УДК 004.001

РАЗРАБОТКА МЕТОДОВ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ВОЗДЕЙСТВИЯ НА ОСНОВЕ КОРРЕЛЯЦИОННОГО АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В SIEM-СИСТЕМАХ

Статья поступила в редакцию 15.04.2022, в окончательном варианте – 29.08.2022.

Шишков Сергей Анатольевич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
магистрант, ORCID: 0000-0001-5681-3850, e-mail: serge_gk4@mail.ru
Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0003-0414-6034, e-mail: putyato.m@gmail.com
Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru
Немчинова Валерия Олеговна, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
ассистент, ORCID: 0000-0002-4428-7128, e-mail: nemchinova.valeriya@yandex.ru

По мере развития информационных технологий обработка информации стала основной проблемой обеспечения защиты, так как число источников, из которых поступают актуальные данные по текущему состоянию защищенности, непрерывно увеличивается. Решением проблемы является использование систем SIEM. SIEM объединяет в себе классы управления информацией по безопасности и управления событиями безопасности. Решения управления информацией по безопасности обеспечивают долгосрочное хранение и анализ данных различных объектов инфраструктуры организации. Системы управления событиями безопасности реализуют мониторинг событий безопасности в реальном времени. Совмещая эти решения в SIEM-системах, специалисты по информационной безопасности могут выявить кибератаки и нарушения политик безопасности на ранних стадиях и минимизировать ущерб от них. Также решения SIEM помогают оценить защищенность информационных систем и актуальные для предприятия риски. В статье представлен анализ существующих решений информационной безопасности в области SIEM-систем. Описаны источники события для систем корреляции, указаны решаемые задачи SIEM, разобрана логика и структура SIEM. Произведен обзор популярных методов корреляции, описано применение данной системы как инструмента в области информационной безопасности. В статье представлена процедура разработки правила корреляции на примере системы MaxPatrol SIEM.

Ключевые слова: SIEM-система, событие ИБ, инцидент ИБ, информационная безопасность, угроза ИБ, уязвимость

DEVELOPMENT OF METHODS FOR DETECTING MALICIOUS IMPACT BASED ON CORRELATION ANALYSIS OF INFORMATION SECURITY EVENTS IN SIEM SYSTEMS

The article was received by the editorial board on 15.04.2022, in the final version – 29.08.2022.

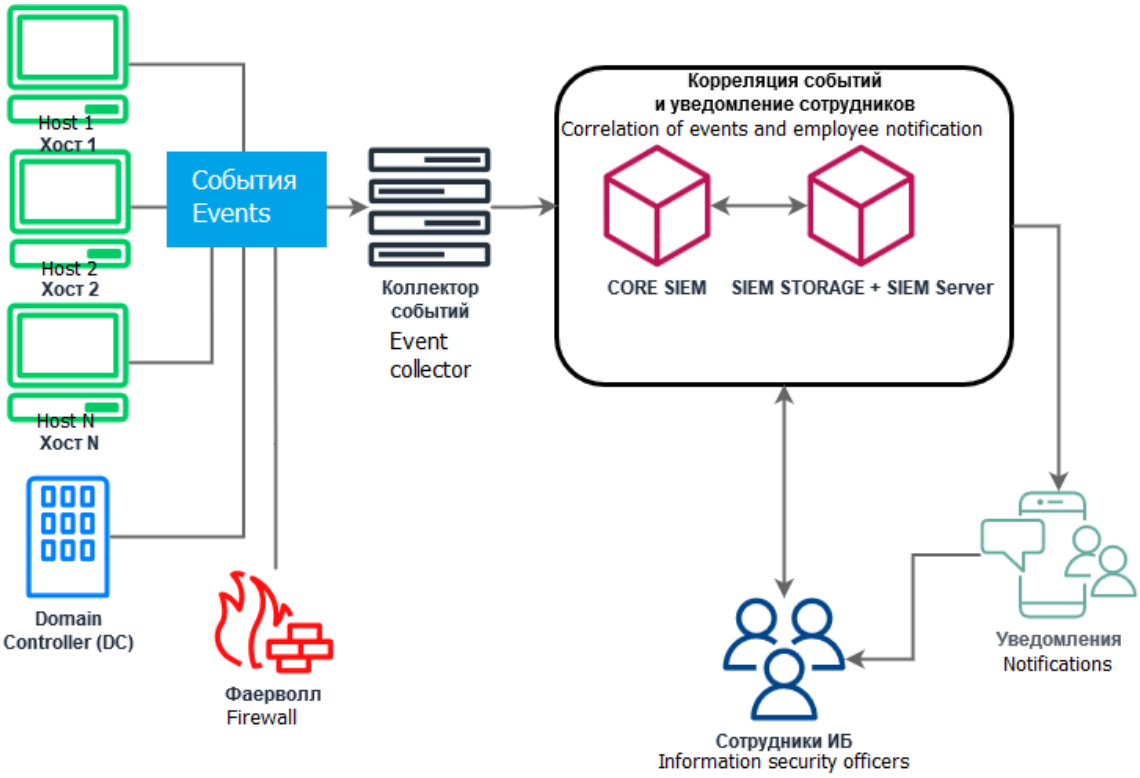
Shishkov Sergey A., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
graduate student, ORCID: 0000-0001-7101-6251, e-mail: michael.evsyukov@gmail.com
Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru
Nemchinova Valeriya O., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Assistant, ORCID: 0000-0002-4428-7128, e-mail: nemchinova.valeriya@yandex.ru

