JETSECURITY
CONFERENCE 2018

КАК ПЕРЕСТАТЬ ГОНЯТЬСЯ ЗА ПРИЗРАКАМИ ИЛИ СОВРЕМЕННЫЙ ПОДХОД К УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ

31 мая, 2018
Radisson Resort, Zavidovo

Проблемы управления уязвимостями

- Как часто Вы сканируете уязвимости?
  - 1 раз в месяц?
  - 1 раз в квартал?

- Как Вы узнаете о новых уязвимостях в период между сканированиями?
- Что делать, если нет возможности сканирования?

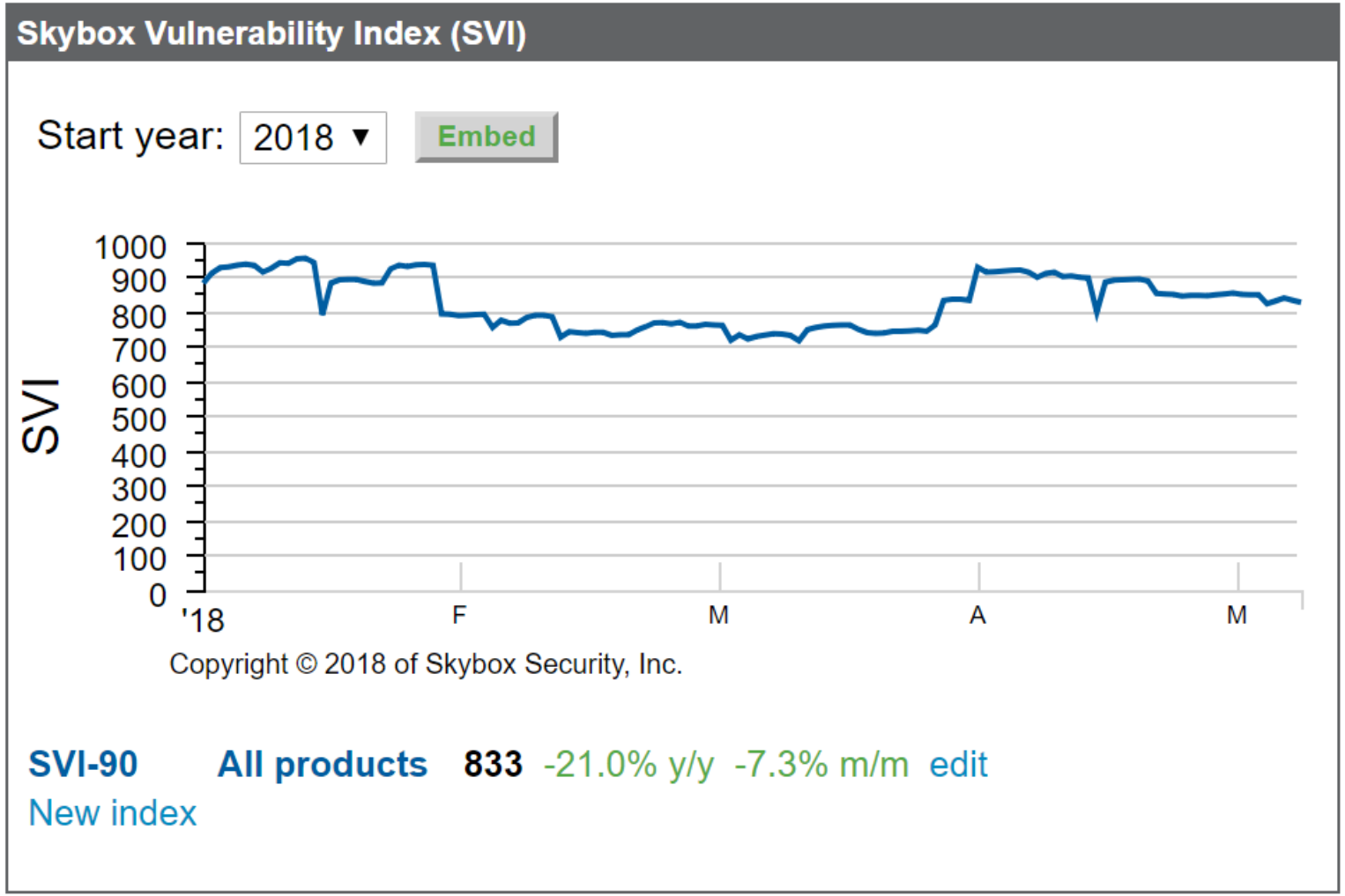
- Как вы оцениваете критичность уязвимостей?
  - На основе CVSS scoring?
  - Вы учитываете настройки Вашей сети? Наличие готовых эксплойтов?

