УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ SIEM ДЛЯ КИБЕРЦЕНТРОВ

Рубанова К.В., студент гр.261401,

Голуб А.А., студент гр.261401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. Статья посвящена роли SIEM-систем в обеспечении кибербезопасности и их интеграции в SOC. Проведен сравнительный анализ популярных SIEM-систем, таких как IBM QRadar Security Intelligence, Splunk Enterprise Security, Kaspersky Unified Monitoring and Analysis Platform (KUMA) и PT MaxPatrol SIEM. Изучены нормативные акты Республики Беларусь, регулирующие использование SIEM в центрах кибербезопасности. Рассматривается актуальность создания SOC и интеграции SIEM-систем в образовательные учреждения для защиты важных информационных ресурсов.

Ключевые слова. Кибербезопасность, киберинциденты, расследование, SIEM, SOC, корреляция событий, мониторинг, реагирование, угрозы, PT MaxPatrol SIEM, Kaspersky KUMA.

Расследование киберинцидентов – одна из ключевых задач кибербезопасности, и в этом процессе главную роль играет взаимодействие SIEM (Security Information and Event Management) и SOC (Security Operations Center). Современные кибератаки становятся все более сложными и изощренными, поэтому организации вынуждены оперативно выявлять и нейтрализовать угрозы. SOC, будучи центром мониторинга и реагирования [1], полагается на SIEM-системы, которые собирают, анализируют и коррелируют огромные объемы логов, помогая быстро обнаруживать инциденты. SIEM отслеживает активность пользователей, серверов, сетевого оборудования, объединяя разрозненные события в единую картину [2]. Например, множественные неудачные попытки входа, затем успешная авторизация с нового IP-адреса и скачивание большого объема данных могут свидетельствовать о проникновении нарушителем, что позволит SOC немедленно реагировать.

Расследование инцидентов с SIEM проходит в несколько этапов: первичный анализ тревоги, корреляция событий для выявления истинных угроз, реагирование, изоляция зараженных систем и последующий анализ для предотвращения аналогичных кибератак в будущем. Основные преимущества SIEM – автоматизированный анализ данных, визуализация сложных атак и снижение нагрузки на аналитиков. Однако система требует грамотной настройки, иначе возможны ложные срабатывания и перегрузка тревогами. Например, SIEM фиксирует аномальное поведение фишинговой кибератаки, специалисты, работающие в SOC, анализируют угрозу, изолируют зараженные устройства и предотвращают дальнейшее распространение кибератаки. Интеграция SIEM в работу SOC значительно повышает скорость и точность расследования инцидентов, что делает его незаменимым инструментом для защиты организации от современных киберугроз.

В Республике Беларусь важную роль в развитии SOC играют нормативные акты, регулирующие кибербезопасность. 14 февраля 2023 года был издан Указ № 40 «О кибербезопасности» [3], который установил единые требования к защите информации и обязал государственные и критически важные объекты информатизации (КВОИ) создать центры кибербезопасности для мониторинга и реагирования на инциденты. Развитие таких центров предполагает активное использование SIEM для анализа угроз и корреляции событий. 25 июля 2023 года вышел Указ № 130 «О мерах по реализации Указа президента Республики Беларусь от 14 февраля 2023 г. № 40» [4], который уточнил требования к функционированию SOC. В частности, центры кибербезопасности обязаны использовать SIEM-системы

для сбора и хранения логов, выявления аномалий и автоматизированного анализа киберинцидентов. Также SOC должны обеспечивать постоянный мониторинг сетевого трафика, проводить аудит событий безопасности и разрабатывать сценарии реагирования на угрозы. Соблюдение этих требований критично для повышения киберустойчивости организаций и защиты от сложных кибератак.

В таблице 1 представлен сравнительный анализ следующих SIEM [5]: IBM QRadar Security Intelligence (США), Splunk Enterprise Security (США), Kaspersky Unified Monitoring and Analysis Platform (KUMA) [6] (РФ), PT MaxPatrol (РФ). Интеграция SIEM в процессы SOC является основой современной защиты информации, обеспечивая оперативное выявление и нейтрализацию киберугроз. Сравнительный анализ различных SIEM-систем, демонстрирует их возможности и ограничения. Например, системы IBM QRadar Security Intelligence [7] и Splunk Enterprise Security [8] выделяются своей высокой скоростью обработки данных и гибкостью настройки правил корреляции, что делает их эффективными для крупных организаций с сложной IT-инфраструктурой. Kaspersky Unified Monitoring and Analysis Platform (KUMA) и PT MaxPatrol SIEM также являются перспективными решениями, предлагающими централизованную архитектуру и корреляцию событий, что важно для защиты от современных кибератак.

