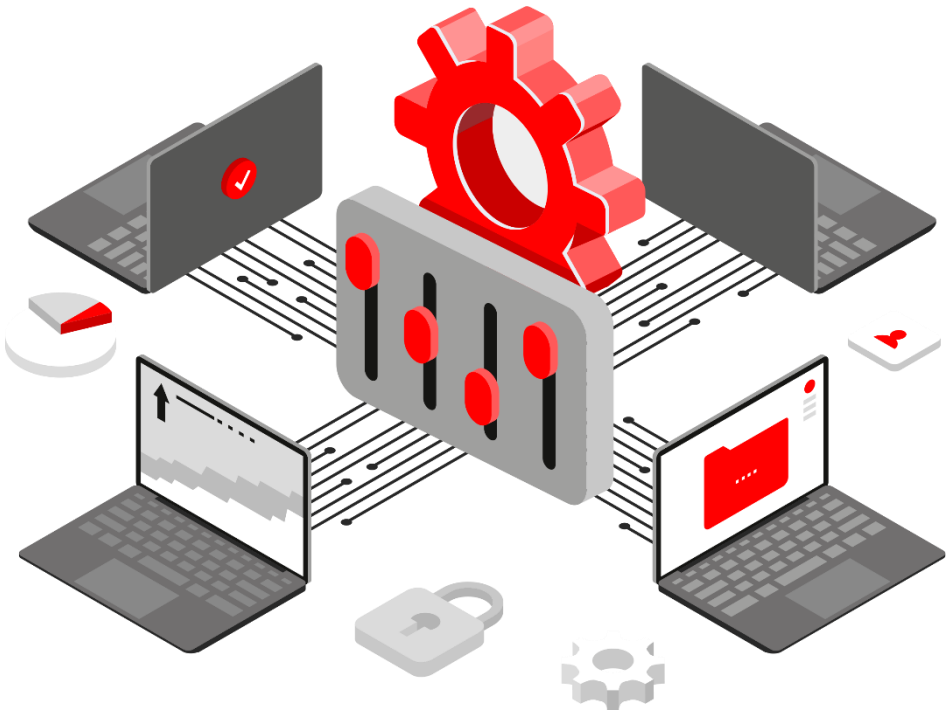
SPACE·BIT

X·CONFIG

Система управления уязвимостями конфигураций программного обеспечения



www.spacebit.ru

Уязвимости, связанные с человеческим фактором

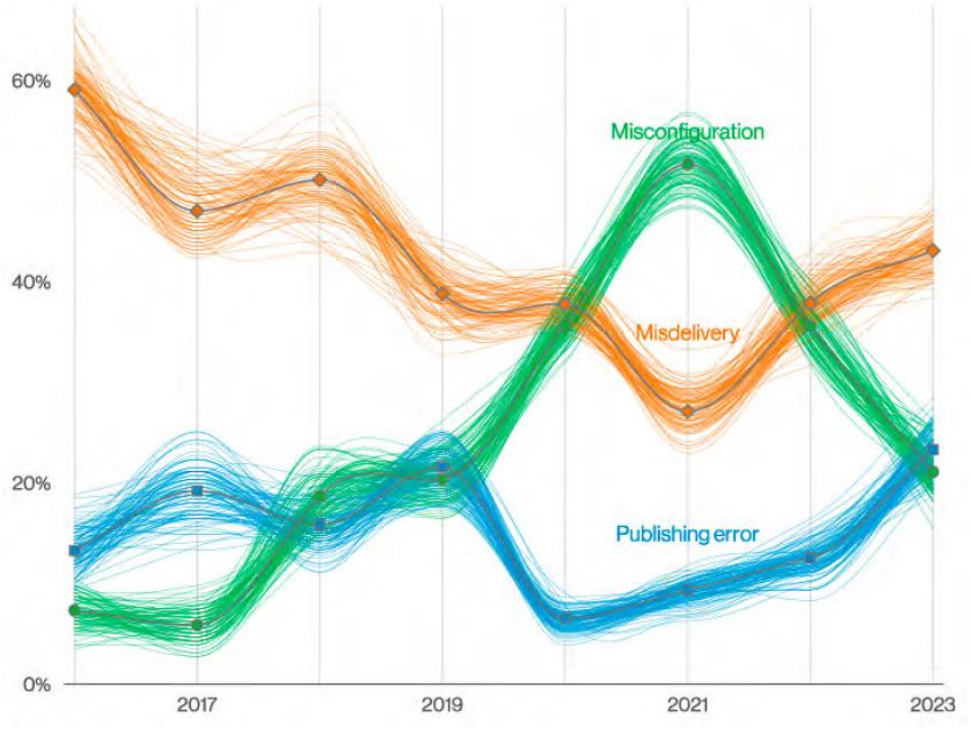


Figure 41. Action varieties over time in Miscellaneous Errors breaches

- **Небезопасные настройки**
- **Ошибки при доставке данных**
- **Ошибки при публикации**

(c) Data Breach Investigations Report, Verizon, 2023

Управление уязвимостями в информационных системах

Категория уязвимости	Распространенные методы предотвращения уязвимостей данной категории	Зона ответственности
Уязвимости проектирования	▪ Моделирование угроз и нарушителей ▪ Включение требований безопасности в задание на создание системы	Разработчик
Уязвимости реализации	▪ Анализ безопасности исходного кода приложений ▪ Тестирование безопасности при приемке системы ▪ Устранение выявленных уязвимостей уровня реализации	Разработчик
Уязвимости конфигурации	▪ Разработка и применение стандартов безопасной конфигурации ▪ Периодическое тестирование безопасности ▪ Периодическое сканирование уязвимостей ▪ Установка обновлений безопасности, устраняющих известные уязвимости	Потребитель

ЛЮБАЯ СИСТЕМА, ДАЖЕ НЕ ОБЛАДАЮЩАЯ УЯЗВИМОСТЯМИ УРОВНЯ ПРОЕКТИРОВАНИЯ И РЕАЛИЗАЦИИ, ПРЕДСТАВЛЯЕТ СОБОЙ СУЩЕСТВЕННУЮ УГРОЗУ БЕЗОПАСНОСТИ, ЕСЛИ ОНА НЕ СКОНФИГУРИРОВАНА ДОЛЖНЫМ ОБРАЗОМ

