ООО «Стратегия Защиты»

ПРОГРАММНЫЙ МОДУЛЬ
Система предупреждения кибератак «Сонар-1М»
Шифр: СПК «Сонар-1М»

Руководство оператора

2018

АННОТАЦИЯ

Настоящий документ - руководство для оператора программного комплекса SONAR-Framework. Документ описывает работу оператора с программной частью комплексного решения. Цель документа - дать читателю понятие об общих элементах веб-интерфейса и детальное руководство к выполнению всех видов операций.

Документ состоит из четырех частей:

- раздел «Назначение программы». Здесь указаны сведения о назначении программы и информация, достаточная для понимания функций программы и ее эксплуатации
- раздел «Условия выполнения программы». Здесь указаны условия, необходимые для выполнения программы (минимальный состав аппаратных и программных средств и т.п.).
- раздел «Выполнение программы». Здесь приведены последовательности действий оператора, обеспечивающих загрузку, запуск, выполнение и завершение программы, приведено описание функций, формата и возможных вариантов команд, с помощью которых оператор осуществляет загрузку и управляет выполнением программы, а также ответы программы на эти команды.
- раздел «Сообщения оператору». Здесь приведены тексты сообщений, выдаваемых в ходе выполнения программы, описание их содержания и соответствующие действия оператора (действия оператора в случае сбоя, возможности повторного запуска программы и т.п.). Указана информация для поиска и устранения ошибок в работе.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Назначение

Программный комплекс СПК «Сонар-1М» предназначен для выполнения анализа трафика в режиме «реального времени», выявление уязвимостей, связанных с ошибками в конфигурациях системного программного обеспечения и сетевого оборудования, которые могут быть использованы нарушителем для реализации атак на систему и компрометации защищаемых данных.

1.2 Функциональные возможности

Функционал СПК «Сонар-1М» включает в себя:

- инспектирование входящего и исходящего сетевого трафика;
- анализ входящего и исходящего трафика по сигнатурам, сравнение сигнатур с набором правил (политик), имеющихся в составе модуля. При соответствии сигнатур осуществляется запись в журнал отчета, фиксируя следующие поля:
    - дата и время события (инцидента);
    - краткая идентификация сигнатуры;
    - ip-адрес и порт отправителя;
    - ip-адрес и порт получателя;
    - данные (при их наличии).
- при обнаружении вредоносных сигнатур, атак и прочих аномалий модуль осуществляет распределение событий по срабатыванию, видам атак, сигнатурам, типам событий и собирает статистику по инцидентам;
- формирование отчетов о произошедших событиях и инцидентах.

В составе СПК «Сонар-1М» присутствует Web-интерфейс управления организующий следующие действия:

- мониторинг за инцидентами, произошедшими в контролируемой системе или сети;

- наблюдение за атаками с распределением по видам атак;
- отображение диаграмм по ip-адресам, портам и событиям;
- геолокацию атак;
- сводную информацию по событиям за текущий день или за выбранный период;
- вывод отчетов по событиям за текущий день или за выбранный период;
- подсчет обнаруженных событий, выводит информаци по наиболее часто встречающимся сигнатурам, самым частым атакующим и атакуемым ip-адресам.

1.3 Функциональные ограничения

Для выполнения анализа трафика требуется подключение сервера СПК «Сонар-1М» к порту, работающему в режиме зеркалирования трафика (SPAN порту), поскольку программный комплекс выполняет пассивное сканирование уязвимостей удаленных подсетей и устройств.

По результатам проводимого анализа зарегистрированные инциденты безопасности помещаются в базу данных и хранятся локально. Необходимый объем устройств хранения информации зависит от интенсивности трафика и требований по времени хранения событий. Рекомендуется выделять объем исходя из расчета – 500Мб в неделю при регистрации 100 событий ежедневно.

Развернутый программный комплекс занимает до 4 Гб дискового пространства.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Требования к техническим средствам

2.1.1 Минимальные системные требования (нерекомендуемые):

- Сервер с процессором Intel Atom 1.6 Ггц;
- 1 Гб ОЗУ;
- 20 Гб свободного места на жестком диске ПЗУ;
- 1 ethernet-карта.

2.1.2 Оптимальные (рекомендуемые) системные требования:

- Сервер, с процессором Intel Xeon 2 ГГц;
- 4 Гб ОЗУ;
- 300 Гб свободного места на жестком диске, желательно, распределение отдельного диска или раздела для /SONAR, /var;
- 2 ethernet-карты с поддержкой pf_ring.

