Security Misconfigurations in Open-Source Kubernetes Manifests: An Empirical Study

Akond Rahman

AUBURN

Shazibul Islam Shamim

AUBURN

Dibyendu Brinto Bose

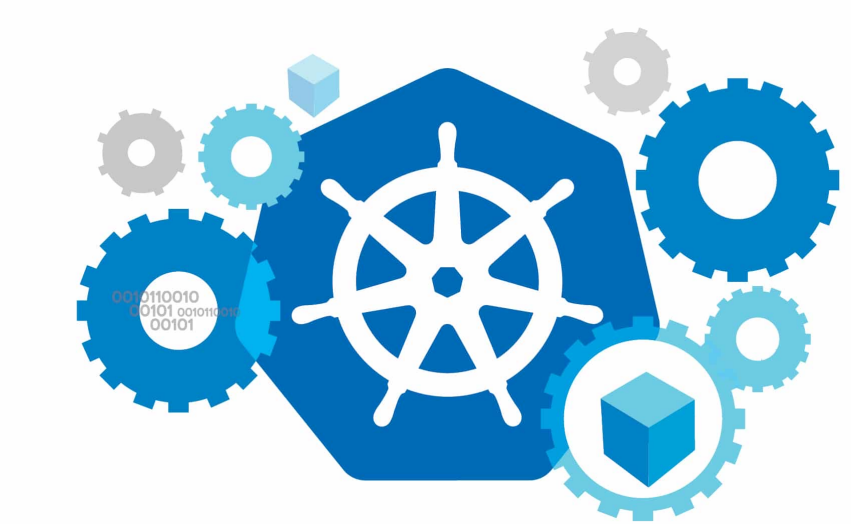
VIRGINIA TECH

Rahul Pandita

GitHub

Container Orchestration

The practice of pragmatically managing the lifecycle of containers with tools, such as Kubernetes.



https://www.opensourceforu.com/2018/06/container-orchestration-kubernetes/

AUBURN

Container Orchestration with Kubernetes

2022

State of Kubernetes security report

“def-facto tool for container orchestration”

[Latest] Global Kubernetes Market Size/Share Worth USD 7.8 Billion by 2030 at an 23.40% CAGR: Markets N Research (Share, Trends, Cap, Adoption, Forecast, Segmentation, Growth, Value)

Markets N Research

https://www.yahoo.com/lifestyle/latest-global-kubernetes-market-size-153000315.html

“Market Size/Share Worth USD 7.8 Billion”

AUBURN

Kubernetes Adoptees

AUBURN

Kubernetes-related Security Concerns

2022

State of Kubernetes security report

Kubernetes security misconfigurations "pose the greatest security concern"

Capital One's Cloud Misconfiguration Woes Have Been an Industry-Wide Fear

Developers and IT decision makers should not be surprised by the recent Capitol One data breach: Misconfigurations have long been the top cloud security concern.

https://thenewstack.io/capital-ones-cloud-misconfiguration-woes-have-been-an-industry-wide-fear/

106 million users affected by a misconfiguration-related security breach

AUBURN

Example of Kubernetes-related Security Misconfigurations

```
securityContext:
   capabilities:
      drop:
         - ALL
   runAsUser: 101
   allowPrivilegeEscalation: true
   ...
```

privileged security context

Example#1: Escalated privilege for child containers

```
rabbitmq:
  username: user
  ## RabbitMQ application password
  password: pFXfkH5cKA
  ...
  ## Value for the RABBITMQ_LOGS environment variable
  ##
  logs: '-'
```

Hard-coded user name

Hard-coded password

Example#2: Hard-coded password

AUBURN

Goal

*The goal of this paper is to **help practitioners** **secure their Kubernetes clusters** by **identifying security misconfigurations** that occur in Kubernetes manifests*

