Повышение уровня автоматизации процессов сбора данных о выявленных событиях и инцидентах информационной безопасности

И.Д. Королев, Е.С. Литвинов, Д.И. Маркин

Краснодарское высшее военное училище им. генерала армии Штеменко С.М.

Аннотация: Актуальность исследования обусловлена необходимостью повышения уровня автоматизации процесса сбора данных при использовании услуг центров информационной безопасности (security operation centers) и систем управления инцидентами информационной безопасностью (SIEM-системы). В статье представлено сравнение наиболее популярных SIEM-систем, а также возможностей их подключения к различным источникам данных о выявленных событиях и инцидентах информационной безопасности. Данная статья направлена на выявление способа (или метода) сбора данных о событиях и инцидентах информационной безопасности с использованием интерфейсов информационного взаимодействия консольного ввода/вывода в автоматическом режиме. Материалы статьи представляют практическую ценность для специалистов и разработчиков, работающих в области информационной безопасности, а также теоретическую ценность для учетных, осуществляющих свои исследования как в области информационной безопасности, так и в области информационных технологий в целом.
Ключевые слова: база данных, сбор данных, событие информационной безопасности, инцидент информационной безопасности, безопасность информации, центр информационной безопасности, SIEM-система, автоматизированная система управления, автоматизация, сопряжение баз данных.

В настоящее время наблюдается активное развитие информационных технологий, а также повышение уровня автоматизации всех возможных сфер деятельности людей, предприятий и организаций, а также государственных систем. Уже сегодня средства вычислительной техники используются для решения бытовых, социальных и финансовых вопросов.

Наиболее важной и наиболее критичной стороной такого развития становится обработка информации с использованием централизованных автоматизированных систем различного назначения, в которых циркулирует и обрабатывается как общедоступная информация, так и информация ограниченного доступа.

Такое положение дел создает предпосылки к осуществлению атак различного рода на такие автоматизированные системы [1]. При этом объектом атаки может быть, как обрабатываемая в системе информация

(например, при попытке получения несанкционированного доступа к банковскому счету физического или юридического лица), так и сама система. В качестве примера могут выступать атаки на автоматизированную систему управления подсистемами электростанций [2] или блокирование работы всей системы [3,4].

Для решения задач противодействия таким угрозам создаются центры информационной безопасности (security operation center или SOC-центры), осуществляющие контроль работы средств защиты информации и аудит защищаемых автоматизированных систем [5,6]. Использование центров информационной безопасности значительно увеличивает уровень защищенности информации и автоматизированных систем в целом за счет:

привлечения дополнительного персонала, высококвалифицированного в области защиты информации;

использования дополнительных средств защиты информации;

использования средств проведения комплексной аналитической обработки информации;

сбора данных о состоянии информационной безопасности из инфраструктур нескольких контролируемых организаций;

расширения средств противодействия компьютерным атакам и т. п.

Схема сопряжения инфраструктуры предприятий и организаций с инфраструктурой центра информационной безопасности представлена на рисунке 1:

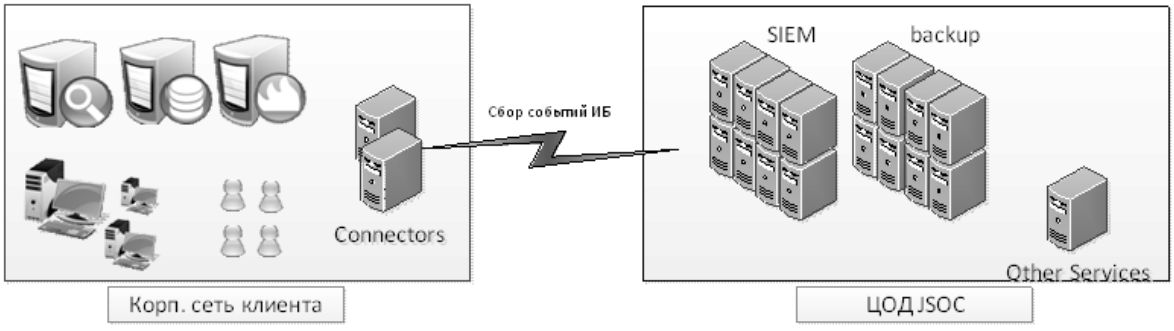

Рис. 1. – Схема сопряжения инфраструктур

При этом, в центр информационной безопасности осуществляется передача данных о выявленных событиях и инцидентах информационной безопасности со всех средств защиты информации и всего коммутационного оборудования, имеющегося в составе инфраструктуры контролируемого предприятия.

