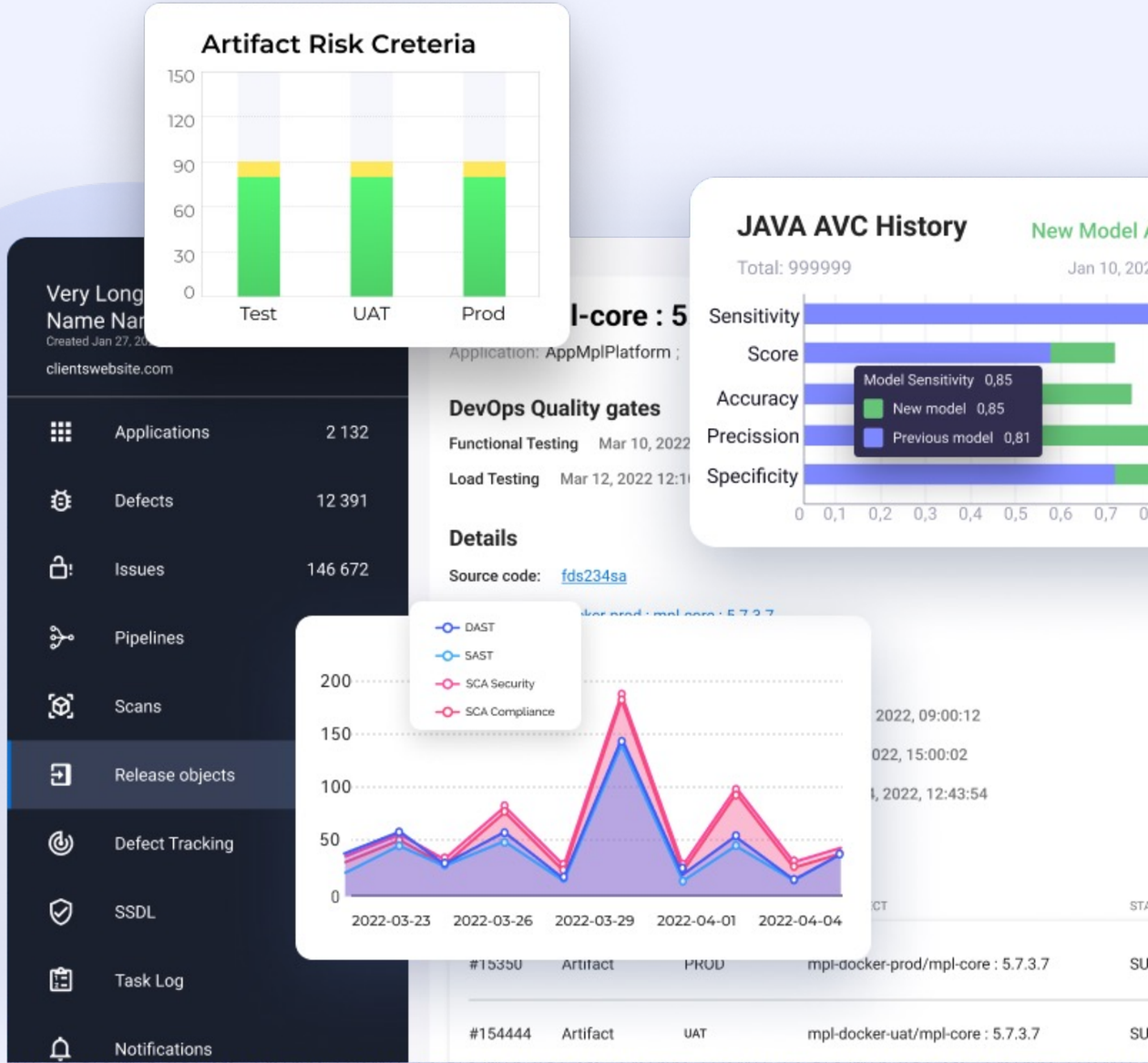
APPSECHUB

Чем грозит опоздание проверки защищенности и как это предотвратить



О себе

APPSECHUB

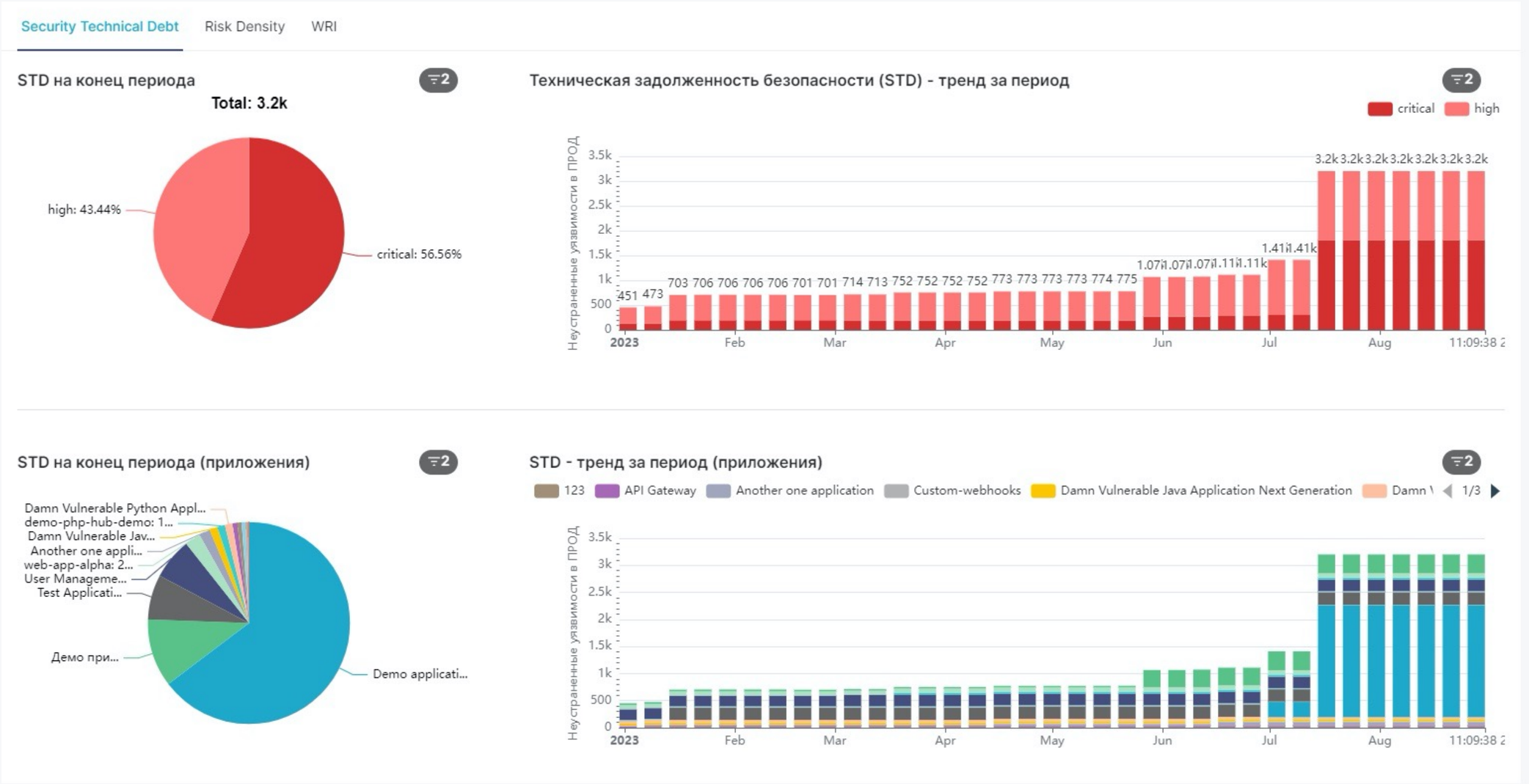
Антон Башарин

- 20 лет в ИТ
- От рядового разработчика до системного архитектора и руководителя команды разработки
- Luxoft, EPAM Systems, Boeing, СберБанк, Альфа-Банк
- СберТех: внедрение SSDL и практик ИБ
- С 2017 в Swordfish Security – разработчик, архитектор, владелец продукта AppSec.Hub

