



кауч

Комфортное управление

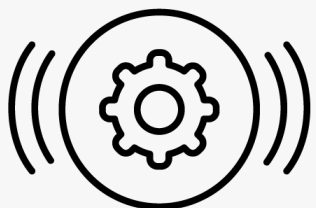
безопасностью конфигураций



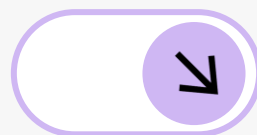
Уязвимости конфигураций

Почему управление безопасностью конфигураций
ИТ-ресурсов важно не только для комплаенса

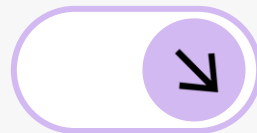
Уязвимости конфигураций



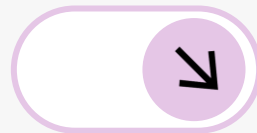
Ошибки
в настройках
штатных
механизмов защиты
ИТ-систем



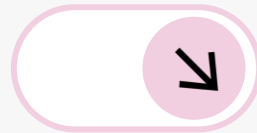
Дефолтные или слабые пароли



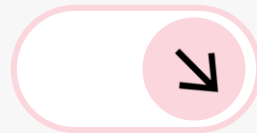
Дефолтные настройки систем



Расширенные права доступа
у обычных пользователей



Отсутствие шифрования
или слабое шифрование

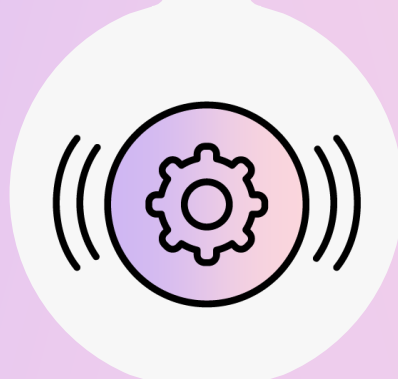


Доступность необязательных
функций систем

Зачем управлять безопасностью конфигураций

Необходимо защищаться от кибератак

Нужно устранять уязвимости конфигураций, чтобы **закрыть для злоумышленников возможность легкого доступа** в корпоративную ИТ-инфраструктуру и быстрого продвижения по ней – а значит, снизить риски финансового или репутационного ущерба



Необходимо соответствовать требованиям

В зависимости от отрасли, **компания должна выполнять требования регуляторов** (например, ГОСТ 57580.1, Указ Президента РФ №250, требования приказа ФСТЭК №117, PCI DSS, SWIFT, ISO 27001 и др.) или каких-либо внутренних политик безопасности

Почему сложно управлять безопасностью конфигураций

>> 1 млн

настроек безопасности ИТ-систем в среднем есть в крупной компании на 10 000 хостов

