электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 02, февраль 2016

УДК 004.056.53

Методика подключения ERP-системы как неподдерживаемого источника событий к системе класса Security Information and Event Management (SIEM)

Волкович Е. К., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность автоматизированных систем»

Кузнецов А. В., *аспирант*
Россия, 125993, г. Москва, Финансовый университет при Правительстве РФ,
кафедра «Информационная безопасность»

Научный руководитель: Иржавский А.А., ст. преподаватель
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
кафедра «Информационная безопасность автоматизированных систем»
volkovichek@student.bmstu.ru

Число инцидентов информационной безопасности (ИБ) непрерывно растет, в том числе за последний год, согласно оценкам компании *PwC*, их количество выросло на 38% [[1]]. В связи с этим, по сей день вопросы защиты информации являются актуальными для большинства современных компаний. Одним из способов выявления, реагирования и расследования произошедших инцидентов ИБ является использование систем класса *Security Information and Event Management (SIEM).*

SIEM-системы – это системы управления ИБ и событиями безопасности, которые предназначены для автоматизации процессов централизованного сбора, накопления и обработки информации о событиях [[2]] от различных источников. На сегодняшний день на рынке представлено свыше 80 подобных решений. Такие разработчики как *IBM, HP, Splunk, Intel, LogRhythm,* а также ряд других компаний согласно отчету *Gartner* по *SIEM*-технологиям за 2015 год [[3]], являются мировыми лидерами в этой области. В рамках настоящего доклада в качестве примера *SIEM* рассматривается решение *McAfee Enterprise Security Manager (ESM)* компании *Intel Security* (ранее – *McAfee, Inc.*). Применительно к данному продукту проанализированы и разработаны пути подключения неподдерживаемых штатно источников событий.

Система *McAfee ESM* позволяет принимать и обрабатывать информацию о событиях от различных источников: операционных систем, СУБД, средств защиты

информации, других систем и приложений. Однако, несмотря на широкий спектр заявленных производителем и штатно поддерживаемых системой источников событий, в продукте отсутствует возможность приема событий от наиболее популярной в России[1] *ERP*-системы для автоматизации управленческих процессов «1С: Предприятие» (далее – 1С). При этом, являясь во многих предприятиях и организациях ключевой системой, 1С играет важную роль в сборе и анализе событий безопасности. В связи с этим возникает объективная потребность в подключении этого неподдерживаемого источника к *SIEM*-системе и, как следствие, – необходимость разработки методики данного подключения, чему и посвящается данный доклад.

На сегодняшний день существует методика подключения неподдерживаемых штатно источников событий, предложенная производителем. Если следовать порядку подключения, установленному в технической документации на данный продукт, *SIEM*-система получает события в формате, как показано на рис. 1. Из рисунка видно, что *SIEM*-система не способна корректно получать информацию о событиях в том виде, в котором хранится журнал событий непосредственно в 1С.

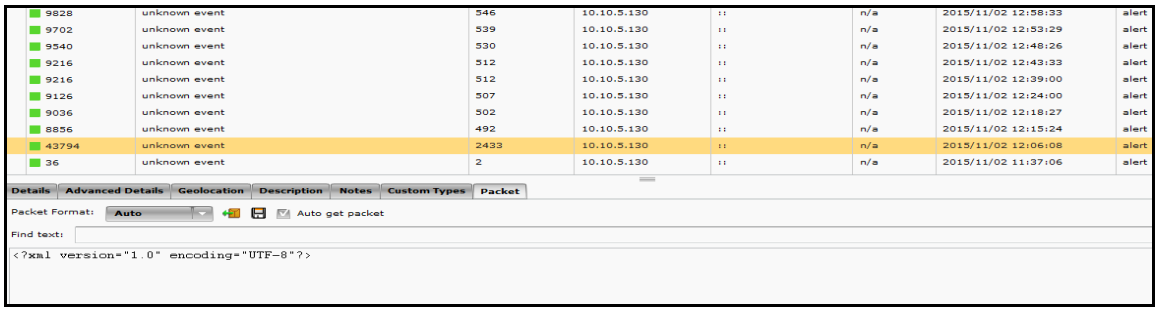


Рис. 1. Получение событий от 1С

Плюс данная методика не позволяет гарантировать целостность получаемых данных. Таким образом, возникает необходимость уточнения и модификации существующей методики, учитывая ее выявленные недостатки.

