Yandex Cloud

Безопасность в Yandex Cloud

Безопасность данных и ИТ-систем клиентов — фундаментальный приоритет нашей облачной платформы. Мы инвестируем в развитие собственных сервисов и рекомендаций в области защиты данных, регулярно проходим аудиты и повышаем уровни соответствия ключевым стандартам индустрии. Для нас важно быть надёжным партнером и помогать обеспечивать безопасную работу в облаке 28 тысячам клиентам, среди которых крупнейшие компании в России.

100+
человек во внутренней команде безопасности

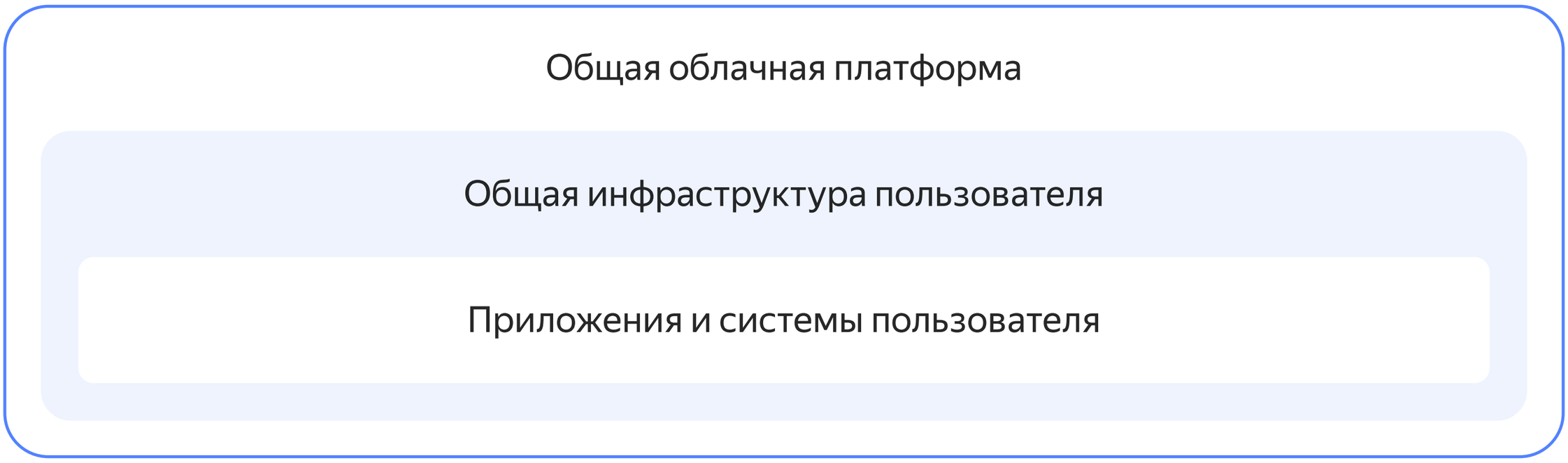
×3,4
рост потребления сервисов Security

820 млн
планирует потратить платформа на развитие безопасности в 2023 году

Первые разработали Стандарт защиты облачной инфраструктуры

В облачной индустрии существует концепция совместной ответственности за обеспечение безопасности. Используя технологии провайдера, компания-клиент делегирует часть задач по защите инфраструктуры облачной платформе. Граница разделения ответственности зависит от сервисов, запущенных в облаке, от модели использования этих сервисов (IaaS — инфраструктура как услуга, PaaS — платформа как услуга, SaaS — программное обеспечение как услуга).

Мы, как и многие провайдеры в мире, придерживаемся этой концепции, при этом выстраиваем работу в Yandex Cloud так, чтобы не только обеспечивать безопасность облачной платформы, но и помогать компаниям-клиентам обеспечивать end-to-end защиту на всех уровнях работы в облаке:



На уровне самой облачной платформы

1

Мы обеспечиваем максимальную защищенность нашей инфраструктуры для клиентов. К ней относятся как физическая безопасность дата-центров, так и защита облачных сервисов платформы.

На уровне облачной инфраструктуры пользователя

2

Мы помогаем клиентам снизить риски при создании облачной инфраструктуры и управлении ей. Для этого мы придерживаемся принципа security by default по отношению к пользовательским настройкам, совершенствуем механизмы защиты: аутентификацию, шифрование данных и мониторинг событий безопасности.

