



**АСТРА**

# **Автоматизация процессов анализа безопасности операционной системы Astra Linux**

**Виктория Егорова**

заместитель директора

Департамента анализа безопасности,

Группа Астра



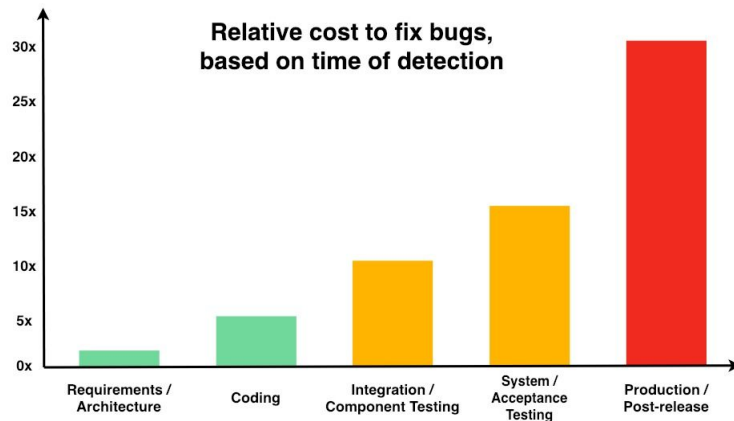
# Agenda

- Актуальность
- Фаззинг ядра
- Фаззинг компонентов пространства пользователя
- Статический анализ
- Хранение и обработка результатов
- Дальнейшие планы



# Актуальность

- Репозиторий main – более 4500 пакетов
- Из них более 120 относятся к пакетам, реализующим функции безопасности
- Анализируем не только СЗИ, но и opensource-пакеты



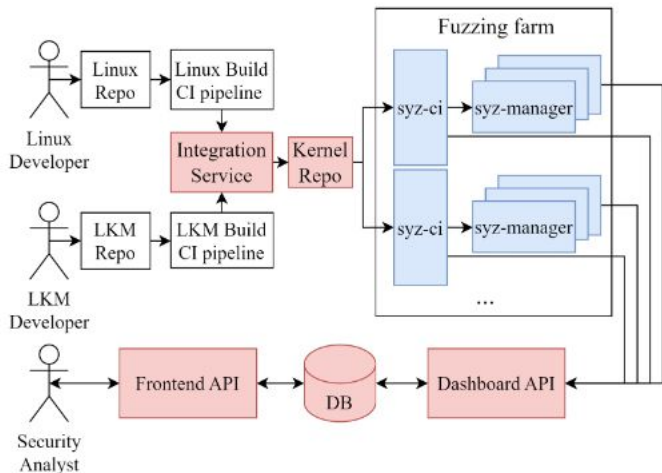


# Автоматизация фаззинга ядра (syz-ci)

- Панель мониторинга
  - Активные настройки стендов фаззинга
  - Обнаруженные ошибки и данные для их воспроизведения
- Интеграция кода собственных модулей в ядро в автоматическом режиме
- Автоматизация и управление стендами в рамках одного веб-интерфейса



# Автоматизация фаззинга ядра (syz-ci)



1. Разработчик ПО вносит изменения в код ядра или модуля в системе контроля версий
2. Запускаются задания сборки в CI
3. В случае успеха в Службу Интеграции отправляется уведомление
4. Служба Интеграции запускает процесс интеграции двух репозиторий в третий – репозиторий фаззинга
5. Syz-ci забирает изменения и запускает сборку ядра для фаззинга
6. Результаты сборки, обнаруженные ошибки, отчеты о покрытии отправляются в API панели управления
7. Аналитик просматривает все результаты с помощью графического интерфейса платформы



# Автоматизация фаззинга ядра (syz-ci)

## Список серверов

Name	Status	LastActivity	UpTime	Corpus	Coverage	BuildStatus
ci-astra-prod-1_8-6_1-kasan-mini-01	Running	17 Jun 2024, 13:25	14 hours	33052	303920	Success
ci-astra-test-1_7-6_1-kasan-mini-01	Running	17 Jun 2024, 13:25	14 hours	31879	296454	Success
ci-astra-test-1_8-6_1-kasan-mini-01	Running	17 Jun 2024, 13:25	14 hours	37066	309657	Success
ci-astra-prod-1_7-6_1-kasan-mini-01	Running	17 Jun 2024, 13:25	14 hours	29628	296547	Success

