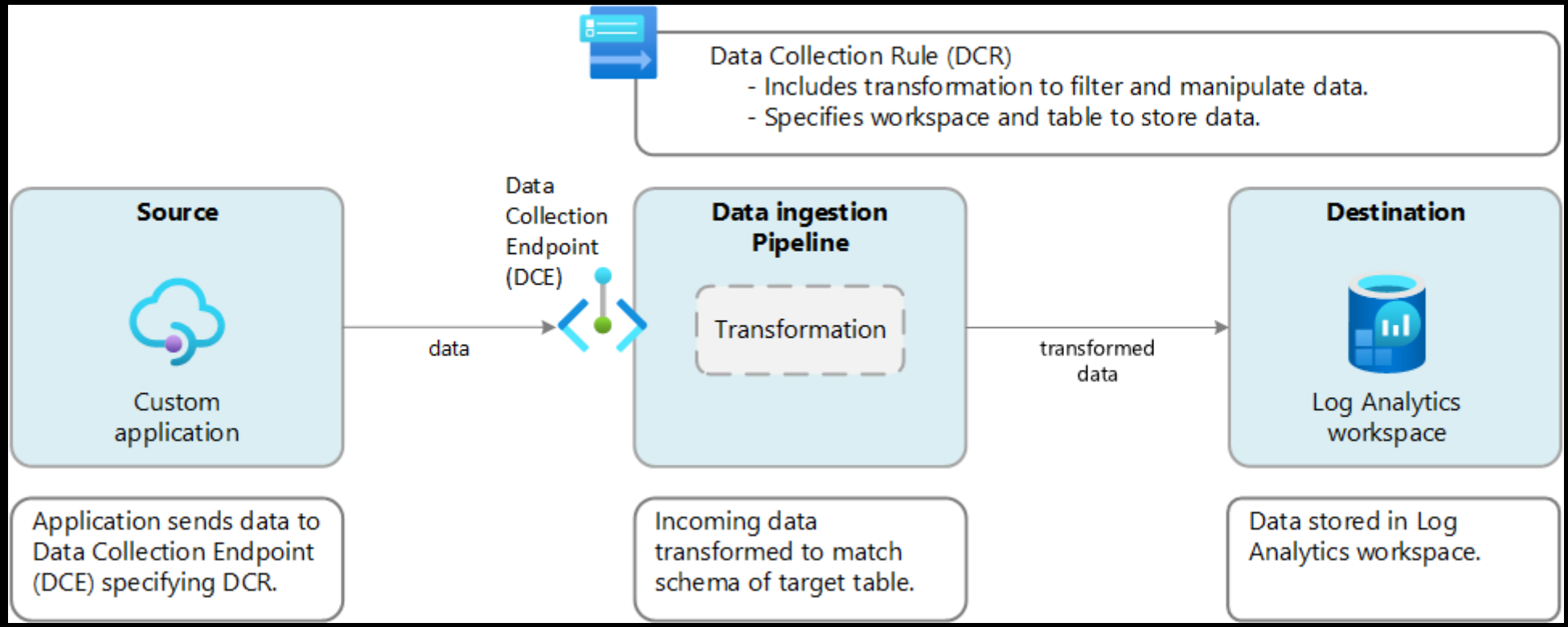
- ***Direktekobling*** *er den minst komplekse oppsettet. Kontroller alle medlems-workspaces med bare ett sentralt arbeidsområde.*
- ***Co-Management*** *støtter scenarier der mer enn ett sentralt arbeidsområde må administrere et medlemsarbeidsområde. For eksempel workspaces som samtidig administreres av et internt SOC-team og en MSSP.*
- ***N-Tier*** *støtter komplekse scenarier der et sentralt arbeidsområde kontrollerer et annet sentralt arbeidsområde. For eksempel ett selskap som administrerer flere datterselskaper, der hvert datterselskap også administrerer flere workspaces.*



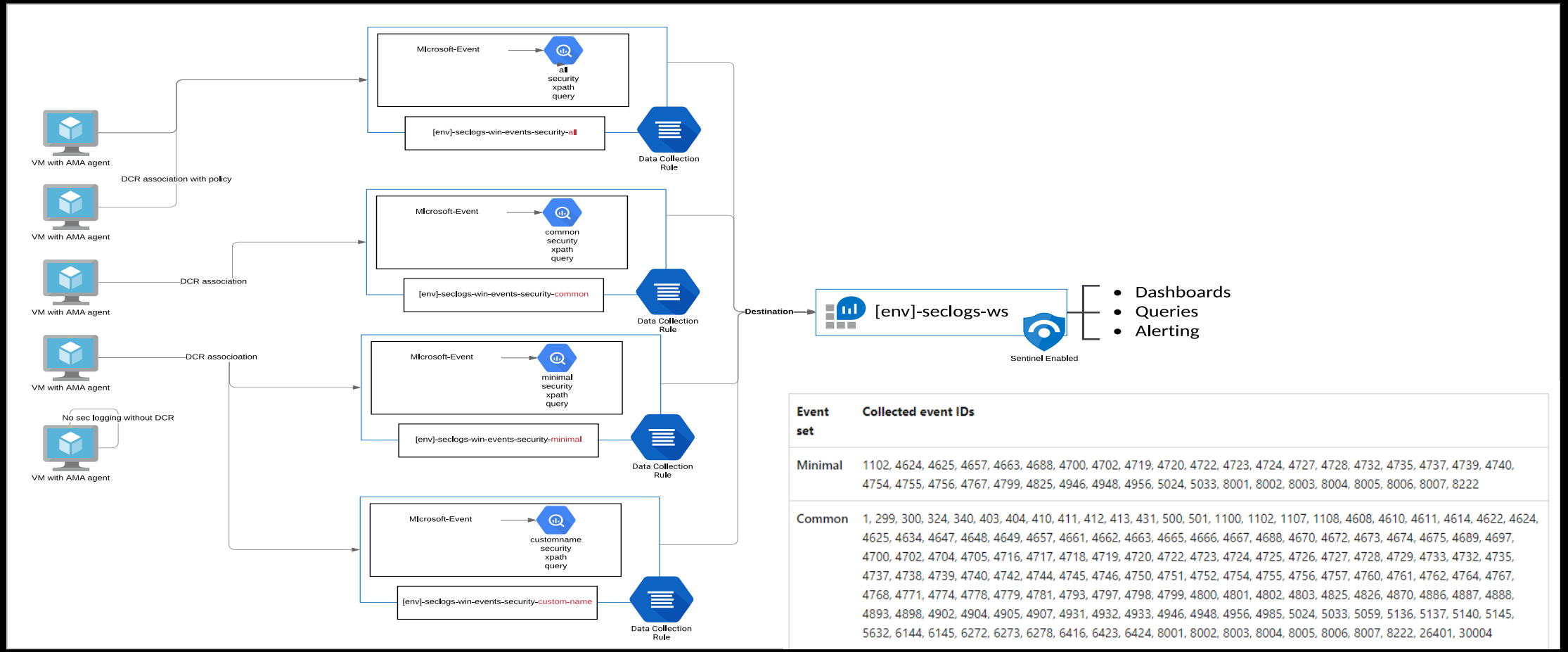
Data collection rules (DCR)



