DOI 10.37882/2223–2966.2020.06.24

РАЗРАБОТКА SIEM–СИСТЕМЫ НА БАЗЕ ОТКРЫТЫХ ТЕХНОЛОГИЙ ДЛЯ ПРЕДПРИЯТИЙ МАЛОГО И СРЕДНЕГО БИЗНЕСА

DEPLOYMENT OF OPEN SOURCE SIEM SYSTEM FOR SMALL AND MEDIUM BUSINESS ENTERPRISES

A. Mansurov
E. Shabala

Summary. SIEM system is a necessity for business enterprises to aggregate and process all the data essential for cyber security incidents investigations. Small and medium business often cannot bear the costs of commercial SIEM systems, so the only option available is to look for alternatives. In this paper, the open source SIEM system is proposed. The proposed SIEM system is capable to collect all the data and perform an automatic and manual analysis and event correlation, thus, is deemed to be suitable to act as a competent SIEM system. It provides the necessary analysis tools for effective cyber security incidents processing and generating reports and alerts for cyber security personnel of small and medium business enterprises.

Keywords: SIEM, security incident, Suricata, ELK, Wazuh.

Мансуров Александр Валерьевич
К.т.н., доцент, ФГБОУ ВО «Алтайский государственный университет», г. Барнаул
mansurov.alex@gmail.com
Шабала Егор Евгеньевич
ФГБОУ ВО «Алтайский государственный университет», г. Барнаул
shegcapcom@gmail.com

Аннотация. Развертывание SIEM-системы для агрегации и обработки данных, критичных для анализа инцидентов информационной безопасности является необходимостью для всех современных предприятий. Однако, предлагаемые коммерческие SIEM-решения на этапах приобретения и эксплуатации являются достаточно дорогими для большинства предприятий среднего и малого бизнеса. Доступной альтернативой в этом случае можно назвать SIEM-системы, построенные с применением компонент на базе открытых технологий. В данной работе предложен подход к построению эффективной SIEM-системы, полностью базирующейся на использовании открытых программных решений. Предлагаемая SIEM-система является полностью информативной, способна выполнять предварительный автоматизированный анализ данных и предлагает необходимый инструментарий для специалистов по защите информации для осуществления комплексного анализа и обработки возникающих инцидентов информационной безопасности на предприятии.

Ключевые слова: SIEM, инцидент безопасности, Suricata, ELK, Wazuh.

Введение

Успешная деятельность современного предприятия базируется на его отлаженной и стабильно работающей ИТ инфраструктуре, на базе которой функционируют жизненно-важные информационные системы предприятия, обеспечивающие его бизнес-процессы. Решение задач информационной безопасности и защиты информации для современных ИТ инфраструктур является комплексной проблемой, требующей своевременный контроль за составляющими элементами, циркулирующими информационными потоками и происходящими событиями. Применяемые решения генерируют огромные потоки событий информационной безопасности. Журналы событий хранятся в различных форматах и местах элементов ИТ инфраструктуры, ручной поиск и сопоставление необходимой информации для определения инцидентов информационной безопасности осуществить крайне сложно [1].

Для решения подобных проблем применяются SIEM-системы (Security Information and Event Management) — системы, которые осуществляют сбор широкого спектра данных системных событий, уведомлений служб безопасности и иной служебной информации в режиме реального времени и в отложенном режиме, накапливают эту информацию для последующего анализа и выявления последовательности событий, которые могут являться нарушениями информационной безопасности [1,2]. Типичная SIEM-система включает в себя специализированные агенты по сбору необходимой информации, которые устанавливаются на значимые элементы корпоративной ИТ инфраструктуры, средства сбора информации о событиях при помощи штатных способов, систему анализа сетевого трафика критичных сегментов корпоративной сети, систему накопления и хранения собранной информации, а также средства для осуществления коррелирования обрабатываемой поступившей информации по определен-

ным правилам для принятия решения в соответствии с заданными триггерами, индикаторами и сценариями действий. Основной задачей SIEM-системы при этом является автоматизация процесса обнаружения инцидентов информационной безопасности и своевременного оповещения о произошедшем инциденте.

