Rakasta

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СЕРВИС

Сервисы и услуги информационной безопасности RAKASTA

Ваша безопасность — наша экспертиза: непрерывный мониторинг угроз, защита ключевых процессов и экспертный подход к информационной безопасности.

Мониторинг событий ИБ

- SOC as a service
- SIEM as a service
- Wazuh SIEM
- Актуализация и ТП
- Экспресс-аудит SIEM
- Аудит SOC-CMM
- Managed IOC feeds

Контроль защищенности

- Контроль целостности файлов FIM
- Аудит паролей AD
- Защита веб-приложений WAF
- Контроль целостности веб-страниц PIM

24*7 и 8*5

Управление уязвимостями

- Внутренние сканирования с аутентификацией
- Внешние сканирования
- Сканирования веб-ресурсов
- ASV-сканирования по требованиям PCI DSS

Знания

- Социальная инженерия (фишинг)
- Обучение
- Тестирование

Построение SSDLC

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

Rakasta

01

Мониторинг событий ИБ

Rakasta

Мониторинг событий ИБ

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

SOC as a service

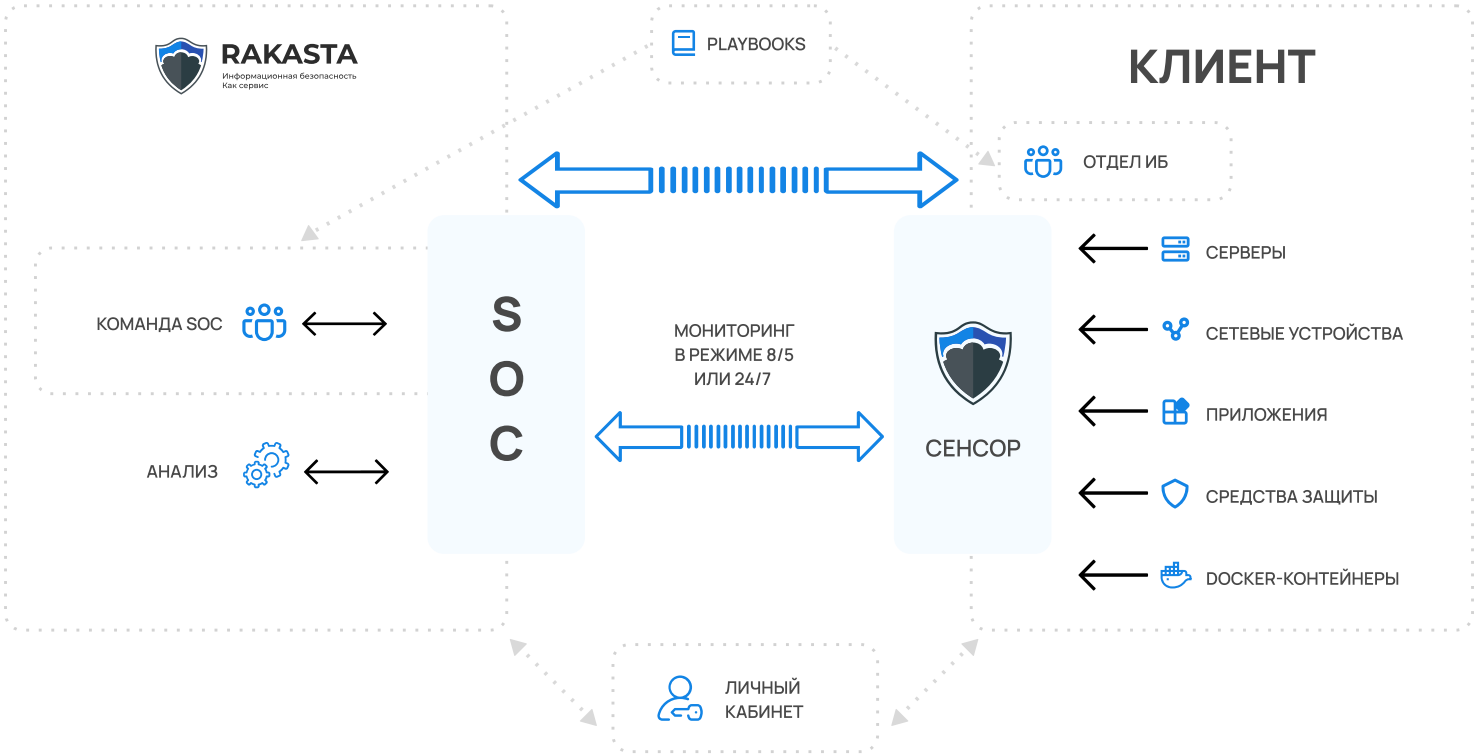
Обеспечивает кибербезопасность, непрерывный мониторинг, обнаружение, реагирование и предотвращение угроз в режиме реального времени.

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

Закрываемые требования PCI DSS 4.0.1

10.2.1, 10.2.1.1, 10.2.1.2, 10.2.1.3, 10.2.1.4, 10.2.1.5, 10.2.1.6, 10.2.1.7, 10.2.2, 10.3.1, 10.3.2, 10.3.3, 10.4.1, 10.4.1.1, 10.4.2, 10.4.3, 10.5.1, 10.6.1, 10.6.2, 10.7.2

Как работает сервис



Rakasta

Сервис

Команда SOC as a service

1

Линия

Операторы-инженеры

- Мониторинг и фиксация событий 8*5 и 24*7
- Оперативная коммуникация с заказчиком

2

Линия

Инженеры

- Подключение новых источников событий
- Поддержание работоспособности системы
- Актуализация критичных инцидентов

3

Линия

Аналитики

- Разбор инцидента
- Настройка правил корреляции
- Консультирование по восстановлению

Rakasta

Сервис

SIEM as a service

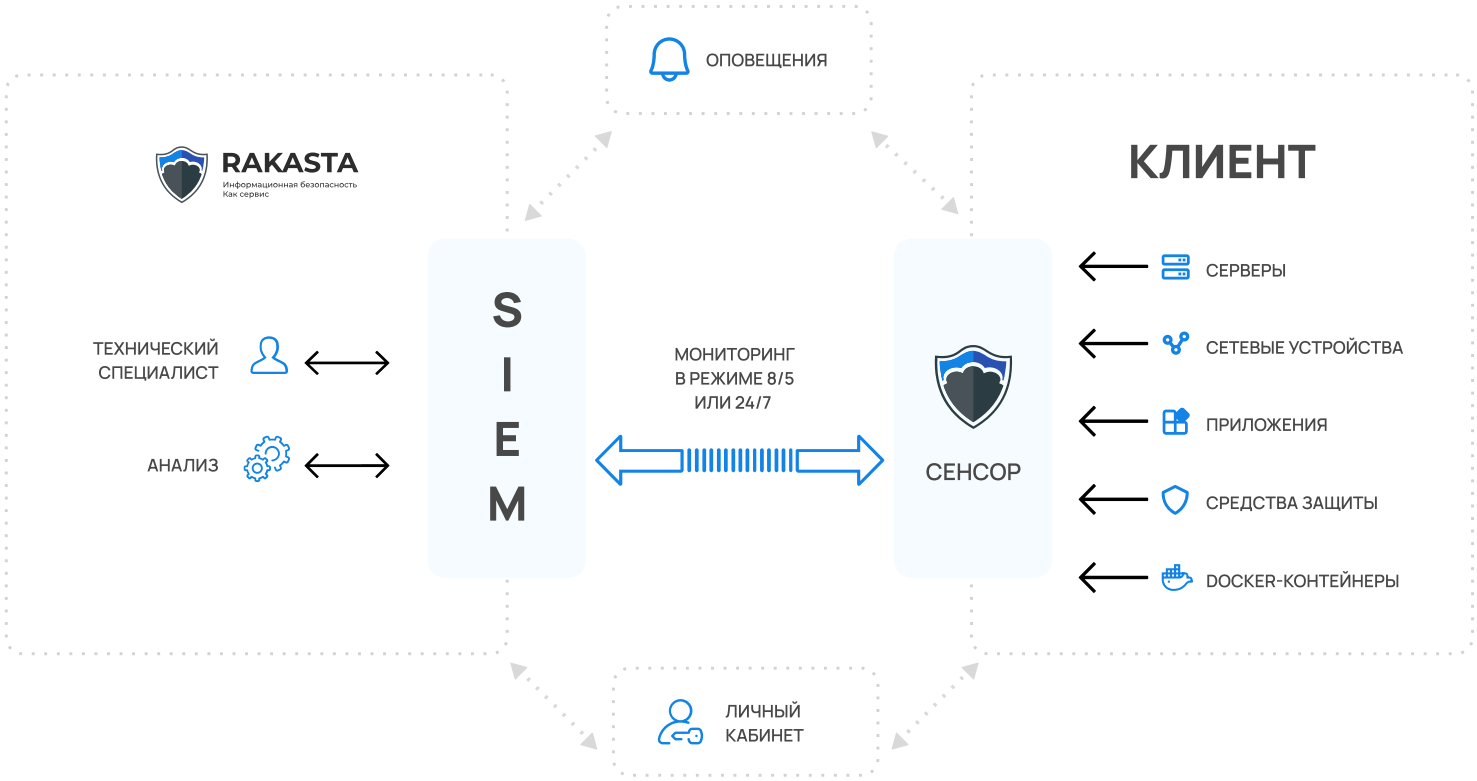
Непрерывный мониторинг инцидентов информационной безопасности без необходимости развертывания собственной SIEM.

