КАК АНТИВИРУС ОБНАРУЖИВАЕТ УГРОЗЫ?

ОН ЗАМЕЧАЕТ ОПАСНОСТЬ...
ЕЩЁ ДО ТОГО, КАК ВЫ ЕЁ ЗАПУСТИТЕ.

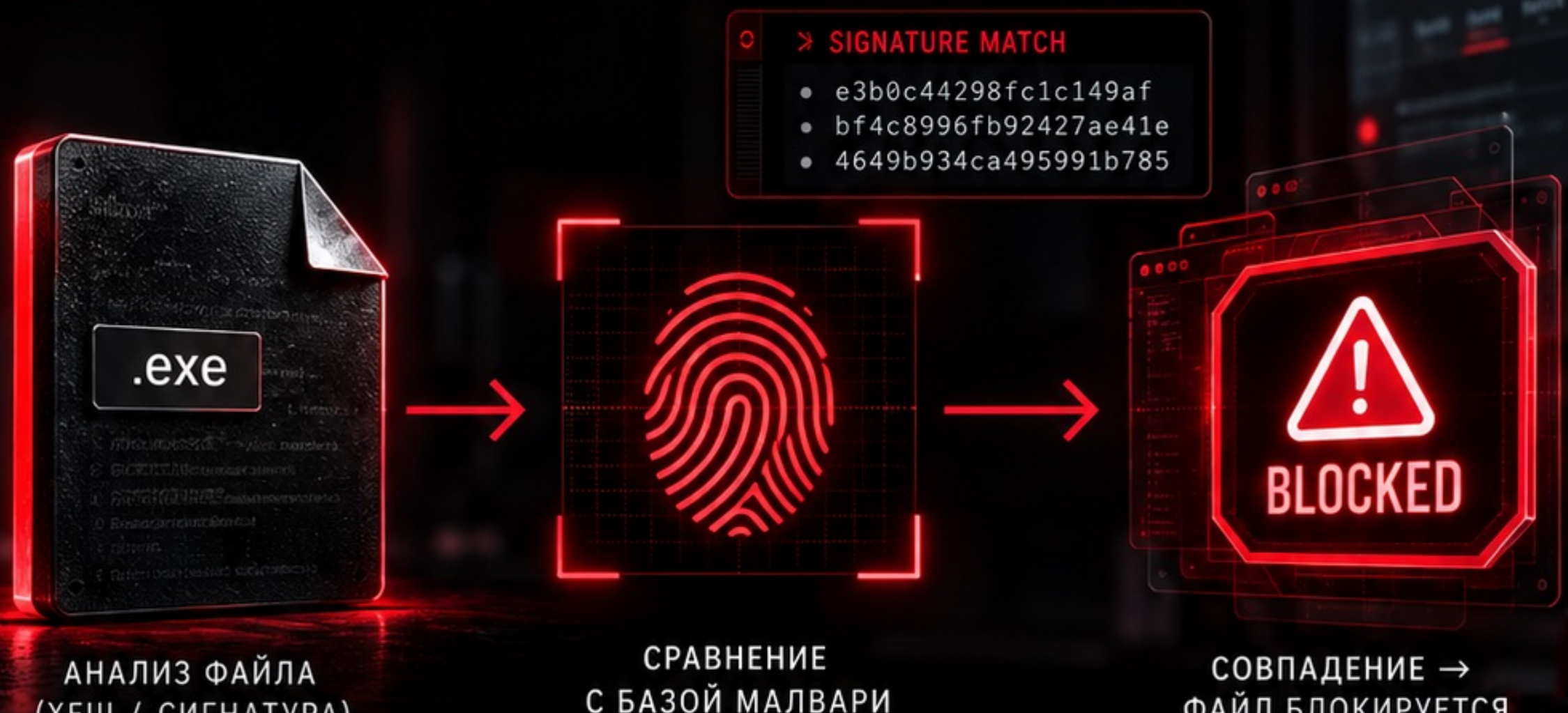
БОЛЬШЕ ПОЛЕЗНОГО В
@lionsoulbatyshchikov

ЛИСТАЙ →

1. ПЕРВАЯ ПРОВЕРКА

АНТИВИРУС ПРОВЕРЯЕТ ИДЕНТИЧНОСТЬ ФАЙЛА

Он сравнивает файлы с базой известных вредоносных сигнатур.



