

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



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



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®?



LUNAR TECHNOLOGY

100+

Daily deploys

400+

Microservices

Founded in
2015

Talents in Tech
113
(563 overall)

21
Squads

+575K
Users
123K new in 2022

3
Hubs
CPH+AAR+STO

Our IT strategy is designed to fuel business growth

Technology should accelerate our ability to scale business opportunities

1

Domain driven design

2

Event driven design

3

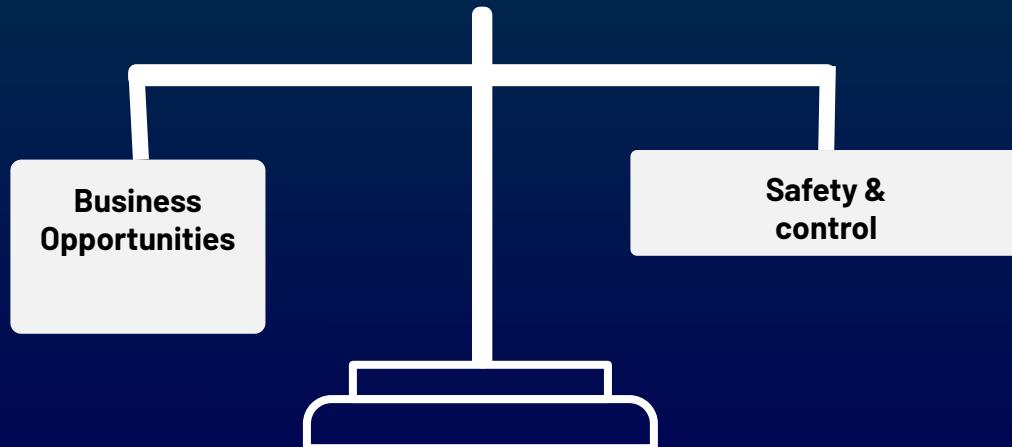
Outsource based on domain distillation

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

GÆLDENDE

BEK nr 1103 af 30/06/2022

Erfvervsministeriet

Yderligere oplysninger >

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

I medier af § 65, stk. 2, § 70, stk. 6, § 71, stk. 2, § 152, stk. 2, og § 373, stk. 4, i lov om finansiell virksomhed, jf. lovbekendtgørelse nr. 406 af 29. marts 2022, § 67, stk. 5, § 188, stk. 2, § 94, stk. 2, og § 270, stk. 1, i lov nr. 1125 af 8. juni 2021 om fondsmæglerselskaber og investeringservice og -aktiviteter, § 21, stk. 5, og § 39, stk. 3, i lov om realkreditdelen og realkreditobligationer m.v., jf. lovbekendtgørelse nr. 315 af 11. marts 2022, § 18c g. stk. 3, og § 255 i lov om kapitalmarkeder, jf. lovbekendtgørelse 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

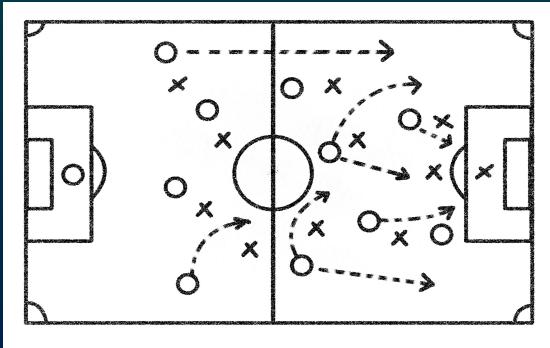
DFSA : "We are working for financial stability and confidence in financial undertakings and markets"



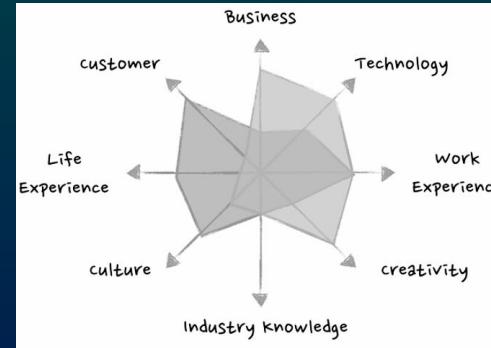
WAYS OF WORKING



Building the best product is a team sport



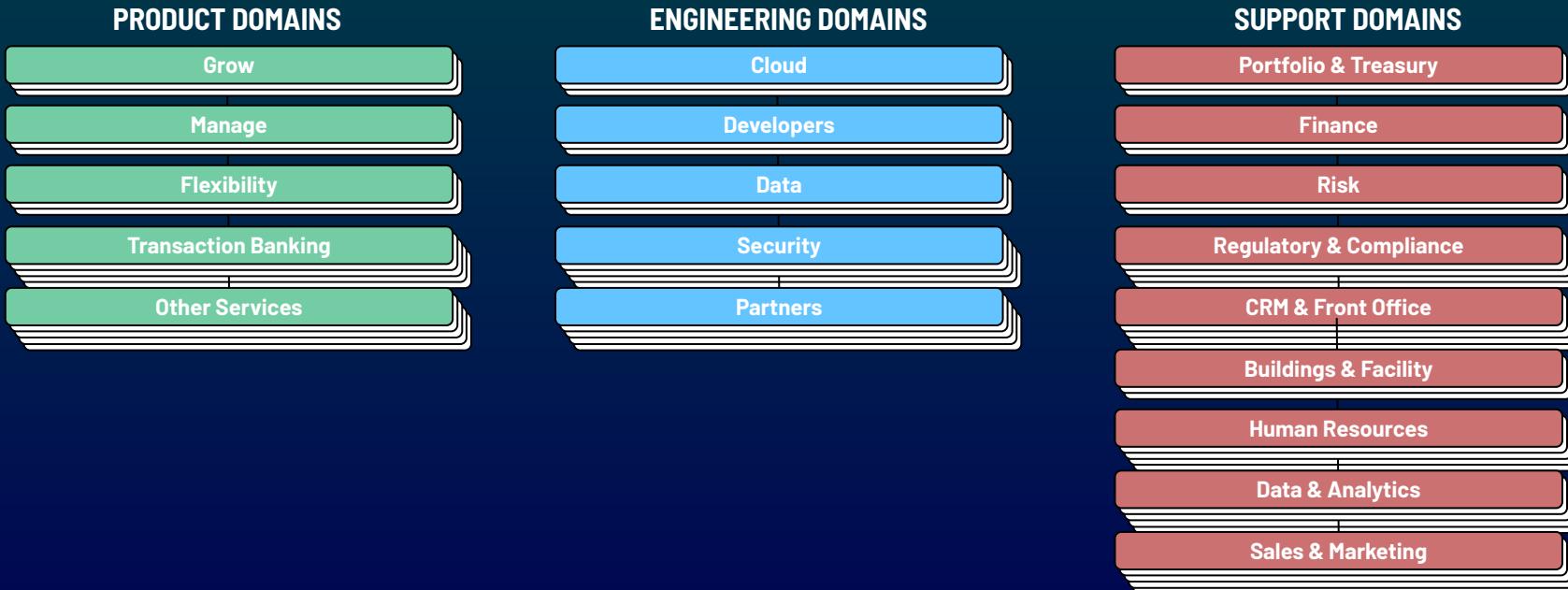
We believe in shared success and a 360 ownership across the business. Building the best product is a team sport, where you must secure all specialised competencies and skills to win.



