ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Endpoint Detection and Response»

Описание процессов, обеспечивающих поддержание жизненного цикла

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Определение
АС	Автоматизированная Система
Заказчик	Зарегистрированный пользователь в системе заказчика передавший третьим лицам все необходимы данные и реквизиты для управления приложением или выполняющий указания третьих лиц за вознаграждение.
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО БУДУЩЕЕ • Компанией-интегратором, по выбору Заказчика
ОС	Операционная Система
ПО	Программное обеспечение F6 Endpoint Detection and Response.
ТС	(«Технический Сервис») Система взаимодействия Заказчика, позволяющая обмениваться сообщениями и создавать цепочки обращений, которая представляет из себя отдельный раздел «Службу Поддержки» в панели управления «F6 Endpoint Detection and Response». В случае недоступности указанных систем формат взаимодействия осуществляется через электронный почтовый ящик.
APT	Advanced Persistent Threat, постоянная угроза повышенной сложности
DLP	Data Leak Prevention, Предотвращение утечек
IP	Internet Protocol
MAC	Media Access Control
MDP	F6 Malware Detonation Platform
MFT	Master File Table
MXDR	Программный комплекс Managed Extended Detection and Response (Managed XDR)

MXDR Console	F6 XDR, MXDR
NTFS	New Technology File System
pytest	Фреймворк для тестирования кода на Python.
RPM	RPM Package Manager
selenium	Инструмент для автоматизации действий веб-браузера.
SIEM	Security Information and Event Management
UEFI	Extensible Firmware Interface
USB	Universal Serial Bus

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание процессов поддержания жизненного цикла программного обеспечения «F6 Endpoint Detection and Response» (далее – ПО, F6 Endpoint Detection and Response, EDR). Поддержание жизненного цикла ПО осуществляется за счет его сопровождения в течение всего периода эксплуатации и совершенствования (проведения обновлений) согласно собственному плану разработки и по заявкам Пользователей.

1.2 Назначение ПО

«F6 Endpoint Detection and Response» — это модуль системы MXDR (Managed XDR) который специализируется на обнаружении, расследовании и реагировании на угрозы, направленные на конечные точки, такие как рабочие станции. ПО обеспечивает защиту от различных киберугроз, включая вредоносное ПО, программы-вымогатели и сложные атаки, такие как APT (Advanced Persistent Threat). При обнаружении угрозы ПО предлагает инструменты для быстрого реагирования на инциденты, что включает изоляцию, расследование и устранение угрозы. Решение также обладает мощными функциями форензики и анализа инцидентов, что помогает понять коренные причины атаки и предотвратить повторные инциденты. ПО поддерживает автоматизацию процессов защиты и позволяет настраивать политики безопасности в соответствии с потребностями организации, а также интегрируется с SIEM и другими системами для комплексного управления инцидентами. ПО доступно в виде клиента для операционных систем Windows, Linux и macOS.

1.3 Функциональные возможности ПО

1.3.1 Функциональные возможности ПО применительно к конечным станциям на базе ОС семейства Microsoft Windows

ПО обладает следующими функциональными возможностями:

- ПО обеспечивает совместимость с установленными антивирусами и DLP-системами заказчика.
- ПО не оказывает негативного влияния на производительность рабочей станции при соблюдении системных требований.
- ПО собирает следующие типы событий:

- События, связанные с процессами: создание и завершение процессов, создание потоков, подгрузка динамических библиотек.
- События, связанные с файлами: создание, открытие, удаление, изменение содержимого, имени и атрибутов файлов, создание ссылок, изменение теневых копий.
- События, связанные с сетью: открытие сетевых соединений, привязка портов к процессам, DNS-запросы, создание общих папок.
- События, связанные с системой: подключение периферийных устройств, создание объектов в диспетчере объектов Windows, выключение станции, создание сервисов и отложенных задач, изменения в настройках локального сетевого экрана.
- События, связанные с реестром: создание, открытие, удаление, переименование ключей и изменение их значений.

– ПО предоставляет функционал для сбора и передачи криминалистически значимых данных на MXDR Console, включая содержимое папки Temp, историю браузеров, журналы событий Windows, фрагменты реестра, NTFS MFT, дампы UEFI прошивки, файлы гибернации и подкачки, дампы оперативной памяти, списки автозагрузок, запущенных процессов и служб, отложенных задач, созданных именованных каналов и открытых сетевых соединений.