Облачный SIEM позволяет оптимизировать расходы на информационную безопасность, сохраняя при этом высокий уровень защиты.

Закрываемые требования PCI DSS 4.0.1

10.2.1, 10.2.1.1, 10.2.1.2, 10.2.1.3, 10.2.1.4, 10.2.1.5, 10.2.1.6, 10.2.1.7,10.2.2, 10.3.1, 10.3.2, 10.3.3, 10.4.1, 10.4.1.1, 10.4.2, 10.4.3, 10.5.1, 10.6.1, 10.6.2, 10.7.2

Как работает сервис



Rakasta

Сервис
WAZUH SIEM

Услуга по настройке и сопровождению WAZUH SIEM для выполнения требований PCI DSS.

Цель работ —

подготовить инфраструктуру к успешному прохождению аудита на соответствие требованиям PCI DSS в области мониторинга и управления событиями информационной безопасности с использованием SIEM-платформы WAZUH.

Дальнейшее сопровождение SIEM-платформы WAZUH:

- Обновления
- Техническая поддержка
- Отчетность и консультации

Закрываемые требования PCI DSS 4.0.1

10.2.1, 10.2.1.1, 10.2.1.2, 10.2.1.3, 10.2.1.4, 10.2.1.5, 10.2.1.6, 10.2.1.7,10.2.2, 10.3.1, 10.3.2, 10.3.3, 10.4.1, 10.4.1.1, 10.4.2, 10.4.3, 10.5.1, 10.6.1, 10.6.2, 10.7.2

Rakasta

Сервис

Актуализация и техническая поддержка

Комплексный подход, включающий актуализацию и техническую поддержку, эффективно защищает вашу организацию от киберугроз.

Сервис «Актуализация и ТП» соответствует современным требованиям кибербезопасности, предлагая высококачественное решение для поддержки бизнес-процессов.

Включает в себя консультации по повышению надежности SIEM-системы и ежемесячные отчеты о состоянии работы источников.

Этапы сервиса

Rakasta

Сервис

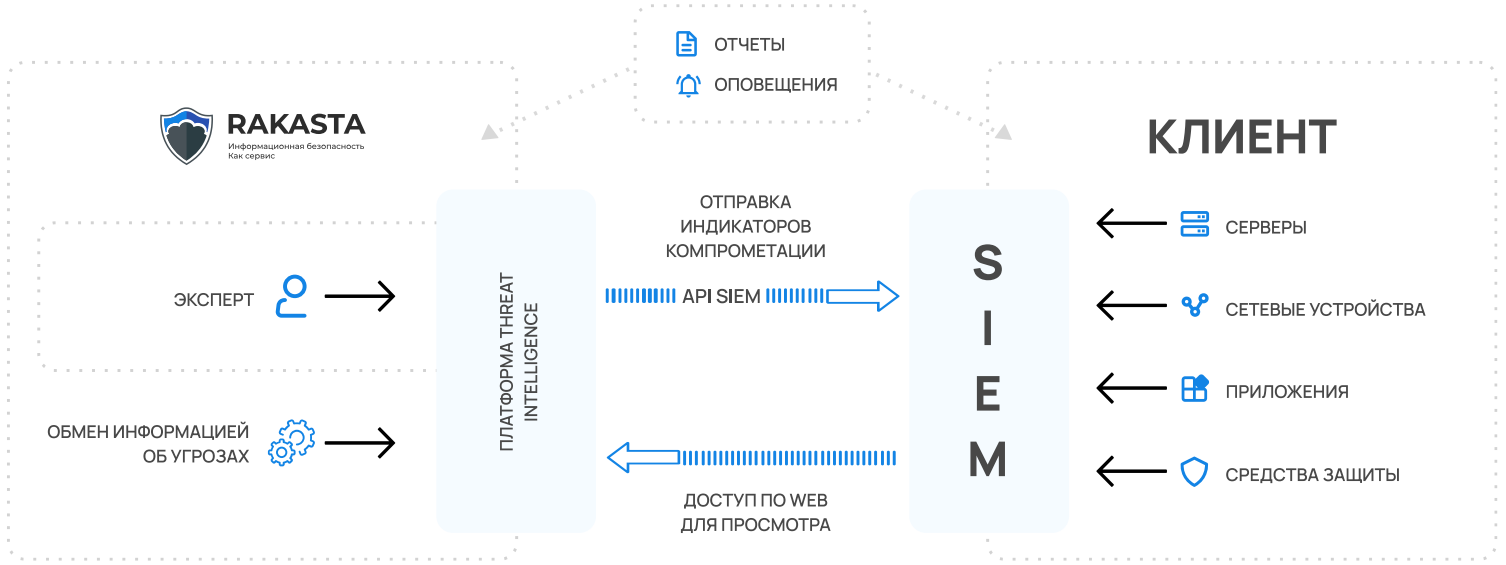
Managed IOC Feeds

Средство повышения эффективности SOC по средствам регулярного обновления сведений об актуальных угрозах и источниках атак.

В таких задачах используются индикаторы компрометации (IOC)- технические признаки, по которым можно определить факт или попытку взлома.

Такая интеграция дает повышение эффективности обнаружения киберугроз, а также ускоряет анализ событий и снижает нагрузку на специалистов компании.

Как работает сервис



Rakasta

Услуга

Экспресс-аудит SIEM QRadar

Это экспресс-проверка как технической “начинки”, так и логической настройки SIEM:

- Проверка аппаратных ресурсов, версии ПО и обновлений;
- Оценка производительности (EPS-нагрузки), здоровье сервисов и корректность резервного копирования.

Итог –
SIEM-система собирает и обрабатывает события без потерь, правильно применяет правила корреляции и своевременно выявляет угрозы.

Услуга

Аудит SOC — CMM

Комплексная процедура оценки эффективности функционирования подразделения, отвечающего за обнаружение, анализ и реагирование на инциденты информационной безопасности. SIEM-система может быть любая.

- В рамках аудита производится исследование организационной структуры, процессов технологий и кадрового состава SOC с целью выявления уязвимостей, неэффективных процессов и зон развития.

Результаты аудита позволяют установить текущий уровень зрелости SOC по адаптированной модели SOC CMM (Capability Maturity Model).

Rakasta

02

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. Поскольку спектр угроз всё время меняется из-за появления всё новых уязвимостей, необходимо их постоянно отслеживать и своевременно на них реагировать.

