

Logs or it didn't happen

Tobias Rødahl Thingnes

Cyber Security Center for Research and Education (eduCSC)

10.09.2026 @ NORDUnet Conference, Luleå, Sweden

Traffic Light Protocol

TLP:RED

Do not share with anyone else.

TLP:AMBER

Limited disclosure. Share within your organisation and its clients on a need-to-know basis.
AMBER+STRICT means your organisation only.

TLP:GREEN

Community-wide. Share with peers and partner organisations, but not on public channels.

TLP:CLEAR

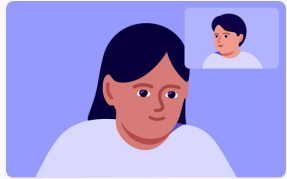
No restrictions. Share freely.



Remember 2020?



Remember 2020?

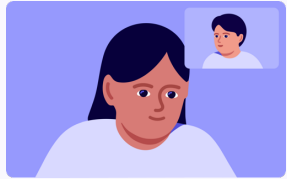


Stay at home

We tried to stop
COVID-19 from
spreading too fast.



Remember 2020?



Stay at home

We tried to stop
COVID-19 from
spreading too fast.

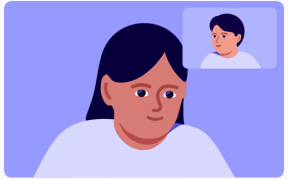


Sour doughs

People had weird
cooking hobbies to
stay sane.



Remember 2020?



Stay at home

We tried to stop COVID-19 from spreading too fast.



Sour doughs

People had weird cooking hobbies to stay sane.

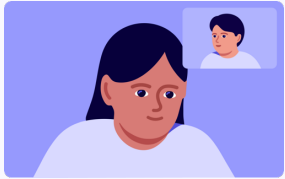


Tiger King

People were obsessed with TV shows about tigers.



Remember 2020?



Stay at home

We tried to stop COVID-19 from spreading too fast.



Sour doughs

People had weird cooking hobbies to stay sane.



Tiger King

People were obsessed with TV shows about tigers.



Log system

EduCSC started using Humio as our main log platform.





CrowdStrike to Acquire Humio and Deliver the Industry's Most Advanced Data Platform for Next-Generation, Index-Free XDR

February 18, 2021

CrowdStrike adds best-in-class data ingestion to extend its leadership with a true multi-tenant, cloud-native platform that delivers superior contextual insights and powers decision-making at enterprise scale

SUNNYVALE, Calif.--(BUSINESS WIRE)--Feb. 18, 2021-- [CrowdStrike Holdings, Inc.](#) (Nasdaq: CRWD), a leader in cloud-delivered endpoint and cloud workload protection, today announced it has agreed to acquire [Humio](#), a leading provider of high-performance cloud log management and observability technology. Under the terms of the agreement, CrowdStrike will pay approximately \$400 million to acquire Humio, subject to adjustments. The acquisition is expected to close during CrowdStrike's fiscal first quarter, subject to customary closing conditions.

CrowdStrike Completes Acquisition of Humio

March 5, 2021

SUNNYVALE, Calif.--(BUSINESS WIRE)--Mar. 5, 2021-- [CrowdStrike Holdings, Inc.](#) (Nasdaq: CRWD), a leader in cloud-delivered endpoint and cloud workload protection, today announced it has completed its acquisition of Humio, a leading provider of high-performance cloud log management and observability technology.





