КЛАССИФИКАЦИЯ СОВРЕМЕННЫХ СИСТЕМ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ БЕЗОПАСНОСТИ

Рыболовлев Д.А.[1], Карасёв С.В.[2], Поляков С.А.[3]

Целью работы *является разработка системы классификации современных решений систем управления инцидентами безопасности (SIEM, Security Information and Event Management)*

Методом исследования *выбран анализ известной литературы и обобщения существующих взглядов на вопросы построения систем класса SIEM. Данный анализ производился за счет изучения научно-технической литературы, включающей актуальные научные публикации, обзорные материалы, подробные описания особенностей архитектуры и применяемых в SIEM системах технологий обработки событий безопасности, документацию коммерческих решений и проектов с открытым исходным кодом.*

Полученный результат. *Среди многообразия характеристик решений SIEM выделены наиболее «рельефные» классификационные признаки, условно разделенные на три группы: отражающие архитектурные особенности систем управления инцидентами безопасности, соответствующие применяемым технологиям обработки событий безопасности и особенностям реализации конечным пользователям. Представленная классификация позволяет систематизировать знания в рассматриваемой предметной области и может быть использована для дальнейших исследований современных SIEM систем, проведения сравнительного анализа, совершенствования существующих и разработки перспективных систем управления инцидентами безопасности.*

Новизна статьи заключается в определении множества наиболее существенных признаков систем управления инцидентами безопасности и предложении на их основе новой системы классификации решений SIEM.

Ключевые слова: *событие безопасности, инцидент, управление информационной безопасностью, SIEM, корреляция событий, система классификации, классификационный признак*

DOI: 10.21681/2311-3456-2018-3-47-53

Введение

В целях выполнения мероприятий по обеспечению информационной безопасности (ИБ) необходимо решение ряда задач, таких как осуществление регистрации, мониторинга и анализа инцидентов ИБ, информирование администрации обо всех случаях нарушений ИБ, сбор свидетельств и доказательств для реагирования по случаям инцидентов и других. Указанные задачи формируют группу задач менеджмента инцидентами ИБ, для решения которых одним из наиболее эффективных подходов считается применение систем класса SIEM [1].

Решения SIEM обеспечивают управление информацией и событиями безопасности, реализуя функции сбора и хранения, обработки и анализа зарегистрированных событий безопасности с целью выявления и разбора инцидентов, а также проверки соответствия системы управления ИБ существующим требованиям и нормам [2].

Сегодня на рынке средств защиты информации представлены десятки решений класса SIEM, отличающиеся архитектурой и функциональными возможностями, производительностью обработки регистрируемых событий безопасности, применяемыми технологиями выявления зависимостей между отдельными событиями, используемыми показателями состояния защищаемой инфраструктуры, особенностями построения интерфейса и др.

Многообразие и вариативность характеристик современных SIEM систем обусловливает актуальность задачи их классификации.

Постановка задачи и релевантные работы

Вопросы построения систем управления инцидентами безопасности активно обсуждаются в последние годы, при этом важным аспектом исследуемой предметной области является классификация SIEM систем.

В работе [3] представлен сравнительный обзор SIEM систем и уточнен критерий выбора решений подобного класса для заказывающих организаций, объединяющий требования к функциональным возможностям и особенностям эксплуатации (полнота документации, уровень интеграции, простота внедрения, перспективы развития). Авторы выделяют два режима сбора данных событий безопасности, применяемых в решениях SIEM: с установкой специализированных программных агентов на устройства источников событий и без использования агентов. Отмечается разнообразие доступных на рынке систем управления инцидентами безопасности, вместе с тем приведенная типология не имеет классификационных признаков систематизации данных, представляя формально перечень функциональных и эксплуатационных характеристик без разделения множества SIEM систем на соответствующие отдельные классы.

