Модуль аналитики состояния системы мониторинга

Описание программы

Содержание

[Аннотация 3](#_Toc25751371)

[Сокращения, термины и определения 4](#_Toc25751372)

[1. Общие сведения 5](#_Toc25751373)

[1.1. Обозначение и наименование модуля 5](#_Toc25751374)

[1.2. Программное обеспечение, необходимое для функционирования программы 5](#_Toc25751375)

[2. Функциональное назначение 6](#_Toc25751376)

[3. Описание логической структуры 10](#_Toc25751377)

[3.1. Алгоритм программы 10](#_Toc25751378)

[3.2. Визуализация и вывод детальной информации о текущем состоянии используемой SIEM системы 13](#_Toc25751379)

Аннотация

Данный документ содержит в себе описание модуля аналитики состояния системы мониторинга SIEM системы. Архитектура и принцип работы модуля являются универсальными и позволяют функционировать модулю совместно с SIEM системой без привязки к конкретному производителю и версии SIEM системы.

Сокращения, термины и определения

В настоящем документе использованы следующие сокращения:

|  |  |
| --- | --- |
| Сокращение | Значение |
| Модуль | Модуль аналитики состояния системы мониторинга |
| SIEM | (сокращенно от англ. Security Information and Event Management) – Система сбора, анализа и корреляции событий информационной безопасности |
| ИТ | Информационные технологии |
| ИБ | Информационная безопасность |
| ПО | Программное обеспечение |
| Дашборд | Информационная панель визуализации бизнес процессов |
|  |  |
|  |  |
|  |  |

1. Общие сведения
	1. Обозначение и наименование модуля

Полное наименование: Модуль аналитики состояния системы мониторинга.

Условное обозначение: Модуль аналитики, Программа.

* 1. Программное обеспечение, необходимое для функционирования программы

Учитывая вендоронезависимую архитектуру модуля, для работы Модуля аналитики необходимо использование любой SIEM системы, реализующей принципы раздельного сбора событий информационной безопасности, а также предоставляющей внутренние механизмы диагностики и мониторинга состояния работоспособности. Примерами указанных SIEM систем являются SIEM платформа ArcSight производства компании Micro Focus, а также Система мониторинга и управления событиями безопасности Ankey SIEM производства компании ООО «Газинформсервис».

1. Функциональное назначение

Программа предназначена для решения следующих задач:

* автоматизированный мониторинг работы компонентов используемой SIEM системы;
* визуализация и вывод детальной информации о текущем состоянии используемой SIEM системы;
* автоматизация рутинных процессов обслуживания используемой SIEM системы;
* выявление проблем в работе компонентов используемой SIEM системы по мере их появления.

Функции Модуля:

1. периодический сбор данных из журналов работы и управляющих консолей, а также через API компонент используемой SIEM системы для мониторинга следующих параметров:
	* работоспособность компонентов;
	* доступность источников событий;
	* целостность данных от источников событий;
	* актуальность данных от источников событий (выявление расхождения временных меток на источниках событий и в модуле управления, выявление некорректной обработки данных, поступающих из различных временных зон, выявление задержек записи событий ИБ в базу данных);
	* производительность компонент SIEM системы;
	* производительность коннекторов SIEM системы, используемых для сбора данных от источников событий;
	* проблемы в конфигурации компонентов компонент SIEM системы;
	* проблемы в конфигурации коннекторов для подключения к источникам событий;
	* иные ошибки в журналах работы компонент SIEM системы.
2. приоритезация и визуализация обработанной информации и предоставление ее для анализа в виде дашбордов и линейных графиков;
3. оповещение об ошибках в работе компонент используемой SIEM системы содержат следующие данные:
	* наименование компонента (коннектора или модуля управления);
	* наименование ошибки;
	* тип ошибки;
	* приоритет ошибки;
	* описание ошибки;
	* рекомендации по устранению ошибки;
	* ссылку на базу собственную базу знаний ошибок подсистемы мониторинга.
4. отправка автоматического почтового оповещения на настраиваемые адреса электронной почты в следующих случаях:
	* остановка любого из компонентов используемой SIEM системы, подключенного к мониторингу;
	* сбой в работе любого из компонентов используемой SIEM системы, подключенного к мониторингу;
	* критическая ошибка, которая может привести к непредвиденной остановке работы компонентов, используемой SIEM системы;
	* потеря сетевого соединения между компонентами используемой SIEM системы;
	* потеря сетевого соединения между компонентами используемой SIEM системы и источниками журналов аудита;
	* иной случай, требующий автоматического почтового уведомления.
5. отражение истории каждой метрики (доступность, целостность, производительность и пр.) всех компонентов и общего уровня работоспособности используемой SIEM системы не менее чем в течение месяца;
6. выгрузка отчетов по каждой метрике и общему уровню работоспособности компонент используемой SIEM системы в формате CSV;
7. фильтрация в интерактивном режиме диагностических данных всех компонентов используемой SIEM системы (по месту расположения, по типу операций (сбор, фильтрация, агрегация, приоритезация, корреляция и пр.), по типу компонентов и т.д.);
8. настройка в интерактивном режиме приоритетов обнаруженных ошибок компонент используемой SIEM системы;
9. настройка в интерактивном режиме автоматического почтового оповещения в зависимости от приоритетов обнаруженных ошибок компонент используемой SIEM системы;
10. отправка автоматического оповещения на указанные адреса электронной почты в следующих случаях:
	* остановка любого из компонентов системы используемой SIEM системы;
	* сбой в работе любого из компонентов системы используемой SIEM системы, подключенного к мониторингу;
	* критическая ошибка, которая может привести к непредвиденной остановке работы компонентов системы используемой SIEM системы;
	* потеря сетевого соединения между компонентами системы используемой SIEM системы;
	* потеря сетевого соединения между компонентами системы используемой SIEM системы и источниками журналов аудита.
11. отражение истории каждой метрики (доступность, целостность, производительность и пр.) всех компонентов и общего уровня работоспособности системы используемой SIEM системы;
12. контроль доступности устройств, сбор данных которых осуществляется компонентами используемой SIEM системы, в разных настраиваемых временных интервалах;
13. автоматизация процесса (Workflow) для работы с ошибками компонент используемой SIEM системы. Процесс поддерживает следующие функции:
	* приоритезация ошибок;
	* настраиваемое автоматическое реагирование на ошибки (останов/запуск/перезапуск службы, изменение настроек конфигурационных файлов, очистка кэша, сбор и архивация журналов событий в указанном каталоге);
	* настраиваемое автоматическое уведомление.
14. настройка в ручном режиме автоматического реагирования на заданные типы/классы обнаруженных ошибок компонент используемой SIEM системы;
15. автоматическое и ручное обновления компонент SIEM системы;
16. ежемесячная актуализация и обновление баз знаний, содержащих описание и рекомендации касаемо ошибок компонент используемой SIEM системы;
17. ведения и актуализации локальной базы знаний, содержащих описания и рекомендации касаемо ошибок компонент используемой SIEM системы без подключения к сети Интернет.
18. Описание логической структуры
	1. Алгоритм программы