## ci-astra-prod-1\_8-6\_1-kasan-mini-01

MANAGER'S PAGE

KERNEL DETAILS

SYZKALLER REPO











CHECK COVERAGE

DOWNLOAD CORPUS

CurrentBuild	9063cac867cfc188aca4d34a03f7fef19f898517
LastAlive	17 Jun 2024, 13:25
BuildStatus	Success
Corpus	33052
Coverage	303920
CrashTypes	17
Crashes	218
Execs	1150349
UpTime	14 hours
FuzzingTime	3 days

## Tasks

НОВЫЙ ШАБЛОН ЗАДАЧИ

Title	Test Stand			Prod Stand			Upstream		Status	Last check	Actions				
	Linux	+	LAM	=	Kernel	Linux	+	LAM				=	Kernel	Linux	LAM
1.8-6.1	8B26F9 Up-to-date		2B3D3E Up-to-date		20F0BC	8B26F9 Up-to-date		2B3D3E Up-to-date		20F0BC	8B26F9 Up-to-date	2B3D3E Up-to-date	checked commits	17 Jun 2024, 05:00	    
1.7-6.1	8B26F9 Up-to-date		EC136B Up-to-date		F338AF	8B26F9 Up-to-date		EC136B Up-to-date		F338AF	8B26F9 Up-to-date	EC136B Up-to-date	checked commits	17 Jun 2024, 05:00	    

# Автоматизация фаззинга ядра (syz-ci)



## Bugs

Title	Count	ReproLevel	Report	First	Last	Managers
<a href="#">SYZFATAL: executor NUM failed NUM times: executor NUM: exit status NUM</a>	1053	<a href="#">ReproSyz</a>	<a href="#">Есть</a>	<a href="#">12 May 2024, 18:12</a>	<a href="#">17 Jun 2024, 13:58</a>	<a href="#">ci-astra-test-1_8-6_1-kasan-mini-01</a> <a href="#">ci-astra-prod-1_8-6_1-kasan-mini-01</a> <a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a> ...
<a href="#">BUG: sleeping function called from invalid context in psc_audit_check</a>	734	<a href="#">ReproOC</a>	<a href="#">Есть</a>	<a href="#">12 May 2024, 17:55</a>	<a href="#">20 May 2024, 20:09</a>	<a href="#">ci-astra-prod-1_7-6_1-kasan-mini-01</a> <a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a> ... <a href="#">ci-astra-test-1_8-6_1-kasan-mini-01</a> <a href="#">ci-astra-prod-1_8-6_1-kasan-mini-01</a> <a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a> ...
<a href="#">corrupted report_INFO: rcu detected stall in corrupted</a>	601	<a href="#">ReproSyz</a>	<a href="#">Есть</a>	<a href="#">12 May 2024, 17:51</a>	<a href="#">17 Jun 2024, 13:57</a>	<a href="#">ci-astra-test-1_8-6_1-kasan-mini-01</a> <a href="#">ci-astra-prod-1_8-6_1-kasan-mini-01</a> <a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a> ...
<a href="#">WARNING: chroot access!</a>	337	<a href="#">ReproOC</a>	<a href="#">Есть</a>	<a href="#">12 May 2024, 18:01</a>	<a href="#">17 Jun 2024, 13:29</a>	<a href="#">ci-astra-test-1_8-6_1-kasan-mini-01</a> <a href="#">ci-astra-prod-1_8-6_1-kasan-mini-01</a> <a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a> ...
<a href="#">suppressed report_suppressed report</a>	314	<a href="#">None</a>	<a href="#">Есть</a>	<a href="#">12 May 2024, 21:55</a>	<a href="#">17 Jun 2024, 12:47</a>	<a href="#">ci-astra-test-1_8-6_1-kasan-mini-01</a> <a href="#">ci-astra-prod-1_8-6_1-kasan-mini-01</a> <a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a> ...

## BUG: sleeping function called from invalid context in psc\_audit\_check

Alternative titles: [ [BUG: sleeping function called from invalid context in psc\\_audit\\_check](#) ]

Первое срабатывание: May 12, 2024 5:53 PM

Последнее срабатывание: May 20, 2024 8:09 PM

Количество срабатываний: 734

Произошло на:  
1. [ci-astra-prod-1\\_7-6\\_1-kasan-mini-01](#)  
2. [ci-astra-test-1\\_7-6\\_1-kasan-mini-01](#)  
...

