Агент

Программный агент системы ATHENA – это кроссплатформенное ПО для рабочих станций и серверов на базе ОС Windows, ОС Linux. Агент позволяет обнаруживать попытки запуска файлов от неизвестных источников, со съёмных дисков, отправлять на проверку в систему ATHENA файлы и блокировать запуск вредоносных файлов.

При первом запуске агент идентифицирует рабочую станцию, собрав о ней необходимую информацию, и отправляет её в систему ATHENA для регистрации и получения уникального токена. После подтверждения регистрации Агент начнёт свою работу.

Для корректной работы агента необходимо обеспечить доступ к системе ATHENA из рабочих станций и/или серверов.

В Агенте по умолчанию настроен перехват всех событий запуска/открытия файлов определённых типов с их последующей проверкой в системе ATHENA. Данное поведение можно настроить из пользовательского интерфейса Агента.

Агент выполняет следующие задачи:

- отслеживание запуска исполняемых файлов;
- отслеживание подключения устройств по шине USB;
- отправка файлов на проверку в систему ATHENA;
- получение и отображение вердикта проверки файла в пользовательском интерфейсе;

– блокирование запуска исполняемых файлов при получении вредоносного вердикта по запускаемому файлу;

– отправка в систему ATHENA информации об используемых рабочей станцией ресурсов, информации о сетевых подключениях, информации о подключаемых съёмных носителях.

Источниками файлов для Агента могут являться:

– ручная загрузка файлов пользователем через пользовательский интерфейс;

– автоматическая загрузка исполняемых файлов при отсутствии информации о них в локальной базе данных;

– загрузка исполняемых файлов автозапуска со съёмных носителей.

Во время своей работы Агент отправляет в систему ATHENA информацию о статусе работы, о количестве потребляемых ресурсов рабочей станции или сервера, о собственных настройках, а также о текущих сетевых соединениях. Данная информация отображается в едином интерфейсе системы ATHENA и может быть просмотрена пользователем.

При получении от системы ATHENA вредоносного вердикта по файлу, попытка запуска блокируется и пользователь получает уведомление об этом.