

JET CONFERENCE

01/06/2017

Современный подход к управлению уязвимостями

Юрий Черкас

Вопросы и ответы

Какие уязвимости я должен устранять в первую очередь?

Те, для которых есть готовые эксплойты и те, которые активно используются атакующими.

Зачем менять подход?

“The top **10 vulnerabilities account for 85% of successful exploit traffic...** the other **15% consists of over 900 CVEs**, which are also being exploited in the wild.”

– *Data Breach Investigations Report*, Verizon, 2016

“Vulnerabilities and their exploitation are still the root cause of most breaches. IT security leaders should refocus their attention on how vulnerabilities are being managed and should track this metric to provide visibility as to how to reduce the biggest risks of being breached.”

– *It's Time to Align Your Vulnerability Management Priorities With the Biggest Threats*, Gartner, September 2016

Платформа Skybox Security

1. Интеграция со 100+ сетевыми устройствами
2. Построение полной карты сети с учетом настроек безопасности
3. Автоматизация процесса внесения изменений в настройки сети
4. Выявление и приоритезация уязвимостей с учетом сетевого контекста
5. Инструмент анализа и реагирования на угрозы



Управление политиками безопасности



Моделирование сети

- › Сетевая топология
- › Данные от 90+ вендоров
- › Моделирование доступов

Понимание контекста сети



Анализ МЭ

- › Проверка правил и конфигураций
- › Анализ доступов
- › Оптимизация правил
- › Отслеживание изменений

Повышение эффективности



Соответствие политикам

- › Автоматизированные аудиты
- › PCI DSS
- › NIST
- › Собственные политики

Соответствие стандартам



Управление жизненным циклом правил

- › Запросы на изменения
- › Техническая детализация
- › Оценка рисков
- › Изменения
- › Проверка и аттестация правил

Непрерывная проверка базы правил

Управления уязвимостями и угрозами



Идентификация уязвимостей

- Пассивное сканирование
- Интеграция со сканерами
- Словари уязвимостей

Оперативная идентификация



Анализ атак

- Анализ уязвимых мест
- Эмуляция атак
- Компенсирующие меры
- В контексте сети
- Влияние на бизнес

Выделение уязвимых мест



Расстановка приоритетов

- Оценка реальных последствий
- Настраиваемые индикаторы
- Вектора атак
- Реальная карта атак

Фокус на реальные проблемы



Контроль исправлений

- Планирование изменений
- Заявки и процессы
- Графики и отчеты

Оперативная реакция

(Не)конкурентная среда

Играют на одном поле, но в разные игры:



Hewlett Packard
Enterprise

POSITIVE TECHNOLOGIES



Моделирование
сети

Анализ МЭ

Управление
изменениями

Управление
уязвимостями

Реагирование
на угрозы



NETWORK
ASSURANCE



FIREWALL
ASSURANCE



CHANGE
MANAGER



VULNERABILITY
CONTROL



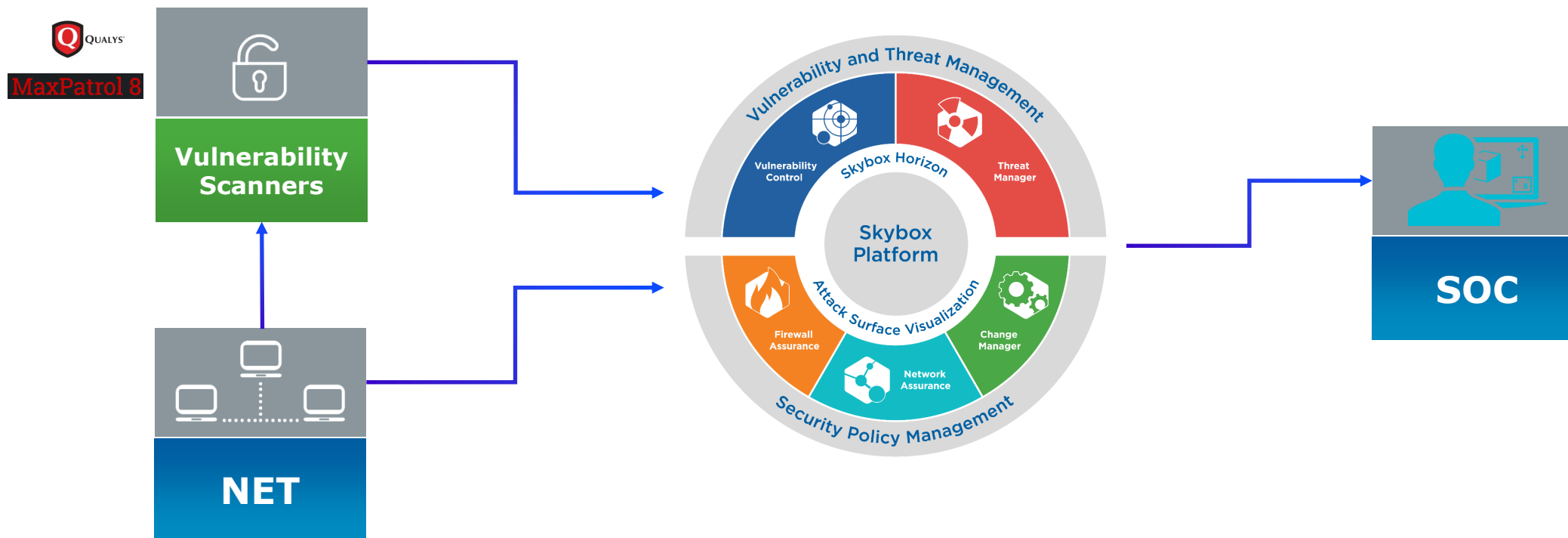
HORIZON



THREAT
MANAGER



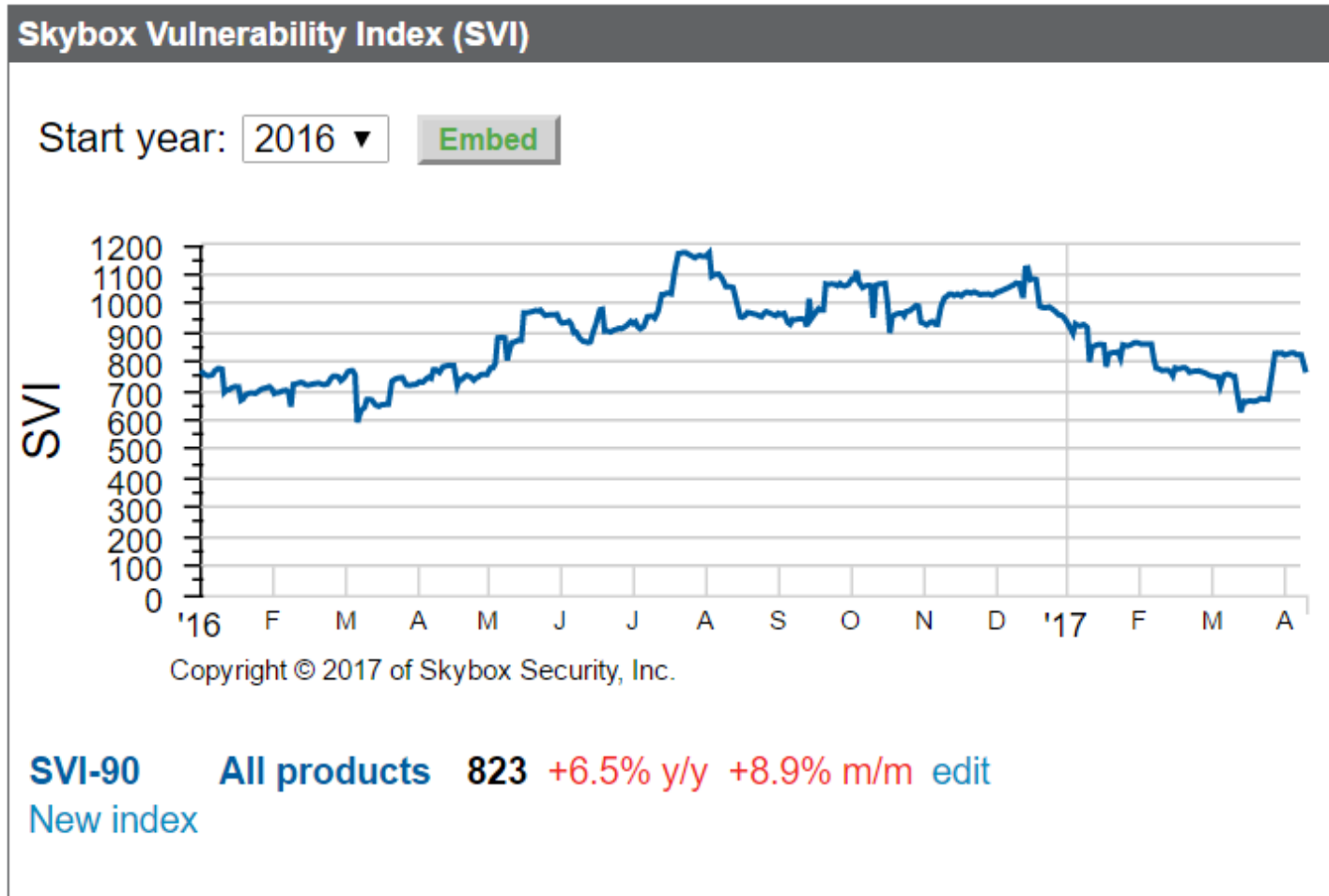
Место Skybox Security в инфраструктуре ИБ



