T&T SECURITY

# tLab

## Высокоточное оружие против современных киберугроз

8 (7172) 57-21-90 info@tntsecure.kz 010000, Nur-Sultan, Alpamys 17

## Система tLab

передовой продукт по защите от киберугроз нового типа, против которых типичный антивирус малоэффективен: от атак нулевого дня, целевого вредоносного программного обеспечения (ВПО) и APT-атак.

### Применимость

tLab – “Песочница” (sandbox), система глубокого анализа объектов обеспечивающая защиту Email и Web - трафика от вредоносных загрузок и вложений, опасных URL, скрытых и сложных атак ВПО (скрипты, приложения и документов).

## tLab в цифрах:

**100** Обнаруживает более 100 видов вредоносной активности

**10** На базе более 10 научных работ из США

**10K** Проверяет до 10000 вирусов в день (на одном сервере)

**60** Позволяет получить вердикт на объект за 60 секунд

## Интелектуальность

Глубокий анализ вредоносного поведения и эвристический анализ, которые обеспечивают распознавание сложных и скрытых атак ВПО.

## Производительность

Быстрая оценка угрозы ВПО на основе комплексного, интерактивного отчета, позволяющего видеть угрозу изнутри.

## Автономность

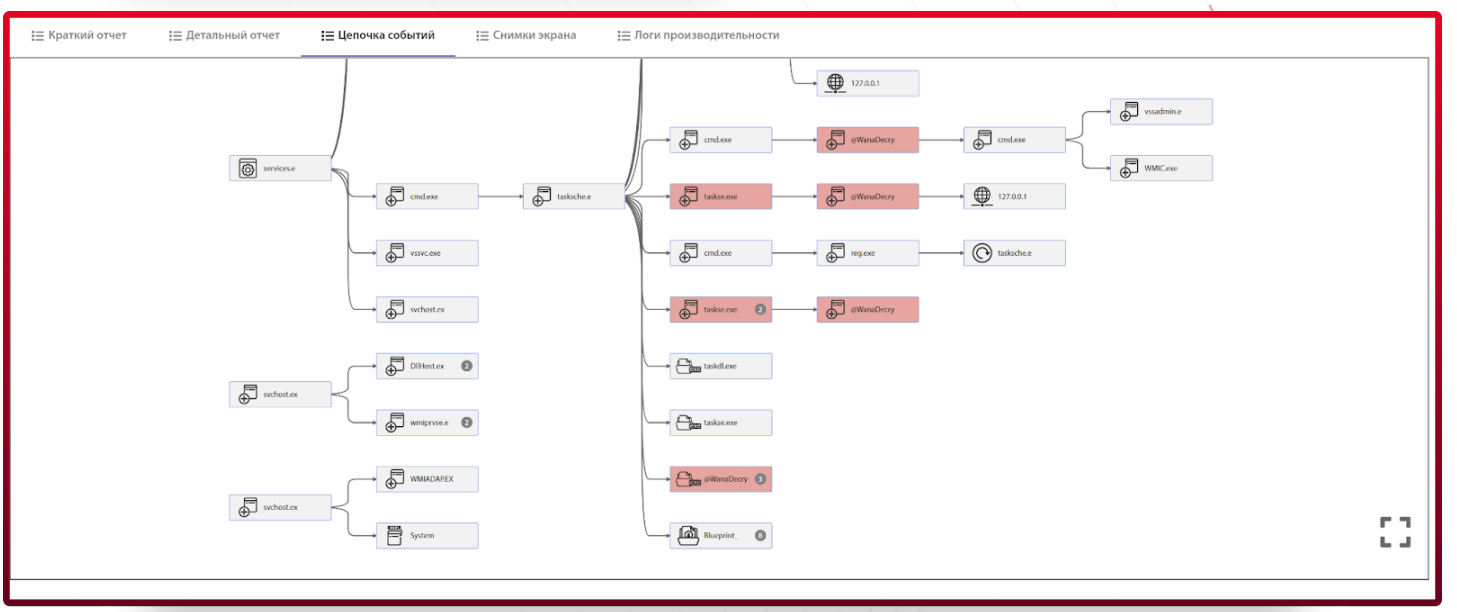
Автоматизация защиты от ВПО путем интеграции с компонентами Mail / Web Gateway и сторонними решениями на основе RESTAPI и стандартных протоколов.

