ПОРІВНЯЛЬНИЙ АНАЛІЗ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ

Пліщенко В.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

В умовах стрімкого зростання обсягів даних та безперервної еволюції складності і адаптивності кібератак, традиційні підходи до захисту інформаційно-телекомунікаційних систем (ІТС), що ґрунтуються на розрізнених компонентах, поступово втрачають ефективність. Це зумовлює провідну роль систем управління інформаційною безпекою та подіями (SIEM) як ядра сучасних центрів моніторингу та реагування на інциденти. Водночас традиційні SIEM-рішення стикаються з проблемами масштабованості, високим рівнем хибнопозитивних спрацювань і обмеженою здатністю виявляти нові, зокрема zero-day, загрози. Сучасні SIEM-платформи поєднують функції систем виявлення та запобігання вторгнень (IDS/IPS), інтегруються з іншими модулями багаторівневої архітектури безпеки, агрегують журнали подій із серверів, клієнтських пристроїв і прикладних додатків та корелюють отримані дані, формуючи цілісну картину стану безпеки ІТС [1]. IDS/IPS, своєю чергою, здійснюють інспекцію трафіку в реальному часі на основі сигнатурного і поведінкового аналізу [2].

Метою доповіді є аналіз архітектури, функціональних можливостей та еволюційного розвитку SIEM-систем — від традиційних платформ до рішень нового покоління. **В доповіді** наводяться результати теоретичного аналізу основних функціональних можливостей IDS/IPS-систем та їх порівняння [3]. Основну увагу приділено компонентам Next-Gen SIEM, зокрема інтеграції модулів аналітики поведінки користувачів і сутностей (UEBA) для виявлення аномалій, а також платформ оркестрації, автоматизації та реагування (SOAR) [4], що формують основу для подальших досліджень специфічних методів детектування, зокрема в умовах обфускації мережевого трафіку.

Список літератури

1. Bezas, K. and Filippidou, F. «Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)». Indonesian Journal of Computer Science, 12(2). pp. 443–468. 2023. DOI: https://doi.org/10.33022/ijcs.v12i2.3182.

2. Sina Ahmadi. «Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches». International journal of advanced computer science and applications (IJACSA), 15 (3). 2024. DOI: 10.14569/IJACSA.2024.0150301.

3. M. Fuentes-García, J. Camacho and G. Maciá-Fernández, «Present and Future of Network Security Monitoring». IEEE Access, vol. 9. pp. 112744-112760. 2021. DOI: 10.1109/ACCESS.2021.3067106.

4. Hassan, A., Rauf, A., Shafqat, N. et al. «ZenGuard a machine learning based zero trust framework for context aware threat mitigation using SIEM SOAR and UEBA». Sci Rep 15, 35871. 2025. DOI: 10.1038/s41598-025-20998-4.