[Есть репорт](#)

[Есть ReproC](#)

[14 воспроизведений](#)

## Related Crashes

Title	Manager	SyzaKillerCommit	Time	Log	Report	ReproSyz	ReproC	VM info	KernelRepo	KernelConfig
<a href="#">BUG: sleeping function called from invalid context in psc_audit_check</a>	<a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a>	<a href="#">b7c3afa5b2</a>	<a href="#">20 May 2024, 20:02</a>	<a href="#">Подробнее</a>	<a href="#">Подробнее</a>	<a href="#">ReproSyz</a>	<a href="#">ReproC</a>	<a href="#">Подробнее</a>	<a href="#">347951648C</a>	<a href="#">Подробнее</a>
<a href="#">BUG: sleeping function called from invalid context in psc_audit_check</a>	<a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a>	<a href="#">b7c3afa5b2</a>	<a href="#">20 May 2024, 19:20</a>	<a href="#">Подробнее</a>	<a href="#">Подробнее</a>	<a href="#">ReproSyz</a>	<a href="#">ReproC</a>	<a href="#">Подробнее</a>	<a href="#">347951648C</a>	<a href="#">Подробнее</a>
<a href="#">BUG: sleeping function called from invalid context in psc_audit_check</a>	<a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a>	<a href="#">b7c3afa5b2</a>	<a href="#">20 May 2024, 10:53</a>	<a href="#">Подробнее</a>	<a href="#">Подробнее</a>	<a href="#">ReproSyz</a>		<a href="#">Подробнее</a>	<a href="#">347951648C</a>	<a href="#">Подробнее</a>
<a href="#">BUG: sleeping function called from invalid context in psc_audit_check</a>	<a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a>	<a href="#">b7c3afa5b2</a>	<a href="#">20 May 2024, 09:40</a>	<a href="#">Подробнее</a>	<a href="#">Подробнее</a>			<a href="#">Подробнее</a>	<a href="#">347951648C</a>	<a href="#">Подробнее</a>
<a href="#">BUG: sleeping function called from invalid context in psc_audit_check</a>	<a href="#">ci-astra-prod-1_7-6_1-kasan-mini-01</a>	<a href="#">b7c3afa5b2</a>	<a href="#">19 May 2024, 07:42</a>	<a href="#">Подробнее</a>	<a href="#">Подробнее</a>	<a href="#">ReproSyz</a>		<a href="#">Подробнее</a>	<a href="#">8FE2CF600D</a>	<a href="#">Подробнее</a>
<a href="#">BUG: sleeping function called from invalid context in psc_audit_check</a>	<a href="#">ci-astra-prod-1_7-6_1-kasan-mini-01</a>	<a href="#">b7c3afa5b2</a>	<a href="#">19 May 2024, 04:51</a>	<a href="#">Подробнее</a>	<a href="#">Подробнее</a>	<a href="#">ReproSyz</a>		<a href="#">Подробнее</a>	<a href="#">8FE2CF600D</a>	<a href="#">Подробнее</a>
<a href="#">BUG: sleeping function called from invalid context in psc_audit_check</a>	<a href="#">ci-astra-prod-1_7-6_1-kasan-mini-01</a>	<a href="#">b7c3afa5b2</a>	<a href="#">19 May 2024, 03:55</a>	<a href="#">Подробнее</a>	<a href="#">Подробнее</a>	<a href="#">ReproSyz</a>		<a href="#">Подробнее</a>	<a href="#">8FE2CF600D</a>	<a href="#">Подробнее</a>
<a href="#">BUG: sleeping function called from invalid context in psc_audit_check</a>	<a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a>	<a href="#">b7c3afa5b2</a>	<a href="#">18 May 2024, 17:31</a>	<a href="#">Подробнее</a>	<a href="#">Подробнее</a>	<a href="#">ReproSyz</a>		<a href="#">Подробнее</a>	<a href="#">347951648C</a>	<a href="#">Подробнее</a>
<a href="#">BUG: sleeping function called from invalid context in psc_audit_check</a>	<a href="#">ci-astra-test-1_7-6_1-kasan-mini-01</a>	<a href="#">b7c3afa5b2</a>	<a href="#">18 May 2024, 08:02</a>	<a href="#">Подробнее</a>	<a href="#">Подробнее</a>	<a href="#">ReproSyz</a>		<a href="#">Подробнее</a>	<a href="#">347951648C</a>	<a href="#">Подробнее</a>