На уровне приложений и систем пользователя

3

Мы предлагаем пользователям комплекс инструментов, который позволяет безопасно разрабатывать и запускать готовые приложения в облаке. Например, развиваем собственные сервисы для защиты веб-ресурсов и технологии сканирования. Часть нашей ответственной политики — помощь в предотвращении киберинцидентов в ИТ-системах клиентов, которые могут повлиять на тысячи компаний и миллионы пользователей.

Как мы делаем инфраструктуру нашей платформы безопасной

1

Мы комплексно подходим к обеспечению безопасности инфраструктуры Yandex Cloud. Это и регулярное прохождение внешних аудитов, тестирований на проникновение, и получение сертификаций, и реализация технических мер защиты. Мы развиваем внутреннюю команду ИБ-специалистов и регулярно обучаем разработчиков новым практикам в области информационной безопасности.

12

пройденных внешних аудитов

5.7 млн

составили выплаты облачной платформой по программе bug bounty Яндекса

1500+

часов потратила команда пентестеров для проверки безопасности инфраструктуры

Прозрачность в прохождении аудитов и соответствии стандартам

Сервисы Yandex Cloud соответствуют требованиям международных и национальных стандартов ISO, GDPR, PCI и ГОСТ Р 57580. Платформа выполняет все требования 152-ФЗ и обеспечивает первый уровень защищённости персональных данных (УЗ-1).

Мы регулярно совершенствуем и повышаем уровни соответствия стандартам. Так, в 2023 году мы стали первой облачной платформой в России, которая получила наивысшую оценку по «усиленному» уровню защиты информации в рамках ГОСТ 57580. Это национальный стандарт безопасности банковских и финансовых операций.

Соответствовать всем стандартам индустрии нам помогают постоянные внутренние и внешние аудиты. За последний год мы прошли 12 проверок безопасности с привлечением экспертов-консалтеров. Вся информация о сертификациях и аудитах доступна на официальном сайте платформы. А по дополнительному запросу пользователей мы предоставляем расширенную информацию о моделях угроз и отчёты по результатам тестирования на проникновение.

ГОСТ Р 57580 · GDPR · ФЗ-152 · Стандарты ISO · CSA · Реестр ПО · Стандарты PCI

Кроме этого, облачная платформа участвует в программе Яндекса «Охота за ошибками». Это постоянная программа компании по премированию этичных хакеров — тех, кто разбирается в компьютерной безопасности, находит уязвимости в продуктах и сообщает им об этом за награду.
За последний год облачная платформа выплатила охотникам 5,7 млн рублей и за счёт их отчётов укрепила защиту своих сервисов. Также Yandex Cloud привлекает экспертов для Pentest и Red Teaming. Это позволяет автоматизировать реагирование на инциденты и узнавать актуальную информацию об инструментах и тактике атакующих.

Строгая регламентация физической безопасности

Для размещения аппаратных ресурсов в Yandex Cloud используют оборудование, спроектированное специалистами Яндекса. Доступ на территорию дата-центров строго регламентирован — нельзя зайти внутрь без предварительно одобренной заявки. Аппаратные ресурсы Yandex Cloud располагаются в трёх географически распределённых дата-центрах на территории России, связанных собственными каналами.

Серверные стойки для дата-центров мы проектируем и собираем сами так, чтобы они могли выдержать любую нагрузку. Все объекты облачных сервисов (серверные стойки, ящики, зоны диагностики оборудования) постоянно находятся под видеонаблюдением, а записи с камер хранятся на серверах компании не менее трех месяцев.

Есть отдельные правила для работы с оборудованием: новое серверное оборудование обязательно проверяется — аппаратная часть проходит тестирование, а критические части стороннего программного обеспечения с открытым кодом переподписываются с помощью внутренних ключей. Такие регламенты позволяют контролировать целостность оборудования и защищают от подмены ПО. Вышедшее из строя оборудование хранится в специальных сейф-пакетах, не заменяется и не выносится из помещений без специальной заявки, а данные каждого жёсткого диска обязательно удаляются, если диск планируется использовать заново. Вышедшее из строя оборудование уничтожается в пределах дата-центров.

