БАГАТОРІВНЕВА СИСТЕМА МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ ІБ НА БАЗІ КОНВЕРГЕНЦІЇ SIEM, SOAR ТА XDR

Доленко О.Д., В'юхін Д.О., Городецький С.Л.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання інтенсивності цілеспрямованих атак та дефіцит аналітиків безпеки обумовлюють необхідність переходу від розрізнених інструментів захисту до конвергентних платформ. Основним завданням сучасного SOC (Security Operations Center) є мінімізація часових показників виявлення та нейтралізації загроз [1]. Сучасна стратегія побудови SOC базується на синергії трьох ключових компонентів. Системи класу SIEM (Security Information and Event Management) забезпечують збір, збагачення контекстом, кореляцію великих обсягів логів із різноманітних джерел IT-інфраструктури. XDR (Extended Detection and Response) збирає телеметрію з кінцевих точок, мережевих вузлів та електронної пошти, дозволяючи ідентифікувати складні багатоетапні атаки шляхом побудови єдиного контекстуального ланцюга подій [2]. Платформи SOAR (Security Orchestration, Automation and Response) функціонують як центральний вузол для керування засобами захисту, впроваджуючи автоматизовані сценарії, що дозволяють виконувати процедури стримування та усунення наслідків без втручання людини [3].

Метою доповіді є огляд конвергентного способу взаємодії систем збору, глибокого аналізу та автоматизації у боротьбі з кібератаками для забезпечення якомога нижчих метрик реагування на інциденти.

Розглянутий підхід полягає в об'єднаному використанні цих систем, і в такий спосіб відбувається трансформування класичної реактивної моделі безпеки у проактивну. Конвергентне використання технологій об'єднує глибокий аналіз кінцевих точок і ланцюгів процесів через XDR з кореляційною потужністю SIEM, а SOAR виступає як центральна консоль, що надає автоматизовані сценарії реагування. Аналітики мають можливість виявити загрози ще до їх безпосереднього впливу завдяки здатності системи ідентифікувати складні вектори атак, які виглядають як окремі законні дії в різних частинах мережі, але в поєднанні складають ланцюг підготовки до експлуатації. Одним з головних недоліків традиційного багатоконсольного підходу до моніторингу є розрізненість систем, через що аналітики витрачають додатковий час на перемикання між різними консолями під час обробки сповіщень; також існує проблема «втоми від сповіщень», через що аналітик може загубити реальну загрозу серед десятків хибних або не шкідливих спрацювань [2]. Об'єднана система дозволяє оптимізувати ключові метрики ефективності: показник MTTD (Mean Time to Detect/час виявлення) мінімізується за рахунок предиктивного аналізу аномалій та інтеграції з XDR, а MTTR (Mean Time to Respond/час реагування) скорочується завдяки виключенню людського фактору на етапі первинного реагування.

Як приклад реальної системи розглянуто захист пристроїв IIoT (Industrial Internet of Things), що беруть учать у технологічних процесах виробництва.

Особливістю критичної інфраструктури є використання специфічних пристроїв (ПЛК, сенсорів) та промислових протоколів (MQTT, Modbus, OPC UA), які зазвичай не підтримуються стандартними IT-засобами моніторингу. Згідно з дослідженнями [4], ефективна інтеграція IIoT у систему SIEM базується на розгортанні спеціалізованих зондів та брокерів повідомлень. Це дозволяє трансформувати низькорівневі події промислової мережі у стандартизовані логи. Таким чином IIoT-сегмент стає частиною XDR, забезпечуючи моніторинг параметрів критичної інфраструктури, SIEM збирає та нормалізує дані, що дозволяє виявляти спроби зловмисного впливу на виробничі цикли на всіх етапах кібератак, а SOAR забезпечує автоматизоване реагування на інциденти.

Порівняльний аналіз операційних метрик (табл. 1) демонструє, що впровадження конвергентної платформи дозволяє скоротити MTTD на більш ніж 90%, а MTTR до лічених секунд [4].

Таблиця 1 – Порівняння метрик для класичних та об'єднаних систем

	Classic SOC	Unified SOC
MTTD	45 хв	2 хв
MTTR	30 хв – 5 год	<40 сек

Це досягається за рахунок усунення часових затримок на передачу даних між різними системами і узгоджень між відділами співробітників та автоматизації етапу прийняття рішень у типових сценаріях атак на інфраструктуру. Таким чином, впровадження об'єднаних платформ безпеки є доцільним і необхідним кроком для підвищення рівня захищеності сучасних інформаційно-комунікаційних систем, що підтверджується значним покращенням операційних показників та ефективності реагування на інциденти інформаційної безпеки.

Список літератури

1. Sievierinov, O., Ovcharenko, M., & Vlasov, A. (2021). Enterprise Security Operations Center. 2021: Fifth International Scientific and Technical Conference "Computer and information systems and technologies".

2. Pavan Paidy. Unified threat detection platform with AI, SIEM, and XDR. International journal of artificial intelligence, data science, and machine learning. 2025. Vol. 6, no. 1.

3. Мартиненко, Я., Сєвєрінов, О., Євгеньєв, А., & Скибенко, М. (2025). Дослідження SOAR-платформ та обґрунтування вибору SPLUNK PHANTOM. *Вісник Херсонського національного технічного університету*, *3*(4 (95)), 145-152.

4. Timi Heino. Real-Time Threat Detection using SIEM for Industrial IoT Protocols. Finland : University of Turku, 2025. 54 p.

5. Москвін, К., Сєвєрінов, О., Сидоренко, З., Балагура, Д., & Литвин, А. (2025). Дослідження впливу інтеграції засобів кіберзахисту на захищеність IT-інфраструктури організації. *Вісник ХНТУ*, *2*(2 (93)), 246-255.