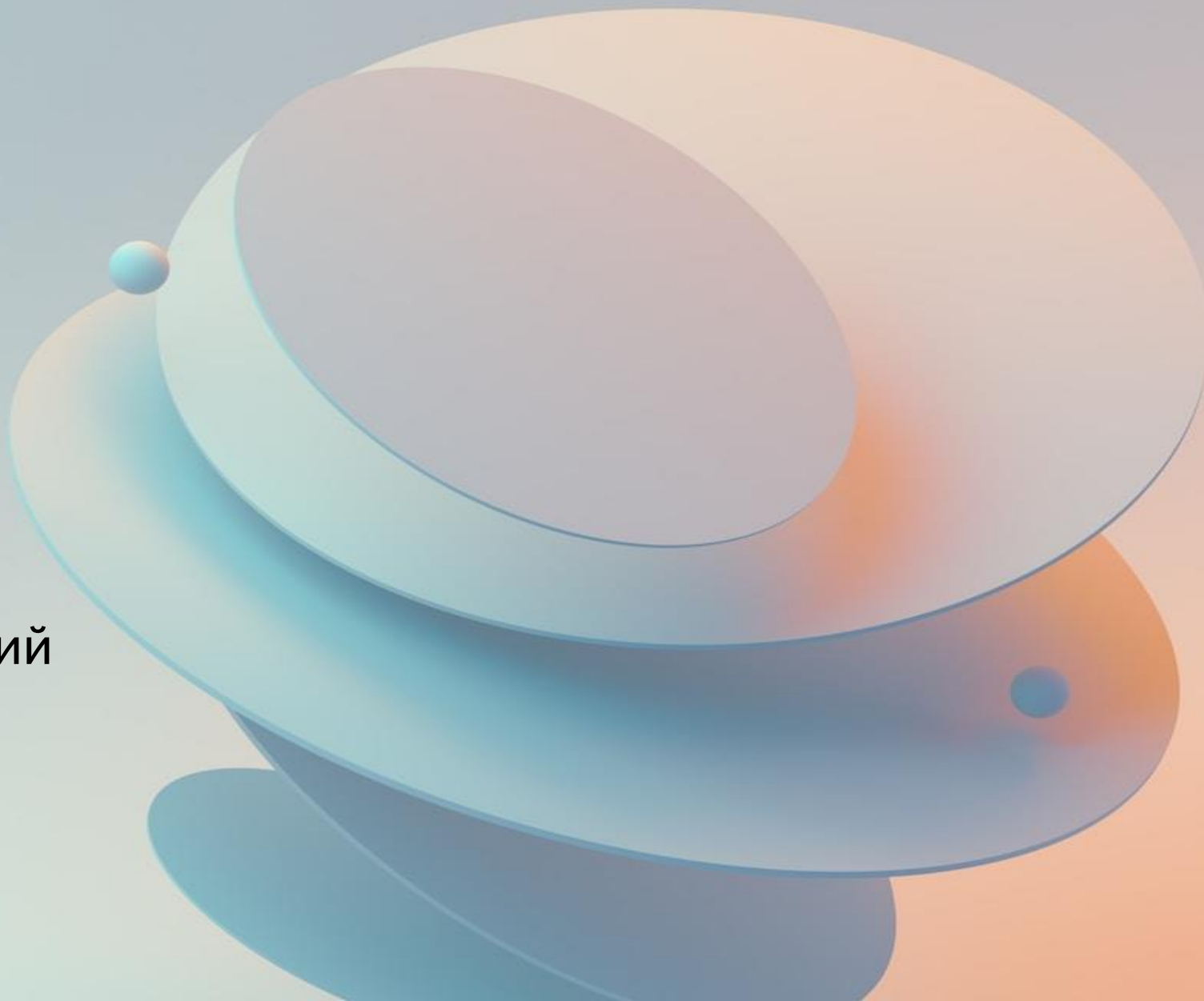


Couch

Комфортное управление
безопасностью конфигураций



О нас

Почему мы знаем, что делаем,
и какие компании нам доверяют



Команда Couch



8 лет

на российском рынке



В нашей команде

эксперты с опытом
в управленческом консалтинге
и тестах на проникновение



Нам доверяют

крупные компании
из банковского сегмента,
промышленности, ритейла, ИТ

С нами сотрудничают



Уязвимости конфигураций

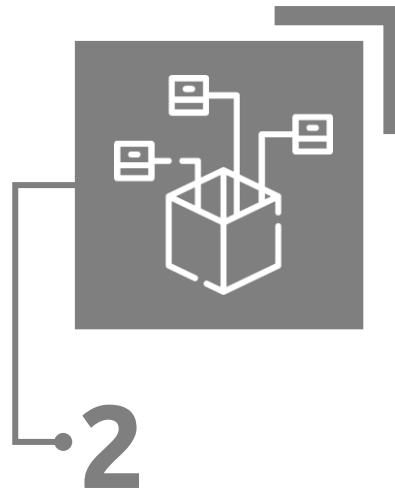
Почему управление безопасностью
конфигураций важно не только
для комплаенса

Уязвимости инфраструктуры



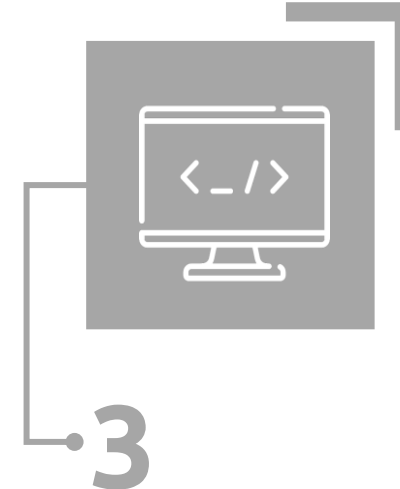
Уязвимости конфигураций

Ошибки в настройках штатных механизмов защиты любых систем



Уязвимости сторонних систем

Ошибки в коде «коробочных» систем стороннего вендора



Уязвимости собственных систем

Ошибки в коде систем, создаваемых внутри компании или на заказ

Уязвимости конфигураций



Необходимо соответствовать требованиям

В зависимости от отрасли, компания должна соответствовать стандартам (таким как PCI DSS, SWIFT, ISO 27*, ГОСТ Р 57580 и др.) или каким-либо внутренним политикам безопасности

Необходимо защищаться от кибератак

Компании нужно оперативно обнаруживать и устранять уязвимости конфигураций, чтобы закрыть для злоумышленников возможность легкого доступа в инфраструктуру

