# Описание процессов, обеспечивающих поддержание жизненного цикла, в том числе устранение неисправностей и совершенствование, а также информацию о персонале, необходимом для обеспечения такой поддержки, ПО «CTT Downloader»

# ОГЛАВЛЕНИЕ

# 1. ВВЕДЕНИЕ

Настоящее руководство описывает процессы, обеспечивающие поддержание жизненного цикла ПО «CTT Downloader», включая регламент технической поддержки.

## 2. ЖИЗНЕННЫЙ ЦИКЛ ПРОГРАММНОГО ПРОДУКТА, ВКЛЮЧАЯ ИНФОРМАЦИЮ О СОВЕРШЕНСТВОВАНИИ ПО

ПО «CTT Downloader» распространяется в виде Standalone-приложения - заказчику предоставляются инструкция и дистрибутив для локальной установки ПО на вычислительном устройстве заказчика, причем заказчику доступна загрузка дистрибутива ПО с сайта правообладателя ПО по ссылке, предоставляемой после приобретения ПО.

Для контроля версий ПО «CTT Downloader» каждый релиз имеет свой номер. Номер выставляется согласно правилам семантического версионирования.

Номер версии представляется в формате «A.B.C», где

- A – мажорная версия, при появлении обратно не совместимых изменений.
- B – минорная версия, дополняющая функции ПО, но не нарушающая обратной совместимости.
- C – патч-версия, исправляющая ошибки, не влияющие на совместимость.

Выпуск мажорной версий производится только при внесении обратно несовместимых изменений в протокол, описанный в Приложении 1 и Приложении 2, без автоматического обновления версий ПО «CTT Downloader», установленных на стороне заказчиков. Независимо от типа установленного решения заказчик сам управляет процессом обновления ПО «CTT Downloader».

# 3. ИНФОРМАЦИЯ О СОВЕРШЕНСТВОВАНИИ ПО

ПО «CTT Downloader» реализовано в виде консольного Standalone-приложения. Данное приложение потребляет фиксированные вычислительные ресурсы и не требует горизонтального, либо вертикального масштабирования.

Процесс обновления экземпляра программного обеспечения представляет собой замену исполняемого файла приложения и/или его конфигурационных файлов и, как правило, связан с полной остановкой и последующим перезапуском приложения.

С выпуском новой версии программного продукта правообладатель оповещает своих заказчиков об этом факте по электронной почте, либо по иным каналам связи, выбранным заказчиком. В рамках данного сообщения правообладатель указывает:

- Причины внесения изменений.
- Детали внесенных изменений.
- Ссылку на новую версию ПО.

В случае, если правообладатель вносит обратно несовместимые изменения в ПО, или протокол, за месяц до внесения изменений правообладатель оповещает заказчиков.

# 4. ИНФОРМАЦИЯ ОБ УСТРАНЕНИИ НЕИСПРАВНОСТЕЙ В ХОДЕ ЭКСПЛУАТАЦИИ ПО

В случае возникновения неисправностей в ПО, алгоритм исправления неисправности включает следующие шаги:

1. Заказчик оповещает правообладателя о выявленных проблемах путем уведомления в электронной почте.
2. Заказчик высылает электронный журнал событий ПО «CTT Downloader».
3. Правообладатель устраняет проблему и выпускает новую патч-версию ПО.
4. Все заказчики оповещаются о выходе новой патч-версии.

# 3 ТИПОВОЙ РЕГЛАМЕНТ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

## 3.1 Условия предоставления услуг технической поддержки

Услуги поддержки оказываются индивидуально для каждого заказчика. В приоритетном режиме рассматриваются запросы о проблемах, блокирующих работу заказчика на ПО «CTT Downloader».

## 3.2 Каналы доставки запросов в техническую поддержку

Запросы на техническую поддержку осуществляются по электронной почте.

