

Баланс скорости разработки и безопасности: конфликт интересов бизнеса и специалистов РБПО

Дмитрий Шаньгин

Технический директор
ЦЗИ ГК «Конфидент»

Станислав Воскресенский

Руководитель центра компетенций
ЦЗИ ГК «Конфидент»



Конфликт интересов

Безопасники хотят



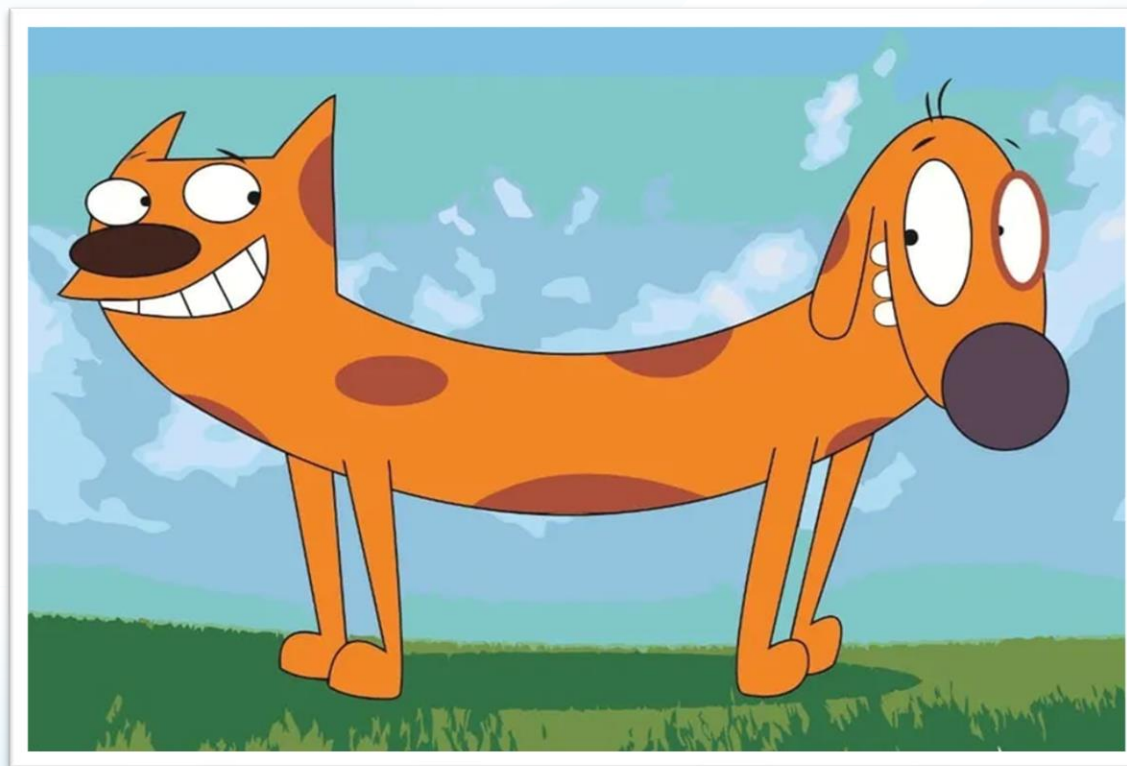
Команду побольше



Инструменты подороже



Сроки подольше



Бизнес хочет



Сроки покороче

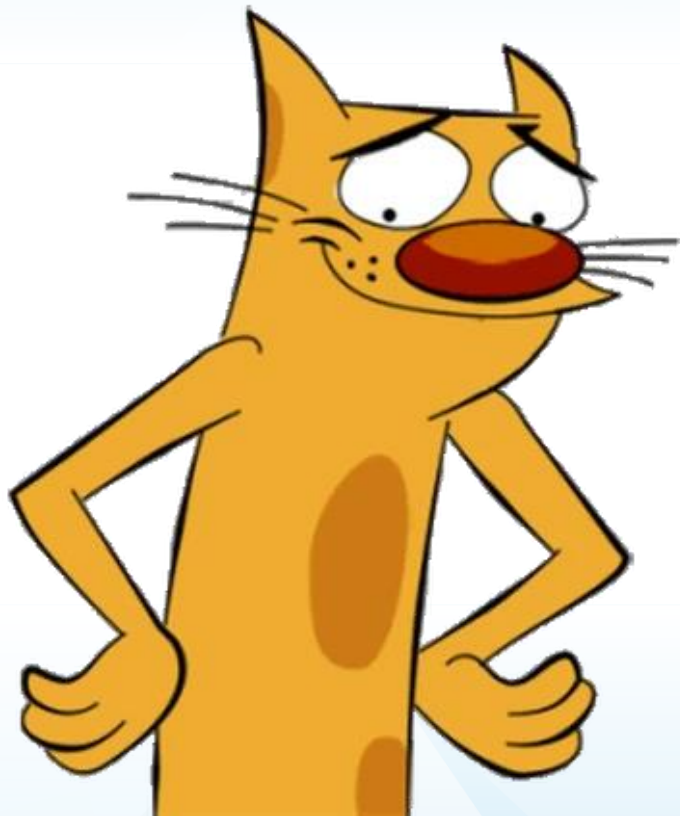


Сертификаты



Прибыль

Конфликты



Разработка: «хотим разрабатывать, а не углубляться в безопасность»



Документаторы: «нам бы успеть основной комплект документов оформить»



Сроки: «давайте побыстрее»



Бизнес: «мы уже все продали, где сертификат?»



Цена: «инструменты дорогие, специалисты – очень дорогие»

Дорогие инструменты

Ряд технологий анализа архитектуры и кода ПО качественно реализуются только проприетарными инструментами анализа, в которые вложены огромные средства и сотни человеко-лет экспертизы высококлассных ученых и инженеров.

