

# ASPM

story about unicorns,  
sneaky business and  
unexpected decisions

Ivan Elkin – AppSec TL  
**exness**

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



OWASP  
Moscow  
2018

Scan Center > Projects Domains Hosts

### Domains

+ ADD NEW DOMAIN REMOVE ALL DOMAINS

Filter...  
sovest|

Missing Headers  External IP

- sovest-test.sovest.com - 195.189.100.20, 195.189.101.20
- api-test.sovest.ru - 195.189.101.22, 195.189.100.22
- api-partner-test.sovest.ru - 195.189.100.32, 195.189.101.32
- api-test.sovest.com - 195.189.101.22, 195.189.100.22
- sovest.ru - 195.189.101.16, 195.189.100.16
- oauth-test.sovest.com - 195.189.100.21, 195.189.101.21

Scan Center > Projects Domains Hosts

### Projects

Secure  Medium  High

afapi\_java - java 2018-02-24 0  
ssh:///afapi\_java

Scan Center > Projects Domains Hosts

### Hosts

Wallarm Monitoring  Wallarm Block  Internal IP  External IP

- afapi.qiwi.com - s3499.qiwi.com - 10.11.43.115  
Wallarm: default:monitoring custom:no  
External IP: 10.250.32.113
- afapi.qiwi.com - s3498.qiwi.com - 10.8.43.127  
Wallarm: default:monitoring custom:no  
External IP: 10.250.32.113

# Initially we developed it ourselves v.2

SCAN CENTER

- Dashboard
- Projects
- Services
- Repositories
- Hosts
- Domains
- Scheduled Tasks

### Dashboard

Scans Today: 12  
▲ high - 3 ▲ low - 3 ▲ secure - 6

Domains: 1001  
Last 24 Hours

Repositories: 1337  
Tracked from Github and Gerrit

Hosts: 2674  
Just Updated

#### CheckMarx scans

updated 4 minutes ago

#### GIXY - Nginx vulnerabilities

Vulnerabilities count 4

Possible HTTP-Splitting vulnerability.  
HIGH  
Using variables that can contain "\n" or "\r" may lead to http injection.  
http\_splitting

Possible SSRF (Server Side Request Forgery) vulnerability.  
HIGH  
The configuration may allow attacker to create a arbitrary requests from the vulnerable server.  
ssrf

#### Last DAST Scans

Scans count 5

Finished	Repository	Severity	Notify Status
2018-11-11T12:14:47.063Z	sovest.com	▲	✓
2018-11-11T12:14:47.027Z	sovest.ru	▲	✓
2018-11-11T12:14:46.970Z	online.contact-sys.com	▲	✓
2018-11-11T12:14:46.863Z	online.contact-sys.com	▲	✓
2018-11-11T12:14:46.668Z	fundl.qiwi.com	▲	✓

#### Last SAST Scans

Scans count 30

Finished	Repository	Severity	Notify Status
2018-11-14 11:45:10	AQW/main	✓	✓

NO OFF ONE 2018

The main problem – you need to have  
programming skills  
to support the code, finding bugs, fixing it  
... so yet another Job

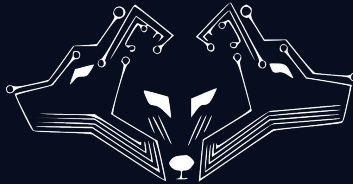


# Finding a better live in open source

# 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)
- Vulnwhisper - [github.com/HASecuritySolutions/VulnWhisperer?tab=readme-ov-file](https://github.com/HASecuritySolutions/VulnWhisperer?tab=readme-ov-file)
- Archery - [github.com/archerysec/archerysec](https://github.com/archerysec/archerysec)
- OWASP VM Center - [owasp.org/www-project-vulnerability-management-center/](https://owasp.org/www-project-vulnerability-management-center/)

