MaxPatrol O2

Руководство администратора

Дата редакции документа: 12.01.2023

Содержание

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по администрированию MaxPatrol O2 (далее также — O2). Руководство также содержит инструкции по установке O2 и использованию основных функций продукта.

Руководство адресовано специалистам, администрирующим O2.

В этом разделе

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о O2

Вы можете найти дополнительную информацию о O2 на сайте ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов «Позитив Текнолоджиз», ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки.

2. О MaxPatrol O2

MaxPatrol O2 (O2) — система, предназначенная для автоматического обнаружения действий злоумышленников и предотвращения недопустимых событий в инфраструктуре предприятия.

O2 упрощает работу экспертов по ИБ, позволяя в одном окне увидеть последовательность хакерских действий и давая рекомендации о том, как остановить злоумышленника.

Ключевыми возможностями O2 являются:

- **Автоматическое определение цепочки подозрительных событий**. O2 анализирует события ИБ, происходящие в инфраструктуре предприятия, определяет связь между этими событиями и степень их опасности.
- **Интерфейс для анализа цепочек событий**. O2 содержит инструменты для анализа событий: схему и таймлайн атаки, визуализацию событий, подробную информацию о вовлеченных в атаку ресурсах и их свойствах.
- **Автоматизированный контроль реагирования**. С помощью набора статусов O2 помогает эксперту управлять реагированием на цепочки событий и показывает, остановлена ли атака в результате реагирования.

3. Состав компонентов ПО и его среды функционирования

В состав О2 входят следующие компоненты (все компоненты со свободной лицензией):

— реляционная система управления базами данных PostgreSQL;

— брокер сообщений RabbitMq;

— брокер сообщений Apache Kafka;

— система передачи данных Debezium;

— система индексирования и аналитики ElasticSearch;

— система централизованного конфигурирования Apache Zookeeper;

— сервер сообщений Schema Registry.

Среда функционирования ПО включает:

— операционную систему Debian версии 10 или 11;

— программное обеспечение для контейнеризации приложений Docker Engine версии 20.10 или выше;

— инструмент для запуска мультиконтейнерных приложений Docker Compose версии 1.28 или выше.

В таблице ниже дана информация о лицензиях компонентов ПО.

Таблица 2. Лицензии компонентов О2

Название компонента	**Лицензия**	**Правообладатель**	**Ссылка на текст лицензии**
PostgreSQL	PostgreSQL	1996—2022, PostgreSQL Global Development Group; 1994, The Regents of the University of California	postgresql.org
RabbitMQ	MPL-2.0	VMware, Inc. or its affiliates	rabbitmq.com/mpl.html
Apache Kafka	Apache License 2.0	Apache Software Foundation	https://www.apache.org/licenses/LICENSE-2.0

Название компонента	Лицензия	Правообладатель	Ссылка на текст лицензии
Debezium	Apache License 2.0	2021 by Red Hat, Inc	https://www.apache.org/licenses/LICENSE-2.0
ElasticSearch	Apache License 2.0	2022. Elasticsearch B.V	https://www.apache.org/licenses/LICENSE-2.0
Apache Zookeeper	Apache License 2.0	Apache Software Foundation	https://www.apache.org/licenses/LICENSE-2.0
Schema Registry	Confluent Community License Version 1.0	Confluent, Inc. 2014-2022	https://www.confluent.io/confluent-community-license/?_ga=2.6736306.1226577767.1670586679-1002194415.1657545498

4. Алгоритм работы O2

O2 работает в инфраструктуре, где развернута SIEM-система.

1. O2 получает от SIEM-системы корреляционные события ИБ (алерты), анализирует и фильтрует их и на основе правил объединяет в цепочки событий (или кейсы). Цепочки отражают последовательность подозрительных действий с ресурсами в инфраструктуре.
2. O2 рассчитывает их опасность с помощью функции скоринга и количество действий в инфраструктуре предприятия, оставшихся предполагаемому злоумышленнику до захвата ключевой системы и до воздействия на целевую систему (до наступления недопустимого события). Кроме того, O2 формирует диаграмму графа развития возможной атаки с визуальным отображением атакующих, атакованных и захваченных ресурсов.
3. Эксперт по информационной безопасности просматривает в O2 цепочки событий ИБ, анализирует агрегированную в них информацию и принимает решение о реагировании. Само реагирование (действия реагирования) в текущей версии O2 выполняется за пределами системы внешними средствами.

Таким образом, O2 предоставляет эксперту интерфейс для просмотра событий, прогнозирования действий злоумышленника и принятия решения о реагировании на атаку.

5. Роли пользователей

В O2 предусмотрены функциональные роли администратора системы и эксперта по ИБ.

Добавление новых пользователей, а также управление ролями пользователей в приложении O2 выполняется в интерфейсе интегрированного приложения Positive Technologies Management and Configuration (PT MC).

Администратор

Администратор выполняет мониторинг работы системы с помощью внутренних индикаторов статуса O2 и внешних решений для мониторинга, предоставляет диагностическую информацию поставщику O2. Кроме того, администратор обновляет систему, при необходимости настраивает ее после обновления, добавляет пользователей O2.

Эксперт по ИБ

Эксперт по ИБ в интерфейсе O2 проверяет цепочки событий, отмечает ложные срабатывания, принимает решение о необходимости реагирования, добавляет информацию о выполненном реагировании. Эксперт также валидирует правила, по которым события «склеиваются» в цепочки, и участвует в создании и доработке этих правил совместно с поставщиком. Эксперт не может управлять пользователями O2.

6. Развертывание O2

Этот раздел содержит описание предварительных условий для развертывания O2, а также инструкции по установке и первоначальной настройке.