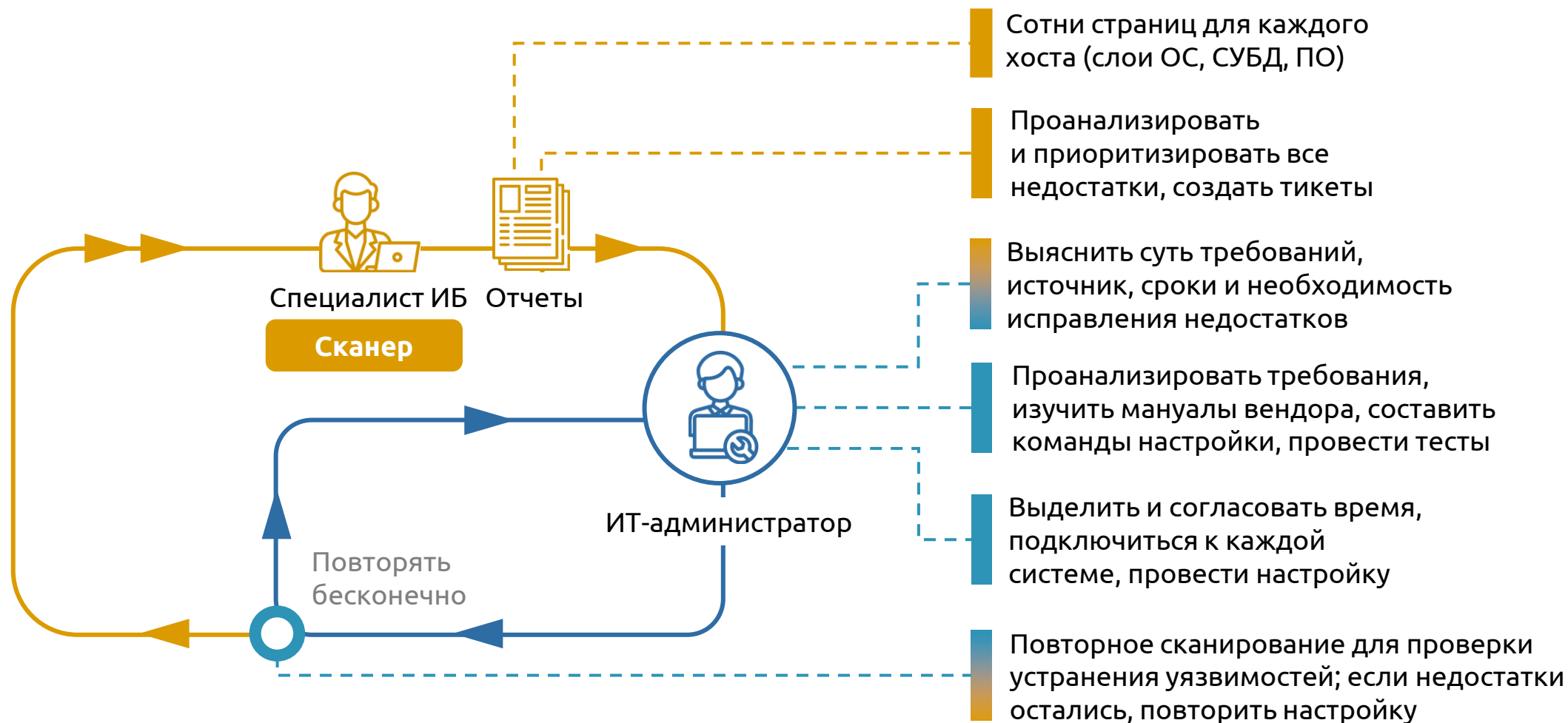
>50%
от общего
числа уязвимостей

Нет баз,
метрик, новостей

Нет универсальных
средств устранения

Проблемы на аудитах

Процесс «по классике»