Количество новых уязвимостей

700-950

новых уязвимостей

КАЖДЫЙ МЕСЯЦ



https://www.vulnerabilitycenter.com

Идея и реализация

Межсетевые экраны

Сетевое оборудование

Системы инвентаризации и патч-менеджмента

Сканеры защищенности

Знание настроек сети

Знание уязвимостей

Расчет индикаторов угроз и прогнозирование наиболее вероятных векторов атак

JETSECURITY
CONFERENCE 2018

Сценарии использования Skybox Security

Network Assurance

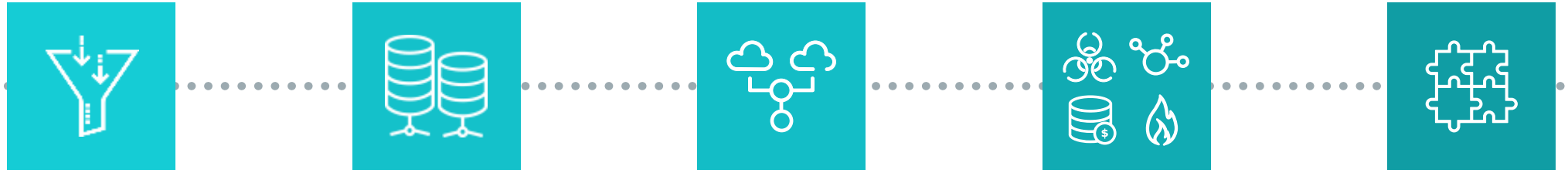
Полная видимость сети

Интерактивная карта сети

Автоматическая проверка соответствия стандартам конфигурирования

Автоматическая проверка соответствия политикам сегментирования

Как Это Работает

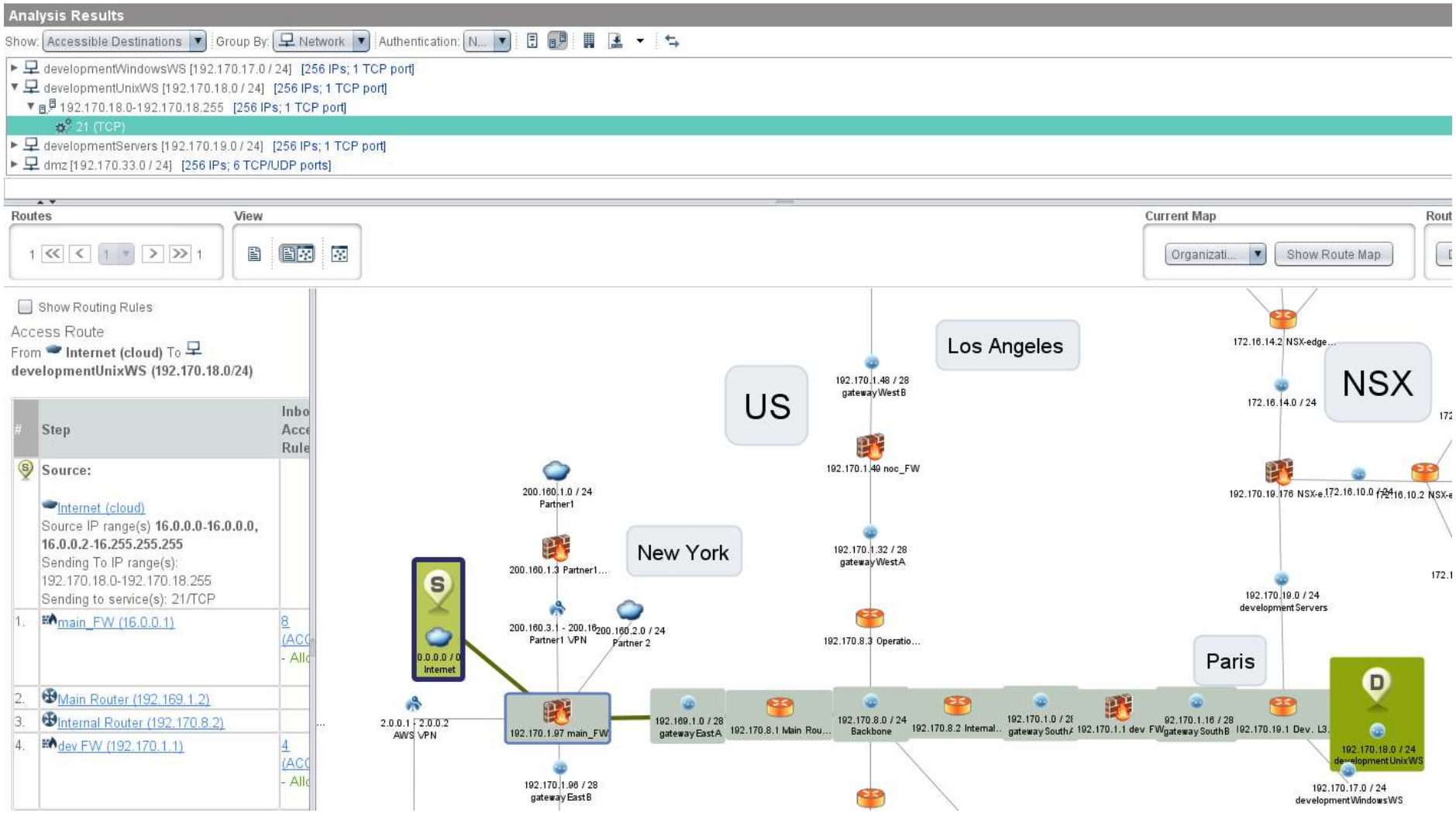


1 Сбор и нормализация

2 Моделирование