1 Рыболовлев Дмитрий Александрович, кандидат технических наук, Академия ФСО России, г. Орел, Россия. E-mail: dmitrij-rybolovlev@yandex.ru

2 Карасёв Станислав Владимирович, Академия ФСО России, г. Орел, Россия. E-mail: sats861@yandex.ru

3 Поляков Сергей Александрович, кандидат технических наук, Академия ФСО России, г. Орел, Россия. E-mail: llmaglu@mail.ru

Возможность использования нереляционных хранилищ данных в целях применения технологий больших данных для корреляций событий безопасности отмечается в статье [4]. Однако в работе не приводятся сведения о других способах организации хранилищ данных и сравнительных преимуществах выбранного подхода.

В [5] рассматриваются вопросы построения SIEM систем и уточняется архитектура систем управления инцидентами безопасности. Поясняется принципиальная организация SIEM систем, приводится краткая характеристика отдельных компонент и особенности их взаимодействия в процессе функционирования. Выделены различные режимы получения данных от источников событий безопасности в зависимости от распределения ролей ведущего и ведомого компонента (push-метод, pull-метод). Рассматриваются три способа организации хранилища данных: базы данных, текстовые и двоичные файлы. Вместе с тем выделенные в работе классификационные признаки не позволяют в полной мере характеризовать применяемые в SIEM решениях технологии обработки событий безопасности и особенности реализации конечным пользователям.

В статье [6] подробно обсуждаются методы, применяемые при реализации ядра обработки событий безопасности типовой SIEM системы. Анализируются существующие методы корреляции, выявляются принципы работы основных компонентов ядра обработки событий безопасности. Авторы выделяют пять методов корреляции, являющихся наиболее используемыми в рассматриваемой предметной области: правило-ориентированный метод; методы на основе математического аппарата конечного автомата, Байесовкой сети, нейронной сети; метод рассуждений на основе прецедентов.

Особенности реализации SIEM решений конечным пользователям рассматриваются в статье [7]. Обсуждаются преимущества модели обслуживания SaaS (Software as a Service, программное обеспечение как услуга) применительно к организации системы управления инцидентами безопасности. Однако отсутствуют сведения об ограничениях «облачных» реализаций и масштабах внедрения SIEM систем.

В отмеченных выше работах подробно описаны отдельные классификационные признаки современных SIEM систем. Однако опубликованные результаты носят недостаточно полный и системный характер с точки зрения разделения множества SIEM систем на отдельные классы – решения задачи классификации.

Решаемая в исследовании задача классификации систем управления инцидентами безопасности в общем виде может быть представлена как задача выбора наиболее «рельефных» признаков и разделения множества рассматриваемых SIEM решений на классы в зависимости от значений соответствующих признаков.

Предлагаемый вариант классификации формализован в табличном виде с указанием перечня классификаторов, позволяющих определить место исследуемой системы на множестве различных систем управления инцидентами безопасности. Для удобства практического использования системы классификации вводится понятие «индекс классификатора». Индекс отдельного классификатора определяет один из выделенных классификационных признаков, а набор индексов позволяет характеризовать исследуемую систему без необходимости указания подробного содержания классификаторов.

В исследовании не рассматриваются вопросы отечественной стандартизации в области оценки соответствия SIEM систем как класса средств защиты информации (СЗИ) по причине отсутствия нормативных требований. В большей степени вопросы формирования новых критериев оценки соответствия СЗИ относятся к компетенциям ФСТЭК России и Технического комитета по стандартизации ТК 362 «Защита информации», которые, как ожидается, в ближайшее время определят отдельные требования к решениям класса SIEM [8]. Разработанная система классификации допускает дополнение множества признаков с целью учета новых нормативных требований.

Классификация SIEM систем

Анализ известной литературы и обобщение существующих взглядов на вопросы построения SIEM систем позволяют среди всего многообразия характеристик выделить следующие классификационные признаки: тип используемого хранилища данных, способ получения данных от источников событий, степень удаленности источников событий, метод выявления зависимостей между отдельными событиями безопасности, способ распространения, масштаб внедрения, используемая модель обслуживания.