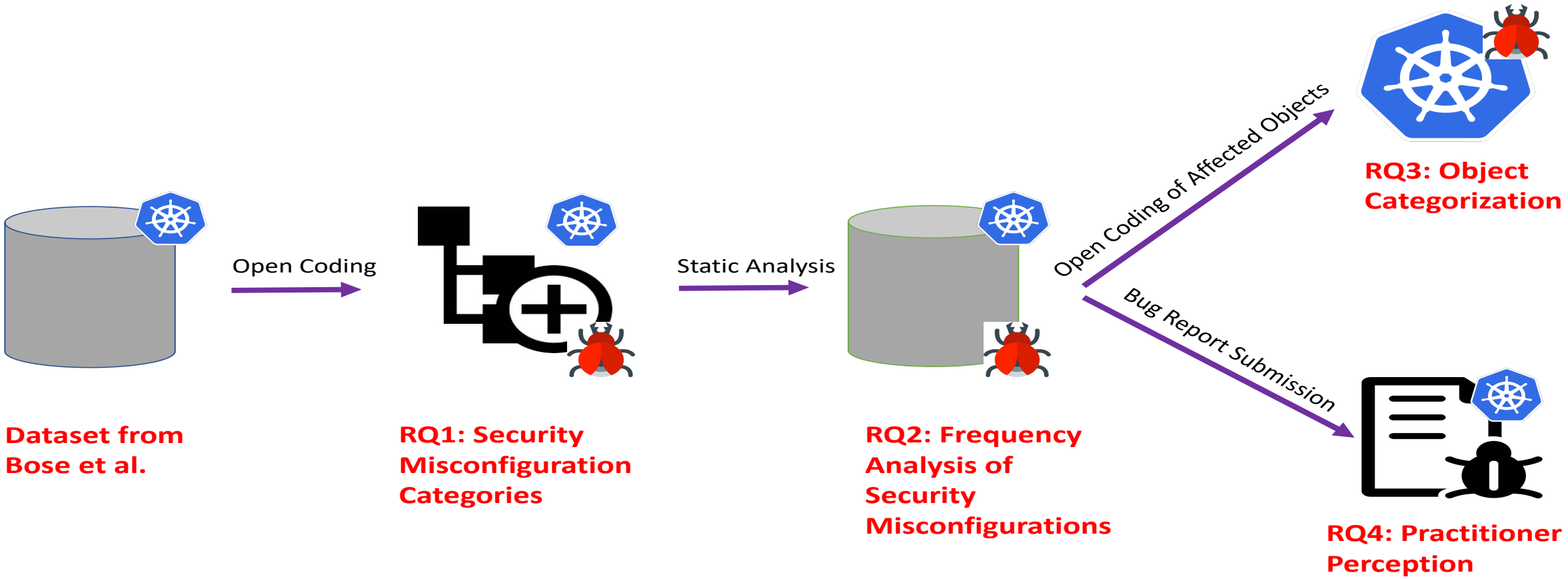
AUBURN

Research Questions

- ***RQ1: What categories of security misconfigurations occur in Kubernetes manifests?***
- ***RQ2: How frequently do security misconfigurations occur in Kubernetes manifests?***
- ***RQ3: What categories of Kubernetes objects are affected by security misconfigurations?***
- ***RQ4: How do practitioners perceive the identified security misconfigurations in Kubernetes manifests?***

AUBURN

Methodology



AUBURN

Answer to RQ1

Absent Resource Limit

```
spec:
  containers:
   - name: employee
     image: piomin/employee-service
```

Absent securityContext

```
spec:
    containers:
    - name: inventory-container
      image: inventory:1.0-SNAPSHOT
```

Activation of hostIPC

```
spec:
     hostIPC: true
```

Activation of hostNetwork

```
spec:
     hostNetwork: true
```

Activation of hostPID

```
spec:
     hostPID: true
```

Capability Misuse

```
capabilities:
     add:
     - CAP_SYS_ADMIN
     - CAP_SYS_MODULE
```

AUBURN

Answer to RQ1 (Contd.)