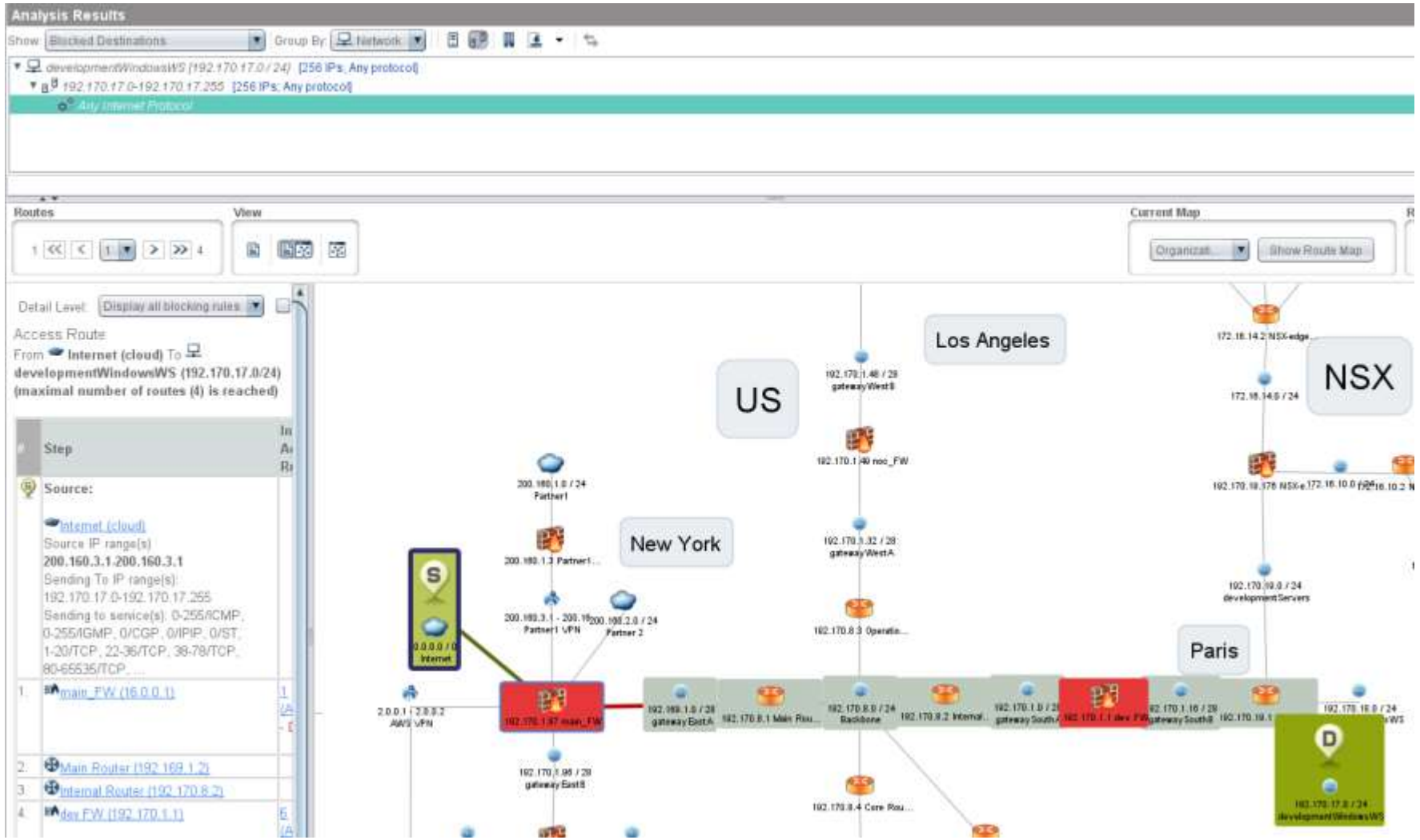
3 Детальный анализ

Проверка доступа на лету



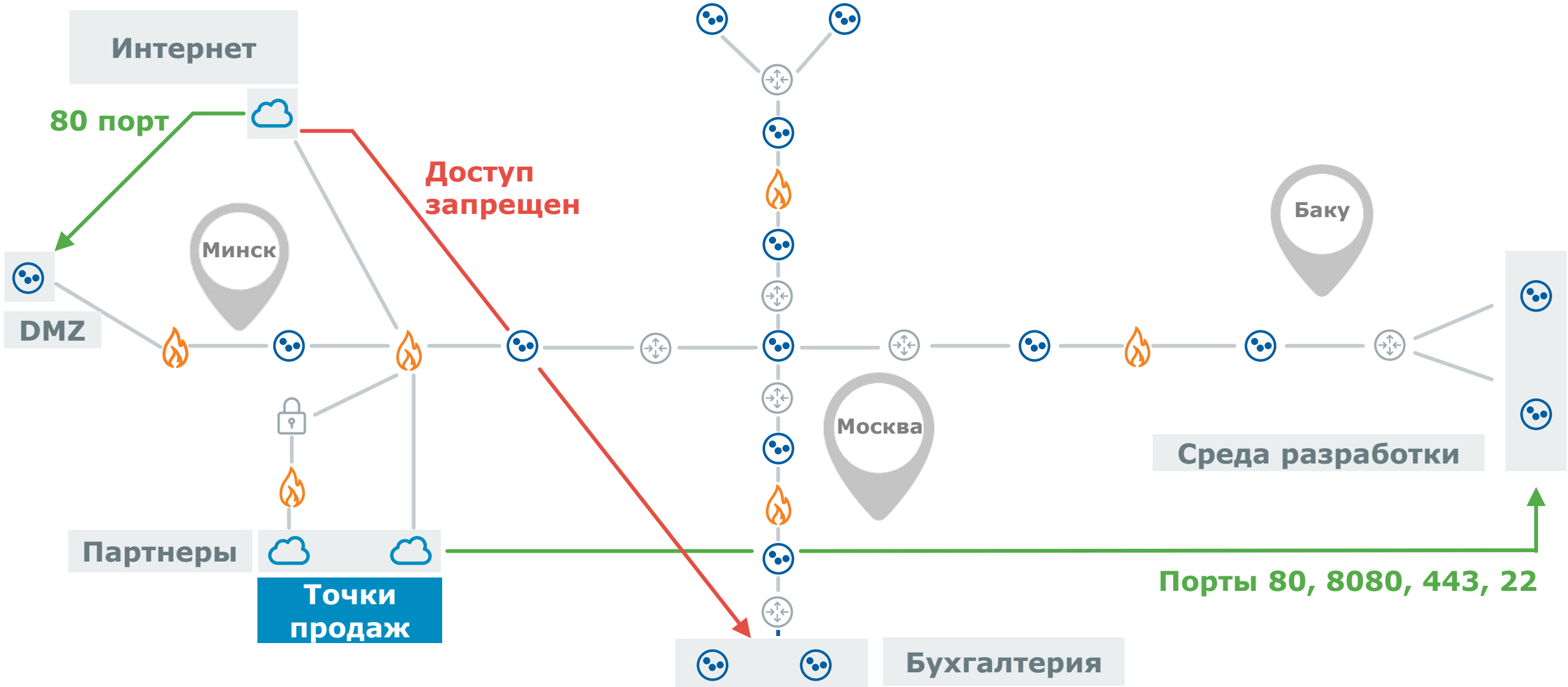
Проверяем наличие доступа в 2 клика

Проверка доступа на лету



Проверяем отсутствие доступа в 2 клика

Контроль политики доступа

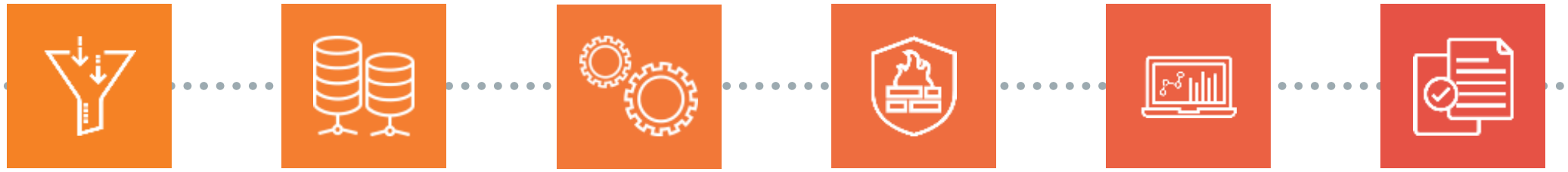


Firewall Assurance

Управление межсетевыми экранами

- Автоматический контроль зон безопасности
- Автоматический контроль соответствия стандартам конфигурирования
- Управление жизненным циклом правил доступа

Как Это Работает



1. Сбор и нормализация
2. Анализ
3. Отчеты и реагирование

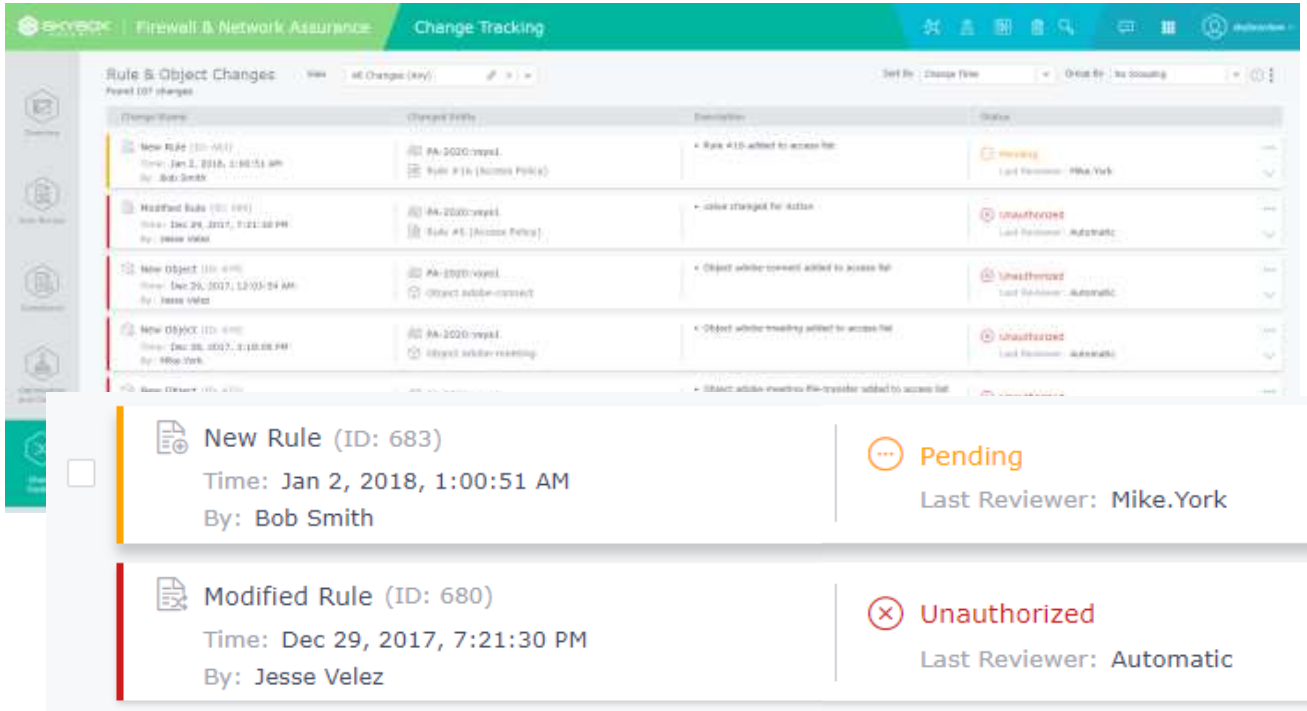
Контроль изменений на МЭ

Как это работает

- Все изменения конфигураций МЭ фиксируются Skybox
- Любое изменение проверяется на наличие соответствующей заявки/тикета

