Positive Technologies Cybersecurity Intelligence

Версия 2.0

Руководство пользователя

POSITIVE TECHNOLOGIES

Дата редакции документа: 14.11.2019

Содержание

1. Об этом документе

Руководство пользователя содержит пошаговые инструкции и справочную информацию об использовании Positive Technologies Cybersecurity Intelligence (далее также — Cybsi). В руководстве описаны ключевые и дополнительные функции Cybsi, а также настройка функций для выполнения конкретных задач. Руководство не содержит инструкции по установке, первоначальной настройке и администрированию Cybsi.

Руководство адресовано специалистам, использующим Cybsi в своей работе.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о Cybsi (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример текста с условным обозначением	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 Cybsi

Вы можете найти дополнительную информацию о Cybsi на 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 учетную запись на портале.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 14).

2. О Cybsi

Cybsi — это программная платформа для накопления знаний о существующих и потенциальных угрозах информационной безопасности, а также о способах их обнаружения. Cybsi собирает, анализирует и хранит информацию об угрозах информационной безопасности и индикаторах компрометации, которые могут быть выделены в рамках угрозы. Индикаторы компрометации — это артефакты, наблюдаемые в сети или в операционной системе и указывающие на вредоносную активность в инфраструктуре.

3. Функциональные возможности Cybsi

Cybsi выполняет следующие функции:

- Сбор угроз и индикаторов компрометации из внешних источников.
- Аналитическая обработка входящих данных.
- Обогащение. Cybsi подвергает входящие данные дополнительной обработке, в результате которой информация о них дополняется.
- Хранение угроз и индикаторов компрометации, полученных от внешних источников, а также угроз и индикаторов, созданных пользователями, в базе данных.
- Отображение накопленной информации в веб-интерфейсе в удобном для анализа виде.
- Экспорт данных во внешние системы.

4. Об объектах в Cybsi

Угрозы и индикаторы компрометации содержатся в базе знаний Cybsi в виде объектов и их атрибутов.

Объект в Cybsi — это сущность, связанная с информационной безопасностью и характеризуемая одним или несколькими атрибутами. Атрибут — это необходимое свойство объекта. Одни атрибуты только характеризуют объект (например, имя файла), другие — однозначно его идентифицируют (например, хэш-сумма файла).

Объекты в базе знаний классифицированы таким образом, чтобы по каждому из них Cybsi мог собирать уникальные атрибуты и устанавливать связь между двумя объектами.

В Cybsi представлены следующие объекты и их атрибуты:

- Файл. Объект содержит информацию о файлах, их метаданных и хеш-суммах.
- Домен. Объект описывает свойства доменного имени. В процессе дополнительной обработки (обогащения) информация о доменном имени дополняется WHOIS- и DNS-записями.
- IP-адрес. Объект описывает свойства IP-адреса. В процессе дополнительной обработки (обогащения) информация об IP-адресе дополняется WHOIS- и DNS-записями.
- Человек / Компания. Объект содержит идентификационную и контактную информацию, а также указание на сферу деятельности участника киберугрозы (жертвы, репортера и т. п.).
- URL. Объект описывает свойства вредоносного URL сайта или отдельной страницы сайта.
- Семейство вредоносного ПО. Объект содержит информацию о вредоносных файлах, объединенных в семейство по общим признакам.
- Адрес эл. почты. Объект содержит адрес электронной почты, с которого злоумышленники могут рассылать письма, содержащие вредоносные вложения, ссылки, заголовки и т. п.
- Телефон. Объект содержит телефонные номера, связанные с объектом Человек / Компания.
- Уязвимость. Объект может содержать информацию об уязвимости нулевого дня или ссылку на внешние ресурсы с описанием уже известных уязвимостей (например, на классификатор уязвимостей CVE).

Cybsi получает объекты из внешних источников. Вы также можете регистрировать объекты в базе данных Cybsi вручную.

5. Источники информации для Cybsi

Источниками информации об угрозах ИБ и индикаторах компрометации для Cybsi являются:

— Пользователи. Вручную регистрируют объекты и их атрибуты в интерфейсе Cybsi.

— Платформы threat intelligence. Содержат знания о существующих и потенциальных угрозах информационной безопасности, а также способах их обнаружения. Информация от платформ поступает в виде фидов. Cybsi взаимодействует с платформой AlienVault Open Threat Exchange (настраивается администратором при установке Cybsi) и с Malware Information Sharing Platforms (не требует дополнительной настройки).

— Анализаторы кода и песочницы. Обогащают информацию о файлах. Cybsi взаимодействует со следующими анализаторами и песочницами, которые настраиваются администратором при установке Cybsi:

- Positive Technologies MultiScanner;
- Trend Micro Deep Discovery Analyzer;
- Pyshok;
- VirusLocal.

— WHOIS- и DNS-серверы. Обогащают WHOIS- и DNS-записи о доменах и IP-адресах (не требуют дополнительной настройки при установке Cybsi).

См. также

Регистрация объектов вручную (см. раздел 12)

Работа с фидами (см. раздел 13)

Обогащение информации об объектах (см. раздел 11)

6. Принцип работы

Cybsi работает по следующему принципу:

1. Cybsi получает информацию об угрозах ИБ и индикаторах компрометации от платформ threat intelligence в виде фидов или от оператора, который вводит данные в интерфейсе Cybsi.
2. Cybsi анализирует полученную информацию и регистрирует в базе данных объекты и их атрибуты, а также связи между объектами.
3. В подсистеме обогащения Cybsi данные о некоторых объектах подвергаются дополнительной обработке, благодаря которой информация о них дополняется, и регистрируются новые связи.
4. Cybsi формирует фиды для экспорта во внешние системы на основе правил, созданных оператором.
5. С заданной частотой, указанной в правиле, Cybsi создает срез данных фида, сохраняет его в файл и запаковывает в архив.
6. Внешние системы, подключенные к Cybsi, отправляют API-запросы для получения необходимого среза данных фида.
7. Cybsi в соответствии с API-запросом отправляет последний созданный архив во внешнюю систему.

См. также

Обогащение информации об объектах (см. раздел 11)

Регистрация объектов вручную (см. раздел 12)

Работа с фидами (см. раздел 13)

7. Вход в Cybsi через PT IAM

Вход в Cybsi осуществляется через сервис управления пользователями и доступом Positive Technologies Identity and Access Management (PT IAM), который обеспечивает механизм единого входа (технология single sign-on) в приложения "Позитив Текнолоджиз".

Перед входом в Cybsi запросите у администратора PT IAM:

— ссылку для входа в интерфейс продукта;

— логин и пароль вашей учетной записи пользователя.

Примечание. Убедитесь, что в браузере разрешены всплывающие окна, а также отключена функция Compatibility view для браузеров Microsoft Edge и Microsoft Internet Explorer.

► Чтобы войти в Cybsi:

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

   Откроется страница входа в сервис PT IAM.

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

PT IAM проверяет введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница поиска объектов (см. раздел 8). Если вы указали неверные данные, отобразится сообщение об ошибке.

8. Интерфейс Cybsi

Все действия в Cybsi вы можете выполнять с помощью пользовательского графического интерфейса.

Основным элементом управления в интерфейсе Cybsi является главное меню. Главное меню отображается на всех страницах и состоит из следующих элементов:

- кнопка для перехода на главную страницу Cybsi;
- раздел **Зарегистрировать** для перехода к страницам регистрации объектов в базе данных Cybsi;
- раздел **Фиды** для перехода к странице создания и просмотра фидов;
- кнопка выбора языка интерфейса;
- кнопка выхода из системы;
- поле поиска (отображается только на странице объекта).

Сразу после входа в интерфейс продукта по умолчанию открывается главная страница. Рабочая область главной страницы содержит поисковую строку, которую вы можете использовать для поиска объектов в базе данных Cybsi (см. раздел 9.1).

