DOI: 10.47026/1810-1909-2024-4-60-74
УДК 519.876.5:004.056
ББК В182:А68

М.М. МУНТЯН, И.Г. СИДОРКИНА

СПОСОБ ИНТЕГРАЦИИ ВСПОМОГАТЕЛЬНОГО МОДУЛЯ С SIEM-СИСТЕМАМИ

Ключевые слова: *информационная безопасность, SIEM, промежуточное программное обеспечение, мониторинг событий, разработка программного обеспечения, микросервисы.*

На сегодняшний день одним из популярных способов обеспечения безопасности информации является использование систем типа SIEM, позволяющих собирать и обрабатывать большой объем данных о защищаемой инфраструктуре посредством определения зависимостей между возникающими событиями безопасности. В связи с этим актуальными являются исследования способов повышения эффективности использования систем такого типа, которые связаны с модернизацией инфраструктуры и разработкой новых алгоритмов осуществления ее мониторинга.

Цели исследования *– повышение уровня автоматизации принятия решения SIEM и эффективности критичных параметров информационной безопасности: скорости анализа поступающих событий и принятия решений, нагрузки на ресурсы обеспечения информационной безопасности в защищаемой инфраструктуре, качества системы защиты при эшелонировании функционала SIEM в небольшие локально-сетевые «представительства».*

Материалы и методы. *В качестве объекта исследования рассмотрен процесс функционирования SIEM, эффективность которого не достигает оптимального для решения поставленного перед системами такого типа значения. Использованы методы классического анализа для определения важных аспектов и этапов процесса функционирования SIEM, методы математического моделирования для проведения аналитических расчетов увеличения эффективности построения взаимодействия «SIEM – защищаемая инфраструктура», методы сравнительного анализа при определении преимуществ и недостатков использования актуальных на сегодняшний день архитектур по разработке программного обеспечения, методы синтеза для определения применимости методов интеллектуального анализа как средства расширения получаемой для вычисления корреляции событий безопасности информации.*

Результаты. *По результатам исследования была предложена новая архитектура защищаемой инфраструктуры для реализации взаимодействия «SIEM – инфраструктура», основанного на децентрализации процессов сбора и предобработки информации за счет делегирования функциональных возможностей SIEM программной платформе. Были определены структурные особенности при реализации программной платформы, а также состав ее базового функционала. Также по результатам сравнительного анализа монолитного, сервис-ориентированного и микросервисного подхода был определен наиболее предпочтительный способ реализации предлагаемой программной платформы, а также представлен перечень расширенного функционала с учетом необходимости использования методов интеллектуального анализа информации для повышения функционирования SIEM.*

Выводы. *Использование предлагаемого решения повышает производительность SIEM-систем при реализации таких этапов, как сбор и предобработка информации, расширяет возможности специалистов по информационной безопасности благодаря получению новых коррелируемых данных за счет использования интеллектуальных методов анализа, а также позволяет перейти от централизованной реализации процесса защиты к децентрализованному. Реализация программной платформы на основе сервис-ориентированного подхода дает возможность повысить уровень интеграции системы и ее отказоустойчивость. Помимо этого, использование предлагаемой платформы совместно с SIEM-системами второго поколения позволяет получить альтернативную оценку о состоянии инфраструктуры, что свидетельствует о возможности повышения точности принятия решений.*

Введение. В настоящее время для обеспечения информационной безопасности часто используется технология SIEM (Security Information and Event Management), которая включает в себя: SIM (Security Information Management) – управление информационной безопасностью; SEM (Security Event Management) – управление событиями безопасности. Несмотря на это, исследования, направленные на поиск способов повышения эффективности систем, основанных на SIEM, продолжаются и являются достаточно актуальными для сферы информационной безопасности.

Функционирование таких систем подробно описано в [1, 11]. На основе данных, приводимых разработчиками компании Security Vission, можно выделить следующие этапы работы SIEM: 1) сбор информации о защищаемой инфраструктуре; 2) проведение процедур нормализации и таксономии; 3) вычисление корреляции; 4) накопление информации о событиях безопасности [1]. Схожее, но несколько сокращенное, описание функционирования такой системы приводит Е.А. Мельников, который в качестве главных этапов выделил только три – нормализацию событий безопасности, агрегирование событий и их фильтрацию [1]. При взаимодействии «SIEM – инфраструктура» выделяют активный и пассивный сбор информации от средств защиты информации и коммутирующего оборудования [11]. Под активным сбором понимается ситуация, когда данные передаются по инициативе источника (средства защиты информации или коммутирующего оборудования), под пассивным – ситуация, когда запрос на получение данных формируется самой системой [11].

Пример программно-аппаратной реализации SIEM-системы в практику управления информационной безопасностью экономической деятельности представлен в работе [2]. Авторы предложили схему внутренней программно-аппаратной структуры типовой архитектуры SIEM, в которой выделены такие компоненты, как собирающее и обрабатывающее программное обеспечение, реализованное в виде сервера и выполняющее функции «коллектора» и коррелятора, связующее программное обеспечение «SIEM – сервер», обеспечивающее распределенный доступ к проанализированным и собранным данным, а также к клиентским приложениям, расположенным на рабочей станции [2].

