КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

19 АПРЕЛЯ 2018
МИНСК

КАК МОЩНО УСИЛИТЬ ВАШУ ОБОРОНОСПОСОБНОСТЬ ОДНИМ ДВИЖЕНИЕМ? ПРЕМЬЕРА РЕШЕНИЯ ISEE

СЕРГЕЙ ГОРБАЧЕВ

Менеджер по развитию IBA Security,
IBA GROUP

ТЕЛЕФОН: +375 (33) 618-39-57

EMAIL: SIARHEI.HARBACHOU@IBA.BY

IBA SECURITY

#CODEIB

IBAGROUPIT.COM • IBA.BY

IBA GROUP

ENVISIONING THE FUTURE

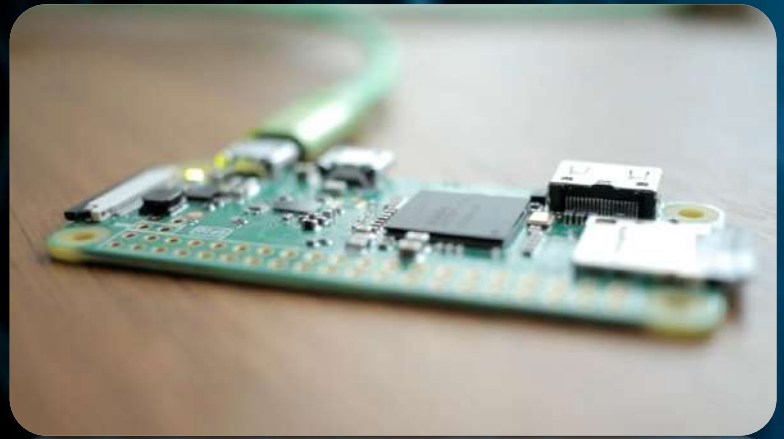
IBA SECURITY

Решение iSEE

Доступность оборудования

IBA SECURITY

IOT для хакинга
Мощности уже достаточно
Цена от 5$ за контроллер



Wi-Fi адаптеры с режимом прослушивания эфира

Цена От 10$
Доступны на Amazon
Продаются с рук

Любой компьютер, ноутбук,
Виртуальная машина
Достаточно мощности:
1 ГГц/RAM 500 МБ

