Microsoft Security

Microsoft Sentinel

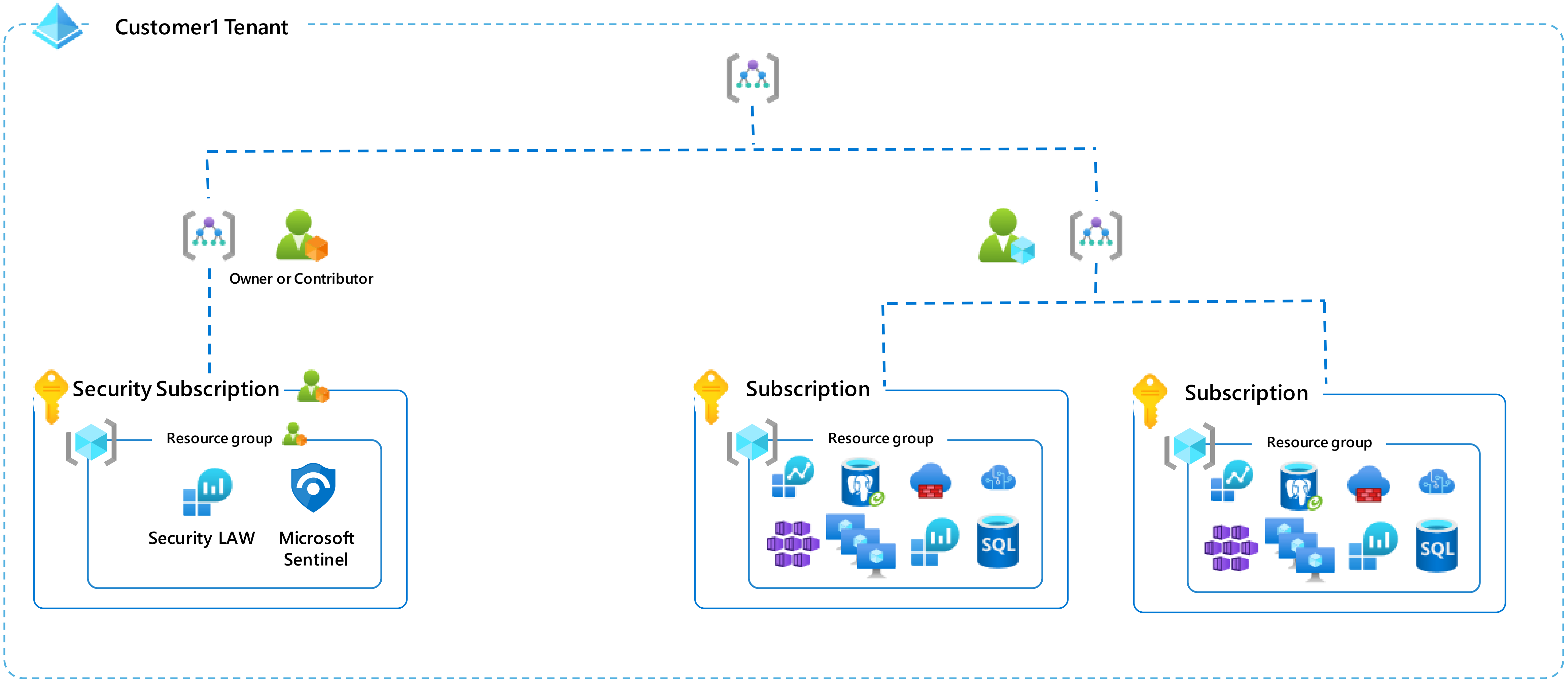
Angelica Faber

Agenda

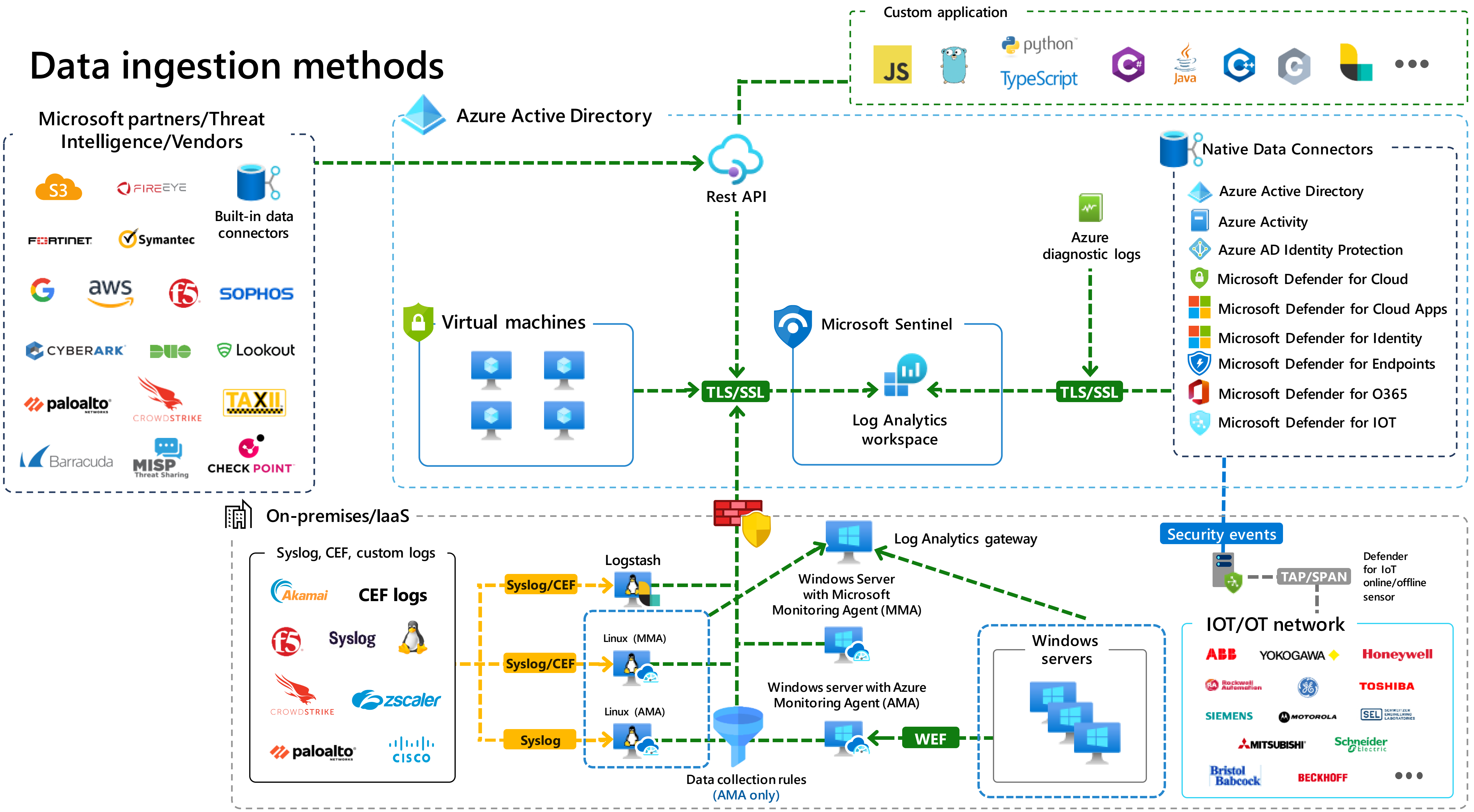
- Quick MSSP Architecture Review
- Demo
  - Sentinel All In One
  - Content Hub & Connectors & Workbooks
  - Data Storage Options & Search
  - Watchlists & Analytic Rules & Anomalies
  - UEBA & Threat Intelligence
  - Repositories & Workspace Manager
  - Incident Investigations & Fusion
  - Automation:
    - Microsoft Sentinel Triage AssistanT (STAT)
    - Integrations with OpenAI

