УДК 004.056.53.

МЕТОД ТИПИЗИРОВАННОЙ КОРРЕЛЯЦИИ СОБЫТИЙ EDR ПРИ РЕКОНСТРУКЦИИ МНОГОЭТАПНЫХ КОМПЬЮТЕРНЫХ АТАК

Лукоянов А.А., Рогозин Е.А., Шевцова Г.А.

ФГАОУ ВО «Российский государственный гуманитарный университет»

г. Москва, Российская Федерация

Системы класса Endpoint Detection and Response (EDR) регистрируют запуск процессов, события аутентификации, действия, выполняемые от имени учётных записей, обращения к файлам и системным объектам, а также сетевую активность процессов. При многоэтапной компьютерной атаке отдельные события могут не отличаться от штатной активности, поэтому для выявления сценария атаки необходимо устанавливать связи между ними. Для решения этой задачи применяются методы корреляции событий и анализа их происхождения [1]. В частности, в подходе Tactical Provenance Analysis используются Tactical Provenance Graphs (графы происхождения и взаимосвязей событий), позволяющие объединять причинно связанные EDR-оповещения [2]. В работе предлагается метод корреляции событий EDR-телеметрии без предварительного обучения модели и без объединения разных типов связей в единый числовой показатель.

Для последующего сопоставления каждое событие EDR-телеметрии описывается единым набором признаков. Сопоставление с MITRE ATT&CK выполняется после построения графа, на этапе интерпретации выявленных последовательностей событий. i-е событие представляется кортежем:

$$e_{\text{i}} = \langle t_i, h_i, u_i, s_i, q_i, q_i^p, a_i, o_i, x_i \rangle,$$

где t_i — время регистрации события; h_i — идентификатор конечного узла; u_i — учетная запись; s_i— идентификатор пользовательской или системной сессии; q_i — устойчивый идентификатор процесса; q_i^p — устойчивый идентификатор родительского процесса; a_i— зарегистрированное действие; o_i — объект, в отношении которого выполнено действие; x_i — дополнительные атрибуты (путь, хеш, командная строка, сетевой адрес и др.). Использование устойчивых идентификаторов процессов позволяет различать отдельные экземпляры процессов и исключает их ошибочное связывание только на

основании совпадающих идентификаторов PID (Process Identifier — идентификатор процесса).

При корреляции учитываются следующие виды связей: процессная, сессионная, объектная и межузловая. Процессная связь устанавливается между событиями одного экземпляра процесса или родительского и дочернего процессов; сессионная — между событиями одной сессии; объектная — при использовании результата одного действия в последующем; межузловая — при переходе активности между конечными узлами.

Связи формируют типизированный ориентированный граф:

$$G = (V, E, \lambda), \quad \lambda : E \rightarrow 2^R,$$

где V — множество EDR-событий; E — множество направленных связей между ними; R — множество типов связей; $\lambda : E \rightarrow 2^R$ — функция, сопоставляющая каждой связи один или несколько типов. Направление связи задается с учетом причинной зависимости и временной последовательности событий. Таким образом, для каждой дуги графа сохраняется основание, по которому соответствующие события были объединены.

После построения графа события сопоставляются с тактиками и способами реализации действий нарушителя, представленными в MITRE ATT&CK [3]. Такое сопоставление позволяет определить назначение отдельных действий и связать их с известными моделями поведения нарушителя. Для представления последовательности и взаимосвязей действий используется модель Attack Flow, позволяющая описывать развитие сценария атаки на основе элементов ATT&CK [4].

Путь рассматривается как возможная многоэтапная атака, если несколько связанных действий совместно указывают на реализацию единого сценария и не соответствуют известной штатной активности. Например, последовательность «открытие вложения фишингового письма → PowerShell (средство выполнения команд и сценариев операционной системы Windows) → выполнение вредоносной программы → создание механизма закрепления → соединение с сервером управления» объединяется по процессным, объектным и межузловым

связям. Совпадение пользователя и времени учитывается только как дополнительный признак.

Предлагаемый подход позволяет перейти от анализа отдельных EDR-событий к восстановлению связанной последовательности действий, что особенно важно при выявлении многоэтапных компьютерных атак. Отдельные действия нарушителя могут не содержать явных признаков компрометации, однако их объединение по процессным, сессионным, объектным и межузловым связям позволяет проследить развитие атаки и отличить действия нарушителя от легитимной активности.

Особенностью предлагаемого метода является типизированное представление связей между EDR-событиями с сохранением основания их установления и последующей интерпретацией полученного графа с использованием MITRE ATT&CK и Attack Flow.

Практическая значимость метода заключается в объединении связанных EDR-событий в последовательность, удобную для анализа и расследования инцидента. Эффективность метода предлагается оценивать по точности восстановления последовательности атаки, количеству ошибочно включённых событий, времени построения графа и вычислительным затратам.

Список использованной литературы

1. Shaukat S.U., Khan S., Parkinson S. Event Log Correlation for Multi-Step Attack Detection // Security and Privacy. — 2026. — Vol. 9, No. 1. — e70151. — DOI: 10.1002/spy2.70151.

2. Hassan W.U., Bates A., Marino D. Tactical Provenance Analysis for Endpoint Detection and Response Systems // 2020 IEEE Symposium on Security and Privacy. — 2020. — P. 1172–1189. — DOI: 10.1109/SP40000.2020.00096.

3. MITRE ATT&CK. Enterprise Matrix [Электронный ресурс]. — URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 25.09.2026).

4. Center for Threat-Informed Defense. Attack Flow v4.0 Documentation [Электронный ресурс]. — URL: https://center-for-threat-informed-defense.github.io/attack-flow/ (дата обращения: 25.09.2026).