Многоуровневая безопасность виртуальной среды

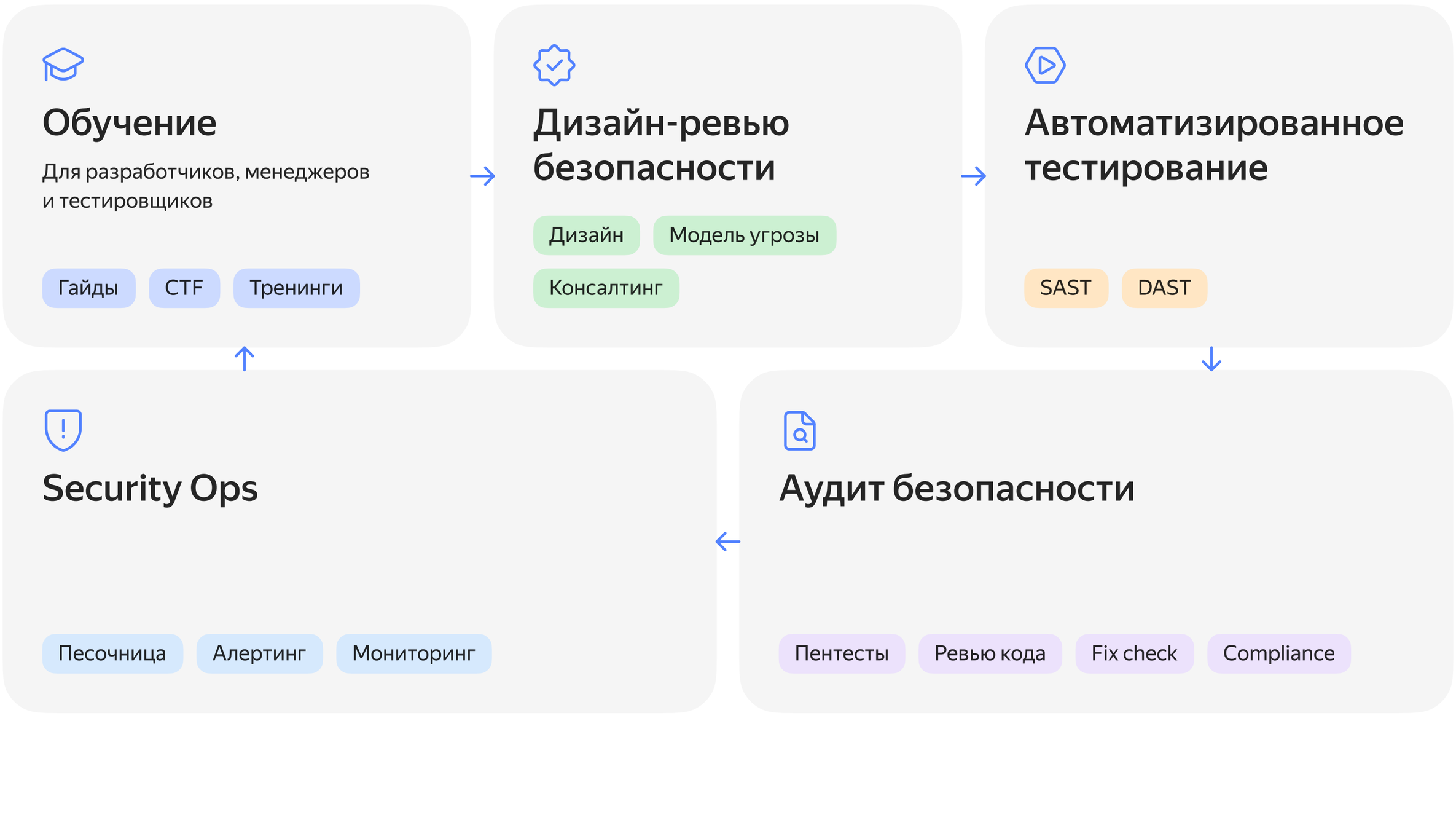
Безопасность виртуальной среды основывается в первую очередь на механизмах изоляции инфраструктуры пользователей друг от друга. У изоляции есть несколько уровней. Например, на уровне гипервизора, на уровне виртуальной сети, на уровне виртуальных дисков и так далее.

Каждая виртуальная машина пользователя дополнительно размещена в sandbox (среде безопасного тестирования), которая обеспечивает дополнительную защиту и помогает детектировать атаки вида “vm escape” (побег из виртуальной машины). При этом планировщик виртуальных машин и операционная система настроены так, чтобы защищать от утечек информации по побочным каналам.

