Rakasta

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КАК СЕРВИС

Сервисы информационной безопасности RAKASTA

Непрерывный контроль уязвимостей, защита бизнес-процессов и готовность к сертификации по стандартам безопасности от ИБ-экспертов.

Контроль защищенности

- Контроль целостности FIM
- Аудит паролей AD

vCISO

- Регламенты
- Процессы
- Знания
- Действия

Знания

- Фишинг
- Обучение
- Тестирование
- Социальная инженерия

24*7 и 8*5

Управление уязвимостями

- Поиск уязвимостей
- Контроль и уведомление
- Threat Intellegence
- Устранение уязвимостей

Построение SSDLC

- Анализ процесса разработки
- Создание рекомендаций, регламентов и процесса
- Помощь во внедрении
- Готовые сервисы SSDLC (SCA, SAST, DAST, vMS)

Мониторинг событий ИБ

- Сбор событий ИБ
- Парсинг
- Нормализация
- Агрегация
- Хранение
- Анализ
- Обогащение
- Тикеты
- Реагирование

Rakasta

01

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

Rakasta

Управление уязвимостями

Управление уязвимостями – процесс выявления, оценки, определения приоритетов и мониторинга уязвимостей в автоматическом режиме. Одним из ключевых параметров процесса управления уязвимостями является его непрерывность. Необходимо постоянно отслеживать уязвимости и вовремя реагировать на них, поскольку появляются новые, и за счет этого меняется спектр угроз

Быстрое выявление уязвимостей, уменьшение поверхности атаки

Оценка и приоритезация уязвимостей, а также контроль их устранения

Поддерживать соответствие требованиям различных **стандартам и нормативам**

PCI DSS, GDPR, ГОСТ Р 57580.1, HIPPA и т.д.

В каждой третьей успешной атаке на организации злоумышленники эксплуатировали уязвимости

34%

Контроль и процесс **внедрения обновлений и патчей**

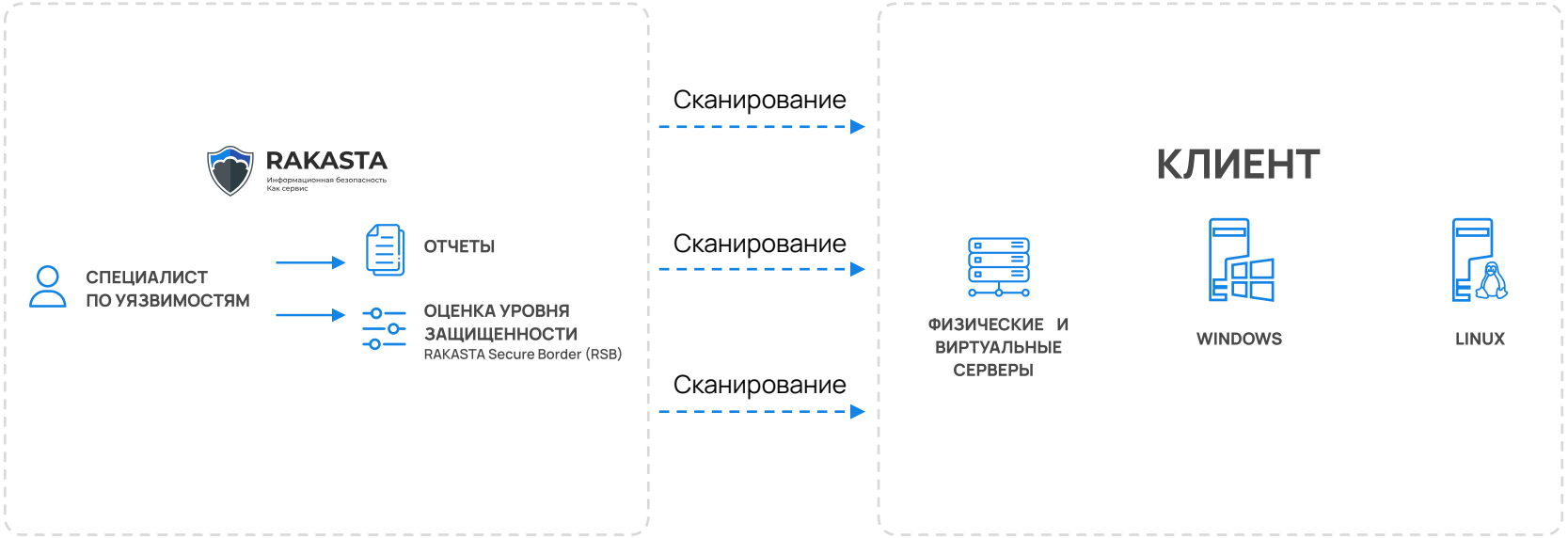
Гибкая настройка отчетности под требования стандартов или под конкретные задачи

Сервис

Внешнее сканирование по требованиям стандарта PCI DSS 4.0

Проведение, по запросу, сканирований внешнего ИТ-ландшафта, попадающего в скоуп стандарта PCI DSS 4.0. Подготовленные инструкции по устранению и отчетность — это отличная практика и ключевой момент в управлении рисками информационной безопасности

Как работает сервис



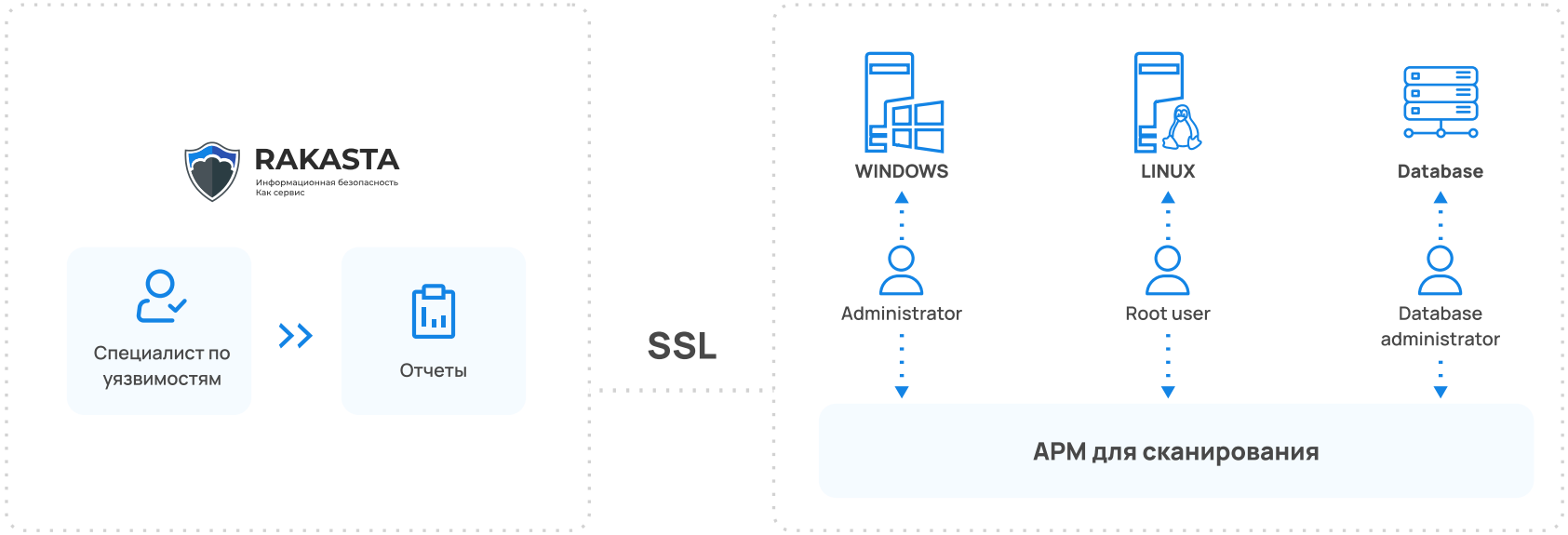
Проведение таких сканирований поможет организации соблюдать требования по безопасности и поддерживать соответствие требований стандарта PCI DSS 4.0.

Сервис

Внутреннее сканирование по требованиям стандарта PCI DSS 4.0

Периодическое проведение сканирований внутри компании, с использованием учетных записей для хостов, попадающих в скоуп стандарта PCI DSS 4.0, оптимизируя ресурсы сотрудников служб ИТ и ИБ.