Возможности

IBA SECURITY

Kali Linux

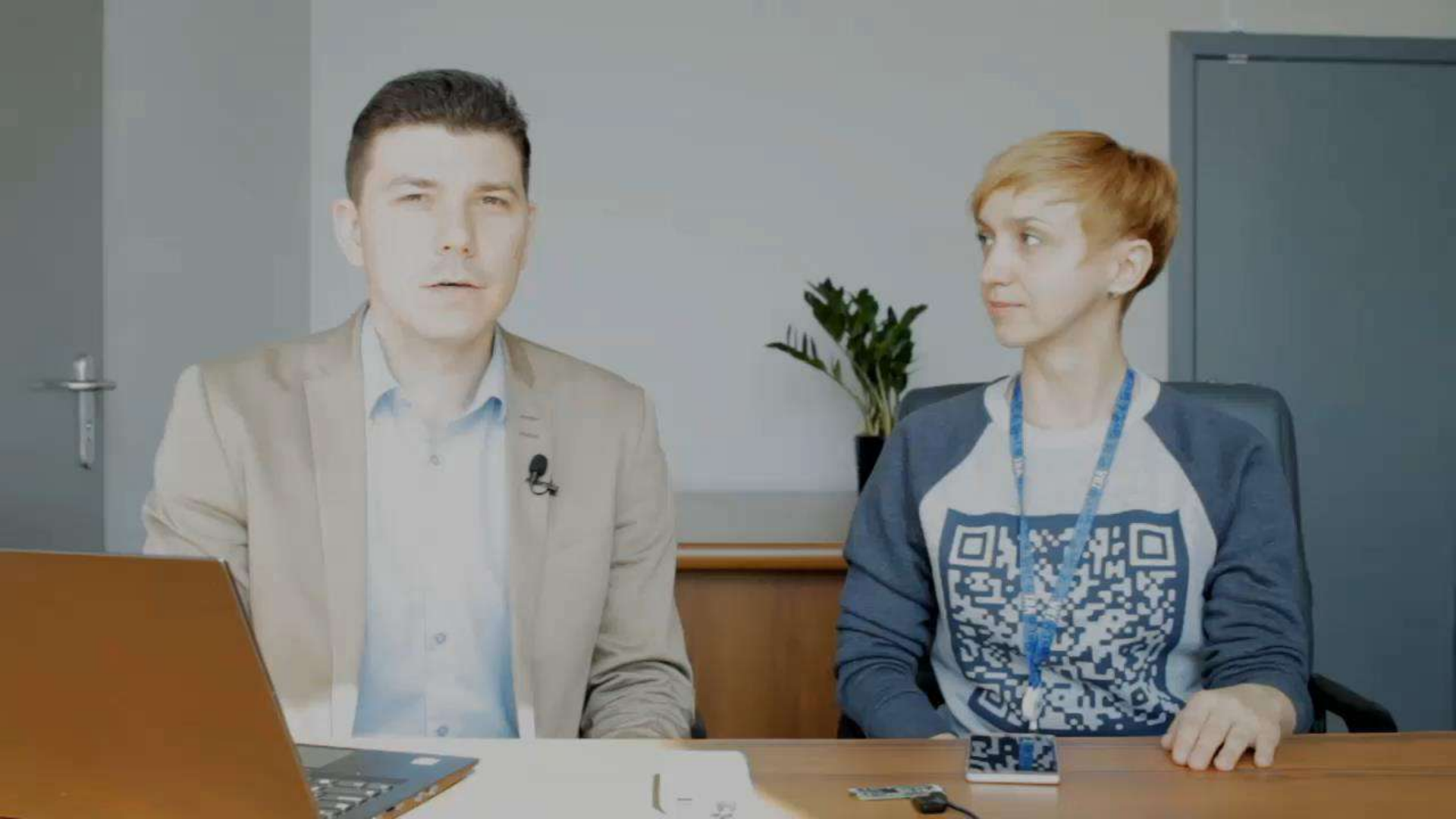
Parrot Security OS

BlackArch Linux

Matriux

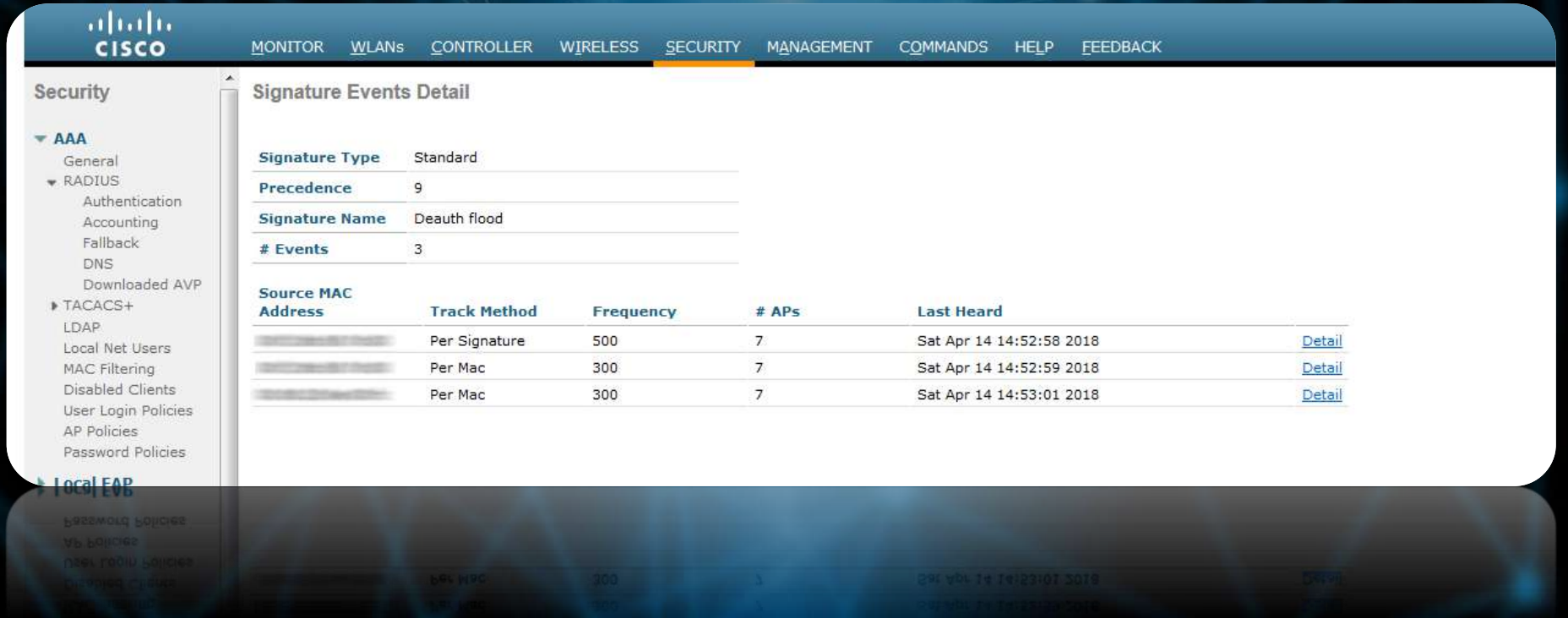
300 спецсредств для взлома:

- Wi-Fi сети (включая WPA, WP2)
- Веб сайты (есть сканеры уязвимостей)
- Роутеры, серверы
- Терминалы, банкоматы
- Работа через DarkNet
- Stealth - режим



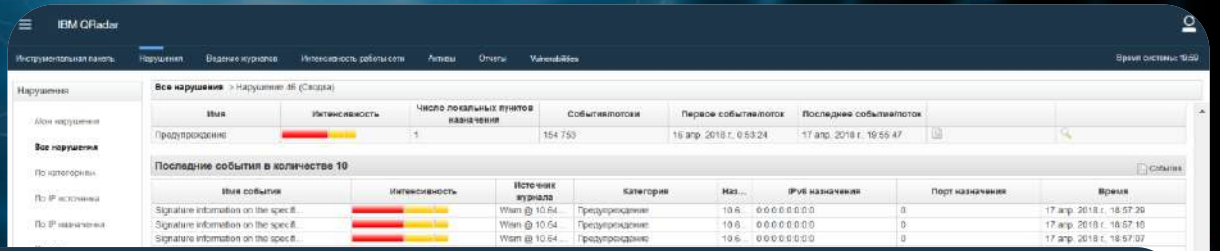
Реакция на периметре

IBA SECURITY



Пример: отлавливаем Wi-Fi атаку в QRadar

IBA SECURITY



IBM QRadar

Инструментальная панель | Нарушения | Ведение журналов | Интенсивность работы сети | Активы | Отчеты | Vulnerabilities | Время системы: 19:

Нарушения

- Мои нарушения
- **Все нарушения**
- По категориям
- По IP источника
- По IP назначения
- По сети
- Правила

Поиск... ▼ | Сохранить критерии | Действия ▼ | Печать | Send Offense to VAS | Последнее обновление: 00:03:15

Все нарушения | Просмотр нарушений: Выбрать опцию:

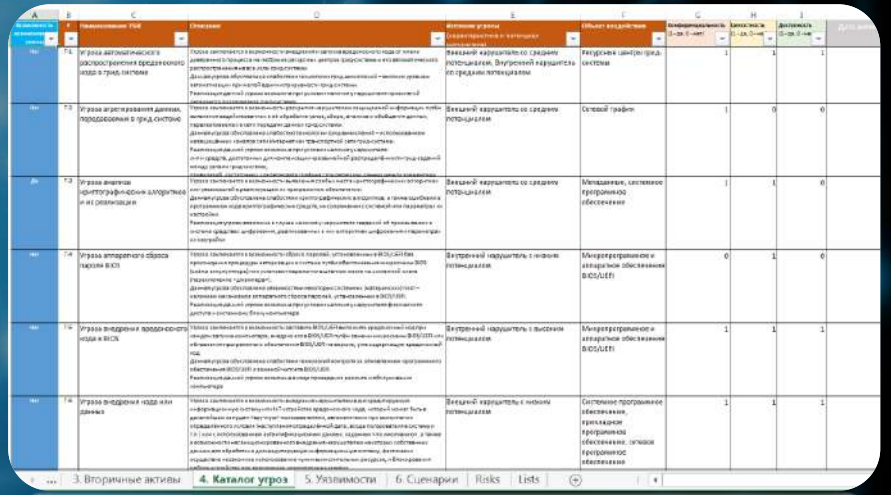
Текущие параметры поиска:

Исключить Скрытые нарушения (Очистить фильтр), Исключить Закрытые нарушения (Очистить фильтр)