Items per page

10

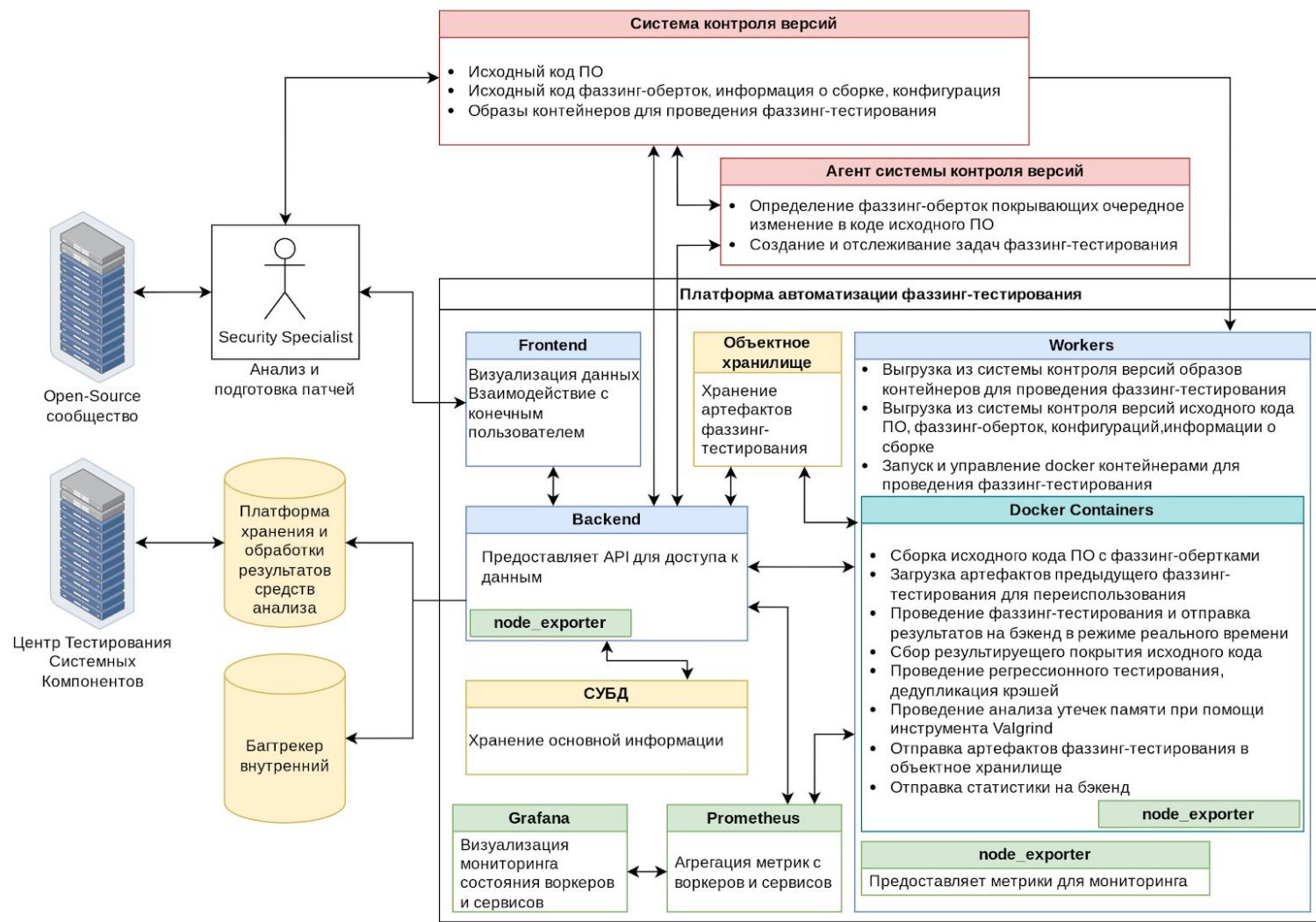
[<](#) [1](#) [2](#) [3](#) [4](#) [5](#) [...](#) [18](#) [>](#)



# Автоматизация фаззинга компонентов пространства пользователя

- Регрессионное тестирование по всем ранее обнаруженным ошибкам (вручную и автоматически)
- Определение набора целевых оберток для фаззинга изменений
- Гибкое конфигурирование проектов и параметров фаззинга
- Ручной запуск и запуск по триггерам в CI
- Графический интерфейс для отображения результатов и статистики текущего процесса фаззинга
- Сбор покрытия по одной обертке и по всем оберткам в проекте
- Удобное отслеживание воспроизводимости ошибки на разных версиях
- Масштабирование и умное динамическое распределение задач
- Взаимодействие с внутренней трекинг-системой и собственной платформой хранения и обработки результатов





## Добавить задание

Обязательные параметры:

Выберите ветку обертки

astra-1.8

Выберите Проект

libgost

Выберите ветку с исходными кодами

master

Выберите базовый Docker образ

sm-180-afl

Необязательные параметры:

Выберите утилиту

gost89

Выберите используемый фаззер

AFL

Выберите обертку таргета

gost89

Коммит исходных кодов

Коммит обертки

Выберите Сервер

Задайте время фаззинга (в секундах)

