РБПО:
Процесс №5.+

Антон Гаврилов
Владелец Продукта «Шерлок»
gavrilov@axel.pro
+7 929 653 42 90

Знакомьтесь,

Axel PRO

Продуктовая студия, разрабатывающая решения в области кибербезопасности

ОПЫТ И ЭКСПЕРТИЗА

Сертифицированных экспертов по кибербезопасности

ОТЕЧЕСТВЕННОЕ ПО

Продукты Axel PRO входят в реестр отечественного ПО

ИННОВАЦИОННЫЕ ПРОДУКТЫ

от инфраструктурной безопасности да аналитических систем

НАШИ ПРОДУКТЫ

- AxelMAC
- LogIQ
- Шерлок

О чем мы сегодня поговорим?

- Контекст
- Проблематика
- Решение
- Выводы

ВНИМАНИЕ!

ВНИМАНИЕ!

AXEL pro

ML не будет в презентации!* 😱

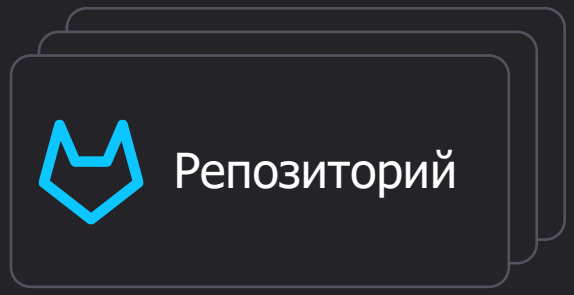
* хотя он много где может пригодиться

О чем мы сегодня поговорим?

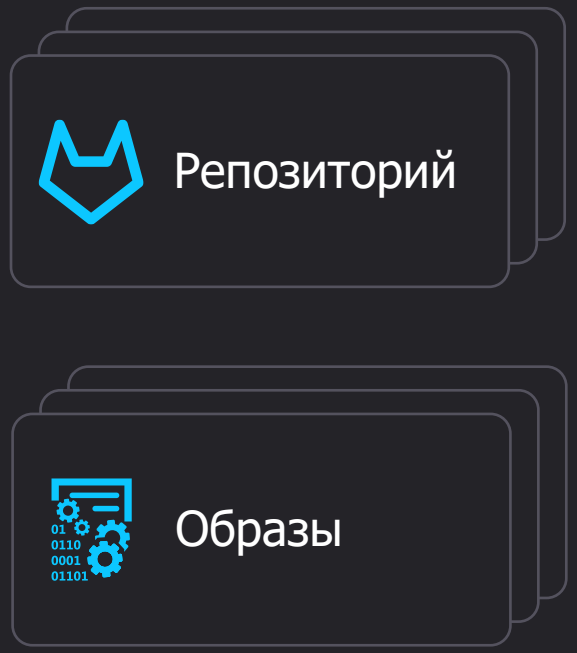
- **Контекст**
- Проблематика
- Решение
- Выводы

Контекст или что у нас есть?

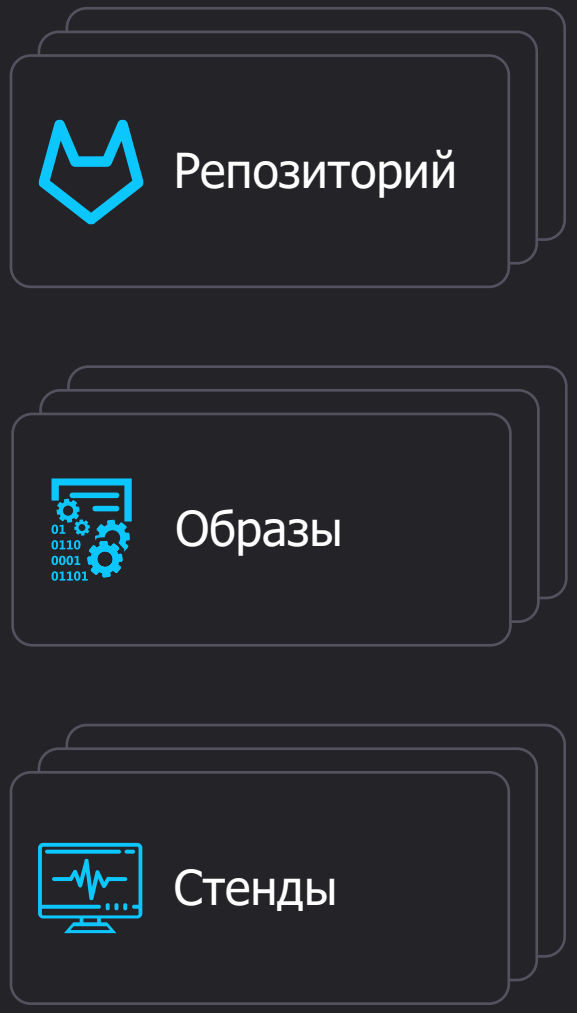
Контекст или что у нас есть?



Контекст или что у нас есть?



Контекст или что у нас есть?



- У нас есть ПО, которое «состоит из»:
  - Нескольких репозиториев
  - Нескольких образов контейнеров
  - Есть несколько стендов (dev, test, stage и т.д.)
- Задача – сделать ПО безопасным

Процессы разработки безопасного ПО

5.1 Планирование процессов разработки безопасного ПО

Процессы разработки безопасного ПО

Процессы разработки безопасного ПО

5.1 Планирование процессов разработки безопасного ПО

5.2 Обучение сотрудников

... ...

Процессы разработки безопасного ПО

5.1 Планирование процессов разработки безопасного ПО

5.2 Обучение сотрудников

... ...

5.10 Статический анализ исходного кода

Процессы разработки безопасного ПО

AxeL pro

- 5.1 Планирование процессов разработки безопасного ПО
- 5.2 Обучение сотрудников
- … …
- 5.10 Статический анализ исходного кода
- 5.11 Динамический анализ кода программы

Процессы разработки безопасного ПО

5.1 Планирование процессов разработки безопасного ПО

5.2 Обучение сотрудников

… …

5.10 Статический анализ исходного кода

5.11 Динамический анализ кода программы

… …

Процессы разработки безопасного ПО

5.1	Планирование процессов разработки безопасного ПО
5.2	Обучение сотрудников
…	…
5.10	Статический анализ исходного кода
5.11	Динамический анализ кода программы
…	…
5.15	Обеспечение безопасности используемых секретов

Процессы разработки безопасного ПО

5.1	Планирование процессов разработки безопасного ПО
5.2	Обучение сотрудников
…	…
5.10	Статический анализ исходного кода
5.11	Динамический анализ кода программы
…	…
5.15	Обеспечение безопасности используемых секретов
5.16	Использование инструментов композиционного анализа

Процессы разработки безопасного ПО

5.1	Планирование процессов разработки безопасного ПО
5.2	Обучение сотрудников
…	…
5.10	Статический анализ исходного кода
5.11	Динамический анализ кода программы
…	…
5.15	Обеспечение безопасности используемых секретов
5.16	Использование инструментов композиционного анализа
…	…

Процессы разработки безопасного ПО

5.1	Планирование процессов разработки безопасного ПО
5.2	Обучение сотрудников
…	…
5.10	Статический анализ исходного кода
5.11	Динамический анализ кода программы
…	…
5.15	Обеспечение безопасности используемых секретов
5.16	Использование инструментов композиционного анализа
…	…
5.25	Обеспечение безопасности при выводе ПО из эксплуатации

Процессы разработки безопасного ПО

5.1	Планирование процессов разработки безопасного ПО
5.2	Обучение сотрудников
…	…
5.10	Статический анализ исходного кода
5.11	Динамический анализ кода программы
…	…
5.15	Обеспечение безопасности используемых секретов
5.16	Использование инструментов композиционного анализа
…	…
5.25	Обеспечение безопасности при выводе ПО из эксплуатации

«Подготовительные работы»

Процессы разработки безопасного ПО

5.1	Планирование процессов разработки безопасного ПО	«Подготовительные работы»
5.2	Обучение сотрудников	
…	…	
5.10	Статический анализ исходного кода	Активная фаза разработки
5.11	Динамический анализ кода программы	
…	…	
5.15	Обеспечение безопасности используемых секретов	
5.16	Использование инструментов композиционного анализа	
…	…	
5.25	Обеспечение безопасности при выводе ПО из эксплуатации	

Процессы разработки безопасного ПО

5.1	Планирование процессов разработки безопасного ПО	«Подготовительные работы»
5.2	Обучение сотрудников	
…	…	
5.10	Статический анализ исходного кода	Активная фаза разработки
5.11	Динамический анализ кода программы	
…	…	
5.15	Обеспечение безопасности используемых секретов	
5.16	Использование инструментов композиционного анализа	
…	…	Защита во время эксплуатации
5.25	Обеспечение безопасности при выводе ПО из эксплуатации	

Процессы разработки безопасного ПО

5.1	Планирование процессов разработки безопасного ПО	«Подготовительные работы»
5.2	Обучение сотрудников	
...	...	
5.10	**Статический анализ исходного кода**	Активная фаза разработки
5.11	Динамический анализ кода программы	
...	...	
5.15	**Обеспечение безопасности используемых секретов**	
5.16	**Использование инструментов композиционного анализа**	
...	...	Защита во время эксплуатации
5.25	Обеспечение безопасности при выводе ПО из эксплуатации	

Процессы: что нам надо сделать?

- Определить обязанности сотрудников и их роли при проведении анализа

Процессы: что нам надо сделать?

- Определить обязанности сотрудников и их роли при проведении анализа
- Определить правила обработки срабатываний средств автоматизации

Процессы: что нам надо сделать?

- Определить обязанности сотрудников и их роли при проведении анализа
- Определить правила обработки срабатываний средств автоматизации
- Определить типы и критичность ошибок (уязвимостей), подлежащих устранению

Процессы: что нам надо сделать?

- Определить обязанности сотрудников и их роли при проведении анализа
- Определить правила обработки срабатываний средств автоматизации
- Определить типы и критичность ошибок (уязвимостей), подлежащих устранению
- Определить приоритеты устранения ошибок (уязвимостей)

Технологии: что нам надо сделать?

- Определить подходящие инструменты

Технологии: что нам надо сделать?

- Определить подходящие инструменты
- Определить конфигурацию и параметры настройки инструментов

Технологии: что нам надо сделать?

- Определить подходящие инструменты
- Определить конфигурацию и параметры настройки инструментов
- Проводить анализ

Технологии: что нам надо сделать?

- Определить подходящие инструменты
- Определить конфигурацию и параметры настройки инструментов
- Проводить анализ
- Устранять найденные недостатки

Технологии: что нам надо сделать?