DEFECT DOJO



ARCHERY  
a security tool



# Problems we faced

## Very specific and not customizable

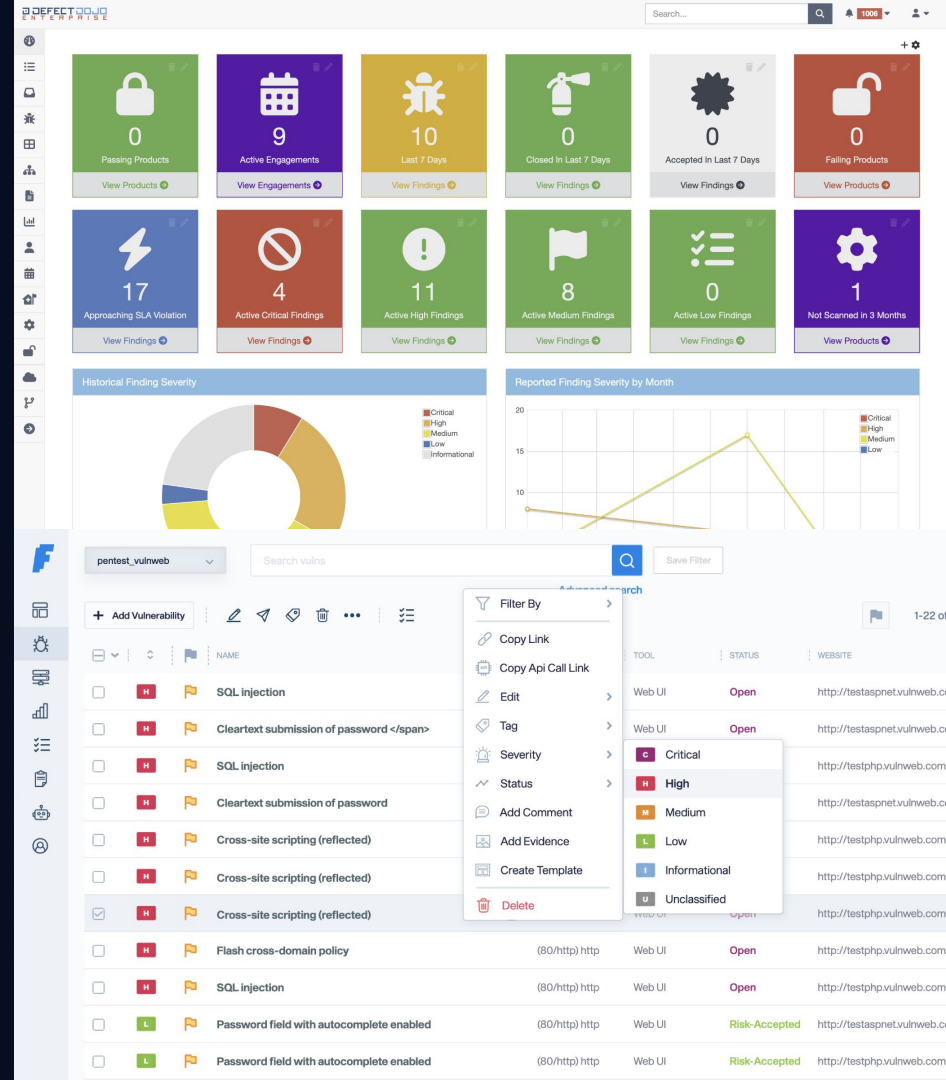
- We need own kind of entities
- We need own metrics and dashboards
- We need custom integrations (scanners)
- Writing integrations is a pain

## 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

The screenshot displays the ENSO security dashboard with the following components:

- Connectors:** A grid of security tool connectors including AppSpider DAST, Checkmarx, Dep Scan SCA, Semgrep, Qualys DAST, Snyk SCA, and Trivy IaC.
- Web Assets:** A table listing discovered assets with columns for Open Tasks, Defects, Tags, Controls, Risk, Class, and Assignee.
- Dashboard Overview:** A central area with widgets for Security Score (1.29), Champion Leader Board, Control Coverage (radar chart), Defects Trend (line chart), and Team performance metrics.
- Workflow Editor:** A foreground window titled "SAST weekly scheduled scan" showing a flowchart with filters, a "Run Scan" step, an "OR" decision diamond, and a "Send Slack Message" step.

# Inventory of any kind of Assets

Asset (2112)	Open Tasks	Defects	Tags	Controls	Risk	Class	Assignee
>  https://jaeger-collector.enso.am 23 Items	798	<span>12</span> <span>43</span> <span>8</span> <span>4</span>	XSS +2		<span>2,545</span>	<span>A</span>	
>  https://_4cce49f60cb4c235 12 Items	647	<span>3</span> <span>102</span>	Dev Prod +2		<span>5,421</span>	<span>B</span>	
>  /enso-emails/static_file 67 Items	154	<span>56</span> <span>43</span> <span>8</span>	Prod		<span>103</span>	<span>C</span>	
https://oapi.enso.io 102 Items	357	<span>102</span>	API Member +1		<span>23</span>	<span>D</span>	
/sfx/track/number/electronic 3 Items	177	<span>82</span> <span>4</span> <span>4</span>	Dev Prod +3		<span>2,112</span>	<span>D</span>	
>  https://desk1.enso.io 11 Items	556	<span>10</span> <span>8</span> <span>4</span>	Account API +3		<span>106</span>	<span>A</span>	
>  Enso.TTD 23 Items	24	<span>12</span> <span>8</span>	Dev Prod +2		<span>24</span>	<span>C</span>	
>  ALTerraform 55 Items	540	<span>42</span> <span>8</span>	Dev Seller +1		<span>504</span>	<span>C</span>	
>  https://studio.enso-records.io 21 Items	583	<span>12</span> <span>4</span>	Dev Product +3		<span>1,011</span>	<span>A</span>	
>  account.sample-client12.com 900 Items	142	<span>12</span> <span>43</span> <span>8</span> <span>4</span>	Dev Product +3		<span>88,888</span>	<span>A</span>	
https://oapi.enso.io 102 Items	357	<span>102</span>	Dev Product +3		<span>23</span>	<span>D</span>	

Values

Observe whole system

Tagging assets by criticality

See total risks

# Vulns for each kind of asset

The screenshot displays the ENSO web assets interface. On the left, a sidebar contains navigation options: Dashboard, Inventory, Defects, Tasks, Policy, and Connectors. The main area is titled 'Web Assets' and shows a search bar and a list of assets. One asset, 'https://jaeger-collector.artlist.m/', is selected, and a detailed view of its vulnerabilities is shown in a modal window.