В этом разделе

6.1. Аппаратные и программные требования

O2 рекомендуется устанавливать на чистую 64-разрядную операционную систему Debian версии 10.

Для работы O2 в операционной системе должны быть установлены следующие компоненты:

— Docker версии 20.10.12;

— Docker Compose версии 1.29.1.

Пользовательский интерфейс O2 работает в браузерах:

— Google Chrome версии 99.0 и выше;

— Mozilla Firefox версии 97.0 и выше.

Таблица 3. Аппаратные требования к серверу O2

Компонент сервера	Рекомендуемые требования
Процессор	Суммарно 10 логических ядер
ОЗУ	32 ГБ
Жесткий диск, свободное дисковое пространство	SSD, 500 ГБ

6.2. Предварительные условия для развертывания

Перед развертыванием O2 должны быть выполнены предварительные условия:

- На сервере O2 установлены Linux Debian 10, Docker версии 20.10.12, Docker Compose 1.29.1.
- В инфраструктуре организации развернуты MaxPatrol SIEM версии 24 или 25 и PT MC, установлена связь сервера O2 с ними. O2 использует MaxPatrol SIEM как источник событий, а PT MC для передачи данных, аутентификации и управления пользователями. Без интеграции с этими продуктами полноценная работа O2 невозможна.
- Выполнена дополнительная настройка MaxPatrol SIEM для получения событий от него (см. раздел 6.3).
- Время ОС O2 синхронизировано с MaxPatrol SIEM, PT MC.
- На сервер, где будет выполнена установка, скопирован дистрибутив O2 (объем дистрибутива 7 ГБ).

Ниже приведены дополнительная информация и инструкции для обеспечения этих условий.

Linux Debian 10

На сервере O2 должен быть установлен Linux Debian 10. К серверу должен быть обеспечен доступ по SSH.

Должны быть установлены вспомогательные пакеты unzip и curl с помощью команд:

```
apt-get install unzip
apt-get install curl
```

Docker и Docker Compose

На сервере O2 должны быть установлены Docker и Docker Compose. Пример инструкции по установке Docker приведен ниже.

```
apt-get update
apt-get install apt-transport-https ca-certificates curl gnupg2 software-properties-common
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add -
add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/debian $(lsb_release -cs) stable"
apt-get update
apt-get install docker-ce
docker --version
```

MaxPatrol SIEM и PT MC

Для корректной работы O2 с PT MC и MaxPatrol SIEM нужно обеспечить следующие условия:

- С сервера O2 есть доступ к PT MC и MaxPatrol SIEM:
  ```
  curl -k https://<ip-fqdn-siem>
  curl -k https://<ip-fqdn-mc>:3334
  curl -k https://<ip-fqdn-mc>:8703
  ```
- В PT MC создана учетная запись с ролью «оператор системы» для получения событий из MaxPatrol SIEM. Данные этой учетной записи используются при установке O2 в конфигурационных файлах `ipc.conf` (в секции [IAM]) и `connectors_config.ini` (в секции [SIEM], в параметрах PT MC).
- Настроен счетчик получения событий от MaxPatrol SIEM:
  ```
  curl -k http://<ip-fqdn-siem-front>:8013/v1/events/checkpoint/recent
  ```
  Если получение событий MaxPatrol SIEM происходит только на локальном компьютере, то нужно выполнить на нем команду `siemcfg set -p FrontendHost 0.0.0.0.`
- Получен ключ ClientSecret для доступа к MaxPatrol SIEM. Он понадобится для настройки коннектора (см. раздел 6.5) при развертывании O2. Ключ можно получить на сервере MaxPatrol SIEM выполнением одной из следующих команд:

  Linux: `cat $(find /var/lib/deployed-roles/mp10-Application -name "default.env") | grep -i ClientSecret`

  Windows: `corecfg get -p ClientSecret`
- В MaxPatrol SIEM настроена экспертиза, поддерживающая получение событий в O2.

6.3. Настройка MaxPatrol SIEM для получения событий

Чтобы O2 мог получать события от MaxPatrol SIEM, необходимо перед установкой O2 изменить параметры MaxPatrol SIEM по умолчанию.

- Чтобы настроить получение событий от MaxPatrol SIEM:

  1. На сервере, на котором развернут MaxPatrol SIEM, перейдите в папку `C:\\Program Data\Positive Technologies\MaxPatrol SIEM CORE\Config\Portal\Routers`.
  2. Откройте на редактирование файл `groups.json` и внесите изменения, как показано ниже.

     До редактирования:

     ```
     [
     {
     "Prefix": "https://<IP-адрес>:8778",
     "Patterns": [
     "/api/groups/v2/acl/roles/?(\\?\\S+)?$",
     ]
     ```

```
}
]
```

После редактирования:

```
[
{
"Prefix": "https://<IP-адрес>:8778",
"Patterns": [
"/api/groups/v2/acl/roles/?(\\?\\S+)?$",
"/api/groups/v2/group/?(\\?\\S+)?$",
"/api/groups/v2/hierarchy/?(\\?\\S+)?$"
]
}
]
```

3. В командной строке Windows введите `inetmgr`.

   Откроется окно Internet Information Services (IIS) Manager

4. В панели **Connections** выберите узел **Application Pools**.
5. Перезапустите сервис SIEMPortalAppPool.

6.4. Установка O2

- Чтобы установить O2 на сервере:

  1. Скачайте на сервер дистрибутив O2.
  2. Распакуйте содержимое в папку `/tmp/IPC_installer`.

     Папка временная, название и путь к ней не имеют значения. Можно указать собственное название и путь.

