УДК 004.056

ПРОЕКТ СТАНДАРТИЗАЦИИ ТЕХНОЛОГИИ РАСШИРЕННОГО ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ

Аспирант Добкач Л. Я.
Кандидат техн. наук, доцент Цирлов В. Л.
Московский государственный технический университет им. Н. Э. Баумана, Москва, Россия

Системы расширенного обнаружения компьютерных атак и реагирования на них (сокращенно – XDR-системы) впервые были предложены компанией Palo Alto в 2018 году, после чего началось их постепенное внедрение на рынке средств защиты информации [1]. Однако это до сих пор больше маркетинговый ход, попытка компаний-разработчиков объединить либо все свои продукты в одном пакете услуг, либо совместить их с продуктами коллег и конкурентов.

С точки зрения защиты информации описанный подход может быть чреват излишними тратами и неэффективным применением СЗИ, что значительно и не лучшим образом влияет на уровень защищенности информационных ресурсов. Отсюда и необходимость подвести ясную, хотя и необязательно единственно возможную теоретическую базу под технологию, которую внедряют прямо в наше время.

Обзор компонентов различных XDR-решений от таких крупных компаний, как Palo Alto, Cisco, Fortinet, Kaspersky Labs и Positive Technologies, выявил принципиальные расхождения подходов к построению комплексной системы безопасности, но также позволил выделить наиболее важные и ключевые черты, которые должны быть присущи этой технологии.

Наиболее близким по функционалу классическим средством защиты информации можно назвать системы обнаружения вторжений (СОВ) уровня сети, и в связке с системой обнаружения и реагирования на конечных узлах (EDR), можно добиться построения минимально необходимого ядра XDR.

Компоненты сетевой СОВ и EDR получают на вход векторы $X(Q')$ и $Y(T')$ событий безопасности с принципиально разных уровней, что требует их приведения к общему виду для последующей работы классификаторов для распознавания компьютерных атак. Результатом этой процедуры является сокращение размерности $Q' \to Q$ параметров сетевой сессии и преобразование $Y(T') \to X(Q)$ параметров конечных узлов сети в формат параметров сессии. Процедура подготовительная и выполняется один раз для защищаемой сети [2].

Считая по умолчанию, что одна сетевая сессия может иметь больше одного узлового события безопасности, мы строим XDR-систему на основе обогащения сетевых данных параллельными сведениями с узлов, образующих защищаемую сеть. Таким образом, осуществляется анализ входящих потоков со всех сторон, что теоретически позволяет добиться более высоких результатов распознавания компьютерных атак, чем при использовании разрозненных классических СЗИ.

Другой немаловажный аспект – возможность внедрения алгоритмов машинного обучения в технологию XDR [3]. Широко известно, что сигнатурные средства защиты информации обладают высокой точностью, но, как правило, неспособны распознать вектор атаки, если ее сигнатура не содержится в базе данных СЗИ. Этот недостаток вынуждает использовать адаптивные методы обнаружения вторжений, в том числе искусственные нейронные сети, деревья решений и другие классификаторы вычислительного интеллекта.

Таким образом, предлагается рассматривать в качестве минимально допустимого стандарта технологии расширенного обнаружения и распознавания компьютерных атак совокупность (ансамбль) сетевой системы обнаружения вторжений и EDR-системы, основанных на адаптивных методах обнаружения вторжений.

Литература

1. Haddon, D. A. E. Zero trust networks, the concepts, the strategies, and the reality / D. A. E. Haddon // Strategy, Leadership, and AI in the Cyber Ecosystem. – Academic Press, 2021. – С. 195–216.

2. Hybrid Network Anomaly Detection Based on Weighted Aggregation Using Endpoint Parameters / L. Y. Dobkacz [et al.] // International Congress on Information and Communication Technology. – Singapore: Springer Nature Singapore, 2023. – С. 269–278.

3. Pissanidis, D. L. Integrating AI/ML in Cybersecurity: An Analysis of Open XDR Technology and its Application in Intrusion Detection and System Log Management / D. L. Pissanidis, K. Demertzis // Preprints. – 2023.