Освоим сначала бесплатные инструменты, затем озаботимся покупкой действительно мощных, дорогих решений.

В то же время существуют практики, в первую очередь требующие творческого подхода, в частности фаззинг, для которых Open source предлагает огромный выбор решений, полностью закрывающих потребности неопитов.



Наши инструменты



Сборка и автоматизация сборки

Bitbucket, Jenkins, Conan



Статический анализ

Svace, Svacer



Динамический анализа

AFL++, WinAFL, DynamoRIO, Valgrind



Анализ уязвимостей

Burp Suite, OWASP ZAP, XSpider, NMap, KaliLinux



Архитектурный анализ

Trivy, Dependency-Track

libcurl

7.79.1

EXTERNAL

3

9

15

2

3

View Details

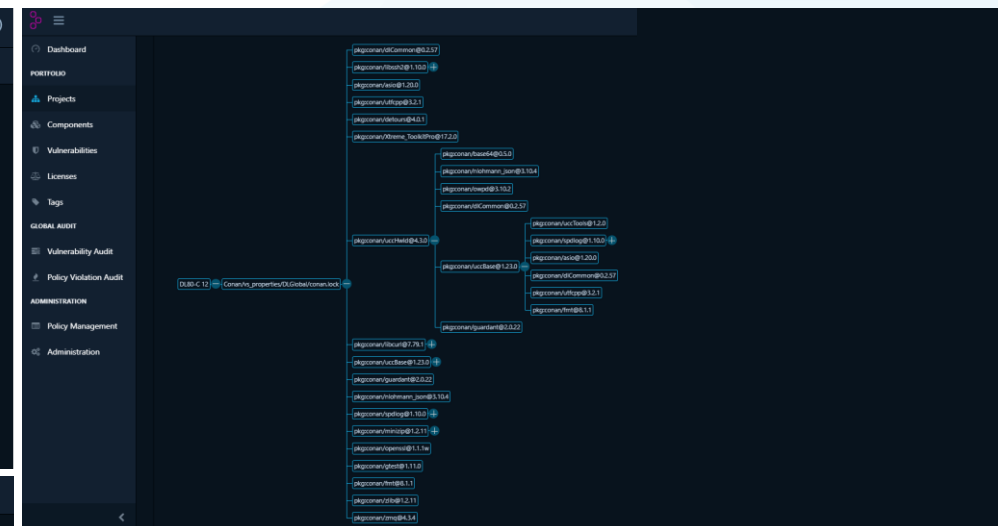
Overview

Vulnerabilities 32

Projects also used in

Search

Name	Published	CWE	Severity
CVE-2022-32207	7 Jul 2022	CWE-276	Critical
CVE-2022-32221	6 Dec 2022	CWE-668	Critical
CVE-2023-38545	18 Oct 2023	CWE-787	Critical
CVE-2022-27781	2 Jun 2022	CWE-835	High
CVE-2022-27782	2 Jun 2022	CWE-295	High
CVE-2022-27775	2 Jun 2022	-	High
CVE-2022-22576	26 May 2022	CWE-306	High



