СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2017. – № 3 (89).** – 124–132

СООБЩЕНИЯ

УДК 004.492.3

ОБЗОР SIEM НА РОССИЙСКОМ РЫНКЕ*

К.А. ДОНСКОЙ[1], Л.С. ЛЕВИН[2], В.А. ТРУШИН[3]

[1] *630087, РФ, г. Новосибирск, Немировича-Данченко, 136, Новосибирский государственный технический университет, студент, кафедра защиты информации. E-mail: kirdon96@mail.ru*
[2] *630087, РФ, г. Новосибирск, Немировича-Данченко, 136, Новосибирский государственный технический университет, студент, кафедра защиты информации. E-mail: tynameislev@bk.ru*
[3] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент кафедры защиты информации. E-mail: troshina@dean.cs.nstu.ru*

Данная работа рассматривает проблемы, на которых основаны задачи работы систем управления информационной безопасностью крупного предприятия, механизмы реализации решений таких задач и базовые принципы, лежащие в основе SIEM. Прежде чем затронуть непосредственно российский рынок SIEM, мы рассматриваем историю и развитие систем управления событиями информационной безопасности. Из истории разработки SIEM мы получаем идеи и направления ее развития и потенциал будущих систем. Мы подчеркиваем интеллектуальность данных систем и широкие возможности применения в любых направлениях информационной безопасности. Применение современных систем позволяет кооперировать эффективные средства и системы защиты информации в единый защитный рубеж. На основе рассматриваемых данных формируются представления качественного и современного продукта SIEM, отвечающего актуальным требованиям информационной безопасности, на которые мы опираемся при отборе систем представителей российского рынка. Проанализировав рынок, мы строим сравнительную таблицу, позволяющую определить отличительные особенности систем и затраты на приобретение и использование данных систем, что поможет потребителям в выборе SIEM для внедрения в свои предприятия. Несмотря на множество актуальных и инновационных решений рынка, мы отбираем самые технологичные и удобные для внедрения системы, которые представлены как зарубежными лидерами рынка, так и отечественными производителями. При выборе систем основными критериями являются: кроссплатформенность, возможность совместного использования с наибольшим количеством различных систем безопасности, цена периферийного программного обеспечения для SIEM продукта и обслуживания, интеллектуальность корреляционных механизмов и механизмов принятия решений в аномальных ситуациях. Также мы уделяем внимание соблюдению требований законодательства Российской Федерации и непосредственно ФСТЭК.

* Статья получена 24 апреля 2017 г.

Ключевые слова: управление безопасностью, корреляция, сбор информации, анализ рынка, преимущества систем

DOI: 10.17212/2307-6879-2017-3-124-132

ВВЕДЕНИЕ

SIEM (Security information and event management) – система управления информацией и событиями, автоматизации процессов выявления и реагирования на инциденты информационной безопасности. SIEM, как и многие другие продукты информационной безопасности, появились в результате объединения систем SIM (Security information management – управление информационной безопасностью) и SEM (Security event management – управление событиями безопасности).

В процессе менеджмента информационной безопасности возникают следующие типовые проблемы, разрешаемые с помощью SIEM:

- большие размеры журналов событий, непригодных для анализа;
- повторяющиеся события (усложнение анализа);
- требуется сопоставлять события из разных источников для выявления сложных событий (атак), что нереализуемо вручную;
- хранение журналов событий большого количества различных информационных систем для анализа и расследований.

Алгоритм работы SIEM

1. SIEM получает и консолидирует информацию о событиях из различных источников, таких как межсетевые экраны, IPS, антивирусы, операционные системы и т. д. посредством резидентных программ (агентов), выполняя фильтрацию полученных данных, приводя их к единому формату.

2. Сервер-коллектор производит аккумуляцию событий от множества агентов.

3. Сервер баз данных и хранилища позволяет создавать (получая события от серверов-коллекторов) и централизованно хранить единые журналы событий.

4. SIEM коррелирует события – ищет взаимосвязи и закономерности, выполняет анализ информации посредством сервера корреляции, что позволяет с высокой вероятностью определять аномалии, потенциальные угрозы, сбои в работе, попытки несанкционированного доступа, атаки.

5. SIEM выполняет процессы реагирования (например, автоматическое оповещение) и менеджмента на инциденты информационной безопасности.

