Программное обеспечение

«F.A.C.C.T. Malware Detonation Platform»

Описание процессов, обеспечивающих поддержание жизненного цикла

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание процессов поддержания жизненного цикла программного обеспечения «F.A.C.C.T. Malware Detonation Platform» (далее – ПО, F.A.C.C.T. Malware Detonation Platform, MDP).

1.2 Назначение ПО

F.A.C.C.T. Malware Detonation Platform – программное обеспечение для поведенческого анализа, обеспечивающее выявление ранее неизвестного вредоносного кода с использованием передовых алгоритмов машинного обучения. Решение позволяет эффективно выявлять ранее неизвестные угрозы, осуществляя анализ файлов в изолированной среде. Он позволяет предотвратить заражения в результате фишинговых рассылок, либо загрузки/получения вредоносных файлов, осуществляющих заражения с использованием ранее неизвестных вредоносных программ и инструментов.

Использование модуля F.A.C.C.T. Malware Detonation Platform обеспечивает обнаружение ранее неизвестного вредоносного ПО и сложных целевых атак.

Основными целями создания ПО являются:

1. Предоставление интерфейса с отображением результатов проведения поведенческого анализа объектов
2. Повышение качества и количества раскрываемых преступлений;
3. Предоставление прозрачной статистической и аналитической информации

2 ЭТАПЫ ЖИЗНЕННОГО ЦИКЛА РАЗРАБОТКИ И ВНЕДРЕНИЯ ПО

Работы Исполнителя на протяжении всего жизненного цикла могут исполняться:

- АО «БУДУЩЕЕ»,
- Компанией-интегратором, по выбору Заказчика ПО.

2.1 Разработка ПО

Процесс разработки ПО включает этапы: сбор и анализ требований, проектирование архитектуры, кодирование, тестирование перед эксплуатацией, запуск, эксплуатация и сопровождение.

Требования к разработке ПО: определяются задачи и цели, выявляются заинтересованные стороны, собираются и анализируются требования, оцениваются риски, создается план проекта. Итог — согласование и документирование требований.

Проектирование архитектуры ПО: определяется структура системы, модули и их взаимодействие. Выбираются технологии и инструменты, документируется архитектура.

Разработка кода: реализуются проектные решения, проверяется и отлаживается код, проводится интеграция и подготовка к тестированию.

Тестирование перед эксплуатацией: оценивается качество, функциональность и безопасность ПО. Включает автоматическое и ручное тестирование всех аспектов с последующей автоматизацией.

2.2 Пилотные испытания

№	Краткое описание	Сторона
1	**Испытания**	
1.1.	Создание и настройка учетных записей клиента.	Исполнитель
1.2.	Проверка привязки данных в системе к учетной записи клиента	Исполнитель

2.3 Запуск в промышленную эксплуатацию

№	Краткое описание	Сторона
2.	**Запуск в промышленную эксплуатацию**	
2.1.	Передача реквизитов доступа к ПО	Заказчик
2.2.	Контроль получаемых данных, ошибок и пр.	Исполнитель

2.4 Промышленная эксплуатация

№	Краткое описание	Сторона
3.	**Промышленная эксплуатация**	
3.1.	Обработка выявляемых алертов и предоставление обратной связи	Заказчик
3.2.	Контроль работоспособности ПО на стороне Заказчика	Заказчик
3.3.	Контроль работоспособности ПО	Исполнитель
3.4.	Доработка ПО и обновление	Исполнитель
3.5.	Периодическая отчетность по работоспособности	Исполнитель

2.5 Вывод из промышленной эксплуатации

№	Краткое описание	Сторона
4.	**Прекращение эксплуатации**	
4.1.	Блокировка учетных записей клиента	Исполнитель

2.6 Сопровождение ПО

Сопровождение ПО включает техническую поддержку, решение инцидентов, устранение ошибок, улучшение ПО, мониторинг и оптимизацию производительности, актуализацию документации, уведомления об обновлениях, обучение пользователей.

2.7 Устранение неисправностей ПО

Устранение неисправностей ПО происходит в 2 этапа:

- Устранение критичных неисправностей. Производится непосредственно при обнаружении неисправности, выпуск исправляющего обновления производится незамедлительно.

- Устранение неисправностей не являющихся критическими. Производится в равно запланированные промежутки времени (раз в 2 недели) одновременно с выпуском других обновлений.

2.8 Совершенствование ПО

ПО находится в состоянии постоянного совершенствования. План совершенствования утверждается на 1 год, впоследствии становится доступен для конечных пользователей. Выпуск готовых обновлений производится не чаще чем раз в 2 недели, не реже 1 раза в месяц.

3 ИНФОРМАЦИЯ О ПЕРСОНАЛЕ

Специалисты должны знать функционал и особенности ПО, языки программирования (Python, Go, Rust, JavaScript), базы данных (PostgreSQL, Elasticsearch, ClickHouse, MongoDB) и мониторинг серверов. Персонал, участвующий в разработке ПО, включает следующий список сотрудников:

- Frontend Разработчик (3 специалиста)

Компетенции сотрудников: JavaScript, Vue.js, TypeScript. Работы: Техническая поддержка, аналитическое сопровождение, разработка и улучшение ПО.

- Backend Разработчик (5 специалистов)

Компетенции сотрудников: Go, Python, Rust, PostgreSQL, Elasticsearch, ClickHouse. Работы: Техническая поддержка, аналитическое сопровождение, разработка и улучшение ПО.

- DevOps Инженер (3 специалиста)

Компетенции сотрудников: Linux, Ansible, Docker, GitLab CI/CD, Elasticsearch, PostgreSQL, Minio. Работы: Техническая поддержка, аналитическое сопровождение, совершенствование ПО.

- Тестировщики (5 специалистов)

Компетенции сотрудников: Allure, Pytest, GitLab CI/CD. Работы: Разработка тест-планов, функциональное и нагрузочное тестирование, автоматизация тестов, регрессионное тестирование.

- Технические Писатели (2 специалиста).

Компетенции сотрудников: Разработка документации, аналитическое сопровождение.

4 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка осуществляется по электронной почте mxdr@facct.ru или в пользовательском интерфейсе Системы по ссылке https://xdr.facct.ru/service-desk.

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

Служба поддержки находится по адресу:

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

5 ФАКТИЧЕСКОЕ РАЗМЕЩЕНИЕ ИНФРАСТРУКТУРЫ И КОМАНДЫ РАЗРАБОТКИ

Команда разработки находится по адресу:

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

Инфраструктура ПО на удаленных серверах компании АО «Селектел» по адресу:

188683, Санкт-Петербург, Ленинградская область, г.п. Дубровка, ул. Советская, дом 1, Литера Б.