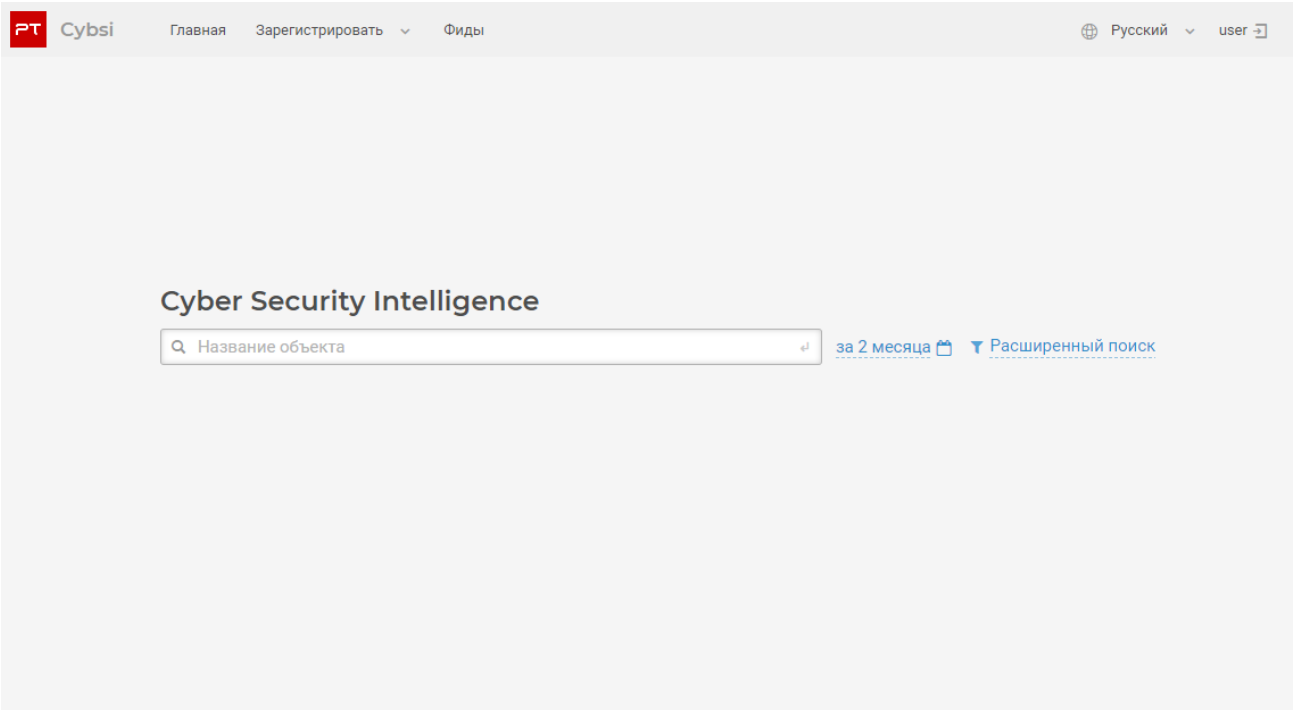

Рисунок 1. Главная страница Cybsi

9. Поиск объектов в Cybsi

В Cybsi вы можете выполнять поиск объектов на главной странице сразу после входа в систему или на других страницах в процессе работы с данными.

В этом разделе

9.1. Стартовый поиск объектов

Вы можете начать поиск объектов на главной странице Cybsi сразу после входа в систему. Стартовый поиск позволяет находить объекты, новая информация по которым поступала в Cybsi за последние два месяца.

► Чтобы выполнить стартовый поиск объекта:

1. Войдите в систему (см. раздел 7).
2. На главной странице в поле **Поиск объектов** введите атрибут, который однозначно идентифицирует объект (например, файл можно идентифицировать по хеш-сумме, но не по имени, так как разные файлы могут иметь одинаковые имена).

   Примечание. Вы можете вводить в поле поиска знак процента (%) или знак подчеркивания (_). Знак подчеркивания соответствует любому одиночному символу, знак процента — любой последовательности символов.

3. Во всплывающем окне по ссылке со значком настройте временной промежуток, в котором объект был впервые и в последний раз замечен во внешнем источнике.

   Примечание. Увеличение временного промежутка снижает скорость поиска объектов в базе данных.

4. Нажмите кнопку ↵ в поле поиска.

   Откроется страница результатов поиска. Если объект не отображается в результатах поиска, вы можете воспользоваться расширенным поиском (см. раздел 9.3).

9.2. Быстрый поиск объекта

По завершении анализа объекта на странице объекта вы можете быстро переключиться на поиск другого объекта с помощью поля поиска в главном меню. Быстрый поиск позволяет находить объекты, новая информация по которым поступала в Cybsi за последние два месяца.

► Чтобы выполнить быстрый поиск объекта:

1. На странице объекта в главном меню нажмите кнопку **Поиск**.

   Отобразится поле поиска.

2. Введите в поле атрибут, который однозначно идентифицирует объект (например, файл можно идентифицировать по хеш-сумме, но не по имени, так как разные файлы могут иметь одинаковые имена).

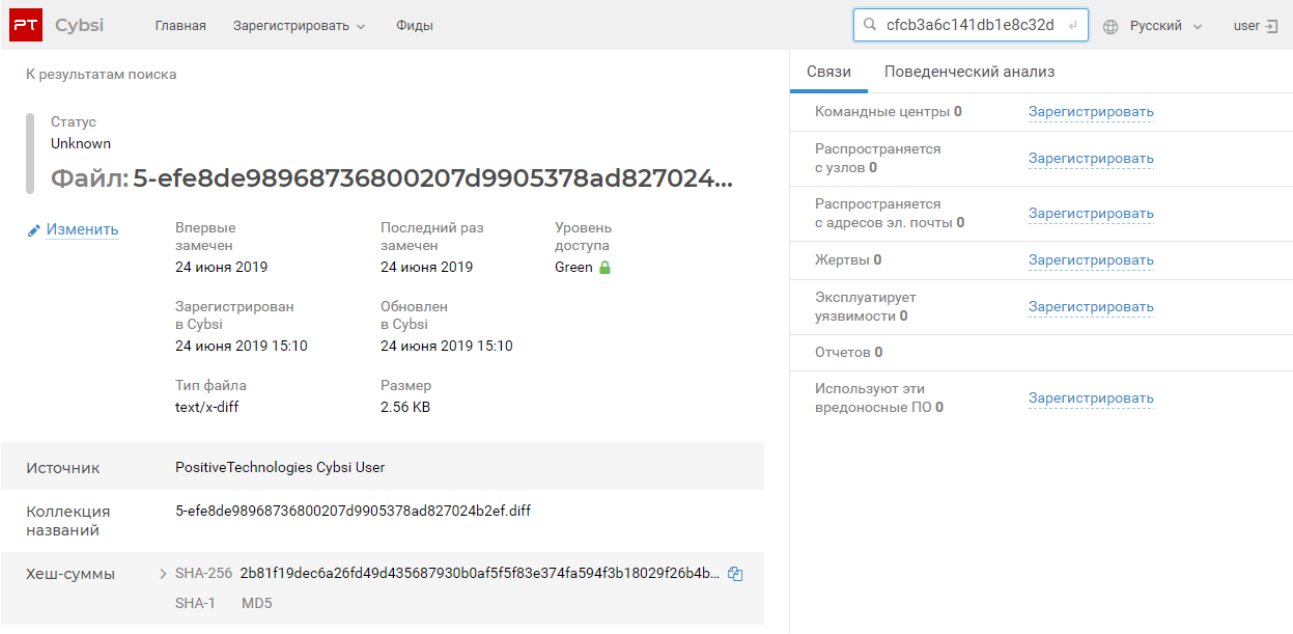

Рисунок 2. Ввод атрибута в поле поиска

3. Нажмите Enter.

   Откроется страница результатов поиска. Если объект не отображается в результатах поиска, вы можете воспользоваться расширенным поиском (см. раздел 9.3).

4. Откройте страницу объекта по ссылке с его названием.

9.3. Расширенный поиск объектов

Вы можете воспользоваться расширенным поиском с указанием параметров объекта, если при стартовом или быстром поиске на странице результатов поиска не отображаются объекты, удовлетворяющие условиям запроса, или вы не знаете, по каким атрибутам искать объект.

Примечание. Вы также можете выполнять расширенный поиск на главной странице Cybsi.

► Чтобы выполнить расширенный поиск объекта:

1. На странице результатов поиска нажмите ссылку **Расширенный поиск**.

В правой части страницы отобразится панель расширенного поиска.

2. В раскрывающихся списках выберите параметры поиска.