The modal window for 'https://jaeger-collector.artlist.m/' shows the following details:

- Discovered: 02/11/2021, Last scan: 28/11/2021
- Score: [empty]
- Defects: [empty]
- Tasks: [empty]
- Events: [empty]
- Attributes: [empty]

The table below lists the vulnerabilities found for this asset:

Defect	Asset	Source	Status	Ticket	Severity	Created
> Generic Secret det...	https://desk.artlist.io		IN PROGRESS	+ Add Ticket	HIGH	Dec 30, 2019
> Log4j2 RCE throu...	https://jaeger-collect...		OPEN	TSV-2001	LOW	Dec 30, 2019
> Azure takeover de...	https://_4cce49f6079...		FIXED	+ Add Ticket	MEDIUM	Dec 4, 2019
> Appspec Yml Disc...	https://oapi.artgrid.io		DISMISSED	TSV-2112	MEDIUM	Mar 20, 2019
> WordPress Core ...	https://em4038.artgri...		IN PROGRESS	TSV-1010	CRITICAL	Feb 2, 2019
> Generic API Key de...	https://_4cce49f6079...		CLOSED	TSV-1001	MEDIUM	Mar 20, 2019
> OAuth token detec...	https://em4038.artgri...		DISMISSED	+ Add Ticket	HIGH	Dec 7, 2019
> Insecure direct obj...	https://studio.art-list.io		OPEN	+ Add Ticket	MEDIUM	Feb 2, 2019

Values

Results of each scan

Details of vulnerabilities

Easy access to any asset

# Automate through workflows

**Rules**

Search

Active First New Rule

- CI Automation - SCA scans for new PRs on Class A repositories** (Asset)
- SAST weekly scheduled scan** (Asset)
- Weekly per-team auto assignment of top impact tasks** (Tasks)
- PT scoping and auto-assignment for a 2-week sprint** (Asset)
- Generate weekly email report on SCA Critical defects with SLA violation** (Defect)
- "New Asset" Slack notification and security review task assignment** (Asset)

## Values

No-code automation

- run scans
- change stats

Event triggers

**SAST weekly scheduled scan**

Asset

Filter → Run Scan

Filter → OR → Send Slack Message

Filter

Filter

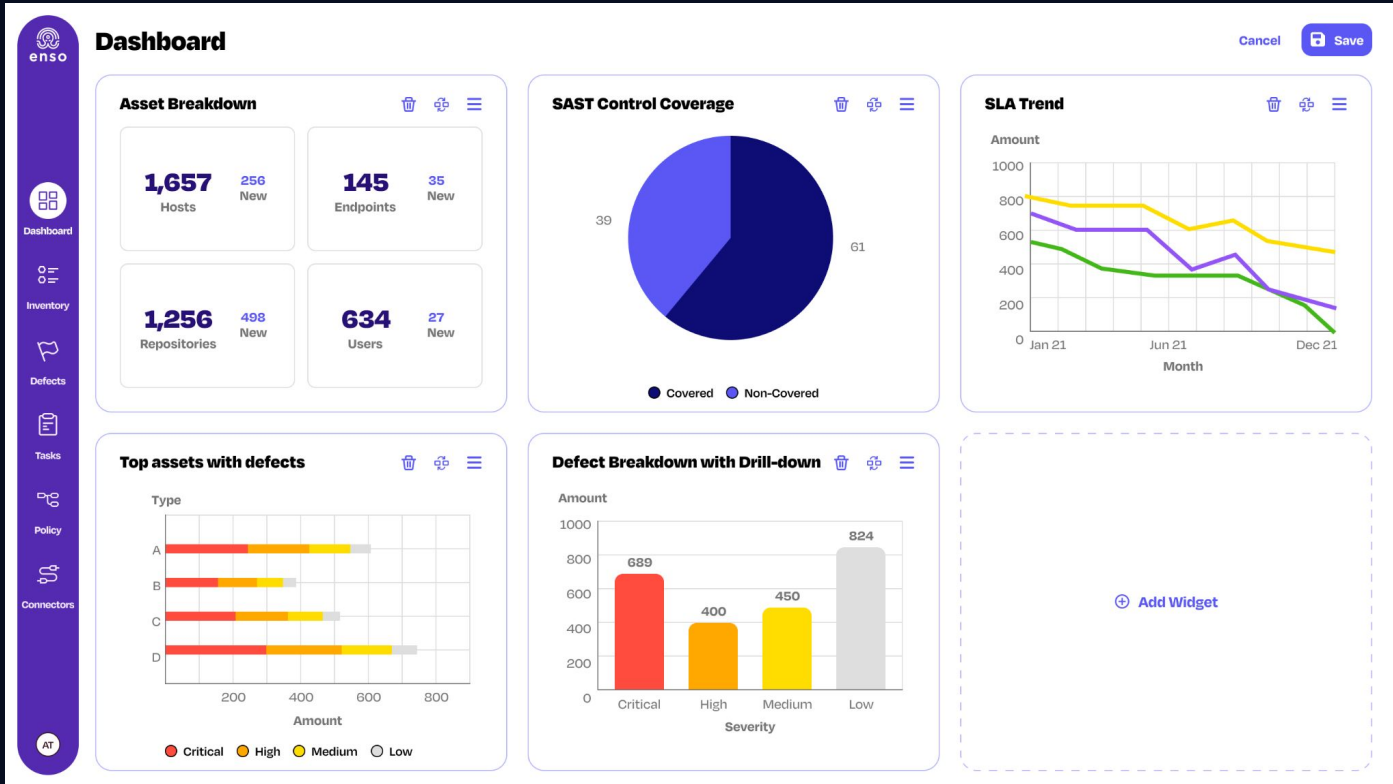
Filter

Simulate Run Edit

Last Modified: Apr 24, 2022 2:31 AM Modified by: james@ensosecurity Created: May 6, 2022 9:31 PM Created by: james@ensosecurity