Docker Socket Mounting

```
- name: dockersocket
    mountPath: /var/run/docker.sock
```

Escalated Privileges for Child Container Processes

```
allowPrivilegeEscalation: true
```

Hard-code Secret

```
POSTGRES_PASSWORD: VGVzdERCQGhvbWUy
```

Insecure HTTP

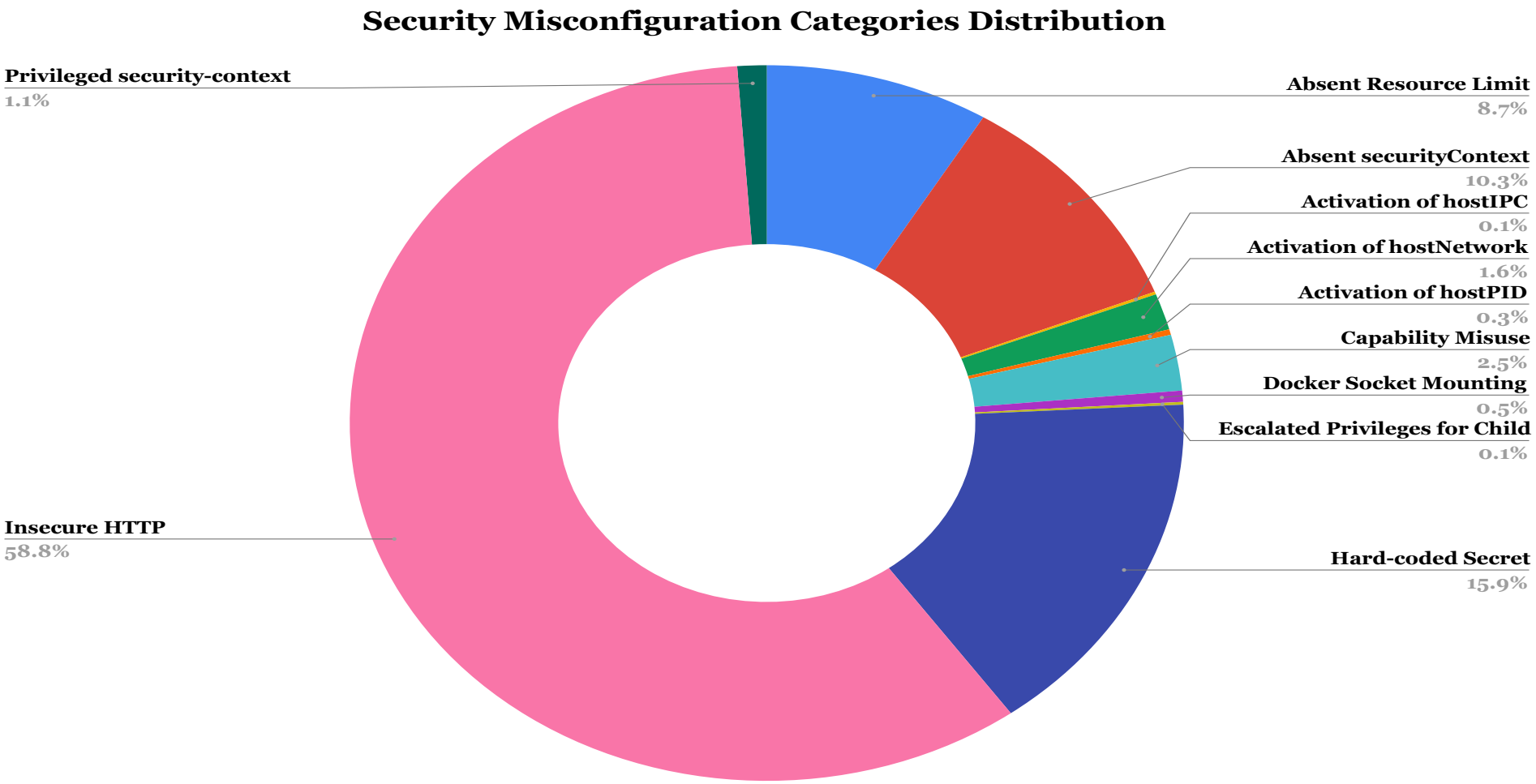
```
value: http://elastisearch-logging:9200
```