2.2 Требования к программным средствам

SONAR-Framework включает несколько готовых программных пакетов, подготовленных для работы с операционной системой CentOS 6.9. Для корректного функционирования комплекса в системе должны быть установлены следующие компоненты:

- mysql-server-5.1.73
- php-5.3.3
- libpcap-1.4.0
- apache-2.2.15

Примечание: версии программных компонентов должны быть не ниже указанных.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1 Вход в web-интерфейс

Взаимодействие пользователя с модулем СПК «Сонар-1М» выполняется через web-интерфейс. Для входа в интерфейс управления требуется запустить браузер в адресной строке ввести ip-адрес или доменное имя сервера с установленным СПК «Сонар-1М». Адрес сервера СПК «Сонар-1М» имеет вид:

```
https://192.168.1.140/SONAR/
```

Примечание: При появлении сообщения об ошибке сертификата, следует согласиться и принять сертификат.

После перехода по указанному адресу откроется окно авторизации (см. Рисунок 1). Учетная запись по умолчанию логин – admin, пароль – SONAR12345678. Управление учтенными записями выполняется в соответствии с руководством администратора СПК «Сонар-1М».

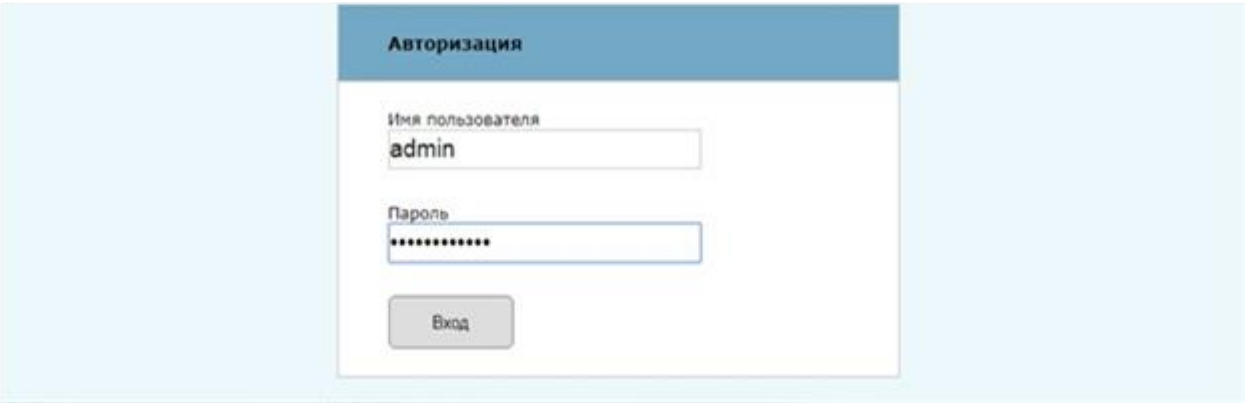
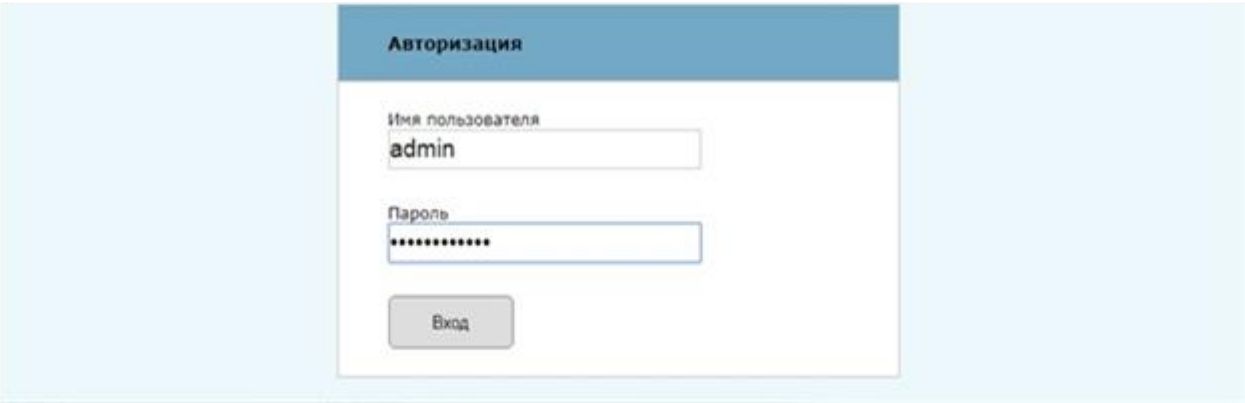


Рисунок 1. Вход в web-интерфейс

После успешной авторизации откроется интерфейс



и основное раздел «Наблюдение».

3.2 Работа с web-интерфейсом

Главным разделом в интерфейсе СПК «Сонар-1М» является - «Наблюдение». В данном разделе отображается обобщенная информация по всем инцидентам безопасности. Разделы «Инциденты», «IP-адреса», «Геолокация» содержат статистическую информацию по всем зафиксированным событиям. Инструменты для проведения детального анализа инцидентов собраны в разделе «Отчеты».