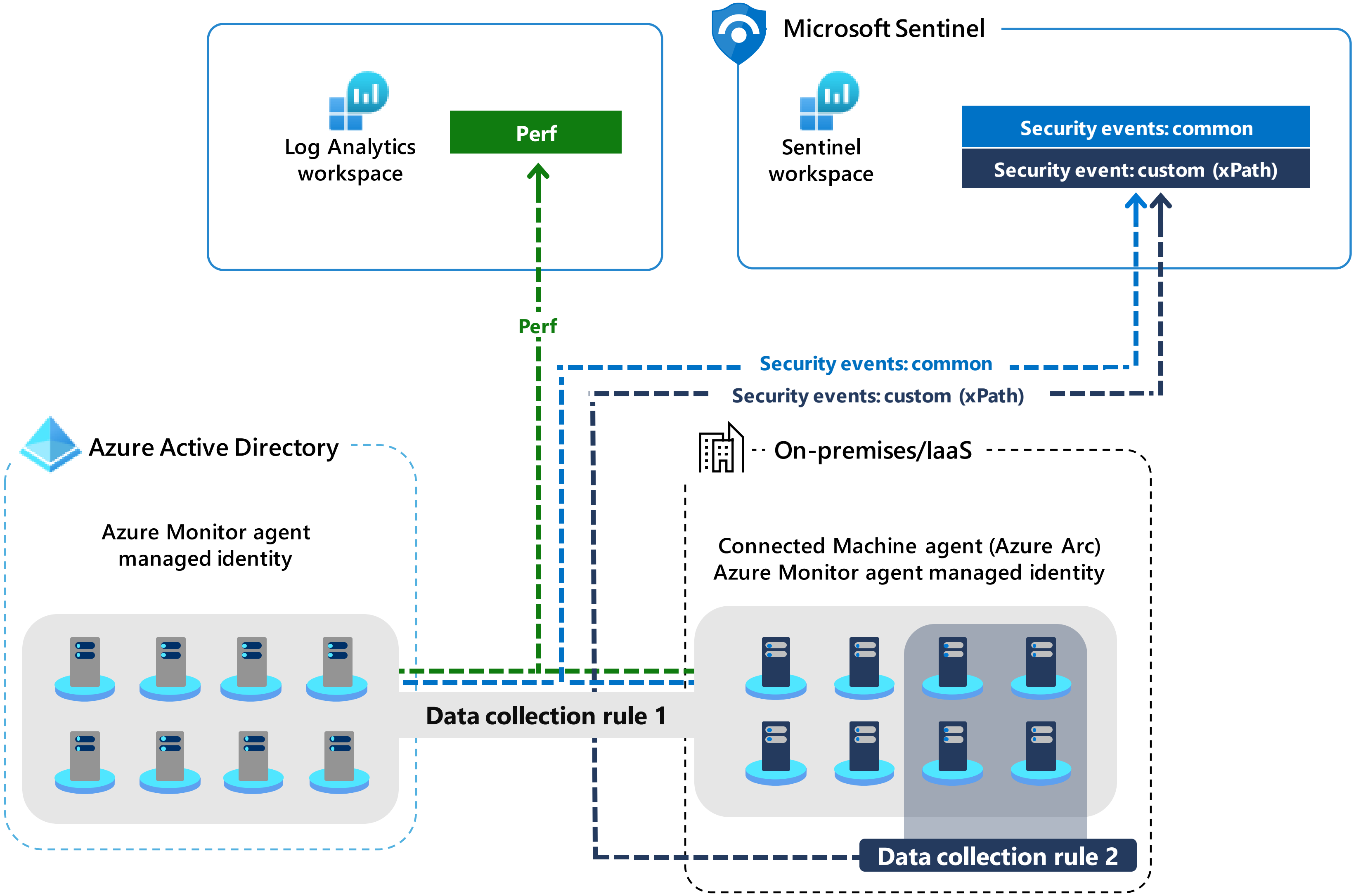
https://aka.ms/SentinelLinks

https://myfabersecurity.com/


Customer1 Tenant
Owner or Contributor
Security Subscription
Resource group
Security LAW
Microsoft Sentinel
Subscription
Resource group
SQL
Subscription
Resource group
SQL

Data ingestion methods





Data collection rule 1

Streams:

- Security events: Common
- Perf

Destinations:

- Microsoft Sentinel workspace
- Log Analytics workspace

Flows:

- Security events > Microsoft Sentinel workspace
- Perf > Log Analytics workspace

Data collection rule 2

Streams:

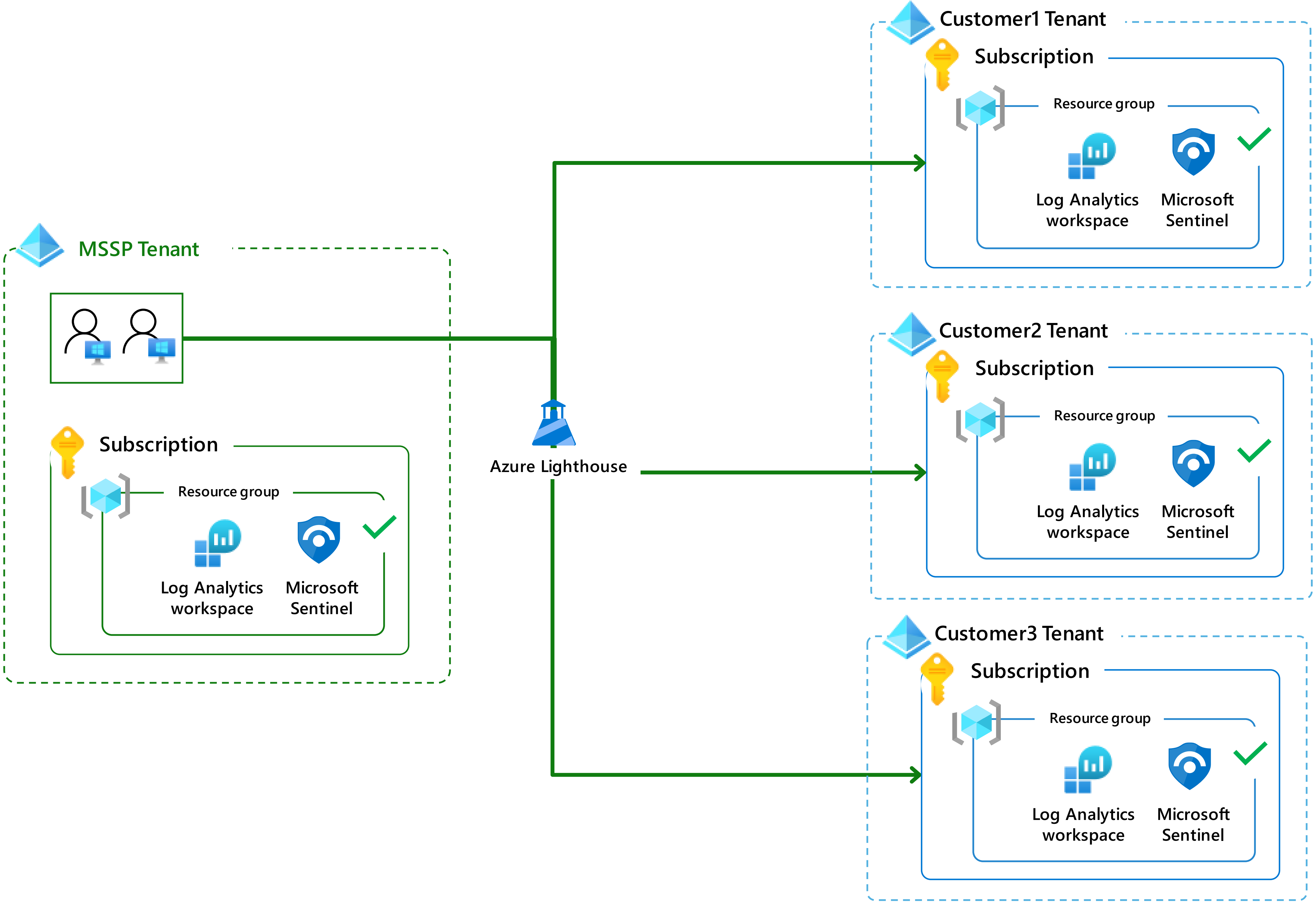
- Security events: custom xPath

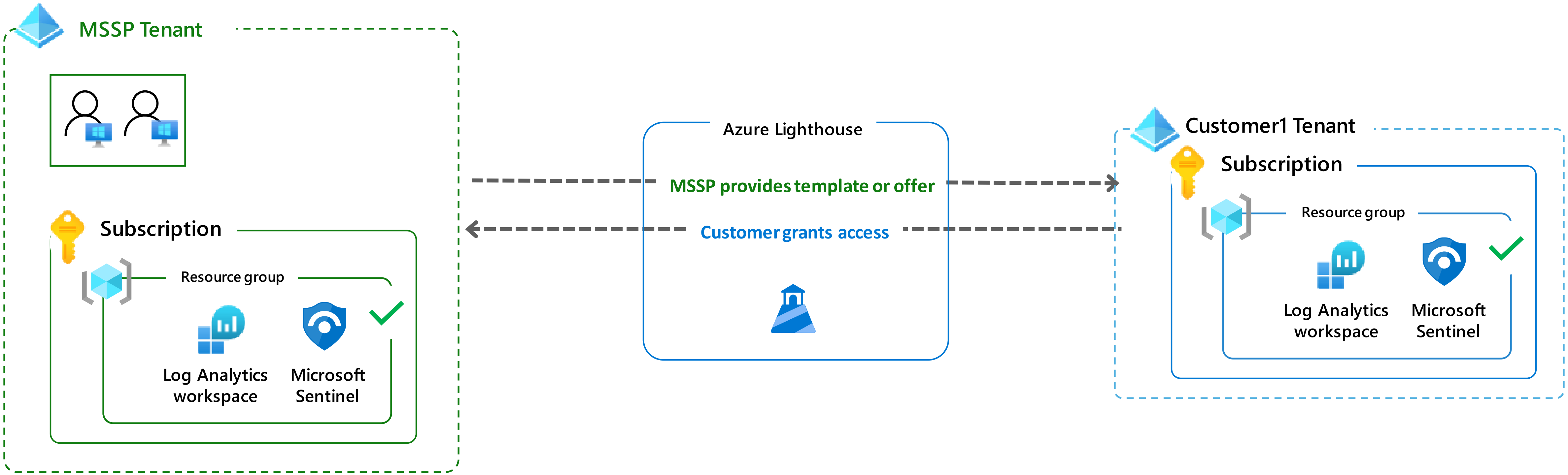
Destinations:

