



MC2MC

Sentinel's Got Game: Unleashing the Power of 3rd party app integrations



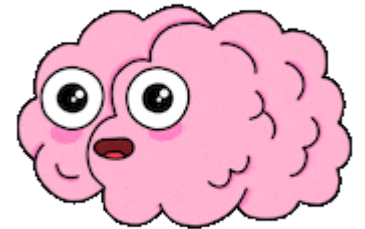
Sander Bougrine

Security Operations Incident Responder
Security Consultant
@ The Collective

Cloud Security & Compliance
Identity Management
Determined Forensic Researcher and KQL expert



Cloud Watcher
(<https://www.cloudwatcher.be/>)



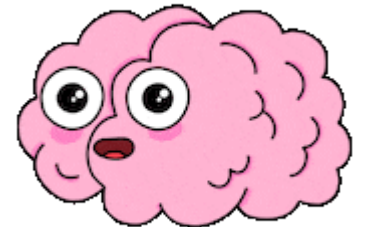
Robbe Van den Daele

Security Operations Incident Responder
Security Consultant
@ The Collective

Security Technology and Procedures
Microsoft Sentinel and Defender
MITRE ATT&CK Gap Analysis



Hybrid Brothers
(<https://hybridbrothers.com>)



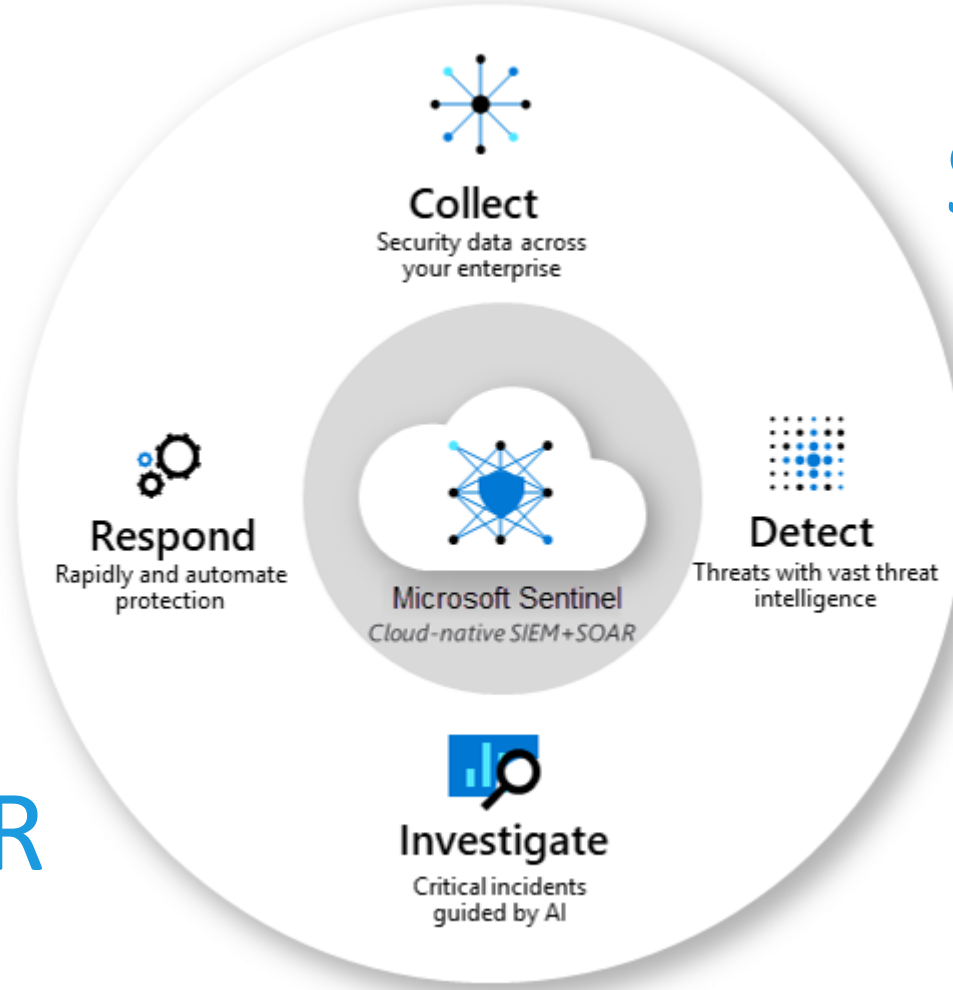
Let



Microsoft Sentinel

SIEM

SOAR



Benefits of integrating 3rd party apps



Increased visibility and context



Improved threat detection and response



Enhanced automation and efficiency



Centralized management

Integration Methods

1. Connector-based integration
2. Direct API integration
3. Agents
4. Custom log ingestion
5. Codeless Connector Platform

1

2

3

4

5

Connector-based integration

Connector-based integration involves using pre-built connectors provided by Microsoft Sentinel or the third-party app vendor.