Быстрое выявление уязвимостей,
уменьшение поверхности атаки

Оценка и приоритизация уязвимостей,
а также контроль их устранения

Поддержание соответствия требованиям **различных стандартам и нормативам**

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

Контроль и процесс **внедрения обновлений и патчей**

Гибкая настройка отчетности
под требования стандартов или
под конкретные задачи

1400+

клиентов уже пользуются нашими сервисами УУ

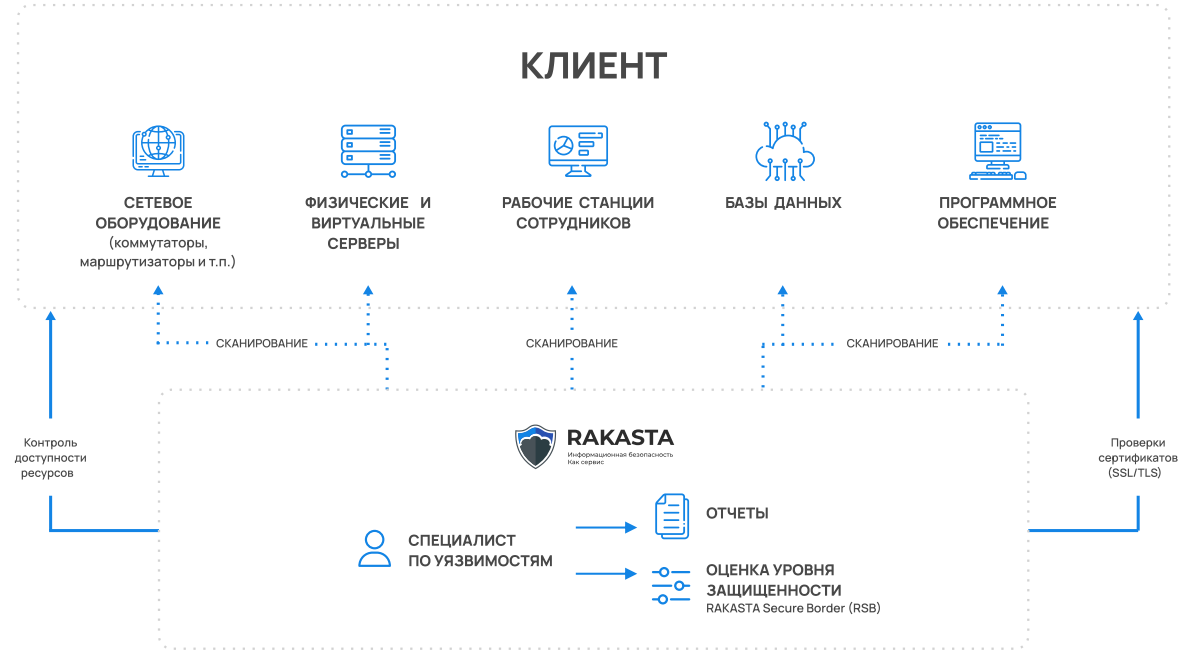
Rakasta

Сервис

Управление внешними уязвимостями и контроль периметра

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

Как работает сервис



100

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

Rakasta

Сервис

Управление внутренними уязвимостями с аутентификацией

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

Закрываемые требования PCI DSS 4.0.1 :
11.3.1.2

Как работает сервис

В каждой третьей успешной атаке на организации злоумышленники эксплуатировали уязвимости

34%

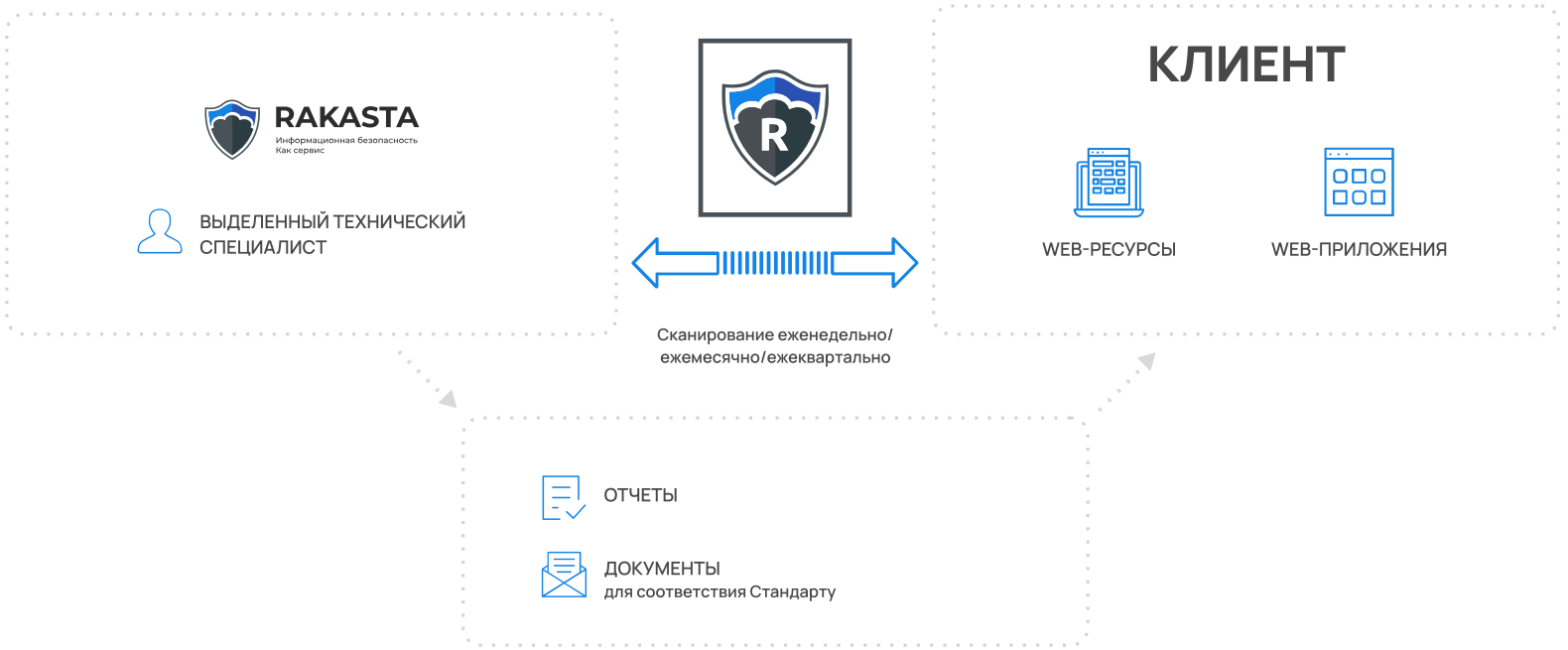
Rakasta

Сервис

Безопасность web-ресурсов

Регулярное проведение сканирований и контроль защищенности внешних и внутренних веб-ресурсов позволят снизить вероятность успешных кибератак и утечек конфиденциальных данных.