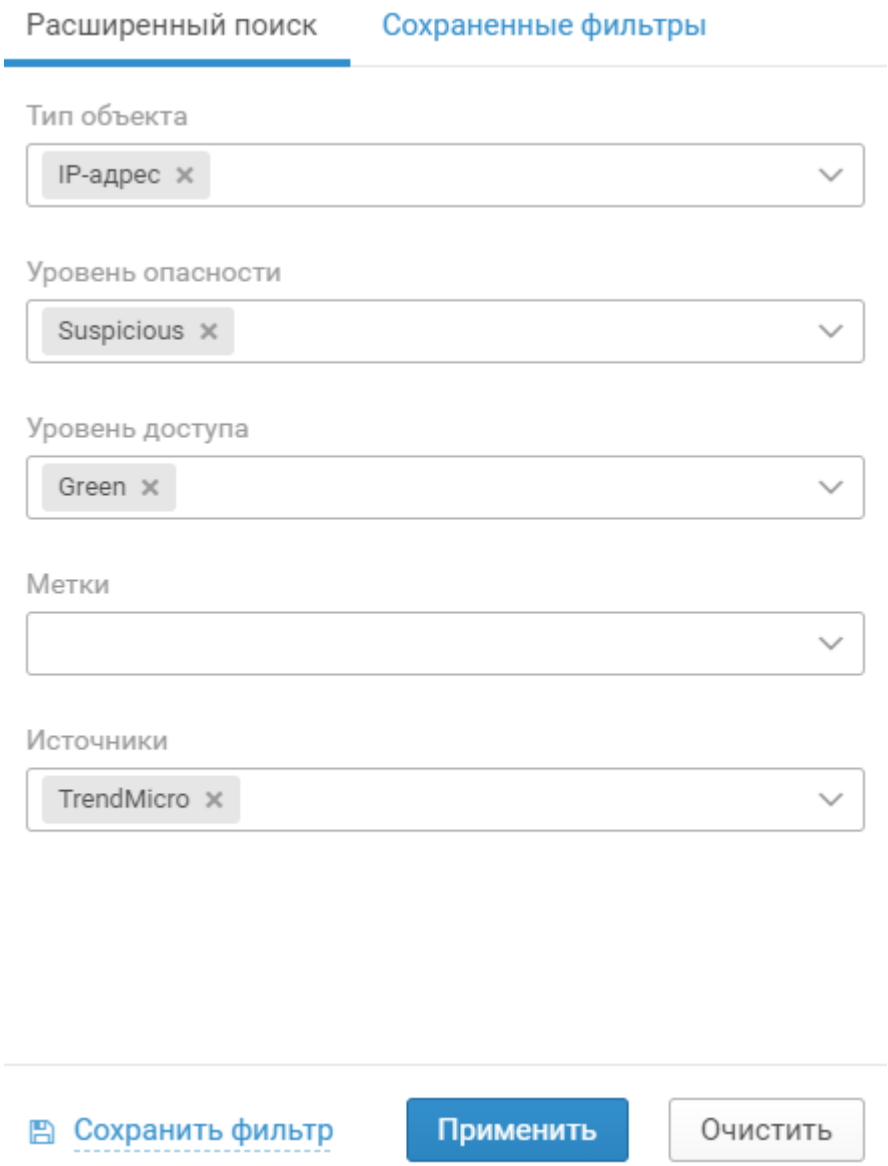

Рисунок 3. Выбор параметров расширенного поиска

3. Нажмите кнопку **Применить**.

   Отобразятся результаты поиска, соответствующие выбранным параметрам.

4. Откройте страницу объекта по ссылке с его названием.

9.4. Создание фильтра

Вы можете сохранять параметры расширенного поиска и использовать их для повторного поиска или для создания фильтра в фидах.

► Чтобы создать фильтр:

1. На главной странице или на странице с результатами поиска нажмите ссылку **Расширенный поиск**.

   В правой части страницы отобразится панель расширенного поиска.

2. В раскрывающихся списках выберите параметры фильтра.
3. Нажмите ссылку **Сохранить фильтр**.

   Отобразится панель **Сохранить фильтр**.

4. Введите название фильтра.

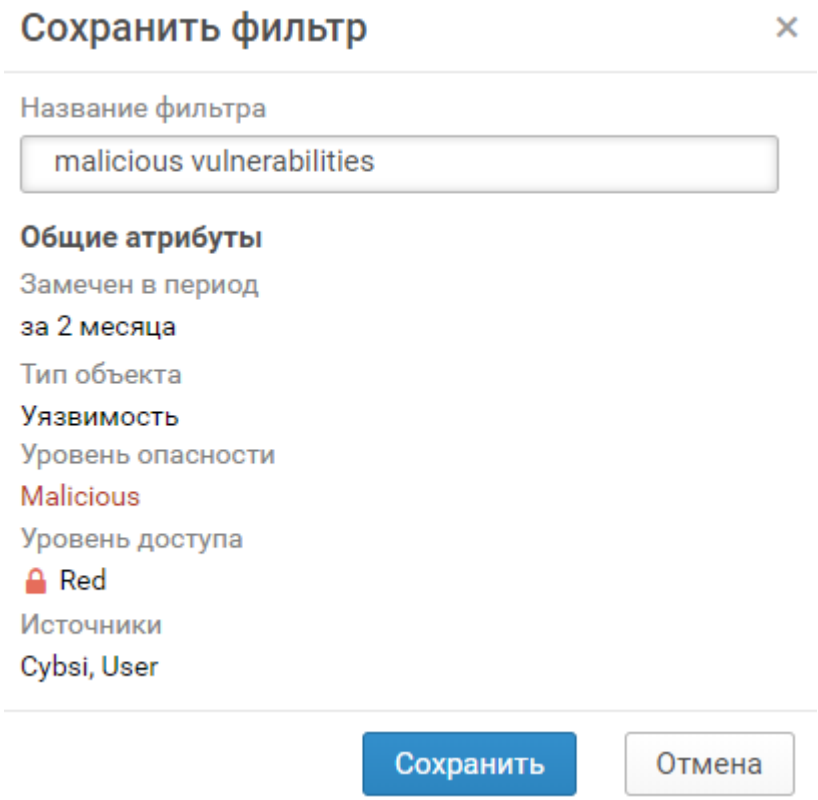

Рисунок 4. Создание фильтра

5. Нажмите кнопку **Сохранить**.

Фильтр создан.

9.5. Поиск по сохраненному фильтру

Вы можете использовать сохраненный фильтр для повторного поиска объектов в Cybsi.

► Чтобы выполнить поиск по сохраненному фильтру:

1. На главной странице или на странице с результатами поиска нажмите ссылку **Расширенный поиск**.

   В правой части страницы отобразится панель расширенного поиска.

2. Выберите вкладку **Сохраненные фильтры**.
3. Раскройте строку с фильтром.

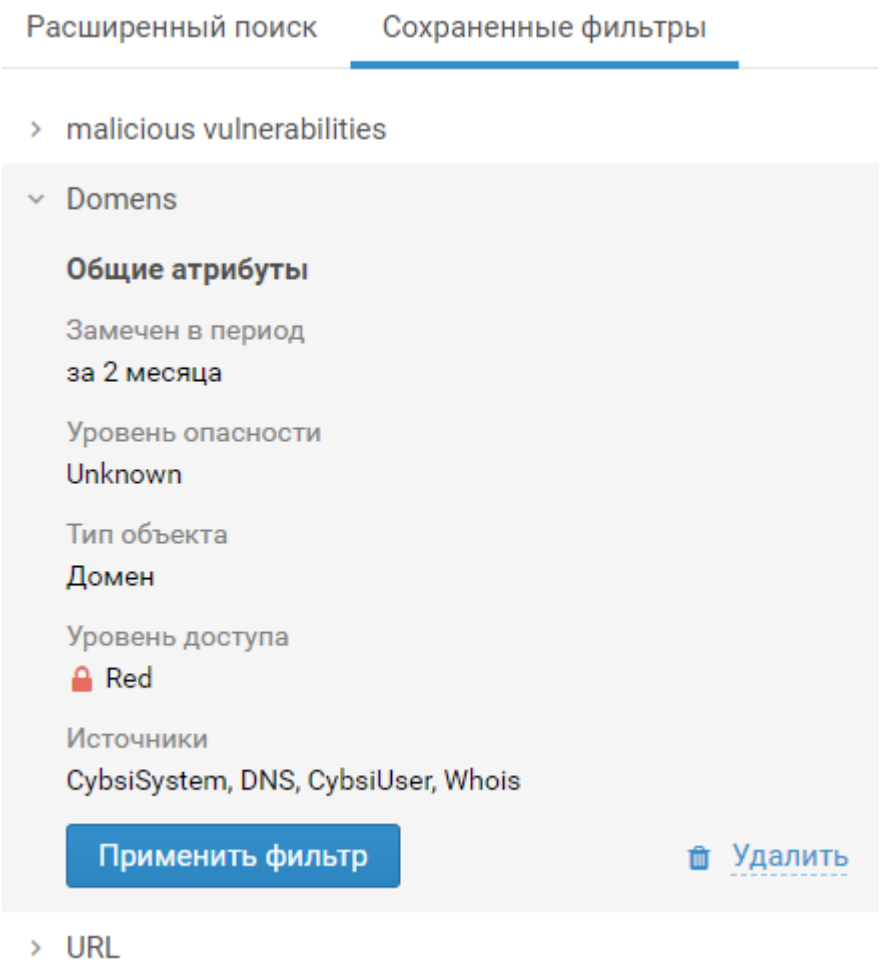

Рисунок 5. Поиск по сохраненному фильтру

4. Нажмите кнопку **Применить фильтр**.

   Отобразятся результаты поиска, соответствующие параметрам сохраненного фильтра.

10. Просмотр данных объекта

Информация об объекте отображается на странице объекта.