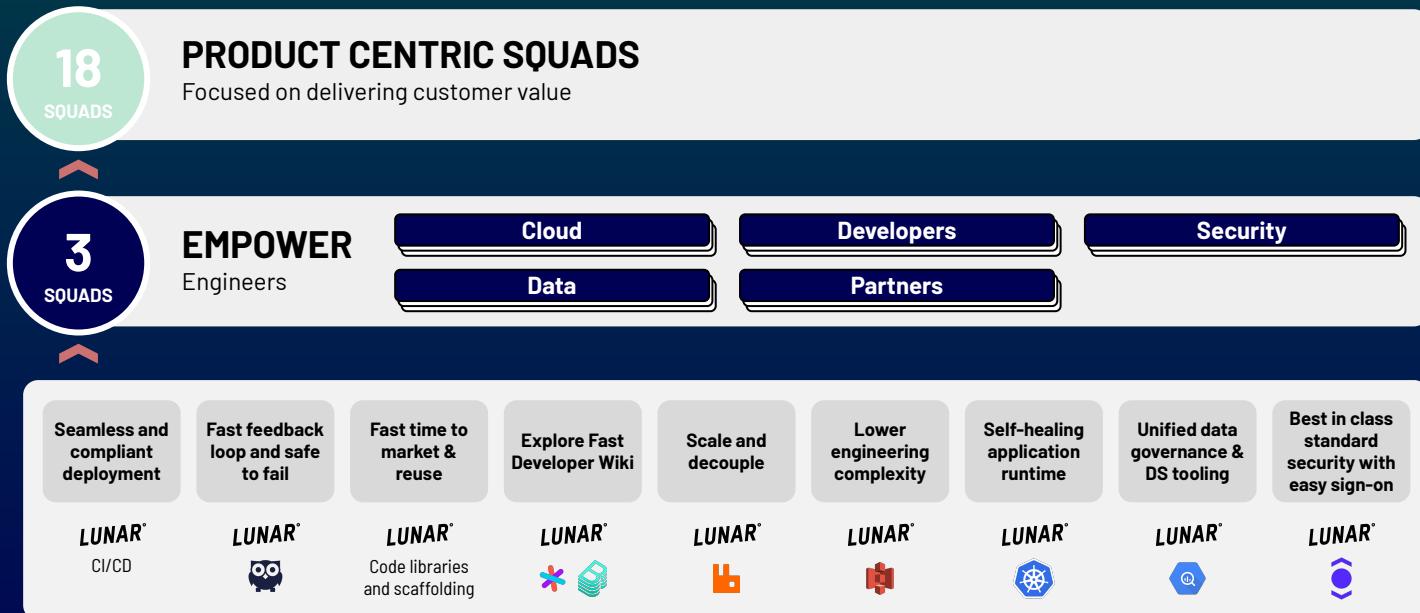
We believe cross-functional teams on a shared mission is the way to create high engagement and performance, and to beat competition.

Lunar's application and cloud architecture

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



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



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

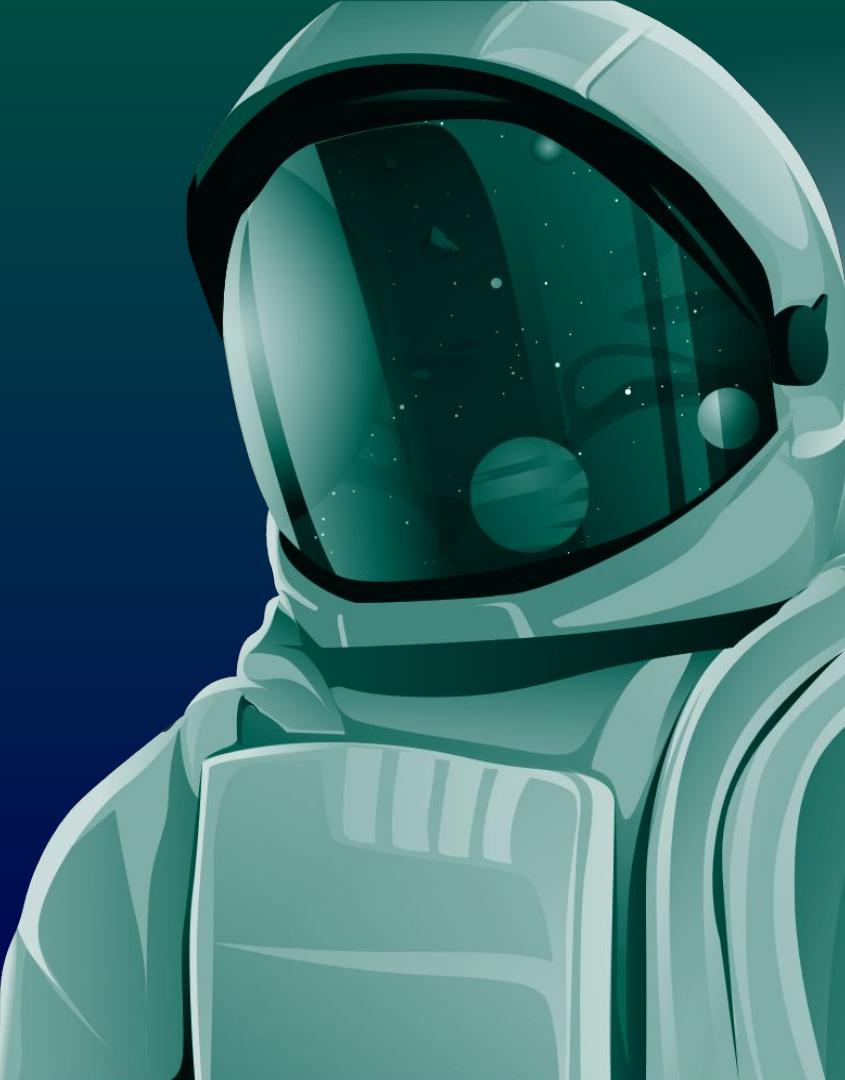
- Suite of development libraries
- Automatic dependency updates