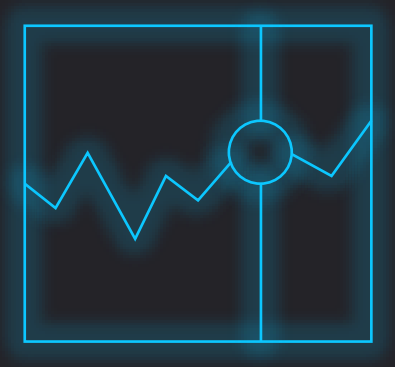
- Определить подходящие инструменты
- Определить конфигурацию и параметры настройки инструментов
- Проводить анализ
- Устранять найденные недостатки
- Адаптировать конфигурации и параметры настройки инструментов

Технологии: что нам надо сделать?

- Определить подходящие инструменты
- Определить конфигурацию и параметры настройки инструментов
- Проводить анализ
- Устранять найденные недостатки
- Адаптировать конфигурации и параметры настройки инструментов
- Повторять при изменениях*

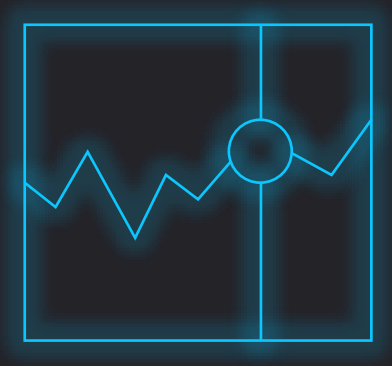
* исходного кода, компиляторов, интерпретаторов, инструментов, их версий и т.д.

Люди: кто нам нужен?

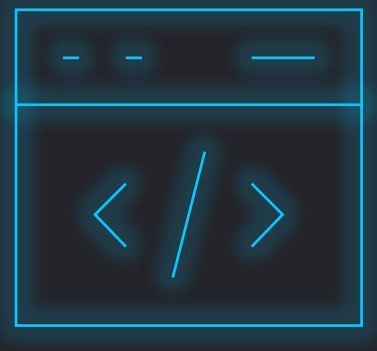


РБПО-
специалисты

Люди: кто нам нужен?

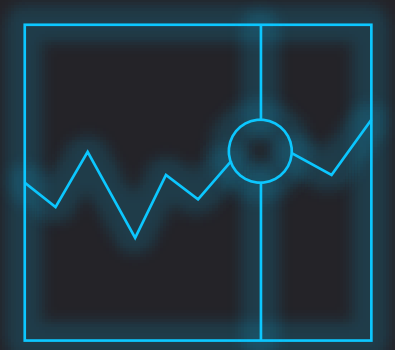


РБПО-специалисты

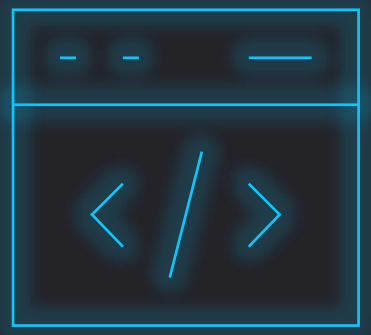


Разработчики

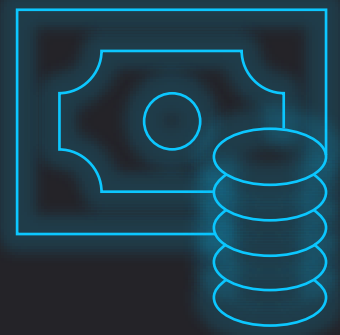
Люди: кто нам нужен?



РБПО-специалисты



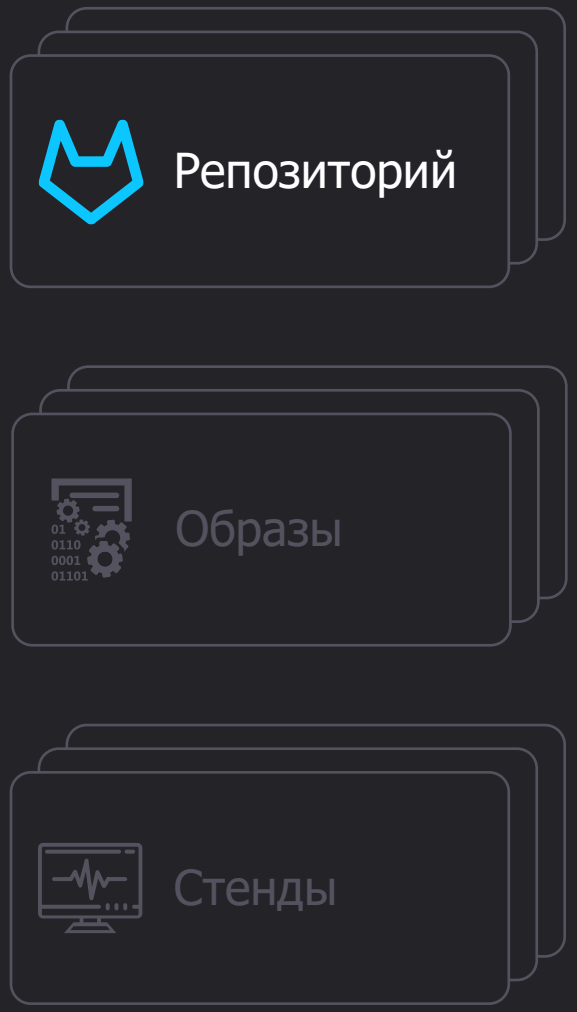
Разработчики



Руководство

Уточним контекст

Уточним контекст



- Мы определили набор «первичных» процессов:
  - Поиск секретов
  - Статический анализ
  - Композиционный анализ
- Нам надо встроить сканеры и настроить их
- Нам надо анализировать отчеты и делать разметку
- Мы знаем ключевых участников процесса
- Цель ясна – сделать так, чтобы количество ошибок (уязвимостей) сокращалось

О чем мы сегодня поговорим?

- Контекст
- **Проблематика**
- Решение
- Выводы

С какими нюансами мы столкнемся*?

* нет, это далеко не все, лишь небольшая выборка

С какими нюансами мы столкнемся*?

Неполный охват

Нам важно убедиться, что мы не пропустили ничего важного. Особенно это характерно для поиска секретов

* нет, это далеко не все, лишь небольшая выборка

С какими нюансами мы столкнемся*?

Неполный охват

Нам важно убедиться, что мы не пропустили ничего важного. Особенно это характерно для поиска секретов

Много «шума»

Большое количество ложных срабатываний, получаемых от сканеров:

- увеличивает длительности и стоимость анализа
- снижает доверие к используемым инструментам
- демотивирует участников процесса

* нет, это далеко не все, лишь небольшая выборка

С какими нюансами мы столкнемся*?

Неполный охват

Нам важно убедиться, что мы не пропустили ничего важного. Особенно это характерно для поиска секретов

Много «шума»

Большое количество ложных срабатываний, получаемых от сканеров:

- увеличивает длительности и стоимость анализа
- снижает доверие к используемым инструментам
- демотивирует участников процесса

Отсутствие указателей

Уровень критичности, установленный сканером, не учитывает:

- «принадлежность» компонента (например, ФБ или ПА)
- возможность эксплуатации
- наличие компенсирующих мер

* нет, это далеко не все, лишь небольшая выборка

С какими нюансами мы столкнемся*?

Неполный охват

Нам важно убедиться, что мы не пропустили ничего важного. Особенно это характерно для поиска секретов

Много «шума»

Большое количество ложных срабатываний, получаемых от сканеров:
- увеличивает длительности и стоимость анализа
- снижает доверие к используемым инструментам
- демотивирует участников процесса

Отсутствие указателей

Уровень критичности, установленный сканером, не учитывает:
- «принадлежность» компонента (например, ФБ или ПА)
- возможность эксплуатации
- наличие компенсирующих мер

«Трудности перевода»

Если мы отправим отчёт по электронной почте – можно забыть про устранение ошибок. Нужны иные каналы. Руководству нужно понимание общей картины

* нет, это далеко не все, лишь небольшая выборка

С какими нюансами мы столкнемся*?

Неполный охват

Нам важно убедиться, что мы не пропустили ничего важного. Особенно это характерно для поиска секретов

Много «шума»

Большое количество ложных срабатываний, получаемых от сканеров:
- увеличивает длительности и стоимость анализа
- снижает доверие к используемым инструментам
- демотивирует участников процесса

Отсутствие указателей

Уровень критичности, установленный сканером, не учитывает:
- «принадлежность» компонента (например, ФБ или ПА)
- возможность эксплуатации
- наличие компенсирующих мер

«Трудности перевода»

Если мы отправим отчёт по электронной почте – можно забыть про устранение ошибок. Нужны иные каналы. Руководству нужно понимание общей картины

«Проблемы роста»

То, что работает на малых количествах практически всегда перестает работать «на объеме» и наоборот

* нет, это далеко не все, лишь небольшая выборка

О чем мы сегодня поговорим?

- Контекст
- Проблематика
- **Решение**
- Выводы

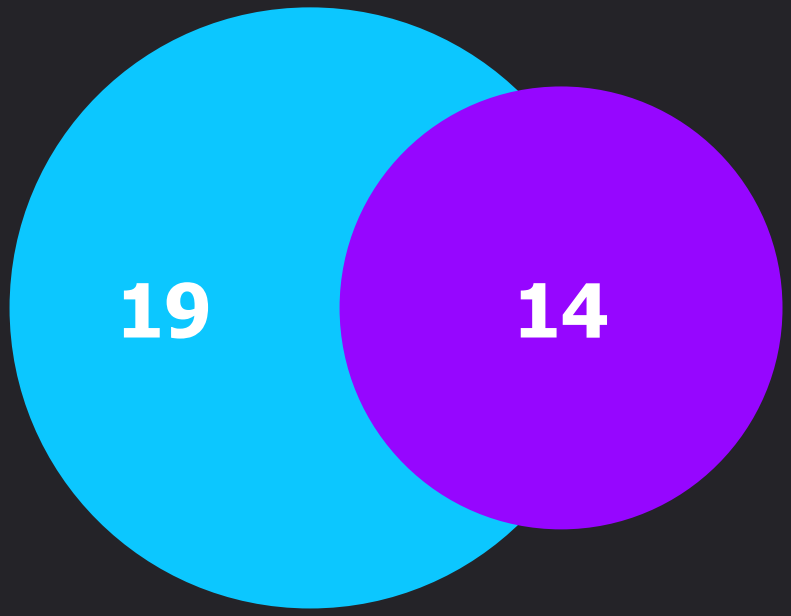
Неполный охват: что можно сделать?

Неполный охват: что можно сделать?

