R-Vision

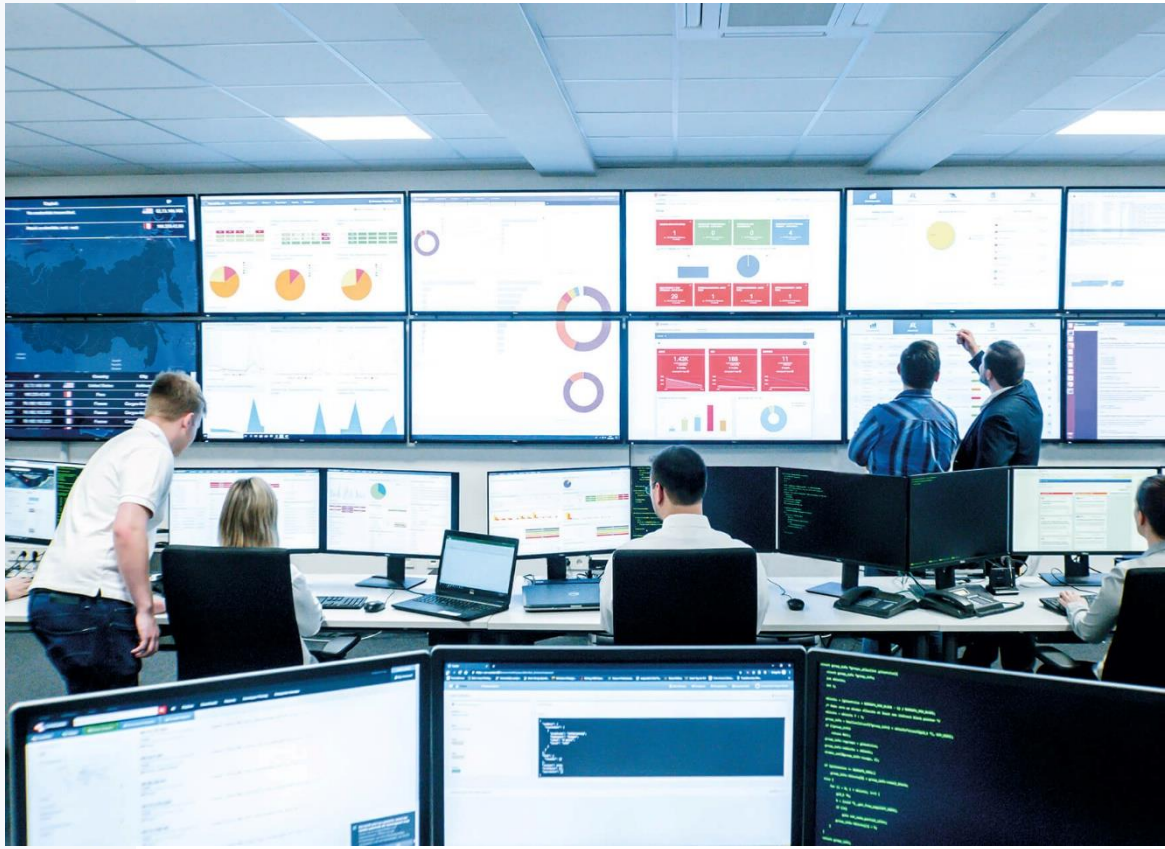
Тернистый путь построения процессов SDL

МАКСИМ КАРЧЕВСКИЙ
Руководитель GR-направления
R-Vision
mkarchevskiy@rvision.ru

Кто мы?