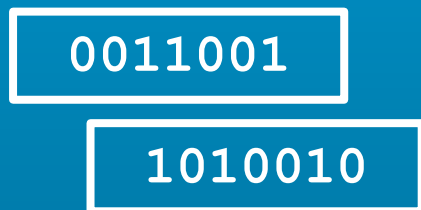
Количество новых уязвимостей

600-1200 новых
уязвимостей

КАЖДЫЙ
МЕСЯЦ



Подход к Vulnerability Management



0011001
1010010

Какие
уязвимости
актуальны для
моей сети?



Какие
критичные
активы
доступны в
моей сети?



Какие
эксплойты есть
в общем
доступе?



Какие эксплойты
наиболее часто
используются при
проведении атак?

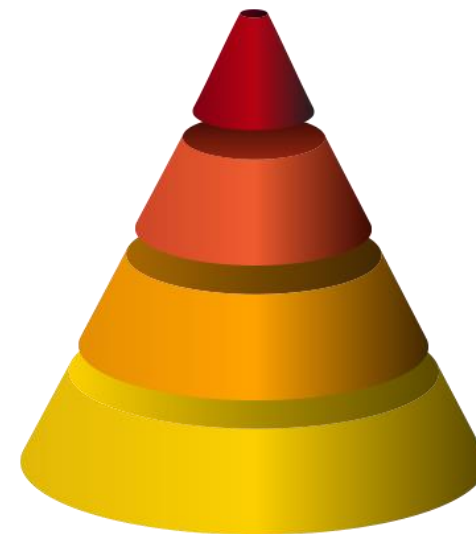
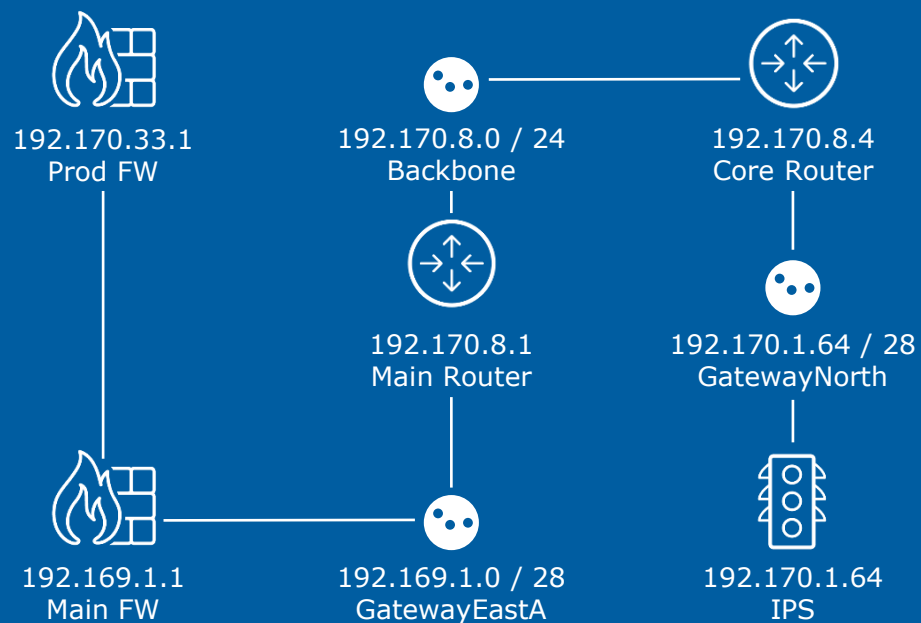
Устранить доступные в сети уязвимости, которые были причиной взлома (**exposed + exploited**)