> 50%

от общего числа уязвимостей в компаниях составляют именно уязвимости настроек

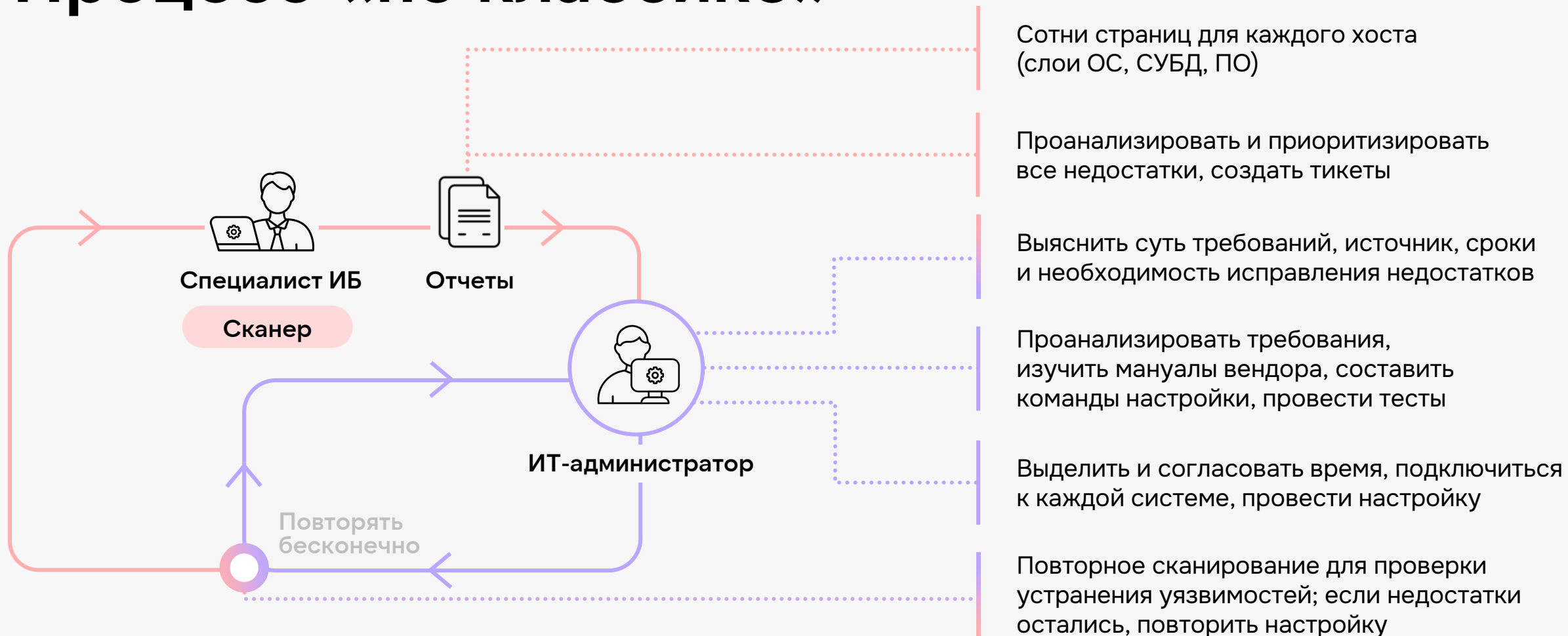
1000+ страниц

в отчете сканера уязвимостей по 1 серверу, который нужно разобрать ИБ и ИТ для исправления настроек

Нет

новостей и «хайпа» вокруг темы уязвимостей настроек, метрик, универсальных средств устранения

Процесс «по классике»