Что получаем

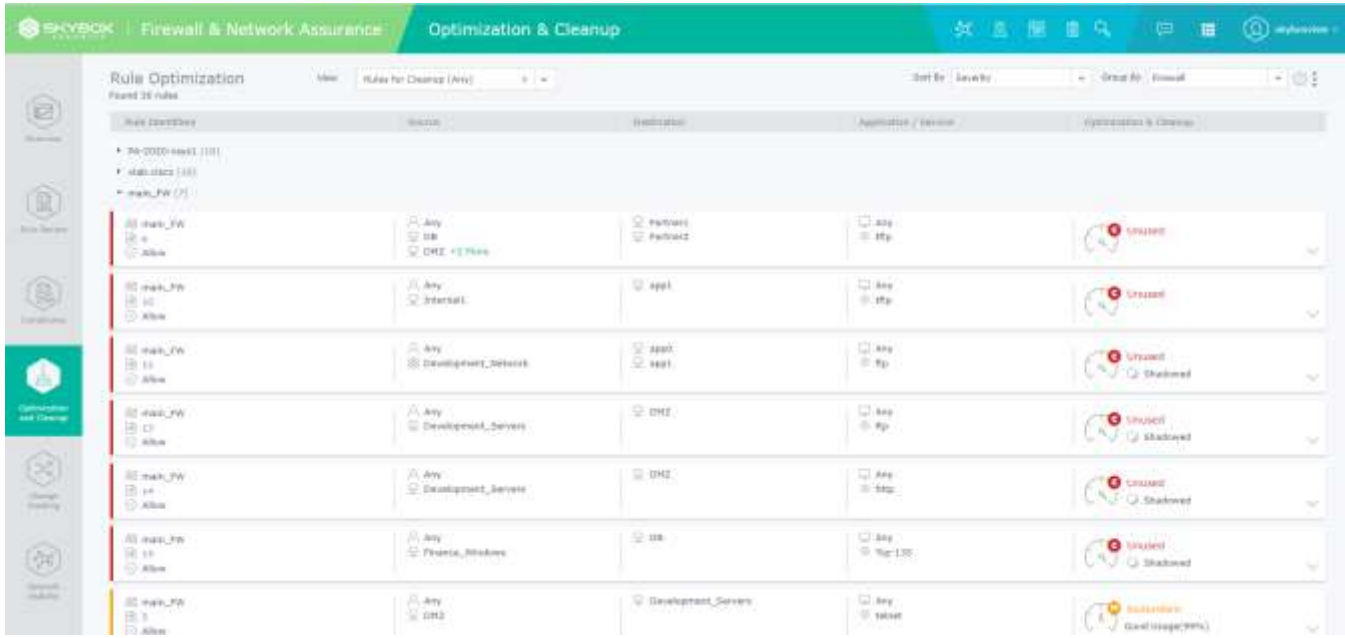
- Мониторинг всех изменений ACL
- Оценка их влияния на доступность сервисов и безопасность
- Выявления неавторизованных изменений, выполненных без соответствующей заявки



Оптимизация загрузки МЭ

Как это работает

- Выявление затененных, избыточных и дублирующих правил
- Выявление неиспользуемых правил
- Формирование рекомендаций



