Содержание

Solar Dozor

«Solar Dozor» - программный комплекс от компании Solar Security, ранее известный как «Дозор Джет». Высокопроизводительная DLP-система, обеспечивающая контроль коммуникаций сотрудников.

Область применения

Комплекс предназначенн для сбора и анализа входящих и исходящих внешних и внутренних сообщений, передаваемых по вычислительным сетям, в целях идентификации событий, которые могут свидетельствовать о нарушении правил информационного обмена. Тем самым обеспечивается соблюдение правил информационного обмена, установленных политикой безопасности организации, а, следовательно, защита от утечек конфиденциальной информации при электронном обмене данными.

Под сообщением в системе понимается объект данных, передаваемый по вычислительным сетям, содержащий тело и служебную информацию – различные заголовки, определяющие тип сообщения, например, тип email – электронная почта, network – сообщение от сенсора webmail, endpoint/screenshot – снимок пользовательского экрана, endpoint/im – сообщения от skype-детектора и т.д.

Solar Dozor решает два основных типа задач. Как классическая DLP-система Solar Dozor решает задачи по мониторингу, фильтрации и анализу каждого сообщения на наличие конфиденциальной информации. Но при решении задач по выявлению корпоративного мошенничества применяется другой подход. Для этого Solar Dozor осуществляет накопление переписки сотрудников, профилирование их действий и в режиме реального времени контроль появления косвенных, на первый взгляд незначительных, признаков противозаконных действий сотрудников, аномалий в их поведении. Эти механизмы позволяют проводить ретроспективный анализ и расследования по накопленным данным и переписке сотрудника на всем объеме коммуникаций сотрудника.

Возможности

«Solar Dozor» позволяет анализировать сообщения различных типов, поступающие как из внешних, открытых сетей, так и из корпоративной сети организации.

Комплекс обеспечивает:

- Анализ сообщений по различным критериям. Объектом анализа может являться как непосредственно информация, передаваемая с помощью сообщения, так и его служебные поля. Если сообщение содержит архив (поддерживаются архивы следующих типов: zip, bzip2, gzip, 7zip, rar, arj, lha, tar, cab, jar), то он распаковывается и его содержимое

- анализируется аналогично самому сообщению.
- Возможность применения определенных действий по отношению к сообщениям, соответствующим заданным критериям. Примерами действий могут являться задержание сообщения, отправка уведомления администратору, отправка уведомления отправителю и т.д.
- Автоматическое помещение в архив сообщений, отвечающих заданным критериям.
- Возможность поиска сообщений в архиве по различным критериям, задаваемым пользователями.
- Настройку механизма фильтрации сообщений в соответствии с принятой политикой безопасности в компании.
- Подключение внешних программ к механизму фильтрации (таких, как антивирусное программное обеспечение).
- Формирование статистических профилей корреспондентов и адресатов по различным критериям, таким как размер сообщения и количество присоединенных файлов.
- Возможность организации многопользовательской работы в системе на основе пользовательских групп и прав доступа.
- Протоколирование работы «Solar Dozor».
- Предоставление уполномоченным пользователям возможности просмотра собранной в процессе мониторинга информации.
- Предоставление уполномоченным пользователям, прошедшим процедуру аутентификации, возможности осуществлять настройку функций безопасности.
- Регистрацию попыток изменения конфигурации, попыток доступа к подсистемам «Solar Dozor» и к хранимым данным (ведение журналов аудита).

Контроль за исполнением правил информационного обмена в корпоративной сети организации предполагает выполнение следующих основных задач:

1. Эффективное управление информационным обменом – подразумевает внедрение политики использования программных средств информационного обмена и контроль за ее исполнением всеми пользователями корпоративной информационной системы.
2. Обеспечение безопасности информационной системы компании – предусматривает осуществление мониторинга и контроля всех входящих, исходящих и внутренних корпоративных сообщений, включая анализ заголовков и структуры сообщений, а
3. также проверку на наличие в тексте сообщения или прикрепленных файлах слов, разрешенных или запрещенных к использованию в электронной переписке.
4. Обеспечение надежного хранения передаваемых сообщений подразумевает хранение большого количества сообщений, передаваемых пользователями, в базе данных с возможностью их экспорта на внешние носители.

Ссылки

Solar Dozor на solarsecurity.ru