Результат, а не процесс ради процесса

Как Кауч помогает подружить ИБ и ИТ

Кауч

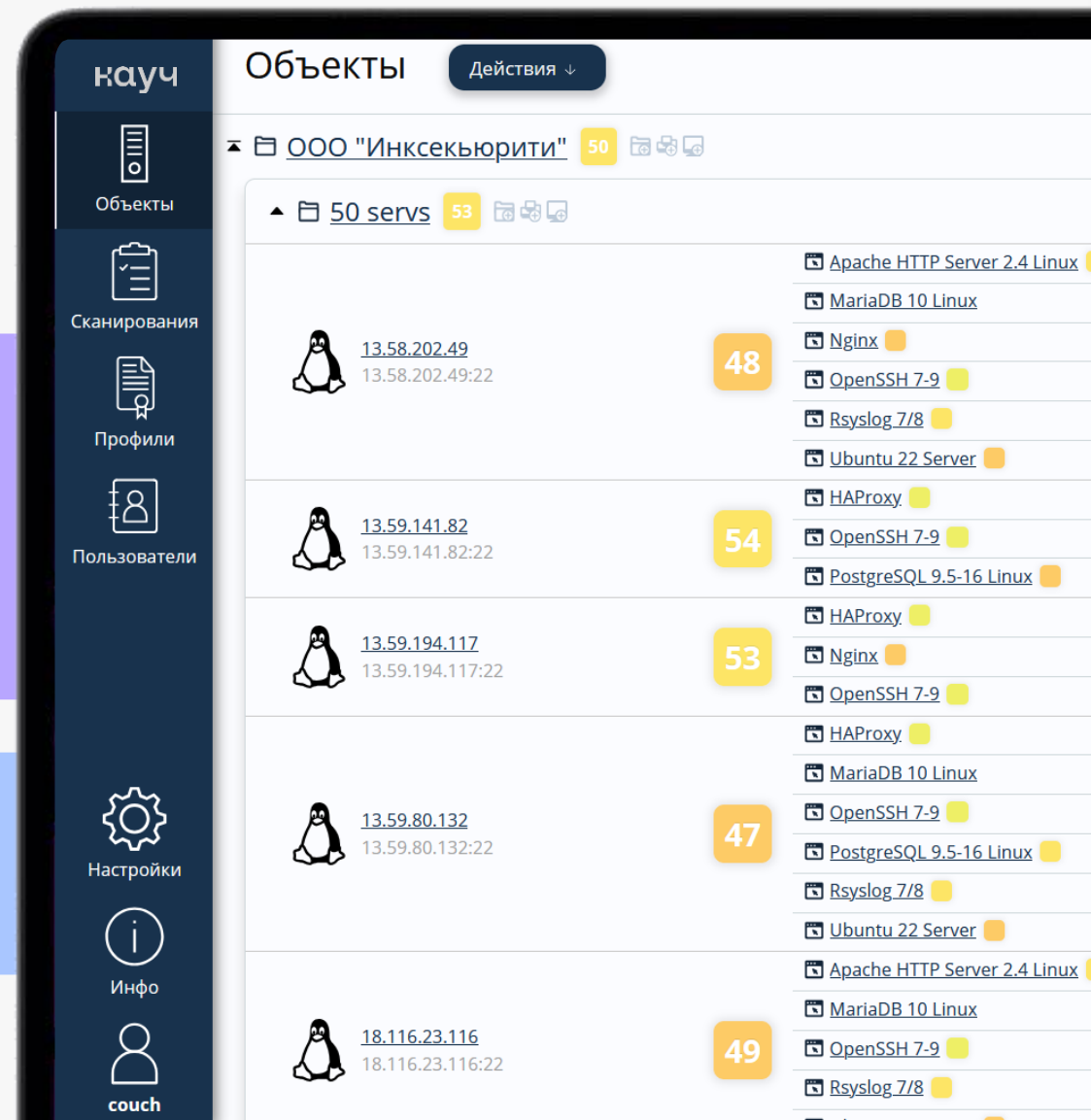
All-in-one платформа для управления безопасностью конфигураций ↗

Единая среда для ИБ и ИТ и всех операций, связанных с управлением безопасностью настроек ИТ-ресурсов

Автоматизированная настройка ресурсов по клику или офлайн с помощью готовых команд и скриптов, доступных «из коробки»

Проверка соответствия ресурсов по клику, расписанию или офлайн с помощью мощного встроенного сканера конфигураций

Гибкое и простое создание политик безопасности любой сложности



Подход Кауча: совместная работа

Управление безопасностью конфигураций



Одна среда для служб ИБ и ИТ и всех операций:

сканирования, настройки и мониторинга. Нет необходимости в рутинных отчетах

CISO, CIO

Получение сводной аналитики для оценки эффективности служб ИБ и ИТ

Внутренние и внешние аудиторы

Самостоятельное получение данных о соответствии компании стандартам в режиме чтения

Воркфлоу ИТ-администратора

старт

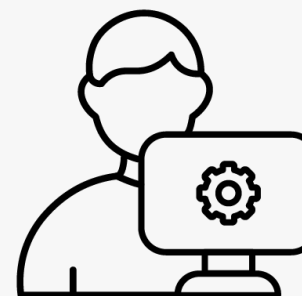
Получить доступ к «своим» ресурсам с уже примененными политиками

Получить актуальный статус по клику для политики целиком или отдельного требования. Создать расписание проверок

Самостоятельно настроить ресурсы в удобное время: из интерфейса или с помощью выгружаемых готовых скриптов и команд