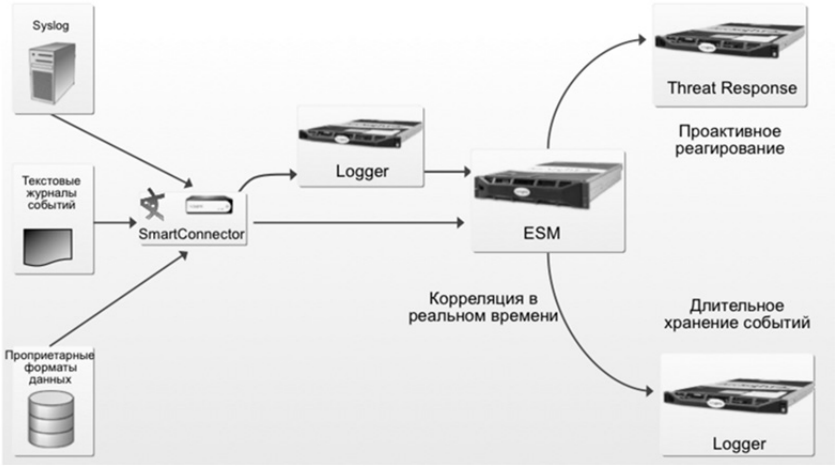

Рис. 1. Принцип SIEM на базе HP ArcSight

Исходя из вышесказанного эффективная SIEM должна поддерживать следующие механизмы обработки событий информационной безопасности:

- консолидация – это сбор, нормализация (устранение избыточной информации), помещение данных в единое хранилище;
- агрегирования событий – группирование однотипных событий вместе;
- корреляция – поиск связей между событиями безопасности и другой информацией безопасности.

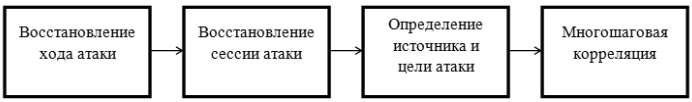

Рис. 2. Механизм корреляции

Здесь многошаговая корреляция отвечает за распознание сложных сценариев, состоящих из отдельных атак.

Приоритизация – выделение сценариев атак в соответствии с их приоритетом для пользователя.

С помощью приведенных механизмов SIEM способны выявлять:

- сетевые атаки;
- вирусные заражения;
- попытки несанкционированного доступа к конфиденциальной информации;
- ошибки и сбои в работе информационных систем;

- уязвимости;
- ошибки конфигураций в средствах защиты и информационных системах и т. д.

1. АНАЛИЗ РЫНКА

Идея SIEM зародилась в недалеком 2005 году. Марк Николетт и Амрит Вильямс из компании Gartner (ныне эксперт рынка SIEM) ввели понятие управления событиями информационной безопасности SIEM. Идея создания такой системы – «бриллиант» в управлении событиями информационной безопасности крупного бизнеса, но он требует особой огранки, на которую ушли последние 10 лет.

2006 год: корпорация EMC приобретает ныне дочернюю RSA Security, отвечающую за разработку решений в области информационной безопасности, следом приобретая Network Intelligence, передает ее SIEM-решение enVision в RSA Security. До 2009 года enVision – флагман рынка SIEM. 2010 год: компания HP покупает компанию ArcSight (на тот момент имеющую значительные наработки своей SIEM), данный продукт остается лидером рынка по сей день. 2011 год: компания IBM приобретает американского разработчика – компанию Q1 Labs. От Q1 Labs в портфель IBM переместилось решение QRadar, вышедшее на второе место в Magic Quadrant for Security Information and Event Management (магический квадрат – рейтинг лучших SIEM продуктов). В то же время McAfee покупает компанию NitroSecurity и занимает 3-е место в рейтинге SIEM.

Следующим шагом развития стало объединение SIEM с Big Data технологиями. Первым подобным проектом стал RSA Security Analytics от EMC. Он сочетает в себе не только SIEM, но и анализ сетевого трафика. Компания IBM также подхватила новое направление развития и, в свою очередь, представила решение IBM Security Intelligence with Big Data, объединяющее SIEM-решение QRadar с функциями IBM InfoSphere BigInsights.

Нижеприведенный список представляет российский рынок SIEM:

1. IBM QRadar SIEM;
2. HP ArcSight;
3. Tibco Loglogic;
4. McAfee NitroSecurity;
5. Symantec SSIM;
6. RSA Envision;
7. Splunk LogRhythm;
8. «НПО «Эшелон» КОМРАД;
9. OSSIM (бесплатна, Open Source);
10. Security Capsule;
11. MaxPatrol;
12. «СёрчИнформ SIEM» (на стадии развития, «КИБ Сёрчинформ» (DLP) входит в рейтинг Gartner);
13. StaffCop Enterprise.

