УДК 004.056
doi: 10.21685/2587-7704-2023-8-1-11

Open Access RESEARCH ARTICLE

Методы увеличения эффективности правил корреляции событий в системах мониторинга информационной безопасности

Александр Николаевич Аккуратнов
Пензенский государственный университет, Россия, г. Пенза, ул. Красная, 40
akkalexnick@yandex.ru

Аннотация. Рассмотрена структура правил корреляции событий в системах мониторинга информационной безопасности. Определены недостатки существующей структуры правил, приводящие к ложным срабатываниям в процессе выявления инцидентов. Предложен способ расширения структуры правил для увеличения эффективности правил корреляции и снижения количества ложных срабатываний.

Ключевые слова: информационная безопасность, система мониторинга, корреляция событий, правила корреляции, последовательность событий, инцидент информационной безопасности

Для цитирования: Аккуратнов А. Н. Методы увеличения эффективности правил корреляции событий в системах мониторинга информационной безопасности // Инжиниринг и технологии. 2023. Т. 8 (1). С. 1–3. doi: 10.21685/2587-7704-2023-8-1-11

Methods for increasing the efficiency of event correlation rules in information security monitoring systems

Alexander N. Akkuratnov
Penza State University, 40 Krasnaya Street, Penza, Russia
akkalexnick@yandex.ru

Abstract. The structure of event correlation rules in information security monitoring systems is considered. The shortcomings of the existing structure of the rules, leading to false positives in the process of identifying incidents, are identified. A method is proposed for extending the structure of rules to increase the efficiency of correlation rules and reduce the number of false positives.

Keywords: information security, monitoring system, event correlation, correlation rules, sequence of events, information security incident

For citation: Akkuratnov A.N. Methods for increasing the efficiency of event correlation rules in information security monitoring systems. *Inzhiniring i tekhnologii = Engineering and Technology*. 2023;8(1):1–3. (In Russ.). doi: 10.21685/2587-7704-2023-8-1-11

Основным методом выявления инцидентов информационной безопасности современными системами мониторинга [1] является сигнатурный метод с использованием правил корреляции событий [2, 3]. Результатом работы правил корреляции является одно или несколько событий, характеризующих инцидент информационной безопасности.

Правила корреляции в каждой системе мониторинга имеют свою собственную структуру, но после изучения многообразия представлений правил [4, 5, 6] можно выделить их общие характерные составляющие.

1. Условия принадлежности события выявляемому инциденту (набор слов или словосочетаний, которые должны встречаться в параметрах событий или условия оценки времени возникновения события).

2. Условия формирования последовательности событий (описание последовательности типов событий или иерархии правил).

3. Условия корреляции событий (набор параметров, которые у смежных событий последовательности должны иметь одинаковые значения).

4. Количество повторений событий, если критерием установления инцидента является появление нескольких однотипных событий.

5. Время, за которое должна сформироваться последовательность событий.

Как в отечественных, так и в зарубежных системах мониторинга структура правил корреляции представлена аналогичным образом. Отличия можно увидеть лишь в формах редактирования условий и описания последовательностей.

Рассмотрим возможность использования правил корреляции для выявления инцидентов информационной безопасности. Для примера возьмем весьма распространенную задачу выявления фактов подбора пароля для какой-либо учетной записи пользователя. Обычно правила корреляции для выявления подобных фактов составлены из одного блока события неуспешной попытки аутентификации с количеством повторений 3–5 за 30–60 мин. Пусть $e1$ – событие неуспешной аутентификации. Тогда последовательность $e1$-$e1$-$e1$ без учета других событий приведет к срабатыванию правила.

Рассмотрим другой пример. Пусть $e2$ – событие успешной аутентификации и в мониторинге существует последовательность событий $e1$-$e2$-$e1$-$e2$-$e1$. Такая последовательность также приведет к срабатыванию правила. Но с учетом наличия событий успешной аутентификации можно утверждать, что это ложное срабатывание, вызванное обычными ошибками пользователя при вводе пароля. Следовательно, основным фактором подтверждения попытки подбора пароля является присутствие в мониторинге последовательности событий $e1$ подряд без появления событий $e2$. При разработке правила корреляции следует учитывать этот фактор, но при существующей структуре правил корреляции этого сделать нельзя. Функция сброса состояния правила по условию появления события, а не по превышению счетчика времени, в редакторах правил отсутствует.

Для решения этой проблемы предлагается расширить структуру представления правил корреляции путем добавления блоков описания событий, при появлении которых осуществляется сброс текущего состояния правила.

На рис. 1 показан пример расширенной структуры правила в графическом виде. В блоке 2 установлены параметры ожидания двух событий неуспешных попыток аутентификации. В блоке 3 установлен признак сброса текущего состояния правила.