– ПО совместно с MXDR Console поддерживает возможность сетевой изоляции конечной станции от глобальной и локальной сети.

– ПО совместно с MXDR Console предоставляет возможность удаленного терминального доступа к конечной станции через веб-интерфейс, независимо от статуса сетевой изоляции.

– ПО обеспечивает логирование удаленного терминального подключения, запросов на сбор криминалистически значимых данных и запросов на сетевую изоляцию через веб-интерфейс.

– ПО позволяет настраивать отправку исполняемых файлов (.exe) и установочных файлов (.msi) для проверки в подсистему поведенческого анализа (MDP) по критериям, таким как недействительная или отсутствующая цифровая подпись, загрузка из интернета, удаление антивирусами.

– ПО автоматически блокирует и помещает в карантин вредоносные файлы, ранее проанализированные подсистемой поведенческого анализа.

– ПО обеспечивает инвентаризацию установленных и удаленных приложений.

– ПО предоставляет возможность настройки политик блокировки для различных действий, таких как запуск методов установки приложений, приложений с недействительной подписью, скриптовых файлов и appx приложений.

– ПО поддерживает создание индивидуальных правил блокировки запуска приложений.

– ПО совместно с MXDR Console создает события информационной безопасности по группе событий, основываясь на поведенческих правилах.

– События информационной безопасности включают полный перечень запущенных процессов, граф процессов, формирующих события, и индикацию вредоносных процессов.

– ПО предоставляет централизованное представление о работе каждого процесса, включая данные о взаимодействии на уровне реестра, файловой системы, сетевой активности, мьютексах, метаданные процесса и перечень импортированных динамических библиотек с результатами проверки цифровой подписи и потоками исполнения.

– ПО позволяет остановку процессов через веб-интерфейс.

– ПО поддерживает Sigma правила.

– ПО логирует IP и MAC адреса сетевых периферийных устройств конечной станции.

– Подсистема поддерживает установку на операционные системы Windows старше Windows 7 SP1 и Windows Server старше 2008 R2 x64.

1.3.2 Функциональные возможности ПО применительно к конечным станциям на базе ОС ядра Linux

ПО обладает следующими функциональными возможностями:

– ПО поддерживает установку на операционные системы с ядром версии старше 3.10 и дистрибутивы, такие как Arch-based (Arch, Manjaro), Debian-based (Ubuntu 20.04+, Ubuntu Server, Linux Mint), RedHat-based (CentOS 7+, Fedora 33+, Oracle Linux 8, RedOS), которые используют систему инициализации systemd.

– ПО совместимо с установленными антивирусами и DLP-системами заказчика.

– ПО не влияет на производительность рабочей станции при соблюдении системных требований.

– ПО осуществляет сбор различных типов событий, включая:

- События, связанные с процессами: создание новых процессов (clone, fork, exec), завершение процессов, изменение прав доступа к памяти процесса, отслеживание ptrace логов.

- События, связанные с файлами: создание, открытие, удаление файлов и изменение их содержимого, изменение имени, прав доступа и владельца файлов, создание и удаление директорий.
- События, связанные с сетью: открытие сетевых соединений, привязка портов к процессам, DNS-запросы.
- События, связанные с системой: подключение и отключение USB-устройств.
- События, связанные с аудит логами: создание и удаление пользователей и групп, авторизация и выход пользователей, запуск и остановка системных сервисов.

– (или EDR), совместно с MXDR Console, предоставляет функционал для сбора и передачи криминалистически значимых данных, включая:

- Приложения, установленные с помощью пакетных менеджеров pacman, RPM и Debian.
- Отложенные задачи, история оболочки shell, Linux lock file, аутентифицированные пользователи.
- Настройки SSH, SELinux, AppArmor, модули ядра.
- Сетевые маршруты, группы пользователей, файл /etc/shadow, Unix-сокеты, DNS резолвы, сетевые интерфейсы, периферийные устройства, информация о точках монтирования, fstab, init subsystem.

