Как SDL формирует будущее компании

Коренберг Марк Михайлович
Технический директор ООО «Айдеко»

О компании Ideco

Ideco — российский разработчик решений для защиты корпоративных сетей от кибератак и фильтрации трафика.

2005 год основания

5500+ компаний-заказчиков

250+ сотрудников в команде

4 мажорных релиза каждый год

Соответствие требованиям регулятора

Сертификат ФСТЭК №4503 от 28.12.2021 г.

+ Требования доверия (4)
+ Требования к МЭ
+ Требования к СОВ
+ Профиль защиты МЭ (А 4-го класса защиты ИТ.МЭ.А4.ПЗ)
+ Профиль защиты МЭ (Б 4-го класса защиты ИТ.МЭ.Б4.ПЗ)
+ Профиль защиты СОВ (4-го класса защиты ИТ.СОВ.С4.ПЗ)

Сертификат ФСБ

Ведем работы
по сертификации ГОСТ VPN

Решение входит
в реестр российского ПО
Минцифры РФ

Сертификат NGFW

Ведем работы по сертификации
на требования к NGFW

Линейка сертифицированных аппаратных платформ

Высокопроизводительные платформы для бизнеса любого масштаба.

Ideco SX+ ФСТЭК

до 100 активных пользователей интернет

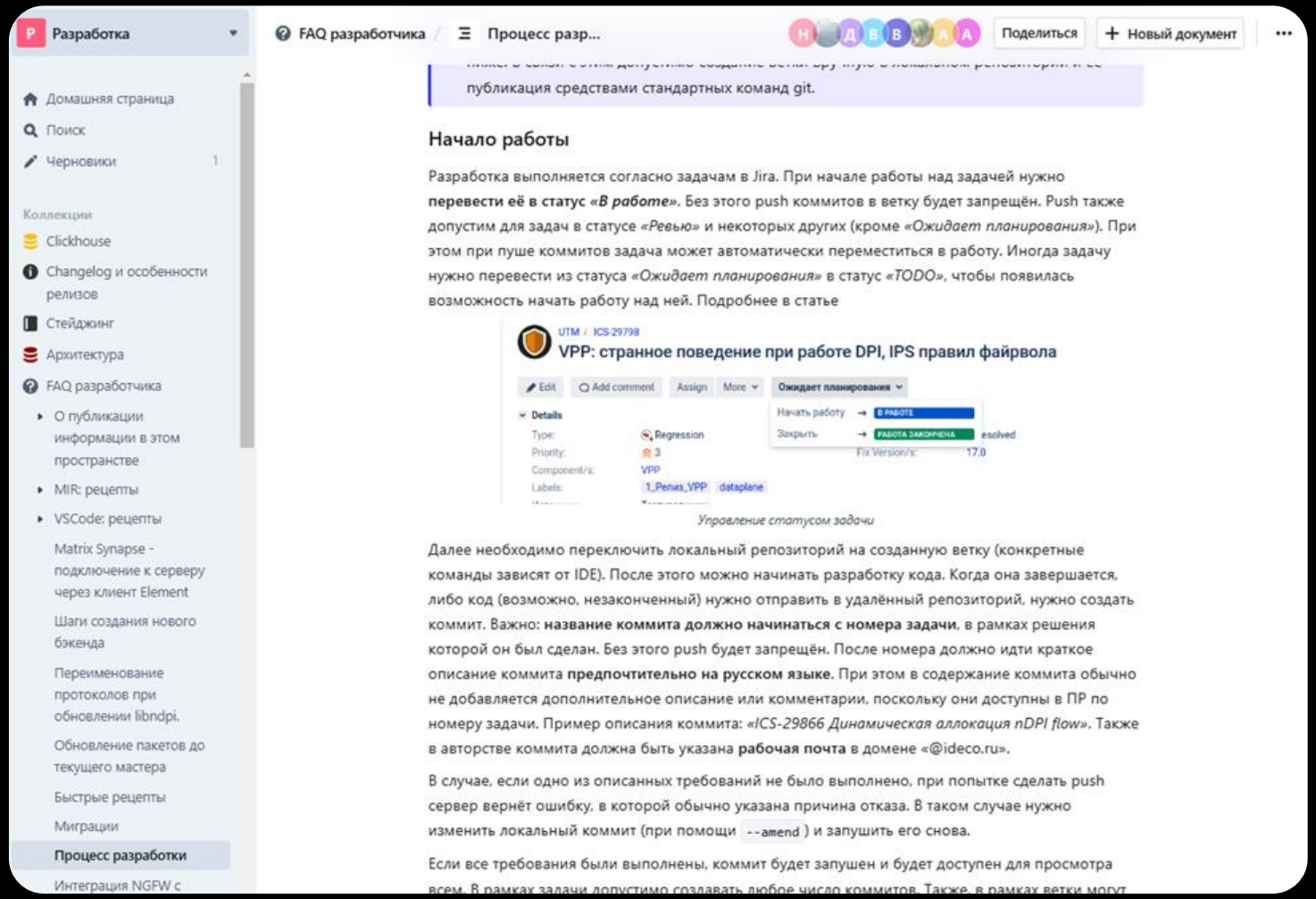
Ideco LX ФСТЭК

от 300 до 1000 активных пользователей интернет

Ideco EX ФСТЭК

для крупных компаний, дата-центров и высоконагруженных сетей

Security Development Lifecycle – процесс разработки



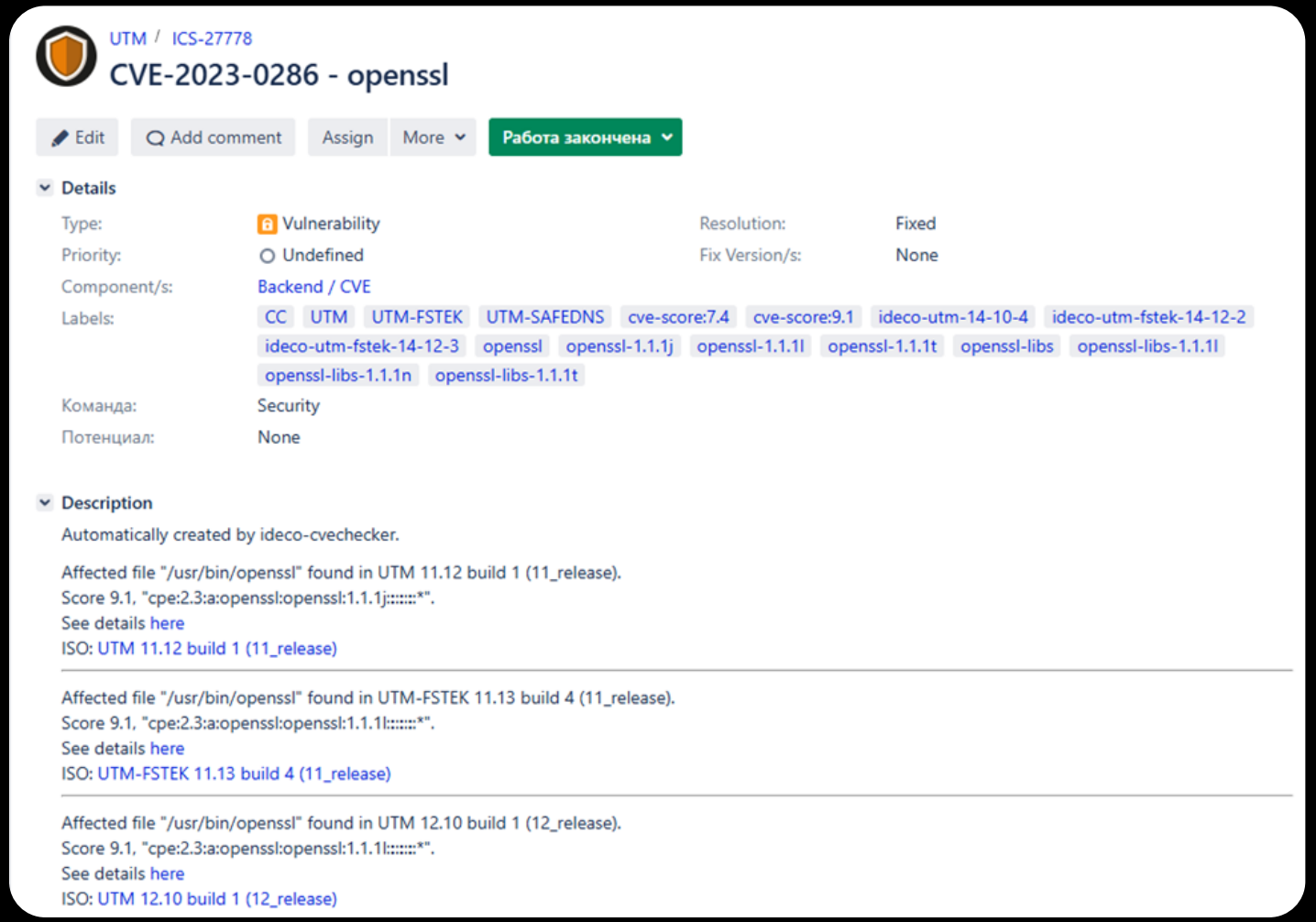
Несмотря на многообразие компаний, методик оценки и мнений, несложно выделить базовые различия в компетенциях при продвижении по карьерному треку. Ниже представлен обзор общепринятых грейдов в индустрии для роли software engineer (indi vidual contributor):

- Intern Software Engineer / Разработчик-стажёр
- Junior Software Engineer / Младший разработчик
- [Middle] Software Engineer / Разработчик
- Senior Software Engineer / Старший разработчик
- Staff Software Engineer / Ведущий разработчик

Компетенции и карьерный трек управленческих позиций: engineering manager, director of engineering, VP of engineering, CTO — не входят в рамки обзора.