Как работает сервис



Поддерживать соответствие требованиям различных стандартов

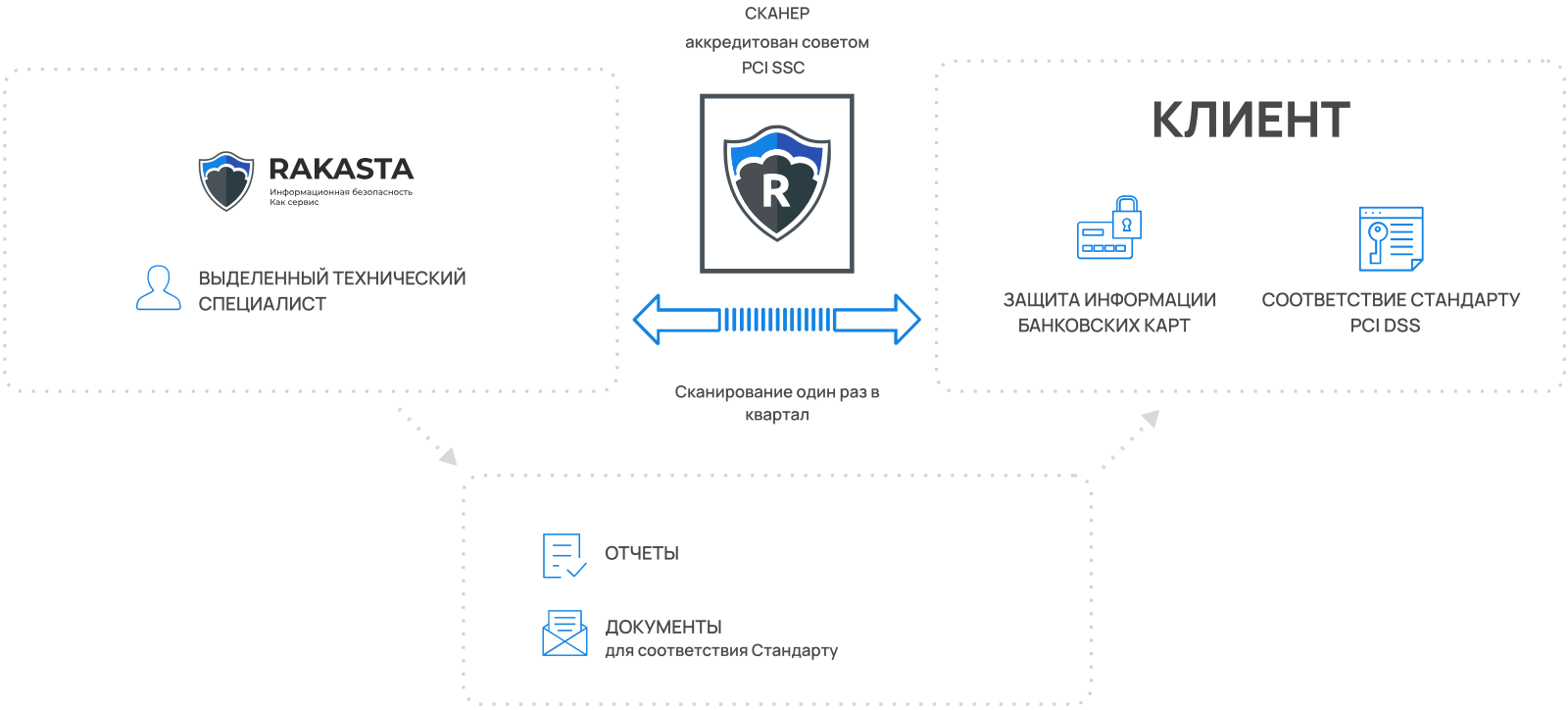
(напр., PCI DSS, 821-П)

Сервис

ASV-сканирование по требованиям PCI DSS 4.0

Ежеквартальные сканирования вашей инфраструктуры, с подробным описанием найденных уязвимостей и путей их решения. Данный сервис призван помочь в решении ряда требований Стандарта PCI DSS, предоставив сертифицированный ASV-сканер.

Как работает сервис



Требования стандарта PCI DSS распространяются на все компании, работающие с международными платежными системами.

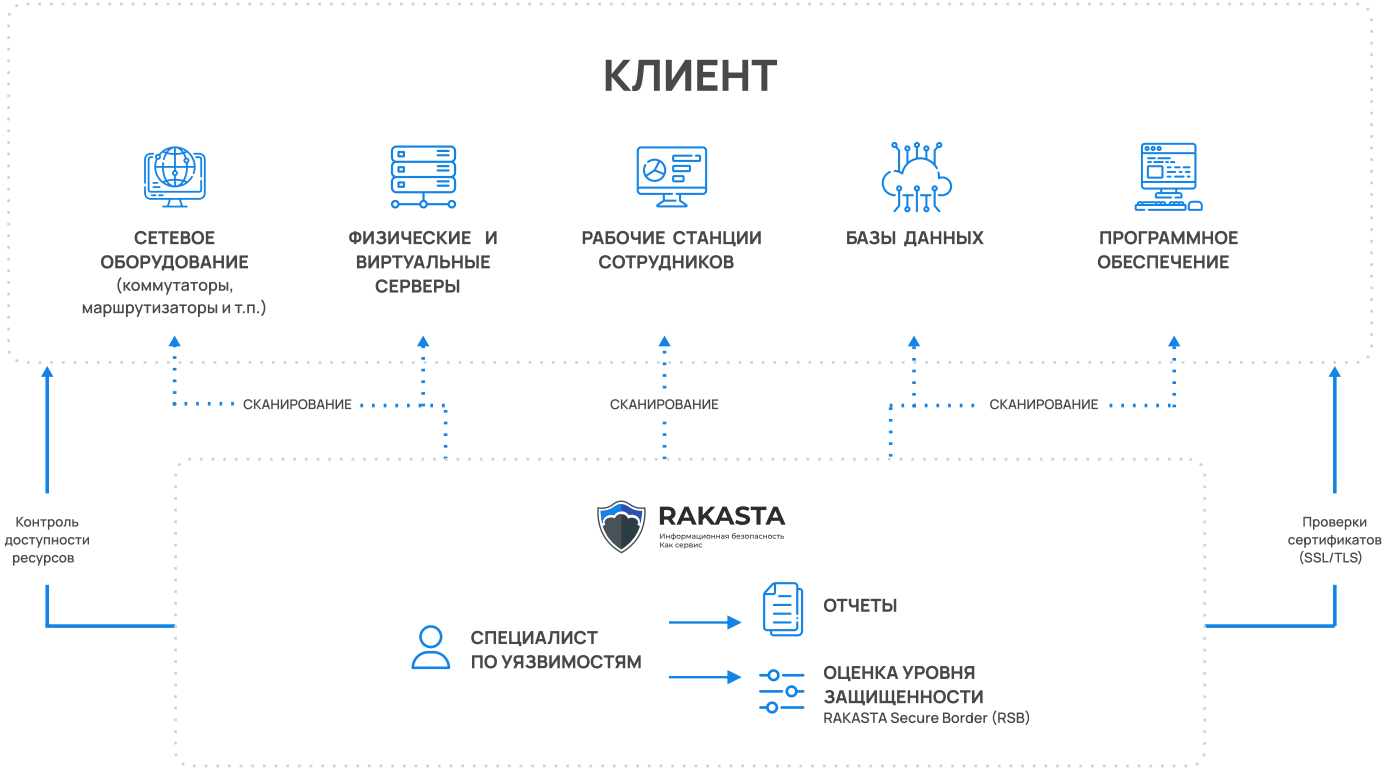
Rakasta

Сервис

Управление внешними уязвимостями и контроль периметра

Периодическое проведение сканирований внешнего ИТ-ландшафта, с привлечением специализированной команды позволит быстро обеспечить высокий уровень контроля за уязвимостями в инфраструктуре.

Как работает сервис



Сократить затраты на содержание профильных специалистов в штате, используя консультационную и техническую поддержку в рамках сервиса

Сервис
Управление внутренними уязвимостями

Периодическое проведение сканирований внутри компании, с использованием учетных записей, с целью выявлять и устранять уязвимости во внутренних сетях, без дополнительного приобретения и обслуживания оборудования.