# Передовое обнаружение атак

tLab идентифицирует ВПО путем глубокого анализа системного поведения программ в изолированной среде. Используется уникальная технология анализа поведения на уровне деревьев активности, которые описывают поток распространения вредоносной активности и взаимосвязи исполняемых объектов.

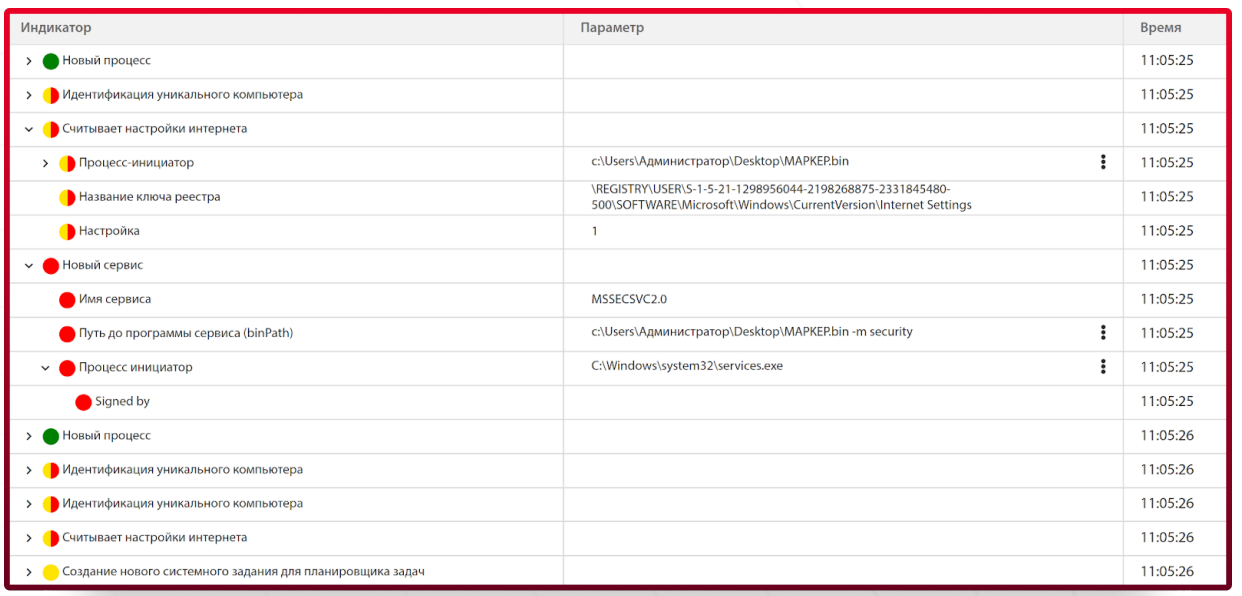
Данная технология позволяет обнаружить скрытые и сложные вредоносные объекты, малозаметные для традиционных систем защиты.

tLab анализирует на вредоносность многие форматы файлов, включая, но не ограничиваясь: документы, скрипты, web-файлы, исполняемые, архивы и файлы клиентских приложений (eml).

