УДК 004.777.056
DOI https://doi.org/10.32782/2663-5941/2026.3.1/07

Головенець М.І.
https://orcid.org/0009-0000-8306-1447
Харківський національний університет радіоелектроніки

Колісник М.М.
https://orcid.org/0000-0002-1075-9470
Харківський національний університет радіоелектроніки

МЕТОД КОРЕЛЯЦІЇ ПОДІЙ ЖУРНАЛІВ ВЕБСЕРВЕРІВ І WAF ДЛЯ ПОПЕРЕДЖЕННЯ КІБЕРІНЦИДЕНТІВ У ВЕБЗАСТОСУНКАХ

Вебзастосунки є одним із найбільш атакованих об'єктів сучасної інформаційної інфраструктури. За даними Verizon Data Breach Investigations Report 2023, понад 43% успішних кіберінцидентів пов'язані саме з атаками на вебзастосунки. Широко застосовуваний стек Nginx + ModSecurity забезпечує журналювання HTTP-трафіку та роботу WAF відповідно, однак ізольований аналіз цих двох джерел не дозволяє ефективно виявляти складні багатоетапні атаки. У статті досліджується метод кореляції подій журналів вебсервера Nginx та міжмережевого екрана вебзастосунків ModSecurity з метою своєчасного виявлення та попередження кіберінцидентів. Розроблено архітектуру системи кореляції, що базується на нормалізації журналів Nginx access.log і ModSecurity audit log та їх часовій і семантичній агрегації з використанням детерміністичного ключа зв'язування за полем X-Request-ID – унікального 32-символьного ідентифікатора HTTP-транзакції. Точність зв'язування записів за цим полем склала 100% на наборі з 494 942 транзакцій. Запропоновано алгоритм виявлення аномалій на основі ковзного вікна (крок 30 секунд) та бібліотеки з 8 правил кореляції патернів атак OWASP Top 10, реалізованих у форматі YAML та завантажуваних динамічно без перезапуску ядра кореляції. Серед розроблених правил особливе місце займає правило виявлення обходу WAF (WAF Bypass) – коли ModSecurity виносить рішення block, але Nginx повертає HTTP 200, що не виявляється жодним базовим підходом при ізольованому аналізі. Проведено експериментальну перевірку методу на синтетичному наборі даних обсягом 494 942 подій (19 680 атакових, 3.97%), що відтворює 15 діб роботи реального вебсервера з чотирма категоріями трафіку: гучні атаки з правилами CRS, stealth-атаки що обходять WAF, хибнопозитивні запити та нормальний трафік. Експеримент підтвердив ефективність підходу: точність виявлення атак (F1-міра) склала 0.943, хибнопозитивний рівень – 2.7%, середній час виявлення інциденту (MTTD) скоротився з 4.2 до 1.8 хвилини. Порівняно з базовим підходом (аналіз лише ModSecurity audit log) приріст F1-міри становить +14.3%, зниження FPR – 55.7%, скорочення MTTD – 57.1%. Результати дослідження можуть бути використані при розробці систем захисту вебінфраструктури підприємств на базі відкритого стеку Nginx + ModSecurity без необхідності придбання комерційних SIEM-рішень.

Ключові слова: *вебзастосунок, кореляція подій, WAF, журнал подій, SIEM, кіберінцидент, виявлення атак, OWASP Top 10, IDS/IPS, Nginx, ModSecurity, X-Request-ID.*

Постановка проблеми. Стрімкий розвиток вебтехнологій та зростання кількості інтернет-сервісів зумовлюють підвищений інтерес зловмисників до вебзастосунків як основного вектора атак. За даними звіту Verizon Data Breach Investigations Report 2023, понад 43% успішних кіберінцидентів пов'язані саме з атаками на вебзастосунки, зокрема ін'єкціями, міжсайтовим скриптингом (XSS) та порушеннями автентифікації [1]. Широко застосовуваний вебсервер Nginx разом із модулем ModSecurity формує ефективний відкритий стек захисту вебзастосунків. Nginx генерує детальний access.log із параметрами HTTP-запитів, тоді як ModSecurity веде audit log із зафіксованими спрацьовуваннями правил Core Rule Set (CRS). Проте ізольований аналіз цих двох джерел не дозволяє ефективно виявляти складні, багатоетапні атаки: Nginx може зафіксувати підозрілу послідовність запитів, яку ModSecurity окремо не класифікував як атаку, і навпаки [2].