На современном рынке доступно множество зарекомендовавших себя SIEM-решений отечественных и зарубежных производителей, такие как MaxPatrol SIEM, IBM QRadar Security Intelligence Platform, RuSIEM и т.п. [3]. Согласно исследованию, проведенному компанией IDC в 2018 г., отмечается эффективность работы предлагаемых решений и их существенный вклад в эффективное обнаружение и реагирование на выявленные инциденты на предприятиях разных отраслевых групп [4]. В то же самое время в исследовании указывается на трудности адаптации поставляемого решения под существующую ИТ инфраструктуру предприятия, отсутствие желаемой функциональности и необходимость регулярных существенных инвестиций в эксплуатацию SIEM-системы (при учете достаточно больших стартовых инвестиций, связанных с приобретением и развертыванием готового SIEM-решения). В этом случае предприятия малого и среднего бизнеса вынуждены либо пользоваться ограниченными версиями платных продуктов, либо полностью отказываться от внедрения данных систем, оставляя ИТ инфраструктуру без должной защиты.

Подобные недостатки могут быть преодолены при использовании SIEM-систем на базе открытых технологий и открытого кода. Существующие обзоры и анализы открытых SIEM-систем демонстрируют соответствие их функционала ожидаемым требованиям, отмечают гибкость и возможность узкопрофильной адаптации под возможности ИТ инфраструктуры, нужды и требования каждого конкретного предприятия [5,6]. Перспективным отмечается построение SIEM-системы на основе комплекса ELK Stack, включающего в себя распределенную систему хранения и поиска данных ElasticSearch, систему сбора и обработки получаемой служебной информации Logstash, а также систему визуализации и анализа данных Kibana [7]. Комплекс разрабатывается компанией Elastic B.V. вместе со всеми связанными проектами, имеет версии с свободно распространяемым открытым исходным кодом. Интегрирование информационных потоков сообщений служб информационной безопасности и системных журналов элементов ИТ инфраструктуры для последующей обработки при помощи ELK Stack позволит выполнять операции по анализу и коррелированию различных событий, зафиксированных в ИТ инфраструктуре предприятия и выполнять пошаговый анализ произошедших инцидентов информационной безопасности.

Данная работа предлагает подход к построению функциональной SIEM-системы на базе открытых технологий с использованием комплекса ELK Stack. Предлагаемое решение включает в себя использование технологий и решений обнаружения вторжений на уровне сети и хоста, генерирование правил корреляции и анализа данных, формирование уведомлений. Решение соответствует большинству популярных стандартов на построение процесса управления инцидентами и событиями информационной безопасности [8–10]. Данный подход может рассматриваться как альтернатива коммерческим SIEM-системам, не требующая существенных финансовых вложений на развертывание и обслуживание.

Предлагаемое SIEM-решение на основе открытых технологий

Предлагаемое SIEM-решение базируется на комплексной платформе ELK Stack (стек ELK), являющейся популярным решением на базе программного обеспечения с открытым кодом, применяющаяся для хранения и анализа разнообразной информации из системных журналов самого широкого спектра устройств и систем. ELK Stack содержит:

1. Масштабируемую базу данных ElasticSearch с функциями полнотекстового поиска по базе и выполнением анализа накопленной информации
2. Конвеерная система обработки записей системных журналов (лог-файлов) LogStash, которая нормализует и подготавливает данные для их помещения в базу ElasticSearch
3. Веб-ориентированная среда Kibana, предназначенная для визуализации накопленных данных, администрирования индексированных в базе данных записей и выполнения аналитических действий

В качестве основной системы сбора первичной служебной информации на серверах и рабочих станциях корпоративной ИТ инфраструктуры и осуществления ее первичного анализа используется открытое решение Wazuh [11], которое включает в себя:

1. Хост-ориентированный агентский компонент Wazuh Agent, который отвечает за сбор первичной информации и ее передачу по защищенному каналу (AES-256) к серверному компоненту.
2. Серверный компонент Wazuh Server, выполняющий удаленный контроль и администрирование агентских компонентов, прием собранной агентами информации и выполнение ее первичной обработки на основе встроенной конфигурируемой системы правил. Результативная информация отправляется в базу ElasticSearch для хранения и последующей работы с ней.

