РОЗРОБКА ЗАХИСНИХ МЕХАНІЗМІВ XDR ЧЕРЕЗ ПРАКТИЧНІ СЦЕНАРІЇ ПЕНТЕСТІВ ТА МОДЕЛЮВАННЯ АТАК

Топіха Т.Б., Смірнов А.О., Городецький С.Л.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах стрімкої цифровізації бізнес-процесів, державного управління та критичних інфраструктур питання забезпечення кібербезпеки набуває стратегічного значення. Кожного року зростає кількість інцидентів, спричинених не лише типовими вірусами чи шкідливими вкладеннями, а й складними багатоступеневими атаками, які використовують соціотехнічні методи, викрадення облікових даних, горизонтальне переміщення в мережі та ексфільтрацію конфіденційної інформації. За даними звітів IBM X-Force Threat Intelligence та Verizon DBIR (2024 р.) [1, 2], понад половину виявлених інцидентів відносяться саме до багатокрокових атак, які важко виявити традиційними засобами [3]. У таких умовах центри операцій безпеки (SOC) змушені працювати у режимі постійного навантаження, обробляючи величезну кількість подій і сповіщень. Це, своєю чергою, збільшує ймовірність пропуску критичних загроз та уповільнює реагування на інциденти.

Традиційні засоби захисту системи IDS/IPS, SIEM та EDR безумовно залишаються важливими елементами сучасної кібербезпеки. Вони дозволяють здійснювати моніторинг мережевого трафіку, централізовано збирати логи, аналізувати події на кінцевих точках та формувати базові правила реагування. Проте їхня фрагментарність, різнорідність форматів даних та відсутність контекстної взаємодії між різними джерелами суттєво обмежують можливості комплексного аналізу. Як наслідок, для аналітиків SOC залишається великий обсяг ручної роботи, що збільшує час ухвалення рішень і ризики людського фактору [3]. Вирішенням цих проблем є впровадження інтегрованих систем XDR (Extended Detection and Response), які поєднують телеметрію з різних кінцевих точок, мережі, хмарних сервісів, пошти, ідентичностей у єдину аналітичну екосистему [4]. XDR не лише централізує збір даних, але й забезпечує автоматичну кореляцію подій, створюючи повний контекст інциденту від початкового проникнення до фінальної дії зловмисника. Таким чином, система дозволяє значно скоротити час виявлення, підвищити точність детекцій та автоматизувати ключові етапи реагування.

Метою даного дослідження стало створення лабораторної XDR-платформи, яка дозволяє перевірити ефективність механізмів виявлення та реагування шляхом практичного моделювання атак і пентест-емуляції. У роботі зроблено акцент на практичне підтвердження теоретичних положень, тобто не лише описано архітектуру, а й реалізовано її в умовах контрольованого середовища з подальшим тестуванням.

У межах дослідження було спроєктовано й розгорнуто лабораторну інфраструктуру в середовищі Microsoft Azure, яка максимально наближена до реальної корпоративної екосистеми. До її складу входить публічний веб-сервер (Nginx), внутрішній файловий сервер, поштовий сервіс (Exchange Online),

кілька користувацьких станцій із агентами Defender for Endpoint, а також аналітична платформа Microsoft Sentinel, що виконує функції SIEM/SOAR [5]. Усі джерела телеметрії передавали дані до Log Analytics Workspace, де вони нормалізувались, аналізувались і корелювались за єдиною схемою. Основою методології став фреймворк MITRE ATT&CK, який забезпечив систематизацію тактик і технік супротивників (TTP) та слугував базою для створення сценаріїв моделювання атак [6]. У рамках експериментів реалізовано сценарії початкового доступу через фішинг (T1566), викрадення облікових даних (T1003), горизонтального переміщення (T1021), ескалації привілеїв (T1068) та ексфільтрації даних (T1041).

Для безпечної емуляції поведінки зловмисників використано інструменти які дозволили відтворити реалістичні техніки без ризику для продуктивних систем. Усі події фіксувалися XDR-агентами, передавалися до Sentinel, де автоматично створювалися інциденти з побудовою ланцюгів подій і подальшою активацією сценаріїв реагування (Logic Apps). Реалізовані плейбуки передбачали ізоляцію хостів, блокування користувачів, надсилання повідомлень аналітикам SOC і автоматичне оновлення списків контролю доступу. Результати практичного етапу дослідження підтвердили, що впроваджене XDR-рішення забезпечує більш глибоку видимість подій, швидшу ідентифікацію інцидентів і зниження кількості хибних сповіщень. Автоматизація процесів реагування дала змогу оптимізувати навантаження на аналітиків SOC, підвищити стабільність роботи команди та скоротити час на обробку подій. Також було продемонстровано можливість інтеграції XDR із різними джерелами даних, що створює передумови для масштабування рішення в умовах реального підприємства.

Отримані результати свідчать, що використання підходу XDR у поєднанні з фреймворком MITRE ATT&CK і практичним моделюванням атак є ефективним шляхом підвищення рівня кіберстійкості організацій. Такий підхід не лише покращує якість виявлення загроз, а й забезпечує комплексне бачення безпекових подій, скорочуючи час реагування та зменшуючи залежність від людського чинника. Проведене дослідження підтвердило доцільність упровадження інтегрованих систем XDR як основи сучасної архітектури кіберзахисту.

Список літератури

1. IBM Security. X-Force Threat Intelligence Index 2024. — IBM Corporation, 2024. — 64 p. URL: https://www.ibm.com/reports/threat-intelligence.
2. Verizon Communications Inc. Data Breach Investigations Report 2024. — Verizon, 2024. — 120 p. URL: https://www.verizon.com/business/resources/reports/dbir/.
3. Ушатов, В., Сєвєрінов, О.В. (2019). Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки.
4. Gartner Research. Market Guide for Extended Detection and Response (XDR). — Gartner, 2023. — 22 p.
5. Microsoft Corporation. Microsoft Defender XDR Documentation. — Microsoft Learn, 2024. URL: https://learn.microsoft.com/en-us/defender-xdr/.
6. MITRE Corporation. MITRE ATT&CK Framework. — 2024. URL: https://attack.mitre.org.