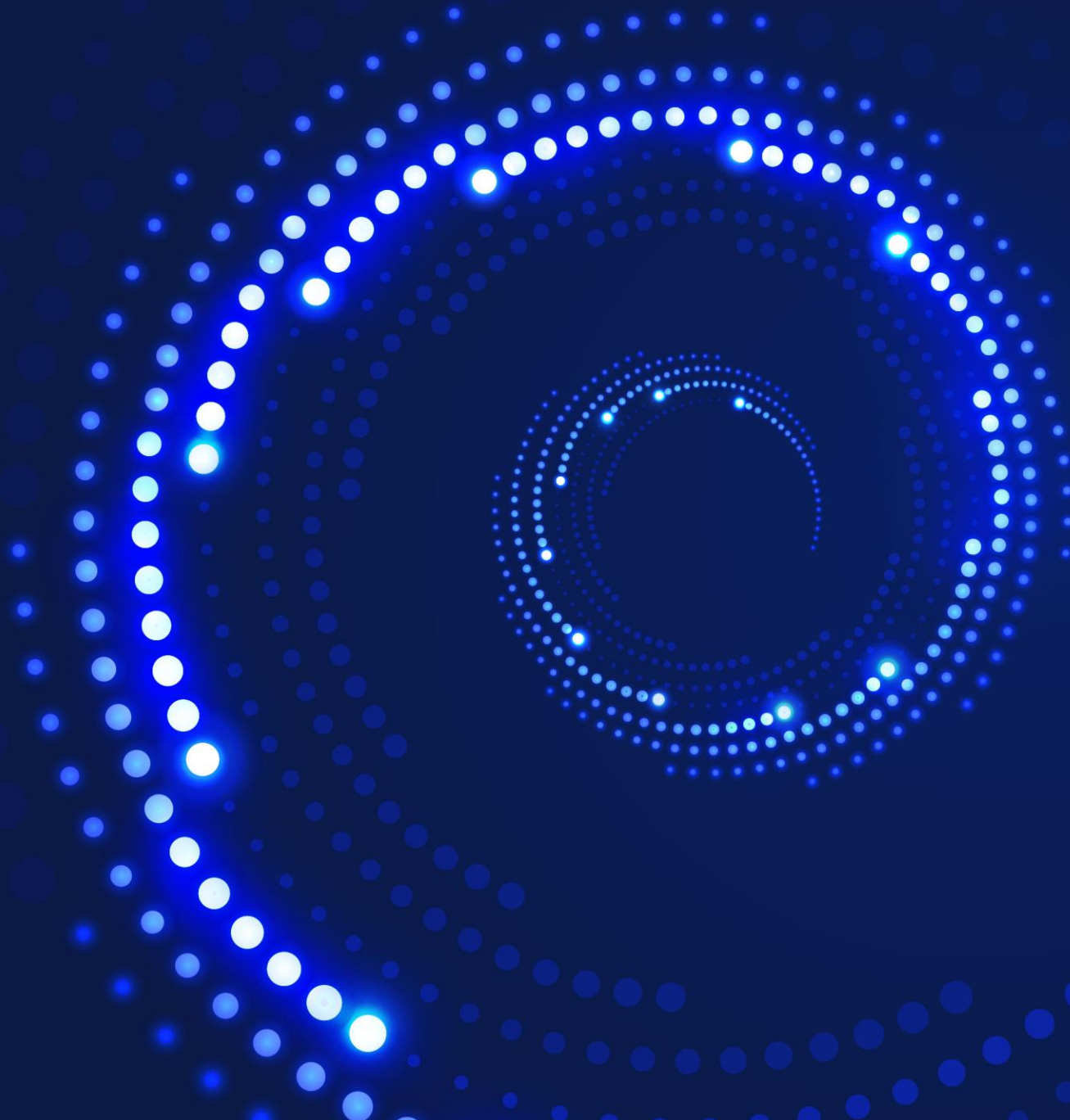


# R-Vision

## Тернистый путь построения процессов SDL



МАКСИМ КАРЧЕВСКИЙ  
Руководитель GR-направления  
R-Vision  
[mkarchevskiy@rvision.ru](mailto:mkarchevskiy@rvision.ru)



