

Руководство пользователя ASoar

Оглавление

Оглавление	1
Системные требования	2
Архитектура и состав системы	3
Установка и развертывание	4
1. Подключение к системе (руководство по установке)	4
2. Главная (Dashboard)	5
3. Устройства (Devices)	6
4. Действия (Actions)	7
5. Списки (Lists)	8
6. Политики (Policies)	9
7. Список разрешений (Allowlist)	10
8. Журналы (Logs)	11
9. Попытки входа (Hostline login attempts)	12
Подключение логов	13
Обновление системы	14
Удаление системы	15

Лицензирование и оплата

Стоимость основана на количестве защищаемых узлов системы. Подробнее с вопросами о стоимости можно обратиться к представителям сертифицированных интеграторов.

Системные требования

В данном разделе представлены требования, предъявляемые к аппаратному и программному обеспечению при развертывании ASoar

1.1. Аппаратное обеспечение

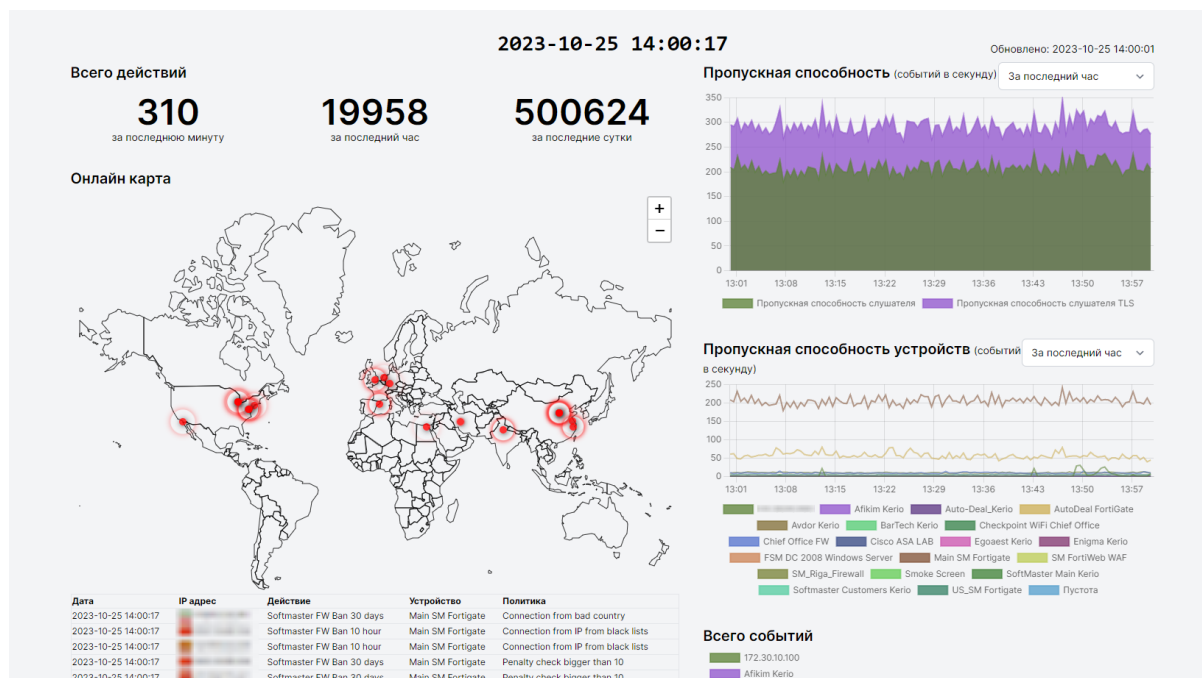
Архитектура процессора	Любая, поддерживающая ОС сервера.
Аппаратное обеспечение	от 8 потоков процессора, от 8 GB RAM, 1 TB в системе хранения. Точные характеристики выявляются в зависимости от количества инцидентов и сценариев реагирования.
Возможность установки обновлений без доступа к Интернет	Да
Архитектура приложения	Модульная

1.2. Программное обеспечение

ОС	Ubuntu 20 и выше, Astra Linux CE, AltLinux, Альт
СУБД	PostgreSQL, ClickHouse, Redis
Клиентское ПО	Веб-браузер

Руководство для конечных пользователей

Главная (Dashboard)



Панель с выводом общей информации по работе системы. Дашборд дает общее представление о работоспособности по системе. Правила, которые дают показания на дашборде настраиваются в разделе Policies.