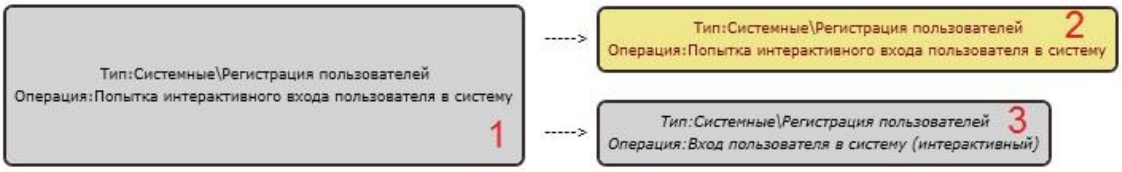

Рис. 1. Пример расширенной структуры правила корреляции

Обработку правила модулем корреляции событий системы мониторинга можно описать следующим образом. При появлении события, соответствующего условиям в блоке 1 (неуспешная попытка аутентификации), правило переходит в состояние ожидания появления событий в блоках 2 и 3. Если далее появляется событие из блока 3, то состояние правила сбрасывается опять в ожидание события блока 1. Если же при отсутствии события блока 3 появляются два события из блока 2, то происходит срабатывание правила и формирование инцидента.

Предложенный способ расширения структуры правила корреляции позволяет решить поставленную задачу и избежать ложных срабатываний. Для ранее рассмотренной последовательности событий $e1$-$e2$-$e1$-$e2$-$e1$ правило не сработает, поскольку появление событий успешной аутентификации $e2$ будет сбрасывать текущее состояние правила.

Предложенная структура правила корреляции может применяться и для более широкого класса задач. Рассмотрим еще один пример. Для администраторов существует задача выявления учетных записей пользователей, которые давно не используются. В целях безопасности учетные записи уволенных сотрудников или сотрудников, которые долго отсутствуют на рабочем месте, должны блокироваться или удаляться. Для поиска таких учетных записей в существующем представлении правило корреляции состояло бы из двух блоков событий: «аутентификация пользователя» – «отсутствие аутентификации в течение N дней». Но правило срабатывало бы для всех учетных записей, в том числе уже заблокированных или удаленных. Предложенное расширение структуры правила позволяет

решить эту проблему и учесть события блокировки или удаления учетной записи для сброса состояния правила.

На рис. 2 показана версия правила в расширенной структуре.

Рис. 2. Пример расширенной структуры правила корреляции

Время последней аутентификации и использования учетной записи фиксируется при появлении события в блоке 1. Если событие аутентификации не появляется в течение *N* дней (блок 2, учетная запись не используется), то происходит формирование инцидента информационной безопасности. Если событие аутентификации появляется (блок 3, учтенная запись используется), то происходит сброс состояния правила. Если появилось событие отключения или удаления учетной записи пользователя (блоки 4 и 5), то также происходит сброс состояния правила. Правило будет срабатывать только для действительно неиспользуемых учетных записей, исключая уже заблокированные или удаленные.

Предложенное расширение текущей структуры правил корреляции событий позволяет увеличить точность анализа событий, существенно уменьшить количество ложных срабатываний и снизить трудозатраты эксплуатационного персонала систем мониторинга событий информационной безопасности.

Список литературы

1. Джуракулов Т. Х., Петросян А. А., Евстропов В. А. SIEM-системы управления событиями // Молодой ученый. 2023. № 4 (451). С. 10–11.
2. Шелестова О. Корреляция SIEM. Сигнатурные методы // Исследовательский центр Positive Research. 2012. URL: http://www.securitylab.ru/analytics/431459.php
3. Сергеев Р. Как писать правила корреляции в SIEM-системе без навыков программирования // Исследовательский центр Positive Research. 2019. URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/kak-pisat-pravila-korrelyacii-v-siem-sisteme-bez-navykov-programmirovaniya/
4. ArcSight ESM. URL: http://www.arcsight.com/products/products–esm/
5. KOMRAD Enterprise SIEM. URL: https://npo-echelon.ru/production/65/11793
6. IBM Security QRadar SIEM. URL: https://www.ibm.com/products/qradar-siem

References

1. Dzhurakulov T.Kh., Petrosyan A.A., Evstropov V.A. SIEM-event management systems. *Molodoy uchenyy = A young scientist*. 2023;(4):10–11. (In Russ.)
2. Shelestova O. Correlation of SIEM. Signature methods. *Issledovatel'skiy tsentr Positive Research = Research Center Positive Research*. 2012. (In Russ.). Available at: http://www.securitylab.ru/analytics/431459.php
3. Sergeev R. How to write correlation rules in a SIEM system without programming skills. *Issledovatel'skiy tsentr Positive Research = Research Center Positive Research*. 2019. (In Russ.). Available at: https://www.ptsecurity.com/ru-ru/research/knowledge-base/kak-pisat-pravila-korrelyacii-v-siem-sisteme-bez-navykov-programmirovaniya/
4. *ArcSight ESM*. Available at: http://www.arcsight.com/products/products–esm/
5. *KOMRAD Enterprise SIEM*. Available at: https://npo-echelon.ru/production/65/11793
6. *IBM Security QRadar SIEM*. Available at: https://www.ibm.com/products/qradar-siem

Поступила в редакцию / Received 05.03.2023

Поступила после рецензирования и доработки / Revised 04.04.2023

Принята к публикации / Accepted 28.04.2023