  3. Перейдите в папку `/tmp/IPC_installer/ipc`.
  4. Запустите разархивирование инсталлятора:

     ```
     unzip /tmp/IPC_installer/IPC_installer.zip -d /tmp/IPC_installer
     ```

  5. Запустите `install.sh`.
  6. Перейдите в папку `/opt/ipc`, созданную инсталлятором.
  7. Настройте глобальные переменные окружения в `ipc.conf`.

     Большая часть данных в `ipc.conf` заполняется автоматически при установке.

     Внимание! Если нет возможности определить компьютер по FQDN, замените подставленное имя на IP-адрес. Также необходимо полностью обновить в файле `ipc.conf` секцию `IAM` (содержит параметры соединения с PT MC) в соответствии с примером ниже.

     ```
     auth__FrontChannelLogoutUri=https://<IP-адрес или FQDN компьютера>/account/iamlogout
     auth__IamApplicationEndpoint=https://<IP-адрес или FQDN компьютера>
     auth__IamClientRedirectUri=https://<IP-адрес или FQDN компьютера>/account/oauthcallback
     ```

```
auth__IamClientPostLogoutRedirectUri=https://<IP-адрес или FQDN компьютера>/account/
oauthcallback
auth__IamApplicationId=<Идентификатор системы в PT MC>
auth__IamApplicationDisplayName=<Отображаемое имя системы в PT MC>
IAM_CLIENT_ID=<Имя системы>
IAM_DOMAIN=PT DC <Имя системы>
#Параметры для pt.sp.connectors (если тут отсутствуют, то будут проверены в
ipc_defaults.conf, а затем уже в конфигурационном файле коннекторов)
INTEGRATION_API_LOGIN=<Логин>
INTEGRATION_API_PASSWORD=<Пароль>


# SignalR
corsOptions__allowedOrigins=https://<IP-адрес или FQDN компьютера >


# IAM
auth__TmUrl=https://<IP-адрес или FQDN IAM>:8703
auth__TmRegistrationId=cabdaed2-5a89-5c0b-d20e-6ee16ffc2613
auth__IamUrl=https://<IP-адрес или FQDN PT MC>:3334
auth__LoginErrorUrlTemplate=https://<IP-адрес или FQDN PT MC>:3334/#/error?


# Environment
IPC_ENVIRONMENT__HOSTNAME=<IP-адрес или FQDN компьютера>
IPC_ENVIRONMENT__FULL_HOSTNAME=< IP-адрес или FQDN компьютера>


# Sopka Emulator
GOSSOPKA_NEW_URL=http://<IP-адрес или FQDN компьютера>:7045/api/emulator


#O2
TelegramBaseUrl=https://<IP-адрес или FQDN компьютера>
IpcUrl=https://<IP-адрес или FQDN компьютера>


# Notifications settings
WEBSITE_BASE_URL=https://<IP-адрес или FQDN компьютера>


# Kafka
KAFKA_LISTENER_SECURITY_PROTOCOL_MAP=PLAINTEXT:PLAINTEXT,PLAINTEXT_HOST:PLAINTEXT,PLAINTEX
T_EXT:PLAINTEXT
KAFKA_ADVERTISED_LISTENERS=PLAINTEXT://broker:29092,PLAINTEXT_HOST://
localhost:9092,PLAINTEXT_EXT://<IP-адрес или FQDN компьютера>:39092
```

8. Настройте журналирование:

   Если нужно журналирование в Elasticsearch (по умолчанию включено, но `hostname` не настроен), в файле `/opt/ipc/fluentd/config/match_section.conf` измените значения `host` и `port` на необходимые. Пример файла (шаблон):

   ```
   @type elasticsearch
   ```

```
host {{elasticsearch_<IP-адрес или FQDN сервера Elasticsearch>}}
port {{elasticsearch_port}}
logstash_format true
logstash_prefix ipc-logs
logstash_dateformat %Y.%m.%d
suppress_type_name true
include_tag_key true
reconnect_on_error true
reload_on_failure true
reload_connections false
```

где `elasticsearch_hostname` может указывать на observability-сервер Elasticsearch.

Если нужно журналирование в файл вместо Elasticsearch, удалите файл `/opt/ipc/fluentd/config/fluent.conf`, а файл `/opt/ipc/fluentd/config/fluent_to_files.conf` переименуйте в `/opt/ipc/fluentd/config/fluent.conf`. Файлы журнала в таком случае будут находиться в `/opt/ipc/logs`.

9. Временно запустите сервисы коннекторов и интеграционного API и зависимости:

   Внимание! Здесь и далее выполнение команд docker-compose осуществляется из каталога `/opt/ipc`, так как в нем находится файл `docker-compose.yaml` с конфигурацией.

   ```
   docker-compose up -d pt.sp.connectors pt.sp.integrationapi
   ```

10. Проверьте, что после старта pt.sp.connectors появилась папка `/opt/ipc/.docker/connectors`.

11. Остановите все сервисы, сделав непродолжительную паузу после успешного запуска сервисов коннекторов и интеграционного API:

    ```
    docker-compose stop
    ```

12. Настройте коннектор к MaxPatrol SIEM (см. раздел 6.5).

13. Настройте коннектор визуализации связей:

    ```
    cp -R /opt/ipc/.docker/connectors/connectors_examples/attack_graph /opt/ipc/.docker/connectors/running_connectors/attack_graph
    ```

14. Запустите сервисы, необходимые для работы страниц редактирования ролей и пользователей:

    ```
    docker-compose up -d pt.sp.gatewayapi pt.sp.integrationapi pt.sp.configuration pt.sp.sos pt.sp.usersync pt.sp.ptdc.ui
    ```

15. Убедитесь, что в PT MC появилось новое зарегистрированное приложение с названием, указанным в конфигурационном файле `ipc.conf`.