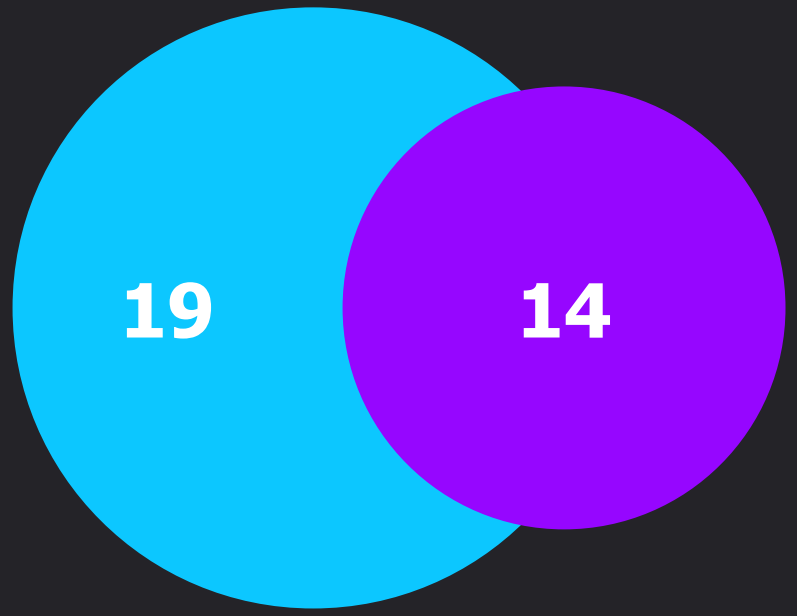
Одна голова хорошо, а две – лучше! **Использование нескольких сканеров** одного типа*

* дальнейшие выкладки не являются полноценной аналитической работой, но хорошо отражают суть

Секреты



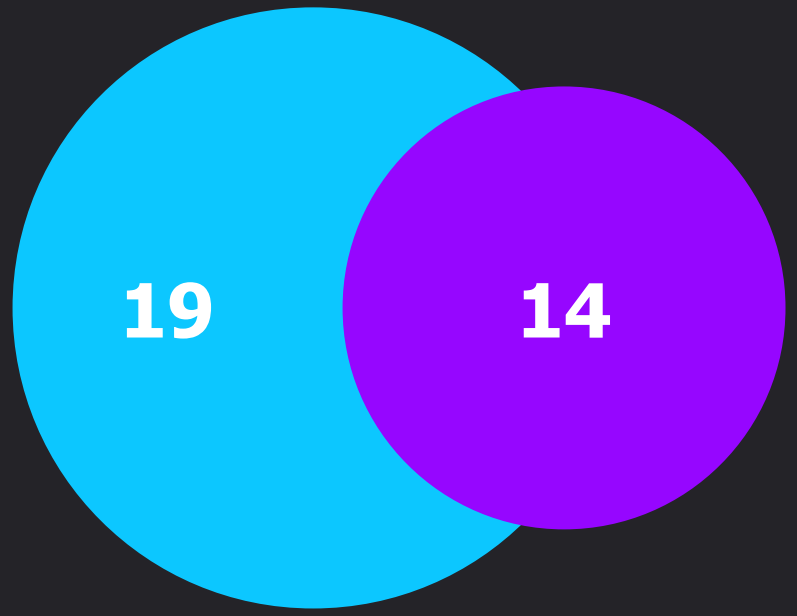
Секреты



Дедупликация

33

Секреты

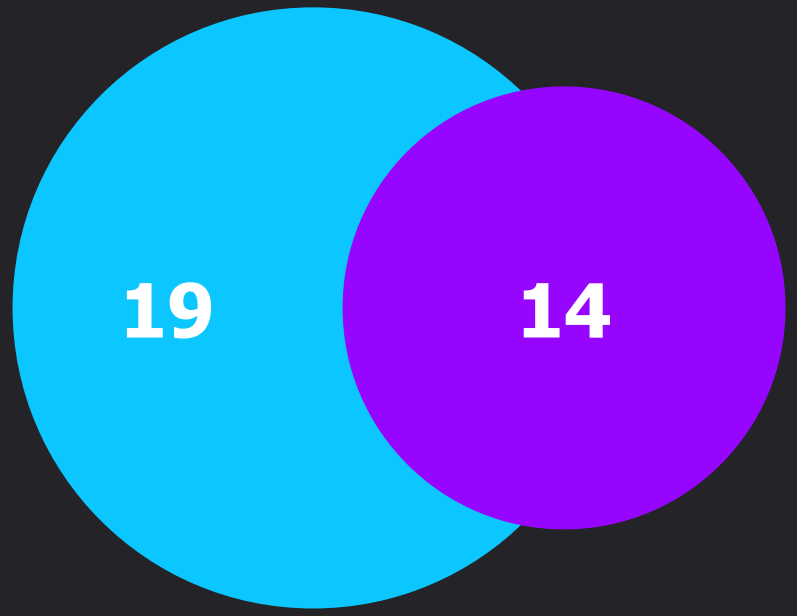


Дедупликация

33

23 - 30%

Секреты



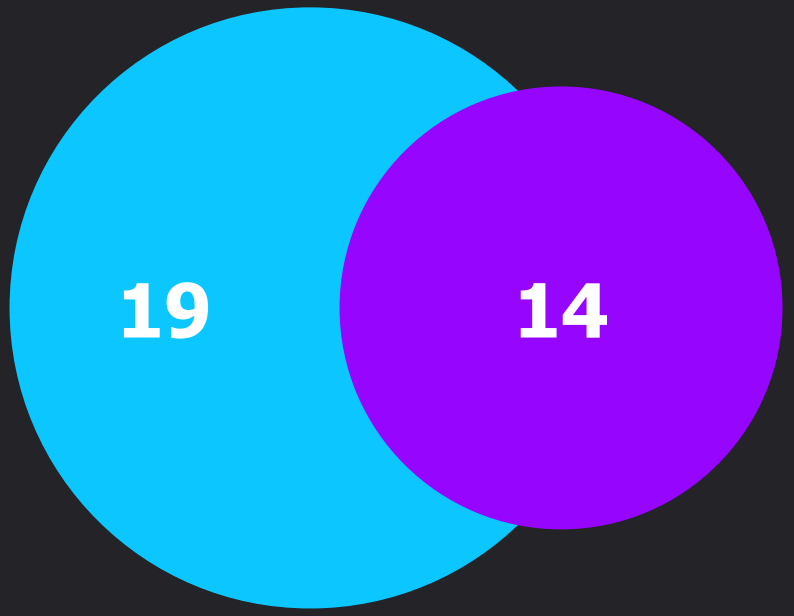
Дедупликация

33

23 - 30%

Уникальных 14 важно

Секреты



Дедупликация
33
23
- 30%

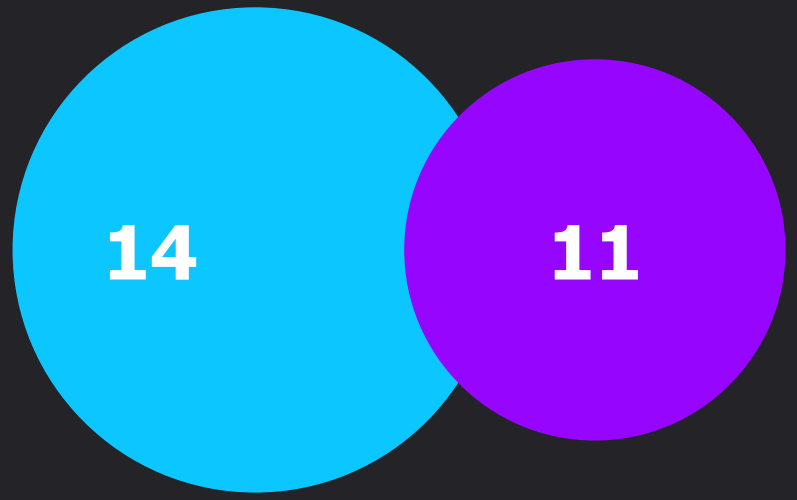
Уникальных
14
важно

ВЫВОД

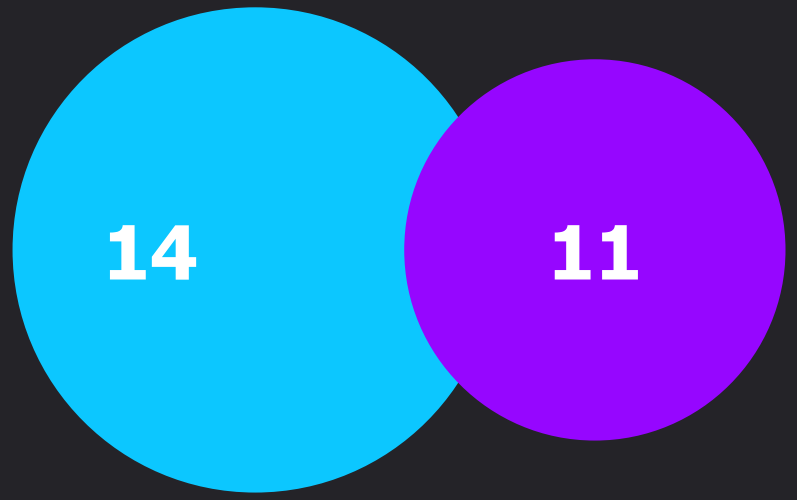
Использование нескольких сканеров **для поиска секретов целесообразно**, т.к. оно помогает решить проблему пропусков*

