

PAVED PATHS LEADING THE WAY TO COMPLIANCE

CloudNativeCon+KubeCon EU 2023 - Amsterdam

Brian Nielsen (@briannielsen76) - Director of Technology
Kasper Nissen (@phennex) - Lead Platform Architect



LUNAR[®]

BRIAN NIELSEN

DIRECTOR OF TECHNOLOGY

Brian is a former engineer & architect turned exec
Working as Technology Director with expertise in
architecture, data, and finance.

He has a keen interest in domain-driven design and is
committed to bridging the gap between technology
and business



@briannielsen76

KASPER BORG NISSEN


LEAD PLATFORM ARCHITECT

Cloud Native Computing Foundation Ambassador
Community lead and founder at Cloud Native Nordics
Organizer and founder at Cloud Native Aarhus
Community Advocate at Ambassador Labs
Linkerd Ambassador
Occasional speaker at Meetups, Conferences

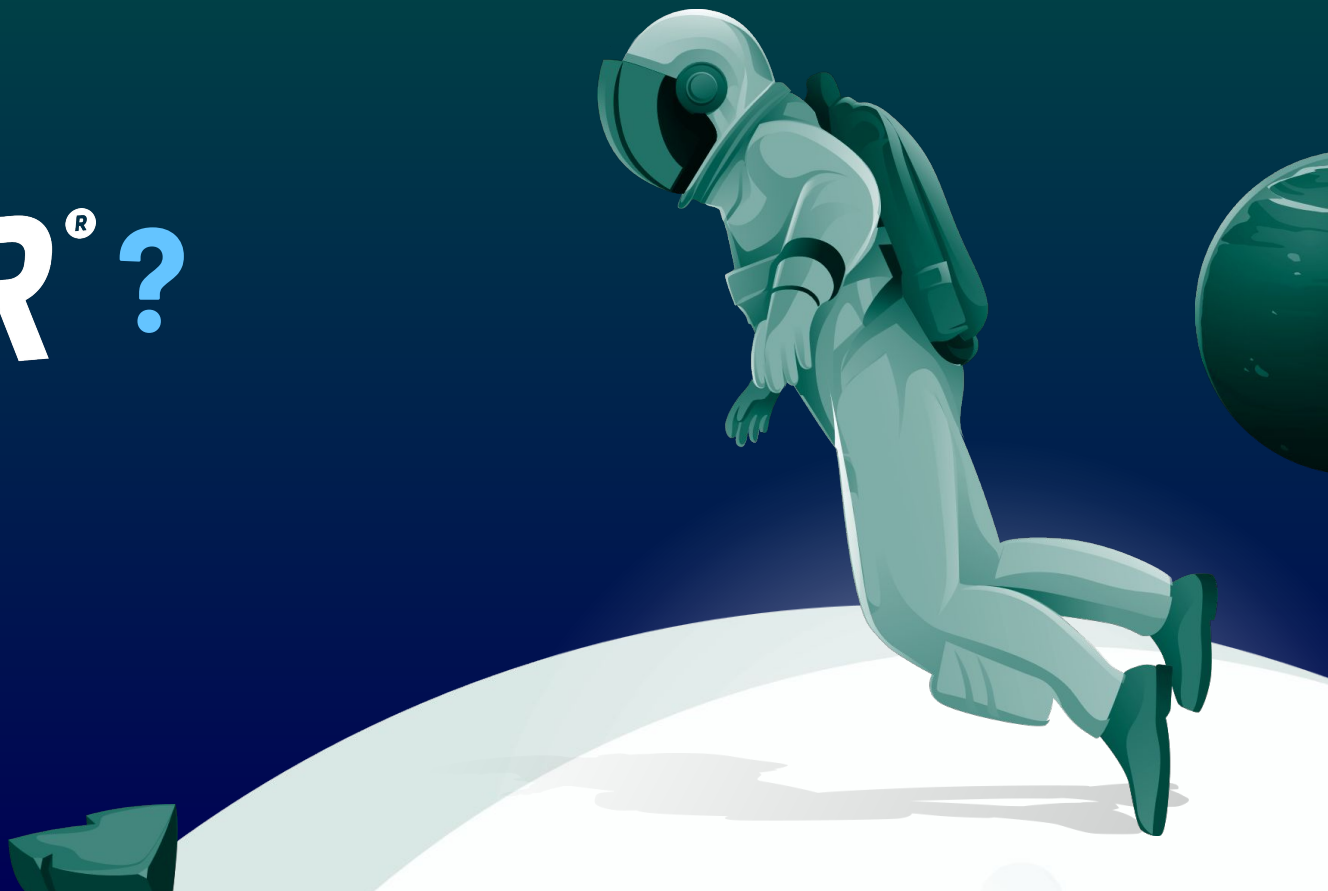


 @phennex

What to expect

- 1 What is Lunar?
 - 2 Compliance Requirements
 - 3 Ways of Working
 - 4 Backstage at Lunar, why and how?
 - 5 Backstage adoption
 - 6 Use case: Asset Management
 - 7 Next steps
- 

WHAT IS
LUNAR[®] ?



16#
Largest
bank in DK

Talents in Tech
113
(563 overall)

21
Squads

LUNAR TECHNOLOGY

+575K
Users
123K new in 2022

3
Hubs
CPH+AAR+STO

100+
Daily deploys

400+
Microservices

Founded in
2015

Our IT strategy is designed to fuel business growth

Technology should accelerate our ability to scale business opportunities

1

Domain driven design

3

Outsource based on domain distillation

2

Event driven design

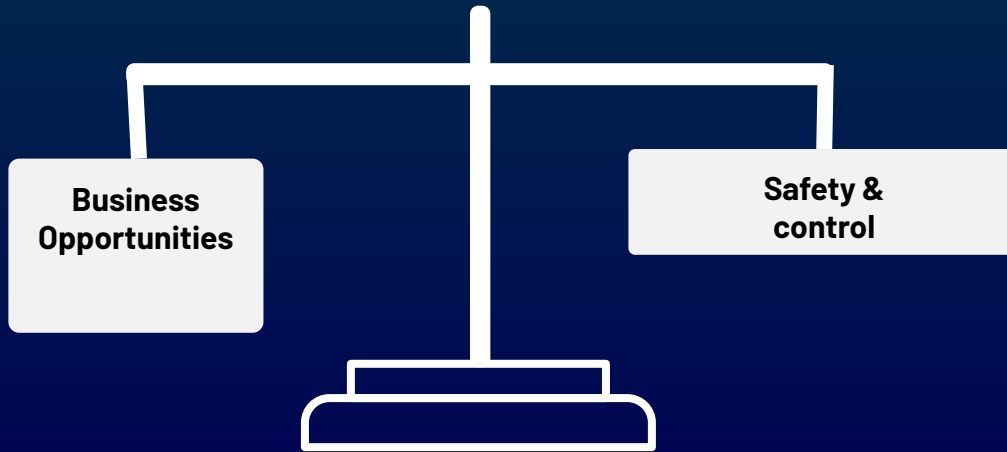
4

Paved Paths engineering



Speed and control is of the essence

Balancing speed of change with compliance



COMPLIANCE REQUIREMENTS



DFSA “Executive Order on Management and Control of Banks”

In Denmark it is specifically the addendum 5 IT-Strategy, IT risk policy and IT security policy that is in play for Technology

§ 23: Asset mgmt for critical functions

§ 24: Asset Classification

§ 25: Asset Confidentiality, integrity and availability

Retsinformation

Søg

Indholdsfortegelse >

Senere ændringer til forskriften

Lovgivning forskriften vedrører

Se detaljeret overblik

LOV nr 1155 af 08/06/2021

LBK nr 315 af 11/03/2022

LBK nr 406 af 29/03/2022

LBK nr 41 af 13/01/2023

Ændrer i/ophæver

Se detaljeret overblik

BEK nr 788 af 01/06/2022

Yderligere dokumenter

Alle cirkulærer, vejledninger m.v. til denne bekendtgørelse

Afgørelser truffet i henhold til

GELDENDE

BEK nr 1103 af 30/06/2022

Erhvervsministeriet

Yderligere oplysninger >

Bekendtgørelse om ledelse og styring af pengeinstitutter m.fl.¹⁾

I medfør af § 65, stk. 2, § 70, stk. 6, § 71, stk. 2, og § 373, stk. 4, i lov om finansiel virksomhed, jf. lovebekendtgørelse nr. 406 af 29. marts 2022, § 67, stk. 5, § 68, stk. 2, § 94, stk. 2, og § 270, stk. 1, i lov nr. 1155 af 8. juni 2021 om fondsmæglerselskaber og investeringservice og -aktiviteter, § 21, stk. 5, og § 39, stk. 3, i lov om realkreditlån og realkreditobligationer m.v., jf. lovebekendtgørelse nr. 315 af 11. marts 2022, § 180 g, stk. 3, og § 255 i lov om kapitalmarkeder, jf. lovebekendtgørelse nr. 2014 af 1. november 2021, som ændret ved lov nr. 2382 af 14. december 2021, fastsættes:

Kapitel 1

Anvendelsesområde

§ 1. Bekendtgørelsen finder anvendelse på følgende virksomheder, jf. dog stk. 4-9:

- 1) Pengeinstitutter.
- 2) Realkreditinstitutter.
- 3) Danmarks Skibskredit A/S.