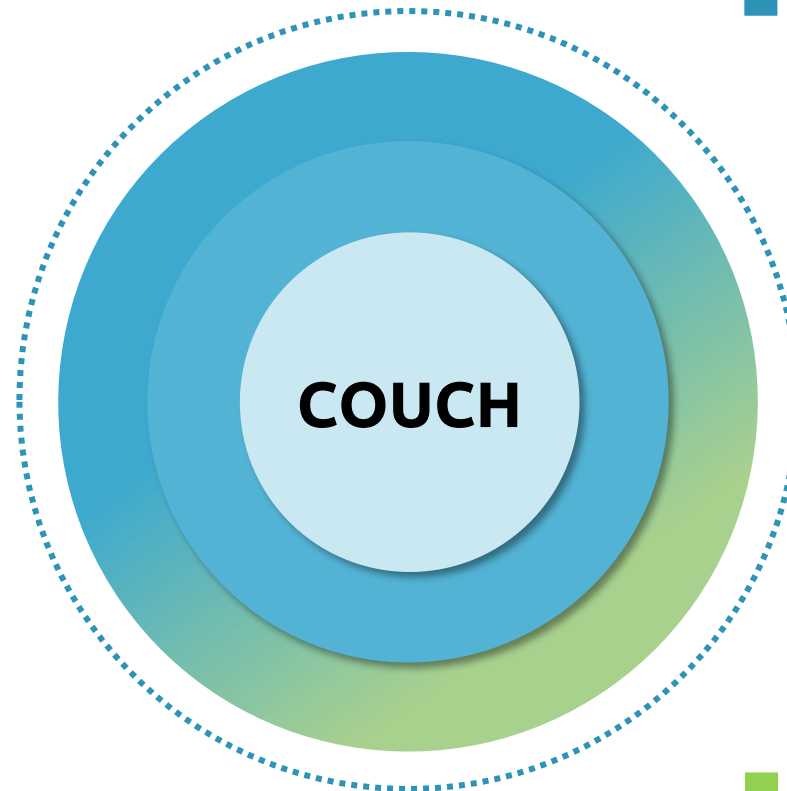


Couch. Больше никаких отчетов

Результат, а не процесс ради процесса –
как Couch помогает подружить ИБ и ИТ

Couch

**All-in-one
платформа
для управления
безопасностью
конфигураций**



Сканирование
на соответствие лучшим
мировым практикам

Совместная работа
и разделение задач

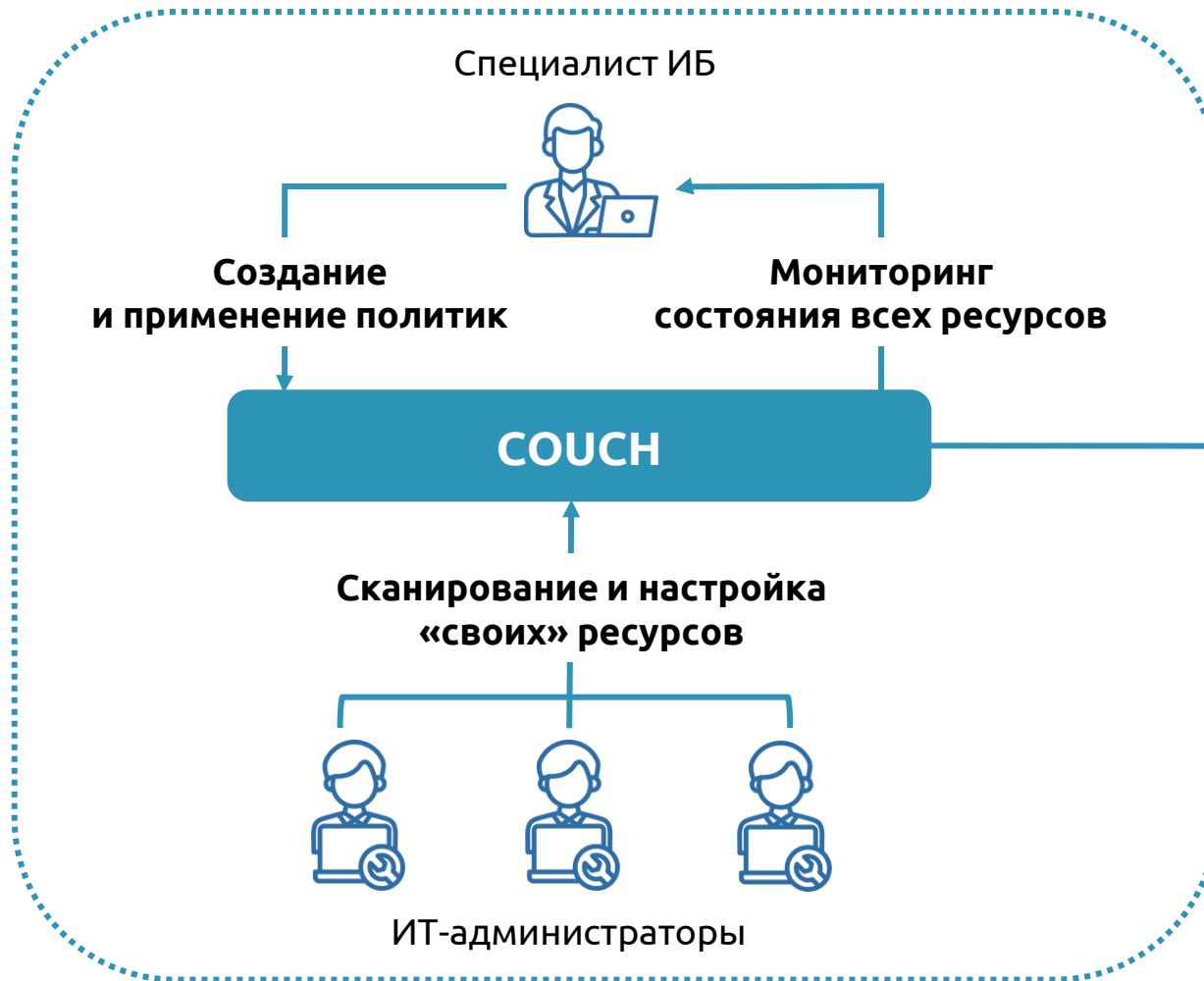
Настройка ресурсов
инструментарием
«из коробки»

Создание политик
любой сложности

Мониторинг
изменений

Подход Couch: совместная работа

Управление безопасностью конфигураций



Одна среда для служб ИБ и ИТ и всех операций: сканирования, настройки и мониторинга.
Нет необходимости в отчетах