* с некоторыми нюансами, о которых мы поговорим далее

Статический анализ



Статический анализ

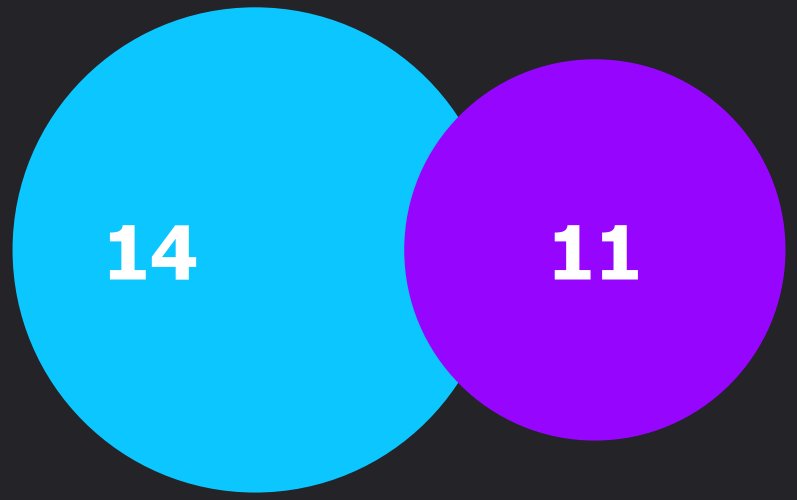


Дедупликация

25

* нам это пригодится чуть позднее

Статический анализ

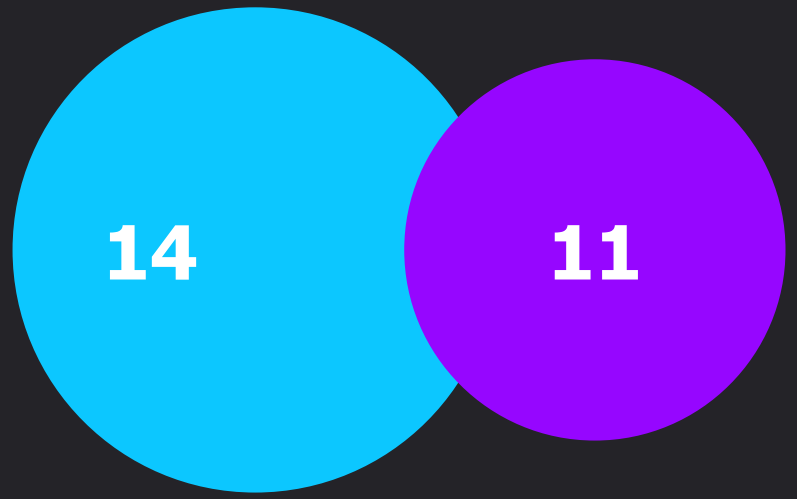


Дедупликация

25

20 - 20%

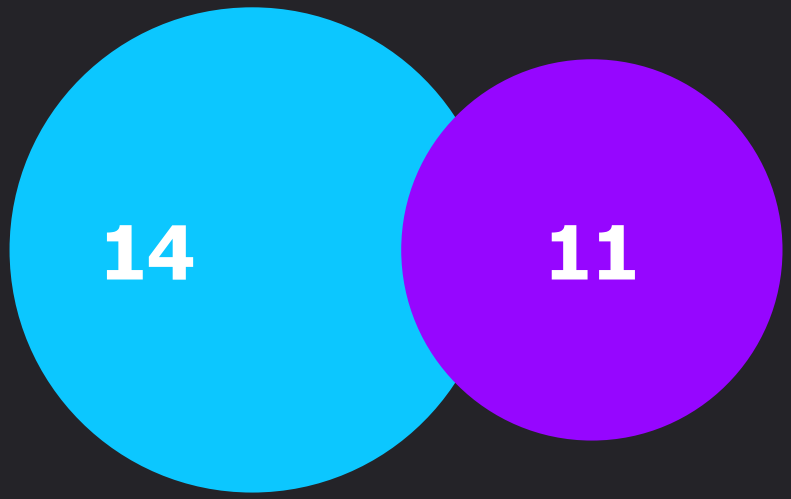
Статический анализ



Дедупликация
- 25
- 20 — **- 20%**

Уникальных — 15 — **важно**

Статический анализ



Дедупликация

25

20 - 20%

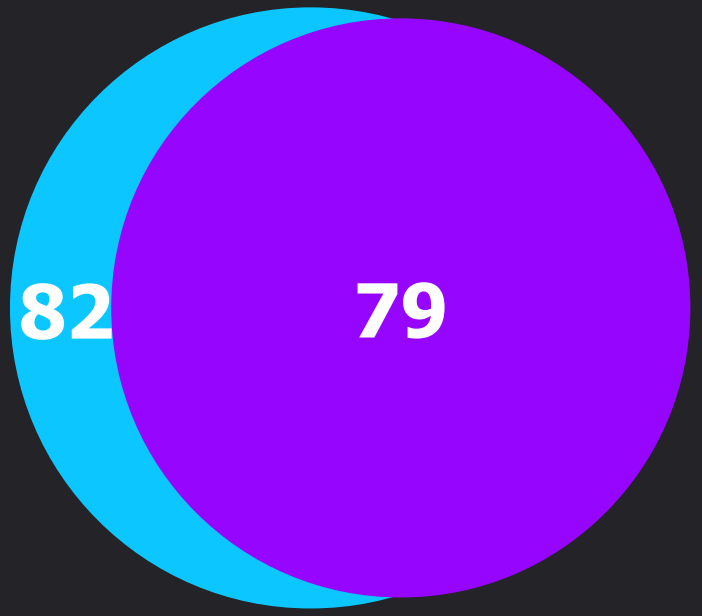
Уникальных 15 **важно**

ВЫВОД

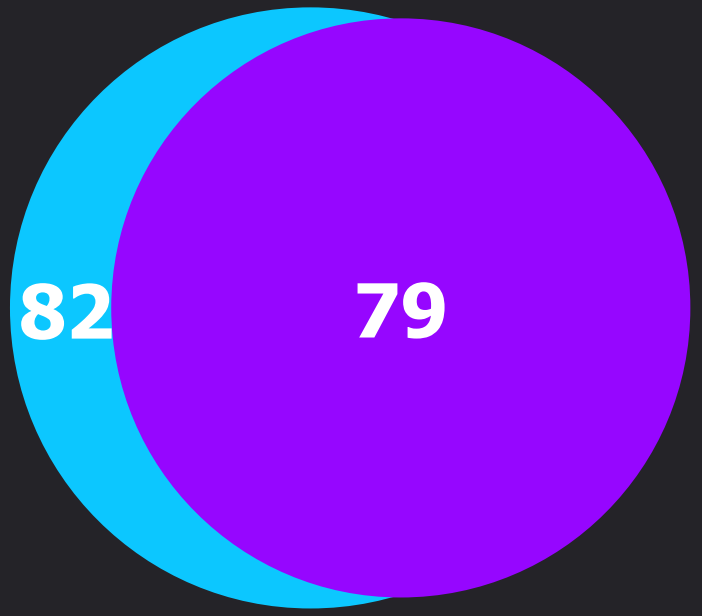
Использование нескольких сканеров **для статического анализа обладает своими сильными и слабыми сторонами***

* нам это пригодится чуть позднее

Композиционный анализ



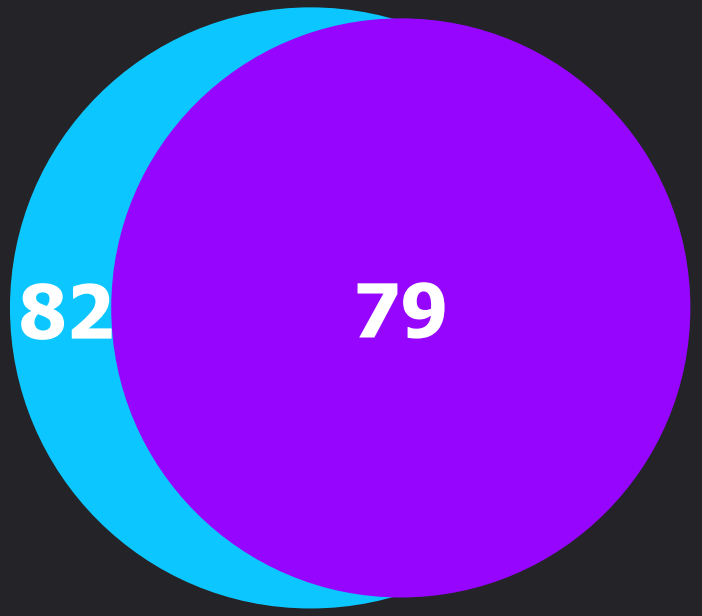
Композиционный анализ



Дедупликация

161

Композиционный анализ

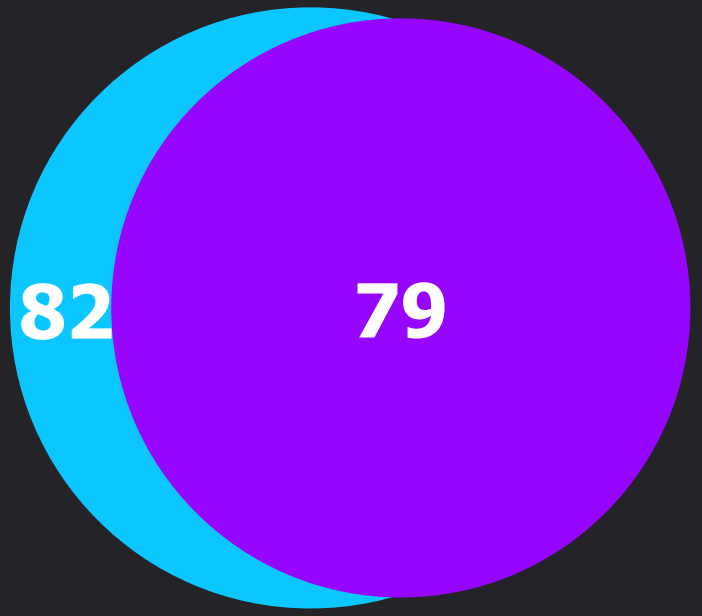


Дедупликация

161

74 - 54%

Композиционный анализ



Дедупликация

161

74

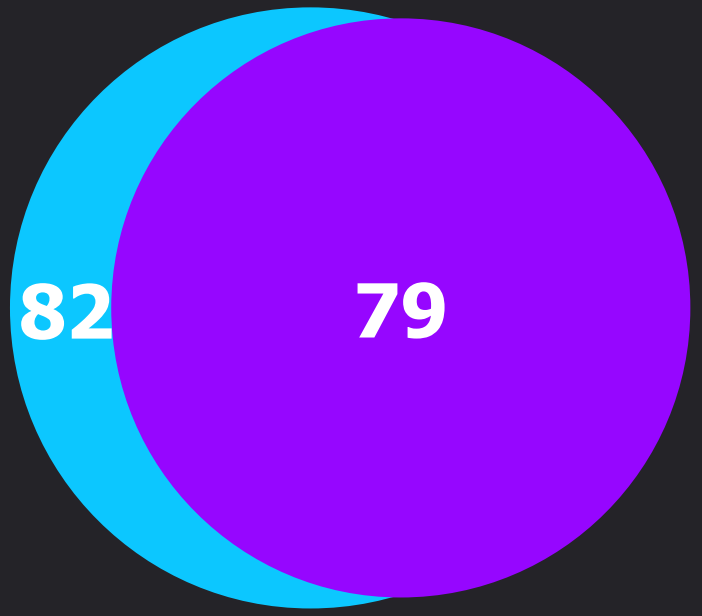
- 54%

Уникальных

14

не очень важно 😉

Композиционный анализ



Дедупликация
- 161
- 74 — **- 54%**

Уникальных — 14 — **не очень важно** 😉

ВЫВОД

Использование нескольких сканеров **для композиционного анализа не принесет много пользы***

* за исключением сканеров, обладающих уникальными feeds

Дедупликация

Дедупликация

Параметры

Дедупликация

AXEL pro

Параметры

Дедупликация

Дедупликация

Параметры — $f(x)$ — **Hash**

Варьируются в зависимости от типа сканера

Дедупликация: секреты (1 из 16)

Описание

Дедупликация: секреты (2 из 16)

~~Описание~~

У всех будет своим

Файл

Дедупликация: секреты (3 из 16)

~~Описание~~	Файл	Строка (начало)
У всех будет своим	Однозначно – да!	

