ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Business Email Protection»

Описание процессов, обеспечивающих поддержание жизненного цикла

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

2FA	–	Двухфакторная аутентификация
API	–	Application Programming Interface
BEC	–	Business Email Compromise
CEF	–	Chromium Embedded Framework
CI/CD	–	Continuous Integration / Continuous Delivery, технология автоматизации тестирования и доставки новых модулей
HTTP	–	HyperText Transfer Protocol
IPv4	–	Internet Protocol version 4
JSON	–	JavaScript Object Notation
MDP		Модуль «F6 MDP» (Malware detonation platform)
MXDR	–	Программный комплекс Managed Extended Detection and Response (Managed XDR)
NTA	–	Модуль F6 (Network Traffic Analysis)
XDR	–	Модуль «F6 XDR» (MXDR Console)
pytest	–	фреймворк для тестирования кода на Python
selenium	–	инструмент для автоматизации действий веб-браузера
SOC	–	Security Operation Center
TI	–	Threat Intelligence
TTP	–	тактики, техники и процедуры
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 Business Email Protection»
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 Business Email Protection». В случае недоступности указанных систем формат взаимодействия осуществляется через электронный почтовый ящик

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание процессов поддержания жизненного цикла программного обеспечения «F6 Business Email Protection» (далее – ПО, BEP). 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 Business Email Protection» это модуль системы MXDR (Managed XDR) который специализируется на анализе и мониторинге электронной почты для выявления киберугроз. Этот модуль сканирует входящие письма для обнаружения фишинга, спама и других видов угроз, направленных на компрометацию пользователей. ПО фокусируется на проверке содержимого писем и выявлении потенциальных угроз. В качестве платформы детонации используется модуль Malware Detonation Platform (MDP). В случае обнаружения угроз модуль формирует отчеты и отправляет уведомления, обеспечивая оперативное реагирование специалистов по кибербезопасности.

1.3 Функциональные возможности ПО

ПО обладает следующими функциональными возможностями:

– Поддержка развертывания в трех вариантах:

- Cloud релей – перенаправление входящего почтового потока через измененные MX-записи в инфраструктуру разработчика для анализа и принятия решений о блокировке.
- Cloud почтовый шлюз – анализ почтового потока в инфраструктуре разработчика при использовании существующего почтового сервера заказчика.
- On-prem шлюз – анализ почтового потока с существующего почтового сервера через подсистему интеграции и анализ контента в инфраструктуре заказчика.

– Возможность настройки маршрутов для почты с указанием приоритетности и веса серверов для балансировки нагрузки и распределения почтового потока.

– Отправка почтовых сообщений по заданным маршрутам после анализа, если сообщение признано безопасным, с применением всех заданных политик фильтрации.

– Возможность создания белых списков для исключения индикаторов из анализа по следующим параметрам: email-адреса, URLs, хеш-суммы, IP-адреса.

– Поведенческий анализ файлов в специально подготовленных виртуальных машинах.

– Статический и эвристический анализ контента писем, заголовков и ссылок на предмет социальной инженерии, включая BEC-атаки и спам, с отчетом о сработавших правилах.

– Возможность применения настраиваемых политик фильтрации для снижения рисков получения нежелательных рассылок и/или вредоносного контента.

– Настройка политик проверки форматов содержимого по критериям: file_name, file_magic, url, recipient, sender, spf, dkim, dmarc.

– Настройка политик действий с непроверенным контентом, включая зашифрованные архивы и недоступные ссылки.

– Возможность добавления пользовательских YARA-правил и настройки политики действий на основе их срабатывания.

– Возможность принудительной отправки заблокированных почтовых сообщений как получателю, указанному в заголовках письма, так и на заданный администратором адрес.

– Представление технических заголовков и структуры почтового сообщения в виде графа.

– Использование низкоуровневого монитора для выявления поведенческих маркеров.

– Применение элементов машинного обучения для улучшения обнаружения угроз.

– Анализ файлов в изолированной среде с использованием русифицированного образа ОС Windows.

– Поддержка анализа файлов до 100 Мб.

– Поведенческий анализ файлов различных расширений и типов в изолированной среде.

– Анализ потенциально вредоносных файлов с возможностью определения различных типов файлов по содержимому.