Для определения подхода к подключению источника событий первоначально необходимо определить формат журнала событий. Поскольку события 1С заносятся в базу данных (БД), необходимо по расписанию выгружать данные из БД в журнал событий в формате *Extensible Markup Language (XML)* с помощью встроенной функции 1С. На рис. 2 представлен пример журнала событий, полученный от системы 1С.

[1] По данным маркетингового агентства *TADVISER* [[4]]

Рис. 2. Пример журнала событий 1С

Далее необходимо определить способ передачи событий в *SIEM*-систему и настроить 1С как источник событий. В зависимости от того, где хранится журнал событий в 1С, на стороне сервера или АРМ пользователя 1С, необходимо установить и настроить специальное программное обеспечение (СПО) *McAfee SIEM Collector*. Данное СПО позволяет получать события от неподдерживаемых штатно источников событий и перенаправлять их в *SIEM*-систему, используя протокол *Syslog*. События от коллектора к собственно *SIEM*-системе могут быть переданы как по защищенному каналу передачи данных *(SSL)*, так и без его использования. Так как журнал событий в формате *XML* хранится на рабочей станции, возникает угроза подмены исходного журнала событий путем получения к нему несанкционированного доступа (НСД). Для того, чтобы в *SIEM*-систему поступали немодифицированные события, необходимо обеспечить их защиту. Предлагается использовать дискреционное разграничение доступа к каталогу, в котором хранится журнал событий с использованием средств файловой системы *New Technology File System (NTFS).*

Для защиты журнала событий от НСД при физическом доступе к компьютеру и дискам необходимо осуществлять «прозрачное шифрование» данных с помощью *Encrypting File System (EFS). EFS* использует симметричное шифрование для защиты файлов, а также шифрование, основанное на паре открытый/закрытый ключ для защиты ключа шифрования для каждого файла. По умолчанию закрытый ключ пользователя защищён с помощью шифрования пользовательским паролем, следовательно, защищённость журналов так же зависит от стойкости пароля пользователя, для этого

необходимо внести соответствующие изменения в парольную политику. Защита канала передачи данных между сервером 1С и СУБД осуществляется средствами той СУБД, которая используется. Все поддерживаемые СУБД могут использовать протокол *SSL*.

Таким образом, мы минимизируем возможность НСД к файлам журнала событий и получаем схему защиты, представленную на рис. 3.

Рис. 3. Схема защиты

Для начала процедуры разбора событий необходимо разработать способ приведения исходного журнала событий к соответствующему однострочному виду. Для выполнения данной задачи был разработан скрипт, представленный на рис. 4.