– ПО совместно с MXDR Console, поддерживает сетевую изоляцию конечной станции от глобальной и локальной сети.

– ПО обеспечивает удаленный терминальный доступ к конечной станции через веб-интерфейс, независимо от статуса сетевой изоляции.

– ПО поддерживает Sigma правила.

– MXDR Console логирует удаленное терминальное подключение, фиксируя перечень введенных команд и результаты их исполнения, запросы на сбор криминалистически значимых данных и запросы на сетевую изоляцию через веб-интерфейс.

1.3.3 Функциональные возможности ПО применительно к конечным станциям на базе ОС семейства macOS

– ПО поддерживает установку на операционные системы macOS 10.15.0 Catalina и выше.

– ПО совместимо с установленными антивирусами и DLP-системами заказчика.

– ПО не влияет на производительность рабочей станции при соблюдении системных требований.

– ПО осуществляет сбор различных типов событий, включая:

- События, связанные с процессами: создание и завершение процессов, изменение директорий процессов (только для macOS 10.15.1 и выше).
- События, связанные с файлами: создание файлов, закрытие файлов, изменение размера, переименование/перемещение файлов, удаление/изменение счетчика ссылок на файлы.
- События, связанные с сетью: входящие и исходящие соединения.

– ПО совместно с MXDR Console, предоставляет функционал для сбора и передачи криминалистически значимых данных, включая:

- Настройки SSH.
- Историю оболочки shell.
- Настройки профилей Apple.
- Настройки конфигураций автоматического старта процессов.
- Файлы из директории /etc/.
- Файлы с логами из всех стандартных папок, включая логи агента и системного расширения.

– ПО, совместно с MXDR Console, поддерживает сетевую изоляцию конечной станции от глобальной и локальной сети (за исключением системных обращений, которые нельзя изолировать).

– ПО поддерживает Sigma правила.

– MXDR Console логирует запросы на сбор криминалистически значимых данных и запросы на сетевую изоляцию хоста через веб-интерфейс.

2 Процесс разработки ПО

Процесс разработки ПО включает в себя:

- Сбор и анализ требований к разработке ПО;
- Проектирование архитектуры ПО;
- Разработка ПО в коде;
- Проведение тестирования ПО перед эксплуатацией;
- Запуск в промышленную эксплуатацию ПО;
- Промышленная эксплуатация ПО;
- Сопровождение ПО.

2.1 Сбор и анализ требований к разработке ПО

На этапе сбора и анализа требований ПО определяются требования всех заинтересованных сторон, включая функциональные и нефункциональные требования.

Основные этапы сбора и анализа требований к разработке ПО:

- Определение основных задач и целей, которые должен решить проект ПО;
- Определение ключевых заинтересованных сторон (заказчики, пользователи, разработчики, другой персонал);
- Сбор требований к ПО;
- Анализ требований, их уточнение, пересмотр на точность и реализуемость;
- Оценка рисков;
- Создание плана и графика реализации проекта;
- Документирование требований и проектных планов;
- Согласование и утверждение требований.

2.2 Проектирование архитектуры ПО

Проектирование архитектуры ПО – это процесс определения общей структуры системы, ее компонентов и модулей, а также взаимодействия между компонентами системы на основе выработанных требований.

Проектирование архитектуры включает в себя следующие этапы:

- Определение архитектурного стиля;
- Определение основных модулей и компонентов системы, их взаимодействие;
- Выбор технологий (языки программирования, базы данных и т.д.) и инструментов для разработки ПО;
- Документирование архитектуры системы.

2.3 Разработка ПО в коде

На этапе разработки ПО в коде осуществляется реализация проектных решений с помощью выбранных технологий и инструментов.

Разработка ПО включает в себя следующие этапы:

- Написание исходного кода ПО с использованием выбранных технологий и инструментов;
- Проверка кода на наличие ошибок и несоответствий;
- Проведение интеграционного тестирования;
- Отладка кода (исправление обнаруженных ошибок);
- Проверка кода для улучшения качества ПО, его производительности и безопасности;
- Интеграция частей кода и модулей ПО в единую систему, проверка их совместимости;
- Подготовка к тестированию ПО перед эксплуатацией.