# КТО МЫ?

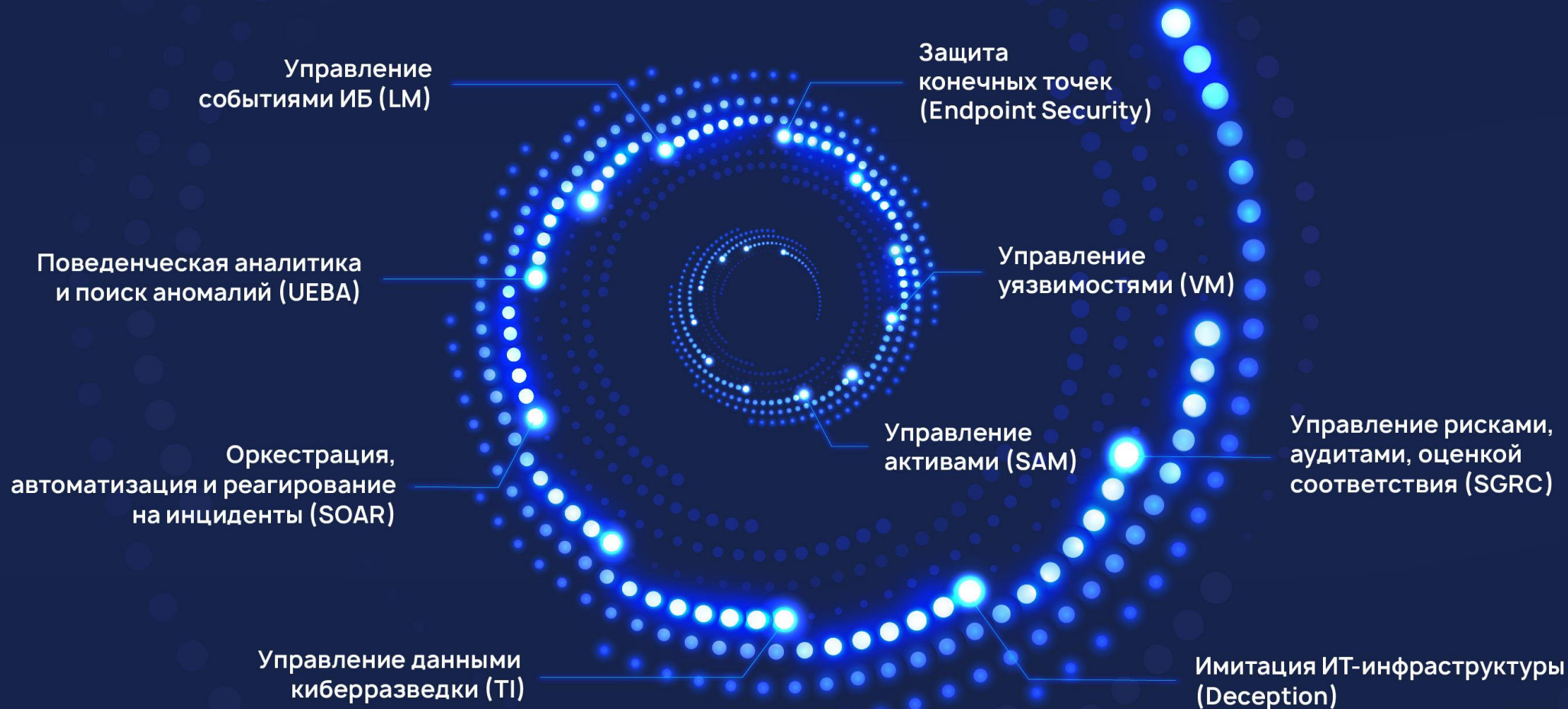
R-Vision работает с 2011 года и специализируется на решениях, автоматизирующих ключевые процессы в ИБ:

- ✓ **Управление ИТ-активами и уязвимостями**
- ✓ **Мониторинг и реагирование на инциденты**
- ✓ **Использование данных о киберугрозах**
- ✓ **Выявление и предупреждение кибератак**
- ✓ **Риск-менеджмент**
- ✓ **Контроль соответствия требованиям (аудиты)**



# R-Vision EVO

Экосистема технологий для эволюции SOC

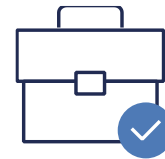


# Подходы к внедрению SDL



## Соответствие требованиям

- ✓ Внешний аудит
- ✓ Сертификация программных продуктов



## Польза для бизнеса

- ✓ Улучшение процессов разработки
- ✓ Повышение качества и безопасности продуктов

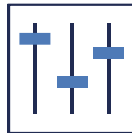
# Затраты на «джентельменский набор»