1

2

3

4

5

Direct API Integration

Direct API integration involves connecting a third-party app directly to Microsoft Sentinel using its API. This method provides the most direct and efficient integration, but it requires the app to have a compatible API.

Azure Sentinel Management API

- GET / CREATE / DELETE Incidents
- GET / CREATE / DELETE Analytic Rules
- GET / DELETE Data Connectors
- POST / UPDATE Bookmarks
- GET Entity Info



Azure Sentinel



Microsoft Graph Security API

- GET Alert Info
- POST Alert Info
- Ingest TI into Sentinel



Log Analytics
Workspace



Log Analytics API

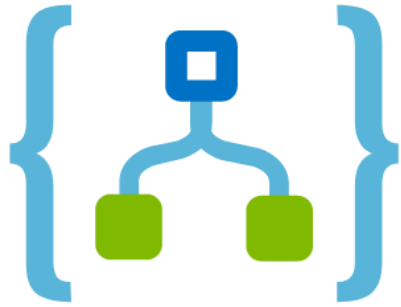
GET data stored in a Log Analytics workspace using a query

HTTP Data Collector API

Store data in a Log Analytics workspace



Possibilities



LOGIC APP



POWERSHELL



AZURE FUNCTIONS

1

2

3

4

5

Agents

Integrations via Microsoft agents are an easy way to send security events from devices to Microsoft Sentinel. They can also be used as log forwarders for other third-party devices.

Agents – MMA | AMA

Microsoft Monitoring Agent

- Legacy
- Less flexibility
- No data transformations
- Connected to Log Analytics Workspace

Azure Monitoring Agent

- More flexibility
- Data transformations available
- Association to DCRs
- Azure ARC

Ingesting Windows Security Logs
Ingesting Linux Syslog data
Ingesting 3rd party syslog (syslog forwarder)

Agents

Custom Log Ingestion

1

2

3

4

5

Custom Log Ingestion - Syslog Forwarding

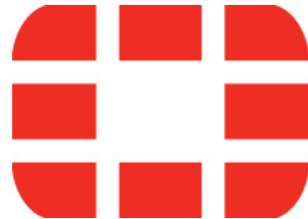
- In most cases (but not limited to) syslog forwarding
- On-premises devices / security appliances



Citrix **NetScaler**



VMware
vSphere®



Custom Log Ingestion

Why

- Detect threats and correlate data
- Full control of normalization and filtering
- Ingest data in standard or custom tables
- Split verbose and non-verbose data

Pitfalls

- Implementation complexity
- Custom normalization and filtering
- Different parts

