



ООО «Базальт СПО»

Российский разработчик
операционных систем «Альт»

basealt.ru

РБПО на конвейере: как Hantis избавляет исследователя от рутины

Костригин Николай Александрович

Руководитель отдела БРПО

nickel@basealt.ru

Платонова Софья Дмитриевна

Менеджер по работе со стратегическими партнерами

platonovasd@basealt.ru





Независимая разработка

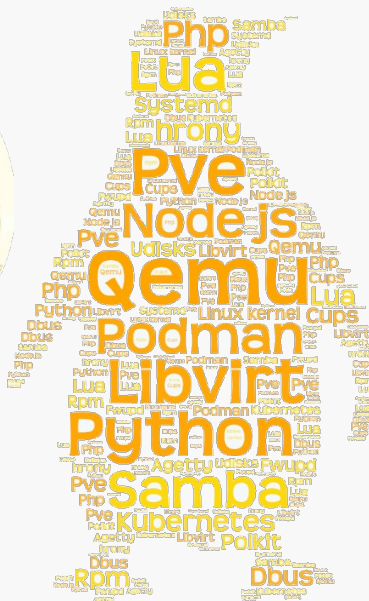
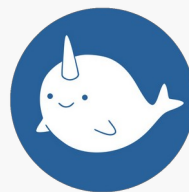
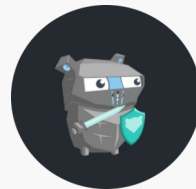
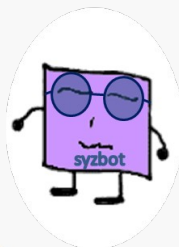
Проект «Сизиф»:

- Все продукты Базальт СПО, включая сертифицированную версию ОС — Альт СП, построены на пакетной базе стабильных ветвей репозитория Сизиф.
- Сизиф один из независимых репозиториях Свободного ПО, вбирает в себя пакеты, разрабатываемые мировым сообществом.
- Основой проекта Сизиф является ALT Linux Team, а поддержку инфраструктуры репозитория обеспечивает ООО «Базальт СПО»
- Многие сотрудники компании являются членам ALT Linux Team





Особенности при проведении РБПО-исследований



- SnapFuzz
- Hopper
- Nyx
- Go-Fuzz
- AFL++
- LibFuzzer
- Clang Static Analyzer
- Cppcheck
- Clippy
- Svace
- Sydr-fuzz
- Syzkaller
- jazzer

Большое число объектов исследования (>30);
Большое число языков программирования, на которых они
написаны;
Необходим большой ассортимент инструментов (>10).

Особенности при проведении РБПО-исследований

- Использование разделяемых библиотек (shared objects) позволяет экономить ресурсы системы и проще исправлять уязвимости, но накладывают ограничения на возможность обновления версий, чтобы не нарушать совместимость.
- Версии ПО в стабильных ветвях репозитория могут отставать от последних релизов разработчиков проекта (апстрима).
- Разработчики в апстримах некоторых проектов неохотно бэкпортируют исправления в старые ветви.

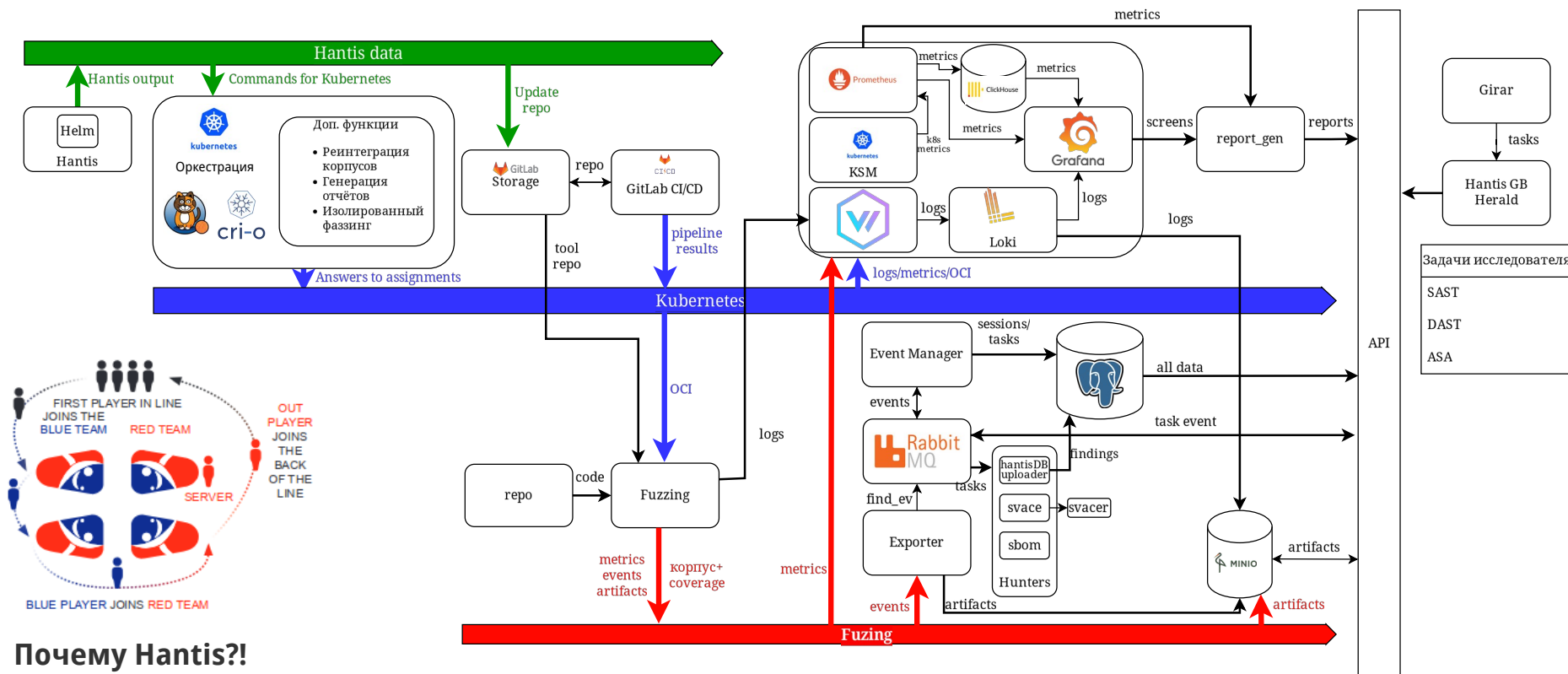
Приводит к:

[минусам] - необходимости разрабатывать исправления для нескольких веток или самостоятельно поддерживать ветку с бэкпортом;

[плюсам] - обнаруженные в старых стабильных ветках недостатки ПО уже исправлены в новых и могут быть бэкпортированы.

Структура конвейера Hantis

Код проекта
лицензирован под
GNU AGPLv3



Hantis Helm-чарты

- **Helm чарты** — это пакеты для Kubernetes, которые содержат все необходимые файлы для развертывания приложения или сервиса в кластере Kubernetes.
- **Основные компоненты Helm чарта:**
 - chart.yaml: Метаданные (название, версия, описание).
 - values.yaml: Настройки по умолчанию, переопределяемые пользователем.
 - templates/: Шаблоны манифестов Kubernetes (Deployment, Service и др.).
 - requirements.yaml (опционально): Зависимости от других чартов.
 - charts/: Вложенные чарты.
 - README.md (опционально): Документация.
- **Преимущества:**
 - Helm значительно ускоряет работу с Kubernetes, особенно при сложных развертываниях, требующих управления несколькими компонентами.
 - Упрощение развертывания.
 - Параметризация для разных окружений.
 - Версионирование для управления обновлениями.
 - Повторяемость развертываний.
 - Управление зависимостями.

Hantis Hunters — механизмы расширения

- **Hantis** позволяет подключать службы **Hunters** расширяющие функциональность для поддержки других методов анализа кода.
- **Hunters** — набор различных сервисов для SAST, DAST, ASA, SCA.
- Плагины, которые оформляются в виде самостоятельных репозиториев

Примеры сервисов:

- ASA: natch, natch-image-builder
- SAST: svace-builder, svace-analyzer





Нантис как инструмент для автоматизации РБПО-практик

- Сохраняет и фиксирует накопленный опыт.
- Автоматически запускает все предыдущие наработки для новых релизов.
- Отслеживает срабатывания инструментов анализа и формирует задания на триаж.
- Позволяет гарантировать устранение всех выявленных несоответствий, не дав им затеряться.



Статистика за 2024 год

Статический анализ		Подготовленные исправления и рекомендации			
Размеченные сработки статического анализатора по всем проектам		Исправления для основной ветки разработки компонентов			
В рамках работы LVC		SAST	Fixes	DAST	Fixes
		Libvirt	10	Libvirt	2
		Lipslirp	-	Lipslirp	1
		PostgreSQL	1	PostgreSQL	-
		QEMU	-	QEMU	1
		Bash	-	Bash	1
		Iptables	-	Iptables	1
Динамический анализ		Исправления в проекте linux-kernel			
Обнаруженные уязвимости		5.10 LVC	6.1 LVC	upstream	
Уязвимость функции udevListInterfacesByStatus() библиотеки Libvirt: CVE-2024-1441 (BDU: 2024-02834)		10	10	6	
Уязвимость функции g_new0() библиотеки Libvirt: CVE-2024-2494 (BDU: 2024-02380)					



Нафаззили! И не только мы.... Что дальше?

Работа с уязвимостями в ПО

- Агрегация и сопоставление информации об уязвимостях из всех доступных источников;
- Хранение в формате OVAL с возможностью выгрузки в XML;
- Возможность реимпорта в оффлайн базу для инструмента сканирования контейнеров **trivy**;
- Автоматическая генерация списков исправлений (errata) с возможностью редактирования;

The screenshot displays the 'Исправления' (Errata) section of the base alt interface. It shows a list of packages with their associated vulnerabilities and errata details.

