ФОРТ
БЕЗОПАСНОСТИ

ЗАЩИТА КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ

от ещё неизвестных атак

С каждым днём растёт количество и сложность кибератак. А всего одной уязвимости достаточно для взлома системы безопасности и утечки данных. Направления атак становятся все более динамичными из-за роста количества IoT-устройств и облачных служб, а квалифицированныхкадров в сфере кибербезопасности постоянно не хватает. Организациям приходится использовать «песочницу» с более эффективными функциями управления и высокой степенью автоматизации.

Комплекс ФОРТ БЕЗОПАСНОСТИ - ваш помощник класса «песочница», помогает бороться с ранее неизвестными угрозами предназначен для получения оперативной информации в режиме реального времени об атаках на периметр, почту и другие корпоративные ресурсы.

ПРЕИМУЩЕСТВА

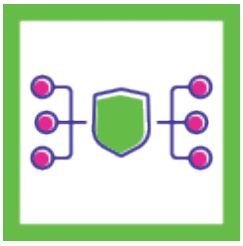
Полностью готовая к использованию система

Простая интеграция и развёртывание

Статистический и динамический анализ

Встроенный искусственный интеллект

Автоматизация обнаружения и реагирования



Интеграция с SIEM системами и другими средствами

СТАТИЧЕСКИЙ И ДИНАМИЧЕСКИЙ АНАЛИЗ

Модельный ряд делится на модели со статическим (серия С) или с статическим и динамическим анализом (серия СД).

СТАТИЧЕСКИЙ АНАЛИЗ

Работает с синтаксической структурой файла, которая может быть замаскирована под легитимное программное обеспечение:

- проверка более чем 20 локальных антивирусных движках;
- подробный анализ синтаксической структуры и содержания файлов;
- проверка во внешних аналитических ресурсах и репутационных базах;
- анализ в моделях машинного обучения.

ДИНАМИЧЕСКИЙ АНАЛИЗ

Дополняет статическое направление:

- запуск файла в эмулируемых средах с имитацией работы пользователя для максимальной провокации вредоносного программного обеспечения;
- анализ поведения процессов на предмет вредоносной активности;
- фиксация потребляемых ресурсов;
- проверка сетевого трафикар.

Изучение поведенческой активности файла без анализа его синтаксической структуры также не всегда эффективно. Программное обеспечение может отказаться от своей вредоносной деятельности в имитационной среде по ряду причин: неподходящая версия ОС, отсутствие необходимого программного обеспечения для запуска файла, неподходящий язык консоли, отсутствие подключения к Интернет и т. д.

Синергия двух методов анализа позволяет повысить вероятность обнаружения вирусов и усилить защиту инфраструктуры компании, как от известных угроз, так и от угроз нулевого дня.

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

ПОЧТОВЫЙ ТРАФИК

КЗИ ФОРТ БЕЗОПАСНОСТИ может проверять следующие типы файлов в почтовом трафике:

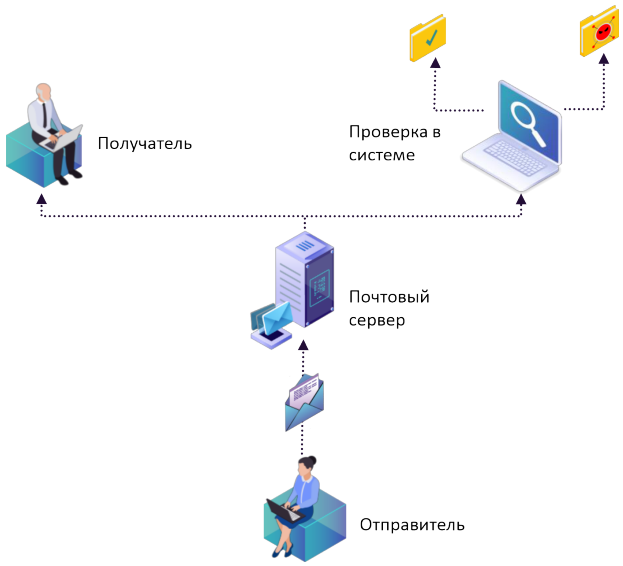
- MSG and EML
- PDF
- MS Office
- Архивы
- Многотомные архивы
- Защищенные паролем архивы и файлы и т.д.

