

A series of parallel diagonal lines in a light blue color, located in the top left corner of the slide.

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?



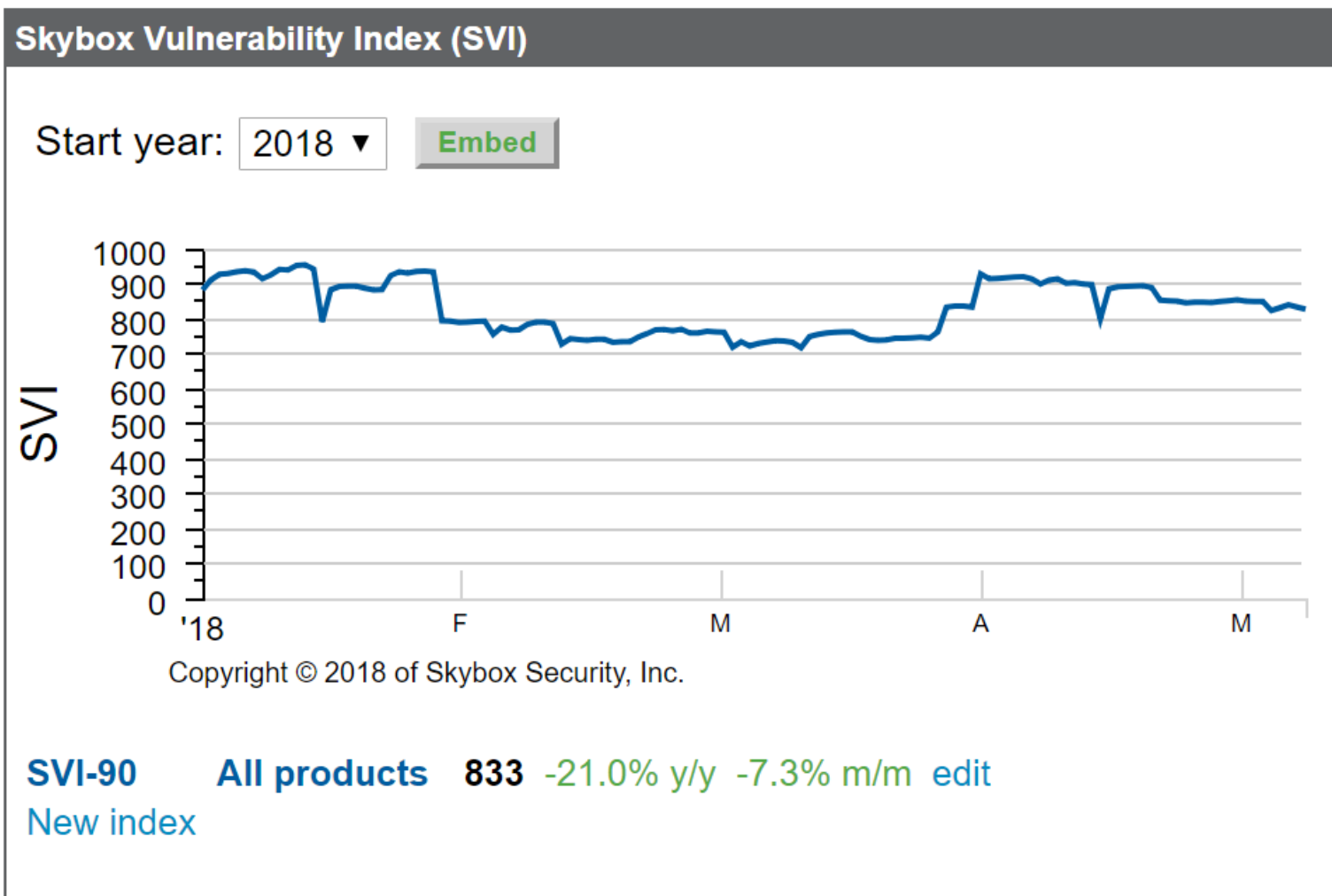
- Как Вы узнаете о новых уязвимостях в период между сканированиями?
- Что делать, если нет возможности сканирования?



- 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**

Сценарии использования Skybox Security



Network Assurance



Полная видимость сети

Интерактивная карта сети

Автоматическая проверка
соответствия стандартам
конфигурирования

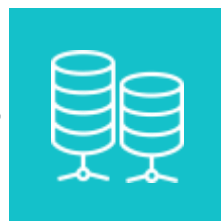
Автоматическая проверка
соответствия политикам
сегментирования

Как Это Работает



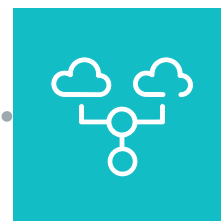
1

Сбор и нормализация



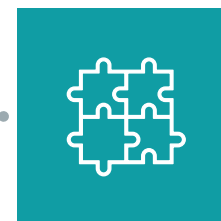
2

Моделирование



3

Детальный анализ



Проверка доступа на лету

Analysis Results

Show: Accessible Destinations | Group By: Network | Authentication: N...