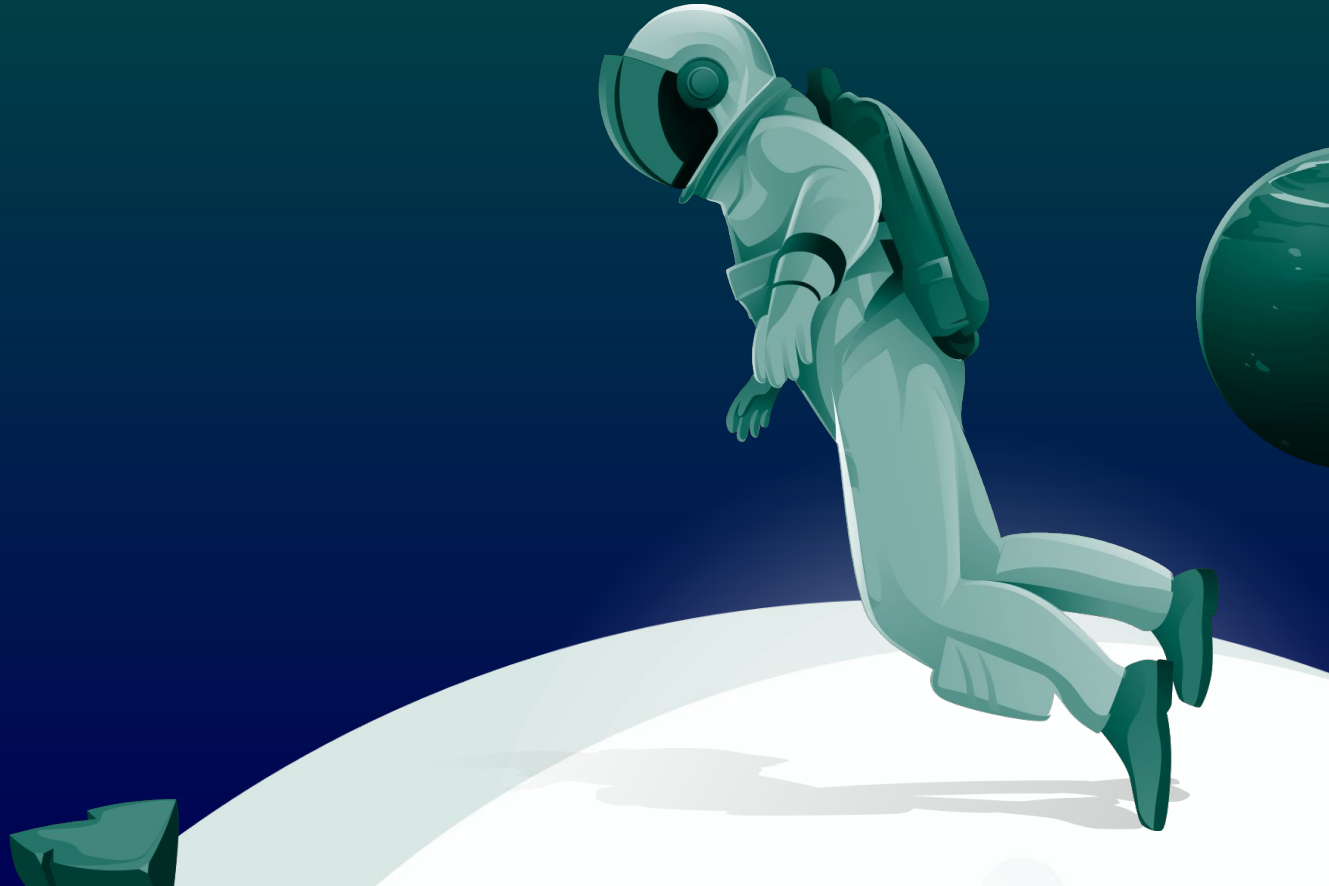
(In Danish - sorry but you get the drift)

Why have compliance? – Trust is key

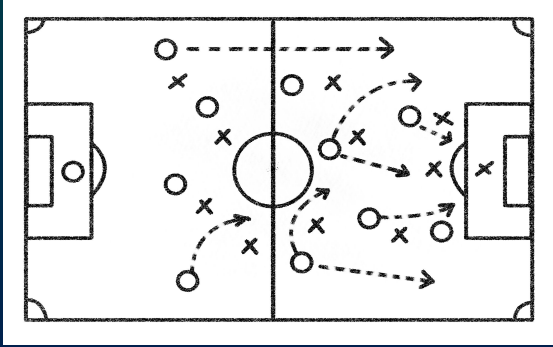
DFSA : “We are working for financial stability and confidence in financial undertakings and markets”



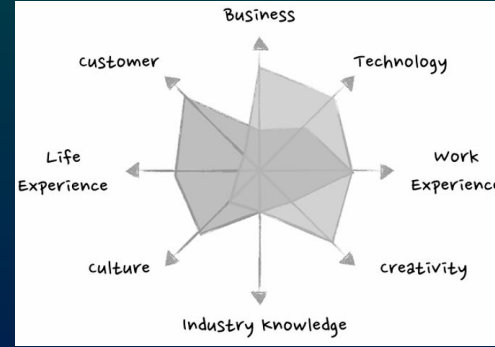
WAYS OF WORKING



Building the best product is a team sport



We believe in shared success and a 360 ownership across the business. Building the best product is a team sport, where you must secure all specialised competencies and skills to win.

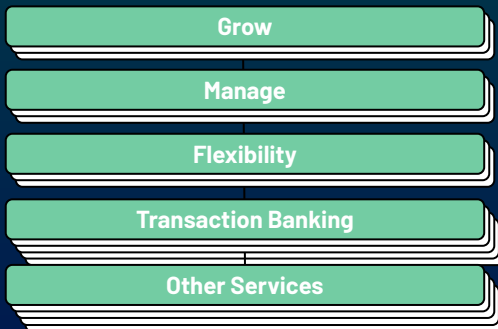


We believe cross-functional teams on a shared mission is the way to create high engagement and performance, and to beat competition.

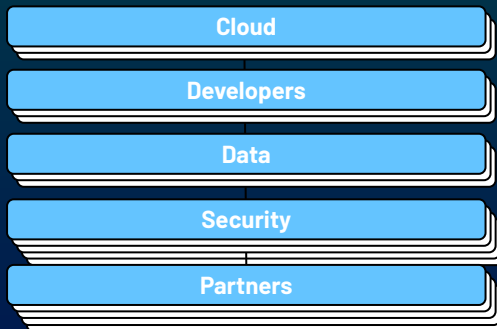
Lunar's application and cloud architecture

consists of +90 domains, supported by +400 microservices...

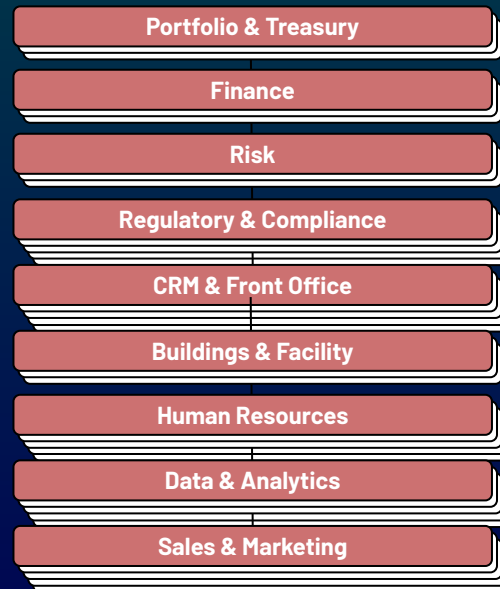
PRODUCT DOMAINS



ENGINEERING DOMAINS



SUPPORT DOMAINS



BUILDING INDUSTRY LEADING ENGINEERING PLATFORM TO HELP ENGINEERS FOCUS ON SOLVING REAL CUSTOMER PROBLEMS

18
SQUADS

PRODUCT CENTRIC SQUADS








Focused on delivering customer value

3
SQUADS

EMPOWER

Engineers

- Cloud
- Data
- Developers
- Partners
- Security

Seamless and compliant deployment	Fast feedback loop and safe to fail	Fast time to market & reuse	Explore Fast Developer Wiki	Scale and decouple	Lower engineering complexity	Self-healing application runtime	Unified data governance & DS tooling	Best in class standard security with easy sign-on
LUNAR [®] CI/CD	LUNAR [®] 	LUNAR [®] Code libraries and scaffolding	LUNAR [®] 	LUNAR [®] 	LUNAR [®] 	LUNAR [®] 	LUNAR [®] 	LUNAR [®] 

Paved paths leads the way

- ✓ Sane configuration defaults
 - HA
 - Resource limits
 - Changes to production requires 4 eyed review
- ✓ Secure by default
 - Least privilege
 - Service enforces global branch restriction rules
 - Release-manager ensures only master branch artifacts in production environments
 - Signed commits required
- ✓ Services are setup for day 2 operations
 - Suite of development libraries
 - Automatic dependency updates

BACKSTAGE AT LUNAR, WHY AND HOW?



MEET SPACY
Developer at Lunar





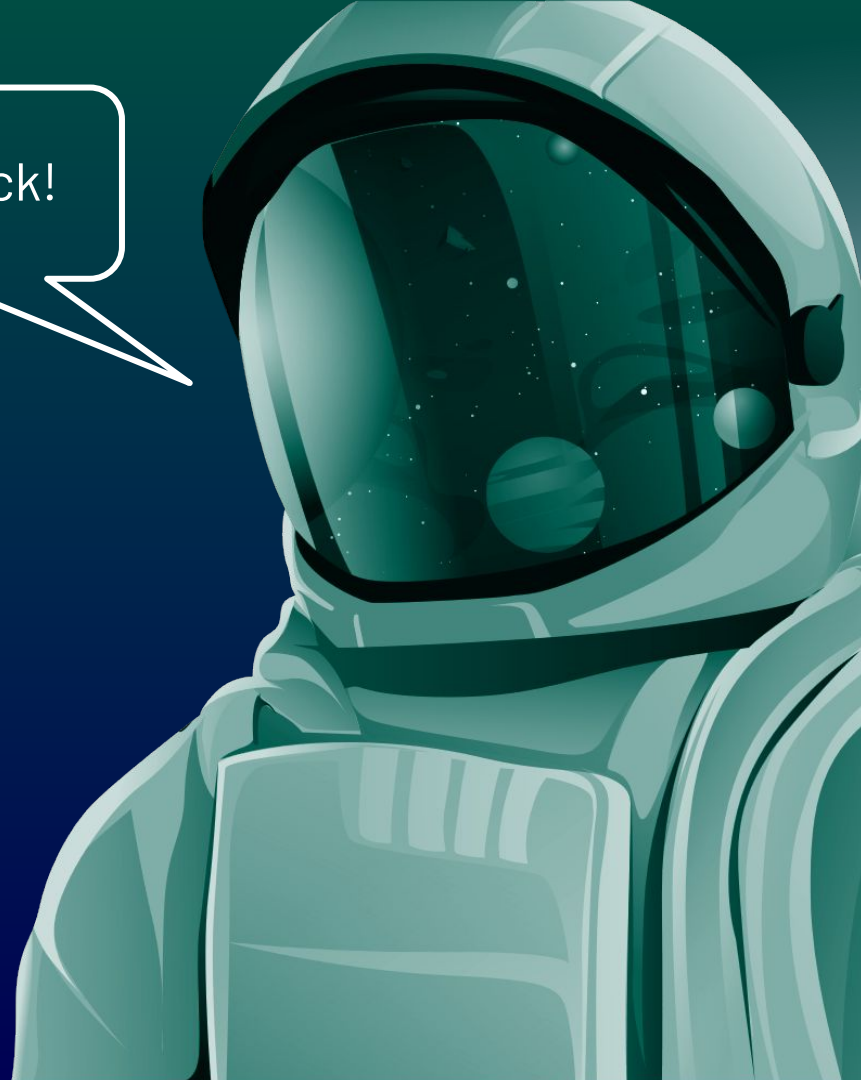
Awesome!
I'm ready!