During the development of information technologies information processing has become the main problem of ensuring protection, since the number of sources from which up-to-date data on the current state of security is continuously increasing. Using SIEM systems can solve the problem. SIEM combines the SEM (Security Event

Management, "Security event management") and SIM (Security Information Management, "security information management") classes. SEM solutions implement real-time monitoring of security events. SIM systems provide long-term data storage and analysis of various infrastructure objects of the organization. SIEM solutions perform both of these tasks. With the help of SIEM, information security specialists can identify cyber attacks and violations of security policies at an early stage and minimize damage from them. SIEM solutions also help to assess the security of information systems and risks relevant to the enterprise. The article presents an analysis of existing information security solutions in the field of SIEM systems. Event sources for correlation systems are described, the SIEM tasks to be solved are indicated, the logic and structure of SIEM are analyzed. The review of popular correlation methods is made, the application of this system as a tool on information security is described. The article presents the procedure for developing a correlation rule using for example the MaxPatrol SIEM system.

Keywords: SIEM system, IS event, IS incident, information security, IS vulnerability, IS threat

Graphical annotation (Графическая аннотация)



Введение. На сегодняшний день существование отделов информационной безопасности в условиях крупных предприятий, а также организаций с высокими требованиями к безопасности хранения, доступности и использования информации является необходимостью. Каждая система защиты информации неумолимо развивается и адаптируется к новым методам и стратегиям кибератак. Количество средств обнаружения атак постоянно увеличивается, соответственно, при использовании нескольких СОВ увеличивается количество инцидентов, а также время для своевременного реагирования на них. Решением подобной проблемы является использование систем управления инцидентами информационной безопасности (SIEM-систем).

Утрата данных может рассматриваться как одна из основных угроз ИТ-безопасности. Преднамеренные действия персонала или злоумышленников, неисправность аппаратных средств могут послужить причиной нарушения целостности информации [15].

Во избежание реализации таких угроз создаются центры информационной безопасности, контролирующие работу средств защиты информации и проверяющие защищаемые автоматизированные системы [13, 14]. Степень защищенности информации и автоматизированных систем можно повысить использованием центров информационной безопасности [12].

Известно, что цифровая трансформация оказывает значительное влияние на технологии: от принятия решений на основе данных до внедрения облачных технологий, мобильности и взрывного развития Интернета вещей (IoT), при этом сам процесс ЦТ выходит за рамки простого развертывания новых решений в области ИКТ-технологий. В ходе ЦТ организации должны пересмотреть сложившиеся бизнес-модели и процессы для стимулирования инноваций и улучшения результатов

своей деятельности. Именно совместное применение цифровых технологий и информационных процессов дает поводы для переосмысления моделей бизнеса, а это – нелегкая задача [9].

Теория SIEM. Для решения задач оперативного мониторинга и реагирования на инциденты безопасности существует определённый класс программного обеспечения – SIEM-системы (Security Information and Event Management) [6]. Система управления инцидентами ИБ не способна к самостоятельному реагированию и предотвращению атак, её задача состоит в удобном и своевременном представлении информации из множества источников данных. Вследствие того, что в некоторых случаях промежуток времени между обнаружением и реакцией на инцидент ИБ должен быть как можно меньше, необходимо как можно больше автоматизировать процесс реагирования на инциденты [8]. Источниками данных могут служить другие информационные системы, такие как: операционные системы, бухгалтерские системы, справочные, сетевые системы, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), файерволлы веб-приложений (WAF), средства защиты информации от несанкционированного доступа, антивирусные средства, почтовые службы, базы данных, системы мониторинга. Кроме представления уже обработанных инцидентов из систем ИБ, SIEM-система позволяет производить множество операций с необработанными (сырыми) данными (например, Windows Event Log). Такими операциями являются нормализация, корреляция, агрегация, обогащение событий. Такая система поддерживает тонкую настройку генерирования инцидентов по предопределенным критериям, а также отправку уведомлений пользователям (например, при превышении определенного значения загрузки ЦП на определенном узле). SIEM-системы позволяют самостоятельно писать правила обработки данных из источников (нормализации), правила обогащения и корреляции.