Под кнопками разделов интерфейса расположена временная шкала соответствующая дате отображаемой информации об инцидентах безопасности (см. Рисунок 2). По умолчанию отображается информация за текущий день. Дата на временной шкале может быть переключена на другое число месяца, другой месяц или год.

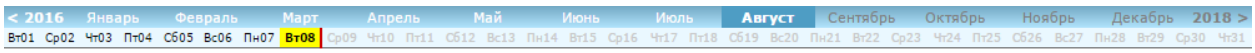


Рисунок 2. Временная шкала.

3.2.1 Раздел «Наблюдение»

В данном разделе отображается обобщенная информация по всем инцидентам безопасности, необходимая для оперативной оценки ситуации за выбранный день (см. Рисунок 3).

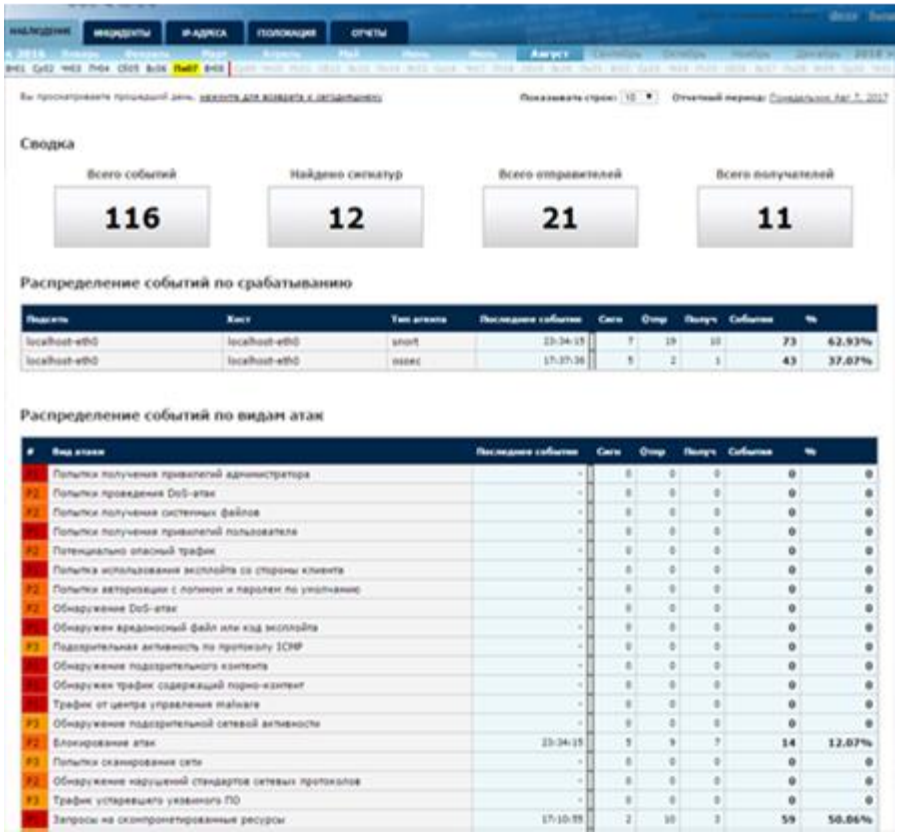


Рисунок 3. Раздел «Наблюдение»

Раздел состоит из нескольких логических частей:

1. Сводка – содержит следующие счетчики зарегистрированных событий, типов обнаруженных сигнатур, ip-адресов отправителей (src ip) и ip-адресов отправителей (dst ip).
2. Распределение событий по срабатыванию – содержит сводную информацию по агентам, регистрирующим события. Агент типа «snort» выполняет анализ трафика и обнаруживает вторжения и подозрительный трафик в сети. Агент типа «ossec» выполняет анализ системных журналов, ведет проверку целостности и обнаруживает атаки на сервер SONAR. Для каждого агента отображается: последнее зарегистрированное событие, набор счетчиков и процент в общем количестве инцидентов.