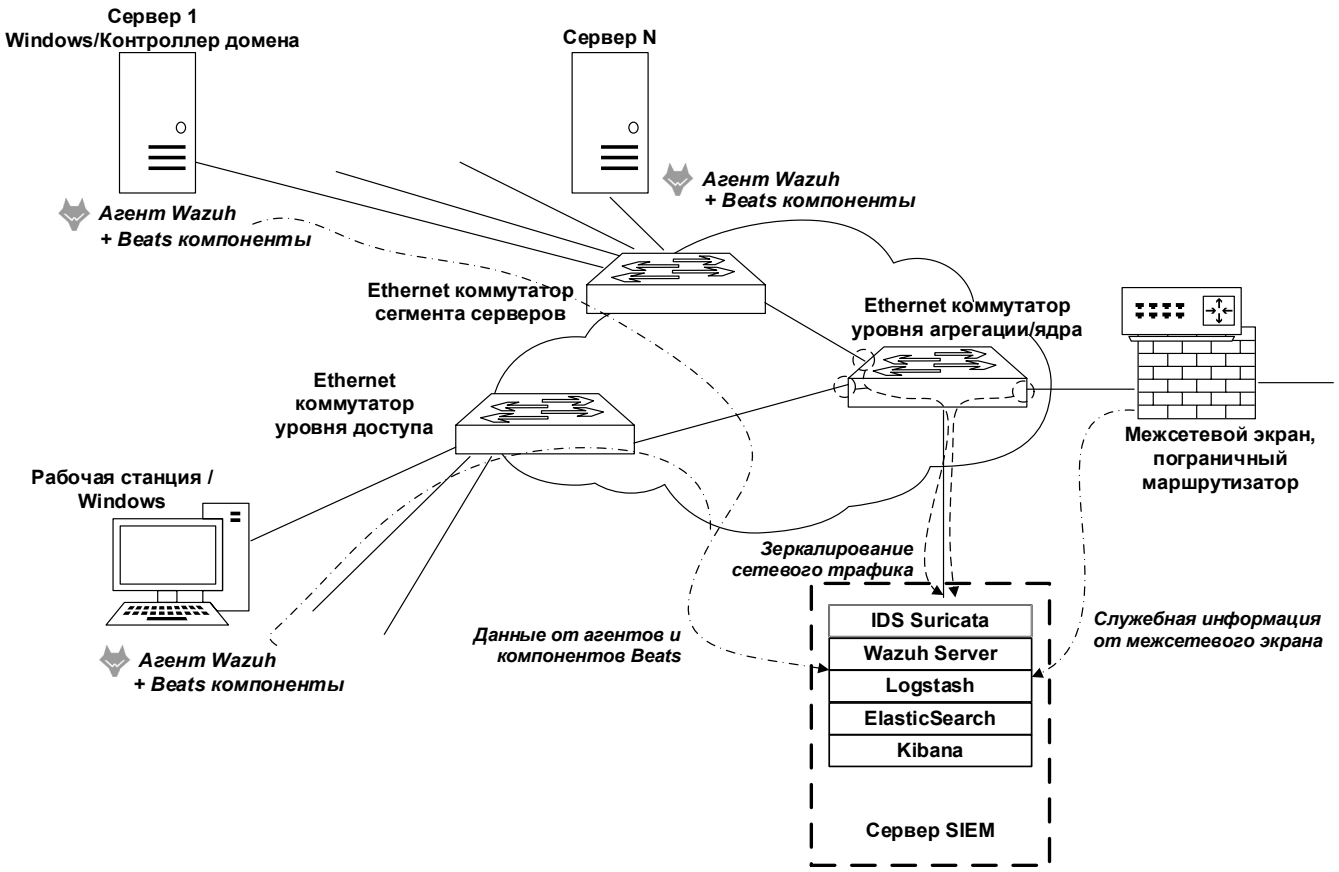


Рис. 1. Интеграция предлагаемого SIEM-решения в типовую корпоративную ИТ инфраструктуру

3. Встраиваемый в визуальную среду Kibana компонент Kibana App для управления серверными и агентскими компонентами Wazuh.

