Кауч

ДиалогНаука

Выводим безопасность конфигураций
на новый уровень с платформой Кауч

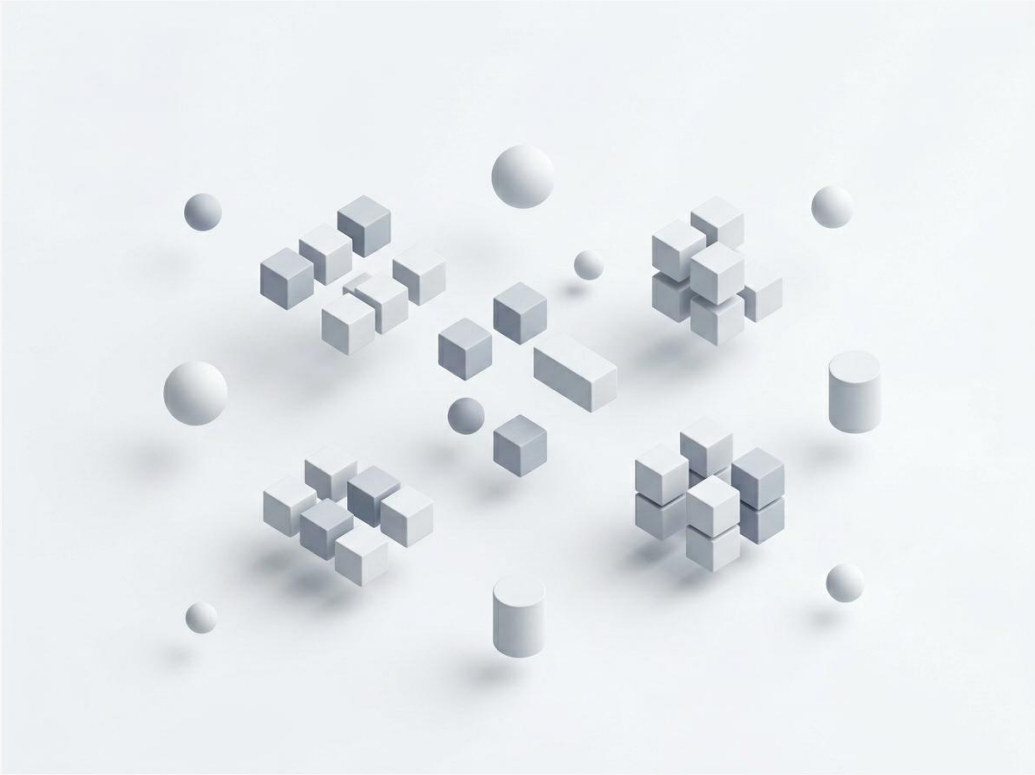
кауч
ДиалОгНаука

Защита сильнее там, где нет пробелов

Усложнение инфраструктуры:
ИТ растет быстрее, чем защита успевает адаптироваться

Фрагментарность: множество СЗИ работают сами по себе, создавая «слепые зоны» на стыках

Смена парадигмы: хакерам не нужен сложный взлом – они ищут одну забытую настройку



Аудит: находим, где «тонко»

Состав средств защиты:
инвентаризация того, что уже работает

Архитектура решений: проверка связности и «стыков» между системами

Настройки и охват: оценка корректности настроек и полноты контроля каналов

Рекомендации: план по заполнению выявленных пробелов

От случайных настроек — к эталону

Разработка Hardening-стандартов: на базе CIS, ISO 27001, NIST, ФЗ-152 и требований ЦБ/PCI DSS

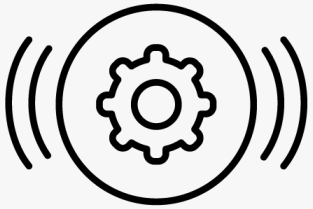
Единый профиль: создание шаблонов конфигураций для всех компонентов ИТ и ИБ

Непрерывный контроль: переход от разовой проверки к регулярному мониторингу соответствия

Уязвимости конфигураций

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

Уязвимости конфигураций



Ошибки в настройках штатных механизмов защиты ИТ-систем

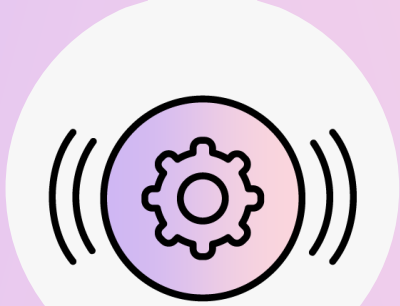
- Дефолтные или слабые пароли
- Дефолтные настройки систем
- Расширенные права доступа у обычных пользователей
- Отсутствие шифрования или слабое шифрование
- Доступность необязательных функций систем