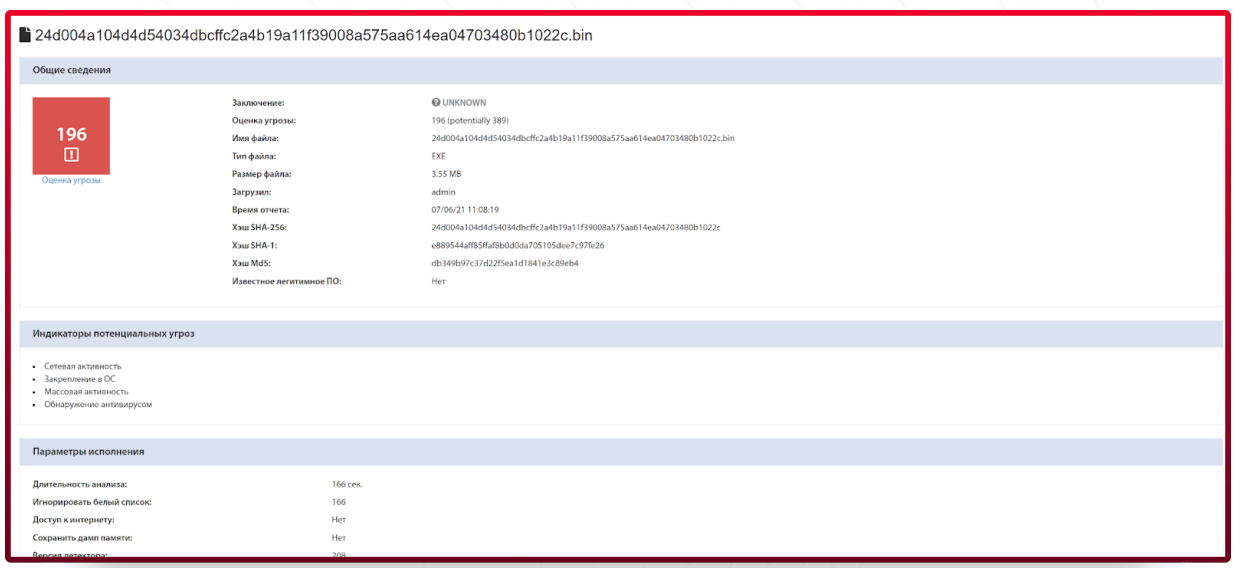



# Детальное исследование угроз

В отличие от классических песочниц, tLab не только обнаруживает и блокирует атаки в реальном времени, но и предоставляет мощный инструментарий для всестороннего исследования угрозы. tLab - идентифицирует уровень угрозы ВПО и предоставляет интерактивный отчет с визуализацией полной активности и указанием вредоносных функций. Отчет содержит полную аналитику по ВПО различного уровня детализации, включая статические характеристики, типы обнаруженных функциональностей, деревья активности (событий), контекст поведения объекта исследования, настройки среды исполнения.



| Индикатор | Параметр | Время |
|---|---|---|
| Новый процесс | | 11:05:25 |
| Идентификация уникального компьютера | | 11:05:25 |
| Считывает настройки интернета | | 11:05:25 |
| Процесс-инициатор | c:\Users\Администратор\Desktop\MAPKEP.bin | 11:05:25 |
| Название ключа реестра | \REGISTRY\USER\S-1-5-21-1298956044-2198268875-2331845480-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings | 11:05:25 |
| Настройка | 1 | 11:05:25 |
| Новый сервис | | 11:05:25 |
| Имя сервиса | MSSECSVC2.0 | 11:05:25 |
| Путь до программы сервиса (binPath) | c:\Users\Администратор\Desktop\MAPKEP.bin -m security | 11:05:25 |
| Процесс инициатор | C:\Windows\system32\services.exe | 11:05:25 |
| Signed by | | 11:05:25 |
| Новый процесс | | 11:05:26 |
| Идентификация уникального компьютера | | 11:05:26 |
| Идентификация уникального компьютера | | 11:05:26 |
| Считывает настройки интернета | | 11:05:26 |
| Создание нового системного задания для планировщика задач | | 11:05:26 |