Custom Log Ingestion – AMA | Logstash



AMA

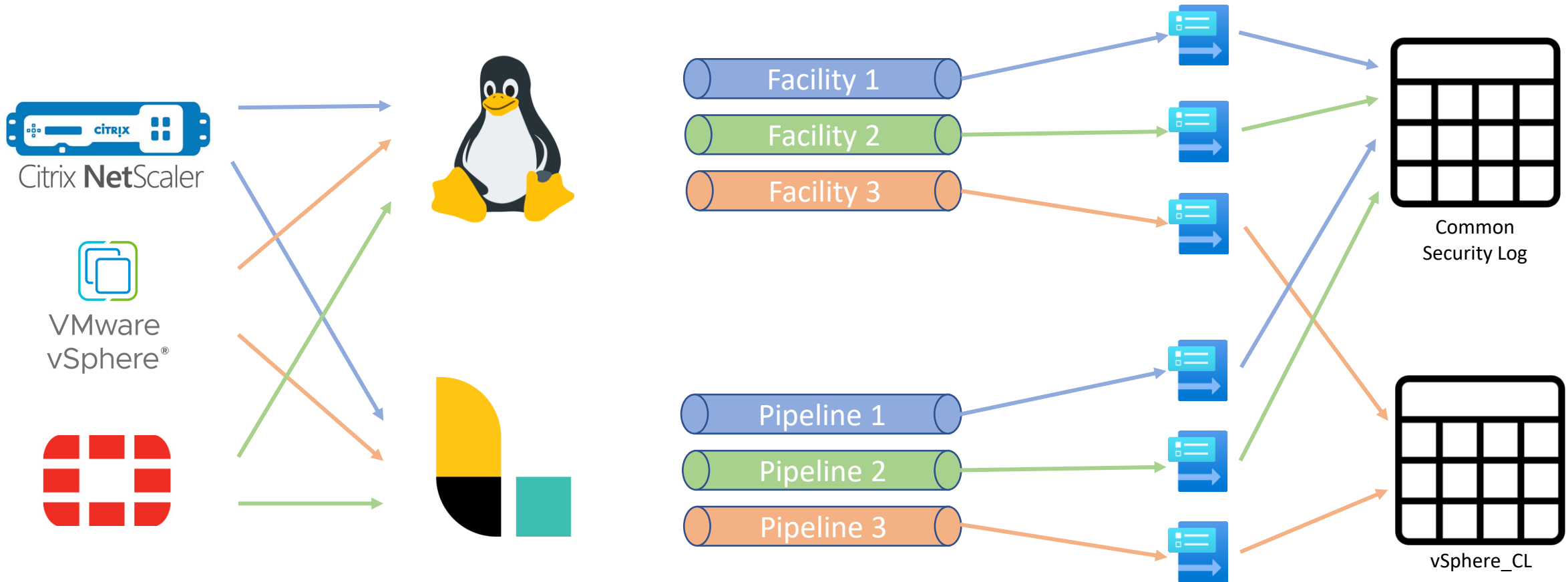
- Easier than Logstash
- Normalization and transformation via DCRs



Logstash

- Local filtering possible
- DCRs supported
- Can run in containers
- Not limited to syslog data
- No ARC onboarding

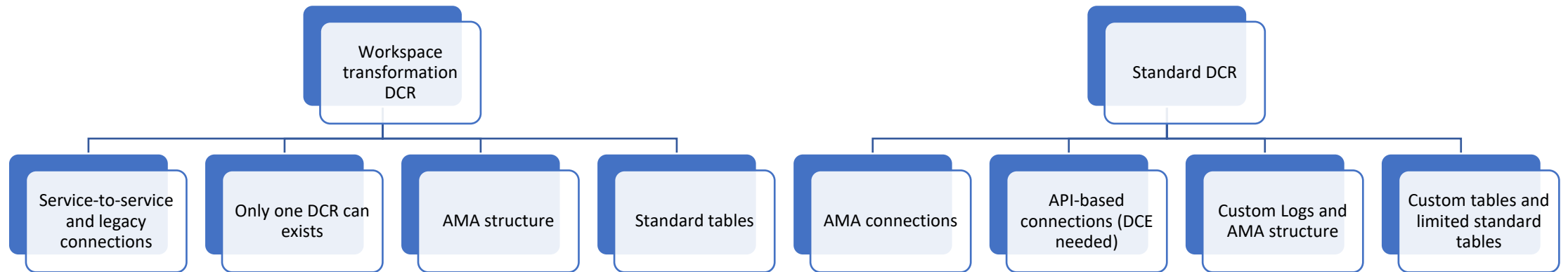
Custom Log Ingestion – AMA | Logstash



Custom Log Ingestion - DCR rules



Custom Log Ingestion - DCR rules



Custom Log Ingestion - DCR rules

- [Demystifying Data Collection Rules and Transformations \(hybridbrothers.com\)](http://hybridbrothers.com)



1

2

3

4

5

Codeless Connector Platform

Connectors created using CCP are fully SaaS, without any requirements for service installations, and also include health monitoring and full support from Microsoft Sentinel

Codeless Connector Platform


- Create you own Data Connector in the Azure Portal
- For pulling use cases (when the data source has an API to pull data from)
- Two parts ([Create a codeless connector for Microsoft Sentinel | Microsoft Learn](#))
 - Connector UI Config
 - Polling Config



Codeless Connector Platform – UI Config

Home > Microsoft Sentinel > Microsoft Sentinel >

GitHub Enterprise Audit Log (Preview) ...

Delete

 **2** GitHub Enterprise Audit Log (Preview) **1**




Connected Status **3**  GitHub Provider  5 days ago Last Log Received

Description


The GitHub audit log connector provides the capability to ingest GitHub logs into Microsoft Sentinel. By connecting GitHub audit logs into Azure Sentinel, you can view this data in workbooks, use it to create custom alerts, and improve your investigation process.