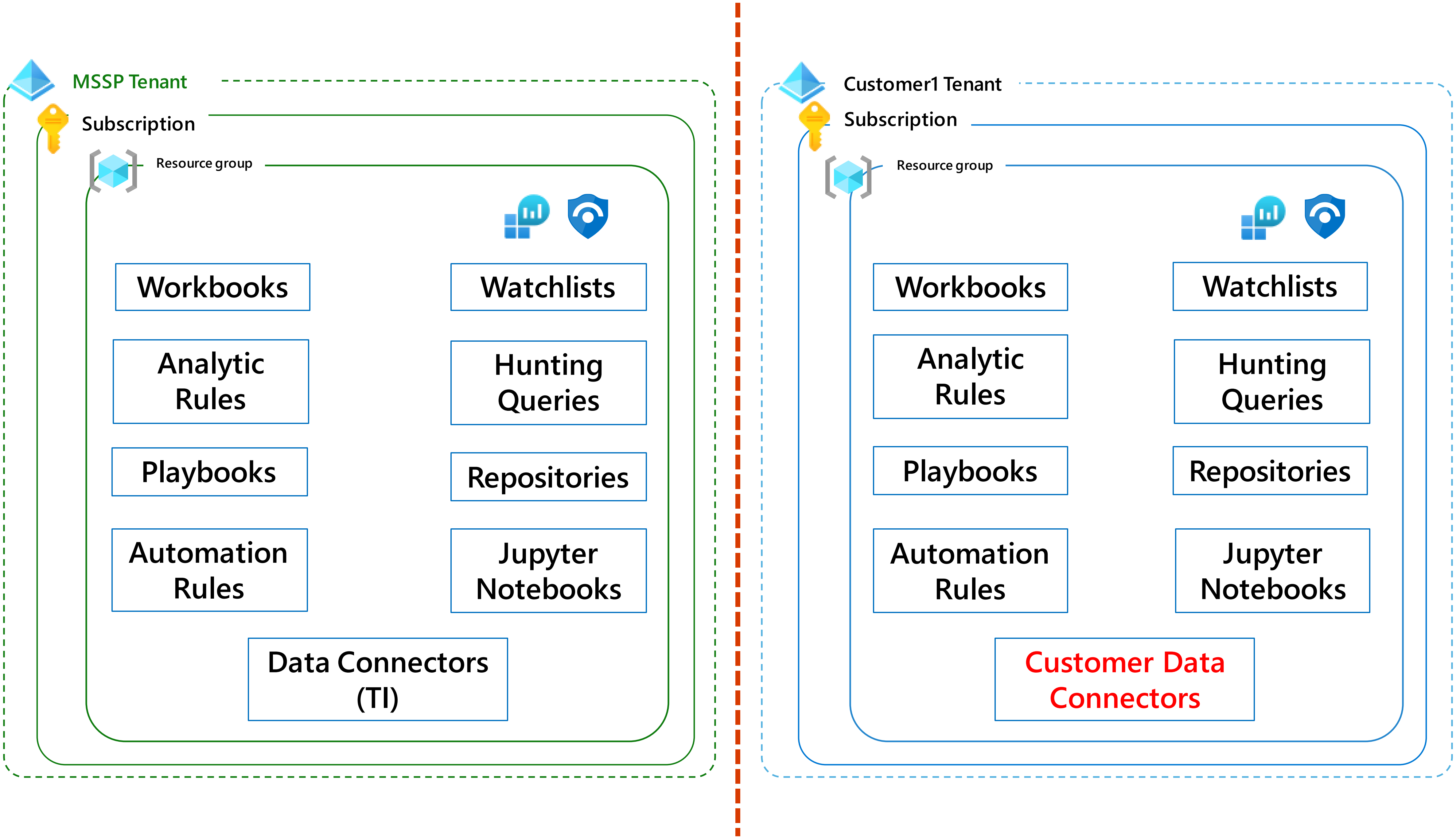
- Microsoft Sentinel workspace

Flows:

- Security events > Microsoft Sentinel workspace


Customer1 Tenant
Subscription
Resource group
Log Analytics workspace
Microsoft Sentinel
MSSP Tenant
Customer2 Tenant
Subscription
Resource group
Log Analytics workspace
Microsoft Sentinel
Subscription
Resource group
Log Analytics workspace
Microsoft Sentinel
Azure Lighthouse
Customer3 Tenant
Subscription
Resource group
Log Analytics workspace
Microsoft Sentinel

MSSP Tenant
Subscription
Resource group
Log Analytics workspace
Microsoft Sentinel
Azure Lighthouse
MSSP provides template or offer
Customer grants access
Customer1 Tenant
Subscription
Resource group
Log Analytics workspace
Microsoft Sentinel



MSSP Tenant

Subscription

Resource group

Workbooks

Watchlists

Analytic Rules

Hunting Queries

Playbooks

Repositories

Automation Rules

Jupyter Notebooks

Data Connectors (TI)

Customer1 Tenant

Subscription

Resource group

Workbooks

Watchlists

Analytic Rules

Hunting Queries

Playbooks

Repositories

Automation Rules

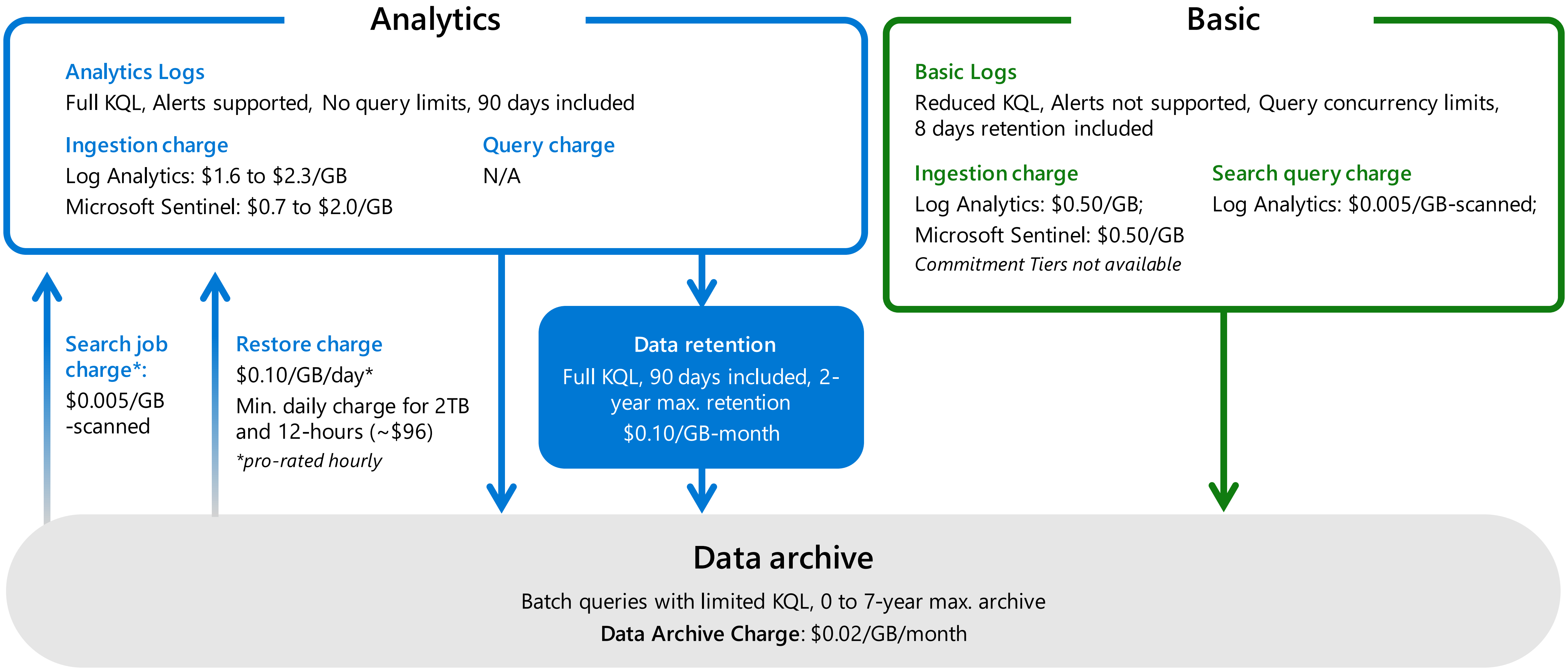
Jupyter Notebooks

Customer Data Connectors

DEMO

Storage Options

	Analytics	Basic	Archive	Azure Blob Storage	Azure Data Explorer
Performance	High	Medium	Medium	Medium to Low	High to Low (2)
Maximum retention	Two years	8 days	7 years	99 years	Unlimited
Cloud model	SaaS	SaaS	SaaS	PaaS	PaaS
Estimated cost	High	Low	Low	Medium	Medium to Low (2)
Purpose	SecOps	Debugging, verbose logs. Not to generate alerts. Limited KQL.	Archive, compliance, auditing	Archive, compliance, auditing	Extended threat hunting, compliance, trend analysis, storage of non-security data, audit.
Usability	Great	Great	Low	High	Good