Статические  
анализаторы



Контроль внешних  
компонентов (SCA)



Динамические  
анализаторы



Тестирование  
на проникновение  
(pentest)

- ✓ Вычислительные ресурсы (особенно на фаззинг)
- ✓ Трудозатраты команд AppSec и разработки
- ✓ Покупка проприетарного ПО\*

# Трудозатраты команды AppSec и разработки

- Один «Человек-оркестр» не справится с построением SDL (в вакансиях компании часто указывают требования к кандидату «динамический анализ, статический анализ, DevSecOps, web-фаззинг, pentester и др.»)
- Часть задач приходится решать команде разработки (например, обновление уязвимых зависимостей, написание фаззинг-оберток и т.д.)



# Ограничения open-source продуктов\*

Отсутствует тех поддержка при интеграции, использовании

→ Пишем «костыли» командой AppSec

Баги, ошибки open-source решений исправляются медленней, есть риск, что продукт перестанет поддерживаться

→ Пишем «костыли» командой AppSec

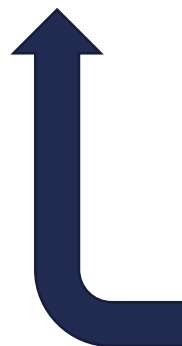
Не всегда являются универсальными для нескольких технологий или языков программирования

→ Ищем и внедряем множество продуктов под каждый ЯП

Не всегда позволяют полностью покрывать требования статического анализа

→ Количество найденных уязвимостей и классификация предупреждений богаче у проприетарного ПО

# На первом этапе – большой backlog задач по устранению уязвимостей



A screenshot of a Jira issue backlog for 'My open issues'. The interface includes a navigation bar with 'Dashboards', 'Projects', 'Issues', 'Boards', 'Structure', 'Service Desk', 'R-Desk', and 'More' menus, along with a 'Create' button. The main content area shows a filter: 'type = Vulnerability AND project = "R-Vision TIP" ORDER BY reporter DESC, summary ASC, priority ASC, cf[13704] ASC'. Below the filter is a list of five issues, each with a red vulnerability icon, a key ID, a summary, and an assignee 'Bender'. The issues are:

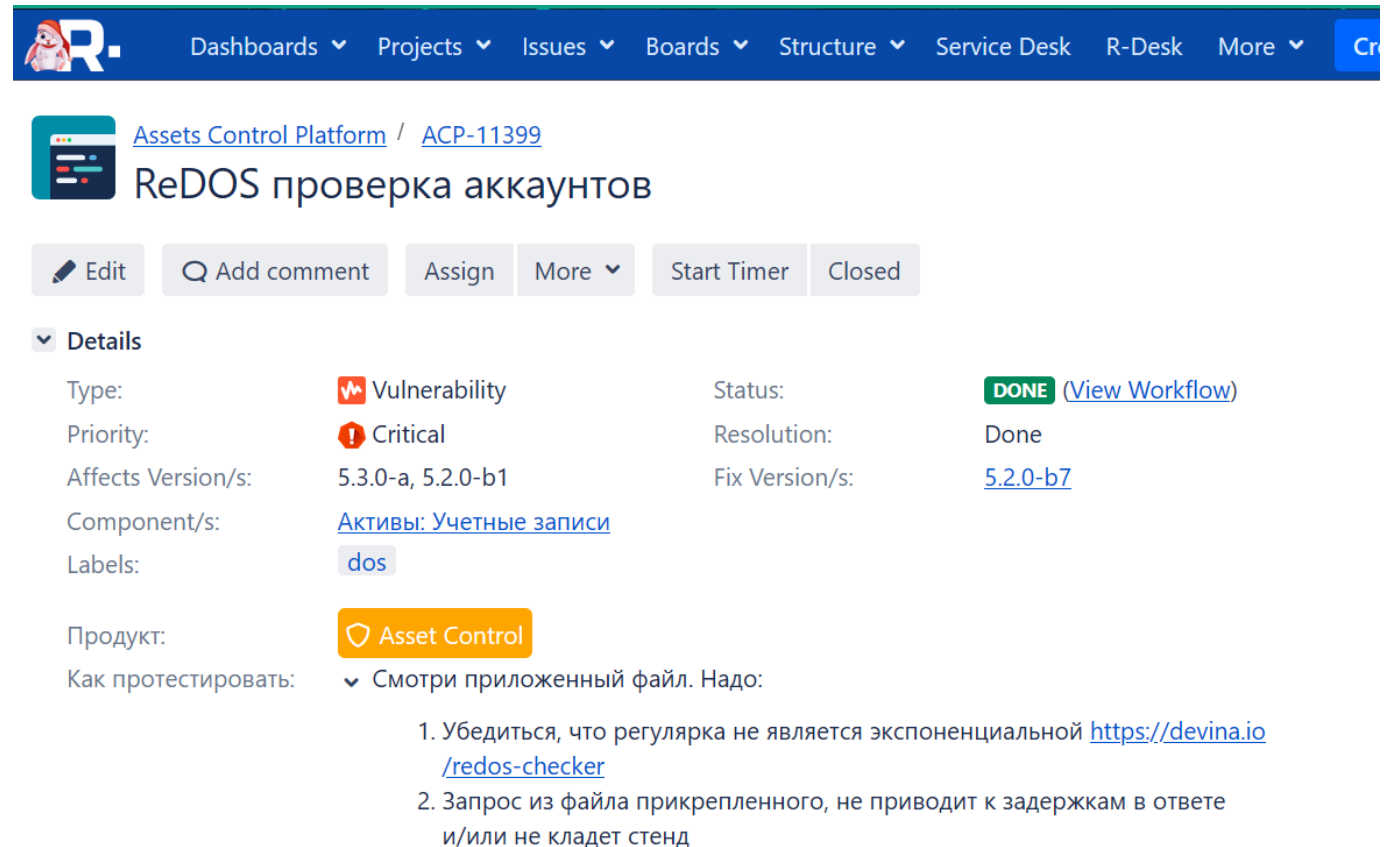
- TIP-2948 [AUTH] Redis:2.8.0 | Node-Redis Is a Node.js Redis Client. Before Version 3.1.1, When a Client Is in Monitoring Mode, the Regex Begin Used to Detected Monitor Messages Could Cause Exponential Backtracking on Some Strings. This Issue Could Lead to a Denia
- TIP-5150 [AUTH] fastify:3.24.1 | 1085030
- TIP-5165 [AUTH] fastify:3.24.1 | CVE-2022-41919
- TIP-3973 [AUTH] minimist:1.2.5 | Minimist <=1.2.5 Is Vulnerable to Prototype Pollution via File index.js, Function setKey().(Lines 69-95).(in minimist:1.2.5)
- TIP-3974 [AUTH] moment:2.29.1 | Moment.js Is a JavaScript Date Library for Parsing, Validating, Manipulating, and Formatting Dates. A Path

At the bottom of the screenshot, the text 'Showing results 51-100 of 404' is visible, with '404' highlighted in a pink box.



# Продукт становится стабильнее

Пример выявленной уязвимости при обработке регулярных выражений, которая позволяла осуществить dos-атаку с любой учетной записи



The screenshot shows a Jira issue page for 'ReDOS проверка аккаунтов' (ACP-11399) under the 'Assets Control Platform' project. The issue is marked as 'DONE' and has a status of 'Done'. The details include:

- Type: Vulnerability
- Priority: Critical
- Affects Version/s: 5.3.0-a, 5.2.0-b1
- Fix Version/s: 5.2.0-b7
- Component/s: Активы: Учетные записи
- Labels: dos
- Product: Asset Control
- How to reproduce: Смотря приложенный файл. Надо:
  1. Убедиться, что регулярка не является экспоненциальной <https://devina.io/redos-checker>
  2. Запрос из файла прикрепленного, не приводит к задержкам в ответе и/или не кладет стэнд

# Унификация в языках и внешних компонентах



Node.js 16.10.0

Node.js 14.21.0

Node.js 12.22.3

Node.js 12.16.3

Node.js 10.22.1



Node.js 16.13.0

# Дисциплинированность разработчиков



Тимлиды несут за себя и команду ответственность, когда жмут на кнопку «merge»

# Польза для бизнеса

- ✓ Возможность «не краснея» отдавать продукт в enterprise
- ✓ Снижение рисков внезапного появления критических уязвимостей
- ✓ Повышение стабильности продукта
- ✓ Унификация в языках, пакетах, внешних компонентах
- ✓ Рост качества кода разработчиков



# R-Vision

Благодарю  
за внимание!

 + 7 (499) 322 80 40

 [sales@rvision.ru](mailto:sales@rvision.ru)

 [rvision.ru](http://rvision.ru)

Подписывайтесь на наш  
бесплатный дайджест ИБ:  
[rvision.ru /blog](http://rvision.ru/blog)