Как работает сервис

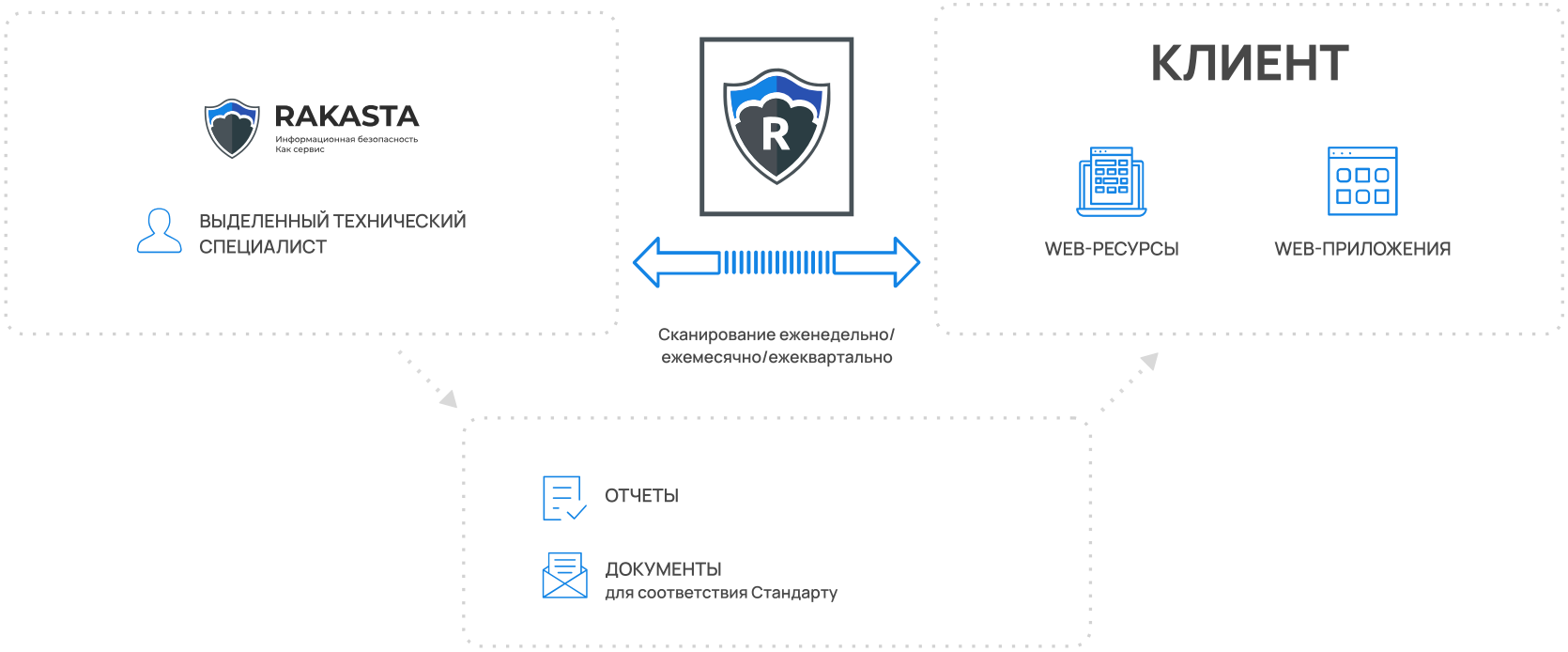
1300+

клиентов уже пользуются нашим сервисом УУ

Сервис
Безопасность web-ресурсов

Регулярное проведение сканирований и контроль защищенности внешних и внутренних web-ресурсов.

Как работает сервис

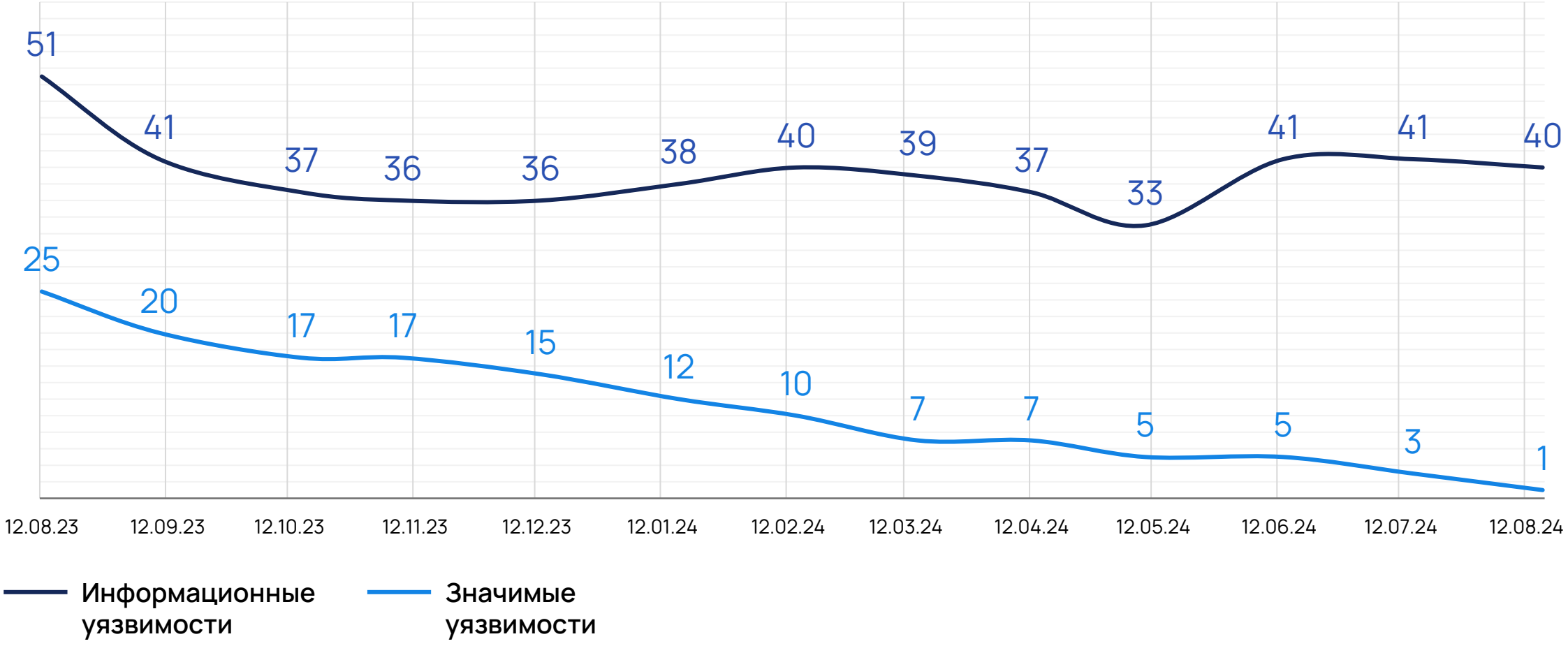


53%

организаций
имеют низкий уровень
защищенности
web-приложений

Rakasta

Пример снижения критичных уязвимостей при использовании сервиса



Rakasta

02

КОНТРОЛЬ ЗАЩИЩЕННОСТИ

Rakasta

Контроль защищенности

Нацелено на выявление внутренних злоумышленников и их вредоносных действий с серверами и системами. Большая часть проникновений во внутреннюю инфраструктуру обычно происходит при помощи использования подбора пароля.

Повышение стойкости учётных записей к атакам на пароли

Оперативное выявление несанкционированных действий с файлами и директориями

Защита критичных файлов от несанкционированных изменений

Интеграция с текущими СЗИ и системами мониторинга ИБ

87%

данных, раскрытых за первый квартал 2024, относятся к финансовым организациям

Сервис

Контроль целостности FIM

В режиме реального времени осуществляет непрерывный мониторинг состояния конфигурации, включая проверку целостности файлов и защиту системы от изменений.

PCI DSS 4.0 требования:

0.2.1 Audit logs are enabled and active for all system components and cardholder data.

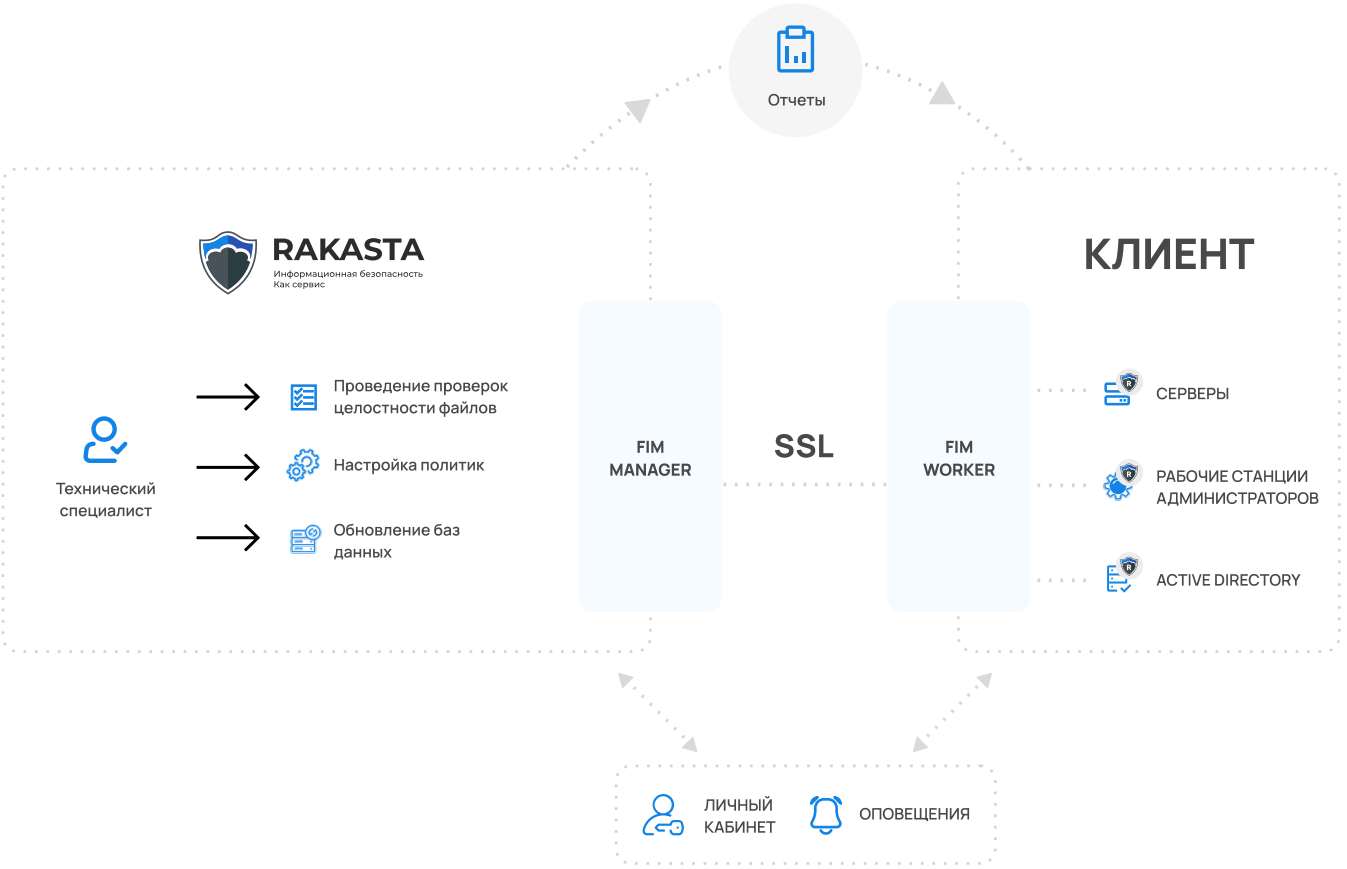
10.2.1.1 Audit logs capture all individual user access to cardholder data.

10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.

10.2.1.3 Audit logs capture all access to audit logs

10.2.1.7 Audit logs capture all creation and deletion of system-level objects.

Как работает сервис



Сервис

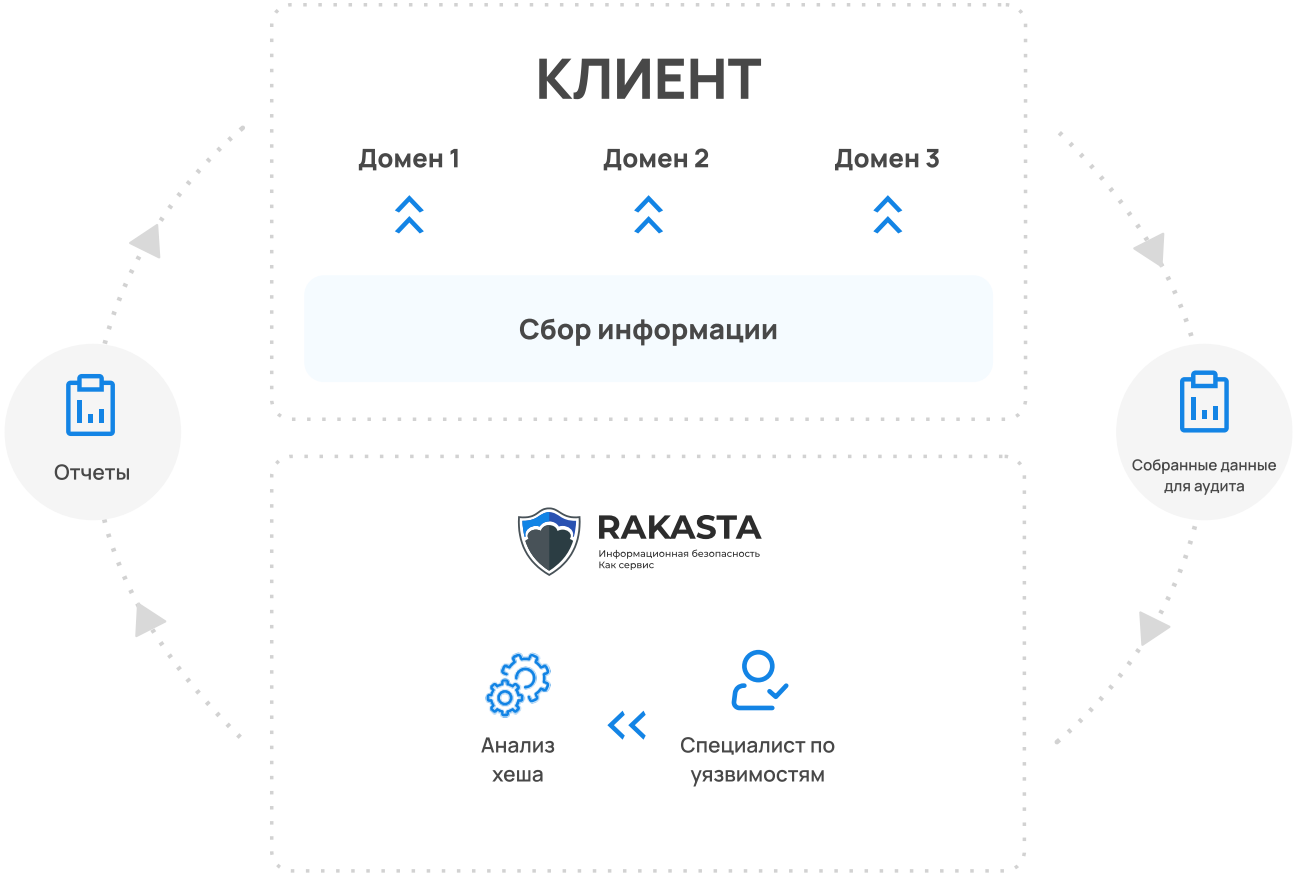
Аудит паролей в среде AD

Обеспечивает комплексный аудит паролей внутри компании, обеспечивая выявление уязвимых паролей, а также потенциально опасные мисконфигурации в Active Directory с точки зрения аудита паролей.

Сервис позволяет выявить пароли, которые возможно подобрать с помощью атаки по словарю, так как проверка проходит по базе паролей, состоящей из более чем 613 миллионов паролей, которые когда-либо утекали в глобальную сеть Интернет. База постоянно обновляется.

> 613 млн паролей

Как работает сервис



03

МОНИТОРИНГ СОБЫТИЙ ИБ

Мониторинг

Это комплексное решение для защиты цифровых систем, объединяющее управление событиями безопасности и анализ информации о событиях в реальном времени.

Инструменты мониторинга собирают и анализируют данные из различных источников, включая серверы, сетевые устройства, антивирусные программы и другие средства защиты, чтобы обеспечить централизованное управление информацией о безопасности.

Комплексный подход, обеспечивающий защиту компании

Снижение затрат на внутренние ресурсы компании

Постоянный мониторинг и быстрое выявление инцидентов на основе корреляционных правил