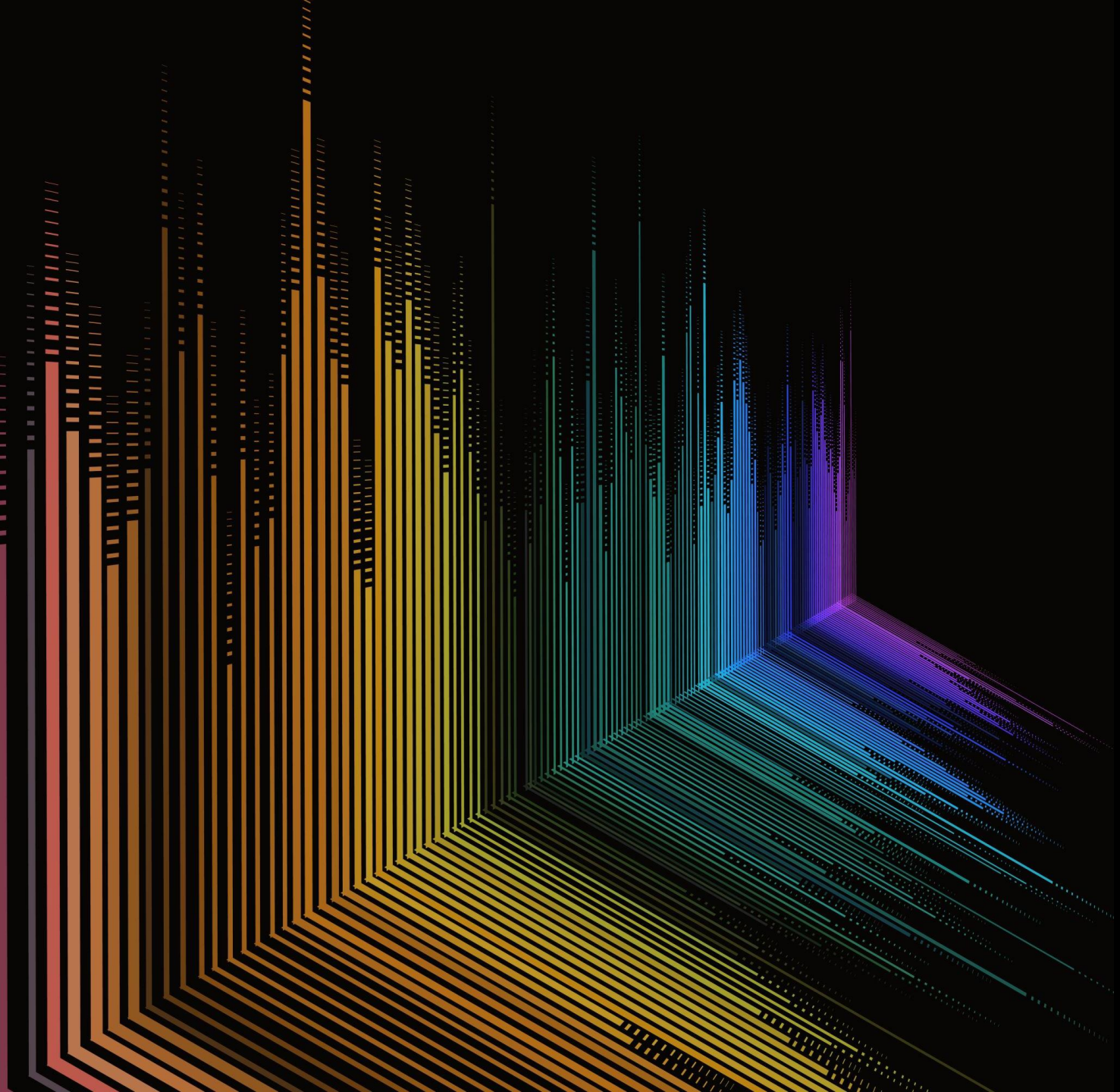
Datacollection endpoint (DCE)



