Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

Колесова
Татьяна Романовна

Методика обработки информации в системах мониторинга информационной безопасности

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

_____

Научный руководитель
Белоусова Елена Сергеевна
к.т.н., доцент

_____

Минск 2019

ВВЕДЕНИЕ

Государственными и международными стандартами предъявляются требования по мониторингу и аудиту событий информационной безопасности к организациям, осуществляющим обработку информации ограниченного распространения. Также ввиду использования большого количества сетевых устройств и приложений (например, межсетевые экраны, базы данных, системы обнаружения вторжений и другое), позволяющих в большей степени обеспечить информационную безопасность предприятия, возникает задача непрерывного анализа событий информационной безопасности, что является довольно сложным и трудоемким процессом. При различных инцидентах должно быть незамедлительное реагирование, в противном случае возрастает вероятность упущения инцидента и угрозы информационной безопасности.

Для оптимального анализа различных событий, которые постоянно поступают от различных систем защиты информации, и обеспечения повышенного уровня информационной безопасности и централизованного управления и анализа журналов необходимо использовать SIEM-системы. Основополагающий принцип SIEM-системы заключается в том, что данные о безопасности информационной системы собираются из разных источников, и результат их обработки предоставляется в едином интерфейсе, доступном для аналитиков безопасности, что облегчает изучение характерных особенностей, соответствующих инцидентам безопасности. При моментальном получении информации об угрозе, SIEM-система позволяет предпринять необходимые меры для устранения различной опасности, что важно для непрерывной работы крупного предприятия. SIEM-системы могут помочь организациям, которым необходимо соответствовать существующим нормативным требованиям в области аудита безопасности, и снизить риск вторжений в сеть.

Для оптимального анализа событий безопасности и последующей своевременной реакции на инциденты в SIEM-системах проводится такой важный этап обработки информации, как нормализация событий безопасности, так как события, приходящие в SIEM-систему, никак не стандартизированы, и равнозначные по смыслу события могут быть записаны в абсолютно разных форматах, что негативно сказывается на дальнейшем анализе. Нормализация событий и то, насколько корректно она выполнена, напрямую влияет на корректность дальнейшей обработки данных.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в совершенствовании работы систем мониторинга информационной безопасности на основе использования методики обработки событий.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

– провести обзор SIEM-систем, их функциональных компонентов;

– изучить требования к SIEM-системам в Республике Беларусь;

– изучить процесс нормализации событий безопасности;

– разработать методику обработки информации в системах мониторинга информационной безопасности;

– апробировать разработанную методику в типовых условиях;

– разработать рекомендации по применению методики обработки информации в системах мониторинга информационной безопасности.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XVI белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, 2018).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликована 1 работа, в том числе 1 тезисы доклада в сборнике материалов конференции.

Личный вклад соискателя

Все основные результаты, выводы получены соискателем самостоятельно.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, трех глав, заключения, библиографического списка и четырех приложений. Общий объем диссертации 67 страниц, 31 наименование в библиографическом списке.

Во **введение** определена область исследований и их актуальность. В общей характеристике работы сформулированы цель и задачи работы, показан личный вклад соискателя и опубликованность результатов исследований.

В **первой главе** приводится общее описание систем мониторинга информационной безопасности. Описана архитектура SIEM-систем, принцип их работы, представлено описание функциональных компонентов. Также приведены основные достоинства использования SIEM-систем, нормативно-правовые требования для использования SIEM-систем и обзор существующих SIEM-систем.

Вторая глава посвящена процессу обработки информации в системах мониторинга информационной безопасности. Подробно рассмотрены схемы взаимодействия сущностей в событиях безопасности для определения обязательных полей событий, извлекаемых в процессе нормализации. Описана разработанная схема полей событий безопасности. Рассмотрены различные способы нормализации событий безопасности. Описывается разработанная методика обработки информации в системах мониторинга информационной безопасности.

В **третьей главе** приведено описание апробации методики обработки информации в системах мониторинга информационной безопасности. Описана среда для апробации, настройка компонентов. Были разработаны правила нормализации событий безопасности и произведена их апробация в рамках среды.

В **заключении с**формулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

Технологический прогресс не стоит на месте, и системы защиты информации развиваются и эволюционируют вместе с ним. SIEM-системы не являются исключением. Ранее функционал классического SIEM решения больших и средних компаний более-менее удовлетворял имеющимся требованиям. Однако в настоящее время необходимы новые механизмы и функции, способные своевременно и адекватно выявлять, обрабатывать и анализировать текущие потоки информации и событий безопасности для гораздо большего количества устройств с учетом существенно возросших объемов информации, в том числе данных о пользователях, трафике, сервисах, событиях и так далее.

Основой оперативного и адекватного реагирования на инциденты безопасности является правильная обработка событий безопасности, которые собирает SIEM-система, что обеспечивается грамотно построенным процессом нормализации.

В данной магистерской диссертации была разработана методика обработки информации в системах мониторинга событий информационной безопасности, которая определяет обработку информации со стороны процесса нормализации.

Особенностью данной методики является углубленное рассмотрение процесса нормализации, в частности, в рамках данной методики была разработана схема полей событий безопасности. Отличием данной схемы является более индивидуальный подход к рассмотрению событий, каждое событие рассматривается отдельно, в нем выделяются поля, которые действительно полезны для дальнейшей обработки SIEM-системой. При разработке данной схемы были проанализированы схемы полей событий безопасности таких решений мониторинга информационной безопасности, как Arcsight ESM и IBM Security Qradar SIEM.

Была произведена апробация разработанной методики в тестовых условиях, которая показала, что разработанная методика подходит для использования при создании собственной SIEM-системы (основанной на свободно распространяемых программных продуктах) и ее внедрении в корпоративную сеть предприятия, при последующей настройке. В частности, данная методика определяет действия на таком этапе обработки событий, как нормализация. Данная методика содержит указания о том, какие подготовительные этапы необходимо пройти, прежде чем приступить к разработке правил нормализации.

В рамках апробации методики были написаны правила нормализации для приведенного макета сети, которые производят общую нормализацию событий

в единую схему полей событий безопасности и осуществляют более глубокий разбор события посредством разработки частных правил нормализации. Данные правила нормализации хороши тем, что в любой момент времени, если информация перестанет быть нужной в рамках дальнейшего анализа нормализованных событий безопасности, их можно откорректировать, удалив определенное поле или изменив его обработку в рамках разработанного правила.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1–А. Колесова, Т.Р. Аудит безопасности в информационных системах/ Т.Р. Колесова, Е.С. Белоусова // Тезисы докладов XVI Белорусско-российской научно-технической конференции, Минск, 5 июня 2018 г. / редкол.: Т.В. Борботько [и др.]. Минск: БГУИР, 2018. – С. 49.