CrowdStrike Drives the Convergence of Security and Observability with Introduction of Falcon LogScale and Falcon Complete LogScale

September 20, 2022

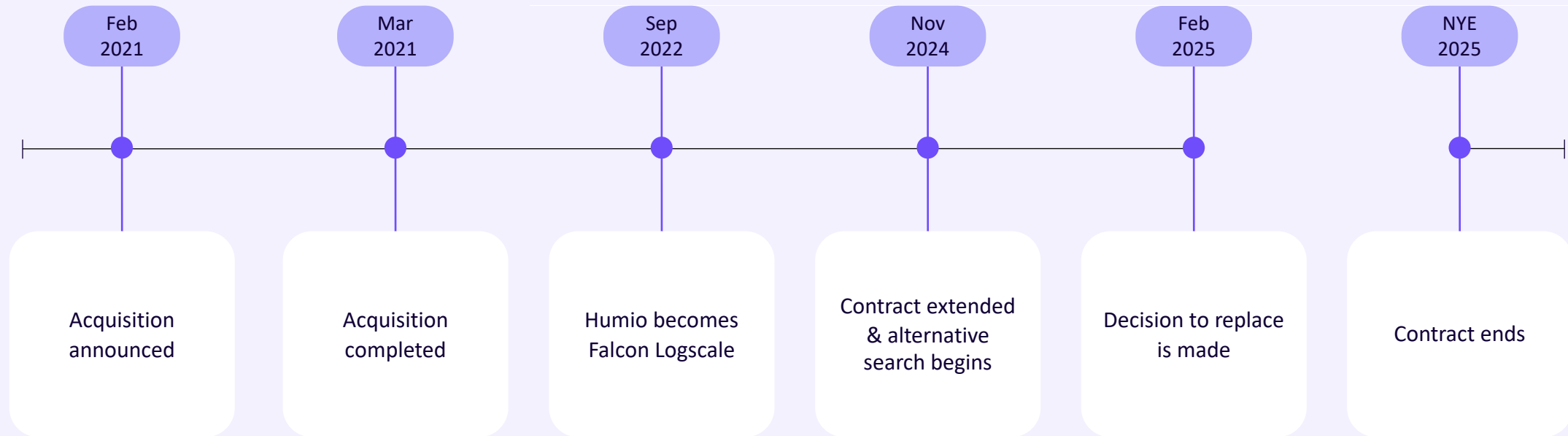
CrowdStrike expands and enhances log management and observability capabilities to help organizations leverage their data for security and non-security use cases

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)--Sep. 20, 2022-- Fal.Con 2022-- CrowdStrike (NASDAQ: [CRWD](#)), a leader in cloud-delivered protection of endpoints, cloud workloads, identity and data, today introduced the [Falcon LogScale](#) module, which enables organizations to log all their data and get answers in real time and at unprecedented scale. Falcon LogScale is the next evolution of Humio, which was [acquired by CrowdStrike in March 2021](#). In addition, CrowdStrike also introduced [Falcon Complete LogScale](#), a fully managed service that brings together the power of Falcon LogScale and the deep expertise of [Falcon Complete](#) (Managed Detection and Response) for highly-personalized log management operations and tailored observability.

