УДК 004.89

СХЕМА ВЗАИМОДЕЙСТВИЯ СППР И SIEM-СИСТЕМЫ

Спиридонов Д.Л. (Национальный исследовательский университет ИТМО)

Аннотация. В представленной работе предлагается к использованию схема применения СППР в области реагирования на инциденты информационной безопасности. Приведен пример дерева решений при обнаружении SIEM-системой атаки методом *brute force*.

Введение. С ростом цифровизации во всех сферах жизни, растет и число кибератак, возникает необходимость в обеспечении информационной безопасности как в крупных, так и в небольших организациях. Возрастающий интерес к сфере информационной безопасности требует быстрой передачи знаний от экспертов к новым сотрудникам, возникает необходимость быстро обучить их принимать решения по устранению инцидентов информационной безопасности, с которыми они могут столкнуться. Предлагаемый подход по применению системы поддержки принятия решений совместно с SIEM-системой позволит ускорить время устранения инцидента информационной безопасности, избежать ошибок, которые могут возникнуть из-за недостаточного опыта у оператора SIEM-системы.

Основная часть. При возникновении инцидента информационной безопасности в SIEM-системе срабатывает правило корреляции, данное правило описывает последовательность событий, которые являются нарушениями политики информационной безопасности и являются неприемлемыми в данной инфраструктуре. После сработки правила корреляции формируется инцидент (далее - сработка), данные о котором записываются в хранилище событий и сработок SIEM-системы. Далее оператор предпринимает действия для устранения инцидента, на данном этапе предлагается подключить систему поддержки принятия решений. Рассмотрим алгоритм взаимной работы СППР и SIEM-системы. После записи данных об инциденте в хранилище данных, SIEM-система отправляет в СППР информацию о сработке (время инцидента, узел, на котором произошел инцидент, учетная запись, адреса источников сетевого взаимодействия, информация о запущенных файлах если такие есть и т.д.), далее СППР может сразу предложить решение, либо отправить дополнительный запрос в SIEM, например, о количестве подобных сработок с данного узла, учетной записи, принадлежности источников сетевого взаимодействия к внутренней или внешней сети, сведениях об учетных записях на этих узлах и т.д. Таким образом, происходит обмен информации между двумя системами, в результате оператору SIEM-системы предлагается алгоритм действий, способствующий устранению инцидента. Рассмотрим пример: SIEM-система зафиксировала инцидент класса “brute force” на узле 10.10.255.10 с учетной записью “User”. Дерево решений СППР может следующие узлы: количество таких сработок для данного пользователя, количество таких сработок для данного узла. Например, при количестве подобных сработок > 2 можно считать, что данный пользователь или пользователи на данном узле пренебрегают парольной политикой компании, используют слабые, словарные пароли, которые легко поддаются подбору. Узлом решения в таком случае могут быть:

1. Блокировка учетной записи данного пользователя, сброс пароля, изменение парольной политики в компании в сторону более сложных паролей
2. Блокировка данного узла, сброс паролей пользователей на данном узле, изменение парольной политики в компании в сторону более сложных паролей
3. Не предпринимать никаких действий, понаблюдать за дальнейшей активностью пользователя, т.к. он мог ошибиться с вводом пароля несколько раз, а затем ввести его успешно.

Выводы. В результате проведенной работы была предложена схема взаимодействия СППР и SIEM-системы. Приведен пример дерева решений при возникновении инцидента класса “brute force”. Рассматриваемый подход планируется апробировать путем создания виртуального тестового стенда на основе open-source решений.