GitHub
GO



CI/CD - check!



GitHub
GO

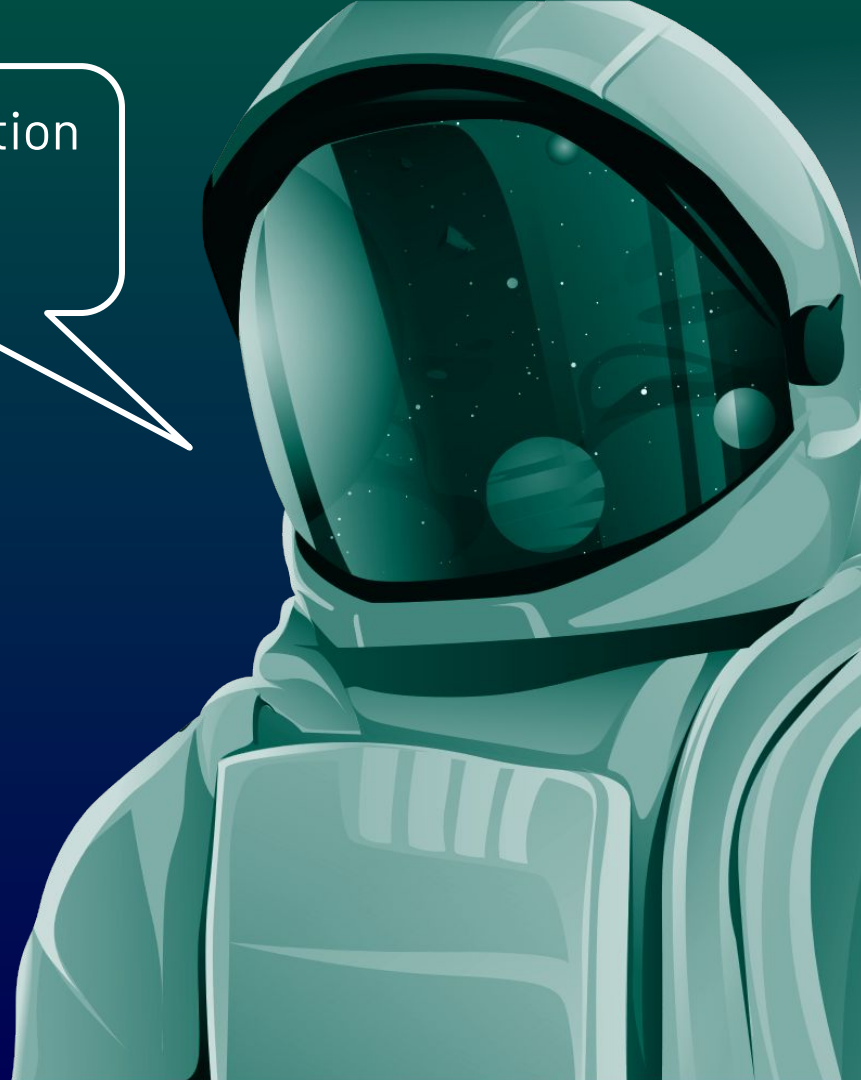


RabbitMQ

gRPC

GraphQL

Communication
protocols..
check!



GitHub

GO



RabbitMQ

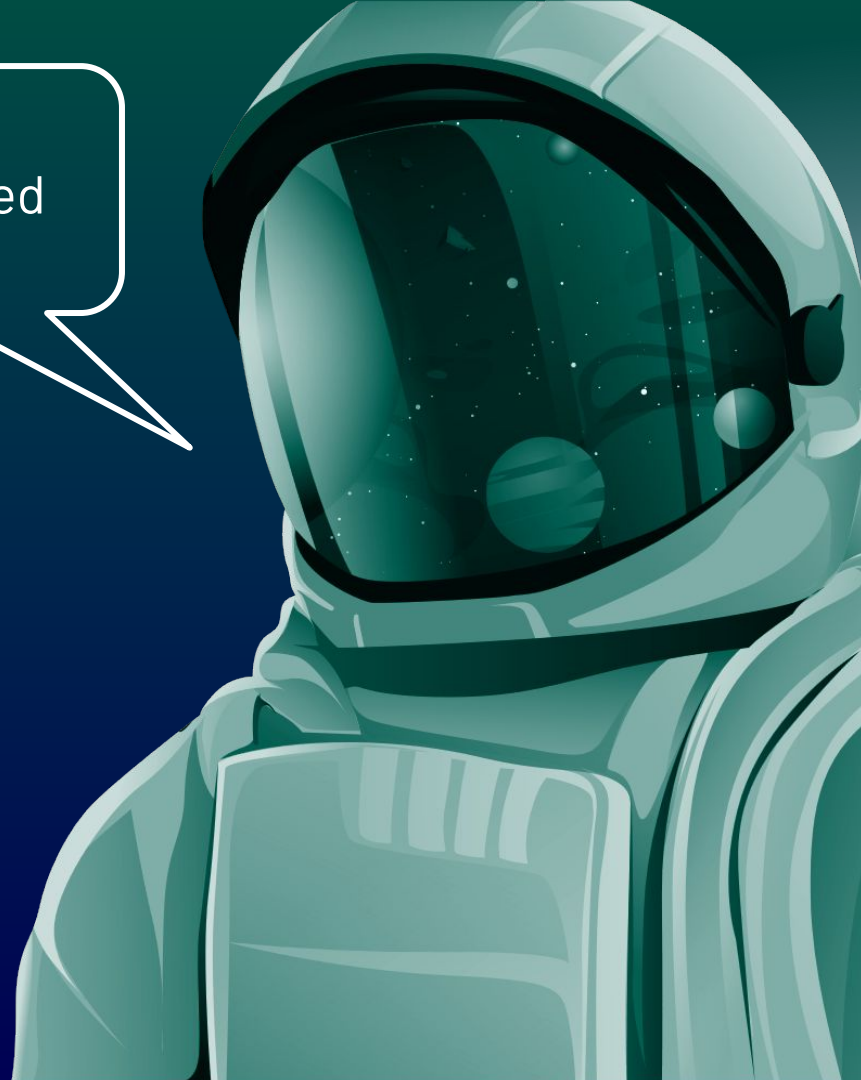
gRPC

GraphQL

aws



Uhh! I guess that's required knowledge!



GitHub
GO



RabbitMQ

gRPC

GraphQL

aws



Are you kidding
me?



Git!



RabbitMQ

gRPC

GraphQL



PROBLEM

Developers were getting overwhelmed with the amount of systems and knowledge required to take on the required ownership.

GOAL

Minimize the cognitive load on developers, and provide them with clear actionable information.





Backstage to the rescue.



But first, let's talk about shuttle

shuttle.yaml

```
plan: git://.../lw-shuttle-go-plan.git
vars:
  service: prometheus
  squad: odyssey
  domain: observability

  ingress: true
  db: true

  k8s:
    dev:
      env:
        log.level: debug
```



shuttle

```
$ shuttle run build
$ shuttle run push
$ shuttle run generate_config
...
```

Anatomy of a service repository

All go service repositories looks more or less the same.

```
.
├── CODEOWNERS
├── Jenkinsfile
├── README.md
├── api
├── cmd
├── go.mod
├── go.sum
├── internal
├── renovate.json
└── shuttle.yaml
```



Entity
processors

```
apiVersion: backstage.io/v1alpha1
kind: Component
metadata:
  name: service
  description: ..
  annotations:
    lunar.tech/domain: domain
spec:
  type: service
  owner: squad-A
  providesApis:
    - service-api
```

account-block | Overview | Lun x +

/catalog/default/component/account-block

LUNAR

COMPONENT — SERVICE

account-block ☆

Owner: squad-maven Lifecycle: unknown

SEARCH

OVERVIEW SECURITY CI/CD PULL REQUESTS TODOS RELEASES DEAD LETTER

Your Squads

Catalog

Docs

APIs

On Call

Dead Letter

Reconstitution

Tech Insights

Create...

Feedback

Settings

Readme

Account Block

This service maintains the block status of an account. The service consumes user suspension events, in order to block the accounts owned by that user. Furthermore, it exposes an API for setting block codes on individual accounts. This API is used by Lunar Employees in Houston CRM in order to block accounts due to FCP and other cases.

Other services downstream consumes the `AccountBlockStatusUpdated` in order to make business decisions based on the block codes.

- Account Management consumes the event in order to decide if the account should have interest and/or overdraft interest disabled.
- Card Management consumes the event in order to decide if cards associated with the account should be blocked.

