SKYBOX™ SECURITY

Полная видимость и понимание сети

и возможных векторов атак

Знание уязвимостей

Будьте в курсе всех уязвимостей вашей сети и знайте о связанных с ними угрозах

Понимание приоритетов

Расставляйте приоритеты и устраняйте пробелы в защите с учетом текущих настроек сети, анализа векторов атак и технологий визуализации атак

Оперативность действий

Автоматически формируйте план устранения уязвимостей вашей сети и принимайте меры по защите своих активов за минуты

Skybox™ Security Suite предоставляет широкий набор инструментов для обеспечения безопасности сети, аналитики и отчетности (SOAR - security operations, analytics and reporting):

- Оптимизация процессов управления безопасностью и повышение их эффективности
- Объединение разрозненных данных путем интеграции с 120+ решениями ИТ и ИБ
- Детальный анализ сети, моделирование и визуализация возможных векторов атак без влияния на работоспособность сети
- Автоматизация сложных процессов управления уязвимостями и политиками сетевой безопасности

SKYBOX™ SECURITY SUITE
Integrated Security Analytics

Vulnerability Control

Анализ уязвимостей с учетом векторов атак

Управление уязвимостями в контексте сети и с учетом потенциально реализуемых векторов атак даже в период между сканированиями

Network Assurance

Видимость и контроль сети

Визуализация сети, автоматический контроль зон безопасности и соответствия настроек сети установленным политикам

Firewall Assurance

Управление межсетевыми экранами

Анализ, конттроль и оптимизация всех межсетевых экранов в одной консоли

Skybox Horizon

Контроль индикаторов угроз

Визуализация индикаторов угроз (Indicators of exposure), связанных с наличием уязвимостей и небезопасными настройками сети

Change Manager

Автоматизация изменений настроек

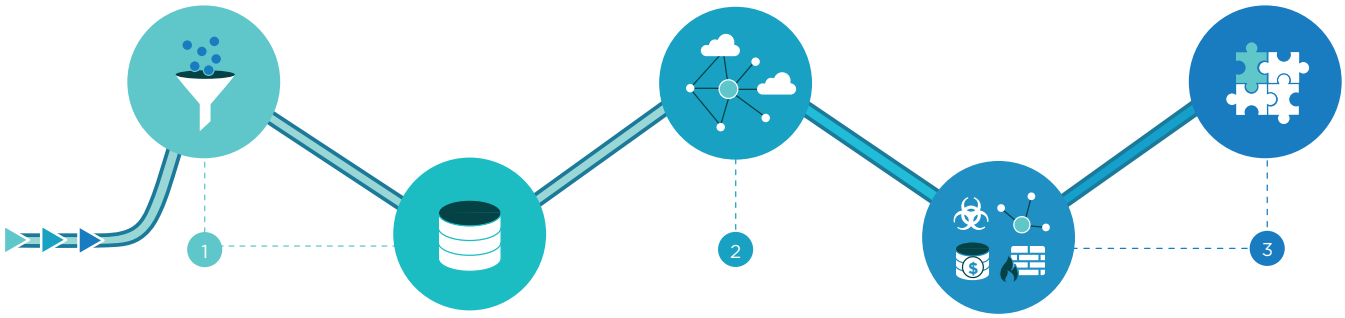
Автоматизация изменений настроек межсетевых экранов и оценка их влияния на безопасность сети и соответствие политикам

Skybox **Network Assurance**

ПОЛНАЯ ВИДИМОСТЬ СЕТИ

- Сбор конфигуаций со всех сетевых устройств и автоматическое построение карты сети
- Контроль соответствия настроек стандартам конфигурирования, лучшим практикам и внутренним политикам
- Анализ и визуализация на карте сети возможных маршрутов для заданного типа трафика, отображение всех разрешающих или запрещающих правил и настроек для данного маршрута
- Автоматический контроль установленных правил сегментирования как в масштабах всей сети, так и на уровне настроек отдельных устройств
- Моделирование изменений в виртуальной сетевой модели What- If ("песочнице")

Как Это Работает



1. Сбор Данных

- Автоматический сбор данных со всех сетевых устройств Layer 3
- Нормализация данных для оперативного и глубокого анализа

2. Построение Модели

- Создание полной визуальной модели сети с учетом реальной топологии
- Отображение различных сетевых сред: физические и виртуальные сети, сети АСУ ТП

