NOSAD & SBOM

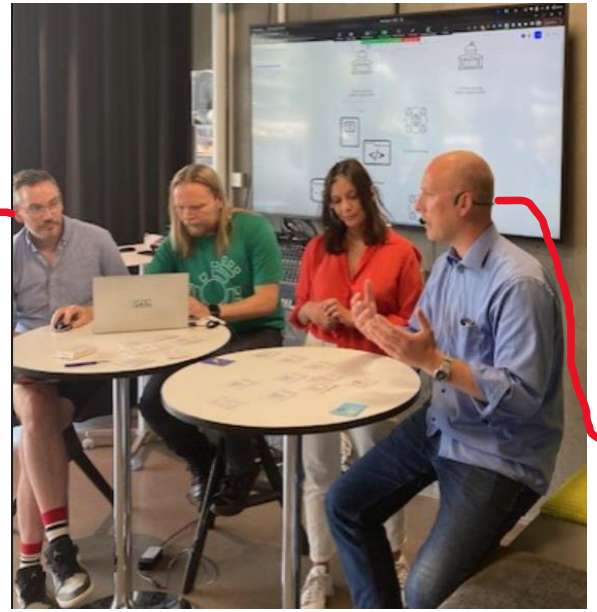
Network Open Source and Data

- About CMS
  - Cybernode & Wordpress
  - Nosad
  - Bomresolver + Nosad + Kubernetes (CDN)
- Demo
  - Generate content
  - Create static content container
  - Deploy static container with Kubernetes

Hans Thorsen Lamm (hans@lammda.se)

NOSAD Meetup 2023-06-08

Johan Linåker RISE



Follow up 2023-06-12
Hans Lamm
Jonas Södergren
Håkan Persson

https://nosad.se/
https://codeberg.org/
https://designsystem.arbetsformedlingen.se/
https://designsystem.skolverket.se/

Förvaltningsmodeller för öppen källkod | Goto 10

Hans Thorsen Lamm (hans@lammda.se)

https://whatcms.org

✔ Success JSON

cybernode.se uses

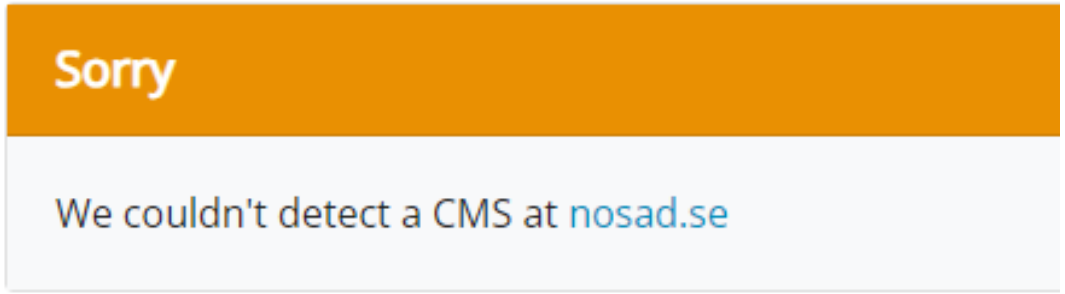
Category	Software	Version
Blog, CMS	WordPress	6.1.1
Programming Language	PHP	7.4.33
Database	MySQL	
Web Server	LiteSpeed	

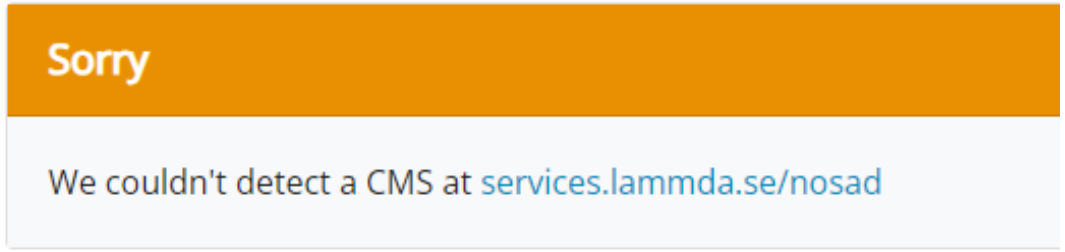
Social Media

Network	Profile	Url
LinkedIn	cybernode-se	https://www.linkedin.com/company/cybernode-se/

