Автоматизированная информационная система

PARUS BOX

Описание функциональных характеристик программного обеспечения

8 листов

Москва, 2024

Содержание

1 Введение

Настоящий документ содержит перечень функциональных возможностей программного обеспечения (далее – ПО) PARUS BOX версии 1.X.X (далее – PBOX, Система, АИС).

PBOX – это облачный сервис (SaaS), предназначенный для потоковой проверки файлов различных типов, в том числе архивов, на предмет осуществления ими вредоносной или потенциально опасной активности.

PBOX представляет собой приложение, работающее в инфраструктуре разработчика, к которому для отправки файлов и получения результатов их проверки подключаются устройства, информационные системы и пользователи конечных заказчиков. Подключение осуществляется по различным протоколам посредством сети Интернет.

2 Назначение

Система предназначена для автоматизации следующих задач компаний-заказчиков:

- потоковой проверки файлов в трафике, обрабатываемом на межсетевых экранах;
- ручной загрузки и проверки подозрительных файлов;
- проверки файлов, обрабатываемых в других информационных системах;
- осуществления статического и динамического (поведенческого) анализа файлов;
- проверки контрольных сумм файлов на наличие их в различных базах вредоносных файлов;
- предоставления вердиктов, отчетов и другой метаинформации о проверках файлов.

Целевой заказчик PBOX – департаменты, отвечающие за информационные технологии и информационную безопасность в компаниях ЕАЭС, перед которыми стоит задача обеспечения информационной безопасности компании либо любые другие задачи, связанные с механизмами определения вредоносных файлов.

3 Функциональные возможности

В состав Системы входят следующие компоненты:

1. Компонент подключения к PBOX, предназначенный для:

– идентификации, авторизации и подключения к Системе устройств различных производителей;

– реализации различных протоколов взаимодействия с устройствами для приёма файлов и отправки результатов проверок;

– реализации защищённых каналов взаимодействия с устройствами.

2. Ядро PBOX, предназначенное для:

– определения информации по поступающим файлам, включая их тип, размер, контрольную сумму, определение архивов и количество файлов в них;

– осуществления проверки контрольной суммы файлов в различных базах;

– осуществления статического анализа файлов;

– осуществления динамического (поведенческого) анализа файлов;

– реализации логики признания файла как чистого, вредоносного или потенциально опасного;

– формирования вердикта, отчёта и передачи этой информации в Компонент хранения PBOX;

– обеспечения возможности взаимодействия с различными антивирусными системами и системами анализа файлов.

3. Компонент хранения PBOX, предназначенный для централизованного хранения настроек Системы, служебной информации о подключающихся клиентских устройствах, статусах и результатах проверок файлов, выданных вердиктах и отчётах, образцах вредоносных и потенциально опасных файлов.

4. Компонент управления PBOX, предназначенный для управления и мониторинга АИС с помощью веб-консоли.

5. Компонент API, предназначенный для подключения к АИС с целью автоматизации отправки файлов на проверку и получения результатов их проверок.

Функции частей Системы приведены в разделах далее (см. разделы 3.1 - 3.53.4).

3.1 Функции компонента подключения к PBOX

1. Обеспечение функциональности идентификации, авторизации и подключения межсетевых экранов Palo Alto Networks и Fortinet к АИС.

2. Обеспечение потокового приёма файлов и метаинформации по ним от устройств и передачу полученных данных на Ядро PBOX.

3. Транслирование устройствам от Ядра PBOX вердиктов по выполненным проверкам файлов.

4. Контроль состояния подключенных к АИС устройств.

5. Обеспечение одновременной работы с множеством устройств.

3.2 Функции Ядра PBOX

1. Обеспечение временного хранения поступающих файлов в S3-хранилище.

2. Определение типа, размера, контрольной суммы поступающих файлов.

3. Определение, является ли файл архивом, и в случае, если это архив, подсчёт количества файлов в нём, их контрольных сумм, распаковка архивов для передачи файлов на дальнейшую обработку.

4. Проверка в Компоненте хранения PBOX файлов по контрольной сумме поступившего файла, проверялся ли он уже ранее, и при наличии такой проверки, выдача соответствующего вердикта.

5. Проверка контрольных сумм файлов на их наличие во внешних базах вредоносных ресурсов, в таких источниках, как Palo Alto Threat Vault, Kaspersky Threat Lookup. При наличии в этих источниках информации о том, что файл является вредоносным, выдача соответствующего вердикта о проверке и занесение его в Компонент хранения PBOX.

6. Обеспечение статического и динамического анализа файлов в системах производства Palo Alto Networks, Fortinet, Kaspersky.

7. Выполнение логики признания файла вредоносным, потенциально опасным или чистым, основываясь на вердиктах со всех этапов его проверки.

8. Передача результатов проверки в Компонент хранения PBOX и Компонент подключения к PBOX.

9. Обеспечение максимального общего времени проверки одного файла – не более 30 минут.

10. Удаление файлов, признанных чистыми, из хранилища S3, и постоянное хранение вредоносных и потенциально опасных файлов в нём.

3.3 Функции компонента хранения PBOX

1. Временное хранение принимаемых на проверку файлов.

2. Постоянное хранение вредоносных и потенциально опасных файлов.

3. Хранение настроек АИС.

4. Хранение результатов проверок файлов.

5. Хранение информации по файлам.

6. Ретроспективный поиск по результатам всех проверок и проверенным файлам.

3.4 Функции Компонента управления PBOX

1. Управление и мониторинг PBOX с помощью веб-консоли управления.

2. Визуализация результатов проверок файлов и информации по файлам в виде таблиц и виджетов.

3. Отображение следующей информации о проверках файлов:

– дата и время начала проверки;

– дата и время конца проверки;

– отправитель (идентификатор устройства или имя пользователя или API);

– статус проверки;

– контрольная сумма проверяемого файла (алгоритм расчета SHA-256);

– вердикт, который был выдан по результатам проверки (malware/grayware/benign);

– имя файла (в случае, если оно было передано вместе с файлом);

– тип файла.

4. Отображение следующей информации о файлах:

– контрольная сумма файла (алгоритм расчета SHA-256);

– вердикт по данному файлу (malware/grayware/benign);

– дата и время, когда впервые данный файл был зарегистрирован в АИС;

– дата и время, когда последний раз данный файл был зарегистрирован в АИС;

– количество раз, которое файл присылался на проверку в АИС;

– размер файла в байтах;

– тип файла;

– имя файла (при его наличии);

– URL-адрес в сети, по которому данный файл был получен (в случае его наличия);

– IP-адрес и порт в сети, по которому данный файл был получен (в случае их наличия);

– таблица проверок в различных антивирусных системах с перечнем их временных меток, вердиктов, отчётов и метаинформации при наличии.

5. Поиск и фильтрация по всем проверкам файлов.

6. Отображение исторических графиков по количеству проверок, подозрительных вердиктов и типов проверенных файлов, за последние 30 дней.

7. Компонент управления PBOX содержит:

- меню для упрощения навигации по веб-консоли;
- рабочую область для отображения содержания вкладок меню
- форму поиска в базе АИС информации о файле по его контрольной сумме (алгоритм SHA-256);
- форму загрузки файла для его проверки в АИС.

3.5 Функции компонента API PBOX

1. Проверка информации о файле по его контрольной сумме (алгоритм SHA-256).
2. Загрузка файла для осуществления его проверки в АИС.
3. Получение результатов проверки загруженных файлов.