Предлагаемый вариант классификации современных систем управления инцидентами безопасности представлен в таблице 1.

Для организации хранилища данных в системах SIEM могут применяться [1, 4, 9]:

1. Реляционные системы управления базами данных (К1.1, здесь и далее в скобках при пояснении указывается индекс соответствующего классификатора, приведенный в таблице 1).
2. Нереляционные хранилища данных (К1.2).

Для организации реляционного хранилища данных в большинстве случаев используется наиболее распространенное решение – СУБД с поддержкой языка структурированных запросов (SQL, structured query language).

Нереляционное хранилище данных (или «NoSQL») может быть построено различными способами в зависимости от используемой модели данных. Среди примеров организации можно выделить следующие: хранилище «ключ-значение» (например, Redis, Amazon DynamoDB), хранилище семейства столбцов (Apache Cassandra), документо-ориентированная СУБД (MongoDB).

По причине возрастающего объема накапливаемых и обрабатываемых данных, необходимых для эффективного функционирования систем управления инцидентами безопасности, в настоящее время разработчики SIEM систем практически отказались от использования реляционных хранилищ данных в пользу нереляционных. Применение нереляционных хранилищ данных позволяет повысить масштабируемость и надежность, реализовать параллельную обработку больших объемов данных.

Таблица 1. – Система классификации решений SIEM

№ п/п	Классификационный признак	Индекс классификатора	Содержание классификатора
1	Тип используемого хранилища данных	К1.1	Реляционная система управления базами данных (СУБД)
		К1.2	Нереляционное хранилище данных
2	Способ получения данных от источников событий	К2.1	С использованием приложений-агентов (agent-based)
		К2.2	Без использования приложений-агентов (agentless)
3	Степень удаленности источников событий	К3.1	С источниками событий в пределах контролируемой зоны
		К3.2	С территориально распределенными источниками событий
4	Метод выявления зависимостей между отдельными событиями безопасности	К4.1	Основанный на заранее заданных правилах обработки (rule-based)
		К4.2	Конечный автомат
		К4.3	Рассуждение на основе прецедентов
		К4.4	Байесовская сеть
		К4.5	Нейронная сеть
5	Способ распространения	К5.1	С открытым исходным кодом
		К5.2	Коммерческий
6	Масштаб внедрения	К6.1	Малый
		К6.2	Средний
		К6.3	Крупный
7	Используемая модель обслуживания	К7.1	Локальная установка
		К7.2	Как услуга (hosted SIEM, SIEM as a service)

По способу получения данных от источников событий выделяют системы SIEM [3, 5]:

1. С использованием приложений-агентов (agent-based, К2.1).

Агент – это специализированное программное средство, устанавливаемое на устройство источника событий. Агент выполняет предварительную обработку, фильтрацию, агрегацию и нормализацию событий, после чего передает нормализованные данные на сервер обработки в режиме, близком к реальному времени, для дальнейшего анализа и хранения. В случае если на устройстве источника используются несколько журналов событий, может потребоваться установка нескольких агентов. Большинство решений класса SIEM имеют в базовой поставке множество агентов для обработки журналов событий поддерживаемых форматов (syslog, SNMP и другие) [11], а также позволяют администратору безопасности создавать собственные агенты для обработки неподдерживаемых форматов.

2. Без использования приложений-агентов (agentless, К2.2).

Сервер обработки получает данные о зарегистрированных событиях непосредственно от источников без необходимости установки дополнительного программного обеспечения. В одном случае сервер посылает источнику запрос и после успешной аутентификации получает данные журнала событий (pull-метод). В другом случае источник может быть настроен таким образом, чтобы с определенной периодичностью подключаться к серверу обработки, аутентифицироваться и пересылать регистрируемые события (push-метод) [10]. И в том, и в другом случае принципиально важным является тот факт, что предварительная обработка, фильтрация, агрегация и нормализация данных журналов событий безопасности выполняются на сервере обработки.

