Skybox **Vulnerability Control**

THREAT-CENTRIC VULNERABILITY MANAGEMENT

- Автоматический сбор информации об ИТ-активах из сканеров, систем инвентаризации и патч-менеджмента, включая данные об уязвимостях, актуальном составе и версиях ПО
- Выявление вновь появляющихся уязвимостей в период до и между сканированиями
- Моделирование сети с учетом реальных настроек оборудования и эмуляция атак
- Приоритезация уязвимостей с учетом возможности их реальной эксплуатации
- Формирование рекомендаций по устранению уязвимостей, включая установку патчей, активацию сигнатур IPS и изменение настроек сети

Skybox™ Vulnerability Control обеспечивает непрерывность и системность процесса управления узявимостями. Решение дает полную видимость сети и возможных векторов атак, и использует этот контекст для анализа, приоритезации и устранения наиболее опасных уязвимостей.

"Сейчас платформа активно используется для решения повседневных задач. Более 50% от всего объема работ, связанных с безопасностью сети, помогает выполнить Skybox Security"

Начальник Управления ИБ крупной процессинговой компании

Процесс TCVM начинается с сбора и актуализации данных об уязвимостях, которые присутствуют в сети. Для этого Skybox использует широкий список источников, включая системы инвентаризации и патч-менеджемента, сетевые устройства, а также выявляет узявимости без сканирования. Skybox также собирает и объединяет данные сразу от нескольких сканеров и формирует централизованную актуальную базу имеющихся узявимостей.

Информация об уязвимостях обогащается за счет базы Skybox™ Research Lab, содержащей данные о наличии эксплойтов и возможных путях устранения уязвимости. Далее эти данные анализируются в контексте сети и с учетом ее настроек на текущий момент.

Моделирование сети и эмуляция векторов атак позволяет Skybox выявлять те уязвимые активы, которые наиболее подвержены угрозам. При этом Skybox при формировании рекомендаций по устранениюю фокусируется на тех доступных уязвимостях, которые наиболее вероятно могут быть использованы атакующими с учетом текущих настроек безопасности вашей сети. Благодаря полному пониманию сети, план устранения не ограничивается установкой патчей. Skybox также информирует вас о возможных изменениях настроек сети, котрые позволят эффективно устранить вектор атаки.

- Поиск доступных уязвимостей и вероятных векторов атак с учетом актуальных данных threat intelligence о ландшафте угроз
- Приоритезация уязвимостей с учетом их влияния на уровень угроз
- Поиск уязвимостей в "пассивном" режиме за счет встроенного механизма Skybox™ Vulnerability Detector
- Фокусирование на наиболее вероятных угроз для немедленного реагирования и устранения вектора атаки с учетом контекста сети
- Сбор, централизация и объединение данных от различных сканеров

ПРОЦЕСС TCVM

- Сбор данных об активах, инфраструктуре и конфигурациях и корреляция их со Skybox Intelligence Feed для "пассивного" выявления уязвимостей
- Информация о наличии доступных и уже использующихся эксплойтах для ваших уязвимостей
- Моделирование сети и эмуляция векторов ататк для выявления наиболее опасных уязвимостей
- Устранение уязвимостей путем установки патчей или изменений настроек безопасности сети; мониторинг состояния защищенности сети
- Отслеживание процесса реагирования и отчетность об эффективности устранения уязвимостей

Ежедневно в вашей сети появляются новые узявимости. Ландшафт угроз также динамически меняется. Очень важно быть уверенным в том, что ваши усилия направлены на устранение наиболее опасных уязвимостей.

Vulnerability Control использует данные о настройках сети, сведения об активах и информацию о текущем ландашфте угроз для выявления наиболее опасных уязвимостей, включая те, которые наиболее часто используются атакующими. Skybox дает вам инструмент автоматизированного сбора данных, моделирования, эмуляции и анализа, который позволяет эффективно реагировать на имеющиеся и вновь появляющиеся уязвимости в разы быстрее, чем при ручной обработке.

Процесс выявления уязвимостей

- Использование данных систем инвентаризации и патч-менеджмента (включая среды виртуализации и сегменты КИИ) и Skybox intelligence feed для выявления уязвимостей без сканирования
- Сбор, централизация и объединение данных из различных сканеров
- Выявление уязвимостей на сетевом оборудовании и сегментов, не подлежащих сканированию
- Skybox Vulnerability Detector использует результаты активного и пассивного сканирования для наиболее полной оценки имеющихся уязвимостей