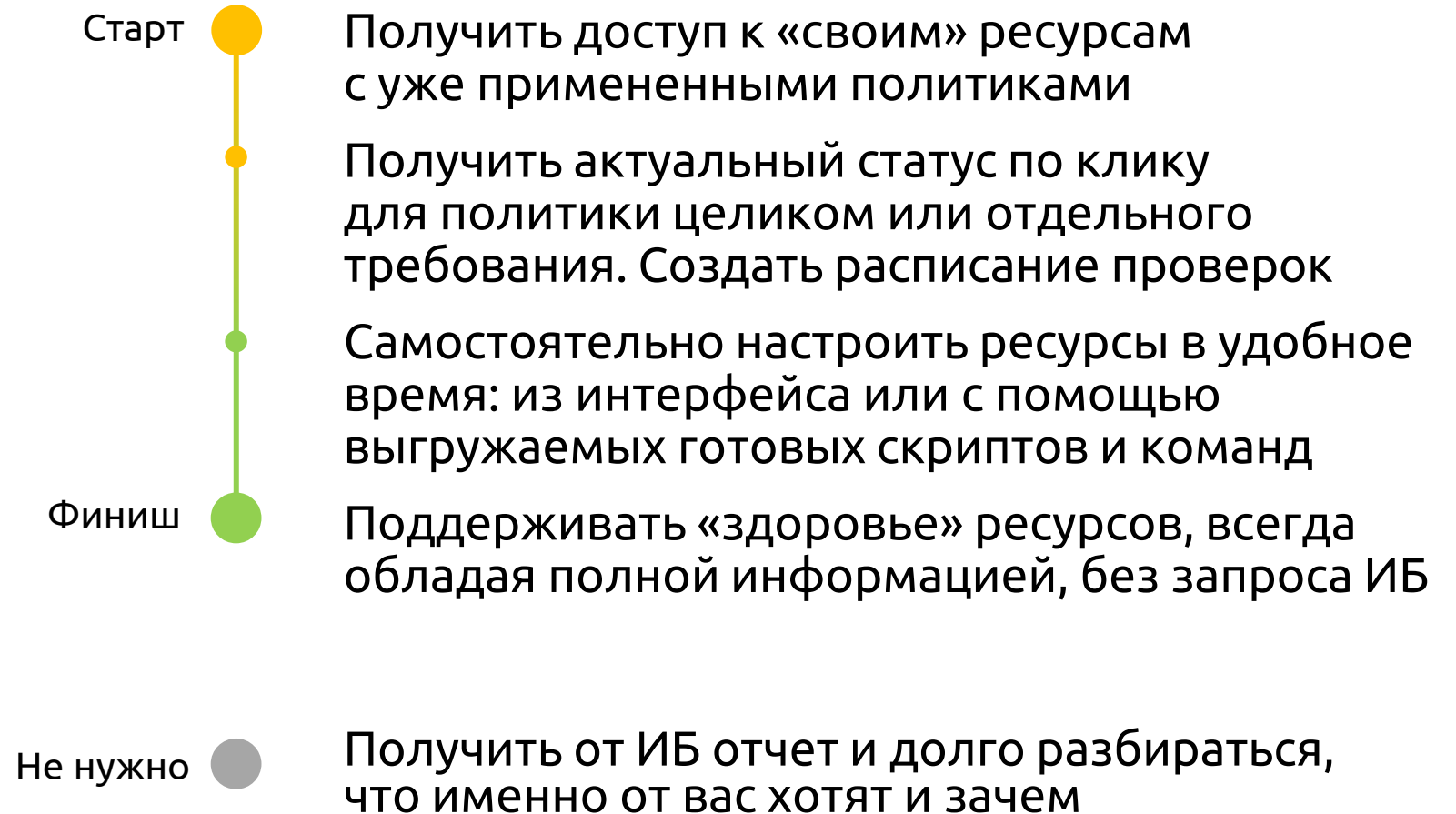
CISO, CIO

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



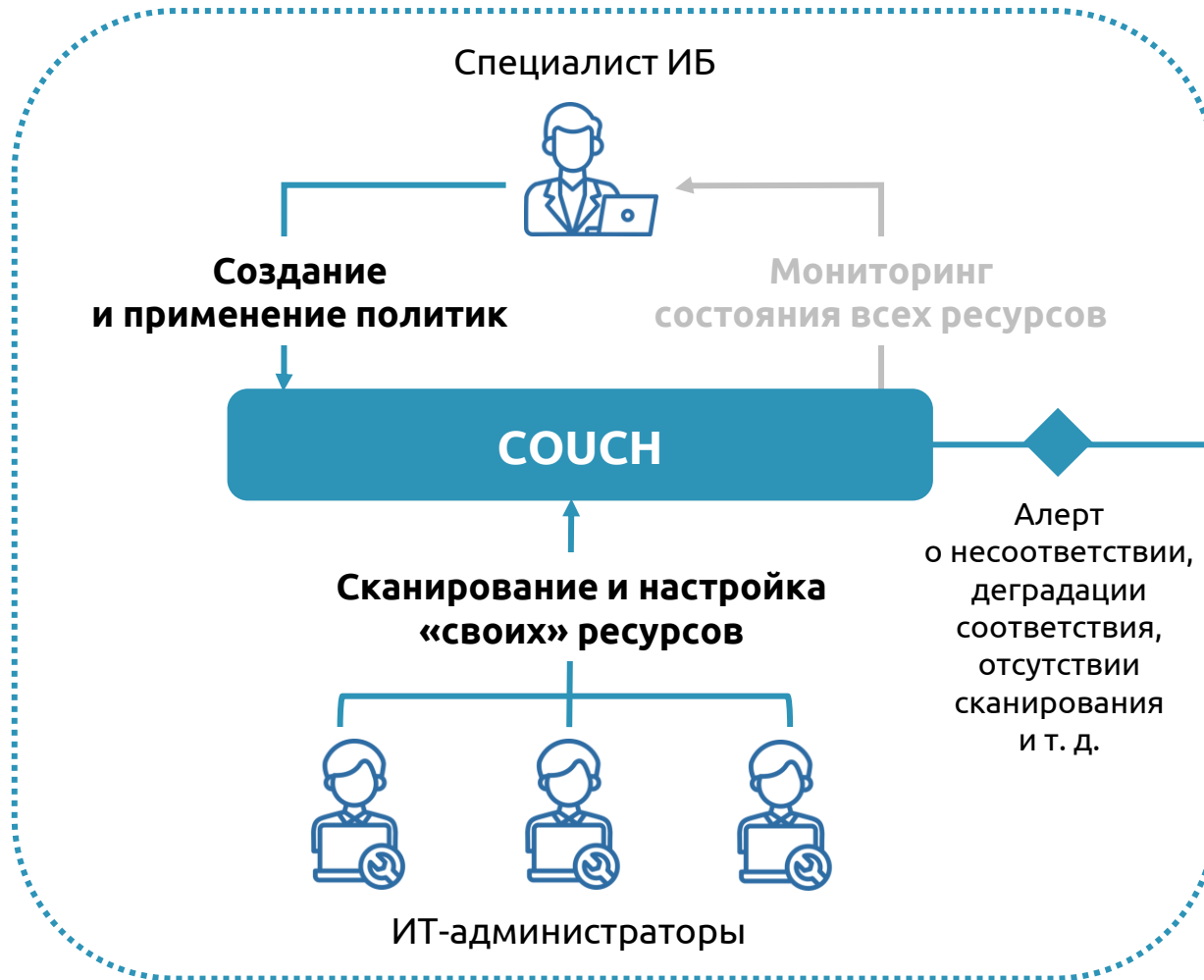
Воркфлоу специалиста ИБ



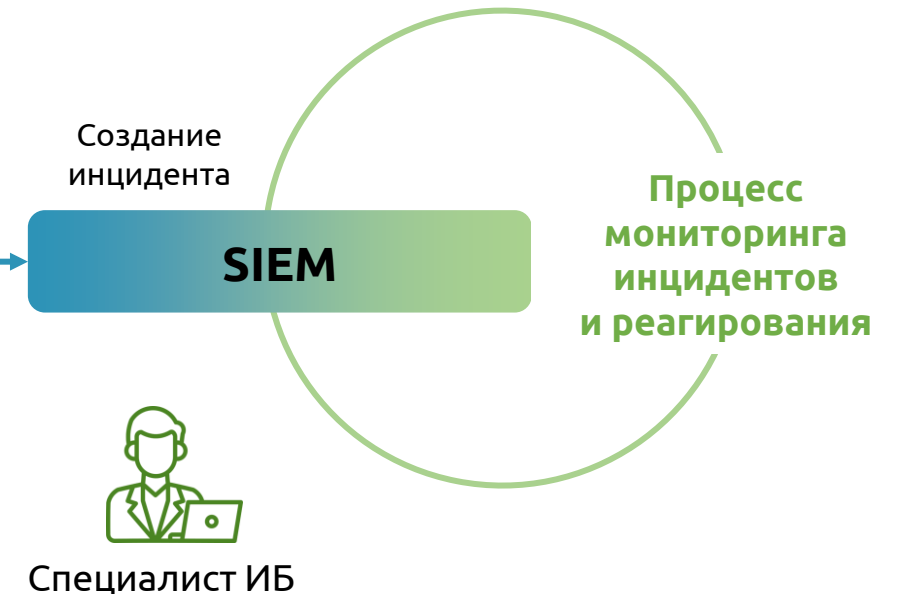
Редко		Создать необходимые политики с помощью готовых шаблонов или инструментов для создания собственных требований
		Применить политики к ресурсам
		Внести новые ресурсы, создать новые учетные записи, распределить права
Регулярно		Проводить мониторинг устранения уязвимостей: с помощью сводных данных по всем системам или отдельным ресурсам
Не нужно		Сканировать всю инфраструктуру для выявления уязвимостей конфигураций

Подход Couch: единый процесс

Управление безопасностью конфигураций



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



Ключевые преимущества



СКАНИРОВАНИЕ И НАСТРОЙКА ПО КЛИКУ

Сканирование по клику, настройка в два действия в интерфейсе, доступные для выгрузки скрипты и команды, механизмы мгновенной перепроверки устранения уязвимости



РАБОТА С СИСТЕМАМИ ОФЛАЙН

Механизмы для удобной работы с системами без сетевого доступа или критически важными системами с запретом на подключение извне



ГИБКОЕ УПРАВЛЕНИЕ ПОЛИТИКАМИ

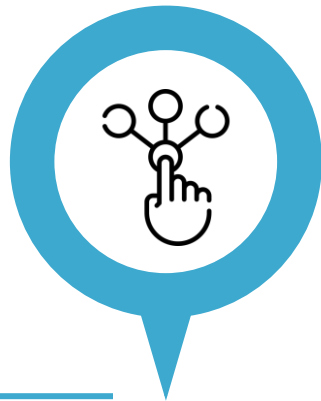
Шаблоны с лучшими мировыми практиками «из коробки», удобное и быстрое создание политик не только на основе регулярных выражений, создание собственных требований



ВЫСОКАЯ СКОРОСТЬ РАБОТЫ

Быстрое сканирование всей инфраструктуры: полная проверка 1000 средненагруженных хостов занимает не более 10 минут

Удобное сканирование



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



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



Пере проверка отдельного требования для получения статуса ресурса занимает секунды и не требует полного повторного сканирования