В статье [3] предложен метод интеграции SIEM с дополнительным модулем (вспомогательным модулем для SIEM) посредством использования принципа промежуточного программного обеспечения. Ранее нами был предложен метод интеграции SIEM с дополнительным (вспомогательным для SIEM) модулем, который основан на использовании принципа промежуточного программного обеспечения, позволяющего повысить эффективность функционирования SIEM за счет совершенствования метода анализа и сбора информации, использования методов интеллектуального анализа для расширения получаемых при вычислении корреляции событий безопасности данных, а также который определяет размещение элементов в защищаемой инфраструктуре. Исходя из этого, возникает необходимость в проведении модификации самой защищаемой инфраструктуры и создании новых способов межпрограммного взаимодействия «SIEM – защищаемая инфраструктура».

Принцип промежуточного программного обеспечения [4], используемый для интеграции разнородных компонентов цельного программного продукта, описывается также и в ряде других работ. Так, И.С. Чернядьев с соавт. предлагают использование таких способов интеграции, как API (при организации взаимодействия различных программных компонентов) и Web-сервисы (при построении Интернет-взаимодействия) [4].

Для практической (программной) реализации таких систем используются три подхода: монолитная разработка (разработка с общей кодовой базой); сервис-ориентированная разработка (разработка с распределением на функциональные блоки меньшего размера, не обладающие общей кодовой базой); микросервисная разработка (деление функциональных блоков на основе решения ими мелких, более неделимых задач) [5–8]. Тестирование систем информационной безопасности может быть реализовано на основе методов искусственного интеллекта и машинного обучения, которые используются для обнаружения аномалий больших объемов данных, поиска шаблонов реализации киберугроз и уязвимостей информационной безопасности, а также построения их прогностических зависимостей на основе исторических данных [9]. Интеллектуальный анализ данных также может использоваться для автоматизации оценки событий безопасности для объектов критической информационной инфраструктуры с использованием технологий семантического анализа их текстового описания [10].

Цели исследования – повышение уровня автоматизации принятия решения SIEM и эффективности критичных параметров информационной безопасности: скорости анализа поступающих событий и принятия решений, нагрузки на ресурсы обеспечения информационной безопасности в защищаемой инфраструктуре, качества системы защиты при эшелонировании функционала SIEM в небольшие локально-сетевые «представительства».

Материалы и методы. Исследование модернизации защищаемой инфраструктуры проводилось на основе детального анализа типового процесса функционирования SIEM-систем: анализа этапа сбора и предобработки информации, анализа этапа корреляции.

Для определения возможности создания нового алгоритма организации взаимодействия SIEM были проанализированы возможность использования комбинированного способа сбора информации (активно-пассивный метод), а также преимущества делегирования обязанностей SIEM по предобработке информации во вспомогательный модуль.

Для расчета эффективности предлагаемого способа сбора информации были использованы результаты аналитических расчетов с учетом применения принципов параллельных вычислений при помощи формул оценки оптимального количества потоков

$$p_{opt} = \frac{1}{1-f}$$

и закона Амдала

$$S(p) = \frac{1}{(1-f) + \frac{f}{p}},$$

где f – процент решаемой задачи, который может быть представлен параллельными вычислениями; p – оптимальное количество используемых потоков.

Исследование рационализации ресурсов сетевой инфраструктуры было проведено путем логических заключений об объеме циркулирующего в инфраструктуре трафика.

Выбор предпочтительного подхода к реализации программного обеспечения был получен путем осуществления сравнительного анализа приводимых в [6–9] подходов к разработке программного обеспечения, критериями которого стали: независимость и гибкость, функциональная избыточность, отказоустойчивость, уровень интеграции, масштабирование разработки, компактность получаемого решения. Предлагаемое решение должно быть реализовано в рамках единой платформы в виде двух крупных функциональных блоков, состав которых был представлен выше. Функционал программного агента должен быть компактен, вследствие чего следует избегать излишней программной избыточности. Реализация платформы как буферной зоны требует высокого уровня интеграции для возможности ее встраивания в инфраструктуру, в которой уже функционирует SIEM.

Результаты исследования

Анализ способов взаимодействия вспомогательного модуля и SIEM. В результате анализа процесса функционирования SIEM, приведенного в [1, 11], было определено, что для интеграции SIEM и вспомогательного модуля необходим новый способ организации взаимодействия между ними. Для этого предлагается произвести преобразование предполагаемой защищаемой инфраструктуры путем выделения в ней такого элемента, как представительство SIEM, под которым будем понимать некий программный агент вспомогательного модуля, установленного на логической границе небольшого логического сегмента инфраструктуры. Исходя из этого, выделим следующие изменения инфраструктуры:

1) процесс сбора информации непосредственно SIEM должен быть направлен на взаимодействие с программным агентом вспомогательного модуля;

2) установление гибридного процесса сбора информации должно осуществляться по следующим правилам:

– сбор информации в границах сегмента делегирован представительству SIEM (программному агенту вспомогательного модуля) и осуществляется последним на основе активного и пассивного способа;

– сбор информации об инфраструктуре преобразовывается в активный для передачи информации от представительства в SIEM и пассивный при необходимости уточнения информации непосредственно для корреляции в SIEM;

3) эшелонирование SIEM должно быть реализовано за счет создания звена предобработки и фильтрации информации (представительства SIEM).