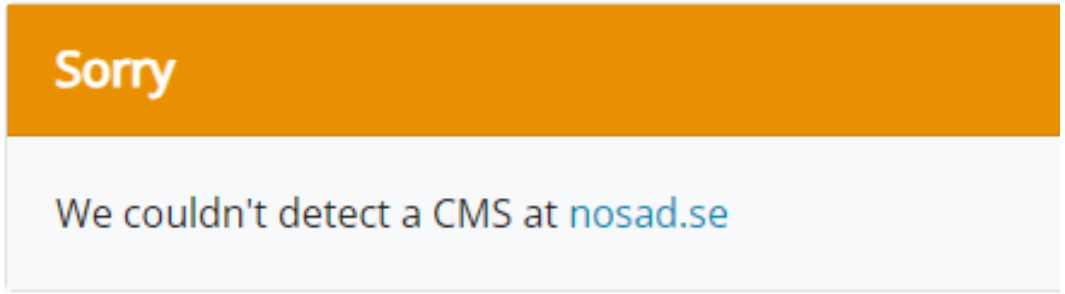
Help us improve these results

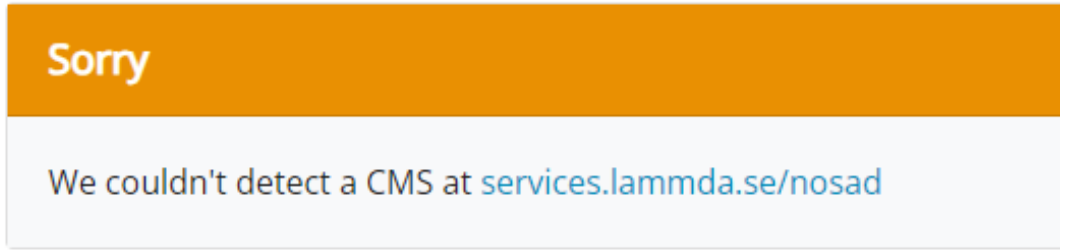
https://whatcms.org



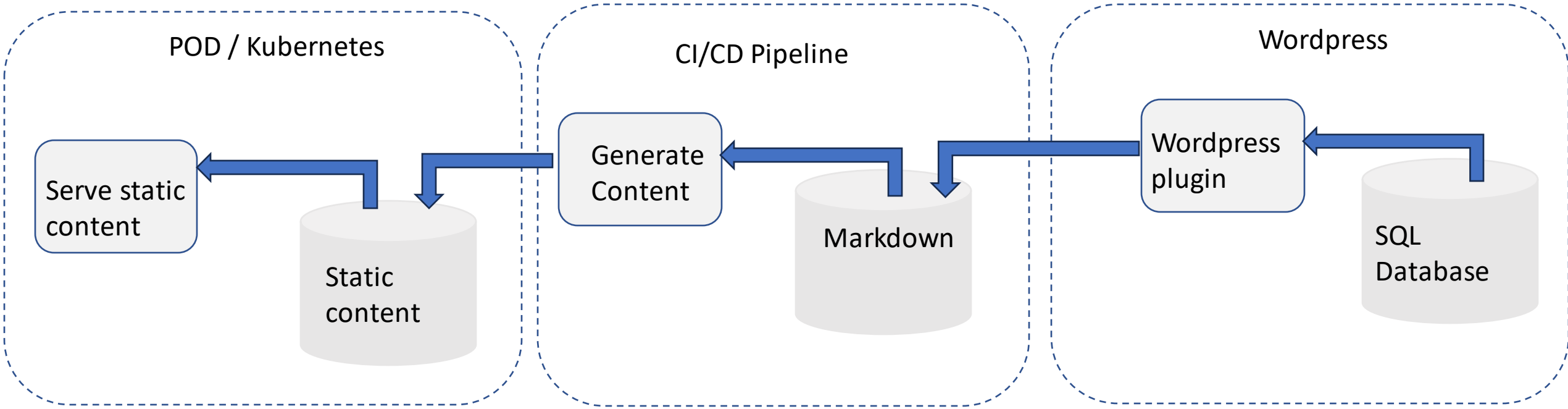


https://whatcms.org





Proposal from presentation 2023-05-12



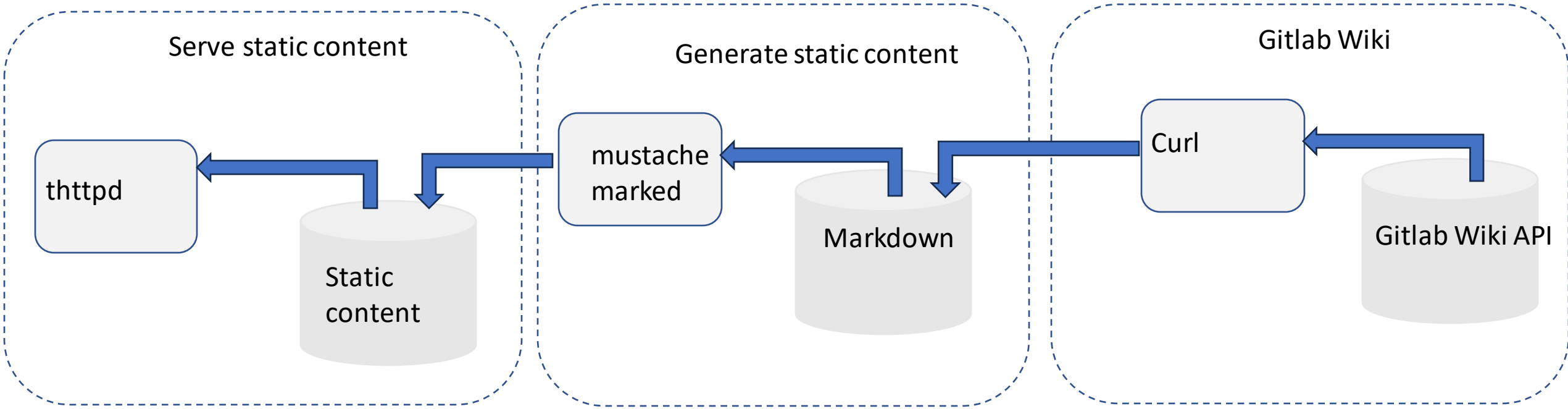
[The world's fastest framework for building websites | Hugo (gohugo.io)]