Полученные с целевых систем события подвергаются первоначальной обработке (фильтрация, нормализация, агрегация, приоритезация, корреляция). Далее происходит проверка соответствия полученных событий, условиям, заложенным в правилах. В свою очередь, при обработке событий, правила используют информацию, хранящуюся в активных листах и фильтрах (или их аналогах). Результатом работы правил, являются вновь созданные корреляционные события (инциденты). На основе событий и инцидентов строятся аналитические отчеты, а также в режиме реального времени информация отображается в активных каналах и инструментальных панелях.

Задачей модуля является анализ и обработка собранных событий с использованием встроенных механизмов системы используемой SIEM системы, таких как:

* фильтры - Filters (компоненты, позволяющие отобразить только необходимые события, имеющие отношения к текущей задаче);
* активные листы - ActiveLists (динамические списки для поддержания актуальных данных о состоянии систем о пользователей);
* правила - Rules (компоненты, позволяющие гибко анализировать, проводить корреляцию поступающих данных и делать выводы на основании обнаруженных событий).

Основным компонентом модуля является набор корреляционных правил.

Для его работы применяются правила, относящихся к мониторингу различных ресурсов, представленных ниже (или их аналогов в зависимости от используемой SIEM системы):

* ресурсы (Resource и Resource Quota);
* активные каналы (Active Channel);
* активные листы (Active List);
* архивы (Archive);
* аутентификация (Authentication);
* коннекторы (Connector Connection, Connector Login, Connector Exceptions, Connector Error);
* мониторы данных (Data Monitors);
* лицензии (License Audit);
* менеджер (Manager External Event Flow Interruption, Manager Activation, Manager Error);
* нотификации (Notification);
* правила (Rule Actions, Rule Activations, Rule Firings, Rule Warnings);
* запуск по расписанию (Scheduler Execution, Scheduling Tasks, Scheduler Skip);
* пользователи (User Login, User Management).

 Правила охватывают весь спектр событий, относящихся к нарушениям корректной работы системы мониторинга. Некоторые группы и примеры правил представлены в таблице 1.

 Таблица 1

|  |  |  |
| --- | --- | --- |
| № | Группа правил | Примеры правила |
| 1 | Ресурсы | * удаление ресурса;
* изменение ресурса в нерабочее время;
* изменение ресурса нелегитимным пользователем.
 |
| 2 | Активные каналы | * медленная загрузка активного канала.
 |
| 3 | Активные листы | * переполнение активного листа.
 |
| 4 | Архивы | * ошибка создания архива;
* ошибка активации архива.
 |
| 6 | Коннекторы | * остановка критичного коннектора;
* нет данных с коннектора в течение заданного времени;
* ошибки разбора событий;
* переполнение кэша коннектора;
* ошибки подключения к целевым источникам.
 |
| 7 | Мониторы данных | * критичное увеличение фиксируемых событий;
* отключение монитора данных.
 |
| 8 | Лицензии | * нарушение лицензионной политики (количество событий);
* нарушение лицензионной политики (количество ресурсов).
 |
| 9 | Менеджер | * останов менеджера;
* останов сбора событий менеджером;
* критичная загрузка менеджера.
 |
| 10 | Нотификации | * Превышение заданного количества отправленных сообщений в единицу времени;
* Отключение нотификации;
* Множественные неудачные попытки доставки сообщений.
 |
| 11 | Правила | * Отключение критичного правила;
* Правило уходит в рекурсию;
* Превышение критичного предела срабатывания правила в единицу времени.
 |
| 12 | Запуск по расписанию | * Ошибка выполнения задачи по расписанию.
 |