Быстрая настройка ресурсов

**Готовый
инструментарий
для работы**



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

**Несколько
доступных опций
настройки**



Настройка ресурсов может производиться онлайн **одним кликом** в интерфейсе продукта или в режиме офлайн

**Полностью
прозрачная работа
с настройками**



Все команды и скрипты можно мгновенно выгрузить; содержимое команд и скриптов доступно в открытом виде, его можно изучить

Работа с системами офлайн

Без ограничений

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

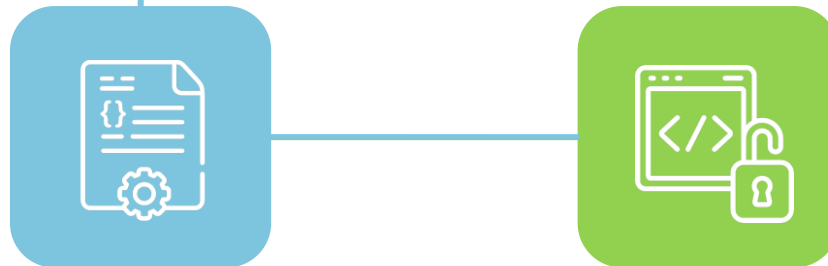


Проверка офлайн

Couch позволяет в одно действие выгрузить скрипты для офлайн-сбора данных о таких системах. 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 в режиме 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
в три строки скрипта



Гибкое управление политиками

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

1

**Быстрое
создание**

**Тестирование
«на лету»**

2

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

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

3

**Настройка
параметров**

Отечественная разработка

1.

Продукт внесен
в Единый реестр
российского
программного
обеспечения

2.

Движок,
реализующий логику
работы продукта,
не содержит open
source компонентов
и разработан с нуля

3.

100% скриптов
и команд написаны
нашими экспертами
и не содержат данные
из публичных баз
(XCCDF, OpenSCAP)

4.

Прямая вендорская
поддержка
на русском языке
с профильной
экспертизой

Результаты применения Couch

Польза от внедрения продукта
в фактах и цифрах

Польза Couch для службы ИБ

Один инструмент

Можно реализовать техническую часть процесса на базе одного продукта (вне зависимости от размера инфраструктуры)

Сканер не нужен

Исчезает роль «оператора сканера»: не нужно работать со сканером уязвимостей (настраивать, 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 Couch для службы ИТ

Удобство работы

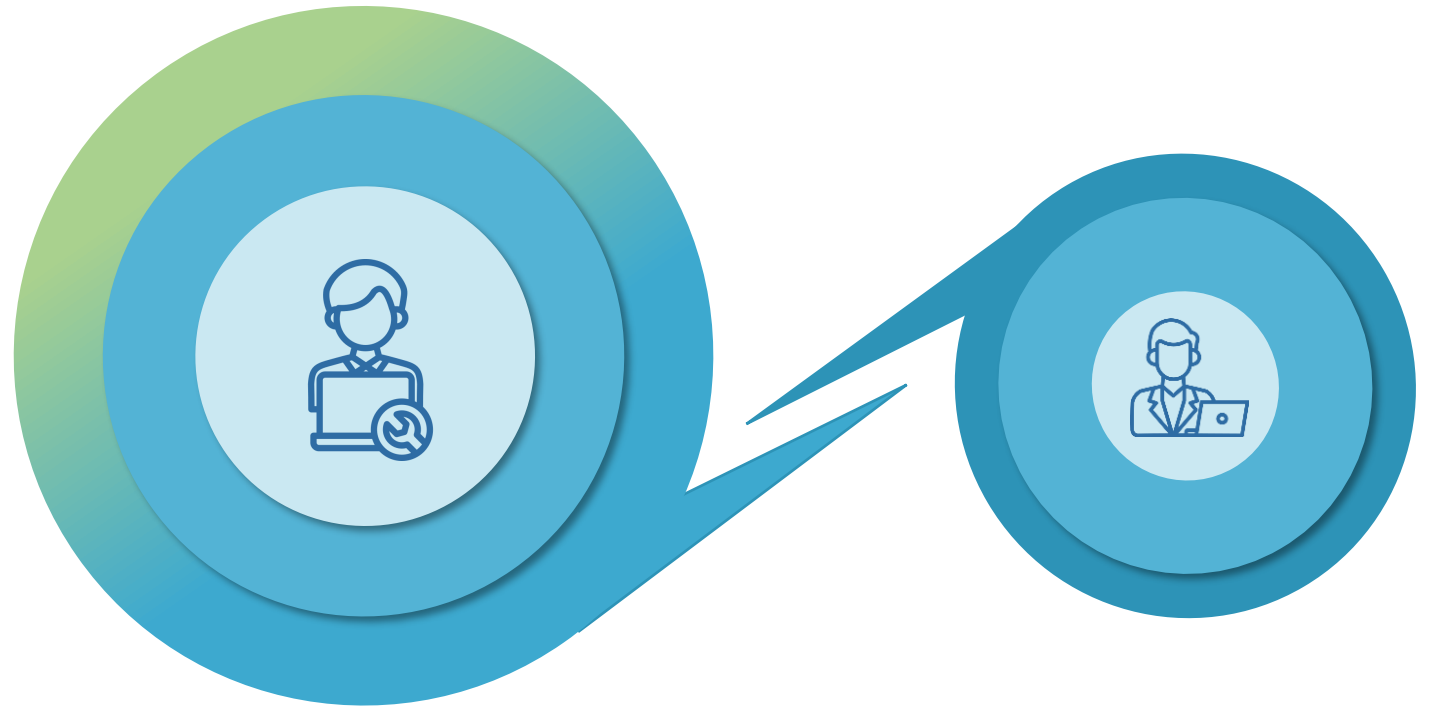
Единственный продукт, который заточен под специфику задач ИТ-службы в процессе управления безопасностью конфигурациями

Меньше трудозатрат

Регулярные трудозатраты ИТ-специалиста на обработку одного требования безопасности сокращаются в 3 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 Couch встраивается в инфраструктуру
и почему вам вряд ли нужен новый сервер

Простая архитектура



Один сервер

Централизованная установка на одном сервере, возможна установка без коллекторов

Три компонента

Нужны только ОС, база данных и дистрибутив Couch. Другие компоненты для установки и клиенты для доступа не потребуются

Системные требования

Аппаратные требования

До 1000 ресурсов

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

До 5000 ресурсов

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

От 5000 ресурсов

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

Программные требования

- Linux любой версии
- Python любой версии
- БД PostgreSQL

Дополнительная настройка
компонентов не требуется.

Лицензирование

Отличия лицензий Standard и Enterprise

Отличия лицензий

STANDARD

- Основная функциональность продукта без ограничений.

ENTERPRISE

- API для автоматизации получения данных об объектах, проверок и получения результатов.
- Сканирующие прокси (сенсоры), которые можно разместить в удаленных или изолированных сегментах сети для проверки и настройки локальных ресурсов.
- Гибкая настройка регистрируемых и отправляемых событий (для интеграции с SIEM); поддержка алертов на «логические» события (появление или деградация несоответствий, необоснованно длительное отсутствие проверок, изменения в политиках и требованиях).
- Режим Free scan: проверка произвольно задаваемых адресов в режиме «сканера» без необходимости предварительного добавления ресурсов в базу объектов, возможность импорта обнаруженных хостов.