Известная малварь = **проще обнаружить.**

Больше полезного в
@lionsoulbatyshchikov

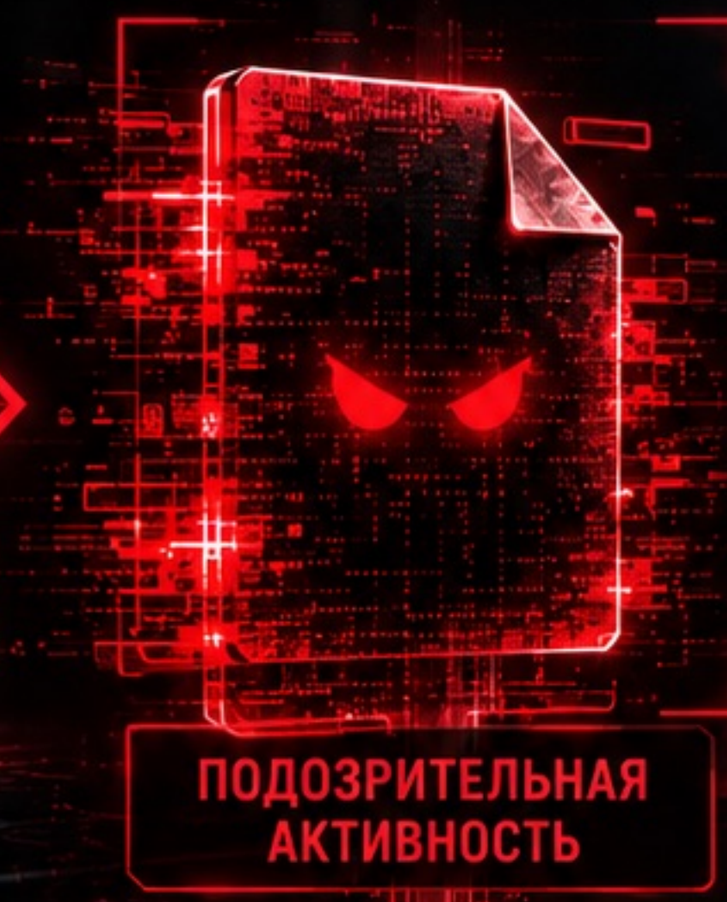
ЛИСТАЙ →

2. А ЧТО С НОВЫМ ВРЕДОНОСНЫМ ПО?

ЕСЛИ НЕТ СИГНАТУРЫ, ЭТО НЕ ЗНАЧИТ, ЧТО ОН БЕЗОПАСЕН.

Антивирус ищет не только известные угрозы, но и **подозрительное поведение**.





ПРОГРАММА ПЫТАЕТСЯ:

- ИЗМЕНЯТЬ СИСТЕМНЫЕ ФАЙЛЫ
- ПОЛУЧИТЬ ДОСТУП К ЧУВСТВИТЕЛЬНЫМ ДАННЫМ
- УСТАНАВЛИВАТЬ НЕОБЫЧНЫЕ СОЕДИНЕНИЯ

Такое поведение может быть признаком угрозы **и вызвать срабатывание защиты.**

Больше полезного в
@lionsoulbatyshchikov

ЛИСТАЙ →

3. ПОВЕДЕНЧЕСКИЙ АНАЛИЗ

АНТИВИРУС ОТСЛЕЖИВАЕТ ЧТО ДЕЛАЮТ ПРОГРАММЫ,

А НЕ ТОЛЬКО ТО, ЧЕМ ОНИ ЯВЛЯЮТСЯ.

ОН МОЖЕТ ЗАМЕЧАТЬ ПОДОЗРИТЕЛЬНЫЕ ДЕЙСТВИЯ, НАПРИМЕР:

РАБОТА С ФАЙЛАМИ
создание, изменение, удаление файлов

АКТИВНОСТЬ ПРОЦЕССОВ
запуск, внедрение кода (injection), создание новых процессов

СЕТЕВАЯ АКТИВНОСТЬ
необычные соединения, передача данных (data exfiltration)

ИЗМЕНЕНИЯ В СИСТЕМЕ
модификация реестра, отключение средств защиты (security tools)



НОРМАЛЬНОЕ ПОВЕДЕНИЕ
соответствует ожидаемой активности

ПОДОЗРИТЕЛЬНЫЙ ПАТТЕРН
может указывать на угрозу

Поведенческий анализ помогает антивирусу находить угрозы, которые скрываются на виду.