Постоянное обновление SIEM для поддержания её в актуальном состоянии

24 / 7

Обнаружение угроз

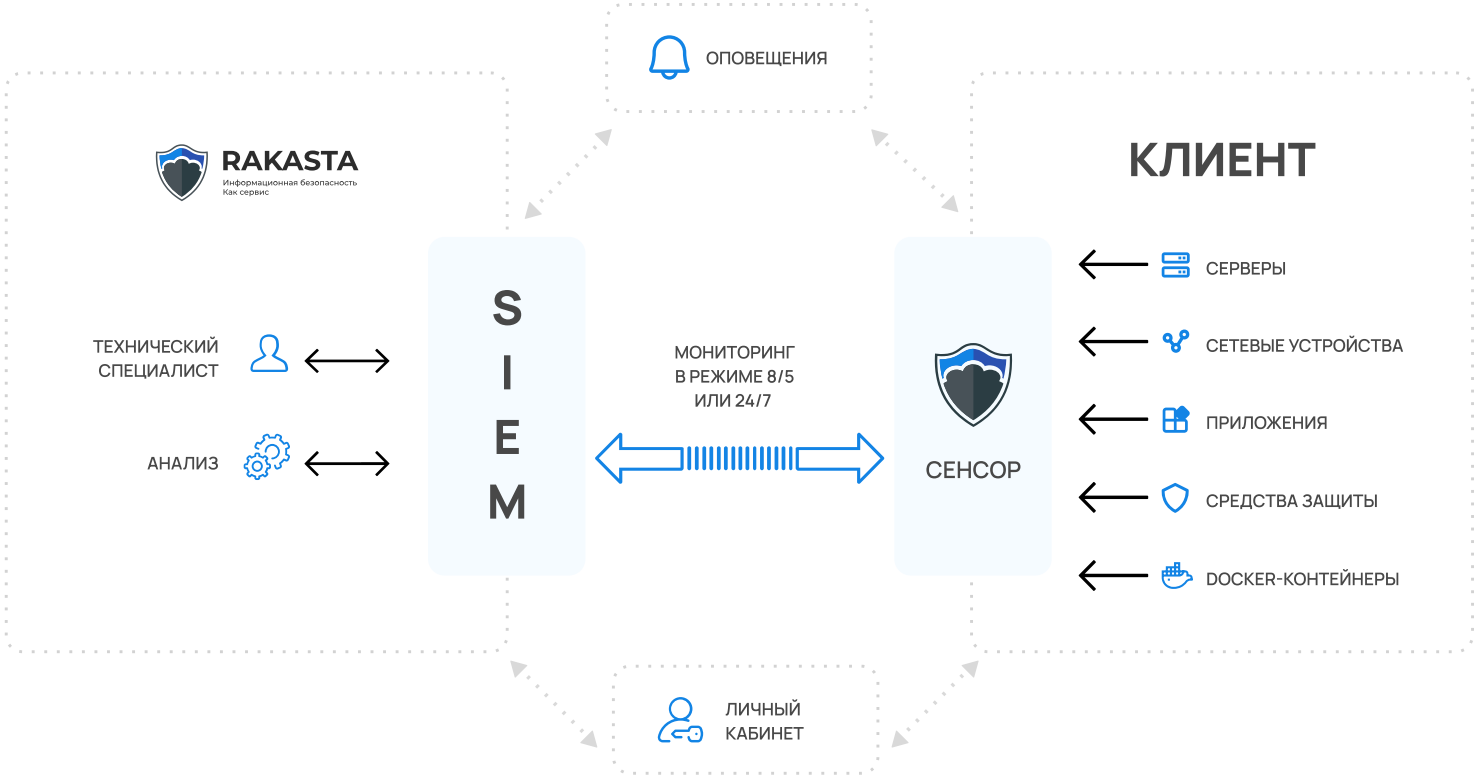
Rakasta

Сервис
SIEM as a service

Непрерывный мониторинг и своевременное выявление инцидентов информационной безопасности без развертывания собственной SIEM на внутренних платформах организаций.

Сервис позволяет компаниям подключиться к готовой SIEM системе, развернутой на нашей платформе и подключить к ней свои источники.

Как работает сервис

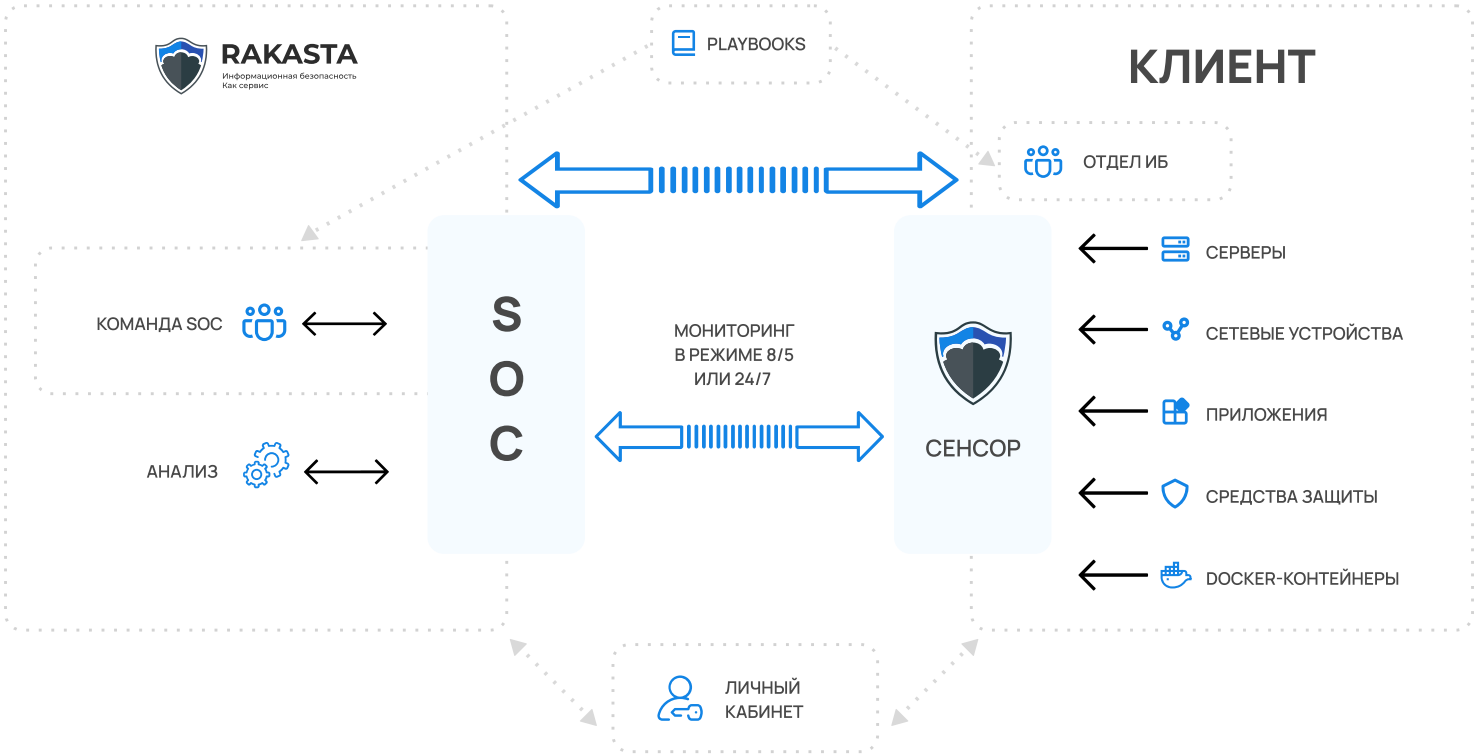


Сервис
SOC as a service

Обеспечение кибербезопасности, непрерывный мониторинг, обнаружение, реагирование и предотвращение угроз в режиме реального времени.

Это специализированный центр, оснащенный передовыми технологиями и командой экспертов, которая обеспечивает непрерывную защиту информационных систем и данных вашей организации.

Как работает сервис



Rakasta

Сервис
Команда SOC as a service

Линия 1

Операторы-инженеры

- Мониторинг событий 8*5 и 24*7
- Подключение новых систем
- Оперативная коммуникация с заказчиком

Сотрудники со статусами CompTIA Security+, QualysGuard specialist и другими вендорскими сертификатами

Линия 2

Аналитики

- Разбор инцидента
- Настройка правил корреляции
- Консультирование по восстановлению

Сотрудники со статусами CISA, CISSP, CISM, ISO 27001 Lead Auditor. QSA и профильными сертификатами вендоров

Линия 3

Pen.test

- Разбор инцидента
- Настройка правил корреляции
- Консультирование по восстановлению

Аттестованные специалисты CEH, OSCP, ASCE, ECSA, ECC CHF и другие

Play Books — готовые сценарии отработки инцидентов

Rakasta

Сервис

Актуализация и техническая поддержка

Обеспечивает безопасность вашей информационной инфраструктуры через обновление компонентов SIEM системы.

Включает регулярное обновление ПО и патчей безопасности, поддерживая систему в актуальном состоянии.

Ежемесячные отчеты о состоянии работы источников

Этапы сервиса

Rakasta

04

ЗНАНИЯ

Rakasta

Знания

Услуга и сервис для выявления уязвимых сотрудников перед фишинговыми рассылками.
Наша команда поможет оценить навыки сотрудников в распознавании подозрительных писем. Обучающие курсы помогут повысить осведомлённость сотрудников в вопросах противодействию атакам методом социальной инженерии.

Защита конфиденциальности

Направление по предоставлению услуги и сервиса по противодействию фишингу помогает снизить вероятность компрометации корпоративных данных сотрудников.

Сохранение бизнес-процессов

Предотвращая фишинговые атаки, направление помогает обеспечить непрерывность и стабильность бизнес-процессов.

Минимизация рисков

Благодаря обучению и регулярным проверкам, компания снижает риски, связанные с потерями от кибератак методом социальной инженерии.

Предотвращение утечек

Регулярные проверки на фишинг помогают предотвратить утечки важной информации, что укрепляет репутацию компании.

Снижение затрат

Минимизируя риски связанные с кибератаками, направление помогает сократить потенциальные финансовые потери.