Источники данных схематично изображены на рисунке 1.

Рисунок 1 – Источники данных SIEM

Структура SIEM состоит из следующих звеньев:

- сервер базы данных для хранения событий и работы с ними;
- агент, осуществляющий сбор данных с настроенных коллекторов;
- сервер-коллектор событий, осуществляющий сбор событий из источников (например, доменный сервер, забирающий логи с доменном АРМ);
- коррелятор, принимающий данные для последующей их обработки по правилам нормализации, корреляции и обогащения.

Задача SIEM-системы – получить данные от источников. Источник данных может быть «активным», который самостоятельно может передавать данные по указанному пути приемника, а также и «пассивным», к которому SIEM-система обращается сама [10].

Реализация механизмов корреляции и прогнозирования в SIEM-системах. Выделяется 2 вида методов корреляции:

- сигнатурные;
- бессигнатурные.

Сигнатурные методы позволяют администратору определять правила идентификации инцидентов, настраивать их конфигурации, определять исключения, вносить правки. Бессигнатурные методы менее гибкие в настройке, а все параметры в них заложены в этапе разработки системы. Управление настройками идентификации угроз при использовании бессигнатурных методов практически невозможно.

Методы корреляций событий в SIEM-системах:

- Statistical – бессигнатурный метод корреляции событий. Основан на измерении двух или более переменных и вычислении степени статистической связи между ними;
- RBR – метод, в котором взаимосвязи между событиями определяются правилами в заранее заданных специфических правилах;
- CBR – корреляция производится по подходящим векторам из предварительно заданной матрицы событий;
- MBR – метод, основанный на абстракции объектов и наблюдения за ними в рамках модели;
- Graph based. Корреляция заключается в поиске зависимостей между системными компонентами в графическом представлении (network devices, hosts, services) и построении графа на их основе. Если зависимость обнаруживается, граф используется для поиска основной причины возникновения проблемы;
- Neural network based – нейронная сеть, обучаемая для обнаружения аномалий в потоке событий [16].

В простейшем варианте в SIEM-системе корреляция работает в режиме RBR (Rule Based Reasoning). Они содержат в себе предопределенные условия, триггеры, счетчики и другие механизмы. Примером может служить механизм правила о создании и быстром удалении задания в ОС Windows – в таком случае при наступлении событии А (создание задания) запускается таймер, и если в момент работы таймера происходит событие Б (удаление задания), то срабатывает правило корреляции и генерируется инцидент ИБ. SIEM-система способна выявлять факты сетевых атак, эпидемиологических заражений вредоносным ПО, попытки несанкционированного доступа к конфиденциальной информации. Кроме этого, используя дополнительные инструменты, представляется возможным определять ошибки в работе информационных систем, определять уровень уязвимости того или иного ресурса [17].

Разработчики SIEM-систем в основном применяют сигнатурные методы, поскольку они гораздо более гибкие, имеют большую эффективность при обнаружении угроз [11].

SIEM как инструмент работы в ИБ. SIEM является мощным инструментом информационной безопасности, но может работать только вкупе с другими инструментами ИБ. Система позволяет добиться автоматического выявления угроз, позволяет обрабатывать события и работать с инцидентами, дает возможность своевременно обнаруживать аномалии и риски, может обеспечивать непрерывность работы информационных систем путем правильной настройки механизма корреляций. В совокупности позволяет существенно сократить риски ИБ, а значит, финансовые, репутационные и иные потери [17].

Внедрение SIEM-системы представляется сложным и дорогим механизмом, требующим должного внимания в длительной настройке, а для использования такой системы требуется высоко квалифицированный персонал, который позволит контролировать бесперебойный сбор событий, управлять правилами корреляций, своевременно их обновлять как с изменениями структуры организации, так и с выходом обновлений. Установка SIEM в формате «как есть» со встроенными разработчиками правил из коробки не даст должного результата, что приведет к нерациональной трате финансовых средств. В то же время успешное внедрение и правильная настройка решает множество задач, такие как:

- осуществление корреляций и оценка событий ИБ;
- проведение анализа структуры организации;
- реализация автоматизации процессов обнаружения угроз и аномалий;
- проведение аудита политик и стандартов соответствия [17], возможность выпуска отчетов;
- проведение правильного реагирования благодаря наличию инструментов и доказательной базы;
- возможность расследования давно произошедших инцидентов.

В России представлены большинство представителей рынка SIEM-систем, многие из которых имеют сертификаты ФСТЭК России. Потенциальным потребителям представляется обширная возможность определения нужной системы с необходимым ему набором функций.

Maxpatrol SIEM позволяет гибко фильтровать, группировать и настраивать выборки событий. А также позволяет строить диаграммы и чарты на основе поступающих событий.