Дедупликация: секреты (4 из 16)

~~Описание~~	Файл	Строка (начало)	Строка (конец)
У всех будет своим	Однозначно – да!	Да, может быть полезно	

Дедупликация: секреты (5 из 16)

~~Описание~~

У всех будет своим

Файл

Однозначно – да!

Строка (начало)

Да, может быть полезно

~~Строка (конец)~~

Не у всех сканеров есть

Отступ (начало)

Дедупликация: секреты (6 из 16)

~~Описание~~

У всех будет своим

Файл

Однозначно – да!

Строка (начало)

Да, может быть полезно

~~Строка (конец)~~

Не у всех сканеров есть

~~Отступ (начало)~~

Есть доступ к фрагменту кода

Отступ (конец)

Дедупликация: секреты (7 из 16)

~~Описание~~

У всех будет своим

Файл

Однозначно – да!

Строка (начало)

Да, может быть полезно

~~Строка (конец)~~

Не у всех сканеров есть

~~Отступ (начало)~~

Есть доступ к фрагменту кода

~~Отступ (конец)~~

Есть доступ к фрагменту кода

Совпадение

Дедупликация: секреты (8 из 16)

~~Описание~~

У всех будет своим

Файл

Однозначно – да!

Строка (начало)

Да, может быть полезно

~~Строка (конец)~~

Не у всех сканеров есть

~~Отступ (начало)~~

Есть доступ к фрагменту кода

~~Отступ (конец)~~

Есть доступ к фрагменту кода

~~Совпадение~~

Разные подходы к определению

Секрет

Дедупликация: секреты (9 из 16)

~~Описание~~

У всех будет своим

Файл

Однозначно – да!

Строка (начало)

Да, может быть полезно

~~Строка (конец)~~

Не у всех сканеров есть

~~Отступ (начало)~~

Есть доступ к фрагменту кода

~~Отступ (конец)~~

Есть доступ к фрагменту кода

~~Совпадение~~

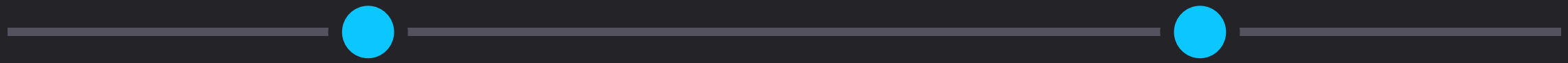
Разные подходы к определению

~~Секрет~~

Иногда маскированные

Коммит

Дедупликация: секреты (10 из 16)



Дедупликация: секреты (10 из 16)

Статус: **«Новый»**

super-file.txt

1	1	data:
2	2	+ - Sup3rMeGAP@ssw0rd

Дедупликация: секреты (10 из 16)

Статус: **«Новый»**

super-file.txt

1	1	data:
2	2	+ - Sup3rMeGAP@ssw0rd

Статус: **«Устранён»**

super-file.txt

1	1	data:
2	2	- - Sup3rMeGAP@ssw0rd

Дедупликация: секреты (10 из 16)

Статус: **«Новый»**

super-file.txt

1	1	data:
2	2	+ - Sup3rMeGAP@ssw0rd

Статус: **«Устранён»**

super-file.txt

1	1	data:
2	2	- - Sup3rMeGAP@ssw0rd

- Мы покажем, что ИБ-дефект устранен – в новом commit нет секрета
- Но секрет все равно хранится в репозитории

Дедупликация: секреты (11 из 16)

~~Описание~~

У всех будет своим

Файл

Однозначно – да!

Строка (начало)

Да, может быть полезно

~~Строка (конец)~~

Не у всех сканеров есть

~~Отступ (начало)~~

Есть доступ к фрагменту кода

~~Отступ (конец)~~

Есть доступ к фрагменту кода

~~Совпадение~~

Разные подходы к определению

~~Секрет~~

Иногда маскированные

Коммит

Это пригодится!

Автор

Дедупликация: секреты (12 из 16)

~~Описание~~

У всех будет своим

Файл

Однозначно – да!

Строка (начало)

Да, может быть полезно

~~Строка (конец)~~

Не у всех сканеров есть

~~Отступ (начало)~~

Есть доступ к фрагменту кода

~~Отступ (конец)~~

Есть доступ к фрагменту кода

~~Совпадение~~

Разные подходы к определению

~~Секрет~~

Иногда маскированные

Коммит

Это пригодится!

~~Автор~~

Не особо важно

Энтропия

Дедупликация: секреты (13 из 16)

~~Описание~~
У всех будет своим

Файл
Однозначно – да!

Строка (начало)
Да, может быть полезно

~~Строка (конец)~~
Не у всех сканеров есть

~~Отступ (начало)~~
Есть доступ к фрагменту кода

~~Отступ (конец)~~
Есть доступ к фрагменту кода

~~Совпадение~~
Разные подходы к определению

~~Секрет~~
Иногда маскированные

Коммит
Это пригодится!

~~Автор~~
Не особо важно

~~Энтропия~~
Какое значение брать?

Правило

Дедупликация: секреты (14 из 16)

~~Описание~~
У всех будет своим

Файл
Однозначно – да!

Строка (начало)
Да, может быть полезно

~~Строка (конец)~~
Не у всех сканеров есть

~~Отступ (начало)~~
Есть доступ к фрагменту кода

~~Отступ (конец)~~
Есть доступ к фрагменту кода

~~Совпадение~~
Разные подходы к определению

~~Секрет~~
Иногда маскированные

Коммит
Это пригодится!

~~Автор~~
Не особо важно

~~Энтропия~~
Какое значение брать?

~~Правило~~
У всех будет своим

Сообщение

Дедупликация: секреты (15 из 16)

~~Описание~~

У всех будет своим

Файл

Однозначно – да!

Строка (начало)

Да, может быть полезно

~~Строка (конец)~~

Не у всех сканеров есть

~~Отступ (начало)~~

Есть доступ к фрагменту кода

~~Отступ (конец)~~

Есть доступ к фрагменту кода

~~Совпадение~~

Разные подходы к определению

~~Секрет~~

Иногда маскированные

Коммит

Это пригодится!

~~Автор~~

Не особо важно

~~Энтропия~~

Какое значение брать?

~~Правило~~

У всех будет своим

~~Сообщение~~

У всех будет своим

Fingerprint

Дедупликация: секреты (16 из 16)

~~Описание~~
У всех будет своим

Файл
Однозначно – да!

Строка (начало)
Да, может быть полезно

~~Строка (конец)~~
Не у всех сканеров есть

~~Отступ (начало)~~
Есть доступ к фрагменту кода

~~Отступ (конец)~~
Есть доступ к фрагменту кода

~~Совпадение~~
Разные подходы к определению

~~Секрет~~
Иногда маскированные

Коммит
Это пригодится!

~~Автор~~
Не особо важно

~~Энтропия~~
Какое значение брать?

~~Правило~~
У всех будет своим

~~Сообщение~~
У всех будет своим

~~Fingerprint~~
Если только сканер «сам с собой»

Дедупликация: статический анализ (1 из 19)

Описание

Дедупликация: статический анализ (2 из 19)

~~Описание~~

У всех будет своим

Правило

Дедупликация: статический анализ (3 из 19)

~~Описание~~

У всех будет своим

Правило

Нужно для определения типа

Тип

Дедупликация: статический анализ (4 из 19)

~~Описание~~

У всех будет своим

Правило

Нужно для определения типа

Тип

Да, пригодится

Дедупликация: статический анализ (5 из 19)

Сканер №1

SQL Injection

Cryptographic Issues

Improper Authorization

Command Injection

Hard-coded Secrets

Дедупликация: статический анализ (5 из 19)

Сканер №1	Сканер №2
SQL Injection	hardcoded_sql_expressions
Cryptographic Issues	snmp_weak_cryptography
Improper Authorization	set_bad_file_permissions
Command Injection	subprocess_popen_with_shell_equals_true
Hard-coded Secrets	hardcoded_password_string
	hardcoded_password_funcarg
	hardcoded_password_default

Дедупликация: статический анализ (5 из 19)

Сканер №1		Сканер №2
SQL Injection	SQL-инъекция	hardcoded_sql_expressions
Cryptographic Issues	Ошибки при работе с криптографией	snmp_weak_cryptography
Improper Authorization	Некорректное управление доступом	set_bad_file_permissions
Command Injection	Внедрение кода	subprocess_popen_with_shell_equals_true
Hard-coded Secrets	Чувствительные данные в исходном коде	hardcoded_password_string
		hardcoded_password_funcarg
		hardcoded_password_default

Дедупликация: статический анализ (5 из 19)

AxeL pro

Сканер №1		Сканер №2
SQL Injection	SQL-инъекция	hardcoded_sql_expressions
Cryptographic Issues	Ошибки при работе с криптографией	snmp_weak_cryptography
Improper Authorization	Некорректное управление доступом	set_bad_file_permissions
Command Injection	Внедрение кода	subprocess_popen_with_shell_equals_true
Hard-coded Secrets	Чувствительные данные в исходном коде	hardcoded_password_string
		hardcoded_password_funcarg
		hardcoded_password_default

Правил может быть очень много*: несколько тысяч

* и тут нейронная сеть может быть полезна

Дедупликация: статический анализ (6 из 19)

~~Описание~~

У всех будет своим

Правило

Нужно для определения типа

Тип

Да, пригодится

Сообщение

Дедупликация: статический анализ (7 из 19)

~~Описание~~

У всех будет своим

Правило

Нужно для определения типа

Тип

Да, пригодится

~~Сообщение~~

У всех будет своим

Файл

Дедупликация: статический анализ (8 из 19)

~~Описание~

У всех будет своим

Правило

Нужно для определения типа

Тип

Да, пригодится

~~Сообщение~

У всех будет своим

Файл

Однозначно - да

Строка (начало)

Дедупликация: статический анализ (9 из 19)

~~Описание~~

У всех будет своим

Правило

Нужно для определения типа

Тип

Да, пригодится

~~Сообщение~~

У всех будет своим

Файл

Однозначно - да

~~Строка (начало)~~

Можно и без нее.
Да, все так!

Строка (конец)

Дедупликация: статический анализ (10 из 19)

~~Описание~~
У всех будет своим

Правило
Нужно для определения типа

Тип
Да, пригодится

~~Сообщение~~
У всех будет своим

Файл
Однозначно - да

~~Строка (начало)~~
Можно и без нее.
Да, все так!

~~Строка (конец)~~
Не у всех сканеров есть

Отступ (начало)

Дедупликация: статический анализ (11 из 19)

~~Описание~

У всех будет своим

Правило

Нужно для определения типа

Тип

Да, пригодится

~~Сообщение~

У всех будет своим

Файл

Однозначно - да

~~Строка (начало)~

Можно и без нее. Да, все так!