2.4 Проведение тестирования ПО перед эксплуатацией

Тестирование ПО перед эксплуатацией – это оценка качества ПО, его функциональности, производительности и безопасности. Цель тестирования заключается в подтверждении того, что ПО удовлетворяет установленным требованиям и корректно работает в различных условиях. Тестирование включает в себя следующие этапы:

- Автоматические unit-тесты, встроенные в pipeline CI/CD процессов при работе с репозиторием хранения исходного кода;

– Автотесты с использованием Allure (pytest + selenium) с покрытием не менее 35%;

– Полуавтоматическое регрессионное тестирование на каждую вновь добавляемую новую функцию;

– Ручное тестирование: интеграционное, функции, API.

После ручного тестирования и добавления каждой функции в ПО, ручное тестирование автоматизируется и добавляется в общий банк автотестов.

2.5 Запуск ПО в промышленную эксплуатацию

Запуск в промышленную эксплуатацию – это процесс подготовки окружения для развертывания ПО на целевой среде Заказчика, а также установка и активация модуля. Запуск в промышленную эксплуатацию осуществляется силами Исполнителя.

2.5.1 Запуск ПО применительно к конечным станциям на базе ОС семейства Microsoft Windows

2.5.1.1 Проверка корректности установки агента на Стенде для проведения тестирования

Для проверки корректности установки агента на конечной станции выполняют следующее тестирование:

1. Проверить, что конечная станция, используемая для тестирования, (далее – Стенд) представляет собой виртуальное окружение и удовлетворяет всем системным требованиям.

2. Проверить, что у Стенда отсутствует сетевой доступ к корпоративной сети организации Заказчика.

3. После установки агента Стенд необходимо перезагрузить.

4. Проверить, что на Стенде установлена рекомендуемая вендором версия агента в соответствии с инструкциями по установке. Для этого необходимо проверить наличие запущенной службы агента или выполнить через командную строку *cmd.exe* от имени Администратора команды проверки установки с соответствующим результатом:

Команда	Архитектура системы	Результат
"c:\Program Files (x86)\Group-IB\THF Huntpoint\gibepcli.exe" driver-version	x64	Проверяет наличие установленного драйвера агента и выводит его версию.
"c:\Program Files\Group-IB\THF Huntpoint\gibepcli.exe" driver-version	x86	Проверяет наличие установленного драйвера агента и выводит его версию.
sc queryex "gibthfhuntpoint"	x64, x86	Выводит статус работы агента. Текущий статус будет указан в параметре “STATE” для английского и “Состояние” для русского интерфейса системы. Опция IGNORES_SHUTDOWN в данном параметре означает, что агент будет запущен после перезагрузки системы.
TASKLIST | find "gibep"	x64, x86	Проверяет запущен и работает ли агент в момент вызова команды.

5. После перезагрузки Стенда перейти в интерфейсе в раздел Моя компания → Активы, выставить быстрый фильтр “Компьютер” и убедиться, что актив Стенда в статусе онлайн (индикатор актива зеленый).

6. Если на Стенде используются снимки файловой системы и был произведен откат, необходимо вернуться на пункт 4.

2.5.1.2 Проверка корректности настроек модуля EDR

1. Перейти в раздел **Настройки → Модули → Группа хостов с Windows EDR → Основные настройки** и активировать опцию **Удаленного терминального доступа**.

2. Проверить, что в разделе **Настройки → Модули → Группа хостов с Windows EDR → Основные настройки** в блоке **События с хостов** для всех категорий событий в колонке **Статус** выставлено значение **Все включены**, кроме категории событий *userModeHooks*, которая должна иметь в колонке **Статус** значение *Отключены: userModeHooks*.

3. Проверить, что на Стенде отключены все сторонние или встроенные средства защиты конечных устройств (Антивирусы, EDR, DLP и т.д.).

4. После применения всех настроек необходимо проверить корректность применения этих настроек на уровне клиента EDR. Для этого необходимо зайти в папку с агентом, открыть файл Config.txt и проверить, что параметры выставлены в соответствии с настройками в веб-интерфейсе.

- C:\Program Files (x86)\Group-IB\THF Huntpoint
- C:\Program Files\Group-IB\THF Huntpoint

5. Далее перейти в раздел **Профиль пользователя → Безопасность и доступ → Двухфакторная аутентификация** и убедиться в наличии статуса *Аккаунт защищен двухфакторной аутентификацией*.