Что получаем

- Оптимизация правил и конфигураций
- Сокращение нагрузки до 50%

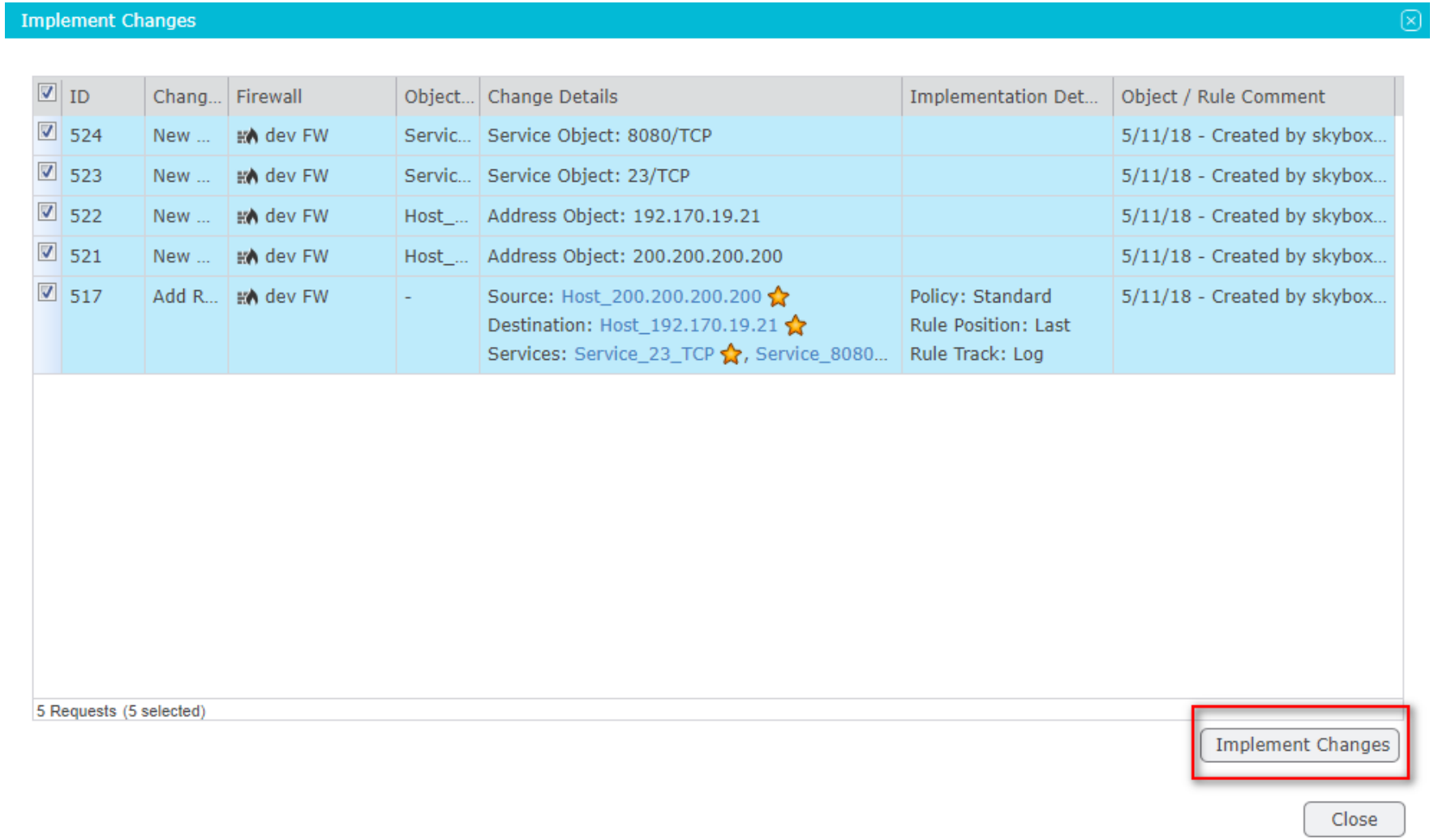
Change Manager

Firewall Change Management

- Автоматизация обработки заявок на изменения
- Автоматическая оценка рисков
- Ресертификация правил

Как Это Работает

Применение изменений



- Check Point
- Palo Alto
- Fortinet
- Cisco*
- Juniper*

Работа с уязвимостями

Vulnerability Control

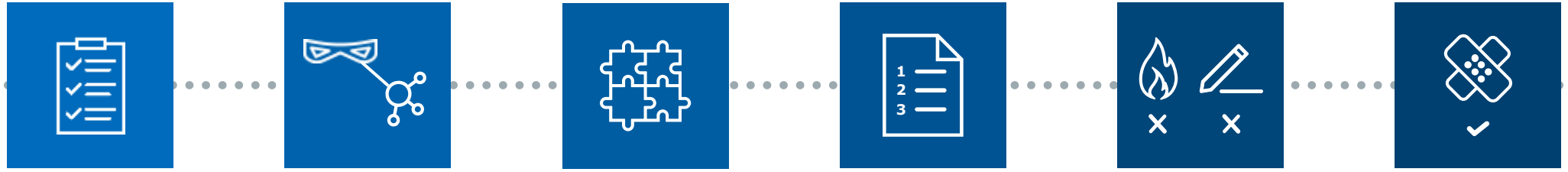
Управление уязвимостями с учетом векторов атак