3. Распределение событий по видам атак – содержит сетку типов атак и для каждого типа отображается последнее зарегистрированное событие, набор счетчиков и процент в общем количестве инцидентов.
4. Топ сигнатур – содержит 10 наиболее часто срабатывающих сигнатур за выбранный день. Для каждого типа отображается последнее зарегистрированное событие, набор счетчиков и процент в общем количестве инцидентов.
5. Топ IP отправителей – содержит 10 ip-адресов отправителей (ip src), с которых наиболее часто регистрировался подозрительный трафик в течение выбранного дня. Для каждого ip-адреса отображается страна (либо local если трафик является исходящем из внутренней сети), последнее зарегистрированное событие, набор счетчиков и процент в общем количестве инцидентов. ip-адрес 0.0.0.0 указывает на пакеты исходящие от сервера SONAR, зарегистрированные агентом типа ossec.
6. Топ IP получателей – содержит 10 ip-адресов получателей (ip dst), трафик направленный которым наиболее часто регистрируется системой обнаружения вторжений в течение выбранного дня.. Для каждого ip-адреса отображается страна (либо local если трафик является исходящем из внутренней сети), последнее зарегистрированное событие, набор счетчиков и процент в общем количестве инцидентов. ip-адрес 0.0.0.0 указывает на пакеты исходящие от сервера SONAR, зарегистрированные агентом типа ossec.

Набор счетчиков для каждого пункта сетки содержит следующие поля:

- «Сигн» – количество найденных сигнатур угроз;
- «Отпр» – количество ip-адресов отправителей (ip src);
- «Получ» – количество ip-адресов получателей (ip dst);
- «События» – количество зарегистрированных событий;
- «%» – процент в общем количестве инцидентов.

3.2.2 Раздел «Инциденты»

В данном разделе отображаются круговые диаграммы, позволяющие визуализировать статистику по зафиксированным событиям за выбранный день (см. Рисунок 4). Информация данного раздела предназначена для выявления попыток сетевых атак и определения вида этих атак.

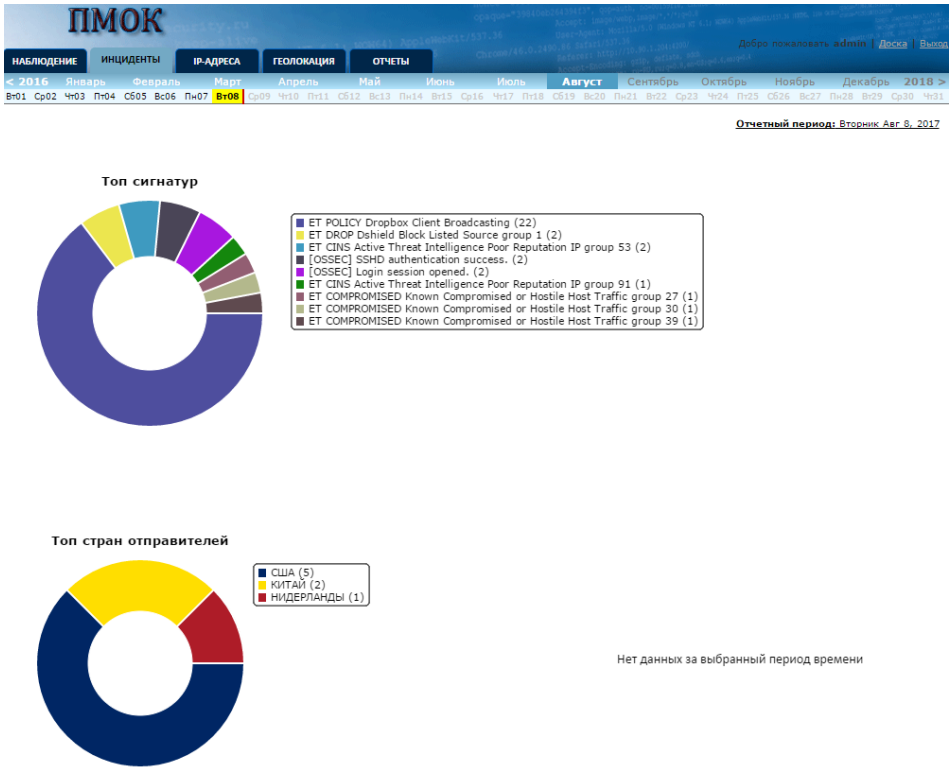


Рисунок 4. Раздел «Инциденты»

В разделе отображаются следующие три круговые диаграммы:

1. Топ сигнатур – диаграмма отображает найденные сигнатуры угроз. Объем каждой из сигнатур являются процентным соотношением от общей совокупности. Количество срабатываний каждой из зарегистрированных сигнатур отображается в легенде.
2. Топ стран отправителей – диаграмма отображает страны (исходя их информации об ip-адресе), от которых наиболее часто регистрировался подозрительный входящий трафик. Объем каждой из стран является процентным соотношением от общей совокупности. Количество ip-адресов отправителей (ip src) для каждой страны отображается в легенде.

3. Топ стран получателей – диаграмма отображает страны (исходя их информации об ip-адресе), для которых наиболее часто регистрировался подозрительный исходящий трафик. Объем каждой из стран является процентным соотношением от общей совокупности. Количество ip-адресов получателей (ip dst) для каждой страны отображается в легенде.