Аналіз останніх досліджень і публікацій. Проблема кореляції журналів безпеки є предме-

том активних досліджень протягом останніх двох десятиліть. Основи теорії кореляції подій закладено в роботах Валдес та Скіннер [3], які запропонували нечітку кластеризацію попереджень IDS на основі подібності атрибутів. Надалі підхід був розвинений у концепціях «alert fusion» та «attack scenario reconstruction» Нінг та ін. [4].

Сучасні SIEM-системи (Splunk, IBM QRadar, Microsoft Sentinel) реалізують кореляцію через механізми правил, статистичного аналізу та машинного навчання. Однак більшість комерційних рішень орієнтовані на корпоративну мережеву інфраструктуру і не враховують специфіку вебзастосунків – унікальні патерни HTTP-трафіку, сесійну логіку та особливості формату журналів Nginx і ModSecurity audit log [5]. Дослідження Зуек та ін. [7] показали, що кореляція мережевих журналів з журналами застосунків збільшує точність виявлення SQL-ін'єкцій на 23% порівняно з аналізом лише мережевого рівня.

В ході аналізу наукової літератури систематизовано існуючі підходи до виявлення кіберінцидентів у вебзастосунках. Виділено три основні класи методів. Сигнатурні методи базуються на порівнянні вхідного трафіку з базою відомих зразків атак; реалізуються в системах IDS/IPS (Snort, Suricata) та WAF з Core Rule Set. Аномальні методи формують базову лінію нормальної поведінки і виявляють відхилення від неї із застосуванням алгоритмів машинного навчання (ізоляційний ліс, автоенкодери, LSTM). Методи кореляції подій аналізують послідовності та взаємозв'язки між подіями з кількох джерел у часовому вікні і реалізуються в SIEM-системах.

Разом з тим, у наявних роботах недостатньо опрацьовано питання темпоральної кореляції повільних розподілених атак, а також детерміністичного зв'язку між ідентифікатором транзакції ModSecurity та відповідним записом у Nginx access.log – що і визначає наукову новизну даного дослідження.

Постановка завдання. Метою статті є розробка та дослідження методу кореляції подій журналів Nginx і ModSecurity для підвищення ефективності виявлення кіберінцидентів у вебзастосунках, що забезпечує переваги над ізольованим аналізом кожного з джерел та не потребує комерційних SIEM-рішень.

Виклад основного матеріалу. Структура журналів Nginx та ModSecurity. Nginx формує журнал доступу у форматі Combined Log Format. Для потреб кореляції до стандартного формату додано поле $request_id – унікальний 32-символьний шістнадцятковий ідентифікатор запиту, який генерується модулем ngx_http_core_module та передається у заголовку відповіді X-Request-ID. Визначено 10 ключових полів, що використовуються у кореляції: IP-адреса джерела, часова мітка, HTTP-метод, URI, версія протоколу, код статусу відповіді, розмір тіла відповіді, User-Agent, request_id, час обробки запиту.

ModSecurity v3 у режимі JSON генерує структурований audit log, що складається з секцій, кожна з яких відповідає певному аспекту транзакції. Досліджено формат секцій A (заголовок транзакції), B (заголовки запиту), C (тіло запиту), F (заголовки відповіді), H (інформація аудиту) та K (список спрацьованих правил). Ключовою технічною задачею є зв'язування запису Nginx access.log із відповідним записом ModSecurity audit log. Серед трьох можливих підходів обрано зв'язування за request_id / transaction.id – детерміністичний метод без хибних збігів.

Архітектура системи кореляції. Запропонована система включає чотири основні компоненти: модуль збору та нормалізації журналів (parser.py), модуль збагачення подій геолокаційними даними, ядро кореляції (correlator.py) та модуль реагування (elastic_writer.py). Ключовою операцією є зв'язування записів Nginx та ModSecurity за полем X-Request-ID з допустимим часовим зсувом ±50 мс (joiner.py).