- developmentWindowsWS [192.170.17.0 / 24] [256 IPs; 1 TCP port]
- developmentUnixWS [192.170.18.0 / 24] [256 IPs; 1 TCP port]
 - 192.170.18.0-192.170.18.255 [256 IPs; 1 TCP port]
- 21 (TCP)
- developmentServers [192.170.19.0 / 24] [256 IPs; 1 TCP port]
- dmz [192.170.33.0 / 24] [256 IPs; 6 TCP/UDP ports]

Routes | **View**

1 << < 1 > >> 1

☐ Show Routing Rules

Access Route
From Internet (cloud) To developmentUnixWS (192.170.18.0/24)

#	Step	Info	Access Rule
1.	Source: Internet (cloud) Source IP range(s): 16.0.0.0-16.0.0.0, 16.0.0.2-16.255.255.255 Sending To IP range(s): 192.170.18.0-192.170.18.255 Sending to service(s): 21/TCP		
2.	main_FW (16.0.0.1)		
3.	Main Router (192.169.1.2)		
4.	Internal Router (192.170.8.2)		
5.	dev FW (192.170.1.1)		

Current Map

Organizati... | Show Route Map

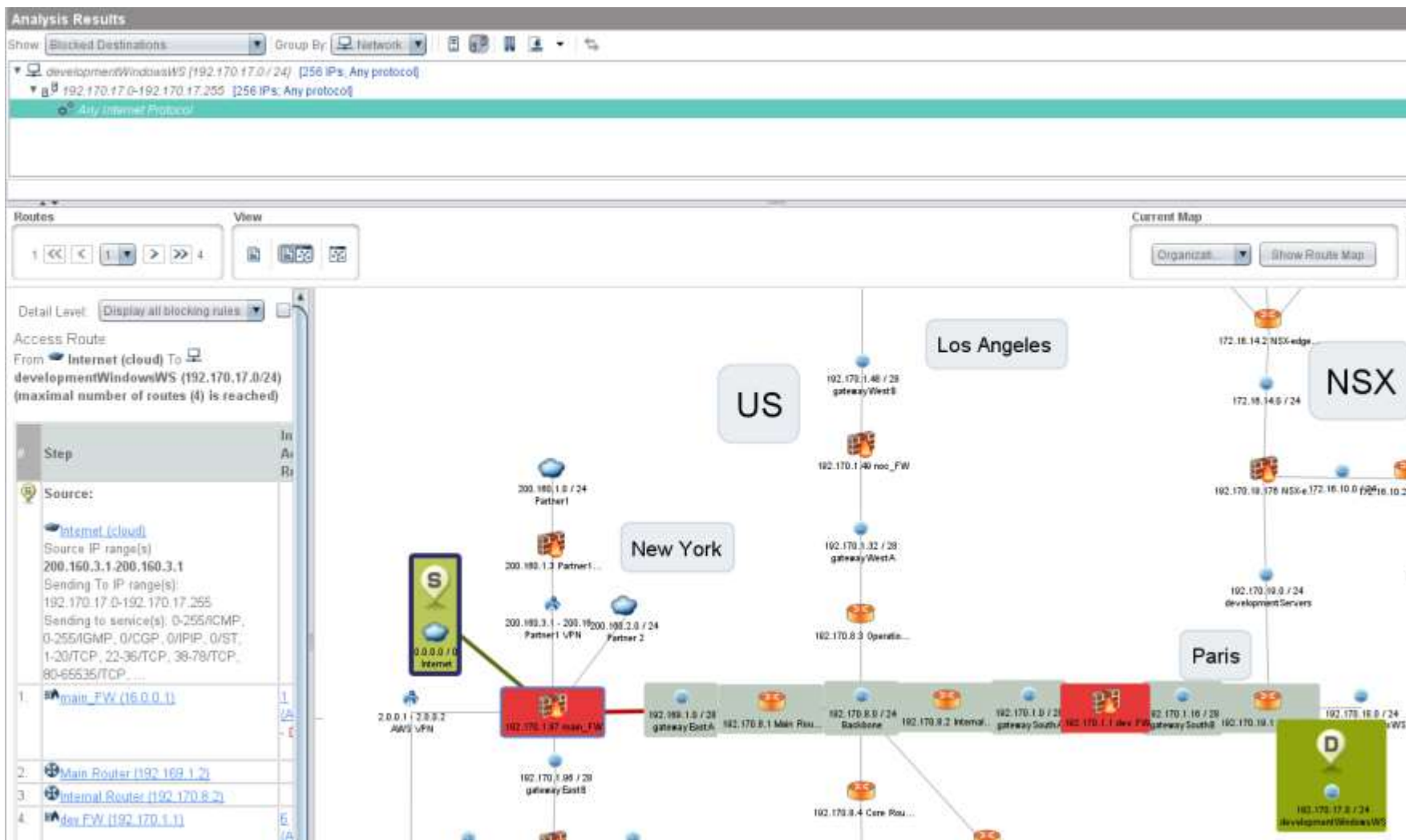
The diagram illustrates a global network topology with four main regions: US, New York, Los Angeles, and Paris. Key components include:

- US:** Internet cloud, Partner1, Partner2, and various gateways.
- New York:** Partner1, Partner2, and a VPN connection.
- Los Angeles:** gatewayWestB, noc_FW, and gatewayWestA.
- Paris:** NSX edge routers, development Servers, and development Unix/Windows WS.

A green path highlights the route from the Internet cloud through the main FW, Main Router, Internal Router, and dev FW to reach developmentUnixWS.