Terms

Term	Description
Block code	A block code that can be used by downstream consumer to decide how to respond to the account being blocked.
User suspension	When the user is suspended for some reason. That could for example be due to fraud or security

Events

Event	Description
AccountBlockStatusUpdated	Emitted when the account status changes

About

VIEW SOURCE VIEW TECHDOCS

DESCRIPTION

Responsible for handling account block status

OWNER: squad-maven SYSTEM: account-block TYPE: service

LIFECYCLE: unknown TAGS: golang

Observability

Humio Grafana Tracing

Score Cards

Valid Domain Components with valid domains. ✓



Solving the needs

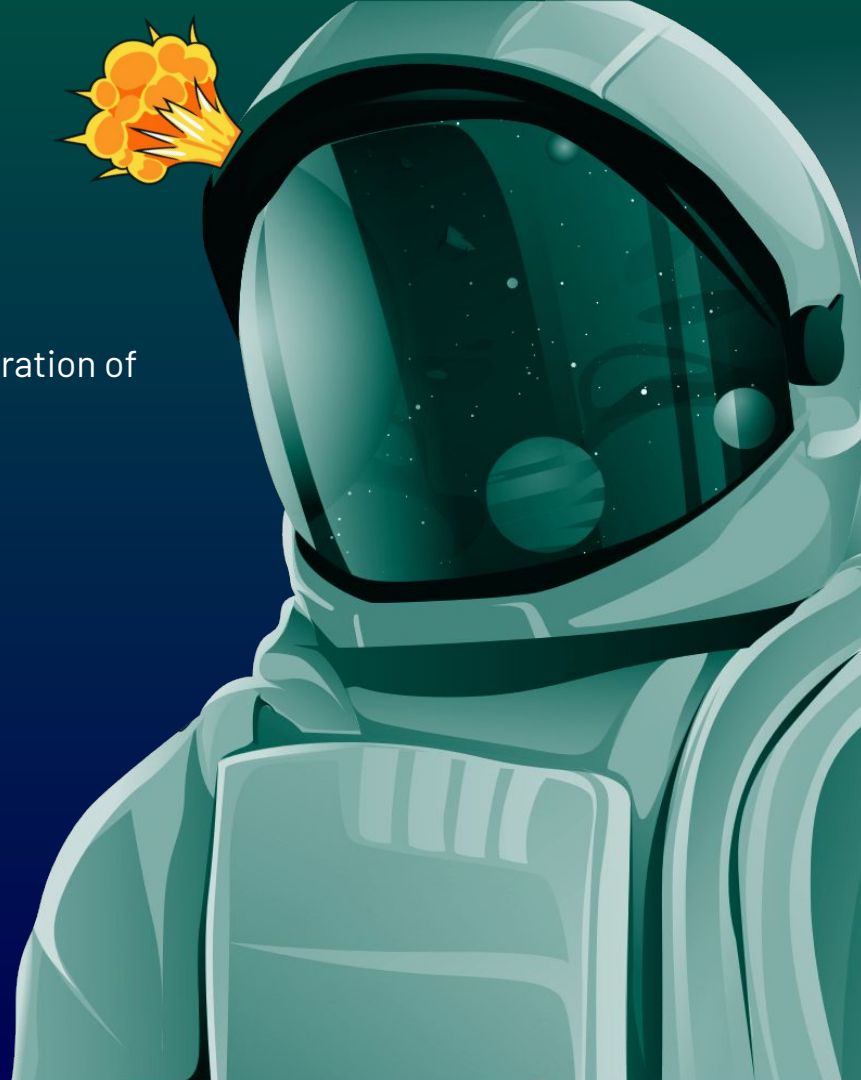
Empower developers to do what they need without requiring them to use Backstage.



Setting up a new service

Setting up a new service required a lot of manual configuration of

- Github Repository
 - Copy over files
 - Configure branch restriction
- Configure Docker Registry
- Setup release policies
- Etc.



The screenshot shows the LUNAR web application interface for creating a new component. The main heading is "Create a New Component" with the subtitle "Create new software components using standard templates". A search bar is present above the "Available Templates" section. The interface is divided into a left sidebar and a main content area.

Left Sidebar:

- Search
- Your Squads
- Catalog
- Docs
- APIs
- On Call
- Dead Letter
- Reconstitution
- Tech Insights
- Create...
- Feedback
- Settings

Main Content Area:

Available Templates (Support icon)

Search

PERSONAL

- Starred: 0

LUNAR

- All: 13

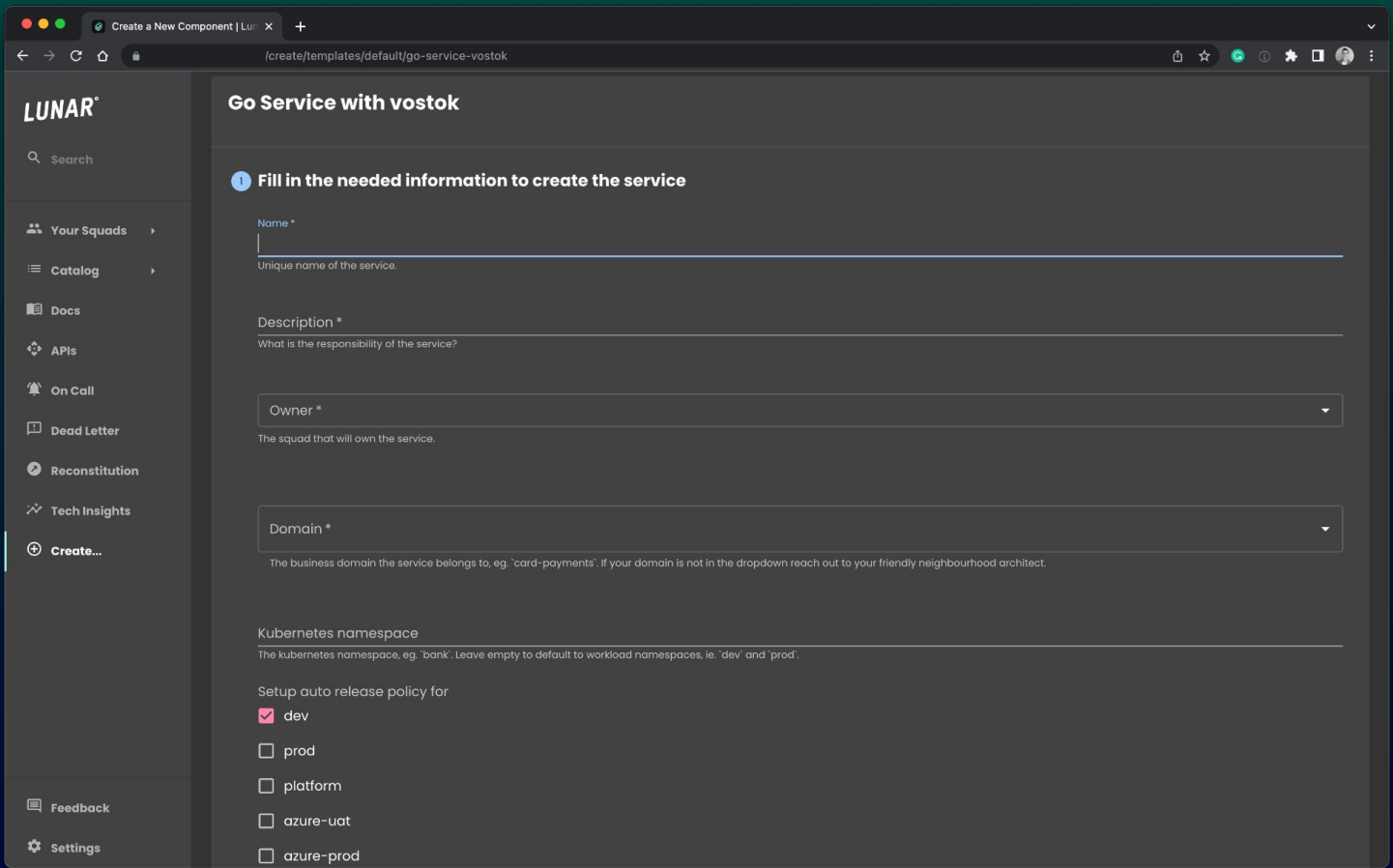
CATEGORIES

Dropdown menu

Templates

Template Name	Category	Description	Owner	Tags	Action
documentation Docs Repository	documentation	Creates a docs repository which is integrated into backstage.	squad-aura		CHOOSE
service Empty Repository	service	Creates a near empty repository with default Lunar files	squad-aura		CHOOSE
service Empty RPA Library Repository	service	Creates a near empty RPA library repository with default Lunar files	squad-pioneer		CHOOSE
service Empty RPA Process Repository	service	Creates a near empty RPA process repository with default Lunar files			
service Empty RPA REFramework Process Repository	service	Creates a near empty RPA REFramework process repository with default Lunar files			
cli Go CLI	cli	Create a new Go cli	squad-aura		

Service generation using Backstage scaffolder



Go service with vostok



That was
almost to easy!





Enable DIY

Showcase how developers can
create their own plugins.



Reconstitution | Add Job | Lun... x +

/reconstitution?env=dev

LUNAR

Search

Your Squads >

Catalog >

Docs

APIs

On Call

Dead Letter

Reconstitution

Tech Insights

Create...