Analytics

Analytics Logs

Full KQL, Alerts supported, No query limits, 90 days included

Ingestion charge

Log Analytics: $1.6 to $2.3/GB

Microsoft Sentinel: $0.7 to $2.0/GB

Query charge

N/A

Search job charge*:

$0.005/GB -scanned

Restore charge

$0.10/GB/day*

Min. daily charge for 2TB and 12-hours (~$96)

pro-rated hourly

Data retention

Full KQL, 90 days included, 2-year max. retention

$0.10/GB-month

Basic

Basic Logs

Reduced KQL, Alerts not supported, Query concurrency limits,
8 days retention included

Ingestion charge

Log Analytics: $0.50/GB;

Microsoft Sentinel: $0.50/GB

Commitment Tiers not available

Search query charge

Log Analytics: $0.005/GB-scanned;

Data archive

Batch queries with limited KQL, 0 to 7-year max. archive

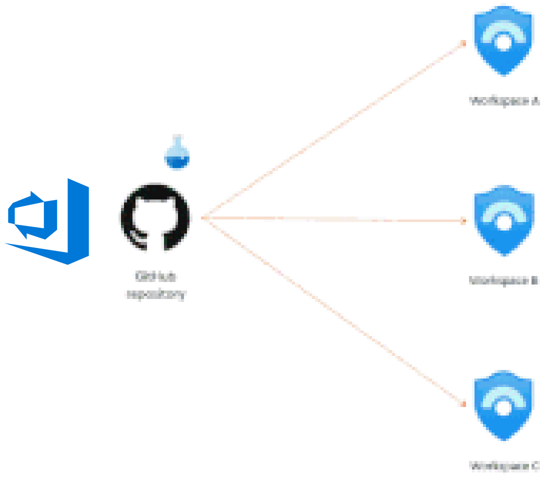
Data Archive Charge: $0.02/GB/month

DEMO

Sentinel Repositories (Preview)

- Supports GitHub and Azure DevOps
- Automated Content Management
- ARM template format

- Content Types:
  - Analytic rules
  - Automation rules
  - Hunting queries
  - Parsers
  - Playbooks
  - Workbooks

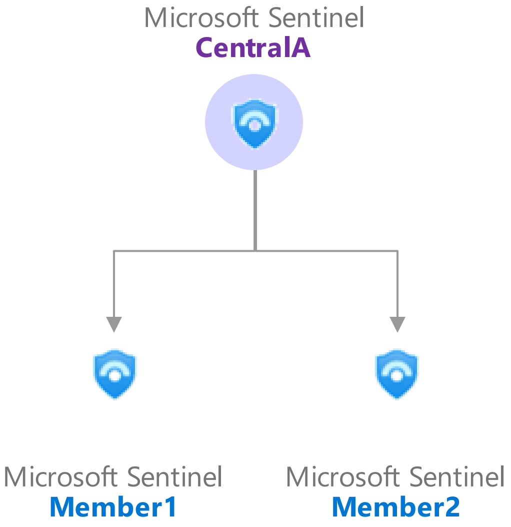


Possible Workspace Manager Architectures

Content Management

- Analytics rules
- Automation rules (excluding Playbooks)
- Parsers, Saved Searches and Functions
- Hunting and Livestream queries
- Workbooks