Privileged securityContext

```
securityContext:
    privileged: true
```

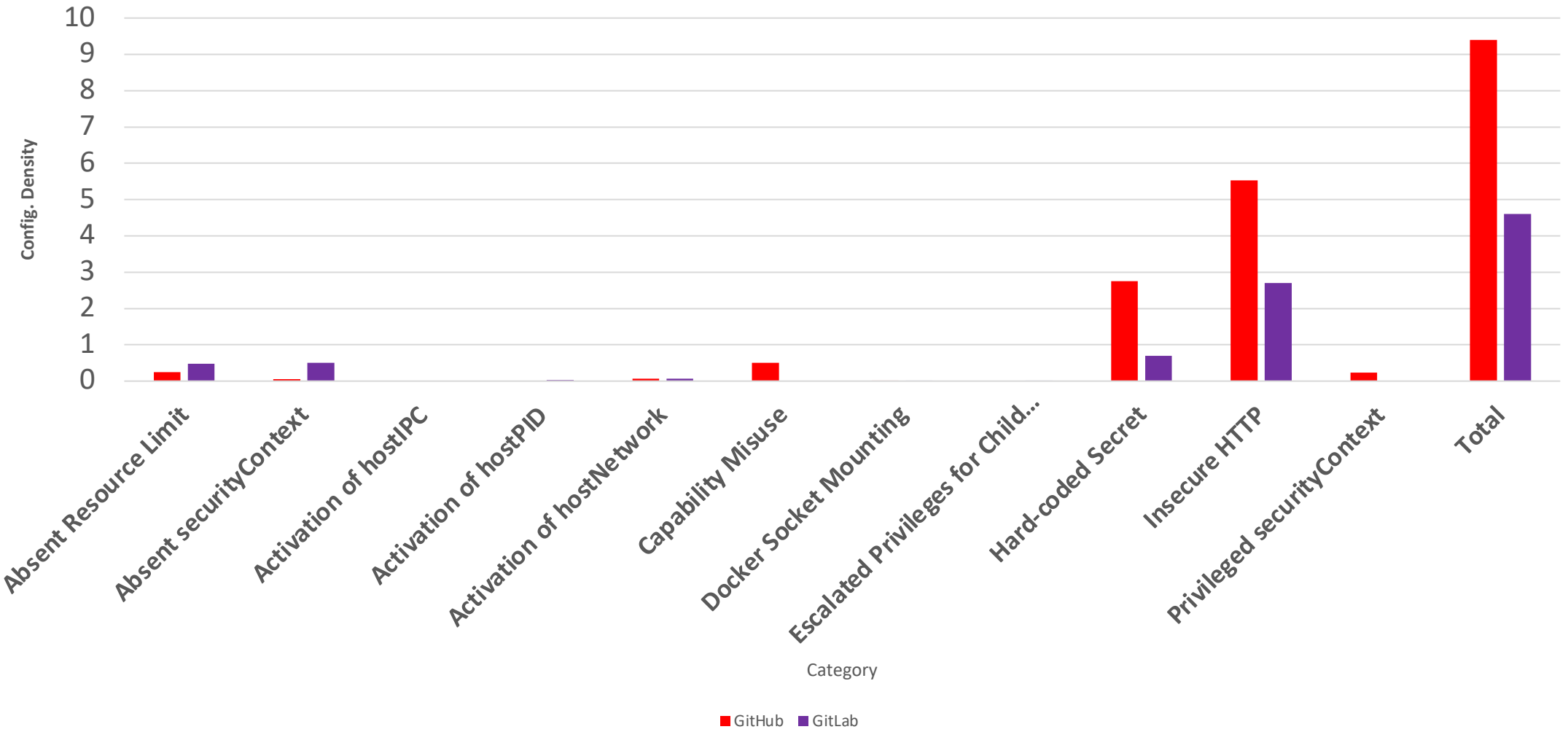
AUBURN

Answer to RQ1 (Contd.)