Сравнение наиболее популярных представителей рынка

№ п/п	Название	Платформа	СУБД	Количество коннекторов	Преимущество перед конкурентами	Цена
1	HP ArcSight	Red Hat Enterprise Linux, версии 6.4 и 6.5 SUSE 11 SP3 (64-разрядная) Windows Server 2012	Своя CORR-E	300 +	• HP ArcSight Configuration Management позволяет провести конфигурацию сетевого оборудования и настроек безопасности • HP ArcSight Fraud Detection – уникальное решение для выявления и предотвращения мошенничества в области интернет-банкинга и банковских (пластиковых) карт	от 4 млн руб.
2	IBM QRadar SIEM	Red Hat Enterprise 6.3	Своя разработка	300+	• Предусматривает автообнаружение источников логов, приложений, активов сети • Осуществляет автоматический аудит конфигурации и автонастройку • Проводит приоритизацию активов сети • Обеспечивает автообновление сигнатур • Предоставляет тысячи предопределенных правил и отчетов	от 3 млн руб.
3	McAfee NitroSecurity	Red Hat Enterprise Linux, версии 6.4 и 6.5 SUSE 11 SP3 (64-разрядная) Windows Server 2012	NitroEDB	400	• Встроенный механизм контроля нормативно-правового соответствия • McAfee Global Threat Intelligence for Enterprise Security Manager (ESM), предназначенная для работы с большими данными в сфере безопасности • McAfee Application Data Monitor выполняет дешифрование полного сеанса приложения до уровня 7, обеспечивая комплексный анализ всей информации непосредственного содержимого приложения	от 2,3 млн руб.

Окончание таблицы

№ п/п	Название	Платформа	СУБД	Количество коннекторов	Преимущество перед конкурентами	Цена
4	КОМРАД от «НПО «Эшелон»	ОС МСВС, ОС Astra Linux, ОС Windows	MySQL, MSSQL, Postgres, Oracle, Sqlite3	–	• Удаленный контроль параметров конфигурации и работы отслеживаемых объектов • Интеграция со следующими отечественными защищенными платформами и системами защиты информации: ОС МСВС, ОС Astra Linux, Сканер-ВС, МЭ и СОВ Рубикон, Xspider, СОПКА и др.	от 1 млн руб.
5	MaxPatrol SIEM	ОС Windows XP\7\8 ОС Windows Server\2008\ 2010\2012	ElasticSearch, MongoDB, MS SQL Express	50 из коробки	• С помощью протокола удаленного доступа происходит подключение к системе, аутентификация, авторизация, сбор логов. На данный момент SIEM Maxpatrol работает в основном только в связке с системой контроля защищенности и соответствия стандартам Maxpatrol	от 3 млн руб.
6	Security Capsule	ОС Windows XP\7\8 ОС Windows Server\2008\ 2010\2012 ОС Red Hat начиная с версии 4.8 Red Hat Enterprise Linux 6.X	MySQL MS SQL	Любые источники событий поддерживающие транспортные протоколы. (SNMP)	• С целью снижения нагрузки на сеть передачи данных первичная обработка событий осуществляется на серверах Security Capsule, установленных в ЛВС • Выполняет все требования ФСТЭК по информационной безопасности • Программное решение, которое требует сравнительно малых вычислительных мощностей	от 200 тыс. руб.

ЗАКЛЮЧЕНИЕ

Таким образом, SIEM необходимы в предприятиях с масштабными информационными ресурсами, где одновременно происходит большое число событий информационной безопасности. Проанализировав текущий россий-

ский рынок SIEM, мы выделили и сравнили шесть наиболее востребованных продуктов. Данные системы охватывают актуальные проблемы SIEM: гетерогенность источников, поддержку и обновления от вендора, защищенность системы, настройку и простоту в использовании. Несмотря на высокую стоимость продуктов, выбранные SIEM решают поставленные задачи информационной безопасности и управления информационными ресурсами, актуальны в обновлениях и имеют большую базу совместимости с источниками сбора событий (агентами).

СПИСОК ЛИТЕРАТУРЫ

1. Анализ методов корреляции событий безопасности в SIEM-системах. Ч. 1 / А.В. Федорченко, Д.С. Левшун, А.А. Чечулин, И.В. Котенко. // Труды СПИИРАН. – 2016. – Вып. 47. – С. 5–27.

2. *Дрозд А.* Обзор SIEM-систем на мировом и российском рынке [Электронный ресурс] // Anti-Malware: web-сайт. – 2014. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market (дата обращения: 29.11.2017).

3. *Хамакев Д.* SIEM: ответы на часто задаваемые вопросы [Электронный ресурс] // Хабрахабр: web-сайт. –. 2013. – URL: https://habrahabr.ru/post/172389/ (дата обращения: 29.11.2017).

4. *Шелестова О.* Что такое SIEM? [Электронный ресурс] // SecurityLab.ru: web-сайт. – 2012. – URL: http://www.securitylab.ru/analytics/430777.php (дата обращения: 29.11.2017).

5. Сравнение SIEM систем [Электронный ресурс] // SIEM Analytics: web-сайт. – 2015. – URL: http://siem.guru/compare_SIEM_systems.php (дата обращения: 29.11.2017).