кауч
ДиалОгНаука

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

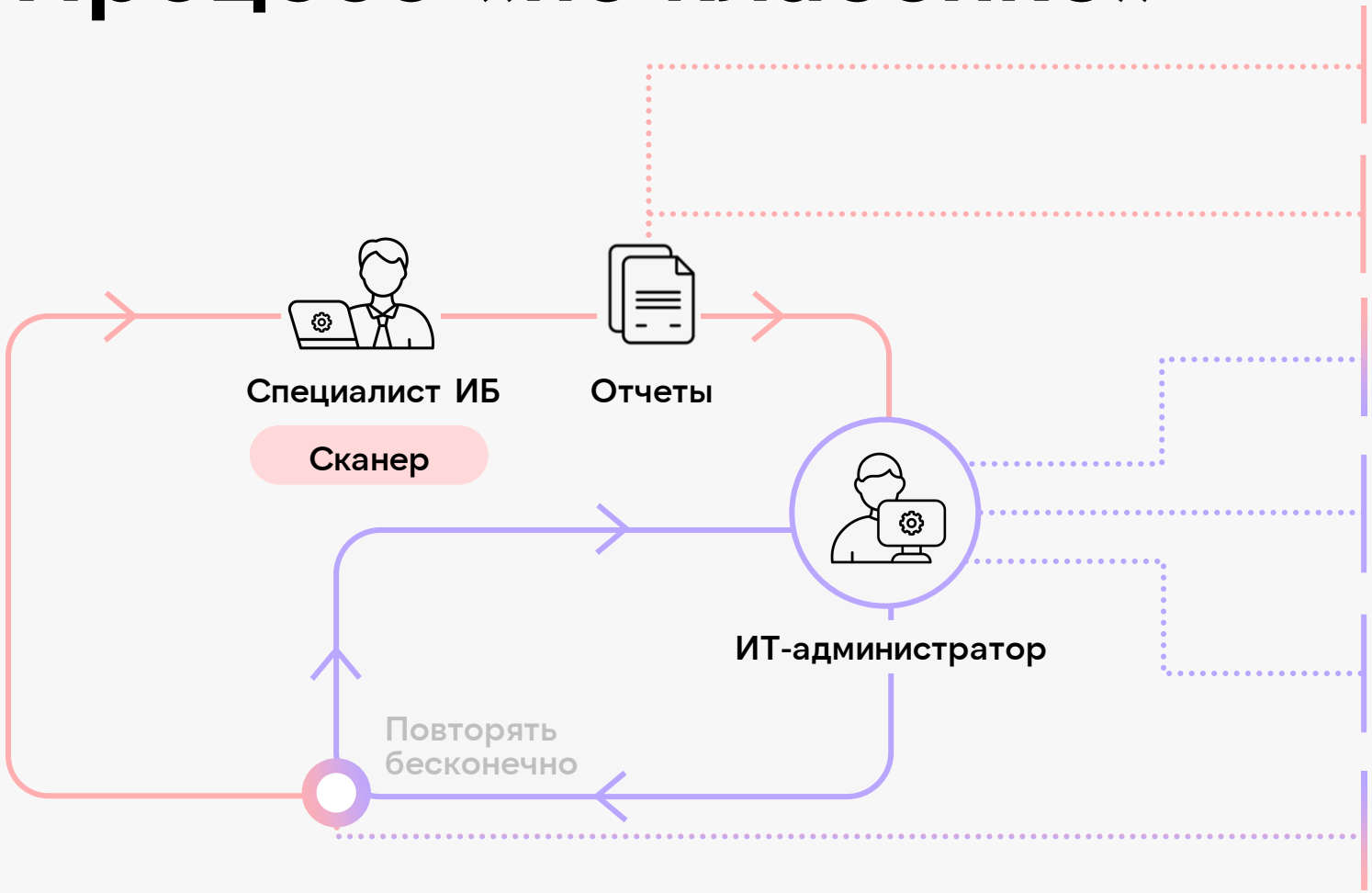
В зависимости от отрасли, **компания должна выполнять требования регуляторов** (например, ГОСТ 57580.1, Указ Президента РФ №250, требования приказа ФСТЭК №117, PCI DSS, SWIFT, ISO 27001 и др.) или каких-либо внутренних политик безопасности

кауч
ДиалОгНаука

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»



Сотни страниц для каждого хоста (слои ОС, СУБД, ПО)

Проанализировать и приоритизировать все недостатки, создать тикеты

Выяснить суть требований, источник, сроки и необходимость исправления недостатков

Проанализировать требования, изучить мануалы вендора, составить команды настройки, провести тесты

Выделить и согласовать время, подключиться к каждой системе, провести настройку

Повторное сканирование для проверки устранения уязвимостей; если недостатки остались, повторить настройку