## 3.3 Выполнение запросов на техническую поддержку

При формировании запроса на техническую поддержку реализуется принцип одна проблема – один запрос. Таким образом, заказчик, для рассмотрения новой проблемы формирует новый запрос, а не включает его в предыдущий.
При формировании запроса заказчик указывает:

- версию ПО «CTT Downloader»;
- журнал событий ПО;
- описание проблемы.

## 3.4 Порядок выполнения работ по оказанию технической поддержки

Каждый запрос в службу технической поддержки обрабатывается следующим образом:

1. Заказчик получает подтверждение получения запроса в ответе на сообщение по электронной почте.
2. Запрос обрабатывается и выполняется согласно установленной системе приоритетов.
3. Правообладатель предоставляет заказчику варианты решения возникшей проблемы согласно содержанию запроса.
4. Заказчик обязуется выполнять все рекомендации и предоставлять необходимую дополнительную информацию специалистам исполнителя для своевременного решения запроса.

## 3.5 Закрытие запросов в техническую поддержку

После доставки ответа запрос считается завершенным, и находится в таком состоянии до получения подтверждения от заказчика о решении инцидента. В случае аргументированного несогласия заказчика с завершением запроса, выполнение запроса продолжается.

Завершенный запрос переходит в состояние закрытого после получения исполнителем подтверждения от заказчика о решении запроса. В случае отсутствия

ответа заказчика о завершении запроса в течение 5 рабочих дней, запрос считается автоматически закрытым. Закрытие запроса может инициировать заказчик, если надобность в ответе на запрос пропала.

## 3.6 Персонал для поддержания жизненного цикла

### 3.6.1 Сотрудники и компетенции у правообладателя

| № | Направление | Компетенции | Количество сотрудников |
|---|---|---|---|
| 1 | Разработчики | Python, Groovy, Java, Apache Nifi, Clickhouse, KeyDB, NGINX | 1 |
| 2 | Специалисты службы технической поддержки | | 1 |

Указанные специалисты являются штатными сотрудниками Правообладателя - ООО "ТЕХНОЛОГИИ КИБЕРУГРОЗ".

# 4 КОНТАКТНАЯ ИНФОРМАЦИЯ ПРАВООБЛАДАТЕЛЯ ПРОГРАММНОГО ПРОДУКТА

## 4.1 Юридическая информация

Информация о юридическом лице компании:

- **Название компании:** ООО «Технологии киберугроз»
- **Юр. адрес:** 121596, город. Москва, вн.тер. г. Муниципальный Округ Можайский, ул Горбунова, дом 2, строение 3, этаж/помещ 9/II, ком./офис 52/250
- **ОГРН:** 1227700260127
- **ИНН:** 9731092317

## 4.2 Контактная информация службы технической поддержки

Связаться со специалистами службы технической поддержки можно одним из следующих способов:

- **Сайт:** https://cyberthreat.tech
- **Email:** support@cyberthreattech.ru, info@cyberthreattech.ru

Фактический адрес размещения инфраструктуры разработки:

- Россия, Москва, ул. Горбунова, д. 2, стр. 3, этаж 9, пом. II, ком. 52, офис 250
- Россия, Москва ул. Берзарина, д. 36 стр. 3
- Россия, Санкт-Петербург ул. Цветочная, д. 19
- Россия, Санкт-Петербург г. п. Дубровка, ул. Советская, д. 1

Фактический адрес размещения разработчиков:

- Россия, Москва, ул. Горбунова, д. 2, стр. 3, этаж 9, пом. II, ком. 52, офис 250

Фактический адрес размещения службы поддержки:

- Россия, Москва, ул. Горбунова, д. 2, стр. 3, этаж 9, пом. II, ком. 52, офис 250

Фактический адрес размещения серверов:

- Россия, Москва ул. Берзарина, д. 36 стр. 3
- Россия, Санкт-Петербург ул. Цветочная, д. 19
- Россия, Санкт-Петербург г. п. Дубровка, ул. Советская, д. 1