финиш

Поддерживать «здоровье» ресурсов, всегда обладая полной информацией, без запроса ИБ



не
нужно

Зависеть от ИБ на каждом этапе решения задачи

Воркфлоу специалиста ИБ

редко

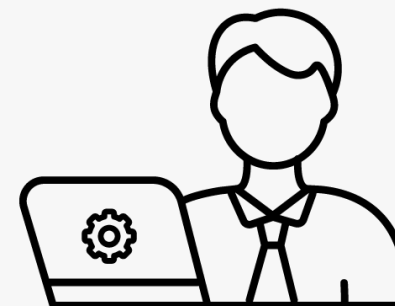
Создать необходимые политики с помощью готовых шаблонов или инструментов для создания собственных требований

Применить политики к ресурсам

Внести новые ресурсы, создать новые учетные записи, распределить права

регулярно

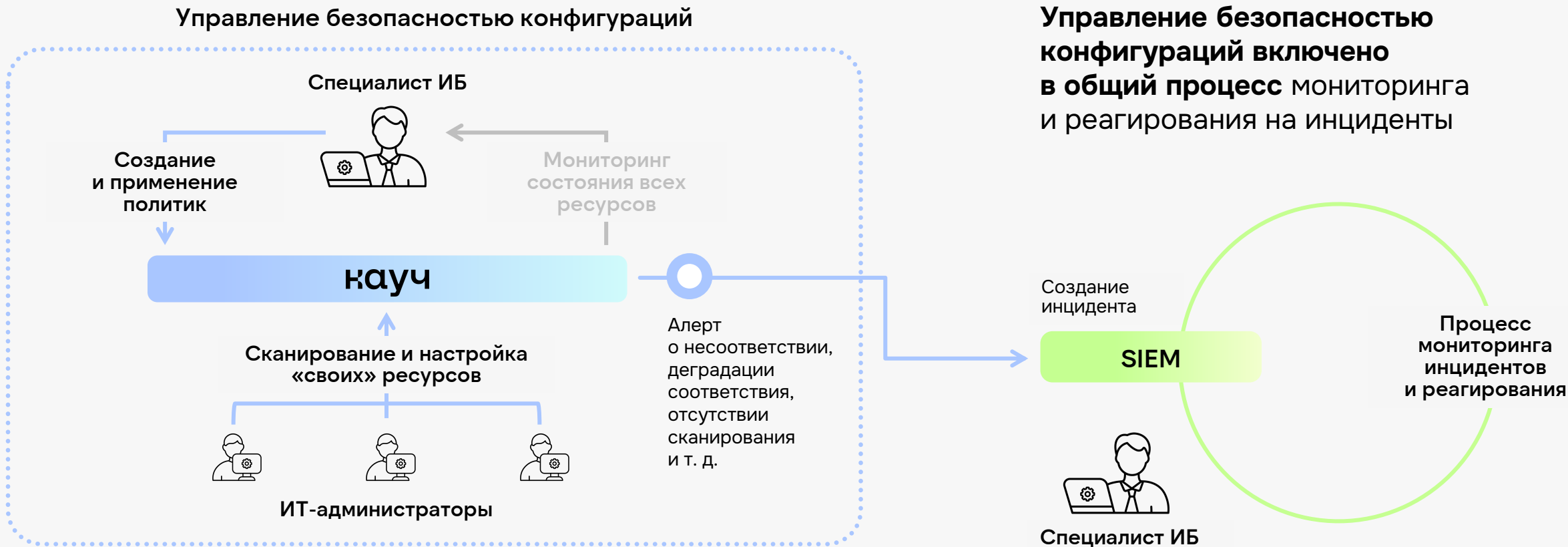
Проводить мониторинг устранения уязвимостей: с помощью сводных данных по всем системам или отдельным ресурсам



не
нужно

Быть фултайм оператором сканера уязвимостей

Подход Кауча: единый процесс



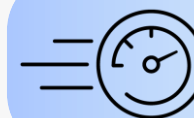
Быстрое и удобное сканирование



Доступно **сканирование в любой конфигурации:** всех ресурсов, отдельного ресурса, компонентов ресурса или отдельных требований