24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.bin

Общие сведения

196

Оценка угрозы

| | |
|---|---|
| Заключение: | UNKNOWN |
| Оценка угрозы: | 196 (potentially 389) |
| Имя файла: | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.bin |
| Тип файла: | EXE |
| Размер файла: | 3.55 MB |
| Загрузил: | admin |
| Время отчета: | 07/06/21 11:08:19 |
| Хэш SHA-256: | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c |
| Хэш SHA-1: | e889544aff85ffaf8b0d0da705105dee7c97fe26 |
| Хэш Md5: | db349b97c37d22f5ea1d1841e3c89eb4 |
| Известное легитимное ПО: | Нет |

Индикаторы потенциальных угроз

- Сетевая активность
- Закрепление в ОС
- Массовая активность
- Обнаружение антивирусом

Параметры исполнения

| | |
|---|---|
| Длительность анализа: | 166 сек. |
| Игнорировать белый список: | 166 |
| Доступ к интернету: | Нет |
| Сохранить дамп памяти: | Нет |
| Версия детектора: | 208 |

## Продвинутая эмуляция активности пользователя *(детонация ВПО)*

Некоторые виды нежелательного и вредоносного ПО требуют взаимодействие с пользователем, соответственно такие образцы не будут активироваться (детонировать), пока пользователь не нажмет на соответствующие элементы графического интерфейса (кнопки, текстовые поля). К таким угрозам относятся троянские программы, маскирующиеся под легитимное или нежелательное ПО, которое требует выполнения полного сценария инсталляции.

Также трояны-вымогатели могут требовать взаимодействия с пользователем для выполнения некоторых операций, например, обращение к серверу злоумышленника для загрузки информации по платежам выкупа. Детонирование подобных объектов ВПО требует продвинутую и эффективную систему эмуляции пользователя как на уровне заскриптованных, так и на уровне авто-сгенерированных сценариев пользовательской активности.

Некоторые образцы ВПО, с целью обхода песочниц, демонстрируют пользователю статичное графическое изображение и не используют системные элементы управления, отслеживая нажатие пользователя на картинку кнопки. Песочницы не могут распознать элементы управления и соответственно не могут нажать и детонировать ВПО. tLab имеет в своем составе модуль распознавания образов для идентификации элементов статичных графических интерфейсов, что позволяет детонировать образцы и обнаружить угрозу.


## Режим анти-уклонения

tLab имеет возможность противодействия известным методам обнаружения и обхода песочниц, включая: обнаружение артефактов среды анализа, отложенное исполнение и продвинутый способ, использующий циклы микрозадержек. Данная технология противодействия обходу песочницы определяет эффективность при обнаружении скрытных целевых и нетипичных атак, которые, согласно мировой практики, составляют основу современной модели угроз ВПО.

# Технические возможности

## Экспорт и отчетность в системе tLab:

- несколько уровней детализации поведенческого отчета (формирование интерактивных отчетов разного уровня детализации и информативности);
- интерактивная визуализация дерева событий - последовательность потенциально вредоносных действий с указанием их взаимосвязи (отслеживание источника и распространения вредоносной / подозрительной активности);
- обнаружение работы с важными файлами (открытие, модификация и удаление). отслеживается: тип источника, кол-во и категорию файлов (например, документ, аудио, бухгалтерия и т. д.);
- экспорт полного отчета в PDF документ на английском и русском языках;
- экспорт и импорт белого списка исключений (использование белых листов для идентификации некоторых легитимных файлов);
- доступ к идентифицированному вредоносному объекту (файлу) путем выгрузки с веб-интерфейса.

## tLab обеспечивает загрузку объектов на анализ в следующих режимах:

- отправка файла в ручном режиме;
- загрузка с указанием командной строки запуска (входные аргументы);
- загрузка группы файлов с указанием запускаемого (для анализа файла с зависимостями);
- автоматическая отправка файлов через REST API (используется компонентами Web / Mail Gateway);
- загрузка и получение отчетов от продуктов Trend Micro (интеграция).