Управление уязвимостями с ориентацией на угрозы

АНАЛИТИКА

ПРИОРИТЕЗАЦИЯ

Моделирование сети и векторов атак



**ДАННЫЕ ОБ
УЯЗВИМОСТЯХ**

Ингредиенты эффективной приоритезации



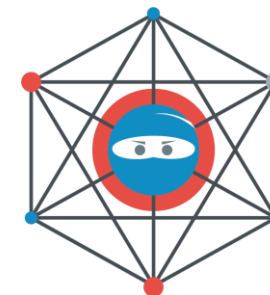
Ориентир на уязвимости

Критичность уязвимости (CVSS рейтинг, последствия эксплуатации, доступность эксплойтов)



Ориентир на контекст

Критичность, значимость и доступность уязвимых активов (доступность из Интернет, доступ партнеров, конфиденциальные данные и т.д.)



Ориентир на угрозы

Использование уязвимостей различным malware, ransomware, exploit kits в мире

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 **Вероятная угроза**
Skybox Research Lab real-time threat intelligence



КОРРЕЛЯЦИЯ С CVSS

ВСЕГО КРИТИЧНЫХ: 3578
CVSS scoring

Потенциальная/вероятная угроза

ДОСТУПНЫЕ В СЕТИ УЯЗВИМОСТИ

ДОСТУПНО В СЕТИ: 141
Skybox network modeling and attack vector analytics

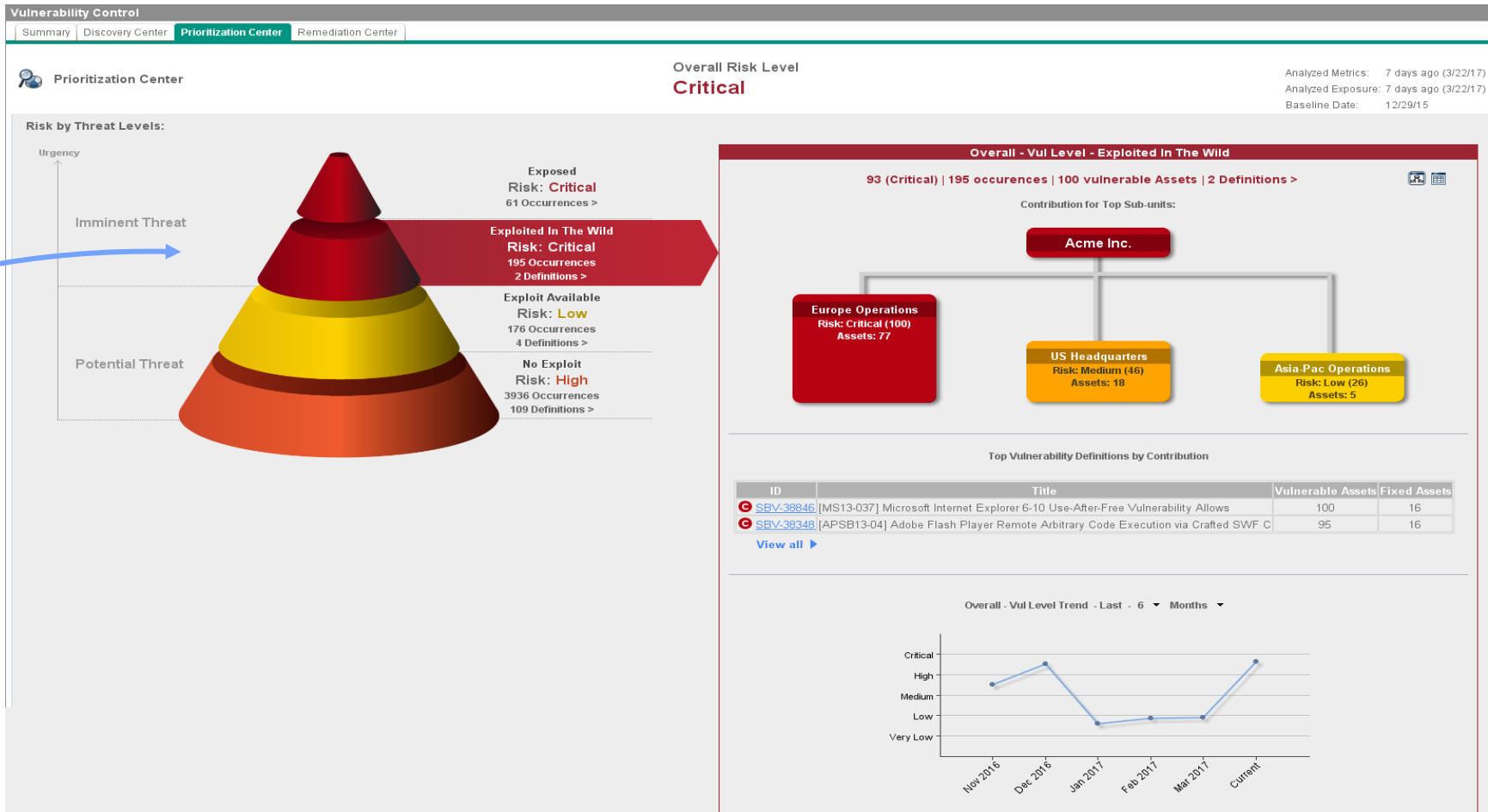
Вероятная угроза

ВЫДЕЛЕНИЕ УЯЗВИМОСТЕЙ С МАКСИМАЛЬНЫМ РИСКОМ

Вероятная угроза ВСЕГО: 13
Skybox Vulnerability Control Prioritization Center

Новый Vulnerability Prioritization Center

**HIGH
PRIORITY**



Exploitability Index

- Доступен в описании найденных уязвимостей
- Значения
 - Эксплойтов не найдено (No exploit)
 - Существуют готовые эксплойты (Potential exploit)
 - Активно эксплуатируется (Exploited in the wild)

EXPLOITABILITY

Vulnerability Definition: [MS13-037] Microsoft Internet Explorer 6-10 Use-After-Free Vulnerability Allows Remote Code Execution (CVE-2013-2551)