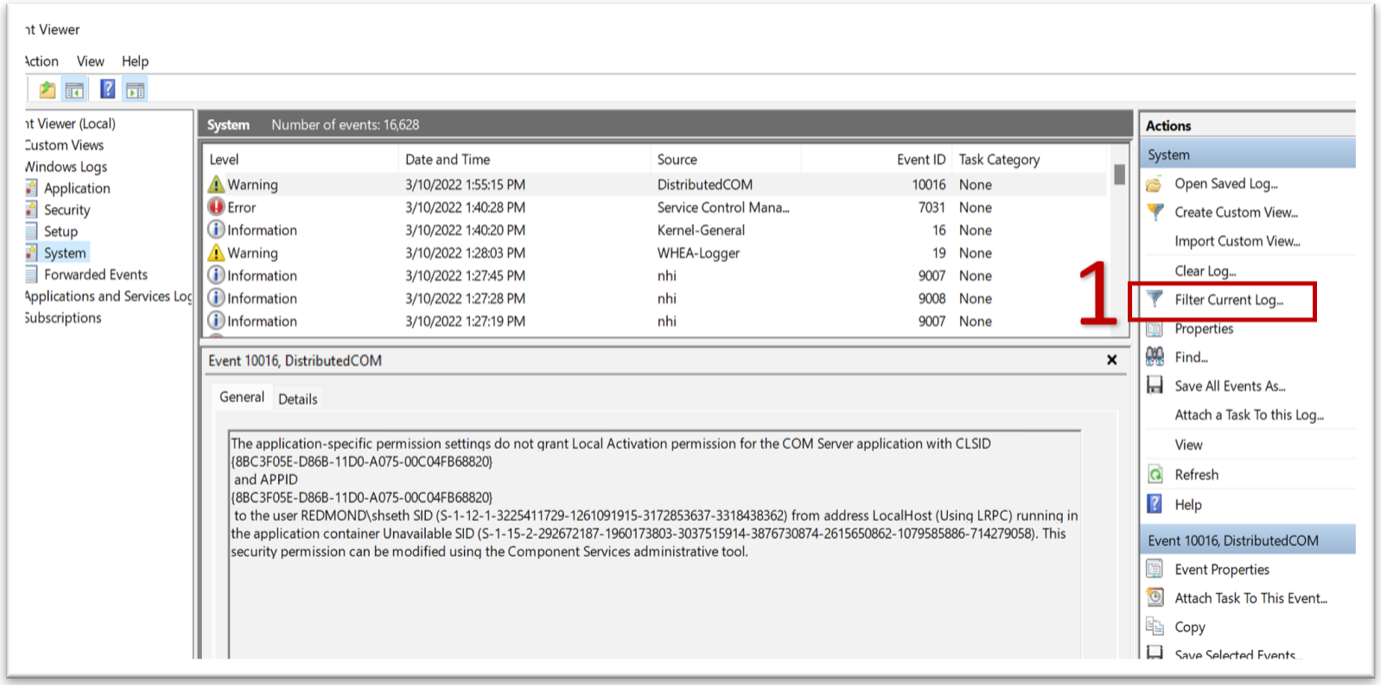
VM logging

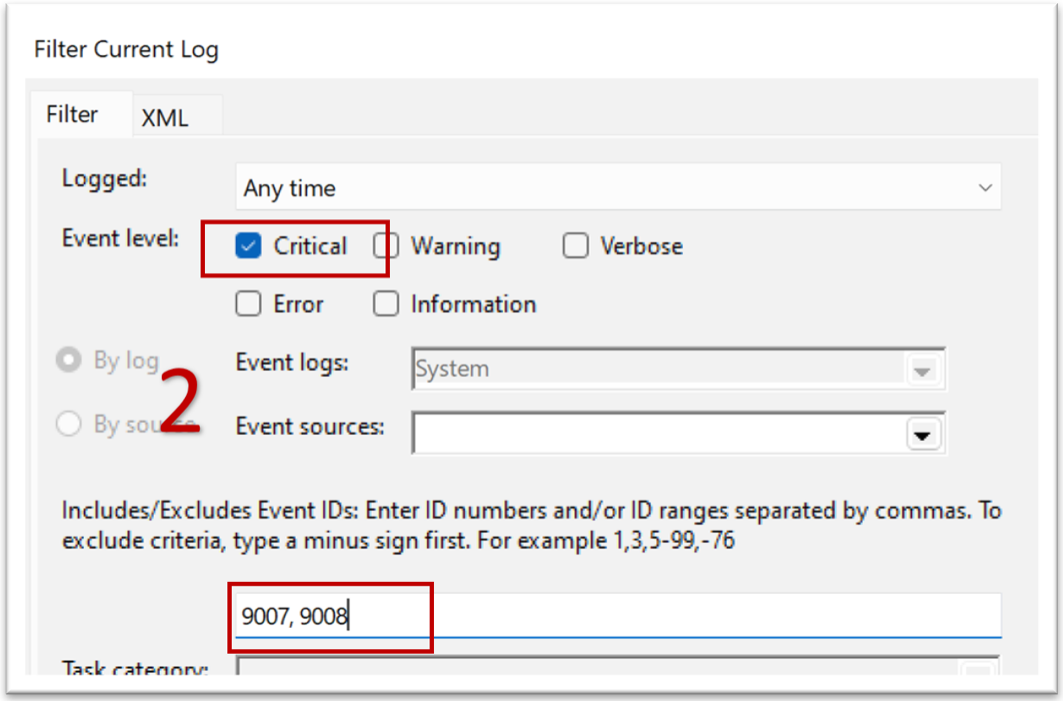


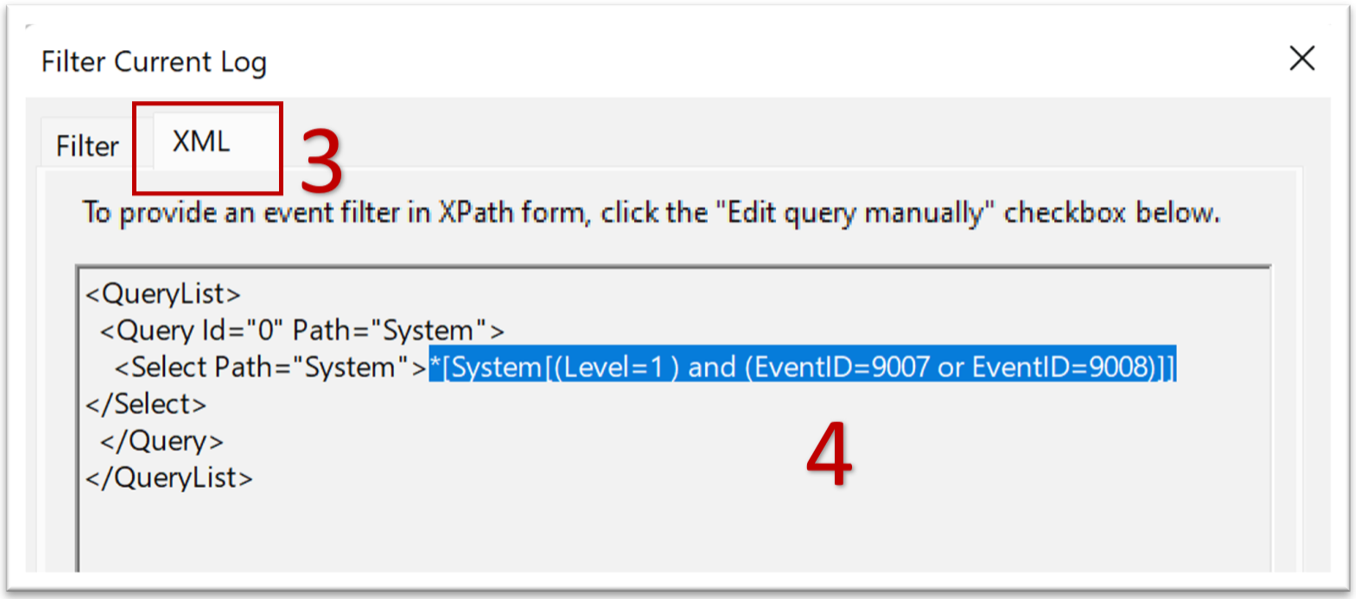
Event set	Collected event IDs
Minimal	1102, 4624, 4625, 4657, 4663, 4688, 4700, 4702, 4719, 4720, 4722, 4723, 4724, 4727, 4728, 4732, 4735, 4737, 4739, 4740, 4754, 4755, 4756, 4767, 4799, 4825, 4946, 4948, 4956, 5024, 5033, 8001, 8002, 8003, 8004, 8005, 8006, 8007, 8222
Common	1, 299, 300, 324, 340, 403, 404, 410, 411, 412, 413, 431, 500, 501, 1100, 1102, 1107, 1108, 4608, 4610, 4611, 4614, 4622, 4624, 4625, 4634, 4647, 4648, 4649, 4657, 4661, 4662, 4663, 4665, 4666, 4667, 4688, 4670, 4672, 4673, 4674, 4675, 4689, 4697, 4700, 4702, 4704, 4705, 4716, 4717, 4718, 4719, 4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4733, 4732, 4735, 4737, 4738, 4739, 4740, 4742, 4744, 4745, 4746, 4750, 4751, 4752, 4754, 4755, 4756, 4757, 4760, 4761, 4762, 4764, 4767, 4768, 4771, 4774, 4778, 4779, 4781, 4793, 4797, 4798, 4799, 4800, 4801, 4802, 4803, 4825, 4826, 4870, 4886, 4887, 4888, 4893, 4898, 4902, 4904, 4905, 4907, 4931, 4932, 4933, 4946, 4948, 4956, 4985, 5024, 5033, 5059, 5136, 5137, 5140, 5145, 5632, 6144, 6145, 6272, 6273, 6278, 6416, 6423, 6424, 8001, 8002, 8003, 8004, 8005, 8006, 8007, 8222, 26401, 30004