~~Строка (конец)~

Не у всех сканеров есть

~~Отступ (начало)~

Есть доступ к фрагменту кода

Отступ (конец)

Дедупликация: статический анализ (12 из 19)

~~Описание~~
У всех будет своим

Правило
Нужно для определения типа

Тип
Да, пригодится

~~Сообщение~~
У всех будет своим

Файл
Однозначно - да

~~Строка (начало)~~
Можно и без нее. Да, все так!

~~Строка (конец)~~
Не у всех сканеров есть

~~Отступ (начало)~~
Есть доступ к фрагменту кода

~~Отступ (конец)~~
Есть доступ к фрагменту кода

Фрагмент кода

Дедупликация: статический анализ (13 из 19)

Сканер №1

```
result = eval(expression)
```

Дедупликация: статический анализ (13 из 19)

Сканер №1

```
result = eval(expression)
```

Сканер №2

```
eval(expression)
```

Дедупликация: статический анализ (13 из 19)

Сканер №1 `result = eval(expression)`

Сканер №2 `eval(expression)`

Сканер №3 `expression = request.POST.get('expression’)\n result = eval(expression)`

Дедупликация: статический анализ (13 из 19)

Сканер №1 `result = eval(expression)`

Сканер №2 `eval(expression)`

Сканер №3 `expression = request.POST.get('expression’)\n result = eval(expression)`

`eval(...)`

Сохранение имени метода с указанием мета-информации о его переменных

Дедупликация: статический анализ (14 из 19)

AxeL pro

~~Описание~~ У всех будет своим	Правило Нужно для определения типа	Тип Да, пригодится	~~Сообщение~~ У всех будет своим
Файл Однозначно - да	~~Строка (начало)~~ Можно и без нее. Да, все так!	~~Строка (конец)~~ Не у всех сканеров есть	~~Отступ (начало)~~ Есть доступ к фрагменту кода
~~Отступ (конец)~~ Есть доступ к фрагменту кода	Фрагмент кода Да, но с нюансами	Трассы	

Дедупликация: статический анализ (15 из 19)

AxeL pro

~~Описание~~ У всех будет своим	**Правило** Нужно для определения типа	**Тип** Да, пригодится	~~Сообщение~~ У всех будет своим
Файл Однозначно - да	~~Строка (начало)~~ Можно и без нее. Да, все так!	~~Строка (конец)~~ Не у всех сканеров есть	~~Отступ (начало)~~ Есть доступ к фрагменту кода
~~Отступ (конец)~~ Есть доступ к фрагменту кода	**Фрагмент кода** Да, но с нюансами	~~Трассы~~ Идея хорошая, но всё разнородно	**Рекомендации**

Дедупликация: статический анализ (16 из 19)

~~Описание~~
У всех будет своим

Правило
Нужно для определения типа

Тип
Да, пригодится

~~Сообщение~~
У всех будет своим

Файл
Однозначно - да

~~Строка (начало)~~
Можно и без нее. Да, все так!

~~Строка (конец)~~
Не у всех сканеров есть

~~Отступ (начало)~~
Есть доступ к фрагменту кода

~~Отступ (конец)~~
Есть доступ к фрагменту кода

Фрагмент кода
Да, но с нюансами

~~Трассы~~
Идея хорошая, но всё разнородно

~~Рекомендации~~
У всех будут свои

CWE

Дедупликация: статический анализ (17 из 19)

AxeL pro

~~Описание~~ У всех будет своим	**Правило** Нужно для определения типа	**Тип** Да, пригодится	~~Сообщение~~ У всех будет своим
Файл Однозначно - да	~~Строка (начало)~~ Можно и без нее. Да, все так!	~~Строка (конец)~~ Не у всех сканеров есть	~~Отступ (начало)~~ Есть доступ к фрагменту кода
~~Отступ (конец)~~ Есть доступ к фрагменту кода	**Фрагмент кода** Да, но с нюансами	~~Трассы~~ Идея хорошая, но всё разнородно	~~Рекомендации~~ У всех будут свои
~~CWE~~ Соотношение на усмотрение автора	**Стандарты**		

Дедупликация: статический анализ (18 из 19)

~~Описание~~
У всех будет своим

Правило
Нужно для определения типа

Тип
Да, пригодится

~~Сообщение~~
У всех будет своим

Файл
Однозначно - да

~~Строка (начало)~~
Можно и без нее. Да, все так!

~~Строка (конец)~~
Не у всех сканеров есть

~~Отступ (начало)~~
Есть доступ к фрагменту кода

~~Отступ (конец)~~
Есть доступ к фрагменту кода

Фрагмент кода
Да, но с нюансами

~~Трассы~~
Идея хорошая, но всё разнородно

~~Рекомендации~~
У всех будут свои

~~CWE~~
Соотношение на усмотрение автора

~~Стандарты~~
Соотношение на усмотрение автора

Референсы

Дедупликация: статический анализ (19 из 19)

~~Описание~~
У всех будет своим

Правило
Нужно для определения типа

Тип
Да, пригодится

~~Сообщение~~
У всех будет своим

Файл
Однозначно - да

~~Строка (начало)~~
Можно и без нее. Да, все так!

~~Строка (конец)~~
Не у всех сканеров есть

~~Отступ (начало)~~
Есть доступ к фрагменту кода

~~Отступ (конец)~~
Есть доступ к фрагменту кода

Фрагмент кода
Да, но с нюансами

~~Трассы~~
Идея хорошая, но всё разнородно

~~Рекомендации~~
У всех будут свои

~~CWE~~
Соотношение на усмотрение автора

~~Стандарты~~
Соотношение на усмотрение автора

~~Референсы~~
У всех будут свои

Дедупликация: композиционный анализ (1 из 12)

Идентификатор уязвимости

Дедупликация: композиционный анализ (2 из 12)

Идентификатор уязвимости

Да, однозначно!

CWE

Дедупликация: композиционный анализ (3 из 12)

Идентификатор уязвимости

Да, однозначно!

~~CWE~~

Не всегда идентичные данные

Описание

Дедупликация: композиционный анализ (4 из 12)

Идентификатор уязвимости

Да, однозначно!

~~CWE~~

Не всегда идентичные данные

~~Описание~~

Могут отличаться

CVSS

Дедупликация: композиционный анализ (5 из 12)

Идентификатор уязвимости

Да, однозначно!

~~CWE~~

Не всегда идентичные данные

~~Описание~~

Могут отличаться

~~CVSS~~

Обычно несколько вариантов

Имя пакета

Дедупликация: композиционный анализ (6 из 12)

Идентификатор уязвимости

Да, однозначно!

~~CWE~~

Не всегда идентичные данные

~~Описание~~

Могут отличаться

~~CVSS~~

Обычно несколько вариантов

~~Имя пакета~~

Тепло…

Версия

Дедупликация: композиционный анализ (7 из 12)

Идентификатор уязвимости

Да, однозначно!

~~CWE~~

Не всегда идентичные данные

~~Описание~~

Могут отличаться

~~CVSS~~

Обычно несколько вариантов

~~Имя пакета~~

Тепло…

~~Версия~~

Теплее…

PURL

Дедупликация: композиционный анализ (8 из 12)

Идентификатор уязвимости

Да, однозначно!

~~CWE~~

Не всегда идентичные данные

~~Описание~~

Могут отличаться

~~CVSS~~

Обычно несколько вариантов

~~Имя пакета~~

Тепло…

~~Версия~~

Теплее…

PURL

Горячо! Берем!

Версия с устранением

Дедупликация: композиционный анализ (9 из 12)

Идентификатор уязвимости

Да, однозначно!

~~CWE~~

Не всегда идентичные данные

~~Описание~~

Могут отличаться

~~CVSS~~

Обычно несколько вариантов

~~Имя пакета~~

Тепло…

~~Версия~~

Теплее…

PURL

Горячо! Берем!

~~Версия с устранением~~

Не особо поможет

Дата публикации

Дедупликация: композиционный анализ (10 из 12)

Идентификатор уязвимости

Да, однозначно!

~~CWE~~

Не всегда идентичные данные

~~Описание~~

Могут отличаться

~~CVSS~~

Обычно несколько вариантов

~~Имя пакета~~

Тепло…

~~Версия~~

Теплее…

PURL

Горячо! Берем!

~~Версия с устранением~~

Не особо поможет

~~Дата публикации~~

Связано с ID уязвимости

Дата обновления

Дедупликация: композиционный анализ (11 из 12)

Идентификатор уязвимости

Да, однозначно!

~~CWE~~

Не всегда идентичные данные

~~Описание~~

Могут отличаться

~~CVSS~~

Обычно несколько вариантов

~~Имя пакета~~

Тепло…

~~Версия~~

Теплее…

PURL

Горячо! Берем!

~~Версия с устранением~~

Не особо поможет

~~Дата публикации~~

Связано с ID уязвимости

~~Дата обновления~~

Связано с ID уязвимости

Референсы

Дедупликация: композиционный анализ (12 из 12)

Идентификатор уязвимости

Да, однозначно!

~~CWE~~

Не всегда идентичные данные

~~Описание~~

Могут отличаться

~~CVSS~~

Обычно несколько вариантов

~~Имя пакета~~

Тепло…

~~Версия~~

Теплее…

PURL

Горячо! Берем!

~~Версия с устранением~~

Не особо поможет

~~Дата публикации~~

Связано с ID уязвимости

~~Дата обновления~~

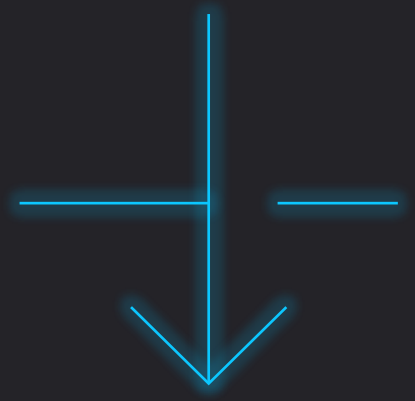
Связано с ID уязвимости

~~Референсы~~

Могут отличаться

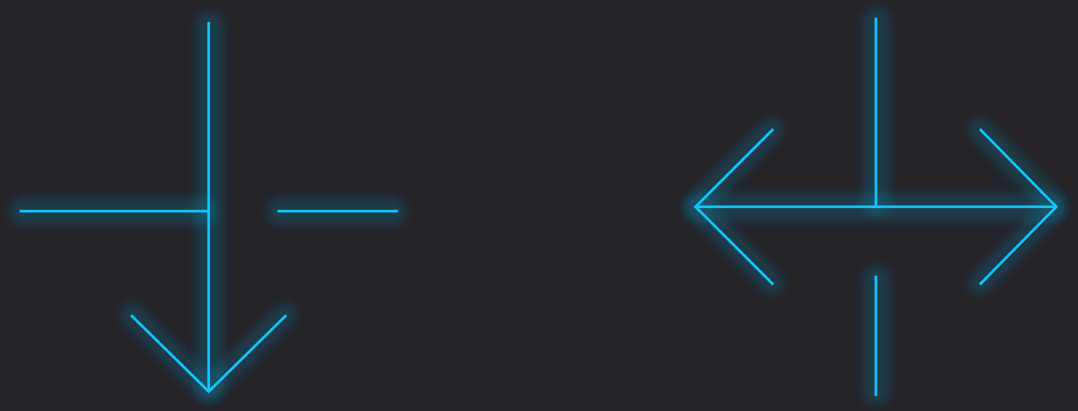
Дедупликация: что еще важно?

