

Программное обеспечение «F.A.C.C.T. Endpoint Detection and Response»

Описание процессов, обеспечивающих поддержание
жизненного цикла

Содержание

1 ОБЩИЕ СВЕДЕНИЯ	3
1.1 Введение	3
1.2 Назначение ПО	3
2 ЭТАПЫ ЖИЗНЕННОГО ЦИКЛА РАЗРАБОТКИ И ВНЕДРЕНИЯ ПО	4
2.1 Разработка ПО	4
2.2 Пилотные испытания.....	4
2.3 Запуск в промышленную эксплуатацию	5
2.4 Промышленная эксплуатация.....	5
2.5 Вывод из промышленной эксплуатации	5
2.6 Сопровождение ПО	6
2.7 Устранение неисправностей ПО.....	6
2.8 Совершенствование ПО	6
3 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА И ИНФОРМАЦИЯ О ПЕРСОНАЛЕ	7
4 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА.....	8
5 ФАКТИЧЕСКОЕ РАЗМЕЩЕНИЕ ИНФРАСТРУКТУРЫ И КОМАНДЫ РАЗРАБОТКИ	8

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание процессов поддержания жизненного цикла программного обеспечения «F.A.C.C.T. Endpoint Detection and Response» (далее – ПО, F.A.C.C.T. Endpoint Detection and Response, EDR).

1.2 Назначение ПО

ПО - комплексное решение предназначено для выявления современных высокотехнологичных атак на ранней стадии, обеспечение процесса threat hunting, оптимизацию процессов реагирования на инциденты и их последующего расследования внутри корпоративной инфраструктуры. Оно определяет заражения, которые пропускают стандартные средства защиты: антивирусы, межсетевые экраны, системы предотвращения вторжений. Применение XDR существенно снижает риски организации, помогая вовремя выявить и предотвратить хищения, финансовые мошенничества, попытки шпионажа, утечку конфиденциальной информации и другие инциденты.

2 ЭТАПЫ ЖИЗНЕННОГО ЦИКЛА РАЗРАБОТКИ И ВНЕДРЕНИЯ ПО

Работы Исполнителя на протяжении всего жизненного цикла могут выполняться:

- 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.	Получение данных о защищаемой инфраструктуре заказчика	Заказчик
1.2.	Определение технической спецификации	Исполнитель
1.2.	Помощь в организации тестовой площадки или использовании реальной площадки	Исполнитель и Заказчик
1.3.	Подготовка ПО и лицензии	Исполнитель
1.4.	Передача ПО и лицензии заказчику	Исполнитель
1.5.	Внесение изменений в пилотный стенд Заказчика для доработки качества внедрения. Внедрение ПО	Заказчик и Исполнитель
1.6.	Проведение тестовых испытаний	Заказчик

1.7.	Проведение испытаний согласно Методике проведения испытаний ПО	Заказчика/ Исполнитель
------	--	---------------------------

2.3 Запуск в промышленную эксплуатацию

№	Краткое описание	Сторона
2.	Запуск в промышленную эксплуатацию	
2.1	Активация ПО на пилотном сегменте	Заказчик
2.2	Контроль получаемых данных, ошибок и пр.	Исполнитель
2.3	Контроль обращений/жалоб клиентов	Заказчик
2.7	Активизация ПО на всём сегменте заказчика	Заказчик

2.4 Промышленная эксплуатация

№	Краткое описание	Сторона
3.	Промышленная эксплуатация	
3.1.	Аналитическое сопровождение и работы по выявлению аномалий и инцидентов в системе Заказчика	Заказчик
3.2.	Обработка выявляемых алертов и предоставление обратной связи	Заказчик
3.3.	Контроль работоспособности ПО на стороне Заказчика	Заказчик
3.4.	Контроль работоспособности ПО	Исполнитель
3.5.	Доработка ПО и обновление	Исполнитель
3.6.	Периодическая отчетность по работоспособности	

2.5 Вывод из промышленной эксплуатации

№	Краткое описание	Сторона
4.	Прекращение эксплуатации	
4.1	Отключение ПО от центров обновления	Исполнитель
4.2	Отключение ПО от систем инфраструктуры заказчика	Заказчик

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 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА И 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.

Backend Разработчик (3 специалистов)

Компетенции сотрудников: Go, Python, Rust, PostgreSQL, Elasticsearch, ClickHouse

Работы: Техническая поддержка, аналитическое сопровождение, разработка и улучшение ПО.

DevOps Инженер (2 специалиста)

Компетенции сотрудников: Linux, Ansible, Docker, GitLab CI/CD, Elasticsearch, PostgreSQL, Minio

Работы: Техническая поддержка, аналитическое сопровождение, совершенствование ПО.

Аналитик разработки детектирующей логики (2 специалиста)

Компетенции сотрудников: Python, Zeek, Suricata

Работы: Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО. 2

Тестировщики (2 специалиста)

Компетенции сотрудников: Allure, Pytest, GitLab CI/CD

Работы: Разработка тест-планов, функциональное и нагрузочное тестирование, автоматизация тестов, регрессионное тестирование.

Технические Писатели (2 специалиста)

Работы: Разработка документации, техническая поддержка, аналитическое сопровождение, совершенствование ПО.

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.