6. *Ниязов Т.* Сравнение SIEM-решений для построения SOC [Электронный ресурс] // Jet Info. – 2015. – № 8. – URL: http://www.jetinfo.ru/jetinfo_arhiv/soc-kak-chasovoj-mekhanizm/sravnenie-siem-reshenij-dlya-postroeniya-soc/2015 (дата обращения: 29.11.2017).

Донской Кирилл Александрович, студент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – современные системы информационной безопасности. E-mail: kirdon96@mail.ru

Левин Лев Сергеевич, студент кафедры защиты информации Новосибирского государственного технического университета. Основное направление

научных исследований – современные системы информационной безопасности. E-mail: mynameislev@bk.ru

Трушин Виктор Александрович, кандидат технических наук, доцент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – техническая защита информации. Имеет более 150 публикаций. E-mail: rastr89@mail.ru

The Review of SIEM In The Russian Market*

K.A. Donskoy[1], L.S. Levin[2], V.A. Trushin[3]

[1] *Novosibirsk State Technical University, 136 Nemirovicha-Danchenko street, Novosibirsk, 630087, Russian Federation, student of information security department. E-mail: kirdon96@mail.ru*
[2] *Novosibirsk State Technical University, 136 Nemirovicha-Danchenko street, Novosibirsk, 630087, Russian Federation, student of information security department. E-mail: mynameislev@bk.ru*
[3] *Novosibirsk State Technical University, 136 Nemirovicha-Danchenko street, Novosibirsk, 630087, Russian Federation, candidate of Technical Sciences, associate professor of information security department. E-mail: rastr89@mail.ru*

This article examines the issues on which the objectives of performance management system information security, large enterprise, implementation mechanisms of decisions of such tasks and the basic principles underlying the SIEM are based. Before describing the Russian market of SIEM, we take a look at the history and development of security event management system. From history of SIEM design we get the ideas and directions of development and potential of future systems. We emphasize the intelligence of these systems and wide range of usage in all areas of information security. The application of modern systems allows cooperating effective tools and systems of information protection in a single protective barrier. Based on this data the submission of high-quality and modern SIEM product, which satisfy the current requirements of information security that we rely on the selection of systems of representatives of the Russian market, is formed. After analyzing the market, we construct a comparative table to determine the distinctive features, the cost of acquisition and usage of the systems from each other and will assist consumers in choosing a SIEM to implement in their businesses. Despite the relevant and innovative solutions in the market, we select systems, the most technologically advanced and convenient for the implementation, which are represented by foreign leaders and high-quality domestic manufacturers. In selection of systems the main criteria are: cross-platform, the possibility of shared use with the greatest number of different security systems, price of peripheral software for SIEM product and service, intelligence of correlation mechanisms and decision-making mechanisms in abnormal situations. We also pay attention to observance of requirements of the Russian Federation legislation and directly FSTEC.

* *Received 24 April 2017.*

Keywords: security management, correlation, information collection, the analysis of the market, advantage of systems

DOI: 10.17212/2307-6879-2017-3-124-132

REFERENCES

1. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. Analiz metodov korrelyatsii sobytii bezopasnosti v SIEM-sistemakh. Ch. 1 [Analysis of methods of correlation of security events in SIEM-systems. Pt. 1]. *Trudy SPIIRAN – SPIIRAS Proceedings*, 2016, iss. 47, pp. 5–27.

2. Drozd A. Obzor SIEM-sistem na mirovom i rossiiskom rynke [Overview of SIEM-systems in the world and Russian market]. *Anti-Malware*: website. 2014. (In Russian). Available at: https://www.anti-malware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market (accessed 29.11.2017).

3. Khamakev D. SIEM: otvety na chasto zadavaemye voprosy [SIEM: answers to frequently asked questions]. *Khabrakhabr* [Habrahabr]: website. 2013. Available at: https://habrahabr.ru/post/172389/ (accessed 29.11.2017).

4. Shelestova O. Chto takoe SIEM? [What is SIEM?]. *SecurityLab.ru*: website. 2012. (In Russian). Available at: http://www.securitylab.ru/analytics/430777.php (accessed 29.11.2017).

5. Sravnenie SIEM sistem [Comparison of SIEM systems]. *SIEM Analytics*: website. 2015. (In Russian). Available at: http://siem.guru/compare_SIEM_systems.php (accessed 29.11.2017).

6. Niyazov T. Sravnenie SIEM-reshenii dlya postroeniya SOC [Comparison of SIEM-solutions for the construction of SOC]. *Jet Info*, 2015, no. 8. (In Russian). Available at: http://www.jetinfo.ru/jetinfo_arhiv/soc-kak-chasovoj-mekhanizm/sravnenie-siem-reshenij-dlya-postroeniya-soc/2015 (accessed 29.11.2017).