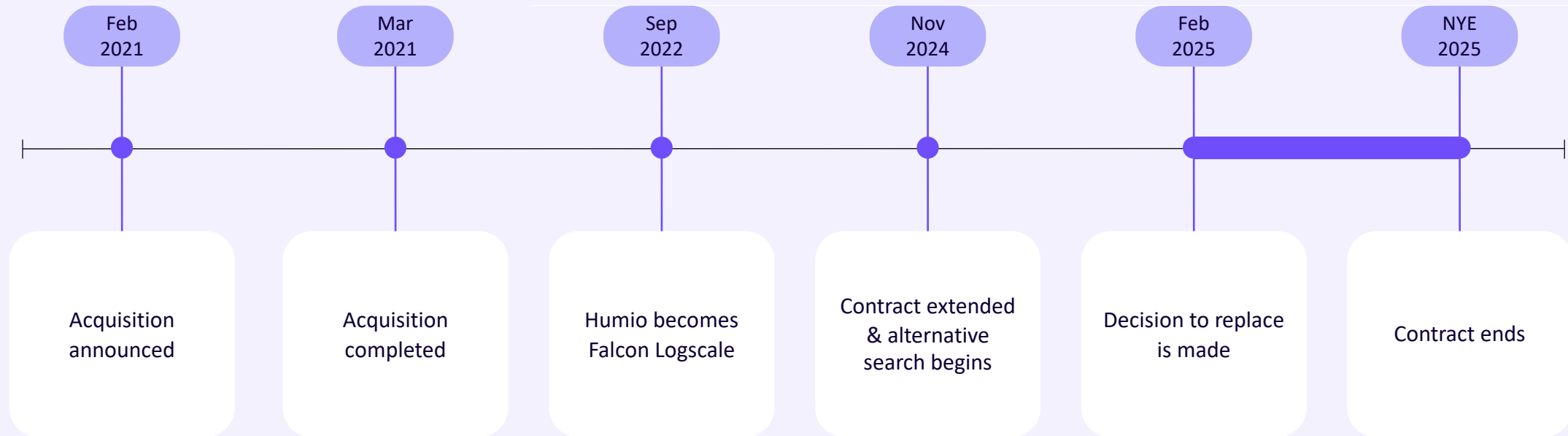




Timeline



Timeline



“A year is a long time”

Where were we in 2025?

Developer team in 2025



Øivind (20 %)



Didrik (20 %)