2.5.1.3 Проверка работоспособности функции блокировки ВПО

1. Перейти в раздел **Настройки → Модули → Группа хостов с Windows EDR → Основные настройки** и в блоке **Анализ файлов** включить опцию **Блокировать вредоносные файлы**.

2. Перейти в раздел **Расследование → Проверенные файлы**, выполнить поиск файлов, признанных вредоносными и загрузить один из таких экземпляров и перенести на Стенд.

3. Для корректного и безопасного проведения данного этапа теста крайне не рекомендуется заходить в веб-интерфейс консоли напрямую со Стенда.

4. После того, как загруженный вредоносный файл был помещен на Стенд, его необходимо извлечь из архива, в который он упаковывается для выгрузки из Web-интерфейса (пароль для извлечения указывается при скачивании). Далее необходимо осуществить попытку запуска загруженного вредоносного файла (открыть документ/запустить исполняемый файл/открыть архив).

5. Перейти в раздел **Атаки → Алерты**, выставить фильтр **Система интеграции → Huntpoint**, **Классификатор → Polygon**, выполнить поиск по имени Стенда и найти алерт о попытке открытия заблокированного файла.

2.5.1.4 Проверка работоспособности функции сбора криминалистических артефактов

Для корректного проведения данного тестирования, необходимо убедиться, что роль пользователя аналитик или админ.

1. Перейти в раздел **Моя компания** → **Активы** выполнить поиск по *machine_id* Стенда → раскрыть в правом верхнем углу меню **Реагирование** → выбрать опцию **Собрать артефакты на хосте**.

2. В открывшемся диалоговом окне выбрать опцию сбора базовых (отладочных) данных.

3. Перейти во вкладку **Реагирование** в раскрытом сайдбаре с информацией о Стенде, выбрать пункт **Артефакты**. Будет доступно отображение всех запрошенных артефактов со статусом выполнения. По итогу сбора запрошенных на предыдущем шаге данных будет доступна карточка для просмотра и скачивания собранных артефактов.

2.5.1.5 Проверка работоспособности функций удаленного терминального доступа

1. Перейти в раздел **Моя компания** → **Активы** выполнить поиск по *machine_id Стенда* → раскрыть в правом верхнем углу меню **Реагирование** → выбрать опцию **Подключиться удаленно**.

2. В открывшемся диалоговом окне ввести одноразовый код 2FA.

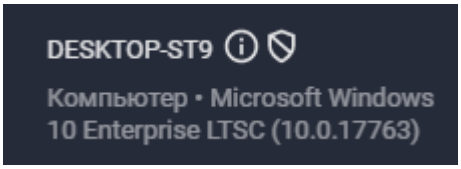
3. Далее по доступности терминала для ввода команды выполнить *ipconfig*, дождаться результата выполнения команды и после этого завершить сессию.

2.5.1.6 Проверка работоспособности функции изоляции конечной станции

1. Перейти в раздел **Моя компания** → **Активы** выполнить поиск по *machine_id* Стенда → раскрыть в правом верхнем углу меню **Реагирование** → выбрать опцию **Изолировать хост**.

2. В открывшемся диалоговом окне ввести имя компьютера, который необходимо изолировать, комментарий о причинах блокировки по необходимости и далее нажать на кнопку **Отправить**.

3. Далее в Web-интерфейсе в таблице активов рядом с записью, которая относится к Стенду, появится индикатор изоляции хоста – значок щита (скриншот ниже):



4. Далее на Стенде выполнить команду *ping 8.8.8.8* (или любой другой IP адрес, к которому компьютер имеет сетевой доступ) непосредственно на Стенде (либо через удаленный терминальный доступ). Результат выполнения команды – *все пакеты потеряны*.

5. Далее провести разблокировку хоста аналогичным блокировке способом и выполнить команду пинг повторно.

2.5.1.7 Проверка работоспособности функций выявления угроз с помощью поведенческого анализа на конечной станции

1. Перейти в раздел **Настройки** → **Модули** → **Группа хостов с Windows EDR** → **Основные настройки** и в блоке **Анализ файлов** проверить, что опции **Блокировать вредоносные файлы** и **Перемещать вредоносные файлы в карантин** выключены.

