DOI 10.37882/2223-2966.2023.6-2.19

СРАВНЕНИЕ ОТЕЧЕСТВЕННЫХ SIEM-СИСТЕМ МЕТОДОМ АНАЛИЗА ИЕРАРХИЙ

COMPARISON OF NATIONAL SIEM SYSTEMS BY THE METHOD OF ANALYTIC HIERARCHY PROCESS

O. Karelova
D. Sinitsyna

Summary: Abstract. This article is devoted to the issue of comparing SIEM systems of Russian production using the method of analytic hierarchy process.

Keywords: SOC, SIEM, security events management, information security, analytic hierarchy process.

Карелова Оксана Леонидовна
Доктор физико-математических наук, доцент, профессор, Московский Государственный Лингвистический Университет, Профессор, Российская академия народного хозяйства и государственной службы при Президенте РФ (Москва)
okarelova@yandex.ru
Синицына Дарья Андреевна
Московский Государственный Лингвистический Университет
sinitsyna_d@inbox.ru

Аннотация. Данная статья посвящена вопросу сравнения SIEM-систем отечественного производства методом анализа иерархий.

Ключевые слова: SOC, SIEM, управление событиями, информационная безопасность, метод анализа иерархий.

В настоящее время наблюдается появление все новых способов передачи, обработки и хранения информации, а также тренд на цифровизацию бизнес-процессов в подавляющем большинстве современных организаций. Это неизбежно приводит к разработке и применению новых методов атак на информационную инфраструктуру, как правило, с целью получения финансовой выгоды. Именно поэтому задача обеспечения информационной безопасности является одной из наиболее приоритетных для руководства организации для обеспечения непрерывности деятельности и минимизации возможных потерь в случае успешной реализации угроз информационной безопасности.

Одним из наиболее эффективных решений в данной сфере на сегодняшний день является Security Operations Center (SOC). SOC — это слаженная система, состоящая из собственной или привлеченной команды квалифицированных специалистов в области ИБ, процессов и технологий. Целью внедрения SOC в организации является осуществление мониторинга ИТ-инфраструктуры для превентивного обнаружения инцидентов кибербезопасности и их обработки. Применение данного решения позволяет централизованно управлять всей системой безопасности, что повышает эффективность уже реализованных мер (как технических, так и организационных) по противодействию угрозам ИБ.

Основным из преимуществ SOC является его гибкость, так как при его построении учитываются нужды организации с целью решения наиболее релевантных задач и выполнения поставленных целей с учетом особенностей инфраструктуры конкретной информационной системы. Эта гибкость предполагает, помимо прочего, не только различные варианты локализации функций SOC, но и возможность применения некоторого количества базовых инструментов, которые в последствии будут дополняться в рамках расширения функциональных возможностей SOC для соответствия области поставленных задач.

Одним из таких базовых инструментов является SIEM-система. SIEM (Security information and event management)-система — это система по управлению событиями информационной безопасности. К основным ее задачам относятся: сбор данных из различных источников, классификация и корреляция событий безопасности согласно установленным правилам, формирование инцидентов безопасности, визуализация результатов работы системы, оповещение ответственных лиц и так далее.

Поскольку SIEM-система является одним из ключевых элементов, на которых базируется SOC в любой организации, существует необходимость чрезвычайно внимательного подхода к выбору решения для внедрения, так как от этого напрямую зависит эффективность использования самого SOC.

В данный момент можно отчетливо наблюдать тенденцию на импортозамещение, в том числе в сфере программных решений для обеспечения информационной безопасности предприятий. Это и явилось причиной того, что для сравнения были выбраны именно отечественные SIEM-системы. Сравнение проводилось методом анализа иерархий.

Применение метода анализа иерархий подразумевает под собой оценку выбранных объектов по ряду критериев, которые являются, с точки зрения специалиста,

наиболее важными в данной ситуации. Для проведения анализа были сформулированы следующие три основные критерия, которые позволяют оценить системы:

1. Сбор событий;
2. Анализ данных;
3. Удобство использования.