Package 1: sisyphus_mipsel: ALT-PU-2023-5798-1
Затронутые пакеты: openssl3
Исправления: BDU:2023-05872, CVE-2023-4807

Package 2: sisyphus_mipsel: ALT-BU-2023-5799-1
Затронутые пакеты: openssl3
Исправления: ALT-PU-2023-5798-1

Package 3: sisyphus: ALT-PU-2023-5753-1 от #329935
Затронутые пакеты: openssl3
Исправления: CVE-2023-4807

Package 4: sisyphus_e2k: ALT-PU-2023-5772-1
Затронутые пакеты: openssl3
Исправления: BDU:2023-05872, CVE-2023-4807

Errata Details for ALT-PU-2023-5798-1:
Имя пакета: openssl3
Версия: 3.1.3-alt1
Обновлено: 21 сентября 2023 г.
Опубликовано: 8 сентября 2023 г.
Уязвимость криптографической библиотеки OpenSSL, связанная с неправильной проверкой ввода, позволяющая нарушителю выполнить атаку типа «отказ в обслуживании»
Важность: HIGH (7.8) Вектор: AV:L/AC:L/PR:L/UI:N/S:U/CN:I/H/AH

Ссылки:
• CVE-2023-4807

Additional Information:
3.1.5-alt1 собрано 3 февраля 2024 г. Gleb Fotengauer-Malinovskiy в задании #339669
2 февраля 2024 г. Gleb Fotengauer-Malinovskiy
- Updated to 3.1.5.
3.1.4-alt1 собрано 25 октября 2023 г. Gleb Fotengauer-Malinovskiy в задании #332632
24 октября 2023 г. Gleb Fotengauer-Malinovskiy
- Updated to 3.1.4 (fixes CVE-2023-5363).
3.1.3-alt1 собрано 20 сентября 2023 г. Gleb Fotengauer-Malinovskiy в задании #329935
19 сентября 2023 г. Gleb Fotengauer-Malinovskiy
- Updated to 3.1.3 (fixes CVE-2023-4807).
Опубликовано: 8 сентября 2023 г.
Обновлено: 21 сентября 2023 г.
05 MAC (message authentication code) corrupt the internal state running on newer X86_64

Конфигурации вычислителей

Hantis – prod (VM)

- CPU: 88
- RAM: 88 GiB
- Disk: 750 GiB



Fuzzing server (HW)

- CPU: 256
- RAM: 256GiB
- Disk: 1 + 4 TB

AMD EPYC

Kernel Fuzzer

- CPU:
- RAM: 128 GiB
- Disk: 1 TB

AMD Ryzen



Kernel Fuzzer New

- CPU: 512
- RAM: 512 GiB
- Disk: 1 + 4 TB

AMD EPYC



0 компании

89

Регионов РФ

8

операционных
систем

11

аппаратных
платформ

24+

лет на рынке

- Собственная технологическая платформа
- Своя инфраструктура на территории РФ
- Офисы в 4 городах

Поставки лицензий

1 300 000+

всего

280 000+

для образования

Обучение

11 000+

специалистов

Семейство ОС «Альт»



Альт СП

Операционная система со встроенными средствами защиты информации. Сертифицировано ФСТЭК РФ.



Альт Платформа

Технологический комплекс для сборки программного обеспечения.



Альт Сервер

Комплексное серверное решение для ИТ-инфраструктуры.



Альт Образование

Операционная система для тех, кто учится и учит.



Альт Виртуализация

Универсальное решение для создания и миграции виртуальной ИТ-инфраструктуры.



Simply Linux

Операционная система для пользователей, которые ценят скорость при ограниченной мощности компьютера.



Альт Рабочая станция, К

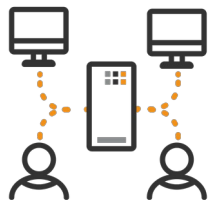
Операционная система, проверенная временем, для оборудования с любыми процессорами.



Альт Mobile

Операционная система для планшетов, смартфонов и других мобильных устройств.

Решения



Альт Домен



Виртуализация PVE



**Виртуализация
Open Nebula**



Контейнеризация



VDI-брокер



**Реестр
контейнеров**



СУБД



Сообщество пользователей



**СПИСКИ
РАССЫЛКИ**
lists.altlinux.org



**TELEGRAM-КАНАЛ
«БАЗАЛТ СПО»**
t.me/basealtspo



**ФОРУМ СООБЩЕСТВА
ALT LINUX**
forum.altlinux.org



VK ВИДЕО
vkvideo.ru



**WIKI-ДОКУМЕНТАЦИЯ
СООБЩЕСТВА**
altlinux.org



ХАБР
habr.com



Контакты:

Тел.: +7 (495) 123-47-99

E-mail: contact@basealt.ru

Бесплатная техническая
поддержка на этапе
тестирования:
basealt.ru/sales2

Офисы:

Москва, ул. Бутырская, д. 75

Санкт-Петербург, 4-я линия В.О., д. 17, БЦ «ЛВА»

Саратов, ул. Октябрьская 44, корпус А, офис № 3

Обнинск, ул. Королёва, д. 4Б, БЦ "Британика"

basealt.ru