УДК 004.056

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ РЕЗУЛЬТАТИВНОСТИ РАБОТЫ ЦЕНТРА МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Снеткова А. А.[1]
Научный руководитель – доктор технических наук, доцент Лившиц И. И.[1]
[1]Университет ИТМО
a.a.snetkova@yandex.ru

Введение

Центр мониторинга и реагирования на инциденты информационной безопасности (SOC) выступает ключевым элементом операционного контура киберзащиты организации, обеспечивая непрерывное наблюдение, выявление аномалий сетевой активности и организацию своевременного реагирования на инциденты информационной безопасности. При этом развёртывание и эксплуатация SOC требуют значимых затрат на персонал, процессы и технологическую инфраструктуру, поэтому возникает объективная необходимость в регулярной и методически корректной оценке результативности его функционирования для обоснования финансовых вложений и принятия управленческих решений. На практике оценивание деятельности SOC нередко сводится к ограниченному набору показателей, автоматически формируемых средствами мониторинга, что не позволяет адекватно учесть контекст инцидента, качество принимаемых решений и влияние человеческого фактора [1].

Оценка результативности функционирования SOC в отечественной практике по-прежнему характеризуется методической незрелостью: наблюдается фрагментарность методик и преобладание количественно-декларативных подходов над контекстуально-аналитическими. Преимущественно измерения происходят по принципу упрощения отчетности без учета аналитической ценности результатов. В литературе также подчёркивается дефицит согласованных показателей, пригодных для оценки результативности работы аналитиков и операционных процессов SOC [2].

Вследствие изложенного научно-прикладное значение приобретает разработка методики оценки результативности функционирования SOC, основанной на процессном подходе и учитывающей его социотехническую природу.

Основная часть

В работе рассматривается задача оценки результативности функционирования SOC как социотехнической системы, в которой достигаемые результаты определяются согласованностью регламентированных процедур, применяемых технологий, качества исходной телеметрии и персонала. В связи с этим центральным результатом исследования выступает формализация процесса измерений и построение процессной модели системы показателей, ориентированной не на фиксацию разрозненных числовых значений, а на получение управленчески интерпретируемых выводов о состоянии ключевых процессов мониторинга, анализа и реагирования.

Для оценки результативности и выявления узких мест предложена система взаимосвязанных показателей, структурированная в соответствии функциями аналитиков SOC и стадиями жизненного цикла обработки инцидента [3]. Суть оценки заключается в выработке оценочного суждения относительно состояния процессов информационной безопасности на основе вычисления метрик и их сопоставления с заданными целевыми и пороговыми значениями. В качестве возможных оценочных суждений предложены интерпретации результатов вычисления метрик в трёх типах: успех, тенденция и аномалия. Успех соответствует ситуации, когда измеренная величина

оказывается лучше целевой и тем самым подтверждает ожидаемую результативность рассматриваемого процесса. Тенденция предоставляет сведения о динамике процесса и указывает на направление изменения полученных значений по отношению к целевым в сравнении с данными, полученными ранее. Аномалия отражает выход измеренной величины за пределы допустимых пороговых значений и указывает либо на некорректность проведения измерений и недостатки учётных данных, либо на наличие проблем в реализации процессов, требующих углублённого анализа причин и выполнения корректирующих действий.

С учётом того, что отдельные метрики оказывают неодинаковое влияние на итоговые результаты интегральной оценки, каждой метрике назначается весовой коэффициент, отражающий её вклад в расчёты и позволяющий избежать ситуации, когда второстепенные признаки искажают общий вывод о состоянии процесса. Приведённая методика расчёта предусматривает определение функционального назначения показателей, установление требований к ним, выделение ключевых атрибутов объекта измерения и уровней измерения, а также формирование правил интерпретации полученных значений. Процесс вычисления итоговых значений и выработки оценочного суждения описан в виде алгоритма и представляет собой последовательность операций от выбора атрибутов объекта измерения до формирования однозначных выводов о состоянии рассматриваемых процессов.

Выводы

Предлагаемое решение позволяет перейти от упрощённой отчётности, не отражающей фактическое состояние процессов и не позволяющей принимать обоснованные управленческие решения, к научно обоснованной оценке результативности SOC, где результативность понимается как степень достижения запланированных результатов при заданных ресурсных ограничениях. Практическая применимость разработанной методики выражается в способности обнаружения узких мест в рамках сложившихся процессов за счет установления устойчивых причинно-следственных связей между наблюдаемыми отклонениями показателей и конкретными аспектами работы аналитиков SOC, что создаёт основу для разработки и внедрения соответствующих корректирующих мероприятий.

Литература

1. Vielberth M., Böhm F., Fichtinger I., Pernul G. Security operations center: a systematic study and open challenges // IEEE Access. 2020. Vol. 8. P. 227756–227779.
2. Agyepong E., Cherdantseva Y., Reinecke P., Burnap P. Towards a Framework for Measuring the Performance of a Security Operations Center Analyst // 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). – Dublin, Ireland: IEEE, 2020. – P. 1–8.
3. Kokulu F.B., Bao T., Doupé A., Shoshitaishvili Y., Ahn G.-J., Zhao Z. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues // Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019. P. 1955–1970.

Автор _____ Снеткова А. А.
Научный руководитель _____ Лившиц И. И.