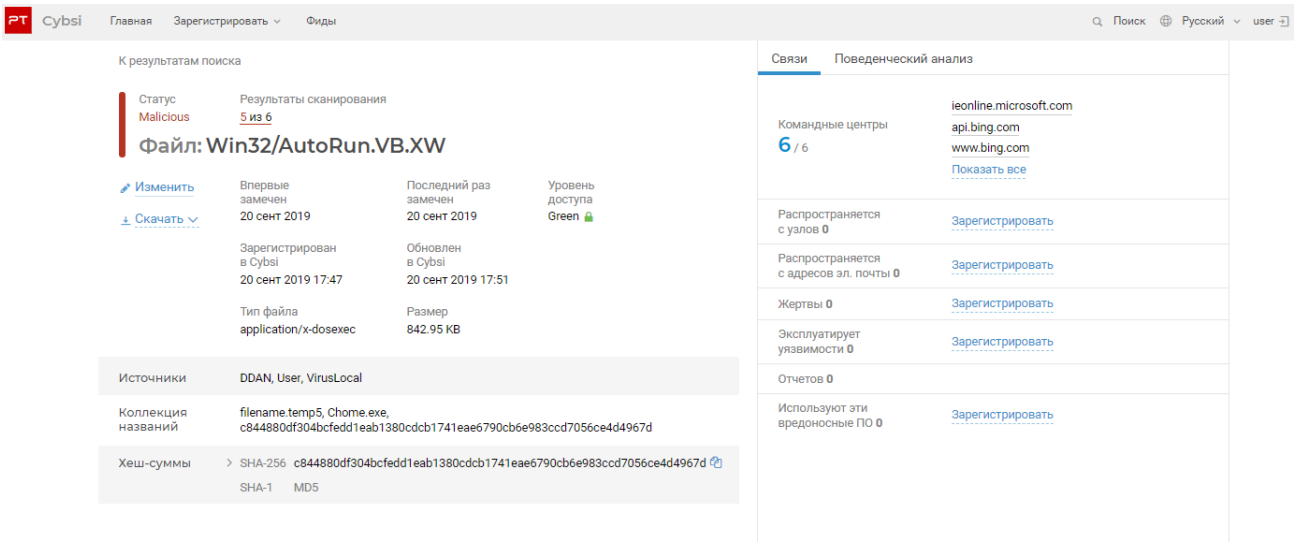

Рисунок 6. Страница объекта

Данные об объекте включают:

- Атрибуты объекта. Атрибуты могут быть стандартными для всех объектов (например, даты, в которые объект был впервые и в последний раз замечен во внешнем источнике, даты, в которые объект был зарегистрирован и обновлен в Cybsi) и уникальными для конкретного объекта (например, DNS- и WHOIS-записи о домене или IP-адресе).
- Пользовательскую информацию. Пользовательская информация не является атрибутом, но позволяет дополнительно характеризовать объект. Эту информацию вы можете изменять по кнопке **Изменить**. Например, вы можете добавить метку объекта, адреса внешних ресурсов, дополнить описание объекта.
- Связи объекта. Связь отображает зависимость между двумя объектами, один из которых может не являться вредоносным, но связан с другим вредоносным объектом.
- Результаты поведенческого анализа (отображаются только для файлов). Поведенческий анализ позволяет моделировать поведение вредоносного файла в песочнице — виртуальном окружении, изолированном от информационной системы организации. С помощью Cybsi вы можете отправить файл на поведенческий анализ в песочницу.

См. также

Поведенческий анализ файлов (см. раздел 11.4)

11. Обогащение информации об объектах

После регистрации Cybsi подвергает некоторые объекты обогащению, в результате которого информация об объектах дополняется.

В Cybsi поддерживаются следующие типы обогащения:

— автоматическое обогащение WHOIS- и DNS-записей о доменах;

— автоматическое обогащение WHOIS- и DNS-записей об IP-адресах;

— ручное обогащение информации о файлах.

Обогащение WHOIS-записей о доменах и IP-адресах происходит по протоколу WHOIS. По этому протоколу Cybsi получает от внешних баз данных сведения о владельцах IP-адресов и доменных имен.

Обогащение DNS-записей о доменах и IP-адресах происходит по протоколу DNS. Cybsi получает обогащенную информацию от DNS-сервера, подключение к которому настраивается в конфигурационном файле при установке.

Обогащение информации о файлах осуществляется за счет сканирования внешними анализаторами кода и поведенческого анализа в песочницах. Некоторые системы могут быть как анализаторами, так и песочницами (Trend Micro Deep Discovery Analyzer и Positive Technologies MultiScanner). Другие — только анализаторами (VirusLocal) или только песочницами (Pyshok).

Обогащенную информацию о доменах и IP-адресах вы можете просмотреть на страницах этих объектов. Результаты сканирования и поведенческого анализа файла отображаются на странице файла на вкладках **Результаты сканирования** и **Поведенческий анализ**.

В этом разделе

11.1. Работа с WHOIS-записями

WHOIS-записи о домене и IP-адресе отображаются в карточках этих объектов.

Блок WHOIS в карточке домена может содержать:

— дату и время получения WHOIS-записей о домене;

— дату регистрации домена;

— дату, до которой оплачен домен;

— данные о юридическом лице, зарегистрировавшем домен;

— данные о физическом или юридическом лице, на чье имя зарегистрирован домен;

— адреса электронной почты, содержащиеся в WHOIS-записи домена.

Блок WHOIS в карточке IP-адреса может содержать:

— дату и время получения WHOIS-записей об IP-адресе;

— дату регистрации и дату обновления регистрационной информации об IP-адресе;

— адрес WHOIS-сервера;

— информацию о владельце IP-адреса;

— информацию об организации, принимающей жалобы по IP-адресу;

— информацию об организации, осуществляющей техническую поддержку IP-адреса;

— адреса электронной почты, содержащиеся в WHOIS-записи IP-адреса.

WHOIS-записи об объекте могут изменяться, вы можете просмотреть историю изменения WHOIS-записей об объекте и обновить WHOIS-записи вручную.

► Чтобы просмотреть историю изменений WHOIS-записей:

1. Перейдите на страницу домена или IP-адреса.

   В блоке WHOIS отобразится обогащенная информация об объекте. Вы также можете просмотреть исходные WHOIS-записи, которые поступают в Cybsi в необработанном виде, по ссылке **WHOIS-запись**.

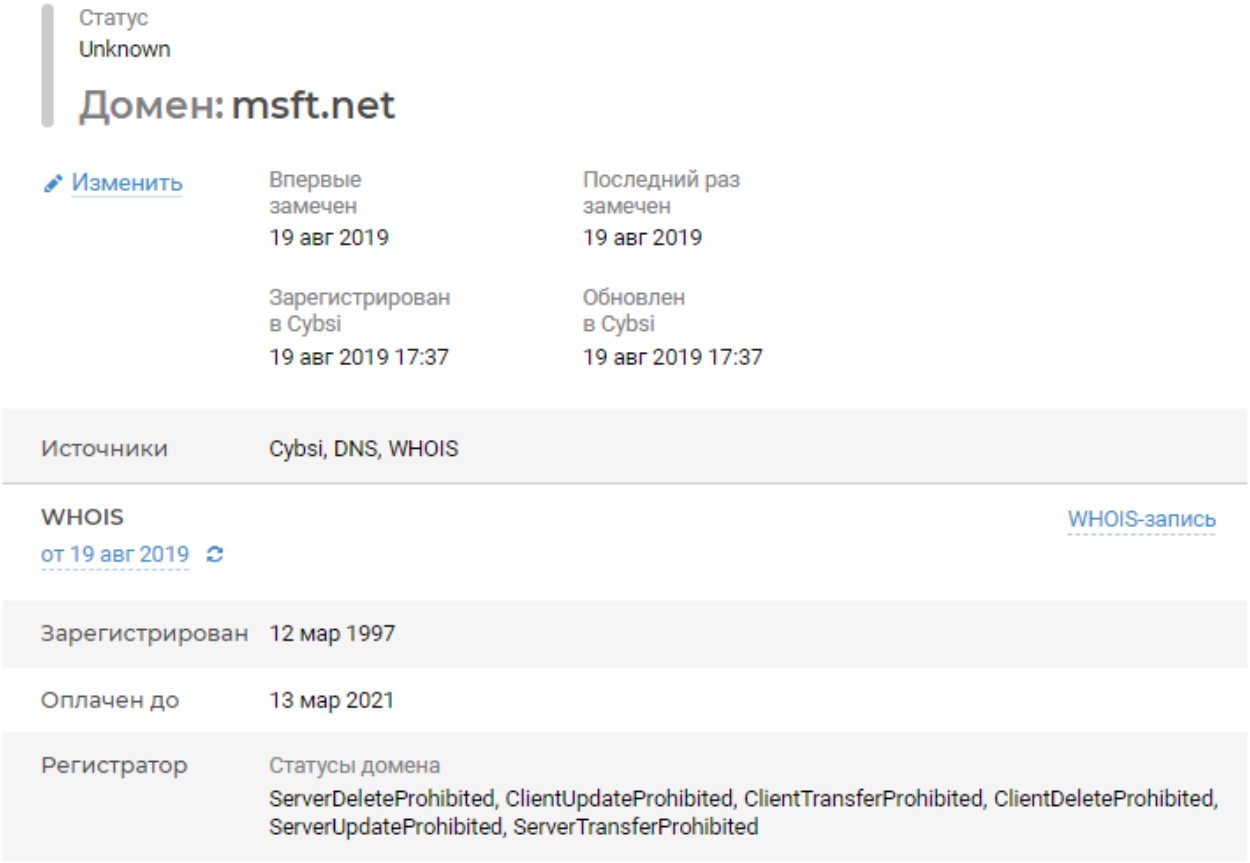

Рисунок 7. Просмотр WHOIS-записей о домене

2. Если требуется обновить WHOIS-записи, нажмите .
3. Нажмите ссылку с датой последнего изменения WHOIS-записей.