– Интерфейс для загрузки файлов на анализ в ручном режиме с возможностью задания параметров виртуализации и анализа.

– Подключение к виртуальной машине во время анализа файла по протоколу RDP.

– Поведенческий анализ архивов с паролем и поиск паролей из различных источников.

– Использование гипервизора для анализа, контроль событий ОС, статический сигнатурный анализ и автоматическое обнаружение техник обхода анализа.

– Формирование отчета по результатам анализа с детализированными данными о процессах, сетевой активности, файловых взаимодействиях и сработавших правилах.

– Обнаружение и извлечение конфигурационных файлов ВПО, атрибуция к известным инструментам и возможность экспорта файлов для дальнейшего анализа.

– Гибкое горизонтальное масштабирование для наращивания производительности при необходимости.

– Возможность изменения маршрута для вывода трафика из виртуальных машин.

– Кастомизация виртуальных машин, включая изменение домена, имени компьютера и имени пользователя.

– Автоматический подбор конфигурации виртуальной машины, эмуляция пользовательской активности, технологии компьютерного зрения, извлечение и запуск дополнительных команд из реестра, опция поддельного SMTP-сервера и использование Mitmproxy.

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 (в случае On-prem размещения) и активация модуля. Запуск в промышленную эксплуатацию осуществляется силами Исполнителя. Для корректного запуска, необходима проверка пунктов по работоспособности MXDR Console и MDP, а также наличие корректной интеграции NTA с MDP. В случае локального размещения проверка ПО осуществляется по ПМИ и включает следующие пункты:

1. Настройка инфраструктуры на стороне заказчика:

– для интеграции по протоколу SMTP (копия писем): сетевая доступность между NTA и почтовым сервером, отправка копии почтового потока на 25 порт NTA;

– для интеграции по POP3/IMAP: почтовый ящик, к которому будет подключаться NTA и забирать копию писем, сетевая доступность между NTA и почтовым сервером;

– для интеграции в режиме MTA: сетевая доступность между NTA и почтовым сервером, настройка отправки почтового потока на 25 порт NTA, настройка получения проанализированного почтового потока от NTA.

2. Настройка на стороне сенсора:

– для интеграции по протоколу SMTP (копия писем): перейти в раздел Настройки → Модули → NTA → Основные настройки → Почта → Почтовый сервер и включить эту опцию. Настройку режима работы модуля выставить в значение “Прием копии писем”.

– для интеграции по POP3/IMAP: перейти в раздел ***Настройки → Модули → NTA → Основные настройки → Почта → Почтовый клиент***

– для интеграции в режиме MTA: перейти в раздел ***Настройки → Модули → NTA → Основные настройки → Почта → Почтовый сервер***. Настройку режима работы модуля выставить в значение “MTA”. Далее проверить наличие почтовых маршрутов для дальнейшей отправки почты и включить режим блокировки почты.

3. Проверить в разделе ***Настройки*** → ***Модули*** → ***NTA*** → ***Основные настройки*** → ***Почта*** → ***Синхронизация с MXDR Console*** в положение “Включено”

4. Далее на тестовый почтовый адрес отправить письмо. Наличие записи об этом письме в разделе ***Расследования*** → ***Письма*** свидетельствует о поступлении почты на анализ.

5. Далее на выбранный почтовый ящик необходимо запустить синтетический тест (отправить ВПО).

6. По завершению теста и завершению анализа всех отправленных писем, должны быть сформированы алерты о вредоносных письмах в разделе ***Атаки*** → ***Алерты***, а также должны быть доступны отчеты MDP по файлам во вложениях/ссылкам. При интеграции в режиме MTA вредоносные письма, не находящиеся в статусе “ретро-анализ” должны быть заблокированы и не доставлены на указанный почтовый ящик.

В случае облачного размещения проверка ПО осуществляется по ПМИ и включает следующие пункты:

1. Проверка подключения необходимой лицензии: перейти в раздел ***Настройки*** → ***Модули*** → ***Business Email Protection*** → ***Индикатор*** слева горит зеленым **ИЛИ** в **Настройках** присутствует пункт “Облачная Почта”.

