Программное обеспечение

«Программный комплекс Bot-Trek TDS»

Описание процессов, обеспечивающих поддержание жизненного цикла

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание этапов жизненного цикла программного обеспечения «Программный комплекс Bot-Trek TDS» (далее – Bot-Trek TDS, ПО).

1.2 Назначение ПО

Программный комплекс Bot-Trek TDS является средством защиты конфиденциальной информации (системой обнаружения вторжений уровня сети) и предназначен для автоматизированного обнаружения компьютерных атак (вторжений) и вредоносного ПО в сетевом трафике при помощи сигнатурного метода выявления атак и эвристического анализа. Изделие устанавливается на границе сети с целью повышения уровня защищенности ИС, ЦОД, серверов и коммуникационного оборудования, АРМ пользователей.

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 Производство ПО

Технический контроль

Особо важные операции производства программных изделий подлежат техническому контролю.

К особо важным операциям производства программных изделий относятся:

1) Изготовление электронного носителя изделия с образа эталонной копии;
2) Проверка контрольной суммы;
3) Маркировка электронного носителя;
4) Изготовление комплекта эксплуатационной документации на электронном носителе;
5) Изготовление документов на бумажном носителе.

Стендовые испытания

Каждая новая версия изделия проверяется на стендовых испытаниях. Порядок и методика проведения стендовых испытаний определяется документом «Программа и методика испытаний».

Завершение испытаний каждой новой версии изделия оформляется протоколом. Новая версия принимается в эксплуатацию только в случае успешного проведения всех испытаний.

2.3 Поставка ПО

Методы идентификации ПО

В настоящем разделе описываются методы уникальной маркировки изделия и связанных с ним компонентов для обеспечения пользователей возможностью идентифицировать изделие и убедиться в том, что они используют сертифицированное изделие и сопутствующую документацию.

Идентификация программного обеспечения

Носитель, на котором поставляется изделие, маркируется следующей информацией:

1. Наименование (логотип) производителя.
2. Наименование изделия.
3. Обозначение изделия.
4. Серийный номер.
5. Контрольная сумма (приводится в формуляре на изделие).
6. Дата изготовления (приводится в формуляре на изделие).

Идентификация документации

Документация маркируется с использованием наименования документа и его обозначения в соответствии с требованиями ГОСТов серии ЕСПД (ГОСТ 19.101, ГОСТ 19.103).

Процедура для поддержки безопасности при распространении версий изделия к местам использования

Распространение версий изделия должно осуществляться на компакт-дисках или USB-накопителях, промаркированных в соответствии с «Техническими условиями».

Установку и обновление изделия должен выполнять уполномоченный администратор, ознакомившийся с эксплуатационной документацией.

Запись на электронные носители осуществляется строго по «Регламенту разработки» в компании – в соответствии с которым выпускающий редактор предоставляет уполномоченному администратору образ для записи на электронный носитель с контрольными суммами для сверки записываемого дистрибутива.

Процедура обнаружения расхождения между оригиналом и полученной версией

Проверка внешнего вида

Порядок проверки внешнего вида приведен ниже.

1) Убедиться, что изделие поставлено на компакт-диске.

2) Убедиться, что маркировка футляра компакт-диска выполнена печатным способом и содержит наименование, обозначение, серийный номер изделия, контрольную сумму и дату изготовления.

3) Убедиться, что маркировка компакт-диска выполнена печатным способом и содержит наименование, обозначение, серийный номер изделия, контрольную сумму и дату изготовления.

Проверка комплектности

Убедиться, что изделие содержит:

- компакт-диск с записанным на нем дистрибутивом;
- копию сертификата на бумажном носителе;
- формуляр на бумажном носителе;
- комплект эксплуатационной документации на электронном носителе.

Проверка соответствия, полученного потребителем изделия, сертифицированному

Проверка изделия проводится сверкой контрольной суммы дистрибутива изделия со значением, указанным в соответствующем разделе формуляра и на этикетке компакт-диска.

Методика проверки контрольной суммы приведена в Формуляре и Технических условиях на изделие.

Процедура обновления ПО

Обновление ПО должно осуществляться уполномоченным администратором после получения официального уведомления об обновлении ПО.

Процедура обновления описана в Руководстве администратора.

Действия при обнаружении несоответствий

В случае обнаружения несоответствий при проведении проверки изделия необходимо обратиться к производителю.

2.4 Промышленная эксплуатация

Фиксация появления нового типа вторжения

Обновление Базы решающих правил (далее – БРП) является одним из важных аспектов эффективного функционирования системы обнаружения вторжения.

Поставщики БРП осуществляют постоянный мониторинг появления новых сетевых атак. Обнаруженные атаки локализуются, и на их основе формируется ежемесячное обновление. Разработчик ежедневно осуществляет загрузку, проверку и анализ обновлений от Поставщиков БРП.