Last data received
01/20/22, 12:04 PM

Related content

 **0** Workbooks  **1** Queries  **0** Analytics rules templates

Data received **4** [Go to log analytics](#)



5 Instructions **6** Next steps



Prerequisites

To integrate with GitHub Enterprise Audit Log (Preview) make sure you have:

- ✖ **Workspace:** read and write permissions are required.
- i** **GitHub API personal token Key:** You need access to GitHub personal token, the key should have 'admin:org' scope



Configuration

Connect GitHub Enterprise Audit Log to Microsoft Sentinel
Enable GitHub audit Logs. Follow [this](#) to create or find your personal key

Organization Name

API key

Re-connect

Disconnect

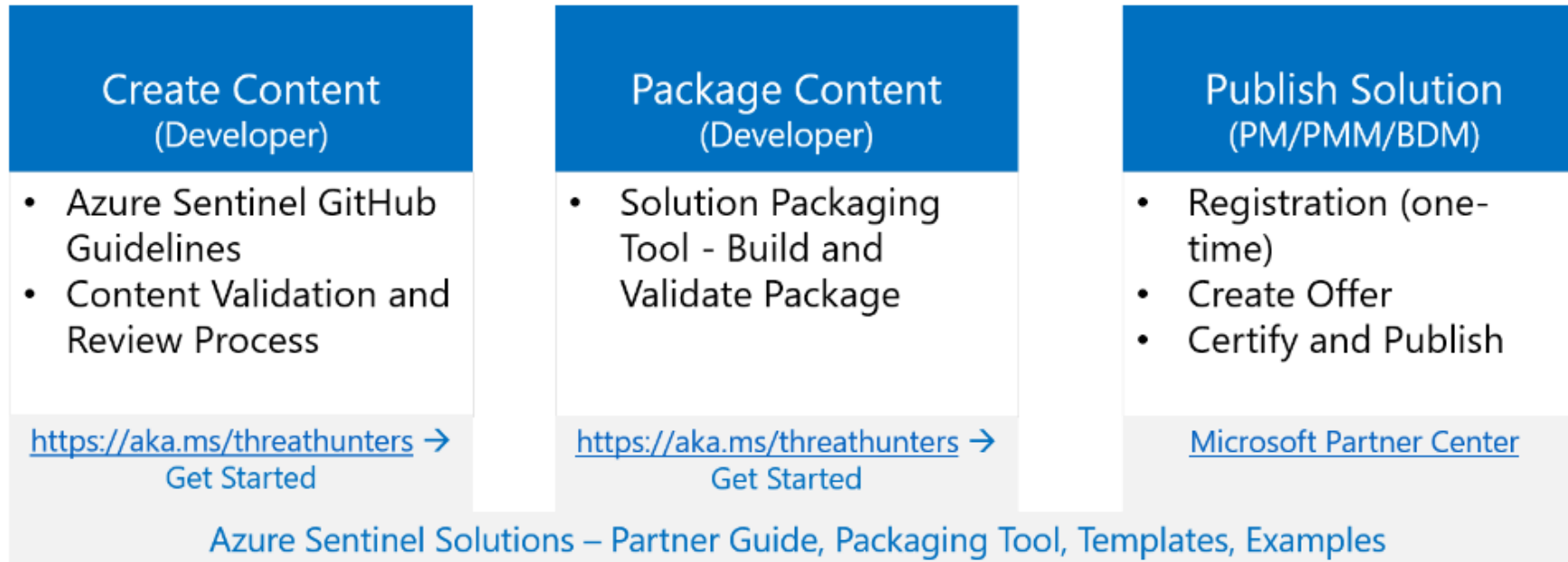
Codeless Connector Platform – Polling Config

JSON

Copy

```
"pollingConfig": {  
  "auth": {  
  },  
  "request": {  
  },  
  "response": {  
  },  
  "paging": {  
  }  
}
```

Codeless Connector Platform – Deploying



[Azure-Sentinel/Solutions/LastPass at master · Azure/Azure-Sentinel · GitHub](#)



Best practices and implementation strategies

- ✓ Clearly define the integration requirements
- ✓ Ensure compatibility and testing
- ✓ Implement proper security controls
- ✓ Monitor and maintain the integration

