Кудусова М.И., Матаев А.Б.**Применение системы SIEM на предприятии***ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»
(Россия, Грозный)*

doi: 10.18411/trnio-12-2021-87

Аннотация

Предприятия и организации неустанно обрастают новыми системами обеспечения информационной безопасности. Однако, практика показывает, что количество неуклонно понижает качество и усложняет процесс обработки данных, поступающих от систем обеспечения защиты информации.

Ключевые слова: система, события, угроза, информационная безопасность.

Abstract

Enterprises and organizations are tirelessly overgrown with new information security systems. However, practice shows that quantity steadily decreases the quality and complicates the process of processing data from information security systems.

Keywords: system, events, threat, information security.

Помимо этого, администраторы по информационной безопасности сталкиваются с трудностями по реагированию на множество событий в системе, а разработки и ПО, занимающиеся обеспечением информационной безопасности, часто проектируются на разных архитектурных основах и программных базах, что усложняет коммуникацию между отдельными компонентами общей структуры. Оповещение о нарушении безопасности и вторжении в информационную среду предприятия не является столь эффективным, если за ним не следуют мероприятия по ликвидации угрозы. Данную и ряд других проблем способна решить система Security Information Event Management.

SIEM система не выступает комплексным и единым методом по устранению угроз и их обнаружению. В ней нет интегрированных инструментов для защиты данных, алгоритмов поиска ненадежных секторов, или чего-то подобного. Функционирование данной системы строится на анализе и сборе информации с множества других источников обнаружения, локализации и устранения угроз безопасности: антивирусное ПО, сетевое оборудование, средства контрольной аутентификации и доступа, регистраторы нарушений в заведомо отлаженной системе, датчики движения, и так далее.

Система анализирует совокупность незначительных отклонений и нарушений, которые по отдельности не несут в себе большой угрозы, однако в дальнейшем могут стать причиной серьезных проблем.

Для того чтобы анализирование и изучение неполадок и зарегистрированных событий было детальным и продуктивным, перед системой SIEM ставятся определенные задачи:

- компоновка и систематизация истории зарегистрированных событий от всех участников системы, с целью изучения и выявления причины сбоев, нарушений, и т. п.;
- обеспечение различным ассортиментом инструментов и методов для анализа событий, упорядочивание ошибок и сбоев по степени угрозы, предоставление отчетной документации и уникального обозначения каждого зарегистрированного события;
- корреляция событий, обработка данных по регламенту;
- интерфейс взаимодействия для передачи оповещений администратору.

Работоспособность системы SIEM осуществляется при использовании некоторых компонентов:

- агенты (программное обеспечение), которые реализуют сбор информации и пересылают их на сервер;
- сервер с наличием базы данных, который осуществляет хранение историю зарегистрированных событий и их обработку;
- сервер-коллектор, является общим сервером для сбора информации от большого количества различных источников;
- коллекторы библиотеки, служат инструментами сортировки и унификации событий, соотнесение их к конкретным журналам событий;
- сервер-коррелятор, собирающий информацию только от программ-агентов и коллекторов, обработка полученной информации реализуется по строгому регламенту алгоритмов и правил.

Гибкая логическая база системы SIEM делает её универсальной и легко подстраиваемой под различные нужды обеспечения безопасности. Но, как в случае с машинным обучением, для более эффективного и детального анализа событий, системе требуются обширные источники и алгоритмы её работы, информационная база по статистике срабатываний положительных и отрицательных явлений в системе.

Применение источников для SIEM сопутствует с отбором по следующим критериям:

- соотношение ценности источника и рисков его использования, тоже самое относится и к информации;
- возможность охвата большого количества каналов получения информации от различных средств и компонентов системы;
- способность решения различных задач в сфере информационных технологий и информационной безопасности;
- правдоподобность и уровень информирования источника системных событий.

Современные SIEM системы используют источники событий и информации такого рода, как:

- системы доступа и контроль идентификации личности;
- обработка серверной информации и рабочие станции;
- активное оборудование по фиксации изменений доступа к сети;
- инструменты по обнаружению и ликвидации событий, угрожающих безопасности сети;
- защита от вирусных угроз;
- системы по расстановке приоритетов и систематизации угроз;
- обработка сетевого трафика, и т. д.