Кроме этого, требуется перераспределение функциональных возможностей из-за модификации процесса взаимодействия, при этом необходимо реализовать:

– делегирование возможностей предобработки информации из SIEM в программный агент (проведение нормализации, таксономии и фильтрации информации);

– обмен информацией не только между программным агентом и SIEM, но и программным агентом и аналитическим компонентом вспомогательного модуля;

– механизмы преобразования форматов для нормализованного представления в SIEM, таксономии и фильтрации событий информационной безопасности (сокращение данных анализа);

– механизм проведения инвентаризации IT-активов и их уязвимостей (расширение параметров информационной безопасности).

Преимущество такой организации взаимодействия «SIEM – вспомогательный модуль – защищаемая инфраструктура» заключается в децентрализации процесса сбора и предобработки информации, рационализации использования ресурсов инфраструктуры, фокусировании мощности SIEM на реализации процедуры корреляции:

Децентрализация сбора и предобработки информации позволит производить сбор информации частично параллельно без усложнения программной организации вспомогательного модуля и SIEM, так как реализация промежуточного звена в виде программного агента позволяет сократить общее количество запросов «коллектора» SIEM (при необходимости) до k (где k – количество групп сегментации). При этом правильный подбор количества элементов сегмента также позволит ускорить процесс сбора информации за счет параллельности, так как сегменты независимы друг от друга и не пересекаются.

Для количественного представления преимуществ децентрализации воспользуемся математическим представлением процесса сбора информации. Примем за константы положения о времени и скорости проведения операции сбора для процесса в условиях сегментации и без сегментации и обозначим общее число узлов как N. Тогда для опроса и сбора log-файлов с N устройств потребуется N последовательных запросов. В то же время для реализации этого процесса в условиях сегментации введем обозначение для количества элементов группы сегментации n. Таким образом, количество последовательных запросов будет снижено до N/n, что равносильно количеству запросов ко всем программным агентам, а запросы внутри группы возможно осуществить параллельно. Определим количество необходимых операций для $N = 1\,000$ и $n = 50$. Тогда без применения параллельности количество последовательных операций при $N = 1\,000$ будет равняться самому числу N. При этом при использовании сегментации $n = 50$ общее количество операций будет представляться как сумма количества сегментов ($1\,000 / 50 = 20$) и количества операций внутри сегмента ($n = 50$). Таким образом, общее количество последовательных операций при неизменности времени их исполнения для случаев сегментации составляет 70, т.е. 0,07% от числа операций при последовательных запросах. Однако на практике осуществление запросов будет неравномерным относительно времени их исполнения. Поэтому фактические результаты могут быть получены только в результате эксперимента, который будет проведен в дальнейших исследованиях. При этом при использовании параллельного способа вычислений число фактических операций также может быть снижено, а производительность получения результатов относительно последовательных запросов на уровне сегмента увеличена.

Для проведения расчетов произведено разбиение задачи на подзадачи с определением возможности организации параллельности при их решении. Для реализации операции сбора информации необходимо выполнить следующие этапы:

– сформировать запрос к необходимому узлу сети (имеет возможность параллельной реализации);

– выполнить запрос (имеет возможность параллельной реализации);

– произвести поиск и считывание информации в рамках запроса (в рамках запроса нельзя организовать дополнительную параллельность на узле сети для выполняемых действий);

– получить ответ запроса (имеет возможность параллельной реализации);

– произвести агрегирование ответа (имеет возможность параллельной реализации).

С учетом результатов оценки возможности параллельной реализации оптимальное количество потоков для рассмотренной задачи будет равно

$$p_{opt} = \frac{1}{1 - 0{,}8} = 5.$$

Подставив это значение в формулу Амдала, получим

$$\mathrm{S}(p) = \frac{1}{(1 - 0{,}8) + \frac{0{,}8}{5}} \approx 2{,}78.$$

Использование параллельных вычислений позволяет добиться ряда преимуществ. Во-первых, рационализируется использование ресурсов инфраструктуры: сокращается время реакции сетевой инфраструктуры за счет децентрализации процессов сбора и предобработки информации; повышается пропускная способность канала связи, так как снижается загруженность коммутирующего оборудования и иных сетевых устройств для общего обмена сообщениями. Во-вторых, вследствие того, что предобработка и сбор информации осуществляются в программных агентах сегмента инфраструктуры, а информация, поступающая на вход SIEM, является уже нормализованной и структурированной, то основная задача SIEM в этом случае заключается в выявлении закономерностей и зависимостей между поступающими событиями, что позволяет сократить время анализа поступивших данных.

Таким образом, предлагаемый способ построения взаимодействия «SIEM – вспомогательный модуль – защищаемая инфраструктура» позволяет снизить общее число операций по сбору информации об инфраструктуре, что, в свою очередь, способствует снижению времени, необходимого на подготовку данных для анализа, и повышению скорости самого анализа. Дополнительным свойством реализации является снижение нагрузки на сетевую инфраструктуру, что ведет к улучшению основных характеристик компьютерной сети: времени реакции и пропускной способности канала связи.