300

Задайте переменные окружения

[ОТМЕНА](#) [ДОБАВИТЬ](#)

## Информация по задаче 253

ID:	253
Задача создана:	14.05.2024 18:02:46
Задача завершена:	14.05.2024 18:52:17
Ветка обертки:	dev-astra-1.8
Проект:	attr
Утилита:	getfattr
Фаззер:	AFL
Обертка:	argv
Ветка исходного кода:	18
Коммит исходного кода:	99bd7054
Коммит обертки:	8adde284

```
american fuzzy loop +4.20c
/out/UBSAN/getfattr-harness
process timing                               overall results
run time : 0 hours, 5 minutes, 0 seconds      cycles done : 0
last new find : 0 hours, 0 minutes, 26 seconds corpus count : 192
last saved crash : 0 hours, 0 minutes, 0 seconds saved crashes : 0
last saved hang : 0 hours, 1 minutes, 42 seconds saved hangs : 5
stage progress                               findings in depth
total execs : 500437                          favored items : 18
exec speed : 1327.88/sec                       new edges on : 168
total crashes : 1
fuzzing strategy yields                      item geometry
var_byte_count : 0                            pending total : 182
havoc_expansion : 0                          stability : 100.00%
auto_dict_entries : 0                        bitmap_cvg : 23.30%
```

Покрыто строк:	59.7%
Покрыто функций:	88.2%
Покрыто ветвей:	47.8%
Docker image:	sm-180-afl
Статус:	DONE

- ПОКРЫТИЕ
- ПОКРЫТИЕ ВМЕСТЕ С ОБЕРТКОЙ
- АРХИВ С РЕЗУЛЬТАТАМИ ЗАДАЧИ
- ЛОГ ВЫПОЛНЕНИЯ ЗАДАЧИ
- ЛОГ КЛИЕНТА

Крэш: 0000000-attr-getfattr-AFL-argv-UBSAN

Крэш: 0000000-attr-getfattr-AFL-argv-UBSAN

ID крэша:	1	Воспроизвелся при последнем запуске:	true
Ветка обертки:	dev-astra-1.8	Exploitable CASR:	NOT_EXPLOITABLE
Проект:	attr	Exploitable User:	
Утилита:	getfattr	Коммит обертки при нахождении:	8adde284
Фаззер:	AFL	Коммит обертки при последней проверке:	8adde284
Обертка:	argv	Коммит исходников при нахождении:	99bd7054
Санитайзер:	UBSAN	Коммит исходников при последней проверке:	99bd7054
Крэш найден:	14.05.2024 18:52:12	Ссылка на VT:	
Информация обновлялась:	14.05.2024 18:52:12		

- ПОСМОТРЕТЬ ОТЧЕТ CASR
- СКАЧАТЬ ФАЙЛ С КРЭШЕМ



Selected columns

ID Создано Название

Санитайзер (+9 others)

Ветка обертки

Проект

Утилита

Фазаер

Обертка

ID	Создано	Название	Санитайзер	Проект	Утилита	Обертка	Трекер	Casr-репорт	Эксплуатируемо Casr	Обновлено	Вос
62	05.04.2024 00:24:18	0000004-pdp-ls-argv-UBSAN	UBSAN	parsec	pdp-ls	argv	<a href="#">BT-32320</a>	<a href="#">Casr-репорт</a>	NOT_EXPLOITABLE	24.04.2024 11:56:50	Di
61	04.04.2024 23:58:49	0000000-pdp-id-argv-LSAN	LSAN	parsec	pdp-id	argv	<a href="#">BT-32322</a>	<a href="#">Casr-репорт</a>	NOT_EXPLOITABLE	24.04.2024 11:57:13	Di
60	04.04.2024 18:33:39	0000000-lib-uttlis-hash-LSAN	LSAN	parsec	lib-uttlis	hash	<a href="#">BT-32341</a>	<a href="#">Casr-репорт</a>	NOT_EXPLOITABLE	24.04.2024 11:57:25	Di
59	04.04.2024 09:19:56	0000000-lib-pdp-mac_wcsetmacent-LSAN	LSAN	parsec	lib-pdp	mac_wcsetmacent	<a href="#">BT-33959</a>	<a href="#">Casr-репорт</a>	NOT_EXPLOITABLE	24.04.2024 11:57:31	Di
58	04.04.2024 08:59:08	0000000-lib-pdp-mac_wcsetcatent-LSAN	LSAN	parsec	lib-pdp	mac_wcsetcatent	<a href="#">BT-27120</a>	<a href="#">Casr-репорт</a>	NOT_EXPLOITABLE	24.04.2024 11:57:40	Di
57	03.04.2024 07:44:24	0000002-lib-aux-maux_settings_read-UBSAN	UBSAN	parsec	lib-aux	maux_settings_read	<a href="#">BT-32312</a>	<a href="#">Casr-репорт</a>	NOT_EXPLOITABLE	24.04.2024 12:43:52	Di
56	03.04.2024 03:23:25	0000000-lib-aux-maux_scnprintf-LSAN	LSAN	parsec	lib-aux	maux_scnprintf	<a href="#">BT-36140</a>	<a href="#">Casr-репорт</a>	NOT_EXPLOITABLE	24.04.2024 11:58:17	Di
55	03.04.2024 03:07:31	0000000-lib-aux-maux_hash-LSAN	LSAN	parsec	lib-aux	maux_hash	<a href="#">BT-36140</a>	<a href="#">Casr-репорт</a>	NOT_EXPLOITABLE	03.04.2024 03:07:31	Di