В большинстве случаев коммерческие SIEM системы позволяют работать как с использованием агентов, так и без них. Среди преимуществ способа сбора данных без использования агентов следует отметить отсутствие необходимости установки и обслуживания дополнительного программного обеспечения на устройствах источников событий. Однако недостатком такого подхода является повышенная нагрузка на канал связи между источником и сервером, поскольку события пересылаются в необработанном виде, а фильтрация, агрегация и нормализация выполняются только на сервере обработки.

По степени удаленности источников событий выделяют следующие классы решений SIEM [2]:

1. С источниками событий в пределах контролируемой зоны (К3.1).
2. С территориально распределенными источниками событий (К3.2).

Рассматриваемый классификационный признак позволяет различать системы SIEM с локальным и удаленным управлением соответственно. В первом случае, когда управляющая система (сервер обработки, консоль администрирования) и объект управления (источник событий) находятся в пределах контролируемой зоны, допускается не использовать средства шифрования управляющих воздействий и передаваемых данных. Во втором случае применение средств криптографической защиты процесса удаленного управления является обязательным.

Системы управления инцидентами безопасности реализуют различные технологии выделения последовательностей контролируемых действий (сценариев компьютерных атак и др.) в целях формирования соответствующих инцидентов безопасности [12]. Среди методов выявления зависимостей между двумя и более событиями безопасности выделяют следующие [6]:

1. Основанный на заранее заданных правилах обработки (rule-based, К4.1).
2. Конечный автомат (К4.2).
3. Рассуждение на основе прецедентов (К4.3).
4. Байесовская сеть (К4.4).
5. Нейронная сеть (К4.5).

Анализ известных источников показывает, что практически все современные SIEM системы в базовой версии поставки применяют один метод корреляции (выявления зависимостей) – на основе заранее заданных правил обработки (К4.1) [13, 14]. Другие методы выявления зависимостей используются ограниченно в связи с трудоемкостью реализации и высокой вычислительной сложностью [12]. Примеры коммерческих решений (использующих методы корреляции, отличные от rule-based подхода) – Micro Focus ArcSight ThreatDetector, IBM QRadar User Behavior Analytics, Splunk Machine Learning Toolkit.

По способу распространения все решения SIEM разделяются на два класса:

1. С открытым исходным кодом.
2. Коммерческие.

Проекты систем SIEM с открытым исходным кодом (наиболее известные представители класса – AlienVault OSSIM, Prelude) доступны для изучения и модификации, что позволяет пользователям участвовать в доработке, тестировании и исправлении ошибок, а также заимствовать исходный код для создания собственных проектов. Большинство систем SIEM с открытым исходным кодом являются одновременно свободными и распространяются бесплатно.

К коммерческим системам относится большинство решений SIEM, представленных на рынке. Основанием для отнесения той или иной системы SIEM к классу коммерческих решений является ориентация разработчика на получение прибыли от использования системы SIEM другими пользователями, например, путем продажи экземпляров и/или оказания услуг поддержки, и монополия правообладателя на использование, копирование и модификацию соответствующего программного обеспечения (в этом смысле понятие коммерческой системы близко к понятию проприетарного программного обеспечения).

В зависимости от масштаба внедрения (развертывания) системы управления инцидентами безопасности разделяются на следующие классы [15]:

1. Малые.
2. Средние.
3. Крупномасштабные.

Указанный классификационный признак характеризует обобщенную оценку трех показателей: числа подключенных источников, количества обрабатываемых (поступающих) событий в секунду, объема репозитория, выделяемого для хранения зарегистрированных событий.