## Симуляция (эмуляция) действий пользователей в среде исполнения tLab для активации ВПО:

- эмуляция пользователя по скриптам активности (выбор существующих или создание новых сценариев для контролируемой детонации (активации) объектов);
- эмуляция пользователя без скриптов (оптимальная активность);
- обнаружение скрытых угроз, использующих нетипичное диалоговое окно в виде статичной картинки.

## tLab обеспечивает анти-уклонение - противодействие методам обнаруженияи обхода песочниц:

- stealth-режим: скрытие артефактов файловой системы (файлы и процессы) для предотвращения обнаружения среды исполнения со стороны ВПО;
- камуфляж (динамическая подмена имени) артефактов реестра (ключи, значения и ветки) и устройств для предотвращения обнаружения среды исполнения со стороны ВПО;
- обнаружение объектов, использующих задержки исполнения (отложенный запуск), включая циклы микро-задержек. Данный функционал обеспечивает противодействия механизму обхода динамического анализа через отложенное исполненные путем сокращения времени ожидания.

## Проверка и анализ объектов в системе tLab:

- анализ файлов разных форматов–документы (rtf, pdf, xlsx, docx, pptx, xls, doc, ppt, xlsm, docm, pptm, pps, ppsx, ppsm, dot, dotm, odt, xps), веб-файлы (html, mht, mhtml), исполняемые файлы (exe, scr, dll, jar,msp, mst, msi, java, job, sct), скрипты (ps1, sh (linux batchscript), js, vbs, bat, ws), архивы и файлы клиентских приложений (iso, bzip2, rar, zip, gzip, arj, 7z, cab, msg, eml);
- поведенческий анализ файлов проводится в операционных системахWindows включая: WindowsXP, Windows 7, Windows 8, Windows 8.1, Windows 10;
- анализ по Yara-сигнатурам;
- глубокий анализ активности поведения исследуемых объектов (программ) с отслеживанием потока распространения вредоносной активности и поведенческой взаимосвязи исполняемых объектов;
- эвристический анализ скриптов -эмуляция хода исполнения и идентификация поведения скриптов (обнаружение супер-целевых угроз заточенных на наличие индикаторов конкретной группы машин, например, имя пользователей, путем эмуляции всех ветвлений кода);
- контекстный анализ документов для обнаружения вредоносного документа на уровне аномалии без сигнатур (позволяет обнаружить угрозу ВПО с эксплоитом нулевого дня);
- Статический и эвристический анализ документов различных типов (rtf, pdf, xlsx, docx, pptx, xls, doc, ppt, xlsm, docm, pptm).

# Внедрение и интеграция



tLab обеспечивает предотвращение атак ВПО, распространяющихся по электронной почте и Веб путем интеграции с компонентами Mail и Web Gateway и сторонними решениями на основе REST API. Кроме того, система tLab поддерживает стандартные протоколы: ICAP для Web Gateway, SMTP в режиме BCC и IMAP с целью мониторинга угроз. В качестве Mail Gateway используется два решения на выбор: MTA-сервер либо плагин для почтового сервера MS Exchange. В качестве Web Gateway используется надежное open-source решение, включающее Next Generation Firewall (NGFW) и IPS с широким набором функционала.