Таблица 1 – Сравнительная таблица SIEM-систем

Характеристика	IBM QRadar Security Intelligence	Splunk Enterprise Security	Kaspersky Unified Monitoring and Analysis Platform (KUMA)	PT MaxPatrol SIEM
Разработчик	IBM	Splunk Inc.	Лаборатория Касперского	Positive Technologies
Год выпуска	2011	2011	2020	2013
Архитектура	Централизо-ванная	Децентрализо-ванная	Централизо-ванная	Централизованная
Лицензирование	Коммерческое	Коммерческое	Коммерческое	Коммерческое
Методы анализа	Корреляция событий, поведенческий анализ, машинное обучение	Корреляция событий, анализ логов, UEBA, машинное обучение	Корреляция событий, поведенческий анализ, ML	Корреляция событий, UEBA, машинное обучение
Интеграция с Threat Intelligence	IBM X-Force, STIX/TAXII	Splunk Security Essentials, STIX/TAXII	Kaspersky Threat Intelligence	PT ISIM, STIX/TAXII
Основной язык написания	Java, Python	Python, Go	C++, Python	Java, C++
Поддерживаемые форматы логов	Syslog, JSON, CEF, LEEF и др.	Syslog, JSON, CEF и др.	Syslog, JSON, CEF	Syslog, JSON, CEF
Отчетность и дашборды	Гибкие дашборды, отчеты	Расширенные дашборды, поиск, отчеты	Кастомизируе-мые дашборды	Расширенные отчеты и визуализация
Скорость обработки данных	Высокая (оптимизиро-ванные алгоритмы обработки)	Высокая, но зависит от конфигурации	Средняя	Высокая
Гибкость настройки правил корреляции	Средняя	Высокая	Средняя	Высокая
Легкость развертывания	Сложная настройка	Требует мощных ресурсов	Относительно простая	Средняя сложность
Страна происхождения	США	США	Россия	Россия

В Республике Беларусь выбор SIEM-систем для центров кибербезопасности осуществляется в соответствии с реестром оперативно-аналитического центра при Президенте Республики Беларусь [9]. В этот реестр включены PT MaxPatrol SIEM и Kaspersky Unified Monitoring and Analysis Platform (KUMA), которые соответствуют требованиям к сбору, корреляции и анализу событий информационной безопасности. Эти решения обеспечивают выполнение нормативных требований по мониторингу и расследованию инцидентов.

Учитывая важность защиты персональных данных, интеллектуальной собственности, научных исследований и других важных активов в различных организациях, включая образовательные учреждения, становится актуальным вопрос об интеграции эффективных SIEM-систем в их процессы безопасности. Однако, в отличие от многих организаций, у которых уже создан SOC, образовательные учреждения, такие как БГУИР, не имеют таких структур. В этом контексте целесообразно рассмотреть создание полноценного SOC для образовательных учреждений, что позволит обеспечить непрерывный мониторинг и реагирование на инциденты безопасности. Для интеграции в такой SOC актуально выбрать SIEM-систему Kaspersky Unified Monitoring and Analysis Platform (KUMA), поскольку она обеспечивает централизованную архитектуру, корреляцию событий и поведенческий анализ, что важно для защиты от современных кибератак. Кроме того, KUMA соответствует требованиям нормативных актов Республики Беларусь и включена в реестр ОАЦ. Таким образом, создание SOC с интеграцией KUMA в образовательных учреждениях может существенно повысить уровень кибербезопасности и защитить важные информационные ресурсы.

Список использованных источников:

[1] SOC - центр мониторинга и реагирования [Электронный ресурс]. – Режим доступа: https://softline.ru/solutions/security/soc

[2] Применение SIEM для расследования инцидентов [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/otus/articles/854440/

[3] О кибербезопасности Указ № 40 от 14 февраля 2023 г. [Электронный ресурс]. – Режим доступа: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g

[4] ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ 25 июля 2023 г. № 130 [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

[5] Сравнение SIEM-систем [Электронный ресурс]. – Режим доступа: https://searchinform.ru/products/siem/sravnenie-siem-sistem/

[6] Центральный элемент вашей системы безопасности [Электронный ресурс]. – Режим доступа: https://go.kaspersky.com/ru-kuma

[7] IBM QRadar Security Intelligence Platform [Электронный ресурс]. – Режим доступа: https://www.ibm.com/docs/ru/qsip/7.4?topic=quick-start-guide

[8] Зачем вам нужен Splunk? Аналитика событий безопасности [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/tssolution/articles/419493/

[9] Реестр средств защиты информации, прошедших сертификацию [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/information-security-tools/activity/technical-and-cryptographic-information-protection/registry-ism

Comparative Analysis of SIEM for Cyber Centers

Rubanova K.V., student of group 261401
Golub A.A., student of group 261401
Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

Belousova E.S. – Candidate of Technical Sciences, Associate Professor

Annotation. The article focuses on the role of SIEM systems in ensuring cybersecurity and their integration into Security Operations Centers (SOC). It analyzes a comparative table of popular SIEM systems, such as IBM QRadar Security Intelligence, Splunk Enterprise Security, Kaspersky Unified Monitoring and Analysis Platform (KUMA), and PT MaxPatrol SIEM. Special attention is paid to the regulatory acts of the Republic of Belarus governing the use of SIEM in cybersecurity centers. The article discusses the relevance of creating SOC and integrating SIEM systems into educational institutions to protect important information resources.

Keywords. Cybersecurity, cyber incidents, investigation, SIEM, SOC, event correlation, monitoring, response, threats, PT MaxPatrol SIEM, Kaspersky KUMA.