Результат проверки ресурса сразу доступен ИТ-администратору; он может сразу приступить к устранению уязвимости без запроса от ИБ



Перепроверка отдельного требования для получения статуса ресурса **занимает секунды** и не требует полного повторного сканирования

→ Полная проверка всей ИТ-инфраструктуры занимает не более 10 минут

Быстрая настройка ресурсов



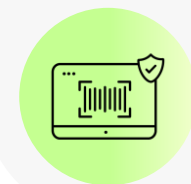
Несколько доступных опций настройки

Настройка ресурсов может производиться онлайн одним кликом в интерфейсе или выгружаемыми командами и скриптами



Готовый инструментарий для работы

Готовые скрипты и команды для настройки систем в соответствии с лучшими практиками поставляются «из коробки»



Полностью прозрачная работа с настройками

Все команды и скрипты доступны в интерфейсе для выгрузки; их содержимое доступно для изучения в открытом виде

Работа с системами офлайн



Без ограничений

Кауч обеспечивает сканирование и настройку даже тех систем, у которых нет сетевого доступа или установлен запрет на внешнее подключение



Проверка офлайн

Кауч позволяет в одно действие выгрузить скрипты для офлайн-сбора данных. После сбора данные о ресурсе и его соответствии политикам загружаются в продукт



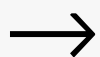
Настройка офлайн

На основе данных о состоянии просканированного ресурса автоматически создаются доступные для скачивания скрипты и команды настройки офлайн



Без скрытых действий

Содержимое скриптов и команд для офлайн-настройки также доступно для оценки ИТ-администратора. Это полезно в случае, если система является критически важной



Простая автоматизация сбора настроек в 3 строки скрипта через API без учетных записей и агента



Гибкое управление политиками

Готовые шаблоны

Готовые требования можно добавлять из шаблонов в собственную политику парой кликов: как целиком, так и выборочно



Быстрое создание и тесты «на лету»

Можно создавать свои проверки с нуля или путем редактирования требований из шаблона, а также тестировать их в реальном времени



Максимальная кастомизация

Можно настраивать любые параметры готовых требований (включая уровень риска, описание, команды настройки/сбора)



Отечественная разработка



Продукт внесен в Единый реестр российского ПО (запись №5312); сертификат ФСТЭК ожидается в 2026 году



Мощный движок, реализующий логику работы продукта, не содержит open source компонентов и **разработан с нуля**



100% скриптов и команд написаны нашими экспертами, не содержат данные из публичных баз



Прямая техподдержка от вендора на русском языке с профильной экспертизой

Результаты применения продукта

Польза от внедрения Кауча в фактах и цифрах

Польза Кауча для службы ИБ

Один инструмент

Можно реализовать всю техническую часть процесса управления настройками **на базе одного продукта**, вне зависимости от размера ИТ-инфраструктуры



Независимость от сканера

В управлении настройками **исчезает роль «оператора сканера уязвимостей»**: не нужно регулярно настраивать отдельный сканер, запускать сканирования, разбирать отчеты



Меньше трудозатрат

Трудозатраты подразделения ИБ на управление всем процессом и администрирование системы **сокращаются до 1-2 часов в день**



Дешевле процесс

Операционные затраты на реализацию процесса управления безопасностью конфигураций **в разы ниже** варианта со сканером уязвимостей



Польза Кауча для службы ИТ

Удобство работы



Единственный продукт, который **заточен под специфику задач ИТ-службы** в процессе управления безопасностью конфигураций

Меньше трудозатрат



Регулярные **трудозатраты ИТ-специалиста** на обработку одного требования безопасности **сокращаются в 3-4 или более раз**