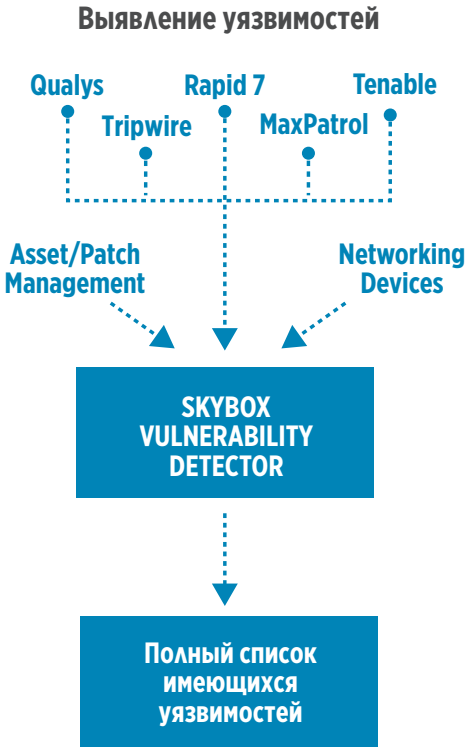
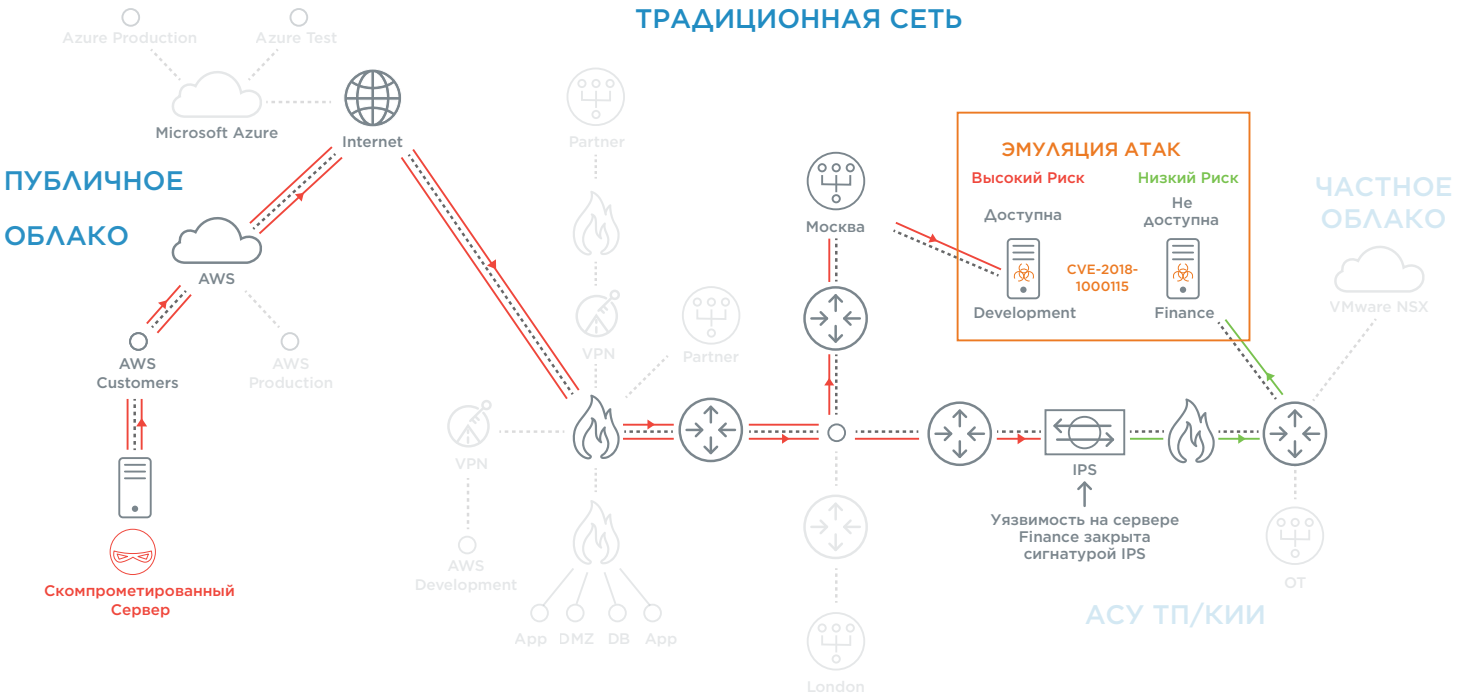


РИСУНОК 1: Skybox объединяет методы активного (сканеры) и пассивного сканирования (Skybox Vulnerability Detector) для выявления всех имеющихся уязвимостей.

Интеллектуальный Анализ и Threat Intelligence

- Выявление доступных уязвимостей за счет моделирования сети, анализа векторов атак и эмуляции многоступенчатых атак
- Выявление потенциальных сценариев атак и формирование компенсирующих мер
- Выделение уязвимостей, для которых уже есть доступные эксплойты или которые уже активно используются атакующими
- Контроль и оценка влияния планируемых изменений настроек сети на достæпность имеющихся уязвимостей

РИСУНОК 2: Анализ векторов атак и оценка возможности эксплуатации уязвимостей в вашей сети.