Эксперты компании Gartner в отчетах «Magic Quadrant for Security Information and Event Management» относят к малому масштабу внедрения систем класса SIEM случаи, когда используется не более 300 источников событий, скорость обработки событий не превышает 1500 EPS (events per second, событий в секунду), объем репозитория составляет 800 Гбайт или менее. Средний масштаб соответствует условиям развертывания в системе с числом источников событий от 400 до 800, при скорости обработки событий от 2000 до 7000 EPS и объеме репозитория 4-8 Тбайт. Крупномасштабные системы SIEM могут подключать 900 и более источников событий, обеспечивать скорость обработки от 15000 EPS и использовать объем репозитория свыше 10 Тбайт. Приведенная градация представлена в таблице 2.

Таблица 2. – Масштабы внедрения (развертывания) SIEM систем

Масштаб внедрения (развертывания)	Число подключенных источников	Количество обрабатываемых событий в секунду, EPS (events per second)	Объем репозитория, выделяемого для хранения зарегистрированных событий
Малый	≤ 300	≤ 1500	≤ 800 Гбайт
Средний	400-800	2000-7000	4-8 Тбайт
Крупный	≥ 900	≥ 15000	≥ 10 Тбайт

По используемой модели обслуживания выделяют следующие классы систем SIEM [7, 15]:

1. Локальной установки.
2. Как услуга (hosted SIEM, SIEM as a service).

Системы управления инцидентами безопасности локальной установки подразумевают традиционную модель обслуживания, при использовании которой программное обеспечение (приложения SIEM решения) устанавливается и обслуживается пользователем в локальной инфраструктуре организации.

В случае применения модели обслуживания SaaS пользователи получают SIEM решение, полностью обслуживаемое провайдером услуг ИБ. Основное преимущество модели SaaS заключается в снижении затрат, связанных с установкой, обновлением и поддержкой соответствующего программно-аппаратного обеспечения. При этом следует отдельно отметить, что пользователь должен обеспечить требуемую пропускную способность и непрерывность канала связи с поставщиком услуг. В качестве примера можно привести решения Splunk Cloud и Alert Logic, наиболее полно соответствующие требованиям к системам SIEM с моделью обслуживания SaaS.

Применение разработанной системы классификации

Ниже поясняется применение предлагаемого подхода на примере классификации современных решений SIEM следующих категорий:

а) иностранного производства:

– система мониторинга и управления событиями безопасности «ArcSight ESM»[4] (разработчик – «Micro Focus», версия 7.0);

– система управления инцидентами безопасности «QRadar SIEM»[5] (разработчик – «IBM», версия 7.2);

б) отечественного производства:

4 Micro Focus ArcSight ESM. URL: https://software.microfocus.com/ru-ru/products/siem-security-information-event-management/overview

5 IBM QRadar SIEM. URL: https://www.ibm.com/ru-ru/marketplace/ibm-qradar-siem

Таблица 3 – Классификация современных SIEM систем

№ п/п	Классификационный признак	Решение SIEM / значение признака (индекс классификатора)				
		ArcSight ESM	QRadar SIEM	MaxPatrol SIEM	КОМРАД	OSSIM
1	Тип используемого хранилища данных	K1.1 K1.2[1]	K1.1	K1.2	K1.2	K1.1
2	Способ получения данных от источников событий	K2.1 K2.2	K2.1 K2.2	K2.1 K2.2	K2.1 K2.2	K2.1
3	Степень удаленности источников событий	K3.1 K3.2	K3.1 K3.2	K3.1 K3.2	K3.1 K3.2	K3.1 K3.2
4	Метод выявления зависимостей между отдельными событиями безопасности	K4.1[2]	K4.1[3]	K4.1	K4.1	K4.1
5	Способ распространения	K5.2	K5.2	K5.2	K5.2	K5.1
6	Масштаб внедрения	K6.3	K6.3	K6.3	K6.3	K6.2
7	Используемая модель обслуживания	K7.1 K7.2	K7.1 K7.2	K7.1	K7.1	K7.1

– система мониторинга событий информационной безопасности «MaxPatrol SIEM»[6] (разработчик – «Позитив Текнолоджиз», версия 4.0);

– система управления событиями информационной безопасности «КОМРАД»[7] (разработчик – НПО «Эшелон», версия 2.0);

в) с открытым исходным кодом:

– система управления инцидентами безопасности «OSSIM»[8] (разработчик – «Alien Vault», версия 5.5).