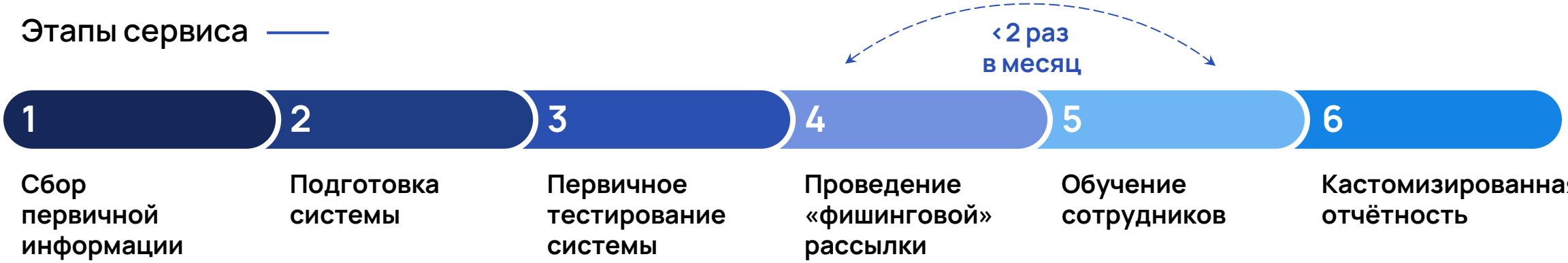
После обучения основам кибербезопасности ваши сотрудники научатся самостоятельно выявлять фишинговые письма.

Rakasta

Сервис
Обучения и тестирования навыков сотрудников по вопросам ИБ

Это платформа для обучения, тестирования и контроля готовности сотрудников компании противостоять фишингу. Имитируя фишинговые атаки, сервис выявляет сотрудников с недостаточным уровнем знаний и предоставляет необходимые электронные курсы и тесты для тренировки навыков по информационной безопасности.

Этапы сервиса



79% фишинга злоумышленники маскируют под финансовую документацию

Rakasta

Сервис
Социальная инженерия

Позволяет оценить уровень осведомлённости сотрудников в вопросах противодействию атакам методом социальной инженерии. На основе этой оценки можно выявить степень готовности сотрудников к противостоянию атакам данного типа.

Этапы сервиса

1	2	3	4	5
Сбор первичной информации	Подготовка системы	Первичное тестирование системы	Проведение «фишинговой» рассылки	Отчетнсть

Использование подобных сервисов помогает организациям соблюдать требования стандартов безопасности, таких как ISO 27001

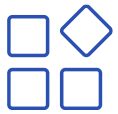
05

SECURE SDLC

Rakasta

SSDLC

Это структурированный процесс, который обеспечивает высокое качество разработки ПО при минимальных затратах и в кратчайшие сроки.



Мы предлагаем набор сервисов DevSecOps, которые позволят внедрить процессы SSDLC в вашу разработку как с нуля, так и отталкиваясь от текущего уровня зрелости.

Наши эксперты помогут организовать безопасную разработку с наименьшими затратами и в короткий срок, получив конкретный и «измеряемый» результат.

Правильная реализация процессов SSDLC и практик DevSecOps требует серьезных усилий и затрат на внедрение и закупку различных технических решений

Rakasta

Сервис

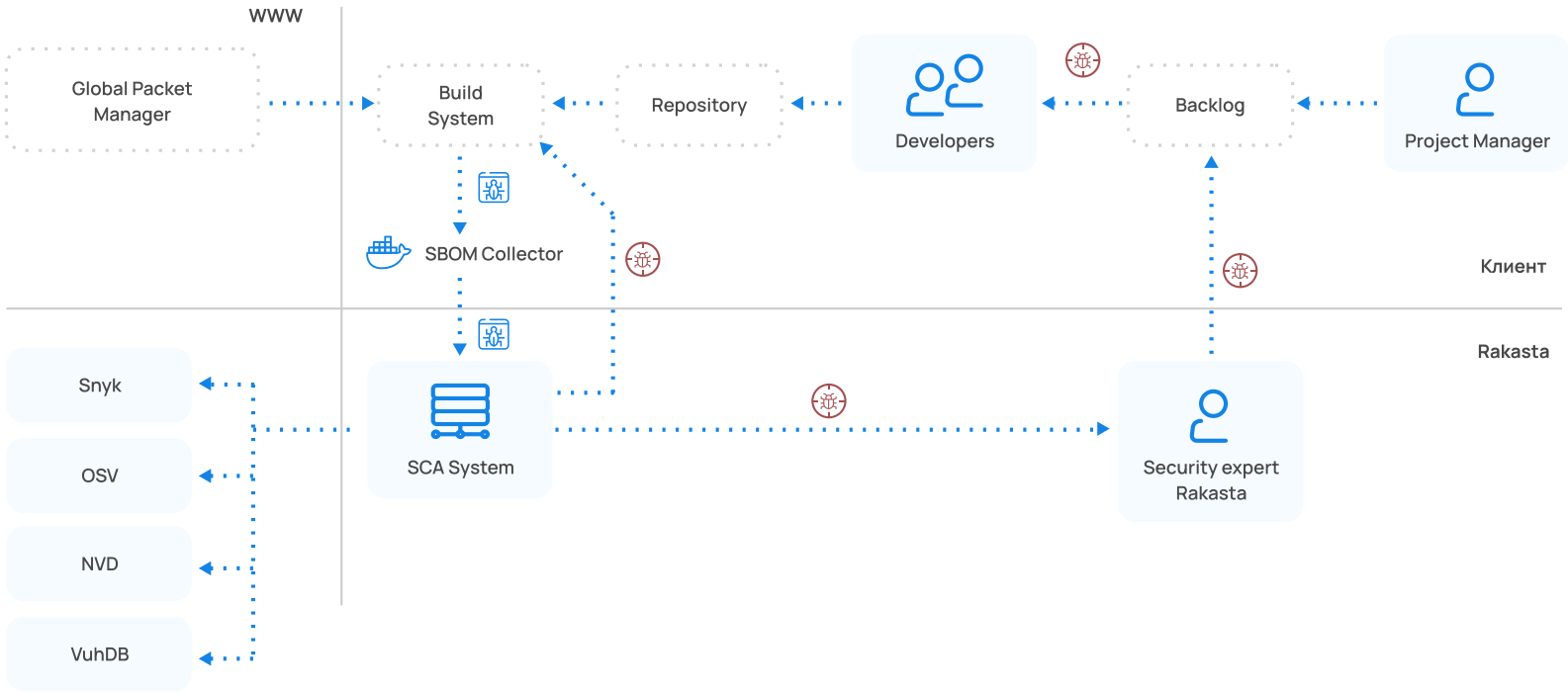
Анализа библиотек и компонентов разработки (software composition analysis) (SCA)

Это анализ компонентного состава приложения.

Такой анализ позволяет обнаруживать уязвимые компоненты и дефекты безопасности.

Сервис «SCA» — эффективное решение для поиска уязвимостей в пакетах с открытым исходным кодом и изучения способов их устранения. Сервис «SCA» позволяет вам защитить свой код и работоспособность ваших приложений.

Как работает сервис



Сервис

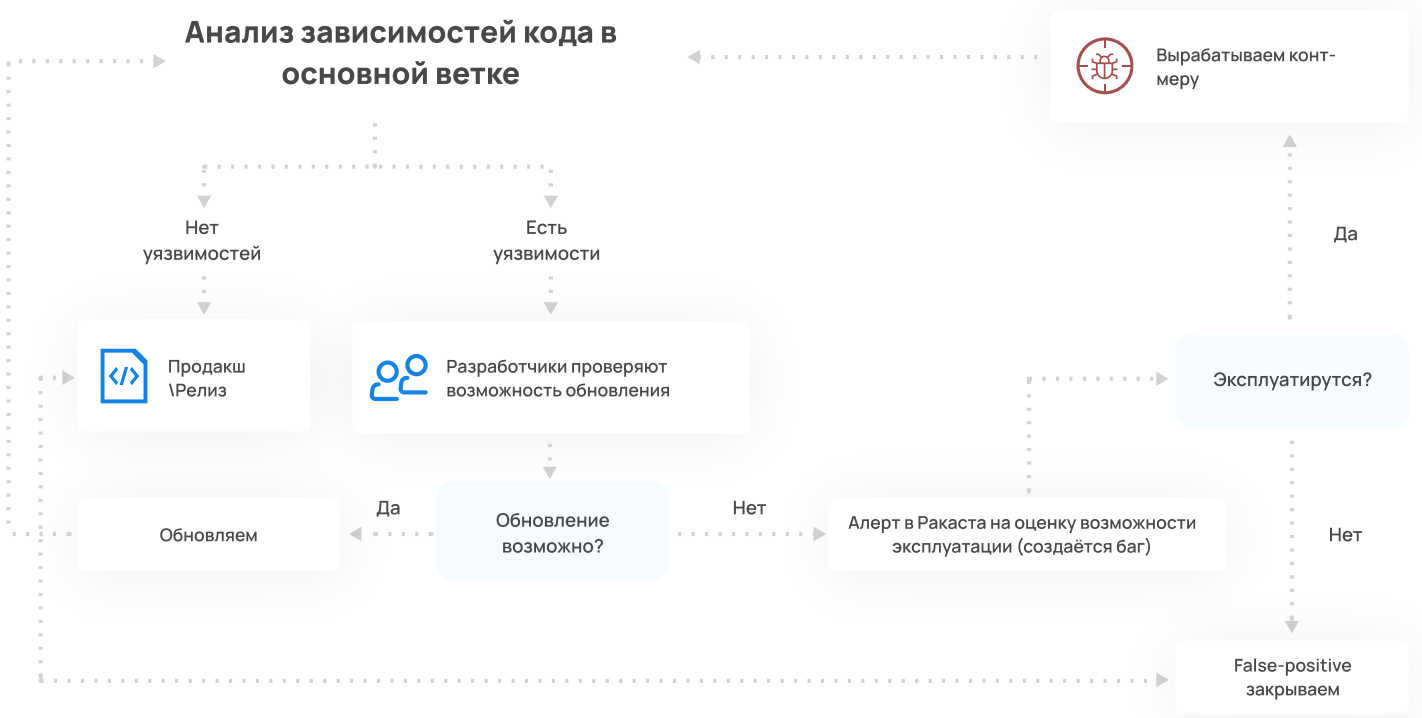
Анализа библиотек и компонентов разработки (software composition analysis) (SCA)