3	DONE	02.04.2024 12:28:13	05.04.2024 09:57:02	astra-1.8	parsec	smolensk-1.8-update	0e2cf818	28bc5749	sm-175-af1	18000	82.2%	68.1%	89.8%	<a href="#">get_coverage</a>
---	------	---------------------	---------------------	-----------	--------	---------------------	----------	----------	------------	-------	-------	-------	-------	------------------------------

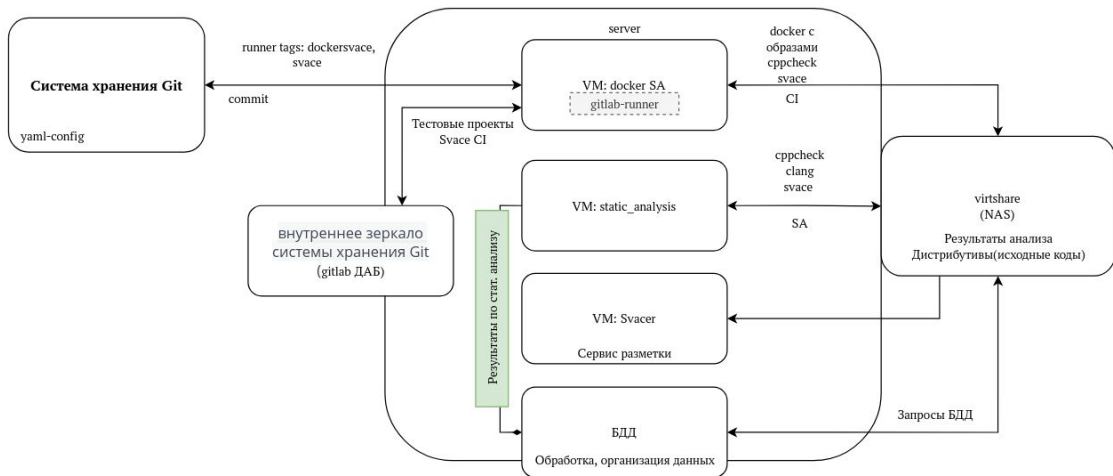
Задачи спринта

ID	Статус	Проект	Утилита	Обертка	Время фазинга	Фазаер	Execs	Corpus	Crashes	Cycles	Lines	Branches	Functions	Coverage	Harness_Coverage	Tar_results
227	DONE	parsec	execcaps	argv	18000	AFL	17898693	98	0	2	95.2%	87.5%	81.8%	<a href="#">get_coverage</a>	<a href="#">get_harness_coverage</a>	<a href="#">get_tar</a>
228	DONE	parsec	getfaud	argv	18000	AFL	5682940	212	0	1	27.9%	18.3%	34.3%	<a href="#">get_coverage</a>	<a href="#">get_harness_coverage</a>	<a href="#">get_tar</a>
229	DONE	parsec	lib-aud	aud_fputaudent	18000	AFL	20147359	60	0	0	13.0%	11.4%	9.4%	<a href="#">get_coverage</a>	<a href="#">get_harness_coverage</a>	<a href="#">get_tar</a>
230	DONE	parsec	lib-aud	aud_from_text	18000	AFL	10037862	266	0	2	47.9%	36.8%	51.4%	<a href="#">get_coverage</a>	<a href="#">get_harness_coverage</a>	<a href="#">get_tar</a>
231	DONE	parsec	lib-aud	aud_parse_aud	18000	AFL	25484013	90	0	5	22.7%	19.6%	18.1%	<a href="#">get_coverage</a>	<a href="#">get_harness_coverage</a>	<a href="#">get_tar</a>
232	DONE	parsec	lib-aud	aud_setaudent	18000	AFL	7640684	48	0	4	18.8%	14.6%	20.3%	<a href="#">get_coverage</a>	<a href="#">get_harness_coverage</a>	<a href="#">get_tar</a>
233	DONE	parsec	lib-aud	aud_wcputaudent	18000	AFL	20147359	63	0	0	14.3%	12.4%	12.3%	<a href="#">get_coverage</a>	<a href="#">get_harness_coverage</a>	<a href="#">get_tar</a>
234	DONE	parsec	lib-aud	aud_wcputaudent	18000	AFL	14900071	47	0	6	19.5%	14.3%	21.0%	<a href="#">get_coverage</a>	<a href="#">get_harness_coverage</a>	<a href="#">get_tar</a>
235	DONE	parsec	lib-aud	aud_wcsetaudent	18000	AFL	8225499	38	0	421	17.7%	12.4%	23.9%	<a href="#">get_coverage</a>	<a href="#">get_harness_coverage</a>	<a href="#">get_tar</a>
236	DONE	parsec	lib-aux	maux_byteorder	18000	AFL	32255623	39	0	75	100.0%	-	100.0%	<a href="#">get_coverage</a>	<a href="#">get_harness_coverage</a>	<a href="#">get_tar</a>