Последствия

Технический долг

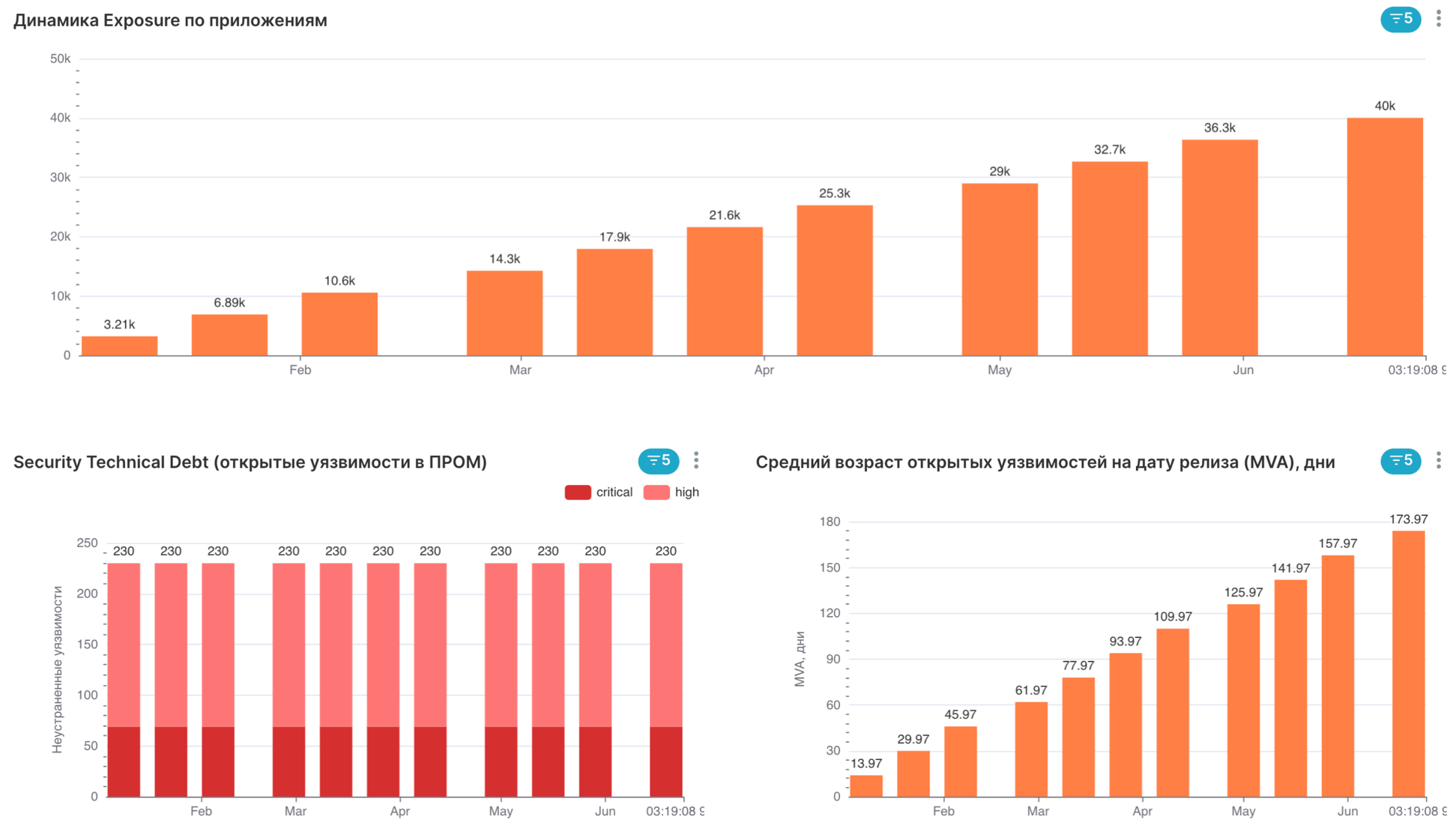
APPSECHUB



Только критичные (Critical, High)