   В левой части страницы отобразится панель с историей изменений WHOIS-записей.
4. Раскройте строку с датой изменения, чтобы просмотреть последнюю измененную информацию.

11.2. Работа с DNS-записями

DNS-записи о домене и IP-адресе отображаются в карточках этих объектов.

Блок DNS в карточке домена может содержать:

— дату и время получения DNS-записей о домене;

— список IP-адресов, полученный из A- и AAAA-записей домена;

— NS-запись (список DNS-серверов, обслуживающих домен);

— CNAME-запись (список поддоменов или других доменов, привязанных к этому имени домена);

— MX-запись (список почтовых серверов, с которыми связан домен);

— TXT-запись (любая текстовая информация о домене в произвольной форме);

— SOA-запись (начальная запись DNS-зоны).

Блок DNS в карточке IP-адреса может содержать дату и время получения DNS-записи об IP-адресе, PTR-запись (IP-адреса узла, привязанный к его доменному имени).

DNS-записи об объекте могут изменяться, вы можете просмотреть историю изменений DNS-записей об объекте и обновить DNS-записи вручную.

► Чтобы просмотреть историю изменения DNS-записей:

1. Перейдите на страницу домена или IP-адреса.

   В блоке DNS отобразится обогащенная информация об объекте.

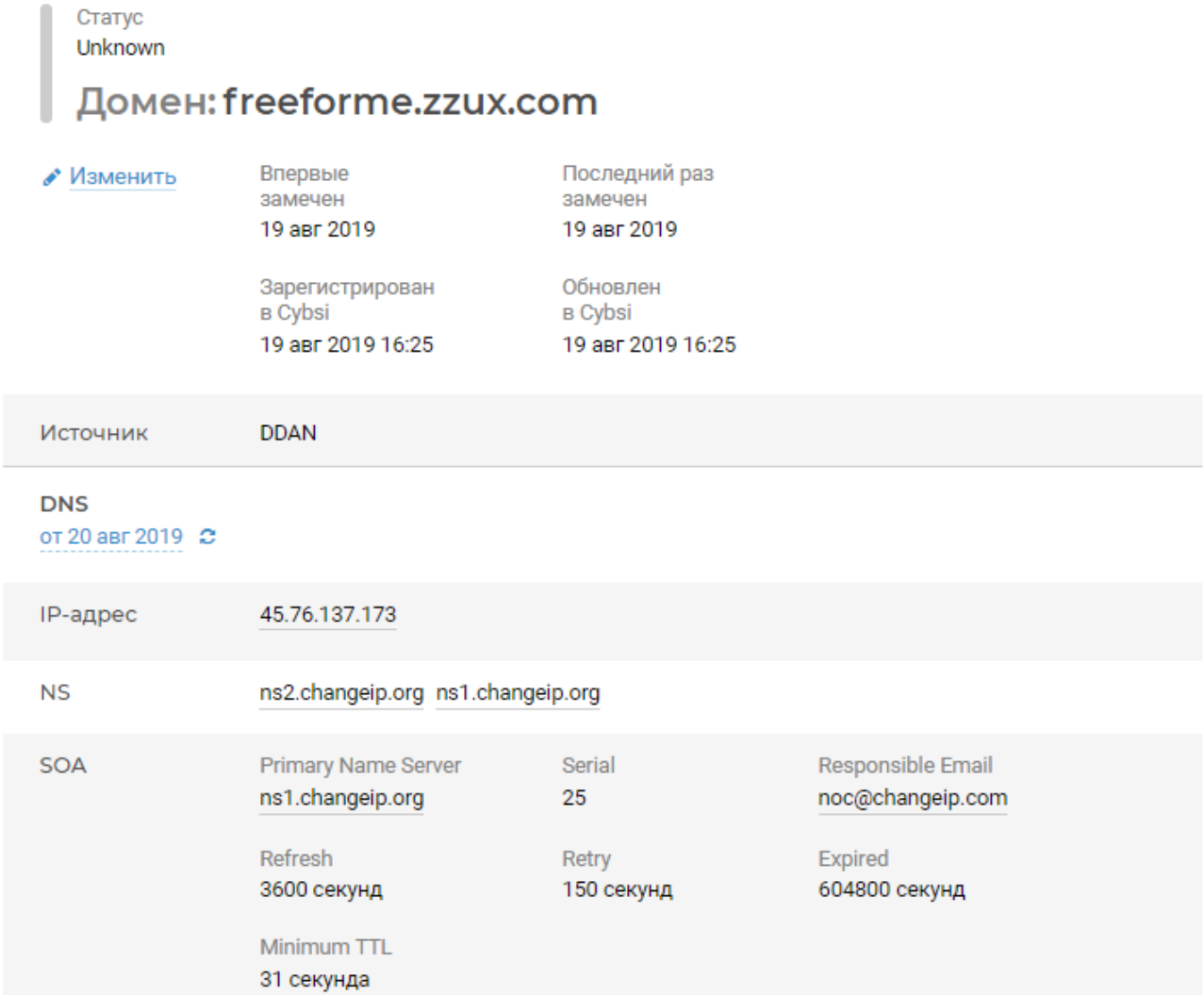

Рисунок 8. Просмотр DNS-записей о домене

2. Если требуется обновить DNS-записи, нажмите ↻.

3. Нажмите ссылку с датой последнего изменения DNS-записей.

   В левой части страницы отобразится панель с историей изменений DNS-записей.

4. Раскройте строку с датой изменения, чтобы просмотреть последнюю измененную информацию.

11.3. Сканирование файлов

Анализаторы кода проверяют файл на наличие вредоносного ПО. По результатам проверки Cybsi присваивает файлу уровень опасности.

Вы можете выполнить сканирование файла, если Cybsi загрузила его образец из внешних источников вместе с данными об объекте или если вы загрузили образец вручную при регистрации нового файла.

Если анализатор кода является одновременно и песочницей (Trend Micro Deep Discovery Analyzer или Positive Technologies MultiScanner), то помимо сканирования файла будет проведен и его поведенческий анализ.

► Чтобы выполнить сканирование:

1. На странице просмотра файла нажмите ссылку **Сканирование не проводилось**.

   В левой части страницы отобразится панель **Результаты сканирования**.

2. Выберите вкладку с анализатором кода.

   Примечание. Вы можете просканировать файл всеми анализаторами одновременно, выбрав вкладку **Сводный результат**.

3. Нажмите кнопку **Сканировать**.

   Анализатор начнет сканировать файл. По завершении сканирования отобразится список вредоносного ПО, содержащегося в файле.

Результаты сканирования

Сводный результат | PT MultiScanner | VirusLocal | Trend Micro Deep Discovery Analyzer

5 из 6 Win32/TrojanClicker.Tiny.NAM

Сканировать

Антивирус	База обновлена	Результаты сканирования	Дата сканирования
Clam AV	16 сент 2019	Угроз не обнаружено	20 сент 2019
DrWeb AV	20 сент 2019	Trojan.Flood.22062	20 сент 2019
ESET-NOD32 AV	20 сент 2019	Win32/TrojanClicker.Tiny.NAM	20 сент 2019
NANO AV	19 сент 2019	Trojan.Win32.Crypted.dlnpqg	20 сент 2019
Trend Micro AV	18 сент 2019	TROJ_VFLOOD.SMCF	20 сент 2019
Windows Defender AV	20 сент 2019	Unknown Trojan:Win32/Vflooder.B	20 сент 2019

Рисунок 9. Сканирование файла

Примечание. Вы можете получить дополнительную информацию о найденном вредоносном ПО на сайте анализатора, наведя курсор мыши на строку с названием вредоносного ПО и нажав .

11.4. Поведенческий анализ файлов

Вы можете выполнить поведенческий анализ вредоносного файла, если Cybsi загрузила его образец из внешних источников вместе с данными об объекте или если вы загрузили образец вручную при регистрации нового файла.

Если песочница для поведенческого анализа является одновременно и анализатором кода (Trend Micro Deep Discovery Analyzer или Positive Technologies MultiScanner), то помимо поведенческого анализа будет проведено и его сканирование.

► Чтобы выполнить поведенческий анализ:

1. На странице просмотра файла выберите вкладку **Поведенческий анализ**.
2. Нажмите ссылку **Выполнить анализ** и выберите песочницу.

