Context-Aware Security Intelligence of Vulnerability Scanners in Cloud-native Environments

Ammer Simon / University of Applied Sciences Upper Austria, Dynatrace, AT (simon.ammer@fhooe.at)

Krösche Jens / University of Applied Sciences Upper Austria, AT

Gierlinger Markus, Kahlhofer Mario / Dynatrace, AT

Contact

Simon Ammer

Mobile Computing Master Student | University of Applied Sciences Upper Austria

Software Engineer for Cloud Application Security | Dynatrace | AT

simon.ammer@fhooe.at

ammerzon

ammerzon

UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Motivation

Can we strengthen the security posture of a cloud-native environment by enriching security scanner results with context information?

Motivation

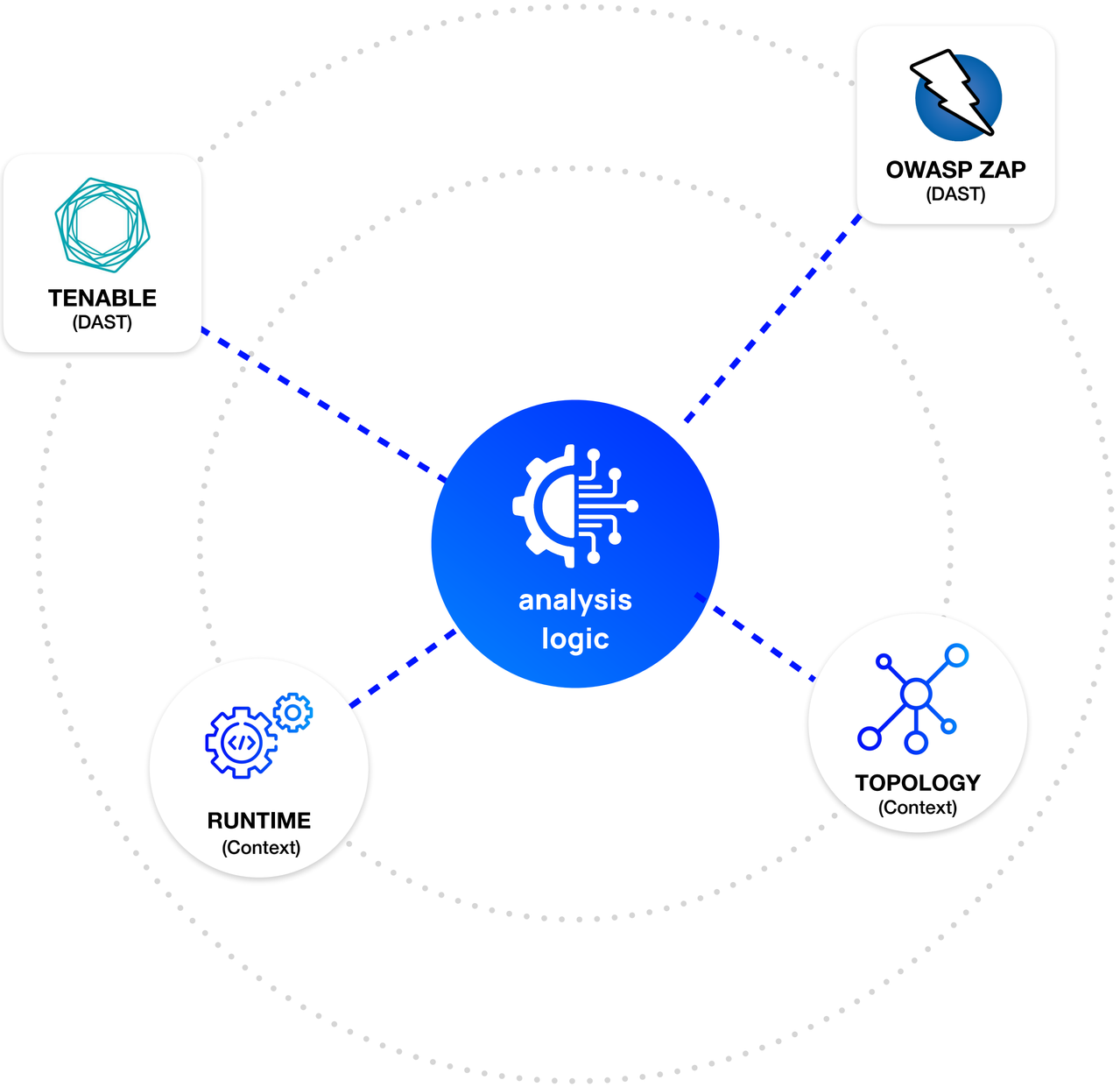
Can we strengthen the security posture of a cloud-native environment by enriching security scanner results with context information?

