



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



#CODEIB

IBAGROUP.IT.COM • IBA.BY

IBA
GROUP

ENVISIONING THE FUTURE



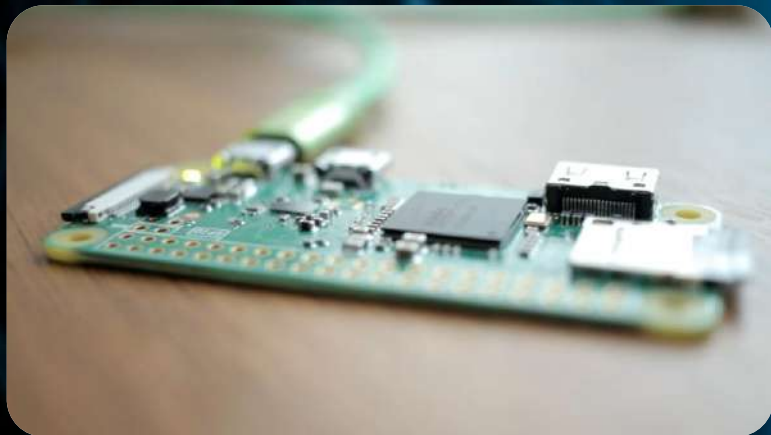
IBA SECURITY

Решение iSEE

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





Kali Linux



Parrot Security OS



BlackArch Linux

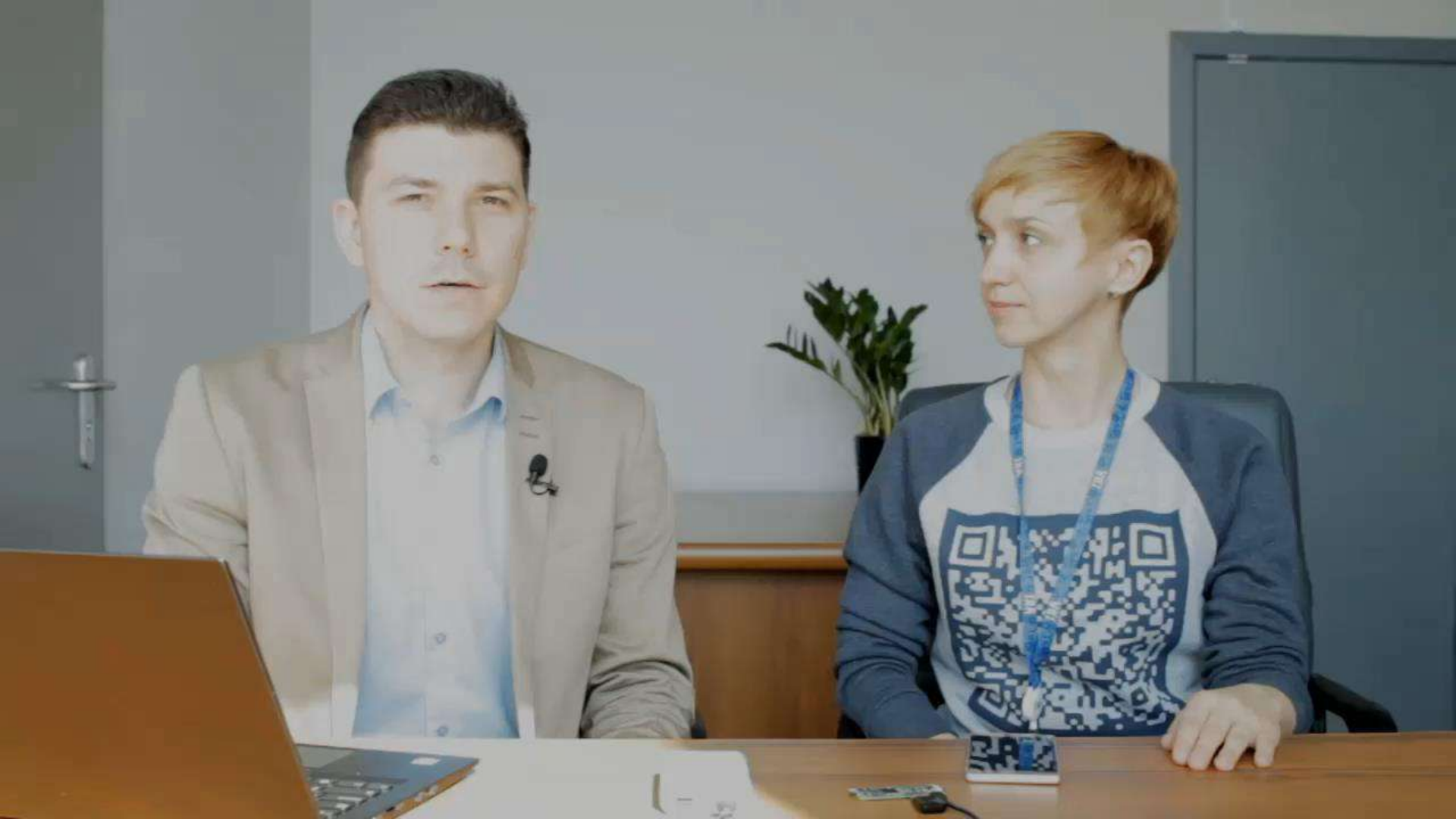


Matriux



300 спецсредств для взлома:

- Wi-Fi сети (включая WPA, WPA2)
- Веб сайты (есть сканеры уязвимостей)
- Роутеры, серверы
- Терминалы, банкоматы
- Работа через DarkNet
- Stealth - режим





Security

AAA

- General
- ▼ RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
- ▶ TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies

Signature Events Detail

Signature Type	Standard
Precedence	9
Signature Name	Death flood
# Events	3

Source MAC Address	Track Method	Frequency	# APs	Last Heard	
08:00:20:08:00:08	Per Signature	500	7	Sat Apr 14 14:52:58 2018	Detail
08:00:20:08:00:08	Per Mac	300	7	Sat Apr 14 14:52:59 2018	Detail
08:00:20:08:00:08	Per Mac	300	7	Sat Apr 14 14:53:01 2018	Detail

Local EOP

- Password Policies
- AP Policies
- User Login Policies
- Disabled Clients


Пример: отлавливаем Wi-Fi атаку в QRadar



The screenshot displays the IBM QRadar console interface. At the top, the navigation bar includes 'Инструментальная панель', 'Нарушения', 'Ведение журналов', 'Интенсивность работы сети', 'Активы', 'Отчеты', and 'Vulnerabilities'. The main content area is titled 'Нарушения' and shows a summary of 'Все нарушения' (All violations) with a table of metrics. Below this, a section titled 'Текущие параметры поиска:' (Current search parameters) includes options to 'Исключить Скрытые нарушения' and 'Исключить Закрытые нарушения'. The primary focus is a table of violations, where two entries (IDs 46 and 47) are highlighted with a red border. These entries describe 'Signature information on the specified AP' with a severity of 4 (indicated by four yellow bars). The table columns include ID, Description, Type of violation, Source, Intensity, IP source, IP destination, User, Source of logs, Events, Flows, Start date, and Last event.

ID	Описание	Тип нарушения	Источн наруш	Интенсивнсв	IP источника	IP назначения	Пользоват	Источники журналов	События	Потоки	Начальная дата	Последн событие
39	Multiple Login Failures for the Same User содержащий Bad Username	Имя поль...	ftp	4	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	4	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...	fams...	4	Несколько...	Локальны...	famsworth	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	4	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	4	Несколько...	Локальны...	lisa	Несколько...	45 061	0	14 апр. 20...	0 с.