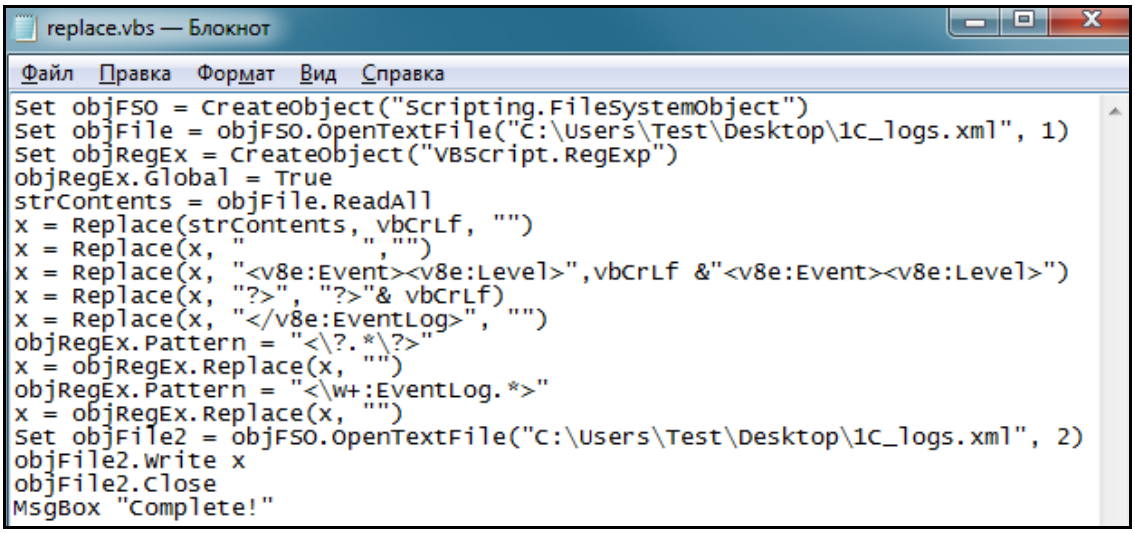


Рис. 4. Скрипт для приведения событий к однострочному виду

Результат выполнения скрипта представлен на рис. 5.

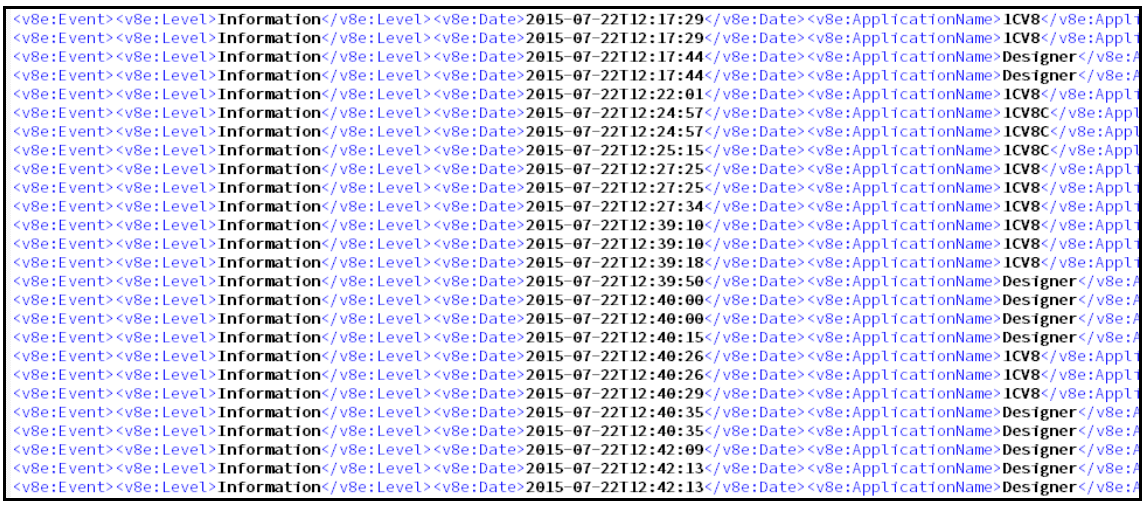


Рис. 5. Подготовленный для анализа журнал событий

Анализируя структуру полученных событий, можно выделить мета-поля (дата, время, приложение, пользователь и другие), которые необходимы для нормализации событий. Для того чтобы *SIEM*-система могла «понимать» приходящие от неподдерживаемого источника события, необходимо написать так называемый «парсер», т.е. регулярное выражение, которое необходимо для разбиения события на части и ассоциирования данных с мета-полями. «Парсер» создается в специальном встроенном редакторе, который с точки зрения оператора представляет собой отдельное окно, представленное на рис. 6.