16. Добавьте администратора этого приложения O2 в PT MC.

    Подробная информация о добавлении пользователей продуктов АО «Позитив Текнолоджиз», управлении их ролями и привилегиями содержится в документации для PT MC.

17. Из папки `/opt/ipc/` запустите оставшиеся сервисы:

    ```
    docker-compose up -d
    ```

18. Проверьте правильность работы системы (см. раздел 6.6).
19. В параметрах системы добавьте администратору роль дежурного оператора системы (см. раздел 6.7).
20. Удалите временную папку `/tmp/IPC_installer`.

Установка O2 завершена.

6.5. Настройка коннектора к MaxPatrol SIEM

Для того чтобы O2 получал события из MaxPatrol SIEM, во время установки O2 нужно настроить коннекторы к MaxPatrol SIEM.

Этот раздел содержит инструкцию для настройки коннекторов во время установки O2.

Для настройки коннекторов используются следующие папки:

- `/opt/ipc/.docker/connectors/connectors_examples` — содержит актуальные примеры коннекторов и файл `connectors_config.ini.template`. Обновляется при каждом старте сервиса, поэтому все изменения, сделанные тут, будут потеряны.
- `/opt/ipc/.docker/connectors/internal_configs` — в этой папке нужно создать файл `connectors_config.ini`, используя шаблон `connectors_config.ini.template`.
- `/opt/ipc/.docker/connectors/running_connectors` — в папку нужно скопировать только необходимые коннекторы из папки connectors_examples. Изменения в папке сохраняются.

► Чтобы настроить коннектор к MaxPatrol SIEM :

1. Скопируйте из папки `/opt/ipc/.docker/connectors/connectors_examples` в папку `/opt/ipc/.docker/connectors/running_connectors` коннекторы, которые необходимо подключить:

   ```
   cp -R /opt/ipc/.docker/connectors/connectors_examples/siem /opt/ipc/.docker/connectors/running_connectors/siem
   ```

2. Скопируйте шаблон `connectors_config.ini.template` в `/opt/ipc/.docker/connectors/internal_configs`:

   ```
   cp -R /opt/ipc/.docker/connectors/connectors_examples/connectors_config.ini.template /opt/ipc/.docker/connectors/internal_configs/connectors_config.ini
   ```

   Файл `connectors_config.ini` отвечает за интеграцию с внешними системами, в том числе с MaxPatrol SIEM.

3. Измените содержимое конфигурационного файла `/opt/ipc/.docker/connectors/internal_configs/connectors_config.ini`:

   В секции `[INTEGRATION_API]` в параметрах `LOGIN` и `PASSWORD` укажите значения, ранее введенные в файле `ipc.conf` в секции `[IAM]`, для параметров `INTEGRATION_API_LOGIN` и `INTEGRATION_API_PASSWORD`.

В секции `[SIEM]` укажите значения параметров `URL`, `MPX_SIEM_URL`, `IAM_URL`, `IAM_CLIENT_ID`, `IAM_LOGIN`, `IAM_PASSWORD`, `MAX_DAYS_INITIAL_LOAD` (максимальное количество дней загружаемой истории событий из MaxPatrol SIEM). При вводе значений руководствуйтесь комментариями к параметрам, добавленными в шаблоне.

6.6. Проверка правильности работы системы

- Чтобы проверить правильность работы системы:

1. Перейдите по адресу `https://< IP-адрес или FQDN сервера O2>/t-cases` и авторизуйтесь в PT MC.

   Отобразится главная страница O2

2. В интерфейсе O2 проверьте наличие кейсов.

   Кейсы отображаются при условии, что в MaxPatrol SIEM есть события и что правила корреляции MaxPatrol SIEM используют логику заполнения полей для O2.

   Примечание. Кейсом называются одно или несколько событий ИБ (алертов), объединенных по заданным правилам аналитическим агрегатором O2.

3. Если кейсы отсутствуют, убедитесь в правильности работы сервисов:

   Проверьте список запущенных сервисов. Из 42 сервисов только следующие 4 должны быть остановлены:

   pt.sp.configurationtool;

   topicctl;

   autoregistration-schemas-in-registry;

   debezium-connector-setup.

   Проверьте журнал сервисов pt.sp.connectors, pt.sp.incidents, pt.sp.correlation на наличие ошибок.

6.7. Добавление роли дежурного оператора системы

Для доступа к всей информации, выводимой в интерфейсе, сразу после установки администратор должен добавить себе техническую роль дежурного оператора в параметрах O2.

- Чтобы добавить роль дежурного оператора:

1. На главной странице приложения O2 нажмите кнопку **Настройки** в правом верхнем углу экрана.
2. В раскрывающемся списке выберите **Пользователи**.
3. На открывшейся странице в панели **Пользователи** слева выберите **Все пользователи**.

