Secrets At Sea

Hunting Exposed Code & Container Registries

Gaetan FERRY & Guillaume VALADON

Introduction

$ whoami

Guillaume

Cybersecurity Researcher

editor-in-chief of the **MISC magazine**

Scapy maintainer

previously at **Quarkslab,** ANSSI…

Gaetan

Cybersecurity Researcher

former researcher **@Sonar**

Synacktiv red teamer for 7 years

Public & Private Leaks

Leaking secrets is very easy

hardcoding secrets is easier than handling them safely!
private things will go public, **PoCs will go to production**…
developers leak in personal projects

35%
Private repos leak

5%
For public repos

Closer to production means leakier

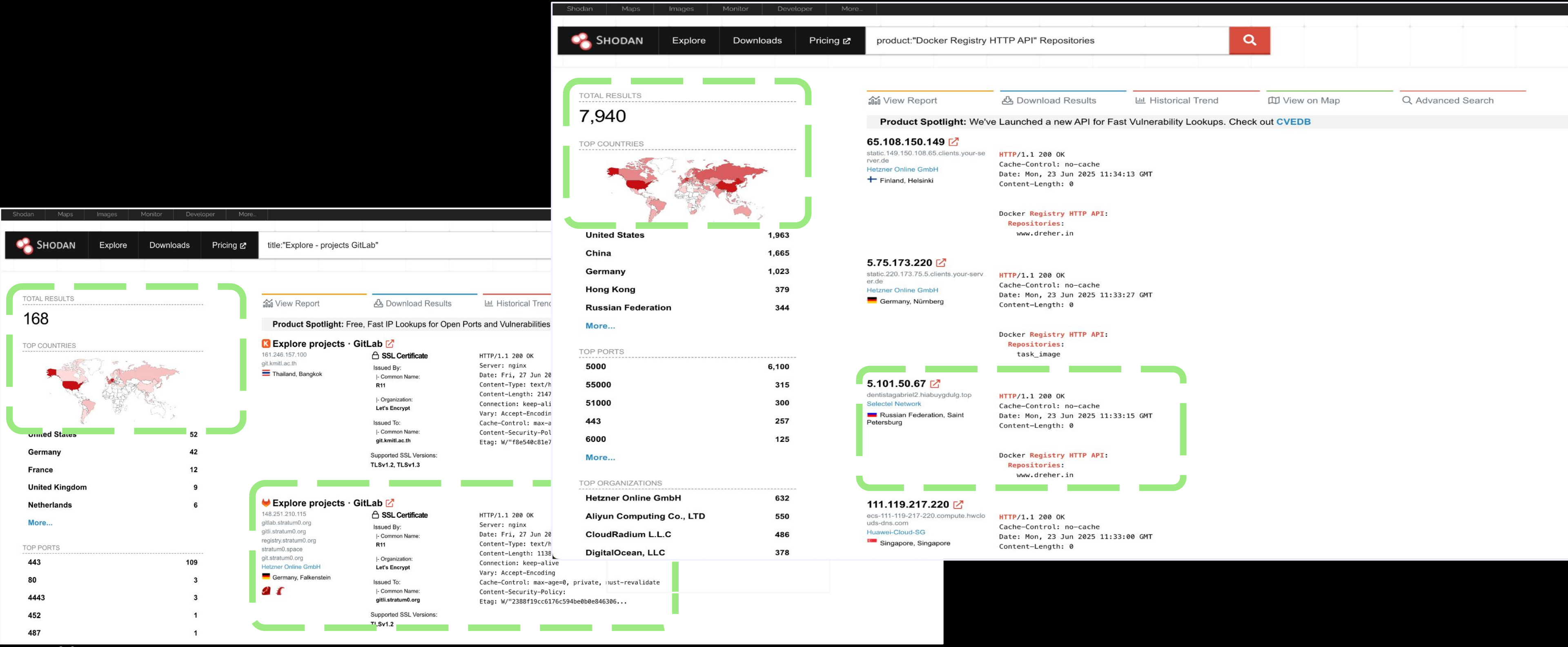
secrets are mostly needed in production
production > container > artifacts > source code

Public leaks are the worst but **private leaks are bad too** 🌐

Research Key Questions

Are there **publicly accessible registries**?
Do they contain **private repositories**?
Do they **leak secrets?**
Who owns them?