Custom logs via agents best practices

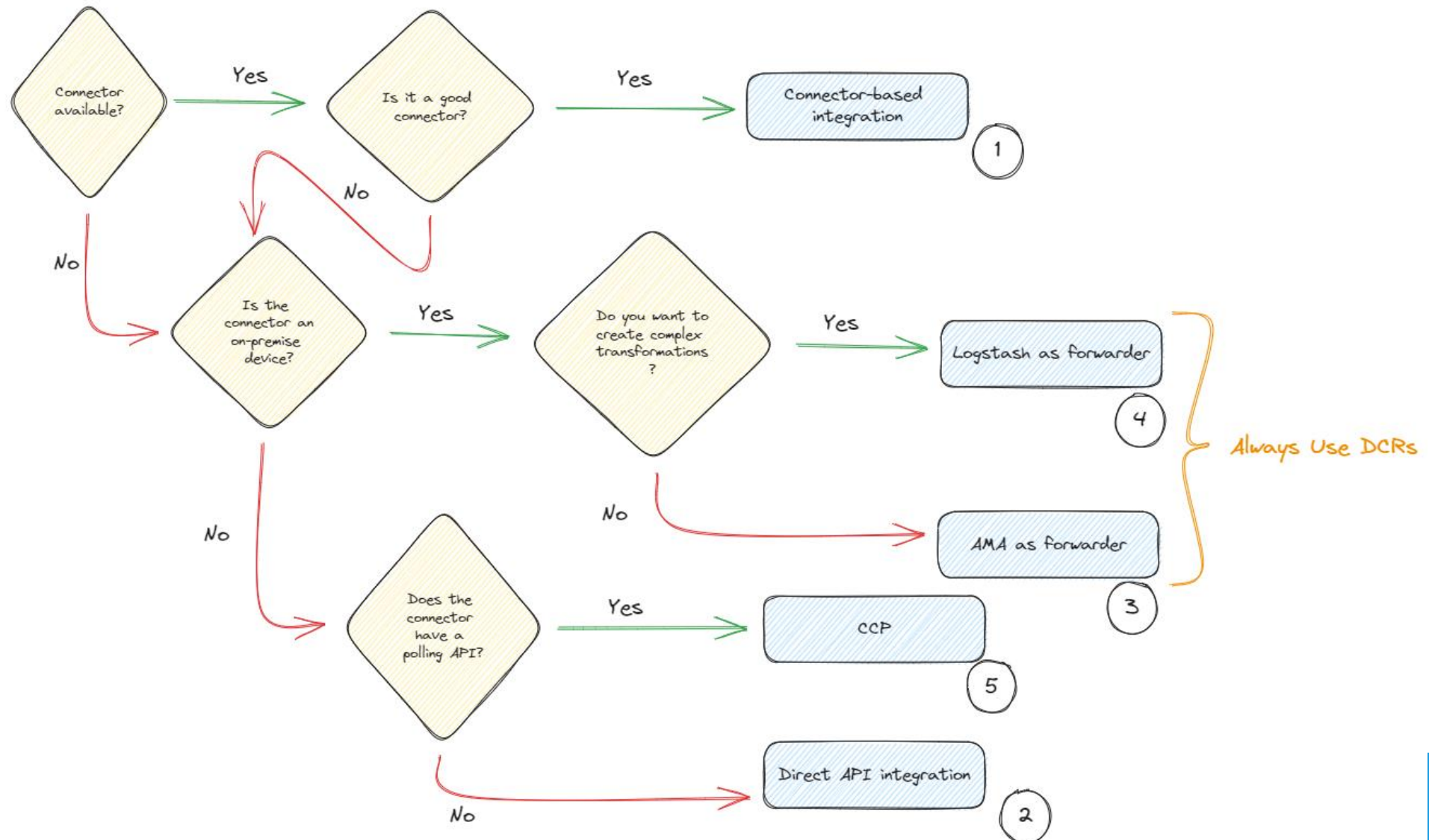
Use AMA for simple connectors ↔ Use Logstash for complex connectors

