УДК 004.45.056.5

Борисов В. И., Шабуров А. С.

О ПРИМЕНЕНИИ СИГНАТУРНЫХ МЕТОДОВ АНАЛИЗА ИНФОРМАЦИИ В SIEM-СИСТЕМАХ

В статье анализируется проблема количества обрабатываемой информации и необходимости использования для этой цели SIEM-систем. Рассматриваются методы бессигнатурного анализа, применяемые в подобных системах. Анализируется порядок применения SIEM-системы на основе сигнатурных методов. Приводится пример работы счетчика донной системы для обнаружения DDoS атаки.

Ключевые слова: *инцидент, SIEM-система, DLP-система, метод бессигнатурного анализа, сигнатурный метод, DDoS- атака*

Borisov V. I., Shaburov A. S.

ABOUT THE APPLICATION OF SIGNATURE ANALYSIS METHOD IN THE SIEM-SYSTEMS

In this article analyzes the problem is the quantity of information processed and the need to use for this purpose SIEM systems. Consideres assignatures methods which are used in such systems. The procedure of use of SIEM system on the basis of signature methods is analyzes. The example of operation of the counter of ground system for detection of DDoS of attack is given.

Keywords: *incident, SIEM-system, DLP-system, method of the assignatures analysis, signatures, DDos-attack*

В настоящее время достаточно актуальной является проблема количества информации, обрабатываемой в информационных системах, объемы которой растут в геометрической прогрессии. Интенсивность информационного обмена обусловлена развитием и разнообразием бизнес-процессов и задач, решаемых в рамках систем управления предприятиями и организациями различных форм собственности. Одновременно увеличивается и количество вредоносной информации, такой как вирусы, троянские программы и т.д., а также разнообразие злоумышленных информационных атак на ресурсы систем: DDoS, брутфорс и т.п. При этом, методы и пути проникновения вредоносной информации в корпоративные информационные системы также постоянно видоизменяются и модифицируются, делая задачу обеспечения информационной безопасности таких систем, достаточно сложной.

Интенсивность информационных событий в корпоративных сетях может достигать нескольких миллионов в день, следовательно, возникает проблема нахождения и локализации вредоносной информации в больших информационных массивах. При этом обработка подобных событий в ручном режиме не представляется возможной, так как потребовала бы значительных человеческих и временных затрат, а так же недопустимых с точки зрения эффективности использования аппаратно-программных ресурсов. Так же многие крупные компании стали переходить на работу в виртуальных платформах, с целью минимизации затрат на аппаратную часть. Размещенные в виртуальной среде информационные системы наиболее уязвимы к увеличениям нагрузок, вызванных DDoS-атаками злоумышленников, а так же нарушениями правил эксплуатации [1]. Решение данных проблем целесообразно на основе применения SIEM систем.

SIEM (System information event management) – системы, появившиеся в результате слияния SEM-систем и SIM-систем. Основным функциональным отличием данных систем является то, что SEM-системы предназначены для анализа информации в режиме реального времени, а SIM-системы анализируют уже накопленную информацию [2].

В свою очередь, преимуществом использования SIEM-систем является то, что осуществляется анализ всей накопленной и оперативной информации, поступающей от разных источников: DLP, средства антивирусной защиты информации, системы учета трафика, сканеры уязвимости, межсетевые экраны и т.д. На основе анализа данных из этих источников выявляется отклонения от нормального функционирования, заданного критериями безопасности, и в случае обнаружения происходит оповещение администратора безопасности.

Кроме того, типовая SIEM-система может использоваться для:

• предоставления доказательной базы при расследовании инцидентов информационной безопасности;

• предоставления структурированной информации необходимой при аудите информационной безопасности;

• обеспечения непрерывности работы сервисов путем обнаружения сбоев в их работе;

• структуризации информационно-телекоммуникационной системы.