# ПРИЛОЖЕНИЕ 1. СПЕЦИФИКАЦИЯ ОТКРЫТОГО ПРОТОКОЛА ВЗАИМОДЕЙСТВИЯ С ВНЕШНИМИ СТОРОННИМИ СЕРВИСАМИ.

1. Для работы с ПО «CTT Downloader» сторонние сервисы обязаны реализовать следующую спецификацию.
2. Протокол: HTTP/HTTPS
3. Аутентификация: Каждый запрос ПО «CTT Downloader» содержит HTTP-заголовок "x-api-key". Значение заголовка содержит API-key, заданный в конфигурационном файле.
4. Основной URL обязан удовлетворять шаблону: <http|https>://<FQDN>/static/v2/full/
5. Реализация запросов метода HEAD:
    a. Точка входа: <Основной URL>/<ip|domain|url|hash>
    b. В заголовке ответа должен присутствовать "Last-Modified", удовлетворяющий форматной строке "%a, %d %b %Y %H:%M:%S %Z"
6. Реализация запросов метода GET:
    a. Точка входа: <Основной URL>/<ip|domain|url|hash>/?type=json&date=<date>
    b. Параметр date должен удовлетворять форматной строке "%Y%m%d" и формироваться на основе поля "Last-Modified" из HEAD-запроса
    c. Ответ: JSON, либо GZ-архив с JSON-файлом, удовлетворяющим формату из Приложения 2.

# ПРИЛОЖЕНИЕ 2. СПЕЦИФИКАЦИЯ ФОРМАТА JSON С ИНДИКАТОРАМИ

Тип индикатора: IP

```
{
 {
 "ip": {
  "v4": <string>,
  "num": <string>      - IPv4 в формате UInt32
 },
 "fseen": <int>,      - timestamp первого появления
 "lseen": <int>,      - timestamp последнего появления
 "collect": <int>,    - timestamp сбора
 "src": {
  "name": <string>      - название источника IoC
  "report": <string>         - URL источника IoC
 }
 "tags": {                - категория индикатора
  "str": [<string>],
 },
 "cve": <string>,                  - связь с CVE
 "industry": <string>,     - в каких секторах экономики наблюдался IoC
 "threat": [<string>],  - атрибуция с группировкой/ВПО/хакерской утилитой
 "score": {                  - уровень опасности
  "total": <int>,               - итоговый уровень
  "src": <double>,              - доверие к источникам
  "tags": <double>,             - уровень опасности по контексту
  "frequency": <double>          - частота появления IoC
 },
 "fp": {                    - вероятного ложного срабатывания
  "alarm": <string>,          - флаг "false"/"true"
  "descr": <string>              - описание причины выставления флага
 },
 "asn": {
  "num": <int>,            - номер ASN
  "firstip": {
   "netv4": <string>, - начало диапазона IP ASN
   "num": <string>   - IPv4 в формате UInt32
  },
  "lastip": {
   "netv4": <string>, - окончание диапазона IP ASN
   "num":  <string>       - IPv4 в формате UInt32
  },
  "cloud": <string>,              - название облачного провайдера, или CDN (AWS, GCP и т.д.)
  "domains": <int>,         - кол-во доменов, зарегистрированных в ASN
  "org": <string>,    - владелец ASN
  "isp": <string>          - владелец ASN
 },
 "geo": {                   - Геоданные
  "city": <string>,
  "country": <string>,
```

```
   "region": <string>
  },
  "related": {
    "domains": [<string>]  - связанные вредоносные домены
  }
}
```