2. Перейти в раздел **Настройки** → **Модули** → **Группа хостов с Windows EDR** → **Основные настройки** и выключить использование модуля **Политики предотвращения угроз**.

3. Далее непосредственно на Стенде (или с помощью опции удаленного терминального доступа) запустить предоставленный вендором вредоносный экземпляр.

4. Перейти в раздел **Атаки** → **Алерты**, выставить фильтр **Система интеграции** → **Huntpoint**, **Классификатор** → **Huntpoint**, выполнить поиск по имени Стенда и найти алерт о вредоносной активности на хосте.

2.5.2 Запуск ПО применительно к конечным станциям на базе ОС ядра Linux

2.5.2.1 Проверка корректности установки агента на Стенде для проведения тестирования

1. Проверить, что конечная станция, используемая для проведения тестирования, представляет собой виртуальное окружение и удовлетворяет всем системным требованиям.

2. Проверить, что у Стенда отсутствует сетевой доступ к корпоративной сети организации Заказчика.

3. После установки агента Стенд необходимо перезагрузить.

4. Проверить, что на Стенде установлена рекомендуемая вендором версия агента в соответствии с инструкциями по установке. Для этого необходимо выполнить через терминал команду *systemctl status linep* и получить результат выполнения: *loaded: enabled; active: active*;

5. После перезагрузки Стенда перейти в интерфейсе в раздел **Моя компания** → **Активы**, выставить быстрый фильтр **Компьютер** и убедиться, что актив Стенда в статусе онлайн (индикатор актива зеленый).

2.5.2.2 Проверка корректности настроек модуля EDR

1. Перейти в раздел **Настройки** → **Модули** → **Группа хостов с Linux EDR** → **Основные настройки** и активировать опцию **Удаленного терминального доступа**.

2. Задать пароль контроля доступа (далее этот пароль нигде отображаться не будет, поэтому крайне важно этот пароль сохранить в менеджере паролей).

3. Проверить, что на Стенде отключены все сторонние или встроенные средства защиты конечных устройств (Антивирусы, EDR, DLP и т.д.).

4. Далее перейти в раздел **Профиль пользователя** → **Безопасность и доступ** → **Двухфакторная аутентификация** и убедиться в наличии статуса **Аккаунт защищен двухфакторной аутентификацией**.

2.5.2.3 Проверка работоспособности функции сбора криминалистических артефактов

Для корректного проведения данного тестирования, необходимо убедиться, что роль пользователя аналитик или админ.

1. Перейти в раздел **Моя компания** → **Активы** выполнить поиск по *machine_id* Стенда, раскрыть в правом верхнем углу меню **Реагирование**, выбрать опцию **Собрать артефакты на хосте**.

2. В открывшемся визарде выбрать опцию сбора данных обо всех залогиненных пользователей (logged users).

3. Перейти во вкладку Реагирование в раскрытом сайдбаре с информацией о Стенде, выбрать пункт **Артефакты**. Будет доступно отображение всех запрошенных артефактов со статусом выполнения. По итогу сбора запрошенных на предыдущем шаге данных будет доступна карточка для просмотра и скачивания собранных артефактов.

2.5.2.4 Проверка работоспособности функций удаленного терминального доступа

1. Перейти в раздел **Моя компания** → **Активы** выполнить поиск по *machine_id* Стенда, раскрыть в правом верхнем углу меню **Реагирование**, выбрать опцию **Подключиться удаленно**.

2. В открывшемся диалоговом окне ввести одноразовый код 2FA.

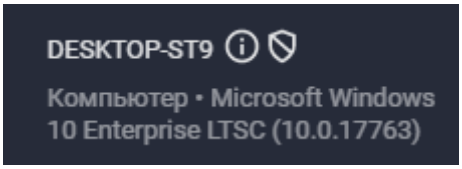
3. Далее по доступности терминала для ввода команды выполнить *whoami*, дождаться результата выполнения команды и после этого завершить сессию.

2.5.2.5 Проверка работоспособности функции изоляции конечной станции

1. Перейти в раздел **Моя компания** → **Активы** выполнить поиск по *machine_id* Стенда, раскрыть в правом верхнем углу меню **Реагирование**, выбрать опцию **Изолировать хост**.