3. Анализ и Контроль

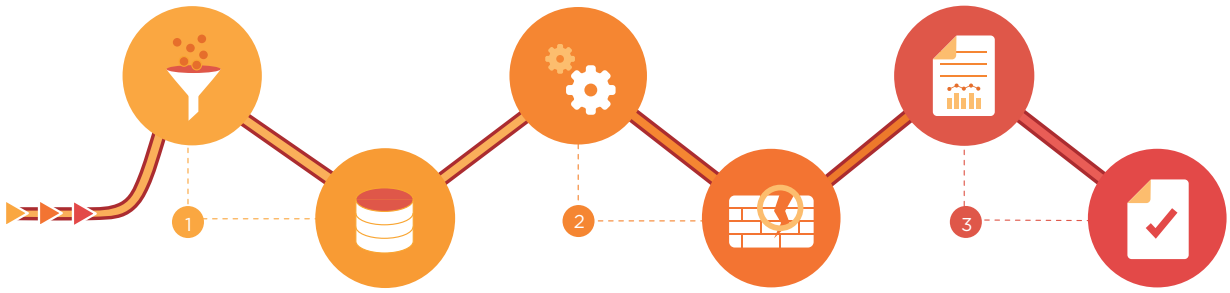
- Выявление проблем в конфигурациях, анализ наличия или отсутствия доступа, контроль соответствия политикам сетевой безопасности

Skybox **Firewall Assurance**

НЕПРЕРЫВНЫЙ КОНТРОЛЬ И АНАЛИЗ СИСТЕМЫ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

- Автоматический сбор конфигураций межсетевых экранов и непрерывный мониторинг настроек, включая отслеживание изменений правил доступа
- Оптимизация списков доступа межсетевых экранов: выявление затененных, дублирующихся и неиспользуемых правил и объектов, формирование рекомендаций по оптимизации
- Контроль соответствия настроек стандартам конфигурирования, лучшим практикам и внутренним политикам, включая выявление причин несоответствия вплоть до конкретных правил на конкретных межсетевых экранах
- Автоматический контроль соответствия политике доступа (встроены стандарты PCI DSS, NIST) на уровне зон безопасности межсетевых экранов и выявление причины нарушений вплоть до конкретных правил на конкретных устройствах

Как Это Работает



1. Сбор и Нормализация

- Автоматический сбор конфигураций и логов
- Нормализация данных для опертивного и детального анализа

2. Анализ

- Анализ соответствия настроек установленным правилам и политикам
- Анализ изменений и их влияния на безопасность

3. Отчеты и Оптимизация

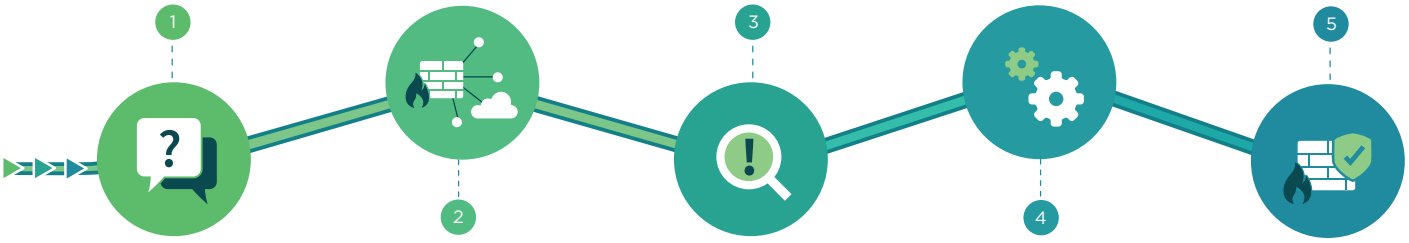
- Формирование настраиваемых отчетов
- Рекомендации по оптимизации правил доступа и настроек

Skybox **Change Manager**

АВТОМАТИЗАЦИЯ ИЗМЕНЕНИЙ ПРАВИЛ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

- **Автоматизированная обработка запросов на изменения правил доступа межсетевых экранов**
- **Определение всех устройств, требующих внесения изменений**
- **Оценка влияния вносимых изменений на соответствие установленным политикам доступа для зон безопасности и на появление новых уязвимостей (при наличии модуля Vulnerability Control)**
- **Формирование рекомендаций по изменениям правил и объектов**
- **Автоматическое применение изменений правил и проверка корректности их реализации**
- **Гибко настраиваемый процесс внесения изменений, включая интеграцию с существующей системой заявок**

