Система управления событиями ИБ

На сегодняшний день вычислительные сети и информационные системы защищают достаточно большим и разнообразным количеством средств информационной защиты. Такими средствами, генерирующими большое количество разных событий безопасности, могут быть сетевые экраны, сетевые устройства, различные системы обнаружения вторжений, операционные системы, также базы данных и антивирусы.

Другие услуги Кибербезопасности

Наведите курсор на иконку для отображения информации. Нажмите на иконку для перехода на WEB-страницу

Журналы событий элементов информационной защиты хранятся отдельно, поэтому ручной поиск для сопоставления необходимой информации о сложившихся инцидентах является довольно сложным. Кроме сигналов о злонамеренной активности средства информационной защиты также генерируют и ложные сигналы, снижая эффективность работы защитников сетевой безопасности. Ситуация усложняется еще и тем фактом, что в этих условиях все ответы на угрозы безопасности должны предприниматься незамедлительно.

Система **Security Information and Event Management** по праву является одним из самых качественных и эффективных решений такой проблемы. Такого рода системы автоматизируют процессы анализа поступающих от средств защиты событий и повышают общую эффективность управления комплексной сетевой структурой, таким образом, упрощая задачу защиты информации.

Главные функции SIEM

- Собирает и анализирует сообщения, поступающие от разных источников: системы обнаружения вторжений, операционные системы, сетевые экраны, различные приложения, антивирусы, базы данных и т.п.;
- Распределяет информацию обо всех событиях ИБ. Это позволяет принимать во внимание в первую очередь самые опасные инциденты;
- Проводит корреляционный анализ получаемых данных, определяя комплексные сетевые атаки и атаки, распределенные по времени;
- Автоматически определяет причины, выявляет и реагирует на проблемы нарушения безопасности;
- Предоставляет возможность немедленного просмотра полученных данных и оповещения операторов системы о сложившихся инцидентах и элементах сети, подверженных атакам.

Вы получаете:

- ☑ Повышение общего уровня защищенности информации;
- ☑ Быстрое определение и расследование инцидентов в автоматическом режиме;
- ☑ Комплексный подход к задачам хранения и обработки событий ИБ.

Больше услуг на сайте www.ftl.ua

FTL
www.ftl.ua
+380 (44) 538-13-00
info@ftl.ua