Почтовые форматы MSG и EML проверяются как письма при отправке на проверку по широкому выбору почтовых протоколов:

- IMAP/ IMAPS
- POP3/ POP3S
- SMTP
- REST API

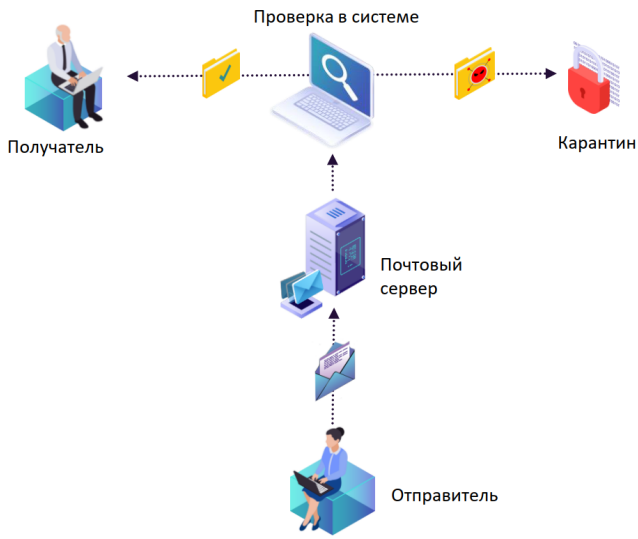
СХЕМЫ ПОДКЛЮЧЕНИЯ

ЗЕРКАЛИРОВАНИЕ



Пользователь получает вложение и одновременно файл проходит проверку в системе на наличие вредоносных элементов.

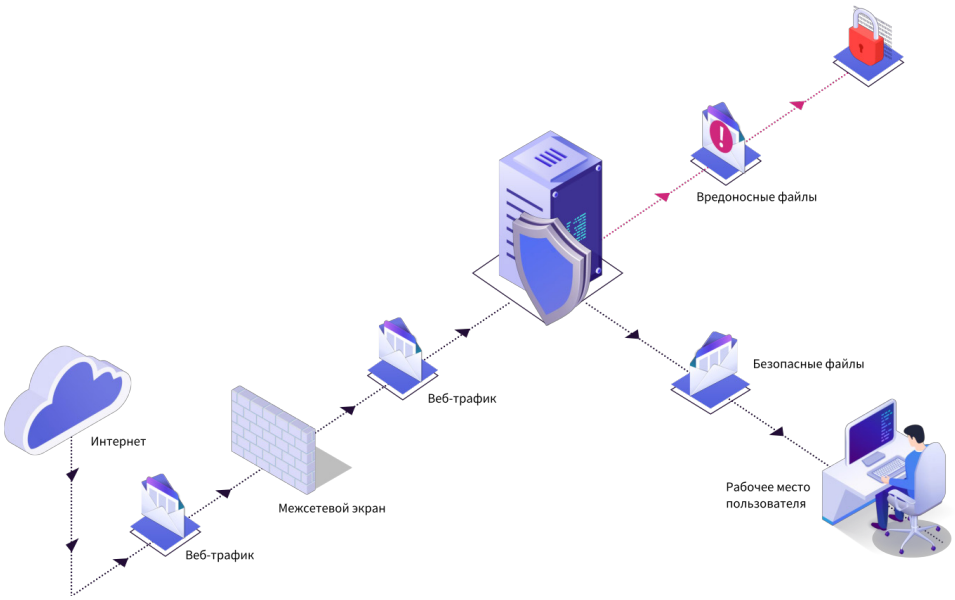
В РАЗРЫВ



Файл проверяется на наличие вредоносных элементов, и только после того, как система присвоит безопасный вердикт, пользователь может получить свой исходный файл