Уровень	Навыки	Деятельность	Зоны роста
Intern Software Engineer / Разработчик-стажёр без опыта	Обладает базовыми техническими знаниями, необходимыми для работы: - знание языка программирования (Java/Python/JavaScript/C++); - умение работать с системами контроля версий (Git, SVN); - понимание принципов ООП и паттернов проектирования, принципов работы операционной системы, компьютерных сетей, клиент-серверных приложений; - основы работы с базами данных. От стажёров не ожидается безупречных знаний в каждой из этих областей, но базовое понимание перечисленного облегчит работу на первых порах.	Решает лёгкие задачи из бэклога команды. Перед началом работы над задачей консультируется с наставником — проговаривает суть проблемы и предполагаемое решение. Самостоятельно ищет ответы на возникающие вопросы, но обращается к наставнику, если заходит в тупик. Старается выполнить взятую задачу в срок, вовремя сообщает о возникающих проблемах.	Изучает лучшие практики разработки, code review, тестирования, ci/cd. Знакомится с процессами компании, учится работать в команде. Активно изучает новые технологии, составляет план развития по советам наставника.
Junior Software Engineer / Младший разработчик	Тот же набор навыков, что описан в секции стажёра. Отличие в том, что с большинством областей уже есть небольшой практический опыт, в идеале сопровождаемый более глубокими теоретическими познаниями.	Решает лёгкие и средние задачи из бэклога с малой степенью неопределённости, занимается исправлением несложных багов. Как правило, работает только с уже проработанными	Активно изучает кодовую базу проектов, накапливает знания об имеющихся механизмах, модулях, API и предметной области.

Security Development Lifecycle – сборка



Автоматизировано:

+ Пересборка всего
+ Автоматический поиск CVE после сборки и создание задач в Jira
+ Unit-, интеграционные и нагрузочные тесты
+ Запуск линтеров
+ Автоматический запуск статического анализа Svace’ом и фаззинг-тестирования (AFL++, syzkaller, pyfuzz, Go-Fuzz)
+ Анализ cppchecker’ом и ossaudit’ом

Исследование Clang

ideco

Объем дискового пространства, занимаемого компилятором Clang, сокращен на 83%

Сам компилятор удалось ускорить на 25% на тестах llvm-lit

Реализована изоляция процесса компиляции, позволяющая ограничить доступ компилятора к следующим ресурсам:

+ системные вызовы;
+ файловая система;
+ оперативная память;
+ процессорное время;
+ сеть.

##	system clang	minimized clang
# 50 rules		
task-clock:u,msec	1,885.17	1,772.47
page-faults:u	22,616	17,225
cycles:u	4,086,991,141	3,876,692,759
instructions:u	3,308,537,300	3,151,656,140
branches:u	628,559,978	605,888,596
branch-misses:u	13,669,351	13,431,089
# 100 rules		
task-clock:u,msec	2,072.36	1,953.07
page-faults:u	23,109	17,722
cycles:u	4,512,246,826	4,288,287,221
instructions:u	3,910,559,990	3,739,260,591
branches:u	746,460,521	722,407,287
branch-misses:u	16,160,156	15,903,207
# 500 rules		
task-clock:u,msec	2,818.43	2,696.09
page-faults:u	28,419	22,988
cycles:u	6,187,706,025	5,957,729,245
instructions:u	6,304,356,638	6,083,309,728
branches:u	1,208,835,544	1,180,488,457
branch-misses:u	23,103,854	23,160,918

# 1000 rules		
task-clock:u,msec	4,297.51	4,129.53
page-faults:u	37,853	32,556
cycles:u	9,515,906,117	9,181,346,471
instructions:u	10,850,001,664	10,554,816,677
branches:u	2,095,999,133	2,061,517,726
branch-misses:u	40,134,331	39,517,168
# 5000 rules		
task-clock:u,msec	27,377.00	26,818.44
page-faults:u	113,768	107,271
cycles:u	61,877,112,647	60,665,706,582
instructions:u	69,317,970,419	68,439,013,289
branches:u	13,694,140,192	13,608,305,308
branch-misses:u	280,977,496	280,021,954
# 10000 rules		
task-clock:u,msec	82,735.14	82,197.12
page-faults:u	230,719	224,981
cycles:u	187,998,859,985	186,845,729,337
instructions:u	202,837,019,424	201,712,677,526
branches:u	40,479,352,603	40,411,265,526
branch-misses:u	877,315,709	883,140,252