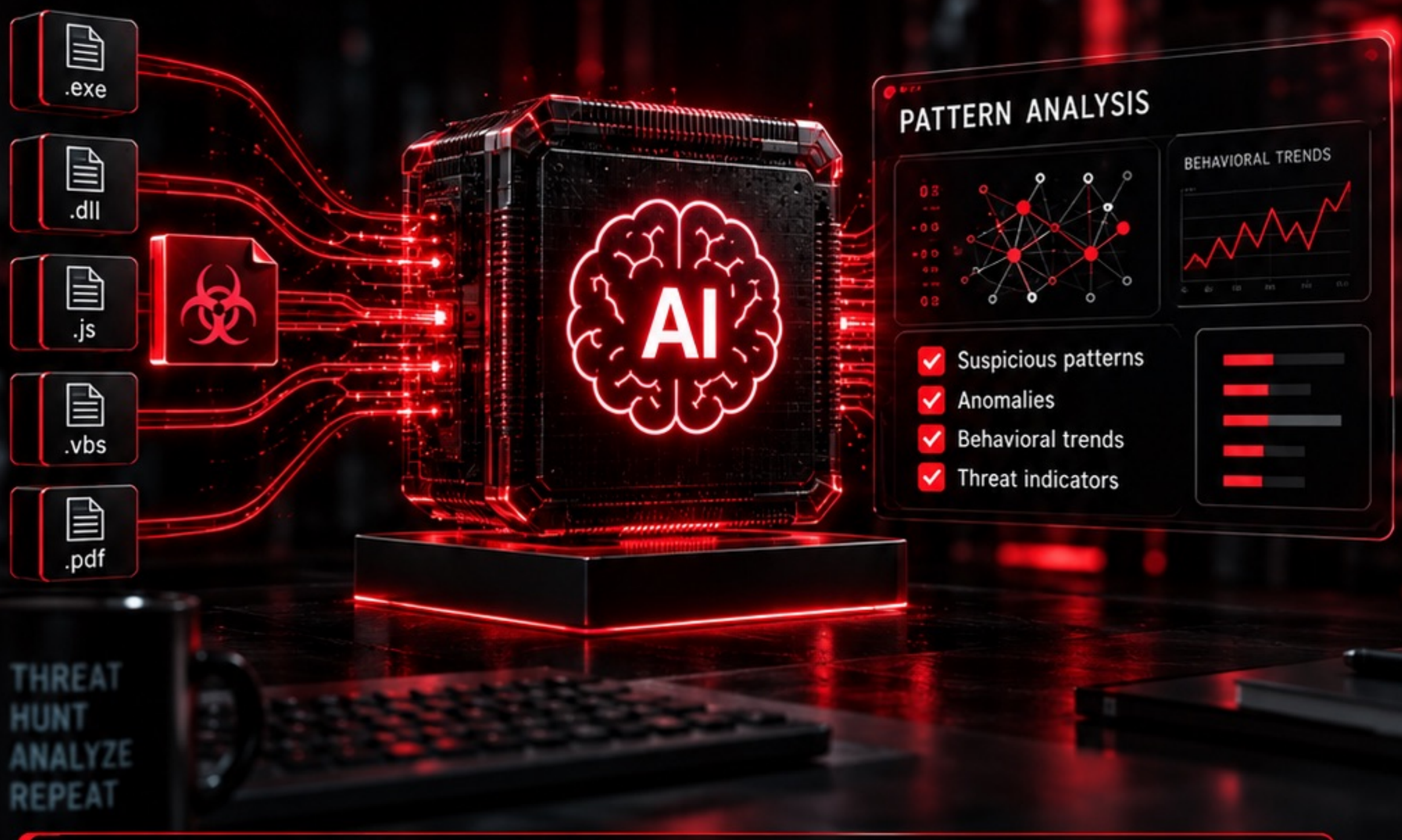
Больше полезного в
@lionsoulbatyshchikov

ЛИСТАЙ →

4. ИИ / МАШИННОЕ ОБУЧЕНИЕ

И ИНОГДА... САМ СОФТ УЧИТСЯ.