BACKSTAGE AT LUNAR, WHY AND HOW?



MEET SPACY

Developer at Lunar





Awesome!
I'm ready!





CI/CD - check!



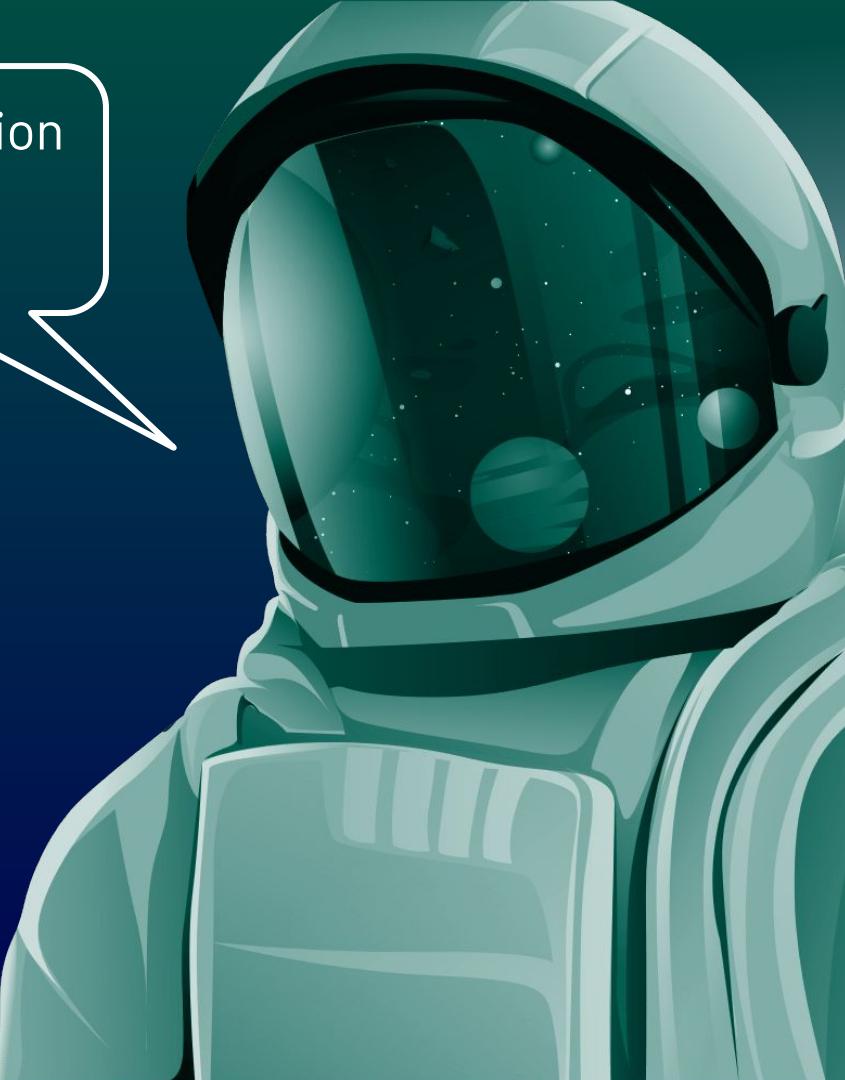


RabbitMQ

gRPC

GraphQL

Communication
protocols..
check!



GitHub

GO



RabbitMQ

gRPC

GraphQL



Uhh! I guess
that's required
knowledge!



GitHub

GO



RabbitMQ

gRPC

GraphQL

aws
A



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
```



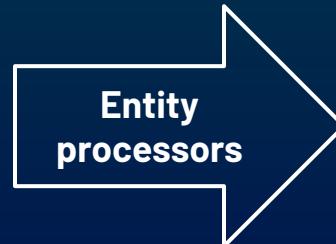
`shuttle`

