ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F.A.C.C.T. Threat Intelligence»

Описание процессов, обеспечивающих поддержание жизненного цикла

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ описывает процессы поддержания жизненного цикла программного обеспечения «F.A.C.C.T. Threat Intelligence» (далее — ПО, Система, Threat Intelligence). 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

F.A.C.C.T. Threat Intelligence – система учета скомпрометированной информации, предназначена для сбора информации о случаях компрометации учетной информации пользователей информационных систем, компрометации информации о банковских картах, сбора информации о первичных получателях похищаемых денежных средств (далее - дропов), а так же предоставления интерфейса для отображения данных и оповещения о выявленных случаях компрометации данных с целью минимизации рисков мошенничества в отношении финансовых организаций в разных странах.

Основными целями создания Системы являются:

- Предоставление единого интерфейса регистрации фактов компрометации учетных данных пользователей интерактивных информационных систем (дистанционного банковского обслуживания, платежных систем, систем обмена электронными сообщениями, систем хранения данных в сети интернет и прочих электронных интерактивных систем);
- Консолидация разрозненной информации по компрометации информации в сферах финансового обслуживания, хранения данных, оказания государственных услуг и электронной коммерции;
- Генерация правил для систем предотвращения мошеннических операций, используемых организациями, участниками системы;
- Оперативное оповещение участников системы;
- Снижение уровня преступлений в сфере электронной коммерции;
- Ускорение процесс обмена информацией о мошенничестве между банками;
- Повышение качества и количества раскрываемых преступлений;
- Предоставление прозрачной статистической и аналитической информации.

2 ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА ПО

1. Определение общей архитектуры ПО, его компонентов и взаимодействия.
2. Выбор технологий (языки программирования, средства компиляции, базы данных и т.д.).
3. Написание и документирование исходного кода.
4. Объединение компонентов системы в единое целое.

3 ТЕСТИРОВАНИЕ

1. Проверка кода на наличие ошибок и отладка (исправление) кода.
2. Оптимизация кода для улучшения производительности, качества и безопасности ПО.
3. Интеграционное тестирование.

4 ИСПЫТАНИЯ

1. Создание и настройка учетных записей клиента.
2. Проверка привязки данных в системе к учетной записи клиента
3. Корректировка сигнатур и настроек для обнаружения данных клиента

5 ЗАПУСК В ПРОМЫШЛЕННУЮ ЭКСПЛУАТАЦИЮ ПО

1. Передача реквизитов доступа к ПО.
2. Контроль получаемых данных, ошибок и пр.
3. Настройка систем мониторинга и анализа.
4. Первичный сбор данных и надстройка.

6 ПРОМЫШЛЕННАЯ ЭКСПЛУАТАЦИЯ ПО

1. Аналитическое сопровождение и работы по выявлению аномалий и мошеннической активности среди клиентов Заказчика.
2. Обработка выявляемых событий и предоставление обратной связи.
3. Тонкая настройка правил выявления мошеннической активности.
4. Контроль работоспособности ПО.
5. Доработка ПО и обновление.
6. Периодическая отчетность по работоспособности.

7 ВЫВОД ИЗ ПРОМЫШЛЕННОЙ ЭКСПЛУАТАЦИИ

1. Блокировка учетных записей клиента.

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.

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.

10 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА И ИНФОРМАЦИЯ О ПЕРСОНАЛЕ

Специалисты, занимающиеся технической и аналитической поддержкой, а также развитием программного обеспечения, должны обладать следующими знаниями и навыками:

- Знание специфики работы с ПО;
- Навыки программирования, соответствующие должностным обязанностям: PHP, Python, Go, JavaScript, TypeScript;
- Знание реляционных и нереляционных баз данных в рамках должностных обязанностей: Cassandra, Elasticsearch, ClickHouse.

Для обеспечения бесперебойной работы ПО необходима команда технической и аналитической поддержки в количестве:

- Специалисты разработки – 14.
- DevOps инженер – 1.
- Специалисты мониторинга и анализа – 14.

Техническая поддержка осуществляется по электронной почте intelligence@facct.ru или в пользовательском интерфейсе Системы по ссылке https://ti.facct.ru/p/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

11 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