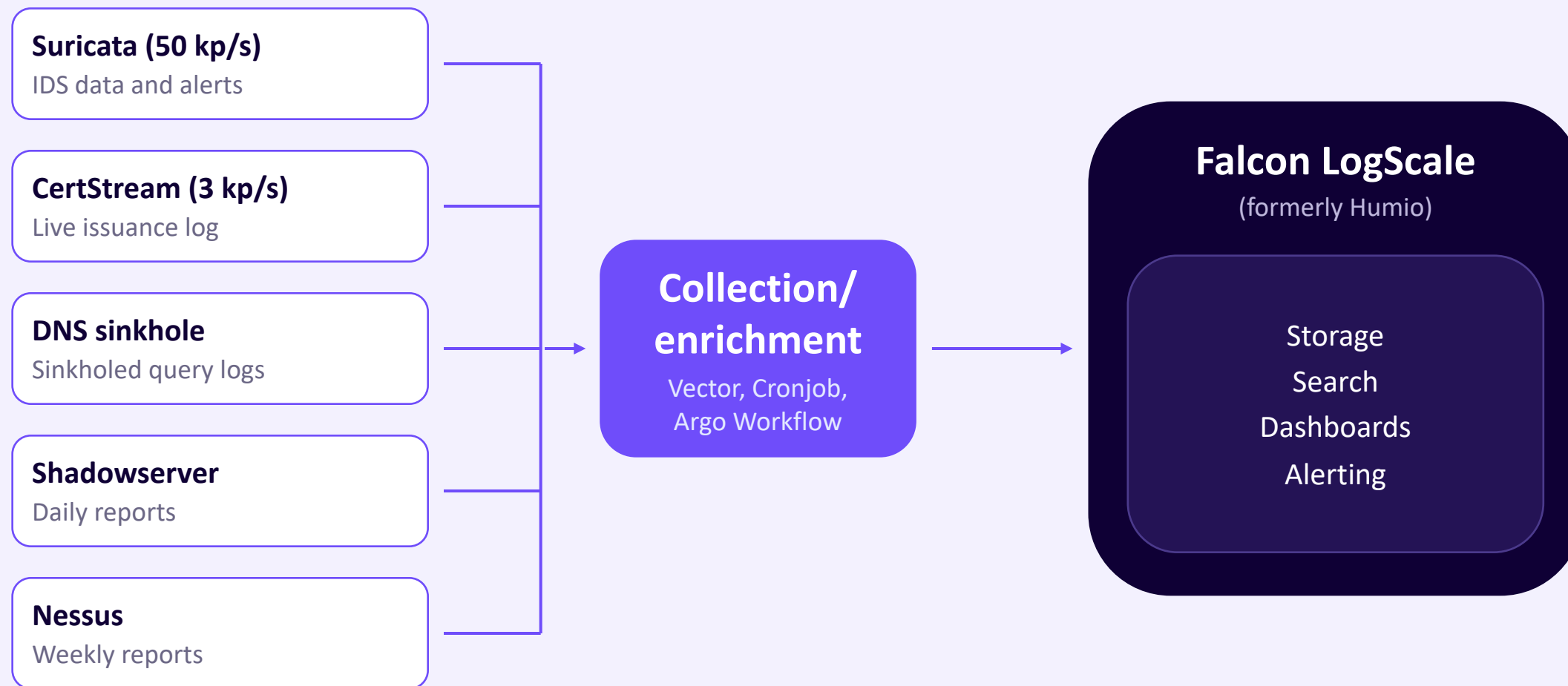


Adhirath



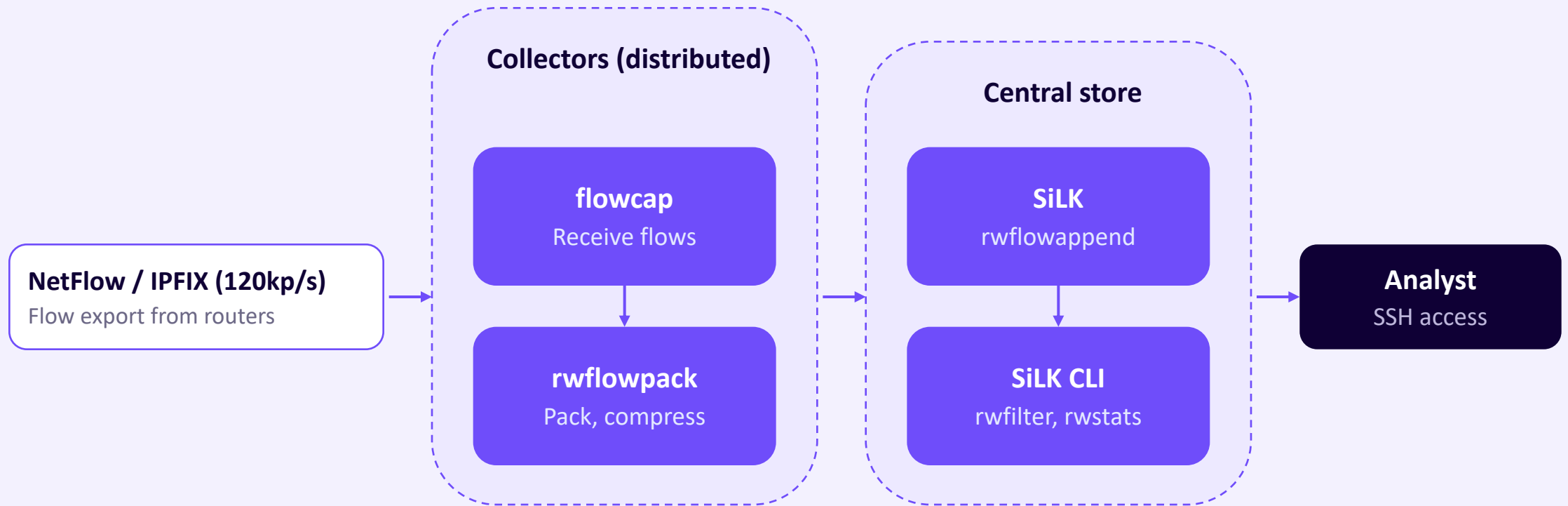
Architecture in 2025

TLP:GREEN



Architecture in 2025

TLP:GREEN



Next-Gen SIEM

Advanced event search

SearchCharlotte AI

🔔🗨️🔗👤🌞

Search

Dashboards

Lookup files

Schedule search

Create rule

Add to case

See in graph

All

Searches

Auto (Event List)

-07:00 Denver

Last 15m

Live

Run

1 event_type=phishing_attempt | #repo=foundry_cb40e50468944c7282c8ffdd04bc575c_applicationrepo

