ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Attack Surface Management»

Описание процессов, обеспечивающих поддержание жизненного цикла

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Описание
ВПО	Вредоносное программное обеспечение
Заказчик	Лицо, которое использует на законных основаниях ПО на основании заключенного договора
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО «БУДУЩЕЕ»; • Компанией-интегратором, по выбору Заказчика
ПО	Программное обеспечение «F6 Attack Surface Management»
Разработчик	АО «БУДУЩЕЕ»
СЗИ	Системы защиты информации
Скриншот	Изображение, «снимок» экрана ПК или мобильного устройства, на котором запечатлено содержимое экрана устройства
API (Application Programming Interface)	Описание способов взаимодействия одной компьютерной программы с другими
DoS/DDoS (Denial of Service)	Хакерская атака с целью довести атакуемый ресурс до состояния «отказ в обслуживании»
DMARC (Domain-based Message Authentication, Reporting and Conformance)	Техническая спецификация, созданная группой организаций, предназначенная для снижения количества СПАМа и фишинговых электронных писем
DNS (Domain Name Service)	Компьютерная распределенная система для получения информации о доменах
DNSSEC (Domain Name System Security Extensions)	Набор расширений протокола DNS
SaaS (Software as a Service)	Модель обслуживания, при которой программное обеспечение размещено в облачной инфраструктуре
SIEM (Security Information and Event Management)	Система управления информационной безопасностью и событиями безопасности
SOAR (Security Orchestration, Automation and Response)	Класс программных продуктов, предназначенных для объединения других защитных решений в единую систему
SPF (Sender Policy Framework)	Стандартный способ аутентификации электронной почты
SSL (Secure Sockets Layer)	Криптографический протокол, который обеспечивает более безопасную связь

TLS (Transport Layer Security)	Криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет
WHOIS	Сервис для получения информации о регистрации доменов, например, дату регистрации и возраст домена, или узнать контакты, по которым можно связаться с организацией или человеком, чей домен вас заинтересовал

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ описывает процессы поддержания жизненного цикла программного обеспечения «F6 Attack Surface Management» (далее — ПО, Система, Attack Surface Management, ASM). 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 Attack Surface Management» (ASM) — это комплексная информационно-аналитическая система, предназначенная для всесторонней оценки поверхности атаки организации, включая ее цифровые активы, доступные в публичном пространстве. Полученные данные, метрики и рекомендации могут выступать основой для построения и совершенствования процессов защиты и реагирования в рамках стратегии информационной безопасности компании.

1.3 Функциональные возможности ПО

ПО обладает следующими функциональными возможностями:

Идентификация активов

- Выявление IP-адресов (IPv4, IPv6), связанных с активами компании;
- Сбор данных о развернутом оборудовании компании и сопоставление с данными об уязвимостях;
- Выявление фактов упоминания активов компании на теневых площадках сети Интернет;
- Сбор данных, относящихся к опубликованным доменам, которые содержат преднамеренные орфографические неточности в доменном имени.

Генерация оповещений

- Сопоставление информации из образов ВПО с данными об инфраструктуре компании и оповещение в случаях, если ВПО имеет файл настроек, где затрагиваются IP-адреса, домены и другие активы компании, или же ВПО делает запрос к активам Заказчика;
- Интеграция системы оповещений через SIEM и SOAR.

Валидация активов

- Отображение полной инфраструктуры компании с технической оценкой активов и уровня защищенности инфраструктуры в режиме реального времени;
- Обнаружение и анализ уязвимостей конфигураций сервисов, приложений, программного и аппаратного обеспечения, в том числе программных библиотек в активах компании;
- Поиск неточностей в конфигурации активов компании, таких как: общедоступные базы данных, файловые хранилища или списки директорий сервисов;
- Обнаружение фактов взаимодействия ВПО, проанализированных в общедоступных решениях типа “песочница”, а также проанализированных в платформах детонации, с активами компании;
- Предоставление информации о принадлежности активов компании к бот-сетям.

Отслеживание изменений

- Пассивное сканирование пространства IPv4 на предмет выявления активов инфраструктуры компании в режиме реального времени;
- Обнаружение неточностей в конфигурации DNSSEC, SPF и DMARC в активах компании;
- Выявление наличия работающего ВПО в выявленных активах компании.
- Обнаружение и анализ самоподписанных сертификатов, актуальных версий SSL/TLS и алгоритмов шифрования в активах;
- Предоставление актуальной информации о событиях фишинга, затрагивающих инфраструктуру компании;
- Выявление использования вредоносного кода типа JS-снифферы на доменах и страницах вебсайтов компании;
- Отслеживание изменений и повторные проверки уровня защищенности.

Активное сканирование

- Выявление уязвимостей в учетных записях, работающих по протоколам SSH, FTP, HTTP и др.
- Выявление скрытых ресурсов веб-приложений с помощью автоматизированного перебора пустей, включая страницы, директории и файлы, не предназначенные для публичного доступа;
- Определение фактического уровня риска путём имитации реальных атак
- Сканирование подсетей компании для определения открытых портов, служб и используемых веб-приложений.

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:

– Определение задач тестирования;
– Написание программы ручного тестирования;
– Проведение ручного тестирования функциональности;
– Отчет о проведенном тестировании;
– Внесение корректировок в работу функциональности после проведенного тестирования.

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 и доступа к ПО;
– Контроль получаемых данных, ошибок и пр.;
– Настройка систем мониторинга и анализа;
– Первичный сбор данных и надстройка.

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:

– Обработка выявляемых событий и предоставление обратной связи;
– Контроль работоспособности ПО;
– Доработка ПО и обновление.

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» либо на электронный ящик info@f6.ru со следующими данными:

1. Четко сформулированная тема обращения;
2. Пошаговое описание воспроизведения ошибки;
3. 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://asm.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 Attack Surface Management»: 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 Attack Surface Management»

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, JavaScript, TypeScript;
- знание реляционных и не реляционных БД, исходя из должностных обязанностей: Cassandra, MySQL, 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.	1
Backend разработчик	Python, Go, Kubernetes, Cassandra, Elasticsearch, MySQL	Техническая поддержка; Аналитическое сопровождение; Разработка и совершенствование ПО.	2
DevOps инженер	Kubernetes, FluxCD, Docker, GitLab CI\CD, Elasticsearch, Cassandra	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	1
Технические писатели	Разработка документации	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	2

7 ИНФОРМАЦИЯ О ФАКТИЧЕСКИХ АДРЕСАХ

Фактический адрес размещения разработчиков ПО «F6 Attack Surface Management»

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

Фактический адрес размещения службы поддержки ПО «F6 Attack Surface Management»

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 Attack Surface Management»

ПО «F6 Attack Surface Management» 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.