Условием построения диаграммы является: значения должны быть больше нуля. Если за выбранный день накопленные данные отсутствуют, то отображается сообщение «Нет данных за выбранный период времени».

3.2.3 Раздел «IP-адреса»

В данном разделе отображаются гистограммы, совмещенные с точечными диаграммами и круговые диаграммы (см. Рисунок 5). Собранная информация позволяет выделить ip-адреса с которых в течение выбранного дня отправлялся подозрительный трафик и выделить атакованные ip-адреса и порты.

Рисунок 5.Раздел «IP-адреса»

В разделе отображаются следующие гистограммы:

1. Топ IP отправителей – гистограмма отражает частоту появления событий для ip-адресов отправителей (ip src). Данные адреса могут быть адресами потенциальных нарушителей. Совмещенная точечная диаграмма показывает количество обнаруженных сигнатур и количество получателей, которым направлялся подозрительный трафик.
2. Топ IP получателей – гистограмма отражает частоту появления событий для ip-адресов получателей (ip dst). Данные адреса могут быть адресами потенциальных атакуемых хостов. Совмещенная точечная диаграмма показывает количество обнаруженных сигнатур и количество отправителей, с которых был направлен подозрительный трафик.
3. Топ IP-портов отправителей – гистограмма отражает частоту появления событий для портов отправителей. Данные порты могут быть портами, по которым работают потенциальные нарушители.

Совмещенная точечная диаграмма показывает количество обнаруженных сигнатур и количество получателей, которым направлялся подозрительный трафик.

4. Топ IP получателей – гистограмма отражает частоту появления событий для портов получателей (ip dst). Данные порты могут быть портами, по которым ведется сетевая атака. Совмещенная точечная диаграмма показывает количество обнаруженных сигнатур и количество отправителей, с которых был направлен подозрительный трафик.

IP-адрес 0.0.0.0 и нулевой порт указывают на события зарегистрированные агентом типа ossec.

Круговые диаграммы «Топ стран отправителей» и «Топ стран получателей» повторяют информацию из раздела «Инциденты». Условием построения диаграммы является: значения должны быть больше нуля. Если за выбранный день накопленные данные отсутствуют, то отображается сообщение «Нет данных за выбранный период времени».

3.2.4 Раздел «Геолокация»

В данном разделе отображается карта мира с выделенными странами с которыми зарегистрирован информационный обмен (см. Рисунок 6). Данный раздел позволяет определить страну из которой ведется сетевая атака.

Рисунок 6. Раздел «Геолокация»

Данный раздел позволяет определить страну из которой ведется сетевая атака.

Для каждой страны ведется набор счетчиков:

- «Отправителей» – количество ip-адресов отправителей (ip src);
- «Получателей» – количество ip-адресов получателей (ip dst);
- «Всего» – общее количество хостов участвующих в информационном обмене.

3.2.5 Раздел «Отчеты»

В данном разделе собраны инструменты для проведения детального анализа событий (см. Рисунок *7*Рисунок *7*. В отличие от других разделов, статистика по зафиксированным событиям может быть сформирована за

различный период времени (минуты, часы, дни, месяцы, годы). Поскольку отчетная информация может содержать большой объем данных, раздел рекомендуется использовать после определения потенциальных адресов нарушителей, потенциальных адресов хостов подвергшимся атакам и портов или после определения типа атаки.