Запустится поведенческий анализ файла. По завершении анализа отобразится отчет. Вы также можете просмотреть исходный отчет, который поступает в Cybsi в необработанном виде по ссылке **Raw-запись отчета**, или просмотреть отчет в песочнице по кнопке .

Примечание. Вы также можете выполнить поведенческий анализ в интерфейсе песочницы, перейдя в нее по ссылке **Перейти в песочницу**.

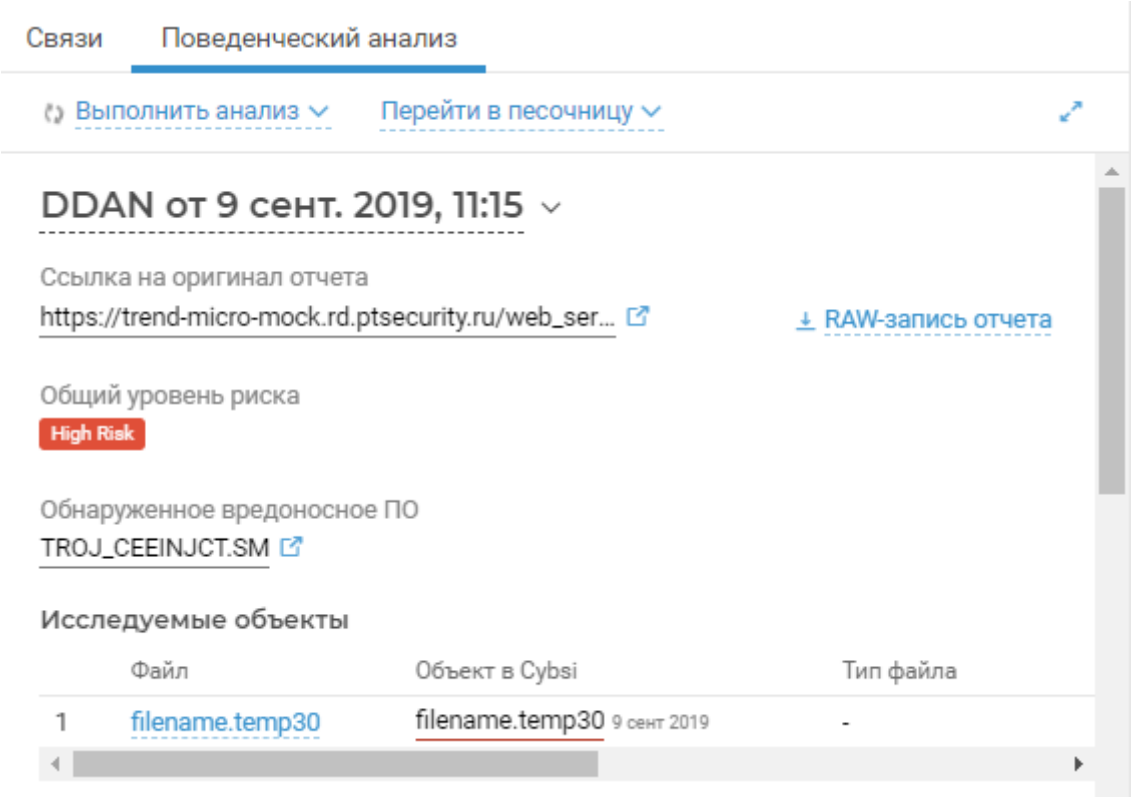

Рисунок 10. Просмотр результатов поведенческого анализа

По итогам поведенческого анализа Cybsi присваивает файлу уровень опасности и по необходимости дополняет информацию о файле, устанавливает новые связи файла с другими объектами.

12. Регистрация объектов вручную

Помимо автоматической регистрации объектов из внешних источников в Cybsi предусмотрена возможность регистрации объектов и их атрибутов вручную оператором.

В этом разделе

12.1. Общий сценарий регистрации объекта

Сценарий регистрации объекта в Cybsi является общим для всех объектов, за исключением регистрации файла с использованием образца (см. раздел 12.4).

► Чтобы зарегистрировать объект в Cybsi:

1. В главном меню в разделе **Зарегистрировать** выберите необходимый объект.

   Откроется страница регистрации объекта.

2. Укажите необходимые атрибуты объекта (см. раздел 12.2).

   Примечание. Вы также можете указать пользовательскую информацию об объекте (см. раздел 12.3).

3. Нажмите кнопку **Зарегистрировать**.

Объект зарегистрирован.

12.2. Атрибуты объекта

Этот раздел содержит информацию об атрибутах, которые идентифицируют и характеризуют объект в Cybsi. Атрибуты, однозначно идентифицирующие объект, называются ключевыми. Ключевые атрибуты необходимо обязательно указывать при регистрации объекта, по ним вы можете искать объекты в базе данных Cybsi.

Таблица 2. Атрибуты объектов в Cybsi

Объект	Атрибут	Описание
Файл	Хеш-суммы	Ключевой атрибут. Возможны три типа хеш-сумм: SHA-256, SHA-1, MD5

Объект	Атрибут	Описание
	Статус	Уровень опасности файла
	Тип файла	MIME-тип файла
	Семейства вредоносного ПО	Семейство, к которому принадлежит вредоносный файл
	Пути к файлу	Расположение файла на компьютере, где он был замечен
Домен	Домен	Ключевой атрибут. Формат записи домена должен соответствовать стандартам RFC 1034 и RFC 5890
IP-адрес	IP-адрес	Ключевой атрибут. IP-адрес стандарта IPv4 или IPv6
Человек / Компания	Имя / Название	Ключевой атрибут. Имя человека или название организации
	Категория	Организационная структура объекта
	Сфера деятельности	Коммерческий или индустриальный сектор, к которому относится человек или компания
	Родительские сущности	Один или несколько объектов, которые находятся выше в иерархической структуре по отношению к создаваемому объекту
	Дочерние сущности	Один или несколько объектов, которые находятся ниже в иерархической структуре по отношению к создаваемому объекту
	Телефоны	Телефонные номера, принадлежащие человеку или компании
	Факсы	Номера факсов, принадлежащие человеку или компании
	Адреса эл. почты	Адреса электронной почты, принадлежащие человеку или компании
URL	URL	Ключевой атрибут. URL сайта или страницы сайта
Семейство вредоносного ПО	Название	Ключевой атрибут. Название семейства
	Типы	Один или несколько типов, к которым относятся файлы в семействе
Адрес эл. почты	Адрес эл. почты	Ключевой атрибут. Адрес электронной почты в соответствии со стандартом RFC 5322

Объект	Атрибут	Описание
	Имена отправителя	Введите имя отправителя электронного письма, которое отображается в почтовом приложении
Телефон	Номер	Ключевой атрибут. Основной номер телефона
	Добавочные номера	Ключевой атрибут. Добавочный номер телефона. Максимальная длина — 5 цифр
Уязвимость	Название	Ключевой атрибут. Тип идентификатора уязвимости и соответствующее ему значение

12.3. Пользовательская информация об объекте

Пользовательская информация не является атрибутом объекта, но позволяет дополнительно характеризовать его. Пользовательскую информацию не обязательно указывать при регистрации объекта, и она может быть изменена после его регистрации.

Таблица 3. Пользовательская информация об объекте в Cybsi

Название	Описание
Уровень доступа	Уровень доступа к данным об объекте
Метки	Справочные метки для быстрого поиска объекта в базе Cybsi. При регистрации любых объектов вы можете выбирать существующие справочные метки или задавать свои
Информация	Дополнительная информация об объекте
Внешние ресурсы	Ссылка на сайт, который содержит информацию об объекте

12.4. Регистрация файлов с использованием образца

Вы можете регистрировать в Cybsi файлы с использованием образца. Если в качестве образца выступает архив, то для каждого файла в архиве будет зарегистрирован отдельный объект.

► Чтобы зарегистрировать в Cybsi файл с использованием образца:

1. В главном меню в разделе **Зарегистрировать** выберите пункт **Файл**.

   Откроется страница регистрации файла.

2. Нажмите кнопку **Загрузить файл**.
3. В открывшемся окне перетащите файл в область загрузки или загрузите файл по ссылке **выберите**.

4. Если вы загружаете файл в архиве, защищенном паролем, установите флажок **Архив** и введите пароль.
5. Нажмите кнопку **Загрузить**.

   На странице регистрации файла отобразятся название загруженного файла, его тип и хеш-суммы.