Feedback

Settings

TOOL

Reconstitution

Republish Integration Events to services

Owner
squad-skylab

Env
dev

Add Job

Receiver * Producer *

Service to receive events

Domain and entity type producing events

From To Entity IDs Event Names

Entity IDs to publish events for

Event names to publish events for

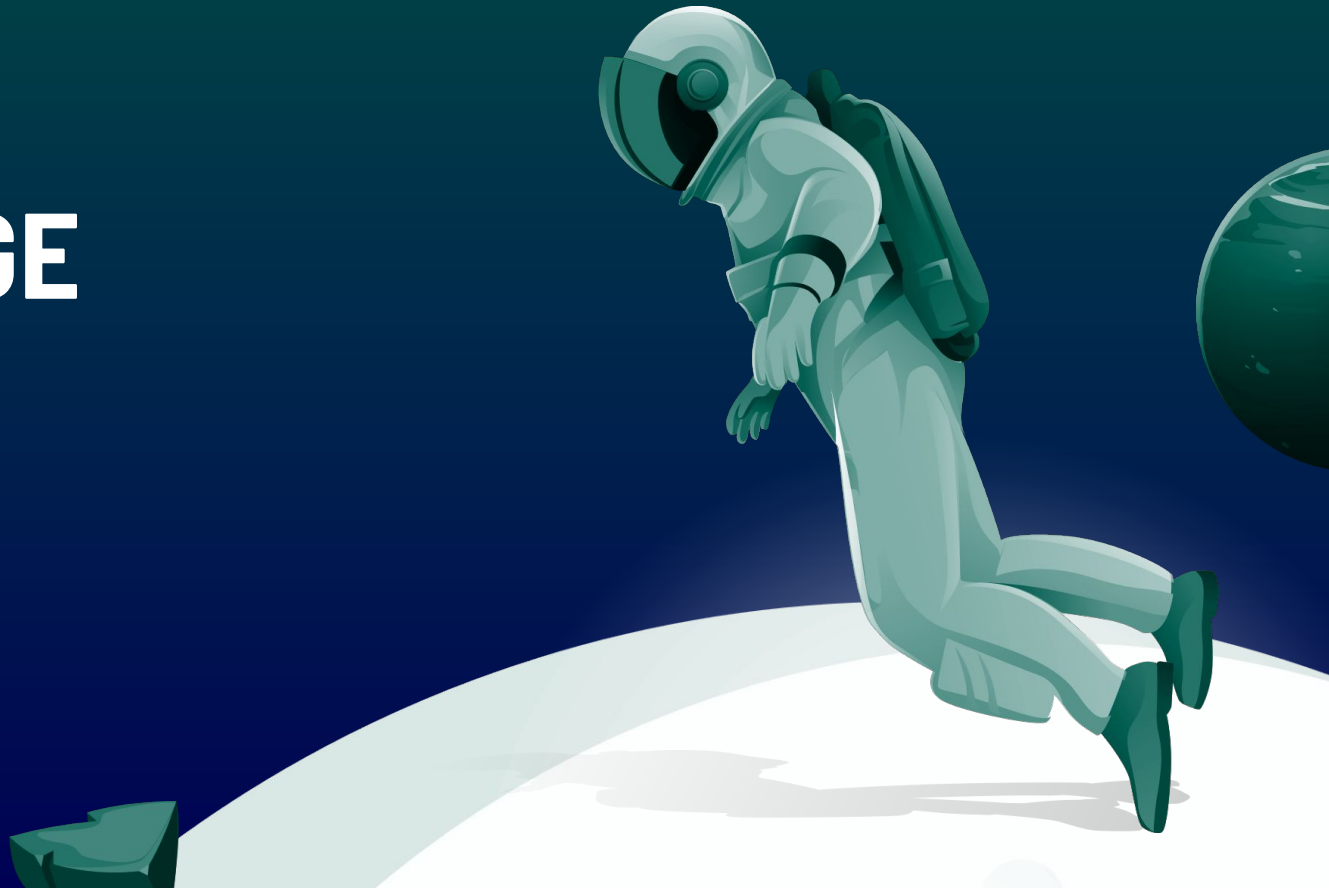
Jobs

Filter

STATUS	ACTIONS	RECEIVER	PRODUCER	CREATED	CREATED BY
COMPLETED		insurance	organisation [organisation]	10/04/2023, 20:46:58	user:default/davidmorch
COMPLETED		insurance	organisation [organisation]	10/04/2023, 16:58:32	user:default/davidmorch
COMPLETED		insurance	organisation [organisation]	10/04/2023, 13:09:25	user:default/davidmorch
COMPLETED		insurance	organisation [organisation]	10/04/2023, 13:07:51	user:default/davidmorch

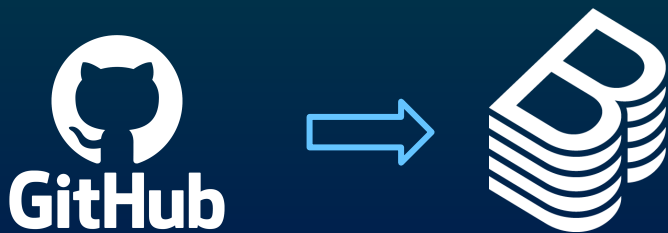
Reconstitution

ADOPTING BACKSTAGE



Paved paths leads the way...

Backstage Scaffolder has allowed us to lock down creation of git repositories in Github.



Every repository is created through Backstage with sane defaults, and everything set up, and ready to go.

What's in the default package?

CI pipeline with security checks and scanning

Automatic updates of dependencies

Configuration of external dependencies taken care of.

```
.
├── CODEOWNERS
├── Jenkinsfile
├── README.md
├── api
├── cmd
├── go.mod
├── go.sum
├── internal
├── renovate.json
└── shuttle.yaml
```

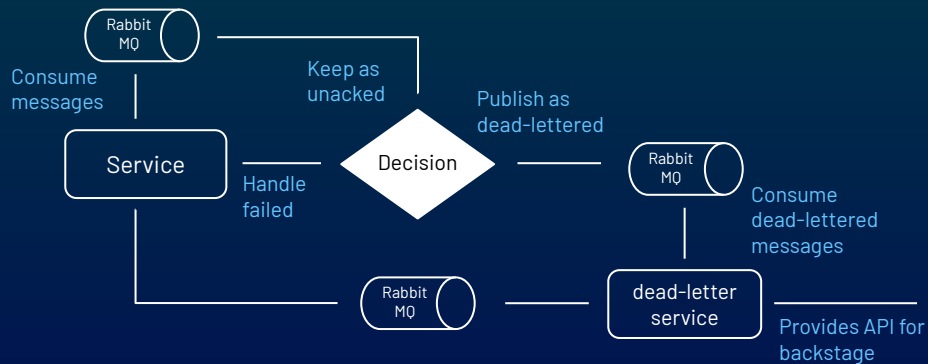
Github configuration;
- Branch protection on **main** branch
- CODEOWNERS - Approval requirement

Initial go-service configuration
Use `shuttle` to generate code

Service ownership, default runtime configuration for the environments



Critical systems and paths



The screenshot shows the LUNAR Dead-letter Squad Overview dashboard. The dashboard displays a table of squads and their message counts. The table has two columns: SQUAD and MESSAGES. The squads listed are: squad-opolo (27), squad-omnis (1547), squad-omni (80), squad-odds (899), squad-ours (8), squad-ossight (1480), squad-ort (799), squad-obergarity (300), squad-gemets (2289), squad-hardon (133), and squad-juno (370).

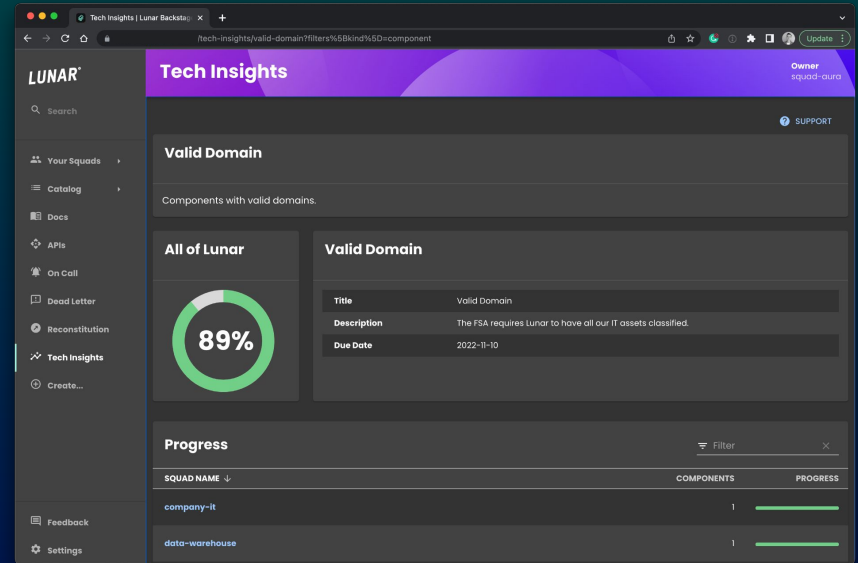
SQUAD	MESSAGES
squad-opolo	27
squad-omnis	1547
squad-omni	80
squad-odds	899
squad-ours	8
squad-ossight	1480
squad-ort	799
squad-obergarity	300
squad-gemets	2289
squad-hardon	133
squad-juno	370

The screenshot shows the LUNAR web application interface. The top navigation bar includes the LUNAR logo, a search bar, and the team name "squad-aura". Below this, a secondary navigation bar lists tabs: OVERVIEW, DEAD LETTER, DOCS, TECH INSIGHTS DETAILS, and ABOUT. The main content area is divided into two sections. The first section, titled "Dead lettered messages", shows a donut chart with the number "18" in the center, indicating the count of dead lettered messages. A "Handle now" button is located below the chart. The second section, titled "Open pull requests", displays a list of pull requests with their status and author information. The pull requests are categorized into three groups: REVIEW REQUIRED, REVIEW IN PROGRESS, and APPROVED. The REVIEW REQUIRED group includes a pull request for "Hide on-call in sidebar and router" by kaspennissen. The REVIEW IN PROGRESS group includes a pull request for "add: add FXRateCurrencyDkk and FXRateEurDkk fielts to ..." by igpemar. The APPROVED group includes a pull request for "Patch/1.11.1" by mahlunar. The bottom of the screenshot shows a URL bar with the address: https://backstage.lunar.tech/catalog/default/Group/squad-aura/dead-letter?env=...

Dead-lettered messages on Squad pages

Gathering insights and surface progress...

Tech-insights helps us surface information on components by comparing it against the rest of the organization.



squad-cassini | Tech Insights

/catalog/default/Group/squad-cassini/tech-insights/checks/valid-domain?filters%5Bkind%5D=component

LUNAR

GROUP — TEAM

squad-cassini

Search

OVERVIEW DEAD LETTER DOCS TECH INSIGHTS DETAILS ABOUT

Your Squads

Catalog

Docs

APIs

On Call

Dead Letter

Reconstitution

Tech Insights

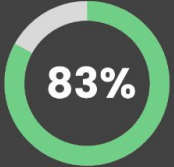
Create...