MaxPatrol SIEM

1. Система собирает данные со всех IT-активов без исключения, что позволяет получить наиболее детальную картину о состоянии информационной инфраструктуры в организации в любой момент времени. В MaxPatrol SIEM реализована возможность отслеживания источников данных с учетом типичной для них активности для выявления нестандартных сценариев поведения (таких как, например, задержка получения данных о событиях) для конкретного источника в целях своевременного реагирования.
2. Для системы на регулярной основе выпускаются пакеты экспертизы, то есть наборы новых правил корреляции событий для выявления атак, индикаторов компрометации, информации о возможных техниках злоумышленника и так далее. Пакеты разрабатываются в соответствии с наиболее релевантными исследованиями специалистов Positive technologies, что способствует повышению эффективности работы системы. Также с помощью данных пакетов можно адаптировать продукт под нужды конкретной организации, делая SIEM-систему гибкой (важность чего была подчеркнута выше). В системе реализован функционал ретроспективного анализа, то есть у специалистов есть возможность заново проверить поступившие ранее события с использованием обновленных правил корреляции или применением новых индикаторов. Правила корреляции могут быть установлены из пакетов или быть созданы самостоятельно с помощью конструктора.
3. В рамках отслеживания актуального состояния инфраструктуры в системе используются дашборды, на которых отображается вся ключевая информация об обнаруженных событиях, уязвимостях, инцидентах, проведенных проверках и так далее. Дашборды можно формировать самостоятельно, выбрав виджеты из предложенных или создавая новые под конкретные задачи. MaxPatrol SIEM отличается наглядной визуализацией всех процессов, позволяющей лучше понимать состояние защищенности системы [1].

Ankey SIEM

1. Система может быть интегрирована с любыми источниками данных, в качестве источников событий могут служить: инфраструктурные сервисы и ПО, операционные системы, средства защиты информации, гипервизоры и так далее. Сбор, фильтрация, категорирование полученных данных о событиях автоматизированы, а доступ к ним осуществляется посредством единой консоли. Поддерживается интеграция с различными ИТ-сервисами, такими как кадровые системы, бизнес-аналитика и так далее.
2. Сервер корреляции входит в базовый состав программного комплекса Ankey SIEM и реализует функции по анализу и управлению событиями с последующим направлением результатов администратору. Также есть возможность подключения дополнительного компонента в виде сервера аналитики, который используется для выявления нетипичных закономерностей и сценариев поведения пользователей.
3. Одним из главных преимуществ установки данной SIEM-системы является наличие трёх возможных вариантов инсталляции: базовой (до 1000 событий в секунду), расширенной (до 5000 событий в секунду) и высокопроизводительной (более 5000 событий в секунду). Это позволяет подстроить систему под вычислительные ресурсы конкретной организации, а также адаптировать ее под масштабы и прочие индивидуальные характеристики информационной инфраструктуры. Ankey SIEM может быть развернута как на выделенной аппаратной платформе, так и в виртуальной среде. Обеспечивается наличие различных форматов представления данных аналитики в виде дашбордов, интерактивных отчетов, сводных таблиц, графиков различного вида с инструментами фильтрации [2].

СёрчИнформ SIEM

1. Сбор данных происходит из большого количества различных программных и аппаратных источников, поддерживается коннекторами, список которых постоянно пополняется. Примерами таких коннекторов могут служить, например, DrWebConnector (работа с базами данных DrWeb) и 1CConnector (работа с журналами 1С). Список коннекторов на данный момент уже является довольно большим и позволяет сделать вывод о возможности охвата системой событий из большинства наиболее популярных, как минимум на отечественном рынке, продуктов для реализации бизнес-процессов.
2. Анализ событий и формирование из них инцидентов происходит в соответствии с определенными правилами. В системе представлено около 300 уже существующих правил корреляции, также можно добавлять собственные с помощью специального редактора. Система автоматически оповещает ответственные лица при обнаружении

возможных нарушений безопасности и предоставляет всю необходимую информацию об обнаруженном событии.

3. Система предоставляет возможность создания карты инцидентов, формирования интерактивных отчетов и настройки дашбордов, экспорт отчетов реализован в нескольких возможных форматах. СёрчИнформ SIEM заявлена достаточно простым и понятным в использовании инструментом [3].

KOMRAD Enterprise SIEM

1. Сбор информации о событиях ИБ осуществляется по шести различным протоколам, система приводит события к одинаковой внутренней структуре и автоматически их индексирует. Поддерживается большое количество отечественных СЗИ и интеграция с внешними системами.
2. В KOMRAD Enterprise SIEM реализован широкий функционал для работы с полученными данными, он включает в себя наличие предустановленных правил корреляции, виджетов для визуального анализа, конструктора для правил фильтрации событий, инструментов для агрегации инцидентов и управления инцидентами ИБ. При рассмотрении конкретного инцидента можно получить доступ к истории генерации инцидента. Для системы также выпускаются пакеты экспертиз, что позволяет эффективнее работать с наиболее актуальными угрозами информационной безопасности.
3. Данные по событиям отображаются в виде различных диаграмм, есть возможность создания дашбордов для управления активами и формирование отчетов. Заявлено, что при установке системы предъявляются низкие требования к аппаратному обеспечению [4].