Внедрённые процессы безопасной разработки

Все сотрудники проходят обучение, которое помогает писать более безопасный код и думать о безопасности сервиса при его проектировании. Это обязательные ежегодные тренинги, встречи с экспертами из индустрии, игра Capture The Flag, которая помогает избегать ошибок при проектировании и разработке реальных сервисов.

Мы регулярно тестируем код на наличие уязвимостей. Команды используют инструменты динамического анализа для sanity- и fuzzy-тестирования. А перед выходом каждого сервиса в продакшн или при добавлении в него существенных изменений проводим анализ защищённости. При этом проверяется не только сам сервис, но и окружение, в котором он функционирует.



Ответственная работа с доступами

В Yandex Cloud внедрен принцип минимальных привилегий. У сотрудников платформы нет бесконтрольного доступа к данным. Если клиенту нужна помощь, например, в рамках инцидента или оказания поддержки, все действия сотрудника логируются в SOC (Security Operations Center). К критическим системам облака выдается гранулярный доступ, на ограниченное время и только с использованием второго фактора в виде аппаратного ключа.

Чтобы сотрудник мог помочь клиенту, используется специальный сервис — бастионный хост. Это промежуточный сервер, который является посредником, фильтром между сотрудником и продакшн-средой клиента. На сервере выполняется контроль сессий и их запись, многофакторная аутентификация, то есть проверяется безопасность всех действий сотрудника.

Как мы помогаем компаниям безопасно управлять облачной инфраструктурой

2

Главные проблемы в облачной безопасности — небезопасное хранение учетных данных и секретов, отсутствие или слабый контроль доступа к данным, ошибки в конфигурациях инфраструктуры. Чтобы помочь их избегать, нам важно обеспечить пользователя максимально безопасными настройками облака и рекомендациями.

8000+
скомпрометированных секретов обнаружили и оповестили об этом клиентов

5
курсов о безопасной работе в облаке запустили

250+
специалистов уже прошли обучение

Безопасные настройки по умолчанию

Мы придерживаемся принципа security by default. Это значит, что при использовании облака все настройки безопасности включены по умолчанию, чтобы обеспечить высокий уровень защищенности в облаке. Конечно, при необходимости у администратора всегда есть возможность изменить их.

Так, например, группы безопасности (набор правил для входящего и исходящего сетевого трафика) действуют по принципу «запрещено всё, что не разрешено». Также платформа предоставляет встроенные функции шифрования при использовании сервисов.

Разработка собственных стандартов и курсов для пользователей

Согласно отчёту компании Check Point, в 23% случаев небезопасные конфигурации являются причиной успешных атак на сервисы в облаке. Чтобы безопасно использовать десятки облачных сервисов одновременно, компаниям необходима систематизация работы с инструментами защиты провайдера. Для этого мы разработали собственный Стандарт по защите облачной инфраструктуры. Это рекомендации, которые компании могут использовать для построения защищенных информационных систем в облаке и создания корпоративных политик безопасности. В каждом разделе пользователи могут найти пошаговые инструкции по настройке сервисов в Yandex Cloud, примеры кода, ссылки на обучающие материалы. Кроме этого, компании могут использовать Стандарт в рамках аудита на соответствие требованиям обработки данных по ФЗ №152 «О персональных данных».

Также мы запустили программу обучения по информационной безопасности в облаке. Это помогает пользователям Yandex Cloud эффективно и безопасно выстраивать работу на облачной платформе. Многие команды сталкиваются с публичными облаками впервые, и курсы позволят быстро освоить необходимые навыки для выстраивания защиты инфраструктуры и приложений в облачной среде. Обучение помогает управлять доступами, выстраивать процессы безопасной настройки, предотвращать уязвимости ИТ-систем, настраивать защиту виртуальных машин от DDoS-атак и не только.

Проактивная помощь в обнаружении утечек и инцидентов

Для анализа и объективной оценки рисков мы предоставляем пользователям готовые инструменты и механизмы безопасности. Пользователи платформы уже применяют сервис Audit Trails, который позволяет контролировать соблюдение установленных процедур и стандартов безопасности компании.

Также мы разработали собственный механизм поиска утекших секретов. Если секрет попадает в один из публичных репозиториев на GitHub или в поисковый индекс Яндекса, то мы проверим валидность облачных учетных данных и направим уведомления на почту, а также настроим отправку событий безопасности в сервис Audit Trails.

Yandex Cloud

Здравствуйте!