Определение значений классификационных признаков осуществлялось на основании анализа технической документации выбранных программных продуктов и обзорных материалов[9,10]. Результаты применения системы классификации приводятся в таблице 3.

Выводы

По результатам выполненной работы представлен вариант классификации систем управления инцидентами безопасности.

Достоверность и обоснованность сделанных выводов подтверждается систематизацией значительного числа актуальных публикаций по исследуемой проблематике, непротиворечивостью известным результатам и соответствием предложенной системы классификации общим принципам построения решений SIEM.

Выделенные классификационные признаки условно могут быть разделены на три группы: отражающие особенности архитектуры систем SIEM (тип используемого хранилища данных, способ получения данных от источников событий, степень удаленности источников событий), соответствующие применяемым технологиям обработки событий безопасности (способ выявления зависимостей между отдельными событиями безопасности) и особенностям реализации конечным пользователям (способ распространения, масштаб внедрения, используемая модель обслуживания).

Представленная классификация позволяет систематизировать знания в рассматриваемой предметной области и может быть использована для дальнейших исследований свойств современных систем класса SIEM и проведения их сравнительного анализа, а также при совершенствовании существующих решений и формировании требований к разрабатываемым системам управления инцидентами безопасности.

Рецензент: *Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры ИУ-8 «Информационная безопасность» МГТУ им.Н.Э.Баумана, г. Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

6 MaxPatrol SIEM. URL: https://www.ptsecurity.com/ru-ru/products/mpsiem/

7 Разработки АО «НПО «Эшелон». Комрад. URL: https://npo-echelon.ru/production/65/11174

8 OSSIM: The Open Source SIEM. URL: https://www.alienvault.com/products/ossim

9 Сравнение SIEM-систем. URL: https://www.anti-malware.ru/compare/SIEM-systems

10 Обзор мирового и российского рынка SIEM-систем 2017. URL: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem#part74

Литература

1. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд. 2012. № 5. С. 54-65.
2. Козачок А.И., Комашинский В.В., Юркин А.А. Управление информационной безопасностью : монография. – Орел : Академия ФСО России, 2013. 328 с.
3. M. Nabil, S. Soukainat, A. Lakbabi, O. Ghizlane. SIEM selection