Motivation

Can we strengthen the security posture of a cloud-native environment by enriching security scanner results with context information?

Motivation

Can we strengthen the security posture of a cloud-native environment by enriching security scanner results with context information?


OWASP ZAP
(DAST)
TENABLE
(DAST)
analysis
logic
RUNTIME
(Context)
TOPOLOGY
(Context)

Goals

Can the false-positive ratio of DAST tools be improved with rules based on contextual information?

How effective is this approach?

Does a graph-based security posture visualisation assist security experts?

Related Work

DAST (Web vulnerability scanner)

high level of disagreement between scan results

recommendation to improve

- the **accuracy** of security verification checks
- the **reporting mechanism**

Mansour Alsaleh, Noura Alomar, Monirah Alshreef, Abdulrahman Alarifi, and AbdulMalik Al-Salman. 2017. **Performance-Based Comparative Assessment of Open Source Web Vulnerability Scanners**. Security and Communication Networks 2017 (May 2017), e6158107. https://doi.org/10.1155/2017/6158107

Related Work

Context-Aware Security

usage of **additional information** to improve security decisions

used in work on **intrusion detection systems**

list the following information as helpful:

network configuration

protocols

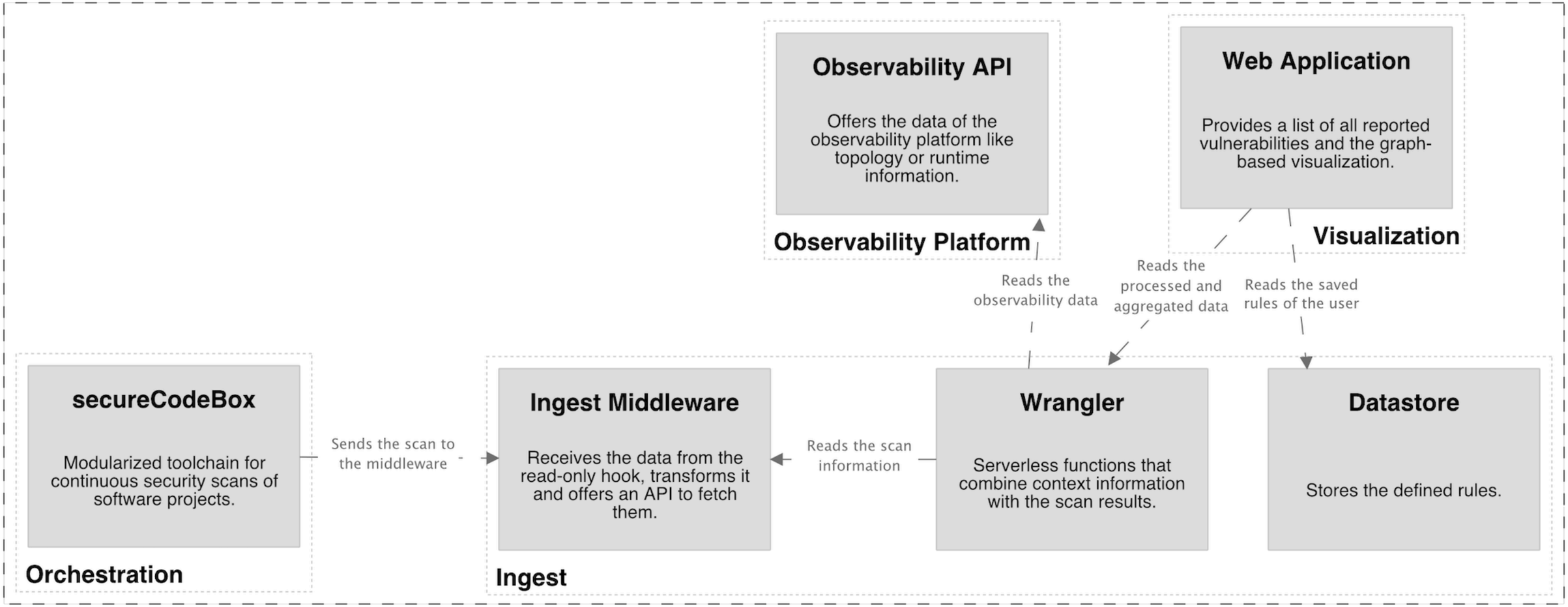
operating systems

services & applications

Nadjah Chergui and Narhimene Boustia. 2020. **Contextual-Based Approach to Reduce False Positives**. IET Information Security 14, 1 (2020), 89–98. https: //doi.org/10.1049/iet-ifs.2018.5479