Мы обнаружили в открытом доступе конфиденциальную информацию, связанную с вашим аккаунтом:

— **часть токена**: aaa t1.9euel…4TDw

— **хэш**: 1920508487739919229

Данные были найдены на этом сайте: https://github.com/yandex-cloud/yc-solution-library-for-security/blob/725c6095921dfca17f5be2ae0cbc44939ef66466/malware-defense/kaspersy-install-in-yc/test-token

Возможно, данная информация была опубликована непреднамеренно (например, учётные данные могли быть по ошибке загружены в GitHub или похожий сервис).

В любом случае обратите внимание: вы являетесь владельцем аккаунта и несёте полную ответственность за безопасность ваших ресурсов.

Как защитить аккаунт

1. Войдите в консоль и просмотрите действия от имени скомпрометированной учётной записи.
2. Отзовите ключи и токены — все или те, которые попали в открытый доступ. Лучше сменить все секретные данные, так как могли быть затронуты все ресурсы.
3. Удалите все неавторизованные ресурсы, если вы их видите.
4. Примите необходимые меры, чтобы данные вашей записи не попали в другие источники, не хранились в каталогах загрузки и не передавались иными способами.

Как мы помогаем компаниям создавать безопасные системы и приложения в облаке

3

Атаки на веб-приложения компаний растут, увеличивается количество уязвимостей в опенсорс-решениях и операционных системах. Мы следим за развитием индустрии для защиты ИТ-систем компаний от атак на цепочку поставок и добавляем необходимые функции безопасности в наши инструменты.

1.5 млн+

сканирований на наличие уязвимостей Docker-образов выполнили пользователи платформы

в 85% случаев

SmartCaptcha отделяет роботов от людей без показа “капчи”

40+

компаний-партнеров по направлению Security

25+

продуктов безопасности доступны в маркетплейсе платформы

Готовые инструменты для защиты веб-ресурсов и API

Для предотвращения и смягчения последствий DDoS-атак на сервисы клиентов платформы в облаке используются различные механизмы защиты — например, фильтрация трафика, ограничение скорости запросов, а также специальные сервисы для анализа и блокировки подозрительного трафика. Yandex Cloud предоставляет сервис защиты от DDoS-атак и будет продолжать развивать собственные механизмы защиты.

Другой готовый сервис — Yandex SmartCaptcha. Он позволяет минимизировать нелегитимные действия роботов на веб-ресурсах компаний клиентов.

Платформа активно сотрудничает с несколькими консалтерами в области информационной безопасности. Эти компании помогают пользователям тестировать инфраструктуру на проникновение, выстраивать процессы безопасной разработки, проходить аттестации и не только. Кроме этого, в маркетплейсе платформы представлены 28 готовых инструментов партнеров для защиты инфраструктуры.