Simple / Direct-Link

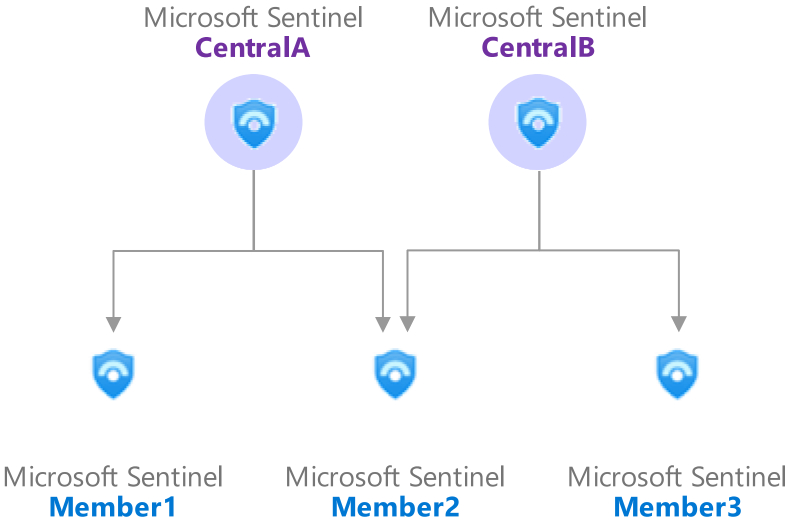


Microsoft Sentinel
CentralA

Microsoft Sentinel
Member1

Microsoft Sentinel
Member2

Co-Management



Microsoft Sentinel
CentralA

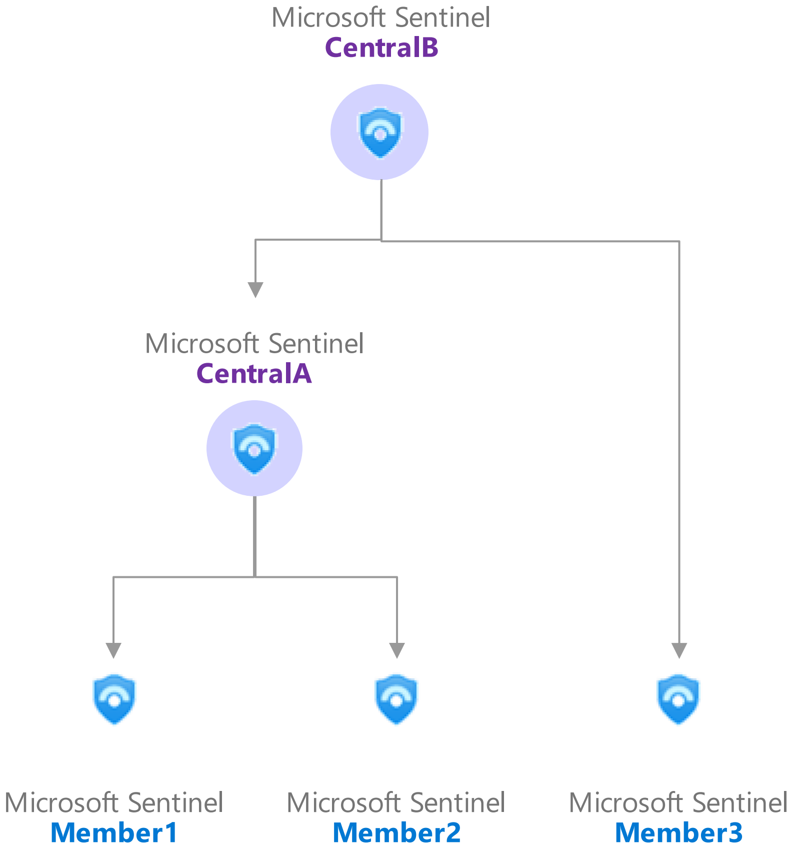
Microsoft Sentinel
CentralB

Microsoft Sentinel
Member1

Microsoft Sentinel
Member2

Microsoft Sentinel
Member3

N-Tier



Microsoft Sentinel
CentralB

Microsoft Sentinel
CentralA

Microsoft Sentinel
Member1

Microsoft Sentinel
Member2

Microsoft Sentinel
Member3

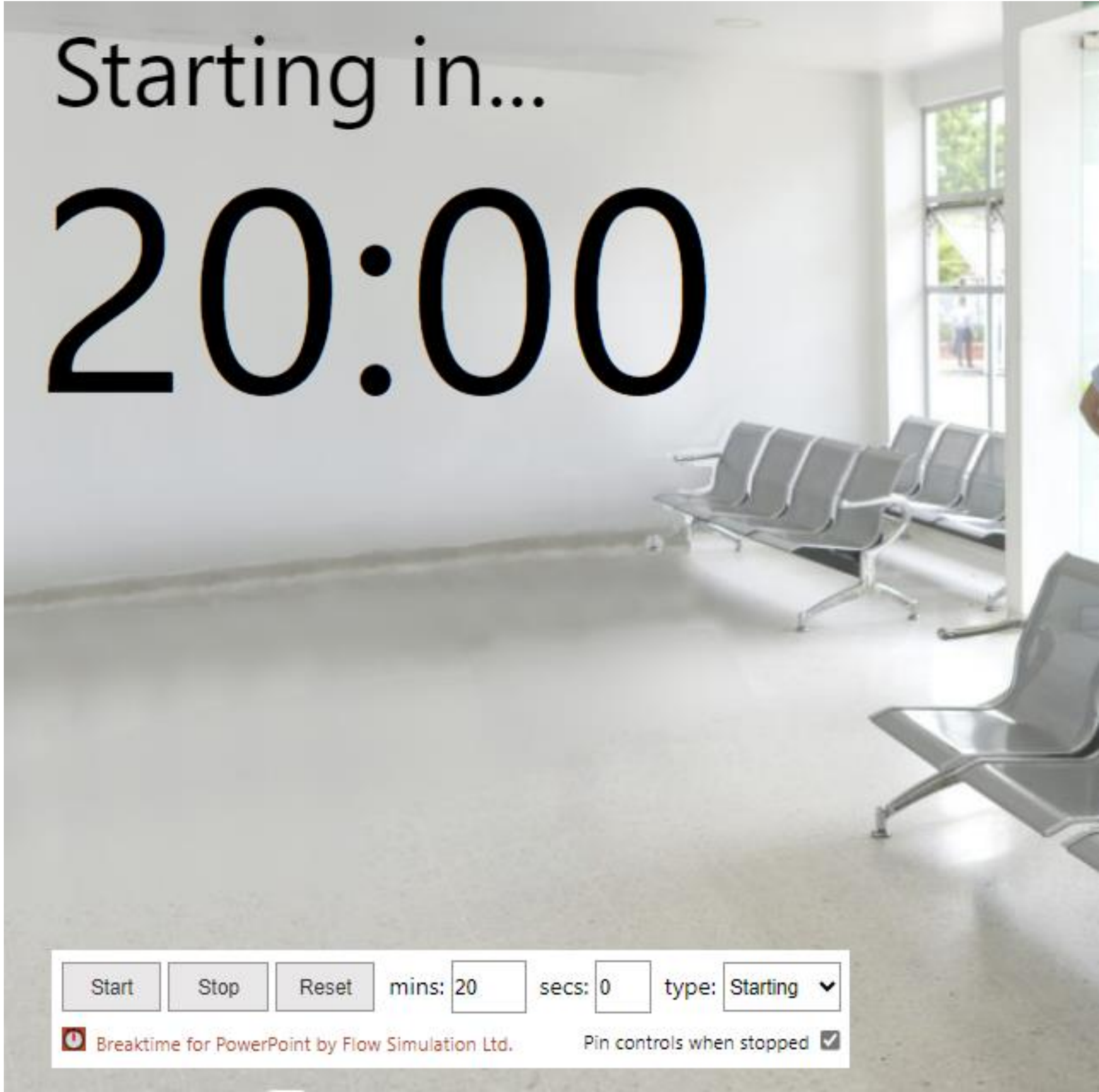
Automation options - Summary

Component	API	PowerShell	ARM	Terraform	Repositories
Onboarding	✓	✓	✓	✓	✗
Connectors	✓	✓	✓	✓	✗
Analytics Rules	✓	✓	✓	✓	✓
Hunting Queries	✓	✓	✓	✓	✓
Workbooks	✗	✗	✓	✗	✓
Playbooks	✓	✓	✓	✓	✓
Watchlists	✓	✗	✓	✗	✗
KQL functions	✓	✓	✓	✓	✗
Automation Rules	✓	✗	✓	✗	✓

Health Break!

Relax, refresh, refocus

About Me



Starting in...

20:00

mins: 20

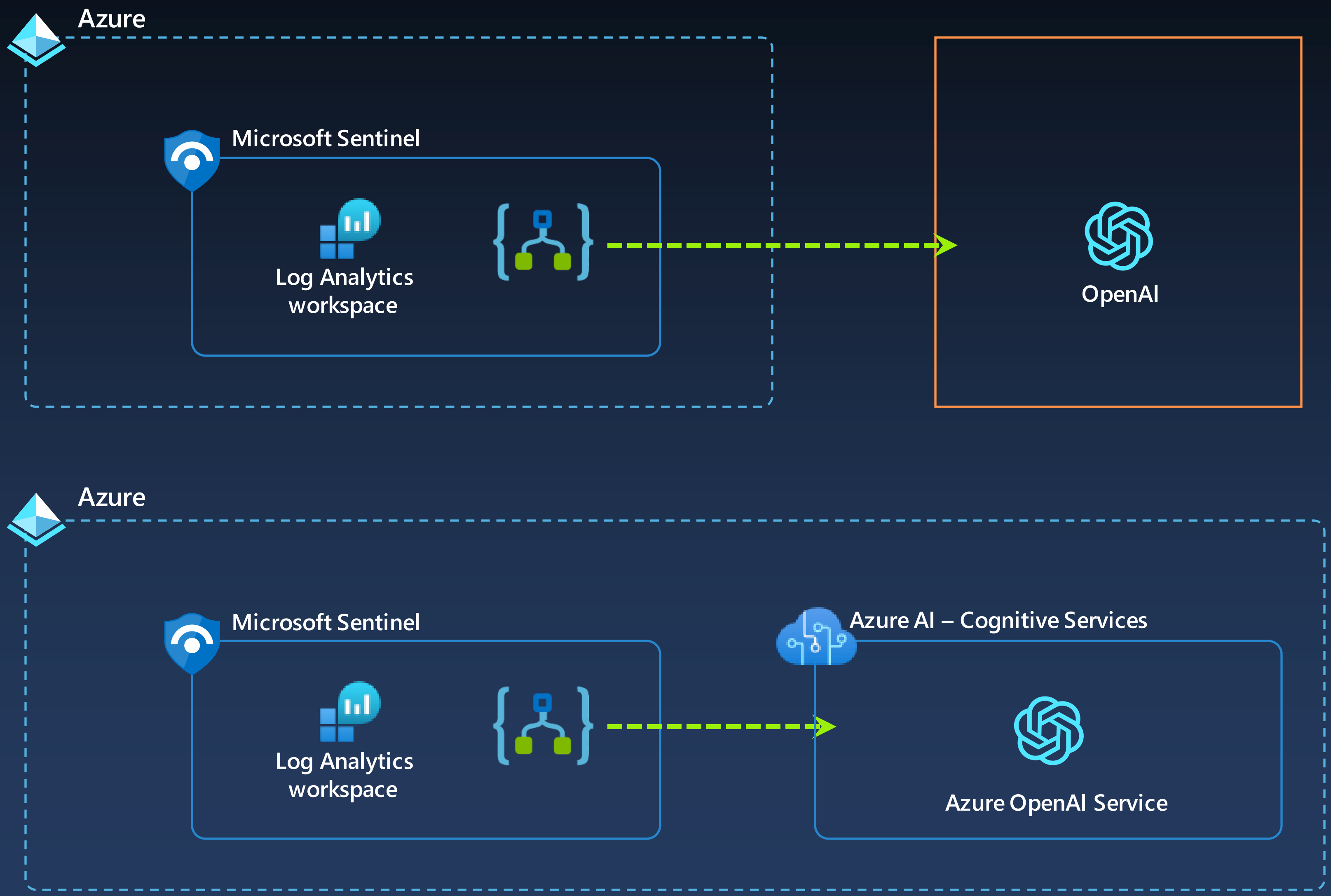
secs: 0

type: Starting

Breaktime for PowerPoint by Flow Simulation Ltd.

Pin controls when stopped ☑

Demos Architecture



Microsoft Sentinel + Azure Monitor Log Analytics

1. Microsoft Sentinel free trial

Ingest up to 10GB/day for first 31 days

OR

Add Microsoft Sentinel to your existing Log Analytics for free for first 31 days

- *Usage beyond these limits will be charged per pricing listed on this page.*
- *Charges related to additional capabilities for automation and bring your own machine learning are still applicable during the free trial.*

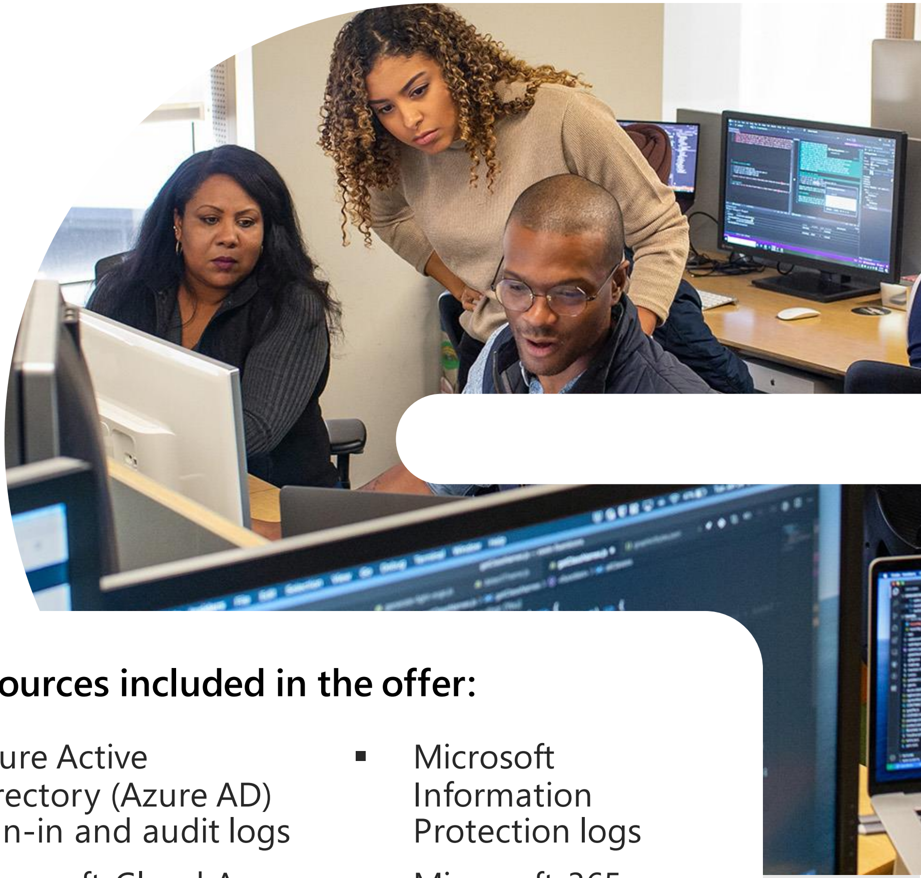
2. Microsoft Sentinel benefit for Microsoft 365 E5, A5,F5 and G5* customers

- **Save up to US2200/month** on a typical 3,500 seat deployment of Microsoft 365 E5 with up to 5MB per user/day of free data ingestion into Microsoft Sentinel

- **Applied automatically** at the end of the month – no enrollment or nomination process.