Выборка может использоваться для изменения представления большого количества данных, а фильтр может использоваться для просмотра на основе критериев выбора[7]. На рисунке 2 показана столбчатая диаграмма, отражающая рейтинг хостов, с которых происходил брутфорс.

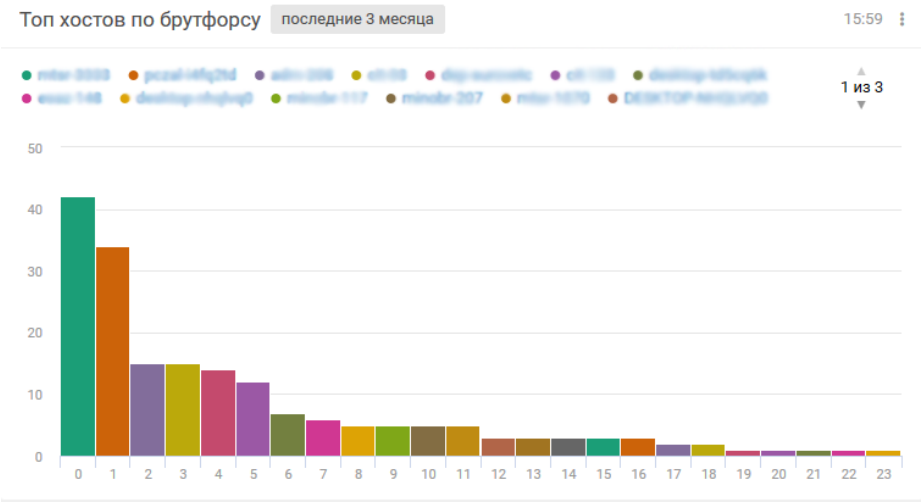


Рисунок 2 – Диаграмма рейтинга хостов по критерию выбора брутфорс

Разработка правила корреляции MaxPatrol SIEM. Для написания правил корреляции можно воспользоваться PTSIEM SDK GUI – набором средств разработки для PT SIEM.

Задача, решаемая правилом корреляции, состоит в следующем:

Существует организация, обслуживающая несколько других организаций в области ИБ. Все обслуживаемые организации имеют собственный домен Active Directory в лесу главного домена, управляемого системой Windows Server. В каждом домене есть свой доменный контроллер. При создании нового доменного пользователя внутри поддомена пользователь создается на хосте доменного контроллера. SIEM получает логи с доменных АРМ и обрабатывает их события. В доменах существуют группы пользователей с административными правами. Необходимо написать правило корреляции, которое будет анализировать следующие события и генерировать инциденты:

- создание нового пользователя и добавление в группу с администраторскими привилегиями;
- добавление любого пользователя в группу с администраторскими привилегиями;
- изменение паролей пользователя, состоящего в группе с администраторскими привилегиями.

Для решения такой задачи необходимо:

- иметь список узлов контроллеров домена;
- иметь список администраторских групп внутри доменов;
- реализовать решение задачи в контексте SIEM-системы.

В написании правил корреляции в выбранной системе используется язык PDQL (Positive Data Query Language). Для начала необходимо создать табличные списки для доменных контроллеров и списков пользователей и заполнить их. Список доменных контроллеров будет динамическим (будет автоматически формироваться при запросе из правила корреляции к нему). Создание динамического списка состоит из 2 шагов:

1. Выборка активов с ролью доменного контроллера. Запрос на языке PDQL – «Host.HostRoles.Role = 'Domain Controller'».

2. Создание табличного списка с запросом – «select(@Host as host_name)».

Теперь приступаем к написанию правила корреляции. При создании пользователя в журнале EventLog Windows генерируется событие с идентификатором 4720, при изменении пароля 4723 или 4724, а при добавлении в группу – 4728. Для удобства будет создано 2 правила – в первом правиле будем отслеживать 2 события:

- создание пользователя и добавление его в группу администраторов в течение 20 минут;
- добавление любого пользователя в группу администраторов.

Таким образом, нам надо фильтровать события с идентификаторами 4720 и 4728.

Во втором правиле отслеживается одно событие – изменение пароля пользователя, состоящего в группе администраторов, то есть событие с идентификатором 4724.

Для проверки написанных правил будем использовать специально созданные тестовые учетные записи. В начале заполняем табличный список в MaxPatrol SIEM, содержащий группы с правами администратора домена – добавляем запись в колонку group «testadmins». Далее создаем группу «testadmins» и доменного пользователя с именем «testsiem» и добавляем его в группу.

Правило корреляции добавления пользователя в группу с правами администратора изображено на рисунке 3.

