

Введение

Система tLab представляет собой корпоративный локальный сервис для удаленного и безопасного анализа подозрительных объектов. Данная система направлена на защиту от киберугроз нового типа, против которых типичный антивирус малоэффективен: от целевых атак, вредоносных программ нулевого дня и атак на пользователя.

tLab производит автономный анализ поведения программ и идентификацию вредоносных функциональностей на сервере (корпоративное облако). Система позволяет автоматизировать процедуру анализа поведения любых программ и выявлять в них признаки вредоносных функций.

Подозрительные объекты запускаются в виртуальных контейнерах, где производится непрерывный анализ поведения всех запущенных программ.

Используется уникальная технология глубокого анализа функциональности программ для надежного обнаружения вредоносных объектов, в том числе и нулевого дня.

Данная технология имеет инновационный аспект, который заключается в механизме распознавания заданных вредоносных функциональностей. Здесь отслеживается история поведения и связываются события различных процессов в реальном времени.

[Отредактировать эту страницу](#)