Ядро кореляції реалізовано мовою Python 3.11 з використанням таких бібліотек: collections.deque для ковзного вікна O(1) вставки/видалення; re для парсингу Nginx access.log; json для парсингу ModSecurity JSON audit log; geoip2 для геолокації; pyyaml для завантаження правил кореляції; elasticsearch для запису інцидентів. Загальний обсяг реалізації – близько 600 рядків коду Python.

Формальна модель кореляції. Нормалізована подія визначається кортежем:

$$e_i = \langle id, t, srcIP, method, uri, status, ruleIDs, anomalyScore, action \rangle$$

де id – унікальний ідентифікатор транзакції (X-Request-ID); t – часова мітка (Unix epoch, мс); srcIP – IP-адреса джерела; method – HTTP-метод; uri – URI ресурсу; status – код відповіді HTTP; ruleIDs – множина ідентифікаторів спрацьованих правил CRS; anomalyScore – сумарний бал аномальності; action – рішення WAF (pass / block).

Кореляційне правило визначається як умовна функція R: 2^E → {0,1}, де R(W) = 1, якщо послідовність подій у часовому вікні $W(t_0, \Delta t) = \{e_i \in E \mid t_0 \le t_i < t_0 + \Delta t\}$ відповідає заданому патерну атаки.

Формула розрахунку ризику інциденту:

$$RiskScore = \max(ruleRisk) \times freqFactor \times reputationFactor,$$

де freqFactor = min(eventCount / threshold, 3.0); reputationFactor = 1.5 якщо IP у базах Threat Intelligence, інакше 1.0. Рівні ризику: Critical (>9), High (6–9), Medium (4–6), Low (2–4), Info (0–2).

Алгоритм кореляції реалізує 8-етапний конвеєр: нормалізація потоку подій; JOIN записів за X-Request-ID; збагачення геолокацією та репутацією IP (MaxMind GeoIP2, AbuseIPDB); ковзне вікно з кроком 30 с; перевірка умов правил (field / operator / value); агрегація спрацьованих правил в інциденти; розрахунок ризику за формулою CVSS v3.1; запис у Elasticsearch та реагування.

Бібліотека правил кореляції. Для покриття загроз OWASP Top 10 розроблено бібліотеку з 8 кореляційних правил у форматі YAML. Правила завантажуються динамічно без перезапуску ядра кореляції. Правило COR-BYP-001 є унікальним внеском запропонованого методу – воно виявляє ситуацію, коли ModSecurity виніс рішення block, але Nginx повернув HTTP 200, що не виявляється жодним базовим підходом при ізольованому аналізі журналів.

Ознаки подій, що свідчать про підготовку або реалізацію атаки. На основі аналізу OWASP Top 10, бази правил ModSecurity CRS 3.3.5 та синтетичного набору тестових логів визначено ознаки кіберінцидентів за 6 класами атак. Ознаки поділено на атомарні (виявляються в одній події) та кореляційні (виявляються лише в послідовності подій).

Окремо визначено ознаки обходу WAF (WAF Bypass) – ситуації, коли атака досягла цілі попри наявність ModSecurity. Виявляються виключно через кореляцію: ModSecurity виніс рішення block, але Nginx повернув HTTP 200 – свідчить про bypass або некоректну конфігурацію; ModSecurity спрацював з anomaly score нижче threshold – запит пропущено, але він містив часткові ознаки атаки; послідовність запитів, кожен з яких нижче порогу спрацьовування CRS, але в сукупності формує повний SQL-запит (split-payload техніка). Ці ознаки є унікальним внеском запропонованого методу, оскільки жоден з них не виявляється при ізольованому аналізі журналів.

Експериментальна перевірка. Для перевірки ефективності методу використано синтетично згенерований набір даних, що імітує 15 діб роботи вебсервера з інтенсивністю 10 запитів/сек. Генератор реалізовано на Python і відтворює реалістичний трафік чотирьох категорій: гучні атаки (з правилами CRS), stealth-атаки (обходять ModSecurity без спрацьовування правил), false positive запити та нормальний трафік. Набір містить 494 942 події, з яких 19 680 є атаковими (3.97%). Тестове середовище: Ubuntu Server 24.04 LTS, Nginx 1.24.0 + ModSecurity v3.0.12 + CRS 3.3.5, Elasticsearch 8.19, Python 3.11 (VirtualBox VM, 2 vCPU, 4 GB RAM).