Техподдержка

Программы стандартной и расширенной
технической поддержки

Стандартная техподдержка

1

ДОСТУП К ПОРТАЛУ ТЕХПОДДЕРЖКИ И ВСЕМ ОБНОВЛЕНИЯМ

- Доступ к онлайн-порталу техподдержки и тикет-системе
- Обновления поддерживаемых систем (новые версии компонентов, новые типы компонентов)
- Обновления шаблонов с лучшими практиками безопасных настроек

2

ДОБАВЛЕНИЕ ПОДДЕРЖКИ НОВЫХ КОМПОНЕНТОВ

- Добавление в продукт поддержки компонентов, входящих в технологический стек лицензиата, предоставляется по запросу
- В стоимость базовой лицензии входит реализация поддержки 1 компонента на каждые 500 лицензируемых ресурсов

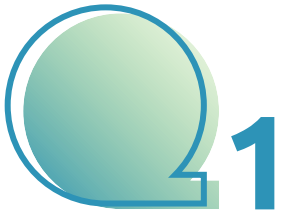
Расширенная техподдержка



Развитие продукта

Наши планы на ближайшие релизы

I квартал 2024 года



Своя база политик

- Создание собственной базы шаблонов и требований со связями и ссылками на стандарты и лучшие практики
- Доступ к аналитике о выполнении одинаковых требований в политиках и компонентах разного типа
- Готовые политики для выполнения требований регуляторов, не требующие кастомизации или с их минимальной необходимостью



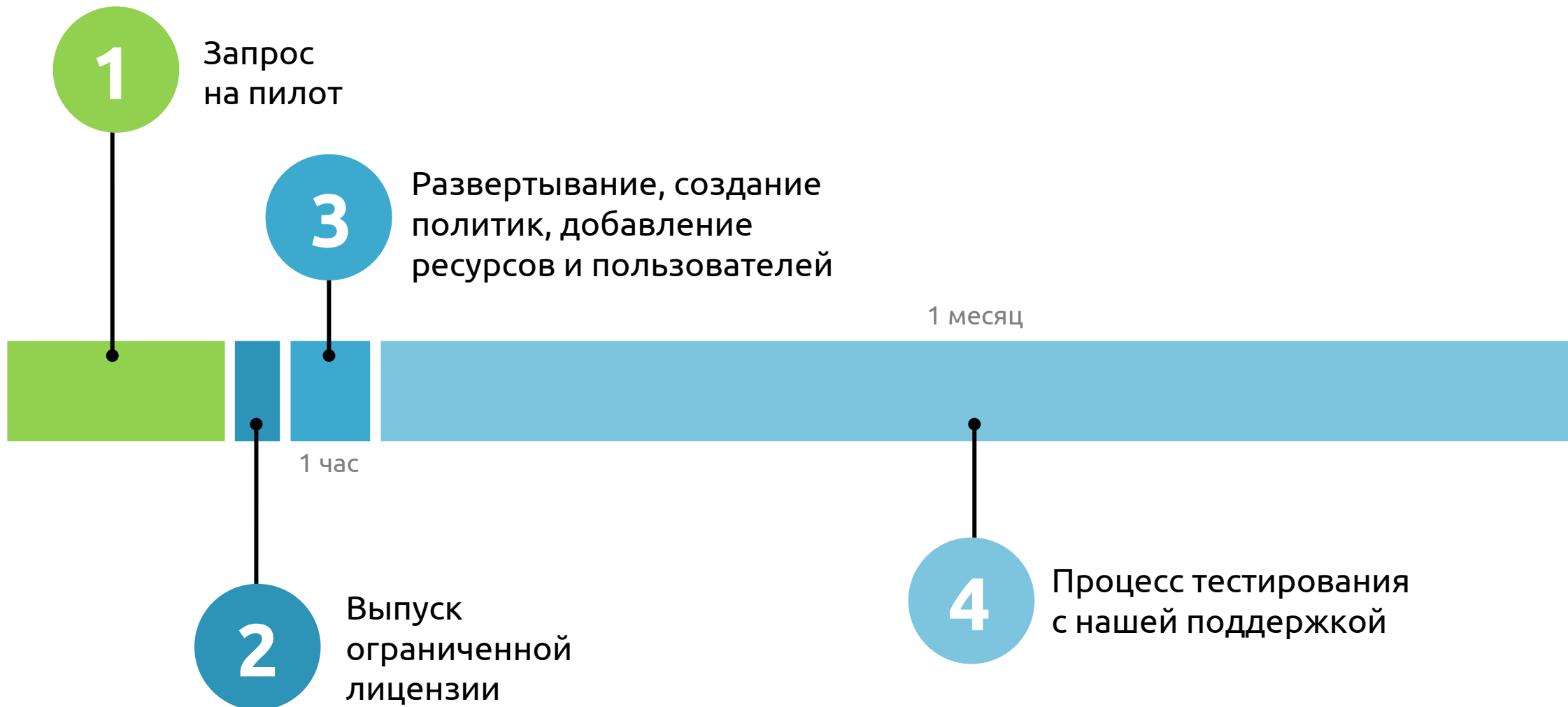
Интерфейс и язык

- Современный интерфейс для удобной работы на очень крупных и сложных распределенных инфраструктурах
- Русификация всего приложения, включая шаблоны политик