- + Открытый код
- + Прост в развертывании
- Не поддерживает БДУ ФСТЭК из коробки

Команда

Чтобы закрыть потребности
бизнеса, нужна большая
команда безопасников



Команда

Давай лучше наладим тесный
контакт команды информационной
безопасности и отдела
тестирования. А еще заведем в
командах разработки секьюрити
чемпионов



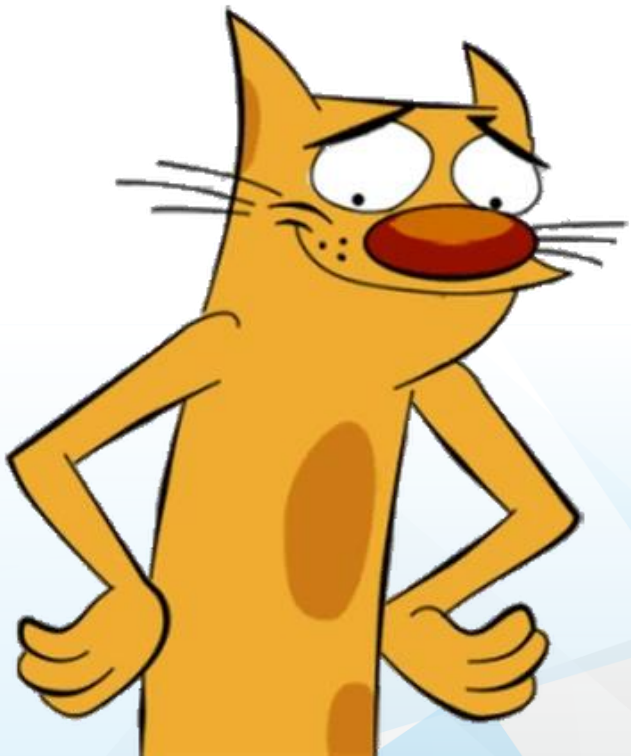
Где брать технических писателей?

 **ПОЛИТЕХ**

УНИВЕРСИТЕТ ИТМО



СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ



Проблемы обучения



Мало курсов переподготовки



Кандидатам на обучение нужен диплом о высшем образовании



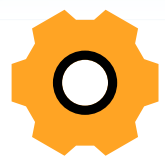
Трудно применить полученные знания на продуктах компании

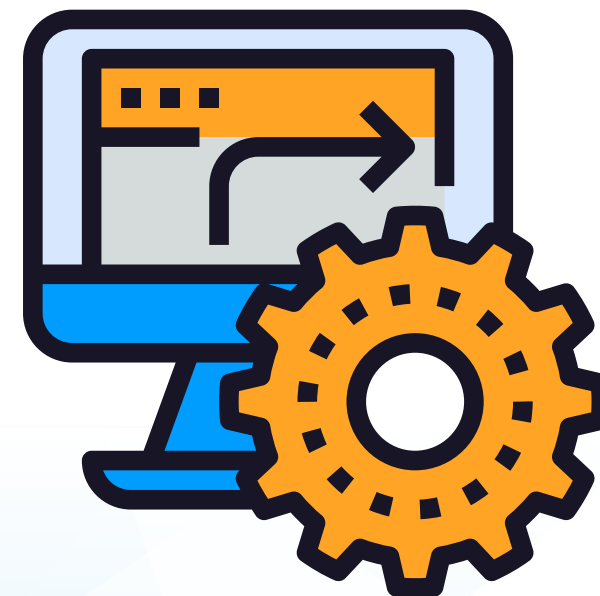


Отрасль развивается быстрее, чем курсы переподготовки специалистов



Автоматизация на службе сертификации

-  Автоматическое развертывание стендов
-  Автоматическое тестирование
-  Автоматическое построение SBOM
-  Фаззинг-конвейер



Что удалось?