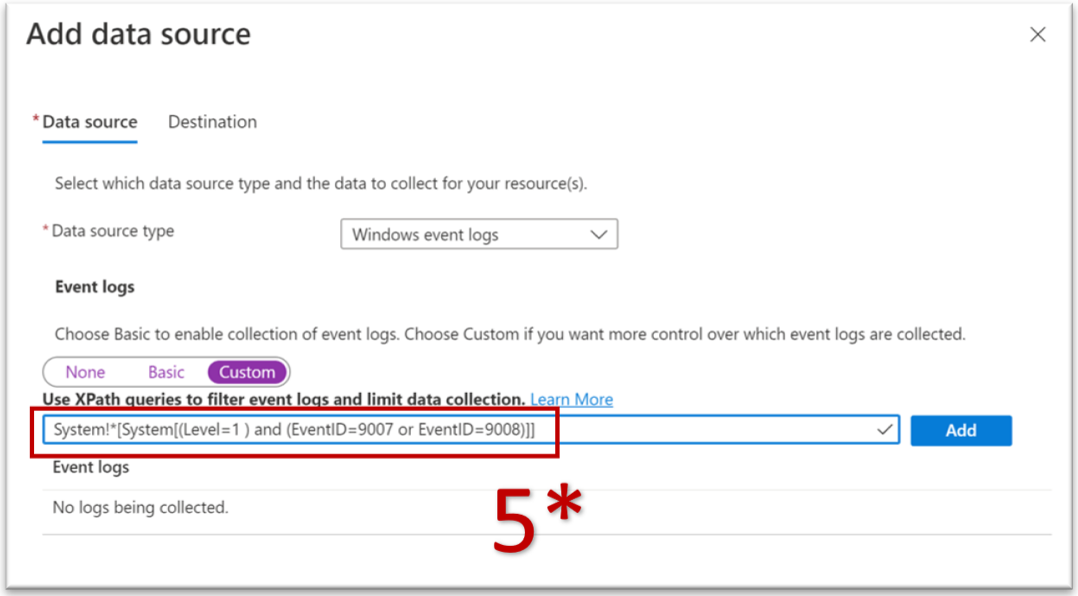


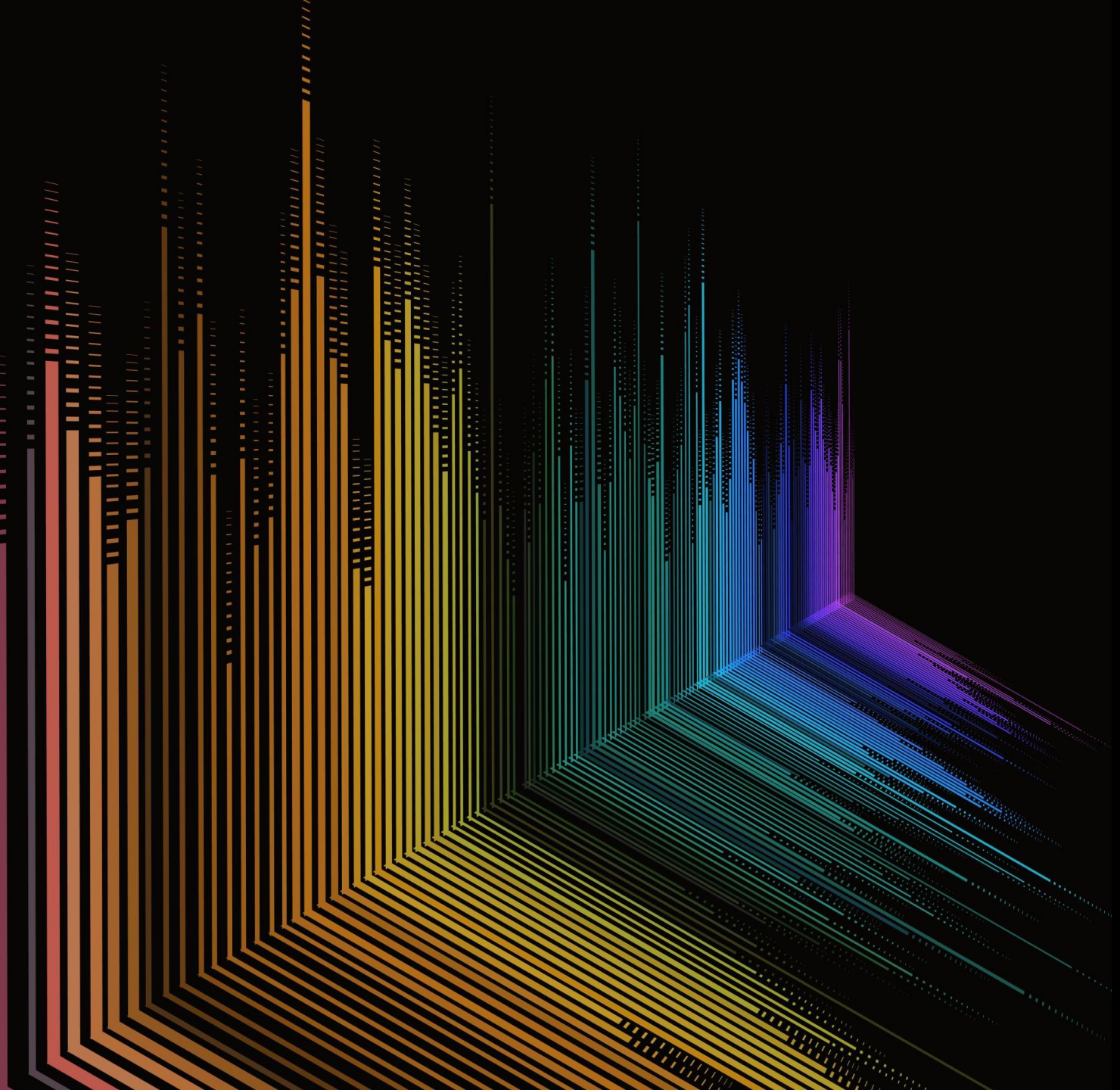
Demo


nt Viewer
Action View Help
nt Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Subscriptions
System Number of events: 16,628
Level Date and Time Source Event ID Task Category
Warning 3/10/2022 1:55:15 PM DistributedCOM 10016 None
Error 3/10/2022 1:40:28 PM Service Control Mana... 7031 None
Information 3/10/2022 1:40:20 PM Kernel-General 16 None
Warning 3/10/2022 1:28:03 PM WHEA-Logger 19 None
Information 3/10/2022 1:27:45 PM nhi 9007 None
Information 3/10/2022 1:27:28 PM nhi 9008 None
Information 3/10/2022 1:27:19 PM nhi 9007 None
1
Event 10016, DistributedCOM
General Details
The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
{8BC3F05E-D86B-11D0-A075-00C04FB68820}
and APPID
{8BC3F05E-D86B-11D0-A075-00C04FB68820}
to the user REDMOND\shseth SID (S-1-12-1-3225411729-1261091915-3172853637-3318438362) from address LocalHost (Using LRPC) running in the application container Unavailable SID (S-1-15-2-292672187-1960173803-3037515914-3876730874-2615650862-1079585886-714279058). This security permission can be modified using the Component Services administrative tool.
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 10016, DistributedCOM
Event Properties
Attach Task To This Event...
Copy
Save Selected Events


Filter Current Log
Filter
XML
Logged:
Any time
Event level:
Critical
Warning
Verbose
Error
Information
By log
By sou
2
Event logs:
System
Event sources:
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
9007, 9008
Task category:


Filter Current Log
Filter
XML
3
To provide an event filter in XPath form, click the "Edit query manually" checkbox below.
<QueryList>
<Query Id="0" Path="System">
<Select Path="System">*[System[(Level=1) and (EventID=9007 or EventID=9008)]]
</Select>
</Query>
</QueryList>
4


Add data source
*Data source
Destination
Select which data source type and the data to collect for your resource(s).
*Data source type
Windows event logs
Event logs
Choose Basic to enable collection of event logs. Choose Custom if you want more control over which event logs are collected.
None
Basic
Custom
Use XPath queries to filter event logs and limit data collection. Learn More
System!*[System[(Level=1) and (EventID=9007 or EventID=9008)]]
Add
Event logs
No logs being collected.
5*



Security Copilot

kostkontroll

Commitments tiers

Pay-as-you-go
Per GB

The Pay-as-you-go pricing tier offers flexible consumption pricing in which you are charged per GB of data ingested. This only includes estimated costs from data ingestion to aid selecting the optimal pricing.

Estimated costs

Item type	Price	Monthly usage (last 31 days)	Estimated monthly data ingestion cost
Analytics Logs data ingestion	30.04 SEK	5640.78 GB	169,449.17 SEK
Basic Logs data ingestion	6.53 SEK	0.00 GB	0.00 SEK
Microsoft Defender allowance	0.00 US$	0.00 GB	0.00 US$
Total			**169,449.17 SEK**

(These estimated costs do not include Microsoft Defender costs. The Microsoft Defender 500 MB/node/day data allowance is factored into the estimate of Log Analytics billing. Learn more.)

Due to the commitment period in another pricing tier, this tier cannot be selected until Mon, 04 Dec 2023 12:42:03 GMT.