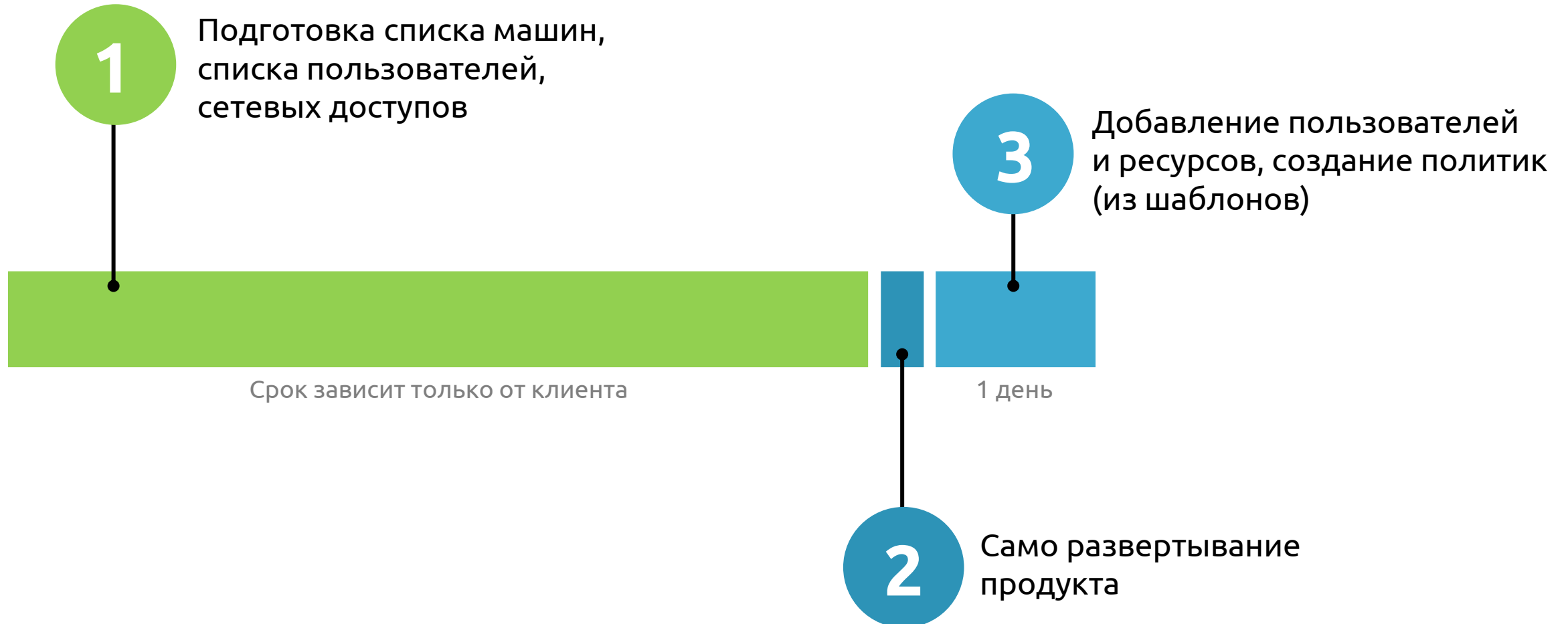
Как протестировать и внедрить

Что вас ждет на пилотном проекте
и на внедрении: процесс и сроки

Как проходит пилотный проект



Как проходит внедрение



Интерфейс продукта



























Основной экран

Couch Objects Multiscan Filters Search for... Search



















demo.incsecurity.ru 65

_Real Systems 53

Information System 1 58 policy1







 Centos 7 82.202.204.150:22	58	 CentOS 7	CentOS 7	 CentOS 7
		 MySQL Linux	MySQL 4/5/8	 MySQL Linux
		 Nginx	Nginx *	 Nginx
		 OpenSSH	OpenSSH 7-9	 OpenSSH 7/8
		 Red Hat Enterprise Linux 7	RHEL 7	 RHEL 7 - Password Policy v2
		 Rsyslog	Rsyslog 7/8	 Rsyslog
 DB 82.202.204.150:22	58	 CentOS 7	CentOS 7	 CentOS 7
		 MySQL 5.7	MySQL 4/5/8	 MySQL Linux
		 Nginx	Nginx *	 Nginx
		 OpenSSH 7/8	OpenSSH 7-9	 OpenSSH 7/8
		 Rsyslog	Rsyslog 7/8	 Rsyslog

Information System 2 48



 Compliance Server 127.0.0.1:2233	50	 OpenSSH 7/8	OpenSSH 7-9	 OpenSSH 7/8
		 OS	Ubuntu 18	 Ubuntu 18
		 PostgreSQL 9.5/9.6/10/11 Linux	PostgreSQL 9.5/9.6/10/11/12	 PostgreSQL 9.5
		 Rsyslog	Rsyslog 7/8	 Rsyslog
 Front Server 80.249.149.210:2233	46	 OpenSSH 7/8	OpenSSH 7-9	 OpenSSH 7/8
		 PostgreSQL 9.5-14 Linux	PostgreSQL 9.5/9.6/10/11/12	 PostgreSQL 9.5-14 Linux
		 Rsyslog 7/8	Rsyslog 7/8	 Rsyslog 7/8
		 Ubuntu 20 Server	Ubuntu 20	 Ubuntu 20 Server

Remote Cloud 61

ATM Controller 75

 ATM Host 10.0.31.16	94	 ATM.Connector	Server 2003 Non-domain	 MS Windows Server 2003 Non-domain
 ATM Host 2 1.1.1.1	56	 ATM.Translator	Server 2003 Domain Member	 Windows Server 2003 Domain Member

Web Site 52

		 Apache 2.2 on Linux	Apache 2.2	 Apache2.2Linux new test
--	--	---	------------	---

Service Info Couch

Данные о ресурсах

Couch

- Objects
- Scans
- Profiles
- Users
- Service
- Info
- couch

Resource

Objects / demo.incsecurity.ru / Real Systems / Information System 1 / DB

DB
Comment: —
Policy: policy1
Address: 82.202.204.150:22

[Scan](#) [Schedule](#) [Edit](#) [Detect components](#)

58

Risks

High	61
Medium	41
Low	20

Compliance

Failed: 122, Passed: 216

[Events](#) [PDE, XLSX, HTML](#)

Components

Component	Version	Package	High	Medium	Low	Passed	Failed
CentOS 7	CentOS 7	CentOS 7	44	20	16	132	0
MySQL 5.7	MySQL 4/5/8 Linux	MySQL Linux	5	5	0	30	12
Nginx	Nginx	Nginx	7	14	3	24	5
OpenSSH 7/8	OpenSSH 7-9	OpenSSH 7/8	1	1	0	19	2
Rsyslog	Rsyslog 7/8	Rsyslog	4	2	0	11	2

[Add component](#)

Users

Name (Login)	Position	Access
Жан-Клод Ван Дам (login10)	Системный Администратор	Global Administrator
Марк Дакакас (login9)	Начальник управления	Global Administrator
Анна Тихая (login16)	Ведущий специалист	Admin ✕
Виктор Тихонов (login1)	Директор дирекции	Admin ✕
Антон Рабитов (login6)	Старший специалист	Read ✕
Гассан Абдуррахман ибн Хоттаб (hottabych)	Генеральный директор	Read ✕
Елена Сазонова (login18)	Специалист	Read ✕

[Add user](#)

Данные о компонентах

Couch

Component [Objects](#) / [demo.incsecurity.ru](#) / [Real Systems](#) / [Information System 1](#) / [Centos 7](#) / CentOS 7

Events? [PDE, XLSX, HTML](#)

CentOS 7

Comment: —

Policy: [policy1](#)

Component type: CentOS 7

Default profile: [CentOS 7 \(ver. 22\)](#)

Online configuration is disabled.