Feedback

Settings

Valid Domain

Components with valid domains.



83%

Valid Domain

Components with valid domains.

Title	Valid Domain
Why	The FSA requires Lunar to have all our IT assets classified.
What	The vars.domain field in shuttle.yaml has a valid value from the catalog domain list
How	Domain docs
Action	Click on each button in 'Items to Complete' to set the domain

Items to complete 1

GO-ISO20022-PARSER

Completed Items 5

crackkey-files-gal

Providing squad-level action items and progress

Driving adoption...

- ★ Show potential
- ★ Collect feedback
- ★ Make it fit
- ★ Critical paths & systems
- ★ Inner sourcing
- ★ Reduce friction



USE-CASE: ASSET MANAGEMENT & MORE



Why asset management?



Increase
performance



Mitigating
risk



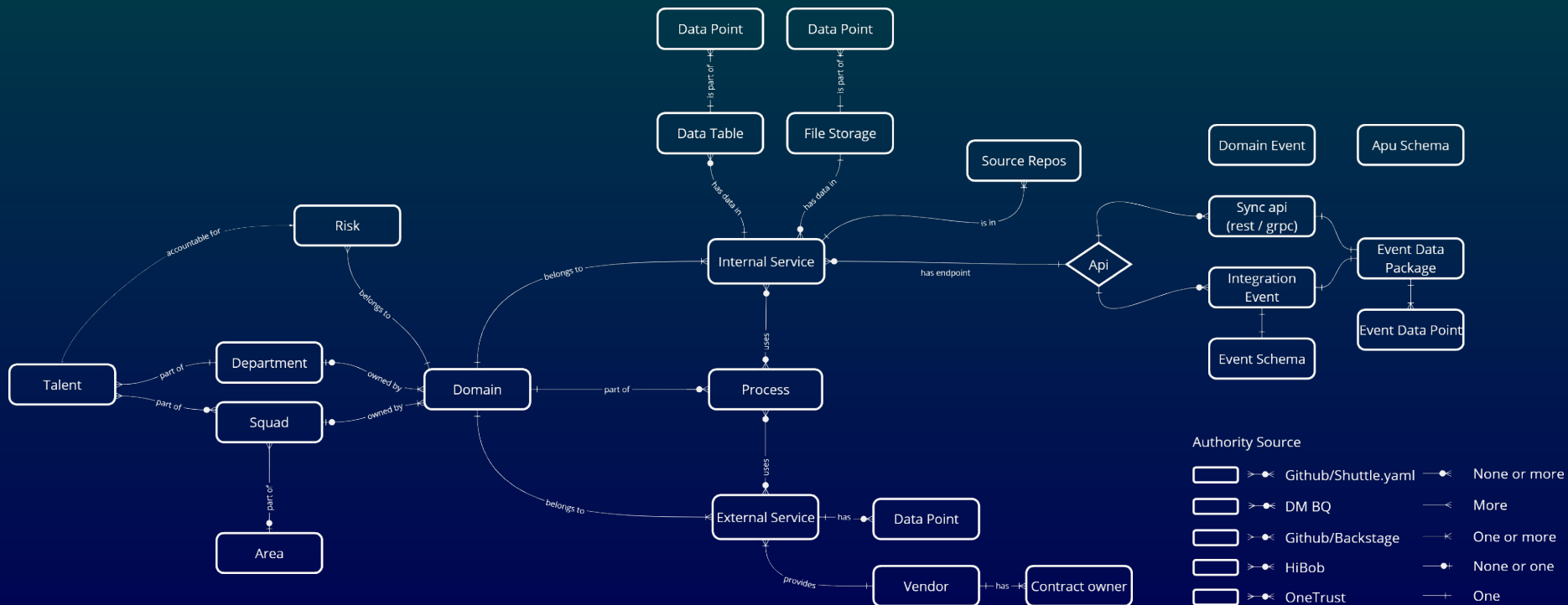
Regulator
requirements
according to
DFSA



Building
customer
trust and
satisfaction.

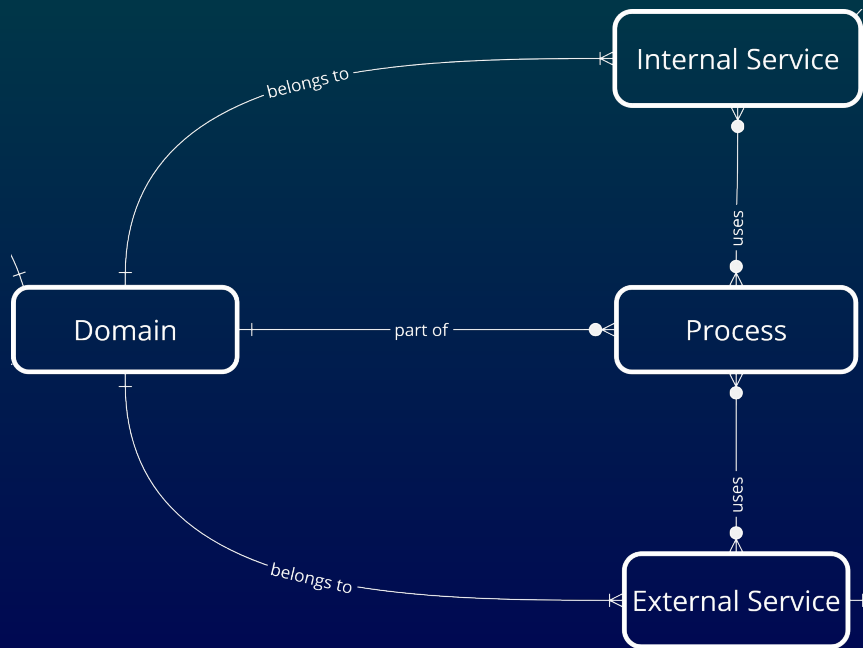
Asset modelling overview

We are in Lunar documenting assets on many levels



Asset modelling overview

We are in Lunar documenting assets on many levels



LUNAR Lunar Catalog

SEARCH

CREATE COMPONENT SUPPORT

Domains -

PERSONAL

- Owned 0
- Starred 0

LUNAR

- All 97

OWNER

- OWNERS

TER

- TER

AREA

- AREA

COLONY

- COLONY

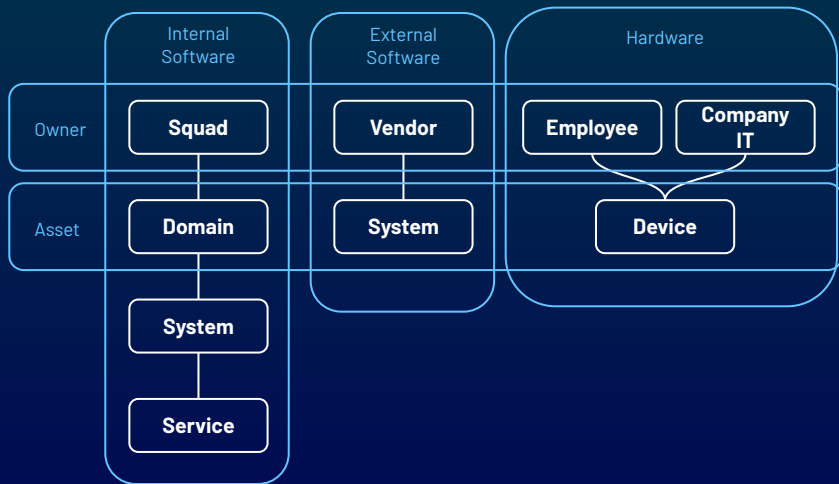
All (97)

NAME	TER	AREA	COLONY	OWNER	ACTIONS
Account Management Creation and management of personal accounts and granting access rights/agreements (Current accounts)	Product Portfolio	Financial Management	sq-asi-genius	sq-asi-genius	🔍 ⚙️ ⭐
Account Settlement The ability to receive settlement files and do reconciliation towards the Lunar financial reporting in certain cases (reversed / dispute)	Banking Services	Transaction Banking	sq-asi-orion	sq-asi-orion	🔍 ⚙️ ⭐
Account Statement Export Exporting account statements (transactions) in various formats (CSV, Excel, etc.)	Banking Services	Unknown	sq-asi-juno	sq-asi-juno	🔍 ⚙️ ⭐
Agreements / Subsidies / Terms Management for the different agreements needed to either be, partly into a subsidiary in the Lunar group (needed to receive a product offered by the Lunar group)	Product Portfolio	Unknown	sq-asi-phoenix	sq-asi-phoenix	🔍 ⚙️ ⭐
AML Reporting to Financial Intelligence Unit Suspicious Activity Reports and Suspicious Transfer Reports of Users we have deemed necessary to report due to suspicion of financial crime	Banking Services	Unknown	sq-asi-burayor	sq-asi-burayor	🔍 ⚙️ ⭐
Async Messaging Provides Async Messaging including SINK, Dead lettering, Deferred messaging, Time Ticks	Empower	Empower	sq-asi-euro	sq-asi-euro	🔍 ⚙️ ⭐
Backend Q&A Provides Q&A tooling for backend developers, including feedback and statistics	Empower	Empower	sq-asi-euro	sq-asi-euro	🔍 ⚙️ ⭐
Banking Central Integration The ability to communicate to and from the BIC banking central for payments, accounts, customers, loans, FIO's and more	Banking Services	Transaction Banking	sq-asi-orion	sq-asi-orion	🔍 ⚙️ ⭐
Benefits Administration of benefits of being a Lunar customer, such as special promotion codes	Product Portfolio	Financial Management	sq-asi-titanus	sq-asi-titanus	🔍 ⚙️ ⭐

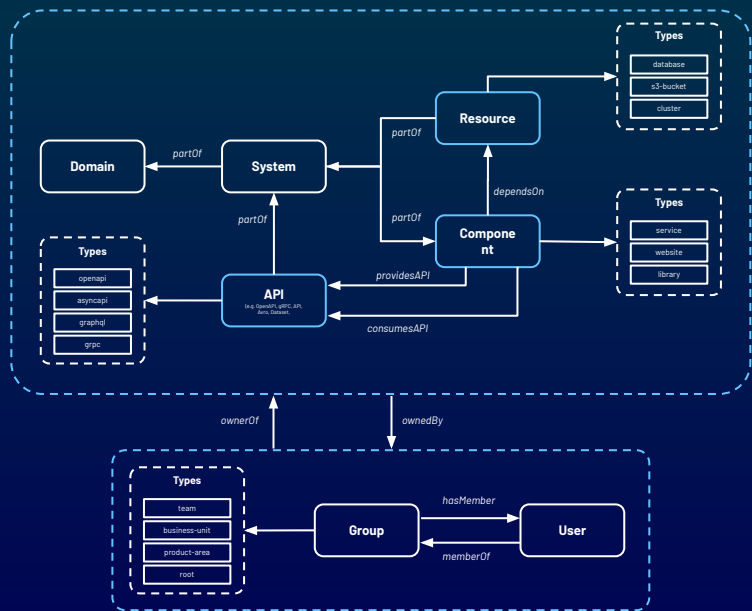
Domain as Assets

We have currently chosen our domains as asset classification level

Lunar



Backstage



Asset classification

Assets are classified as either:

- **Tier 1: Mission critical**
- **Tier 2: Highly critical**
- **Tier 3: Non critical**

Based on the criticality classification there might be set different requirements for the asset



Search

Your Squads

Catalog

Docs

APIs

On Call

Dead Letter

Reconstitution

Tech Insights

Create...