Как работает сервис



53%

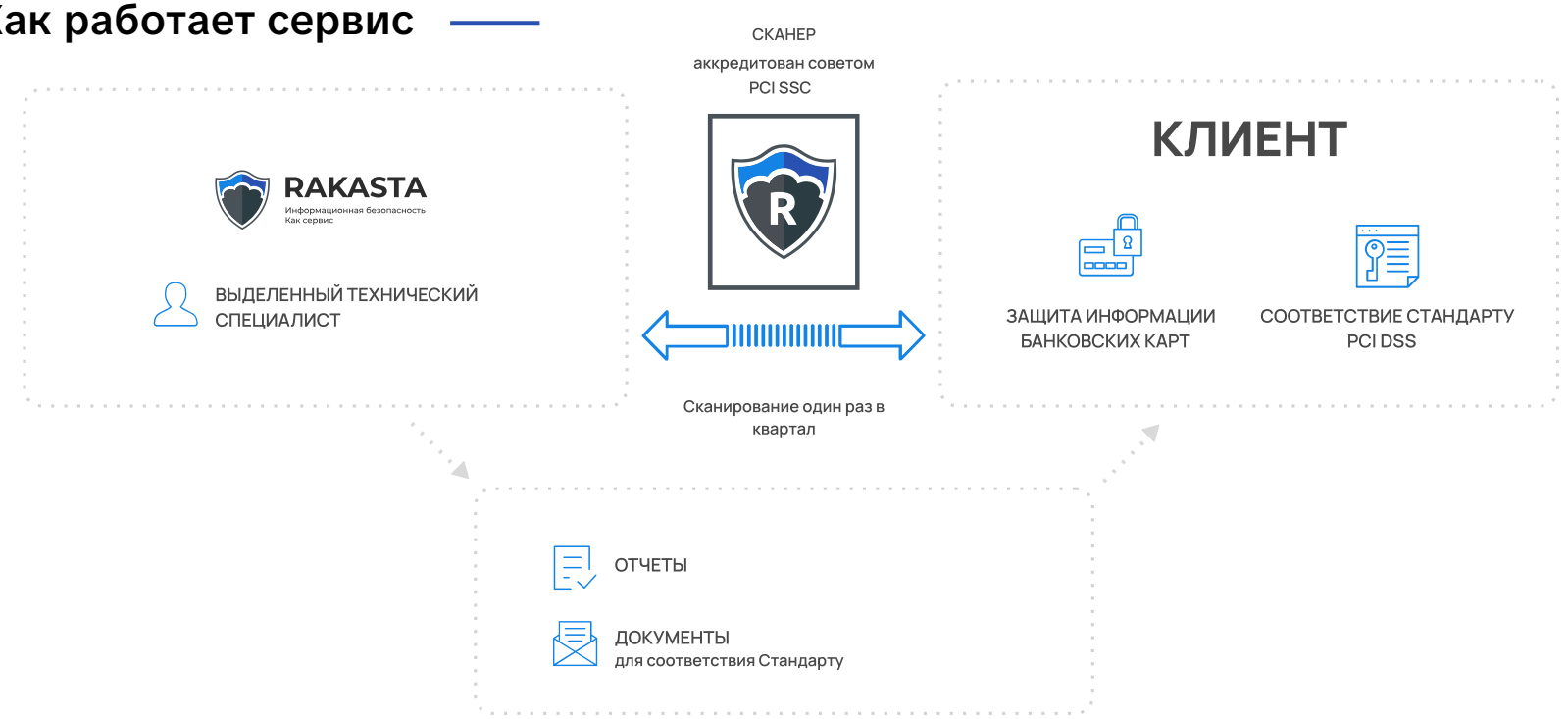
организаций имеют низкий уровень защищенности web-приложений

Сервис

ASV-сканирование по требованиям PCI DSS 4.0.1

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.

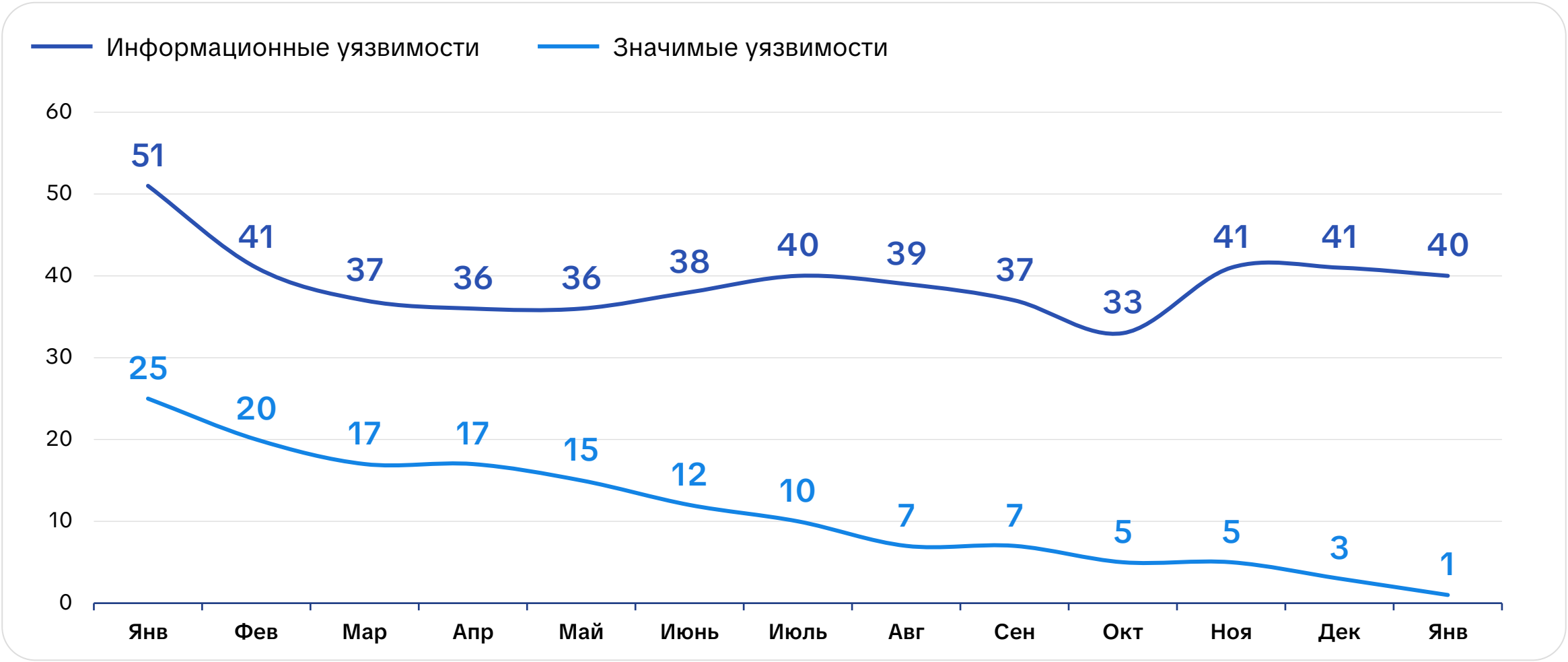
Как работает сервис



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

Rakasta

Пример снижения критичных уязвимостей при использовании сервиса в течение года



Rakasta

03

Контроль защищенности

Rakasta

Контроль защищенности

Нацелен 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

ТОП-3

Финтех входит в ТОП-3 организаций по утечкам данных за 2025-й год!

Rakasta

Сервис

Контроль целостности файлов FIM

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

Возможность интеграции FIM с нашим облачным SIEM.

PCI DSS 4.0.1 требования:

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

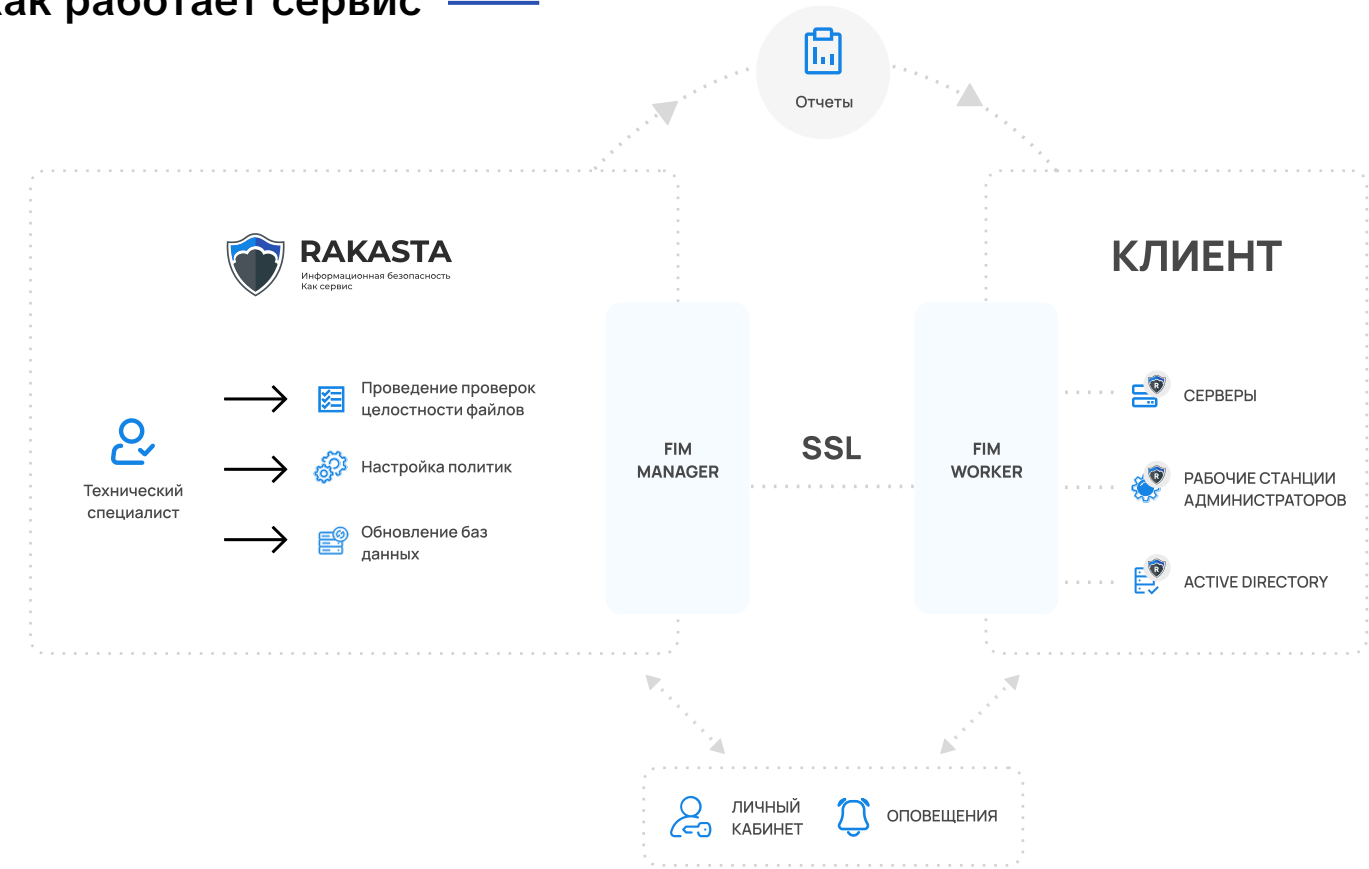
10.2.1.1 Audit logs capture all individual user access to cardholder data.