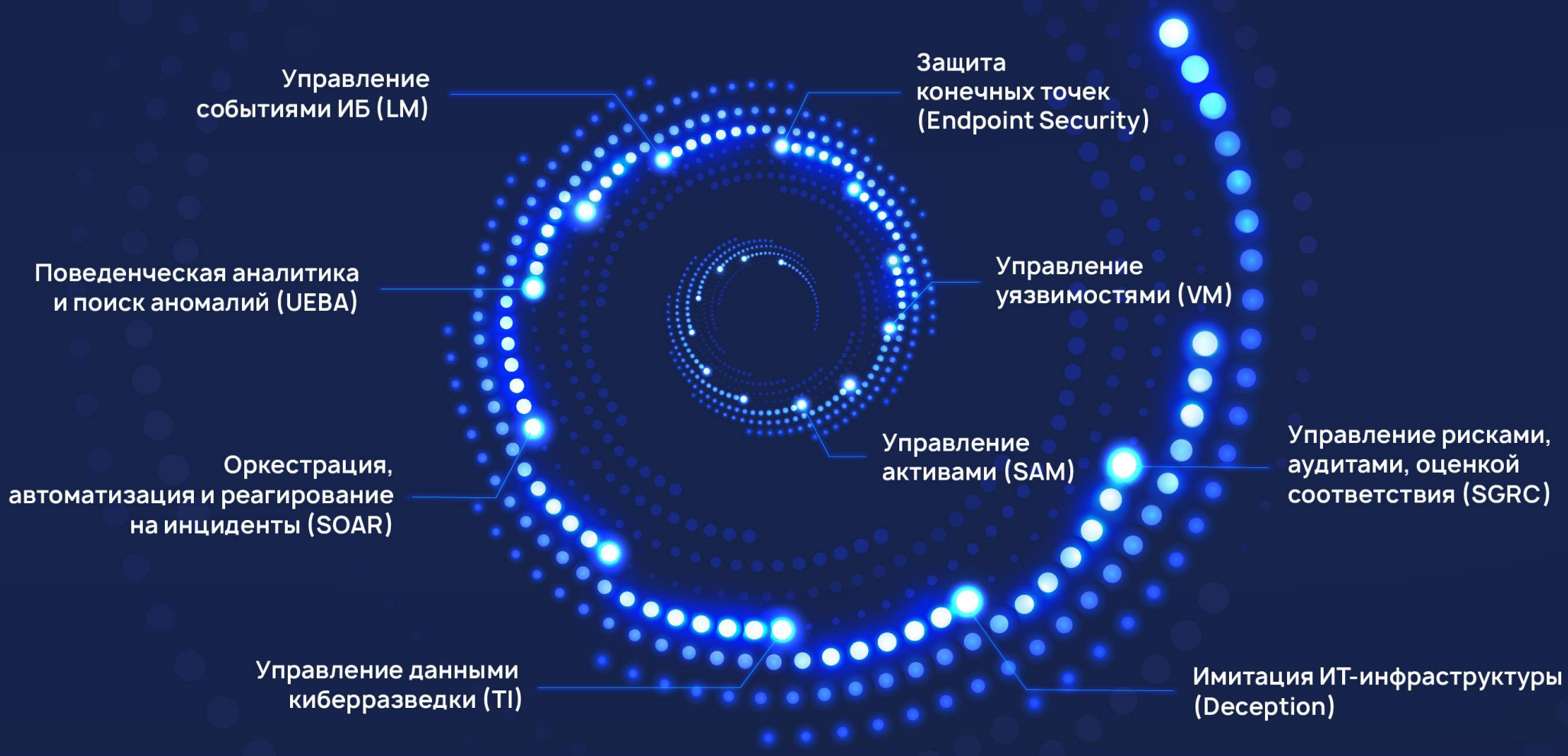
R-Vision работает с 2011 года
и специализируется на решениях,
автоматизирующих ключевые процессы в ИБ:

- ✓ **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

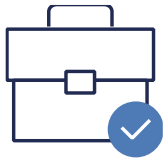
Экосистема технологий для эволюции SOC



Подходы к внедрению SDL

Соответствие требованиям

- ✓ Внешний аудит
- ✓ Сертификация программных продуктов



Польза для бизнеса

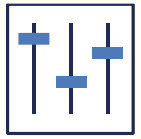
- ✓ Улучшение процессов разработки
- ✓ Повышение качества и безопасности продуктов

Затраты на «джентельменский набор»

Статические анализаторы

Контроль внешних компонентов (SCA)

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



Динамические анализаторы

Тестирование на проникновение (pentest)