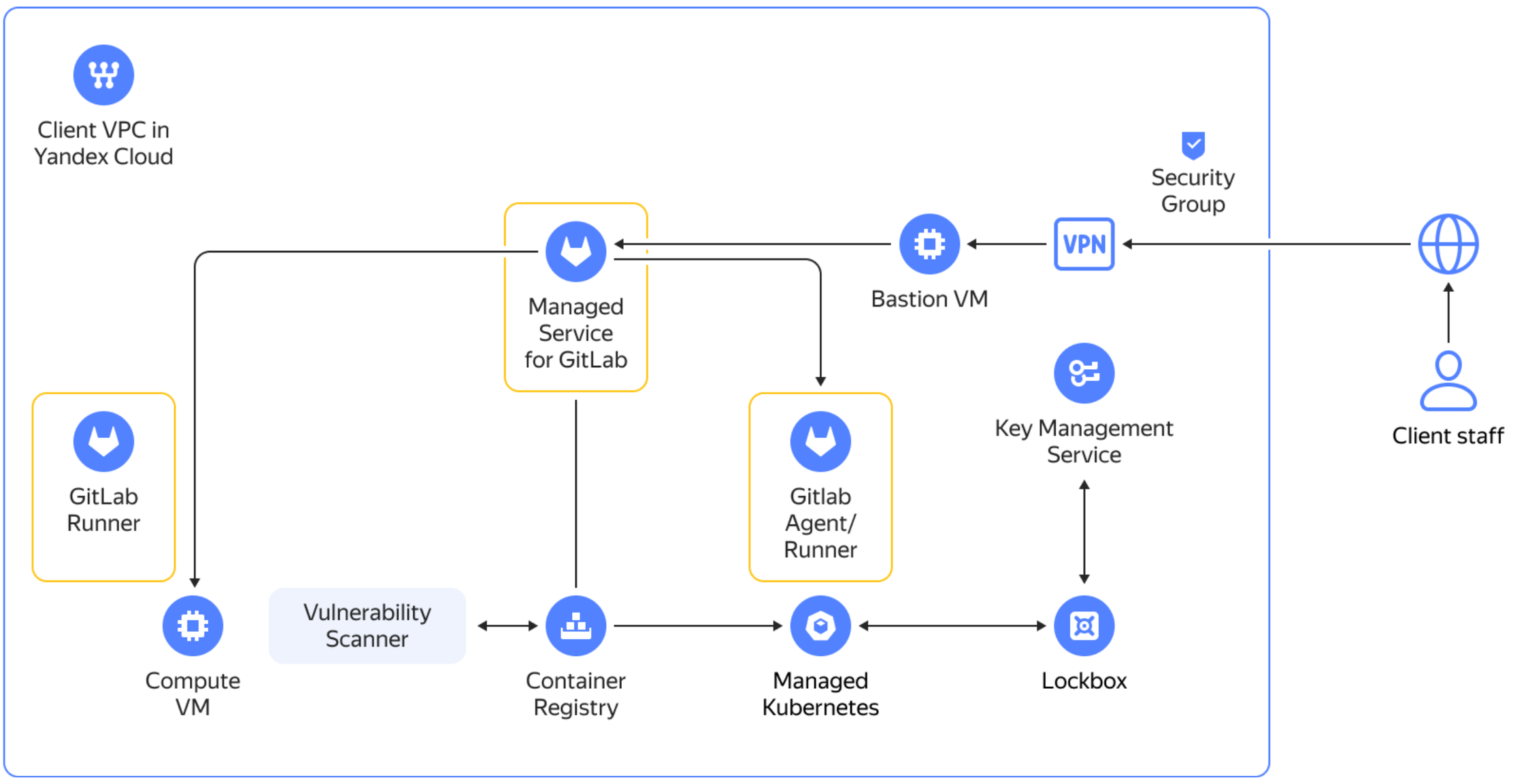
Автоматизация процессов безопасной разработки и защита цепочки поставок ПО

Платформа предоставляет пользователям готовые инструменты, которые помогают легче и быстрее настроить безопасную разработку. Для автоматизации процесса создания и тестирования кода, сборки и выкладки приложений в Yandex Cloud доступны управляемые сервисы GitLab и Container Registry. Кроме этого, платформа предоставляет инструменты и настройки безопасности для построения DevOps-пайплайна: Key Management Service (KMS) для шифрования данных и управления ключами шифрования, SAST- и DAST-анализы в GitLab для проверки исходного кода на наличие распространенных уязвимостей.

В 2023 году на платформе Yandex Cloud появился новый сервис — сканер уязвимостей. Он проверяет на наличие уязвимостей образы, содержащие компоненты и зависимости, необходимые для корректной работы приложений. После этого проходит сравнение содержимого выбранного образа с крупнейшими общеизвестными базами уязвимостей. В итоге пользователь получает подробный отчёт с выявленными проблемами безопасности и возможными исправлениями.

Также платформа Yandex Cloud открыла доступ к собственному сервису для хранения секретов Yandex Lockbox для компаний. Он помогает защищать конфиденциальную информацию для работы с доступами в облаке, например, пароль от базы данных или ключи сертификата сервера.