Основным инструментом, осуществляющим сбор данных о выявленных событиях и инцидентах информационной безопасности, в инфраструктуре центров информационной безопасности является система управления инцидентами информационной безопасности (или SIEM-система) [7].

Кроме того, SIEM-системы осуществляют и решение следующих задач:

контроль аутентификации пользователей;

контроль активности вредоносного программного обеспечения;

мониторинг сетевого трафика;

контроль целостности системных файлов;

проведение расследования компьютерных инцидентов;

сбор и ведение статистики событий и инцидентов информационной безопасности;

выявление скрытых инцидентов информационной безопасности, и др.

Таким образом, для эффективного решения своих задач, SIEM-система должна осуществлять сбор данных с максимально возможного количества источников, которые эти данные могут предоставить. Для этого необходимо, чтобы в составе SIEM-системы был модуль сопряжения, способный осуществлять сбор с источников таких данных.

Список интерфейсов межпрограммного взаимодействия наиболее популярных SIEM-систем различных производителей представлен в таблице 1 [8-10].

Таблица № 1

Возможности SIEM-систем по сопряжению с различными источниками

	Syslog	Windows Event Log	Windows File Log	NetFlow	ODBC	OSSEC-WEB	АПМДЗ	Cisco NSEL	SQLite
Splunk ES	+	+	+	+	+	+	-	+	-
Qradar SIP	+	+	+	+	+	-	-	+	-
McAffee NitroSecurity	+	+	+	+	+	-	-	-	-
MaxPatrolSIEM	+	+	+	+	+	-	-	-	-
Rusiem	+	+	+	+	+	-	-	+	-
ArcSight	+	+	+	+	+	+	-	-	-
OSSIM	+	-	-	+	+	+	-	-	-
Комрад	+	+	+	+	+	+	-	+	+

Однако, не все источники данных о выявленных событиях и инцидентах информационной безопасности обладают интерфейсами межпрограммного взаимодействия. Например, такими интерфейсами не обладают:

OSSEC-WEB – разновидность системы обнаружения вторжений, направленная на представление информации через собственный WEB-сервер;

АПМДЗ «Центурион» – программно-аппаратный модуль доверенной загрузки, осуществляющий локальное хранение системных журналов;

АПМДЗ «Максим-М1» – программно-аппаратный модуль доверенной загрузки, осуществляющий локальное хранение системных журналов;

средства защиты информации, использующие в качестве хранилища локальную реляционную базу данных SQLite (например Dr.Web Server Security Suite).

Формализацию данного процесса можно представить в следующем виде:

$$I = \{R_1, R_2, \ldots, R_n\}, \quad (1)$$

где I — множество всех возможных интерфейсов информационного взаимодействия источников данных о выявленных событиях и инцидентах информационной безопасности (R_n).

Исходя из того, что каждое средство защиты информации может обладать интерфейсами информационного взаимодействия 3-х типов (программного интерфейса, графического интерфейса пользователя и интерфейса консольного ввода/вывода), множество всех интерфейсов, входящих в состав одного средства защиты информации, можно рассчитать по следующей формуле:

$$R = \{r^p, r^h, r^g\}, \text{ где } r = \begin{cases} 1, \text{если интерфейс существут} \\ \varnothing, \text{если интерфейс не существует} \end{cases}, \quad (2)$$

где r^p – интерфейс программного взаимодействия, r^h – интерфейс консольного ввода/вывода, r^g – графический интерфейс пользователя.

При этом, количество интерфейсов информационного взаимодействия SIEM-системы можно рассчитать по следующей формуле:

$$R^p = \{ R \mid r^p \neq \varnothing \}, \quad (3)$$

$$I_s = R^p, \quad (4)$$

где R^p – множество средств защиты информации, обладающих интерфейсами программного взаимодействия.

Особое внимание следует обратить на то, что все источники данных о выявленных событиях и инцидентах информационной безопасности в конечном счете направлены на работу с пользователем, а значит, обладают интерфейсами взаимодействия с человеком (графический пользовательский интерфейс или средства консольного ввода/вывода). Следовательно, реализация возможности их использования в составе системы сбора данных о выявленных событиях и инцидентах информационной безопасности повысит и уровень автоматизации процесса сбора таких данных. При этом, множество всех возможных интерфейсов взаимодействия источников данных о выявленных событиях и инцидентах информационной безопасности примет следующий вид:

$$R^h = \{ R \mid r^h \neq \varnothing \}, \quad (5)$$

$$I'_s = R^p \cup R^h, \quad (6)$$

где R^h – множество средств защиты информации, обладающих интерфейсами взаимодействия консольного ввода/вывода.