Не только безопасность

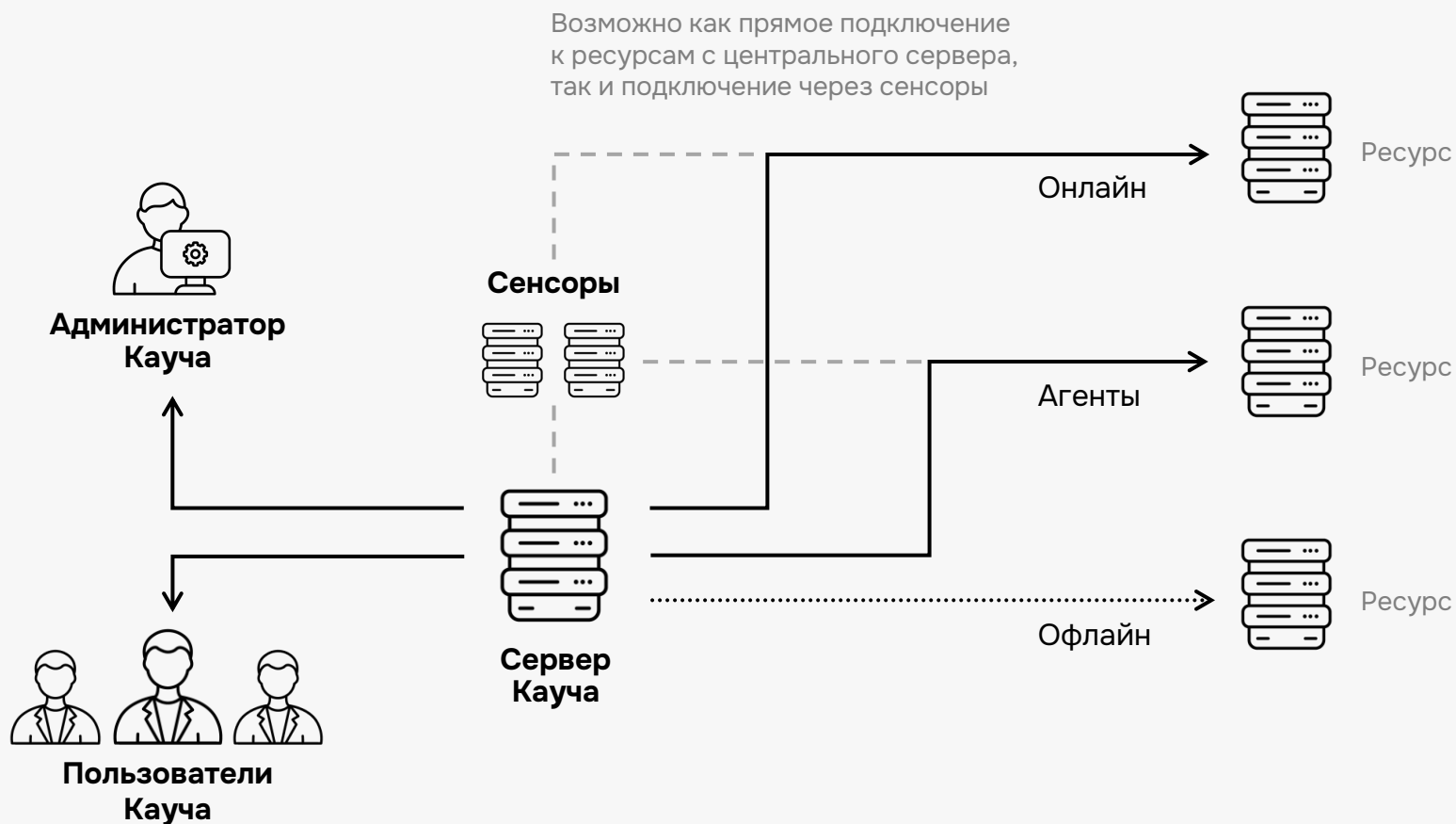


Можно упростить работу не только с требованиями ИБ: **доступна проверка и настройка любых параметров** на всех подключенных ресурсах

Архитектура и системные требования

Как Кауч встраивается в инфраструктуру
и почему вам вряд ли нужен новый сервер

Простая архитектура



Один сервер

Централизованная установка продукта на одном сервере (в минимальной инсталляции)