Наиболее важным этапом работы SIEM-системы для принятия решения может считаться процесс корреляции событий важных с точки зрения безопасности. Рассмотрим данный процесс подробнее.

После получения информации от источников, система начинает анализировать эту информацию. В большинстве SIEM уже есть стандартный набор правил корреляции (Rule Based Reasoning). Данные правила состоят из определенных наборов условий и сценариев действий, а корреляция событий, как правило, основана на бессигнатурных методах, т.е. система сама определяет появление нежелательных процессов и обеспечивает их фиксирование и подсчет. Кроме того, существуют сигнатурные методы корреляции, в которых правила определения инцидентов в конкретную группу устанавливаются оператором SIEM-системы [3].

Существует множество методов бессигнатурного анализа. Обычно на практике используются следующие методы:

• Statistical — сложный бессигнатурный метод корреляции событий, основанный на измерении двух или более переменных и вычислении степени статистической связи между ними.

• RBR Rule-based (pattern based) (HP ECS, IMPACT, RuleCore) — метод, в котором взаимосвязи между событиями определяются аналитиками в заранее заданных специфических правилах.

• CBR Codebook based. Корреляция производится по подходящим векторам из предварительно заданной матрицы событий.

• MBR model based reasoning (слишком большой MTTR) — метод основан на абстракции объектов и наблюдения за ними в рамках модели.

• NMBR — Normalized model based reasoning. Схож с MBR, известен как baseline.

• Graph based. Корреляция заключается в поиске зависимостей между системными компонентами в графическом представлении (network devices, hosts, services) и построении графа на их основе. Если зависимость обнаруживается, то граф используется для поиска основной причины возникновения проблемы.

• Neural network based — идеологический метод. Нейронная сеть обучается для обнаружения аномалий в потоке событий.

Разнообразие бессигнатурных методов не позволяет преодолеть их основной недостаток. Так как бессигнатурные методы разра-

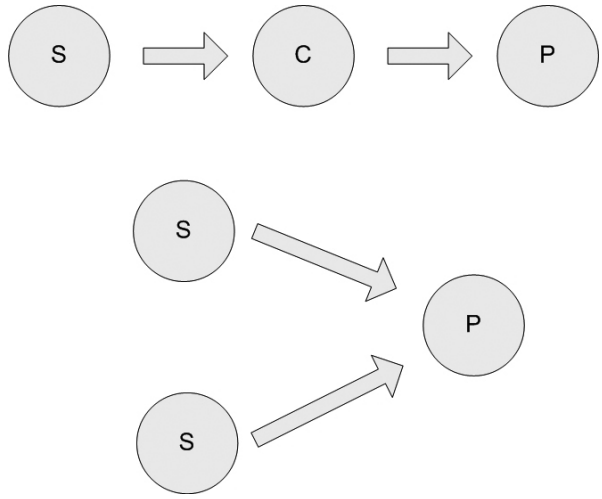

Рис. 1. Схема появления инцидента, с учетом возможного объединения его симптомов

батываются и внедряются производителями SIEM-систем, этими методами невозможно управлять. В свою очередь, сигнатурные методы отличаются гибкостью и эффективностью обнаружения угроз безопасности информации, что в современных условиях может значительно повышать эффективность систем защиты информации.

Для пояснения работы сигнатурных методов введем следующие обозначения:

- P – проблема (problem,инцидент);
- C – причина (cause);
- S – симптом (symptoms).

Структурная схема появления инцидента показана на рис.1.

Для адекватной реакции на инциденты необходимо выявлять причины и симптомы. Появление инцидента в системе может быть вызвано такими симптомами, как установление соединения по закрытым портам (попытки), создание учетной записи с повышенными привилегиями (повышение привилегий учетной записи). Необходимо объединять симптомы для предотвращения возникновения инцидента. Один инцидент может быть образован объединением нескольких симптомов.

Критичность инцидента зависит от количества симптомов. Существует два метода определения критичности инцидента: количественный и вероятностный.