[Wordpress-to-hugo-exporter]

A few years ago, dynamic content was the way to go: everything could be easily changed and updated, allowing for an entire website redesign within seconds.

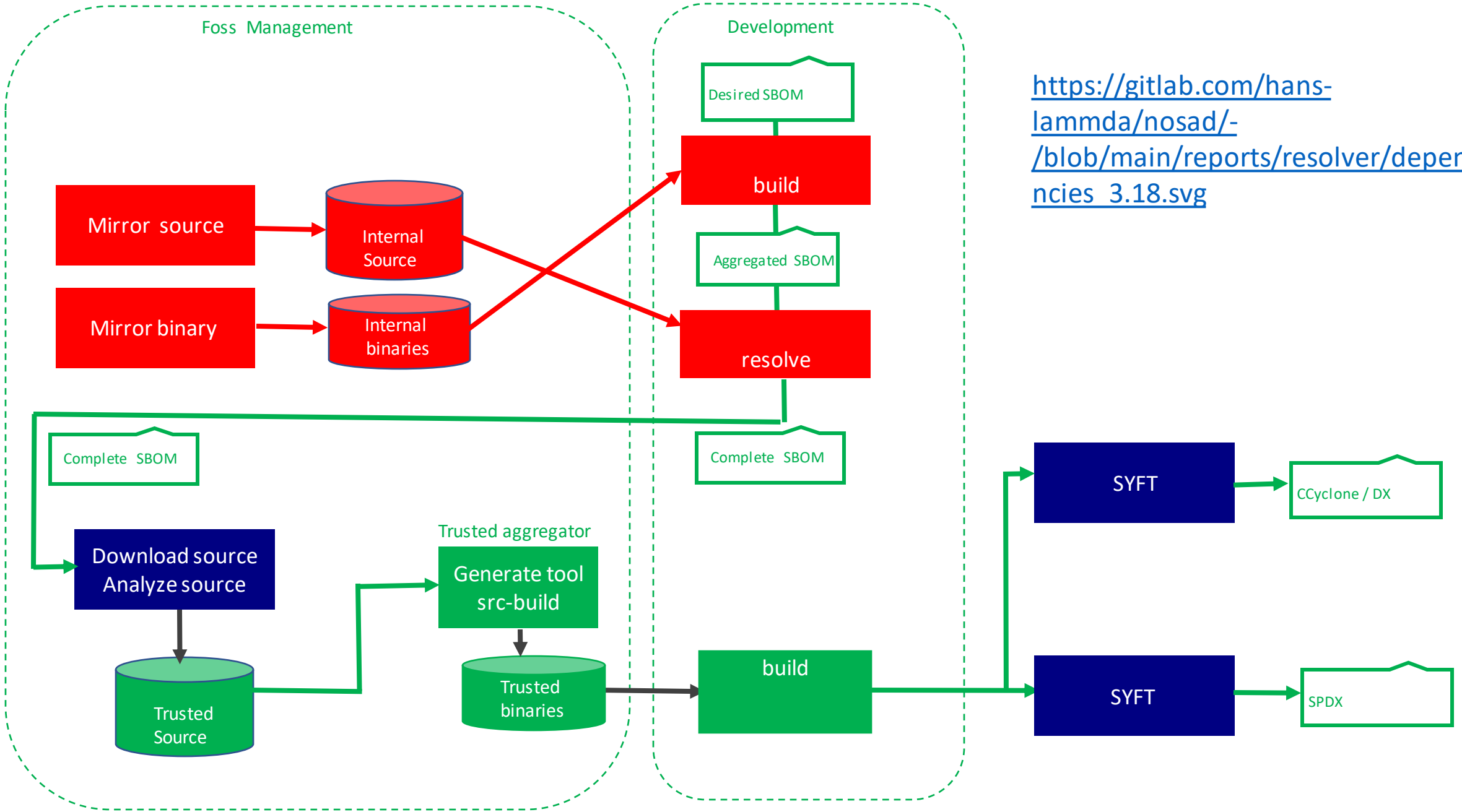
But then, speed became the top priority, and static content suddenly became cool again