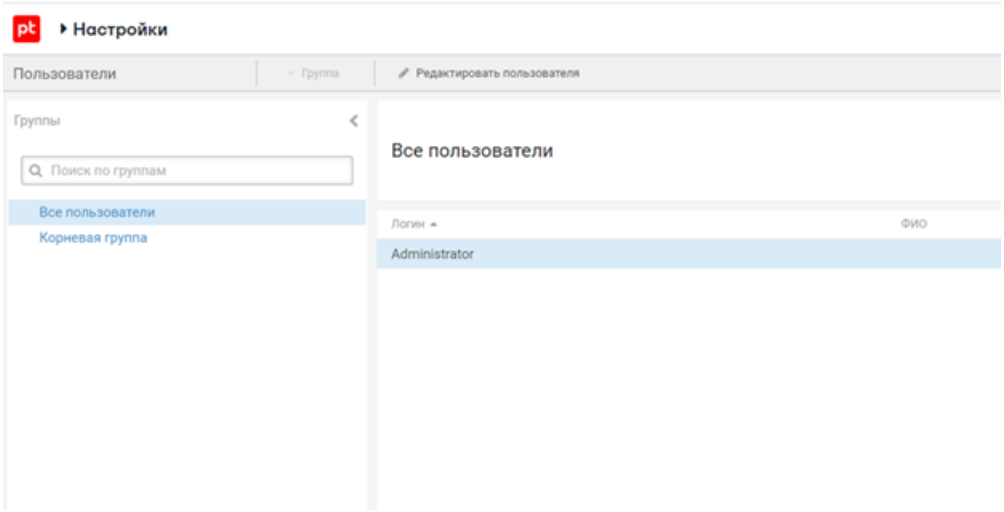

Рисунок 1. Выбор пользователя

4. В блоке параметров **Все пользователи** выберите **Administrator** и нажмите кнопку **Редактировать пользователя**.
5. В блоке **Права доступа** добавьте роль **Дежурный оператор**.

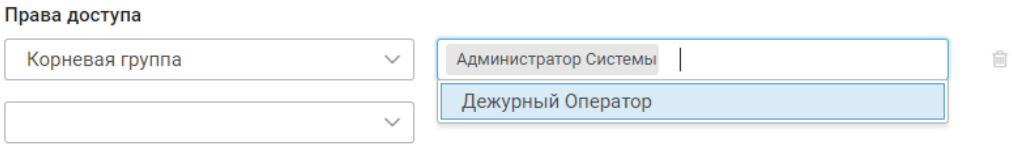

Рисунок 2. Добавление дежурного оператора

Роль дежурного оператора добавлена.

7. Устранение неисправностей

В этом разделе описаны причины и способы устранения неисправностей при работе с O2.

Закончилось свободное место

Очистите папку `/var/log`. Размеры дочерних папок можно узнать с помощью команды: `sudo du -ah {путь к корневой папке} --max-depth=1 | sort -hr`.

Если у вас нет доступа к папке `/tmp/IPC_installer`, вы можете выполнить команду: `sudo chmod go+rx /tmp/IPC_installer`.

Ошибка 500 api gateway после авторизации в PT MC

Если после авторизации в PT MC происходит перенаправление на страницу с ошибкой 500 api gateway, то наиболее вероятные причины:

— у пользователя нет прав доступа к приложению PT MC;

— не синхронизировано время между серверами O2 и PT MC;

— сервер PT MC недоступен.

Если в конфигурационном файле `ipc.conf` заменен FQDN на IP-адрес или изменены другие параметры взаимодействия O2 с PT MC, необходимо выполнить следующие действия:

1. В БД `sp_sos`, таблице `ValueStorages`, удалить целиком строку с ключом IamRegistrationFact.
2. Пересоздать (для маппинга новых переменных окружения) контейнеры `pt.sp.sos` и `pt.sp.gatewayapi` командой `docker-compose up -d pt.sp.sos pt.sp.gatewayapi.`

После нового запуска `pt.sp.sos`, произойдет перерегистрация в PT MC с новыми параметрами. Перезапуск gateway api нужен для обновления redirect_uri при обращении клиента к PT MC.

В случае, если сервисы `pt.sp.ptdc.ui` и `pt.sp.pipeline` не запустились после последнего шага, попробуйте запустить их самостоятельно (например, с помощью решения Portainer).

8. Обновление O2

Обновление O2 выполняется путем установки новой версии на сервере с развернутой системой. В состав новой версии входят добавленные функции и прочие усовершенствования O2, а также исправления известных проблем предыдущей версии (при наличии).

Для обновления нужно скопировать дистрибутив с новой версией O2 на сервер где развернута система, разархивировать его и запустить установку согласно инструкциям из комплекта документации для новой версии.

9. Вход в O2

Сервис управления пользователями и доступом PT MC обеспечивает механизм единого входа (технология single sign-on) в приложения «Позитив Текнолоджиз». Ссылку для входа, логин и пароль предоставляет администратор O2.

- Чтобы войти в O2:

  1. В адресной строке браузера введите ссылку для входа в интерфейс O2.

     Откроется страница входа в O2

  2. В поле **Логин** введите логин учетной записи.
  3. В поле **Пароль** введите пароль учетной записи.
  4. Нажмите кнопку **Войти**.

10. Интерфейс

Интерфейс O2 состоит из главной страницы приложения и страниц кейсов.

Кейсом называются одно или несколько событий ИБ (алертов), объединенных по заданным правилам аналитическим агрегатором O2.

На главной странице вы можете выбрать просмотреть общий список кейсов, отфильтровать их, выбрать нужный вам кейс и «провалиться» к его странице. Главная страница нужна для того, чтобы быстро увидеть новые кейсы, оценить ситуацию и выбрать кейсы, которым нужно уделить внимание в первую очередь.

Страница кейса содержит схему возможной атаки и подробную информацию о ресурсах (узлах сети и учетных записях), вовлеченных в атаку. Страница кейса нужна для анализа кейса и планирования действий реагирования.

В этом разделе

Главная страница (см. раздел 10.1)

Страница кейса (см. раздел 10.2)

10.1. Главная страница

После входа открывается страница веб-приложения O2 со списком кейсов. Кейсом в интерфейсе называется событие или цепочка событий ИБ, объединенных O2. По умолчанию отображаются кейсы, требующие внимания эксперта (статус **Требуют внимания**).

