О. Ю. Сапожников, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.732

ОРГАНИЗАЦИЯ СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО ХРАНЕНИЯ И ОБРАБОТКИ СОБЫТИЙ СРЕДСТВАМИ SIEM-СИСТЕМЫ „KOMRAD“

Аннотация. В статье рассмотрены способы обнаружения инцидентов в сети предприятия средствами SIEM-системы „Komrad“, а также сформулированы требования к системе управления информационной безопасностью, определена значимость SIEM-систем. В результате проведенного анализа построена практическая модель применения отечественной SIEM-системы в моделируемой сети предприятия.
Ключевые слова: SOC, SIEM-система, „Komrad“, инцидент, директивы.

Введение. С развитием информационных технологий растет и количество возможных уязвимостей, через которые злоумышленники могут реализовать различные векторы атаки на конфиденциальность, целостность и доступность информации [1]. Для предотвращения или минимизации ущерба от компьютерных атак необходимо вести постоянное наблюдение за всеми участниками сети, а также за процессами, происходящими в ней, и информационными технологиями, входящими в сеть предприятия [2]. Для этого существуют Security Operations Center (SOC) [3], главным компонентом которых являются системы управления событиями безопасности (SIEM) [4].

На данный момент в мире имеется большое количество SIEM-систем: IBM QRadar SIEM, HP ArcSight, McAfee NitroSecurity, Splunk LogRhythm и т. д. В России можно выделить трех главных разработчиков, которые выпускают такие продукты как Komrad, MaxPatrol и StaffCop Enterprise [5]. В данной статье основное внимание будет уделено SIEM-системе „Komrad“.

Проблема исследования. Поскольку обнаружение инцидентов средствами SIEM-системы „Komrad“ в компьютерных сетях является достаточно трудоемким комплексным процессом, нами определяются следующие задачи данного исследования:

1. Изучить основные виды событий, которые может собирать «Komrad».

2. Проанализировать возможности SIEM-системы „Komrad“ для обнаружения инцидентов.

3. Смоделировать компьютерную сеть компании с использованием SIEM-системы с помощью программного эмулятора.

Материалы и методы. Для исследования использовались такие методы, как наблюдение, сравнение, эксперимент, измерение и абстрагирование. Для моделирования работы SIEM-системы была выбрана среда виртуализации GNS3 2.2.37.

Результаты. В SIEM-системах существует такое понятие, как активы. Это устройства, которые отправляют свои системные журналы на коллекторы системы. Коллектор данных — это приложение или его часть, которые принимают данные от интересующих источников, выполняют предварительную их обработку и обеспечивают их передачу серверу данных. В «Komrad» реализовано 7 таких коллекторов: Syslog, WMI, SNMP, SQL, HTTP, NetFlow и файловый.

Сотрудникам SOC необходимо реагировать на несанкционированный доступ к устройству или информации, на срабатывание антивирусного программного обеспечения, на подозрительные запросы к базам данных и т. д. Однако информации, которую собирают коллекторы, очень много (рис. 1), и чтобы не пропустить важные сведения, следует настроить срабатывание оповещений при данных инцидентах.

SIEM-система „Komrad“ обладает определенным функционалом для работы с инцидентами [6], которые можно разделить на 3 группы: неподтвержденные — это все новые инциденты, с которыми не проводились какие-либо действия; подтвержденные — это инциденты, которые были подтверждены; ложные — это отклоненные инциденты. Кроме того, есть возможности произвести настройку таким образом, чтобы при возникновении инцидента сразу отправлять всю необходимую информацию в ГосСОПКУ.

Для выполнения базовых настроек обнаружения инцидентов была спроектирована упрощенная модель сети малого предприятия. Эта топология содержит в себе устройства, находящиеся во внешней, внутренней и демилитаризованной зонах (рис. 2).