Кроме того, Разработчик независимо от Поставщиков БРП осуществляет постоянный мониторинг появления новых сетевых угроз. На основании проведенного мониторинга Разработчик может пополнить обновленную БРП собственными правилами, а также модифицировать полученные от Поставщика БРП правила.

Существует два механизма, которые используются для обнаружения новых типов вторжений:

- исследовательские работы, выполняемые сотрудниками предприятия-производителя (АО «БУДУЩЕЕ») сертифицированного Программного комплекса Bot-Trek TDS (далее по тексту – изделие);
- акты рекламации, поступающие от пользователей сертифицированного изделия.

Исследовательские работы предусматривают анализ открытых источников, данных сети «Интернет», содержащих сведения об уязвимостях программного обеспечения.

При получении акта рекламации выполняется анализ вторжения, описание которого не присутствует в текущей БРП. Выполняются тестовые атаки и исследования на стенде предприятия-разработчика для изучения атаки и формирования ее признаков.

По результатам изучения нового типа вторжения устанавливается его актуальность и признаки, которые могут быть использованы для его обнаружения.

Процедура уведомления об обновлении БРП

Разработчик с использованием электронных почтовых сообщений направляет в адрес организаций, эксплуатирующих сертифицированное изделие «Информационный манифест», содержащий краткое описание нового типа вторжения и декларацию факта обновления базы решающих правил для обнаружения нового типа вторжения в течение 1 месяца.

Разработчик ведет учет списка атак в документе «Описание новых типов вторжений». Для каждого нового типа вторжения указывается следующая информация: идентификатор, дата внесения в перечень, идентификатор документа «Информационный манифест», описание атаки и ее признаки, статус (изменение в БРП внесено/не внесено). Момент появления нового типа вторжения фиксируется в документах «Информационный манифест» и «Описание новых типов вторжений».

Предприятие-производитель ведет учет покупателей сертифицированного изделия. Выполняется регистрация следующей информации: наименование организации, адрес организации, номер знака соответствия, контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование изделия). Уведомление пользователей о выпуске обновления БРП выполняется с использованием рассылки электронных почтовых сообщений.

Процедура доставки обновлений БРП

Процедура предоставления обновлений БРП в общем случае выглядит следующим образом:

1) загрузка обновлений с серверов Поставщика БРП, предоставляющих обновления БРП для Разработчика;
2) проверка целостности загруженных обновлений;
3) обработка БРП;
4) тестирование работоспособности изделия с обновленными правилами;
5) оценка влияния обновленных БРП на функции безопасности изделия;
6) подготовка к отгрузке обновленных БРП:
   - формирование архива с БРП;
   - формирование файла с контрольной суммой БРП;
   - формирование файла с временной меткой;
7) отправка файлов с архивом обновлений на электронные почтовые адреса зарегистрированным организациям.

Процедура контроля целостности обновлений БРП

Обновления БРП, успешно прошедшие контроль влияния на безопасность изделия, отправляются в виде файла архива на электронные почтовые ящики зарегистрированных организаций, эксплуатирующих изделие. Контрольная сумма архива, также высылается электронным сообщением. После получение обновления БРП пользователь имеет возможность выполнить контроль его целостности с использованием механизма контрольного суммирования.

2.5 Обновление ПО

При выпуске обновления (исправление ошибок, улучшение в функционировании компонентов, добавление новых функций безопасности информации или изменение в имеющихся функциях безопасности информации), после испытания средства защиты информации (самостоятельно или с привлечением испытательной лаборатории), производитель изделия с использованием электронных почтовых сообщений направляет в адрес организаций, эксплуатирующих сертифицированное изделие, уведомление о необходимости применения обновления.

После согласования испытаний в ФСТЭК России производитель предоставляет пользователю изделия:

- бумажную заверенную копию обновленного сертификата (если обновлялся) и извещение о внесении изменений в формуляр;
- ссылку на файл дистрибутива для обновления версии программного обеспечения;
- ссылку на архив с электронными копиями измененных эксплуатационных документов.

Сведения о контрольных суммах файла дистрибутива и файла с архивом эксплуатационных документов высылается в бумажном виде в адрес организации, эксплуатирующей изделие, в виде уведомления, подписанного руководителем предприятия – производителя изделия и скрепленного печатью.

Верификация обновления осуществляется путем расчета контрольных сумм файлов дистрибутива с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС 2.0.2» по алгоритму «ГОСТ Р 34.11-94» и их сравнения со значениями, указанными в уведомлении.

После верификации файлов дистрибутива изделия пользователю изделия надлежит провести верификацию файла с электронными копиями измененных эксплуатационных документов и сравнить контрольную сумму файла с архивом со значением, указанным в уведомлении.

В разделе формуляра «Особые отметки» необходимо произвести запись о получении и применении файлов обновления.

