

Как эффективно настраивать правила безопасности

Практические кейсы

Роман Клименко

Руководитель представительства Falcongaze в УРФО

Что такое эффективное правило безопасности?

Политика безопасности - совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной Информации.

ОСНОВНЫЕ ШАГИ НАСТРОЙКИ ПРАВИЛ БЕЗОПАСНОСТИ

1

**Анализ инфраструктуры
организации**

2

**Инвентаризация
информационных активов
организации**

3

**Определяем степень
критичности информации**

4

**Изучение активности
пользователей**

5

**Обозначение потенциальных
каналов утечки**

6

**Определение степени
важности при помощи
уровней риска**

7

**Категорирование
критичности нарушений при
помощи уровней риска**

8

**Анализ инцидентов и
формирование «досье»**

9

**Расследование инцидентов с
регистрацией принятых мер и
выводом**

10

**Регулярное внесение
корректировок в правила
безопасности**

СКОЛЬКО ВРЕМЕНИ ЭТО МОЖЕТ ЗАНЯТЬ?

КАСТОМИЗАЦИЯ ПРАВИЛ БЕЗОПАСНОСТИ: большие шаги кастомизации

НАБОР ПРЕДУСТАНОВЛЕННЫХ ПОЛИТИК БЕЗОПАСНОСТИ

ПРОТИВ САМЫХ РАСПРОСТРАНЕННЫХ УГРОЗ



ОПРЕДЕЛЯЕМ

ключевые моменты,
что именно
отслеживать



ВЫДЕЛЯЕМ

группу пользователей,
взаимодействующих с
информацией



МОНИТОРИМ

количество сработок
и анализируем их
релевантность



ОПТИМИЗИРУЕМ

правила безопасности
сокращая количество
невалидных сработок



КЕЙС №1: Контроль подключаемых накопителей

Искать ▾ | Добавить в избранное | Показать избранное | Экспорт\Импорт ▾ | Show request string (test) | Show XML structure (test)

Интервал поиска: | Количество результатов:

Доступный интервал поиска: 04.05.2018 - 06.09.2019

Группы Active Directory

Условия поиска

Выберите операцию, применяемую к условиям в блоке: И Или Не (отрицание)

Область поиска ▾	<input type="checkbox"/> Почта	<input type="checkbox"/> Мессенджеры	<input type="checkbox"/> Web	<input checked="" type="checkbox"/> Прочее
	<input type="checkbox"/> POP3	<input type="checkbox"/> Skype	<input type="checkbox"/> Посещённые web-страницы	<input type="checkbox"/> FTP
	<input type="checkbox"/> SMTP	<input type="checkbox"/> Telegram	<input type="checkbox"/> Поисквые запросы	<input type="checkbox"/> Файлы с устройств
	<input type="checkbox"/> IMAP	<input type="checkbox"/> Viber	<input type="checkbox"/> Отправленные запросы	<input checked="" type="checkbox"/> Аудит устройств
	<input type="checkbox"/> MAPI	<input type="checkbox"/> WhatsApp	<input type="checkbox"/> Web-коммуникации	<input type="checkbox"/> Сетевые ресурсы
	<input type="checkbox"/> Прочая почта	<input type="checkbox"/> Lync	<input type="checkbox"/> Браузер-активность	<input type="checkbox"/> Облачные хранилища
	<input type="checkbox"/> Вложения	<input type="checkbox"/> SIP	<input type="checkbox"/> Файлы	<input type="checkbox"/> Снимки экрана
		<input type="checkbox"/> XMPP (Jabber)		<input type="checkbox"/> Активность ПК
		<input type="checkbox"/> ICQ (OSCAR)		<input type="checkbox"/> Принтеры
		<input type="checkbox"/> Mail.RU Агент		<input type="checkbox"/> Буфер обмена
		<input type="checkbox"/> Yahoo		<input type="checkbox"/> Кейлоггер
		<input type="checkbox"/> Hangouts		<input type="checkbox"/> Совпадения по
		<input type="checkbox"/> Slack		
		<input type="checkbox"/> Web-переписки		
		<input type="checkbox"/> Файлы		

[\[Добавить условие\]](#) | [\[Добавить блок\]](#) | [\[Обрамить блоком\]](#)

ПРОМЕЖУТОЧНЫЙ РЕЗУЛЬТАТ:

Большое количество устройств, которые нам не интересны

Локальный пользователь:  [naiadm](#)

Типы устройств

Все устройства
 USB устройство
 Сетевые устройства
 Порты
 Модемы
 Накопители на флоппи-дисках
 Мультимедиа
 Накопители на CD/DVD дисках
 Портативные устройства