2. В открывшемся диалоговом окне ввести имя компьютера, который необходимо изолировать, комментарий о причинах блокировки по необходимости и далее нажать на кнопку **Отправить**.

3. Далее в Web-интерфейсе в таблице активов рядом с записью, которая относится к Стенду, появится индикатор изоляции хоста - значок щита (скриншот ниже):



4. Далее на Стенде выполнить команду *ping 8.8.8.8* (или любой другой IP адрес, к которому компьютер имеет сетевой доступ) непосредственно на Стенде (либо через удаленный терминальный доступ). Результат выполнения команды – все пакеты потеряны.

5. Далее провести разблокировку хоста аналогичным блокировке способом и выполнить команду пинг повторно.

2.6 Промышленная эксплуатация

Промышленная эксплуатация (далее – Эксплуатация) – это этап жизненного цикла, когда установленное ПО используется в реальных рабочих условиях на постоянной основе.

Эксплуатация включает в себя следующие этапы:

– Аналитическое сопровождение и работы по выявлению аномалий и мошеннической активности среди клиентов Заказчика;

– Обработка выявляемых событий и предоставление обратной связи;

– Тонкая настройка правил выявления мошеннической активности;

– Контроль работоспособности АС Заказчика;

– Контроль работоспособности ПО;

– Доработка и регулярное обновление ПО для устранения ошибок, повышения производительности, а также введения новых функций;

– Периодическая отчетность по работоспособности и устранениям неисправностей ПО;

– Поддержка актуальной документации.

2.7 Сопровождение ПО

В течение всего периода эксплуатации ПО Заказчику предоставляется сопровождение ПО, в рамках которого оказываются следующие услуги:

– Техническая поддержка Пользователей;

– Решение инцидентов (экстренных неисправностей), возникающих в процессе эксплуатации ПО;

– Устранение сбоев и ошибок, выявленных в ПО;

– Совершенствование ПО;

– Мониторинг производительности ПО;

– Оптимизация эффективности работы ПО;

– Поддержка актуальной технической документации по ПО;

– Уведомление об обновлениях и изменениях ПО;

– Обучение новых пользователей.

3 Совершенствование ПО

ПО на постоянной основе подвергается развитию и улучшению в рамках процессов:

– развития и добавления новых функциональных возможностей, позволяющих расширить области применения ПО;

– оптимизации работы модулей ПО, обеспечивающей повышение производительности, скорости обработки данных и отказоустойчивости;

– обновления пользовательского интерфейса.

Совершенствование ПО происходит за счет проведения модернизаций ПО в соответствии с собственным планом доработок, а также с учетом заявок клиентов по вопросам испытаний установки и эксплуатации, полученных через ТС.

4 Устранение неисправностей ПО

Неисправности, которые были выявлены в ходе полноценной эксплуатации ПО, могут быть исправлены следующими способами:

- Массовое обновление компонентов ПО;
- Единичная работа технического специалиста по запросу Пользователя.

В случае возникновения неисправности клиент направляет заявку через Технический Сервис (далее – ТС) Разработчика с подробным описанием воспроизведенной проблемы (версия ПО, описание конфигурации, версия приложения клиента, прикрепленные скриншоты). Затем технический специалист проводит следующие действия:

- подтверждает наличие неисправности в соответствии с описанием проблемы от Заказчика;
- тестирует неисправность в функционале ПО и создает отчет по результатам тестирования;
- фиксирует задачу на исправление проблемы в текущий или ближайший релиз обновления ПО или консультирует клиента по корректности выполняемых действий.

Задачи по устранению неисправностей в функционале ПО осуществляются силами Разработчика. В соответствии с внутренним планом выхода обновлений подсистемы предоставляется исправленный механизм работы ПО.

Процессы по устранению неисправностей протекают непрерывно, без остановки функционирования ПО.

4.1 Устранение экстренных неисправностей ПО

В экстренном случае, когда ошибка препятствует полноценному использованию функционала ПО, группа разработчиков готовит внеплановый выход обновления или предоставляет исправленную версию ПО.