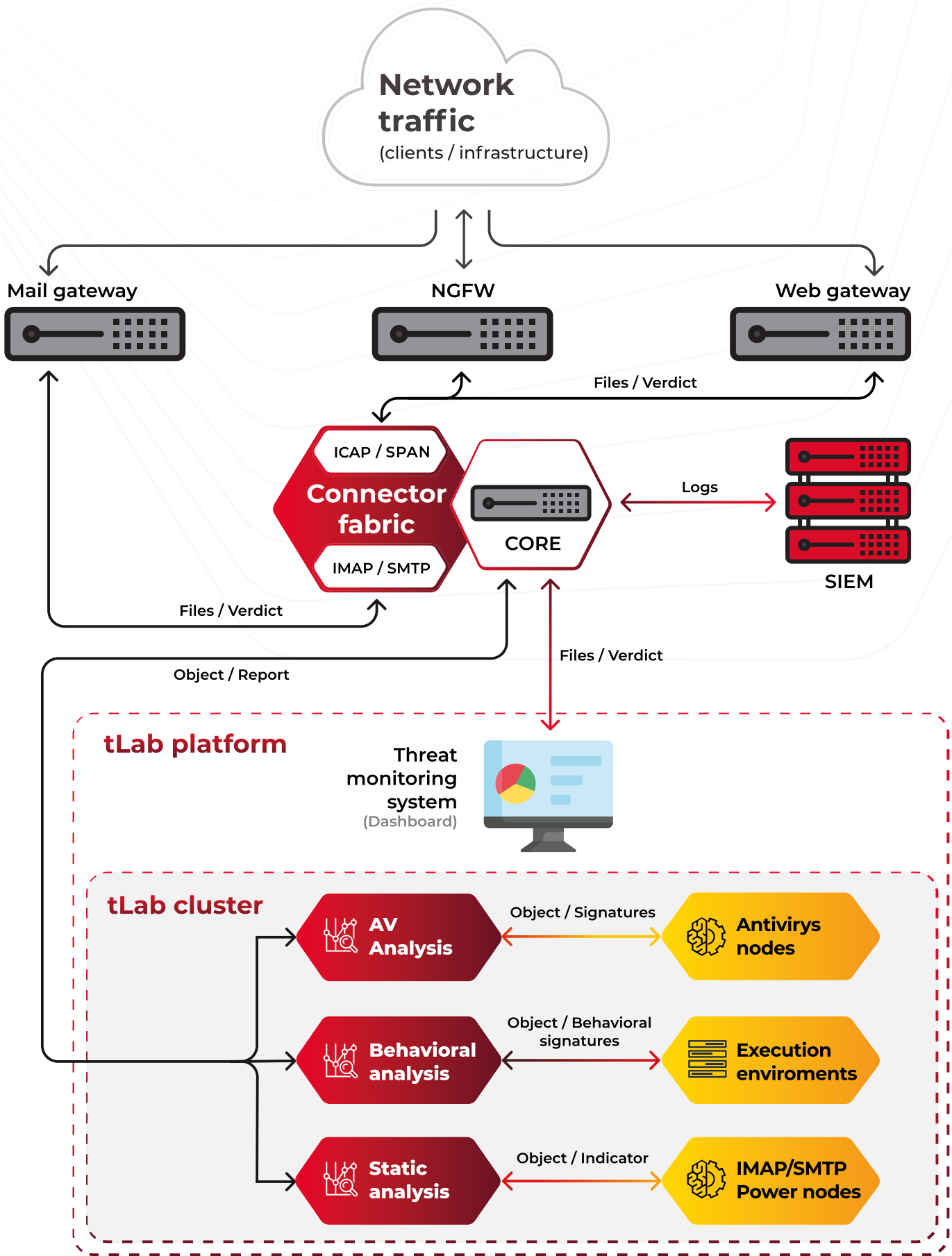
TREND MICRO™

***Нативная интеграция с решениями Trend Micro для обеспечения безопасности во всех средах и сегментах инфраструктуры организации от сети до рабочих станций и серверов.***

Данные решения проверяют каждый вложенный файл в песочнице и при выявлении угрозы вырезают опасные файлы из письма. Также поддерживается возможность проверки группы файлов в одной среде, для обнаружения компонентных, распределенных атак. Система tLab имеет технологию контекстного анализа документов (Context Document Analysis), которая позволяет обнаружить вредоносные документы MS Office на основе валидации формата и идентификации аномалий. Это позволяет детально проверять документы с угрозами нулевого дня без использования сигнатур. Обновления tLab включают: семантические сигнатуры YARA (эксплоиты), сигнатуры сторонних/клиентских антивирусов, белые листы, модели вредоносного поведения, образы виртуальных машин и новые механизмы обнаружения и идентификации угроз.

# Внедрение и интеграция






T&T SECURITY