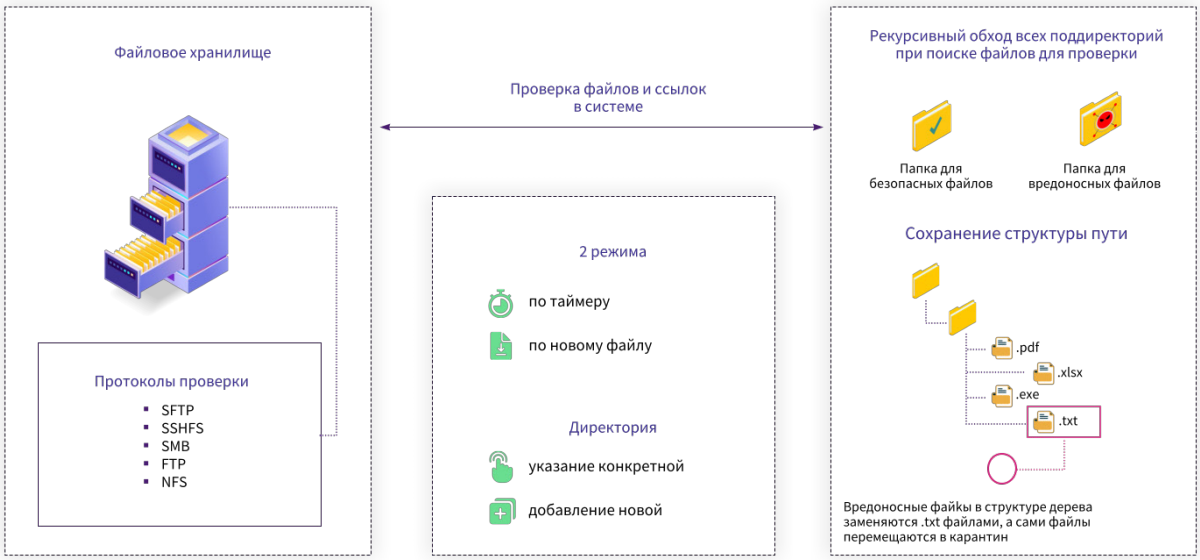
ВЕБ-ТРАФИК

Осуществляется проверка веб-трафика и блокировка загрузки вредоносных файлов из Интернета. Отображается вся информация по проверкам сетевого трафика в системе. Указываются сведения об источнике (IP-адрес) и дате создания. По каждому пункту можно увидеть ссылку на веб-адрес, контрольную сумму (хеш SHA-256) и вердикт. По проверке конкретной ссылки доступен подробный отчёт.



ФАЙЛОВОЕ ХРАНИЛИЩЕ

проверка файловых хранилищ в нескольких режимах по расписанию или появление в них новых файлов. Структура файлов после проверки сохраняется, а файлы сортируются по папкам в зависимости от вердикта: безопасные, подозрительные, вредоносные. Также возможно проверять данные на дисках и файлообменниках Google Drive, Yandex Disk, Dropbox.



ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Источники для проверки

- веб-трафик;
- почтовый трафик;
- сетевой трафик;
- мессенджеры;
- мобильные устройства;
- серверы и рабочие станции;
- ручная загрузка;
- API

Типы песочниц

- MS Windows 10 – 7;
- Windows Server (2008 R2 - 2019);
- Linux;
- Astra Linux;
- Debian 9.8 (Stretch);
- openSUSE Leap 15;
- CentOS 7.6.1810;
- Ubuntu 18.1

Типы объектов

- файлы;
- архивы;
- веб-ссылки;
- мобильные приложения

Поддерживаемые протоколы почтового трафика

- IMAP/ IMAPS
- POP3/ POP3S
- SMTP
- REST API

Виды проверяемых файлов

- исполняемые файлы (EXE, ELF, CMD)
- офисные документы (DOCX, XLSX, PPTX, PDF, RTF)
- мобильные приложения (APK)
- архивы, в том числе многотомные и защи-
- щенные паролем (ZIP, JAR)
- скрипты (BAT, SH) и др.

Проверка файлов в почтовом трафике

- MSG and EML;
- PDF;
- MS Office;
- Архивы;
- Многотомные архивы;
- Защищенные паролем архивы и файлы и т.д.

Статический анализ

- проверка более чем 20 локальных антиви-русных движках;
- подробный анализ синтаксической струк-туры и содержания файлов;
- проверка во внешних аналитических ре-сурсах и репутационных базах;
- анализ в моделях машинного обучения

Проверка файлов в облаке

- Google Drive
- Yandex Disk
- Dropbox

Динамический анализ

- запуск файла в эмулируемых средах с ими тацией работы пользователя для максимальной провокации вредоносного программного обеспечения;
- анализ поведения процессов на предмет вредоносной активности;
- фиксация потребляемых ресурсов;
- проверка сетевого трафика

Типы моделей машинного обучения

- RandomForestClassifier;
- EXtreme Gradient Boosting (XGBoost);
- Light Gradient Boosted Machine (LightGBM);
- Neural networks: multilayer perceptron, deep neural networks (VGG, NasNet, efficientnet);
- Catboost

МОДЕЛЬНЫЙ РЯД

Широкий выбор моделей комплексов ФОРТ БЕЗОПАСНОСТИ может быть использован как для небольших предприятий, так и для крупных корпораций. Для конфигураций свыше 5 000 пользователей заказываете (это слово должно быть гиперссылкой на форму обращение) конфигурацию комплекса именно под вашу организацию.