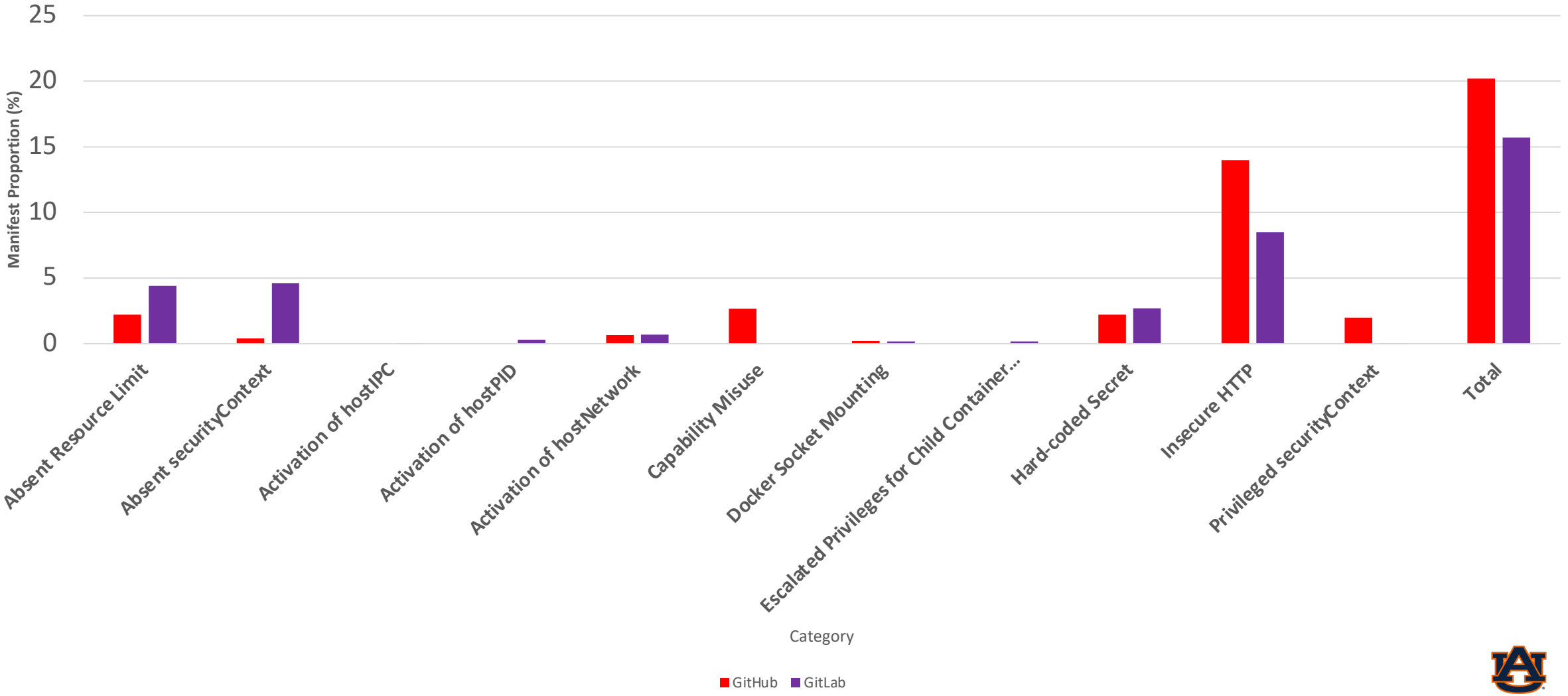
AUBURN

Answer to RQ2 (Misconfiguration Density per KLOC)