Research Short Answer



title:"Explore - projects GitLab"

TOTAL RESULTS

168

TOP COUNTRIES

United States	52
Germany	42
France	12
United Kingdom	9
Netherlands	6

More...

TOP PORTS

443	109
80	3
4443	3
452	1
487	1

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities

Explore projects · GitLab
161.246.157.100
git.kmitl.ac.th
Thailand, Bangkok

SSL Certificate
Issued By:
|- Common Name:
R11
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
git.kmitl.ac.th
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 27 Jun 20
Content-Type: text/h
Content-Length: 2147
Connection: keep-ali
Vary: Accept-Encodin
Cache-Control: max-a
Content-Security-Pol
Etag: W/"f8e540c81e7
```

Explore projects · GitLab
148.251.210.115
gitlab.stratum0.org
gitli.stratum0.org
registry.stratum0.org
stratum0.space
git.stratum0.org
Hetzner Online GmbH
Germany, Falkenstein

SSL Certificate
Issued By:
|- Common Name:
R11
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
gitli.stratum0.org
Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 27 Jun 20
Content-Type: text/h
Content-Length: 1138
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: max-age=0, private, must-revalidate
Content-Security-Policy:
Etag: W/"2388f19cc6176c594be0b0e846306...
```

product:"Docker Registry HTTP API" Repositories

TOTAL RESULTS

7,940

TOP COUNTRIES

United States	1,963
China	1,665
Germany	1,023
Hong Kong	379
Russian Federation	344

More...

TOP PORTS

5000	6,100
55000	315
51000	300
443	257
6000	125

More...

TOP ORGANIZATIONS

Hetzner Online GmbH	632
Aliyun Computing Co., LTD	550
CloudRadium L.L.C	486
DigitalOcean, LLC	378

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

65.108.150.149
static.149.150.108.65.clients.your-server.de
Hetzner Online GmbH
Finland, Helsinki

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Date: Mon, 23 Jun 2025 11:34:13 GMT
Content-Length: 0


Docker Registry HTTP API:
  Repositories:
    www.dreher.in
```

5.75.173.220
static.220.173.75.5.clients.your-server.de
Hetzner Online GmbH
Germany, Nürnberg

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Date: Mon, 23 Jun 2025 11:33:27 GMT
Content-Length: 0


Docker Registry HTTP API:
  Repositories:
    task_image
```

5.101.50.67
dentistagabriel2.hiabuygdulg.top
Selectel Network
Russian Federation, Saint Petersburg

