ASPM

story about unicorns, sneaky business and unexpected decisions

Ivan Elkin – AppSec TL
In the middle of nowhere
You are an AppSec

What is your daily routine

- Repositories
- Domains
- Libraries
- Vulnerabilities
- Developers

- Scanners:
  - SAST
  - DAST
  - SCA
  - Secrets

Simply you are Running Scanners and Validating Vuls
You are an AppSec

What is your daily routine

- Repositories: 8000
- Domains: 1000
- Libraries: 10000
- Vulnerabilities: 10000
- Developers: 300

- Scanners Findings
  - SAST: 3000
  - DAST: 2000
  - SCA: 2000
  - Secrets: 1000

Take your shovel, pitchfork and go for a work
Let’s put it everything together into one system
Initially we developed it ourselves v.1
Initially we developed it ourselves v.2
The main problem – you need to have programming skills to support the code, finding bugs, fixing it

... so yet another Job
Finding a better live in open source 🦋
What kind of VM tools do you know?

- DefectDojo - [github.com/DefectDojo/django-DefectDojo](https://github.com/DefectDojo/django-DefectDojo)
- Faraday - [github.com/infobyte/faraday](https://github.com/infobyte/faraday)
- Archery - [github.com/archerysec/archerysec](https://github.com/archerysec/archerysec)
Problems we faced

Very specific and not customizable
- We need own kind of entities
- We need own metrics and dashboards
- We need custom integrations (scanners)
- Writing integrations is a pain

UX is not so useful
- From Engineers to Engineers
- You have to click 5 times just to mark one vulnerability as a False Positive

Some of them is not highload
- Horizontal scaling not working
One day we found a Unicorn 🦄
And it’s name ASPM
Inventory of any kind of Assets

Values

Observe whole system

Tagging assets by criticality

See total risks
Vulns for each kind of asset

Values

Results of each scan

Details of vulnerabilities

Easy access to any asset
Automate through workflows

Values

- No-code automation
  - run scans
  - change stats

Event triggers
Nice **CUSTOM** Dashboards!

Values

- Coverage
- AppSec team
- Dev teams
Pros, Cons, Kudos

- Made by good engineers and specifically AppSecs for AppSec
- Many new features that it will rise day by day
- Startup with $16.5M on 2nd round of investments
- PoC Pilot went very good even with Highload (Hybrid installation)
- Fair price as we are one of the first big customers
- Good support (slack, often meetings, quick response)
Security tools Never works out-of-the-box, but it’s not a problem

- Spend 100+ m/h to resolve some issues
- Created 60+ issues to support

Let me tell a short story...
Short fairy tale about Fails
or how to hack yourself

1. Find cyber-unicorn 🦄
2. Spend 100+ hours to integrate unicorn on-prem
3. Create 60+ issues to unicorn-support
4. Believe that in the end unicorn will solve all your problems!
5. Receive news that cyber-wolves ate your unicorn 🐶
So, what happened?

Q1  - We started integrating ASPM
Q3  - Big company bought ASPM startup
Q4  - Big company **discontinued** ASPM
So, I have to say to wolves
Unexpected solution
and follow the 🐰
User: I need something to visualize tables in database change data on a flight build charts and dashboard and it should be open source...

... 7 minutes after...

AI: Use Headless-CMS
NO-Code Headless CMS solutions
No-code Headless CMS

- strapi
- Budibase
- appsmith
- directus
ASPM based on Headless CMS
Customizable assets

Views and bookmarks
Filters
Batch update
Dashboards - yes, they are custom!

Drag’n’Drop widgets
Aggregations
Filters
Workflows

- CRON and Webhooks
- Drag’n’drop flows
- Custom JS extensions
Even Custom styles

Using Built-in styles

Writing custom component

```html
custom CSS

```
```html
```
<table>
<thead>
<tr>
<th></th>
<th>Self developed</th>
<th>Open Source</th>
<th>Vendor</th>
<th>Headless CMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to first start</td>
<td>Very Slow</td>
<td><strong>Fast</strong></td>
<td>Fast / Slow</td>
<td>Medium</td>
</tr>
<tr>
<td>Customization</td>
<td><strong>100%</strong></td>
<td>50%</td>
<td>Very Low ?</td>
<td><strong>80%</strong></td>
</tr>
<tr>
<td>Customization speed</td>
<td>Slow</td>
<td>Slow</td>
<td>Medium ?</td>
<td><strong>Very Fast</strong></td>
</tr>
<tr>
<td>Support</td>
<td>Slow</td>
<td>Very Slow</td>
<td><strong>Very Fast</strong></td>
<td>Fast</td>
</tr>
<tr>
<td>Integrations</td>
<td><strong>Any</strong></td>
<td>Any but Limited</td>
<td>Limited</td>
<td><strong>Any</strong></td>
</tr>
</tbody>
</table>

* In my humble opinion
P.S.  Hacking the marketing
P.S Hacking the marketing

What is an ASMP?
Just yet another Buzzword that cost like an airplane
1. Asset discovery and inventory

2. Risk assessment

3. Scanners Orchestration

4. Reports and Dashboards

5. Real-time monitoring

6. No-Code Automation

7. Compliance Monitoring

8. It’s not just a security tool

---

**7 Essential Components for ASPM**
(Application Security Posture Management)

<table>
<thead>
<tr>
<th>Category</th>
<th>ASPM</th>
<th>Traditional AppSec</th>
<th>ASOC</th>
<th>CISM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Manage and scale an AppSec program based on business risk</td>
<td>Secure applications against vulnerabilities</td>
<td>Orchestrate and correlate security activities</td>
<td>Manage and monitor the security of cloud environments</td>
</tr>
<tr>
<td>Benefits</td>
<td>Provides holistic visibility into the app environment to enable effective risk management and remediation</td>
<td>Enhances app security against threats</td>
<td>Streamlines security operations and responses</td>
<td>Identifies and mitigates cloud security risks</td>
</tr>
<tr>
<td>Integrations</td>
<td>On-premises and cloud-based environments</td>
<td>Embedded in app development lifecycle</td>
<td>Organization-wide deployment</td>
<td>Cloud infrastructure and services</td>
</tr>
</tbody>
</table>
2. De-duplication is not a feature
2. De-duplication is not a feature

In most cases de-duplication can be done by creating unique ID, based on Vulnerability META-information.

\[
\text{sha256}(\text{repo + filename + param + vuln\_type}) [0:31]
\]

( "tfg_" + sha256(\text{repo + filename + secret})) [0:31]

( "dast_" + sha256(\text{domain + param + vuln\_type})) [0:31]
3. Feature requests & Support

Sometimes is easier to help yourself

No need to wait several month until vendor will add a requested feature to product.

You can write a feature by your hands, even if you are not a professional developer
4. We have AI

Also is a kind of marketing to sell you an AI

Summarizing of yesterday commits to get latest news per project

Everyone have own AI :)
5. PoC for you

- Linked models (Defects, Repositories...)
- Dashboard
- Workflows and Extensions
  - Github Loader
  - Nuclei
  - SemGrep
  - Trufflehog

github.com/vankyver/directus-aspm-poc
The END - Morale

Sec tools won’t work out-of-the-box
- All the companies are unique (because of technology stack)

You need ability to develop it by yourself
- You have to adjust security tools to your needs / team / company

Think out of the box
- Don’t use only what market gives you

Use new technologies
- No Code
- AI
P.P.S Remember!

There are a lot of cool Open Source tools nowadays

But there is a Big Company behind the each Big Open Source
Thank you!

ivan.elkin@exness.com

@vankyver