Агенты Wazuh работают на разных платформах, включая Windows, Linux, Mac OS X, AIX, Solaris и HP-UX. Они могут быть настроены и управляться с сервера Wazuh, в том числе сервер способен отправлять команды агентам, например, чтобы инициировать ответ при обнаружении угрозы. Основные возможности агентов, которые задействованы в предлагаемом решении:

- Сбор данных журнала и событий
- Мониторинг целостности файлов и ключей реестра
- Инвентаризация запущенных процессов и установленных приложений
- Мониторинг открытых портов и конфигурации сети
- Обнаружение руткитов или вредоносных артефактов
- Оценка конфигурации и мониторинг политики
- Произведение активных ответов на обнаруженные угрозы

Сбор дополнительной информации с рабочих станций и серверов корпоративной ИТ инфраструктуры дополняется (при необходимости) компонентами Beats, входящими в стек ELK.

Информация об активности в корпоративной сети предприятия собирается и анализируется при помощи открытой системы обнаружения вторжений (IDS) Suricata [11,12], которая обрабатывает сетевой трафик в режиме реального времени, использует мощные и обширные правила и язык сигнатур, имеет развитую поддержку сценариев Lua для обнаружения сложных угроз.

Общая схема интеграции предлагаемого SIEM-решения в типовую корпоративную ИТ инфраструктуру приведена на рис. 1. Информация о системных событиях, записи журналов на рабочих станциях и серверах собираются при помощи агентов и отправляются на SIEM-сервер. Сетевой трафик сегментов корпоративной сети, требующий мониторинга и анализа — входящий и исходящий трафик, трафик серверного сегмента и трафик направлений выше уровня доступа (агрегация и ядро корпоративной сети) — копируется при помощи технологий зеркалирования на входной интерфейс ана-