X-CONFIG

Система управления уязвимостями конфигураций программного обеспечения. Решение позволяет выстроить постоянный процесс управления безопасностью конфигураций системного и прикладного программного обеспечения и снизить риски информационной безопасности, связанные с некорректной настройкой ПО.

X-Config необходим, если:

- **Отсутствует актуальная информация** о состоянии конфигураций ПО с точки зрения ИБ
- В результате аудита **образуется большой объем неструктурированных и неприоритизированных данных**
- **Большая нагрузка на ИТ и ИБ-службы** в результате отсутствия выстроенного процесса
- Используемые **групповые политики не закрывают проблему**, необходим контроль

Обеспечение соответствия требованиям регуляторов

- Частично АН3.1
- Частично АН3.3
- Частично АН3.4
- Частично УКФ.2
- Частично УКФ.4

Приказ ФСТЭК №21

- АУД.1
- АУД.10
- УКФ.4

Приказ ФСТЭК № 31 и 239

- Частично АН3.1
- Частично АН3.3
- Частично АН3.4

Приказ ФСТЭК № 17

Выгода X-Config

Для ИБ

- **Сокращение рисков ИБ** за счет повышения защищенности ресурсов и минимизации влияния человеческого фактора
- **Соблюдение требований** регулятора и внутренних политик ИБ
- **Сокращение трудозатрат** за счет автоматизации процесса управления конфигурациями