Инструменты Yandex Cloud для безопасной разработки

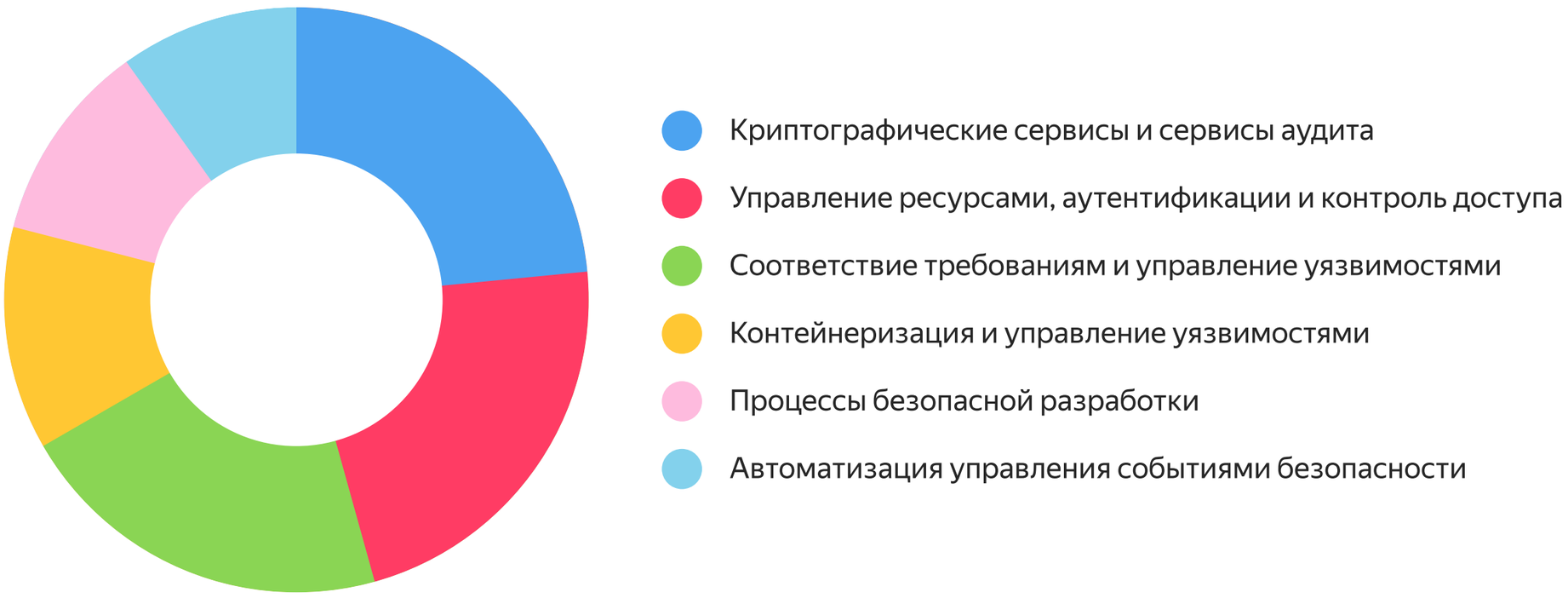


Работа с сообществом

Команда Yandex Cloud развивает платформу в соответствии с общими трендами и острыми проблемами в сфере ИБ-сообщества. За 2023 год мы приняли участие в нескольких крупных конференциях по информационной безопасности в качестве докладчиков, в том числе CISO Forum, PHDays, Paymentsecurity и других. Сама платформа регулярно организует собственные мероприятия по информационной безопасности. Это, например, Yandex Cloud Security, митапы команды Identity Access Management, мероприятия с обзором сервисов Security about:cloud. Также мы ведём диалог с экспертами индустрии, ключевыми вендорами, регуляторами — это делает эффективнее общие усилия в области безопасности. В 2023 году мы запустили медиапроект о безопасной работе в облаке — подкаст “Безопасно говоря”.

О команде безопасности Yandex Cloud

Безопасностью в Yandex Cloud занимаются более 100 специалистов. Они решают задачи автоматизации обеспечения защиты всей инфраструктуры платформы и разрабатывают собственные сервисы безопасности.



Евгений Сидоров

Директор по информационной безопасности

Наша команда — это десятки сильных программистов, инженеров по информационной безопасности, менеджеров по продукту и развитию бизнеса. Мы каждый день улучшаем защиту инфраструктуры платформы и разрабатываем собственные сервисы, чтобы компании и пользователи могли доверять облачным инновациям

Алексей Миртов

Руководитель группы продуктовой архитектуры Security & Compliance

Мы выстраиваем работу так, чтобы помогать бизнесу, ИТ и специалистам по информационной безопасности разговаривать на одном языке. Это помогает организациям формировать целостную культуру безопасности при миграции в облако. А именно — запускать DevSecOps-процессы, выстраивать практическую безопасность и соблюдать требования регуляторов

Мы уделяем приоритетное внимание безопасности данных. Наша цель — помочь клиентам обеспечить желаемый уровень защиты своих данных в облаке с учетом меняющихся требований законодательства, стандартов и актуальных рисков. Для её достижения мы постоянно улучшаем политики, процессы и внедряем дополнительные контроли и сервисы

Екатерина Липова

Руководитель направления по защите данных