Select

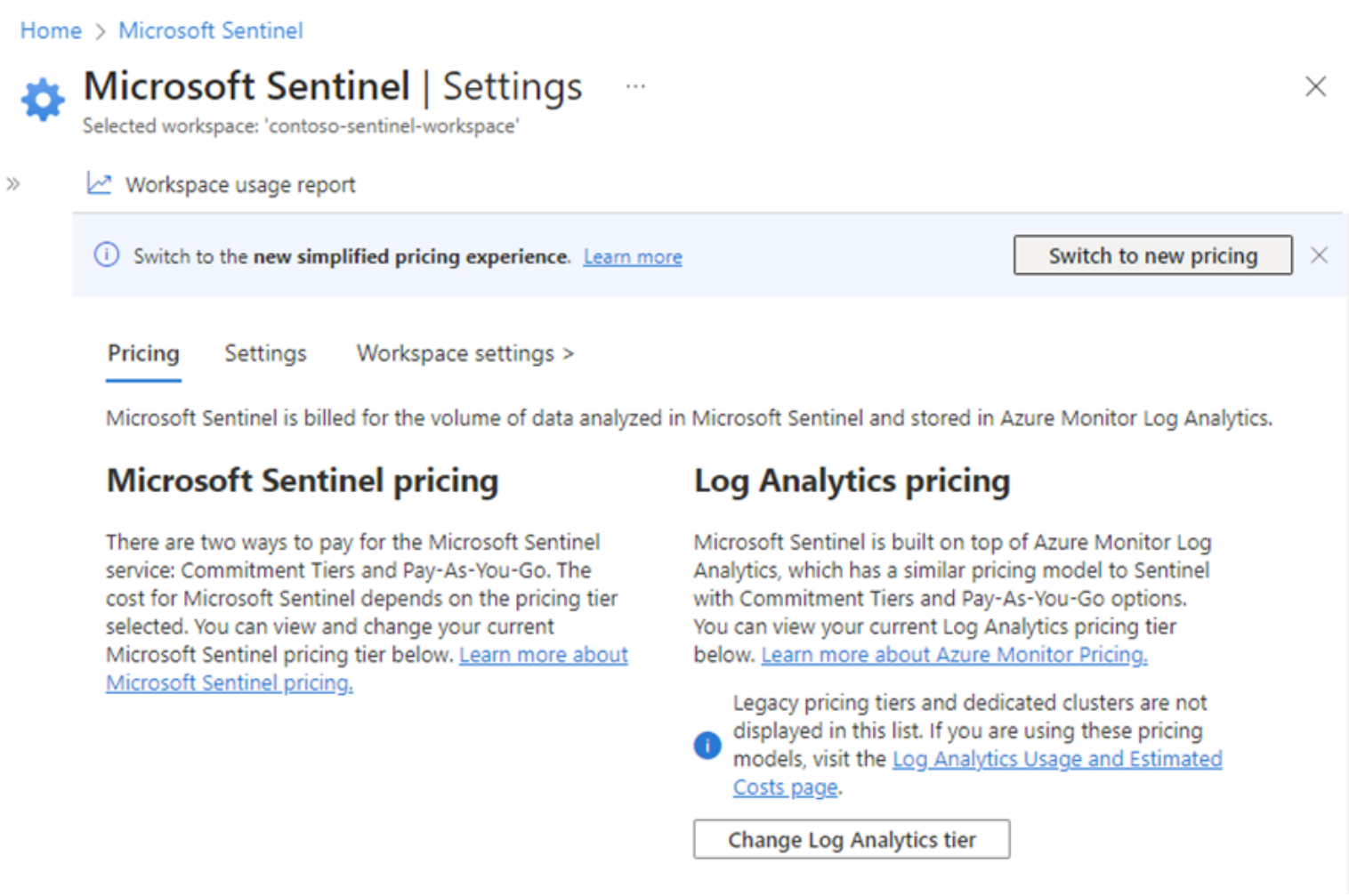
100 GB/day Commitment Tier
15.44% discount over Pay-as-you-go

The 100 GB/day Commitment Tier tier provides you with a fixed predictable fee with a 15.44% discount over the Pay-as-you-go pricing. Data ingested above the Commitment Tier (overage) is billed at the pro-rated per GB rate of this tier. This only includes estimated costs from data ingestion to aid selecting the optimal pricing.

Estimated costs

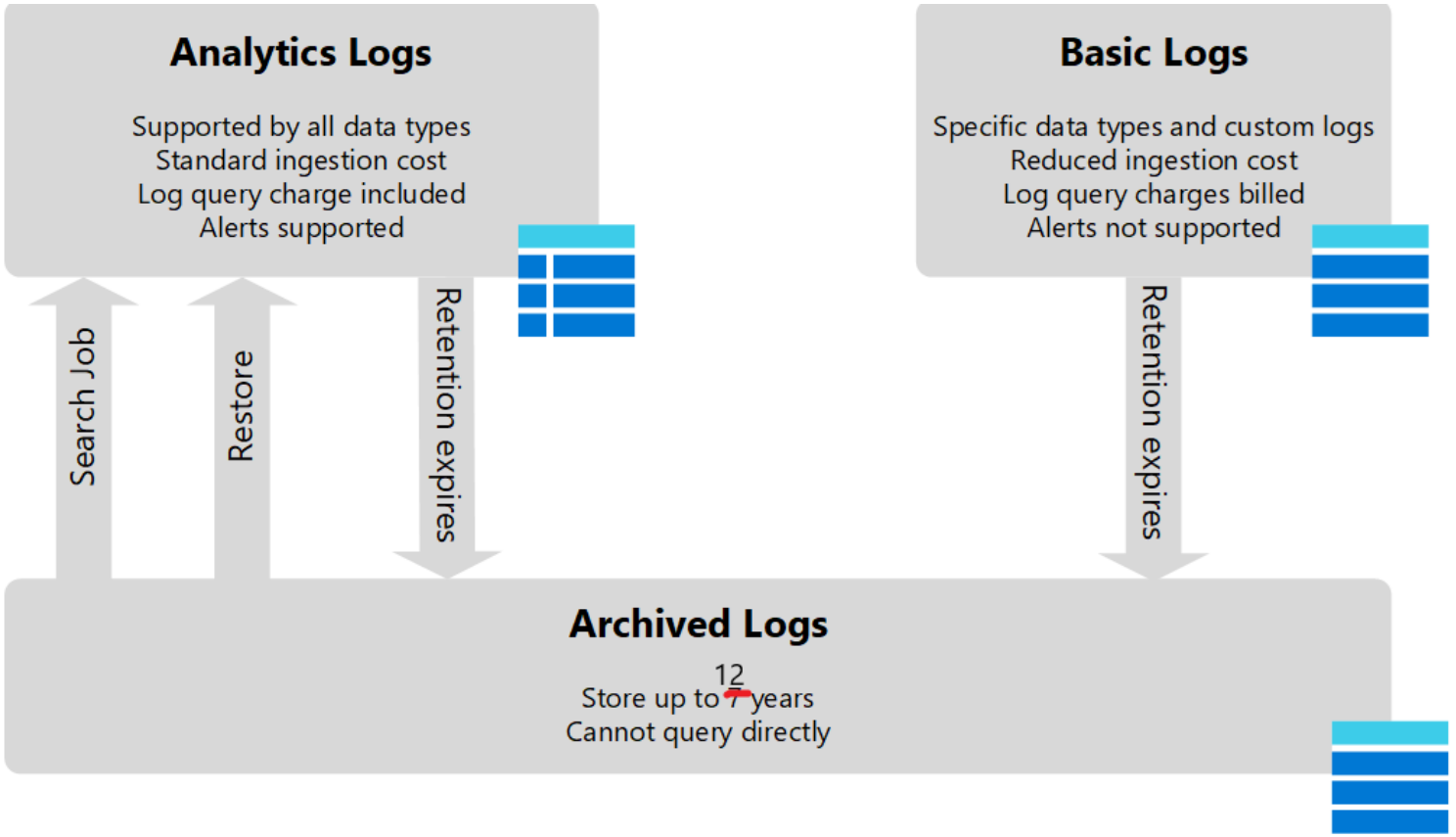
Item type	Price	Monthly usage (last 31 days)	Estimated monthly data ingestion cost
100 GB/day Commitment Tier	2,540.32 SEK/day	31 days	78,749.92 SEK
Basic Logs data ingestion	6.53 SEK	0.00 GB	0.00 SEK
Microsoft Defender allowance	0.00 US$	0.00 GB	0.00 US$
Overage	25.40 SEK/GB	2474.52 GB	62,860.78 SEK
Total			**141,610.70 SEK**

Ny prismodell




```
"properties":
{"workspaceResourceId":"/subscriptions/{SubscriptionId}/resourcegroups/{ResourceGroup}/providers/
microsoft.operationalinsights/workspaces/{YourWorkspaceName}",
"sku": {
        "name": "Unified" }
    }
```