# Статический анализ

- Svace
- Clang Static Analyzer (CSA)
- АК-BC 3
- Cppcheck
- AppScreener
- CodeQL

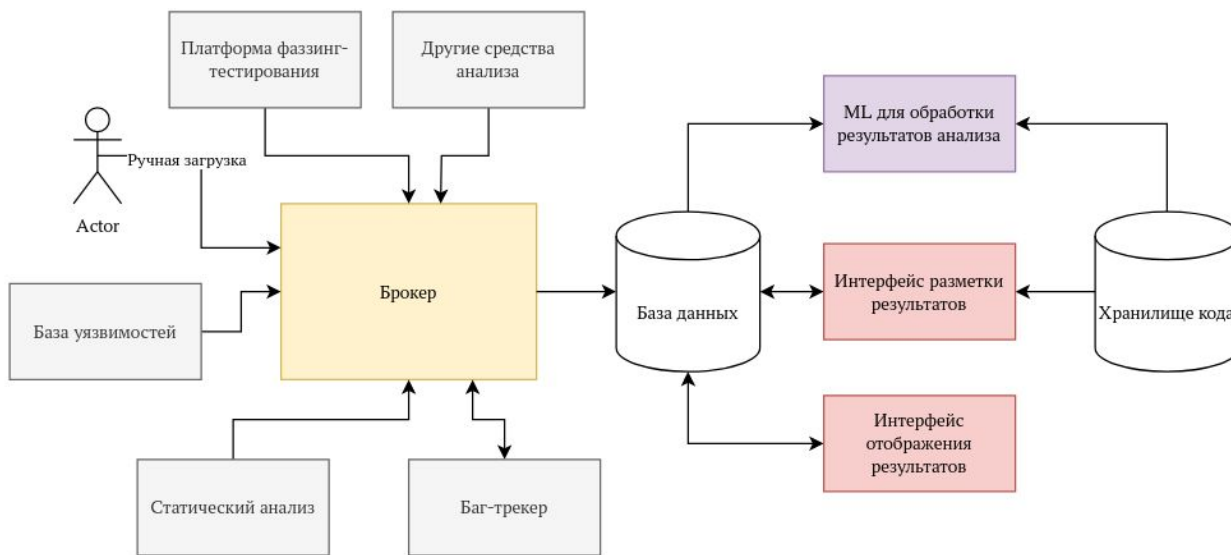


# Платформа хранения и обработки результатов (БДД)



- **Интерфейс разметки** результатов статического анализа
- Автоматическая **приоритизация** обнаруженных ошибок
- **Сопоставление результатов** от различных средств анализа
- **Хранение и обработка** статистики об обнаруженных ошибках
- **Распределение задач** между специалистами, функционал отправки на **ревью**
- Кросс-разметка и **верификация** ранее полученных результатов
- Автоматизированное **формирование отчетов** об обнаруженных ошибках в рамках пакета или продукта
- **Централизованный доступ** ко всем результатам анализа, их выгрузка и загрузка