Подверженность риску

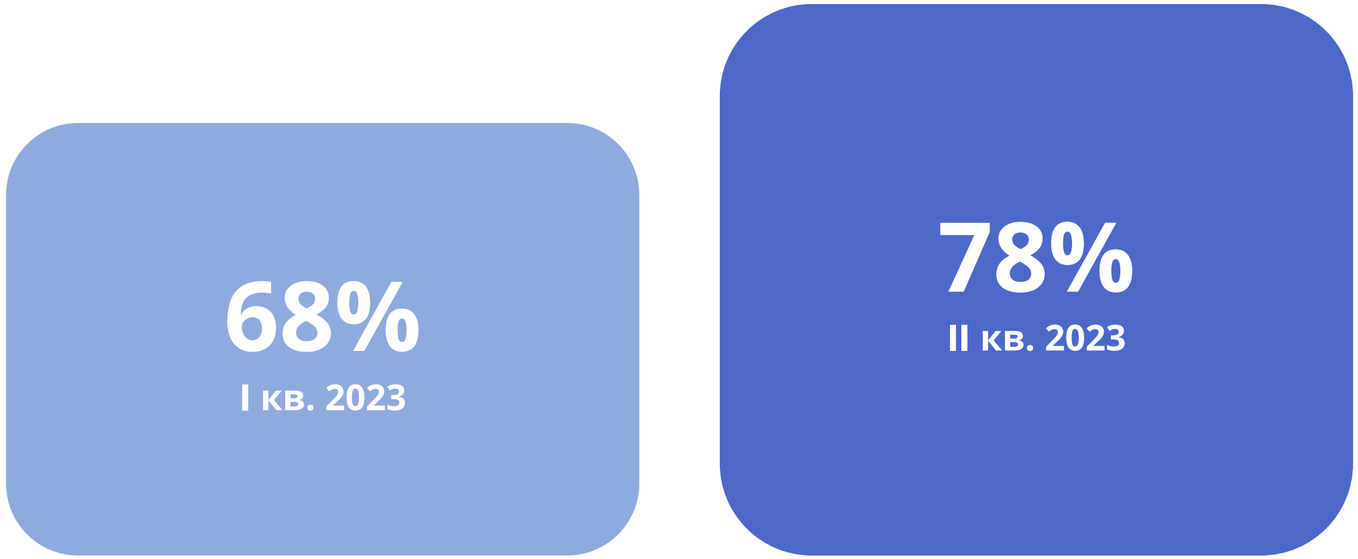
APPSECHUB



Только критичные (Critical, High)

Доля целевых атак

APPSECHUB



Согласно исследованию Positive Technologies: 1кв и 2кв 2023 года.