Showing fields from 2 events

Fetch more

Filter fields

Columns	#	%	
@timestamp	2	100%	
Fields	#	%	
#repo	1	100%	
#repo.cid	1	100%	
#type	1	100%	
@id	2	100%	
@ingesttimestamp	2	100%	
@rawstring	2	100%	
@timestamp.nanos	1	100%	
@timezone	1	100%	
affected_service	1	50%	
cve_id	1	50%	
description	2	100%	
destination_ip	1	50%	
event_type	1	100%	
exploit_technique	1	50%	
hostname	1	50%	
patch_available	1	50%	
process	1	50%	
severity	2	100%	
source_ip	1	50%	
user	1	50%	

Results

14:2514:2614:2714:2814:2914:3014:3114:3214:3314:3414:3514:3614:3714:3814:3914:40

@timestamp

Field List

Dec. 10, 2025 14:39:17.853

#repo: foundry_cb40e50468944c7282c8ffdd04bc575c_applicationrepo

#repo.cid: 96915a3748b64a079458e21f1fdf4b8c

#type: json

@id: XKRIenV7vz9hJPrzMYTm6yBT_2_1_1765402757

@ingesttimestamp: 1765402759362

@rawstring: {"@timestamp":"2025-12-10T21:39:17.853Z","affected_service":"apache_httpd","cve_id":"CVE-2023-12345","description":"Suspicious executable attempting to modify system files","event_type":"phishing_attempt","exploit_technique":"buffer_overflow","patch_available":true,"severity":"low"}

@timestamp: 1765402757853

@timestamp.nanos: 0

@timezone: Z

affected_service: apache_httpd

cve_id: CVE-2023-12345

description: Suspicious executable attempting to modify system files

event_type: phishing_attempt

exploit_technique: buffer_overflow

patch_available: true

severity: low

Query status: Done

Execution time: 267ms

Hits: 2

EPS: 64

Work: 1

LogScale version: 1.213.0



What did we do?

Objectives



Objectives

1

Build a team



Objectives

1

Build a team

2

Understand
needs and
plan solution



Objectives

1

Build a team

2

Understand
needs and
plan solution

3

Run, test, and
integrate



Where are we today?

Current developer team



Øivind (20 %)



Didrik (20 %)



