Методи та алгоритми детектування кіберзагроз і реагування на інциденти інформаційної безпеки у мультихмарних середовищах

УДК 004.056.57

Венгерський Петро [1], Радченко Максим [2]

Львівський національний університет ім. Івана Франка,
[1]petro.venherskyy@lnu.edu.ua, [2]maksym.radchenko@lnu.edu.ua

Сучасні підприємства масово переходять до мультихмарних середовищ: понад 75 % організацій одночасно використовують ресурси Amazon Web Services, Microsoft Azure та Google Cloud Platform [1]. Різнорідність подій безпеки з хмарних джерел породжує критичну проблему alert fatigue - перевантаження аналітиків центрів оперативної безпеки хибними спрацюваннями. За даними результатами систематичного огляду, аналітики витрачають понад половину робочого часу на обробку хибних алертів, що безпосередньо збільшує середній час виявлення та усунення реальних інцидентів [2].

Метою роботи є розробка та програмна реалізація методів і алгоритмів детектування кіберзагроз і реагування на інциденти інформаційної безпеки у мультихмарних середовищах, що забезпечують зниження рівня хибних спрацювань та скорочення часу реагування.

Існуючі комерційні рішення класу CDR (Prisma Cloud, Microsoft Defender for Cloud, Google Chronicle) та відкриті системи (Wazuh, Falco) або не забезпечують формалізованої пре-фільтрації подій до їх запису в сховище, або реалізують post-ingestion фільтрацію без врахування семантичної схожості алертів від різних джерел. Це призводить до надлишкового накопичення дублюючих записів і знижує якість кореляції подій [3].

Наукова новизна роботи полягає у формалізації п'ятистадійного конвеєра пре-фільтрації подій безпеки як функціональної композиції із принципом short-circuit evaluation; розробці алгоритму оцінки семантичної схожості алертів на основі зваженої метрики Жаккара; 3) побудові FSM-моделі життєвого циклу інциденту з вбудованими SLA-метриками MTTA/MTTR.

Конвеєр пре-фільтрації формалізовано, як

$$F = F_5 \circ F_4 \circ F_3 \circ F_2 \circ F_1$$

де кожна стадія $F_i : \mathscr{E} \to \{0,1\}$ реалізує послідовно: порогову фільтрацію за рівнем критичності, фільтрацію за списком блокування `rule_ID`, зіставлення з шаблонами хибних спрацювань, пригнічення шуму методом ковзного часового вікна та оцінку схожості алертів. П'ята стадія є ключовим внеском роботи: для двох алертів *a* та *b* визначено зважену функцію схожості:

$$\mathrm{sim}(a, b) = 0{,}40 \cdot \mathbb{1}[\tau_a = \tau_b] + 0{,}30 \cdot \mathbb{1}[\theta_a = \theta_b] + 0{,}20 \cdot \mathbb{1}[\alpha_a = \alpha_b] + 0{,}10 \cdot J(T_a, T_b)$$

де τ - MITRE-тактика, θ - MITRE-техніка, α - ідентифікатор агента, $J(T_a, T_b)$ - індекс Жаккара токенів заголовку. При перевищенні порогу $\delta = 0{,}7$ виконується злиття семантично близьких алертів замість створення дублюючих записів.

Розроблено алгоритм об'єднання подій із гетерогенних джерел у єдиний нормалізований потік та механізм дедуплікації хмарних знахідок. Модель рушія детектування формалізує п'ять типів правил: порогове, паттерн, відсутність, кореляція, послідовність. Модель інциденту реалізовано як детермінований скінченний автомат $M = (Q, \Sigma, \delta, q_0, F)$ із шістьма станами та вбудованим контролем SLA.

Програмну реалізацію виконано у складі хмарно-нативної платформи uSafe. Основний модуль аналізу реалізовано у модулях alert_filters, alert_ingest та rule_engine. Також, модуль сканування хмарної безпеки, наприклад - AWS, охоплює 239 перевірок безпеки у 12 категоріях. Верифікацію алгоритмів проведено на синтетичних тестових наборах, що підтвердили коректність усіх стадій конвеєра.

Аналіз статистики FilterStats підтверджує ефективність розробленого конвеєра: pass rate складає ~14 %, тобто ~86 % подій відсіюється до їх запису в базу даних як події безпеки. Цей результат порівнянний із показниками ML-підходів (Carbon Filter: 82-84 % [3]) за суттєво вищої детермінованості та пояснюваності рішень. Розроблені методи впроваджено в продуктивному середовищі платформи uSafe та можуть бути застосовані у комерційних продуктах класу MSSP.

1. Illumio. The 2025 Global Cloud Detection and Response Report. URL: https://www.illumio.com/resource-center/2025-global-cloud-detection-and-response-report (дата звернення: 08.04.2026).
2. Tariq S., Chhetri M. B., Nepal S., Paris C. Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities. ACM Computing Surveys. – 2025. – Vol. 57, No. 9. – DOI: 10.1145/3723158.
3. Yang L., Li Z., Chen H. Carbon Filter: Reducing False Positive Alerts in Security Operations Centers. IEEE Transactions on Information Forensics and Security. – 2022. – Vol. 17. – P. 2341–2354.

Виявлення несанкціонованого доступу та компрометації облікових записів завдяки SIEM системі

УДК 004.056

Степовенко Юрій[1], Ілля Фалендиш[2], Євгеній Юр'єв[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]urastepovenko1@gmail.com, [2]illia.falendysh02@gmail.com, [3]yurev05@gmail.com

У сучасному світі важко переоцінити роль кібербезпеки. Враховуючи кількість існуючих вірусів, атак та загроз комп'ютерні системи вимагають особливої уваги до своєї активності. Саме тому сучасні компанії часто вводять в експлуатацію SIEM системи, які завдяки централізованому збору логів та евристичному аналізу здатні виявляти аномалії в активності системи та повідомляти про це IT команду. Головною проблемою подібних систем є велика кількість хибних спрацювань - поведінка як інтернет трафіку, так і користувачів рідко буває стабільною та передбачуваною, проте автоматизований алгоритм чи штучний інтелект не можуть відрізнити істинні спрацювання від хибних.