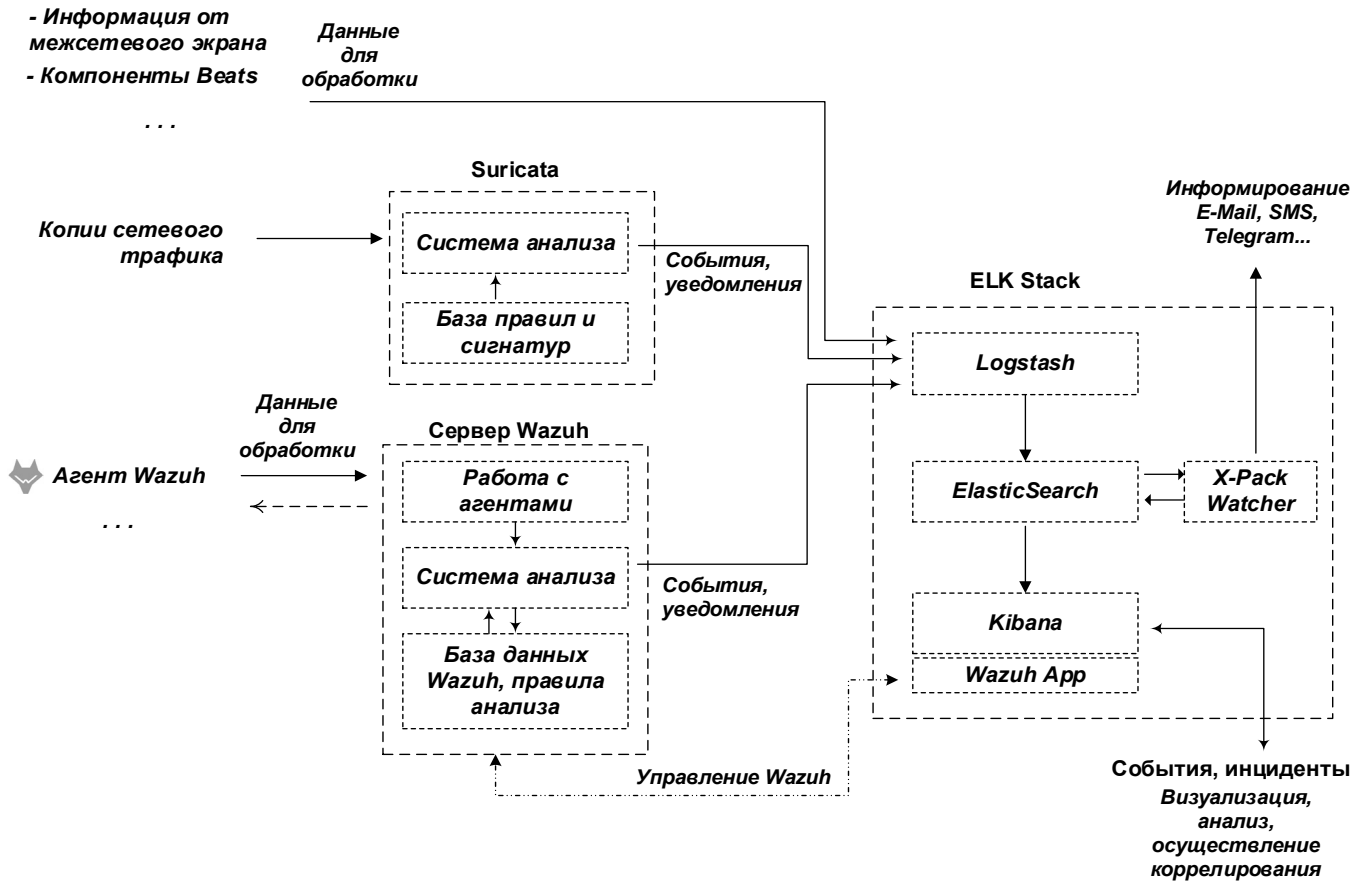


Рис. 2. Схема движения обрабатываемых потоков данных в предлагаемом SIEM-решении

лизатора сетевого трафика. В дальнейшем обработкой полученного трафика занимается система Suricata, конструктивно размещаемая на том же SIEM-сервере. При необходимости повышения производительности работы IDS-системы она может быть вынесена на отдельный сервер. Структурная схема движения обрабатываемых потоков данных в предлагаемом SIEM-решении представлена на рис. 2.

Анализ собранных данных выполняется в несколько этапов. Первоначальный автоматизированный анализ осуществляется при помощи встроенных систем анализа Wazuh и Suricata, которые работают на основании предварительно сконфигурированных систем правил. Этих действий достаточно для того, чтобы распознавать типовые ситуации и идентифицировать простые инциденты и нарушения безопасности. Прошедшая подобную обработку информация далее передается на дальнейшую обработку и хранение в базу ElasticSearch. В эту же базу попадает и исходная информация, получаемая при помощи компонентов Beats от элементов ИТ инфраструктуры напрямую (например, записи журнала межсетевого экрана).

Визуализация собранных данных, анализ и обнаружение событий, относящихся к инцидентам информационной безопасности, оператором или специалистом по защите информации «вручную» осуществляется при помощи веб-интерфейса Kibana. В Kibana настраиваются различные представления (dashboards) собранных данных, что позволяет использовать различные подходы для выполнения корреляции разных событий при расследовании инцидента и формировать свои собственные методики и алгоритмы корреляции. Обобщенная информация собирается на панелях представления таким образом, что оператор предлагаемого SIEM-решения может воочию наблюдать изменения тех или иных параметров системы, возникновение событий, обнаруженные атаки, их развития и последствия, а также меры, предпринятые после их обнаружения. Модуль визуализации данных Suricata позволяет анализировать полученные от IDS системы в более удобном формате, а модуль взаимодействия с Wazuh (Wazuh App) дополнительно предоставляет возможность по управлению работой Wazuh-сервера и агентов. Также модуль Wazuh включает в себя панели мониторинга для соответствия нормативным требованиям (например, PCI DSS, GDPR,

t	computer_name	com
t	event_data.AccountName	LocalSystem
t	event_data.ImagePath	winexesvc.exe
t	event_data.ServiceName	winexesvc
t	event_data.ServiceType	user mode service
t	event_data.StartType	demand start
#	event_id	7,045
t	host.name	W2012
t	keywords	Classic
t	level	Information
t	log_name	System
t	message	A service was installed in the system. Service Name: winexesvc Service File Name: winexesvc.exe Service Type: user mode service Service Start Type: demand start Service Account: LocalSystem
#	process_id	428
t	provider_guid	{555908d1-a6d7-4695-8e1e-26931d2012f4}
t	record_number	13414
t	source_name	Service Control Manager