Предоставленный в электронном виде формуляр должен быть распечатан, в разделе «Особые отметки» должна быть сделана запись о замене формуляра со знаком соответствия системы сертификации на обновленный формуляр. На замененном формуляре следует сделать запись: «Формуляр аннулирован. Знак соответствия системы сертификации

(голографическая наклейка) действителен». Замененный формуляр следует хранить вместе с обновленным для сохранения знака соответствия системы сертификации.

При возникновении проблем с установкой или работой изделия необходимо обратиться за помощью в службу технической поддержки по телефону в Москве: +7 (495) 984-33-64.

2.6 Устранение уязвимостей

Процедура устранения уязвимостей изделия должна обеспечивать возможность обновления программного обеспечения изделия для устранения актуальных уязвимостей, имеющих критический характер для функционирования изделия. Устранение уязвимостей должно производиться производителем изделия с использованием организационно-технических процедур представленных ниже.

Производитель периодически, не реже одного раза в месяц, должен проводить поиск известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях. В качестве общедоступных источников в первую очередь должна использоваться база данных уязвимостей в составе банка данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), а также следующие дополнительные источники:

- банк данных уязвимостей CVE (http://cve.mitre.org/);
- банк данных уязвимостей Tenable research team (https://www.tenable.com/sc-dashboards);
- и другие.

Поиск информации в базах данных по уязвимостям изделия проводят с целью проверки соответствия изделия требованиям, указанным в документах «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

Производитель должен провести анализ выявленных уязвимостей изделия.

При анализе уязвимостей необходимо учитывать следующие критерии:

- тип ошибки;
- версию программного обеспечения изделия, подверженную уязвимости;
- уровни опасности уязвимости:
  - критическая (Critical);
  - высокая (High);

- средняя (Medium);
- низкая (Low);

- информацию об устранении.

В случае выявления информации об уязвимости изделия из различных источников и отсутствия информации об этой уязвимости в базе данных уязвимостей (далее по тексту БДУ), производитель предоставляет информацию о данной уязвимости в ФСТЭК России для размещения в БДУ.

При выявлении уязвимостей изделия производитель должен осуществить следующие мероприятия:

- подготовить дистрибутив с устраненными уязвимостями;
- уведомить пользователей об уязвимостях изделия путем рассылки электронных почтовых сообщений.
- довести информацию до пользователей изделия об организационно-технических мерах по устранению в нем уязвимостей;
- производитель оповещает пользователей изделия о необходимости установки обновленной версии изделия;
- производитель обеспечивает гарантированную доставку пользователям изделия файла с обновленной версией изделия;
- пользователь изделия обновляет программное обеспечение с соответствующими отметками в разделах формуляра;
- в случае внесения в изделие изменений, связанных с устранением уязвимостей или обновлением баз данных, необходимых для реализации функций безопасности изделия, производитель обязан провести испытания средства защиты информации самостоятельно или с привлечением испытательной лаборатории;
- по результатам проведенных испытаний изделия в связи с внесением в него изменений производитель представляет материалы испытаний в ФСТЭК России;
- после согласования материалов испытаний в ФСТЭК России производитель должен предоставить пользователю изделия:
  - бумажную заверенную копию обновленного сертификата (если обновлялся) и извещение о внесении изменений в формуляр;
  - ссылку на файл дистрибутива для обновления версии программного обеспечения;
  - ссылку на архив с электронными копиями измененных эксплуатационных документов.

Сведения о контрольных суммах файла дистрибутива и файла с архивом эксплуатационных документов высылается в бумажном виде в адрес организации, эксплуатирующей изделие, в виде уведомления, подписанного руководителем предприятия – производителя изделия и скрепленного печатью.

– в случае невозможности устранения уязвимостей изделия, в том числе путем применения обновления, производитель разрабатывает ограничения по применению изделия, которые незамедлительно доводит до испытательной лаборатории;

– если в соответствии с заключением испытательной лаборатории ограничение по применению позволит устранить уязвимость, производитель незамедлительно и гарантированно с подтверждением доводит его до пользователей;

– производитель вносит необходимые изменения в эксплуатационную документацию и направляет ее совместно с заключением испытательной лаборатории в ФСТЭК России. Пользователи реализуют указанное ограничение по применению изделия;

– если пользователь не может реализовать ограничение по применению изделия он прекращает его применение;

– если уязвимость не устраняется путем установления ограничений по применению, производитель незамедлительно и гарантированно с подтверждением сообщает об этом всем пользователям и в ФСТЭК России. Пользователи прекращают применение изделия.

2.7 Сопровождение ПО

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

2.8 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.

2.9 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, ClickHousePаботы: 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.

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 КОМАНД РАЗРАБОТКИ И ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Команда разработки и технической поддержки 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.