Таким образом, появляется возможность расширения функциональных возможностей SIEM-системы, которая, в свою очередь, увеличивает и эффективность работы центров информационной безопасности.

Для реализации такой возможности предлагается:

1. Определить порядок сбора данных о выявленных событиях и инцидентах информационной безопасности;

2. Определить правило преобразования данных о выявленных событиях и инцидентах информационной безопасности;

3. Определить порядок внесения данных о выявленных событиях и инцидентах информационной безопасности в базу данных центра информационной безопасности.

На первом этапе необходимо обратить внимание на то, что информационный обмен между человеком и источником данных о

выявленных событиях и инцидентах информационной безопасности осуществляется по форме «запрос-ответ», исходя из чего, необходимо составить правила формирования запроса.

При использовании такого подхода необходимо обратить внимание на то, что большинство источников данных о выявленных событиях и инцидентах информационной безопасности способны функционировать в консольном режиме, с использованием терминала командной строки. Следовательно, для формирования запроса к удаленной базе данных необходимо создать набор команд для подключения к интерфейсу информационного взаимодействия, осуществления запроса к базе данных источника данных о выявленных событиях и инцидентах информационной безопасности и обработки полученного ответа.

Так как база данных удаленного источника будет иметь определенную структуру, большая часть запроса для получения данных о выявленных событиях и инцидентах информационной безопасности будет статичной, а значит, не будет видоизменяться. Динамическая часть будет видоизменяться закономерно.

Например, для обращения к удаленной базе данных текстового формата, отдельные элементы команды (набора команд) будут такими:

запрос на подключение к удаленному рабочему месту — статический;

команда вывода содержания файла — статический;

номер выводимой строки — динамический;

расположение и название файла — статический.

При этом, номер строки представляет собой простую арифметическую прогрессию с шагом 1.

На втором этапе следует обратить внимание на то, что форма запроса к любой базе данных позволяет определить форму ответа. То есть, при формировании однотипных запросов к базе данных будут получены

однотипные ответы (за исключением случаев получения технических сообщений от системы управления базой данных). То есть, полученные ответы от конкретного источника данных будут находится в одной форме, что позволяет определить порядок классификации отдельных элементов ответа.

На третьем этапе следует обратить внимание на то, что информационный обмен с базой данных SIEM-системы также осуществляется по форме «запрос-ответ», исходя из чего, необходимо составить правило формирования запроса.

База данных SIEM-системы будет иметь определенную структуру, так же как и в случае обращения к удаленным источникам, и большая часть запроса на внесение данных о выявленных событиях и инцидентах информационной безопасности будет статичной. Динамическая же часть будет получена при выполнении второго этапа.

Таким образом, расширение функционала SIEM-системы за счет сбора данных о выявленных событиях и инцидентах информационной безопасности представляется реализуемым. На рисунке 2 [11] представлен алгоритм работы модуля сопряжения, программная реализация которого способна выполнять задачу сбора данных о выявленных событиях и инцидентах информационной безопасности в условиях отсутствия интерфейсов межпрограммного взаимодействия.

Следовательно, существует возможность повышения уровня автоматизации процессов сбора данных о выявленных событиях и инцидентах информационной безопасности центров информационной безопасности, которая:

- позволяет повысить эффективность процесса сбора данных о выявленных событиях и инцидентах информационной безопасности;