# Nice CUSTOM Dashboards!



## Values

Metrics for

- 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

Monospace

Content Customers 1-100 of 17,048

	First Name	Last Name	Visits	Date Created
	Keri	Guzman	636	just now
	Heather	Robles	426	
	Ollie	Padilla	24	
	Marina	Numbers	87	
	Enrique	Numbers	7,432	
	Leonor	Prefix	158	
	Dorothy	Suffix	254	

Articles

Customers

Languages

Locations

Mailing List

Metrics

Services

Support Tickets

My Draft Articles

Welcome 🙌

We hope you are making good progress on your project! Feel free to read the latest news about Strapi. We are giving our best to improve the product based on your feedback.

[SEE MORE ON THE BLOG](#)

**Content-type Builder**

**Read the documentation**  
Discover the concepts, reference, guides and tutorials.

**Code example**  
Learn by testing real project developed by the community

**Tutorial**  
Discover the concepts, reference, guides and tutorials.

**Blog**  
Discover the concepts, reference, guides and tutorials.

**Join the community**  
Discuss with team members, contributors and developers on different channels.

[SEE OUR ROAD MAP](#)

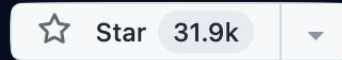
[GitHub](#) [Discord](#)

[Reddit](#) [Twitter](#)

[Blog](#) [Forum](#)

?

# No-code Headless CMS



[github.com/strapi/strapi](https://github.com/strapi/strapi)

[github.com/budibase/budibase](https://github.com/budibase/budibase)

[github.com/appsmithorg/appsmith](https://github.com/appsmithorg/appsmith)

[github.com/directus/directus](https://github.com/directus/directus)

# ASPM based on Headless CMS

The image displays the ASPM (Application Security Platform) interface, specifically the Data Model configuration section. The interface is divided into several panels:

- Left Sidebar:** Contains navigation icons and menu items: ASPM, Data Model, Access Control, Flows, Settings, Appearance, Bookmarks, Translations, Marketplace (Beta), Extensions, Report Bug, Request Feature, and Directus 10.11.0.
- Main Panel (Data Model):** Shows a list of collections under the heading "Data Model". The collections listed are: repository, defect, web\_assets, containers, commits, developer, and scans. Below this list is a section for "System Collections".
- Modal (Repos):** A modal window titled "Repos" is open, showing a list of fields and their types for the "repository" collection. The fields listed are: id\* (string), url (string), name\_with\_namespace (string), tags (array), date\_created (datetime), archived (boolean), reviewed (boolean), commits (array), scans (array), and defects (array).
- Configuration Panel (Defects (repository)):** A configuration panel for the "Defects (repository)" collection. It includes:
  - This Collection:** A list of fields: repository, url.
  - Related Collection:** A list of related collections: defect, repository.
  - Sort Field:** A section for defining sort fields, with a button "Add Sort Field...".
  - Relational Triggers:** A section for defining triggers, including "On Deselect of defect..." and "On Delete of repository...", both with a dropdown menu set to "Nullify the repository field".

# Customizable assets

The screenshot shows a web application security tool interface. On the left is a navigation sidebar with categories like Repository, Defect, Web Assets, Containers, Commits, Developer, and Scans. The main area displays a table of SAST vulnerabilities under the 'SAST Vuln' filter. The table has columns for Source, Severity, Status, and Summary. The first four items are marked as 'moderate' severity and 'open' status, while the remaining items are marked as 'info' severity and 'open' status. A search bar and a '+2' button are visible at the top right of the table area.