При количественном методе учитывается количество связей, идущих от симптомов к определенной проблеме. При вероятностном методе (рис.2) каждой связи выставляется рейтинг опасности. В зависимости от суммы данных рейтингов выставляется критичность инцидента.

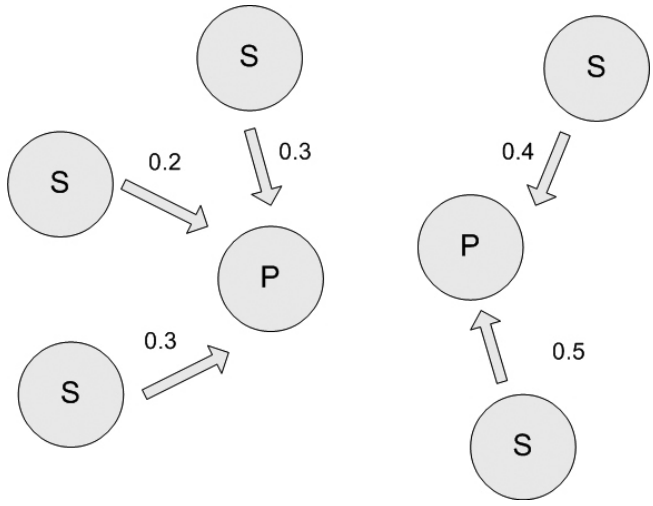

Рис. 2. Схема вероятностного метода определения инцидента

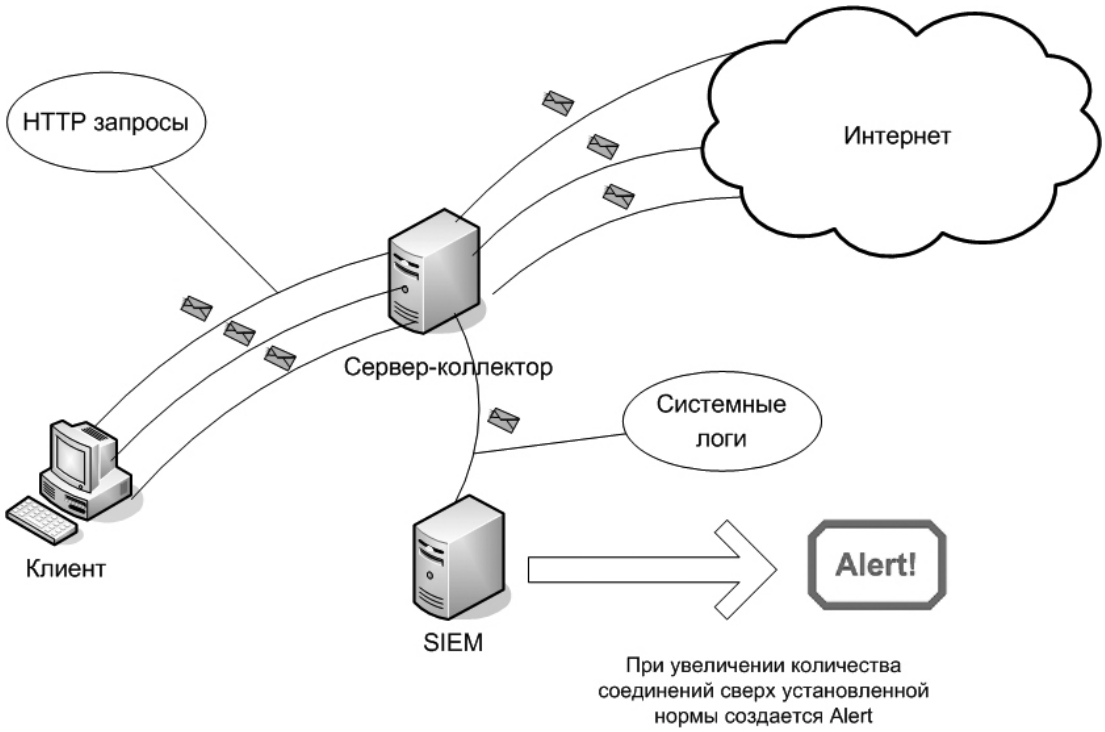

Рис. 3. Схема обнаружения DDoS-атаки с использованием SIEM-системы

Идея сигнатурного метода заключается в нахождении совпадений с составленными правилами корреляции. Каждое правило разрабатывается под определенную проблему. Но по одному инциденту или симптому возможно срабатывание нескольких правил одновременно.

В соответствии с общим принципом действия правил в состав правила входит триггер, состоящий из условия, счетчика и сценария реакции на инцидент.

Счетчик необходим для подсчета количества совпадений по правилу (одному и тому же). Рассмотрим работу счетчика на примере обнаружения DDoS- атаки. DDoS — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён [4]. Количество подобных атак с каждым годом растет. При этом DDoS атаки являются самым эффективным способов выведения из строя систем обмена информацией в международном пространстве, а компьютеры атакуемой сети могут быть и атакующими устройствами (участниками ботнета).

Триггер может считать различные численные характеристики для каждого метода DDoS- атак. Например, для SYN-флуда характерна передача TCP пакетов5. В условие срабатывания триггера мы можем записать максимальное число «полуоткрытых» соединений с одного IP адреса, за определенное время (сессия). Схема обнаружения DDoS атаки с использованием SIEM-системы изображена на рис. 3.

В случае с HTTP-флудом, возможно установление максимального количества подключений по 80 порту, а так же количества процессов Apache. За максимальное значение берем среднестатистическое значение за определенный период времени (сессия).