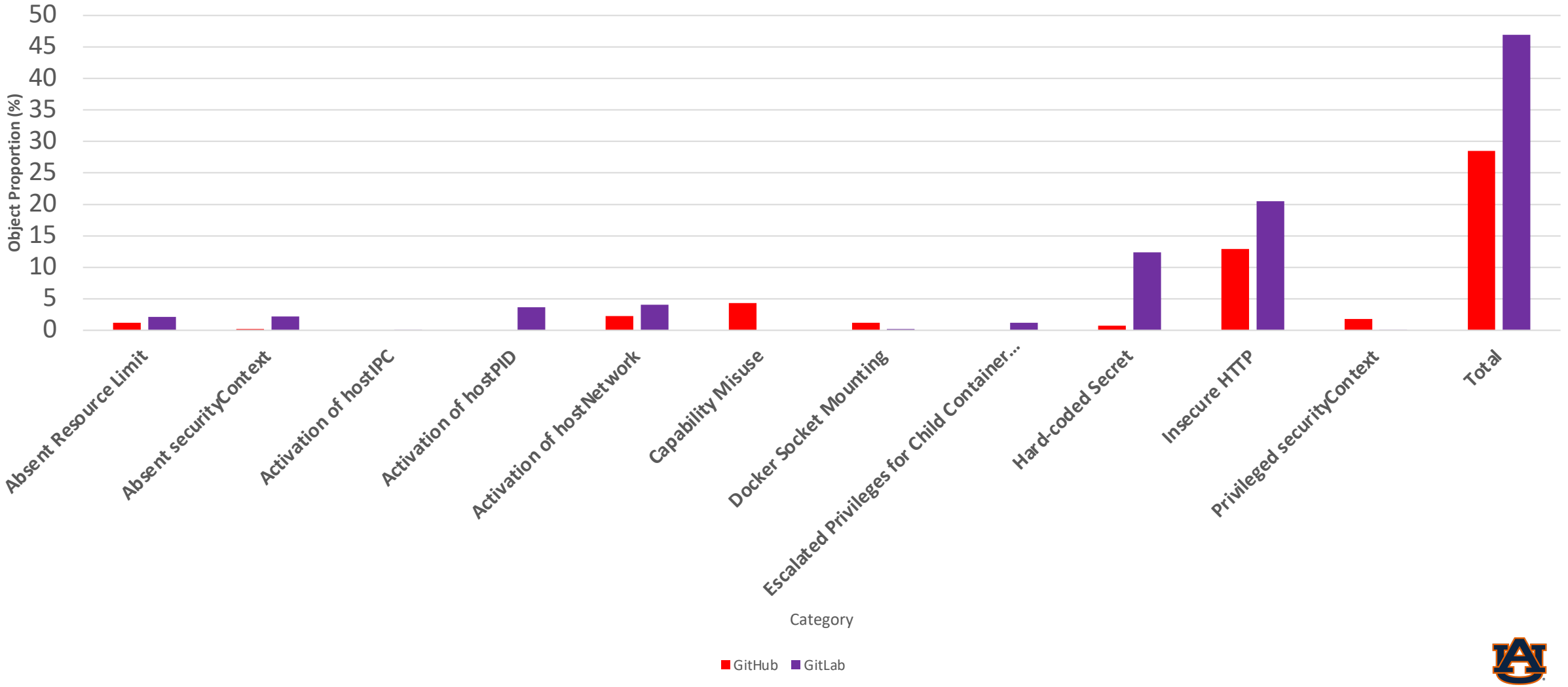
AUBURN

Answer to RQ2 (Manifest Proportion)



AUBURN

Answer to RQ2 (Object Proportion)



AUBURN

Answer to RQ2 (Correlation with Manifest Factors)

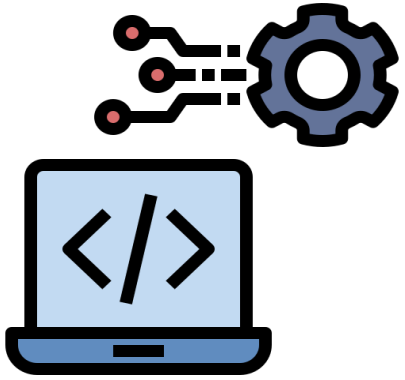
- IsDeployed ❌
- Size ✅
- Age ❌
- Commits ❌
- Developers ❌
- Minor Contributors ❌