Адаптация схемы интеграции вспомогательного модуля на основе концепции промежуточного программного обеспечения. Для раскрытия концепции промежуточного программного обеспечения при их интеграции

с SIEM воспользуемся определением, предлагаемым в [12]: промежуточное программное обеспечение – программное обеспечение, используемое различными приложениями для взаимодействия друг с другом. Исходя из этого определения предлагаемый вспомогательный модуль должен быть реализован в виде платформы, которая обладает инструментарием для таксономии и нормализации поступающих данных, а также набором интеллектуальных возможностей их дополнительной обработки для последующей передачи в SIEM. Реализация такой платформы может быть осуществлена по аналогии с облачными сервисами типа AWS, предлагающими среду разработки для любого языка программирования, например, при помощи интерфейсов прикладного программного обеспечения (API) [4].

Данная платформа должна содержать в себе сразу несколько разнонаправленных модулей: детектирования и нормализации, таксономии, формализации, интеллектуального анализа собранных данных. При этом целесообразно распределенное размещение этих модулей в защищаемой инфраструктуре.

Принимая во внимание необходимость учета состояния экосреды функционирования программного модуля, также произведем разделение модулей между программным агентом и аналитическим модулем. Модуль детектирования и нормализации, а также модуль таксономии должны быть реализованы на каждом программном агенте для возможности организации предлагаемого способа децентрализации сбора и предобработки информации. При этом, как отмечалось выше, должна быть организована как внутренняя, так и внешняя коммуникация этих модулей (возможность обмена информацией как с аналитическим модулем платформы, так и с SIEM). Модули формализации и интеллектуального анализа собранных данных должны составлять структуру аналитического модуля платформы и реализовывать функционал по пополнению данных о коррелируемых событиях путем формирования новых кластеров угроз/уязвимостей, а также представлять прогностическую информацию о потенциальном развитии инцидентов.

Таким образом, в результате адаптации схемы интеграции для реализации предлагаемого вспомогательного модуля он (вспомогательный модуль) должен быть реализован в виде программной платформы, выполняющей функции буферной зоны между SIEM и защищаемой инфраструктурой. Назначение такой зоны заключается в повышении производительности и расширении поступающего в SIEM объема предобработанной информации.

«Коммуникативные» возможности вспомогательного модуля. Основываясь на результатах, описывающих способ построения взаимодействия между элементами вспомогательного модуля и SIEM-системы, обязательным является реализация следующих функций:

1) в программном агенте:
- параллельный сбор информации;
- нормализация собранных данных (приведение форматов);
- таксономия собранных данных;
- организация взаимодействия с SIEM;
- организация внутреннего взаимодействия в рамках платформы;

– обработка запросов SIEM;

2) в аналитическом компоненте:

– формализация собранных данных;

– вычисление корреляции;

– обновление правил корреляции на основе решения задачи классификации на основе корреляции;

– формирование новых кластеров угроз/уязвимостей на основе корреляции;

– дополнение информации о событиях безопасности на основе формирования прогнозов развития компьютерных инцидентов;

– организация взаимодействия с SIEM;

– организация внутреннего взаимодействия в рамках платформы.

Выбор направления реализации вспомогательного модуля в рамках современных подходов к разработке программного обеспечения. Основываясь на современных тенденциях разработки программного обеспечения, можно выделить две архитектуры: монолитную и сервис-ориентированную. Монолитной называют традиционную архитектуру, которая основана на разработке программного обеспечения, имеющего общее кодовое пространство (общую базу кода), которая сочетает в себе реализацию в одной программе нескольких крупных функций. Главный аспект такого подхода заключается в наличии взаимосвязанности модулей программного обеспечения из-за встроенных механизмов обмена данными.

Сервис-ориентированная архитектура, напротив, базируется на том, что цельный проект разбивается на небольшие компоненты, которые осуществляют взаимодействие друг с другом на основе запросов. Особенностью такой разработки является независимость компонентов такой архитектуры друг от друга, что значительно упрощает процесс их модернизации. В рамках архитектуры такого типа отдельно выделяют микросервисы (MSA – Micro Service Architecture), сконцентрированные на решении небольшой задачи.

Сравнительный анализ аспектов трех рассмотренных выше архитектур разработки программного обеспечения при их использовании для реализации вспомогательного модуля приведен в таблице [5–8].

Сравнение подходов к разработке программного обеспечения

Критерий сравнения	**Подход**		
	монолитный	**сервис-ориентированный**	**MSA**
Независимость и гибкость	Программные модули являются сильно связанными для реализации в рамках одной платформы	Позволяет организовать независимость модулей в рамках платформы	Позволяет организовать независимость модулей в рамках платформы
Избыточность функционала	Избыточность функционала отсутствует	Средний уровень избыточности функционала вследствие отсутствия необходимости частого обмена данными	Высокий уровень избыточности функционала вследствие потребности в постоянном обмене данными между микросервисами

Окончание таблицы

Критерий сравнения	Подход		
	монолитный	сервис-ориентированный	MSA
Отказоустойчивость	Низкий уровень отказоустойчивости вследствие свойства архитектуры – общая база кода	Высокий уровень отказоустойчивости вследствие наличия независимости между модулями	Высокий уровень отказоустойчивости вследствие наличия независимости между модулями
Уровень интеграции	Низкий уровень интеграции, внедрение изменений требует изменения многих связанных друг с другом элементов	Высокий уровень интеграции вследствие независимости сервисов друг от друга	Высокий уровень интеграции вследствие независимости сервисов друг от друга
Масштабирование разработки	Масштабирование в рамках разработки требует изменения многих связанных друг с другом элементов	Средний уровень масштабирования разработки вследствие концентрации программных модулей на реализации функции	Высокий уровень масштабирования вследствие концентрации программных модулей на реализации небольшой задачи
Компактность	Низкий уровень компактности вследствие большого количества связей между блоками	Средний уровень компактности вследствие частичного дублирования функционала	Низкий уровень компактности вследствие большого количества дублирования функционала