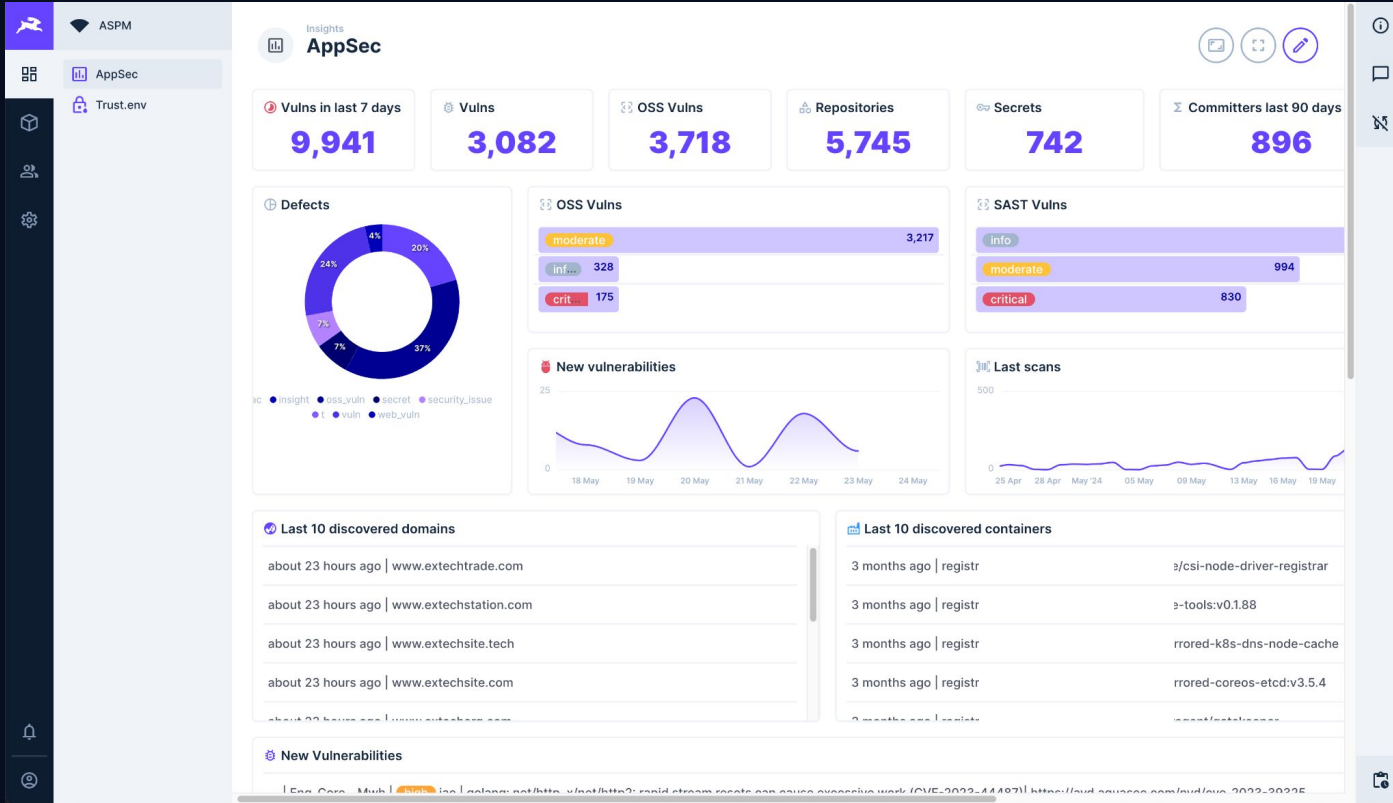
Source	Severity	Status	Summary
shiftleft	moderate	open	vuln Weak Hash: Usage of Weak Cryptographic Hash Function in `CacheHandler...
shiftleft	moderate	open	vuln Weak Hash: Usage of Weak Cryptographic Hash Function in `create_mock_v...
shiftleft	moderate	open	vuln Invalid Certificate Validation: Certificate Validation is Disabled in `newDB`
shiftleft	moderate	open	vuln Invalid Certificate Validation: Certificate Validation is Disabled in `getJWTPa...
shiftleft	info	open	vuln Log Forging: Attacker-controlled Data is Written Directly to Log via `r` in `Ag...
shiftleft	info	open	vuln Log Forging: Attacker-controlled Data is Written Directly to Log via `param1...
shiftleft	info	open	vuln Log Forging: Attacker-controlled Data is Written Directly to Log via `r` in `Ag...
shiftleft	info	open	vuln Log Forging: Attacker-controlled Data is Written Directly to Log via `param1...
shiftleft	info	open	vuln Log Forging: Attacker-controlled Data is Written Directly to Log via `r` in `Ag...
shiftleft	info	open	vuln Log Forging: Attacker-controlled Data is Written Directly to Log via `param1...
shiftleft	info	open	vuln Log Forging: Attacker-controlled Data is Written Directly to Log via `r` in `Ag...
shiftleft	info	open	vuln Log Forging: Attacker-controlled Data is Written Directly to Log via `param1...
shiftleft	info	open	vuln Log Forging: Attacker-controlled Data is Written Directly to Log via `r` in `Ag...
shiftleft	info	open	vuln Log Forging: Attacker-controlled Data is Written Directly to Log via `param1...