# Общая архитектура платформы хранения и обработки результатов анализа



# Машинное обучение: цели и задачи

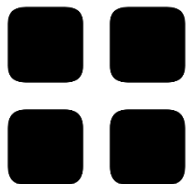
<b>Приоритизация</b>	<ul style="list-style-type: none"><li>● Предварительная разметка с использованием машинного обучения и алгоритмов принятия риска.</li><li>● Определение критичности ошибки.</li></ul>
<b>Классификация</b>	<ul style="list-style-type: none"><li>● Классификация ошибок по типам (CWE)</li></ul>
<b>Кластеризация</b>	<ul style="list-style-type: none"><li>● Разделение ошибок на кластеры по ключевым словам в описании, по коду и др.</li><li>● Сопоставление результатов анализаторов по разным кластерам и их сравнение</li></ul>







# Автоматическая разметка



## Откуда данные

- Разметка от команды статического анализа
- Разметка от Центра исследования Ядра Linux
- Разметка от Центра тестирования системных компонентов
- Открытые наборы данных для обучения



## Что берем

- Данные о разметке (SARIF)
- Код



## Какой результат

- Достигнута точность 86% на наших данных
- Дообучаем модель



### Моя разметка

ID	Дистрибутив	Пакет	Файл	Строка	Статус	
33521	Astra Linux SE 1.7.4	apt 1.8.2.3	/library/adenroll.c	299	MAJOR	Перейти
33522	Astra Linux SE 1.7.4	apt 1.8.2.3	/library/adenroll.c	432	MINOR	Перейти
34522	Astra Linux SE 1.7.4	apt 1.8.2.3	/src/bin/aldd/ADTaskThread.cpp	22	MEDIUM	Перейти
34523	Astra Linux SE 1.7.4	apt 1.8.2.3	/src/bin/aldd/ADTaskThread.cpp	29	WON'T FIX	Перейти
34524	Astra Linux SE 1.7.4	apt 1.8.2.3	/src/bin/aldd/ADTaskThread.cpp	78	MINOR	Перейти

< 1 2 >

### Последние события

Даниил Шварев прокомментировал запись Astra Linux SE 1.7.4 apt ( ID: 29987 )

Добавлено 369 записей для пакета apt ( Astra Linux SE 1.7.4 )

Добавлено 190 записей для пакета audit ( Astra Linux SE 1.7.4 )

### Прогресс

Дистрибутив	Пакет	Прогресс
Astra Linux SE 1.7.4	apt	<div style="width: 12%;"></div> 12%
Astra Linux SE 1.7.4	enigmail	<div style="width: 1%;"></div> 1%
Astra Linux SE 1.7.4	ldm	<div style="width: 17%;"></div> 17%
Astra Linux SE 1.7.4	libebml	<div style="width: 23%;"></div> 23%
Astra Linux SE 1.7.4	qemu	<div style="width: 4%;"></div> 4%

< 1 2 >

### Запросы на ревью

Екатерина Есина : Astra Linux SE 1.7.4 apt ( ID: 29987 )

Екатерина Есина : Astra Linux SE 1.7.4 apt ( ID: 44854 )

Анастасин Любимова : Astra Linux SE 1.7.4 apt ( ID: 23483 )



База Данных Доверия
Гончарук Станислав admin

#### UNINITLOCAL\_VAR

Uninitialized data is read from local variable 'larg' at AACmdTask.cpp:370

[/src/rhorns/ald-core-a/commands/AACmdTask.cpp:370](#) Save

BT	Статус	Приоритет	Критичность	Воспроизводимость	Описание	Исправлено
Ошибка SEGV on unknown address в файле main.c	Открыт	Средний	Малая	Всегда	На стандартном тестировании в библиотеке libxml в файле main.c (commit 751662d0ff939411d016107810161562e9b6d33) обнаружена ошибка, связанная с обращением к неинициализированной памяти. Ошибка возникает, например, при выводе (code data) main._dname"/tests/test5"). (code) Сторейко ошибки lmare-2023-03-06-19-48-07-587.pngwidth=1233,height=219	

#### Dead Code

The product contains dead code, which can never be executed.

[/src/common/ALDCommand.cpp:305](#) Save CWE-561

< 1 2 3 >
100 / page



# Что дальше?

## Фаззинг. Юзерспейс:

- Интеграция с [Fuzz Introspector](#)
- Добавление на платформу фаззинга [среды для воспроизведения](#) и детального анализа обнаруженных падений
- Внедрение [LLM](#) для генерации фаззинг-оберток

## Фаззинг. Ядро:

- Интеграция платформы с [Jira](#) для оптимизации процессов обработки обнаруженных ошибок
- Добавление функционала [направленного фаззинга](#)

## Платформа хранения и обработки результатов:

- Внедрение [VulBERTA](#) для обнаружения и подтверждения ошибок в исходном коде
- Добавление функционала [сравнения результатов](#) статического анализа в разных версиях ПО в интерфейс разметки

Спасибо за внимание!