Таким образом, для реализации предлагаемого решения наиболее подходящей является сервис-ориентированная архитектура, что объясняется необходимостью использования двух независимых блоков, способных осуществлять обмен информации как друг с другом, так и с SIEM. Монолитный подход к разработке программного обеспечения при таких условиях становится неэффективным. При этом MSA также не подходит, так как добавляет излишнюю программную избыточность, что значительно увеличивает «размер» программного агента, а значит, накладывает дополнительные аппаратные требования для его реализации.

Функционал компонентов вспомогательного модуля при проведении интеграции с SIEM. Обратимся к схеме из работы [3] (рис. 1). Из рис. 1 следует, что для получения собранных программными агентами данных SIEM и аналитический модуль должны обратиться к серверу.

При обычном функционировании SIEM сервер получает данные в двух случаях: если данные уже прошли корреляцию и были отправлены на хранение или если SIEM не смогла обработать событие в данный момент (производилась обработка других, поступивших ранее, событий).

При использовании гибридного решения SIEM приобретает возможность производить дополнительную обработку еще не обработанных, «сырых» данных, в том числе при помощи методов интеллектуального анализа.

Основываясь на предложенном способе организации взаимодействия SIEM со вспомогательным модулем, реализованного в виде программной платформы, изменим схему, предложенную в [3], и функционал компонентов вспомогательного модуля.

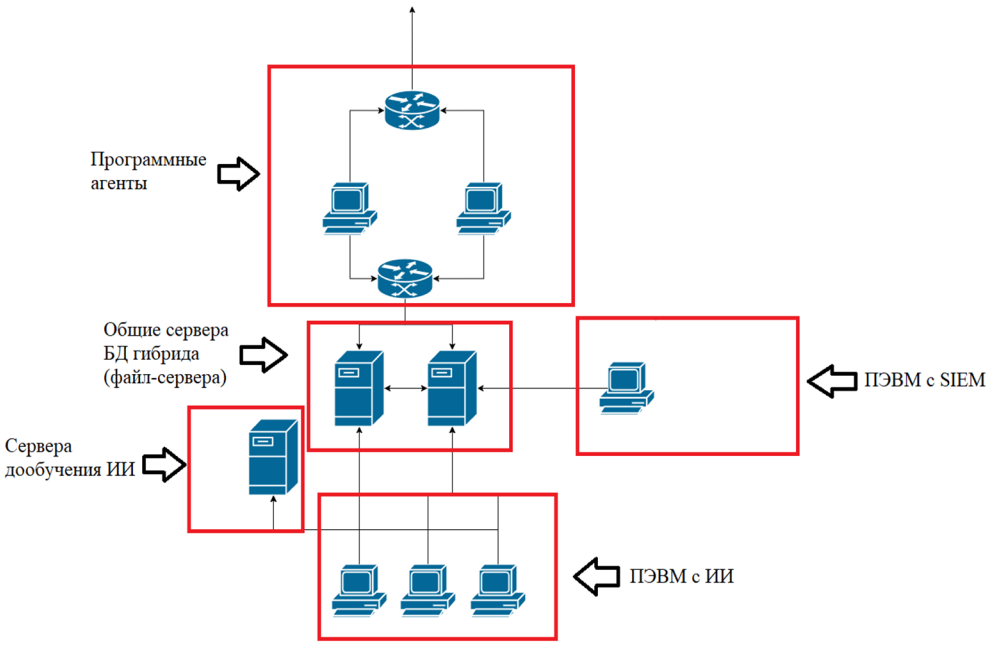

Рис. 1. Схема гибридного решения [3]

В рамках реализации платформы (вспомогательного модуля) после сбора информации программными агентами о своей инфраструктуре при выявлении «подозрительных» событий информационной безопасности информация от программных агентов направляется в аналитический модуль (обмен данными внутри платформы), SIEM (внешний обмен данных) и на сервер (в ситуации, когда один из предыдущих адресатов занят обработкой предыдущего запроса).

При возникновении события только в одном из сегментов и их поступлении в SIEM последняя формирует запрос к другим сегментам для проверки возникновения похожих инцидентов и продолжает вычисление корреляции поступивших событий. Другие программные агенты производят сбор информации на основе предоставленных SIEM запросов и направляют информацию также в SIEM и на сервер, если в данный момент SIEM занята. По мере готовности SIEM и программный агент производят запрос к серверу для получения новых данных. По достижении итогов вычисления корреляции текущих событий SIEM производит передачу информации на сервер и в аналитический модуль. Таким образом, новая схема взаимодействия имеет вид, представленный на рис. 2.