МОДЕЛИ СО СТАТИЧЕСКИМ АНАЛИЗОМ

Модель	ФБ-П-100С	ФБ-П-250С	ФБ-П-500С	ФБ-П-1000С	ФБ-П-2500С	ФБ-П-5000С
Модули программного обеспечения*						
Модуль проверки электронной почты	✓	✓	✓	✓	✓	✓
Модуль проверки веб-трафика	✓	✓	✓	✓	✓	✓
Модуль приема файлов на проверку по протоколу ICAP	✗	✓	✓	✓	✓	✓
Модуль проверки файловых хранилищ	✗	✗	✓	✓	✓	✓
Аппаратное обеспечение						
Сетевые интерфейсы	4x1GE				4x1GE, 2x10GE	
Источники питания	2 БП горячей замены					
Кол-во процессоров	1	1	1	1	2	2
Общее кол-во ядер	8	12	16	24	32	52
Кол-во RAM, ГБ	32	32	64	64	64	96
Общая ёмкость SAS SSD, ГБ	480	480	960	960	1920	1920
Общая ёмкость SAS HDD, ТБ	1	1	2	4	6	8
Кол-во антивирусов	9	9	9	9	15	15
Рекомендуемое кол-во пользователей в защищаемой сети	100	250	500	1000	2500	5000
Форм-фактор	1U				2U	
Потребляемая мощность, не более, Вт	600		750		1000	
Источники питания	2 БП горячей замены					
Высота x Ширина x Глубина, мм	43 x 437 x 399		43 x 437 x 754		89 x 437 x 647	
Рабочая температура, С	+5 - +35					
Температура хранения, С	-20 - +50					
Влажность	до 80%					
Соответствие требованиям	ПРГД.466452.001-ТУ					
Сертификация	EAC					

*Дополнительные модули, отсутствующие в базовой конфигурации могут быть приобретены под заказ.

МОДЕЛИ С ДИНАМИЧЕСКИМ И СТАТИЧЕСКИМ АНАЛИЗОМ

Модель	ФБ-П-100СД	ФБ-П-250СД	ФБ-П-500СД	ФБ-П-1000СД	ФБ-П-2500СД	ФБ-П-5000СД
Модули программного обеспечения*						
Модуль «песочницы» с ОС Windows	✓	✓	✓	✓	✓	✓
Модуль «песочницы» с ОС на базе ядра Linux	✗	✗	✗	✗	✓	✓
Модуль «песочницы» с ОС Android	✗	✗	✗	✗	✓	✓
Модуль управления физическими «песочницами»	✗	✗	✗	✗	✗	✓
Модуль проверки электронной почты	✓	✓	✓	✓	✓	✓
Модуль проверки веб-трафика	✓	✓	✓	✓	✓	✓
Модуль приема файлов на проверку по протоколу ICAP	✗	✓	✓	✓	✓	✓
Модуль проверки файловых хранилищ	✗	✗	✓	✓	✓	✓
Аппаратное обеспечение						
Сетевые интерфейсы	4x1GE				4x1GE, 2x10GE	
Кол-во процессоров, CPU	1	1	2	2	2	2
Общее кол-во ядер	16	24	32	40	52	64
Кол-во RAM, ГБ	32	64	64	96	128	192
Ёмкость SAS SSD дисков, ГБ	960	960	1920	1920	3840	3840
Ёмкость SAS HDD дисков, ТБ	1	2	4	8	12	20
Кол-во виртуальных машин	2	3	5	8	11	14
Кол-во антивирусов	9	9	9	9	15	15
Рекомендуемое кол-во пользователей в защищаемой сети	100	250	500	1000	2500	5000
Форм-фактор	1U				2U	
Потребляемая мощность, не более, Вт	600		750		1000	
Источники питания	2 БП горячей замены					
Высота x Ширина x Длина	43 x 437 x 399		43 x 437 x 754		89 x 437 x 647	
Рабочая температура	+5 - +35					
Температура хранения	-20 - +50					
Влажность	до 80%					
Соответствие требованиям	ПРГД.466452.001-ТУ					
Сертификация	EAC					

* Дополнительные модули, отсутствующие в базовой конфигурации могут быть приобретены под заказ.

ФБ-П-100С , ФБ-П-250С ,
ФБ-П-100СД , ФБ-П-250СД

ФБ-П-500С, ФБ-П-500СД,
ФБ-П-1000С, ФБ-П-1000СД

ФБ-П-2500С, ФБ-П-2500СД,
ФБ-П-5000С, ФБ-П-5000СД

+7 495 725 55 44

fort@trinitis.ru

г. Москва, 5-й Донской проезд, 21Б, стр.10

www.fortrinitis.ru

Продукция компании «Тринитис»

TRINITIS
Intellectual services

www.monolith.trinitis.ru

Создано совместно с компанией «АВ Софт»

AVSOFT

www.avsw.ru