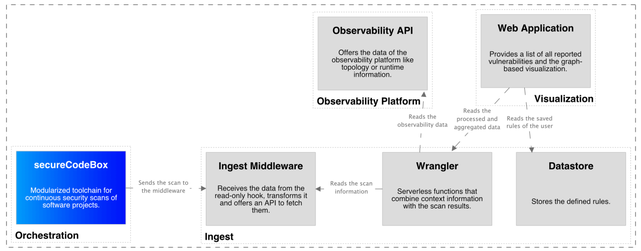
Methodology

Overview



Methodology

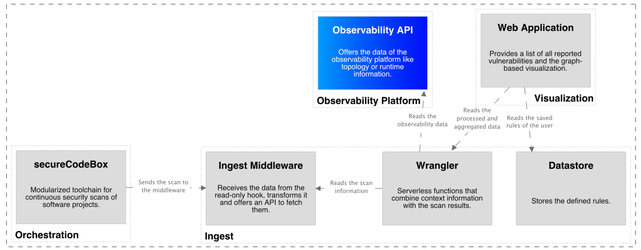
Orchestration




```
{
   "id":"1aaa4efc-14f1-4847-8e43-1413a06c2b0a",
   "name":"Log4Shell (CVE-2021-44228)",
   "description":"Log4j2 ≤2.14.1 JNDI features used in configuration, ...",
   "location":"http://unguard-proxy.unguard.svc:3000",
   "osi_layer":"APPLICATION",
   "severity":"HIGH",
   "attributes":{
      "host":"unguard-proxy.unguard.svc",
      "port":"3000",
      "..."
   }
}
```

Methodology

Observability Platform



Monitoring

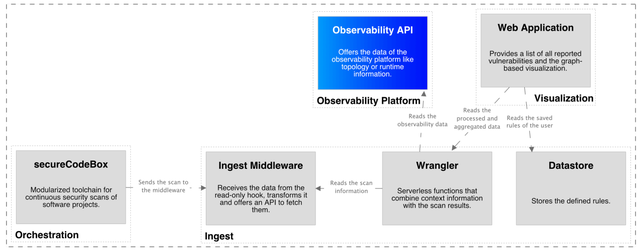
- Alerting
- Overview
- Debugging
- Profiling
- Dependency Analysis
- Anticipating the Future

Observability

UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Methodology

Observability




```
[
   {
      "entityId":"24e1-4247",
      "displayName":"Unguard",
      "hostname":"unguard-proxy.unguard.svc",
      "toRelationships":{
         "..."
      },
      "metadata":{
         "..."
      }"softwareTechnologies":[
         "jdk8u121"
      ],
      "fromRelationships":{
         "..."
      }
   }
]
```

Methodology

Ingest

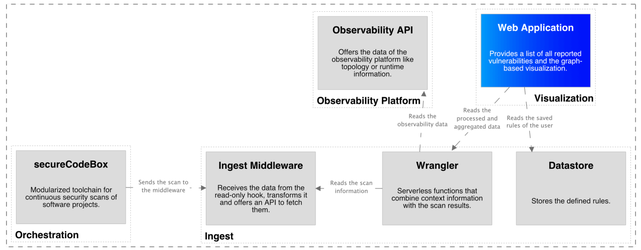

```
{
   "id":"1aaa4efc-14f1-4847-8e43-1413a06c2b0a",
   "name":"Log4Shell (CVE-2021-44228)",
   "description":"Log4j2 ≤2.14.1 JNDI features used
in configuration, ...",
   "location":"http://unguard-proxy.unguard.svc:3000",
   "osi_layer":"APPLICATION",
   "severity":"HIGH",
   "attributes":{
      "host":"unguard-proxy.unguard.svc",
      "port":"3000",
      "..."
   }
}
```

```
[
   {
      "entityId":"24e1-4247",
      "displayName":"Unguard",
      "hostname":"unguard-proxy.unguard.svc",
      "toRelationships":{
         "..."
      },
      "metadata":{
         "..."
      }"softwareTechnologies":[
         "jdk8u121"
      ],
      "fromRelationships":{
         "..."
      }
   }
]
```


UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Methodology

Visualization



Rule Editor

```
package themis.dast
package themis.runtime

deny[msg] {
    input.vulnerability.type == "Log4Shell"
    not input.host.runtime.version in ["6u141", "7u131", "8u121
    msg: sprintf ("Log4Shell vulnerability '%s' host
  runtime does not match the required JDK version" , input.vuln
}
```

Input

```
"findings": [
    {
        "id": "1aaa4efc-14f1-4847-8e43-1413a06c2b0a",
        "name": "Log4Shell (CVE-2021-44228)",
        "description": "Log4j2 <=2.14.1 JNDI features used
        "location": "http://unguard-proxy.unguard.svc:3000
        "osi_layer": "APPLICATION",
        "severity": "HIGH",
        "attributes": {
            "host": "unguard-proxy.unguard.svc",
            "port": "3000",
            ...
        }
    }
]
```

Output

```
Found 1 result in 274µs.
{
    "deny": [
        "Log4Shell vulnerability 1aaa4efc-14f1-4847-8e43-1
    ]
}
```

Save | Evaluate | Coverage

Rule Editor

```
1  package themis.dast
2  package themis.runtime
3
4  deny[msg] {
5      input.vulnerability.type == "Log4Shell"
6      not input.host.runtime.version in ["6u141", "7u131", "8u121"
7      msg: sprintf ("Log4Shell vulnerability '%s' host
8    runtime does not match the required JDK version" , input.vuln
9  }
```

Input

```
1  "findings": [
2      {
3          "id": "1
4          "name":
5          "descrip
6          "locatio
7          "osi_lay
8          "severit
9          "attribu
10             "hos
11             "por
12             ...
13         }
14     }
15 ]
```

Output

```
1  Found 1 result i
```

```
Shell"
 ["6u141", "7u131", "8u121"
ility '%s' host runtime
 version" ,
```

Input

```
1  "findings": [
2      {
3        "id": "1aaa4efc-14f1-4847-8e43-1413a06c2b0a",
4        "name": "Log4Shell (CVE-2021-44228)",
5        "description": "Log4j2 <=2.14.1 JNDI features used i
6        "location": "http://unguard-proxy.unguard.svc:3000",
7        "osi_layer": "APPLICATION",
8        "severity": "HIGH",
9        "attributes": {
10         "host": "unguard-proxy.unguard.svc",
11         "port": "3000",
12          ...
13       }
14     }
15 ]
```

Output

```
1  Found 1 result in 274µs.
2  {
3      "deny": [
4          "Log4Shell vulnerability 1aaa4efc-14f1-4847-8e43-1
5      ]
6  }
```

Themis | Findings | Editor | Settings

Ammersche's Ruleset, Themis

Default

- [x] Themis
- [x] Ammersche's Ruleset

Custom

- [ ] Pentester 1

Findings

Filtered | Non Filtered

Filter By

Scanner	Finding	Score	Affected services	First seen	Last change
OWASP Zap	Log4Shell (CVE-2021-44228)	CRITICAL 9.5	Unguard	5d	2d
Unknown	Content Security Policy (CSP) Header Not Set	MEDIUM 7.9	Unguard	6d	6d
Tenable	Cross-Domain Misconfiguration	LOW 4.3	Unguard	5w	4d

10 rows per page

Page 1 of 1

Ammersche's Ruleset, Themis

Default

- [x] Themis
- [x] Ammersche's Ruleset

Custom

- [ ] Pentester 1

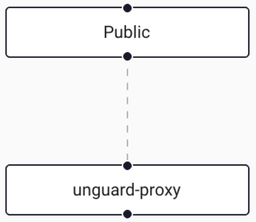
Filtered Non Filtered

ices	First seen	Last change
	5d	2d
	6d	6d
	5w	4d

Log4Shell (CVE-2021-44228)

Category: Remote Code Execution

Apache Log4j2 lower than 2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default.