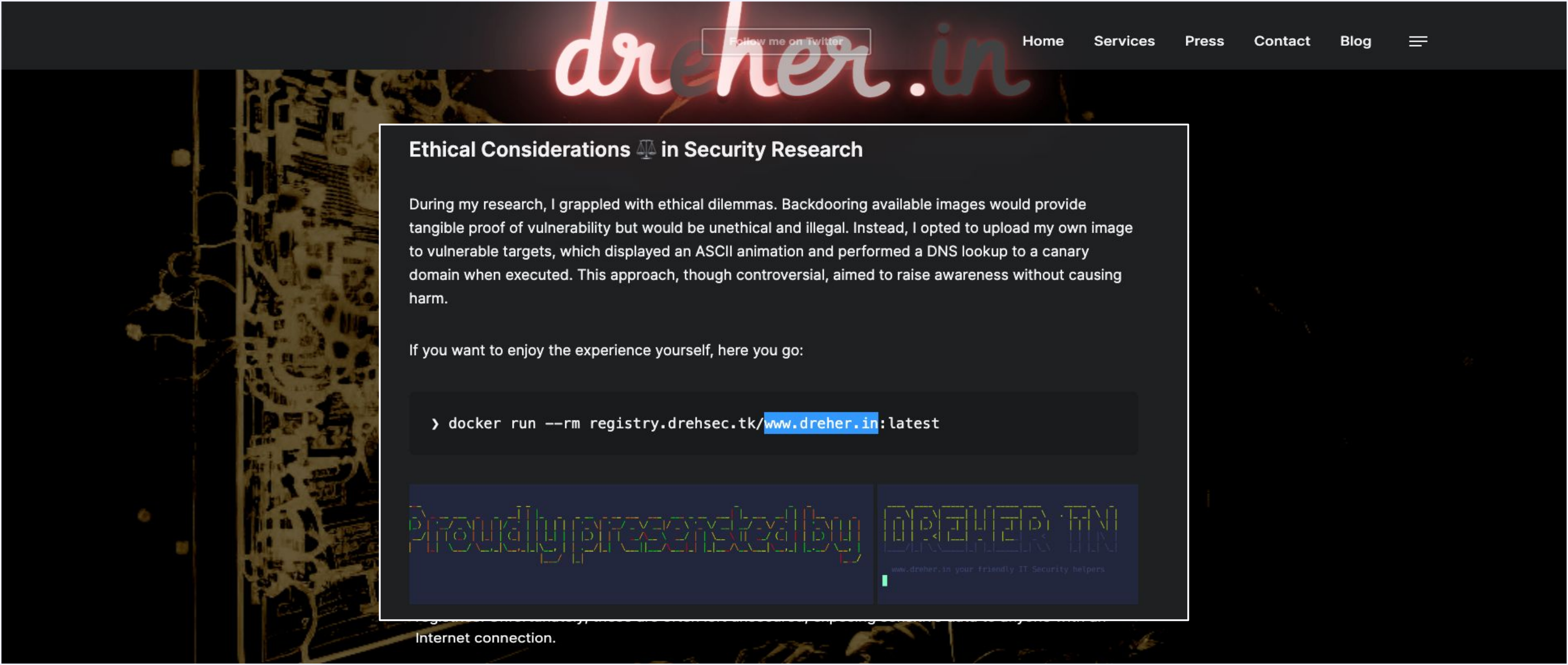
```
HTTP/1.1 200 OK
Cache-Control: no-cache
Date: Mon, 23 Jun 2025 11:33:15 GMT
Content-Length: 0


Docker Registry HTTP API:
  Repositories:
    www.dreher.in
```

111.119.217.220
ecs-111-119-217-220.compute.hwclouds-dns.com
Huawei-Cloud-SG
Singapore, Singapore

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Date: Mon, 23 Jun 2025 11:33:00 GMT
Content-Length: 0
```

Research Previous Work - www.dreher.in



Ethical Considerations ⚖️ in Security Research

During my research, I grappled with ethical dilemmas. Backdooring available images would provide tangible proof of vulnerability but would be unethical and illegal. Instead, I opted to upload my own image to vulnerable targets, which displayed an ASCII animation and performed a DNS lookup to a canary domain when executed. This approach, though controversial, aimed to raise awareness without causing harm.

If you want to enjoy the experience yourself, here you go:

```
❯ docker run --rm registry.drehsec.tk/www.dreher.in:latest
```

```
www.dreher.in your friendly IT Security helpers
```

Internet connection.

🔗 https://www.dreher.in/blog/unprotected-container-registries

02
Methodology

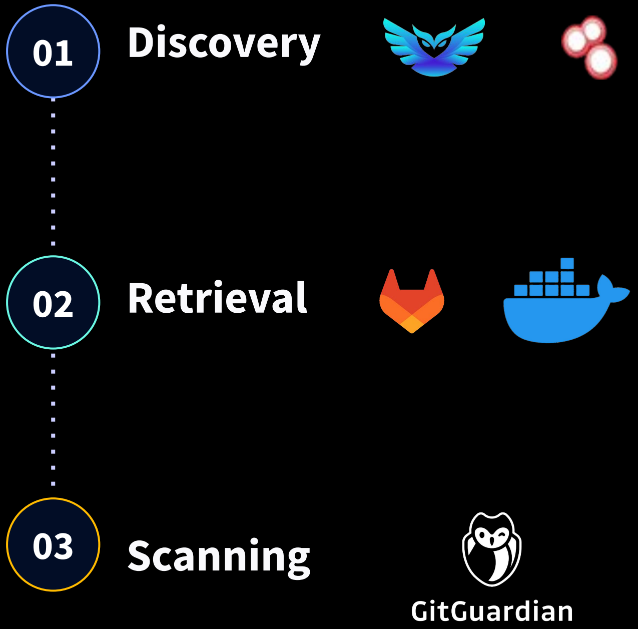
Discovering exposed registries ourselves.

Methodology

From One to Three

Three simple and common steps.

Looking for vulnerabilities at scale is often splitted into three distinct phases.



01 Discovery

02 Retrieval

03 Scanning

Discovery Phase Examples

🔍 **Product queries**

Docker Registry

GitLab Self-Managed

🫆 **Specific HTTP fingerprinting**

X-gitlab-meta HTTP header

well-known HTTP titles

SHODAN

📋 **Keywords**

docker

gitlab

registry

harbor

MERKLEMAP

Retrieval Phase Examples

Various TCP ports

443, **80**, 8099, 8080…

GET /explore

list public repositories
might be authn !

GET /api/v4/projects

More reliable

`git clone`

Various TCP ports

443, **80**, 5000…

GET /v2/_catalog

list Docker repositories

`docker pull`

Docker Registry Over Plain HTTP

Not supported by common tools

must build a custom tool based on the Registry API.