Тип индикатора: Domain

```
{
  {
  "domain": <string>,
  "fseen": <int>,      - timestamp первого появления
  "lseen": <int>,      - timestamp последнего появления
  "collect": <int>,    - timestamp сбора
  "src": {
    "name": <string>      - название источника IoC
    "report": <string>         - URL источника IoC
  }
  "tags": {                - категория индикатора
    "str": [<string>],
  },
  "cve": <string>,                  - связь с CVE
  "industry": <string>,     - в каких секторах экономики наблюдался IoC
  "threat": [<string>],  - атрибуция с группировкой/ВПО/хакерской утилитой
  "score": {                  - уровень опасности
    "total": <int>,               - итоговый уровень
    "src": <double>,              - доверие к источникам
    "tags": <double>,             - уровень опасности по контексту
    "frequency": <double>          - частота появления IoC
  },
  "fp": {                     - вероятного ложного срабатывания
    "alarm": <string>,          - флаг "false"/"true"
    "descr": <string>               - описание причины выставления флага
  },
  "resolved": {          - дополнительная информация (whois, dns)
    "ip": {
      "a": [             - DNS A-записи
        <string>
      ],
      "alias": <string>,        - основной домен, если IoC является CNAME-записью
      "cname": [<string>]         - DNS CNAME-записи
    },
    "whois": {           - WHOIS
      "created": <string>,
      "updated": <string>,
      "expires": <string>,
      "age": <int>,
      "registrar": <string>,
      "registrant": <string>,
      "havedata": "none"  - "false" - whois сервис не нашел записи
                          "true"  - whois нашел запись
                          "none"  - whois не ответил
```

```
   }
  }
}
```

Тип индикатора: URL

```
{
  {
  "url": <string>,
  "fseen": <int>,      - timestamp первого появления
  "lseen": <int>,      - timestamp последнего появления
  "collect": <int>,    - timestamp сбора
  "src": {
    "name": <string>      - название источника IoC
    "report": <string>         - URL источника IoC
  }
  "tags": {                - категория индикатора
    "str": [<string>],
  },
  "cve": <string>,                  - связь с CVE
  "industry": <string>,     - в каких секторах экономики наблюдался IoC
  "threat": [<string>],  - атрибуция с группировкой/ВПО/хакерской утилитой
  "score": {                  - уровень опасности
    "total": <int>,               - итоговый уровень
    "src": <double>,              - доверие к источникам
    "tags": <double>,             - уровень опасности по контексту
    "frequency": <double>          - частота появления IoC
  },
  "fp": {                     - вероятного ложного срабатывания
    "alarm": <string>,          - флаг "false"/"true"
    "descr": <string>               - описание причины выставления флага
  },
"resolved": {             - HTTP-код ответа от Web-сервера на момент сбора IoC
    "status": <int>
  },
  "parsed": {               - декомпозиция URL
        "schema": <string>,
        "domain": <string>,
        "port": <int>,
        "path": <string>,
        "params": <string>,
        "anchor": <string>
  }
}
```

Тип индикатора: Hash

```
{
  {
  "md5": <string>,
  "sha1": <string>,
  "sha256": <string>,
  "filename": [<string>],
  "fseen": <int>,      - timestamp первого появления
```

```
  "lseen": <int>,      - timestamp последнего появления
  "collect": <int>,    - timestamp сбора
  "src": {
    "name": <string>      - название источника IoC
    "report": <string>        - URL источника IoC
  }
  "tags": {               - категория индикатора
    "str": [<string>],
  },
  "cve": <string>,                  - связь с CVE
  "industry": <string>,     - в каких секторах экономики наблюдался IoC
  "threat": [<string>],  - атрибуция с группировкой/ВПО/хакерской утилитой
  "score": {                  - уровень опасности
    "total": <int>,               - итоговый уровень
    "src": <double>,              - доверие к источникам
    "tags": <double>,             - уровень опасности по контексту
    "frequency": <double>         - частота появления IoC
  },
  "fp": {                     - вероятного ложного срабатывания
    "alarm": <string>,          - флаг "false"/"true"
    "descr": <string>             - описание причины выставления флага
  }
}
```