В качестве результата предлагаемых корректировок выделим функционал каждого элемента вспомогательного модуля:

1) в программном агенте:
- осуществление параллельного сбора информации;
- нормализация собранных данных (приведение форматов);
- таксономия собранных данных;
- организация взаимодействия с SIEM;

– организация внутреннего взаимодействия в рамках платформы;
– обработка запросов SIEM;
– обработка исключений;
– обработка нештатных ситуаций;
2) в аналитическом компоненте:
– формализация собранных данных;
– осуществление корреляции;
– обновление правил корреляции на основе решения задачи классификации на основе корреляции;
– формирование новых кластеров угроз/уязвимостей на основе корреляции;
– дополнение информации о событиях безопасности на основе формирования прогнозов развития компьютерных инцидентов;
– организация взаимодействия с SIEM;
– организация внутреннего взаимодействия в рамках платформы;
– функционал разработки стратегии для локализации и нивелирования инцидента информационной безопасности;
– обработка исключений;
– обработка нештатных ситуаций.

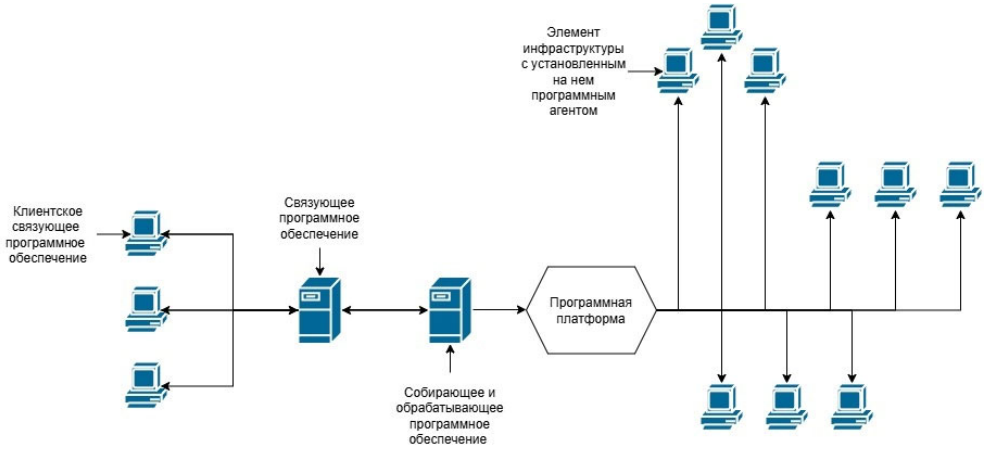

Рис. 2. Измененная схема гибридного решения

Предложенный функционал позволяет определить структурный состав программных модулей предлагаемого решения. Реализация предлагаемого функционала позволит достичь большей точности в процессе принятия решений, что в первую очередь окажет положительное влияние на качество обеспечения безопасности информации в инфраструктуре. Такое утверждение основано на получении дополнительных аналитических данных, основанных на применении методов интеллектуального анализа информации, реализуемых в программных модулях аналитического блока за счет применения методов классификации, кластеризации и прогнозирования [9]. Использование последнего также позволяет дать количественную оценку вероятности наступления

и тяжести тех или иных последствий при помощи математики вероятностей [9]. Тем не менее предлагаемый перечень функций является проектным, на этапе реализации он может быть скорректирован или дополнен новыми.

Выводы. Предложен новый способ интеграции вспомогательного модуля с SIEM, особенностями которого являются следующие:

– вспомогательный модуль предлагается реализовать в виде программной платформы, назначение которой – создание буферной зоны между защищаемой инфраструктурой и SIEM, которая позволяет произвести эшелонирование системы сбора и обработки событий безопасности;

– предлагаемый способ организации взаимодействия позволяет повысить производительность процесса сбора и предобработки информации о защищаемой инфраструктуре, а также общую сетевую нагрузку;

– предложение децентрализации функций SIEM путем делегирования части из них в программные агенты позволяет сконцентрировать все мощности системы анализа рисков информационной безопасности на ее основной функции – корреляции событий безопасности информации;

– реализация платформы на основе сервис-ориентированного подхода позволяет создать независимость между функционалом по сбору и предобработке информации, что ведет к повышению отказоустойчивости системы защиты информации;

– применение интеллектуальных методов анализа направлено на расширение возможностей специалистов по информационной безопасности в части предоставления им количественной оценки вероятности наступления и тяжести прогнозируемых событий;

– использование предлагаемой платформы для SIEM систем высокого порядка (SIEM с использованием интеллектуальных методов) дает возможность получить дополнительную (альтернативную) оценку состояния защищенности инфраструктуры, что позволяет повысить точность принятия решений.

Литература

1. *Мельников Е.А.* Типовые схемы взаимодействия в системах сбора и анализа событий информационной безопасности SIEM // Электронный научный журнал. 2020. № 3(32). С. 21–24.

2. *Сизов В.А., Киров А.Д.* Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности // Открытое образование. 2020. Т. 1, № 24. С. 69–79.

3. *Мунтян М.М., Сидоркина И.Г.* Метод интеграции вспомогательного модуля в существующие SIEM-системы // Инженерные кадры – будущее инновационной экономики России: материалы IX Всерос. студ. конф., Йошкар-Ола, 7–10 ноября 2023 г. Йошкар-Ола, 2023. С. 567–572.