Как Это Работает



1–2. Запрос и Анализ

- Формализация запроса на изменение доступа
- Определение всех устройств, требующих внесения изменений

3–4. Оценка и Применение

- Оценка соответствия политикам и влияния на появление уязвимостей
- Формирование рекомендаций по изменению правил и объектов и их применение

5. Проверка

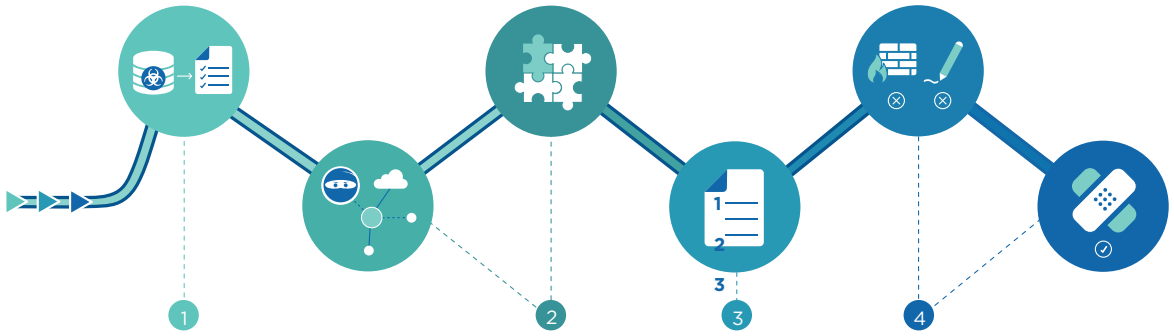
- Проверка корректности применения изменений

Skybox **Vulnerability Control**

ИННОВАЦИОННЫЙ ПОДХОД К УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

- Автоматический сбор информации об ИТ-активах (имеющиеся уязвимости, актуальный состав и версии ПО) из сканеров, систем инвентаризации и патч-менеджмента
- Выявление вновь появляющихся уязвимостей в период до и между сканированиями
- Расчет возможных векторов атак с учетом настроек сетевого оборудования, включая активированные сигнатуры IPS
- Приоритезация найденных уязвимостей с учетом возможности их реальной эксплуатации при текущих настройках сети
- Формирование рекомендаций по устранению уязвимостей, встроенная система заявок

Как Это Работает



1. Обнаружение

Загрузка данных из внешних сканеров и систем, дополнение за счет собственной базы уязвимостей Skybox

2. Анализ

Моделирование векторов атак в контексте вашей сети и с учетом ее настроек

3. Приоритезация

Расчет приоритетов с учетом наличия доступа к уязвимости и готовых эксплойтов

4. Устранение

Формирование плана устранения уязвимостей и векторов атак

Skybox **Horizon**

ВИЗУАЛИЗАЦИЯ И КОНТРОЛЬ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ СЕТИ

- Простое и наглядное представление наиболее проблемных мест с точки зрения безопасности сети
- Отображение индикаторов угроз (Indicators of exposure), отражающих наличие уязвимостей, которые могут быть проэксплуатированы с высокой вероятностью, некорректных конфигураций сетевого оборудования и правил межсетевых экранов

О компании Skybox Security

Skybox Security – новатор на рынке информационной безопасности, который предлагает решение совершенно нового класса. С одной стороны, платформа дает полную видимость сети, интегрируясь с 120+ различными ИТ и ИБ-решениями, и успешно реализует функционал, свойственный продуктам класса Firewall Management. С другой стороны, компонент Vulnerability and Threat Management работает с уязвимостями, имеющимися в ИТ-инфраструктуре, и позволяет моделировать вектора атак на конкретные активы с учетом настроек сети, что дает возможность своевременно выявлять наиболее опасные уязвимости и фокусироваться на их устранении. Такое сочетание возможностей продукта в рамках одной платформы делает ее действительно уникальной и одинаково востребованной как ИТ, так и ИБ-службами организаций различных отраслей.

SKYBOX™ SECURITY

www.skyboxsecurity.com | sales.russia@skyboxsecurity.com | +7 800 511 08 28