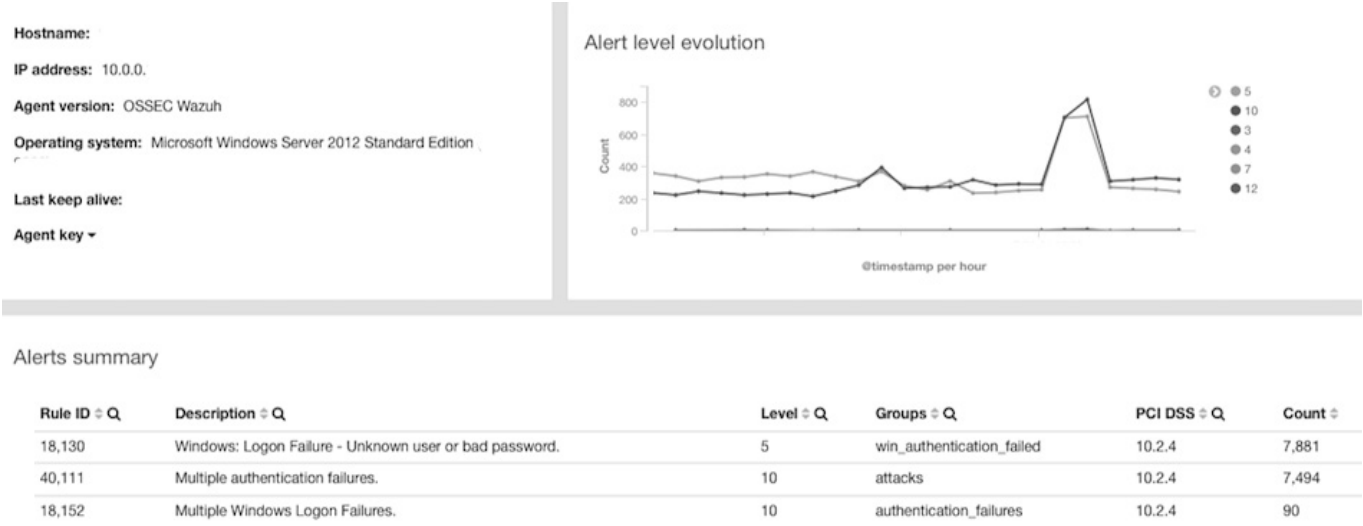
Рис. 3. Фрагмент полнотекстовой записи о событии в предлагаемой SIEM-системе

NIST, HPAA), обнаруженные уязвимые приложения, мониторинг целостности файлов, оценку конфигурации, события безопасности и т.п.

В качестве базового набора правил для Wazuh и Suricata используются стандартные наборы, включаемые в дистрибутивы указанных систем. Для IDS Suricata инсталлируется и с регулярной периодичностью обновляется набор готовых правил и сигнатур от OISF (Open Information Security Foundation), которые включают в себя наборы типа «Proofpoint Emerging Threats Open Rulesets», «Positive Technologies Attack Detection Team Ruleset», «Abuse.ch SSL Blacklist», «Threat Hunting Rules» и т.п. Отдельные локальные правила создаются и добавляются с учетом специфики ИТ инфраструктуры каждого конкретного предприятия, на котором разворачивается предлагаемое SIEM-решение.

Автоматизированные уведомления о зарегистрированных инцидентах и событиях в предлагаемой SIEM-системе, которые могут рассылаться специалистам по защите информации при помощи e-mail, SMS или иными способами, генерируются модулем X-Pack Watcher (является частью ELK Stack). Модуль X-Pack Watcher поддерживает развитую нотацию JSON для определения произвольных, определяемых пользователем событий и триггеров, а также желаемую реакцию системы на событие и срабатывание заданных триггеров. Этого функционала вполне достаточно для выполнения простейших автоматизированных действий по коррелированию событий и идентифицированию инцидентов безопасности.

Каждая зарегистрированная в предлагаемой SIEM-системе запись содержит достаточно большое количество информативных элементов, которые можно использовать для поиска, выполнения анализа и коррелирования цепочки записей в единое событие информационной безопасности. При необходимости число информативных элементов каждой записи может быть расширено при помощи функционала системы обработки записей Logstash. Визуальный интерфейс позволяет



Alerts summary

Rule ID	Description	Level	Groups	PCI DSS	Count
18,130	Windows: Logon Failure - Unknown user or bad password.	5	win_authentication_failed	10.2.4	7,881
40,111	Multiple authentication failures.	10	attacks	10.2.4	7,494
18,152	Multiple Windows Logon Failures.	10	authentication_failures	10.2.4	90

Рис. 4. Вывод информации при помощи панелей представления

работать с каждой записью в полнотекстовом режиме или использовать упрощенное представление при помощи настраиваемых панелей представления (рис. 3, 4).