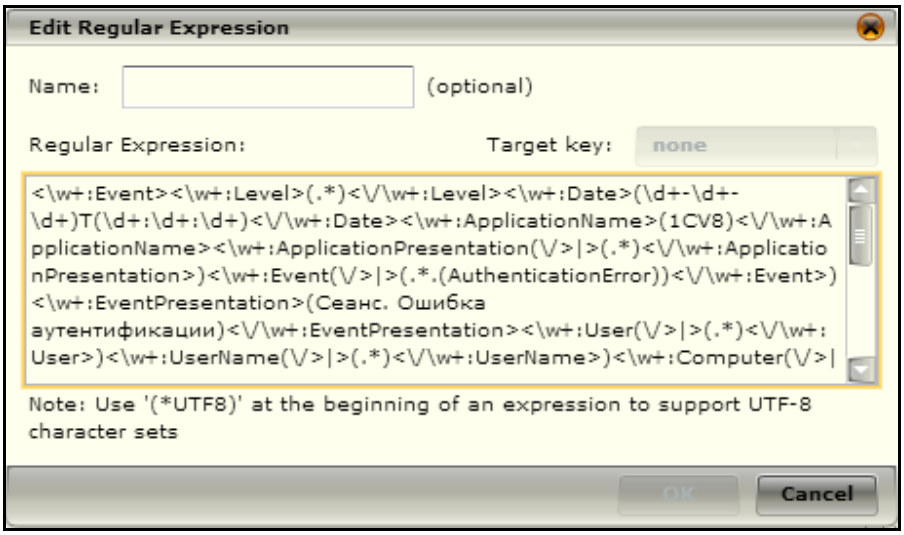


Рис. 6. Написание «парсера» для нормализации событий

После создания регулярного выражения в интерфейсе оператора отобразится разбиение тестовой строки, введенной в качестве примера в поле «*Sample Log Data*», для данного регулярного выражения, как показано на рис. 7.

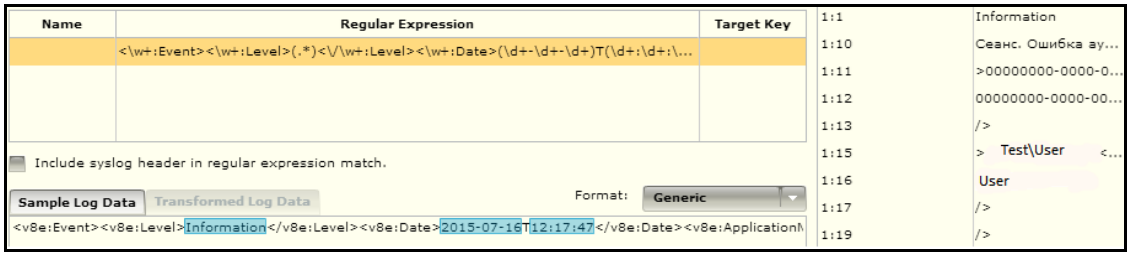


Рис. 7. Разбиение тестовой строки

Далее необходимо соотнести поля, полученные после разбиения строки, с информационными полями в *McAfee ESM*, служащими для отображения информации о событии (см. рис. 8), задать параметр «важность» для произошедшего события и определить действие, которое нужно выполнить по отношению к поступившему событию.

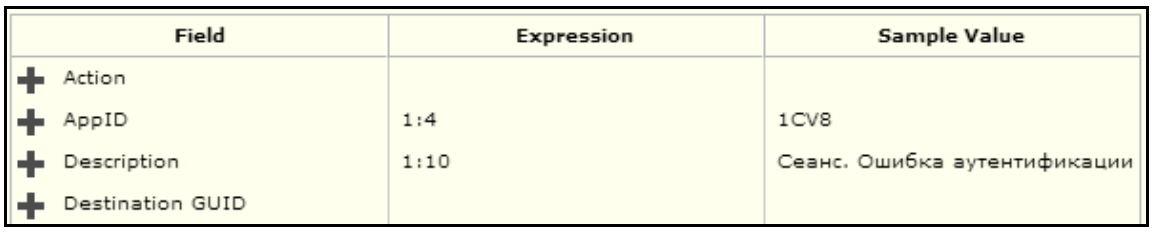
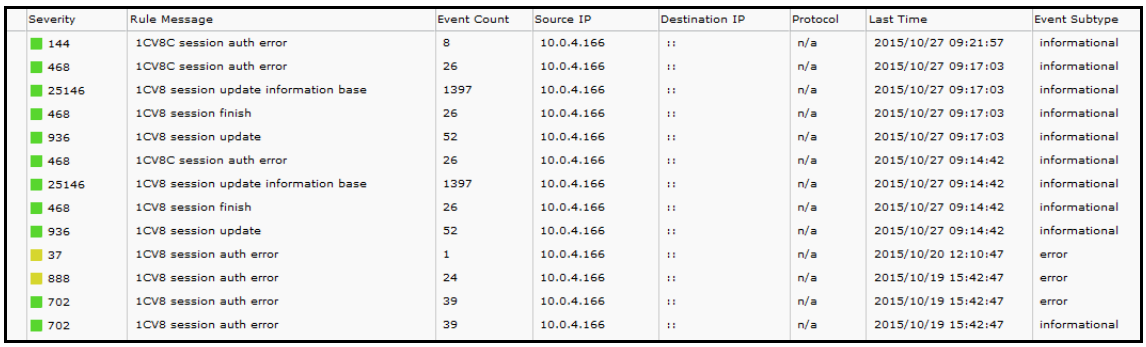