```
$ docker pull 192.0.2.28:5000/pts2025:latest
Error response from daemon: Get "https://192.0.2.28:5000/v2/": http: server gave
HTTP response to HTTPS client
```

🔬Inspecting images

https://github.com/containers/skopeo

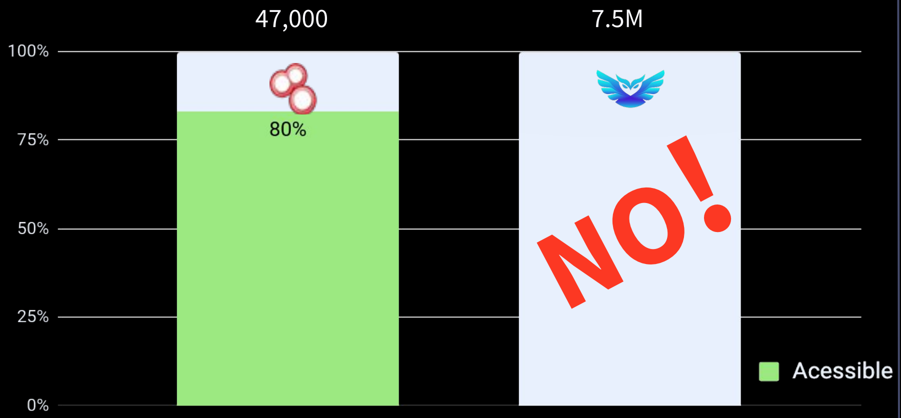
Endpoints

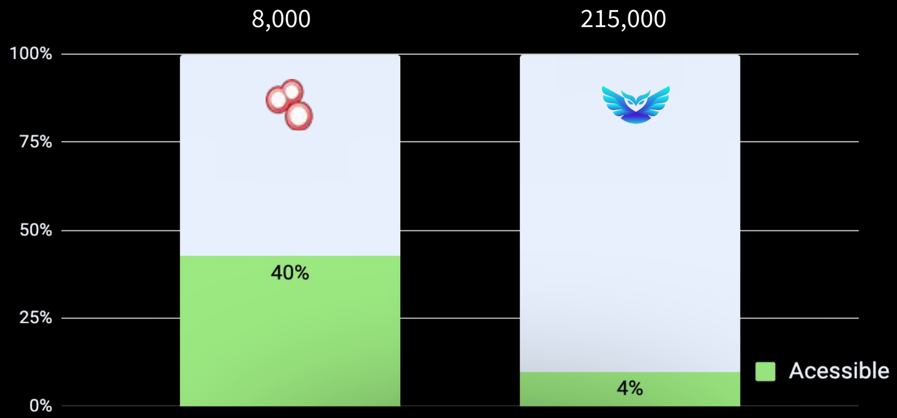
/v2/<repository>/tags/list

/v2/<repository>/manifest/<tag>

/v2/<repository>/blobs/<blob>

Discovery Phase Results





Key Findings

39k registries

11k public

67k git repositories

~2 TB

Key Findings

4500 registries

75k repositories

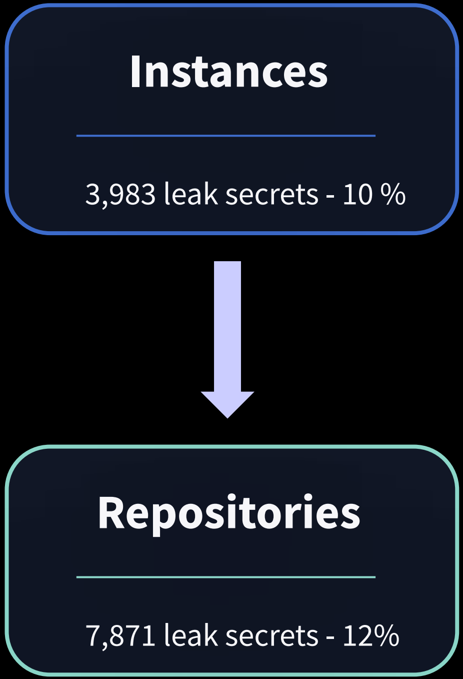
225k Docker images

04

Secrets Analysis

Charts & Numbers.

Secrets Exposures

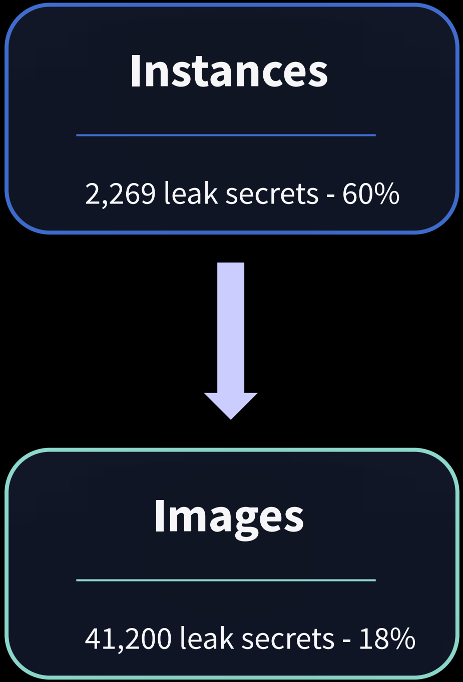


Instances

3,983 leak secrets - 10 %

Repositories

7,871 leak secrets - 12%



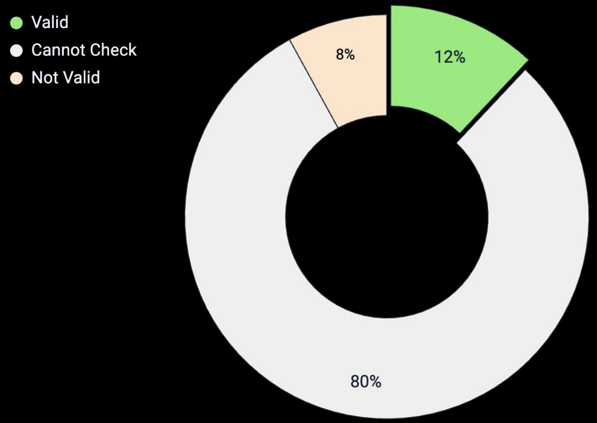
Instances

2,269 leak secrets - 60%

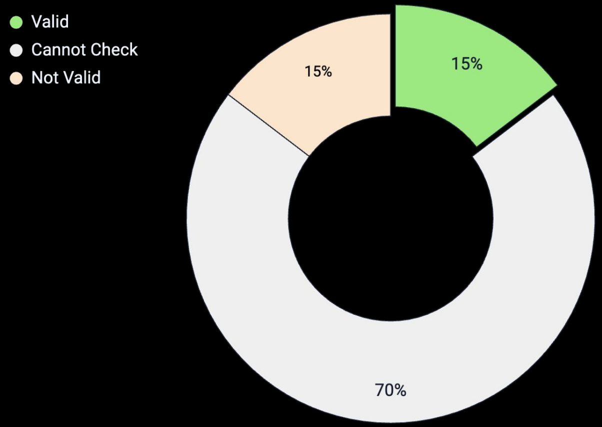
Images

41,200 leak secrets - 18%

Secrets Validity



Total secrets: 57,000
Specifics: 20,000
Generics: 37,000



Total secrets: 23,000
Specifics: 9,000
Generics: 14,000

Secret Types Breakdown

VCS

🦊 930
2% valid

🐳 130
40% valid

Cloud

🦊 1200
47% valid

🐳 800
60% valid

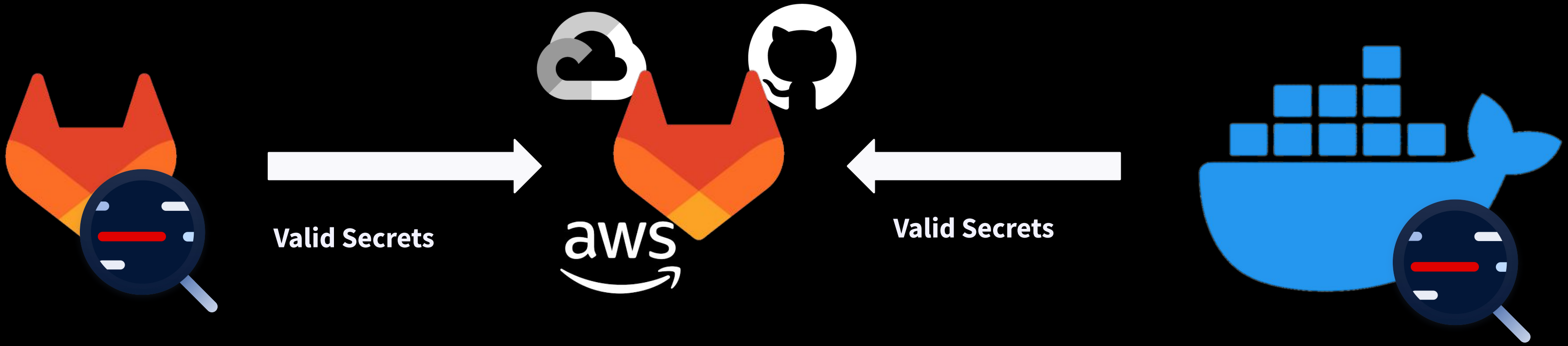
Data Storage

🦊 3100
4% valid

🐳 1000
32% valid

Docker: less secrets, more valids - It’s **closer to production**!

Secrets Russian Dolls



Publicly exposed leaks lead to private repositories, code, and **other secrets being exposed**. ∞

Name Dropping

Well, not today.