NOSAD



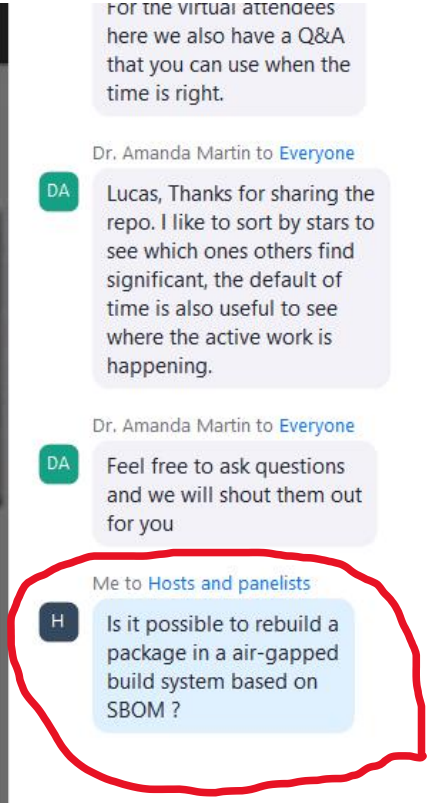
https://gitlab.com/open-data-knowledge-sharing/open-data-knowledge-sharing.gitlab.io/-/blob/master/Dockerfile

Rebuild in Isolation



https://gitlab.com/hans-lammda/nosad/-/blob/main/reports/resolver/dependencies_3.18.svg