Правило корреляции CIT_incident_create_user_important

```
query Check_Important_host($host_name) from Domain_Controllers {(host_name == $host_name)}
query Check_Admin_Groups($group) from CIT_Admin_Groups {(group==$group)}

    event Create_User_4720:
    key:
        event_src.host
    filter{
        msgid == "4720"
        and exec_query ("Check_Important_host", [lower(event_src.host)])
    }
    event Add_User_To_Admins:
    key:
        event_src.host
    filter{

        msgid =="4728"
        and exec_query("Check_Admin_Groups",[lower(object.name)])
        }
    rule CIT_incident_create_user_important: ((Create_User_4720 -> Add_User_To_Admins) within 20m) or Add_User_To_Admins
        on Create User 4720 {
```

Рисунок 3 – Правило корреляции при добавлении пользователя в группу с правами администратора

Результат корреляции представлен на рисунке 4. Из карточки инцидента мы видим, что инцидент состоит из 3 событий – создание пользователя «testsiem», добавление в группу «testadmins» и события корреляции (Пользователь … с узла … добавил пользователя в группу «testadmins»).

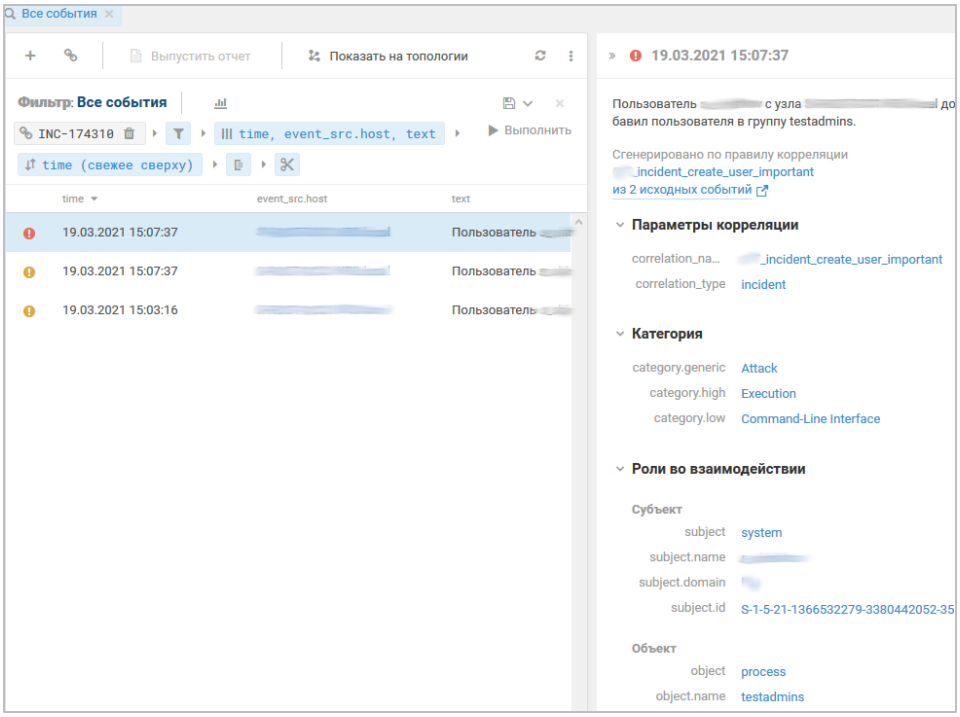


Рисунок 4 – Карточка инцидента 1

Корреляционное правило для отслеживания изменения паролей пользователей представлена на рисунке 5. В нем система будет отслеживать события с идентификатором 4724, при котором имя субъекта будет входить в табличный список «CIT_Admin_Users».

Для проверки правила создадим АРМ «test_server». В нем создадим пользователя «тест_администратор». Далее добавим в табличный список запись с именем этого пользователя. Теперь после смены пароля данному пользователю возникает корреляционное событие. Карточка инцидента представлена на рисунке 6.

Правило корреляции CIT_Incident_Change_User_Important

```
query Check_Admin_Users($username) from CIT_Admin_Users{(username==$username)}

    event Change_User_Pass:
    key:
        event_src.host
    filter{
        msgid =="4724"
        and string(regex(lower(object.name), "healthmailbox", 0)) == null
        and exec_query("Check_Admin_Users",[lower(object.name)])
        }

    rule CIT_Incident_Change_User_Important: Change_User_Pass


    on Change_User_Pass {

        $subject.id = subject.id
        $subject.name = subject.name
        $subject.domain = subject.domain
        $subject.privileges = subject.privileges
```