criteria for an efficient contextual security // 2017 International Symposium on Networks, Computers and Communications (ISNCC), 2017. DOI: 10.1109/ISNCC.2017.8072035.
4. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. № 5 (24). С. 2-16. DOI: 10.21681/2311-3456-2017-5-2-16.
5. D.R. Miller, S. Harris, A.A. Harper, S. VanDyke, C. Blask. Security Information and Event Management (SIEM) Implementation. – N.Y. : McGraw-Hill, 2011. 430 p.
6. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 // Труды СПИИРАН. 2016. Вып. 49. С. 208-225. DOI: 10.15622/sp.49.11.
7. VM Cotenescu. SIEM (Security Information and Event Management Solutions) Implementations in Private or Public Clouds. J. Lee, Y.S. Kim, J.H. Kim, I.K. Kim. Toward the SIEM architecture for cloud-based security services // Naval Academy Scientific Bulletin. 2016. Volume XIX. Issue 2. DOI: 10.21279/1454-864X-16-I2-058.
8. Марков А.С., Цирлов В.Л. Структурное содержание требований информационной безопасности // Мониторинг правоприменения. 2017. № 1 (22). С. 53-61. DOI: 10.21681/2412-8163-2017-1-53-61.
9. J. Lee, Y.S. Kim, J.H. Kim, I.K. Kim. Toward the SIEM architecture for cloud-based security services // Communications and Network Security IEEE Conference, 2017. DOI: 10.1109/CNS.2017.8228696.
10. K. Kent, M. Souppaya. Guide to Computer Security Log Management // NIST Special Publication 800-92. 2006. 72 p.
11. Ершов А.Л., Карасёв С.В., Поляков С.А., Рыболовлев Д.А. Подход к формированию модели данных события информационной безопасности // Информационные системы и технологии. 2017. № 6 (104). С. 124-129.
12. Карасёв С.В., Рыболовлев Д.А. Применение методов выявления зависимостей между событиями при построении систем управления инцидентами безопасности // Информатика: проблемы, методология, технологии : материалы межд. науч. конф. (11–12 фев. 2016 г., Воронеж). Воронеж. 2016. Секция №3. С. 154–156.
13. C. Maimbo. Exploring the Applicability of SIEM Technology in IT Security : masters thesis // Auckland University of Technology, 2014. 116 p.
14. G.G. Granadillo, M. El-Barboni, H. Debar. New Types of Alert Correlation for Security Information and Event Management Systems // New Technologies, Mobility and Security IFIP International Conference, 2016. DOI: 10.1109/NTMS.2016.7792462.
15. M. Kavanagh, O. Rochford. Magic Quadrant for Security Information and Event Management // Gartner technical report. 2015. 15 p.

Рецензент: *Ершов Алексей Леонидович, кандидат технических наук, Академия ФСО России, сотрудник, г. Орел, Россия. E-mail: ershov_fman@mail.ru*

CLASSIFICATION OF MODERN SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEMS

Rybolovlev D.A.[11] , Karasev S.V.[12], Poljakov S.A.[13]

The article *suggests one of the options for the classification of Security Information and Event Management systems (SIEM) based on the analysis of the well-established scientific works and systematization of the existing views on the issues of SIEM systems construction. This analysis was carried out by studying the scientific and technical literature, including current scientific publications, review materials, detailed descriptions of architecture features and security event processing technologies used in SIEM, documentation of commercial solutions and open source projects. Among the variety of characteristics of SIEM solutions the most "salient" classification features are singled out and divided into three groups reflecting the architectural features of security information and event management systems, corresponding to the applied technologies used for processing security events and specifics of their implementation by an end-user. The proposed approach is demonstrated on the example of the classification of modern SIEM solutions of the following categories: foreign production («ArcSight ESM», «QRadar SIEM»), domestic production («MaxPatrol SIEM», «COMRAD»), open source («OSSIM»). The presented classification allows to systematize the knowledge in the subject area and it can be used in further studies of modern SIEM systems, for the conduct of a comparative analysis and the improvement of existing as well as the development of advanced security information and event management systems.*

Keywords: *security event, incident, information security management, SIEM, event correlation, classification system, classification feature*

References

1. Kotenko I.V., Sayenko I.B. SIEM-sistemy dlya upravleniya informatsiyey i sobytiyami bezopasnosti // Zashchita informatsii. Insayd. 2012. № 5. P. 54-65.
2. Kozachok A.I., Komashinskiy V.V., Yurkin A.A. Upravleniye informatsionnoy bezopasnost›yu : monografiya. – Orel : Akademiya FSO Rossii, 2013. 328 p.
3. M. Nabil, S. Soukainat, A. Lakbabi, O. Ghizlane. SIEM selection criteria for an efficient contextual security // 2017 International Symposium on Networks, Computers and Communications (ISNCC), 2017. DOI: 10.1109/ISNCC.2017.8072035.

