УДК 004.056 DOI: 10.14529/ctcr160116

ПРИМЕНЕНИЕ САМООБУЧАЮЩЕЙСЯ СИСТЕМЫ КОРРЕЛЯЦИИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ ПРИ АВТОМАТИЗАЦИИ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л.В. Астахова, В.И. Цимбол

Южно-Уральский государственный университет, г. Челябинск

В настоящее время наиболее широкое распространение на рынке SIEM-систем получили системы, использующие сигнатурные методы корреляции событий информационной безопасности, что обусловлено простотой их реализации и гибкостью при настройке и дальнейшей эксплуатации. Однако системы, построенные по этому принципу, не способны адаптироваться к условиям быстро изменяющегося ИТ-ландшафта в силу предопределенности инцидентов информационной безопасности, на которые они могут реагировать. К числу недостатков таких систем относятся большое количество ложных срабатываний и относительная сложность настройки и внедрения. В статье рассматривается способ применения аппарата нечеткой логики для построения самообучающейся системы корреляции событий информационной безопасности в качестве альтернативы широко распространенным сигнатурным методам. В рамках настоящей статьи обоснована схема реализации самообучающейся системы корреляции событий, описаны преимущества данной системы перед сигнатурными методами корреляции.

Ключевые слова: нечеткая логика, SIEM-системы, самообучающиеся системы, системы менеджмента информационной безопасности.

Введение

В условиях современного уровня развития инфокоммуникационных и компьютерных технологий, а также систем связи, вопрос обеспечения информационной безопасности ИТ-инфраструктуры предприятий становится более сложным, многогранным, требующим привлечения большого количества людских и временных ресурсов. Решение данного вопроса в условиях крупных компаний немыслимо без применения соответствующих автоматизированных систем менеджмента информационной безопасности, в основе которых лежат SIEM-системы.

В настоящее время наиболее широкое распространение на рынке SIEM-систем получили системы, использующие сигнатурные методы корреляции событий информационной безопасности, что обусловлено, в первую очередь, простотой реализации данных систем, а также гибкостью при настройке и дальнейшей эксплуатации [1, с. 223]. К таким системам относятся:

- HP ArcSight;
- IBM QRadar;
- Symantec SIM;
- RSA Envision и другие.

Однако системы, построенные по такому принципу, не способны адаптироваться к условиям быстро изменяющегося ИТ-ландшафта в силу предопределенности инцидентов информационной безопасности, на которые они могут реагировать. Также в качестве недостатков таких систем можно выделить большое количество ложных срабатываний (false-positive события) и относительную сложность настройки и внедрения [2, с. 35].

Для устранения вышеописанных недостатков, на мой взгляд, прекрасно подходит применение аппарата нечеткой логики с построением на его основе самообучающейся системы корреляции событий информационной безопасности, которая упростит процесс внедрения SIEM-системы в ИТ-инфраструктуру предприятия, а также обеспечит своевременное реагирование системы как на общеизвестные виды атак, так и на ранее не изученные.

Описание принципов функционирования системы.

Основным понятием аппарата нечеткой логики выступает понятие нечеткого множества, представляющее собой совокупность упорядоченных пар вида:

$C = \{(MF_c(x), x) | x \epsilon X\}$,

где $MF(x)$ – характеристическая функция принадлежности (функция принадлежности), принимающая значения в упорядоченном множестве $M = [0 \dots 1]$ и отражающая степень принадлежности элемента x к множеству C;

x – элемент некоего множества X.

Еще одним фундаментальным понятием выступает понятие лингвистической переменной, представляющей собой набор (β, T, X, G, M), где:

β – название лингвистической переменной;

T – терм-множество (множество значений лингвистической переменной);

X – область рассуждений (универсальное множество);

G – синтаксическая процедура, позволяющая оперировать элементами терм-множества T;

M – семантическая процедура, позволяющая превратить каждое новое значение лингвистической переменной, образуемое процедурой G, в нечеткую переменную [3, с. 125].

Из лингвистических переменных посредством операции нечеткого логического вывода строятся нечеткие высказывания. Основой для проведения операции нечеткого логического вывода является база правил, содержащая нечеткие высказывания вида:

R_i: *Если* x_1 *это* A_{i1}, *то* y *это* B_i,

где x_j – четкое значение входной переменной;

y – четкое значение выходной переменной;

A_{ij} – заданные нечеткие множества с функциями принадлежности;

B_i – высказывание[4, с. 207].