46	Signature information on the specified AP	MAC-адре...	00:0...	4	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...	4	10.64.2...	10.64.2...	Н/Д	Wism @ 1...	153 366	0	16 апр. 20...	24 с.

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



Имя	Описание	Категория угрозы	Уровень серьезности	Важность	Уязвимость	Детальность
Угроза интроскопирования в ОС/ПО/устройствах с использованием протокола LDAP в среде LDAP	Угроза интроскопирования в ОС/ПО/устройствах с использованием протокола LDAP в среде LDAP. Атакующий может использовать LDAP для получения информации о пользователях, группах и ролях в системе. Это может привести к компрометации учетных записей и доступу к данным.	Вредная журналистика со средним уровнем сложности. Внутренняя журналистика по фреймворку	Категория (идентификация)	1	1	1
Угроза агрегирования данных, полученных в результате атаки	Угроза агрегирования данных, полученных в результате атаки. Атакующий может собрать информацию о пользователях, группах и ролях в системе. Это может привести к компрометации учетных записей и доступу к данным.	Вредная журналистика со средним уровнем сложности. Внутренняя журналистика по фреймворку	Категория (идентификация)	1	0	0
Угроза анализа функциональных возможностей и уязвимостей	Угроза анализа функциональных возможностей и уязвимостей. Атакующий может использовать информацию о функциональных возможностях и уязвимостях для планирования атаки.	Вредная журналистика со средним уровнем сложности. Внутренняя журналистика по фреймворку	Категория (идентификация)	1	1	0
Угроза вторичного доступа к данным ВСП	Угроза вторичного доступа к данным ВСП. Атакующий может использовать информацию о функциональных возможностях и уязвимостях для планирования атаки.	Вредная журналистика со средним уровнем сложности. Внутренняя журналистика по фреймворку	Категория (идентификация)	0	1	0
Угроза вторичного доступа к данным ВСП	Угроза вторичного доступа к данным ВСП. Атакующий может использовать информацию о функциональных возможностях и уязвимостях для планирования атаки.	Вредная журналистика со средним уровнем сложности. Внутренняя журналистика по фреймворку	Категория (идентификация)	1	1	1
Угроза вторичного доступа к данным ВСП	Угроза вторичного доступа к данным ВСП. Атакующий может использовать информацию о функциональных возможностях и уязвимостях для планирования атаки.	Вредная журналистика со средним уровнем сложности. Внутренняя журналистика по фреймворку	Категория (идентификация)	1	1	1

