ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Threat Intelligence»

Описание процессов, обеспечивающих поддержание жизненного цикла

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Описание
Заказчик	Лицо, заключившее договор на использование ПО
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО «БУДУЩЕЕ»; • Компанией-интегратором, по выбору Заказчика
ИТ	Информационные Технологии
ПО, Система или F6 Threat Intelligence	Программа для ЭВМ «F6 Threat Intelligence»
Пользователь	Лицо, непосредственно использующее ПО
Разработчик	АО «БУДУЩЕЕ»
Скриншот	Изображение, «снимок» экрана ПК или мобильного устройства, на котором запечатлено содержимое экрана устройства
Угроза или Киберугроза	Потенциально возможное происшествие, преднамеренное или нет, которое может оказать нежелательное воздействие на систему или хранящуюся информацию (т. е. нечто плохое, что может произойти)
TTP (Tactics, Techniques and Procedures)	Тактики, техники и процедуры по матрице MITRE ATT&CK

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ описывает процессы поддержания жизненного цикла «F6 Threat Intelligence». 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 Threat Intelligence» — это система киберразведки, предназначенная для сбора, анализа и распространения информации о событиях безопасности, Киберугрозах и уязвимостях.

Система представляет собой обширную базу знаний, содержащую информацию по злоумышленникам, Угрозам и возможным уязвимостям, а также предоставляет данные о вредоносном программном обеспечении. По выявленным событиям кибербезопасности Система генерирует оповещения.

Кроме того, в Системе представлены аналитические отчеты о последних Киберугрозах, что позволяет выстроить наиболее эффективную защиту инфраструктуры.

1.3 Функциональные возможности ПО

«F6 Threat Intelligence» предоставляет доступ к уникальным средствам, позволяющим эффективно решать сложнейшие задачи по противодействию злоумышленникам. В частности, использование графового анализа позволяет быстро дойти до источника актуальной Угрозы, отследить существующие связи участников киберпреступных группировок. В систему встроены механизмы, обеспечивающие автоматизацию деятельности аналитика и хорошую визуализацию всех компонентов и событий.

Функциональные возможности ПО предоставляют возможность получать технические индикаторы, оперативные и стратегические данные, обогащенные контекстом. Все данные в Системе могут быть ранжированы.

- **Технические индикаторы** — используются для обогащения внутренних баз эксплуатируемых средств защиты. Также применяются в работе служб информационной безопасности при расследовании инцидентов, для оперативной интеграции в существующую ИБ-инфраструктуру и выполнения незамедлительных действий. К таким данным относятся: хеш-суммы файлов, IP-

адреса, доменные имена и URL-ссылки, подозрительные IP-адреса и сведения из конфигурационных файлов вредоносных программ.

– **Оперативные данные** — используются для построения гипотез о возможных действиях атакующих, на основании известных TTP. К оперативным данным относятся сведения о новых атакующих, проведённых кампаниях (сериях атак), изменениях в тактике проведения атак, новых видах мошенничества и т. п.

– **Стратегические данные** — используются для формирования ландшафта Угроз и управления им, для информированного принятия решений о распределении бюджетов на обеспечение информационной безопасности и для выбора технических решений по защите ИТ-инфраструктуры. К таким данным относятся: ежегодный отчёт с прогнозами, ежемесячные и ежеквартальные отчёты с анализом развития Угроз, отдельные специальные отчёты по запросу клиентов, например, с обзором дарквеб-форумов или сканированием сети.

– **Контекст данных** — такие данные позволяют узнать о способах осуществления атак и об используемых для их осуществления инструментах, а также выявить, кто именно инициировал ту или иную атаку.

2 ПРОЦЕСС РАЗРАБОТКИ ПО

Процесс разработки ПО включает в себя следующие элементы:

- 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:

- Создание и настройка учетных записей клиента;
- Проверка привязки данных в системе к учетной записи клиента;
- Корректировка сигнатур и настроек для обнаружения данных клиента.

2.5 Запуск в промышленную эксплуатацию ПО

Запуск в промышленную эксплуатацию — это процесс подготовки окружения для развертывания ПО на целевой среде Заказчика. Запуск в промышленную эксплуатацию осуществляется силами Исполнителя.

Запуск в промышленную эксплуатацию включает следующие этапы:

- Передача реквизитов доступа к ПО
- Контроль получаемых данных, ошибок и пр.;
- Мониторинг запуска и сбор отзывов:

- Контроль получаемых данных, возникающих ошибок и пр.;
- Контроль обращений/жалоб клиентов;
- Контроль нагрузки.

2.6 Промышленная эксплуатация

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

Промышленная 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 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 раздел «Поддержка».

4 УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ ПО

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

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

В случае возникновения неисправности клиент направляет заявку через раздел «Поддержка» 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 раздел «Поддержка» 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:

- По электронной почте: info@f6.ru;
- По номеру телефона: +7 495 984-33-64;
- Через создание запроса во вкладке «Поддержка» по ссылке https://ti.f6.security/service_desk.

В рамках технической поддержки Пользователей 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 Threat Intelligence»: 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 «Справка» 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 веб-браузеров;
- Знания в соответствующей предметной области.

6.2 Персонал, обеспечивающий техническую поддержку, аналитическую поддержку и модернизацию ПО «F6 Threat Intelligence»

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: Java, Python, GO, JavaScript, TypeScript, Kotlin;
- Знание реляционных и не реляционных БД, исходя из должностных обязанностей: Cassandra, ClickHouse, Elasticsearch;
- Знание средств мониторинга производительности серверов.

Должность	Компетенции	Выполняемые работы	Количество специалистов
Frontend разработчик	JavaScript, React, TypeScript	Техническая поддержка; Аналитическое сопровождение; Разработка и совершенствование ПО.	3

Backend разработчик	JavaScript, TypeScript, Go, Kubernetes, Cassandra, Elasticsearch, ClickHouse, Kotlin	Техническая поддержка; Аналитическое сопровождение; Разработка и совершенствование ПО.	9
Инженер интеграционных решений	JavaScript, TypeScript, Go, Kubernetes, Cassandra, Elasticsearch, ClickHouse, Kotlin	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	3
Аналитики	Python, TypeScript, Go, Cassandra, Elasticsearch, ClickHouse,	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	6
DevOps инженер	Kubernetes, FluxCD, Docker, GitLab CI\CD, Elasticsearch, Cassandra	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	3
Тестировщики	Разработка авто тестов, функционального и нагрузочного тестирования	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	2
Технические писатели	Разработка документации	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	2

7 ИНФОРМАЦИЯ О ФАКТИЧЕСКИХ АДРЕСАХ

Фактический адрес размещения разработчиков ПО «F6 Threat Intelligence»

115088, г. Москва, ул. Шарикоподшипниковская, д. 1

Фактический адрес размещения службы поддержки ПО «F6 Threat Intelligence»

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 «F6 Threat Intelligence»

ПО «F6 Threat Intelligence» поставляется в виде облачного сервиса и размещается на удаленных серверах компании АО «Селектел» по адресу:

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