- **Eligibility:** Microsoft 365 E5, A5,F5 and G5* or Microsoft 365 E5, A5,F5 and G5* security customers

https://aka.ms/m365-sentinel-offer



Data sources included in the offer:

- Azure Active Directory (Azure AD) sign-in and audit logs
- Microsoft Cloud App Security shadow IT discovery logs
- Microsoft Information Protection logs
- Microsoft 365 advanced hunting data

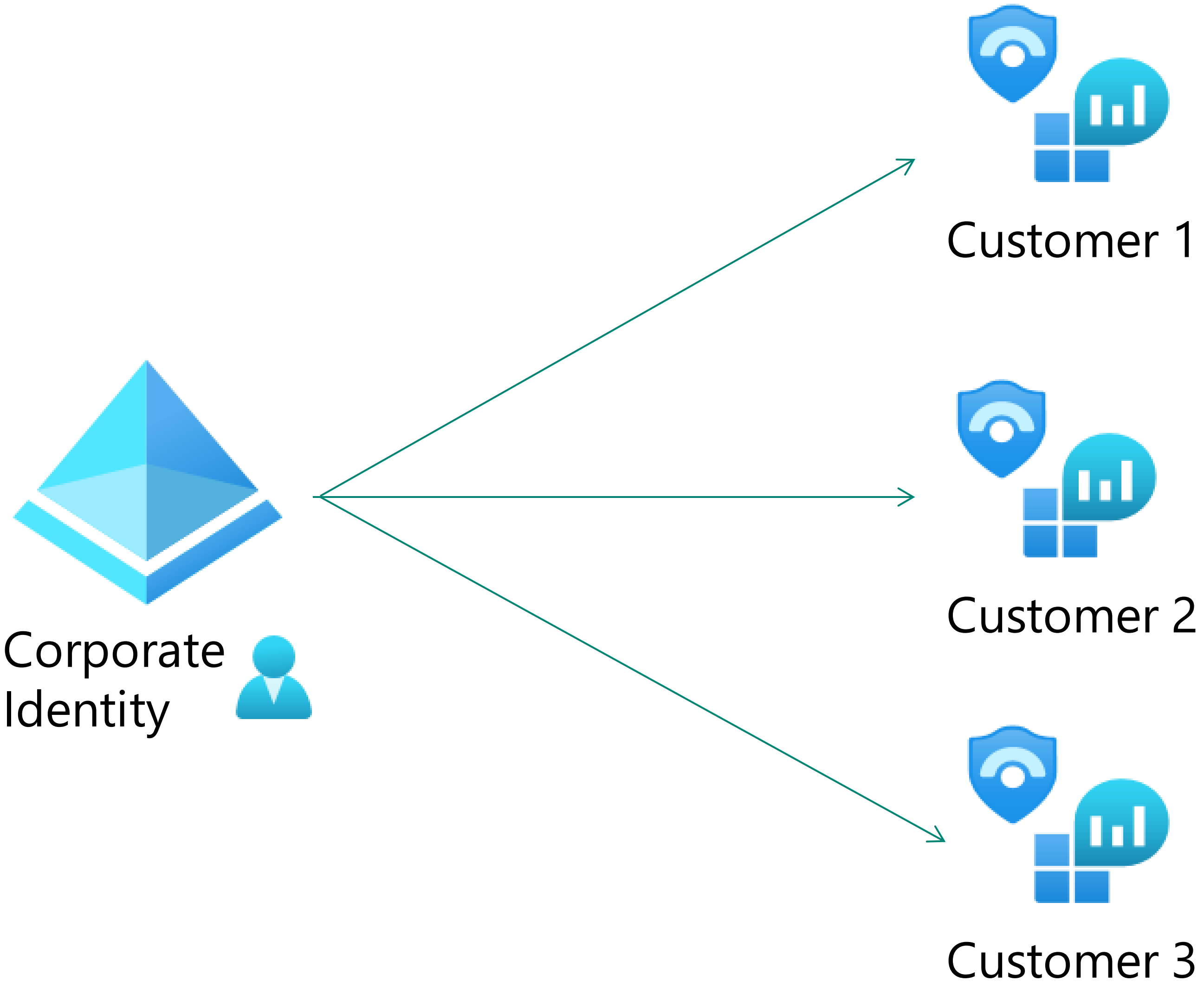
*Microsoft waives any and all entitlement to compensation for the services provided to you under this agreement. Microsoft intends that these services and associated terms be in compliance with applicable laws and regulations with respect to gratuitous services. It is specifically understood that all services and services deliverables provided are for the sole benefit and use of the government entity and are not provided for personal use or benefit of any individual government employee.

3. Always Free Data Sources

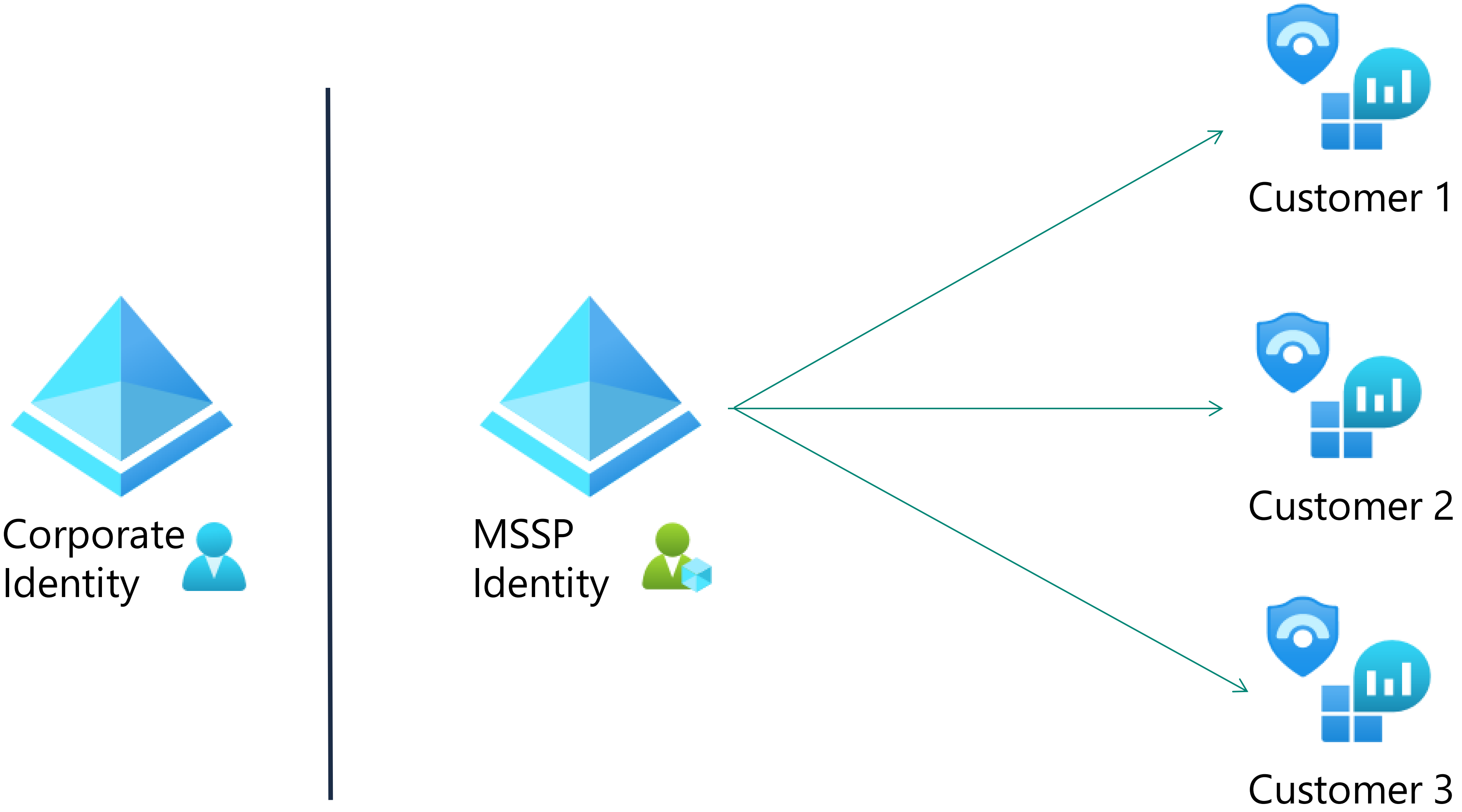
- Azure Activity Logs
- Office 365 Audit Logs, including all SharePoint activity, Exchange admin activity, and Teams.
- Alerts from Microsoft Defender for Cloud, Microsoft 365 Defender, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Endpoint and Microsoft Defender for Cloud Apps