Для порівняння використано два базові підходи: аналіз лише ModSecurity audit log та об'єднаний аналіз без кореляції. Результати порівняльного оцінювання наведено у табл. 2.

Запропонований метод кореляції забезпечив F1-міру 0.943 та FPR 2.7%, що є суттєвим покращенням порівняно з базовим підходом (F1 = 0.825, FPR = 6.1%). MTTD скоротився з 4.2 хв до 1.8 хв завдяки ковзному вікну з кроком 30 с. Точність зв'язування записів Nginx та ModSecurity за полем X-Request-ID склала 100% (14 808 зв'язаних пар). Результати за класами атак наведено у табл. 3.

Таблиця 1

Бібліотека правил кореляції

ID правила	Клас атаки	Умова кореляції	Вікно	Ризик
COR-942-001	SQL Injection	≥2 події CRS 942xxx від одного IP	5 хв	Critical
COR-941-001	XSS Reflected	CRS 941xxx + status 200/403	2 хв	High
COR-930-001	Brute Force	≥5 HTTP 401/403 на /login* від IP	1 хв	High
COR-930-002	Path Traversal	≥3 URI з ../ або %2e%2e + HTTP 403	5 хв	Critical
COR-913-001	Scanner/Recon	≥10 HTTP 404 від одного IP	10 хв	Medium
COR-000-001	DDoS Layer 7	≥50 req/хв від IP на один URI	1 хв	Critical
COR-BYP-001	WAF Bypass	action=block + Nginx status=200	–	Critical
COR-942-002	Split-payload SQLi	≥3 запити 942xxx від IP на URI	3 хв	High

Таблиця 2

Порівняння ефективності методів виявлення атак

Метод	Precision	Recall	F1-міра	FPR	MTTD (хв)
Тільки ModSecurity audit log (базовий)	0.871	0.783	0.825	0.061	4.2
Nginx + ModSecurity (без кореляції)	0.889	0.812	0.849	0.048	3.6
Запропонований метод кореляції	0.951	0.936	0.943	0.027	1.8

Таблиця

F1-міра за класами атак

Клас атаки	Зразків	F1 (базовий)	F1 (метод)	Приріст
SQL Injection	4 200	0.841	0.971	+15.5%
Brute Force	3 750	0.893	0.962	+7.7%
XSS Reflected	2 900	0.812	0.944	+16.3%
Path Traversal	2 100	0.778	0.931	+19.7%
Scanner/Recon	3 800	0.921	0.957	+3.9%
DDoS Layer 7	1 500	0.654	0.912	+39.4%
WAF Bypass	500	0.000	0.847	+∞
Split-payload SQLi	–	0.000	0.881	+∞

Найвищу ефективність показано для SQL Injection (F1 = 0.971) та Brute Force (F1 = 0.962). Найбільший відносний приріст досягнуто для DDoS Layer 7 (+39.4%), WAF Bypass та Split-payload SQLi – класів, що базовий підхід не виявляє взагалі. Дещо нижчі результати отримано для Scanner/Recon (+3.9%) через перекриття з активністю легітимних краулерів.

Висновки. У статті запропоновано та досліджено метод кореляції подій журналів вебсерверів і WAF для попередження кіберінцидентів у вебзастосунках. Основні наукові результати:

1. Розроблено архітектуру системи кореляції на базі стеку Nginx + ModSecurity v3 + CRS 3.3.5, що включає модулі нормалізації із детерміністичним зв'язуванням записів за X-Request-ID (точність 100%), збагачення, ядро кореляції та підсистему реагування.

2. Формалізовано модель кореляції подій на основі часових вікон та кортежного представлення атрибутів об'єднаного запису Nginx access. log і ModSecurity audit log.

3. Сформовано бібліотеку з 8 кореляційних правил у форматі YAML для 6 класів атак OWASP Top 10 з визначеними умовами, часовими вікнами та рівнями ризику CVSS.

4. Експериментально підтверджено підвищення F1-міри до 0.943 (+14.3% vs базовий підхід), зниження FPR до 2.7% (−55.7%) та скорочення MTTD до 1.8 хв (−57.1%) на наборі 494 942 подій.

5. Вперше виявлено та формалізовано клас інцидентів WAF Bypass через кореляцію рішення ModSecurity action=block з кодом відповіді Nginx HTTP 200.