Кейсы расположены по убыванию опасности: самые опасные — наверху. Кейсы можно фильтровать по близости к риску, уровню опасности, времени последнего обновления статуса и последнего события.

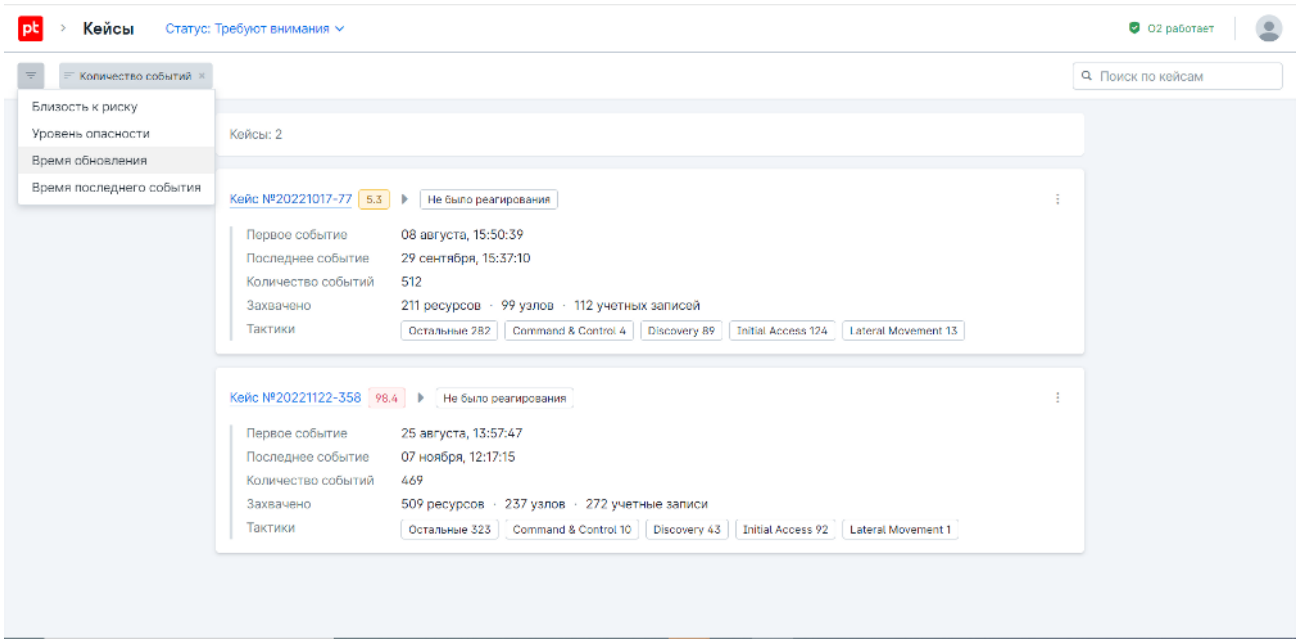

Рисунок 3. Главная страница

В карточке кейса отображается сводная информация о нем: уровень опасности, количество событий, собранных в кейсе, количество захваченных объектов, вероятные тактики MITRE ATT&CK, которые используются злоумышленниками. По нажатию на карточку кейса открывается его страница со схемой возможной атаки.

В правом верхнем углу страницы находится индикатор статуса работы O2. При наведении курсора на индикатор отображается всплывающая подсказка с временем получения последнего события и общим числом полученных событий.

Рядом с индикатором отображается кнопка перехода к пользовательским параметрам. Эксперты по этой кнопке могут включить темную тему или выйти из приложения. Администраторы могут перейти к просмотру, добавлению и настройке пользователей и их ролей.

10.2. Страница кейса

Страница кейса предоставляет информацию об атаке для анализа и реагирования. Она по умолчанию открывается на схеме возможной атаки с вовлеченными в нее ресурсами инфраструктуры.

O2 поддерживает два типа ресурсов: узлы и учетные записи. Схема показывает узлы, события на них и между ними, а также учетные записи. По нажатию на событие отображается всплывающее окно с подробной информацией о нем.

По кнопке **Открыть таймлайн** в левом нижнем углу страницы можно «проиграть» событие на схеме и увидеть развитие атаки в динамике.