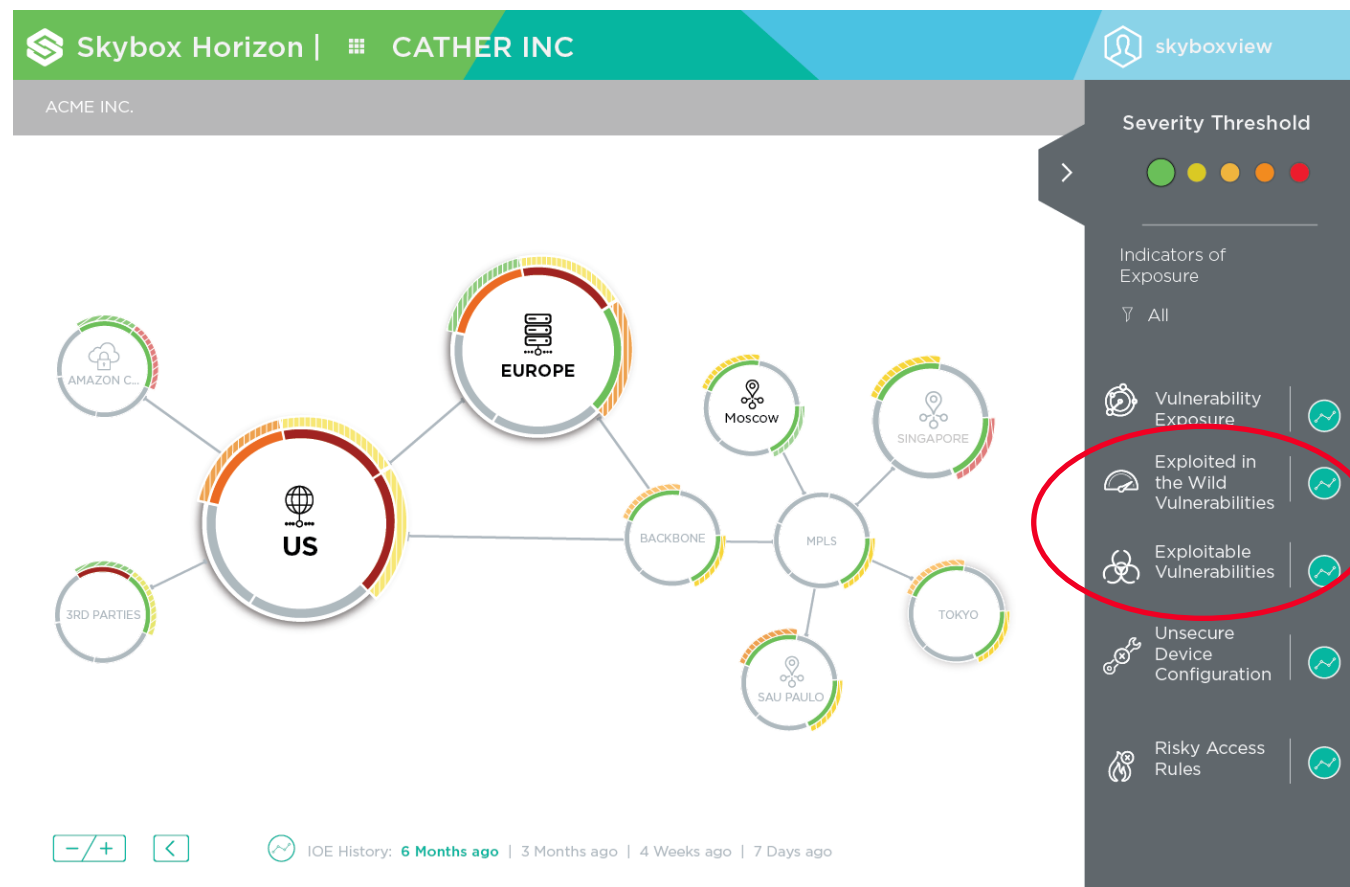
General CVSS Vulnerability Occurrences Malware & Exploits Related Sources Solutions External URLs Affected Platforms Tickets History Vulnerable Assets

Title:	[MS13-037] Microsoft Internet Explorer 6-10 Use-After-Free Vulnerability Allows Remote Code Execution (CVE-2013-2551)		ID:	Skybox	SBV-38846
Type:	Vulnerability Definition		CVE:	CVE-2013-2551	
Severity:	Critical (9.3)		Exploitability:	Exploited In The Wild	
Catalog:	Microsoft	Catalog ID:	MS13-037	BID:	BID-59785
Reported Date:	3/2/13		Modification Date:	10/6/16	
For Review:	No				
Vulnerability Occurrences:	100		Asset Count:	104	
Description:	Use-after-free vulnerability in Microsoft Internet Explorer 6 through 10 allows remote attackers to execute arbitrary code via a crafted web site that triggers access to a deleted object, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2013, aka "Internet Explorer Use After Free Vulnerability," a different vulnerability than CVE-2013-1308 and CVE-2013-1309.				
User Comments:					



Skybox Horizon

- Визуализация состояния безопасности на бизнес уровне
- Отслеживание динамики состояния защищенности
- Просмотр наиболее критичных мест
- **Теперь с ориентацией на реальные угрозы**



Threat Centric Vulnerability Management

- Применяйте современный подход к управлению уязвимостями:
- защищайте активы, которые:
 - доступны потенциальному злоумышленнику в сети
 - уязвимы для существующих эксплойтов
- Устраняйте уязвимости, которые активно используются вредоносным ПО, exploit kits и атакующими по всему миру

Что дает Skybox Security



- Прозрачность и реальный контроль над безопасностью сети



- Сокращение затрат на эксплуатацию сети и средств сетевой безопасности, оптимизация сети и безопасности



- Эффективный механизм для работы с уязвимостями в составе конкретной ИТ-инфраструктуры и с учетом ее особенностей

Click to edit Master title style



JET CONFERENCE

01/06/2017

ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!

JET CONFERENCE