Adhirath



Tobias



Emil



Oda



Robert

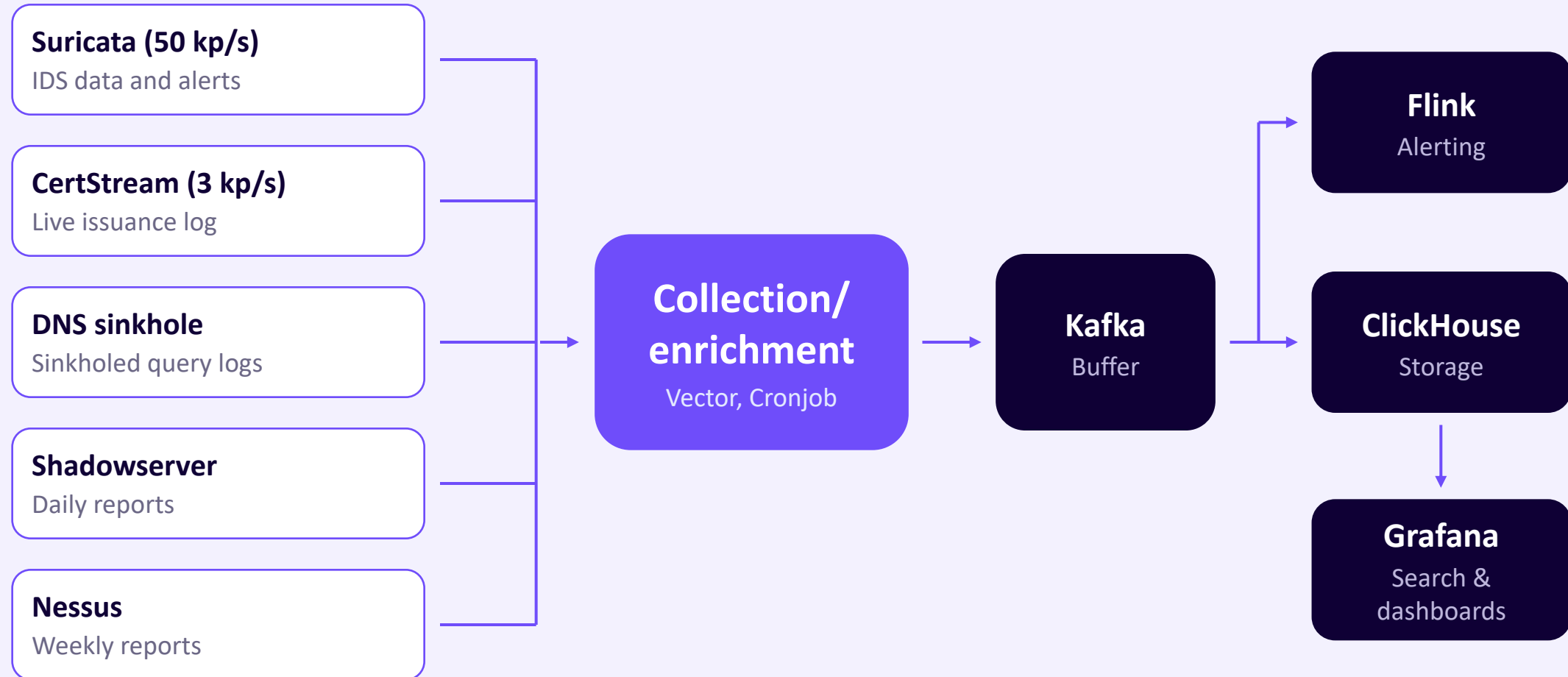


Andreas



Current architecture

TLP:GREEN



Current architecture

TLP:GREEN



Grafana

Dashboards > Frontpage

Q Search...

⌘+k

+

?



Edit

Home

Bookmarks

Starred

Dashboards

Playlists

Snapshots

Library panels

Shared dashboards

Recently deleted

Explore

Drilldown

Alerting

Connections

Administration



Welcome to eduCSC Peiling

Peiling gives you access to your organization's data directly and through dashboards.

New to Peiling? [Our documentation](#) explains how to get started.