Перспективи подальших досліджень: адаптація розмірів вікон кореляції засобами машинного навчання; підтримка у хмарних середовищах (Kubernetes Ingress); розширення правил для захисту REST API та GraphQL.

Список літератури:

1. Verizon Communications Inc. Data Breach Investigations Report 2023. Verizon, 2023. 87 p. URL: https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

2. Endler D., Shema O. Web Application Firewall Evaluation Criteria. WASC-WAFEC, 2006. 32 p.

3. Valdes A., Skinner K. Probabilistic alert correlation. Recent Advances in Intrusion Detection: Lecture Notes in Computer Science. *Springer*, 2001. Vol. 2212. P. 54–68. https://doi.org/10.1007/3-540-45474-8_4

4. Ning P., Cui Y., Reeves D. S. Constructing attack scenarios through correlation of intrusion alerts. Proceedings of the 9th ACM Conference on Computer and Communications Security. *Washington*, 2002. P. 245–254. https://doi.org/10.1145/586110.586144

5. Sommer R., Paxson V. Outside the closed world: on using machine learning for network intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy. *Oakland*, 2010. P. 305–316. https://doi.org/10.1109/SP.2010.25

6. OWASP Foundation. ModSecurity Core Rule Set (CRS): Official Documentation. Version 3.3.5. OWASP Foundation, 2023. URL: https://coreruleset.org/docs/

7. Zuech R., Khoshgoftaar T. M., Wald R. Intrusion detection and big heterogeneous data: a survey. Journal of Big Data. *Springer*, 2015. Vol. 2, No. 1. P. 1–41. https://doi.org/10.1186/s40537-015-0013-4

8. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. *National Institute of Standards and Technology*, 2007. 127 p. https://doi.org/10.6028/NIST.SP.800-94

9. OWASP Foundation. OWASP Top 10: 2021. The Ten Most Critical Web Application Security Risks. *OWASP Foundation*, 2021. 26 p. URL: https://owasp.org/www-project-top-ten/

10. Chuvakin A., Schmidt K., Phillips C. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. *Syngress*, 2012. 460 p.

Holovenets M.I., Kolisnyk M.M. METHOD OF CORRELATING WEB SERVER AND WAF LOG EVENTS FOR PREVENTION OF CYBER INCIDENTS IN WEB APPLICATIONS

Web applications represent one of the most frequently attacked components of modern information infrastructure. According to the Verizon Data Breach Investigations Report 2023, over 43% of successful cyber incidents involve web application attacks. The widely adopted Nginx + ModSecurity stack provides HTTP traffic logging and WAF capabilities respectively; however, isolated analysis of these two sources fails to detect complex multi-stage attacks effectively. This paper proposes and investigates a method for correlating events from Nginx web server access logs and ModSecurity WAF audit logs for timely detection and prevention of cyber incidents in web applications. A four-component correlation system architecture is developed: a log normalization module (parser.py), an event enrichment module (MaxMind GeoIP2), a correlation engine (correlator.py) with a sliding window mechanism based on collections.deque with O(1) insertion/deletion complexity, and a response module (elastic_writer.py). The deterministic linking key X-Request-ID achieves 100% join accuracy across 494,942 transactions. A library of 8 YAML-defined correlation rules covering OWASP Top 10 attack patterns is developed, including a novel WAF Bypass detection rule that identifies cases where ModSecurity issues a block decision while Nginx returns HTTP 200 – a class of incidents undetectable by any baseline approach. Experimental evaluation on a synthetic dataset of 494,942 events (19,680 attack events, 3.97%) simulating 15 days of real web server operation confirmed the effectiveness: F1-score of 0.943 (+14.3% vs baseline), false positive rate of 2.7% (−55.7%), and mean time to detect reduced from 4.2 to 1.8 minutes (−57.1%). The proposed solution operates entirely on open-source software without requiring commercial SIEM licenses.

Keywords: *web application, event correlation, WAF, event log, SIEM, cyber incident, attack detection, OWASP Top 10, IDS/IPS, Nginx, ModSecurity, X-Request-ID.*

Дата першого надходження статті до видання: 25.03.2026
Дата прийняття статті до друку після рецензування: 21.04.2026
Дата публікації (оприлюднення) статті: 19.05.2026