При возникновении экстренных неисправностей Заказчик отправляет запрос через ТС со следующими данными:

- Четко сформулированная тема обращения;
- Версия приложения заказчика, на которой осуществляется эксплуатация ПО;
- Версия ПО;

- Пошаговое описание воспроизведения ошибки;
- Скриншоты, демонстрирующие наличие найденной ошибки.

5 Техническая поддержка

Техническая поддержка Пользователей осуществляется в соответствии с условиями контракта следующими способами:

- Приоритетный способ осуществления техподдержки через создание запросов во вкладке «Поддержка» по ссылке https://xdr.f6.security/service-desk
- по электронной почте: info@f6.ru;
- по номеру телефона: +7 495 984-33-64;

В рамках технической поддержки оказываются следующие услуги:

- консультация по фактическому наличию имеющегося функционала в системе;
- помощь в настройке и интеграции ПО;
- помощь в эксплуатации ПО;
- решение технических проблем;
- пояснение принципов работы имеющихся механизмов ПО;
- поиск, тестирование и фиксирование найденных ошибок;
- предоставление актуальной документации по настройке, эксплуатации и работе ПО.

Время работы технической поддержки: с понедельника по пятницу с 9:00 до 18:00 UTC+3.

Фактический адрес размещения службы поддержки ПО «F6 Endpoint Detection and Response»: 115088, г. Москва, ул. Шарикоподшипниковская, д. 1

6 Информация о персонале

6.1 Персонал, обеспечивающий работу ПО на рабочих местах пользователей

К эксплуатации ПО допускаются лица, ознакомившиеся с документацией по эксплуатации ПО в разделе «Помощь» пользовательского интерфейса ПО.

К эксплуатации ПО привлекается штатный персонал Заказчика, имеющий следующие навыки:

- навыки работы с персональным компьютером на уровне опытного пользователя;
- опыт работы с электронными документами;
- опыт использования web-браузеров;
- Знания в соответствующей предметной области.

6.2 Персонал, обеспечивающий техническую поддержку, аналитическую поддержку и модернизацию ПО «F6 Endpoint Detection and Response»

Специалисты, обеспечивающие техническую и аналитическую поддержку и развитие ПО, должны обладать следующими знаниями и навыками:

- знание функциональных возможностей ПО;
- знание особенностей работы с ПО;
- знание языков программирования, исходя из должностных обязанностей: Python, GO, Rust, JavaScript, TypeScript;
- знание реляционных и не реляционных БД, исходя из должностных обязанностей: PostgreSQL, Elasticserch, ClickHouse, MongoDB;
- знание средств мониторинга производительности серверов.

Должность	Компетенции	Выполняемые работы	Количество специалистов
Системный программист-разработчик под Windows	C, C++, Go	Техническая поддержка; Аналитическое сопровождение; Разработка и совершенствование ПО.	3

Системный программист-разработчик под Linux	C, C++, Go, Rust	Техническая поддержка; Аналитическое сопровождение; Разработка и совершенствование ПО.	5
Системный программист-разработчик под macOS	C, C++, Go	Техническая поддержка; Аналитическое сопровождение; Разработка и совершенствование ПО.	3
Анатилик разработки детектирующей логики	Rust, Sigma	Техническая поддержка; Аналитическое сопровождение; Разработка и совершенствование ПО.	5
DevOps инженер	Linux, Ansible, Docker, GitLab CI\CD, Elasticsearch, PostgreSQL, Minio.	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	2
Тестировщики	Allure, Pytest, Gitlab CI/CD, Разработка авто тестов, функционального и нагрузочного тестирования	Разработка тест-планов дял тестирований продуктового функционала; Проведение ручного тестирования согласно разработанным планам; Разработка автоматических тестов и анализ его результатов; Проведение регрессионного тестирования.	5

ИНФОРМАЦИЯ О ФАКТИЧЕСКИХ АДРЕСАХ

Фактический адрес размещения разработчиков ПО 115088, г. Москва, ул. Шарикоподшипниковская, д. 1

Фактический адрес размещения службы поддержки ПО 115088, г. Москва, ул. Шарикоподшипниковская, д. 1

Контакты службы поддержки:

- Электронная почта: info@f6.ru
- Телефон: +7 495 984-33-64