```
$ 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
```



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

LUNAR®

account-block | Overview | LUNAR

/catalog/default/component/account-block

COMPONENT — SERVICE

account-block

Owner: squad-maven Lifecycle: unknown

OVERVIEW SECURITY CI/CD PULL REQUESTS TODOS RELEASES DEAD LETTER

Your Squads Catalog Docs APIs On Call Dead Letter Reconstitution Tech Insights Create...

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

Feedback Settings

About

VIEW SOURCE VIEW TECHDOCS

DESCRIPTION Responsible for handling account block status

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

LIFECYCLE: unknown TAGS:

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.



Create a New Component | Test

/create?filters%5Bkind%5D=template&filters%5Buser%5D=all

LUNAR®

Search

Your Squads

Catalog

Docs

APIs

On Call

Dead Letter

Reconstitution

Tech Insights

Create...

Feedback

Settings

Create a New Component

Create new software components using standard templates

Available Templates

Search

Templates

PERSONAL

Starred 0

LUNAR

All 13

CATEGORIES

documentation Docs Repository

Creates a docs repository which is integrated into backstage.

OWNER squad-aura

TAGS

CHOOSE

service Empty Repository

Creates a near empty repository with default Lunar files

OWNER squad-aura

TAGS

CHOOSE

service Empty RPA Library Repository

Creates an near empty RPA library repository with default Lunar files

OWNER squad-pioneer

TAGS

CHOOSE

service Empty RPA Process Repository

Creates an near empty RPA process repository with default Lunar files

OWNER

TAGS

CHOOSE

service Empty RPA REFramework Process Repository

Creates an near empty RPA REFramework process repository with default Lunar files

OWNER

TAGS

CHOOSE

cli Go CLI

Create a new Go cli

OWNER squad-aura

TAGS

CHOOSE

SUPPORT

This screenshot shows the LUNAR component creation interface. The left sidebar contains navigation links for Your Squads, Catalog, Docs, APIs, On Call, Dead Letter, Reconstitution, Tech Insights, Create..., Feedback, and Settings. The main area is titled 'Create a New Component' and 'Available Templates'. It displays six template cards in a grid:

- Docs Repository**: A documentation template that creates a repository integrated into Backstage. Owner: squad-aura.
- Empty Repository**: A service template that creates a near-empty repository with default Lunar files. Owner: squad-aura.
- Empty RPA Library Repository**: A service template that creates a near-empty RPA library repository with default Lunar files. Owner: squad-pioneer.
- Empty RPA Process Repository**: A service template that creates a near-empty RPA process repository with default Lunar files. Owner: squad-aura.
- Empty RPA REFramework Process Repository**: A service template that creates a near-empty RPA REFramework process repository with default Lunar files. Owner: squad-aura.
- Go CLI**: A command-line interface (cli) template that creates a new Go CLI. Owner: squad-aura.

Service generation using Backstage scaffolder

Create a New Component | LUNAR

/create/templates/default/go-service-vostok

LUNAR®

Search

Your Squads

Catalog

Docs

APIs

On Call

Dead Letter

Reconstitution

Tech Insights

+ Create...

Feedback

Settings

Go Service with vostok

1 Fill in the needed information to create the service

Name *

Unique name of the service.

Description *

What is the responsibility of the service?

Owner *

The squad that will own the service.

Domain *

The business domain the service belongs to, eg. 'card-payments'. If your domain is not in the dropdown reach out to your friendly neighbourhood architect.

Kubernetes namespace

The kubernetes namespace, eg. 'bank'. Leave empty to default to workload namespaces, ie. 'dev' and 'prod'.

Setup auto release policy for

dev

prod

platform

azure-uat

azure-prod

Go service with vostok



That was
almost too easy!





Enable DIY

Showcase how developers can
create their own plugins.

LUNAR®

TOOL

Reconstitution

Republish Integration Events to services

Owner
squad-skylab

Search

Your Squads Env dev

Catalog

Docs

APIs

On Call

Dead Letter

Reconstitution

Tech Insights

Create...

Feedback

Settings

Add Job

Receiver * Service to receive events

Producer * Domain and entity type producing events

From To Entity IDs to publish events for

Event Names Event names to publish events for

ADD +

Jobs

Filter

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

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

```
.  
├── 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

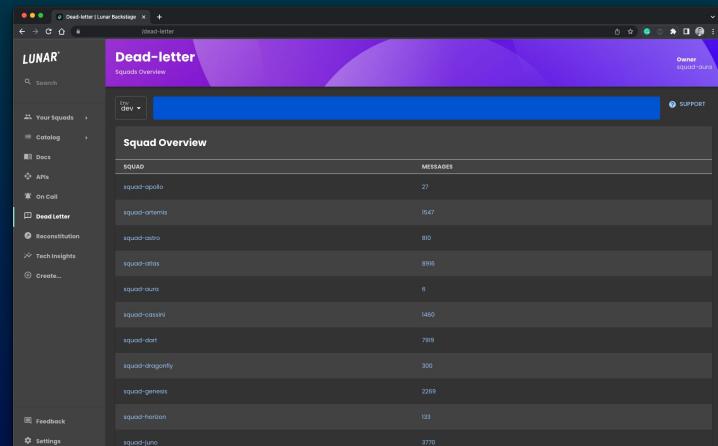
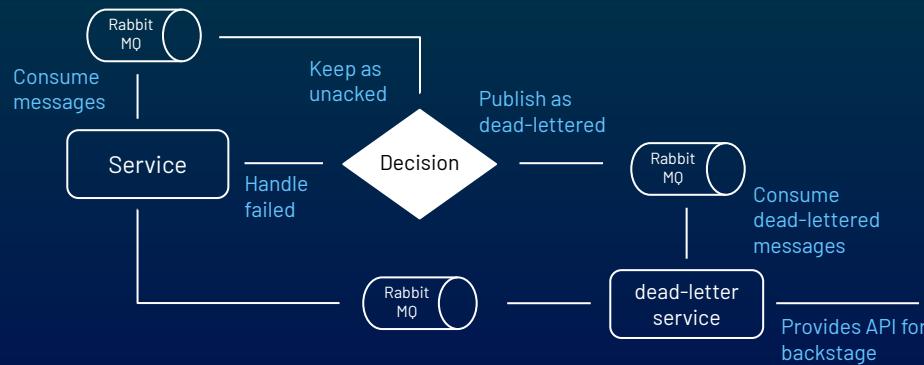
Automatic updates of dependencies

Initial go-service configuration
Use shuttle to generate code

Configuration of external dependencies taken care of.

Service ownership, default runtime configuration for the environments

Critical systems and paths



squad-aura | Overview | Lunar

/catalog/default/group/squad-aura?filters%5Bkind%5D=component

LUNAR®

GROUP — TEAM

squad-aura ☆

Search

OVERVIEW DEAD LETTER DOCS TECH INSIGHTS DETAILS ABOUT

Your Squads Catalog Docs APIs On Call Dead Letter Reconstitution Tech Insights Create...