Дедупликация: что еще важно?



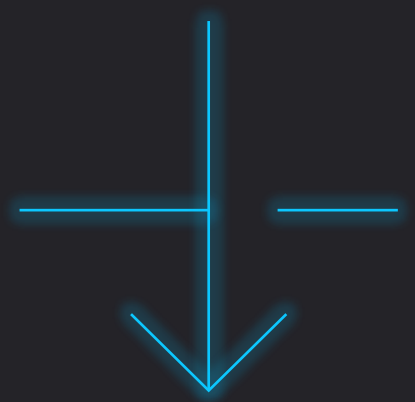
Сам с собой

Дедупликация: что еще важно?



Сам с собой С «другом»

Дедупликация: что еще важно?



Сам с собой **С «другом»** **По веткам**

Использование нескольких сканеров: выводы

Может быть полезно для:

- Поиска секретов (решение задачи пропусков)
- Статического анализа (пригодится далее), но важно помнить, что помимо «дублей» мы получим уникальные ложные срабатывания

Практически бесполезно для:

- Композиционного анализа

Дедупликация:

- Помогает сократить количество ИБ-дефектов для разметки
- Добиться 100% практически нереально, что обусловлено нюансами работы сканеров

Много шума: что можно сделать?

Много шума: что можно сделать?

Невероятно, но факт – **использовать возможности сканеров** и выбирать нужные!*

- *Определить инструменты*
- *Определить конфигурацию и параметры настройки инструментов*
- *Осуществлять пересмотр конфигурации и параметров настройки инструментов*

* про ML мы все еще не говорим, да и до разметки пока не дошли

Настройка сканеров для сокращения «шума»

- Секреты

Настройка сканеров для сокращения «шума»

- Секреты
  - Отключить не релевантные правила

Настройка сканеров для сокращения «шума»

- Секреты
  - Отключить не релевантные правила
  - Выставить уровень энтропии

Настройка сканеров для сокращения «шума»

Секреты

- Отключить не релевантные правила
- Выставить уровень энтропии
- Добавить собственные правила

Настройка сканеров для сокращения «шума»

Секреты

- Отключить не релевантные правила
- Выставить уровень энтропии
- Добавить собственные правила
- Проверка валидности секретов

Настройка сканеров для сокращения «шума»

- Секреты
- Статический анализ

Настройка сканеров для сокращения «шума»

- Секреты
- Статический анализ
  - Управлять директориями анализа

Настройка сканеров для сокращения «шума»

- Секреты
- Статический анализ
  - Управлять директориями анализа
  - Управлять набором правил

Настройка сканеров для сокращения «шума»

- Секреты
- Статический анализ
  - Управлять директориями анализа
  - Управлять набором правил
  - Добавить собственные правила

Настройка сканеров для сокращения «шума»

- Секреты
- Статический анализ
- Композиционный анализ

Настройка сканеров для сокращения «шума»

- Секреты
- Статический анализ
- Композиционный анализ
- Создавать максимально точный SBOM

Настройка сканеров для сокращения «шума»

- Секреты
- Статический анализ
- Композиционный анализ
  - Создавать максимально точный SBOM
  - Не анализировать build, development-зависимости

Отсутствие указателей: что можно сделать?

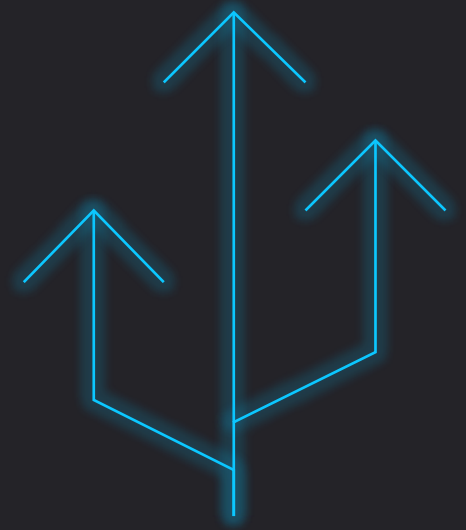
Отсутствие указателей: что можно сделать?

Обратиться к **другим процессам РБПО** и некоторым **«продвинутым» способам анализа***

* вот тут ML местами показывает себя очень хорошо!

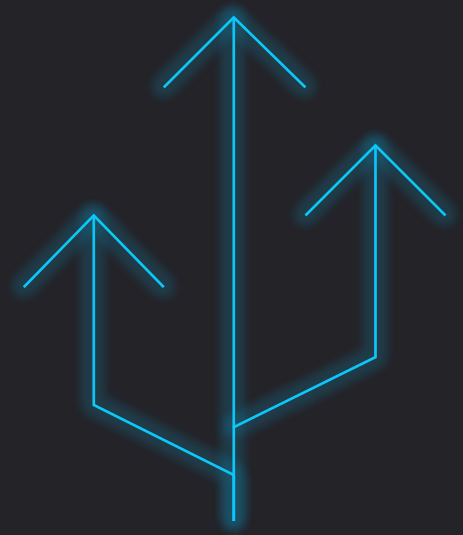
Например, можно сделать 2 шага

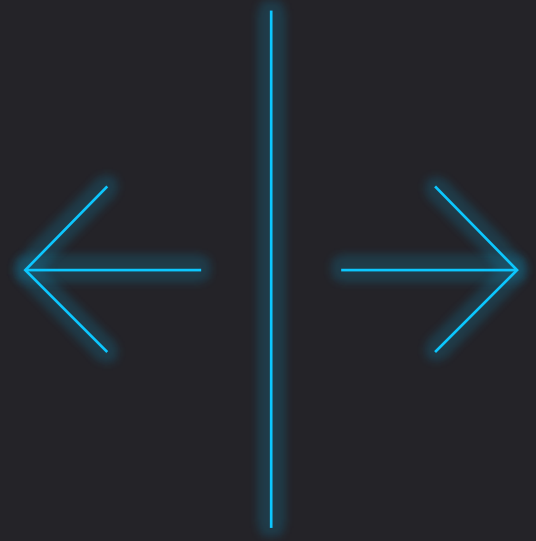
Например, можно сделать 2 шага



Куда идти?

Например, можно сделать 2 шага





Куда идти?

Что делать?

Куда идти? (1 из 2)

5.7 Моделирование угроз и разработка описания поверхности атаки

- Выполнить первичное моделирование угроз для ПО
- Выполнить первичное описание поверхности атаки
- Выполнить первичное описание функций безопасности*
- Выполнить первичное описание интерфейсов*

* добавил немного от себя

Куда идти? (1 из 2)

5.7 Моделирование угроз и разработка описания поверхности атаки

- Выполнить первичное моделирование угроз для ПО
- Выполнить первичное описание поверхности атаки
- Выполнить первичное описание функций безопасности*
- Выполнить первичное описание интерфейсов*

Это позволит определить вектор движения – куда стоит «бросаться» в первую очередь. Нюанс в том, что **это не всегда просто сделать.** Особенно в начале

* добавил немного от себя

Куда идти? (2 из 2)

Оценка рисков анализируемых сущностей

```
(K1*Count(Critical) + K2*Count(High) + K3*Count(Medium) + K4*Count(Low))*Value
```

Где:

- K1…K4 – коэффициенты (например, 10, 8, 4, 2)
- Value – уровень ценности ПО

Куда идти? (2 из 2)

Оценка рисков анализируемых сущностей

```
(K1*Count(Critical) + K2*Count(High) + K3*Count(Medium) + K4*Count(Low))*Value
```

Где:

- K1…K4 – коэффициенты (например, 10, 8, 4, 2)
- Value – уровень ценности ПО

Это тоже позволит определить вектор движения – куда стоит «бросаться» в первую очередь. Сделать это чуть проще, но менее результативно

Что делать? (1 из 2)

Теорема Кондорсе о присяжных*

Если **каждый член** жюри присяжных имеет независимое мнение, и если **вероятность** правильного решения члена жюри **больше 0.5**, то тогда **вероятность правильного решения** присяжных в целом **возрастает с увеличением количества членов жюри**, и стремится к единице

Работает и наоборот 😅 «Нет в мире совершенства!» (с) Лис

* https://en.wikipedia.org/wiki/Condorcet%27s_jury_theorem

Что делать? (2 из 2)

Допущение: мы уже «отсекли» много лишнего, используя возможности сканеров

Что делать? (2 из 2)

Допущение: мы уже «отсекли» много лишнего, используя возможности сканеров

- Обращать внимание на то, что «схлопнулось». Не панацея, но шанс (на мой взгляд) больше

Что делать? (2 из 2)

Допущение: мы уже «отсекли» много лишнего, используя возможности сканеров

- Обращать внимание на то, что «схлопнулось». Не панацея, но шанс (на мой взгляд) больше
- Обращать внимание на наиболее «страшные» типы ошибок (уязвимостей)

Что делать? (2 из 2)

Допущение: мы уже «отсекли» много лишнего, используя возможности сканеров

- Обращать внимание на то, что «схлопнулось». Не панацея, но шанс (на мой взгляд) больше
- Обращать внимание на наиболее «страшные» типы ошибок (уязвимостей)
- Повторно использовать разметку, но вдумчиво и аккуратно

Что делать? (2 из 2)

Допущение: мы уже «отсекли» много лишнего, используя возможности сканеров

- Обращать внимание на то, что «схлопнулось». Не панацея, но шанс (на мой взгляд) больше
- Обращать внимание на наиболее «страшные» типы ошибок (уязвимостей)
- Повторно использовать разметку, но вдумчиво и аккуратно
- Использовать расширенные возможности сканеров (анализ достижимости, трассы и т.д.)

Что делать? (2 из 2)

Допущение: мы уже «отсекли» много лишнего, используя возможности сканеров

- Обращать внимание на то, что «схлопнулось». Не панацея, но шанс (на мой взгляд) больше
- Обращать внимание на наиболее «страшные» типы ошибок (уязвимостей)
- Повторно использовать разметку, но вдумчиво и аккуратно
- Использовать расширенные возможности сканеров (анализ достижимости, трассы и т.д.)
- Применять ML (но мы сегодня не о нём)

Трудности перевода: что можно сделать?

Трудности перевода: что можно сделать?

Научиться понимать других: их образ мысли, их цели, их приоритеты, их «ритуалы», их образ жизни

Разработчики: что хочется?

AXEL pro

Зачем, что, в привычном «окружении»

Учиться, учиться и еще раз учиться!