Рисунок 5 – Правила корреляции изменения паролей пользователей

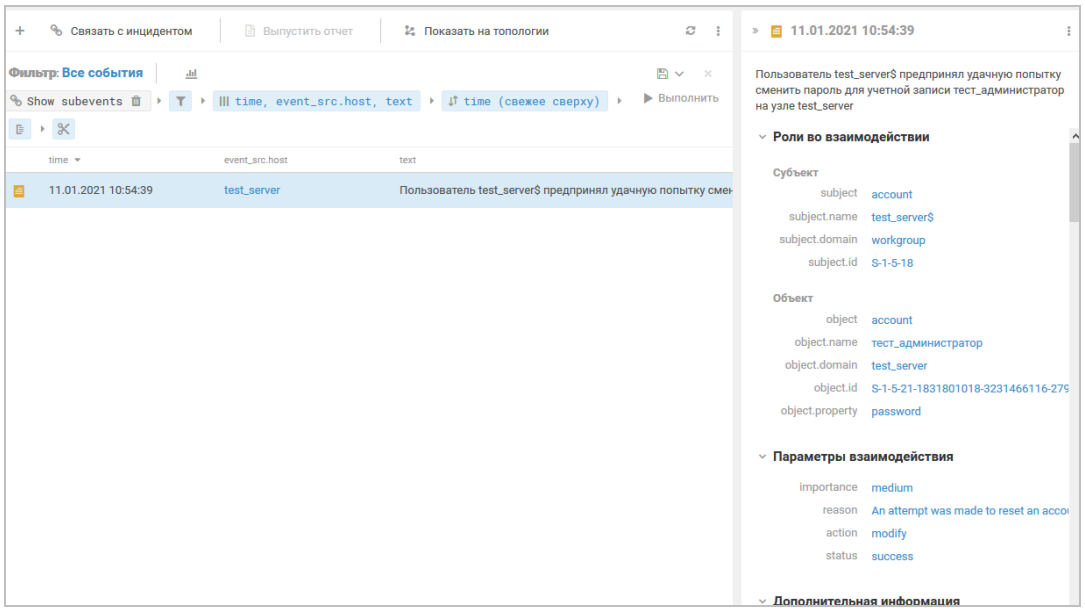


Рисунок 6 – Карточка инцидента 2

В результате внедрения данных корреляций отдел ИБ может отслеживать создание и редактирование учетных записей с критическими высокими и важными в области безопасности правами. При проникновении злоумышленника в корпоративную сеть злоумышленник будет пытаться получить доступ к целевой системе посредством использования скомпрометированных учетных записей или путем эксплуатации уязвимостей в системе. Если ему удастся получить доступ к учетной записи администатора путем сброса пароля, либо создать такую учетную запись, то сотрудники отдела ИБ будут об этом осведомлены.

Для своевременного реагирования следует настроить уведомления по электронной почте на срабатывание данных коррелляций и подключить уведомления в мессенджеры, чтобы иметь возможность оперативно реагировать.

Заключение. SIEM-системы предлагают богатый инструментарий для обеспечения состояния информационной безопасности на предприятии. Для эффективного использования требуется тонкая настройка под каждую конкретную информационную систему, иначе SIEM не будет эффективным инструментом в руках сотрудников отдела ИБ. Главным плюсом этой системы является предоставление широких возможностей для конфигурирования правил, возможность использования собственных корреляций, настройка и отправка уведомлений по множеству критериев.

В рамках данной статьи была продемонстрирована возможность реализаций собственных правил корреляций в среде Maxpatrol SIEM, тем самым повышая степень уровня контроля действий с учетными записями администраторов доменной инфраструктуры, что является крайне важным для защиты от перемещения по периметру и эскалации привилегий в уже зараженной системе и позволяет оперативно обнаружить злоумышленника в корпоративной сети.

Библиографический список

1. Золотухин, А. В. Принцип работы и типовая структура средств управления событиями безопасности информации / А. В. Золотухин, А. С. Тимохович // Academy. – 2017. – № 10 (25). – Режим доступа: https://cyberleninka.ru/article/n/printsip-raboty-i-tipovaya-struktura-sredstv-upravleniya-sobytiyami-bezopasnosti-informatsii, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 08.10.2021).

2. Королев, И. Д. Анализ проблематики системы управления информацией и событиями безопасности в информационных системах / И. Д. Королев, В. И. Попов, В. А. Ларионов // Инновации в науке. – 2018. – № 12 (88). – Режим доступа: https://cyberleninka.ru/article/n/analiz-problematiki-sistemy-upravleniya-informatsiey-i-sobytiyami-bezopasnosti-v-informatsionnyh-sistemah свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 08.10.2021).

3. itsec.by: Информационная безопасность. Системы управления информацией и событиями безопасности (Security Information and Event Management). – Режим доступа: http://itsec.by/produktyi-siem-sistemyi-upravleniya-infor-2/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 09.10.2021)

4. www.pacifica.kz: Инновационное решение MaxPatrol SIEM для управления событиями и информацией ИБ. – Режим доступа: https://www.pacifica.kz/catalog/monitoring-sobytiy-bezopasnosti-siem-/maxpatrol-siem/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 09.10.2021).