Starred dashboards

Starred dashboards

IRT-brief

Sektorbrief

★

Recently viewed

Recently viewed dashboards

IRT-brief

Sektorbrief

★

Network sensor alerts

Provided by eduCSC

☆

Breddesøk

Breddesøk

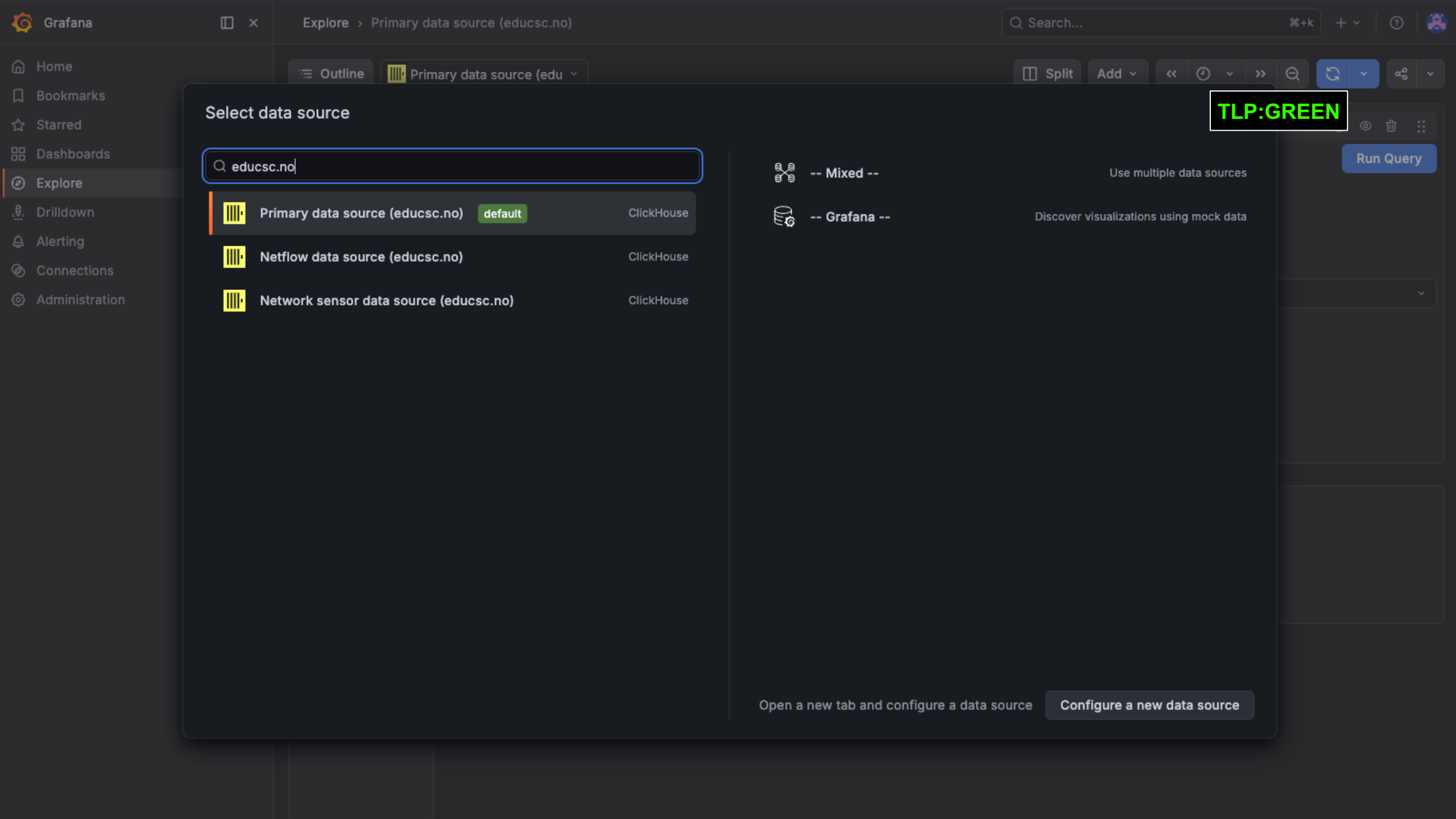
☆

Breddesøk etter instanser i sektoren

CERT og analyse

☆

TLP:GREEN



Select data source

educsc.no



Primary data source (educsc.no)

default

ClickHouse



Netflow data source (educsc.no)

ClickHouse



Network sensor data source (educsc.no)

ClickHouse



-- Mixed --

Use multiple data sources



-- Grafana --

Discover visualizations using mock data

Open a new tab and configure a data source

Configure a new data source

TLP:GREEN

Run Query

Reflections

Choosing technologies

- Proprietary vs. open-source?