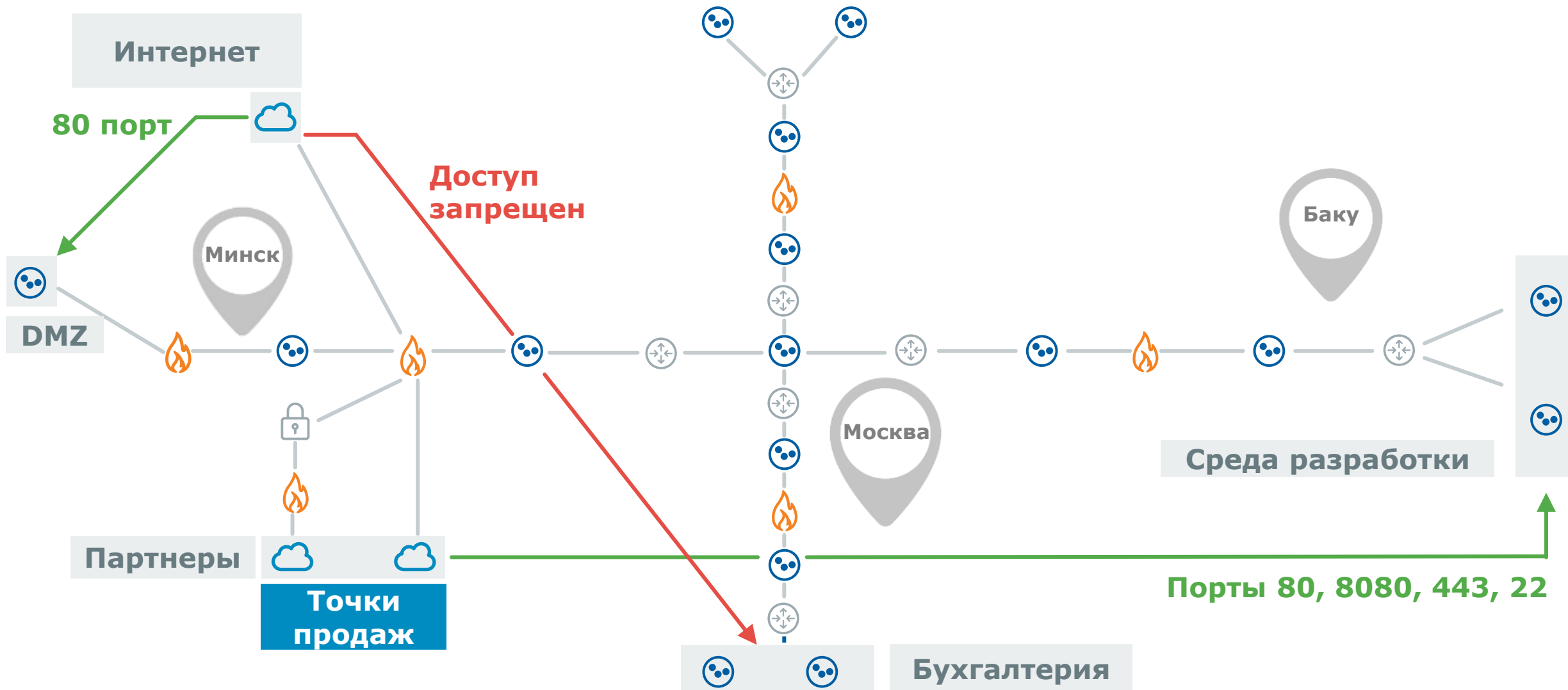
Проверяем
наличие доступа
в 2 клика

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

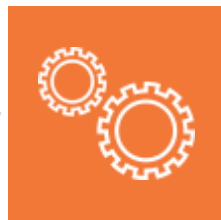
Управление жизненным
циклом правил доступа

Как Это Работает



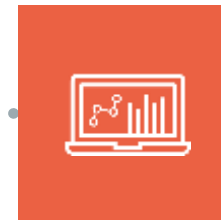
1

Сбор и нормализация



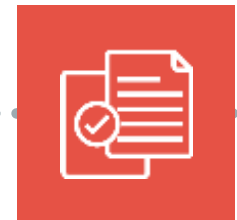
2

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

Change Name	Changed Profile	Description	Status
New Rule (ID: 683) Time: Jan 2, 2018, 1:00:51 AM By: Bob Smith	PA-2020-vyprl Rule #16 (Normal Policy)	Rule #16 added to access list	Pending Last Reviewer: Mike.York
Modified Rule (ID: 680) Time: Dec 29, 2017, 7:21:30 PM By: Jesse Velez	PA-2020-vyprl Rule #5 (Access Policy)	rule changed for action	Unauthorized Last Reviewer: Automatic
New Object (ID: 678) Time: Dec 26, 2017, 12:00:54 AM By: Jesse Velez	PA-2020-vyprl Object address-connect	Object address-connect added to access list	Unauthorized Last Reviewer: Automatic
New Object (ID: 679) Time: Dec 26, 2017, 1:10:08 PM By: Mike.York	PA-2020-vyprl Object address-mapping	Object address-mapping added to access list	Unauthorized Last Reviewer: Automatic
New Object (ID: 677) Time: Dec 26, 2017, 1:10:08 PM By: Mike.York	PA-2020-vyprl Object address-mapping	Object address-mapping added to access list	Unauthorized Last Reviewer: Automatic

New Rule (ID: 683) Time: Jan 2, 2018, 1:00:51 AM By: Bob Smith	Pending Last Reviewer: Mike.York
Modified Rule (ID: 680) Time: Dec 29, 2017, 7:21:30 PM By: Jesse Velez	Unauthorized Last Reviewer: Automatic