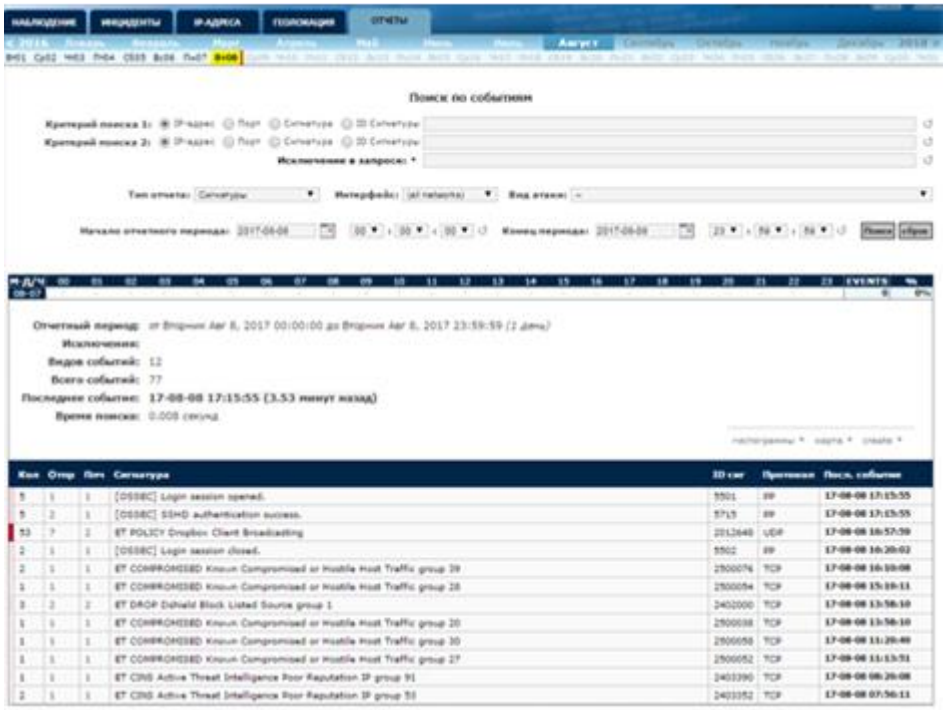


Рисунок 7. Раздел «Отчеты»

Для повышения эффективности работы с отчетной информацией присутствуют инструменты для формирования выборки по событиям, зарегистрированным за отчетный период времени. Выборка настраивается в блоке «Поиск по событиям» следующими компонентами:

1. Критерии поиска. Можно выполнить поиск по ip-адресу (отправителя или получателя), порту (отправителя или получателя), названием сигнатуры, либо по цифровому идентификатору сигнатуры (ID Сигнатуры). Реализована возможность задавать одновременно два критерия поиска, но параметры поиска при этом должны различаться. Для задания диапазона параметров должна применяться маска.
2. Исключения в запросе. Исключения функционально противоположны критериям поиска. При выполнении поиска можно

исключить события по ряду параметров: название сигнатуры (sig), цифровой идентификатор сигнатуры (sig_id), агент (sen_id), ip-адрес отправителя (src_ip), ip-адрес получателя (dst_ip), порт отправителя (src_port) или порт получателя (dst_port). Для задания диапазона параметров может применяться маска. В примере ниже исключаются события по протоколу http и события из одной внутренней подсети:

```
dst_port=80;src_ip=10.10.10.%;dst_ip=10.10.10%
```

3. Тип отчета. Определяет тип проводимой выборки и отображаемые результаты. Доступны варианты:
    - «Сигнатуры». Вариант отчета по умолчанию. События в отчете будут сгруппированы по названиям сигнатур. Для каждого пункта сетки формируются данные: количество событий (колонка «Кол»), количество уникальных для данного события ip-адресов отправителей (колонка «Отпр») и ip-адресов получателей (колонка «Плч»), цифровой идентификатор сигнатуры, протокол и последнее зарегистрированное событие.
    - «Сигнатуры и ip-адреса». События в отчете будут сгруппированы по названиям сигнатур и ip адресам. Для каждого пункта сетки формируются данные: количество событий (колонка «Кол»), код страны, цифровой идентификатор сигнатуры и последнее зарегистрированное событие.
    - «Детализация событий». В отчете выводятся события без группировки, отсортированные по времени. Для каждого пункта сетки формируются данные: вид (уровень угрозы), время регистрации события, ip-адрес и порт получателя, ip-адрес и порт отправителя, страна, названием сигнатуры, цифровой идентификатор сигнатуры. При нажатии на время события будет отображена детальная информация по соответствующему событию.
4. Интерфейс. Определяет тип агента, события от которого будет включены в отчет. Тип «snort» соответствует агенту системы обнаружения вторжений. Тип «ossec» соответствует агенту модуля

обеспечения собственной защиты SONAR. При выборе типа «Network» в отчет будут помещены события зарегистрированные обоими агентами.

5. Вид атаки. Определяет атаку, события по которой будут помещены в отчет.
6. Отчетный период. Позволяет задавать интервал времени, за который требуется просмотреть зарегистрированные события.

По завершению задания критериев следует нажать кнопку «Поиск», после чего будет сформирован отчет. Для сброса критериев в исходное значение следует нажать копку «Сброс». Сформированный отчет содержит сводную информацию об отчете, временную линию событий и сетку событий (см. Рисунок *7*Рисунок *7*.

На временной линии событий (см. Рисунок *8*) строчки соответствуют дням заданного периода, столбцы соответствуют часам регистрации событий. Красный цвет ячеек определяет количество событий за выбранный час, более темный тон означает большое количество событий. При нажатии на ячейку будут отображены события за выбранный час. Дополнительно, на временной линии отображается общее количество событий безопасности за день и процентное соотношение за весь период.

Рисунок 8.Временная линия событий

В области сводной информации об отчете, в нижней части можно нажать на копку «гистограммы» (см. Рисунок *9*), откроется блок гистограмм сформированных по выборке:

- Гистограмма «Распределение по протоколам» отражает частоту появления событий по определенным протоколам.
- Гистограмма «Распределение по видам атак» отражает частоту появления событий с определенным классом угроз.
- Гистограмма «Распределение событий по часам» отражает частоту появления событий в зависимости от часа.