	ID	Описание	Тип нарушения	Источ нарущ	Интенсивнс	IP источника	IP назначения	Пользовате	Источники журналов	События	Потоки	Начальная дата	Последне событие
	39	Multiple Login Failures for the Same User содержащий Bad Username	Имя поль...	ftp		Несколько...	Локальны...	ftp	Несколько...	45 077	0	14 апр. 20...	1 м. 46 с.
	3	Multiple Login Failures for the Same User содержащий Bad Username	Имя поль...	ed		Несколько...	Локальны...	ed	Несколько...	45 152	0	14 апр. 20...	1 м. 11 с.
	35	Multiple Login Failures for the Same User содержащий Bad Username	Имя поль...	farns...		Несколько...	Локальны...	farnsworth	Несколько...	45 041	0	14 апр. 20...	2 м. 2 с.
	26	Multiple Login Failures for the Same User содержащий Bad Username	Имя поль...	bart		Несколько...	Локальны...	bart	Несколько...	45 063	0	14 апр. 20...	35 с.
	27	Multiple Login Failures for the Same User содержащий Bad Username	Имя поль...	lisa		Несколько...	Локальны...	lisa	Несколько...	45 061	0	14 апр. 20...	0 с.
	46	Signature information on the specified AP	MAC-адре...	00:0...		10.64.2...	10.64.2...	Н/Д	Wism @ 1...	154 272	0	16 апр. 20...	26 с.
	47	Signature information on the specified AP	MAC-адре...	00:F...		10.64.2...	10.64.2...	Н/Д	Wism @ 1...	153 366	0	16 апр. 20...	24 с.

Построение модели угроз

IBA SECURITY



1. Каталог угроз
2. Первичные активы
3. Вторичные активы (ИС)
4. Уязвимости
5. Сценарии реализации угроз
6. Риски
7. План реагирования

Корреляционные правила в QRadar на базе рисков

Аудит СИБ – CSF, NIST 800

IBA SECURITY

Категория	InfoSec Service Catalog	Уровень риска	Закрытие рисков	Бюджет 2018 $	Бюджет 2019 $	Бюджет 2020 $	Compliance: CSC 20	Compliance: NIST	Уровень зрелости по SSE-CMM: Level 1 Performed informally	Level 2 Planned & Tracked	Level 3 Well defined	Level 4 Quantitatively controlled	Level 5 Continu impro
	Управление удаленным доступом	Low						PR.AC-3					
	Защита целостности сети, сегрегация где это целесообразно	Low						PR.AC-5					
Обучение и информирование	Обучение и информирование сотрудников, привелегированных пользователей, сторонних партнеров, руководителей высшего звена, персонала физической и информационной безопасности **- внедрение eUni**	High					5,17	PR.AT					
Защита данных	Защита баз данных **- Внедрение активных систем защиты для критических баз данных**	High					1,2	PR.DS-1					
	Защита каналов транспорта данных **- Выделение бизнес приложение и баз данных в отдельный сегмент сети** **- Внедрение шифрования каналов передачи данных между БД и серверами активов расположенных в общих сетях**	Moderate						PR.DS-2					
	Формализованное управление перемещениями, уничтожением активов **- Внедрение Asset Management системы (на выбор проприетарная либо open-source)**	Moderate						PR.DS-3					
	Обеспечение запаса емкостей и мошностей	Low						PR.DS-4					
	Защита данных от утечек **- Внедрение DLP**	High						PR.DS-5					
	Защита целостности ПО, операционных систем, данных	Moderate						PR.DS-6					
	Отделение сред разработки и тестирования от продуктива	Low						PR.DS-7					
Процессы	Процессы ITSM управление активами, конфигурацией, процессом разработки	Low					3, 4 7, 9 10, 11 18, 19	PR.IP-1 PR.IP-2 PR.IP-3					
	Автоматизация процесса резервного копирования, регулярное тестирование	High						PR.IP-4					
	Выполнение политик безопасности относительно физических активов, правил удаления данных. Улучшение политик защиты данных на регулярной основе.Информирование регуляторов иб эффективности исполнения политик.	Low						PR.IP-5 PR.IP-6 PR.IP-7					

О | УПРАВЛЕНИЕ ИБ | ЗАЩИТА | ОБНАРУЖЕНИЕ | РЕАГИРОВАНИЕ | ВОССТАНОВЛЕНИЕ | N ...