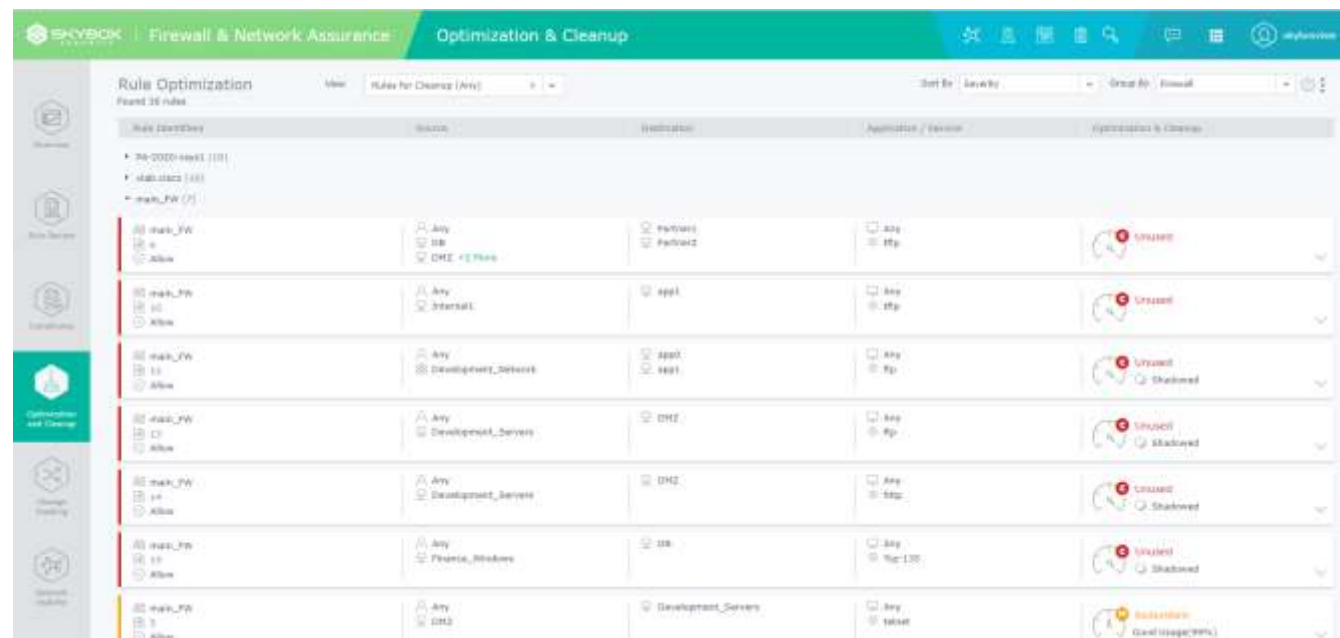
Оптимизация загрузки МЭ

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



1

Запрос



2

Идентификация



3

Оценка



4

Применение



5

Верификация

Применение изменений

Implement Changes ✕

☒	ID	Chang...	Firewall	Object...	Change Details	Implementation Det...	Object / Rule Comment
☒	524	New ...	dev FW	Service...	Service Object: 8080/TCP		5/11/18 - Created by skybox...
☒	523	New ...	dev FW	Service...	Service Object: 23/TCP		5/11/18 - Created by skybox...
☒	522	New ...	dev FW	Host_...	Address Object: 192.170.19.21		5/11/18 - Created by skybox...
☒	521	New ...	dev FW	Host_...	Address Object: 200.200.200.200		5/11/18 - Created by skybox...
☒	517	Add R...	dev FW	-	Source: Host_200.200.200.200 ★ Destination: Host_192.170.19.21 ★ Services: Service_23_TCP ★, Service_8080...	Policy: Standard Rule Position: Last Rule Track: Log	5/11/18 - Created by skybox...

