Программные средства, которые обеспечат информационную безопасность

В настоящее время для исключения случаев утечки информации устанавливают специальное программное обеспечение. С помощью профессиональных средств системные администраторы справляются с задачей обеспечения информационной безопасности.

Среди популярных приложений можно выделить следующие:

- StaffCop – программное обеспечение, защищающее данные и предотвращающее их утечку. Вы самостоятельно можете настраивать режим работы утилита и параметры. Оповещения и возможность записи экрана позволяет оперативно обнаружить утечку данных и несанкционированный доступ к системе. В результате вам удается беспрепятственно выявить источник и определить все обстоятельства инцидента;
- IBM QRadar SIEM – современный инструмент обнаружения угроз и вирусных атак. Утилита осуществляет сбор данных о пользователях, локальной сети, подключенных устройствах и других объектах. Путем проведения расширенной аналитики программное обеспечение отслеживает вероятные угрозы и препятствует их распространению. Такая программа представляет собой комплексное решение, обладающее множеством функций. Клиенты могут использовать ее, как ПО или виртуальное устройство локальной или облачной среды;
- SolarWinds собирает всю полезную информацию и фиксирует ее в журналах. В результате вы может оперативно справляться и устранять угрозы в режиме онлайн. Утилита предполагает возможность использования клиентом средств визуализации, с помощью которых легко можно обнаружить подозрительную активность. Несомненным преимуществом является наличие интуитивной понятной панели и удобного интерфейса;
- Sumo Logic – система интеллектуального анализа, благодаря которой удается обеспечить информационную безопасность компании. В рамках платформы проводится аналитика безопасности, осуществляется управление журналами, устраняются возникшие угрозы. Несанкционированный доступ системный администратор может запретить в режиме реального времени. Своевременная ликвидация угроз обеспечивает надлежащий уровень безопасности;
- ManageEngine – современное решение, которое позволяет получить необходимую информацию о работе системы через различные журналы, в которых регистрируется важная информация. Во время работы данного приложения поступают оповещения о

несанкционированном доступе к системе и ресурсам компании. Основной целью работы приложения является мониторинг веб-серверов, баз данных и почтовых служб.

- AlienVault – приложение, с помощью которого осуществляется комплексная диагностика. После установки утилиты возможно оперативное обнаружение угроз и вирусных атак. Продукт многофункционален и эффективно справляется с обеспечением информационной безопасности. Для удобства утилита предполагает поступление оповещений на электронную почту. Во время работы программного обеспечения проводится автоматический анализ различных журналов. Информация о пройденной проверке отображается на панели мониторинга;
- LogRhythm, многофункциональное оборудование, работа которого строится на основе искусственного интеллекта и поведенческого анализа. В рамках платформы имеется расширенное хранилище, в котором структурированно собирается вся ценная информация. ПО подходит для установки в компаниях среднего и малого предпринимательства;
- Rapid7 InsightlDR – одно из лучших решений безопасности, которое позволяет выявить инциденты и отреагировать на несанкционированный доступ. Многофункциональное приложение позволяет обнаруживать большое количество угроз, учитывая кражу данных и вредоносные программы. По своему функционалу и особенностям работы утилита подходит для ведения бизнеса на малых, средних и крупных предприятиях. Благодаря специальным журналам осуществляется оперативный поиск угрозы и ее ликвидация;
- Splunk – эффективный инструмент, который защитит компьютер от несанкционированного доступа. Настроить приложение можно в зависимости от характера работы организации и необходимости мониторинга определенной информации. Инструмент является универсальным и работает в любой сфере жизни. К преимуществам ПО относят оперативное обнаружение угрозы, реальную оценку рисков, сбор информации и упорядочение событий;
- Varonis позволяет аналитическому отделу обзавестись практическими отчетами и предупреждениями. С целью оперативной реакции даже на малейшие угрозы, системные администраторы могут настраивать работу оборудования точнейшим образом.