В общем случае механизм логического вывода включает в себя три этапа:

1) фаззификация (введение нечеткости, на данном этапе рассчитываются значения лингвистических переменных);

2) нечеткий логический вывод;

3) дефаззификация (приведение к четкости).

В качестве примера для наглядности описанных теоретических основ, приведем лингвистическую переменную «давление». Терм-множеством данной переменной будет выступать множество, состоящее из двух элементов – «слабое», «сильное». В качестве универсального множества будет выступать значение измеренного давления. Тогда, используя стандартные операции над нечеткими множествами, вычислим степени принадлежности рассматриваемых физических величин к значениям лингвистической переменной. Допустим, в нашем случае значение лингвистической переменной «давление» приняло следующий вид: «слабое» – 0,65, «сильное» – 0,35. Если принять в качестве правил следующий набор:

1) если давление низкое, то закрыть клапан;

2) если давление высокое, то открыть клапан.

Результаты работы правил будут выглядеть следующим образом:

1) закрыть клапан: 0,65;

2) открыть клапан: 0,35.

В результате работы механизма нечеткого логического вывода клапан будет закрыт.

Данный механизм прекрасно подходит для реализации систем, обеспечивающих принятие решений на основе относительных входных параметров, в случаях, когда нет точного критерия принятия решений, что также прекрасно вписывается в общую концепцию построения SIEM-систем.

В рамках рассматриваемой самообучающейся системы корреляции событий информационной безопасности предполагается использование двух лингвистических переменных: «Типичность события» и «Взаимосвязь». В качестве терм-множества принято множество

$T = \{\text{Высокая}, \text{Умеренная}, \text{Низкая}\}$.

В качестве характеристической функции принадлежности предполагается использовать функцию принадлежности гауссова типа, которая описывается формулой:

$MF(x) = e^{[-(\frac{x-c}{\sigma})^2]}$.

Выбор данной функции обусловлен большей точностью вычисления степени принадлежности по сравнению с симметричной треугольной и трапецеидальной функциями.

Параметры c и σ задаются в качестве начальных значений и в дальнейшем изменяются в ходе обучения системы, обеспечивая ее адаптацию к условиям эксплуатации.

Значение лингвистической переменной «Типичность события» рассчитывается на основе собранных статистических данных о работе конкретных служб, действий пользователей и прочих процессов ИТ-инфраструктуры. События со значением «низкая» немедленно оформляются в виде инцидента информационной безопасности. В качестве примера можно привести события, связанные с попытками подключения к АРМ и прочим объектам ИТ-инфраструктуры предприятия, не характерные или не обусловленные должностными инструкциями работника данного АРМ. Сюда же относятся все события, оповещающие о неудачных попытках авторизации.

Значение лингвистической переменной «Взаимосвязь» рассчитывается между событиями с высокой частотой на основе их классификации по группам и собранных ранее статистических данных. Данный механизм позволит обнаруживать новые виды атак, а также создавать новые правила, пополняя тем самым базу знаний системы. В качестве примера можно выделить появление в SIEM-системе событий, связанных с подключением к БД и неудачными попытками авторизации в ней.

В общем виде, структура рассматриваемой самообучающейся системы корреляции событий информационной безопасности, имеет вид, представленный на рисунке.

Структура самообучающейся системы корреляции событий информационной безопасности

Анализ рынка SIEM-систем подтвердил уникальность описанной системы корреляции событий информационной безопасности. Направлением дальнейших исследований является внедрение в описанную систему зависимости значения лингвистической переменной «Типичность события» от уровня возможной угрозы, исходящей от конкретного работника организации в соответствии с занимаемой им должностью, а также разработка прототипа данной системы с последующими испытаниями.