AUBURN

Answer to RQ3

Load Balancers

Pod Provisioning



Process Execution

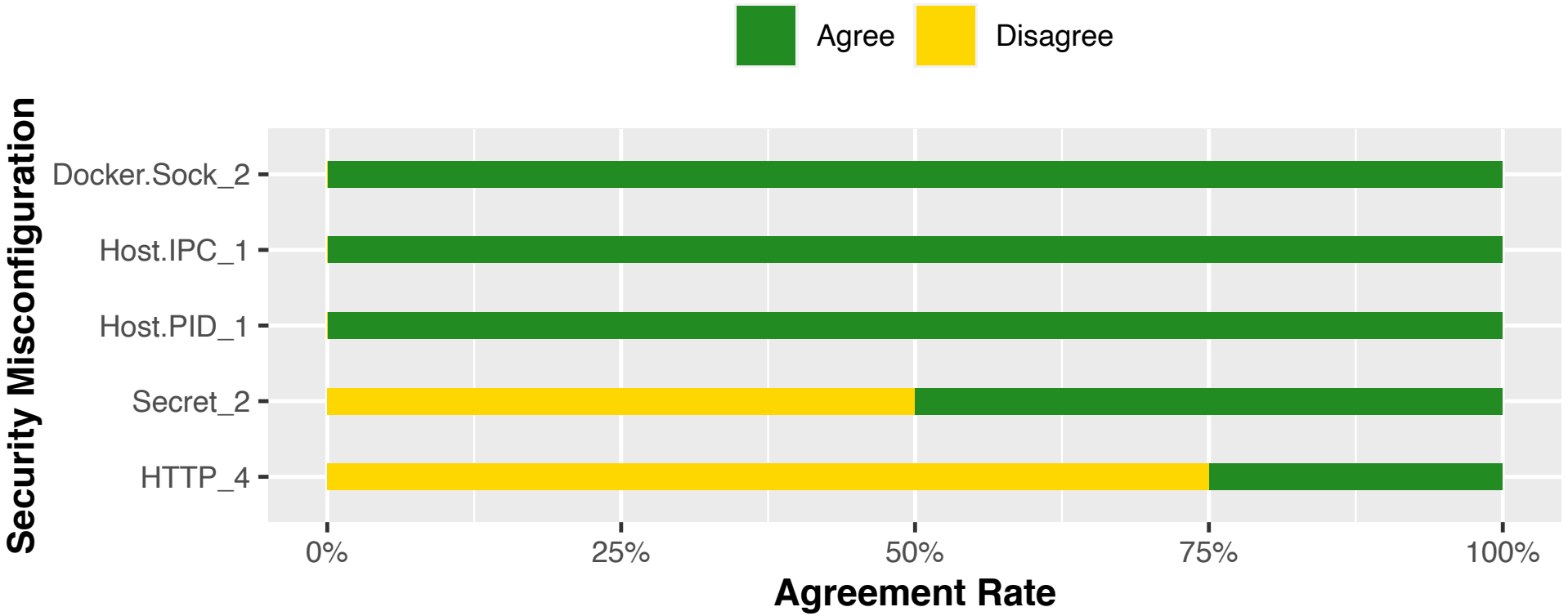
Secret

Stateful Applications

Routing

AUBURN

Answer to RQ4



4.1% response rate for submitted 242 security misconfigurations

AUBURN

Answer to RQ4 (Contd.)

Semi-structured interview with 9 practitioners

ID	Job Title	Usefulness
I1	Consultant	Yes
I2	Site Reliability Engineer	Yes
I3	Site Reliability Engineer	Yes
I4	Site Reliability Engineer	Yes
I5	Software Developer	Yes
I6	Software Developer	Yes
I7	Software Developer	Yes
I8	Site Reliability Engineer	Yes
I9	Software Developer	Yes

AUBURN

Answer to RQ4 (Contd.)

Insights on how to integrate tool

- CI pipeline integration
- Kubernetes integration
- Severity-based prioritization
- Flexibility for users

AUBURN

Threats to Validity

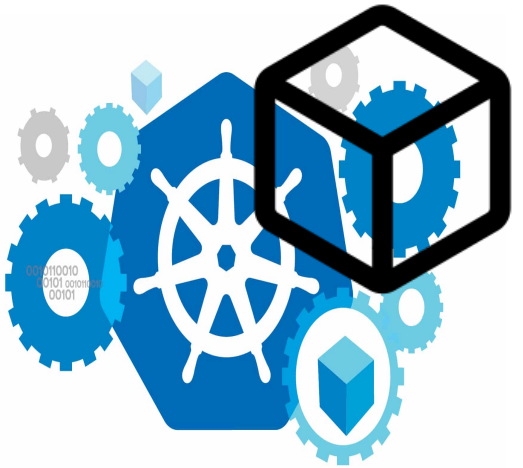
- **Conclusion validity**: limitations related to open coding, closed coding, selection criteria
- **Construct validity**: Limitations of the tool used for analysis
- **External validity**: Use of open-source repositories