Всего действий (Actions Totals)

Указывает количество зафиксированных инцидентов за последнюю минуту, час и 24 часа.

Онлайн карта (Live Action Map)

Наглядно демонстрирует географию источников угроз. Под картой расположена таблица с зафиксированными инцидентами, обновляющаяся в режиме реального времени.

Пропускная способность (Total Throughput)

График показывает общую пропускную способность системы.

Пропускная способность устройств (Devices Throughput)

График показывает общее количество зафиксированных инцидентов по каждому устройству.

Всего событий (Total Events)

Круговая диаграмма, которая показывает общее количество событий по каждому устройству.

Попытки входа (Hostile Login attempts detected - 10 Latest)

Список зафиксированных пар логин-пароль, которые были скомпрометированы.

Действий за минуту (Actions per minute)

График по количеству совершенных действий в отношении IP-адресов источников.

Устройства (Devices)

ID	Название ↑	IP устройства	Тип	Первое сообщение	Статус
	<input type="text" value="Название"/>	<input type="text" value="IP устройства"/>	<input type="text" value="Выберите тип"/>		<input type="text" value="Выбор..."/>
10062	Сетевая камера	192.168.1.100	Сетевая камера	2023-08-25T17:39:27Z	Разрешено
10059	Сетевая камера	192.168.1.101	Сетевая камера	2023-04-10T14:50:50Z	Неизвестно
10061	Сетевая камера	192.168.1.102	Сетевая камера	2023-05-23T14:10:06Z	Неизвестно
18	Сетевая камера	192.168.1.103	Сетевая камера	2022-06-21T11:01:20Z	Разрешено
10060	Сетевая камера	192.168.1.104	Сетевая камера	2023-04-18T19:20:23Z	Разрешено
15	Сетевая камера	192.168.1.105	Сетевая камера	2022-06-21T10:59:18Z	Разрешено
19	Сетевая камера	192.168.1.106	Сетевая камера	2022-06-21T11:01:27Z	Разрешено
20	Сетевая камера	192.168.1.107	Сетевая камера	2022-06-21T11:01:40Z	Разрешено
30	Сетевая камера	192.168.1.108	Сетевая камера	2023-02-16T22:36:06Z	Разрешено
27	Сетевая камера	192.168.1.109	Сетевая камера	2022-12-07T11:44:25Z	Разрешено
29	Сетевая камера	192.168.1.110	Сетевая камера	2023-01-09T23:18:50Z	Запрещено
24	Сетевая камера	192.168.1.111	Сетевая камера	2022-12-05T14:49:10Z	Разрешено
14	Сетевая камера	192.168.1.112	Сетевая камера	2022-06-21T10:59:08Z	Запрещено
22	Сетевая камера	192.168.1.113	Сетевая камера	2022-06-21T12:15:50Z	Разрешено
17	Сетевая камера	192.168.1.114	Сетевая камера	2022-06-21T10:59:50Z	Разрешено

Показано 1 - 15 из 23 записей

15 на страницу

Список устройств, подключенных к системе ASoar. Здесь видны все устройства, которые отправляют логи в ASoar. Также в рамках ASoar каждому устройству присваивается свой уникальный IP-адрес.

Примечания

Для добавления нового типа устройств в систему ASoar, обратитесь к представителям сертифицированных интеграторов.

Действия (Actions)

В разделе «Действия» создаются действия, которые будут выполняться по достижению определенных условий правил (раздел «Правила» (Policies)).