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



Rakasta

Сервис

Контроль целостности веб-страниц PIM

В режиме реального времени осуществляет непрерывный мониторинг целостности веб-страниц и JavaScript-файлов, осуществляя своевременное обнаружение несанкционированных изменений клиентского кода, включая внедрение вредоносных скриптов и подмену логики.

PCI DSS 4.0.1 требования:

6.4.3: Managing risks associated with changes to payment form pages.

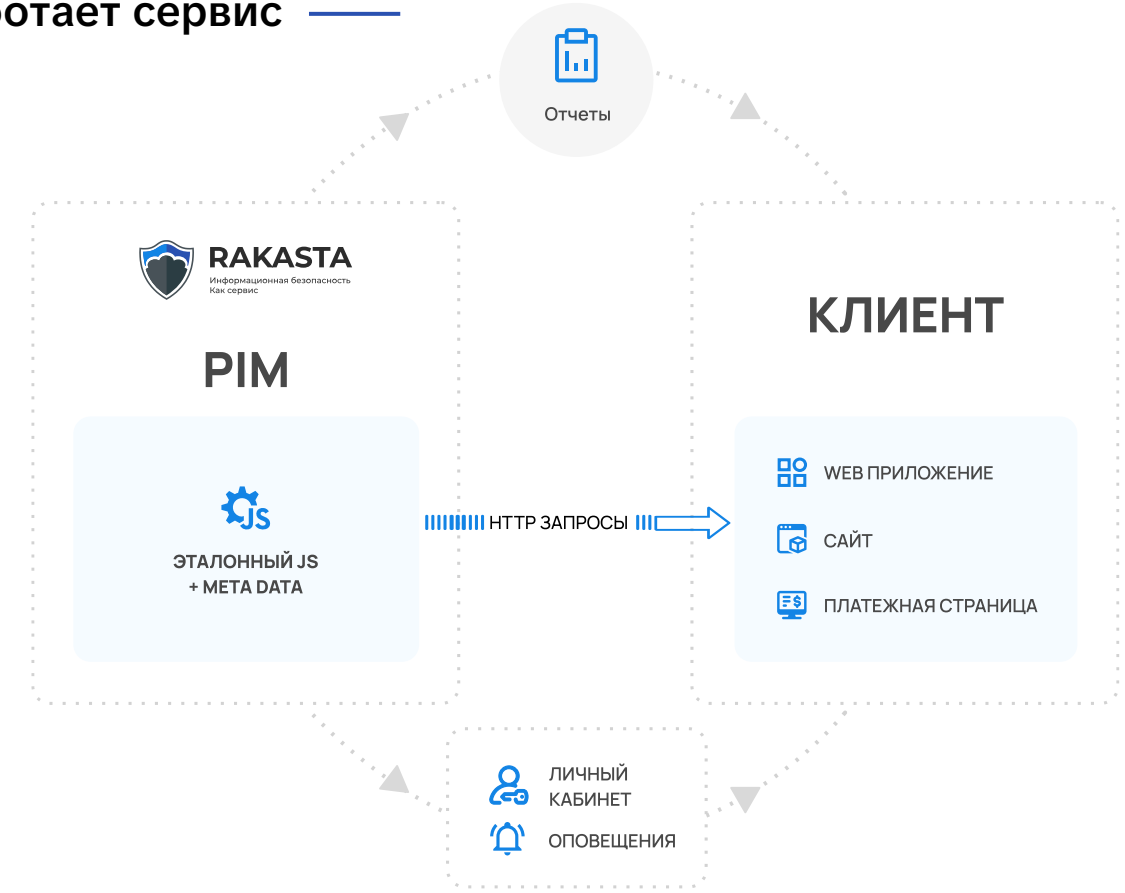
6.2.1: Eliminating system and software vulnerabilities.

11.6.1: Detecting and responding to unauthorized changes.

11.4.1: Detecting and preventing web attacks.

4.1: Using strong cryptographic protocols.

Как работает сервис



Rakasta

Сервис

Защита веб-приложений WAF

Фильтрации трафика прикладного уровня, специально ориентированные на веб-приложения.

Защита от атак из списка OWASP Top 10 (SQL-Injections, Broken Authentication and Session Management, XSS и др.)

PCI DSS 4.0.1 требования:

6.4.1 (Customized Approach): Securing Public-facing Web Applications.

6.4.2 (Defined Approach): Installation of technical protective measures.

11.6.1: Detection and prevention of intrusions and unauthorized changes.