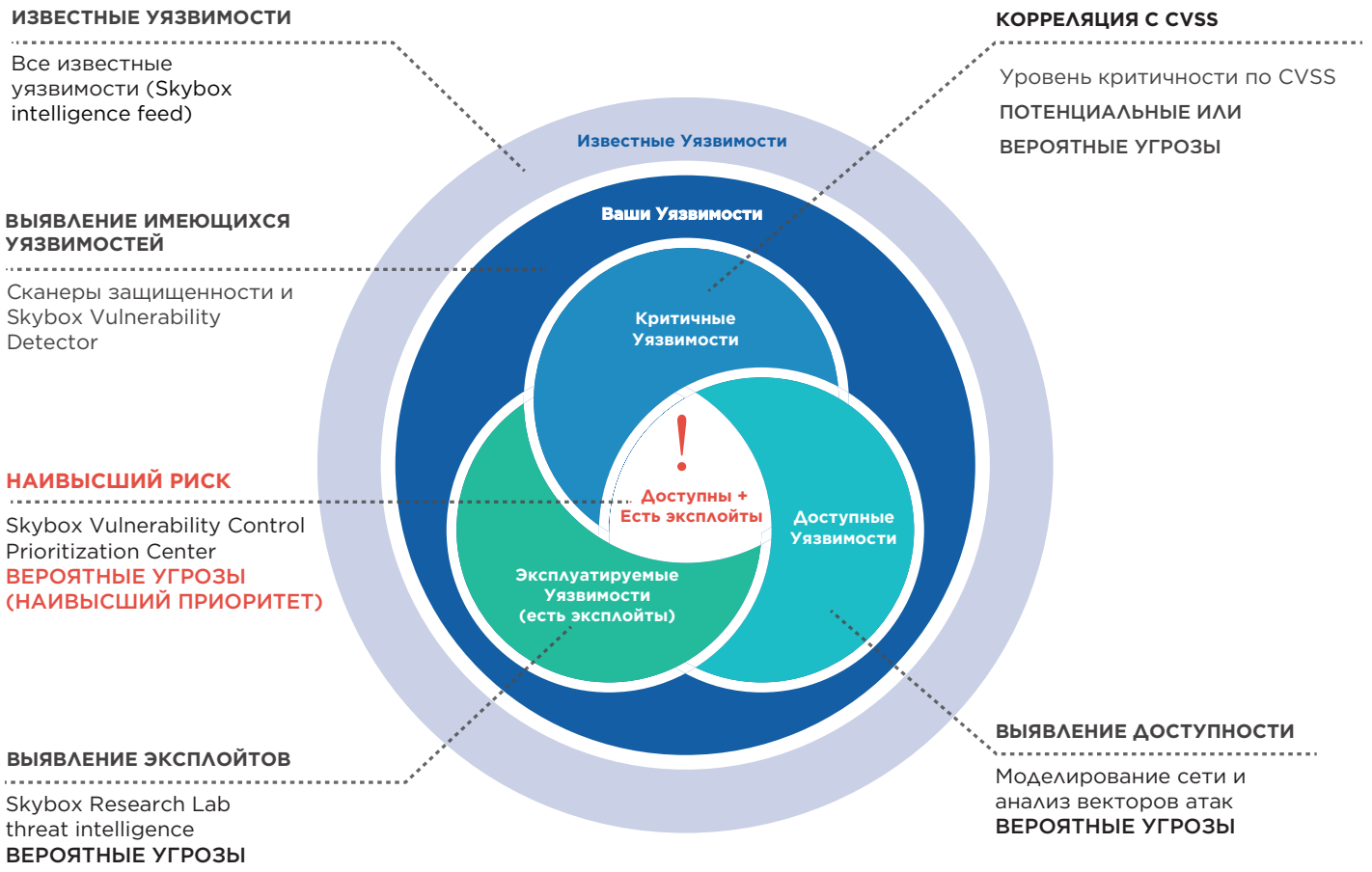
Оперативное Устранение Уязвимостей

- Информация о доступных патчах, сигнатурах IPS, обновлениях или изменениях ACL, которые могут устранить уязвимость или возможный вектор атаки
- Рекомендации по устранению ÞÉÖÊßÜÑÑ ËÑâßöäÞñè æÍâßÕ Ë äÑëÑÞÖÑ ëÉãßË, É ÞÑ ÏÞÑØ
- Непрерывный мониторинг потенциальных угроз с целью недопущения их перехода в статус вероятных
- Формирование возможных мер по снижению уровня угроз с учетом индивидуальных метрик

Приоритезация Уязвимостей с Учетом Уровня Угроз

- Повышение приоритета для доступных уязвимостей, которые наиболее вероятно могут быть использованы атакующими
- Анализ векторов атак с учетом настроек сети и базы знаний Skybox Threat Intelligence
- Приоритезация наиболее вероятных угроз, связанных с наличием уязвимостей для их дальнейшего оперативного устранения

РИСУНОК 3: Выделение уязвимостей, доступных для эксплуатации.



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.

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