Scan
Schedule
Upload
Edit

Risks

60

Risk Level	Count
High	43
Medium	18
Low	16

Compliance

Status	Count
Passed	135
Failed	77

Dynamics

Scans

[Recent](#) / [Upcoming](#) / [Compare](#)

Time	Task	Profile	Status
#1044 at 01.03.2023 13:07:47 UTC+03	Centos 7 — 1.03.2023 13:07	CentOS 7	43 High, 18 Medium, 16 Low, 135 Passed
#1029 at 29.11.2022 11:35:18 UTC+03	29.11.2022 11:35	CentOS 7	42 High, 18 Medium, 16 Low, 136 Passed
#1017 at 27.10.2022 16:49:54 UTC+03	27.10.2022 16:49	CentOS 7	44 High, 19 Medium, 16 Low, 133 Passed
#1007 at 18.10.2022 11:06:29 UTC+03	Centos 7 — 18.10.2022 11:06	CentOS 7	46 High, 20 Medium, 16 Low, 130 Passed
#1006 at 17.10.2022 12:44:10 UTC+03	CentOS 7 — 17.10.2022 12:44	CentOS 7	46 High, 20 Medium, 16 Low, 130 Passed
#1005 at 12.10.2022 00:16:31 UTC+03	12.10.2022 00:16	CentOS 7	46 High, 21 Medium, 16 Low, 129 Passed
#1000 at 12.10.2022 00:14:49 UTC+03	Centos 7 — 12.10.2022 00:14	CentOS 7	46 High, 24 Medium, 16 Low, 126 Passed
#997 at 28.09.2022 18:20:08 UTC+03	CentOS 7 — 28.09.2022 18:20	CentOS 7	47 High, 24 Medium, 16 Low, 125 Passed

Objects

Scans

Profiles

Users

Service

Info

couch

Данные о сканировании

Couch

- Objects
- Scans
- Profiles
- Users
- Service
- Info
- couch

Scan

Scans / OpenSSH 7/8 — 18.10.2022 13:04 / #1012

#1012 at 18.10.2022 13:04:28 UTC+03

Profile: OpenSSH 7/8 (ver. 4)

Resource: Ubuntu Component: OpenSSH 7/8

Address: 178.154.240.211:22

Online configuration is disabled for this component.

[Run again](#) [Configuration script](#) [Delete](#)

Risks

High	5
Medium	3
Low	3

Compliance

Passed	11
Failed	11

# Title	Description	Remediation	Risk	Score	Value
1.1. Keep the Version Updated	As new security vulnerabilities are discovered, the corresponding fixes are implemented by software package provider. Installing the latest software version ensures these fixes are available on your system.	Upgrade the OpenSSH service to a version that has no security bugs and apply any patches recommended by the vendor.	High	✓	[Status Compliant was set by couch on 13.03.2023 14:36:13] Package: openssh-server Status: install ok installed Priority: optional Section: net
1.2. Enable authentication based on public / private keys	PubkeyAuthentication - Specifies whether to try public key authentication.	Use authentication based on public / private keys	Medium	✓	pubkeyauthentication yes authorizedkeysfile .ssh/authorized_keys .ssh/authorized_keys2
1.3. Set SSH Protocol to 2	SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure.	Edit the /etc/ssh/sshd_config file to set the parameter as follows: Protocol 2	High	✗	Not configured
1.4. Set LogLevel to INFO	The INFO parameter specifies that record login and logout activity will be logged.	Edit the /etc/ssh/sshd_config file to set the parameter as follows: LogLevel INFO	Medium	✓	loglevel INFO
1.5. Set Permissions on /etc/ssh/sshd_config	The /etc/ssh/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root.	If the user and group ownership of the /etc/ssh/sshd_config file are incorrect, run the following command to correct them: # chown root:root /etc/ssh/sshd_config If the permissions are incorrect, run the following command to correct them:	High	✓	0 0 644
1.6. Disable SSH X11 Forwarding	The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.	Edit the /etc/ssh/sshd_config file to set the parameter as follows: X11Forwarding no	Medium	✗	x11forwarding yes
1.7. Set SSH MaxAuthTries to 4 or Less	The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure.	Edit the /etc/ssh/sshd_config file to set the parameter as follows: MaxAuthTries 4	Low	✗	maxauthtries 6

Данные по профилю

Couch

- Objects
- Scans
- Profiles
- Users
- Service
- Info
- couch

Profile Components Report

Profiles / [OpenSSH 7/8 \(ver. 14\)](#)

[OpenSSH 7/8 \(ver. 14\)](#)
Comment: —
Component type: OpenSSH 7-9
Reports: [Requirements](#)

Risks

High	78%
Medium	11%
Low	11%

Compliance

Failed	34%
Passed	57%
Other	9%

Components	Status	Latest Successful Scan
Version 14 (actual) — 8 components		
OOO "Инксекьюрити" / Lab Linuxes		
Centos 7 / OpenSSH 7/8		#998 at 22.02.2023 15:18:20 UTC+03
Ubuntu 22 / OpenSSH 7/8		#996 at 22.02.2023 15:18:14 UTC+03
AlmaLinux 8 / OpenSSH 7/8		#997 at 22.02.2023 15:18:17 UTC+03
Rocky 8 / OpenSSH 7-9		#289 at 24.01.2023 13:02:16 UTC+03
SUSE 15 / OpenSSH 7/8		#326 at 08.02.2023 14:13:38 UTC+03
OOO "Инксекьюрити" / Test Clouds		
openSLES 15.3 / OpenSSH 7-9		#330 at 08.02.2023 14:35:03 UTC+03
aws-sles-15 / OpenSSH 7-9		#1001 at 22.02.2023 15:18:27 UTC+03
aws-sles-15-double / OpenSSH 7-9		#1002 at 22.02.2023 15:18:29 UTC+03

Old versions

Сводный отчет по требованиям

Couch Profile Requirements Report [Profiles](#) / [OpenSSH 7/8 \(ver. 14\)](#)

[XLSX](#)

Risk: ---
Score: ---
Components: 8 / 8
Requirements: ---

OpenSSH 7/8 (ver. 14)
Comment: ---
Component type: OpenSSH 7-9
Report: [Components](#)

Report

	Rocky 8	SUSE 15	openSLES 15.3	aws-sles-15	AlmaLinux 8	Centos 7	aws-sles-15-do...	Ubuntu 22
1.1 Keep the Version Updated	⚙️	⚙️	⚙️	⚙️	⚙️	⚙️	⚙️	⚙️
1.2 Enable authentication based on public / private keys	✅	✅	✅	✅	✅	✅	✅	✅
1.3 Set SSH Protocol to 2	✅	✅	✅	✅	✅	✅	✅	✅
1.4 Configure LogLevel	❌	✅	✅	✅	✅	✅	✅	✅
1.5 Set Permissions on configuration files	✅	✅	✅	✅	✅	✅	✅	✅
1.8 Disable SSH X11 Forwarding	❌	❌	❌	❌	✅	❌	❌	✅
1.9 Set SSH MaxAuthTries to 4 or Less	❌	❌	❌	❌	✅	❌	❌	✅
1.10 Set SSH IgnoreRhosts to Yes	✅	✅	✅	✅	✅	✅	✅	✅
1.11 Set SSH HostbasedAuthentication to No	✅	✅	✅	✅	✅	✅	✅	✅
1.12 Disable TCP Connection Forwarding	❌	❌	❌	❌	❌	❌	❌	✅
1.13 Disable SSH Root Login	❌	❌	❌	❌	❌	❌	❌	✅
1.14 Set SSH PermitEmptyPasswords to No	✅	✅	✅	✅	✅	✅	✅	✅
1.15 Do Not Allow Users to Set Environment Options	✅	✅	✅	✅	✅	✅	✅	✅
1.16 Ensure SSH LoginGraceTime is set to one minute or less	❌	❌	❌	❌	❌	❌	❌	❌

Objects
Scans
Profiles
Users
Service
Info
couch

Запросите демо Couch

Оставьте заявку на сайте:



Или свяжитесь с нами по адресу
info@couch.ru