Причины

Причины

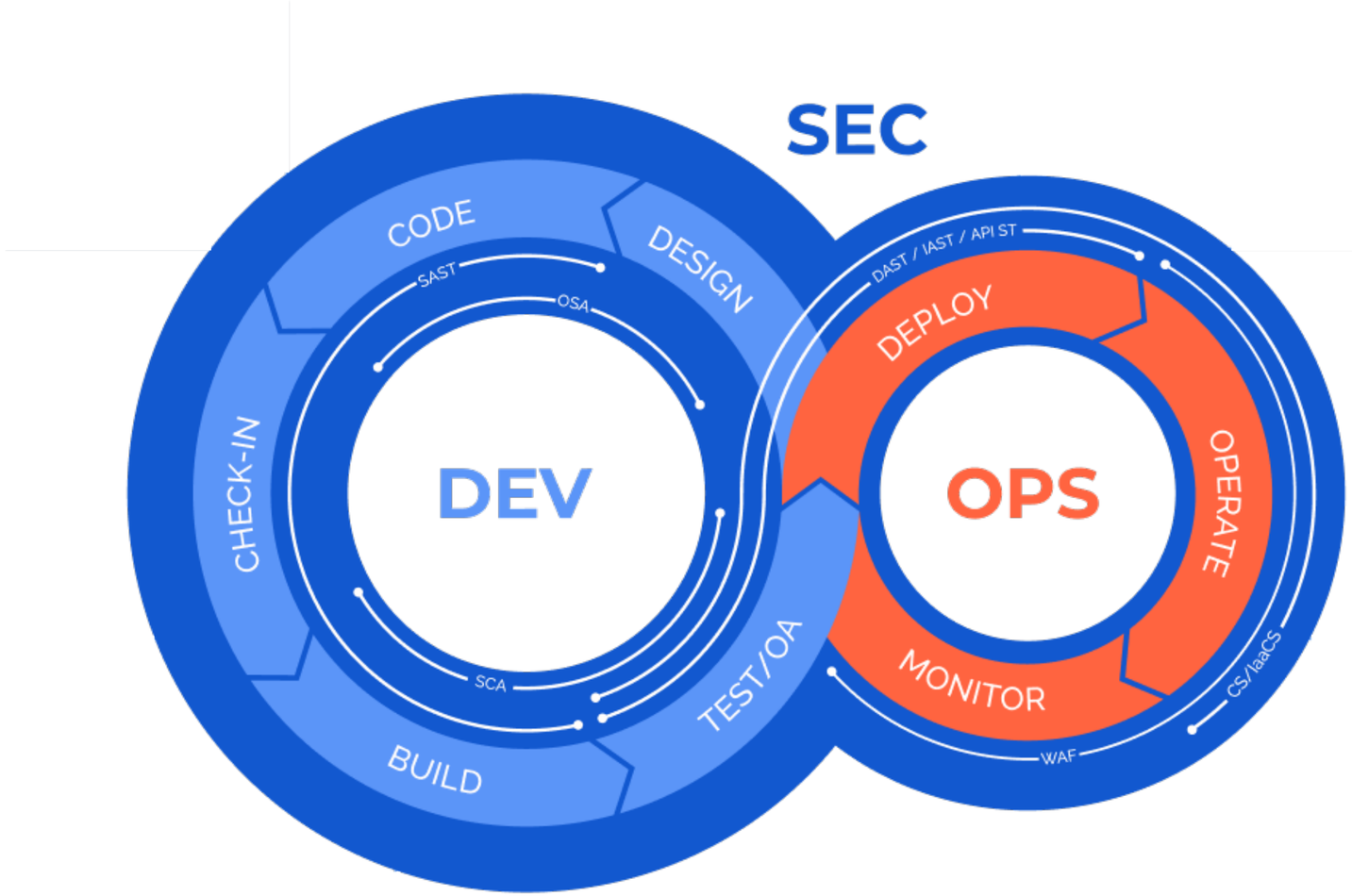
APPSECHUB

- Неправильная оценка приоритетов
- Нехватка ресурсов
- Отсутствие культуры и процессов

Как предотвратить?

DevSecOps – ключ к автоматизации

APPSECHUB



Контроль применения практик ИБ

APPSECHUB

Применение практик ИБ

SAST	SCA	DAST
15.7%	**15.2%**	**0.0%**

Раннее обнаружение и устранение

APPSECHUB

MTTD (дни)

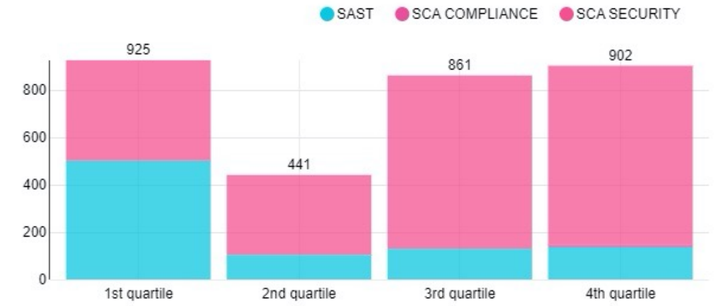
15.99

за выбранный период

Обнаруженные уязв-ти

Total: 3.13k

Стадия обнаружения уязвимостей (Практика ИБ)



MTT (дни)

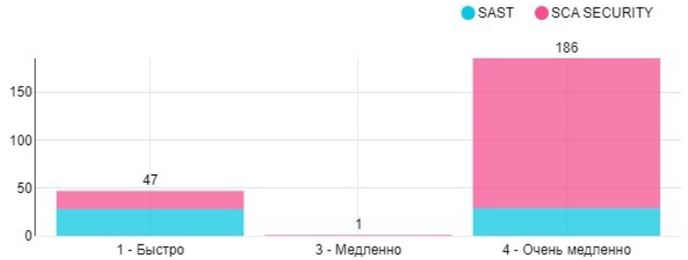
99.45

за выбранный период

Проанализированные уязв-ти

Total: 233

SLA триажа (практика ИБ)