Dead lettered messages

dev

18

Handle now →

Open pull requests C

REVIEW REQUIRED

lunar-backstage kaspernissen Hide on-call in sidebar and router

REVIEW IN PROGRESS

go-events igpemar add: add FXRateCurrencyDkk and FXRateEurDkk fields to

APPROVED

lunar-backstage mahlunar Patch/1.11.1

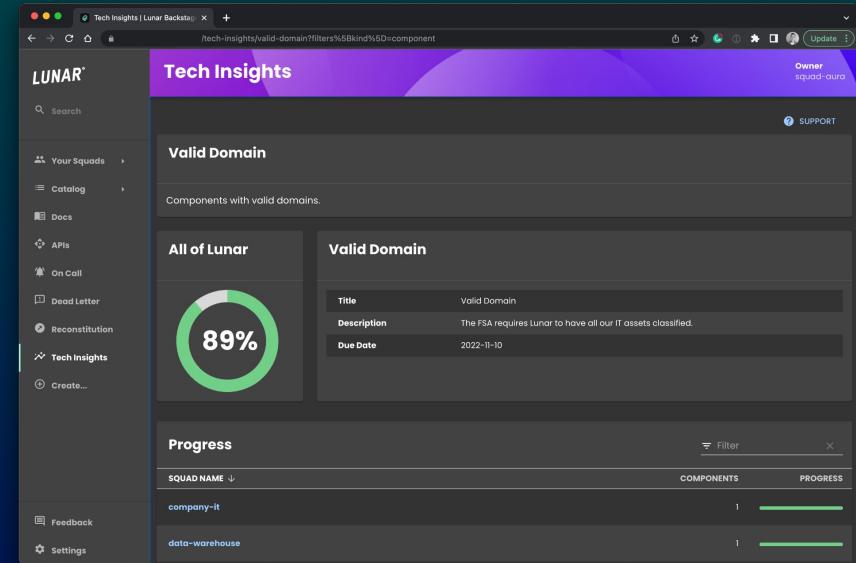
Created at: 21 days ago Last update: 21 days ago

<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...

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

crosskey-files-gcl

Providing squad-level action items and progress

Driving adoption...

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

USE-CASE: ASSET MANAGEMENT & MORE



Why asset management?



Increase
performance



Mitigating
risk



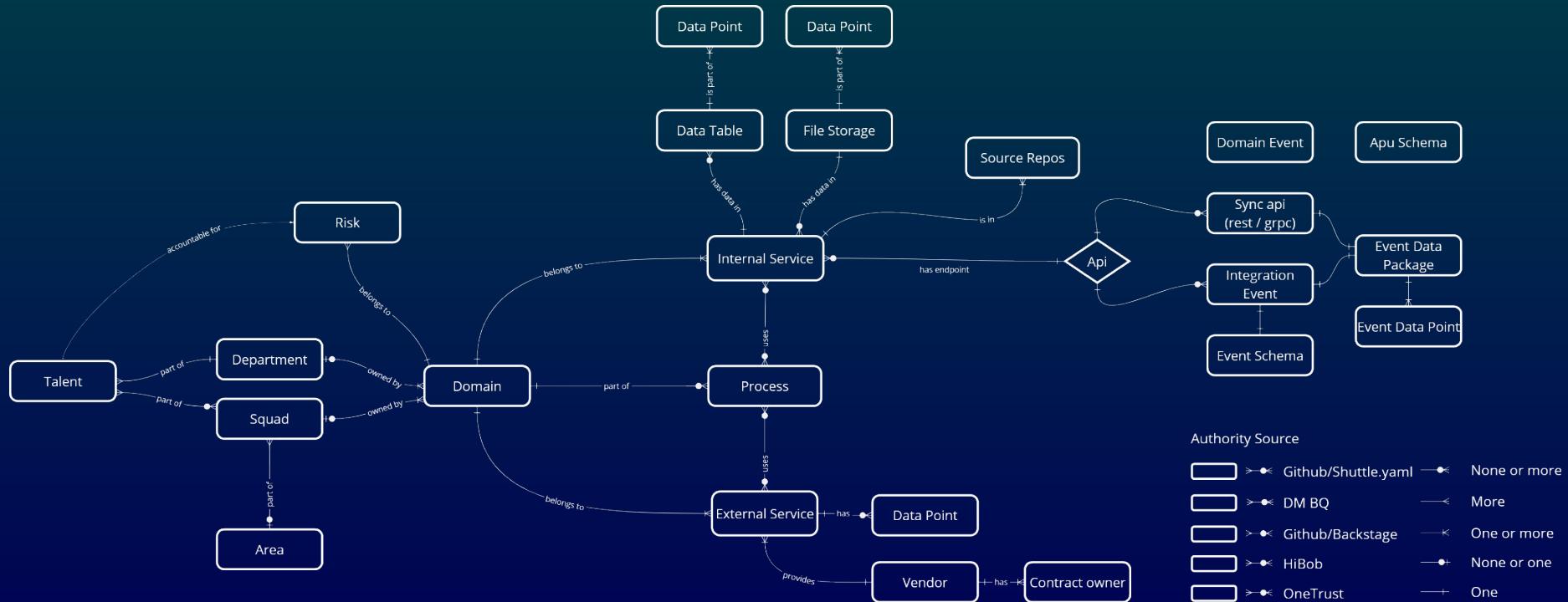
Regulator
requirements
according to
DFSA



Building
customer
trust and
satisfaction.

