

УДК 004.056

Формирование методики расширенного обнаружения и реагирования на компьютерные атаки

Добкач Леонид Яковлевич^(*)

dobkachleo@mail.ru

SPIN-код: 4795-0607

АО «Аксифт», Москва, Россия

Аннотация. Отмечена необходимость формализованного представления современных комплексных средств защиты информации, таких как системы расширенного обнаружения и реагирования (XDR) на атаки. Предложена конфигурация XDR-системы как сетевой системы обнаружения вторжения и EDR-системы. Сформирована методика распознавания компьютерных атак, позволяющая реализовать такую систему. В отличие от традиционных поисков исключительно способа классификации поступающих событий, предлагаемая методика также учитывает формат представления входных данных и способ верификации результатов классификации, производимой методами машинного обучения. Показана эффективность применения описанной методики для реализации XDR-систем.

Ключевые слова: системы обнаружения вторжений, XDR-системы, методика распознавания атак, сокращенная диаграмма решений, машинное обучение

Введение. Системы расширенного обнаружения и реагирования на атаки (XDR) впервые появились в 2018 году и формально относятся к классу средств обнаружения и реагирования на атаки, т. е. к *DR-системам [1]. Если EDR-системы можно привести в соответствие с традиционными системами обнаружения вторжения (COB) уровня узла, а NDR-системы — с COB уровня сети, то за XDR-системы производители СЗИ зачастую выдают несколько продуктов в одном пакете услуг, что не гарантирует эффективную защиту информационных систем.

Методы и материалы; результаты. Применение современных методов машинного обучения, искусственных нейронных сетей делает комплексные СЗИ конкурентоспособными и более гибкими по отношению к постоянно меняющемуся ландшафту информационных угроз. В связи с этим предлагается рассматривать XDR как совокупность COB уровня сети и EDR-систем, анализирующих данные сетевого трафика и узловые события посредством ансамбля методов машинного обучения.

Обучение классификаторов машинного обучения и дальнейший анализ требует работы с колоссальным объемом входных данных, который можно оптимизировать, удалив малоинформативные параметры и объединив схожие посредством сокращенной диаграммы решений [2], что позволяет повысить точность распознавания даже сигнатурной COB на 2 %.

Поскольку адаптивные методы обладают свойством неточности, прежде чем выводить результаты классификации, выходы ансамбля подаются на тер-

минальный классификатор взвешенного голосования, на этапе которого осуществляется верификация и корректировка результатов как между собой, так и с данными сигнатурного анализа [3]. Благодаря этому тестовая реализация XDR-системы показывает результаты на 11 % лучше, чем классические COB.

Заключение. Распознавание компьютерных атак следует рассматривать более широко, нежели этап анализа и классификации событий в дискретных последовательностях — в данном случае сетевого трафика. Оптимизированная подготовка входных данных и проверка полученных результатов классификации не менее важны. Таким образом, методика расширенного обнаружения и реагирования на компьютерные атаки состоит из трех способов на каждом из этапов: 1) Способ преобразования входных данных в формат сокращенной диаграммы решений для оптимизации их представления в памяти; 2) Гибридный подход к обнаружению вторжений на основе сетевой COB и EDR-системы, реализующих ансамбль машинного обучения; 3) Верификация результатов данного ансамбля с помощью взвешенного голосования и сигнатурного анализа. Тестирование на больших наборах данных показывает повышение точности выявления атак в среднем на 11 %, что подтверждает эффективность методики.

Список источников

- [1] Добкач Л.Я., Цирлов В.Л. Проект стандартизации технологии расширенного обнаружения и реагирования. *Новые направления развития приборостроения. 17-я Междунар. науч.-техн. конф. молодых ученых и студентов: материалы*. Минск, БНТУ, 2024, 257 с.
- [2] Бибило П.Н., Романов В.И. Минимизация многоуровневых представлений систем полностью определенных булевых функций с использованием разложений Шеннона и алгебраических представлений кофакторов. *Информатика*, 2021, т. 18, № 2, с. 7–32. <https://doi.org/10.37661/1816-0301-2021-18-2-7-32>
- [3] Сакулин С.А., Алфимцев А.Н., Ломанов А.А., Добкач Л.Я., Недашковский В.М. Выявление сетевых аномалий на основе взвешенного агрегирования с учетом узловых параметров. *Вестник компьютерных информационных технологий*, 2022, т. 19, № 7 (217), с. 48–56.