Create DCR per data connector / per destination table

Mix basic and analytics tables for high data amounts

Workspace transformation DCRs cannot have other DCRs as a source

How to choose between the connector types

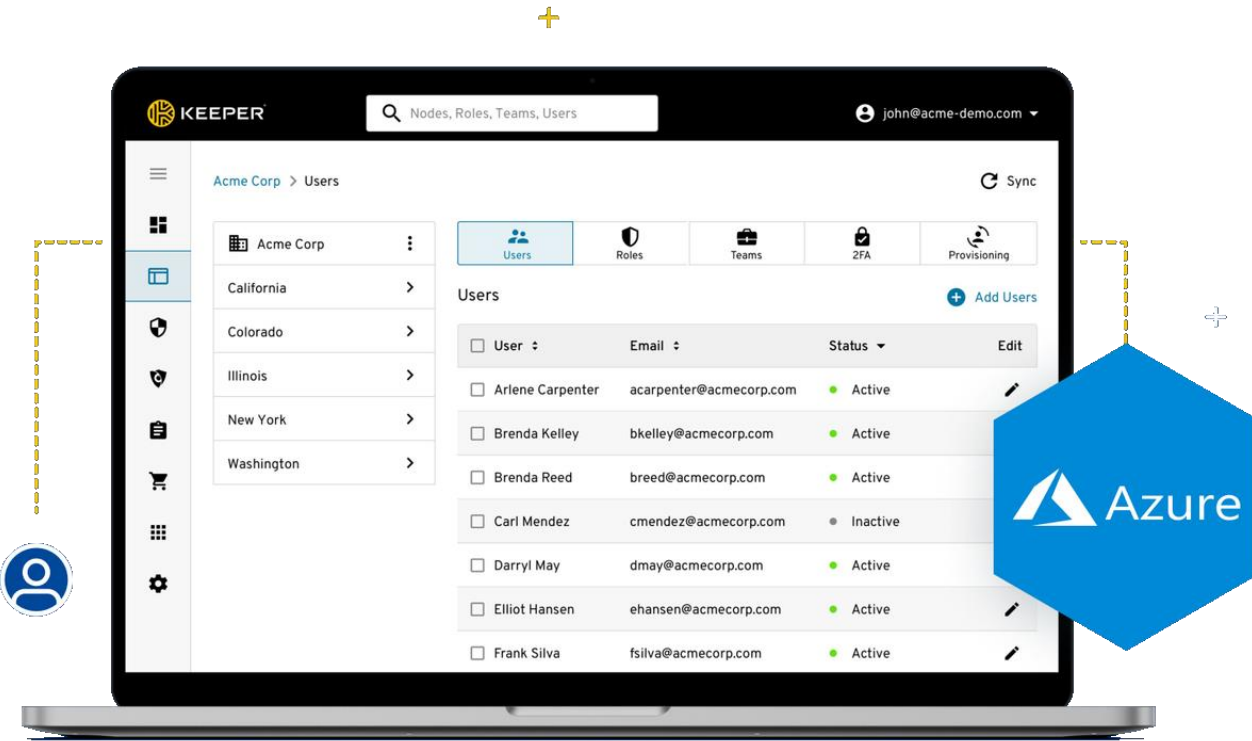




Xylos

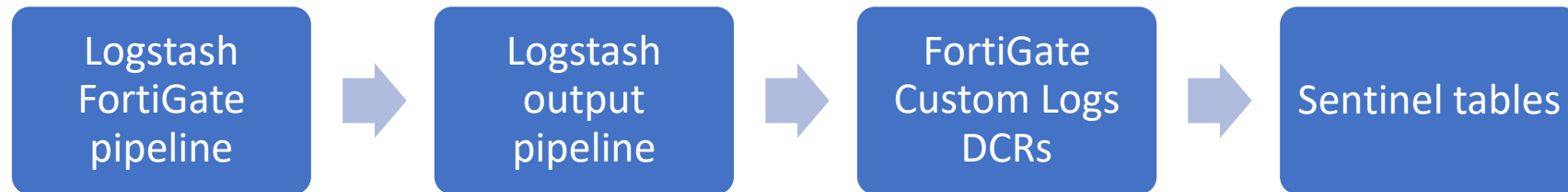
Real-world use cases

Integrating Keeper in Microsoft Sentinel



Custom Logs and DCR demo

- FortiGate ingestion to multiple tables via Logstash and DCRs



Thanks for having us!



[Robbe Van den Daele | LinkedIn](#)



[Hybrid Brothers](#)



[Robbe Van den Daele / Twitter](#)



vandendaele.robbe@outlook.com
info@hybridbrothers.com



[Sander Bougrine | LinkedIn](#)



[Cloud Watcher](#)



404 Not Found



Sander.Bougrine@hotmail.com