11 Dmitry Rybolovlev, Ph.D., The Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: dmitrij-rybolovlev@yandex.ru
12 Stanislav Karasev, The Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: sats861@yandex.ru
13 Sergey Poljakov , Ph.D., The Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: ilmaglu@mail.ru

4. Kotenko I.V., Fedorchenko A.V., Sayenko I.B., Kushnerevich A.G. Tekhnologii bol›shikh dannykh dlya korrelyatsii sobytiy bezopasnosti na osnove ucheta tipov svyazey // Voprosy kiberbezopasnosti. 2017. № 5 (24). P. 2-16. DOI: 10.21681/2311-3456-2017-5-2-16.
5. D.R. Miller, S. Harris, A.A. Harper, S. VanDyke, C. Blask. Security Information and Event Management (SIEM) Implementation. – N.Y. : McGraw-Hill, 2011. 430 p.
6. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. Analiz metodov korrelyatsii sobytiy bezopasnosti v SIEM-sistemakh. Chast› 2 // Trudy SPIIRAN. 2016. Vyp. 49. P. 208-225.
DOI: 10.15622/sp.49.11.
7. VM Cotenescu. SIEM (Security Information and Event Management Solutions) Implementations in Private or Public Clouds. J. Lee, Y.S. Kim, J.H. Kim, I.K. Kim. Toward the SIEM architecture for cloud-based security services // Naval Academy Scientific Bulletin. 2016. Volume XIX. Issue 2. DOI: 10.21279/1454-864X-16-I2-058.
8. Markov A.S., Tsirlov V.L. Strukturnoye soderzhaniye trebovaniy informatsionnoy bezopasnosti // Monitoring pravoprimeneniya. 2017. № 1 (22). P. 53-61. DOI: 10.21681/2412-8163-2017-1-53-61.
9. J. Lee, Y.S. Kim, J.H. Kim, I.K. Kim. Toward the SIEM architecture for cloud-based security services // Communications and Network Security IEEE Conference, 2017.
DOI: 10.1109/CNS.2017.8228696.
10. K. Kent, M. Souppaya. Guide to Computer Security Log Management // NIST Special Publication 800-92. 2006. 72 p.
11. Yershov A.L., Karasov S.V., Polyakov S.A., Rybolovlev D.A. Podkhod k formirovaniyu modeli dannykh sobytiya informatsionnoy bezopasnosti // Informatsionnyye sistemy i tekhnologii. 2017. № 6 (104). P. 124-129.
12. Karasov S.V., Rybolovlev D.A. Primeneniye metodov vyyavleniya zavisimostey mezhdu sobytiyami pri postroyenii sistem upravleniya intsidentami bezopasnosti // Informatika: problemy, metodologiya, tekhnologii : materialy mezhd. nauch. konf. (11–12 fev. 2016 g., Voronezh). Voronezh. 2016. Sektsiya №3. P. 154–156.
13. S. Maimbo. Exploring the Applicability of SIEM Technology in IT Security : masters thesis // Auckland University of Technology, 2014. 116 p.
14. G.G. Granadillo, M. El-Barboni, H. Debar. New Types of Alert Correlation for Security Information and Event Management Systems // New Technologies, Mobility and Security IFIP International Conference, 2016. DOI: 10.1109/NTMS.2016.7792462.
15. M. Kavanagh, O. Rochford. Magic Quadrant for Security Information and Event Management // Gartner technical report. 2015. 15 p.

(Footnotes)

1 Хранилище данных CORRE, используемое в решении ArcSight ESM, реализует гибридную модель организации данных с применением реляционных и нереляционных подходов. URL: https://community.softwaregrp.com/t5/ArcSight-User-Discussions/Arcsight-Databases/td-p/1575775

2 Расширения ArcSight ESM (User & Entity Behavior Analytics, ThreatDetector и др.) в дополнение к rule-based подходу реализуют несигнатурные методы выявления зависимостей между отдельными событиями безопасности. URL: https://www.microfocus.com/media/data-sheet/arcsight_user_behavior_analytics_ds.pdf

3 Расширение IBM QRadar User Behavior Analytics реализует несигнатурные методы корреляции событий безопасности. URL: https://www.ibm.com/ru-ru/marketplace/qradar-user-behavior-analytics