СИБ - это:

IBA SECURITY

1. ЗАЩИТА
2. ВОССТАНОВЛЕНИЕ
3. УПРАВЛЕНИЕ ИБ
4. ОБНАРУЖЕНИЕ

IBA iSEE

- Аудит ИБ
- Модель угроз
- Radar®
- Корреляционные правила
- Система отчетности
- Система оповещений

5. РЕАГИРОВАНИЕ

СИБ - это:

IBA SECURITY

1. ЗАЩИТА
2. ВОССТАНОВЛЕНИЕ
3. УПРАВЛЕНИЕ ИБ
4. ОБНАРУЖЕНИЕ
5. РЕАГИРОВАНИЕ

IBA iSEE

- Аудит ИБ
- Модель угроз
- QRadar®
- Корреляционные правила
- Система отчетности
- Система оповещений
- Visual Analysis Studio
- План реагирования

IBA SECURITY

IBA Visual Analysis Studio

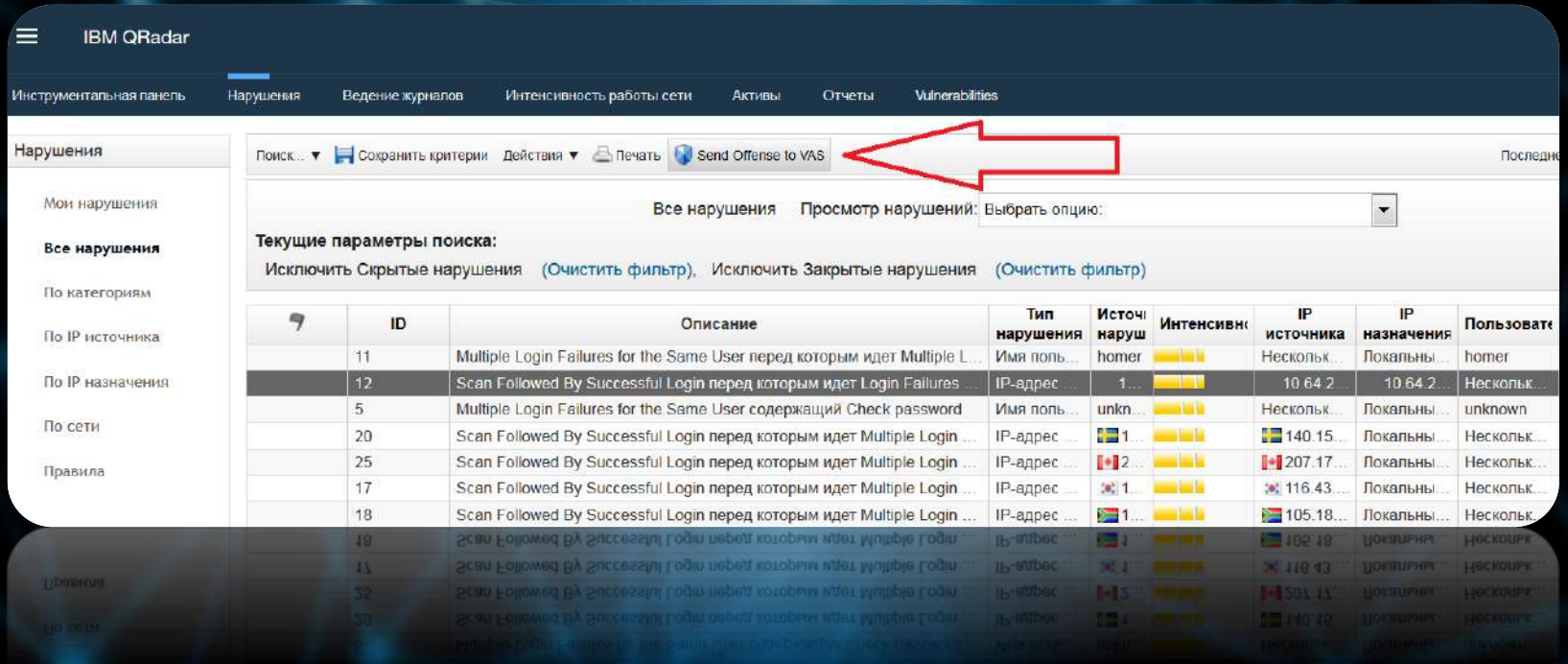
для

QRadar®

ДЕМО

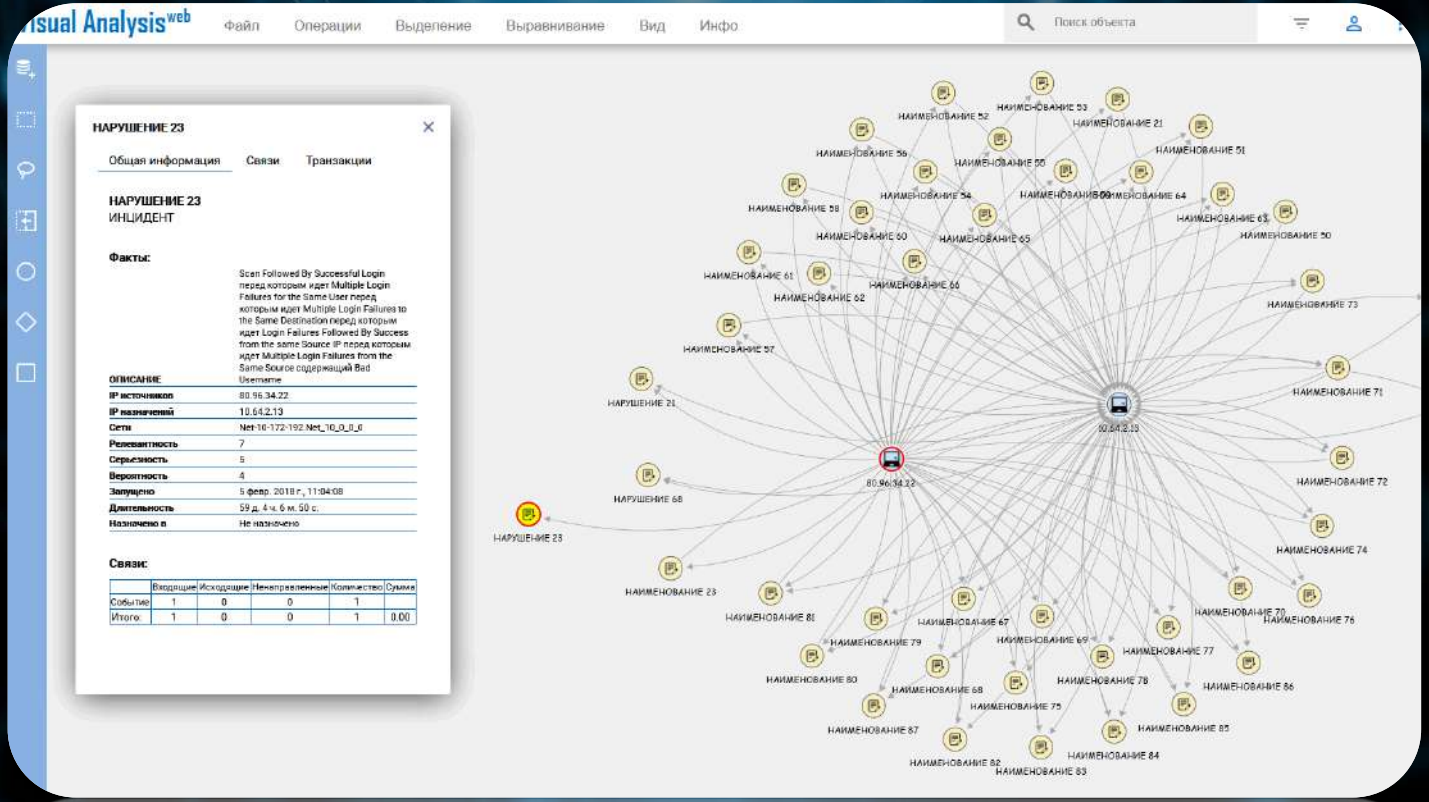
Расследовать в VAS!