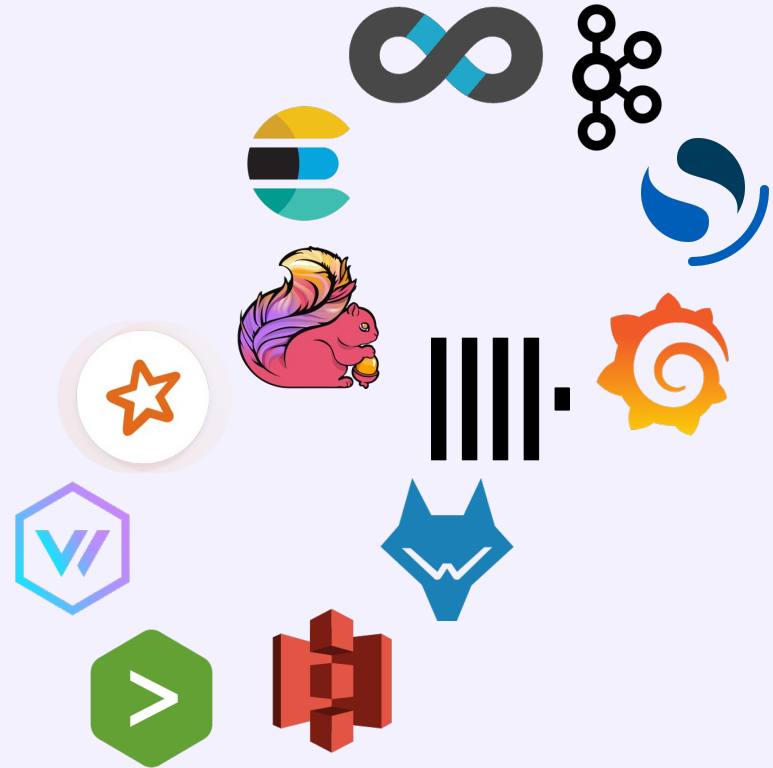
Is the business model viable?

- All-in-one vs. standalone?

Do we prefer deeper lock-in or extra maintenance?

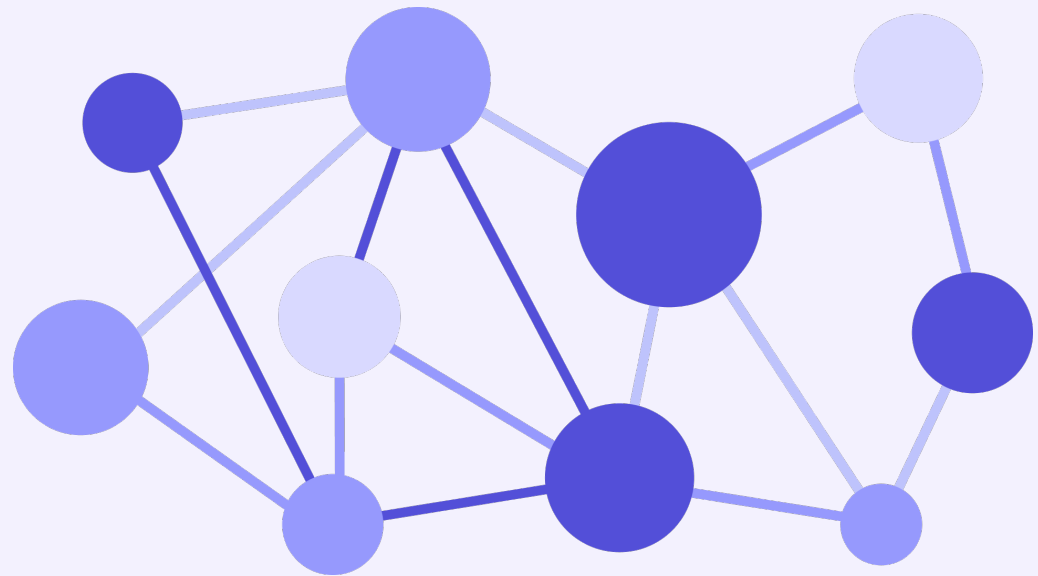
- Cloud-based vs. self-hosted?

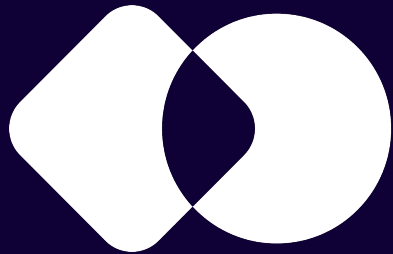
What level of certainty do we need?



Future opportunities

- Targeted data retention (aggregation + TTL)
- Universal data format
 - Apache Iceberg, Delta Lake
- Multi-source stream analysis
- AI/ML-based stream analysis
 - Flink ML, MLFlow
- Improved alert management





Sikt
Norwegian Agency for Shared
Services in Education and Research