Результат, а не процесс ради процесса

Как Кауч помогает подружить ИБ и ИТ

кауч
ДиалогНаука

Кауч

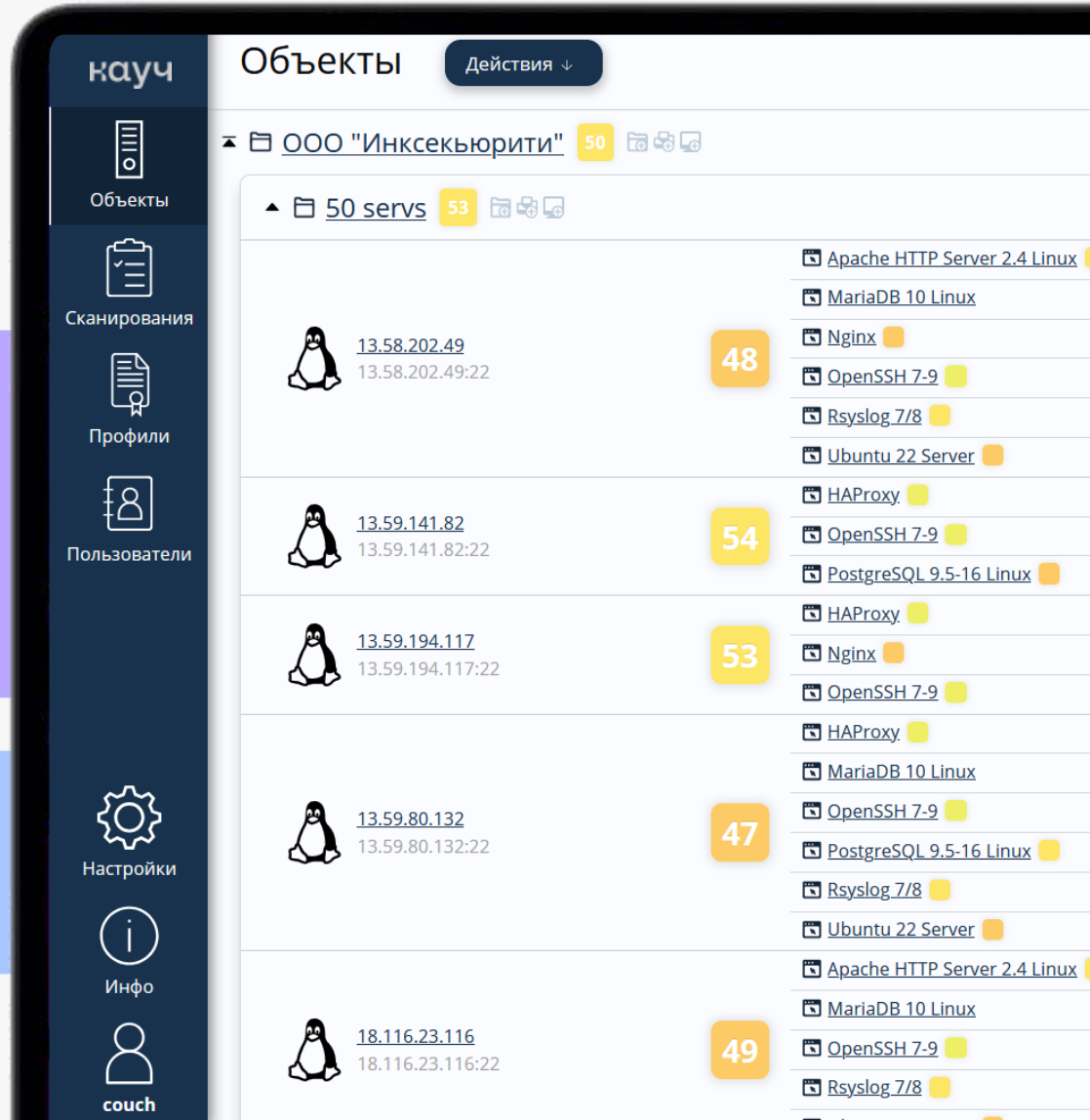
All-in-one платформа для управления безопасностью конфигураций ↗

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



кауч
ДиалОгНаука

Подход Кауча: совместная работа

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

кауч
ДиалОгНаука

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

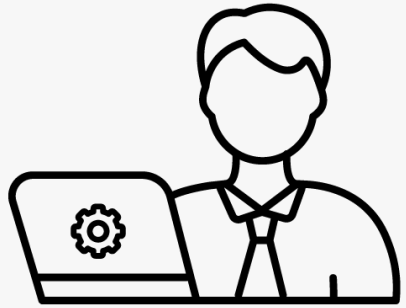
Создать необходимые политики с помощью готовых шаблонов или инструментов для создания собственных требований