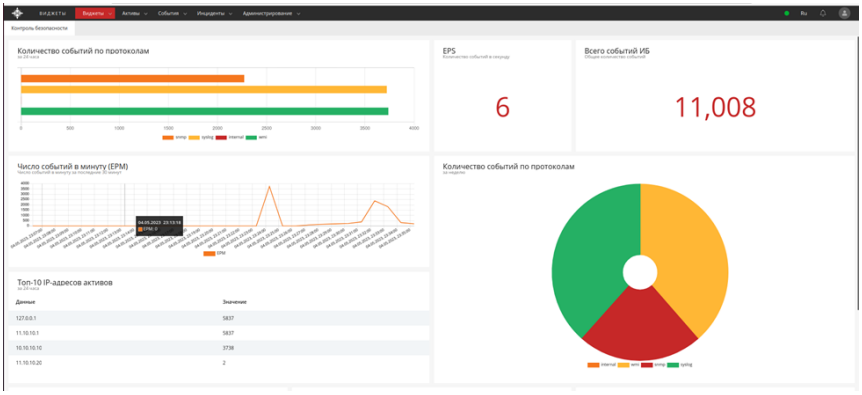

Рис. 1. Пример работы коллекторов Syslog, SNMP, WMI

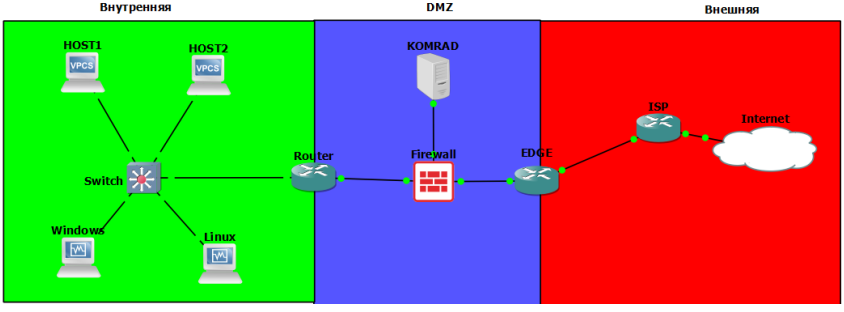

Рис. 2. Упрощенная топология сети предприятия

Для корректной настройки системы требуется определить активы и интересующие коллекторы. Далее следует создать несколько фильтров, на основании которых впоследствии будут отбираться необходимые пакеты данных. В нашем случае это авторизация пользователей (как успешная, так и провальная) и подключение к устройствам через протокол SSH.

Для обнаружения инцидентов необходимо настроить директивы (рис. 3) на основе фильтров, которые были созданы ранее. И теперь, когда пользователь не сможет авторизироваться, сработает системное уведомление о возможном несанкционированном доступе или

же о попытке удаленного подключения к устройству (рис. 4), на что оператор SOC может своевременно отреагировать и помешать потенциальным злоумышленникам.

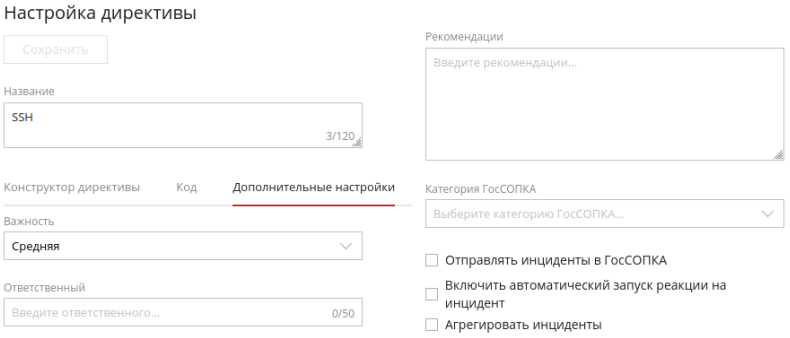

Рис. 3. Настройка директив

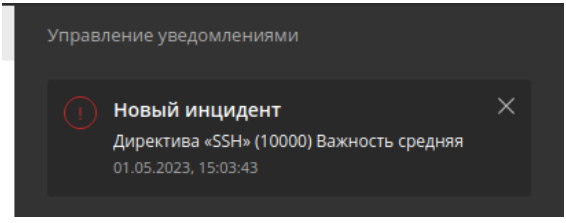

Рис. 4. Уведомление об инциденте

Заключение. Таким образом, в статье были рассмотрены некоторые возможности SIEM-системы „Komrad“, проанализированы основные разновидности системных журналов, которые может собирать система; определены базовые способы обнаружения инцидентов, работа которых была апробирована в среде эмуляции. В результате проведенной работы была смоделирована система обнаружения инцидентов средствами SIEM-системы „Komrad“.

СПИСОК ЛИТЕРАТУРЫ

1. Калач А. В. Особенность защищенности системы от угроз конфиденциальности, целостности и доступности информации при ее хранении

и обработке / А. В. Калач, Т. Е. Урусова. — Текст: электронный // Актуальные проблемы деятельности подразделений УИС. — 2019. — С. 429–430. — URL: https://www.elibrary.ru/item.asp?id=39167961 (дата обращения: 30.04.2023).
2. Аграновский А.В. Выявление угроз безопасности как способ предотвращения атак на компьютерные сети / А. В. Аграновский, Н. Г. Милославская. — Текст: электронный // Безопасность информационных технологий — 2008. — С. 5–15. — URL: https://elibrary.ru/item.asp?id=18811158 (дата обращения: 28.05.2023).
3. Голубева Е. В. Подходы к созданию центра реагирования и мониторинга инцидентов информационной безопасности (SOC)/ Е. В. Голубева, А. Д. Коротеева, Б. С. Серендук. — Текст: электронный // МНСК-2017: информационные технологии. — 2017. — С. 46. — URL: https://www.elibrary.ru/item.asp?id=34924066 (дата обращения: 30.04.2023).
4. Власова А. В. Краткая характеристика программных продуктов SIEM / А. В. Власова, В. А. Дударев. — Текст: электронный // Современные научные исследования: теория, методология, практика. — 2022. — С. 144-149. — URL: https://www.elibrary.ru/item.asp?id=49958522 (дата обращения: 30.04.2023).
5. Донской К. А. Обзор SIEM на российском рынке / К. А. Донской, Л. С. Левин. — Текст: электронный // Сборник научных трудов новосибирского государственного технического университета. — 2017. — С. 124-132. — URL: https://elibrary.ru/item.asp?id=32278921 (дата обращения: 28.05.2023).