5 Requests (5 selected)

Implement Changes

Close

- 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



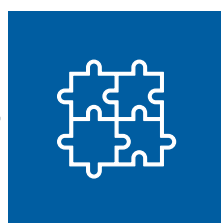
1

Выявление



2

Анализ



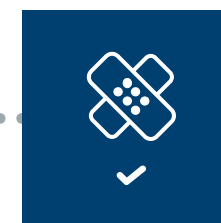
3

Приоритезация

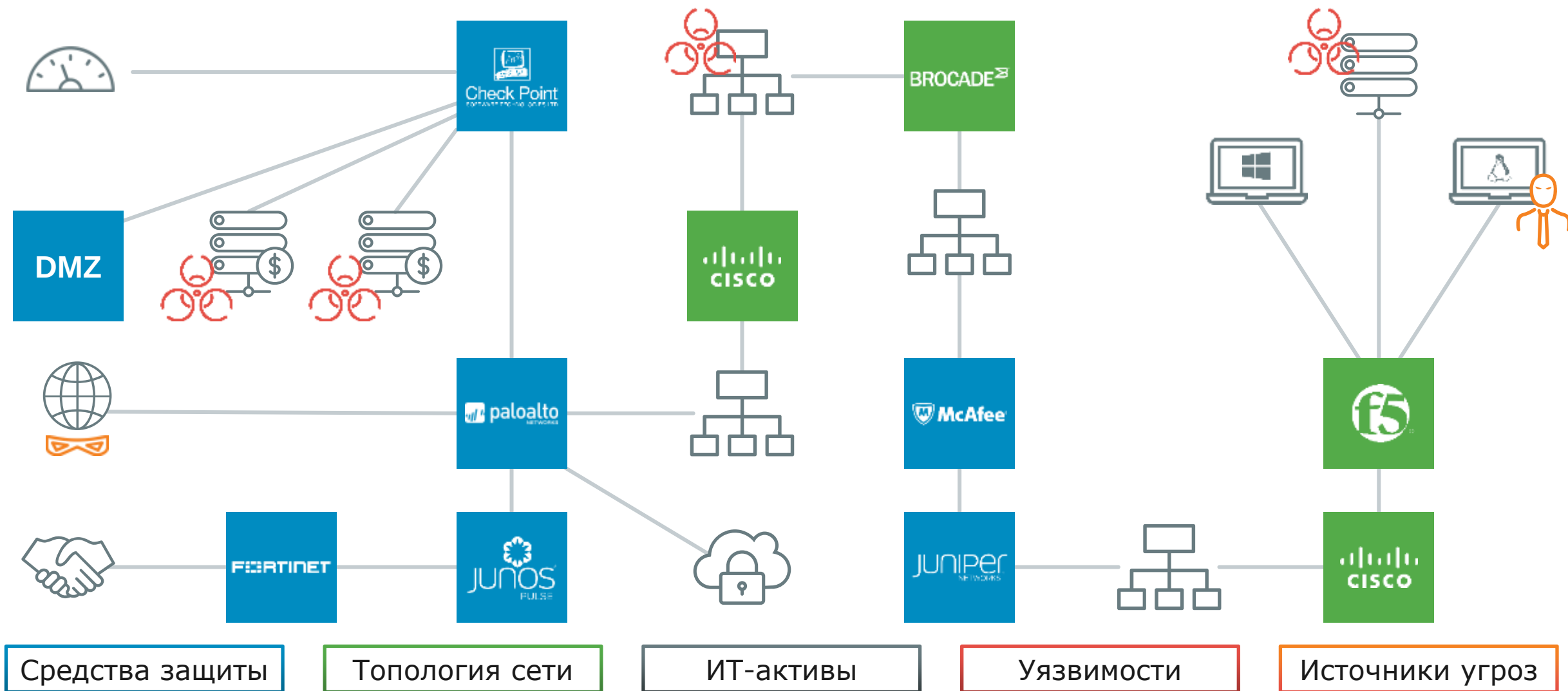


4

Реагирование



Моделирование вектора атаки

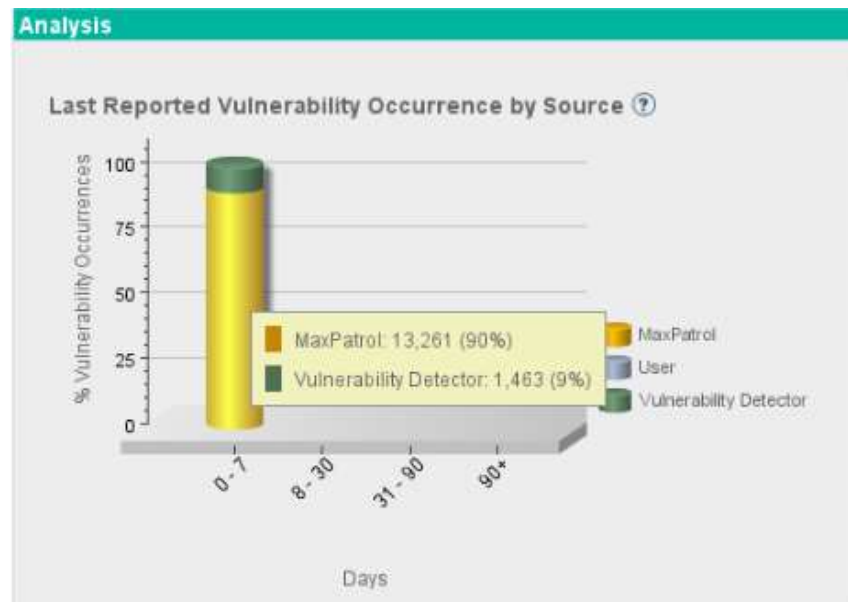


Выявление уязвимостей

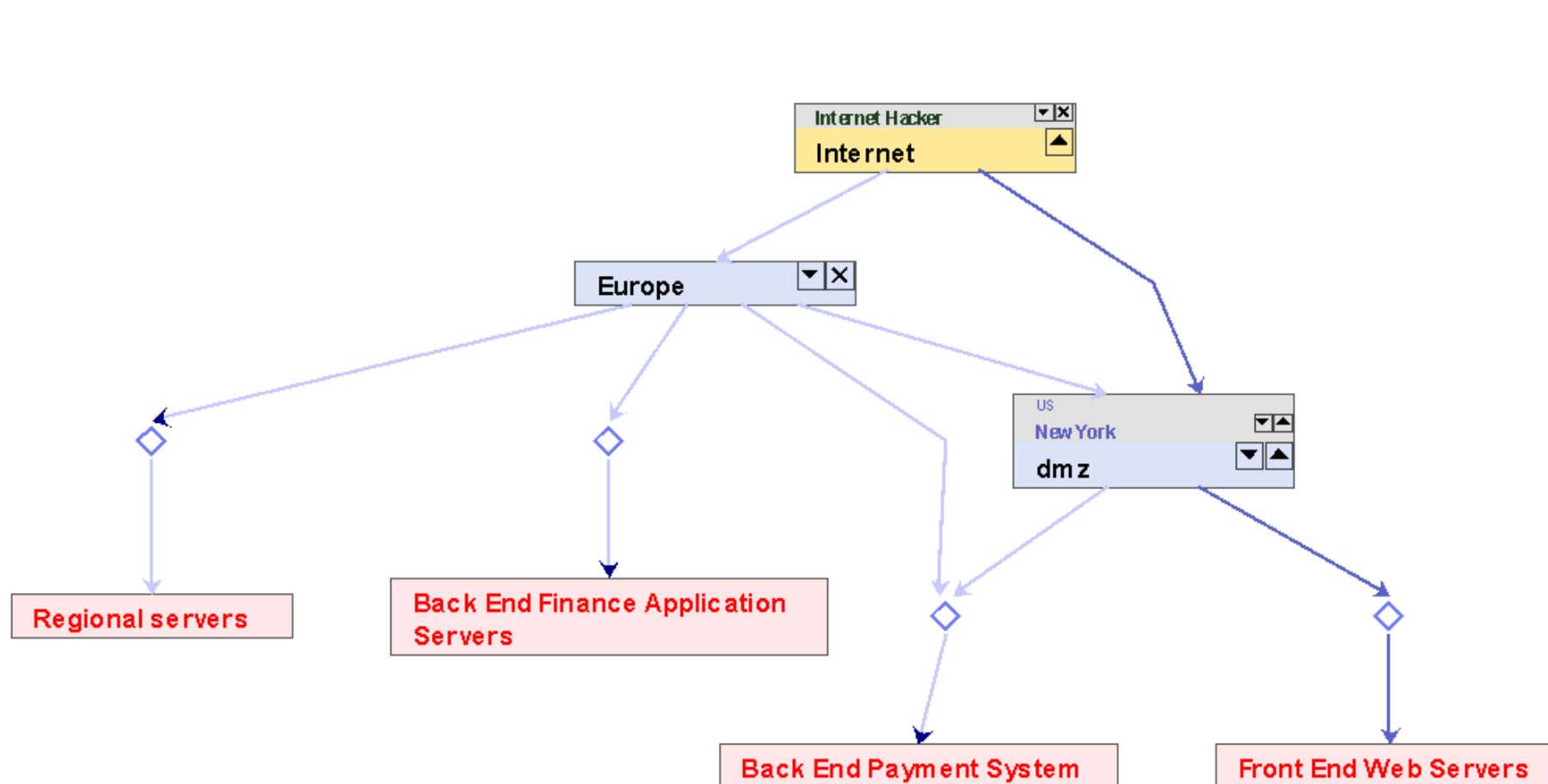
- Загрузка отчетов сканеров
- Загрузка отчетов систем инвентаризации SCCM, WSUS и др.
- Ежедневное обновление собственной базы уязвимостей
- Ежедневное «пассивное» сканирование

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

The screenshot displays the Skybox Security interface, specifically the 'Vulnerability Occurrences Analysis: Exposed (Direct & Indirect)' section. The table lists various vulnerabilities, including CVE-2012-1515 and CVE-2012-1516, with their associated assets, services, and risk levels. A blue arrow points to the 'Mitigate by IPS' solution for CVE-2012-1515.

Exposure	Title	Source	ID	CVE	Asset	OS	Service Ports	Service Name	Service V.	Status	Risk	Exploitability	Has
Direct	[MS14-072] Micros...	Skybox	SBV-47012	CVE-201...	dmz_web...	Windo...	80/TCP	SS (http)		Found	Low	No Exploit	
Direct	[MS14-072] Micros...	Skybox	SBV-47012	CVE-201...	dmz_web...	Windo...	80/TCP	Unidentified (Loca...		Found	Low	No Exploit	
Direct	ISC Bind 10.x Rem...	Skybox	SBV-51699	CVE-201...	dmz_dns0...	Linux	53/TCP	BIND (domain_b...		Found	Low	No Exploit	
Direct	ISC Bind 10.x Rem...	Skybox	SBV-51699	CVE-201...	dmz_dns1...	Linux	53/TCP	BIND (domain_b...		Found	Low	No Exploit	