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

кауч
ДиалОгНаука

Подход Кауча: единый процесс

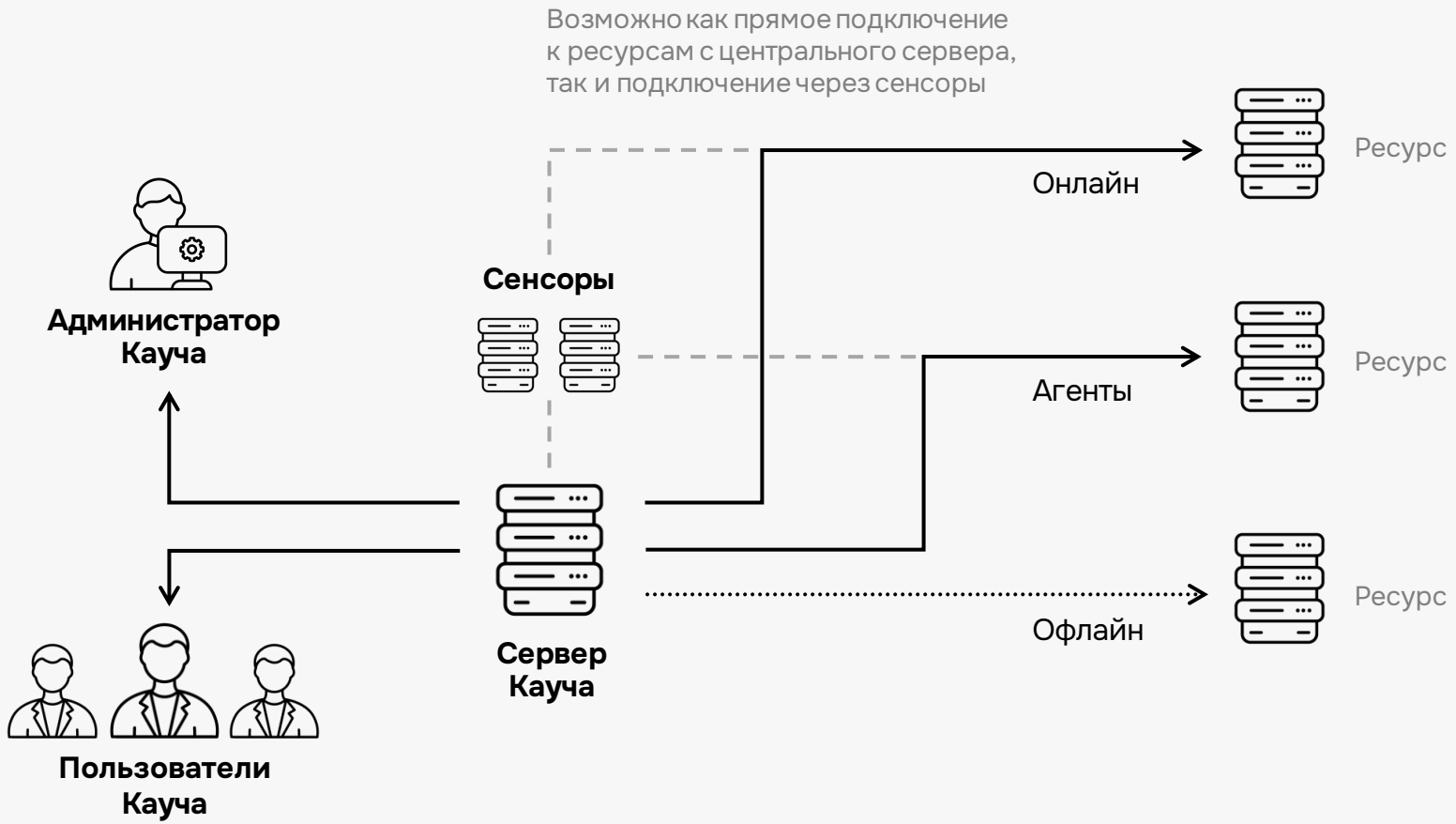
Управление безопасностью конфигураций включено в общий процесс мониторинга и реагирования на инциденты

Архитектура и системные требования

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

кауч
ДиалОгНаука

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

Список поддерживаемых систем постоянно пополняется.

kauч
ДиалОгНаука

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

Список поддерживаемых систем постоянно пополняется.

кауч

О компании Кауч

10 лет
на российском рынке ИБ

В команде Кауча
эксперты с большим опытом в управленческом консалтинге и тестах на проникновение

Среди клиентов
крупные компании из финансового сегмента, промышленности, ритейла, ИТ

Уже используют Кауч

Райффайзен Банк
ПСБ
БСПБ
МОСОБЛБАНК
МЕТКОМБАНК
axenix
АТБ Азиатско-Тихоокеанский Банк
СБЕР НПФ
СБЕР РЕШЕНИЯ
ERG
MR GROUP
столото