ID	Название ↑	Тип	Параметры	Ссылки	Статус	Принудительно	Главная
	<input type="text" value="Имя"/>	<input type="text" value="Выберите тип"/>			<input type="text" value="..."/>	<input type="text" value="..."/>	
15	Add External IP to Ignore List	add_to_list	Добавить в список: 7		Активно	Нет	Скрытый
13	Add to Detected by Bad Outbound connections	add_to_list	Добавить в список: 5		Активно	Да	Скрытый
12	Add to list of mail attackers	add_to_list	Добавить в список: 3		Активно	Нет	Скрытый
11	Add to SDefender block list	add_to_list	Добавить в список: 1		Активно	Нет	Скрытый
2	Increase penalty by 1	increase_penalty	Величить на: 1	Штрафы	Активно	Нет	Скрытый
3	Increase penalty by 3	increase_penalty	Величить на: 3	Штрафы	Активно	Нет	Показано
8	Riga SoftMaster Firewall 10 hours ban	fortigate_ban	Адрес Fortigate: https://195.13.202.242:28485/ Таймаут: 36000	Карантинный список	Активно	Нет	Скрытый
9	Riga SoftMaster Firewall 30 days ban	fortigate_ban	Адрес Fortigate: https://195.13.202.242:28485/ Таймаут: 2419200	Карантинный список	Активно	Нет	Скрытый
14	Send e-mail to chief@soft-master.com	email_notification	Отправить: chief@soft-master.com		Активно	Да	Скрытый
16	Send e-mail to mark@sdefender.com	email_notification	Отправить: mark@sdefender.com		Активно	Да	Скрытый
5	Send e-mail to support@soft-master.com	email_notification	Отправить: support@soft-master.com		Активно	Да	Показано
4	Softmaster FW Ban 10 hour	fortigate_ban	Адрес Fortigate: https://172.20.10.254:28485/ Таймаут: 36000	Карантинный список	Активно	Нет	Показано
1	Softmaster FW Ban 30 days	fortigate_ban	Адрес Fortigate: https://172.20.10.254:28485/ Таймаут: 2419200	Карантинный список	Активно	Нет	Показано
10	Softmaster FW Ban Debug	fortigate_ban	Адрес Fortigate: https://172.20.10.254:28485/ Таймаут: 3600	Карантинный список	Отладка	Нет	Скрытый

В данном разделе представлена таблица с действиями с возможностью отфильтровать действия по нужным параметрам:

- **Название (Name)**
Наименование действия
- **Тип (Choose device)**
Тип действия. Список доступных типов:
 - **Карантинный список Fortigate (fortigate_ban)**
Блокировка IP-адреса злоумышленника
 - **Увеличить штраф (increase_penalty)**
Увеличивает пенальти для ip-адреса на определенное количество
 - **Уведомление по электронной почте (email_notification)**
Уведомление на электронную почту
 - **Добавить в список (add_to_list)**
Добавляет объект в указываемый список
 - **Фид угроз Fortigate (fortigate_threat_feed)**
Групповая работа со списком IP-адресов
- **Статус (Status)**
Фильтр по статусам:
 - **Активно (Active)**
Действие находится в состоянии “активно”
 - **Отладка (Debug)**
Действие будет выполняться только в тестовом режиме. Они будут отображены в логах и в разделе Dashboard, но никаких санкций по отношению к источникам выполняться не будет.
- **Принудительно (Forced)**

Статус «Принудительно» отвечает за приоритет действия по отношению к Списку разрешенных. То есть, если у действия указано Принудительно= “Yes”, то IP-адрес, внесенный в список разрешенных, попадет под санкции данного действия.

В правом верхнем экране доступна кнопка создания нового действия «Создать новое действие».

Список доступных действий:

- **Добавить в карантин Fortigate**

Содержит следующие поля:

- Наименование действия
- Fortigate URL
- Fortigate API token
- Отключение ip-адреса на определенный период
- Список флагов (test connection, enable rate limiting и тд)

- **Добавить в список угроз Fortigate.**

Содержит следующие поля:

- Наименование действия
- Fortigate URL
- Fortigate API token
- Feed Name
- Отключение ip-адреса на определенный период
- Список флагов (test connection, enable rate limiting и тд)

- **Выдать штраф.**

Содержит следующие поля:

- Наименование действия
- Число, на которое повысить уровень штрафа
- Время сгорания штрафа
- Список флагов (Enable rate limiting; Ignore allowlist (action will be executed, even if the IP is in Allowlist); Enable debug mode (In debug mode action will not be executed); Don't show on dashboard)

- **Отправить уведомление на почту.**

Содержит следующие поля:




- Наименование действия
- Адрес, куда отправить уведомление
- Список флагов (Enable rate limiting; Ignore allowlist (action will be executed, even if the IP is in Allowlist); Enable debug mode (In debug mode action will not be executed); Don't show on dashboard)