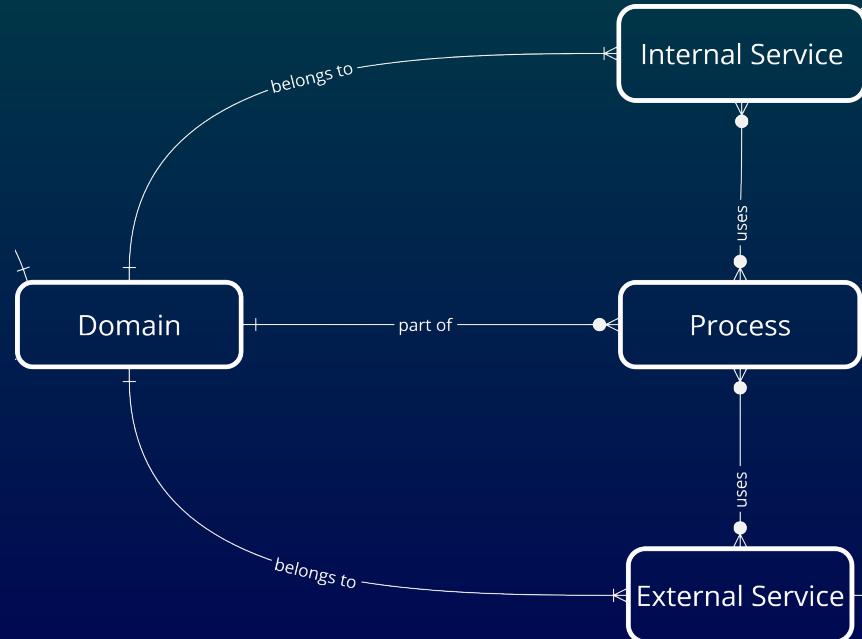
Asset modelling overview

We are in Lunar documenting assets on many levels



Asset modelling overview

We are in Lunar documenting assets on many levels



The screenshot shows the **Lunar Catalog** interface with the following details:

Domains -

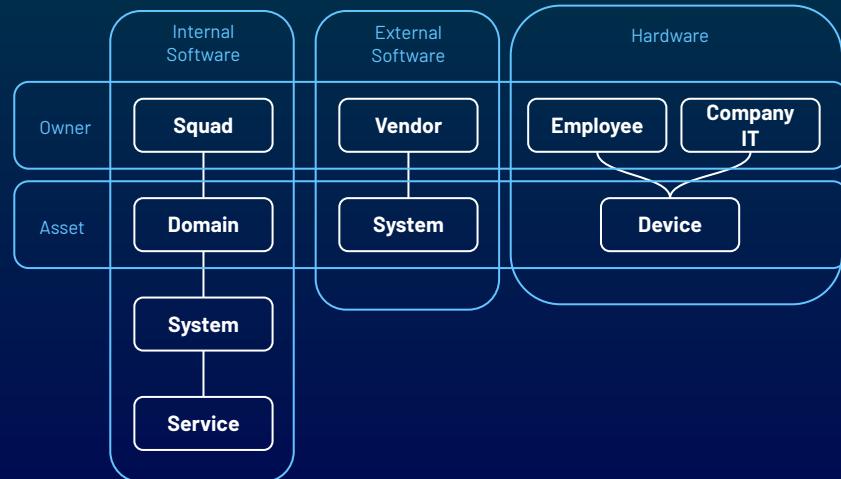
NAME	TIER	AREA	COLONY	OWNER	ACTIONS
Account Management	Product Portfolio	Financial Management	squad-general	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Account Settlement	Banking Services	Transaction Banking	squad-onion	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Account Statement Export	Banking Services	Unknown	squad-junior	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Agreements / Subsidiaries / Teams	Product Portfolio	Unknown	squad-conveyor	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
AML Reporting to Financial Intelligence Unit	Banking Services	Unknown	squad-onion	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Async Messaging	Empower	Empower	squad-onion	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Blockchain API	Empower	Empower	squad-round	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Banking Central Integration	Banking Services	Transaction Banking	squad-onion	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Benefits	Product Portfolio	Financial Management	squad-onion	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

All (97)

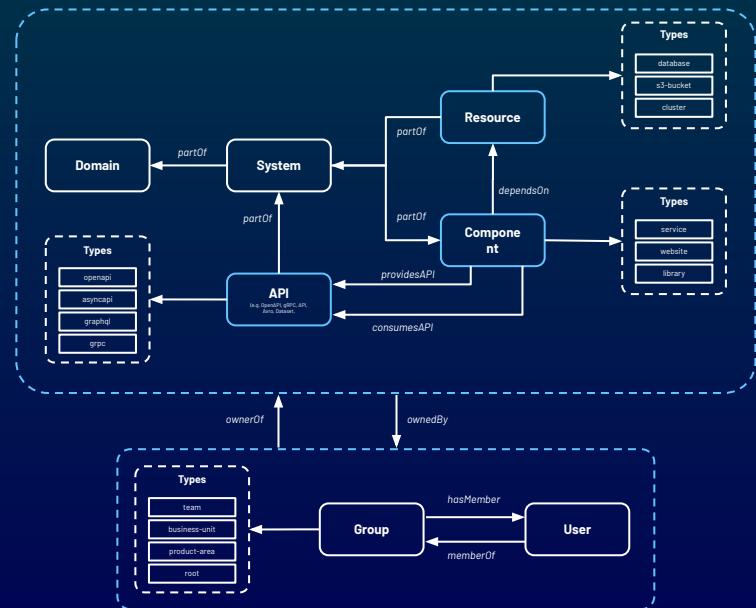
Domain as Assets

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



Lunar Catalog | Lunar Backstage

/catalog?filters%5Bkind%5D=domain&filters%5Buser%5D=all&filters%5Bowners%5D=squad-skylab...

LUNAR®

Search

Your Squads

Catalog

Docs

APIs

On Call

Dead Letter

Reconstitution

Tech Insights

Create...

Feedback

Settings

Lunar Catalog

Domains

CREATE COMPONENT ? SUPPORT

All (2)

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	

PERSONAL

Owned 0

Starred 0

LUNAR

All 2

OWNER

SQUAD...