Feedback

Settings

Domains

CREATE COMPONENT

SUPPORT

PERSONAL

Ownec 0

Starrec 0

LUNAR

All 2

OWNER

SQUAD...

TIER

1

AREA

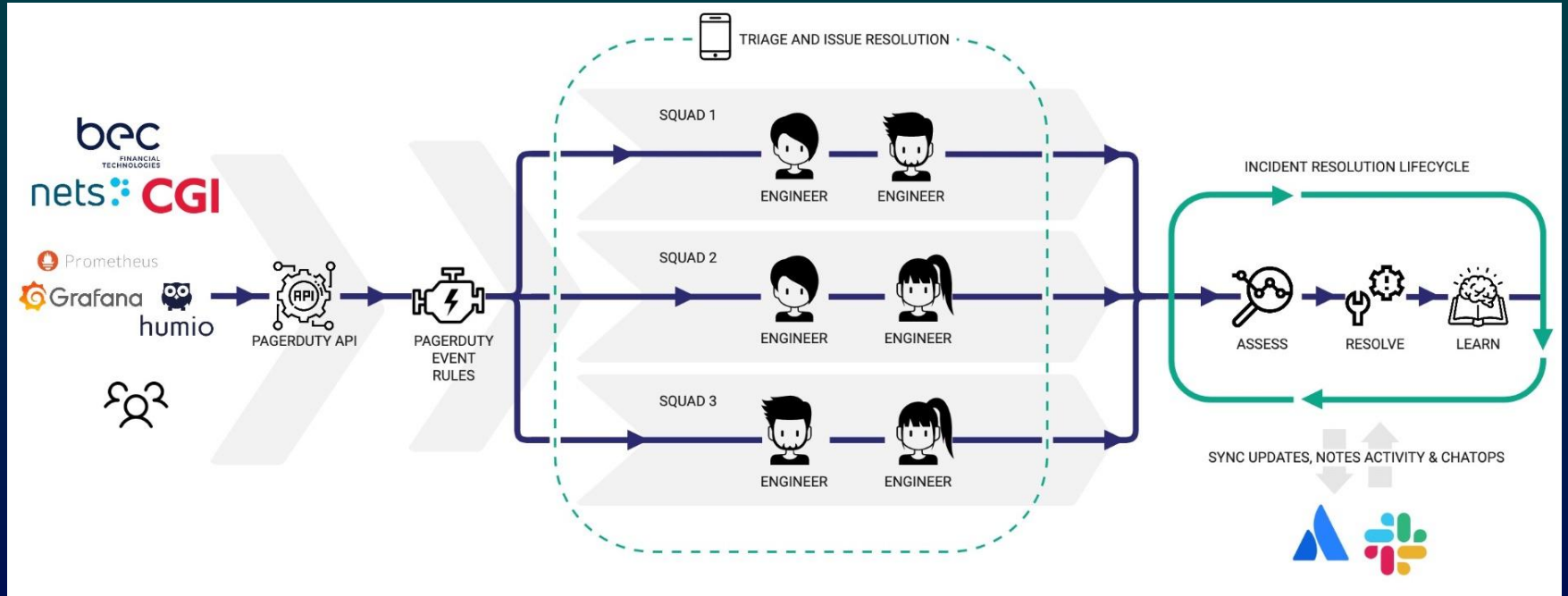
COLONY

All (2)

Filter

NAME	TIER	AREA	COLONY	OWNER	ACTIONS
Card Payments All processes around the use of a Lunar Card to do Payments.	1	Banking Services	Transaction Banking	squad-skylab	
Card Utility All utilities around the use of a Lunar Card	1	Banking Services	Transaction Banking	squad-skylab	

Incident response



Automating controls to ensure continuous compliance

AWS config change

rds-storage-encrypted Actions ▾

▼ Rule details Edit

Description
Checks whether storage encryption is enabled for your RDS DB instances.

Config rule ARN
arn:aws:config:eu-west-1:183926245532:config-rule/config-rule-bk5grz

Trigger type
• Oversized configuration changes
• Configuration changes

Last successful evaluation
🟢 March 30, 2022 8:14 AM

Scope of changes
Resources
Resource types
RDS DBInstance

Parameters

Key	Type	Value	Description
kmsKeyId	String	-	KMS key ID or ARN used to encrypt the storage.

▼ Resources in scope View details Remediate ↻

All ▾ < 1 2 > ⌂

ID	Type	Status	Annotation	Compliance
<input type="radio"/> production-rds	RDS DBInstance	-	-	🟢 Compliant
<input type="radio"/> crypto-rds	RDS DBInstance	-	-	🟢 Compliant
<input type="radio"/> lunar-openbanking-back...	RDS DBInstance	-	-	🟢 Compliant
<input type="radio"/> dead-letter	RDS DBInstance	-	-	🟢 Compliant
<input type="radio"/> auth	RDS DBInstance	-	-	🟢 Compliant

Humio & snyk alerts

Humio APP 08:05

Humio Alert

Develop query against authentication database - Click to Open in Humio

Env
<NO VALUE>

Query type
<NO VALUE>

Database
authentication

Database host
<NO VALUE>

Timestamp
2022-03-30 06:05:41

Developer
mzc

Today at 08:05

Humio APP 17:18

Humio Alert

Developer CloudTrail action not READONLY - Click to Open in Humio

Request IP address
AWS Internal

Request parameters
<NO VALUE>

AWS account ID
183926245532

Event name
CreateInvalidation

Event source
cloudfront.amazonaws.com

Developer email
che@lunar.app

AWS Region
us-east-1

Yesterday at 17:18

TwilightMoonBeam APP 12:10

Snyk Alert

alert/audit/github/changes-to-branch-protections - Click to Open in Humio

GitHub - Change to branch protection rule

Default branch
main

Changed rule for branch
main

Timestamp
2022-11-14T11:10:52.082Z

Action
created

Repository
lunar-feature-toggles-framework-ios

User
MadsBogeskov

New 14th

snyk-bot APP 11:04

Snyk Input Validation

New vulnerability in package go-lang.org/x/text/language at the Squad

Artemis organization.

Severity **Medium** Package go-lang.org/x/text/language

Issue ID
SNYK-GOLANG-GOLANGORGXTEXTLANGUAGE-3043869

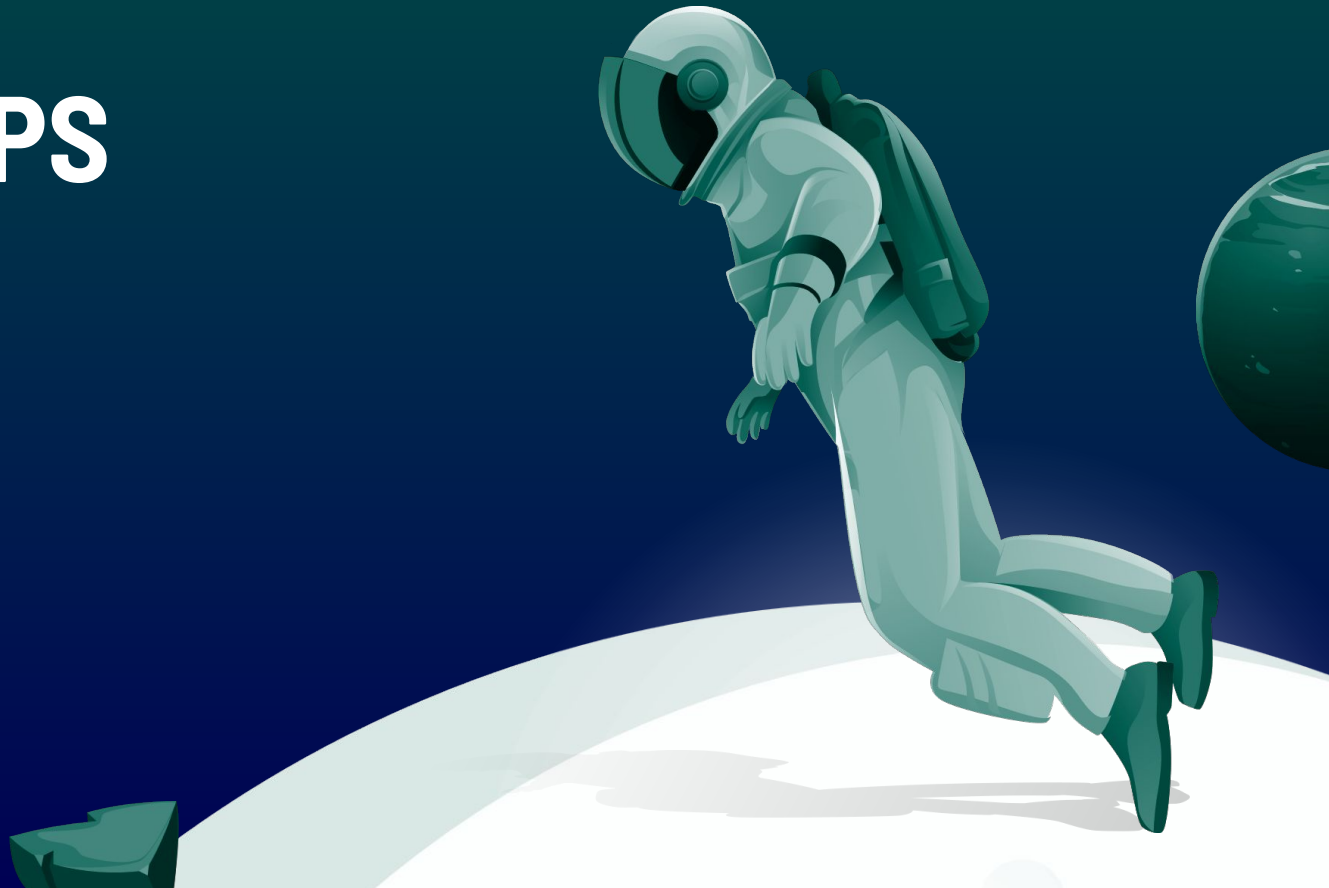
Affected projects:

- lunar-way-credit-application-flow-service:go.mod

Package version: 0.3.7

Fix manually or ignore

NEXT STEPS



What do we have today?