ВАЖНО!

Сервис «SCA» помогает отслеживать библиотеки с открытым исходным кодом, используемые при разработке приложений и уязвимости в них.

Это важно как с точки зрения производительности, так и с точки зрения безопасности.

Этапы работы



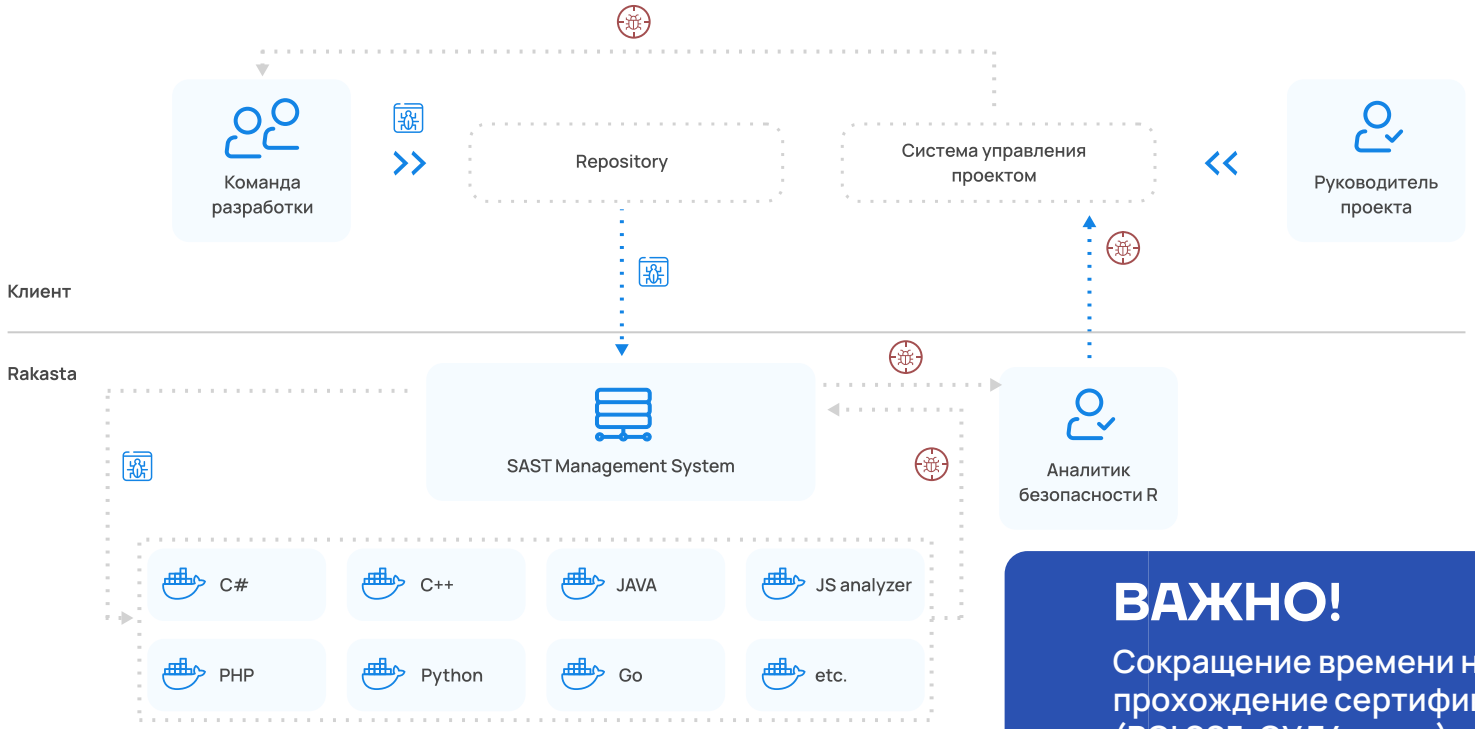
Сервис

Статический анализ кода (static application security testing) (SAST)

Это процесс тестирования приложения на наличие ошибок и уязвимостей в исходном коде с применением статического анализа.

Сервис «Статический анализ кода» (SAST) помогает выявить уязвимости «нулевого дня». Под уязвимостями «нулевого дня» понимаются ошибки, которые найдены злоумышленником и могут быть эксплуатированы. Задача сервиса - обнаружить дефекты безопасности на этапе разработки приложения.

Как работает сервис



ВАЖНО!

Сокращение времени на прохождение сертификации (PCI SSF, ОУД4 и д.р.)

Сервис
DAST (dynamic application security testing) as a service

Это метод тестирования безопасности, который направлен на обнаружение уязвимостей в уже развернутом и функционирующем приложении.

Тестирование DAST хорошо подходит для поиска уязвимостей таких как SQL-инъекции, XSS (межсайтовый скриптинг) и другие.

Однако DAST не способен выявлять некоторые виды уязвимостей, такие как недостаточные права доступа или проблемы с аутентификацией, а также может давать ложно-положительные результаты, которые необходимо обрабатывать в ручную.

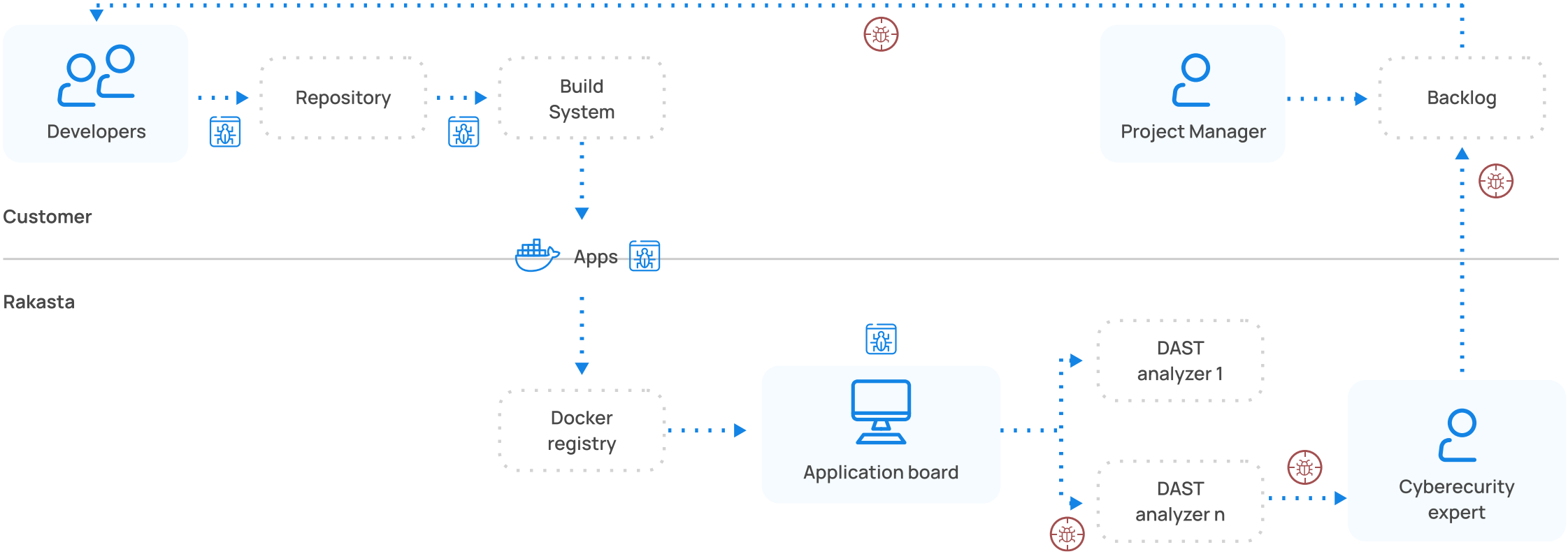
ВАЖНО!