TIER

1

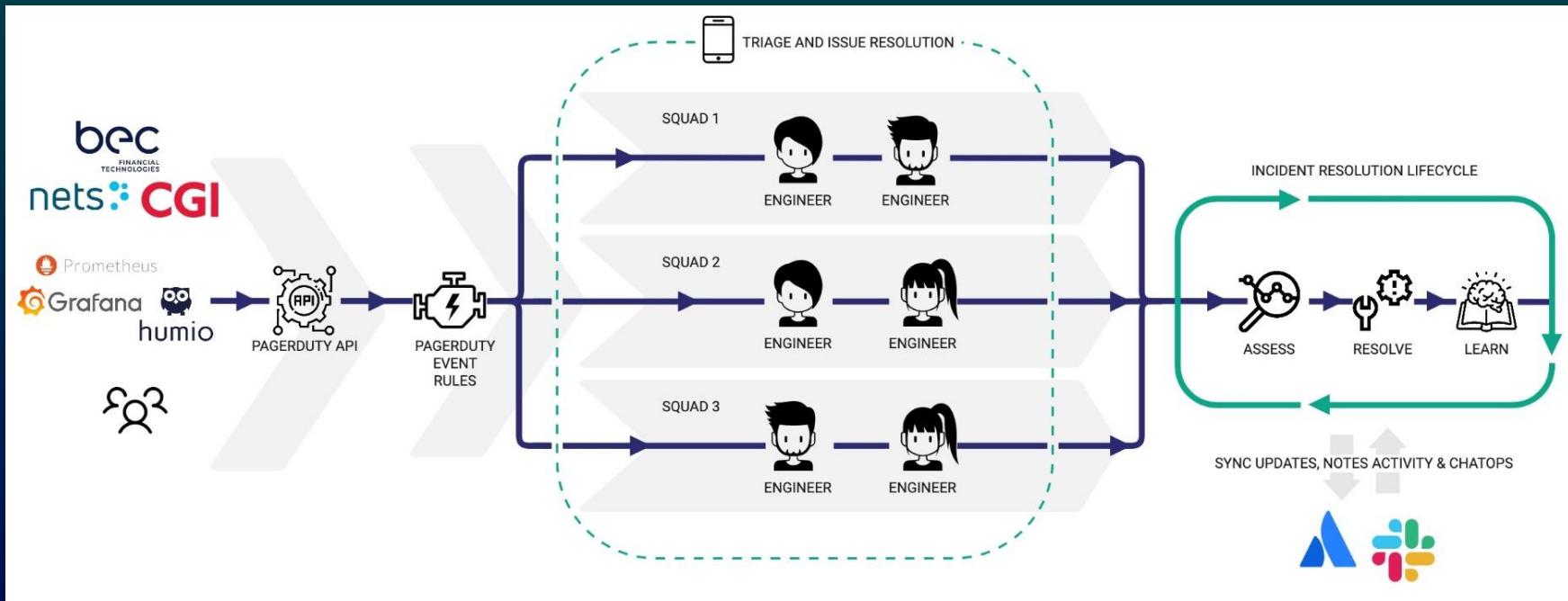
AREA

COLONY

Filter

CREATE COMPONENT ? SUPPORT

Incident response



Automating controls to ensure continuous compliance

AWS config change

rds-storage-encrypted

Rule details

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

All	ID	Type	Status	Annotation	Compliance
1	production-rds	RDS DBInstance	-	-	Compliant
2	crypto-rds	RDS DBInstance	-	-	Compliant
3	lunar-openbanking-back...	RDS DBInstance	-	-	Compliant
4	dead-letter	RDS DBInstance	-	-	Compliant
5	auth	RDS DBInstance	-	-	Compliant

Humio & snyk alerts

Humio APP 08:05
Humio Alert
Developer 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 17:19
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 17:19

TwilightMoonBeam APP 12:10
Humio 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
2022-11-14T11:10:52.08Z Action created Repository
lunar-feature-toggles-framework-ios User
MadBogoskov Nov 14th

snyk-bot APP 11:04
Improper Input Validation
New vulnerability in package golang.org/x/text/language at the Squad Artemis organization. Severity
Medium 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