Views and bookmarks

Filters

Batch update

# Dashboards – yes, they are custom!



Drag'n'Drop widgets

Aggregations

Filters

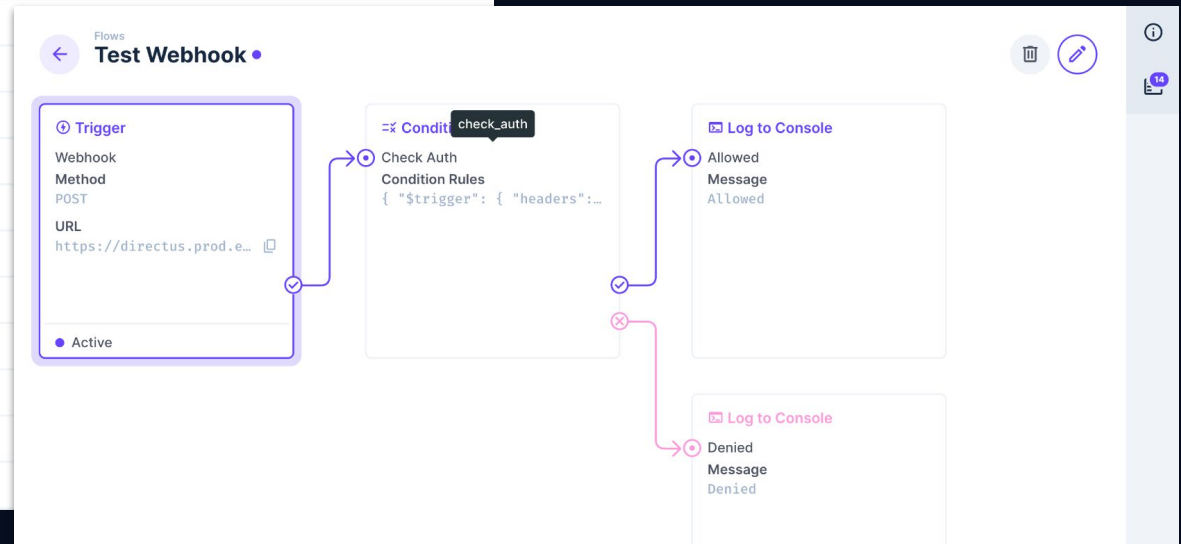
# Workflows

Status	Name	Description
Active	CRON - Aggregate Develop...	
Active	CRON - Containers Loader	Loads list of deployed containers through Sp...
Active	CRON - Gitlab Loader	Loads Gitlab repos by cron
Active	CRON - Shiftleft Loader	Loads ShiftLeft scan results
Active	CRON - Webassets	
Active	Manual - Container Loader	
Active	Manual - Gitlab Loader	
Active	Manual - Shiftleft Loader	
Active	Manual - Webassets	
Active	Update - Shiftleft hook	
Active	Webhook - Gitleaks	
Active	Webhook - Nuclei	
Active	Webhook - Trivy	
Active	Webhook - Trufflehog	
Active	Webhook-trufflehog2	

CRON and Webhooks

Drag'n'drop flows

Custom JS extensions



# Extensions

Settings

## Extensions

### Bundles

directus-extension-asmp-bundle 0.0.18	Enabled	⋮
web-assets-loader	Enabled	⋮
table-selector	Enabled	⋮
display-multiline	Enabled	⋮
defect-writer	Enabled	⋮
gitlab-loader	Enabled	⋮
splunk-loader	Enabled	⋮
shiftright-loader	Enabled	⋮
repository-url-to-name	Enabled	⋮
repository-display	Enabled	⋮
ai-release-summary-loader	Enabled	⋮

- src
  - ai-release-summary-loader
  - defect-writer
  - display-multiline
  - example-loader-template
  - flow-scripts
  - gitlab-loader
    - api.ts
    - app.ts
    - gitlab-client.ts
    - models.ts
  - nuclei-loader
  - repository-display
  - repository-url-to-name
  - shiftright-loader
  - splunk-loader
  - table-selector
  - web-assets-loader

# Even Custom styles

## Using Built-in styles

```
Custom CSS
1 .metric-bar {
2   min-width: 20%;
3 }
4 .v-list-item-content .render-template {
5   white-space: pre-wrap!important;
6 }
7 .links .v-list-item-content {
8   height: initial!important;
9 }
10 .v-list-item-content .datetime {
11   color: var(--theme--primary);
12 }
```

## Writing custom component

```
<template>
  <div class="text-multiline" v-html="formattedValue"></div>
</template>

<script>
1+ usages   ▸ Ivan Elkin *
export default {

  props: {
    value: {
      type: String,
      default: null,
    },
  },
  computed: {
    formattedValue() {
      return this.value.replace(
        searchValue: /([A-Z]+-d+)/g,
        replaceValue: '<a href="https://jira.exness.io/browse/$1" target="_blank">$1</a>'
      );
    }
  }
};
</script>
```

```
display-multiline
└─ display.vue
   index.ts
   shims.d.ts
```



# Profit comparison

	Self developed	Open Source	Vendor	Headless CMS
Time to first start	Very Slow	<b>Fast</b>	Fast / Slow	Medium
Customization	<b>100%</b>	50%	Very Low ?	<b>80%</b>
Customization speed	Slow	Slow	Medium ?	<b>Very Fast</b>
Support	Slow	Very Slow	<b>Very Fast</b>	Fast
Integrations	<b>Any</b>	Any but Limited	Limited	<b>Any</b>

\* 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

 CrowdStrike  
<https://www.crowdstrike.com> > cloud-security > applicati...

## What is Application Security Posture Management (ASPM)?

**ASPM** is the holistic process of evaluating, managing, and enhancing the security stance of an organization's custom applications.

 Gartner  
<https://www.gartner.com> > reviews > market > applicati...

## Application Security Posture Management (ASPM) Tools

**Application security posture management (ASPM)** tools continuously manage application risk through collection, analysis and prioritization of security issues ...

 ArmorCode  
<https://www.armorcode.com> > learning-center > what-is...

## What is Application Security Posture Management (ASPM)?

**ASPM** unifies testing, ticketing, CI/CD, and other development tools to create holistic visibility into the security posture of applications, prioritize findings ...

 Synopsys  
<https://www.synopsys.com> > glossary > what-is-applicati...

## Application Security Posture Management

**Application security posture management (ASPM)** is a holistic approach to application security (AppSec) that provides a single source of truth to identify, ...

 Check Point Software  
<https://www.checkpoint.com> > Secure The Cloud

## What is Application Security Posture Management (ASPM)?

Application security posture management (**ASPM**) helps to scale and enhance AppSec programs through automation. **ASPM** solutions automatically identify applications ...

 Cycode  
<https://cycode.com> > blog > application-security-posture-...