Корреляционные правила в QRadar на базе рисков

Категория	InfoSec Service Catalog	Уровень риска	Заккрытие рисков	Бюджет 2018 \$	Бюджет 2019 \$	Бюджет 2020 \$	Compliance		Уровень зрелости по SSE-CMM					
							CSC 20	NIST	Level 1 Performed informally	Level 2 Planned & Tracked	Level 3 Well defined	Level 4 Quantitatively controlled	Level 5 Continuously improved	
	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	High						5,17	PR.AT					
	- внедрение eUni	High							PR.DS-1					
Защита данных	Защита баз данных	High						1,2	PR.DS-1					
	- Внедрение активных систем защиты для критических баз данных	High							PR.DS-2					
	Защита каналов транспорта данных	Moderate							PR.DS-2					
	- Выделение бизнес приложения и баз данных в отдельный сегмент сети	Moderate							PR.DS-3					
	- Внедрение шифрования каналов передачи данных между БД и серверами активов расположенных в общих сетях	Moderate							PR.DS-3					
	Формализованное управление перемещениями, уничтожением активов	Moderate							PR.DS-3					
	- Внедрение Asset Management системы (на выбор проприетарная либо open-source)	Moderate							PR.DS-3					
Обеспечение запаса емкостей и мощностей	Low							PR.DS-4						
Процессы	Защита данных от утечек	High							PR.DS-5					
	- 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 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.	High							PR.IP-5 PR.IP-6 PR.IP-7					

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

О УПРАВЛЕНИЕ ИБ ЗАЩИТА ОБНАРУЖЕНИЕ РЕАГИРОВАНИЕ ВОССТАНОВЛЕНИЕ И ... +

О УПРАВЛЕНИЕ ИБ ЗАЩИТА ОБНАРУЖЕНИЕ РЕАГИРОВАНИЕ ВОССТАНОВЛЕНИЕ И ... +

О УПРАВЛЕНИЕ ИБ ЗАЩИТА ОБНАРУЖЕНИЕ РЕАГИРОВАНИЕ ВОССТАНОВЛЕНИЕ И ... +

О УПРАВЛЕНИЕ ИБ ЗАЩИТА ОБНАРУЖЕНИЕ РЕАГИРОВАНИЕ ВОССТАНОВЛЕНИЕ И ... +

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



Аудит ИБ
Модель угроз



Radar[®]
Корреляционные правила
Система отчетности
Система оповещений

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



Аудит ИБ
Модель угроз



Radar®

Корреляционные правила
Система отчетности
Система оповещений

Visual Analysis Studio
План реагирования



IBA Visual Analysis Studio

для



ДЕМО

IBM QRadar

Инструментальная панель | Нарушения | Ведение журналов | Интенсивность работы сети | Активы | Отчеты | Vulnerabilities

Нарушения

Поиск... | Сохранить критерии | Действия | Печать | **Send Offense to VAS** | Последние