Q & A

Single Identity Model



Multiple Identities Model



Corporate Identity

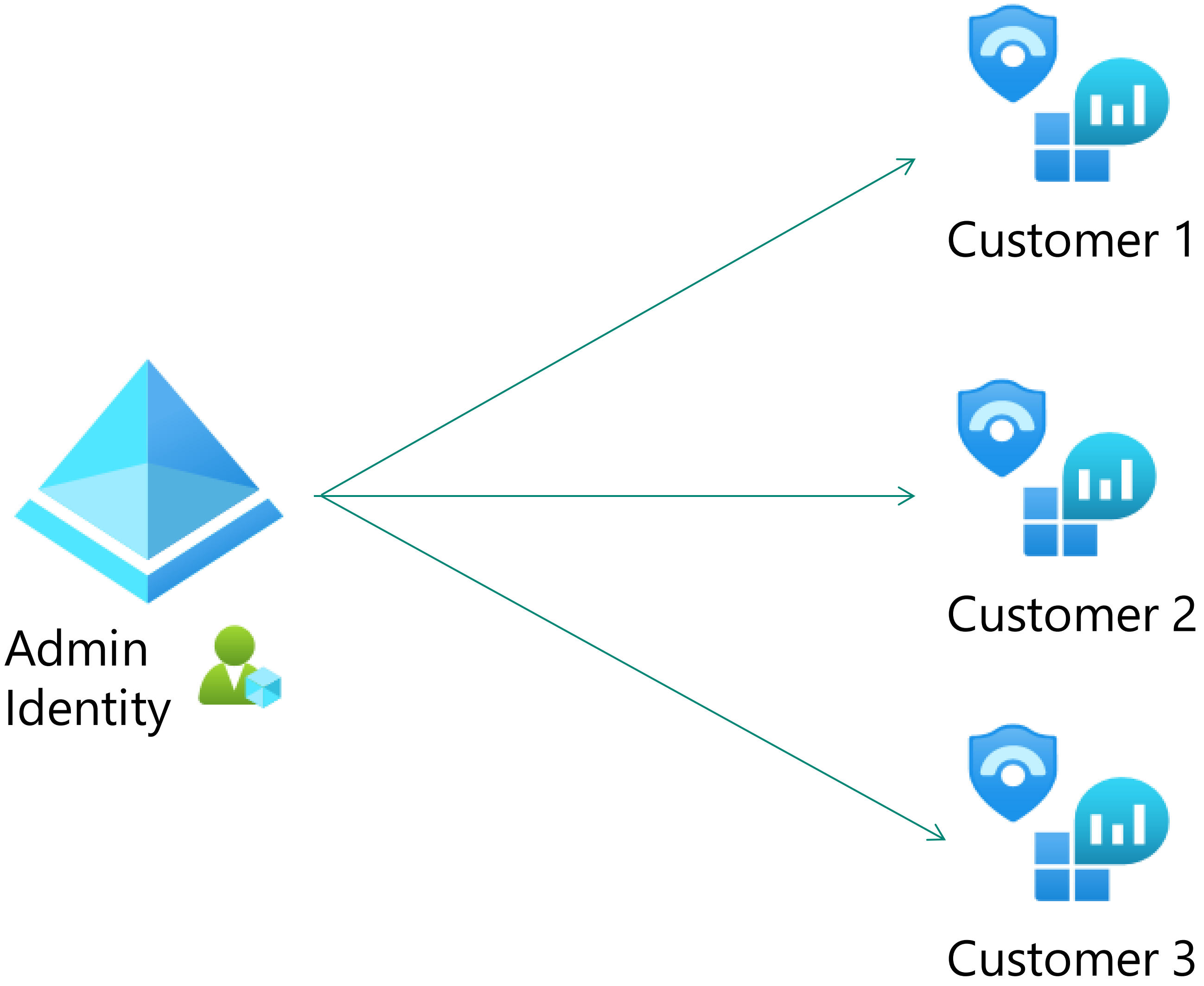
MSSP Identity

Customer 1

Customer 2

Customer 3

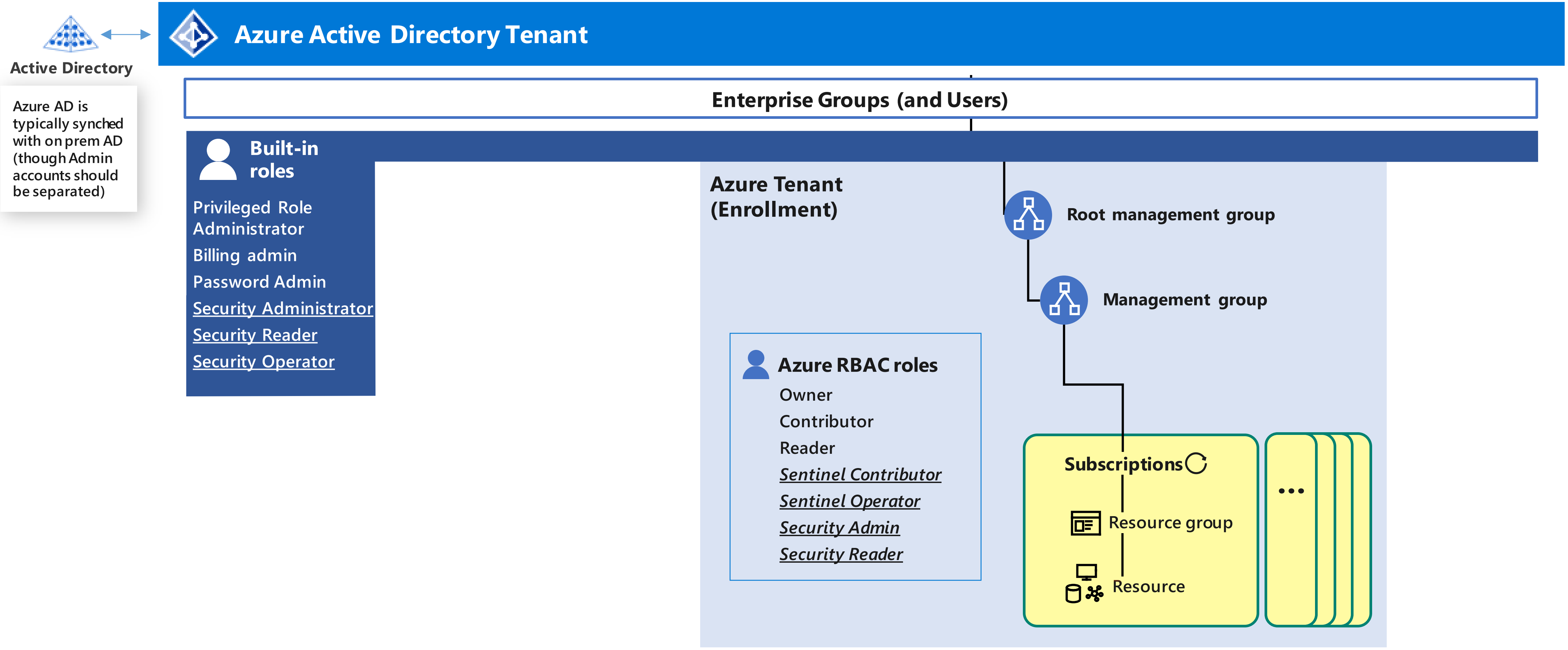
“In Between”