Выявление уязвимостей в период до и между сканированиями

Расчет векторов атак в контексте сети

Расчет приоритетов и реагирование

Как Это Работает



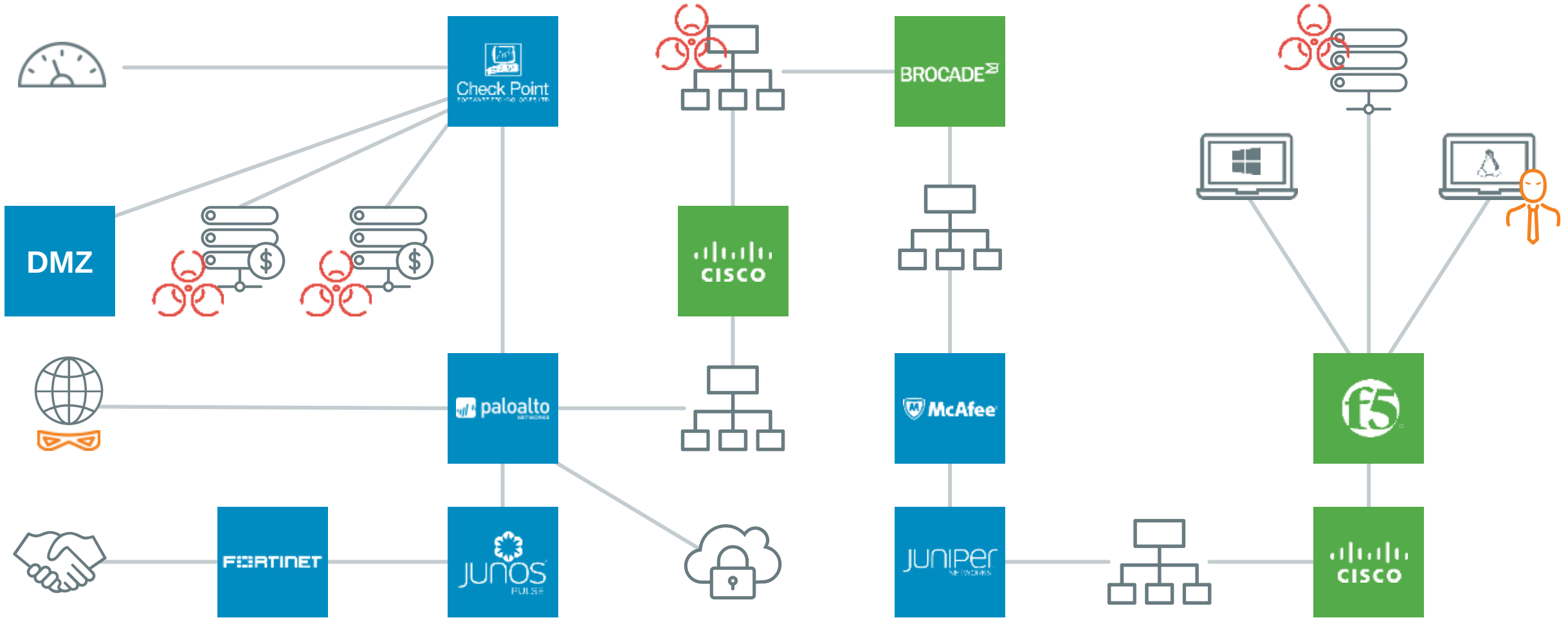
1 Выявление

2 Анализ

3 Приоритезация

4 Реагирование

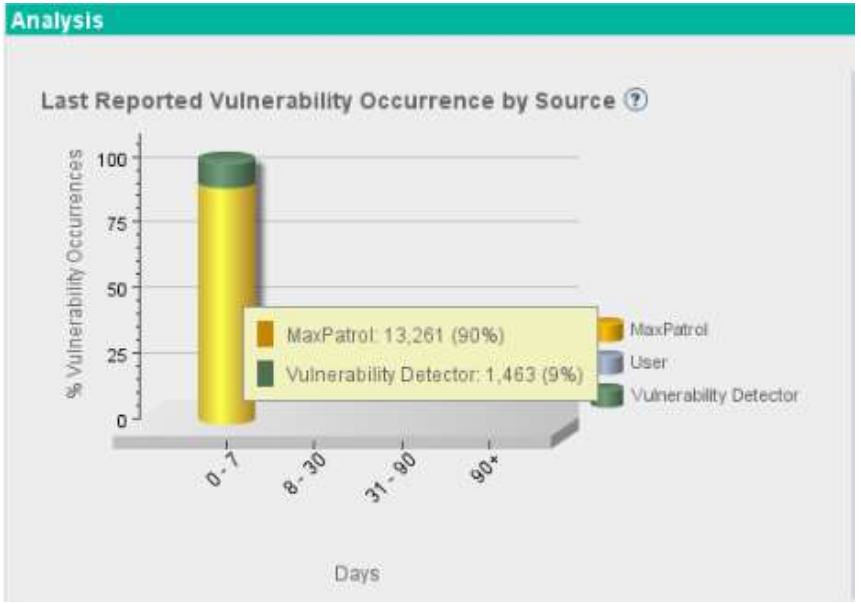
Моделирование вектора атаки



Средства защиты | Топология сети | ИТ-активы | Уязвимости | Источники угроз

Выявление уязвимостей

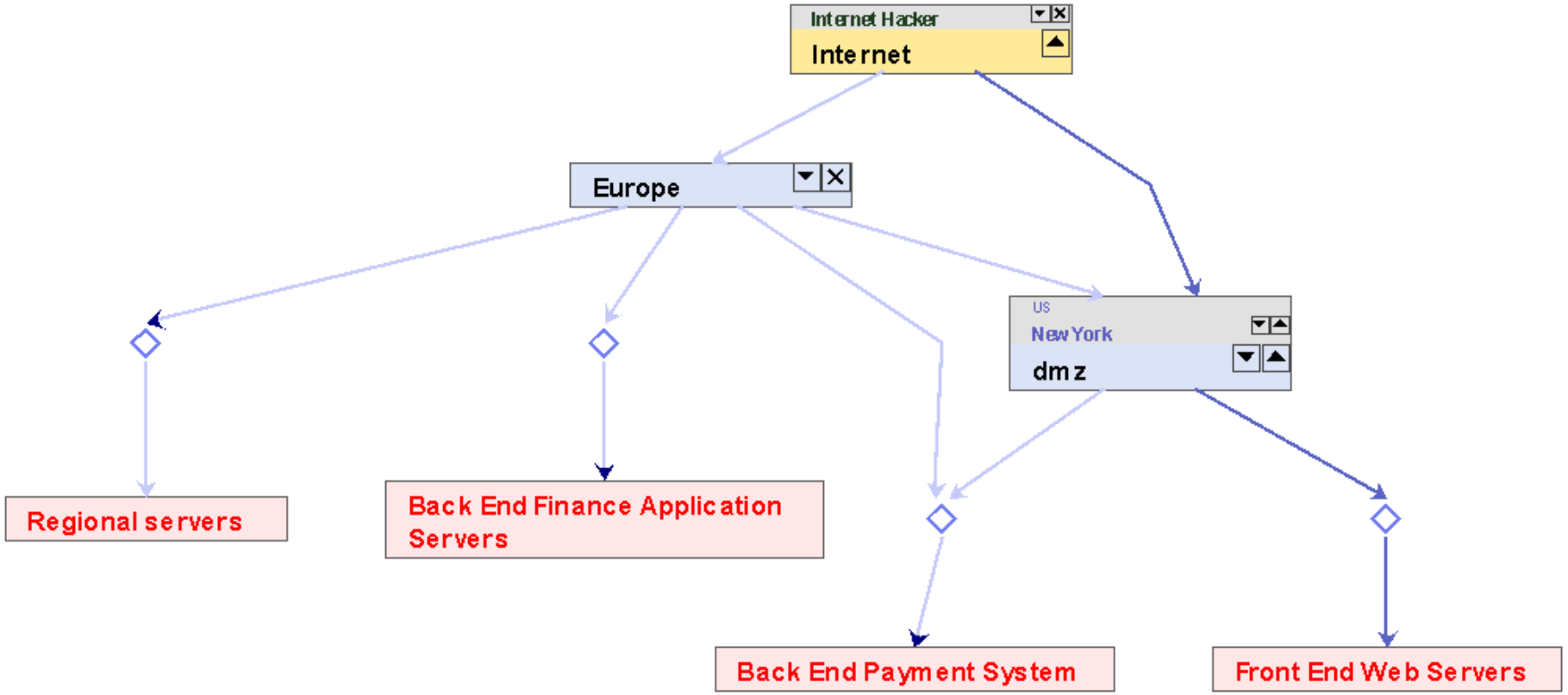
- Загрузка отчетов сканеров
- Загрузка отчетов систем инвентаризации SCCM, WSUS и др.
- Ежедневное обновление собственной базы уязвимостей
- Ежедневное «пассивное» сканирование

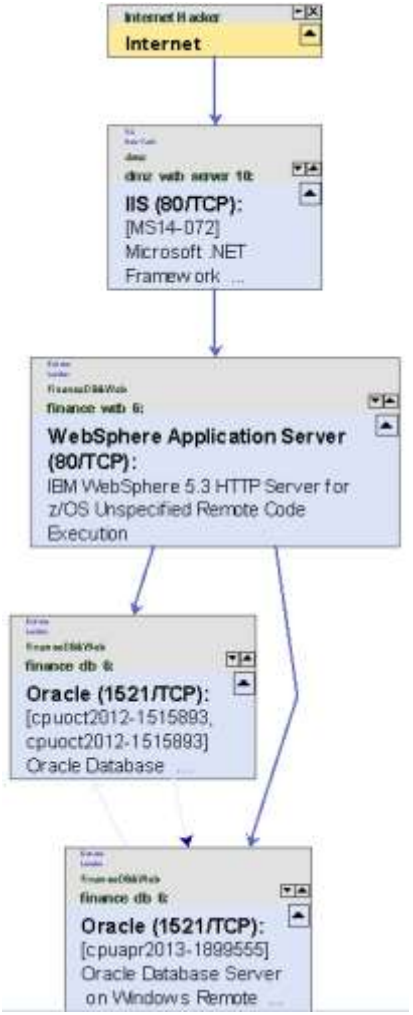


Что получаем

- Актуальный список всех известных уязвимостей (обновляемая база Skybox из 30+ источников)
- Актуальный список уязвимостей, существующих в ИТ-инфраструктуре