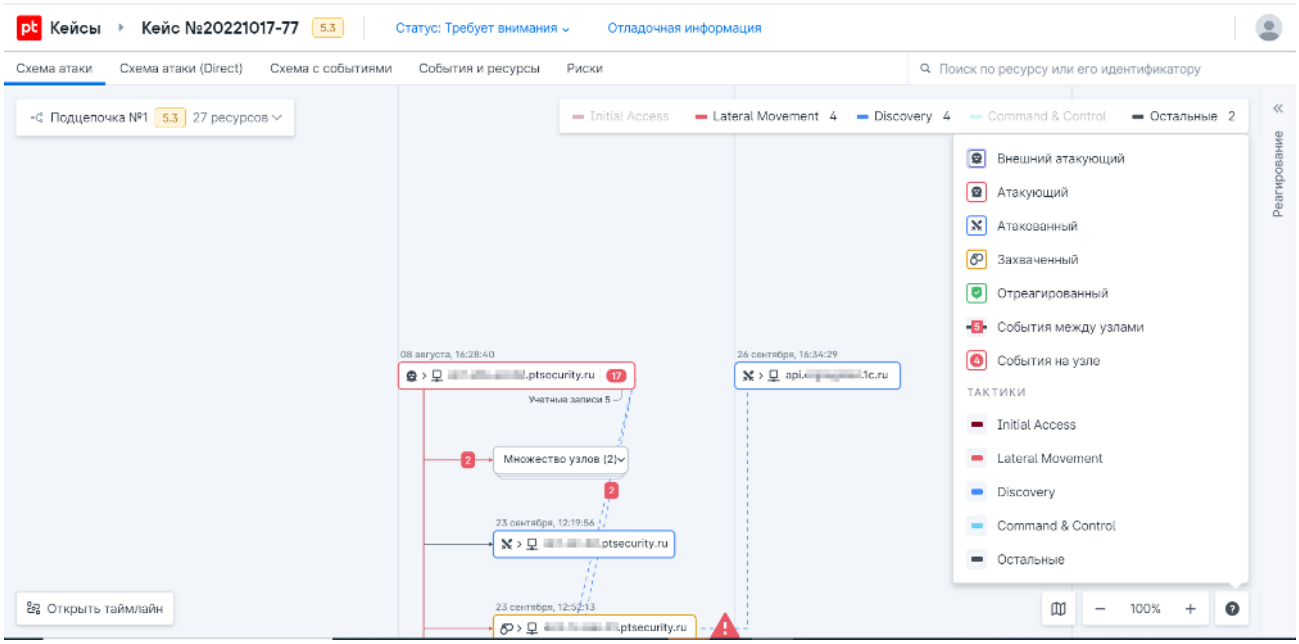

Рисунок 4. Схема атаки

В раскрывающемся блоке **Реагирование** в правой части страницы можно выбрать и отметить узлы, к которым уже были применены действия реагирования вне О2.

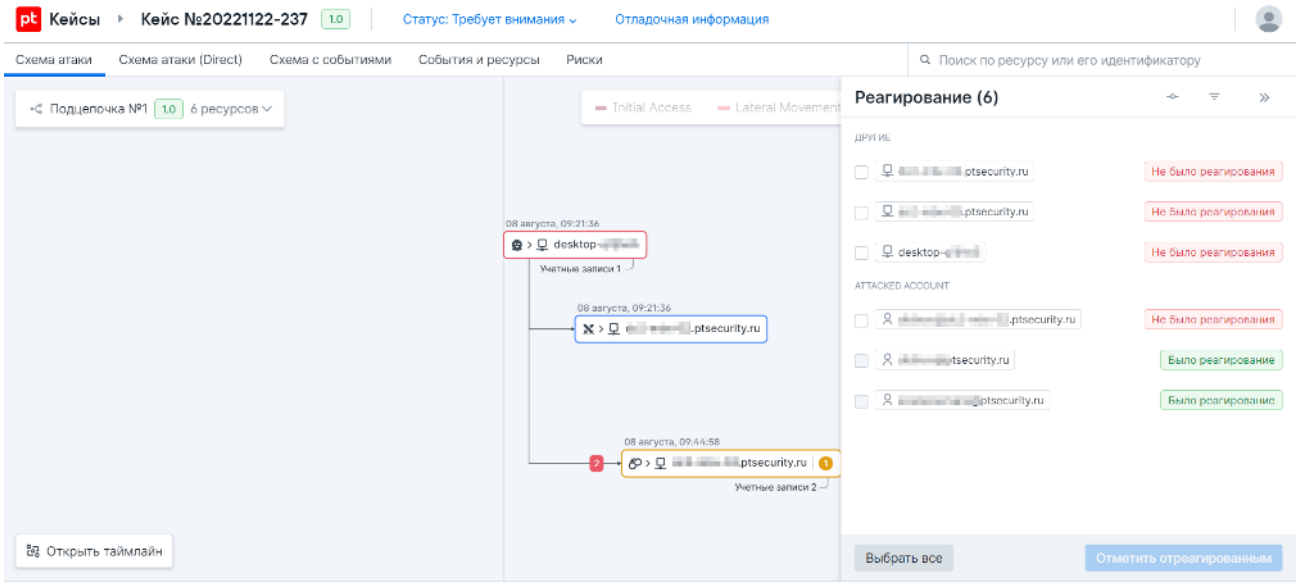

Рисунок 5. Блок реагирования

На вкладке **События и ресурсы** содержится подробная информация о событиях на каждом ресурсе, затронутом атакой, — и о связях между ними.

11. Работа эксперта в O2. Статусы кейсов

В этом разделе описана общая последовательность работы эксперта по ИБ с кейсами в O2. Она не является жестким шаблоном, ее можно изменять в зависимости от условий.

1. Просмотреть список требующих внимания кейсов на главной странице.
2. Выбрать кейс, по которому хотите просмотреть подробности, и нажать его карточку. Откроется страница кейса со схемой развития возможной атаки.
3. Просмотреть схемы развития атаки, события и ресурсы, затронутые атакой.
4. Принять решение о необходимых действиях реагирования по отношению к узлам сети и учетным записям, вовлеченным в атаку. Действия реагирования в текущей версии O2 планируются и выполняются за пределами системы.
5. Если действия не требуются и кейс является ложным срабатыванием, установить для него соответствующий статус.
6. После реагирования отметить в O2, что в отношении объектов в составе кейса было выполнено реагирование. После этого O2 переводит кейс в статус **Было реагирование**. Если развитие атаки прекратится (в течение часа в кейс не «подклеиваются» новые события), кейс будет перенесен в архив.

О статусах кейсов

Статусы кейсов используются в O2 для приоритизации и планирования работы эксперта с ними.