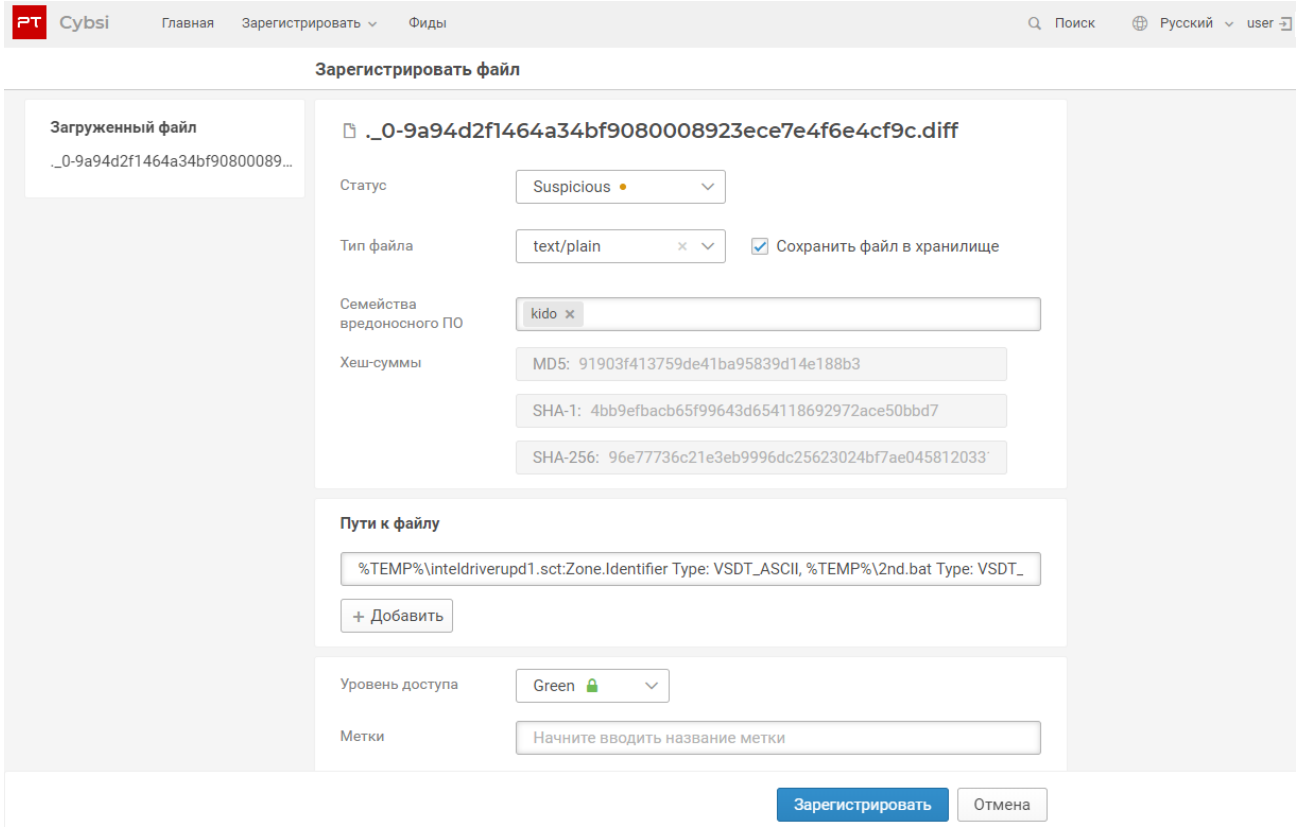

Рисунок 11. Регистрация файла с использованием образца

6. Снимите флажок **Сохранить файл в хранилище**, если вы хотите исключить загрузку образца файла в базу Cybsi.

   При этом атрибуты файла (название, тип, хеш-суммы) будут сохранены.
7. Нажмите кнопку **Зарегистрировать**.

Файл зарегистрирован.

12.5. Выборочная регистрация файлов из архива

Если в качестве образца выступает архив, вы можете регистрировать в Cybsi не весь архив, а только отдельные файлы из этого архива.

► Чтобы зарегистрировать в Cybsi отдельные файлы из архива:

1. В главном меню в разделе **Зарегистрировать** выберите пункт **Файл**.

Откроется страница регистрации файла.

2. Нажмите кнопку **Загрузить файл**.
3. В открывшемся окне перетащите архив с файлами в область загрузки или загрузите архив по ссылке **выберите**.
4. Если архив защищен паролем, установите флажок **Архив** и введите пароль.
5. Нажмите кнопку **Загрузить**.

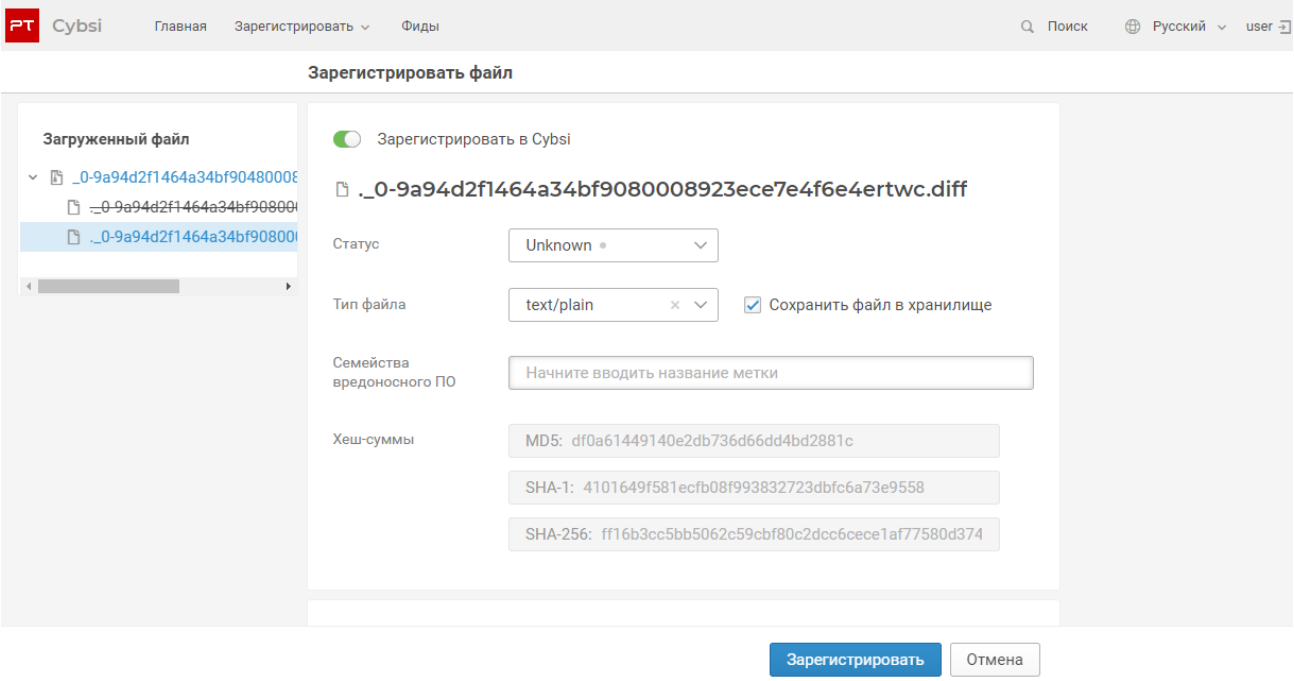

Рисунок 12. Выборочная регистрация файлов из архива

На странице регистрации файла отобразятся название загруженного архива, его тип и хеш-суммы, а также файлы, входящие в архив.

6. Выберите архив или файл в левой части страницы и выключите его регистрацию.
7. Снимите флажок **Сохранить файл в хранилище**, если вы хотите исключить загрузку образца архива или отдельного файла в базу Cybsi.

   При этом атрибуты файла или архива (название, тип, хеш-суммы) будут сохранены.
8. Нажмите кнопку **Зарегистрировать**.

Выбранные файлы зарегистрированы.

12.6. Регистрация объектов через связи

Регистрация объектов вручную по одному может занимать длительное время. Поэтому в Cybsi предусмотрена возможность одновременной регистрации нескольких объектов через их связи.

Например, у вас есть письменный отчет о расследовании вредоносной кампании. Отчет содержит информацию о хеш-суммах вредоносных файлов, названиях семейств вредоносного ПО, доменах, IP-адресах и других индикаторах компрометации, связанных с этой кампанией. Вы можете зарегистрировать в Cybsi объект типа файл, а затем связать этот объект со всеми содержащимися в письменном отчете индикаторами компрометации. При этом индикаторы будут зарегистрированы в Cybsi как новые объекты. Cybsi обеспечивает уникальность индикаторов. Если объект, регистрируемый через связь, уже есть в Cybsi, связь будет зарегистрирована с существующим объектом.

► Чтобы зарегистрировать объект через связь:

1. Откройте страницу зарегистрированного ранее объекта, через связи с которым вы хотите зарегистрировать новые объекты.
2. На вкладке **Связи** нажмите кнопку **Зарегистрировать** напротив типа связи.

   Отобразится панель регистрации новой связи.
3. Если требуется, в раскрывающемся списке **Тип объекта** выберите тип регистрируемого через связь объекта.
4. Укажите ключевой атрибут объекта (см. раздел 12.2).