4. *Чернядьев И.С., Хамидуллин М.Р.* Способы интеграции программного обеспечения: API, Веб-сервисы и промежуточное программное обеспечение // Школа молодых новаторов: сб. науч. ст. 5-й Междунар. науч. конф. перспективных разработок молодых ученых: в 3 т. Курск: Университетская книга, 2024. С. 266–270.

5. Просто о микросервисах [Электронный ресурс]. URL: https://habr.com/ru/companies/raiffeisenbank/articles/346380/ (дата обращения 17.09.2024).

6. В чем разница между SOA и микросервисами [Электронный ресурс]. URL: https://aws.amazon.com/ru/compare/the-difference-between-soa-microservices/ (дата обращения 17.09.2024).

7. Основные протоколы интеграции приложений [Электронный ресурс]. URL: https://dynamicsun.ru/blog/protokoli-inteegrasii-prilozheniy.html (дата обращения 17.09.2024).

8. Интеграция программного обеспечения. Описание процесса от бизнес-консультанта. [Электронный ресурс]. URL: https://habr.com/ru/companies/trinion/articles/245615/ (дата обращения 17.09.2024).

9. *Цветкова О.Л., Исак Д.А.* Применение методов интеллектуального анализа данных при тестировании систем информационной безопасности // Новости науки 2024: Гуманитарные и точные науки: сб. материалов XLIII Междунар. очно-заоч. науч.-практ. конф. М.: Империя, 2023. С. 30–31.

10. *Вульфин А.М.* Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных // Системная инженерия и информационные технологии. 2023. Т. 5, № 4(13). С. 50–76.

11. Security Vision. SIEM системы (Security information and Event Management) – что это и зачем нужно? [Электронный ресурс]. URL: https://www.securityvision.ru/blog/siem-chto-eto-i-zachem-nuzhno/ (дата обращения 15.09.2024);

12. AWS. Что такое промежуточное ПО [Электронный ресурс]. URL: https://aws.amazon.com/ru/what-is/middleware/ (дата обращения 15.09.2024);

МУНТЯН МИХАИЛ МИХАЙЛОВИЧ – аспирант кафедры математического и аппаратного обеспечения информационных систем, Чувашский государственный университет, Россия, Чебоксары (muntyanmickhail@gmail.com; ORCID: https://orcid.org/0009-0009-6836-8921).

СИДОРКИНА ИРИНА ГЕННАДЬЕВНА – доктор технических наук, профессор кафедры математического и аппаратного обеспечения информационных систем, Чувашский государственный университет, Россия, Чебоксары; заведующая кафедрой информационной безопасности, Поволжский государственный технологический университет, Россия, Йошкар-Ола (igs592000@mail.ru; ORCID: https://orcid.org/0009-0000-2869-0419).

Mikhail M. MUNTYAN, Irina G. SIDORKINA

METHOD OF INTEGRATING AN UTILITY MODULE WITH SIEM

Key words: *information security, SIEM, middleware, event monitoring, software development, microservices.*

The current tool for information security is the use of SIEM-type systems, which allow collecting and processing a large amount of data on the protected infrastructure by defining dependencies between emerging security events. The ways in which such systems used more effectively are therefore equally valuable. This process linked to the development of new algorithms for infrastructure monitoring and the need for its (infrastructure) modernization. Classical analysis methods were used to identify important aspects and stages of the SIEM process, mathematical modelling methods for analytical calculations were used to increase the efficiency of the SIEM interaction – protected infrastructure, methods of comparative analysis in determining the advantages and disadvantages of using current software development architecture, synthesis methods for determining the applicability of intelligent application methods as a means of expansion of the obtained for the calculation of correlation events without-danger information.

The objectives of the study *are to increase the level of automation of SIEM decision-making and the efficiency of critical information security parameters: the speed of analysis of incoming events and decision-making, the load on information security resources in the protected infrastructure, the quality of the protection system when separating SIEM functionality into small local network «representative offices».*

Materials and methods. *Subject of study, the process of functioning SIEM, whose efficiency does not reach optimal for solution given to systems of this type value. Classical analysis methods were used to determine important aspects and stages of the SIEM process, mathematical modeling methods for analytical calculations increase efficiency of interaction construction «SIEM – protected infrastructure», methods of comparative analysis in the determination of pre-advantages and disadvantages of using today's current architecture*

for software development, synthesis methods for determining the applicability of mining methods as a means of extending the information security events correlation obtained.
Results. *Based on the results of the research, a new architecture of protected infrastructure for implementing SIEM interaction proposed – an infrastructure based on decentralization of information collection and preprocessing processes through delegation of SIEM software functionalities platform. The structural features of the implementation of the program platform as well as its basic functionality defined. In addition, based on the results of a comparative analysis of monolithic, service-oriented and micro-service approach, the most preferred way to implement the proposed software platform was determined, and a list of advanced functionalities, taking into account the need to use information-mining techniques to improve SIEM performance.*
Conclusions. *The use of the proposed solution increases the performance of SIEM systems when implementing such stages as information collection and pre-processing, expands the capabilities of information security specialists by obtaining new correlated data through the use of intelligent analysis methods, and also allows you to move from a centralized implementation of the protection process to a decentralized one. The implementation of the software platform based on a service-oriented approach makes it possible to increase the level of system integration and its fault tolerance. In addition, the use of the proposed platform in conjunction with second-generation SIEM systems allows you to get an alternative assessment of the state of the infrastructure, which indicates the possibility of improving the accuracy of decision-making.*

References

1. Mel'nikov E.A. *Tipovye skhemy vzaimodeistviya v sistemakh sbora i analiza sobytii informatsionnoi bezopasnosti SIEM* [Typical interaction schemes in SIEM information security event collection and analysis systems]. *Elektronnyi nauchnyi zhurnal*, 2020, no. 3(32), pp. 21–24.