От спектра необходимых функций зависит итоговая ценовая стоимость интеграции системы SIEM, что может вылиться в немалую денежную сумму. Однако, на фоне отсутствия какой-либо конкуренции в данном сегменте информационной безопасности, обсуждаемый нами продукт является наилучшим средством обнаружения угроз систем разного рода предназначения.

SIEM система полностью автоматизирует процесс установки причин нарушения системы безопасности и позволяет администратору не отвлекаться на события, которые в последствии могут быть ложными, а работать непосредственно с инцидентом. Стоит отметить, что установка такой системы в то или иное предприятие не является выходом в образе «поставил и забыл». Требуется квалифицированный специалист для отладки и настройки всей сетевой конструкции, реализации непрерывной работы и устранения сбоев в работе SIEM.

1. ISO/IEC 27001:2013 «Information security management system» и ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»

2. ISO/IEC TR 18044:2004 «Information technology. Security techniques. Information security incident management» и ГОСТ Р ИСО/МЭК ТО 18044-2007. «Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»
3. NIST SP 800-61 «Computer security incident handling guide»
4. Аксенов В. Руководство по обработке инцидентов компьютерной безопасности [Электронный ресурс] //Itsec <http://itsec.by/rukovodstvo-po-obrabotke-incidentov-kompyuternoj-bezopasnosti-nist-sp-800-61-r2/> (дата обращения 25.11.2020).
5. CMU/SEI-2004-TR-015 «Defining incident management processes for CSIRT»
6. Безмалый В. Реагирование на инциденты информационной безопасности Add-Ons [Электронный ресурс] //It-community <https://www.it-community.in.ua/2014/07/reagirovanie-na-incidenty-informatsionnoj-bezopasnosti.html/> (дата обращения 25.11.2020).
7. СТО БР ИББС - 1.0 - 2014. «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения».
8. РС БР ИББС - 2.5 - 2014. «Менеджмент инцидентов информационной безопасности».
9. ISO/IEC 27035:2011 «Информационные технологии. Метод обеспечения безопасности. Управление случайностями в системе информационной безопасности»

Кудусова М.И., Миндиева И.М., Хасуева Ж.Ш.

Электронная цифровая подпись как фактор обеспечения безопасности документа

ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»

(Россия, Грозный)

doi: 10.18411/trnio-12-2021-88

Аннотация

Данная статья покажет, как электронная подпись стала неотъемлемой частью в сфере документации. В последнее время значительные массивы данных передаются, обрабатываются и хранятся в электронной форме в автоматизированных информационных системах. Поэтому важное значение имеет определение правового статуса электронного документа с точки зрения возможности его применения наряду с традиционным бумажным документом.

Ключевые слова: подпись, личность, пароль, защита, цифровая подпись, документ.

Abstract

This article will show how the electronic signature has become an integral part in the field of documentation. Recently, significant amounts of data are transmitted, processed and stored electronically in automated information systems. Therefore, it is important to determine the legal status of an electronic document in terms of the possibility of its application along with a traditional paper document

Keywords: signature, identity, password, protection, digital signature, document.

Электронная цифровая подпись - это зашифрованная электронная подпись, которая может гарантировать происхождение электронного документа, его целостность и подлинность. Когда вы вручную подписываете документ, вы гарантируете свое согласие с текстовым содержанием. Цифровая подпись делает то же самое и добавляет еще больше информации. Она гарантирует подлинность подписи, доказывая, что вы являетесь лицом, подписавшим, она обеспечивает целостность документа, то есть он не подвергался изменениям с момента подписания, а также подтверждает устойчивость документа, гарантируя его действительность на долгие годы.

Электронная подпись позволяет выполнять все процессы подписи удаленно и практически с любого устройства. Все, что вам нужно, это подключение к Интернету. Кроме того, электронная подпись имеет такую же юридическую силу, как и подпись, написанная от руки чернилами на бумаге. Компании также переходят на программные решения для электронной подписи, чтобы сократить потребление бумаги, сократить расходы и повысить эффективность.