После изучения приведенных выше характеристик четырех наиболее известных и распространенных отечественных SIEM-систем, а также применения метода анализа иерархий были получены следующие результаты:

Таблица 1.

Присвоение рангов критериям

Критерии		Ранги
К1	Сбор событий	2
К2	Анализ данных	1
К3	Удобство использования	3

Таблица 2.

Присвоение исследуемым объектам рангов

		К1	К2	К3
А1	MaxPatrol SIEM	2	1	3
А2	Ankey SIEM	1	3	1
А3	СёрчИнформ SIEM	3	4	2
А4	KOMRAD Enterprise SIEM	4	2	4

Таблица 3.

Матрица сравнений для критериев

	К1	К2	К3	∑	a — вектор приоритетов
К1	1	0,50	2	3,5	0,308823529
К2	2	1	3	6	0,529411765
К3	0,5	0,33	1	1,83	0,161764706
S	3,5	1,83	6	11,33	

Таблица 4.

Матрица сравнений для альтернатив по критерию 1

	А1	А2	А3	А4	∑	b_1 — вектор приоритетов
А1	1	0,5	2	3	6,5	0,289963
А2	2	1	3	4	10	0,446097
А3	0,5	0,33	1	2	3,83	0,171004
А4	0,33	0,25	0,5	1	2,08	0,092937
S	3,83	2,08	6,5	10	22,42	

Аналогично были получены векторы приоритетов альтернатив по каждому из критериев:

Таблица 5.

Векторы приоритетов альтернатив по критериям 2 и 3

b_2	b_3
0,446097	0,171004
0,171004	0,446097
0,092937	0,289963
0,289963	0,092937

Таблица 6.

Итоговая таблица

a	0,3088235	0,529412	0,161765	Приоритет
А1	0,2899628	0,446097	0,171004	0,3533785
А2	0,4460967	0,171004	0,446097	0,3004592
А3	0,1710037	0,092937	0,289963	0,1489176
А4	0,0929368	0,289963	0,092937	0,1972447

Таким образом, по итоговой таблице можно видеть, что приоритетным выбором исходя из сформулированных критериев и оценок, поставленных каждой из представленных систем, является MaxPatrol SIEM.

Необходимо заметить, что в данном случае анализ SIEM-систем носит субъективный характер, так как все оценки и ранги присваивались исходя из личных соображений о важности отдельных факторов для эффективной работы SIEM-системы в организации.

ЛИТЕРАТУРА

1. MaxPatrol SIEM. — Текст: электронный // Positive Technologies: [сайт]. URL: https://www.ptsecurity.com/ru-ru/products/mpsiem/ (дата обращения: 13.02.2023).
2. Ankey SIEM. — Текст: электронный // GIS Газинформсервис : [сайт]. URL: https://www.gaz-is.ru/produkty/upravlenie-ib/ankey-siem.html (дата обращения: 13.02.2023).
3. СёрчИнформ SIEM. — Текст: электронный // SearchInform: [сайт]. URL: https://searchinform.ru/products/siem/ (дата обращения: 13.02.2023).
4. KOMRAD Enterprise SIEM. — Текст: электронный // Эшелон: [сайт]. URL: https://npo-echelon.ru/production/65/11793 (дата обращения: 13.02.2023).
5. Комаров, А.Н. АНАЛИЗ И МОНИТОРИНГ СЕТИ ПРЕДПРИЯТИЯ В РЕАЛЬНОМ ВРЕМЕНИ // Кронос: естественные и технические науки. 2020. № 4 (32). С. 12–14.
6. Кириллов, В.А. СИСТЕМА СБОРА И КОРРЕЛЯЦИИ СОБЫТИЙ (SIEM) КАК ЯДРО СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ // Вестник технологического университета. 2016. Т. 19, № 13. С. 132–134.
7. Рыболовлев, Д.И., Карасёв С.В., Поляков С.А. Классификация современных систем управления инцидентами безопасности // Вопросы кибербезопасности. 2018. № 3(27). С. 47–52.

Журнал «Современная наука: актуальные проблемы теории и практики»