Для ИТ

- **Повышение эффективности** работы по устранению уязвимостей за счет наглядной и приоритизированной отчетности
- **Сокращение трудозатрат** за счет автоматизации процесса управления конфигурациями

Для бизнеса

- **Сокращение затрат** за счет экономии времени высококвалифицированных специалистов и минимизации рисков финансовых и репутационных потерь из-за атак на ИТ-инфраструктуру
- **Повышение прозрачности и контроля** работы ИБ и ИТ-служб

Возможности X-Config

Обеспечение соответствия требованиям и лучшим практикам конфигурации ПО
Система отслеживает соответствие ресурсов требованиям регуляторов, а также лучшим общепризнанным практикам безопасного конфигурирования

Приоритизация несоответствий по степени критичности
Система автоматически расставляет приоритеты для ликвидации выявленных уязвимостей и отслеживает их устранение

Инвентаризация ресурсов сети
Система проводит инвентаризацию защищаемых машин, в рамках которой определяются: тип аппаратного обеспечения, платформа (ОС), установленное ПО, обновления, открытые сетевые порты

Организация процесса управления уязвимостями конфигураций ПО
Система выстраивает рабочий процесс по управлению конфигурациями ПО на основе политик ИБ: проверяет ресурсы, контролирует фактическое закрытие уязвимостей и формирует отчеты

Формирование корпоративных политик безопасного конфигурирования
Механизм профилирования позволяет вносить изменения в готовые стандарты в соответствии с внутренними политиками

Масштабирование для применения в крупных разветвленных инфраструктурах
Сеть коллекторов позволяет масштабировать сбор информации о конфигурациях до необходимой производительности

Ролевая модель взаимодействия

Администратор X-Config	Главный офицер безопасности	Офицер безопасности	ИТ специалист
управляет всеми настройками и пользователями системы	утверждает профили стандартов безопасного конфигурирования	наполняет реестр ресурсов, заводит задачи, создает профили проверки	на основе отчетности организует работы по устранению уязвимостей

Преимущества X-Config

Поддержка лучших практик безопасного конфигурирования и богатая собственная экспертиза

Проработанная регулярно расширяемая **библиотека готовых стандартов** с информацией по каждой настройке

Гибкое профилирование стандартов, учитывающее неоднородность и индивидуальность каждой инфраструктуры

Безагентная технология не требует установки дополнительного ПО и более безопасна

Возможность кастомизации решения с учетом бизнес-задач, а также индивидуальной разработки стандартов

Возможность интеграции с другими средствами защиты информации (SIEM, IRP, SOAR, CMDB)

Масштабируемость для обслуживания десятков тысяч хостов в рамках одной инсталляции системы

Полностью **российская разработк**а (номер в Реестре российского ПО 7045), техподдержка и сопровождение проектов от вендора

Источники для формирования стандартов безопасного конфигурирования

- Лучшие международные практики
- Требования регуляторов и отраслевых стандартов
- Собственная экспертиза
- Технологическое сотрудничество с производителями ПО

Готовые стандарты

СПО:

Windows:

- Windows Server 2012/2016/2019/2022
- Windows 10/11

***NIX:**

- Astra Linux SE 1.7 
- РЕД ОС 
- ОС Альт 
- CentOS 7/8
- Debian 10/11
- OpenSUSE 15.2
- RHEL 7/8
- Ubuntu 18/20/22
- FreeBSD 12.2
- AlterOS
- ОС Атлант

ППО:

Веб-серверы:

- Nginx 1.x
- Microsoft IIS
- Apache HTTP Server
- Angie Pro

Контейнеры сервлетов:

- Apache Tomcat 9

Почтовые серверы:

- Microsoft Exchange Server

СУБД:

- PostgreSQL / Postgres Pro 
- Microsoft SQL Server
- Apache Cassandra
- Oracle DB

Офисные пакеты :

- Microsoft Office 2016/2019/2022/365E

Веб-браузеры:

- Google Chrome
- Microsoft Edge / Internet Explorer 11
- Яндекс.Браузер 
- Mozilla Firefox

Виртуальные инфраструктуры:

- VMware
- Docker

Кейсы

Заказчик: **Территориально распределенная государственная организация**

Проблема:

- В ИТ-инфраструктуре более 1500 АРМ, серверов и виртуальных машин, в настройках информационных систем ежедневно совершаются сотни изменений
- Штат сотрудников, ответственных за информационную безопасность, составляет всего 3 человека
- В ситуации ограниченности ресурсов оперативный контроль за безопасностью конфигураций оборудования и ПО крайне затруднителен

Решение: Для минимизации рисков, связанных с уязвимостями конфигураций ПО, и повышения общего уровня ИБ была внедрена система X-Config, которая позволила выстроить непрерывный процесс управления конфигурациями программного обеспечения. Благодаря X-Config были автоматизированы процессы инвентаризации ресурсов сети и контроля соответствия настроек системного и прикладного ПО практикам безопасного конфигурирования и требованиям регуляторов.

Результат:

- Существенно снижены трудозатраты высококвалифицированных специалистов
- Обеспечено оперативное выявление уязвимостей и отслеживание их устранения

Кейсы

Заказчик: **Страховая организация**

Проблема:

- Необходимость обеспечить практическую безопасность ИТ-инфраструктуры, а также соответствие законодательству. Компания осуществляет процесс импортозамещения, обрабатывает большие объемы конфиденциальной информации и обязана соблюдать требования регуляторов (21 Приказ ФСТЭК России, 239 Приказ ФСТЭК России, ГОСТ Р 57580.1-2017, PCI-DSS) в части ИБ

Решение: Т.к. управление безопасностью конфигураций программного обеспечения является базовым элементом системы ИБ, стояла задача автоматизировать этот процесс. Была выбрана система X-Config, которая позволила не только выполнить все требования регуляторов и отраслевых стандартов в части безопасного конфигурирования ПО, но и существенно повысить реальный уровень ИБ в организации, снизив риски утечек конфиденциальных данных. X-Config обеспечивает регулярную проверку безопасности настроек информационных систем и, благодаря приоритизированным отчетам, позволяет устранять уязвимости в кратчайшие сроки.

Результат:

- Обеспечен эффективный контроль за конфигурациями как иностранного ПО, так и значительного количества российских систем, на которые перешла компания, в том числе отечественных ОС.

Кейсы

Заказчик: Агрохолдинг

Проблема:

- Постоянная нехватка ИБ- и ИТ-специалистов приводит к недостаточному вниманию к безопасности информационных систем, неопределенности в разделении полномочий и зонах ответственности. Проверки конфигураций ПО производятся раз в год.

Решение: С внедрением X-Config компания смогла автоматизировать процесс формирования и применения корпоративных политик безопасности. ИБ- и ИТ-специалисты получили удобный инструмент для совместной работы, анализа ситуации и оперативной реакции на несоответствие текущих конфигураций управляемых систем эталонным. С помощью гибкого механизма профилирования сотрудники департамента ИБ создают и утверждают корпоративные стандарты безопасного конфигурирования, наполняют реестр ресурсов, заводят задачи, создают профили проверки, а ИТ-специалисты на основе отчетности от X-Config организует работы по устранению выявленных уязвимостей.