Интеграции

Доступны интеграции с Active Directory, LDAP; провайдерами аутентификации; SIEM, почтой и другими системами через API

Системные требования

Аппаратные требования



До 1 000 ресурсов

2+ ядра с частотой не менее 2 ГГц
современного серверного CPU x64, 2+ Гб RAM



До 5 000 ресурсов

4+ ядра с частотой не менее 2 ГГц
современного серверного CPU x64, 4+ Гб RAM



От 5 000 ресурсов

8+ ядер с частотой не менее 2 ГГц
современного серверного CPU x64, 8+ Гб RAM

Программные требования



Linux любой версии



Python (от версии 3.7)



БД PostgreSQL

Дополнительная настройка
компонентов не требуется

Поддерживаемые системы

Операционные системы

- AlmaLinux
- ALT Linux
- Apple MacOS
- Astra Linux
- CentOS
- Debian
- FreeBSD
- Gentoo
- IBM AIX
- MS Windows Desktop
- MS Windows Server
- Oracle Linux
- Oracle Solaris
- Red Hat Enterprise Linux
- Rocky Linux
- SberLinux OS
- SelectOS
- SUSE Linux Enterprise Server
- Ubuntu Server
- VMware ESXi
- VMware Photon
- РЕД ОС
- РОСА Хром

Сетевые устройства

- Check Point Firewall
- Cisco ASA
- Cisco Firepower
- Cisco Firewall
- Cisco IOS, IOS XE
- Cisco Nexus
- Cisco WiFi Controller
- Fortinet FortiGate
- Hikvision
- HP Aruba
- HP ProCurve
- Mikrotik
- Radware Alteon
- UserGate NGFW

СУБД

- Apache Cassandra
- IBM DB2
- MariaDB
- MS SQL Server
- MySQL
- Oracle RDBMS
- Pangolin DB
- Postgres Pro
- PostgreSQL

Поддерживаемые системы

Прикладное ПО

- Alteon VA
- Apache ActiveMQ Artemis
- Apache Artemis
- Apache Flink
- Apache Hadoop
- Apache HTTP Server
- Apache Ignite
- Apache Kafka
- Apache Ranger
- Apache Spark
- Apache Tomcat
- Apache Zookeeper
- Arenadata Cluster Manager
- Arenadata Enterprise Tools
- Arenadata QuickMarts
- Basis WorkPlace
- Bind
- Camunda Community Platform
- Ceph
- Confluent Schema Registry
- Consul
- Containerd
- Debezium
- Deckhouse Kubernetes Platform
- Docker
- ETCD
- FreeIPA
- GitLab Runner
- Google Chrome
- Grafana
- GridGain
- HAProxy
- Keycloak
- Kubernetes
- LibercatEE
- Memcached
- Mozilla Firefox
- MS Active Directory
- MS DNS
- MS Edge
- MS Exchange Server
- MS Hyper-V
- MS IIS
- MS Internet Explorer
- MS Office
- MS Sharepoint
- MS Skype
- Nginx
- Node exporter
- Node.js
- OpenSearch
- OpenSSH
- Patroni
- Prometheus
- RabbitMQ
- Red Hat OpenShift
- Redis
- Rsyslog
- Squid
- Springboot
- Syslog-ng
- Tarantool
- Vector
- VMware Photon
- VMware vCenter
- Wildfly

О нас

10 лет

на российском
рынке ИБ

В нашей команде

эксперты с большим опытом
в управленческом консалтинге
и тестах на проникновение

Нам доверяют

крупные компании из финансового
сегмента, промышленности,
ритейла, ИТ

С нами сотрудничают



Наши партнеры

Интеграторы и дистрибьюторы



Технологические партнеры



**Запросите
демо Кауча**

Оставьте заявку на сайте
или свяжитесь с нами
по адресу info@couch.ru



кауч

→ couch.ru

→ +7 495 775-75-74