OPENSSF & SBOM



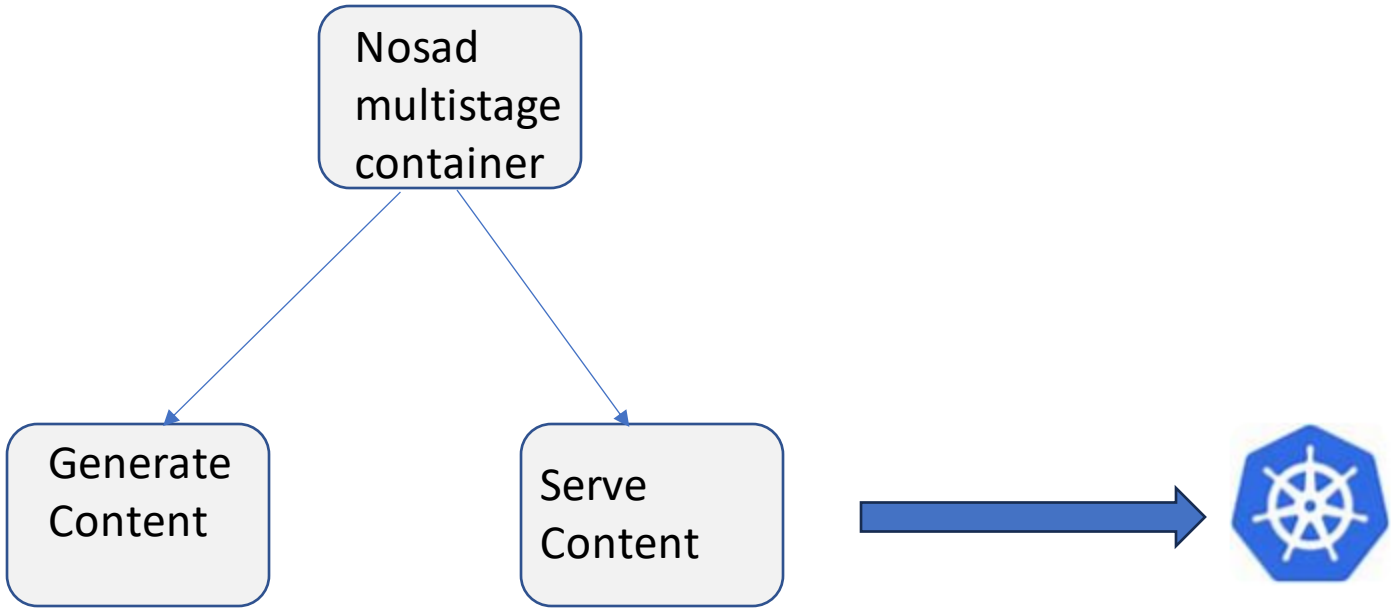
[Reproduce in Isolation question from Hans (11 minutes from start)]

Adapt Nosad to Bom Resolver

Analyze existing code from Gitlab
Replace thttpd with lighttpd
Divide one container into two
Generate SBOMS:
(Cyclone/DX , SPDX and BomResolver)

Deploy on Kubernetes

https://gitlab.com/hans-lammda/nosad



3 Layer container
Service (build.sh)
Middleware (npm)
Base (Alpine)

2 Layer container
Service (lighttpd.conf)
Base (Alpine)

DEMO / GENERATE

```
rm -rf static
mkdir -p static
podman run   -v "/home/hans/development/git-
clones/nosad/content/service/static:/static"   content_builder:1.0.1
generate
Processing build/staging/Anmälan-till-Meetup
Processing build/staging/Benchmarking-2019
Processing build/staging/Brno
```

DEMO / SERV

```
kubectl get pods -n   nosad
NAME                      READY   STATUS    RESTARTS   AGE
nosad-6c4f776cb5-rz4qp    1/1     Running   0          5d1h
```

```
kubectl get pods -n   nosad
NAME                      READY   STATUS    RESTARTS   AGE
nosad-6c4f776cb5-h92hc    1/1     Running   0          4s
nosad-6c4f776cb5-kbjtf    1/1     Running   0          4s
nosad-6c4f776cb5-nckw2    1/1     Running   0          4s
nosad-6c4f776cb5-npswk    1/1     Running   0          4s
nosad-6c4f776cb5-rz4qp    1/1     Running   0          5d1h
```

DEMO / SCALE

```
kubectl get pods -n  nosad
NAME                READY   STATUS    RESTARTS   AGE
nosad-6c4f776cb5-rz4qp   1/1     Running   0        5d1h
```

```
kubectl get pods -n  nosad
NAME                READY   STATUS    RESTARTS   AGE
nosad-6c4f776cb5-h92hc   1/1     Running   0        4s
nosad-6c4f776cb5-kbjtf   1/1     Running   0        4s
nosad-6c4f776cb5-nckw2   1/1     Running   0        4s
nosad-6c4f776cb5-npswk   1/1     Running   0        4s
nosad-6c4f776cb5-rz4qp   1/1     Running   0        5d1h
```