5.2 Обучение сотрудников

- Проводить анализ существующих обучающих курсов и тренингов по разработке безопасного ПО
- Разрабатывать план обучения **с учетом потребностей разработчика**
- Проводить обучение сотрудников

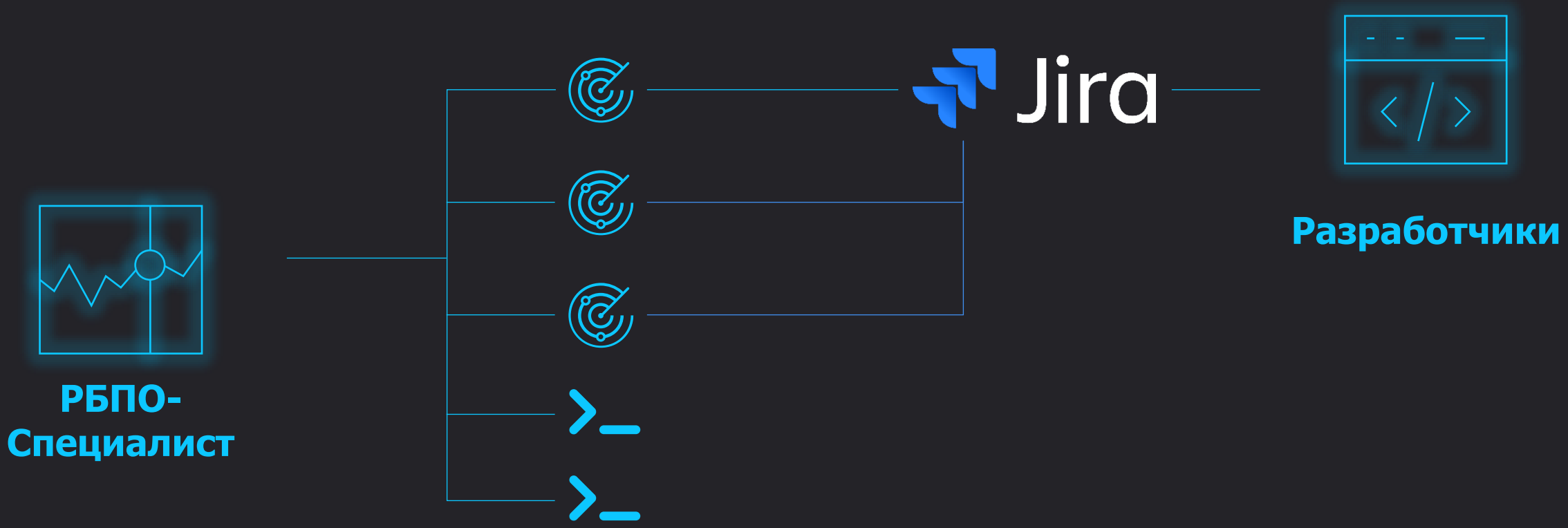
Учиться, учиться и еще раз учиться!

5.2 Обучение сотрудников

- Проводить анализ существующих обучающих курсов и тренингов по разработке безопасного ПО
- Разрабатывать план обучения **с учетом потребностей разработчика**
- Проводить обучение сотрудников

Дополнительно можно реализовывать практики создания **Security Champions, AppSec Business Partners,** но сегодня не об этом

Использовать привычные инструменты!



Менеджмент: что хочется?

У нас **всё хорошо** или **всё плохо**?

Типичный процесс подготовки отчетности

- Скачать отчет сканера

Типичный процесс подготовки отчетности

- Скачать отчет сканера
- Эм… перевести JSON в 

Типичный процесс подготовки отчетности

- Скачать отчет сканера
- Эм… перевести JSON в 
- Немного формул…

Типичный процесс подготовки отчетности

- Скачать отчет сканера
- Эм… перевести JSON в 
- Немного формул…
- Скачать второй отчет

Типичный процесс подготовки отчетности

- Скачать отчет сканера
- Эм… перевести JSON в 
- Немного формул…
- Скачать второй отчет
- Повезло! Стоп… Иные данные?

Типичный процесс подготовки отчетности

- Скачать отчет сканера
- Эм… перевести JSON в 
- Немного формул…
- Скачать второй отчет
- Повезло! Стоп… Иные данные?
- ГРАААААФИКИ!!!

Проблемы роста: что можно сделать?

Проблемы роста: что можно сделать?

А что если **взглянуть на всё** то, о чем **мы сегодня говорили** – возможно, что там мы **найдем ответ?**

Собираем всё вместе!

Источники данных

Собираем всё вместе!

Источники данных

Репозиторий

Собираем всё вместе!

Источники данных

Репозиторий

Образы

Собираем всё вместе!

Источники данных

Репозиторий

Образы

Стенды

Собираем всё вместе!

AXEL pro

Источники данных

Репозиторий

Образы

Стенды

Конвейер

Собираем всё вместе!

Источники данных


Репозиторий

Образы


Стенды


Конвейер

Собираем всё вместе!

Источники данных

Анализ

Репозиторий

Образы

Стенды

Конвейер

Собираем всё вместе!

Источники данных

- Репозиторий
- Образы
- Стенды
- Конвейер

Анализ

Поиск секретов

Собираем всё вместе!

Axel pro

Источники данных

- Репозиторий
- Образы
- Стенды
- Конвейер

Анализ

- Поиск секретов
- Статический анализ

Собираем всё вместе!

Источники данных

- Репозиторий
- Образы
- Стенды
- Конвейер

Анализ

- Поиск секретов
- Статический анализ
- Композиционный анализ

Собираем всё вместе!

Axel pro

Источники данных

- Репозиторий
- Образы
- Стенды
- Конвейер
- ...

Анализ

- Поиск секретов
- Статический анализ
- Композиционный анализ
- ...

Собираем всё вместе!

Axel pro

Источники данных

Анализ

Работа с результатами

Репозиторий

Образы

Стенды

Конвейер

Поиск секретов

Статический анализ

Композиционный анализ

Собираем всё вместе!

Источники данных

Анализ

Работа с результатами


Репозиторий

Образы


Стенды


Конвейер

Поиск секретов

Статический анализ

Композиционный анализ

Консолидация

Собираем всё вместе!

Axel pro

Источники данных


Репозиторий

Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

Консолидация

Нормализация

Собираем всё вместе!

Axel pro

Источники данных


Репозиторий

Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

Консолидация

Нормализация

Дедупликация

Собираем всё вместе!

AxeL pro

Источники данных


Репозиторий

Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

Консолидация

Нормализация

Дедупликация

Максимум информации

Собираем всё вместе!

AxeL pro

Источники данных

- Репозиторий
- Образы
- Стенды
- Конвейер
- ● ● ●

Анализ

- Поиск секретов
- Статический анализ
- Композиционный анализ
- ● ● ●

Работа с результатами

- Консолидация
- Нормализация
- Дедупликация
- Максимум информации
- Работа с результатами

Собираем всё вместе!

AxeL pro

Источники данных


Репозиторий

Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

- Консолидация
- Нормализация
- Дедупликация
- Максимум информации
- Работа с результатами
- Управление правилами

Собираем всё вместе!

AXEL pro

Источники данных


Репозиторий

Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

- Консолидация
- Нормализация
- Дедупликация
- Максимум информации
- Работа с результатами
- Управление правилами
- Управление задачами

Собираем всё вместе!

AxeL pro

Источники данных


Репозиторий

Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

- Консолидация
- Нормализация
- Дедупликация
- Максимум информации
- Работа с результатами
- Управление правилами
- Управление задачами
- Контроль SLA

Собираем всё вместе!

AxeL pro

Источники данных


Репозиторий


Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

- Консолидация
- Нормализация
- Дедупликация
- Максимум информации
- Работа с результатами
- Управление правилами
- Управление задачами
- Контроль SLA
- Контекст

Собираем всё вместе!

AXEL pro

Источники данных


Репозиторий


Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

- Консолидация
- Нормализация
- Дедупликация
- Максимум информации
- Работа с результатами
- Управление правилами
- Управление задачами
- Контроль SLA
- Контекст
- Анализ рисков

Собираем всё вместе!

AXEL pro

Источники данных


Репозиторий


Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

- Консолидация
- Нормализация
- Дедупликация
- Максимум информации
- Работа с результатами
- Управление правилами
- Управление задачами
- Контроль SLA
- Контекст
- Анализ рисков
- База знаний

Собираем всё вместе!

AXEL pro

Источники данных


Репозиторий

Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

Консолидация	Нормализация	Дедупликация
Максимум информации	Работа с результатами	Управление правилами
Управление задачами	Контроль SLA	Контекст
Анализ рисков	База знаний	Генерация отчетности

Собираем всё вместе!

AXEL pro

Источники данных

- Репозиторий
- Образы
- Стенды
- Конвейер
- ● ● ●

Анализ

- Поиск секретов
- Статический анализ
- Композиционный анализ
- ● ● ●

Работа с результатами

- Консолидация
- Нормализация
- Дедупликация
- Максимум информации
- Работа с результатами
- Управление правилами
- Управление задачами
- Контроль SLA
- Контекст
- Анализ рисков
- База знаний
- Генерация отчетности
- Визуализация данных

Собираем всё вместе!

AXEL pro

Источники данных


Репозиторий

Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

- Консолидация
- Нормализация
- Дедупликация
- Максимум информации
- Работа с результатами
- Управление правилами
- Управление задачами
- Контроль SLA
- Контекст
- Анализ рисков
- База знаний
- Генерация отчетности
- Визуализация данных
- ...

Собираем всё вместе!

AXEL pro

Источники данных


Репозиторий

Образы


Стенды


Конвейер

Анализ

Поиск секретов

Статический анализ

Композиционный анализ

Работа с результатами

Консолидация	Нормализация	Дедупликация
Максимум информации	Работа с результатами	Управление правилами
Управление задачами	Контроль SLA	Контекст
Анализ рисков	База знаний	Генерация отчетности
Визуализация данных	...	...

Собираем всё вместе!

AXEL pro

Источники данных

- Репозиторий
- Образы
- Стенды
- Конвейер
- ● ● ●

Анализ

- Поиск секретов
- Статический анализ
- Композиционный анализ
- ● ● ●

Работа с результатами

Консолидация	Нормализация	Дедупликация
Максимум информации	Работа с результатами	Управление правилами
Управление задачами	Контроль SLA	Контекст
Анализ рисков	База знаний	Генерация отчетности
Визуализация данных	...	...

О чем мы сегодня поговорим?

Контекст

Проблематика

Решение

Выводы

И это, но мой взгляд, и есть Процесс №5.+

Централизованная работа с ошибками (уязвимостями), выявленными сканерами при разработке безопасного программного обеспечения

А что вы думаете по этому поводу?

Спасибо!

Антон Гаврилов
gavrilov@axel.pro
+7 929 653 42 90

С радостью отвечу на ваши вопросы!!!