Собираются: еще не ясно, требуется ли внимание эксперта

Этот статус система присваивает кейсам, которые имеют признаки атаки, но их еще нельзя автоматически отнести к требующим внимания эксперта. Например, статус **Собирается** может быть присвоен кейсу, когда пользователь выполняет легитимный вход в какую-либо программу с нового места. Если атака развивается и к кейсу добавляются («подклеиваются») новые события и цепочки событий, O2 переводит кейс в статус **Требует внимания**.

Требует внимания: реальная атака или ложное срабатывание

Кейсы в этот статус переводятся автоматически или вручную. Требующие внимания кейсы нужно проанализировать и выполнить реагирование на них либо вручную перевести их в статус **Ложное срабатывание**. После того как реагирование выполнено и информация об этом внесена в O2, кейс автоматически переходит в статус **Было реагирование**.

Было реагирование: временный статус для контроля результатов реагирования

Статус **Было реагирование** автоматически присваивается кейсу, для которого были выполнены действия реагирования. Этот статус нужен для контроля результатов реагирования (чтобы понимать, развивается ли атака после реагирования). По умолчанию кейс находится в статусе **Было реагирование** один час. Затем, если в течение этого часа в кейс не

добавлялись новые события, он автоматически переводится в статус **Архив**. Кейс в статусе **Было реагирование** можно также вручную перевести в другой статус, например вернуть статус **Требуют внимания**.

Ложное срабатывание: статус, который можно назначить только вручную

Если по результатам анализа кейса стало понятно, что он является срабатыванием, ему нужно присвоить соответствующий статус. Отметить кейс как ложное срабатывание может только эксперт вручную: O2 не присваивает этот статус автоматически. Цепочки событий, отмеченные как ложные срабатывания, не учитываются при расчете других цепочек.

12. Обращение в службу технической поддержки

Уполномоченные представители эксплуатационной службы заказчика могут обращаться в диспетчерскую службу АО «Позитив Текнолоджиз», формируя для этого заявки любым из способов:

— по телефонам (в рабочие дни с 9:00 до 18:00 по московскому времени):

  +7 812 385 11 03 (для звонков из Санкт-Петербурга и Ленинградской области);

  +7 800 700 09 87 (для звонков из любой точки России);

— по электронной почте: support@gaz-is.ru;

— на сайте gaz-is.ru в разделе **Поддержка**.

Требования к содержанию заявки

Заявки принимаются по следующим вопросам:

— неисправность в работе программного обеспечения,

— неисправность оборудования.

В заявке необходимо указать:

— полное наименование организации,

— номер договора либо наименование объекта эксплуатации,

— контактные данные для обратной связи (имя, телефон, адрес электронной почты).

Кроме того, необходимо предоставить:

— подробное описание неисправности, сопутствующих обстоятельств, при которых она возникла (какие операции проводились, при каких условиях выполнялась работа и т. п.);

— журналы событий технических средств, копии экранов, которые наглядно отображают проявление неисправности, и иные дополнительные сведения, которые могут помочь при устранении неисправности.

В случае неисправности оборудования необходимо также указать наименование и серийный номер оборудования, вышедшего из строя.

Порядок регистрации и учета заявок

Все поступающие заявки регистрируются в автоматизированной системе учета заявок и получают уникальный идентификационный номер:

— при обращении по телефону диспетчер на основании полученных данных регистрирует заявку, сообщает идентификационный номер и предварительный порядок ее отработки;

— при обращении по электронной почте заявка регистрируется автоматически и в ответ высылается уведомление с указанием ее идентификационного номера;

— при обращении через сайт АО «Позитив Текнолоджиз» заявка регистрируется автоматически и уведомление с указанием ее идентификационного номера высылается на адрес, указанный при заполнении формы заявки.

Для дальнейшего взаимодействия при обработке заявки необходимо знать ее регистрационный номер.

Глоссарий

алерт

Обработанное О2 и обогащенное данными о ресурсах корреляционное событие.

атакованный ресурс

Подвергшийся атаке ресурс, для которого отсутствует подтверждение, что он захвачен.

атакующий ресурс

Ресурс, используемый в атаке на другие ресурсы. Может быть внешним или внутренним (захваченным злоумышленником).

захваченный ресурс

Ресурс, к которому злоумышленник получил доступ и может использовать его для неправомерных действий.

ключевые системы

Информационные системы, без воздействия на которые злоумышленник не сможет развить атаку на целевую систему, а также такие системы, взлом которых существенно упростит последующий сценарий атаки для компрометации целевых систем.

корреляционное событие

Результат срабатывания правил СЗИ из-за подозрительных или вредоносных действий.

корреляция событий

Процесс обнаружения нарушений ИБ на основе анализа потока событий от источников. Виды и сочетания событий, характерные для различных видов нарушений, указываются в заранее созданных правилах.

недопустимое событие

Отдельное событие, цепочка или сочетание событий, в результате которых наступает одно или несколько негативных последствий, характеризующихся неприемлемым уровнем ущерба.

ресурс

Объект IT-инфраструктуры, защищаемой или внешней, который злоумышленник может использовать в атаке.

событие

Идентифицированное возникновение определенного состояния системы, сервиса или сети.

тактика

Тактическая цель злоумышленника, причина совершения действия. Компонент матриц Mitre Att&ck.

техника

Конкретный способ реализации тактики злоумышленником. Компонент матриц Mitre Att&ck.

целевые системы

Информационные системы, в результате воздействия злоумышленника на которые непосредственно, происходит недопустимое для бизнеса событие. Эти системы являются конечной целью злоумышленника при реализации недопустимого события. Такие системы, как правило, являются основными в рамках рискового бизнес-процесса.

positive technologies

ptsecurity.com
pt@ptsecurity.com