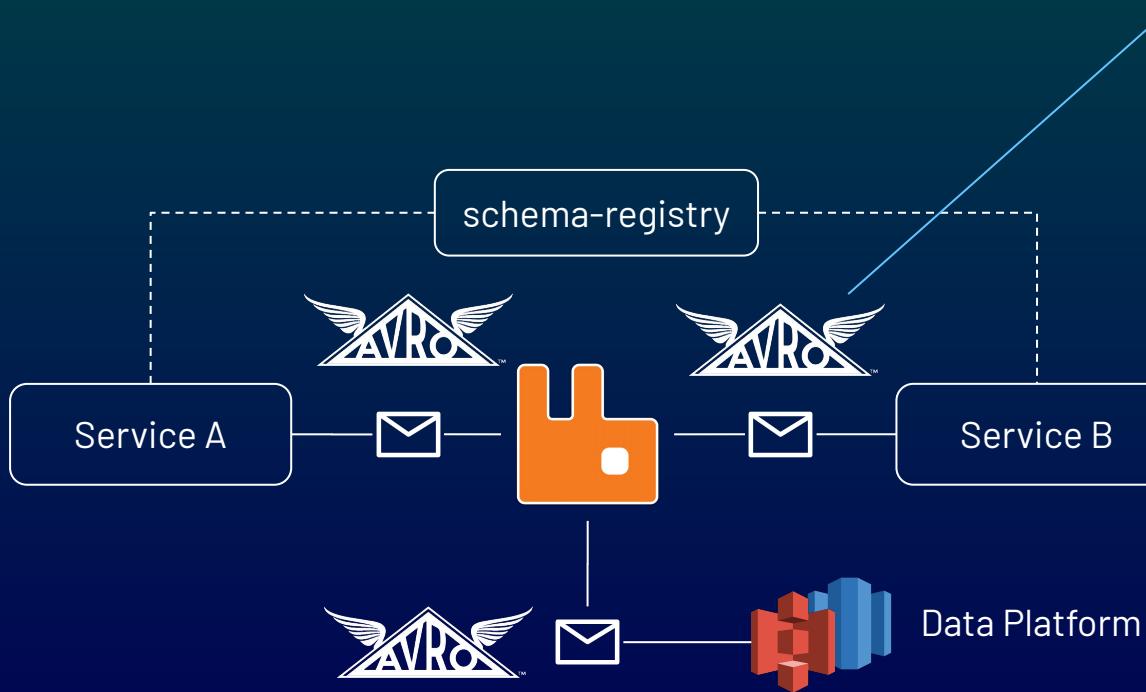
Pagerduty: trigger on-call schedules

Reconstitution: resend events

Dead Letter: handle events that failed

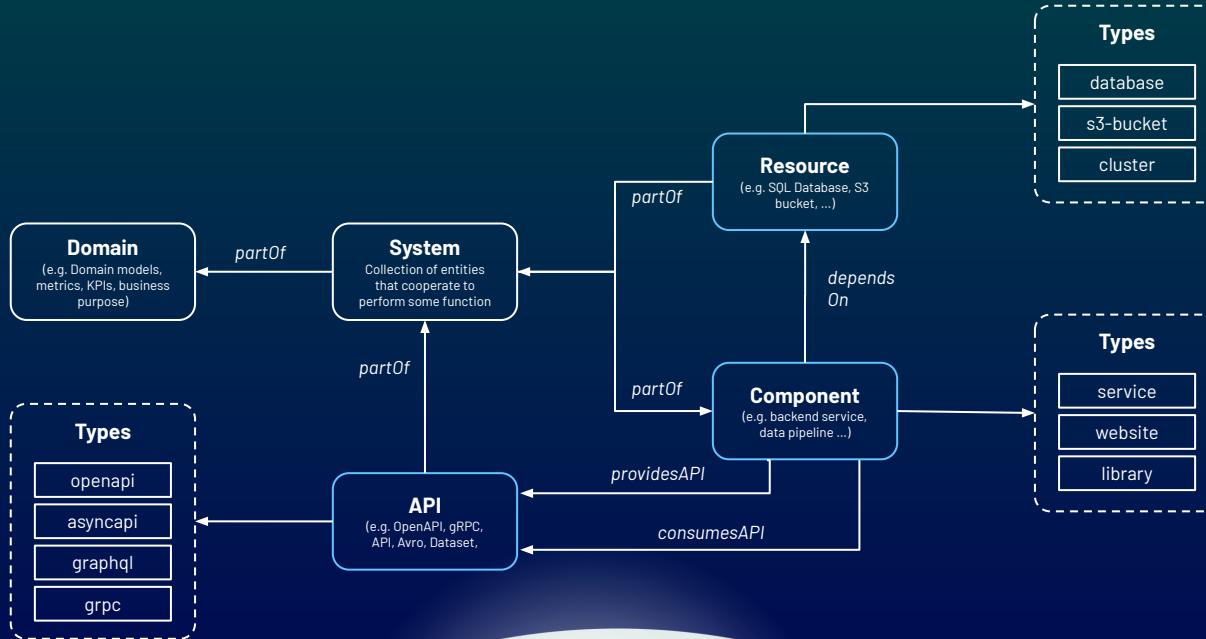
Tech-insights: provide progress on squad and company level

Event schemas and PII Data

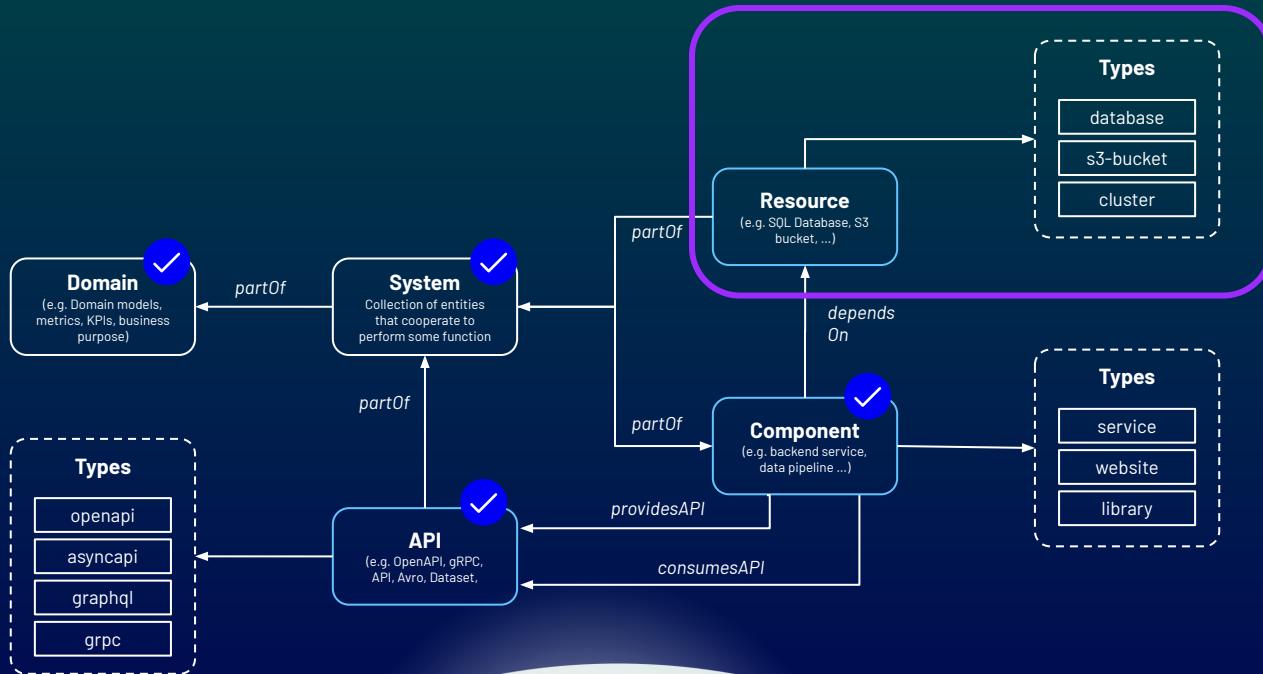


```
apiVersion: backstage.io/v1alpha1
kind: API
metadata:
  name: service
  description: ...
  relations:
    - type: apiProvidedBy
      targetRef: component:default/service
      target:
        kind: component
        name: service
spec:
  type: asyncapi
  owner: squad-maven
  definition: |
    {
      "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
Twitter: @briannielsen76

Kasper Nissen
Twitter: @phennex

LUNAR[®]