Информация аудита использования устройств (устройств: 7, соответствующих фильтру: 7)

+	🖥️	VMWARE_SATA_CD00	NECVMMWAR, ParallelPort	Время подключения	Состояние
				2019.08.27 16:50:56 - 2019.08.27 17:05:06	Остановлено
				2019.08.27 16:50:56 - 2019.08.27 17:05:06	Остановлено
				2019.08.27 16:50:56 - 2019.08.27 17:05:06	Остановлено
				2019.08.27 16:50:56 - 2019.08.27 17:05:06	Остановлено
				2019.08.27 16:50:56 - 2019.08.27 17:05:06	Остановлено
				2019.08.27 16:50:56 - 2019.08.27 17:05:06	Остановлено
				2019.08.27 16:53:07 - 2019.08.27 17:05:06	Остановлено

Активация Windows

бы активировать Windows, перейдите в компонент панели управления "Система".

КАСТОМИЗИРУЕМ:
Исключаем из поисковой выдачи «Virtual»

Интервал поиска
 За последние 30 дней

Количество результатов
 500 результатов

Доступный интервал поиска: 04.05.2018 - 06.09.2019

Группы Active Directory

Условия поиска
 Выберите операцию, применяемую к условиям в блоке: И Или Не (отрицание)


Область поиска	Почта	Мессенджеры	Web	Прочее
	<input type="checkbox"/> POP3	<input type="checkbox"/> Skype	<input type="checkbox"/> Посещённые web-страницы	<input type="checkbox"/> FTP
	<input type="checkbox"/> SMTP	<input type="checkbox"/> Telegram	<input type="checkbox"/> Поисковые запросы	<input type="checkbox"/> Файлы с устрой
	<input type="checkbox"/> IMAP	<input type="checkbox"/> Viber	<input type="checkbox"/> Отправленные запросы	<input checked="" type="checkbox"/> Аудит устройств
	<input type="checkbox"/> MAPI	<input type="checkbox"/> WhatsApp	<input type="checkbox"/> Web-коммуникации	<input type="checkbox"/> Сетевые ресурсы
	<input type="checkbox"/> Прочая почта	<input type="checkbox"/> Lync	<input type="checkbox"/> Браузер-активность	<input type="checkbox"/> Облачные храни
	<input type="checkbox"/> Вложения	<input type="checkbox"/> SIP	<input type="checkbox"/> Файлы	<input type="checkbox"/> Снимки экрана
		<input type="checkbox"/> XMPP (Jabber)		<input type="checkbox"/> Активность ПК
		<input type="checkbox"/> ICQ (OSCAR)		<input type="checkbox"/> Принтеры
		<input type="checkbox"/> Mail.RU Агент		<input type="checkbox"/> Буфер обмена
		<input type="checkbox"/> Yahoo		<input type="checkbox"/> Кейлогер
		<input type="checkbox"/> Hangouts		<input type="checkbox"/> Совпадения по
		<input type="checkbox"/> Slack		
		<input type="checkbox"/> Web-переписки		
		<input type="checkbox"/> Файлы		



И

Устройства | Аудит устройств | Название устройства | Не содержит | **Virtual**

[\[Добавить условие\]](#) [\[Добавить блок\]](#) [\[Обрамить блоком\]](#)

РЕЗУЛЬТАТ:
Выдача более релевантная

Локальный пользователь:  [naiadm](#)



Текущий документ может быть найден по следующему пути:
 [Аудит устройств 192.168.2...](#) ->  Аудит устройств 192.168.2...

Типы устройств

Все устройства
 USB устройство
 Сетевые устройства
 Порты
 Модемы
 Накопители на флоппи-дисках

Мультимедиа
 Накопители на CD/DVD дисках
 Портативные устройства

Информация аудита использования устройств (устройство: 1, соответствующих фильтру: 1)

  DataTraveler G4 Kingston Technology, UsbDevice 5404A6F4E0A6F2A1292A039F	Время подключения	Состояние
	2019.08.27 16:53:07 - 2019.08.27 17:05:06	Остановлено

КЕЙС №2: Контроль запуска специализированного ПО

Интервал поиска **Количество результатов**

За последние 30 дней 500 результатов

i Доступный интервал поиска: 04.05.2018 - 06.09.2019

▼ **Группы Active Directory**

Условия поиска

Выберите операцию, применяемую к условиям в блоке: И Или Не (отрицание)

Процесс Имя файла Содержит cmd.exe Любая активность

Или

Процесс Имя файла Содержит regedit.exe Любая активность

[\[Добавить условие\]](#) [\[Добавить блок\]](#) [\[Обрамить блоком\]](#)

РЕЗУЛЬТАТ:

Логично предположить, что применение данного правила для системных администраторов создаст огромное количество сработок. И исключения из области действия правила группы администраторов оправдано.