5. Хлестова, Д. Р. Анализ актуальности использования SIEM-систем на предприятиях / Д. Р. Хлестова, К. Г. Попов // Символ науки. – 2016. – № 7–1. – Режим доступа: https://cyberleninka.ru/article/n/analiz-aktualnosti-ispolzovaniya-siem-sistem-na-predpriyatiyah, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 09.10.2021).

6. Макарян, А. С. Анализ практической реализации механизмов выявления кибератак в SIEM-системе Splunk / А. С. Макарян, М. М. Путято, А. Р. Очередько // Информационные системы и технологии в моделировании и управлении : сборник трудов V Международной научно-практической конференции. Ялта, 20–22 мая 2020 года / отв. редактор К. А. Маковейчук. – Ялта : Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2020. – С. 252–256.

7. Подход к построению процедур выявления и предотвращения распределенных атак типа отказ в обслуживании на основе SIEM-систем / А. Р. Очередько, Д. А. Бачманов, М. М. Путято, А. С. Макарян // Научные труды КубГТУ. – 2021. – № 1. – С. 20–32.

8. Очередько, А. Р. Исследование igp-систем на основе анализа механизмов реагирования на инциденты информационной безопасности / А. Р. Очередько, Д. А. Бачманов, М. М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2021. – № 1 (53).

9. Артамонов, В. А. Кибербезопасность в условиях цифровой трансформации социума / В. А. Артамонов, Е. В. Артамонова // Большая Евразия: развитие, безопасность, сотрудничество. – 2022. – № 5–1.

10. Комаров, А. Н. Анализ и мониторинг сети предприятия в реальном времени / А. Н. Комаров // Глобус: технические науки. – 2020. – № 5 (36).

11. Очередько, А. Р. Исследование SIEM-систем на основе анализа механизмов выявления кибератак / А. Р. Очередько, В. С. Герасименко, М. М. Путято, А. С. Макарян // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2020. – № 2 (261).

12. Королев, И. Д. Повышение уровня автоматизации процессов сбора данных о выявленных событиях и инцидентах информационной безопасности / И. Д. Королев, Е. С. Литвинов, Д. И. Маркин // ИВД. – 2021. – № 10 (82).

13. Махлин, Б. М. Единая система управления информационной безопасности / Б. М. Махлин // Научный формат. – 2019. – № 2 (2).

14. Madani, A. Log management comprehensive architecture in security operation center (soc) / A. Madani, S. Rezayi and H. Gharaee // Computational Aspects of Social Networks (CASoN) 2011 : International Conference. – 2011. – P. 284–289.

15. Курбанова, Н. Э. Методы предотвращения угроз кибербезопасности / Н. Э. Курбанова // Science and Education. – 2021. – № 8.

16. Борисов, В. И. О применении сигнатурных методов анализа информации в SIEM-системах / В. И. Борисов, А. С. Шабуров // Вестник УРФО. Безопасность в информационной сфере. – 2015. – № 3 (17).

17. Кириллов, В. А. Система сбора и корреляции событий (SIEM) как ядро системы информационной безопасности / В. А. Кириллов, А. Р. Касимова, А. Д. Алёхин // Вестник технологического университета. – 2016. – № 13.

References

1. Zolotukhin, A. V., Timokhovich, A. S. Princip raboty i tipovaya struktura sredstv upravleniya sobytiyami bezopasnosti informatsii [Principle of operation and typical structure of information security event management tools]. *Academy*, 2017, no. 10 (25). Available at: https://cyberleninka.ru/article/n/printsip-raboty-i-tipovaya-struktura-sredstv-upravleniya-sobytiyami-bezopasnosti-informatsii (accessed 08.10.2021).

2. Korolev, I. D., Popov, V. I., Larionov, V. A. Analiz problematiki sistemy upravleniya informatsiey i sobytiyami bezopasnosti v informatsionnykh sistemakh [Analysis of security information and event management system issues in information systems]. *Innovatsii v nauke* [Scientific Innovation], 2018, no. 12 (88). Available at: https://cyberleninka.ru/article/n/analiz-problematiki-sistemy-upravleniya-informatsiey-i-sobytiyami-bezopasnosti-v-informatsionnyh-sistemah (accessed 08.10.2021).

3. *itsec.by: Informatsionnaya bezopasnost. Sistemy upravleniya informatsiey i sobytiyami bezopasnosti (Security Information and Event Management)* [itsec.by: Information security. Security Information and Event Management systems]. Available at: http://itsec.by/produktyi-siem-sistemyi-upravleniya-infor-2/ (accessed 09.10.2021).