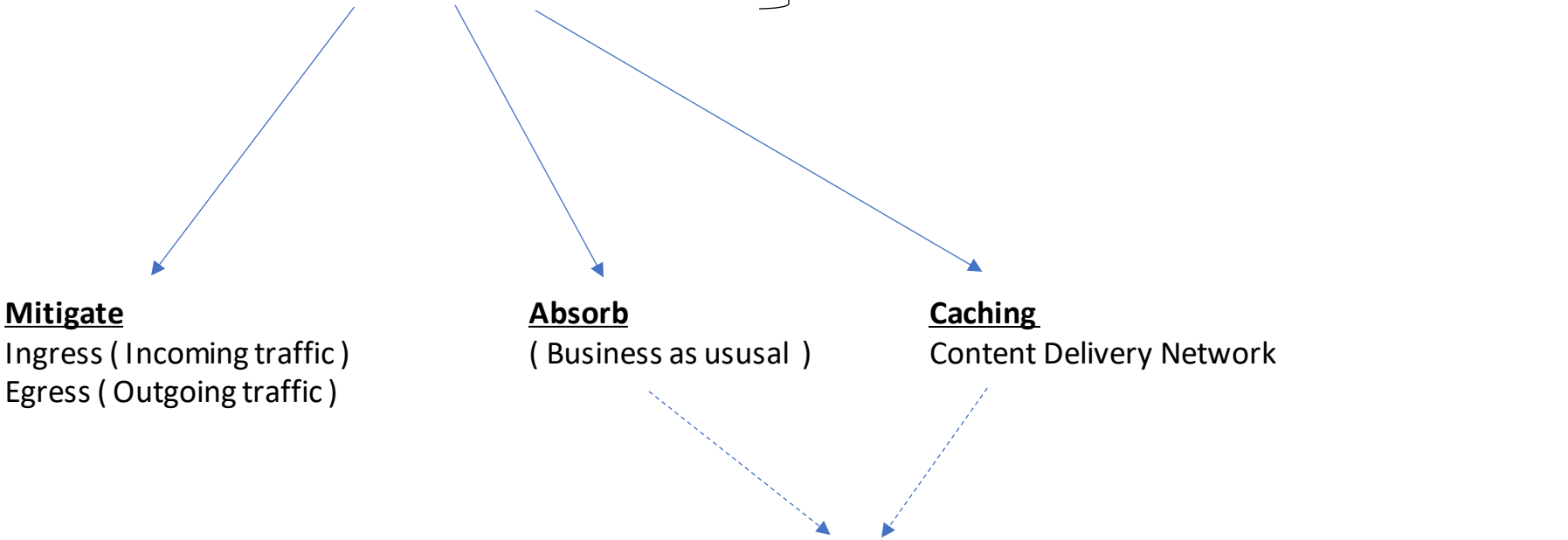
Next Step

Bom Resolver use Nosad Wiki
Nosad wiki migrated to Kubernetes

C.I.A

- Confidentiality
- Integrity
- **Availability**

Cornerstone in many security standards / frameworks



Record breaking DDOS attack !!!

Cloudflare mitigates record-breaking 71 million request-per-second DDoS attack

This was a weekend of record-breaking DDoS attacks. Over the weekend, Cloudflare detected and mitigated dozens of *hyper-volumetric* DDoS attacks. The majority of attacks peaked in the ballpark of 50-70 million requests per second (rps) with the largest exceeding **71 million rps.** This is the largest reported **HTTP DDoS** attack on record, more than 54% higher than the previous reported record of 46M rps in June 2022.
The attacks were HTTP/2-based and targeted websites **protected by Cloudflare**. They originated from over **30,000** IP addresses. Some of the attacked websites included a popular gaming provider, cryptocurrency companies, hosting providers, and cloud computing platforms. The attacks originated from numerous cloud providers, and we have been working with them to crack down on the botnet

Rate: 71 000 000 Request per second
Protocol: HTTP
Source: 30.000 individual IP addresses
Destination: Let´s assume one target for the attack

Migration of BomResolver to RISE Datacenter
https://www.ri.se/sv/ice-datacenter

recordedfuture.com. 7099 IN NS leah.ns.cloudflare.com.
services.lammda.se digital ocean

Is it possible to absorb DDOS attack ?

Considerations for large clusters | Kubernetes

A cluster is a set of nodes (physical or virtual machines) running Kubernetes agents, managed by the control plane. Kubernetes v1.27 supports clusters with up to 5,000 nodes. More specifically, Kubernetes is designed to accommodate configurations that meet *all* of the following criteria:

- No more than 110 pods per node
- No more than 5,000 nodes
- No more than 150,000 total pods
- No more than 300,000 total containers

You can scale your cluster by adding or removing nodes. The way you do this depends on how your cluster is deployed

Assume 80.000.000 RPS being distributed among 300.000 containers, each container get sprayed with **266** RPS.

(The container may contain different servers that server request by threads and processes)

Industry Q&A with NaWAS Anti-DDoS | Netnod

WE DO Security - WEDOS WE DO Security - WEbhosting DOmains Servers