Logtyper I Sentinel

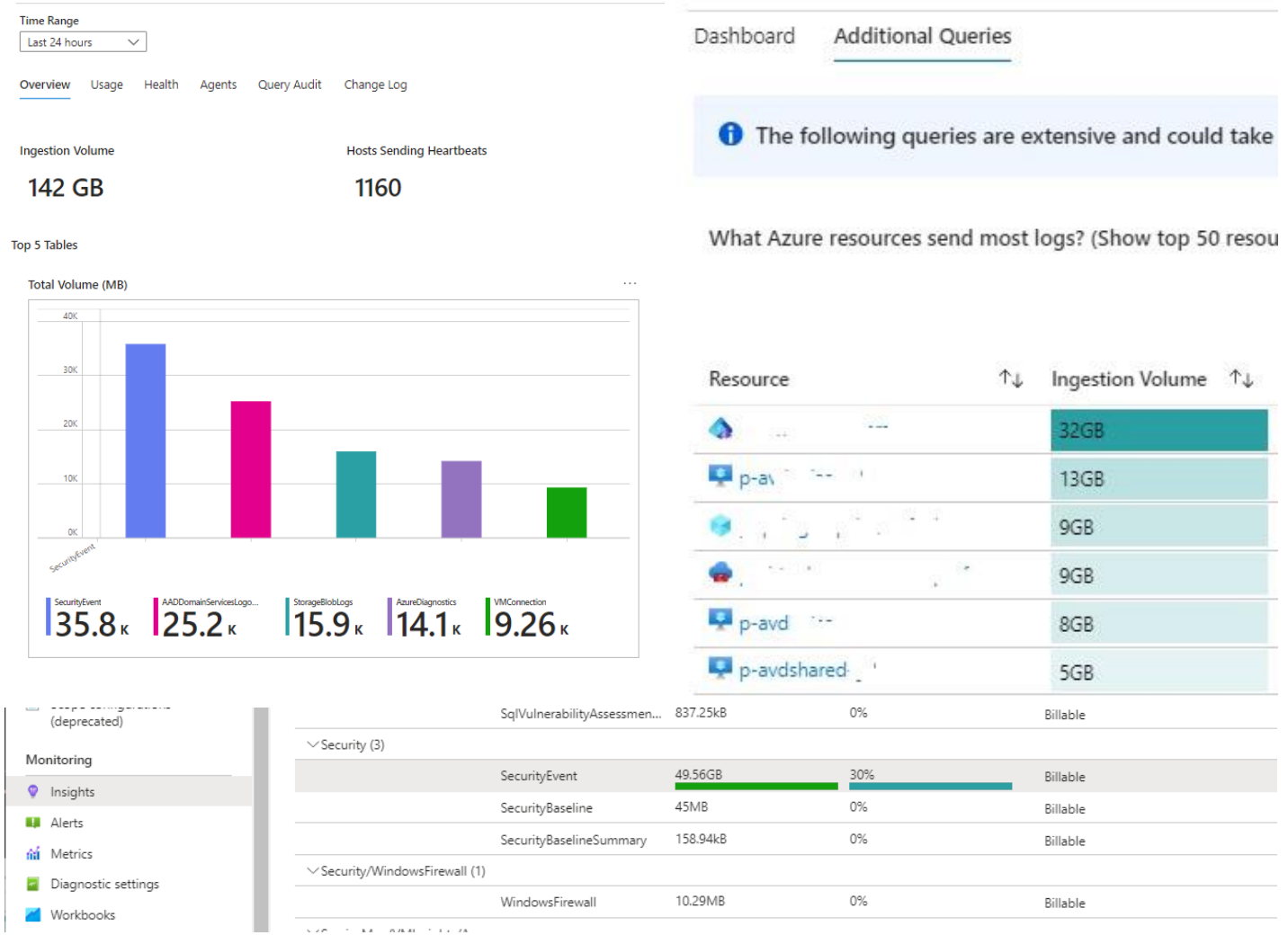


Gratis datakilder

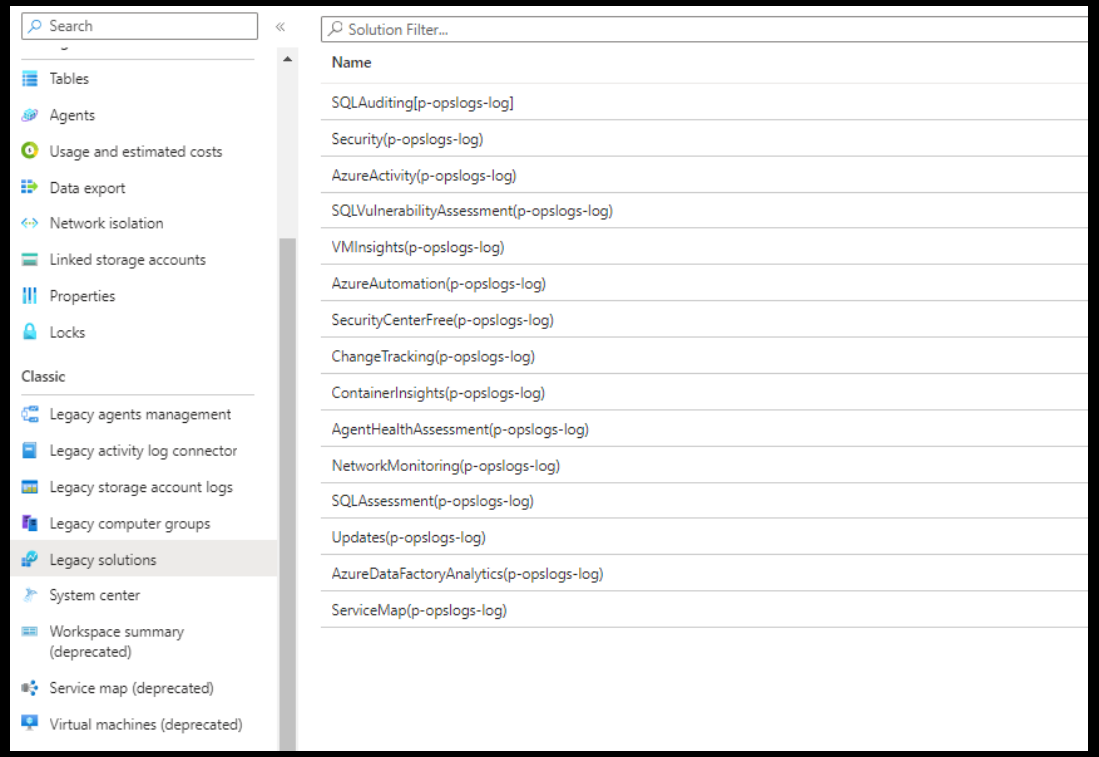
Microsoft Sentinel data connector	Free data type
Azure Activity Logs	AzureActivity
Microsoft Entra ID Protection	SecurityAlert (IPC)
Office 365	OfficeActivity (SharePoint)
	OfficeActivity (Exchange)
	OfficeActivity (Teams)
Microsoft Defender for Cloud	SecurityAlert (Defender for Cloud)
Microsoft Defender for IoT	SecurityAlert (Defender for IoT)
Microsoft 365 Defender	SecurityIncident
	SecurityAlert
Microsoft Defender for Endpoint	SecurityAlert (MDATP)
Microsoft Defender for Identity	SecurityAlert (AATP)
Microsoft Defender for Cloud Apps	SecurityAlert (Defender for Cloud Apps)

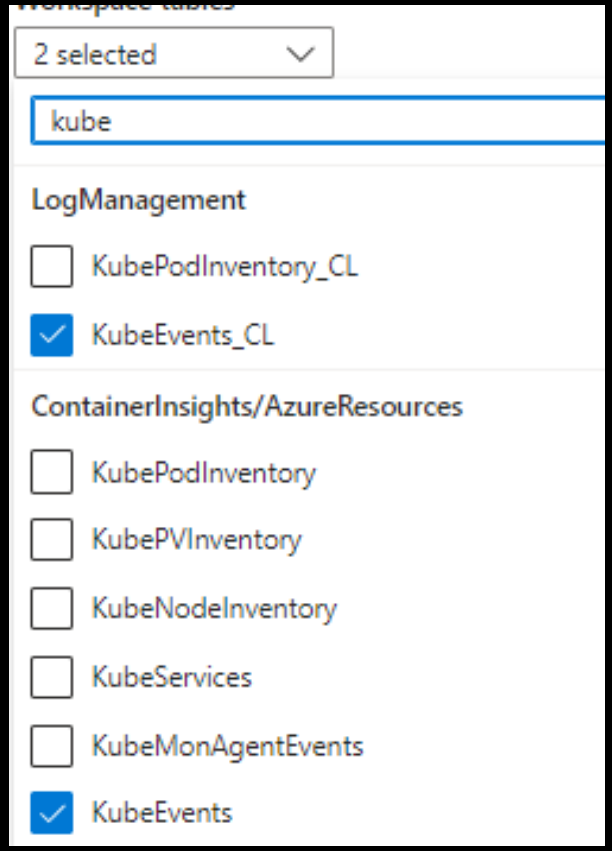
Although alerts are free, the raw logs for some Microsoft 365 Defender, Defender for Cloud Apps, Microsoft Entra ID, and Azure Information Protection (AIP) data types are paid.