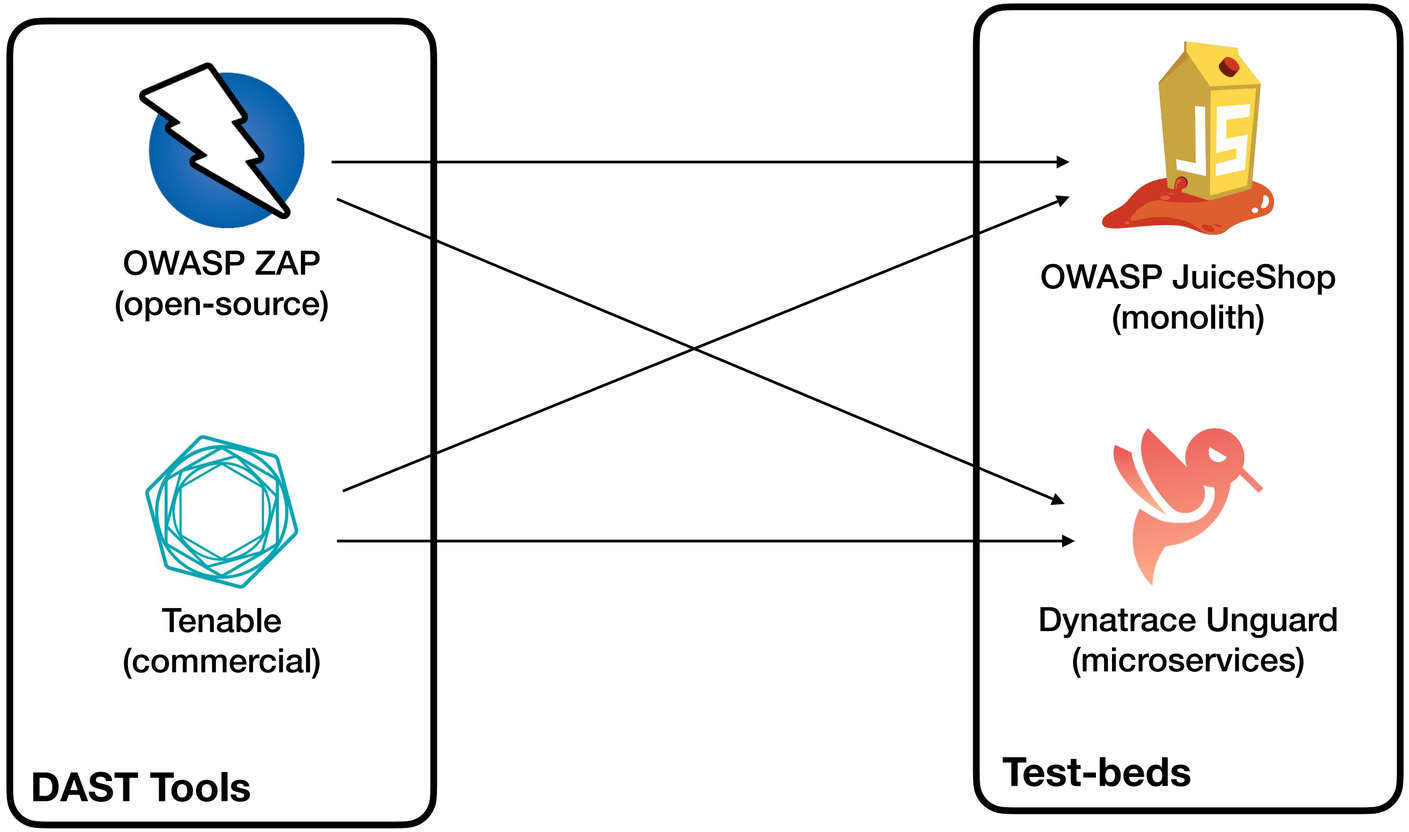


Paths

Path	Method
/user/simuser_4	GET
/mytimeline	GET
[root]	GET

Evaluation & Results

Details



amount of false positives most important metric

Conclusion

Summary & Outlook

reduce false positives of security tools with context information

better results are expected for microservice-based applications (topology)

the effectiveness will be evaluated in the near future with the two projects, Unguard and OWASP JuiceShop

graph-based visualisation has to be tested with production data

Q&A

Key outcomes

reduce false positives of security tools with context information

the effectiveness will be evaluated in the near future with the two projects, Unguard and OWASP JuiceShop

simon.ammer@fhooe.at

ammerzon

ammerzon