Визуализация вектора атаки





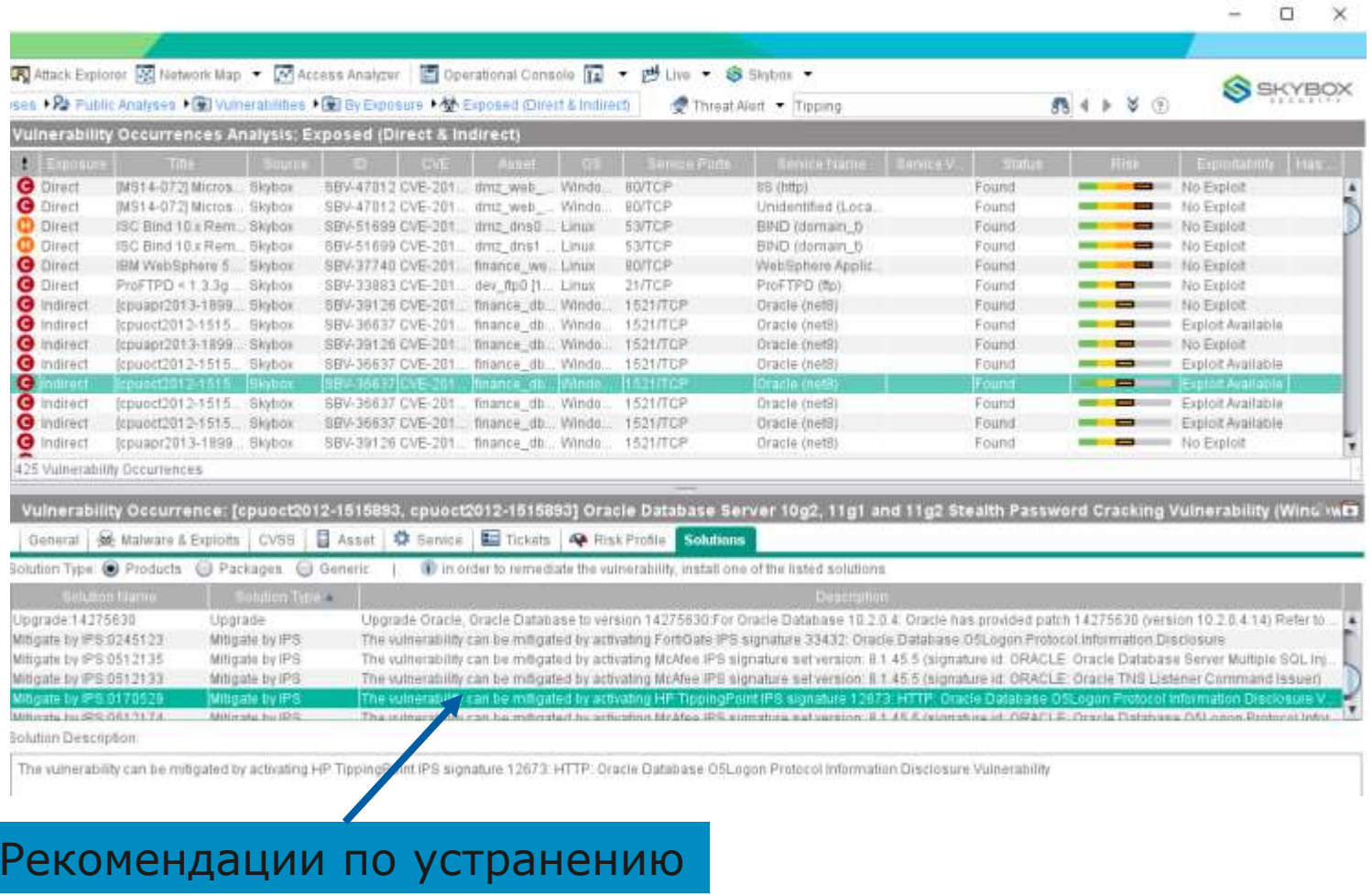
Расчет индикатора угроз

Учитываются:

- Достижимость (наличие доступа)
- Критичность
- Ценность актива
- Уровень злоумышленника
- Наличие готового эксплойта
- Статистика атак с использованием конкретной уязвимости

Результат:

- выделяем только действительно опасные уязвимости и максимальным уровнем риска



Важность приоритезации

Сократить до управляемого количества

ОПРЕДЕЛЕНИЕ ВСЕХ ИЗВЕСТНЫХ УЯЗВИМОСТЕЙ

ВСЕГО: 60K
Skybox Vulnerability Database

Потенциальная угроза

ОПРЕДЕЛЕНИЕ СУЩЕСТВУЮЩИХ УЯЗВИМОСТЕЙ

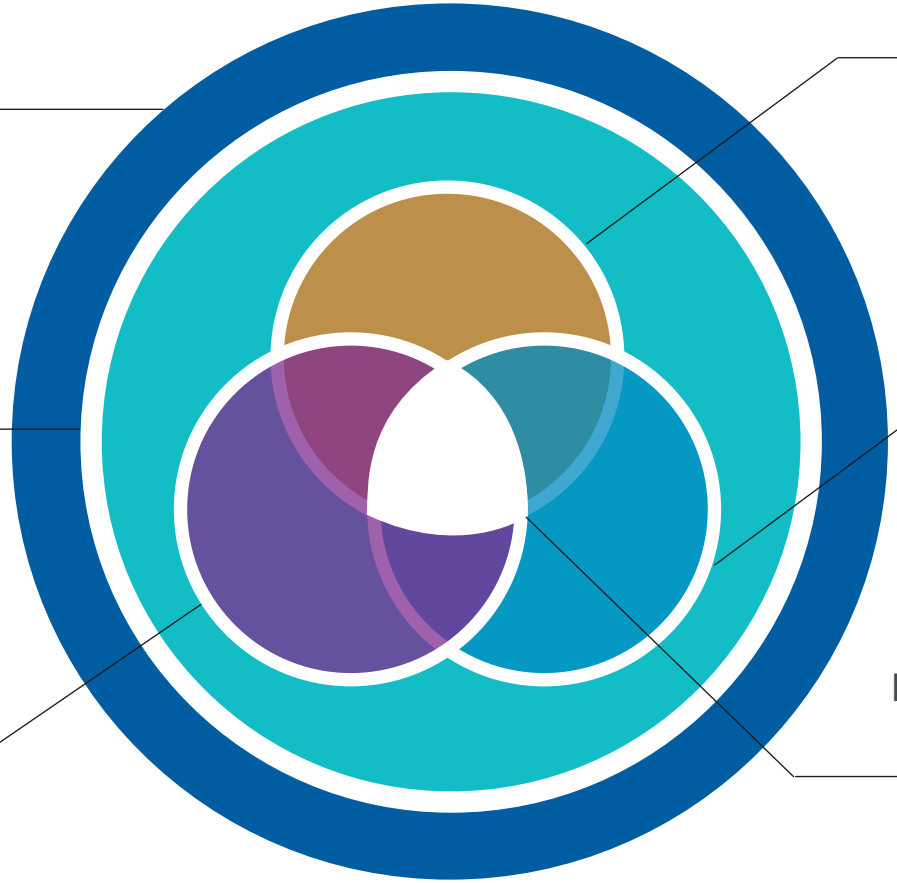
ВСЕГО НАЙДЕНО: 7122
Сканеры защищенности,
Skybox Vulnerability Detector