В обоих случаях триггер будет ждать выполнения одного из условий. А при прохождении определенного момента времени (обнуление сессии), триггер вернется в нулевое состояние и продолжит свой цикл работы сначала.

Таким образом, благодаря использованию SIEM-систем может значительно снижаться время реагирование на атаки, а следовательно и экономические затраты на восстановление системы. Это, в свою очередь, обуславливает необходимость внедрения SIEM-систем на основе сигнатурных методов для повышения уровня управляемости системой защиты информации.

Примечания

1. Тыщенко С.В., Соловьев Н.А. Системный анализ доступности ресурсов информационных систем в гетерогенной виртуальной среде //Вестник УрФО. Безопасность в информационной среде. — Челябинск: Изд. центр ЮУрГУ, 2014. — № 2(12). — С.24-31

2. Алексей Дрозд, Обзор SIEM-систем //SearchInform [Электронный ресурс] — Режим доступа. — URL: http://www.anti-malware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market

3. Олеся Шелестова. Корреляция SIEM . Сигнатурные методы //исследовательский центр Positive Research [Электронный ресурс] 2012. URL:http:// www.securitylab.ru/analytics/431459.php

4. DoS-атака//Википедия [Электронный ресурс]. URL:http:// https://ru.wikipedia.org/wiki/DoS-D0%B0%D1%82%D0%B0%D0%BA%D0%B0

5. Обнаружение информационных атак//Академия Microsoft.[Электронный ресурс] URL:http:// www.intuit.ru/studies/courses/600/456/lecture/10220?page4

Шабуров Андрей Сергеевич, доцент, кандидат технических наук, Пермский Национальный Исследовательский Политехнический Университет, г. Пермь. E-mail: shans@at.pstu.ru

Борисов Владислав Игоревич, студент, Пермский Национальный Исследовательский Политехнический Университет, г. Пермь. E-mail: borisovvi94@yandex.ru

Shaburov Andrew, Associate Professor, Candidate of Technical Sciences, National Research Polytechnic University, Perm. E-mail: shans@at.pstu.ru

Borisov Vladislav, student National Research Polytechnic University. E-mail: borisovvi94@yandex.ru