Автоматизоване реагування на інциденти безпеки з використанням Suricata та SIEM Wazuh

УДК 004.056

Базилевський Д. В.[1], Цаволик Т. Г.[2]

Західноукраїнський національний університет, [1]bazilevskijdavid6@gmail.com

З огляду на стрімке зростання кількості кіберзагроз, спрямованих на критичну інфраструктуру та корпоративні мережі, автоматизація процесів реагування на інциденти стає важливим складником сучасної кібербезпеки [3]. Згідно зі звітами провідних організацій у сфері кібербезпеки, автоматизація атак зловмисниками вимагає від захисників впровадження систем, здатних реагувати на інциденти у режимі реального часу. Традиційний ручний моніторинг журналів подій уже не є ефективним через високу інтенсивність трафіку та складність векторів атак. Тому розробка та впровадження систем автоматизованого реагування на базі рішень з відкритим кодом є актуальним завданням для сучасних фахівців з інформаційної безпеки.

Автоматизоване реагування на інциденти безпеки — це процес виявлення, аналізу та нейтралізації загроз без безпосередньої участі людини на початкових етапах. Основна мета полягає у мінімізації часу перебування зловмисника в мережі (Dwell Time) та зменшенні навантаження на аналітиків центру моніторингу безпеки (SOC). Ключовими компонентами такої системи є: 1) джерела даних — мережеві сенсори, журнали ОС, антивірусні системи; 2) аналітичне ядро — системи класу SIEM (Security Information and Event Management), що корелюють події; 3) механізми дії — системи IDS/IPS (Intrusion Detection/Prevention System), що здатні блокувати трафік у режимі реального часу [5].

Використання Suricata IDS/IPS як активного засобу захисту. Suricata — це високопродуктивний механізм моніторингу мережевої безпеки, який підтримує виявлення вторгнень (IDS), запобігання вторгненням (IPS) та моніторинг мережевої безпеки (NSM) [1]. У режимі IPS (Inline mode) система забезпечує не лише фіксацію підозрілої активності, а й автоматичне блокування IP-адрес або розірвання з'єднань у реальному часі. Приклад правила для блокування SQL Injection:

```
drop http any any -> 10.10.20.2 80 \
    (msg:"LAB SQLi auth bypass in payroll_app.php"; \
    flow:established,to_server; \
    http.uri; content:"/payroll_app.php"; nocase; \
    http.request_body; pcre:"/(\%27|')(\s|\+)*(or|OR)(\s|\+)*(1=1|'1'='1)/i"; \
    classtype:web-application-attack; priority:1; \
    sid:1001030; rev:1;)
```

Рис. 1. Правило Suricata для виявлення SQL Injection

Команда drop ініціює негайне блокування трафіку, що є базовим етапом автоматизованого реагування [1].

Інтеграція з SIEM Wazuh для візуалізації та управління. Wazuh є платформою для моніторингу безпеки, яка інтегрує функції збору журналів, аналізу файлової цілісності та виявлення вразливостей. У даній роботі Wazuh

виступає як центральна консоль SOC-аналітика [2]. Suricata аналізує трафік та формує події у форматі eve.json, після чого Wazuh Agent передає їх на Wazuh Manager для обробки декодерами та правилами кореляції. Отримана інформація відображається на Wazuh Dashboard із зазначенням IP-адреси джерела атаки, типу загрози, часу та статусу реагування. Для ефективного реагування у Wazuh налаштовані спеціалізовані панелі моніторингу (Dashboards), які дозволяють швидко ідентифікувати найбільш атаковані сервіси, географічне розташування джерел атак (GeoIP) та динаміку спрацювань правил Suricata за рівнем критичності. Це забезпечує повну видимість мережевих інцидентів та дозволяє проводити цифрову криміналістику (Digital Forensics) після автоматичного блокування загроз [4].

Поєднання Suricata IPS та SIEM Wazuh створює багаторівневу систему захисту мережі. Suricata забезпечує швидку автоматичну реакцію на рівні мережевого трафіку, а Wazuh надає аналітичний інструментарій для моніторингу та розслідування інцидентів.

1. OISF. Suricata User Guide – Intrusion Detection and Prevention. [Електронний ресурс]. – Режим доступу: https://docs.suricata.io/en/latest/ips/index.html.
2. Wazuh Inc. Integration of Suricata with Wazuh for Network Threat Detection. [Електронний ресурс]. – Режим доступу: https://documentation.wazuh.com/current/proof-of-concept-guide/integrate-network-ids-suricata.html.
3. ENISA Threat Landscape Report 2025. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
4. MITRE Corporation. ATT&CK Framework – Command and Control, Initial Access and Web Attacks Techniques. [Електронний ресурс]. – Режим доступу: https://attack.mitre.org/
5. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST SP 800-94). – Gaithersburg: NIST, 2007. – 127 p. [Електронний ресурс]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf.

Нормативно-правове регулювання кіберзахисту систем штучного інтелекту в Україні

УДК 004.8:342 (043.2)

Артем Жилін[1], Олександра Ценцеря[2]

Київський політехнічний інститут імені Ігоря Сікорського,
[1]zhylinartem@gmail.com, [2]o.tsentseria.s01@kpi.ua

Метою роботи є аналіз нормативно-правової бази кіберзахисту систем штучного інтелекту (далі – ШІ) в Україні та визначення напрямів її удосконалення.