2. Sizov V.A., Kirov A.D. *Problemy vnedreniya SIEM-sistem v praktiku upravleniya informatsionnoi bezopasnost'yu sub»ektov ekonomicheskoi deyatel'nosti* [Problems of implementation of SIEM-systems in the information security management practice of economic activity entities]. *Otkrytoe obrazovanie,* 2020, vol. 1, no. 24, pp. 69–79.

3. Muntyan M.M., Sidorkina I.G. *Metod integratsii vspomogatel'nogo modulya v sushchestvuyushchie SIEM-sistemy* [Method of integration of the utility module into existing SIEM systems]. In: *Inzhenernye kadry – budushchee innovatsionnoi ekonomiki Rossii: materialy IX Vseros. stud. konf.* [Proc. of the IX Russ. Conf. «Engineers – future of innovative economy of Russia»]. Yoshkar-Ola, 2023, pp. 567–572.

4. Chernyad'ev I.S., Khamidullin M.R. *Sposoby integratsii programmnogo obespecheniya: API, Veb-servisy i promezhutochnoe programmnoe obespechenie* [Integration software: API, Web-services and intermadiate software]. In: *Shkola molodykh novatorov: sb. nauch. st. 5-i Mezhdunar. nauch. konf. perspektivnykh razrabotok molodykh uchenykh* [Proc. of the 5th Int. Conf. «School of young innovators»]. Kursk, 2024, pp. 266–270.

5. *Prosto o mikroservisakh* [Simply about micro services]. Available at: https://habr.com/ru/companies/raiffeisenbank/articles/346380/ (Access Date: 2024, Sept. 17).

6. *V chem raznitsa mezhdu SOA i mikroservisami* [SOA and micro services difference]. Available at: https://aws.amazon.com/ru/compare/the-difference-between-soa-microservices (Access Date: 2024, Sept. 17).

7. *Osnovnye protokoly integratsii prilozhenii* [Basic protocols for application integration]. Available at: https://dynamicsun.ru/blog/protokoli-inteegrasii-prilozheniy.html (Access Date: 2024, Sept. 17).

8. *Integratsiya programmnogo obespecheniya. Opisanie protsessa ot biznes konsul'tanta* [Software integration. Description from business conseltant]. Available at: https://habr.com/ru/companies/trinion/articles/245615 (Access Date: 2024, Sept. 17).

9. Tsvetkova O.L., Isak D.A. *Primenenie metodov intellektual'nogo analiza dannykh pri testirovanii sistem informatsionnoi bezopasnosti* [Application of data mining methods in testing information security systems]. In: *Novosti nauki 2024: Gumanitarnye i tochnye nauki: sb. materialov XLIII Mezhdunar. ochno-zaochnoi nauch.-prakt. konf.* [Proc. of XLIII Russ. Conf. «Science news 2024: Humanities and precise sciences»]. Moscow, Empire Publ., 2023, pp. 30–31.

10. Vul'fin A.M. *Modeli i metody kompleksnoi otsenki riskov bezopasnosti ob»ektov kriticheskoi informatsionnoi infrastruktury na osnove intellektual'nogo analiza dannykh* [Models and methods of integrated security risk assessment of critical information infrastructure objects based on data mining]. *Sistemnaya inzheneriya i informatsionnye tekhnologii,* 2023, no. 4(13), pp. 50–76.

11. *Security Vision. SIEM sistemy (Security information and Event Management) – chto eto i zachem nuzhno?* [Security information and event management (SIEM) systems – main appointment]. Available at: https://www.securityvision.ru/blog/siem-chto-eto-i-zachem-nuzhno/ (Access Date: 2024, Sept. 15).

12. *AWS. Chto takoe promezhutochnoe PO* [AWS. What is intermediate software]. Available at: https://aws.amazon.com/ru/what-is/middleware (Access Date: 2024, Sept. 15).

MIKHAIL M. MUNTYAN – Post-Graduate Student, Department of Mathematical and Hardware Support of Information Systems, Chuvash State University, Russia, Cheboksary (muntyanmickhail@gmail.com; ORCID: https://orcid.org/0009-0009-6836-8921).

IRINA G. SIDORKINA – Doctor of Technical Sciences, Professor, Department of Mathematical and Hardware Support of Information Systems, Chuvash State University, Russia, Cheboksary; Head of the Department of Information Security, Volga State University of Technology, Russia, Yoshkar-Ola (igs592000@mail.ru; ORCID: https://orcid.org/0009-0000-2869-0419).

Формат цитирования: *Мунтян М.М., Сидоркина И.Г.* Способ интеграции вспомогательного модуля с SIEM-системами // Вестник Чувашского университета. 2024. № 4. С. 60–74. DOI: 10.47026/1810-1909-2024-4-60-74.