Современные средства защиты используют **machine learning** для выявления паттернов, связанных с вредоносной активностью.



ЦЕЛЬ:
Находить подозрительную активность, которая не совпадает с известными malware signatures.

5. ФИНАЛЬНОЕ РЕШЕНИЕ

КАК АНТИВИРУС ПРИНИМАЕТ РЕШЕНИЕ?

Антивирус объединяет **несколько источников** сигнатур и анализов, чтобы вынести вердикт.

SIGNATURE
Сравнивает с базой известных угроз (сигнатуры).

+

BEHAVIOR
Анализирует подозрительное поведение и активность в системе.

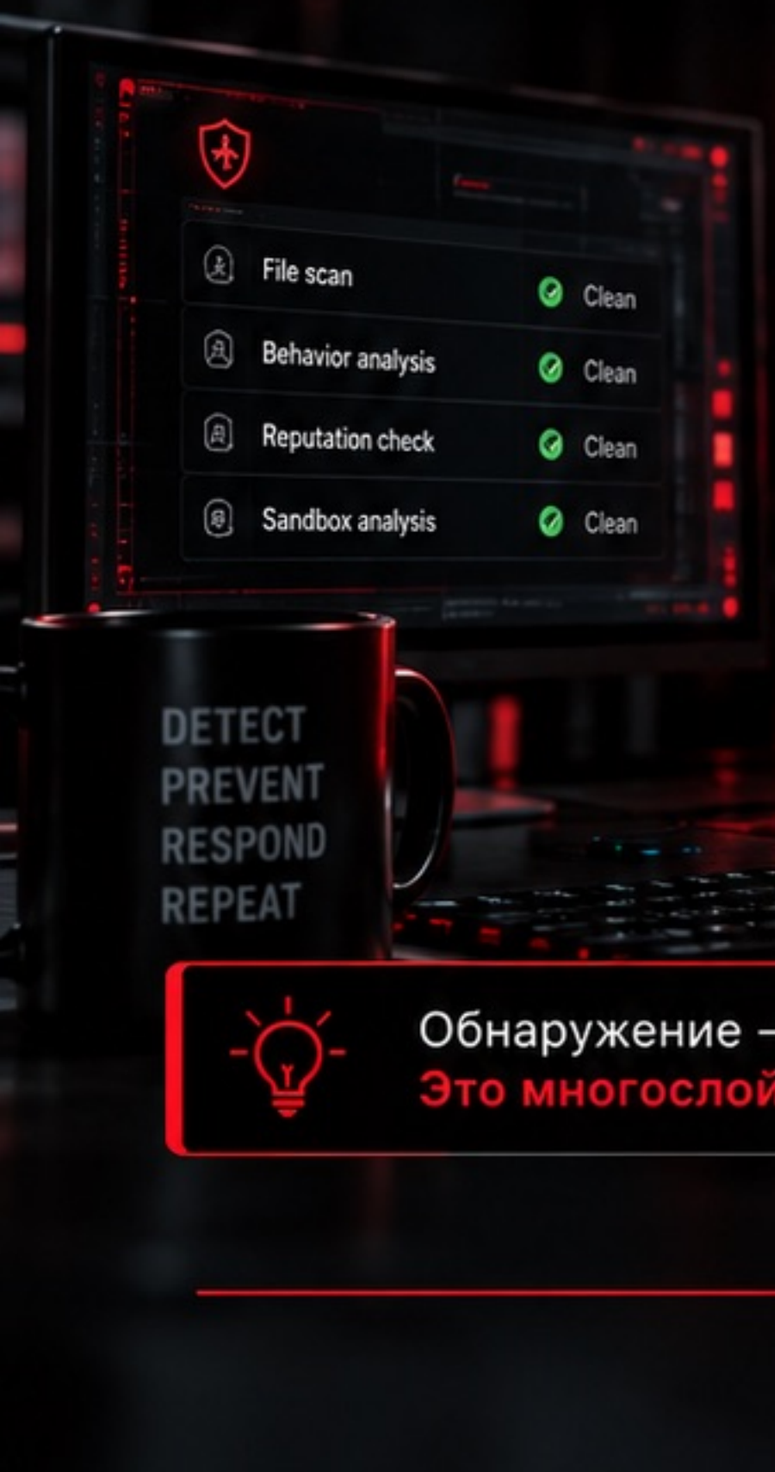
+

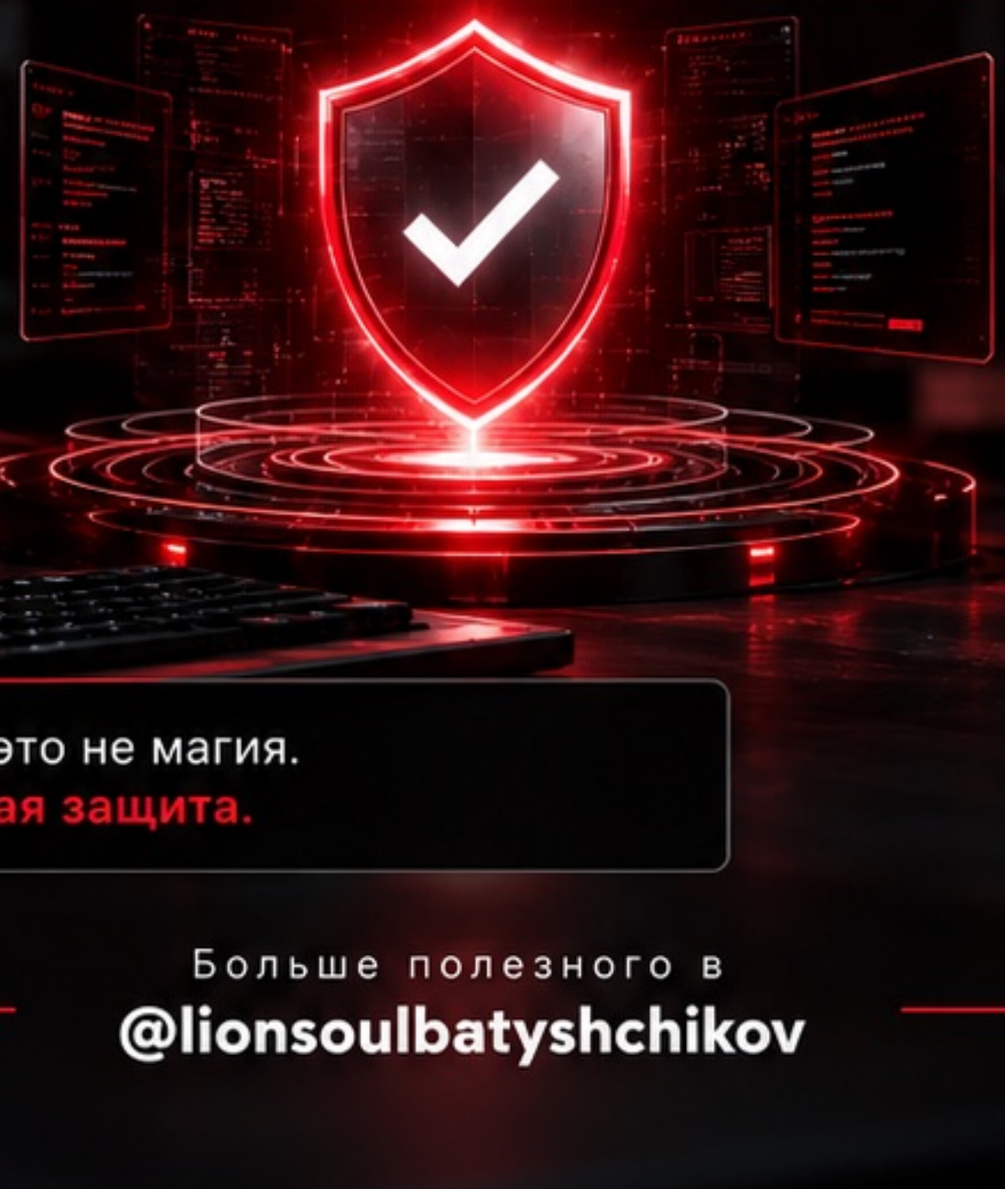
REPUTATION
Проверяет репутацию файла, ссылки или источника (например, через Threat Intelligence).

