Монитор

Назначение шаблона

Шаблон предназначен для организации мониторинга событий в системе, которая может быть использована самостоятельно как пассивный механизм отслеживания потоков данных, потоков управления и выполняемых в системе операций, или в составе активного механизма применения правил и политик безопасности к этим потокам и операциям.

Типовые цели безопасности

Типовые цели безопасности при применении шаблона включают:

- мониторинг и регистрация событий в системе, важных для безопасности;
- отслеживание передачи данных в системе и применение политики безопасности к обмену данными в системе и между системой и внешним окружением;
- отслеживание системных вызовов, передачи управления и управляющих запросов в системе.

Предположения безопасности

Предположения безопасности включают:

- учитываемость данных/событий (accountability);
- известный и прозрачный формат данных и протокол обмена данными.

Предположения и условия, при которых шаблон не может быть применен:

- данные, которые требуется отслеживать при помощи монитора, подвергаются шифрованию, и нет возможности расшифровать их на уровне монитора (модуля анализа монитора).

Описание решения

Элементы системы, реализующей шаблон:

- модуль сбора данных (датчик);
- модуль анализа (детектор);
- модуль реакции;
- база данных / база знаний, используемых и пополняемых алгоритмами анализа, которые реализуются детектором.

Взаимодействие элементов монитора представлено на рисунке 1.

Шаблон используется самостоятельно, либо как основа для других шаблонов, в том числе из числа перечисленных в настоящем стандарте. Он также может входить в состав элементов систем, построенных на основе других шаблонов, не определяя при этом их основные свойства.

Требования к технологии разработки элементов системы

Технология сбора данных, реализованная модулем сбора данных, должна исключать вмешательство в процессы работы системы, она должна быть реализована прозрачным для этих процессов образом так, чтобы минимизировать влияние на временные характеристики работы системы, показатели ее производительности, надежности и безопасности;

Модуль анализа, в зависимости от потребностей мониторинга может реализовать анализ в режиме времени выполнения или отложенный анализ на основе данных, поступающих от датчика;

Алгоритмы анализа должны минимизировать количество ошибок первого рода и ложных срабатываний, но пороговые значения и показатели производительности анализа устанавливаются индивидуально в зависимости от потребностей и назначения мониторинга.

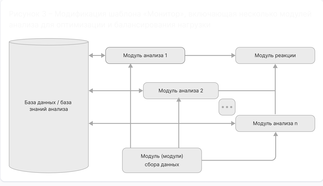
Ограничения на применение шаблона

Применение шаблона может быть ограничено в системах с требованиями к выполнению в реальном времени, а также в системах с повышенными требованиями к функциональной безопасности и надежности в тех случаях, когда датчик реализует технологию перехвата потоков данных и/или потоков управления с последующей ретрансляцией этих потоков, что потенциально может повлиять на выполнение упомянутых требований.

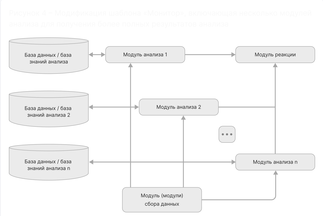
Допустимые модификации шаблона

Допустимо использовать не один, а несколько датчиков или систему модулей сбора данных, поставляющих данные в модуль анализа (рисунок 2).

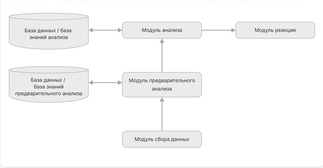
Допустимо использовать несколько модулей анализа, реализующих одни и те же алгоритмы, для оптимизации и балансирования нагрузки на модуль анализа (рисунок 3).



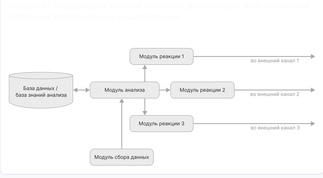
Допустимо использовать несколько модулей анализа, реализующих несколько различных алгоритмов анализа, для получения более полных результатов анализа (рисунок 4).



Допустимо организовывать модули анализа в иерархию, нижние уровни которой служат датчиками для верхних для получения более точных результатов анализа (рисунок 5).



Допустимо использовать не один, а несколько модулей реакции, реализующих связь с внешними системами через одни и те же или различные типы каналов связи (рисунок 6).



Допустимо реализовывать обратную связь от внешних систем, подключенных через модуль реакции, для переконфигурирования монитора с целью обеспечения его устойчивой работы, а также для корректировки параметров сбора данных и подстройки алгоритмов анализа. Для управления и конфигурирования модулями шаблона вводится дополнительный отдельный модуль – агент управления и конфигурации, действующий внутри шаблона (рисунок 7).

Допустимость модификаций, не входящих в указанный перечень, должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.