Notable Industries Leaking Repositories

Public entities (Govs)

Consulting co.

Software development

Software development

Video game industry

Universities

Legal services

Beyond Secret Leaks - Private Code

Lots of hints the exposed data should sometimes not be public
- 80% failed check DB creds -> DB hosts are internal!
- Confidentiality mentions

This software is the confidential and proprietary information of REDACTED.

Might include juicy information for a RedTeam
- 67k GitLab repos revealed 300k+ email addresses (2k .gov)
- (Open?) Source code to look for vulnerabilities in
  - 🪲Bug Bounty tip🪲
- But also: S3 bucket names, SaaS application URL, domain names,... 🍽️

Takeaways

transient leaks

18% of the Docker registries not accessible anymore

most secrets are still valid

GitLab servers badly protected by a frontend

GitLab API's web_url provides a host, the host is IP whitelisted

But the IP we found is different **and not filtered!?** 🤨

hardcoding secrets in private repositories is **also a bad practice**

private repositories might turn public,

or are indeed public

Takeaways

(or else? DockerHub quotas?)

Self hosting **to better** **acy**…

… ontrol security and privacy.

Thank you

Question Time 🔥

Docker Images Retrieval Methodology

Based on GitGuardian R&D

latest 5 tags per repository

ADD & COPY layers up to 45MB

RUN layers up to 5MB

deduplication based on layers names

Informed trade-off to **limit the amount of data** to be downloaded and scanned.