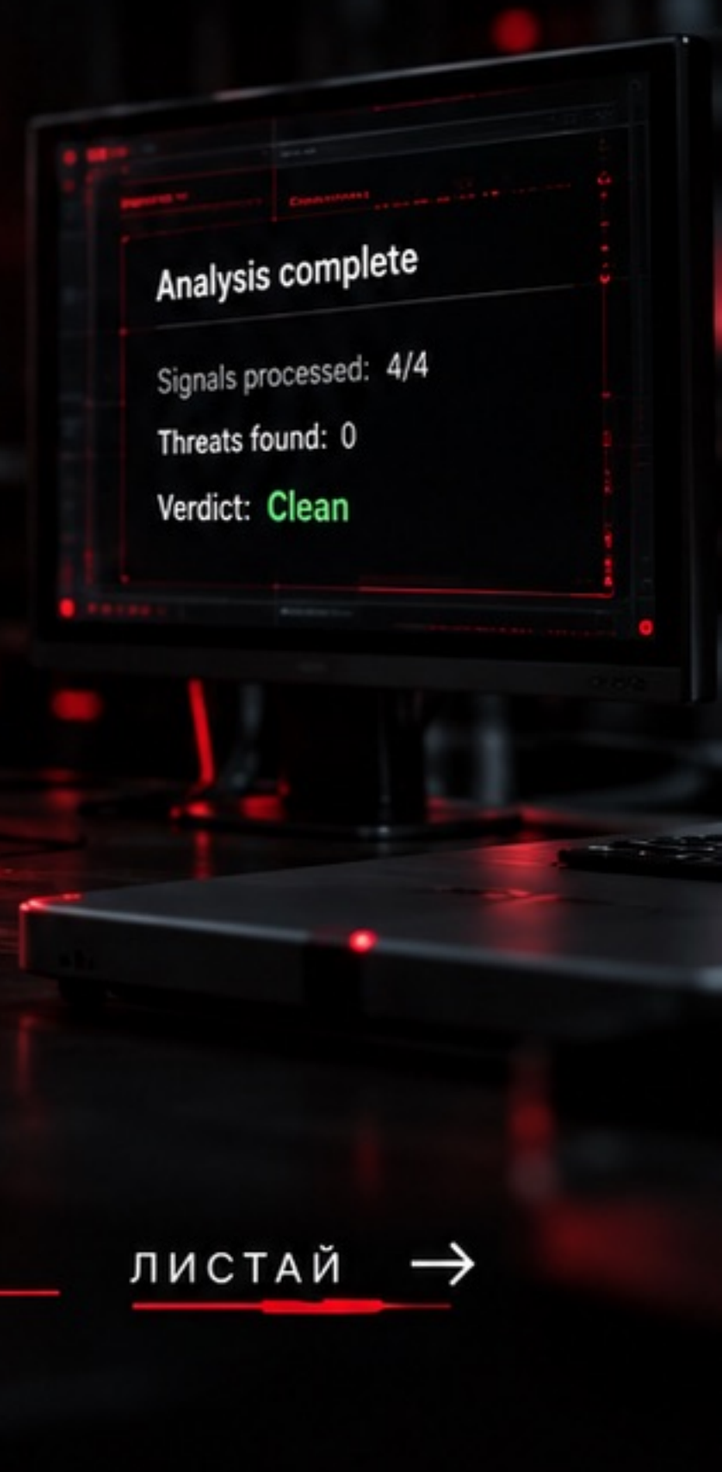
+

OTHER SIGNALS
Использует дополнительные проверки (sandbox, cloud, эвристики и др.).

THREAT VERDICT
Совокупный анализ всех сигналов даёт итоговое решение.







Обнаружение — это не магия.
Это многослойная защита.

Больше полезного в
@lionsoulbatyshchikov

ЛИСТАЙ →