Немного в цифрах

ideco

Фаззинг-тестирование

Найдено и исправлено – **13**
В апстрим отправлено – **3**

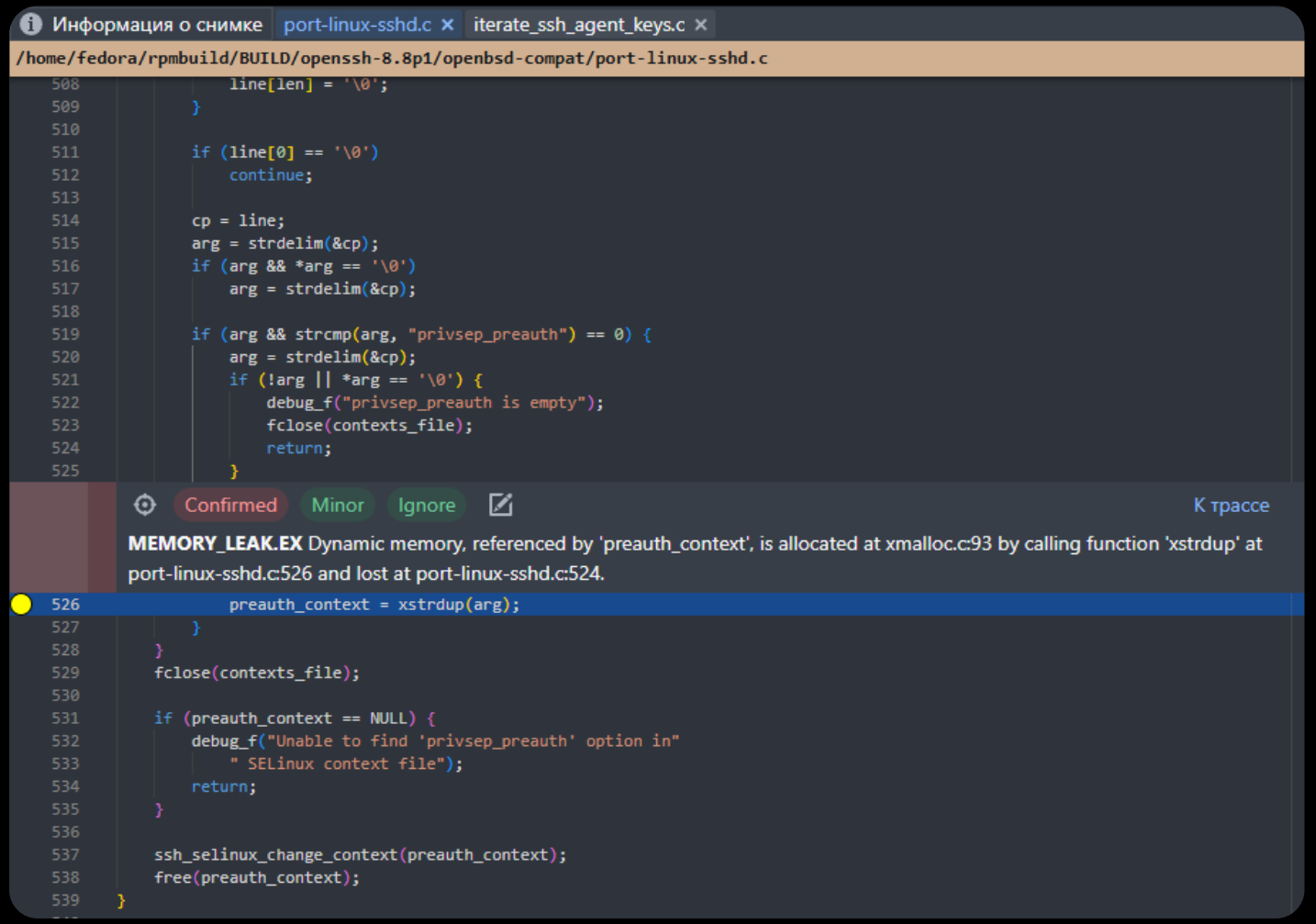
Статический анализ

Найдено и исправлено – **36**
В апстрим отправлено – **2**

CVE-уязвимости

Найдено и исправлено – **13**

Примеры



/etc/selinux/targeted/contexts/openssh_contexts

privsep_preauth=sshd_net_t

К чему мы пришли

ideco

Регулярное обновление используемых open sousce библиотек

Регулярная проверка библиотек по открытым базам данных (bdu.fstek.ru, cve.mitre.org)

Регулярная проверка кода статическими анализаторами

Статический анализ не может найти все проблемы в коде

ideco СОЗДАЕМ ВМЕСТЕ

Коренберг Марк Михайлович
Технический директор ООО «Айдеко»

e-mail: mmarkk@ideco.ru
tg: @socketpair