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

Dashboards Projects Issues Boards Structure Service Desk R-Desk More Create

My open issues EDITED Save as ••• PDF No sc

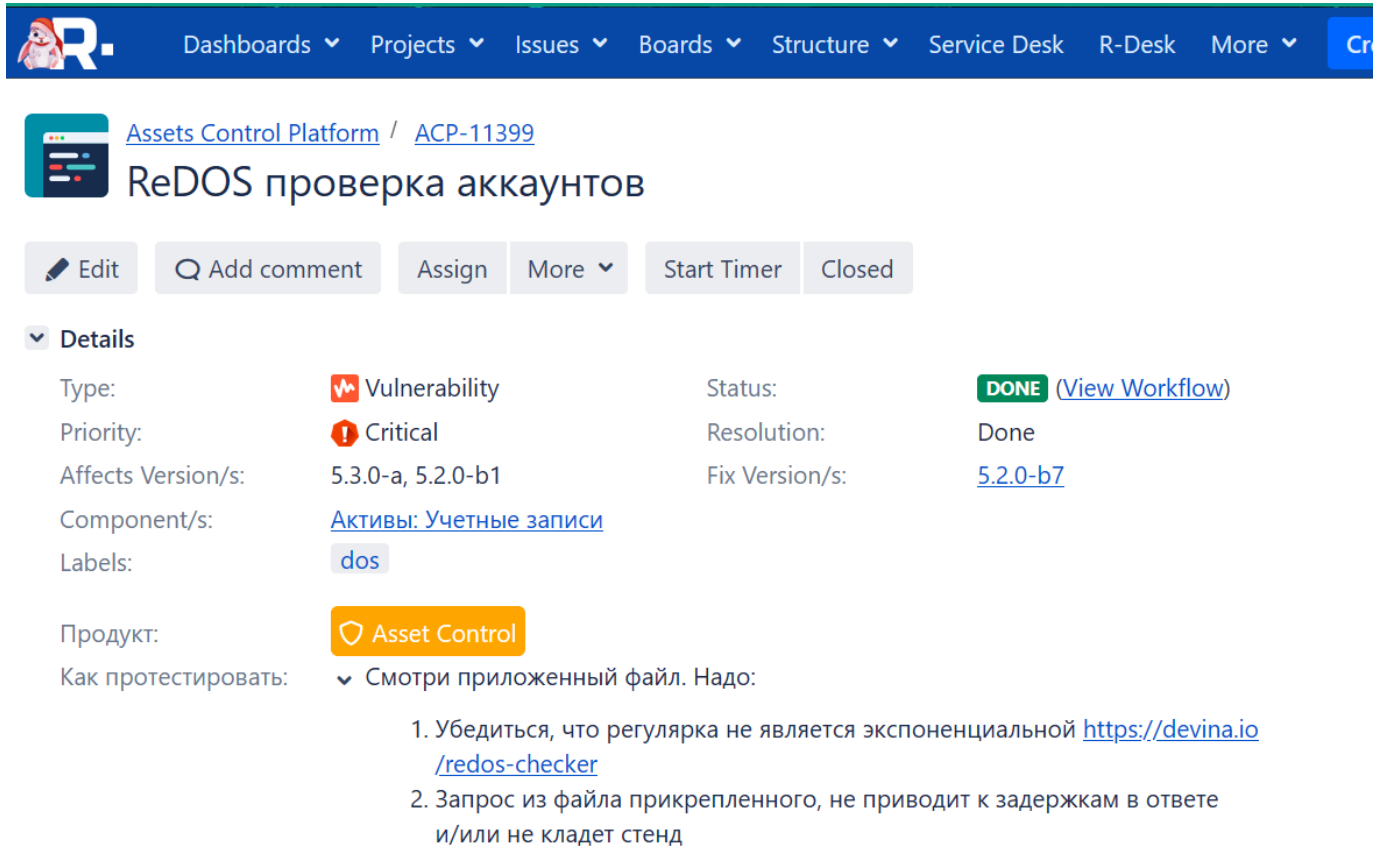
type = Vulnerability AND project = "R-Vision TIP" ORDER BY reporter DESC, summary ASC, priority ASC, cf[13704] ASC

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			Bender
TIP-5150	[AUTH] fastify:3.24.1 | 1085030	From Allure		Bender
TIP-5165	[AUTH] fastify:3.24.1 | CVE-2022-41919	From Allure		Bender
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)			Bender
TIP-3974	[AUTH] moment:2.29.1 | Moment.js Is a JavaScript Date Library for Parsing, Validating, Manipulating, and Formatting Dates. A Path			Bender

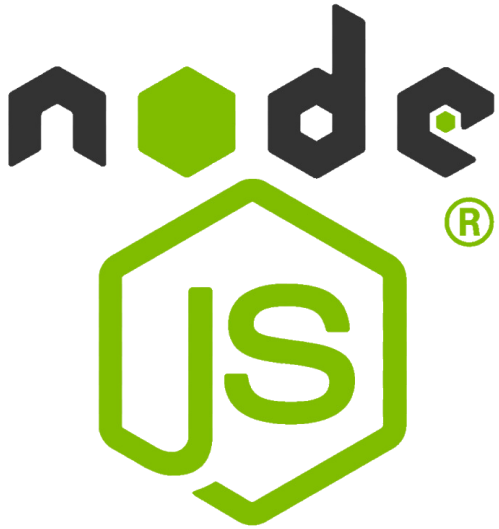
Showing results 51-100 of 404

Продукт становится стабильнее

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



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

rvision.ru

Подписывайтесь на наш бесплатный дайджест ИБ:
rvision.ru /blog