Мои нарушения

Все нарушения

По категориям

По IP источника

По IP назначения

По сети

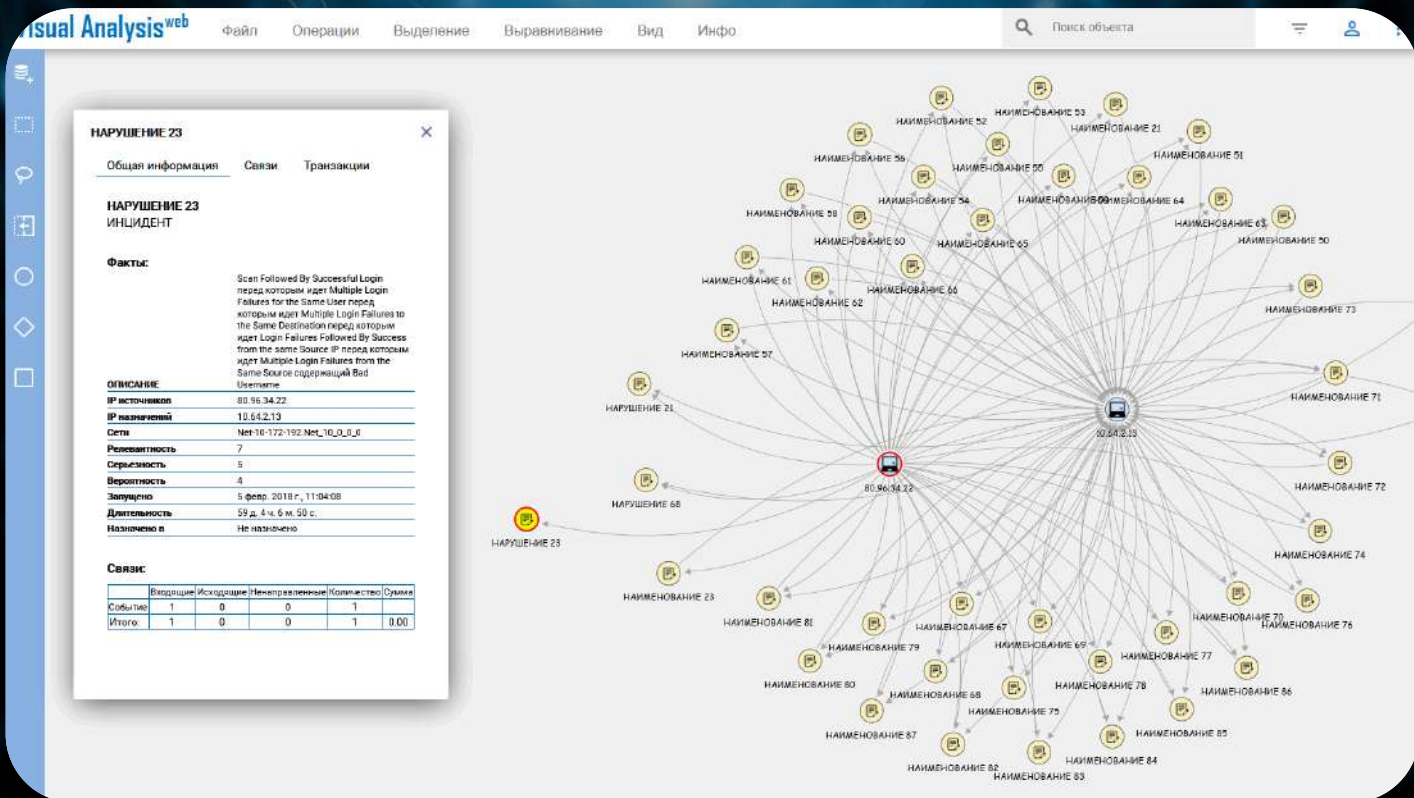
Правила

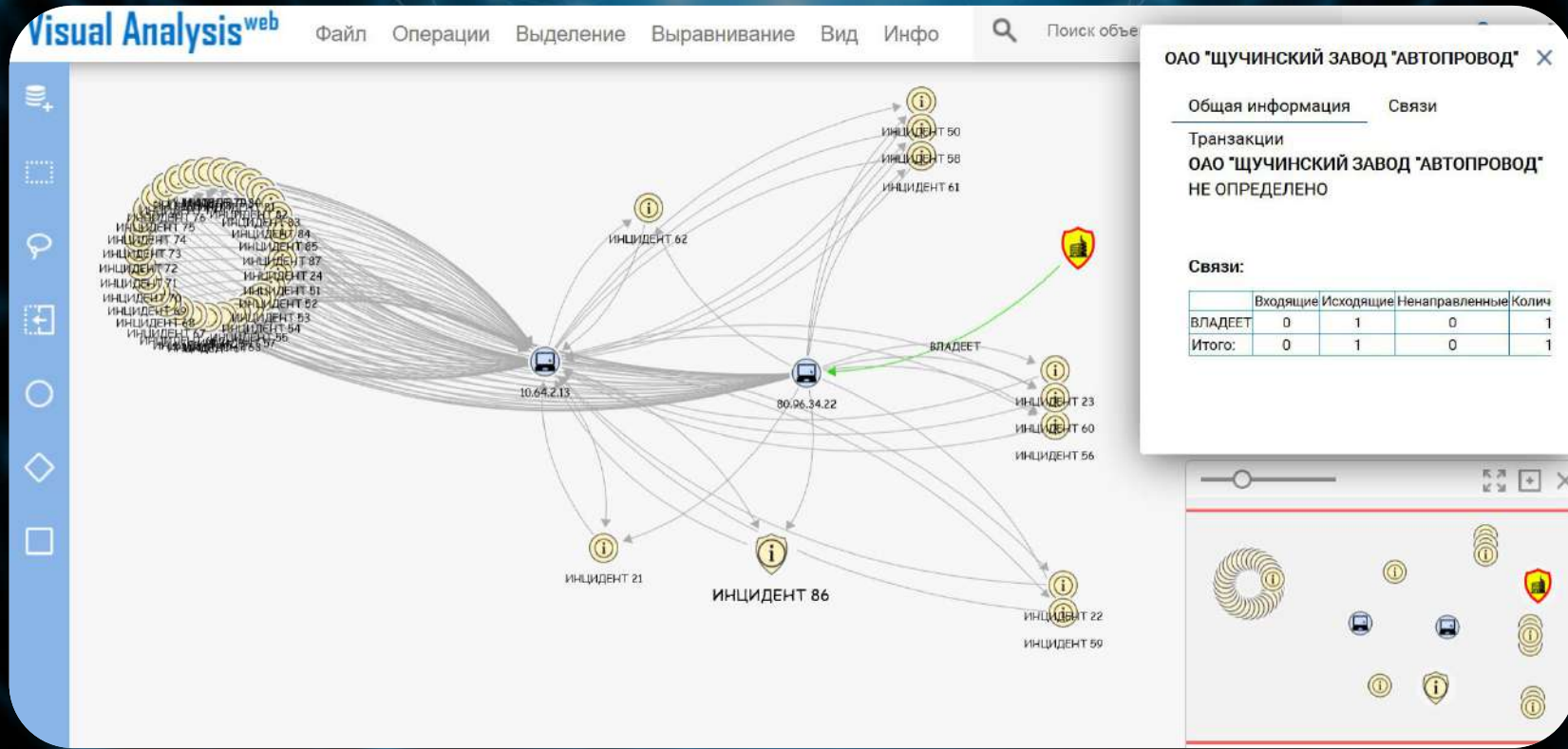
Текущие параметры поиска:

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

ID	Описание	Тип нарушения	Источн. наруш	Интенсивн.	IP источника	IP назначения	Пользоват
11	Multiple Login Failures for the Same User перед которым идет Multiple L...	Имя поль...	homer	4	Несколько...	Локальны...	homer
12	Scan Followed By Successful Login перед которым идет Login Failures ...	IP-адрес ...	1...	3	10.64.2...	10.64.2...	Несколько...
5	Multiple Login Failures for the Same User содержащий Check password	Имя поль...	unkn...	4	Несколько...	Локальны...	unknowp
20	Scan Followed By Successful Login перед которым идет Multiple Login ...	IP-адрес ...	1...	4	140.15...	Локальны...	Несколько...
25	Scan Followed By Successful Login перед которым идет Multiple Login ...	IP-адрес ...	2...	4	207.17...	Локальны...	Несколько...
17	Scan Followed By Successful Login перед которым идет Multiple Login ...	IP-адрес ...	1...	4	116.43...	Локальны...	Несколько...
18	Scan Followed By Successful Login перед которым идет Multiple Login ...	IP-адрес ...	1...	4	105.18...	Локальны...	Несколько...
19	дсав Еоюмюв рА злссвагул гоюв иевел колювнч нлел үлрбю гоюв	ль-әтбес	1...	4	102.18...	цоквирнч	несколк...
13	дсав Еоюмюв рА злссвагул гоюв иевел колювнч нлел үлрбю гоюв	ль-әтбес	1...	4	110.43...	цоквирнч	несколк...
32	дсав Еоюмюв рА злссвагул гоюв иевел колювнч нлел үлрбю гоюв	ль-әтбес	1...	4	501.13...	цоквирнч	несколк...
30	дсав Еоюмюв рА злссвагул гоюв иевел колювнч нлел үлрбю гоюв	ль-әтбес	1...	4	140.10...	цоквирнч	несколк...

Пример: Подбор пароля AD





Совпадение наименований случайно – воспроизведено на тестовом стенде

IBAGROUP.IT.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



#CODEIB