Direct	IBM WebSphere 5...	Skybox	SBV-37740	CVE-201...	finance_we...	Linux	80/TCP	WebSphere Applic...		Found	Low	No Exploit	
Direct	ProFTPD < 1.3.3g	Skybox	SBV-33883	CVE-201...	dev_ftpd [1...	Linux	21/TCP	ProFTPD (ftp)		Found	Low	No Exploit	
Indirect	[cpuact2013-1899...	Skybox	SBV-39126	CVE-201...	finance_db...	Windo...	1521/TCP	Oracle (net8)		Found	Low	No Exploit	
Indirect	[cpuact2013-1515...	Skybox	SBV-36637	CVE-201...	finance_db...	Windo...	1521/TCP	Oracle (net8)		Found	Low	Exploit Available	
Indirect	[cpuact2013-1899...	Skybox	SBV-39126	CVE-201...	finance_db...	Windo...	1521/TCP	Oracle (net8)		Found	Low	No Exploit	
Indirect	[cpuact2012-1515...	Skybox	SBV-36637	CVE-201...	finance_db...	Windo...	1521/TCP	Oracle (net8)		Found	Low	Exploit Available	
Indirect	[cpuact2012-1515...	Skybox	SBV-36637	CVE-201...	finance_db...	Windo...	1521/TCP	Oracle (net8)		Found	Low	Exploit Available	
Indirect	[cpuact2012-1515...	Skybox	SBV-36637	CVE-201...	finance_db...	Windo...	1521/TCP	Oracle (net8)		Found	Low	Exploit Available	
Indirect	[cpuact2012-1515...	Skybox	SBV-36637	CVE-201...	finance_db...	Windo...	1521/TCP	Oracle (net8)		Found	Low	Exploit Available	
Indirect	[cpuact2012-1515...	Skybox	SBV-36637	CVE-201...	finance_db...	Windo...	1521/TCP	Oracle (net8)		Found	Low	Exploit Available	
Indirect	[cpuact2013-1899...	Skybox	SBV-39126	CVE-201...	finance_db...	Windo...	1521/TCP	Oracle (net8)		Found	Low	No Exploit	

425 Vulnerability Occurrences

Vulnerability Occurrence: [cpuact2012-1515893, cpuact2012-1515893] Oracle Database Server 10g2, 11g1 and 11g2 Stealth Password Cracking Vulnerability (Windo...