Результат:

- Снижено влияние человеческого фактора как источника потенциальных уязвимостей
- Усилена безопасность информационных систем
- Совместная работа ИБ- и ИТ-специалистов стала более продуктивной и сфокусированной на контроле критически важных параметрах и ресурсов, что позволило оптимизировать трудозатраты, четко разграничить полномочия и избежать дублирования усилий

Кейсы

Заказчик: Крупная медицинская организация с распределенной филиальной структурой и сетью франчайзи

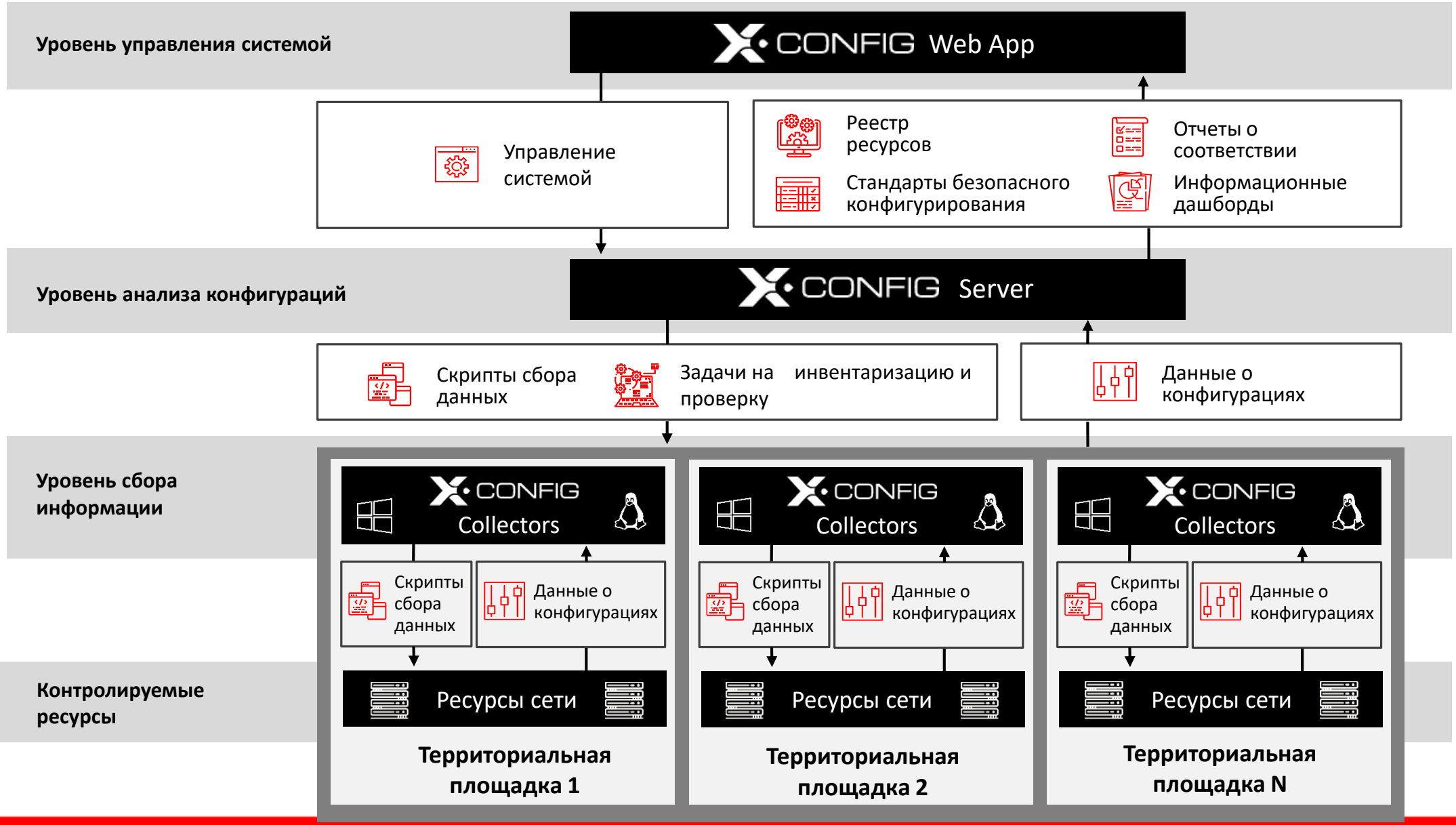
Проблема:

- Из-за отсутствия контроля за конфигурациями было допущено проникновение вируса-шифровальщика, в результате чего работа была практически полностью парализована (зашифрованы данные клиентов, их медицинские карты, результаты анализов в лабораториях, весь архив МРТ и рентгенографии)

Решение: X-Config позволил избежать повторных атак на ИТ-инфраструктуру, благодаря выстроенному с его помощью непрерывному процессу контроля за состоянием настроек используемого системного и прикладного программного обеспечения. Автоматизация управления уязвимостями конфигураций обеспечивает инвентаризацию ресурсов и проверку состояния их настроек по выбранному расписанию, что дает возможность ИБ-специалистам оперативно контролировать фактическое закрытие выявленных несоответствий на основе информативных отчетов с приоритизацией уязвимостей по степени критичности.

Результат:

- Усилен контроль за конфигурациями ПО, что существенно снизило риски проникновений со стороны злоумышленников и утечки конфиденциальной информации
- Заказчик пересмотрел свое отношение к развитию ИБ, значительно повысил ее уровень и стал более готовым к возможным угрозам и вызовам в будущем


Уровень управления системой
CONFIG Web App
Управление системой
Реестр ресурсов
Отчеты о соответствии
Стандарты безопасного конфигурирования
Информационные дашборды
Уровень анализа конфигураций
CONFIG Server
Скрипты сбора данных
Задачи на инвентаризацию и проверку
Данные о конфигурациях
Уровень сбора информации
CONFIG Collectors
Скрипты сбора данных
Данные о конфигурациях
Ресурсы сети
Территориальная площадка 1
Территориальная площадка 2
Территориальная площадка N
Контролируемые ресурсы

Рекомендуемые системные требования

X-Config App:

- Веб-браузер
- Разрешение: 1366x768

X-Config Server:

- OS: ОС с Docker
- CPU: 6 Cores
- RAM: 12 GB
- HDD : 200 GB

Collector Windows:

- OS: Windows Server
- CPU: 2 Core
- RAM: 4 GB
- HDD: 80 GB

Collector Linux:

- OS: Linux
- CPU: 1 Core
- RAM: 2 GB
- HDD: 50 GB

Стек технологий:

- Java 11, Spring
- React
- NodeJS
- Nginx
- PostgreSQL
- MongoDB

Установка:

- Docker
- RPM
- DEB

О компании Spacebit

Spacebit - российский разработчик современных программных продуктов в области информационной безопасности. Компания создает эффективные инструменты, помогающие бизнесу и государственным организациям различного масштаба повышать уровень защищенности ИТ-инфраструктуры и автоматизировать процессы управления ИБ.

SPACE-BIT

Решения

X-CONFIG

Система управления уязвимостями конфигураций программного обеспечения

X-CONTROL

Система управления жизненным циклом средств криптографической защиты информации

SpaceView

Система мониторинга и реагирования на инциденты информационной безопасности

Наши преимущества

Российская разработка
все продукты создаются на территории РФ и включены в Реестр отечественного ПО

Универсальность применения
решения подходят для любых организаций вне зависимости от отрасли и масштаба

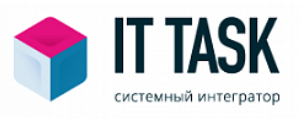
Простота развертывания и обслуживания
продукты быстро интегрируются в ИТ-инфраструктуру и легко поддерживаются

Гибкость и масштабируемость
системы масштабируются и кастомизируются под бизнес-требования заказчика

Политика лицензирования
модель лицензирования позволяет подобрать оптимальное решение для каждой компании

Оперативная техподдержка
специалисты помогут решить любые вопросы по настройке, эксплуатации и обновлению систем

Наши партнеры



Контакты

SPACE·BIT

www.spacebit.ru

info@spacebit.ru

+7 (495) 989-90-01