- **Добавить в выбираемый список.**



Содержит следующие поля:

- Наименование действия
- Выбор списка
- Список флагов (Enable rate limiting; Ignore allowlist (action will be executed, even if the IP is in Allowlist); Enable debug mode (In debug mode action will not be executed); Don't show on dashboard)

В правом углу каждой строки созданного действия доступен функционал:

- Редактирование действия  .
- Удаление действия  .
- Функция принудительного выполнения действия на указанный ip-адрес  . Для этого:
 - Укажите ip-адрес к которому необходимо применить выбранное действие.
 - Нажмите кнопку **“Execute Action”**


Инструкция к использованию

1. Составьте список предполагаемых действий по отношению к отслеживаемым событиям.
 - 1.1. Нажмите кнопку **“Create new action”** .
 - 1.2. Определите необходимый вид действия:
 - 1.2.1. **Карантинный список Fortigate (fortigate_ban)**
 - 1.2.2. **Увеличить штраф (increase_penalty)**
 - 1.2.3. **Уведомление по электронной почте (email_notification)**
 - 1.2.4. **Добавить в список (add_to_list)**
 - 1.2.5. **Фид угроз Fortigate (fortigate_threat_feed)**
 - 1.3. Выберите вид действия и заполните поля
 - 1.4. Нажмите кнопку **“Save”** для сохранения
2. Для редактирования действия нажмите кнопку  .
3. Для удаления действия нажмите кнопку  .

Списки (Lists)

В разделе Lists создаются пользовательские списки, которые делятся на списки ручного заполнения и автоматического заполнения. Каждый список состоит из записей IP-адресов, полученных ручным или автоматическим путем.

В каждый список можно дополнить адреса вручную нажав на кнопку редактирования

списка  и кнопку **“Добавить запись”**

Ручной список (manual list)

В списки ручного заполнения попадают IP-адреса, которые прошли по условиям раздела Policies или были добавлены в ручную по кнопке **“Добавить запись”**

Примеры:

1. Заполненный список можно использовать в ASoag для защиты других сетей от уже известных угроз.
2. Мы заранее знаем IP-адрес источника угрозы и включаем его в список потенциальных угроз.

Автоматический список (Automatic List)

В автоматические списки попадают IP-адреса источников угрозы из открытых источников.

Примеры:

1. Полученный список можно использовать для предотвращения события угрозы еще до его возникновения.

Инструкция к использованию:



1. Составьте ручные или автоматические списки, в которые будут попадать IP-адреса после указанных «Действий»

Списки

ID	Название ↑	Описание	Тип	Обновлено в
	<input type="text" value="ИМЯ"/>		<input type="text" value="Выберите тип списка"/>	
5	1_Detected by Bad Outbound connections		manual	2023-03-05 12:18:21
9	Binary Defense List		automatic [ip]	2023-10-25 04:25:01
1	Blocked by SDefender	Our own blocks.	manual	2023-02-06 13:09:29
4	blocklist.de		automatic [any]	2023-10-25 04:25:01
10	Denied by Checkpoint		manual	2023-08-24 19:53:41
7	Detected External IP to ignore		manual	2023-02-23 11:08:54
3	Mail attackers		manual	2023-02-02 23:15:52
8	Maltrail IPSum List		automatic [ip]	2023-10-25 04:25:09
6	talosintelligence.com IP black list		automatic [ip]	2023-10-25 04:25:02

Показано 1 - 9 из 9 записей на страницу

1.1. Ручной список:

- 1.1.1. Нажмите кнопку **“Создать новый список”**
 - 1.1.2. Выберите тип списка **“Ручной”**
 - 1.1.3. Укажите название списка и его описание
 - 1.2. Автоматический список:
 - 1.2.1. Нажмите кнопку **“Создать новый список”**
 - 1.2.2. Выберите тип списка **“Автоматический”**
 - 1.2.3. Укажите название списка
 - 1.2.4. Укажите удаленный URL
 - 1.2.5. Выберите тип списка
 - 1.2.5.1. **“Любой”**
 - 1.2.5.2. **“IP”**
 - 1.2.6. Укажите описание списка
2. Для редактирования списка нажмите кнопку  у каждого списка на экране просмотра всех списков
3. Для удаления списка нажмите кнопку  у каждого списка на экране просмотра всех списков

Политики (Policies)

Каждая политика — это набор правил и действий, направленных на определенный тип логов. Правило — это логическая конструкция на основе атрибутов события, атрибуты можно проверять в различных предустановленных списках, применять к атрибутам регулярные выражения и делать простые логические и арифметические операции. Правила можно объединять в группы по принципу «и», «или» используя операторы OR, AND. Действия также можно вызывать по синтаксису похожему на вызов функций.