Заключение

В данной статье представлен вариант использования аппарата нечеткой логики для совершенствования процесса корреляции событий информационной безопасности. К основным досто-

инствам системы можно отнести высокую адаптационную способность системы к быстро изменяющемуся ИТ-ландшафту, большую вероятность обнаружения новых видов атак по сравнению с используемыми в настоящее время сигнатурными методами, относительную легкость внедрения за счет самообучения системы, что в свою очередь снижает затраты на внедрение данной системы. Интеграция данной системы с уровнями возможных внутренних угроз, проистекающих от работников организации в соответствии с занимаемыми ими должностями, позволит решить актуальную проблему обнаружения инсайдеров среди штата сотрудников организации. Нечеткая логика является в настоящее время бурно развивающейся ветвью классической математической логики, что, в свою очередь, указывает на перспективность дальнейшей разработки данной системы.

Литература

1. Miller, D.R. Security Information and Event Management (SIEM) implementation / D.R. Miller, S. Harris, S. Vandyke. – McGrawHill, 2011. – 464 c.

2. Рудинский, И.Д. Технология проектирования автоматизированных систем обработки информации и управления / И.Д. Рудинский. – Горячая линия-Телеком, 2014. – 304 с.

3. Жданов, А.А. Метод автономного адаптивного управления / А.А. Жданов // Известия академии наук. Теория и системы управления. – 1999. – № 5. – С. 125.

4. Zadeh, L.A. The Concept of a Linguistic Variable and its Application to Approximate Reasoning. Parts 1 and 2 / L.A. Zadeh. – Information Sciences, 1975. – 357 p.

Астахова Людмила Викторовна, д-р пед. наук, профессор, профессор кафедры безопасности информационных систем, Южно-Уральский государственный университет, г. Челябинск; lvastachova@mail.ru.

Цимбол Владимир Игоревич, студент кафедры безопасности информационных систем, Южно-Уральский государственный университет, г. Челябинск; yuashick@mail.ru.

Поступила в редакцию 13 января 2016 г.

DOI: 10.14529/ctcr160116

APPLICATION SELF-LEARNING SYSTEM EVENT CORRELATION INFORMATION SECURITY BASED ON FUZZY LOGIC AUTOMATION IN MANAGEMENT SYSTEMS INFORMATION SECURITY

***L.V. Astakhova**, lvastachova@mail.ru,*
***V.I. Tsimbol**, yuashick@mail.ru*
South Ural State University, Chelyabinsk, Russian Federation

Currently, the most widely used on the market SIEM-systems using the signature event correlation methods of information security, which is due, ease of implementation and flexibility in configuring and further exploitation. This system, built on this principle, are not able to adapt to the rapidly changing IT-landscape by virtue of predetermined information security incidents to which they can respond. The disadvantages of such systems include a large number of false positives and the relative complexity of the configuration and implementation. The article discusses how to use fuzzy logic to construct a self-learning system of information security event correlation as an alternative to the widespread signature methods. The article explains the scheme of the self-learning system event correlation and its advantages over signature-based correlation.

Keywords: fuzzy logic, SIEM-system self-learning system, information security management system.

References

1. Miller D.R., Harris S., Vandyke S. Security Information and Event Management (SIEM) implementation. McGrawHill, 2011. 464 p.

2. Rudinskiy I.D. *Tehnologiya proektirovaniya avtomatizirovannykh sistem obrabotki informatsii i upravleniya* [Technology Development of Automated Information Processing and Management]. Moscow, Hotline Telecom, 2014. 304 p.

3. Zhdanov A.A. [The Method of Autonomous Adaptive Control]. *Proceedings of the Academy of Sciences. Theory and control systems*, 1999, no. 5, p. 125. (in Russ.)

4. Zadeh L.A. The Concept of a Linguistic Variable and its Application to Approximate Reasoning. Parts 1 and 2. Information Sciences, 1975. 357 p.

Received 13 January 2016

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Астахова, Л.В. Применение самообучающейся системы корреляции событий информационной безопасности на основе нечеткой логики при автоматизации систем менеджмента информационной безопасности / Л.В. Астахова, В.И. Цимбол // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2016. – Т. 16, № 1. – С. 165–169. DOI: 10.14529/ctcr160116

FOR CITATION

Astakhova L.V., Tsimbol V.I. Application Self-Learning System Event Correlation Information Security Based on Fuzzy Logic Automation in Management Systems Information Security. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*, 2015, vol. 16, no. 1, pp. 165–169. (in Russ.) DOI: 10.14529/ctcr160116