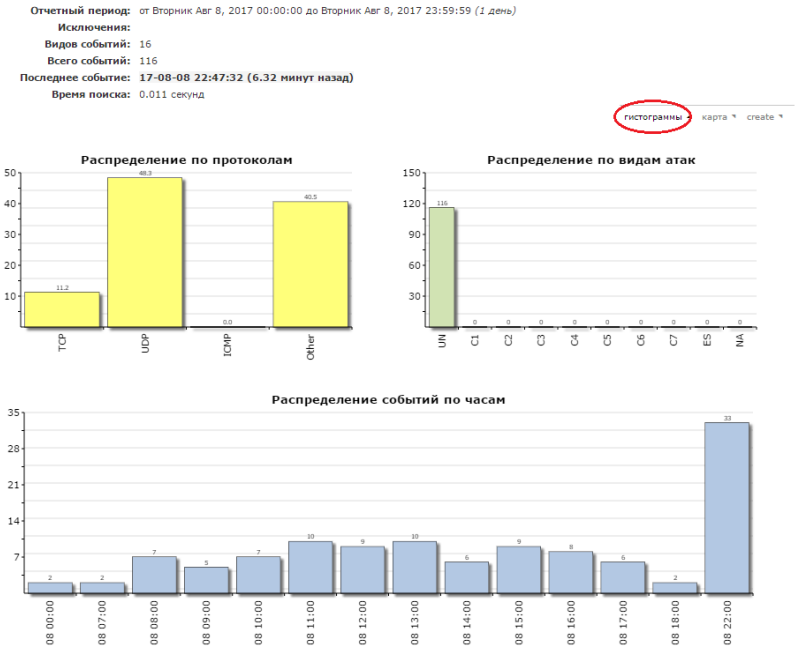


Рисунок 9. Построение гистограмм по отчетному периоду

3.2.6 Детализация выбранных событий

В интерфейсе SONAR реализована возможность просмотра события до уровня заголовочной информации IP пакетов. Детальный просмотр событий рекомендуется выполнять целенаправленно, имея информацию об ip-адресах, портах, приблизительного времени события или вида атаки.

Для детализации событий необходимо выполнить следующие действия (см. Рисунок *10*):

- перейти в раздел «Отчеты»;
- задать критерии выборки (рекомендуется);
- выбрать тип отчета - Детализация событий;
- нажать кнопку «Поиск»;
- в появившейся сетке событий нажать на время регистрации необходимого события (колонка «Время»);
- откроется новое окно, содержащее детальную информацию о событии.

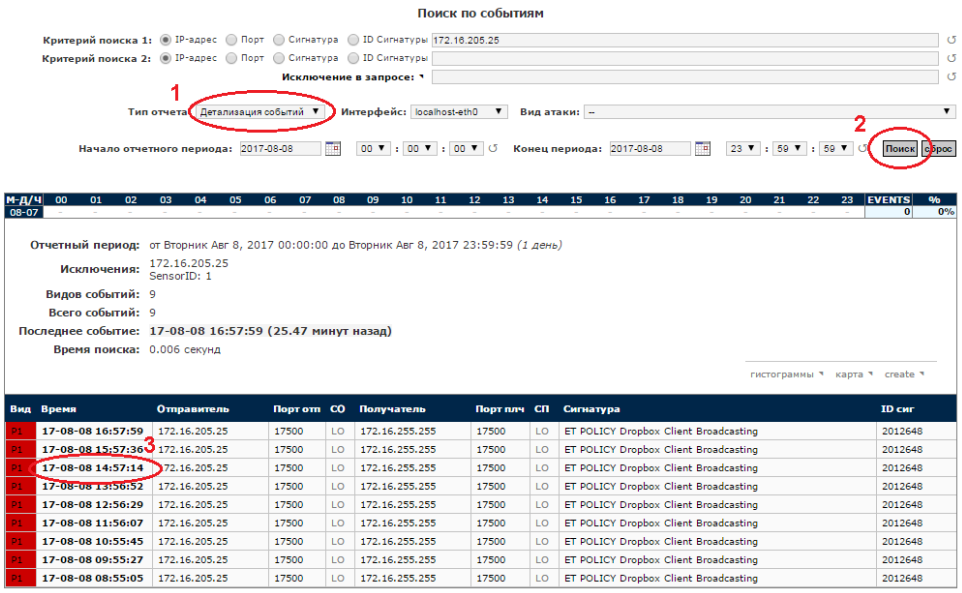


Рисунок 10. Выбор события для детализации

Окно детальной информации события (см. Рисунок *11*) имеет несколько разделов. В первом разделе, называемом «Инфо» содержится информация о времени события, сигнатуре события, идентификаторе агента (интерфейса) зарегистрировавшем событие и уникальном номере события в базе данных. Другие разделы отражают IP, TCP/UDP заголовки пакета вызвавшего событие безопасности и полезную нагрузку при её наличии. Полезная нагрузка отображается в шестнадцатеричном виде и в раскодированном виде (ASCII).