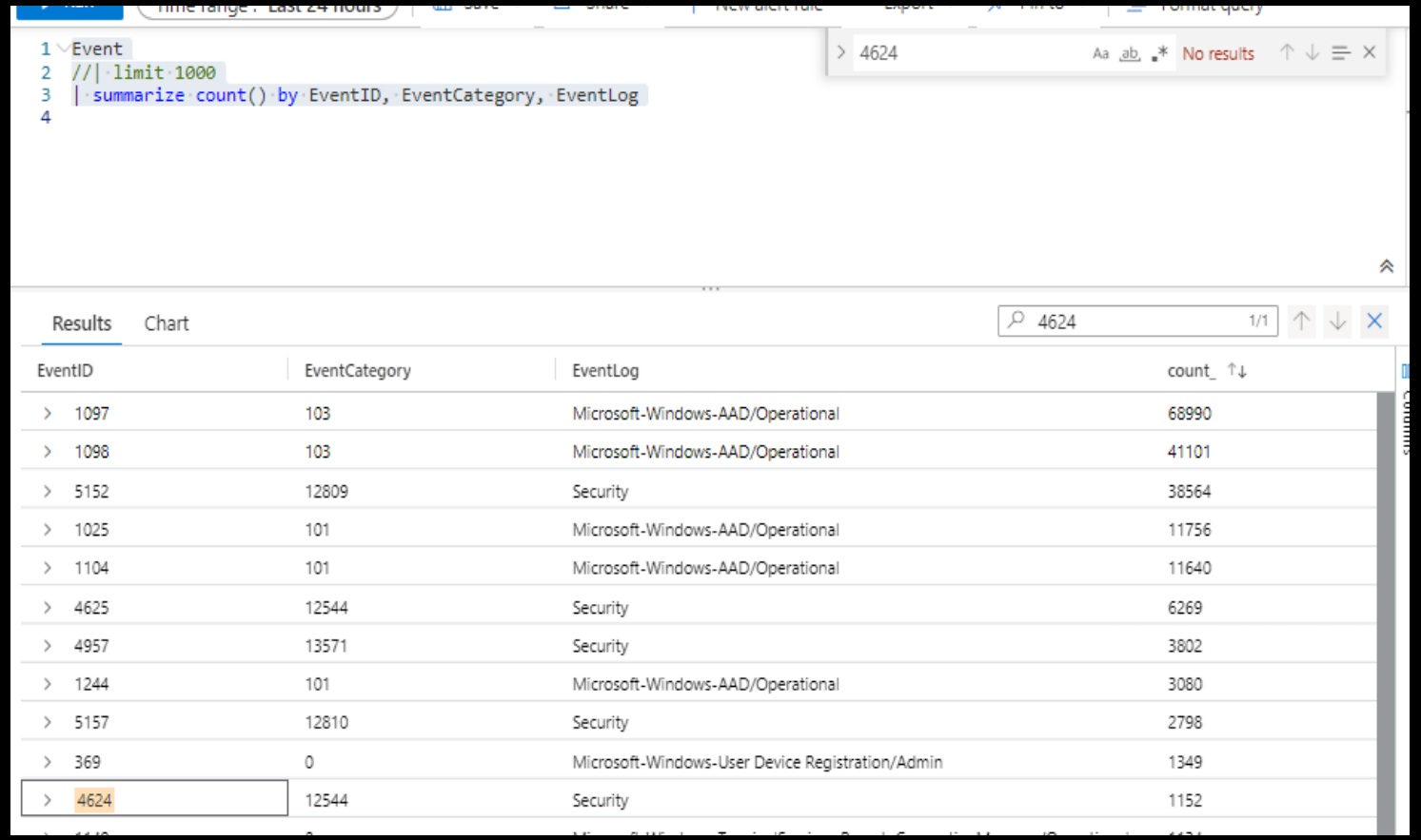
Exempel med innebygde verktøy



Dual logging setup with legacy solutions:

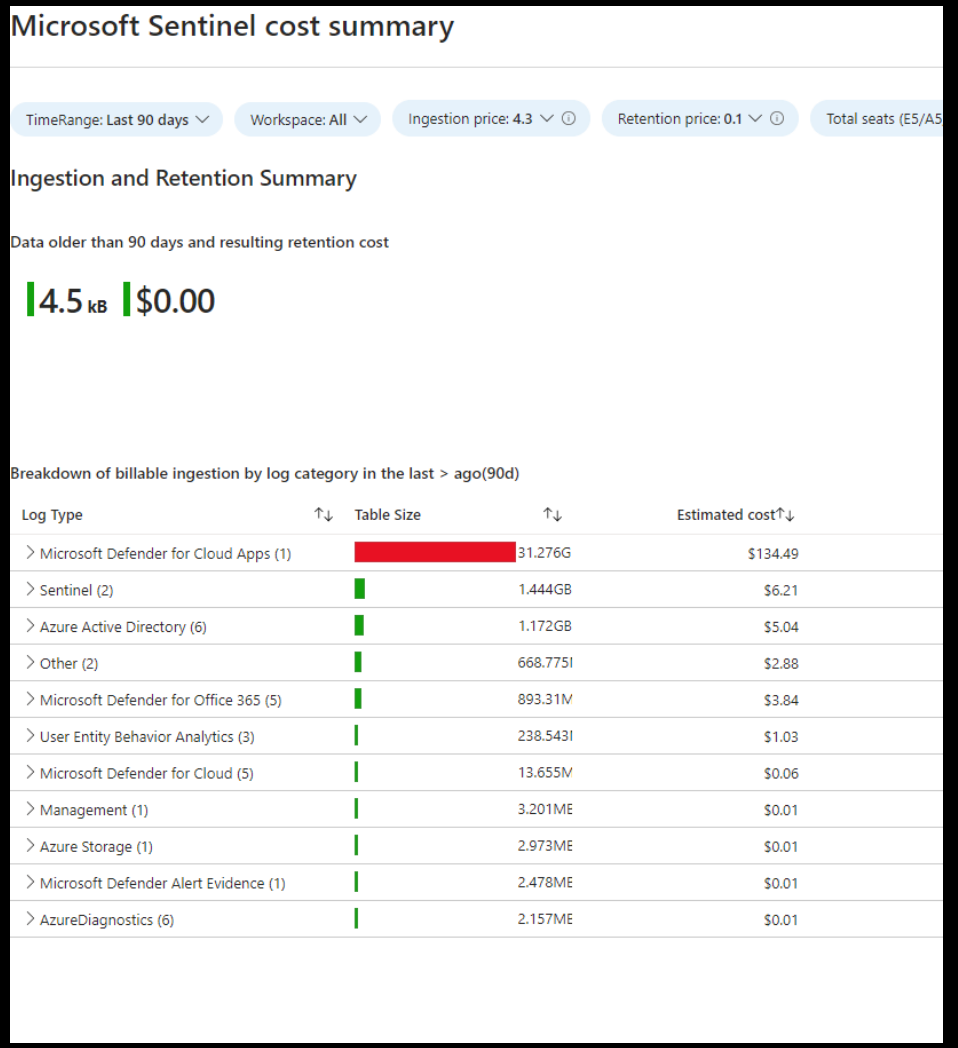






Security solution vs eventlog in AMA

Workbooks

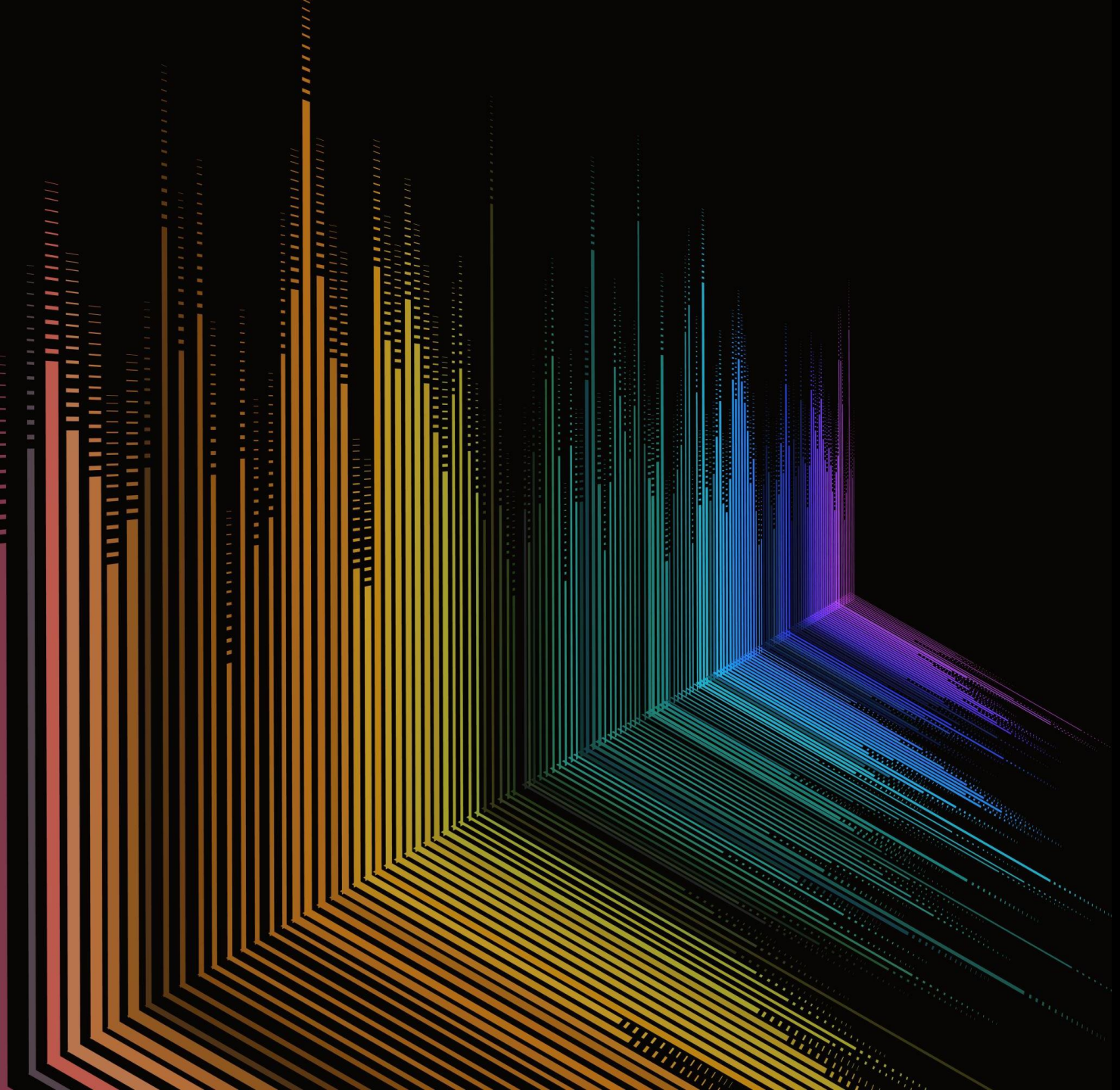

Microsoft Sentinel cost summary
TimeRange: Last 90 days
Workspace: All
Ingestion price: 4.3
Retention price: 0.1
Total seats (E5/A5
Ingestion and Retention Summary
Data older than 90 days and resulting retention cost
4.5 kB
$0.00
Breakdown of billable ingestion by log category in the last > ago(90d)
Log Type
Table Size
Estimated cost
Microsoft Defender for Cloud Apps (1) 31.276G $134.49
Sentinel (2) 1.444GB $6.21
Azure Active Directory (6) 1.172GB $5.04
Other (2) 668.775I $2.88
Microsoft Defender for Office 365 (5) 893.31M $3.84
User Entity Behavior Analytics (3) 238.543I $1.03
Microsoft Defender for Cloud (5) 13.655M $0.06
Management (1) 3.201ME $0.01
Azure Storage (1) 2.973ME $0.01
Microsoft Defender Alert Evidence (1) 2.478ME $0.01
AzureDiagnostics (6) 2.157ME $0.01

Elementer for kostnadskontroll

- commitments tiers
- design av workspaces
- archive,basic, analytics logs
- daily cap
- retention
- regelmessig analyse
- Cost workbooks, **Microsoft Sentinel Cost**
- Kostnad av analytics queries

Sentinel Content (preview)

Hvorfor bruke tid på dette?



Sentinel innhold som kode demo

The process

Accelerated Cloud Enabler
by devoteam M Cloud

Analysis

The first step is analyzing your security requirements and priorities. All our experts are opinionated advisors. Therefore, after the analysis, we will have a clear idea of what Azure Sentinel features and designs a company like yours needs – and a clear idea of what you don't need.

Workshops

With ACE SIEM, our goal is not only to provide a state-of-the-art security operation. Through collaborative sprints and workshops, Devoteam ensures that our customers can operate and adjust their SIEM system in-house.

Implementation

Based on a collaborative process, ACE SIEM works alongside you and your IT security team to get you onboarded and operating – fast. Devoteam has created a set of readily deployable, validated designs and design decisions, saving you a lot of time and deliberation. We provide a scalable and cost-effective set of rules, workbooks, and automation tasks for Azure Sentinel.

devoteam
M Cloud

ACE SIEM

Accelerated Cloud Enabler
by devoteam M Cloud

100+ design decisions

60+ Azure policy controls

100+ Sentinel artifacts

Assessment

Through thorough analysis, we have a clear idea of what Azure Sentinel features and design an organization like your needs.

Implementation

Devoteam provides a scalable and cost-effective set of rules, workbooks and automation tasks for Azure Sentinel.

Workshops

Devoteam ensures that our customers can operate and adjust their SIEM system in-house.

Operations

ACE SIEM gives analysts and security operators what they need to perform security tasks and automate security responses.

Design

ACE SIEM delivers sets of readily deployable, validated designs and design decisions.

devoteam
M Cloud

The outcome

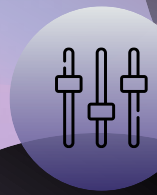
Accelerated Cloud Enabler
by devoteam M Cloud

Acceleration

ACE SIEM is faster to deploy and configure than comparable solutions available on the market today. In 8 to 12 weeks, we design, deploy and adjust a cost-effective and scalable cloud security operation for your enterprise needs. Devoteam delivers great results quickly by building solutions on enterprise-ready rules, workbooks, and automation tasks.

Competence

Through sprints and workshops, we give your organization a thorough introduction to every part of your SIEM solution. We transform your digital infrastructure and strengthen the organization's digital competency, enabling you to operate securely and confidently in the cloud.



Control

With ACE SIEM, you can be confident that your security and compliance requirements are met. By building solutions on infrastructure as code (IaC) principles, you also reduce the risk of human errors to an absolute minimum. Maximising the system's capacity makes it easier for you to devote time, focus, and resources to running your business.

Cost

ACE SIEM provides cost control and helps your company cut costs. We do this by deploying ready-made, battle-tested solutions for your Azure Sentinel needs. By enabling our clients to maintain and run their systems themselves, while also developing their internal IT resources, you get an increased return on your investment.

devoteam
M Cloud

devoteam
M Cloud

Takk

Accelerated
Cloud Enabler
by devoteam M Cloud

Creative Tech for Better Change