Заключение

В работе предложен подход к развертыванию функциональная SIEM-система на базе открытых технологий. Система строится путем интеграции системы Wazuh, сетевой системы обнаружения вторжений Suricata и программного комплекса ELK Stack. Предлагаемое решение способно эффективно консолидировать требуемую исходную информацию из системных журналов, данные сетевой активности, а также данные о целостности основных компонентов, текущей активности работающих процессов на всех элементах контролируемой ИТ инфраструктуры предприятия. Формируемые результаты являются информативными для выполнения анализа инцидентов информационной безопасности в «ручном» и автоматизированном режимах. Дальнейшая работа предполагает разработку для составляющих компонентов предложенной SIEM-системы специализированных правил идентификации подозрительной активности, а также подходы к автоматизации анализа событий и инцидентов информационной безопасности с использованием возможностей предложенной SIEM-системы.

ЛИТЕРАТУРА

1. Safarzadeh M., Gharaee H., Panahi A. H. A Novel and Comprehensive Evaluation Methodology for SIEM. In: Heng SH., Lopez J. (eds) Information Security Practice and Experience. ISPEC2019. Lecture Notes in Computer Science, vol. 11879. Springer, Cham. [Электронный ресурс] — Режим доступа — URL: https://doi.org/10.1007/978–3–030–34339–2_28 (дата обращения 25.04.2020)
2. Шелестова О. Что такое SIEM? [Электронный ресурс] — Режим доступа — URL: https://www.securitylab.ru/analytics/430777.php (дата обращения 25.04.2020)
3. Сапрыкина А. Обзор мирового и российского рынка SIEM-систем. [Электронный ресурс] — Режим доступа — URL: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem (дата обращения 25.04.2020)
4. Исследование IDC: оценка уровня удовлетворенности системами SIEM в компаниях России. [Электронный ресурс] — Режим доступа — URL: https://www.ptsecurity.com/ru-ru/research/analytics/idc-siem-research-2018/ (дата обращения 25.04.2020)
5. Leszczyna R., Wróbel M. Evaluation of open source SIEM for situation awareness platform in the smart grid environment. In: IEEE International Workshop on Factory Communication Systems — Proceedings, WFCS. 2015. [Электронный ресурс] — Режим доступа — URL: https://doi.org/10.1109/WFCS.2015.7160577 (дата обращения 25.04.2020)
6. Vazão A., Santos L., Piedade M., Rabadão C. SIEM open source solutions: a comparative study. In: 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal. 2019. [Электронный ресурс] — Режим доступа — URL: https://doi.org/10.23919/CISTI.2019.8760980 (дата обращения 25.04.2020)
7. ELK Stack: Elasticsearch, Logstash, Kibana. [Электронный ресурс] — Режим доступа — URL: https://www.elastic.co/what-is/elk-stack (дата обращения 25.04.2020)
8. ISO/IEC27001:2005. Международный стандарт по информационной безопасности. Системы обеспечения информационной безопасности.— Международная организация по стандартизации и Международная электротехническая комиссия, 2005.

9. СТО БР ИББС-1.3–2016. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств.— Москва: Банк России; М.: Из-во Банка России, 2016.
10. ГОСТ Р ИСО/МЭК 27001:2006. Национальный стандарт Российской федерации. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.— Москва: Федеральное агентство по техническому регулированию и метрологии; М.: Изд-во стандартов, 2008
11. Suricata | Open Source IDS / IPS / NSM Engine. [Электронный ресурс] — Режим доступа — URL: https://suricata-ids.org/ (дата обращения 25.04.2020).
12. Fekolkin R. Intrusion Detection and Prevention Systems: Overview of Snort and Suricata. 2015. [Электронный ресурс] — Режим доступа — URL: https://www.researchgate.net/publication/297171228_Intrusion_Detection_and_Prevention_Systems_Overview_of_Snort_and_Suricata (дата обращения 25.04.2020).

Журнал «Современная наука: актуальные проблемы теории и практики»

Г. Барнаул