Solution Type: Products Packages Generic | In order to remediate the vulnerability, install one of the listed solutions

Solution Name	Solution Type	Description
Upgrade 14275630	Upgrade	Upgrade Oracle, Oracle Database to version 14275630 For Oracle Database 10.2.0.4: Oracle has provided patch 14275630 (version 10.2.0.4.14) Refer to...
Mitigate by IPS 0245123	Mitigate by IPS	The vulnerability can be mitigated by activating FortiGate IPS signature 33432: Oracle Database OSLogon Protocol Information Disclosure
Mitigate by IPS 0512135	Mitigate by IPS	The vulnerability can be mitigated by activating McAfee IPS signature set version: 8.1.45.5 (signature id: ORACLE: Oracle Database Server Multiple SQL Ins...
Mitigate by IPS 0512133	Mitigate by IPS	The vulnerability can be mitigated by activating McAfee IPS signature set version: 8.1.45.5 (signature id: ORACLE: Oracle TNS Listener Command Issuer)
Mitigate by IPS 0170529	Mitigate by IPS	The vulnerability can be mitigated by activating HP TippingPoint IPS signature 12673: HTTP: Oracle Database OSLogon Protocol Information Disclosure V...
Mitigate by IPS 0613174	Mitigate by IPS	The vulnerability can be mitigated by activating McAfee IPS signature set version: 8.1.45.5 (signature id: ORACLE: Oracle Database OSLogon Protocol Infor...

Solution Description:

The vulnerability can be mitigated by activating HP TippingPoint IPS signature 12673: HTTP: Oracle Database OSLogon Protocol Information Disclosure Vulnerability