IBA SECURITY



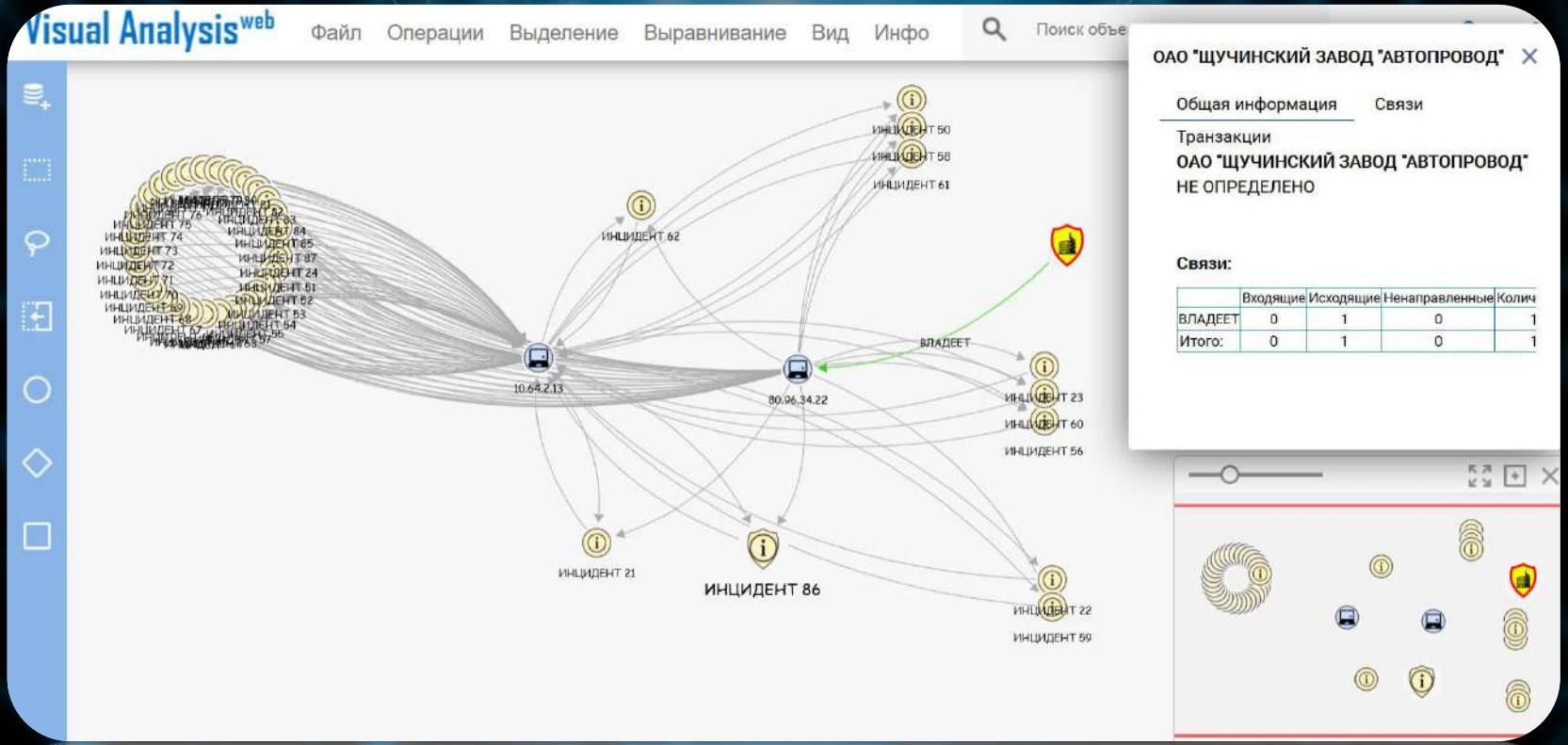
Пример: Подбор пароля AD

IBA SECURITY



Расследование ИБ в расследование СБ

IBA SECURITY



Совпадение наименований случайно – воспроизведено на тестовом стенде

IBAGROUPIT.COM • IBA.BY

IBA GROUP

ENVISIONING THE FUTURE

IBA SECURITY

Евгений Буря
Сергей Горбачев

+375 33 6183957
siarhei.harbachou@iba.by
Skype: sharbachou

www.ibasecurity.com
Service Desk: security@iba.by

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

19 АПРЕЛЯ 2018
МИНСК

КАК МОЩНО УСИЛИТЬ ВАШУ ОБОРОНОСПОСОБНОСТЬ ОДНИМ ДВИЖЕНИЕМ? ПРЕМЬЕРА РЕШЕНИЯ ISEE

СЕРГЕЙ ГОРБАЧЕВ

Менеджер по развитию IBA Security,
IBA GROUP

ТЕЛЕФОН: +375 (33) 618-39-57

EMAIL: SIARHEI.HARBACHOU@IBA.BY

IBA SECURITY

#CODEIB