ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«F6 XDR»

Описание процессов, обеспечивающих поддержание
жизненного цикла

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ	3
1 ОБЩИЕ СВЕДЕНИЯ	4
1.1 Введение.....	4
1.2 Назначение ПО.....	4
1.3 Функциональные возможности ПО	4
2 Процесс разработки ПО	7
2.1 Сбор и анализ требований к разработке ПО.....	7
2.2 Проектирование архитектуры ПО	7
2.3 Разработка ПО в коде	8
2.4 Проведение тестирования ПО перед эксплуатацией.....	8
2.5 Запуск ПО в промышленную эксплуатацию.....	9
2.6 Промышленная эксплуатация.....	9
2.7 Сопровождение ПО	10
3 Совершенствование ПО	11
4 Устранение неисправностей ПО	12
4.1 Устранение экстренных неисправностей ПО	12
5 Техническая поддержка.....	14
6 Информация о персонале	15
6.1 Персонал, обеспечивающий работу ПО на рабочих местах пользователей .	15
6.2 Персонал, обеспечивающий техническую поддержку, аналитическую поддержку и модернизацию ПО «F6 XDR»	15
7 ИНФОРМАЦИЯ О ФАКТИЧЕСКИХ АДРЕСАХ.....	17

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Определение
2FA	Двухфакторная аутентификация
API	Application Programming Interface
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
MXDR	Программный комплекс Managed Extended Detection and Response (Managed XDR)
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: <ul style="list-style-type: none"> • АО БУДУЩЕЕ; • Компанией-интегратором, по выбору Заказчика
ПО	Программное обеспечение «F6 XDR» (MXDR Console)
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 XDR». 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 «F6 XDR» (далее – ПО, MXDR Console). 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 XDR» является центральным элементом в составе программного комплекса Managed XDR (MXDR), представляя собой высокоинтегрированную платформу для управления, мониторинга и реагирования на киберугрозы. Консоль предоставляет единый интерфейс для сбора и анализа данных из различных источников, включая сетевые устройства, системы защиты конечных точек и журналы событий, что обеспечивает централизованное управление безопасностью всей инфраструктуры безопасности. ПО поддерживает функции продвинутого поиска угроз (threat hunting) и детализированного анализа инцидентов, позволяя выявлять сложные и скрытые атаки. Автоматизация процессов реагирования на инциденты минимизирует время отклика и снижает нагрузку на команды SOC. Интеграция с внешними источниками данных о киберугрозах обеспечивает доступ к актуальной информации в режиме реального времени. Кроме того, ПО поддерживает коллективную работу, что упрощает координацию действий между специалистами. Функциональность отчетности и визуализации данных в ПО позволяет эффективно отслеживать состояние безопасности и принимать обоснованные решения.

1.3 Функциональные возможности ПО

ПО обладает следующими функциональными возможностями:

- Реализация центра обновлений, централизованной системы хранения данных, пользовательского интерфейса, нативной интеграции с TI-решением и API-взаимодействия.
- Поддержка развертывания в двух вариантах:
 - Cloud, где ПО размещается в инфраструктуре разработчика
 - On-prem, когда все данные остаются внутри защищаемого периметра.

- Корреляция событий всех подсистем в единой базе данных для выявления потенциальных инцидентов, а также объединение зарегистрированных событий из дочерних подсистем в единое событие информационной безопасности.
- Возможность автоматической и ручной консолидации событий информационной безопасности в единую сущность.
- Обеспечение безопасного взаимодействия между дочерними модулями через центр обновлений.
- Надежное и масштабируемое хранение данных в централизованной системе с поддержкой кластеризации для горизонтального масштабирования.
- Функционал для изоляции конечных станций от сети, блокировки вредоносных процессов и файлов с целью локализации инцидента.
- Возможность изучения инфраструктуры атакующих через регулярное сканирование IPv4-адресов и визуализацию данных в виде графа, обогащенного контекстом из системы Threat Intelligence.
- Пользовательский интерфейс в формате веб-приложения с доступом через HTTP и возможностью шифрования трафика, а также функции корреляции записей, поиска и построения отчетов.
- Настройка почтовых уведомлений для пользователей системы, включая уведомления о новых событиях, изменении статуса, ошибках интеграции и взаимодействии с центрами мониторинга.
- Поддержка почтовых уведомлений при блокировке сообщений.
- Передача на другие подсистемы обновлений сигнатур, решающих правил, индикаторов угроз и обновлений программного обеспечения.
- Возможность передачи телеметрии и информации о событиях через Syslog в форматах JSON и CEF, а также API для интеграции с другими решениями.
- Функционал для управления группами статических Suricata правил и загрузки пользовательских Suricata и YARA правил.
- Взаимодействие с Центром обновлений для обновления внутреннего ПО.
- Возможность автоматического поиска угроз на основе тактик, техник и процедур (TTP по матрице MITRE ATT&CK) с ретроспективным анализом файлов, метаинформации о

сетевых соединениях и проанализированных почтовых сообщений. Технические требования к составу оборудования при размещении в инфраструктуре Заказчика.

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

- Проверка физической работоспособности ПО;
- Проверка корректности загрузки исполняемого программного обеспечения ПО;
- Проверка работоспособности интерфейса ПО;
- Настройка двухфакторной аутентификации (2FA);
- Проверка режима обновления ПО;
- Проверка наличия дочерних лицензий.

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

- Проверка работоспособности интерфейса ПО;
- Настройка двухфакторной аутентификации (2FA);
- Проверка наличия дочерних лицензий.

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 вредоносной активности в инфраструктурах клиентов Заказчика;
- Обработка выявляемых событий и предоставление обратной связи;
- Тонкая настройка правил выявления вредоносной 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 устранением 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 XDR»: 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 XDR»

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
Frontend разработчик	JavaScript, Vue.js, TypeScript	Техническая поддержка; Аналитическое сопровождение; Разработка и совершенствование ПО.	3

Backend разработчик	Go, Python, Rust, PostgreSQL, Elasticsearch, ClickHouse	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.	3
Тестировщики	Allure, Pytest, Gitlab CI/CD, Разработка авто тестов, функционального и нагрузочного тестирования	Разработка тест-планов для тестирования продуктового функционала; Проведение ручного тестирования согласно разработанным планам; Разработка автоматических тестов и анализ его результатов; Проведение регрессионного тестирования.	5
Технические писатели	Разработка документации	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	2

7 ИНФОРМАЦИЯ О ФАКТИЧЕСКИХ АДРЕСАХ

Фактический адрес размещения разработчиков «F6 XDR»

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

Фактический адрес размещения службы поддержки «F6 XDR»

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 XDR»

ПО «F6 XDR» может поставляться в виде облачного сервиса, в таком случае ПО размещается на удаленных серверах компании АО «Селектел» по адресу:

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