ID	Название ↑	Устройства	Фильтры	Действия
21	Attack detected by firewall	<input type="text" value="Имя"/> Выберите устройство	srcintfrole - eq - wan and action - eq - detected	Выберите дейс... FW 10 hour ban [fortigate_ban] Add to SDefender block list [add_to_list] Send e-mail to [email_notification] Firewall 10 hours ban [fortigate_ban] FW Ban 10 hour [fortigate_ban]
22	Attack detected by WAF		type - eq - attack and message - not_contains - matomo.php and message - not_contains - attack_type="Information Disclosure"	Firewall 30 days ban [fortigate_ban] FW Ban 30 days [fortigate_ban] Add to block list [add_to_list] Ban 30 days [fortigate_ban]

Примеры:

1. Для предполагаемых угроз мы заранее составляем правило, которое будет отбирать угрозы в определенный список и выдавать Penalty по IP-адресу.



3	Добавить в список и повысить пенальти	Enigma Kerio(172.30.10.186) [kerio] Enigma Kerio(172.44.10.3) [kerio]	message - contains - exited	up penalty by 1 for 1 day [increase_penalty] add to test list [add_to_list]	✎ 🗑
---	---------------------------------------	--------------------------------------------------------------------------	-----------------------------	--------------------------------------------------------------------------------	-----

2. При многократной попытке ввода неверного пароля система будет выдавать временный бан с уведомлением пользователя по Email

4	Временный бан за многократную попытку ввода неверного пароля	172.20.10.100(172.20.10.100) [kerio]	message - contains - SMTP: Invalid password for user	Notify [email_notification] Ban [fortigate_ban]	✎ 🗑
---	--------------------------------------------------------------	--------------------------------------	------------------------------------------------------	----------------------------------------------------	-----

Инструкция к использованию

1. Составьте правила, по которым будут отбираться логи и что с ними нужно сделать.
 - 1.1. Нажмите кнопку **“Добавить политику”**
 - 1.2. Введите имя правила
 - 1.3. Выберите устройства для которых будет распространяться правило (можно выбрать несколько)
 - 1.4. Выберите оператор **“И”** или **“ИЛИ”**, который будет объединять условия.
 - 1.4.1. **“И”** - все условия должны быть выполнены
 - 1.4.2. **“ИЛИ”** - хотя бы одно из условий должно быть выполнено
 - 1.5. Добавьте все необходимые условия, нажимая кнопку **“Add filters”** или выбирая из шаблонов

- 1.6. Кнопка **“Добавить фильтр”** вызовет несколько полей, каждое из которых необходимо заполнить:
 - 1.6.1. Выберите атрибут по которому будет составлено условие
 - 1.6.2. Выберите оператор для выбранного атрибута
 - 1.6.3. Укажите значение атрибута для положительного исхода условия
- 1.7. Выберите действия из списка (Action ids), которые будут выполняться при положительном исходе правила (можно выбрать несколько)
- 1.8. Нажмите кнопку **“Сохранить”** для сохранения
2. Для редактирования правила нажмите кнопку 
3. Для удаления правила нажмите кнопку 

Список разрешений (Allowlist)

Добавление IP-адресов в “белый” список, который будет игнорироваться правилами и действиями, кроме действий со статусом “Принудительно”.

Примечания

Параметр “Принудительно” у действия игнорирует список Allowlist.

Журналы (Logs)

Данный раздел предоставляет доступ к инструментам работы с логами («живые журналы» и «просмотр журналов»).

При заходе в данный раздел доступна таблица поступающих на обработку системе логов в реальном времени (Живые журналы).