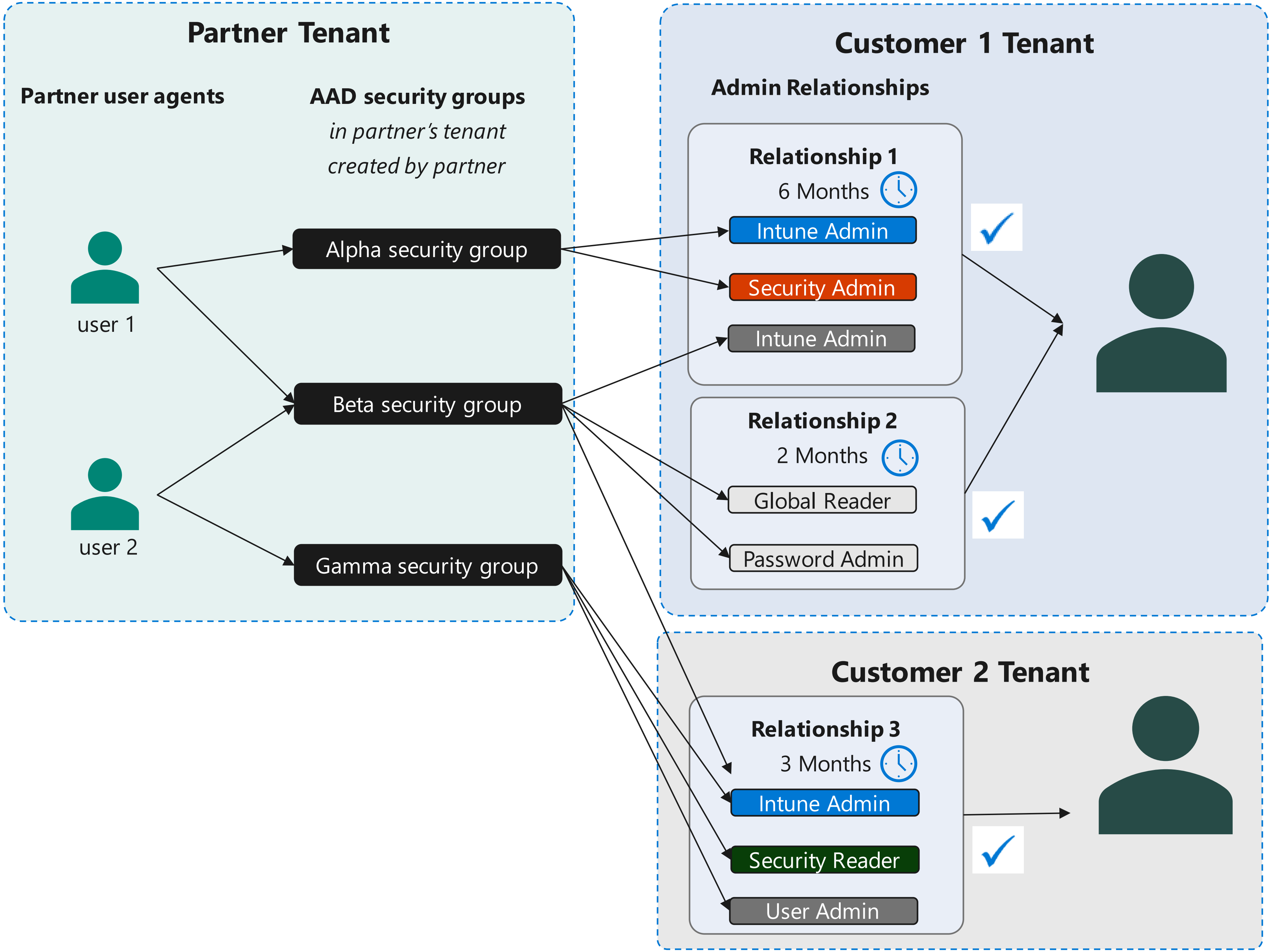


Role	View and run playbooks	Create and edit playbooks	Create and edit analytic rules, workbooks, and other Microsoft Sentinel resources	Manage incidents (dismiss, assign, etc.)	View data, incidents, workbooks, and other Microsoft Sentinel resources
Microsoft Sentinel Reader	--	--	--*	--	✓
Microsoft Sentinel Responder	--	--	--*	✓	✓
Microsoft Sentinel Contributor	--	--	✓	✓	✓
Microsoft Sentinel Playbook Operator	✓	--	--	--	--
Logic App Contributor	✓	✓	--	--	--

*** Users with these roles can create and delete workbooks with the Workbook Contributor role**

Azure AD (tenant) and Azure RBAC (subscription)





Partner Tenant

Partner user agents

AAD security groups

in partner's tenant

created by partner

user 1

user 2

Alpha security group

Beta security group

Gamma security group

Customer 1 Tenant

Admin Relationships

Relationship 1

6 Months

Intune Admin

Security Admin

Intune Admin

Relationship 2

2 Months

Global Reader

Password Admin

Customer 2 Tenant

Relationship 3

3 Months

Intune Admin

Security Reader

User Admin

Microsoft Sentinel | Fusion – Advanced Multistage Attack Detection

Analyzing activities across multiple cloud services into high-fidelity security cases using Graph-powered Machine Learning

Activity

Identity
(millions of events)

Office 365 activity
(millions of events)

Azure / AWS / GCP activities
(millions of events)

Host activities
(millions of events)

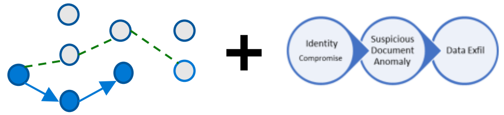
Firewall
(multi-billion events)

Anomalous signals

Security alerts
(thousands)

Anomalies
(thousands)

Graph-powered ML + probabilistic kill chain



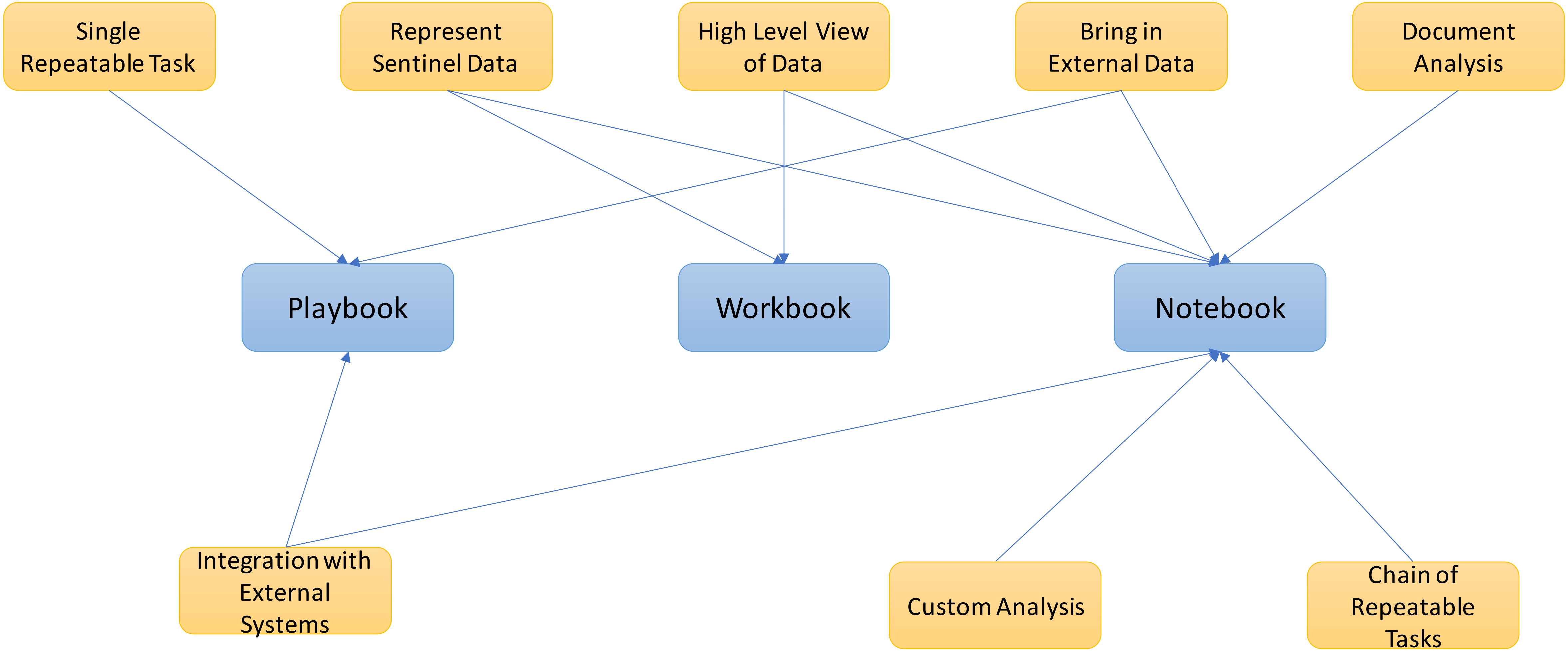
Suspicious candidates
(hundreds)

Further ML analysis

2.4	1.5	2.3	1.1
....			

High Fidelity Incidents

Where notebooks fit in



Single Repeatable Task

Represent Sentinel Data

High Level View of Data

Bring in External Data

Document Analysis

Playbook

Workbook

Notebook

Integration with External Systems

Custom Analysis

Chain of Repeatable Tasks

When and Why

	Playbooks	Workbooks	Notebooks
Persona	• SOC Engineer • Analyst of al tiers	• SOC Engineer • Analyst of al tiers	• Threat hunters / Tier 2-3 analysts • Incident investigators • Data scientists • Security researcher
Uses	Automation of simple, repeatable tasks: • Ingestion – bring in internal data • Enrichment (TI, GeoIP, Lookups) • Investigation • Remediation	• Visualization	• Sentinel and external data querying • Enrichment (TI, GeoIP, WhoIs lookups, etc.) • Investigation • Visualization • Hunting • Machine Learning & Big Data Analytics
Pros	❑ Best for single repeatable tasks ❑ No coding knowledge required	❑ Best for high level view ❑ No coding knowledge required	❑ Best for more complex chain of repeatable tasks ❑ Ad-hoc, more procedural control – easy to pivot due to the interactive capabilities ❑ Rich Python libraries for data manipulation & visualization options ❑ Machine Learning & Custom Analysis ❑ Easy to document & Share analysis evidence
Cons	• Not suitable for ad-hoc & complex chains • Not great for documenting & sharing evidence	• Cannot integrate with external data	• Higher learning curve – requires coding knowledge