Catalog: software asset management

Techdocs: keeping docs together with the code and dynamically updated

Scaffolder: make it easy to create new services

Catalog-graph: graphing the software catalog

Pagerduty: trigger on-call schedules

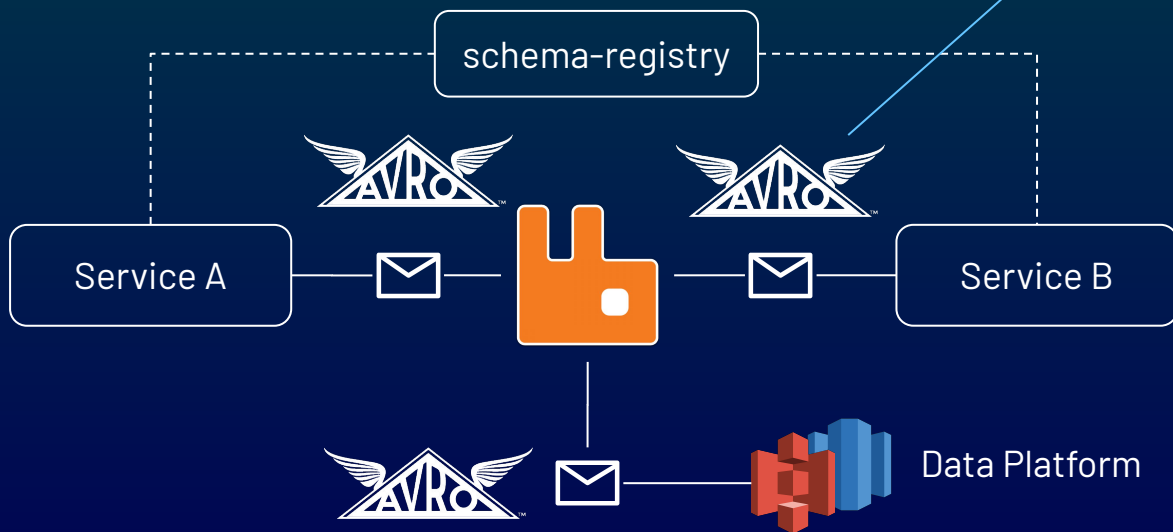
Reconstitution: resend events

Dead Letter: handle events that failed

Tech-insights: provide progress on squad and company level

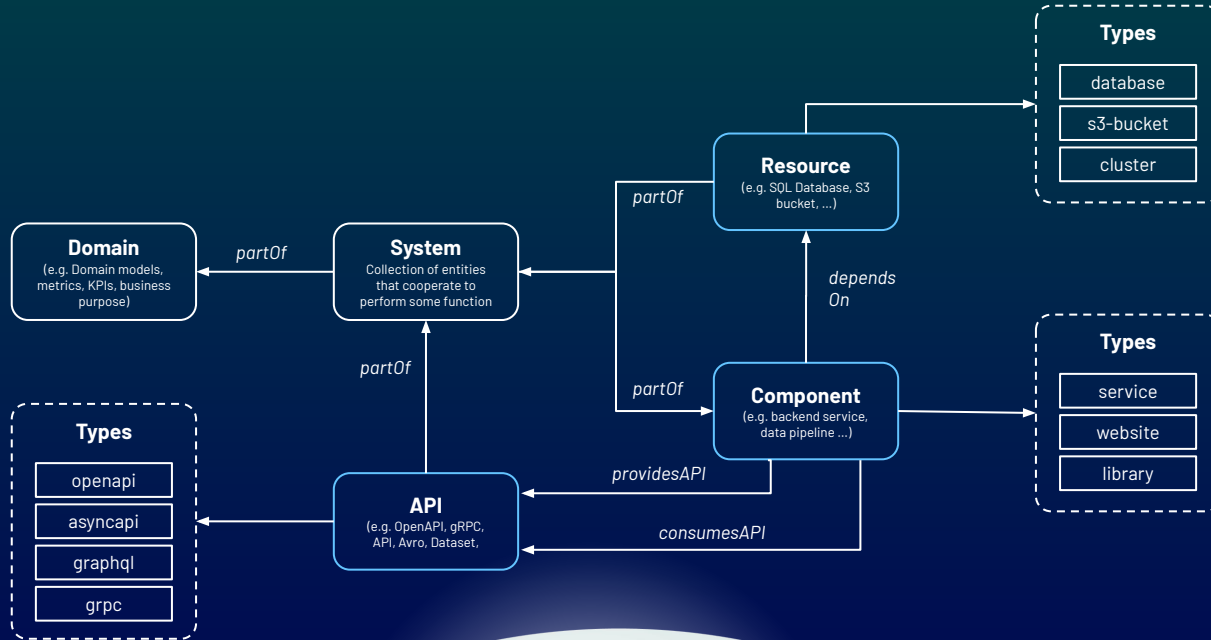


Event schemas and PII Data

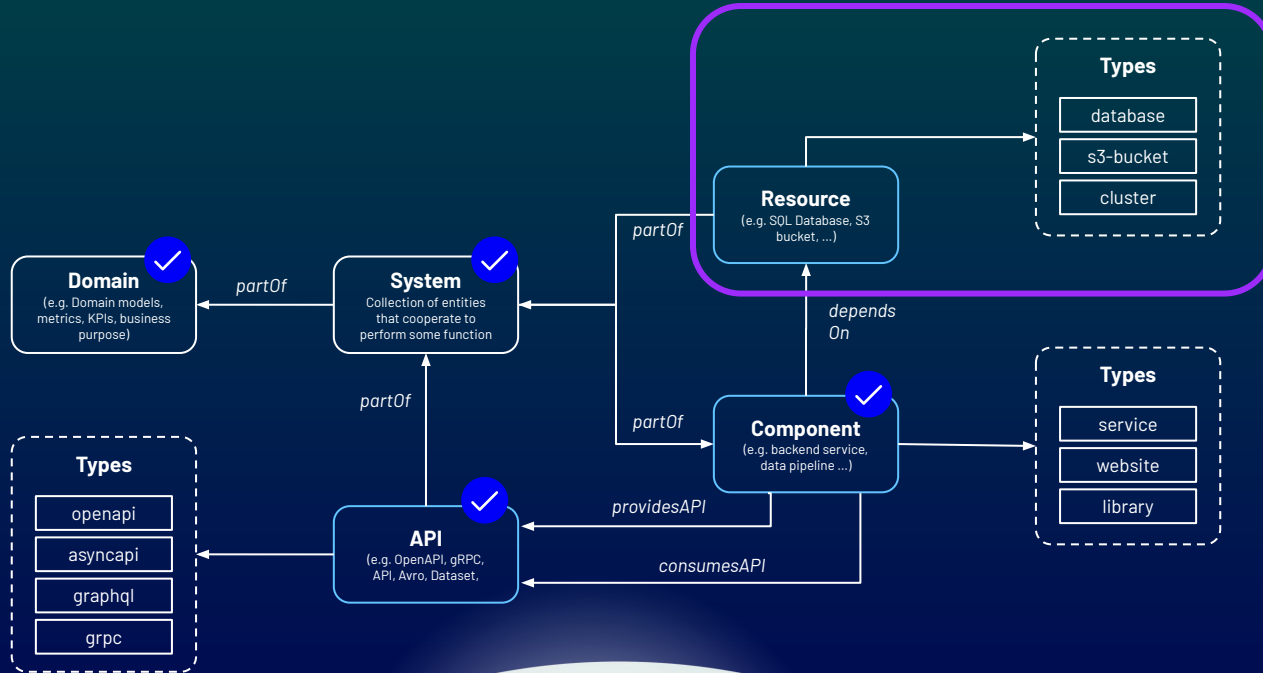


```
apiVersion: backstage.io/v1alpha1
kind: API
metadata:
  name: service
  description: ...
relations:
  - type: apiProvidedBy
    targetRef: component:default/service
    target:
      kind: component
      name: service
spec:
  type: asyncapi
  owner: squad-maven
  definition: |
    {
      "type": "record",
      "namespace":
        "integrationevents.onboarding.user",
      "name": "userCreated",
      "fields": [
        { "name": "Name", "type": "string" },
        { "name": "Street", "type": "string" },
      ]
    }
  }
```


Data Resources and PII Data



Data Resources and PII Data



Key takeaways

- Business value perspective
 - T2M - No friction
 - Engineers can focus on creating customer value
 - Compliance through automation
- Tech perspective
 - Reducing cognitive load results in happier developers
 - Paved paths and sane defaults, ensure developers can focus on creating customer value
 - Backstage for everyone






THANK YOU



Brian Nielsen

 @briannielsen76

Kasper Nissen

 @phenex

LUNAR[®]