MTTR (дни)

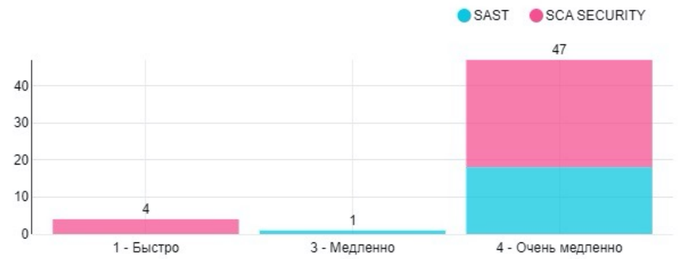
56.30

за выбранный период

Устраненные уязв-ти

Total: 52

SLA устранения (практика ИБ)



Только критичные (Critical, High)

Авто-ревью и корреляция

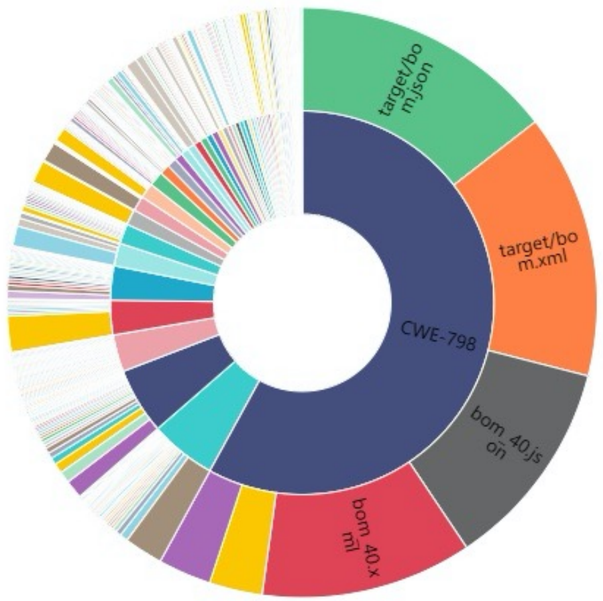
APPSECHUB

Модель корреляции на примере

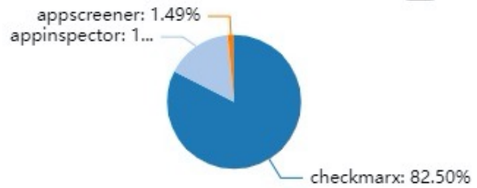
APPSECHUB

Total issues	Unique groups	Issues w/o groups	Average issues in group
5429	438	585	12.48

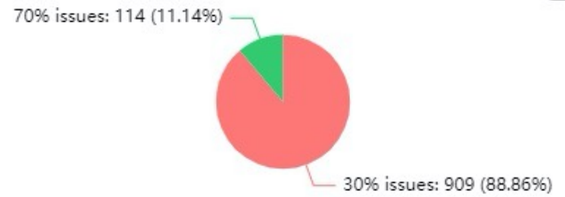
Correlation groups



Issues by tools



Groups with 70% issues



Groups

group_id	group_cwe_id	group_cwe_name	group_filename	issues in group
1371	798	Use of Hard-coded Credentials	target/bom.xml	603
1370	798	Use of Hard-coded Credentials	target/bom.json	603
1368	798	Use of Hard-coded Credentials	bom_40.json	482
1369	798	Use of Hard-coded Credentials	bom_40.xml	482
1367	798	Use of Hard-coded Credentials	bom_38.xml	121
1366	798	Use of Hard-coded Credentials	bom_38.json	121

Модель автоматической обработки

APPSECHUB

6 %
Критичных - SAST

51 %
Критичных - SCA

51 %
Авто-ревью

18 %
Корреляция - SAST

31 %
Корреляция - SCA

82 %
SAST

69 %
SCA

На сегодня всё!

Антон Башарин

anton@swordfishsecurity.ru

@nirahsab

https://appsec-hub.ru