## What Is Application Security Posture Management (ASPM)?

2 Nov 2023 — **Application Security Posture Management (ASPM)** detects, correlates, prioritizes, and remediates security vulnerabilities across the SDLC.

# 1. What we achieved in General

1. Asset discovery and inventory

2. Risk assessment

3. Scanners Orchestration

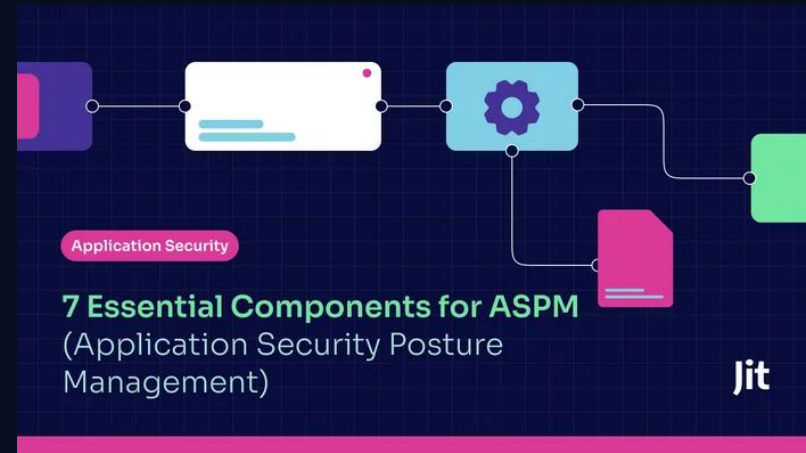
4. Reports and Dashboards

5. Real-time monitoring

6. No-Code Automation

7. Compliance Monitoring

8. It's not just a security tool



Category	ASPM	Traditional AppSec	ASOC	CSPM
Purpose	Manage and scale an AppSec program based on business risk	Secure applications against vulnerabilities	Orchestrate and correlate security activities	Manage and monitor the security of cloud environments
Benefits	Provides holistic visibility into the app environment to enable effective risk management and remediation	Enhances app security against threats	Streamlines security operations and responses	Identifies and mitigates cloud security risks
Integrations	On-premises and cloud-based environments	Embedded in app development lifecycle	Organization-wide deployment	Cloud infrastructure and services

# 2. De-duplication is not a feature

Project: RiskAssessment Labels: InternetFacing

Dashboard Scans Imports Vulnerabilities ASVS Files Images SBOM Settings

AppSec AppSec Duplicates Vulnerabilities are already de-duplicated so that you can start to triage!  
← 18/42 next

Change View:

Total: 721 Quick Filters Search Vuln Name Per Page: 15 Actions

<input type="checkbox"/>	Issue	ID	Vulnerability Name	Branch	Status	Scanner	Severity	CVSS	First Seen	
<input type="checkbox"/>		eec3e	<a href="#">Blocklisted import crypto/md5: weak cryptographic primitive</a>	master	Recurrent		High	8.0	17 May 2023	
<input type="checkbox"/>		778fa	Blocklisted import crypto/md5: weak cryptographic primitive	master	Recurrent		Medium	6.0	17 May 2023	
<input type="checkbox"/>		eec3c	Use of weak cryptographic primitive	master	Recurrent		Critical	10.0	17 May 2023	
<input type="checkbox"/>		778f8	Blocklisted import crypto/md5: weak cryptographic primitive	master	Recurrent		Medium	6.0	17 May 2023	
<input type="checkbox"/>		4203d	Use of weak cryptographic primitive	master	Recurrent		Medium	6.0	17 May 2023	
<input type="checkbox"/>		ba664	GHSA-x4jg-mjrx-434g   node-forge:0.10.0	master	New		Low	3.0	16 May 2023	
<input type="checkbox"/>		ba662	CVE-2022-24771   node-forge:0.10.0	master	New		Critical	10.0	16 May 2023	
<input type="checkbox"/>		38393	CVE-2022-24773   node-forge:0.10.0	master	New		Low	3.0	16 May 2023	
<input type="checkbox"/>		38391	GHSA-cfm4-qjh2-4765   node-forge:0.10.0	master	New		High	7.5	16 May 2023	

## 2. De-duplication is not a feature

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

```
sha256(repo + filename + param + vuln_type) [0:31]
```

```
( "tfg_" + sha256(repo + filename + secret) ) [0:31]
```

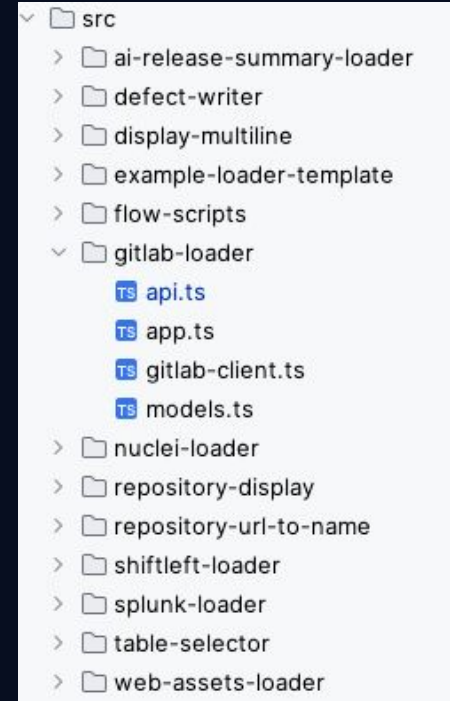
```
( "dast_" + sha256(domain + param + vuln_type) ) [0:31]
```