   Примечание. Вы можете регистрировать несколько объектов одного типа (например, несколько доменов), указывая их через точку с запятой. Для каждого ключевого атрибута в Cybsi будет зарегистрирован отдельный объект. При регистрации файла, который содержит несколько хеш-сумм, необходимо указывать только одну из них. В противном случае для каждой хеш-суммы одного файла в Cybsi будет зарегистрирован отдельный объект со связью.
5. Если требуется, в раскрывающемся списке **Уровень доступа** выберите уровень доступа для регистрируемого через связь объекта.

   Примечание. Если регистрируемый объект уже есть в Cybsi, то уровень доступа у регистрируемого объекта не может быть ниже, чем у существующего.
6. Если требуется, добавьте описание связи, метки и дату установки связи.

   Примечание. По умолчанию датой установки связи является текущая дата.
7. Нажмите кнопку **Зарегистрировать**.

Объект зарегистрирован.

13. Работа с фидами

Фид — это обновляемые данные с заданной структурой их представления. В Cybsi существуют два типа фидов:

— Внешние. Поступают в Cybsi из внешних источников (Malware Information Sharing Platforms и AlienVault), содержат экспертные данные об угрозах ИБ и индикаторы компрометации. На основе таких фидов Cybsi формирует объекты.

— Пользовательские. Формируются пользователями в интерфейсе Cybsi для экспорта во внешние системы и организации. Содержат данные об угрозах ИБ и индикаторы компрометации, специфичные для сферы деятельности и внутренних задач определенного заказчика.

Примером пользовательского фида может служить набор IP-адресов, доменов и URL командных центров для вредоносного ПО. Межсетевой экран с загруженным в него таким фидом будет предупреждать о том, что в сети организации происходят подключения к командным центрам.

Данные, хранящиеся в фиде, постоянно обновляются. Чтобы предоставлять заказчику наиболее актуальную информацию, Cybsi делает срез данных фида с частотой, заданной при создании фида. Вы можете выгрузить последний сделанный срез из Cybsi в виде файла и передать его заказчику.

В этом разделе

13.1. Создание и активация фида

► Чтобы создать и активировать фид:

1. В главном меню выберите раздел **Фиды**.

   Откроется страница **Фиды**.

2. Нажмите кнопку **Создать**.
3. В поле **Название** введите название фида.
4. В поле **Часть ссылки на фид** введите префикс, который будет указан в названии файлов со срезами данных фида.
5. В раскрывающемся списке **Формат** выберите формат экспорта фида.

Примечание. В настоящее время Cybsi поддерживает экспорт фидов только в формате JSON.

6. В поле **Частота обновления** укажите временной промежуток, через который фид будет обновляться в системе.
7. В блоке **Правило формирования фида** нажмите ссылку выбора сохраненных фильтров.

   В правой части страницы отобразится панель **Сохраненные фильтры** со списком существующих фильтров.
8. Раскройте необходимый фильтр.

   Отобразятся объекты и атрибуты, которые попадут в фид.
9. Нажмите кнопку **Выбрать фильтр**.

   При создании фида Cybsi будет использовать сохраненный фильтр. В блоке **Атрибуты для вывода** отобразятся объекты и атрибуты, данные о которых будут представлены в экспортированном файле.

   Примечание. Вы можете просмотреть, какие объекты попадают в фид, по кнопке **Проверить правило**.

Название: Malicious_hash_feed

Часть ссылки на фид: malicious_hash_feed

cybsi-integration.rd.ptsecurity.ru/feeds/api/malicious_hash_feed

Форматы: JSON ×

Частота обновления: 1 час

Введите значение от 1 до 24

Правило формирования фида

Используйте в качестве правила один из сохраненных фильтров.

Проверить правило

Замечен в период: За 2 недели

Общие атрибуты

Тип объекта: Файл

Атрибуты для вывода

Файл

Идентификатор объекта | Тип объекта | Замечен впервые | Последний раз замечен

MD5 | SHA-1 | SHA-256

Создать | Отмена

Рисунок 13. Создание фида

10. Нажмите кнопку **Создать**.
11. Активируйте фид по кнопке **Активировать**.

Фид создан и активирован. Активированный фид формирует срезы данных в Cybsi с заданной частотой.

13.2. Изменение частоты формирования среза данных

Частота формирования среза данных фида задается при создании фида. Вы можете изменить частоту, чтобы передавать заказчику более актуальную информацию об угрозах ИБ.

► Чтобы изменить частоту формирования среза данных фида:

1. В главном меню выберите раздел **Фиды**.

   Откроется страница **Фиды**.

2. Выберите фид в списке.

   Откроется страница фида.

3. По значку измените частоту формирования среза данных фида.

13.3. Скачивание среза данных фида

Вы можете скачивать созданный в Cybsi срез данных фида и передавать его во внешние системы. Cybsi хранит только последний сформированный срез, этот срез выгружается при скачивании.

► Чтобы скачать срез данных фида:

1. В главном меню выберите раздел **Фиды**.

   Откроется страница **Фиды**.

2. Выберите фид в списке.

   Откроется страница фида.

3. Нажмите кнопку **Скачать**.

Срез данных фида скачан. Вы можете передать файл заказчику удобным для вас способом.

13.4. Деактивация фида

Активированный фид формирует срезы данных в Cybsi. Процесс формирования срезов данных — ресурсоемкий и снижает скорость работы с системой, поэтому неиспользуемый фид рекомендуется деактивировать.

► Чтобы деактивировать фид:

1. В главном меню выберите раздел **Фиды**.

   Откроется страница **Фиды**.

2. Выберите фид в списке.

Откроется страница фида.

3. Нажмите кнопку **Деактивировать**.

Фид деактивирован.

13.5. Удаление фида

Вы можете удалить фид, предварительно деактивировав его.

► Чтобы удалить фид:

1. В главном меню выберите раздел **Фиды**.

   Откроется страница **Фиды**.

2. Выберите фид в списке.

   Откроется страница фида.

3. Нажмите кнопку **Деактивировать**.
4. Нажмите ⋮, в раскрывшемся меню выберите **Удалить фид** и подтвердите удаление.

Фид удален.

14. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале support.ptsecurity.com или по телефону. Запросы на портале — основной способ обращений за технической поддержкой.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

14.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

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

Портал технической поддержки доступен на русском, английском, немецком и итальянском языках.

14.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по следующим телефонам:

- Великобритания +44 20 3769 3606
- Италия +39 06 9763 1532
- Казахстан +7 727 350 52 92
- Россия +7 495 744 01 44
- США +1 857 208 7273
- Чехия +420 530 510 700
- Южная Корея +82 2 6410 8582

Техническая поддержка по телефону предоставляется на русском и английском языке.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданному запросу.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте запрос на портале support.ptsecurity.com. Запрос на портале, созданный и обновляемый по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

14.3. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся запросам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

14.4. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

14.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста "Позитив Текнолоджиз" нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

"Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

14.4.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист "Позитив Текнолоджиз" оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). "Позитив Текнолоджиз" не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

"Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, "Позитив Текнолоджиз" обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

14.4.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 4).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 4. Время реакции на запрос и время его обработки

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта	До 24 часов	Не ограничено

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
	и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес		
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

14.4.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, "Позитив Текнолоджиз" включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;

- проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;
- проблема классифицирована как неподдерживаемая.

Глоссарий

Атрибут объекта

Необходимое свойство, характеризующее объект.

Внешний фид

Фид, поступающий в Cybsi из внешних источников, содержит экспертные данные об угрозах информационной безопасности и индикаторы компрометации. На основе внешних фидов Cybsi формирует объекты.

Индикатор компрометации

Сущность, наблюдаемая в сети или в операционной системе и указывающая на вредоносную активность в инфраструктуре.

Ключевой атрибут объекта

Атрибут, однозначно идетнифицирующий объект.

Обогащение

Дополнительная обработка индикаторов компрометации в Cybsi, в результате которой информация об индикаторах дополняется.

Объект

Сущность в Cybsi, связанная с информационной безопасностью и характеризуемая одним или несколькими атрибутами. Объекты поступают в Cybsi из внешних источников или регистрируются пользователями вручную в интерфейсе.

Платформа threat intelligence

Платформа анализа и обработки данных о существующих и потенциальных угрозах информационной безопасности, а также способах их обнаружения.

Поведенческий анализ

Метод проверки файла, в ходе которой выполняется анализ поведения файла в виртуальном окружении, изолированном от информационной системы организации.

Пользовательский фид

Фид, формируемый пользователем в интерфейсе Cybsi для экспорта во внешние системы и организации. Содержит данные об угрозах ИБ и индикаторы компрометации, специфичные для сферы деятельности и внутренних задач определенного заказчика.

Связь объектов

Зависимость между двумя объектами, один из которых может не являться вредоносным, но связан с другим вредоносным объектом.

Срез данных фида

Набор данных фида, существующий в Cybsi в настоящий момент.

Фид

Обновляемые данные с заданной структурой их представления.

Предметный указатель

О компании

"Позитив Текнолоджиз" — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения "Позитив Текнолоджиз" для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты "Позитив Текнолоджиз" заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com