* 1. Визуализация и вывод детальной информации о текущем состоянии используемой SIEM системы

Для вывода детальной информации о текущем состоянии используемой SIEM системы используются настроенные отчетные таблицы и графики, перечень которых представлен в таблице 1 и 2 соответственно.

Таблица 1 - Перечень отчетных таблиц

|  |  |  |
| --- | --- | --- |
| № | Название | Описание  |
| 1. | Доступность источников событий | Выявленные случаи потери сетевого соединения с источниками событий |
| 2. | Доступность компонентов используемой SIEM системы | Выявленные случаи потери сетевого соединения с компонентами используемой SIEM системы |
| 3. | Целостность данных от источников событий | Выявленные случаи нарушения целостности данных от источников событий |
| 4. | Актуальность данных от источников событий | Выявленные случаи нарушения актуальности данных от источников событий (расхождения временных меток) |
| 5. | Проблемы в конфигурации компонентов используемой SIEM системы | Перечень обнаруженных проблем в конфигурации компонентов используемой SIEM системы |
| 6. | Производительность компонентов | Перечень обнаруженных проблем с производительностью компонентов используемой SIEM системы |
| 7. | Производительность коннекторов | Перечень обнаруженных проблем с производительностью коннекторов |
| 8. | Остановки компонентов используемой SIEM системы | Выявленные случаи остановки используемой SIEM системы |
| 9. | Сбои в работе компонентов используемой SIEM системы | Перечень критичных ошибок компонентов используемой SIEM системы |
| 10. | Ошибки в работе компонентов используемой SIEM системы | Перечень критичных и некритичных ошибок компонентов используемой SIEM системы |
| 11. | Потеря сетевого соединения | Выявленные случаи потери сетевого соединения между компонентами используемой SIEM системы |
| 12. | Количество событий, получаемых с коннекторов | Таблица с количеством событий, получаемых с каждого из коннекторов  |
| 13. | Количество событий, получаемых с источников событий | Таблица с количеством событий, получаемых с каждого из источников |
| 14. | Всплески потоков событий | Выявленные случае всплесков количества событий, получаемых с источника (в минуту) |
| 15. | Прекращение потока событий | Выявленные случае прекращения получения событий с источника |

Таблица 2 - Перечень графиков

| № | Название | Описание  |
| --- | --- | --- |
| 1. | Потери сетевого соединения с источниками событий | ТОП источников с событий с наибольшим количеством выявленных за месяц случаев потери сетевого соединения  |
| 2. | Потери сетевого соединения с компонентами используемой SIEM системы | ТОП компонентов используемой SIEM системы с наибольшим количеством выявленных за месяц случаев потери сетевого соединения |
| 3. | Нарушения целостности данных от источников событий | ТОП источников с событий с наибольшим количеством выявленных за месяц случаев нарушения целостности поступающих данных  |
| 4. | Нарушения актуальности данных от источников событий | ТОП источников с событий с наибольшим количеством выявленных за месяц случаев нарушения актуальности поступающих данных (расхождения временных меток) |
| 5. | Проблемы в конфигурации компонентов используемой SIEM системы | ТОП компонентов используемой SIEM системы с наибольшим количеством обнаруженных за месяц проблем в конфигурации  |
| 6. | Проблемы с производительностью компонентов | ТОП компонентов используемой SIEM системы с наибольшим количеством обнаруженных за месяц проблем с производительностью |
| 7. | Проблемы с производительностью коннекторов | ТОП коннекторов с наибольшим количеством обнаруженных за месяц проблем с производительностью |
| 8. | Остановки компонентов используемой SIEM системы | ТОП компонентов используемой SIEM системы с наибольшим количеством случаев остановки за месяц |
| 9. | Сбои в работе компонентов используемой SIEM системы | ТОП компонентов используемой SIEM системы с наибольшим количеством критичных ошибок за месяц |
| 10. | Ошибки в работе компонентов используемой SIEM системы | ТОП компонентов используемой SIEM системы с наибольшим количеством критичных и некритичных ошибок за месяц |
| 11. | Потеря сетевого соединения | ТОП компонентов используемой SIEM системы с наибольшим количеством случаев потери сетевого соединения |
| 12. | Количество событий, получаемых с коннекторов | ТОП коннекторов по количеству получаемых событий ИБ |
| 13. | Количество событий, получаемых с источниками событий | ТОП источников по количеству получаемых событий ИБ |
| 14. | Всплески потоков событий | ТОП источников по количеству выявленных всплесков количества событий (в минуту) |
| 15. | Прекращение потока событий | ТОП источников по количеству выявленных случаев прекращения получения событий  |