AUBURN

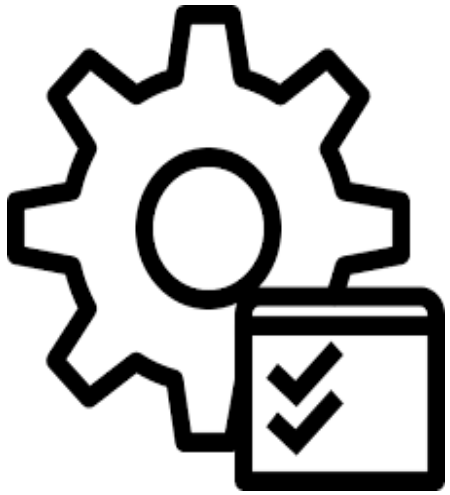
Contributions

Taxonomy

Empirical Evaluation



Object Categories



SLI-KUBE

AUBURN

Summary

2022

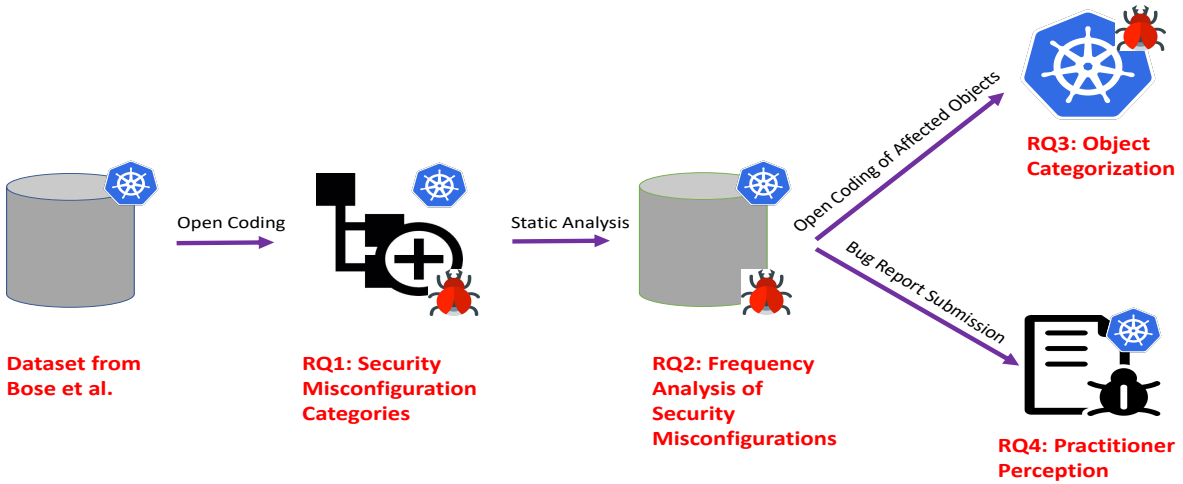
State of Kubernetes security report

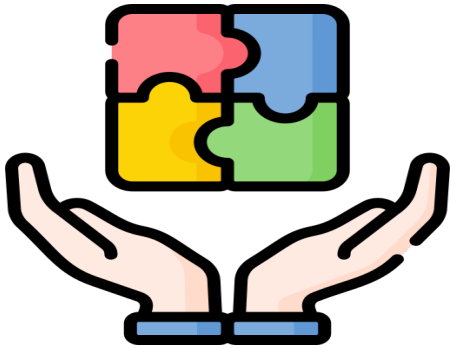
"def-facto tool for container orchestration"

[Latest] Global Kubernetes Market Size/Share Worth USD 7.8 Billion by 2030 at an 23.40% CAGR: Markets N Research (Share, Trends, Cap, Adoption, Forecast, Segmentation, Growth, Value)

Markets N Research

"Market Size/Share Worth USD 7.8 Billion"





Open to Collaborations

akond@auburn.edu
akondrahman.github.io
@akondrahman
AUBURN