6.4.3 Managing scripts on the payment page

Как работает сервис

Rakasta

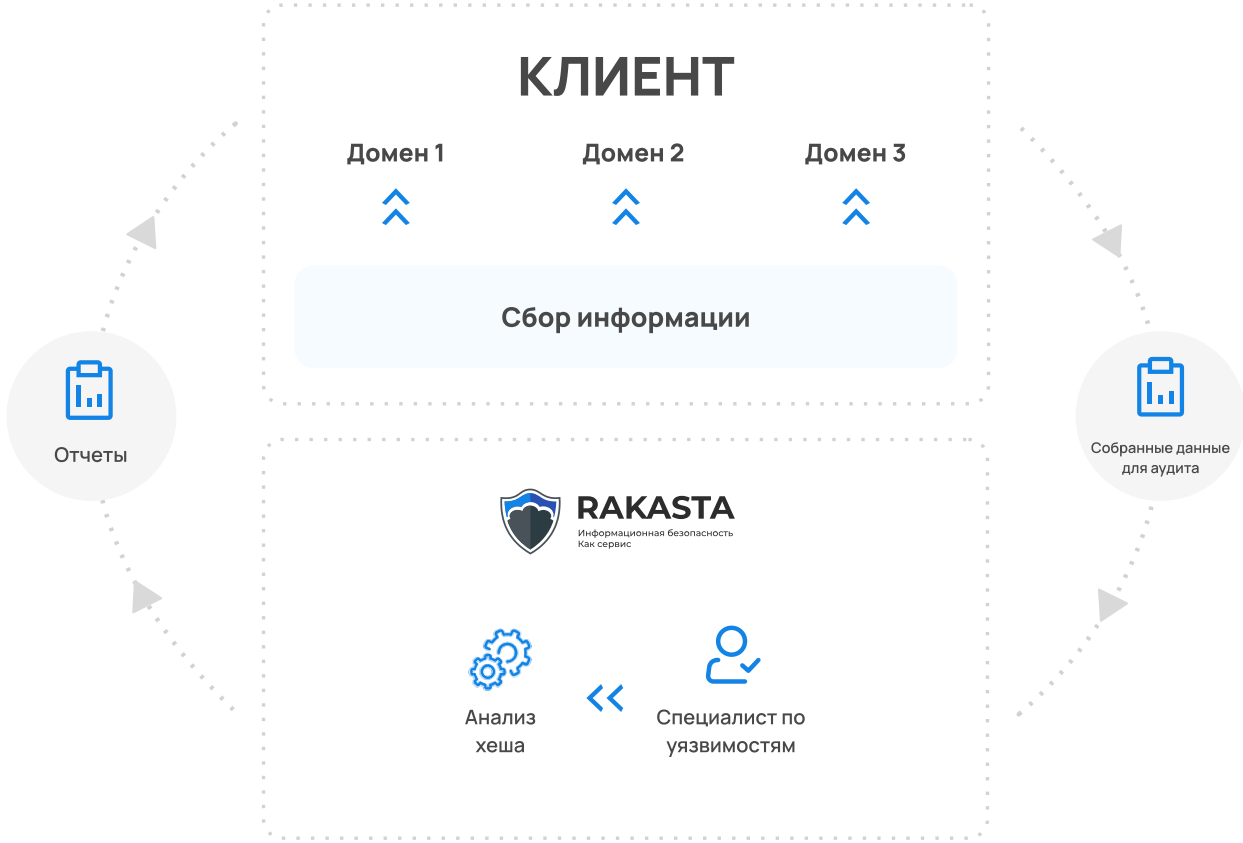
Сервис

Аудит паролей в среде AD

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

- Сервис позволяет выявить пароли, которые когда-либо утекали в глобальную сеть Интернет.
- Проверка идет по базе, состоящей из более чем 800 миллионов паролей, уже слитых в сеть.
- База постоянно обновляется.

Как работает сервис



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 противодействия 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

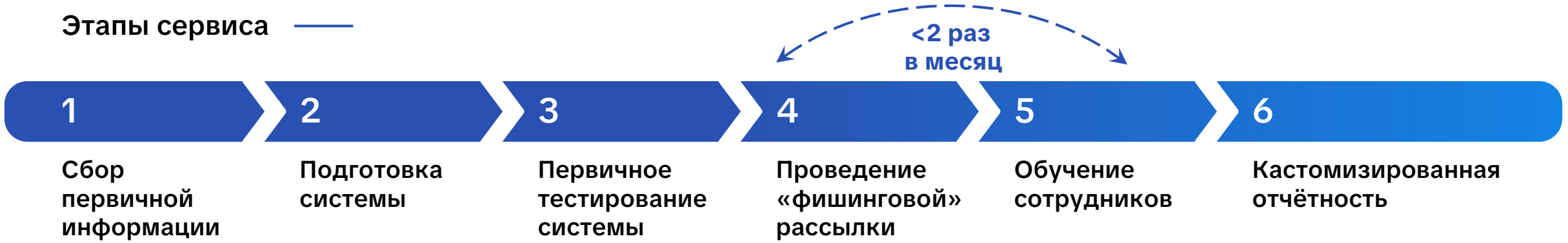
Сервис

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



Требование PCI DSS 4.0.1

12.6.1: Implement a security awareness program for all personnel.

79%

фишинга злоумышленники маскируют под финансовую документацию

Rakasta

Сервис

Социальная инженерия

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

Этапы сервиса

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

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

Rakasta

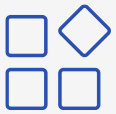
05

Secure SDLC

Rakasta

Secure SDLC (Secure Software Development Lifecycle, 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

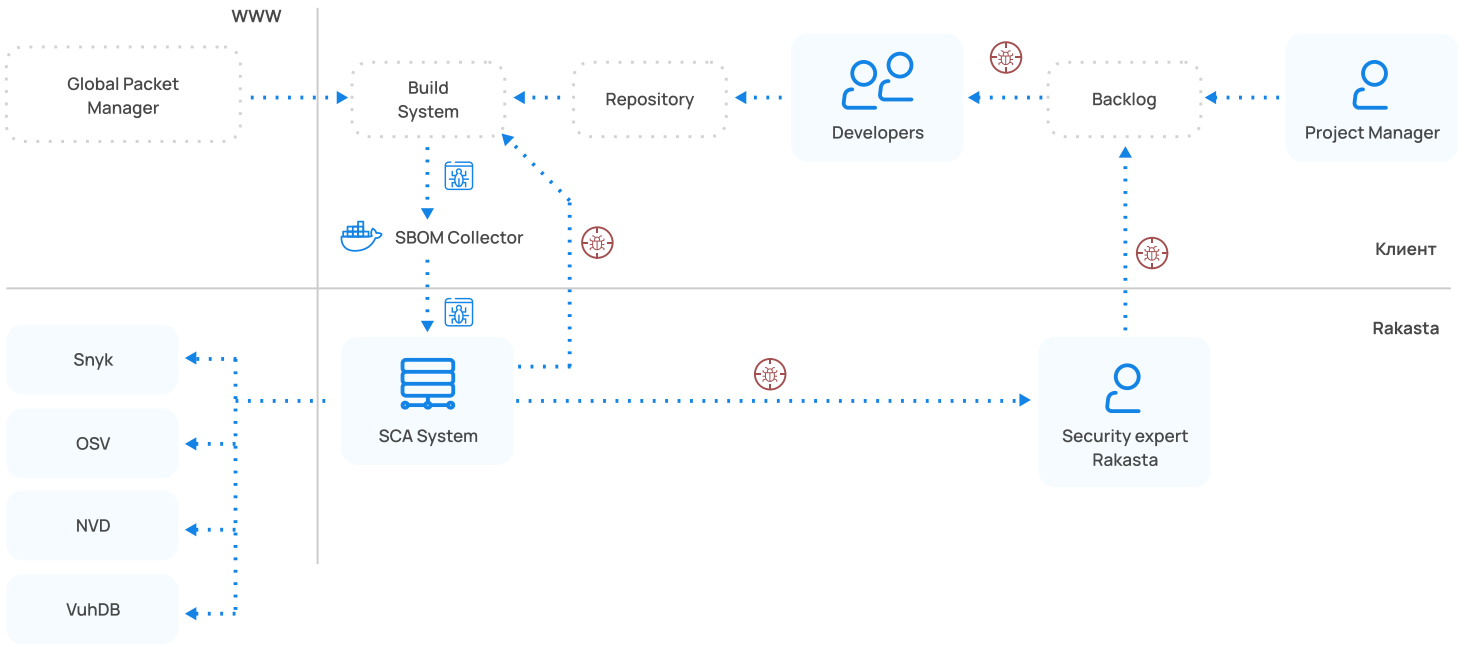
Анализ библиотек и компонентов разработки (software composition analysis) (SCA)

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 код и работоспособность ваших приложений.