Рекомендации по устранению

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

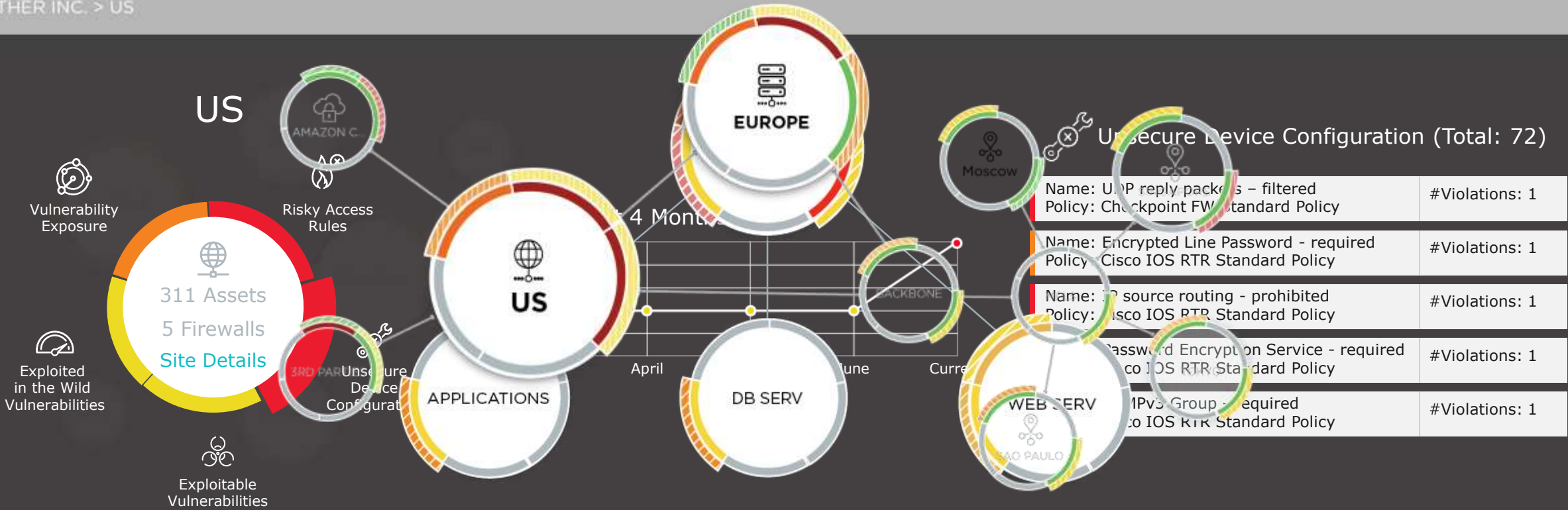


Визуализация поверхности атаки

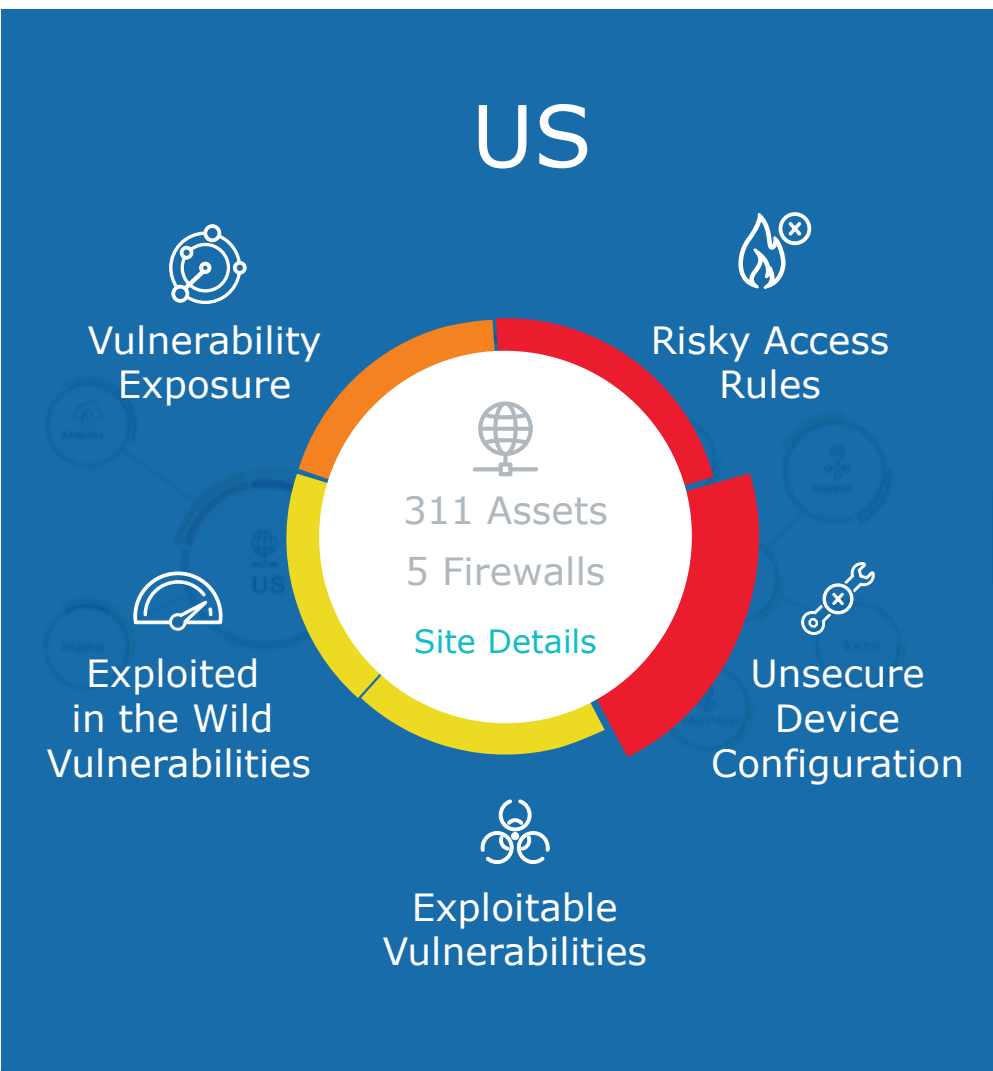
Skybox Horizon | CATHER INC



CATHER INC. > US



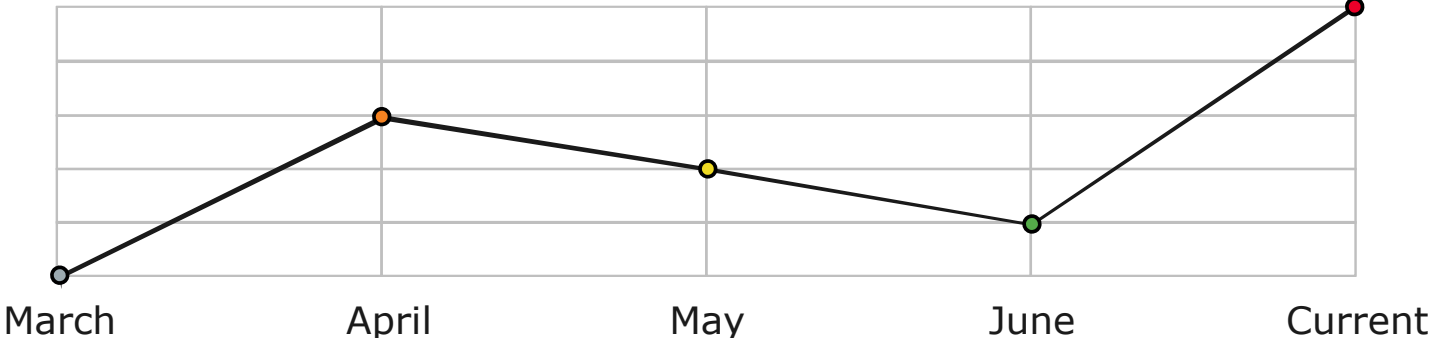
Индикаторы угроз



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

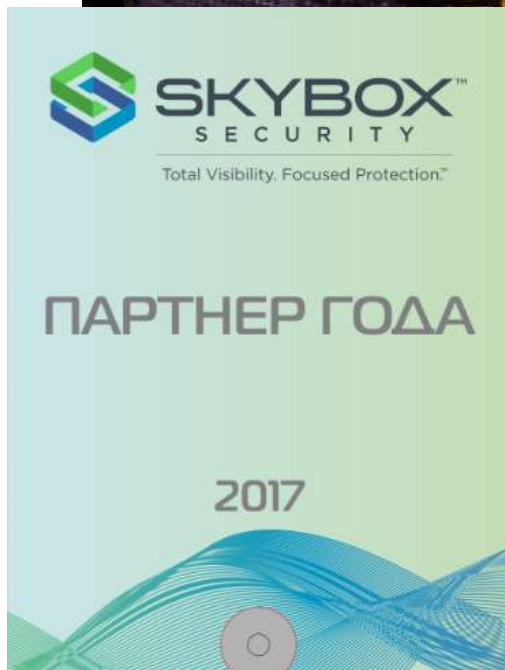
Оптимизация правил доступа

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



//////

Спасибо за внимание!

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ

//////