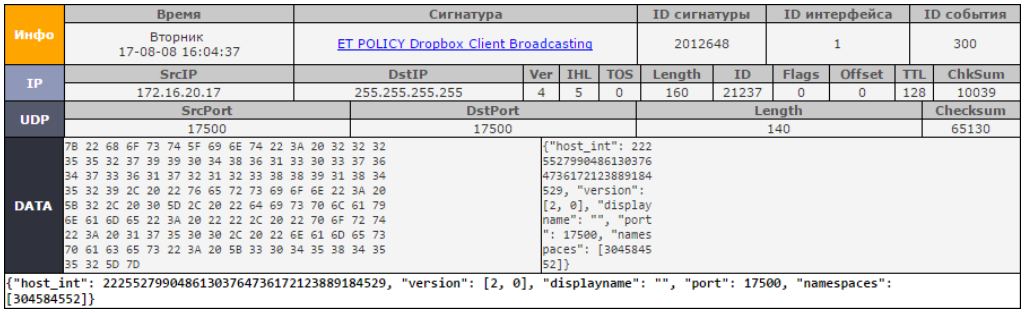


Рисунок 11. Окно детальной информации события

Из окна детальной информации события можно просмотреть правило его вызвавшее. Для этого необходимо нажать на название сигнатуры, откроется окно просмотра правила (см. Рисунок *12*). В данном окне отображено правило (в том виде, в котором оно описано в rules-файлах т.е. в формате snort) с указанием файла правила и строчки.

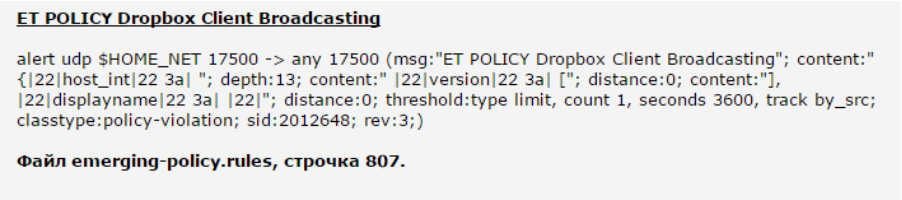


Рисунок 12. Окно просмотра правила

3.3 Управление службой СПК «Сонар-1М»

Программный комплекс SONAR-Framework состоит из нескольких компонентов, взаимодействующих друг с другом, сведенных в одну серверную службу. Для управления службой необходимо подключится к командной строке сервера, на котором установлен SONAR. Запуск службы выполняется автоматически при старте операционной системы.

Команда запуска службы SONAR-Framework

```
service SONAR start
```

Команда останова службы SONAR-Framework

```
service SONAR stop
```

Команда перезапуска службы SONAR-Framework

```
service SONAR restart
```

Просмотр состояния службы SONAR-Framework

```
service SONAR status
```

4. СООБЩЕНИЯ ОПЕРАТОРУ

Программный комплекс СПК «Сонар-1М» в процессе функционирования выдаёт ряд сообщений. Эти сообщения информируют оператора о состоянии приложения

4.1 Сообщения при входе в web-интерфейс

Сообщение «Неправильное имя пользователя или пароль» отображается при вводе неправильного имени пользователя или пароля при входе в веб-интерфейс. Учетная запись по умолчанию логин – admin, пароль – SONAR12345678. Управление учтенными записями выполняется в соответствии с руководством администратора SONAR.

Сообщение «Connection Failed» свидетельствует об ошибке, возникшей при подключении к базе данных mysql. Для устранения причины необходимо подключится к командной строке сервера, на котором установлен SONAR, и далее проверить настройки подключения web-интерфейса к базе данных. Настройки подключения хранятся в файле /var/www/html/SONAR/.inc/ config.php.

4.2 Названия сигнатур в событиях

Названия сигнатур содержатся в каждом зарегистрированном событии. Агент модуля обеспечения собственной защиты SONAR помечает сигнатуры префиксом [OSSEC], остальные сигнатуры относятся к системе обнаружения вторжений.

Модуль обеспечения собственной защиты SONAR отслеживает системные журналы сервера, сообщения из данных журналов соответствуют названиям сигнатур в событиях безопасности.

Модуль системы обнаружения вторжений помещает в название сигнатуры сообщение, выдаваемое при срабатывании правила. Данное сообщение задается опцией «msg» присутствующей в каждом правиле.