Как работает сервис



Rakasta

Сервис

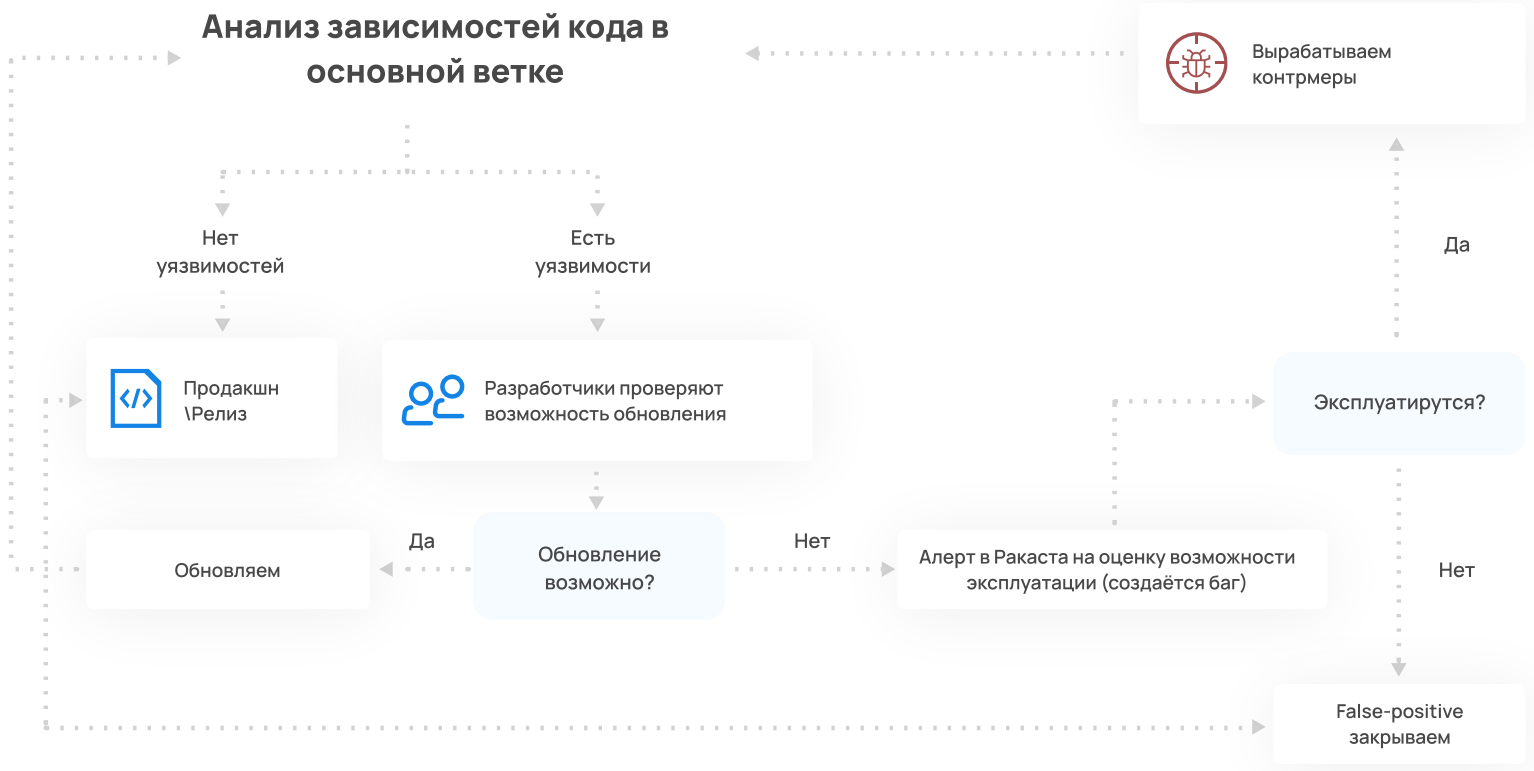
Анализ библиотек и компонентов разработки (software composition analysis) (SCA)

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



Rakasta

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.

ВАЖНО!

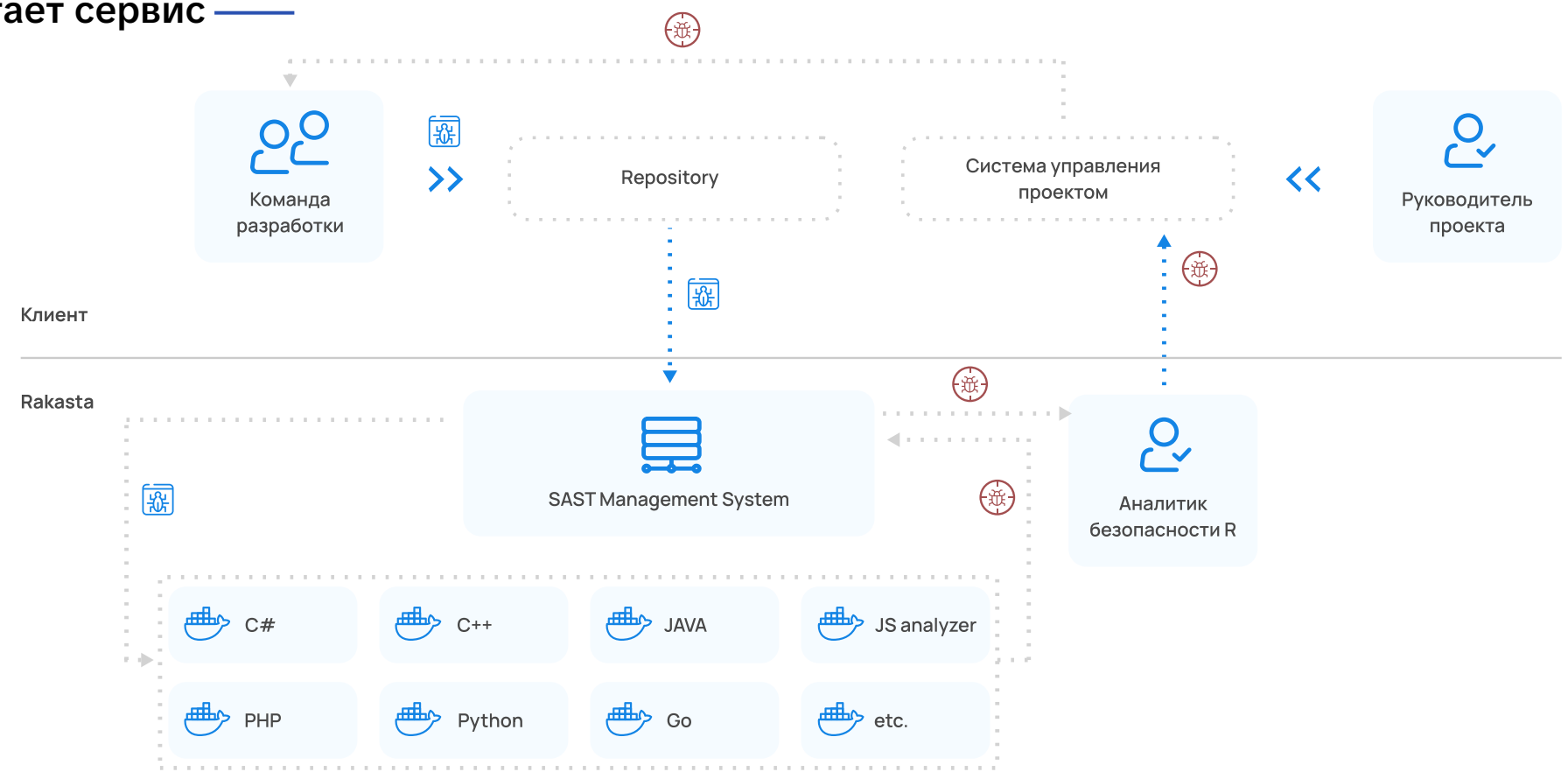
Сокращение времени на прохождение сертификации (PCI SSF, ОУД4 и др.)