Интервал поиска **Количество результатов**

За последние 30 дней 500 результатов

i Доступный интервал поиска: 04.05.2018 - 06.09.2019

^ **Группы Active Directory (1)**

Укажите группы Active Directory, по которым будет производиться поиск

Группа исключена Администраторы домена

[Добавить условие](#)

Условия поиска

Выберите операцию, применяемую к условиям в блоке: И Или Не (отрицание)

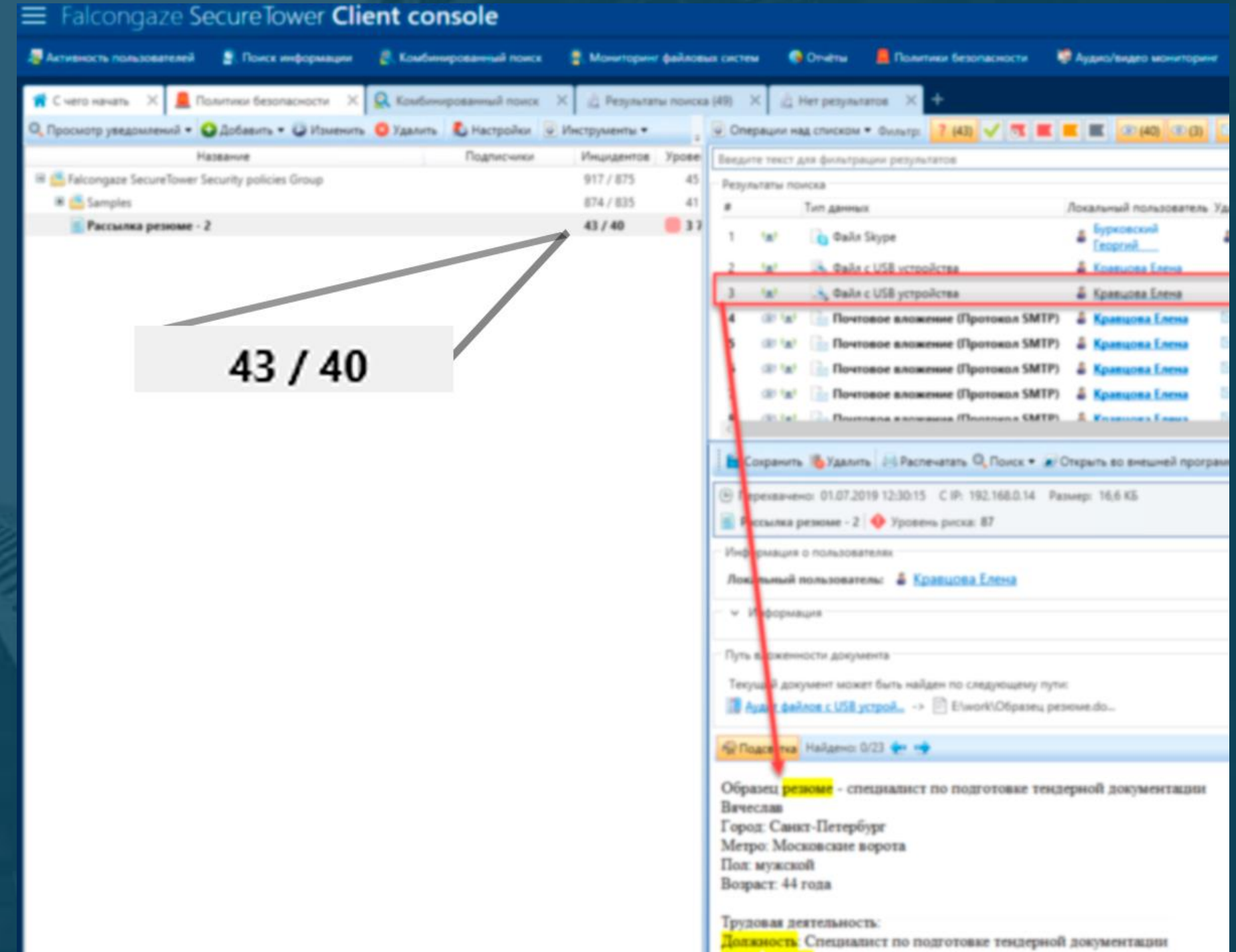
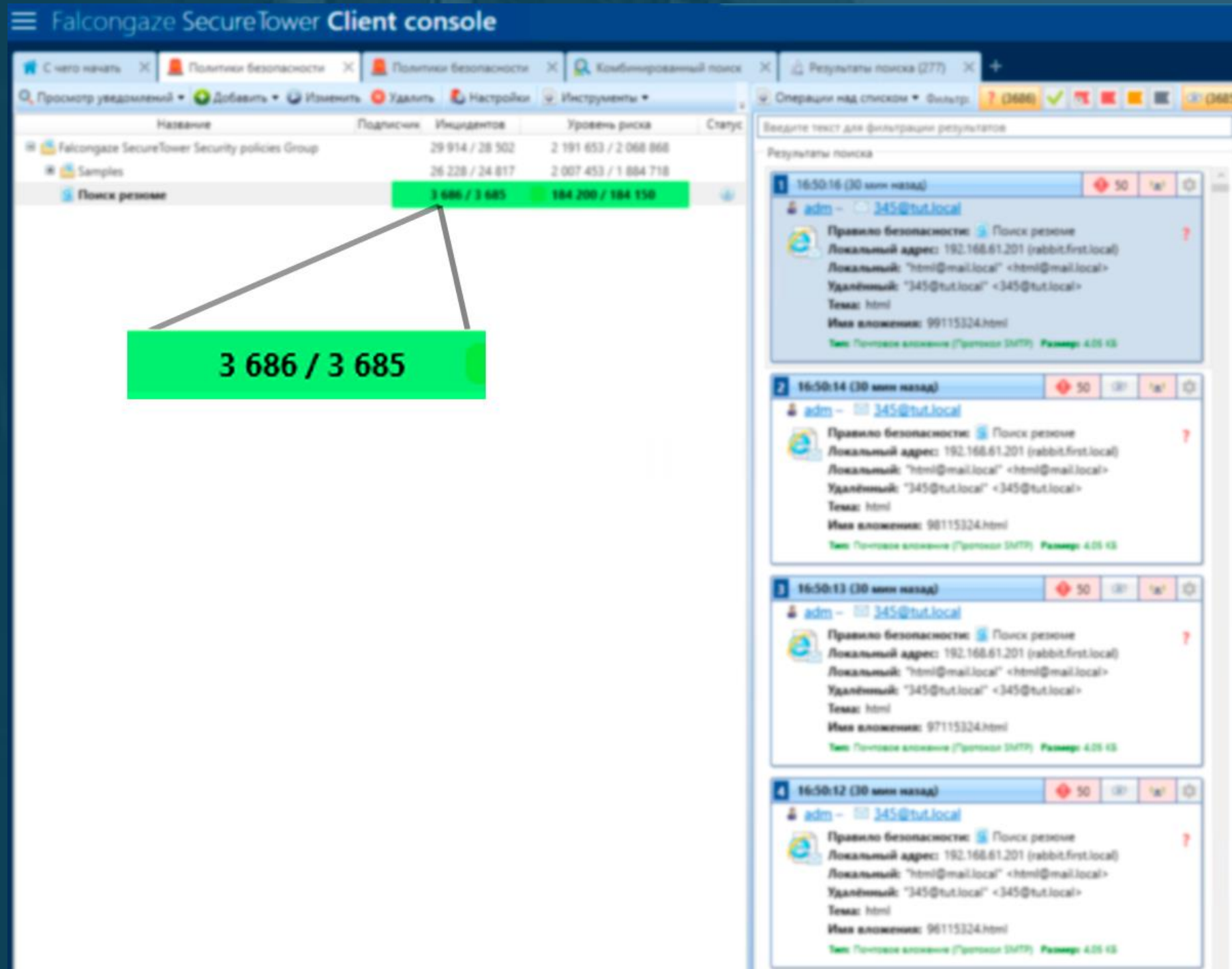
Процесс Имя файла Содержит cmd.exe Любая активность ...

Или

Процесс Имя файла Содержит regedit.exe Любая активность ...

[Добавить условие](#) [Добавить блок](#) [Обрамить блоком](#)

Кастомизация правил безопасности. Кейс: поиск по резюме



ДО

ПОСЛЕ

1

**Анализ инфраструктуры
организации**

2

**Инвентаризация
информационных активов
организации**

3

**Определяем степень
критичности информации**

4

**Изучение активности
пользователей**

5

**Обозначение потенциальных
каналов утечки**

6

**Определение степени
важности при помощи
уровней риска**

7

**Категорирование
критичности нарушений при
помощи уровней риска**

8

**Анализ инцидентов и
формирование «досье»**

9

**Расследование инцидентов с
регистрацией принятых мер и
выводом**

10

**Регулярное внесение
корректировок в правила
безопасности**



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ



РОМАН КЛИМЕНКО

Руководитель представительства Falcongaze в УРФО

r.klimenka@falcongaze.ru

+7 343 339 41 42

+7 963 035 42 48