Справа доступна кнопка для переключения режимов работы:

- работа в режиме просмотра логов в режиме реального времени

Живые журналы						⏸ Остановить
Время	Устройство	Тип	IP источника	IP получателя	Порт назначения	
2023-10-25 14:22:05	192.168.1.100	traffic	192.168.1.1	192.168.1.100	5060	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	9080	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	9080	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	57691	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	53	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	53	
2023-10-25 14:22:04	192.168.1.100	event	192.168.1.1		0	
2023-10-25 14:22:04	192.168.1.100	event	192.168.1.1		0	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	35797	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	58111	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	514	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	514	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	514	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	6344	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	25565	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	514	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	514	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	514	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	514	
2023-10-25 14:22:04	192.168.1.100	traffic	192.168.1.1	192.168.1.100	514	

- работа в режиме просмотра журналов

Просмотр журналов ⏪ Запустить

Время от: 2023-10-25 13:52:41 до: 2023-10-25 14:22:41

Время	Устройство	Тип	IP источника	IP получателя	Порт назначения	Действие
	<input type="text" value="Выберите устройство"/>	<input type="text" value="тип"/>	<input type="text" value="Фильтр IP"/>	<input type="text" value="Фильтр IP"/>	<input type="text" value="Порт"/>	<input type="text" value="Действие"/>
> 2023-10-25 14:22:40	ASUS ROG Strix	event	192.168.1.100	<input type="checkbox"/>	0	ban-ip
> 2023-10-25 14:22:40	ASUS ROG Strix	event	192.168.1.100	<input type="checkbox"/>	0	ban-ip
> 2023-10-25 14:22:40	ASUS ROG Strix	event	192.168.1.100	<input type="checkbox"/>	0	ban-ip
> 2023-10-25 14:22:40	ASUS ROG Strix	event	192.168.1.100	<input type="checkbox"/>	0	ban-ip
> 2023-10-25 14:22:40	ASUS ROG Strix	event	192.168.1.100	<input type="checkbox"/>	0	ban-ip
> 2023-10-25 14:22:40	ASUS ROG Strix	traffic	192.168.1.100	192.168.1.100	443	client-rst
> 2023-10-25 14:22:40	ASUS ROG Strix	traffic	192.168.1.100	192.168.1.100	5060	accept
> 2023-10-25 14:22:40	ASUS ROG Strix	traffic	192.168.1.100	192.168.1.100	4481	accept
> 2023-10-25 14:22:40	ASUS ROG Strix	traffic	<input type="checkbox"/>	192.168.1.100	4806	accept
> 2023-10-25 14:22:40	ASUS ROG Strix	traffic	<input type="checkbox"/>	<input type="checkbox"/>	6970	timeout
> 2023-10-25 14:22:40	ASUS ROG Strix	traffic	<input type="checkbox"/>	<input type="checkbox"/>	6970	ip-conn
> 2023-10-25 14:22:40	ASUS ROG Strix	traffic	<input type="checkbox"/>	<input type="checkbox"/>	53	accept
> 2023-10-25 14:22:40	ASUS ROG Strix	traffic	<input type="checkbox"/>	<input type="checkbox"/>	53	ip-conn
> 2023-10-25 14:22:40	ASUS ROG Strix	traffic	<input type="checkbox"/>	<input type="checkbox"/>	53	accept
> 2023-10-25 14:22:40	ASUS ROG Strix	traffic	<input type="checkbox"/>	192.168.1.100	53	accept

Показано 1 - 15 из 523066 записей на странице >

Live Logs

В данном режиме таблица отображает все поступающие в систему логи в режиме реального времени, отображая следующие столбцы в таблице:

- **Время**
Время поступления лога в систему
- **Устройство**
Имя устройства, породившего события из списка устройств, настраиваемых во вкладке «Devices»
- **Тип**
Тип события лога
- **IP источника**
IP адрес источника соединения, которое привело к журналируемому действию
- **IP получателя**
IP адрес адресата соединения, которое привело к журналируемому действию
- **Порт назначения**
Порт адресата соединения, которое привело к журналируемому действию

При управлении небольшой системой опытному пользователю бывает достаточно беглого взгляда на этот экран чтобы понять, что все системы работают в штатном режиме.