Ориентир на поиск уязвимостей из списка OWASP Top 10, включая SQL-инъекции, XSS, CSRF и многие другие, гарантируя высокий уровень безопасности

OWASP TOP 10

Сервис
DAST (dynamic application security testing) as a service

Как работает сервис



Сервис
Vulnerability management system (VMS)

Единая веб-консоль, которая агрегирует уязвимости из инструментов (SAST, DAST, SCA, Infrastructure Scanner), которые выявляют их.

Сервис «VMS» позволяет получить комплексный отчет не только по векторам, но и корреляцию между ними.

С помощью сервиса «Vulnerability Management System» осуществляется управление уязвимостями на уровне кода в рабочей среде.

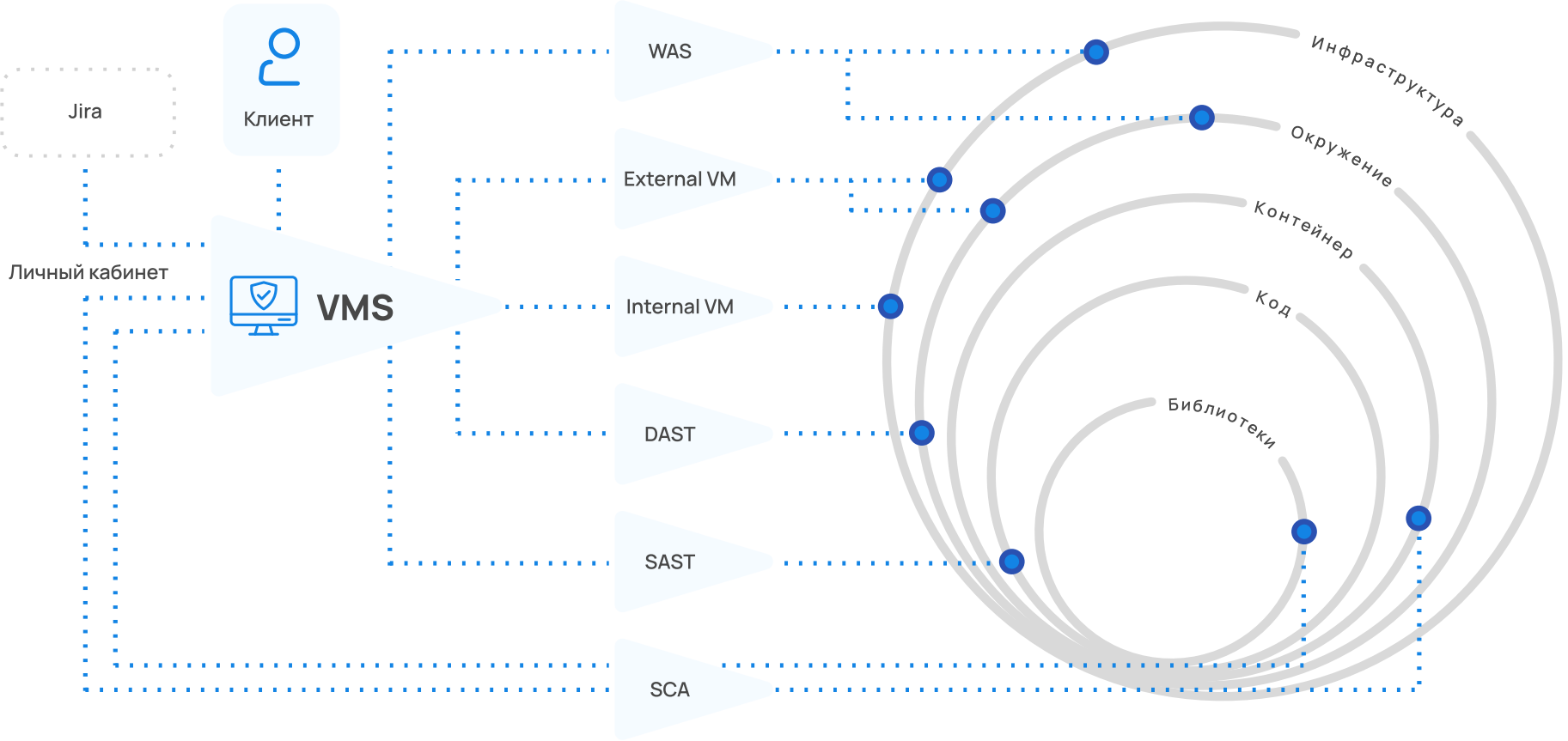
Что подразумевает под собой уязвимости уже в контексте, а не абстрактного стенда.

ВАЖНО!

Используя единую консоль с ролевым доступом, сервис «Vulnerability Management System» позволяет работать с данными по выявленным уязвимостям на всех уровнях, помогая в их устранении и приоритезации.

Сервис
Vulnerability management system (VMS)

Как работает сервис



Rakasta

06

VIRTUAL CISO

Rakasta

Сервис VIRTUAL CISO

Это возможность для компаний воспользоваться услугами от экспертов и опытных специалистов в данной области, которые выступят в роли главного сотрудника по информационной безопасности Вашего бизнеса.

Получать консультационные услуги от экспертов в области информационной безопасности

Создать и оптимизировать политику безопасности, процессы и процедуры

Запустить процесс управления уязвимостями, оценивать и контролировать риски

Обеспечить соблюдение требований безопасности и стандартов в отрасли (ISO 27001, PCI DSS)

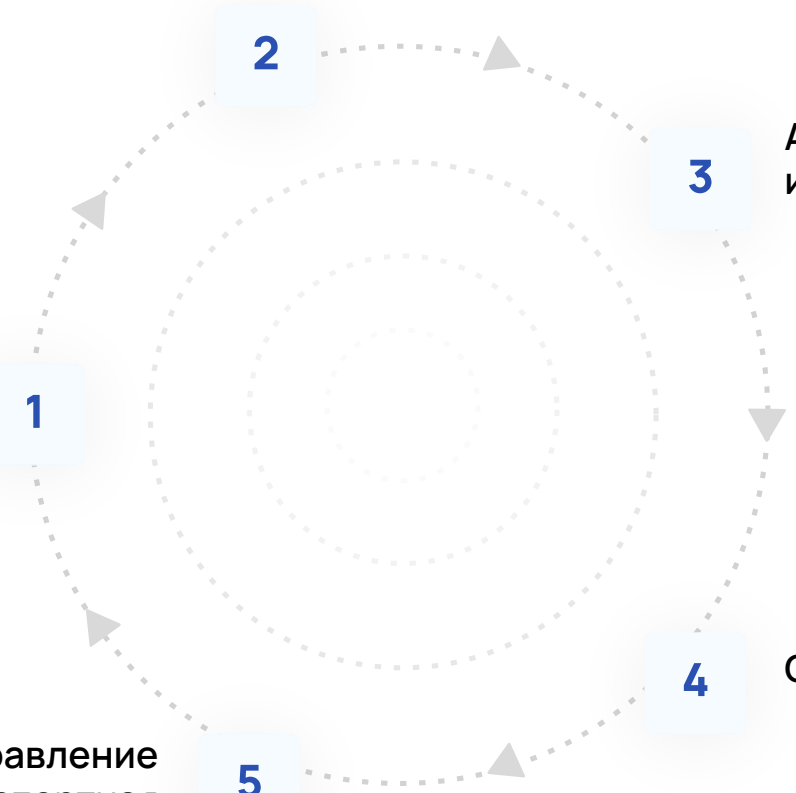
Делегировать управление и решение задач компетентным и профессиональным специалистам

Быстрый запуск сервиса оперативно решит базовые задачи, связанные с обеспечением ИБ, обеспечив должный уровень

Rakasta

Сервис VIRTUAL CISO

Этапы сервиса



1 **Постановка целей**
знакомство с компанией
и определение задач

2 **Определение рисков ИБ**
формулировка и приоритезация
инцидентов

3 **Аудит**
инфраструктуры

4 **Обучение**

5 **Консалтинг и управление**
экспертная
поддержка сервиса

Rakasta

О КОМПАНИИ

Наш опыт

10+
лет опыта

40+
экспертов

4
страны присутствия

Наши клиенты

6
стран

1500+
клиентов каждый год

Доверьте нам решение вопросов информационной безопасности вашего бизнеса

И сконценрируйтесь на его развитии!

Rakasta

СПАСИБО!

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СЕРВИС

143600, Москва, Варшавское шоссе,
1с6, W-Plaza 2, оф.409

+7 (495) 968 57 66

www.rakasta.ru