# 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

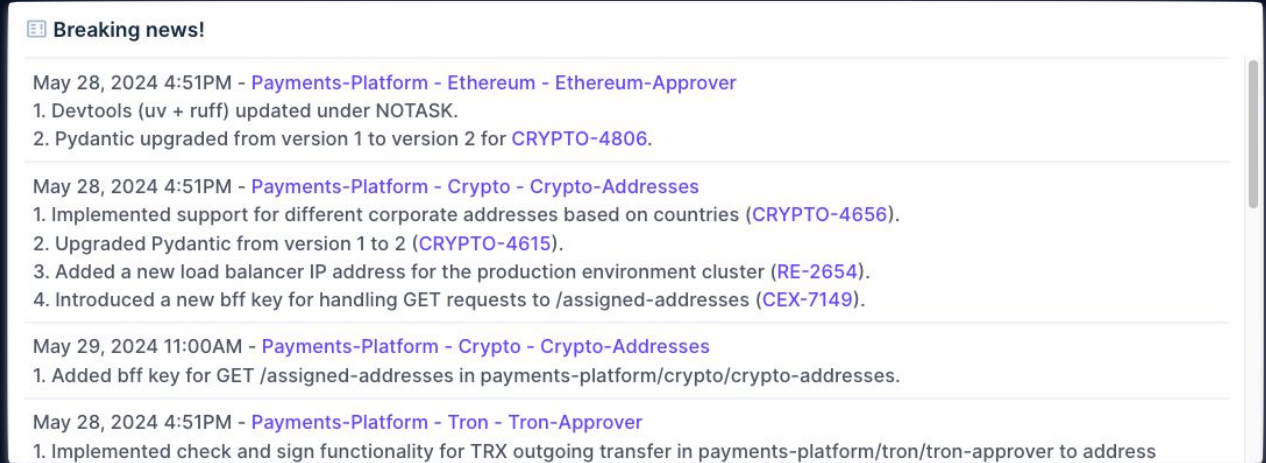


# 4. We have AI

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 :)



**Breaking news!**

May 28, 2024 4:51PM - [Payments-Platform - Ethereum - Ethereum-Approver](#)

1. Devtools (uv + ruff) updated under NOTASK.
2. Pydantic upgraded from version 1 to version 2 for [CRYPTO-4806](#).

May 28, 2024 4:51PM - [Payments-Platform - Crypto - Crypto-Addresses](#)

1. Implemented support for different corporate addresses based on countries ([CRYPTO-4656](#)).
2. Upgraded Pydantic from version 1 to 2 ([CRYPTO-4615](#)).
3. Added a new load balancer IP address for the production environment cluster ([RE-2654](#)).
4. Introduced a new bff key for handling GET requests to /assigned-addresses ([CEX-7149](#)).

May 29, 2024 11:00AM - [Payments-Platform - Crypto - Crypto-Addresses](#)

1. Added bff key for GET /assigned-addresses in payments-platform/crypto/crypto-addresses.

May 28, 2024 4:51PM - [Payments-Platform - Tron - Tron-Approver](#)

1. Implemented check and sign functionality for TRX outgoing transfer in payments-platform/tron/tron-approver to address



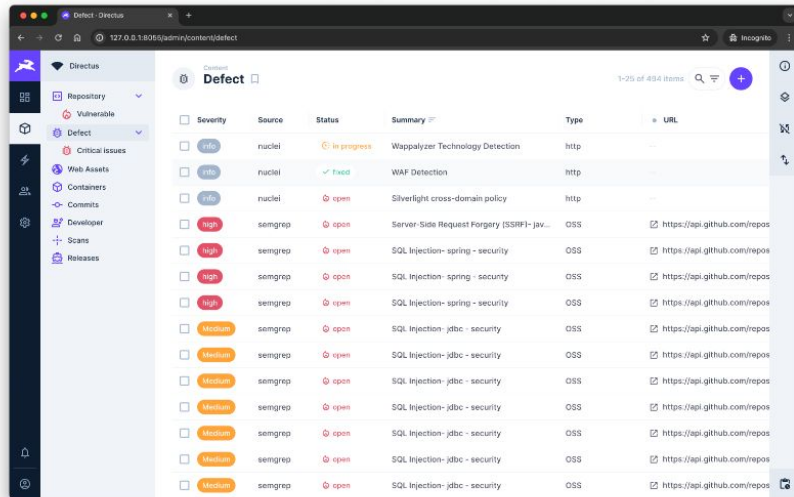
# 5. PoC for you

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

[github.com/vankyver/directus-aspm-poc](https://github.com/vankyver/directus-aspm-poc)



## Directus-ASPM-PoC



Proof of Concept for building Application Security Posture Management (ASPM) based on [Directus Headless-CMS](#).

### Running

```
docker-compose up
```

use following credentials to login to Directus:

```
email: admin@example.com  
password: d1r3ctu5
```

# 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

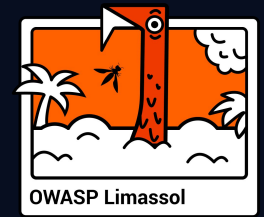


# P.P.S Remember!

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](mailto:ivan.elkin@exness.com)

@vankyver