Потенциальная угроза

НАЛИЧИЕ ЭКСПЛОЙТОВ

ВСЕГО ОПРЕДЕЛЕНО: 1105
Skybox Research Lab real-time threat intelligence

Потенциальная угроза



КОРРЕЛЯЦИЯ С CVSS

ВСЕГО КРИТИЧНЫХ: 3578
CVSS scoring

Потенциальная угроза

ДОСТУПНЫЕ В СЕТИ УЯЗВИМОСТИ

ДОСТУПНО В СЕТИ: 141
Анализ векторов атак

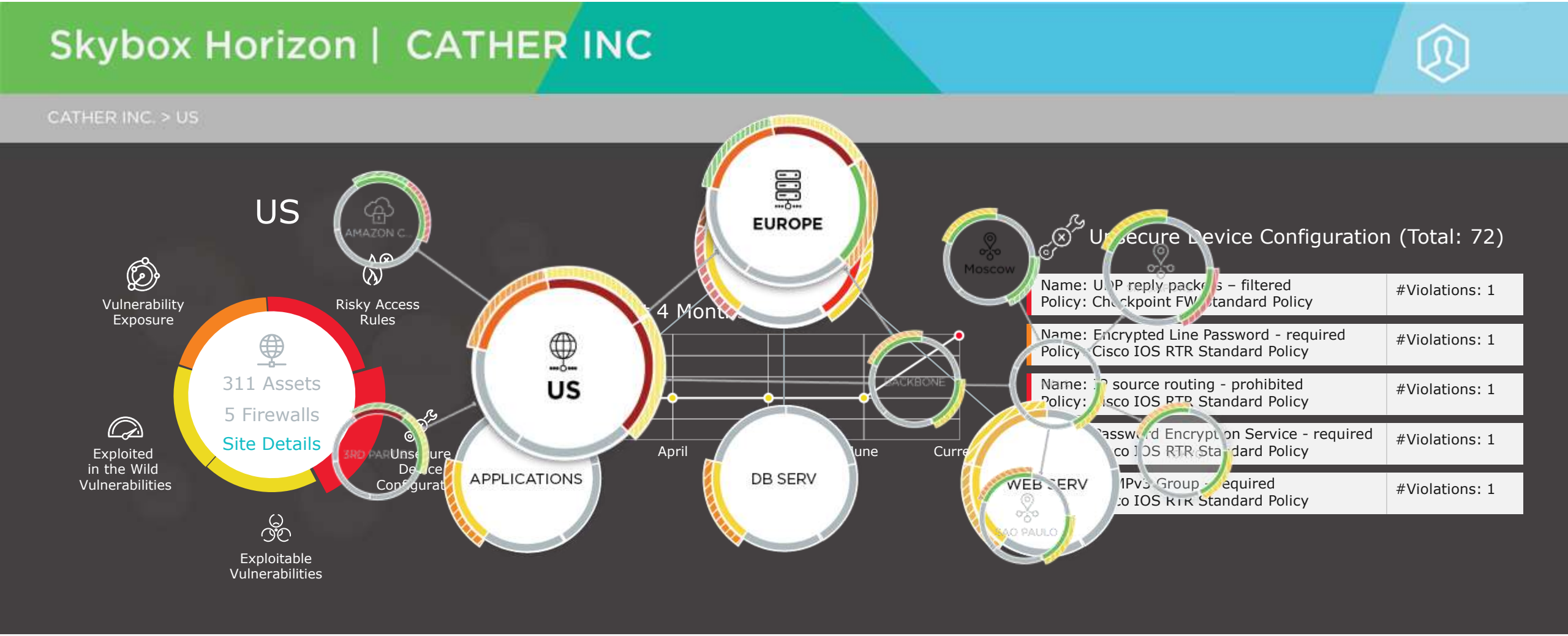
Вероятная угроза

ВЫДЕЛЕНИЕ УЯЗВИМОСТЕЙ С МАКСИМАЛЬНЫМ РИСКОМ

ВСЕГО: 13
Skybox Vulnerability
Control Prioritization Center

Вероятная угроза

Визуализация поверхности атаки

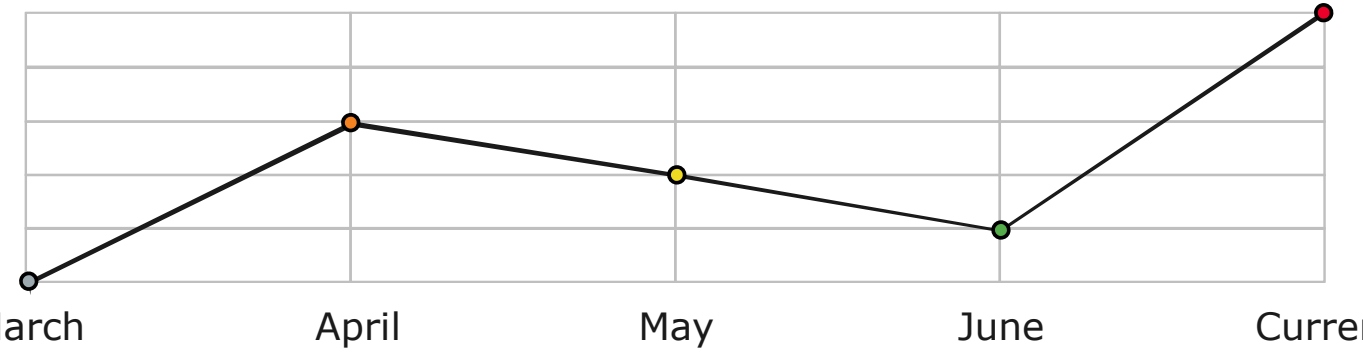


Индикаторы угроз

Unsecure Device Configuration (Total: 72)

Name: UDP reply packets – filtered Policy: Checkpoint FW Standard Policy	#Violations: 1
Name: Encrypted Line Password - required Policy: Cisco IOS RTR Standard Policy	#Violations: 1
Name: IP source routing - prohibited Policy: Cisco IOS RTR Standard Policy	#Violations: 1
Name: Password Encryption Service - required Policy: Cisco IOS RTR Standard Policy	#Violations: 1
Name: SNMPv3 Group - required Policy: Cisco IOS RTR Standard Policy	#Violations: 1

Last 4 Months



Чем полезен Skybox

Контроль сегментирования и зон безопасности

Анализ векторов атак

Автоматизация процесса изменений правил доступа

Выявление уязвимостей в период до и между сканированиями

Контроль корректности конфигураций

Приоритезация уязвимостей и формирование рекомендаций по их устранению

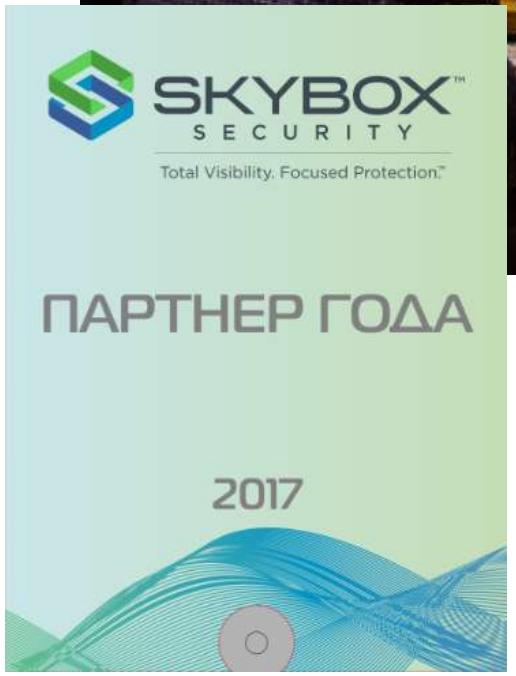
Оптимизация правил доступа

Автоматизация управления уязвимостями (от обнаружения до контроля устранения)

Сетевая безопасность

Управление уязвимостями

Вместо заключения



Управлять – значит предвидеть

Sales.Russia@skyboxsecurity.com

+7 800 511 08 28

JETSECURITY
CONFERENCE 2018

Спасибо за внимание!

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