4. *www.pacifica.kz: Innovatsionnoe reshenie MaxPatrol SIEM dlya upravleniya sobytiyami i informatsiey IB* [www.pacifica.kz: The innovative MaxPatrol SIEM solution for managing IS events and information]. Available at: https://www.pacifica.kz/catalog/monitoring-sobytiy-bezopasnosti-siem-/maxpatrol-siem/ (accessed 09.10.2021).

5. Khlestova, D. R., Popov, K. G. Analiz aktualnosti ispolzovaniya SIEM-sistem na predpriyatiyakh [Analysis of the relevance of the use of SIEM systems in enterprises]. *Simvol nauki* [Symbol of Science], 2016, no. 7–1. Available at: https://cyberleninka.ru/article/n/analiz-aktualnosti-ispolzovaniya-siem-sistem-na-predpriyatiyah (accessed 09.10.2021).

6. Makaryan, A. S., Putyato, M. M., Ocheredko, A. R. Analiz prakticheskoy realizatsii mekhanizmov vyyavleniya kiberatak v SIEM-sisteme Splunk [Analysis of the practical implementation of cyberattack detection mechanisms in the Splunk SIEM system]. *Informatsionnye sistemy i tekhnologii v modelirovanii i upravlenii : sbornik trudov V Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Yalta, 20–22 maya 2020 goda* [Information systems and technologies in modelling and management : Proceedings of the V International Scientific-Practical Conference, Yalta, May 20–22, 2020]. Yalta : Typography «Arial» Publ., 2020, pp. 252–256.

7. Ocheredko, A. R., Bachmanov, D. A., Putyato, M. M., Makaryan, A. S. Podkhod k postroeniyu protsedur vyyavleniya i predotvrashcheniya raspredelennykh atak tipa otkaz v obsluzhivanii na osnove SIEM-sistem [An approach to building procedures for detecting and preventing distributed denial of service attacks based on SIEM systems]. *Nauchnye trudy KubGTU* [Scientific Proceedings of Kuban State Technical University], 2021, no. 1, pp. 20–32.

8. Ocheredko, A. R., Bachmanov, D. A., Putyato, M. M., Makaryan, A. S. Issledovanie IRP-sistem na osnove analiza mekhanizmov reagirovaniya na intsidenty informatsionnoy bezopasnosti [A study of IRP systems based on an analysis of information security incident response mechanisms]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: control and high technologies], 2021, no. 1 (53).

9. Artamonov, V. A., Artamonova, E. V. Kiberbezopasnost v usloviyakh tsifrovoy transformatsii sotsiuma [Cybersecurity in the Digital Transformation of Society]. *Bolshaya Evraziya: razvitie, bezopasnost, sotrudnichestvo* [Greater Eurasia: Development, Security, Cooperation], 2022, no. 5–1.

10. Komarov, A. N. Analiz i monitoring seti predpriyatiya v realnom vremeni [Real-time enterprise network analysis and monitoring]. *Globus: tekhnicheskie nauki* [Globe: Technical Sciences.], 2020, no. 5 (36).

11. Ocheredko, A. R., Gerasimenko, V. S., Putyato, M. M., Makaryan, A. S. Issledovanie SIEM-sistem na osnove analiza mekhanizmov vyyavleniya kiberatak [SIEM research based on analysis of cyber-attack computation mechanisms]. Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki [Vestnik of Adygeyan State University], 2020, no. 2 (261).

12. Korolev, I. D., Litvinov, E. S., Markin, D. I. Povyshenie urovnya avtomatizatsii protsessov sbora dannykh o vyyavlennykh sobytiyakh i intsidentakh informatsionnoy bezopasnosti [Improving automation of data collection processes for detected information security events and incidents]. *IVD* [IVD], 2021, no. 10 (82).

13. Makhlin, B. M. Edinaya sistema upravleniya informatsionnoy bezopasnosti [A unified information security management system]. *Nauchnyy format* [Scientific Format], 2019, no. 2 (2).

14. 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.

15. Kurbanova, N. E. Metody predotvrashcheniya ugroz kiberbezopasnosti [Methods to prevent cybersecurity threats]. *Science and Education*, 2021, no. 8.

16. Borisov, V. I., Shaburov, A. S. O primenenii signaturnykh metodov analiza informatsii v SIEM-sistemakh [About the application of signature analysis method in the SIEM-systems]. *Vestnik URFO. Bezopasnost v informatsionnoy sfere* [Bulletin of URFO. Information-technology (IT) security], 2015, no. 3 (17).

17. Kirillov, V. A., Kasimova, A. R, Alyokhin, A. D. Sistema sbora i korrelyatsii sobytiy (SIEM) kak yadro sistemy informatsionnoy bezopasnosti [Event Collection and Correlation System (SIEM) as the core of an information security system]. *Vestnik tekhnologicheskogo universiteta* [Bulletin of the Technological University], 2016, no. 13.