Рис. 8. Нормализация событий

Как видно из рис. 9 заключительным этапом является проверка корректности получаемых событий в *McAfee ESM*.



Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
144	1CV8C session auth error	8	10.0.4.166	::	n/a	2015/10/27 09:21:57	informational
468	1CV8C session auth error	26	10.0.4.166	::	n/a	2015/10/27 09:17:03	informational
25146	1CV8 session update information base	1397	10.0.4.166	::	n/a	2015/10/27 09:17:03	informational
468	1CV8 session finish	26	10.0.4.166	::	n/a	2015/10/27 09:17:03	informational
936	1CV8 session update	52	10.0.4.166	::	n/a	2015/10/27 09:17:03	informational
468	1CV8C session auth error	26	10.0.4.166	::	n/a	2015/10/27 09:14:42	informational
25146	1CV8 session update information base	1397	10.0.4.166	::	n/a	2015/10/27 09:14:42	informational
468	1CV8 session finish	26	10.0.4.166	::	n/a	2015/10/27 09:14:42	informational
936	1CV8 session update	52	10.0.4.166	::	n/a	2015/10/27 09:14:42	informational
37	1CV8 session auth error	1	10.0.4.166	::	n/a	2015/10/20 12:10:47	error
888	1CV8 session auth error	24	10.0.4.166	::	n/a	2015/10/19 15:42:47	error
702	1CV8 session auth error	39	10.0.4.166	::	n/a	2015/10/19 15:42:47	error
702	1CV8 session auth error	39	10.0.4.166	::	n/a	2015/10/19 15:42:47	informational

Рис. 9. События, получаемые от 1С

Таким образом, методика подключения неподдерживаемых источников событий состоит из следующих этапов:

1. Определение формата хранения журналов событий на стороне источника.

2. Определение способа передачи событий от источника событий в *SIEM*-систему, и настройка источника для передачи событий.

3. Подключение источника событий к *SIEM*-системе, выбранным ранее способом передачи с помощью ПО *McAfee SIEM Collector*.

4. Настройка правил разграничения доступа к каталогу, где хранится журнал событий, с помощью *NTFS*.

5. Написание скрипта для приведения журнала событий к однострочному виду.

6. Написание «парсеров» и создание правил нормализации событий.

7. Проверка корректности получаемых событий.

8. Доработка правил нормализации (при необходимости).

Подводя итог, можно сказать, что данная методика инвариантна и может применяться для других неподдерживаемых источников событий.

Список литературы

[1]. PwC. Key findings from The Global State of Information Security® Survey 2016. Turnaround and transformation in cybersecurity. Available at: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html, accessed 25.10.2015.

[2]. Кузнецов А.В. Способ организации процесса управления событиями, в части их обработки, в рамках системы управления информационной безопасностью предприятия // Вопросы защиты информации. № 2. 2015. 78 с.

[3]. Magic Quadrant for Security Information and Event Management. Available at: http://zlonov.ru/gartner-magic-quadrants/, accessed 25.10.2015.

[4]. Системы управления предприятием (рынок России). Режим доступа: http://www.tadviser.ru/index.php/Статья%3ASистемы_управления_предприятием_%28рынок_России%29 (дата обращения 25.10.2015).