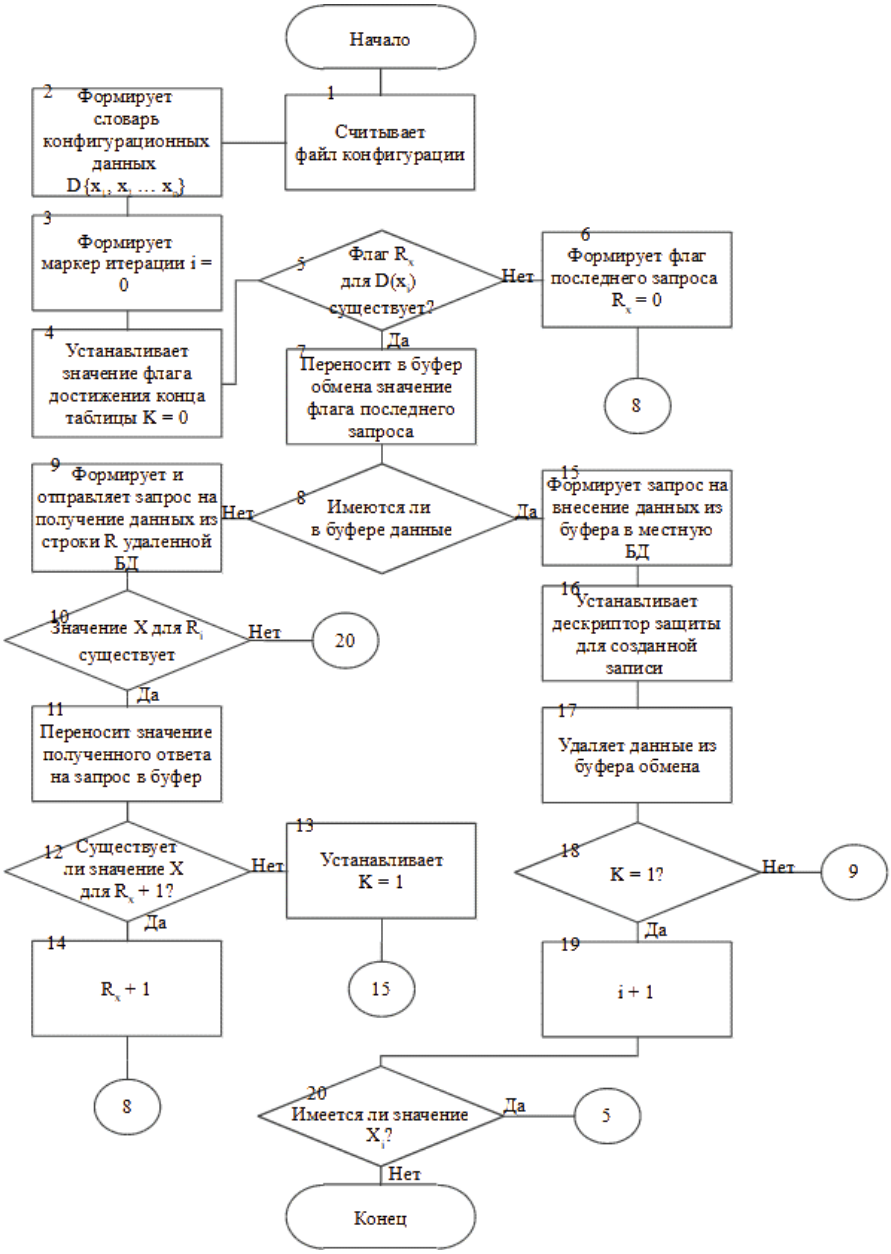

Рис. 2. – Алгоритм автоматизированного сбора данных [11]

- требует проведения модернизации только SIEM-системы, используемой в центре информационной безопасности;

- не требует вмешательства в инфраструктуры контролируемых предприятий и организаций;

- позволяет адаптировать структуру запросов, при наличии нескольких однотипных источников, реализованных по различным принципам.

Литература

1. Тершуков Д.А. Анализ современных угроз информационной безопасности // NBI-technologies. Волгоград. 2018. №3. С.6-11.

2. Харланов А.С., Белый Р.В. Новые реалии ведения войны: «кибертерроризм» и информационные войны // Юридическая наука. Москва. 2021. №6. С 106-110.

3. Курейчик В.М., Сахарова О.Н., Пирожков С.С. Угрозы в области хранения данных // Инженерный вестник Дона. 2021. №7. URL: ivdon.ru/ru/magazine/archive/n7y2021/7111 (Дата обращения 13.10.2021).

4. Петрова О.В., Королев И.Д., Крюков Д.М., Колесников В.Л. Способ оценки защищенности автоматизированной информационной системы специального назначения от DDOS-атак на основе теоретико-эмпирического подхода // Инженерный вестник Дона. 2021. №1. URL: ivdon.ru/ru/magazine/archive/n1y2021/6779 (Дата обращения 13.10.2021).

5. Махлин Б.М. Единая система управления информационной безопасности // Научный формат. 2019. №2 (2). URL: cyberleninka.ru/article/n/edinaya-sistema-upravleniya-bezopasnostyu-kompanii-kak-sovremennoe-sredstvo-obespecheniya-informatsionnoy-bezopasnosti.