Rakasta

Сервис

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

Как работает сервис



Rakasta

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

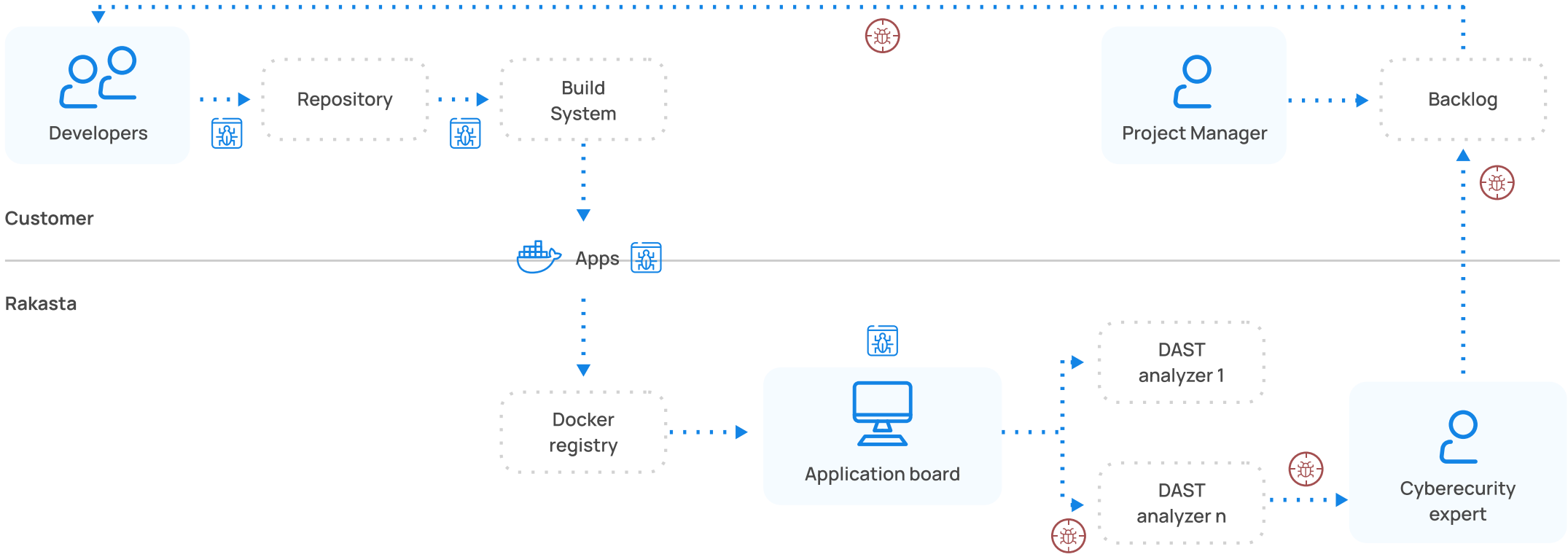
OWASP TOP 10

Rakasta

Сервис

DAST (dynamic application security testing) as a service

Как работает сервис



Rakasta

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 корреляции 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 на абстрактном стенде.

ВАЖНО!

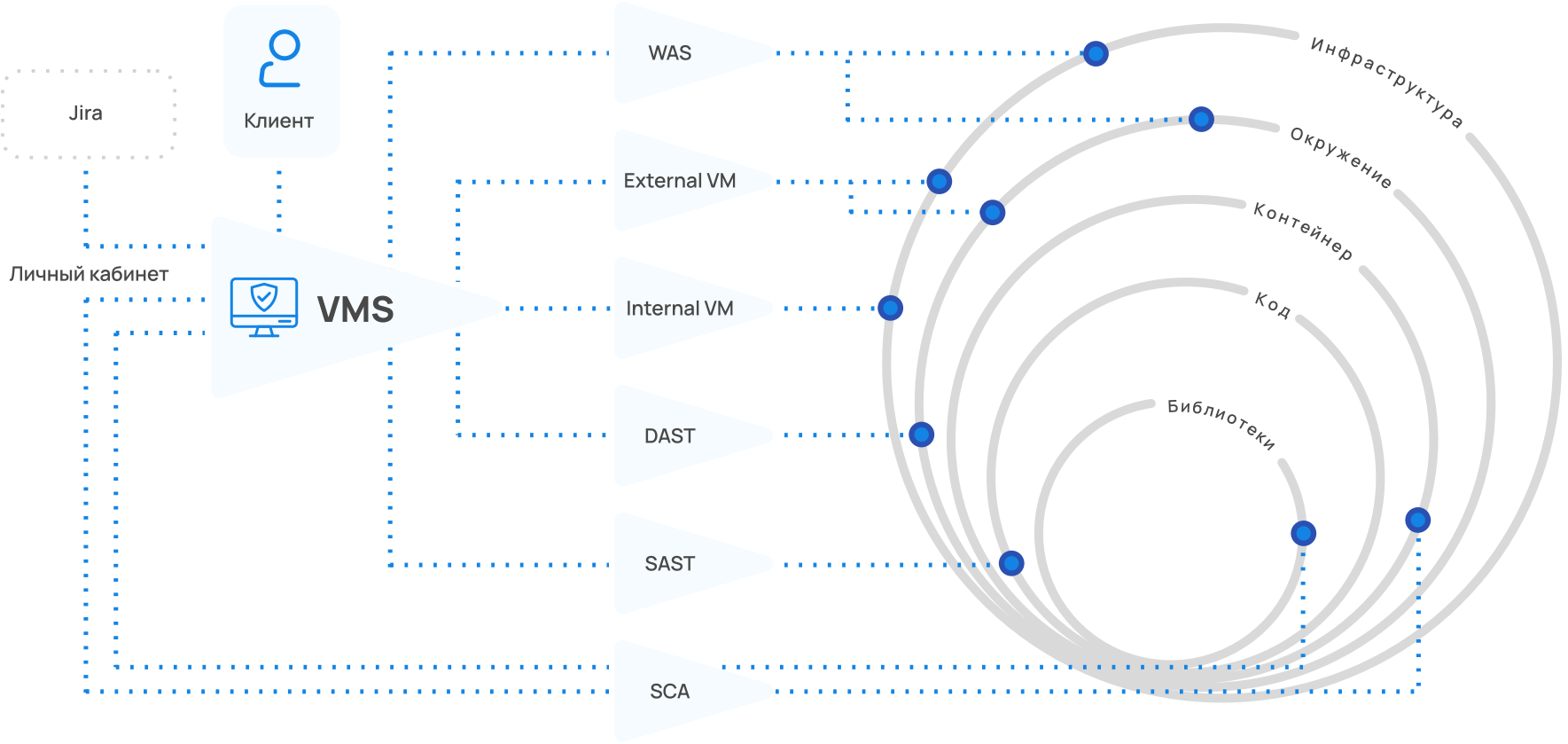
Используя единую консоль с ролевым доступом, сервис «Vulnerability Management System» позволяет работать с данными по выявленным уязвимостям на всех уровнях, помогая в их устранении и приоритезации.

Rakasta

Сервис

Vulnerability management system (VMS)

Как работает сервис



Rakasta

О компании

Наш опыт

10+
лет опыта

40+
экспертов

Наши клиенты

10+
стран

1500+
клиентов
каждый год

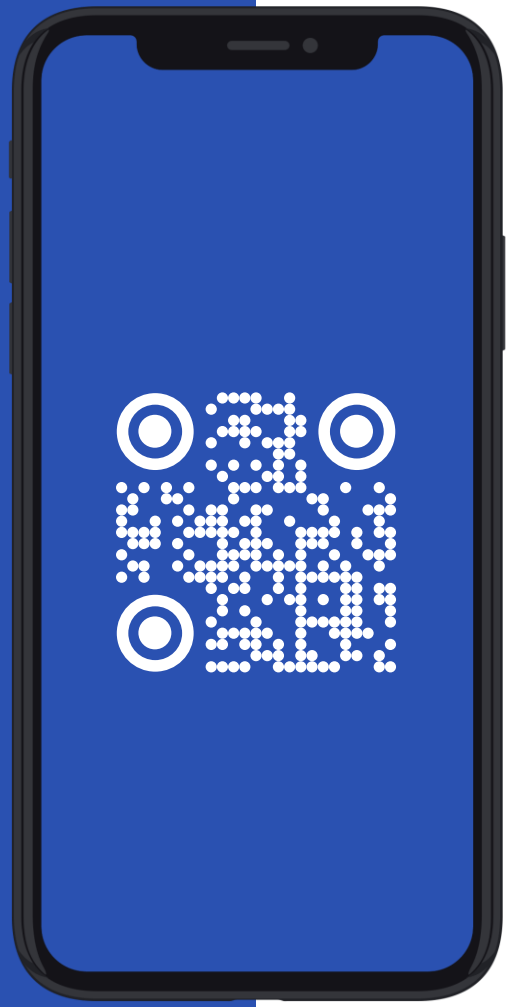
Доверьте нам решение вопросов информационной безопасности вашего бизнеса

И сконцентрируйтесь 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

Артем Покровский
Пресейл-менеджер

+7 (987) 916-27-40

a.pokrovskiy@rakasta.ru