Сократить сроки сертификации
приблизительно в 3-4 раза



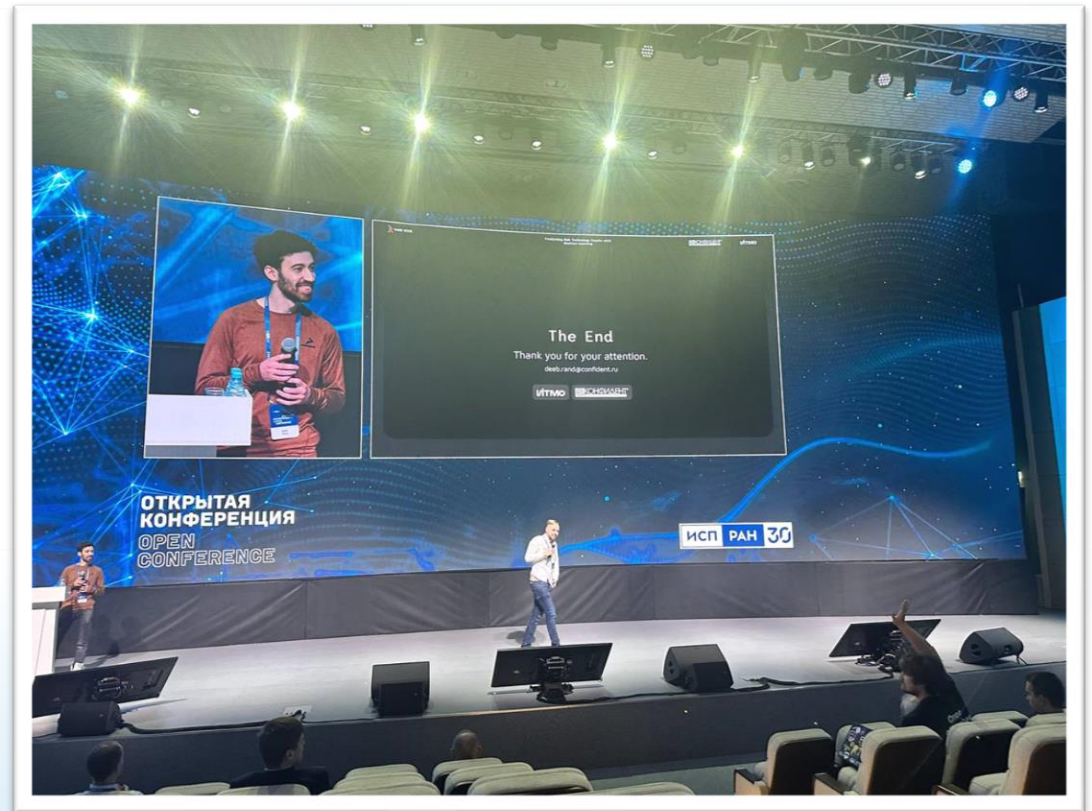
Воспитать квалифицированных
сотрудников с институтской скамьи



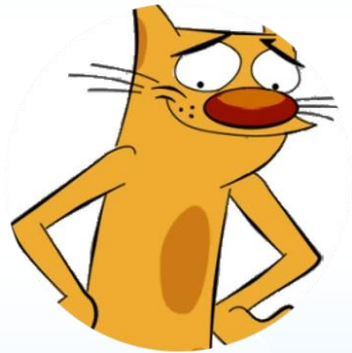
Выступить силами наших сотрудников на
ISPRAS OPEN 2024 с докладом



Подать заявку на сертификацию
процессов безопасной разработки по
ГОСТ 56939-2024

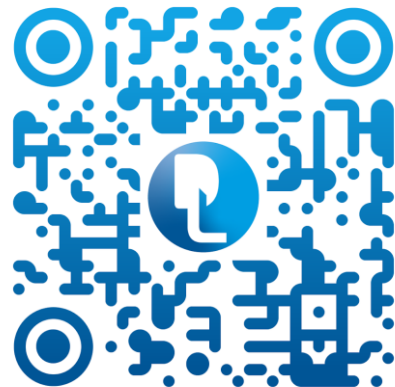


Приглашаем в наш телеграм-канал!



Дмитрий Шаньгин

Технический директор
ЦЗИ ГК «Конфидент»



Станислав Воскресенский

Руководитель центра компетенций
ЦЗИ ГК «Конфидент»