2. Настройка модуля:

- В настройках модуля, в разделе “Домены и маршруты” в пункт “Почтовые домены” добавлены защищаемые домены и находятся в статусе “Подтверждено”;
- В настройках модуля, в разделе “Домены и маршруты” в пункт “Почтовые маршруты” добавлены маршруты доставки почтовых сообщений после проведения проверки;
- Если модуль используется в качестве второго почтового релея, в настройках модуля, в разделе “Домены и маршруты” в пункт “Входящий шлюз” внесен IP-адрес отправляющего контент первого шлюза.

3. Настройка инфраструктуры на стороне заказчика:

- IP-адреса BEP внесены в список доверенных отправителей в настройках почтового шлюза;
- MX-записи BEP внесены в MX-записи защищаемых доменов;

– При интеграции модуля внутри инфраструктуры в качестве второго почтового релея необходимо убедиться, что в настройках первого почтового релея добавлен маршрут об отправке почты на IP-адреса модуля BEP.

4. Послать тестовое письмо на защищаемый домен с внешнего источника. Чтобы увидеть результат, необходимо перейти в раздел ***Расследование → Проверенные письма*** и отфильтровать почту по отправителю письма, используя ключевое выражение *mail_from*.

5. Настройка белого списка: в раздел ***Настройки → Модули → Business Email Protection → Основные настройки → Политика и обнаружение → Белый список антиспама*** **ИЛИ** в ***Настройки → Облачная почта → Политика и обнаружение → Белый список антиспама*** внесены доверенные домены отправителей, а также другие домены, относящиеся к инфраструктуре заказчика.

6. Настройка модуля анализа нежелательных писем: перейти в раздел ***Настройки → Модули → Business Email Protection → Основные настройки → Политика и обнаружение → Выявление нежелательных писем*** **ИЛИ** в ***Настройки → Облачная почта → Политика и обнаружение → Выявление нежелательных писем*** и проверить, он сконфигурирован следующим образом:

– Включен Статический классификатор,

– Включен Эвристический классификатор,

– ***Действие → Карантин***.

7. Отправить тестовое нежелательное письмо, предоставленное разработчиками АО «БУДУЩЕЕ», на защищаемый почтовый ящик. Чтобы увидеть результат, необходимо перейти в раздел **Расследование → Проверенные письма → Нежелательные** и отфильтровать почту по отправителю письма, используя ключевое выражение mail_from.

8. Настройка модуля детонации файлов (при наличии модуля детонации): перейти в раздел ***Настройки → Модули → Business Email Protection → Основные настройки → Политика и обнаружение → Детонация файлов*** **ИЛИ** в ***Настройки → Облачная почта → Политика и обнаружение → Детонация файлов*** и проверить, что данный модуль включен и настроен следующим образом:

– ***Действие → Карантин*** + Уведомление получателя,

– Язык в виртуальных машинах – Соответствует локализации заказчика.

9. Отключить для проведения теста модуля детонации файлов модуль выявления нежелательных писем. Далее отправить тестовое письмо на защищаемый домен с внешнего источника. В письме должна содержаться вредоносная нагрузка (будет предоставлена сотрудниками АО «БУДУЩЕЕ». Самостоятельно можно пройти бесплатное тестирование Trebuchet). Чтобы увидеть результат, необходимо перейти в раздел ***Расследование*** → ***Проверенные письма*** → ***Вредоносные*** и отфильтровать почту по отправителю письма, используя ключевое выражение mail_from.

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 Business Email Protection»: 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 Business Email Protection»

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
Backend разработчик	Go, Python, Rust, MongoDB	Техническая поддержка; Аналитическое сопровождение; Разработка и совершенствование ПО.	3

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 для тестирований продуктового функционала; Проведение ручного тестирования согласно разработанным планам; Разработка автоматических тестов и анализ его результатов; Проведение регрессионного тестирования.	2

7 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

Информация о фактическом адресе размещения инфраструктуры разработки ПО

ПО поставляется может поставляться в виде облачного сервиса, в таком случае Пи размещается на удаленных серверах компании АО «Селектел» по адресу:

188683, Ленинградская область, Всеволожский район, г.п. Дубровка, ул. Советская, дом 1, литера Б.