ПІДХІД ДО ІНТЕГРАЦІЇ РІШЕНЬ SIEM, XDR ТА DLP У МЕХАНІЗМИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Неборак М.О., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

З початку повномасштабної війни об'єкти критичної інфраструктури (ОКІ) стали однією з основних цілей кібератак. Прикладом є атака з використанням Industroyer2 на енергетичну компанію у квітні 2022 р. Додаткову складність створює те, що в мережі ОКІ поряд із корпоративними системами працюють технологічні системи (SCADA), для яких критичною є безперервність роботи [1].

На практиці для захисту використовують SIEM, XDR та DLP. SIEM-система збирає журнали подій з різних джерел і корелює їх [2, 3]. XDR розвиває підхід EDR [4]: аналізує телеметрію кінцевих точок і мережі та може автоматично ізолювати заражений вузол. DLP контролює передачу конфіденційної інформації за межі організації [6]. Зазвичай SIEM є центральною точкою збору подій від інших засобів захисту [3, 5]. Проте, на нашу думку, саме по собі пересилання подій у SIEM ще не означає їх спільного аналізу.

Наприклад, DLP фіксує відправлення файлу, але не знає, що комп'ютер відправника вже скомпрометований, і не може відрізнити помилку працівника від викрадення даних. Як наслідок, аналітик отримує велику кількість розрізнених сповіщень і змушений зіставляти їх вручну.

Для технологічного сегмента ситуація ще складніша: встановити агенти захисту на такі вузли можливо не завжди, а журнали подій без окремих правил кореляції рідко стають підставою для сповіщень.

Єдина платформа одного виробника спрощує інтеграцію, але обмежує вибір засобів захисту, а сценарії систем автоматизації реагування (SOAR) для ОКІ потрібно доповнювати правилами з урахуванням критичності активу.

Метою доповіді є обґрунтування підходу до інтеграції SIEM, XDR та DLP, за якого сповіщення різних систем об'єднуються в один інцидент з урахуванням критичності активів. На поточному етапі підхід має концептуальний характер.

Підхід передбачає три кроки.

Спочатку події всіх систем приводяться до єдиного формату засобами самої SIEM-платформи та доповнюються даними з реєстру активів (роль і критичність вузла). Далі події, що стосуються одного активу або облікового запису в певному часовому вікні, об'єднуються в один інцидент, а правила кореляції прив'язуються до технік MITRE ATT&CK. Наприклад, підозрілий процес на комп'ютері (XDR), копіювання службових документів (DLP) і з'єднання з невідомою зовнішньою адресою (SIEM) розглядаються як один інцидент, а не три окремі. Нарешті, для кожної категорії активів визначається, які дії реагування можна виконувати автоматично, а які лише після підтвердження аналітиком.

Для пріоритизації інцидентів пропонується показник

$$R = K_a \cdot (w_1 \cdot S_{SIEM} + w_2 \cdot S_{XDR} + w_3 \cdot S_{DLP}),$$

де K_a – коефіцієнт критичності активу; S_{SIEM}, S_{XDR}, S_{DLP} – оцінки відповідних систем від 0 (подій немає за умови справної роботи джерела) до 1 (критичний рівень); w_1, w_2, w_3 – вагові коефіцієнти, сума яких дорівнює 1.

Коефіцієнт K_a пропонується задавати за трьома рівнями (початкові значення, обрані автором): 1,0 – вузли, що забезпечують основну функцію об'єкта (зокрема сервери SCADA та робочі місця операторів); 0,6 – інші критичні сервіси; 0,3 – звичайні робочі станції. Вагові коефіцієнти на початковому етапі можна прийняти рівними. Якщо на робочому місці оператора (K_a = 1,0) кожна з трьох систем зафіксувала подію середнього рівня (S = 0,5), то R = 0,5. Такий самий набір подій на звичайній робочій станції дає R = 0,15. Тобто однакові сповіщення отримують різний пріоритет залежно від ролі вузла. Водночас втрату даних від джерела слід фіксувати окремо, а не прирівнювати до S = 0, інакше значення R буде заниженим.

Для перевірки підходу планується порівняти окрему та інтегровану роботу засобів захисту за такими показниками: середній час виявлення (MTTD) і реагування (MTTR), частка хибнопозитивних сповіщень і кількість інцидентів, які доводиться аналізувати вручну. Перевірку передбачається провести в тестовому середовищі на типових сценаріях атак. Подальші дослідження будуть спрямовані на уточнення шкал оцінювання, вибір вагових коефіцієнтів та експериментальну перевірку підходу.

Список літератури

1. Stouffer K., Pease M., Tang C., Zimmerman T., Pillitteri V., Lightman S., Hahn A., Saravia S., Sherule A., Thompson M. Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3. Gaithersburg : NIST, 2023. 316 p. DOI: https://doi.org/10.6028/NIST.SP.800-82r3

2. Sheeraz M., Durad M. H., Paracha M. A., Mohsin S. M., Kazmi S. N., Maple C. Revolutionizing SIEM security: an innovative correlation engine design for multi-layered attack detection. Sensors. 2024. Vol. 24, No. 15. Art. 4901. DOI: https://doi.org/10.3390/s24154901

3. González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors. 2021. Vol. 21, No. 14. Art. 4759. DOI: https://doi.org/10.3390/s21144759

4.Shulika K., Balagura D., Smirnov A., Nepokrytov D., Lytvyn A. A method of using modern endpoint detection and response (EDR) systems to protect against complex attacks. Innovative Technologies and Scientific Solutions for Industries. 2024. No. 2(28). P. 182–195. DOI: https://doi.org/10.30837/2522-9818.2024.2.182

5. Смірнова Т., Константинова Л., Конопліцька-Слободенюк О., Козлов Я., Кравчук О., Козірова Н., Смірнов О. Дослідження сучасного стану SIEM-систем. Кібербезпека: освіта, наука, техніка. 2024. Т. 1, № 25. С. 6–18. DOI: https://doi.org/10.28925/2663-4023.2024.25.618

6. Alneyadi S., Sithirasenan E., Muthukkumarasamy V. A survey on data leakage prevention systems. Journal of Network and Computer Applications. 2016. Vol. 62. P. 137–152. DOI: https://doi.org/10.1016/j.jnca.2016.01.008