Примеры

1. Отсутствие ожидаемых логов от привычно работающей подсистемы говорит о ее недоступности или сетевой поломке.
2. Визуальный анализ столбца используемых портов системы покажет, какие сервисы сейчас используются в сети наиболее интенсивно

Просмотр журналов

Данный инструмент открывает доступ к журналу логов, поступающих в систему. При необходимости данный временной промежуток может быть изменен посредством фильтров. Фактически данный инструмент служит рабочим местом инженера обеспечения безопасности.

Есть возможность отфильтровать логи по нужным параметрам:

- **Время**
Смысл такой же, как и в режиме «Live Logs»
- **Устройство**
Смысл такой же, как и в режиме «Live Logs»
- **Тип**
Смысл такой же, как и в режиме «Live Logs»
- **IP источника**
Смысл такой же, как и в режиме «Live Logs»
- **IP получателя**
Смысл такой же, как и в режиме «Live Logs»
- **Порт назначения**
Смысл такой же, как и в режиме «Live Logs»
- **Действие**
Результат оценки работы системы, сгенерировавшей событие

Отдельные части строки каждого лога интерактивны, так например:

- крайняя левая часть отдана кнопке раскрытия строки лога, при нажатии на эту часть откроется полный просмотр залогированного сообщения
- справа от IP-адреса источника и IP-адреса назначения есть выпадающее меню.

Возможные действия:

- отфильтровать все логи по выбранному IP-адресу
- отчет по действиям выполненным в сторону выбранного IP-адреса
- запустить действие из списка, настраиваемого на вкладке «actions» в сторону выбранного IP-адреса
- добавить IP-адрес в белый лист
- NS Lookup показывает есть ли домены, зарегистрированные за данным IP адресом
- посмотреть отчет по выбранному IP-адресу на сервисах Virustotal, AbuseIPDB, Whois и IP Lookup

Просмотр журналов ⌂ Запустить

Время от: 2023-10-25 13:54:16 до: 2023-10-25 14:24:16

Время	Устройство	Тип	IP источника	IP получателя	Порт назначения	Действие	
2023-10-25 14:24:15	<input type="text" value="Выберите устройство"/>	<input type="text" value="тип"/>	<input type="text" value="Фильтр IP"/>	<input type="text" value="Фильтр IP"/>	<input type="text" value="Порт"/>	<input type="text" value="Действие"/>	
>	2023-10-25 14:24:15	Main SM Fortigate	traffic			876	deny
<div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>IP Logs as Source</p> <p>Как адрес назначения</p> <p>Отчет о действиях для IP</p> <p>Поиск по доменному имени</p> <p>Show on VirusTotal</p> <p>Показать на AbuseIPDB</p> <p>Whois</p> <p>Поиск по IP адресу</p> </div> <div style="width: 35%; border-left: 1px solid #ccc; padding-left: 10px;"> <p>IP Logs as Source</p> <p>Как адрес назначения</p> <p>Отчет о действиях для IP</p> <p>Поиск по доменному имени</p> <p>Show on VirusTotal</p> <p>Показать на AbuseIPDB</p> <p>Whois</p> <p>Поиск по IP адресу</p> </div> </div>							
>	2023-10-25 14:24:15	Main SM Fortigate	traffic			514	deny

Примеры

- Если есть подозрение, что какой-либо пользователь не может получить доступ к сервису по причине отказа от обслуживания, то можно произвести простейшее расследование, указав IP адрес пользователя и увидев результаты работы систем с его запросами. Если какие-либо из них отказывают в обслуживании — это будет отражено в логах.

Попытки входа (Hostile login attempts)

Список логинов и паролей, которые были скомпрометированы или с которыми допускались попытки взлома.

Скомпрометированные имя пользователя/пароли	
Имя пользователя	Пароль
<input type="text" value="Имя пользователя"/>	<input type="text" value="Пароль"/>
root	root
ubnt	ubnt
tech	tech
root	root
admin	admin
root	root
root	root
root	root
admin	admin
root	root
supervisor	supervisor
root	root
admin	admin
root	root
sa	sa

Показано 1 - 15 из 35619 записей 15 на страницу >

Руководство для опытных пользователей и интеграторов

Установка и развертывание

Подключение логов

Архитектура и состав системы

Обновление системы

Интеграция с внешними системами

Прекращение эксплуатации системы