6. Madani A., Rezayi S. and Gharaee H., "Log management comprehensive architecture in security operation center (soc)", Computational Aspects of Social Networks (CASoN) 2011 International Conference, 2011, pp. 284-289.

7. Шепелев А.Н., Букатов А.А., Пыхалов А.В., Березовский А. Н. Анализ подходов и средств обработки сервисных журналов // Инженерный вестник Дона. 2013. №4. URL: ivdon.ru/ru/magazine/archive/n4y2013/1966 (Дата обращения 13.10.2021).

8. Schutte J., Rieke R., Winkelvos T. Model-Based Security Event Management // Proc. Of the 6th Intern. Conf. on Mathematical Methods, Models

and Architectures for Computer Network Security: Computer Network Security (MMM-ACNS'12). Springer-Verlag, Berlin, Heidelberg, 2012. pp. 181-190.

9. Bachane I., Adsi Y. I. K. and Adsi H. C., "Real time monitoring of security events for forensic purposes in Cloud environments using SIEM", 2016 Third International Conference on Systems of Collaboration (SysCo), 2016, pp. 1-3,.

10. Detken K.-O., Jahnke M., Kleiner C., Rohde M., Combining Network Access Control (NAC) and SIEM functionality based on open source, 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017, pp. 31-42.

11. Королев И.Д., Литвинов Е.С., Крюков Д.М., Захарченко Р.И., Костров С.О. Способ проведения миграции и репликации данных с использованием технологии защищенного доступа к базе данных. Патент России № 2745679 Бюл. № 10. URL: new.fips.ru/registers-doc-view/fips_servlet?DB=RUPAT&DocNumber=2745679&TypeFile=html.

References

1. Tershukov D.A. NBI-technologies. Volgograd. 2018. №3. pp.6-11.

2. Harlanov A.S., Belyj R.V. Juridicheskaja nauka. Moskva. 2021. №6. Pp. 106-110.

3. Kurejchik V.M., Saharova O.N., Pirozhkov S.S. Inzhenernyj vestnik Dona. 2021. №7. URL: ivdon.ru/ru/magazine/archive/n7y2021/711.

4. Petrova O.V., Korolev I.D., Krjukov D.M., Kolesnikov V.L. Inzhenernyj vestnik Dona. 2021. №1. URL: ivdon.ru/ru/magazine/archive/n1y2021/6779.

5. Mahlin B.M. Nauchnyj format. 2019. №2 (2). URL: cyberleninka.ru/article/n/edinaya-sistema-upravleniya-bezopasnostyu-kompanii-kak-sovremennoe-sredstvo-obespecheniya-informatsionnoy-bezopasnosti.

6. Madani A., Rezayi S. and Gharaee H., "Log management comprehensive architecture in security operation center (soc)", Computational Aspects of Social Networks (CASoN) 2011 International Conference, 2011, pp. 284-289.

7. Shepelev A.N., Bukatov A.A., Pyhalov A.V., Berezovskij A. N. Inzhenernyj vestnik Dona. 2013. №4. URL: ivdon.ru/ru/magazine/archive/n4y2013/1966.

8. Schutte J., Rieke R., Winkelvos T. Model-Based Proc. Of the 6th Intern. Conf. on Mathematical Methods, Models and Architectures for Computer Network Security: Computer Network Security (MMM-ACNS'12). Springer-Verlag, Berlin, Heidelberg, 2012. pp. 181-190.

9. Bachane I., Adsi Y. I. K. and Adsi H. C., "Real time monitoring of security events for forensic purposes in Cloud environments using SIEM", 2016 Third International Conference on Systems of Collaboration (SysCo), pp. 1-3.

10. Detken K.-O., Jahnke M., Kleiner C., Rohde M., Combining Network Access Control (NAC) and SIEM functionality based on open source, 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), pp. 31-42, 2017.Korolev I.D., Litvinov E.S., Krjukov D.M., Zaharchenko R.I., Kostrov S.O. Sposob provedenija migracii i replikacii dannyh s ispol'zovaniem tehnologii zashhishhennogo dostupa k baze dannyh [A method of data migration and replication using secure database access technology]. Patent Rossii № 2745679 Bjul. № 10. URL: new.fips.ru/registers-doc-view/fips_servlet?DB=RUPAT&DocNumber=2745679&TypeFile=html.