УДК 004.056:005.7 DOI: https://doi.org/10.30837/IYF.IRTTPI.2024.437

РОЛЬ СИСТЕМ SIEM ТА UEBA В ЗАДАЧІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Щербак В.О.
Науковий керівник – к.т.н., доц. Іванова О.О.
Харківський національний університет радіоелектроніки,
каф. КРіСТЗІ, м. Харків, Україна
e-mail: valeriia.shcherbak@nure.ua

The advantages of using a solution that combines the functions of SIEM and UEBA when building an effective information security system are considered.

Побудова ефективної системи управління безпекою великої корпоративної мережі з великою кількістю робочих станцій, серверів, мережевого та комутаційного обладнання, телефонії, технологічного та іншого обладнання є пріоритетним завданням для будь-якої сучасної компанії або організації. Стрімкий розвиток технологій машинного навчання, заснованих на математичних моделях, збільшення потужності обчислювальних мереж, обчислювальних потужностей серверного обладнання, необхідність збільшення засобів автоматизації для досягнення високої швидкості реакції на інциденти інформаційної безпеки задають вектор розвитку засобів захисту у бік інтеграції з технологією машинного навчання. Використання SIEM (Security Information and Event Management) спільно з UEBA (User and Entity Behavior Analytics) є прикладом такого рішення.

SIEM та UEBA – це інструменти забезпечення безпеки в інформаційних системах, які на ринку вітчизняного програмного забезпечення представлені як окремі, автономні рішення. SIEM є інструментом для збирання, аналізу та нормалізації різних даних про безпеку в інформаційній системі, таких як журнали подій, «логи» мережевих пристроїв тощо. Система SIEM використовується для виявлення та аналізу потенційних загроз за рахунок кореляції (об'єднання подій у ланцюжки) подій безпеки в системі та дозволяє швидко реагувати на них. Також ця система може використовуватися для забезпечення відповідності нормам та вимогам безпеки [1]. UEBA використовує аналіз даних, зібраних з різних джерел, таких як журнали подій, «логи» мережевих пристроїв, інформація про користувачів тощо, щоб виявити потенційні загрози безпеці, пов'язані з незвичайною поведінкою користувачів або інших сутностей у системі. Ця система використовує технології машинного навчання для формування моделі поведінки користувачів, завдяки чому може використовуватися для виявлення внутрішніх загроз безпеці, таких як виток даних або крадіжка облікових даних [2].

SIEM збирає та класифікує дані, що надходять з усіх пристроїв у мережі, та створює події, використовуючи правила кореляції, засновані на алгоритмах, в абсолютній більшості яких не враховується специфіка роботи обладнання, а лише заздалегідь описана поведінка шкідливого програмного забезпечення, інструментів для злому та іншої поведінки порушника SIEM. Ці події та дані збагачуються контекстом модуля UEBA, який має вирішальне значення для виявлення відхилення поведінки користувача від сформованої моделі поведінки користувачів та об'єктів мережі [3].

Синергія використання SIEM та UEBA дозволяє вирішувати наступні задачі:

1) автоматичне виявлення внутрішніх загроз;
2) пріоритизація інцидентів;
3) запобігання витоку даних;
4) цільове навчання користувачів;
5) зниження кількості хибних спрацьовувань;
6) аудит ефективності віддалених працівників;
7) скорочення ручної праці аналітиків;
8) автоматичне виявлення внутрішніх загроз.

Такі атаки, як фішинг, компрометація електронної пошти, крадіжка облікових даних та захоплення облікових записів, роблять інсайдерські загрози однією з найнебезпечніших дій у мережі організації. Існує три типи інсайдерських загроз.

Недбайливий інсайдер. Співробітник або користувач мережі з привілейованим доступом, який не дотримується належних IT-процедур, може представляти загрозу. Не використовуючи належних заходів безпеки, цей користувач стає слабким місцем для проникнення порушника за периметр організації.

Зловмисний інсайдер. Це співробітник із привілейованим доступом до системи, який він має намір використовувати для зловмисної діяльності.

Скомпрометований інсайдер. З'являється у мережі як авторизований користувач, який виконує типові мережеві завдання. Однак це зловмисник, який одержав облікові дані інсайдера.

Традиційні засоби безпеки розглядають дії авторизованих користувачів як звичайну поведінку. UEBA додає контекст користувача до даних про події, завдяки чому стає зрозуміло, коли користувачі поводяться незвичайним підозрілим чином. Уніфіковане використання SIEM та UEBA зіставляє підозрілі дії в ланцюжок загроз, який можна легко ідентифікувати як шаблон атаки. Це автоматичне виявлення дозволяє системі відправляти оповіщення та автоматизувати своєчасний запуск дій у відповідь для блокування загрози до того, як вона перетвориться на успішну атаку.

Наведемо приклад. Зловмисник, який зламав систему за допомогою атаки фішингу, може спочатку відображатися як авторизований користу-

вач. Коли цей авторизований користувач намагається отримати привілейований доступ, UEBA розпізнає цю дію як підозрілу. Оповіщення видаються при аномальній кількості невдалих входів у систему або під час входу користувача з незвичайного пристрою чи місця.

Пріоритизація інцидентів.

Зазвичай SIEM система обробляє інформацію від досить великого набору різних інструментів безпеки і критично важливих систем. Якщо кожен із цих фрагментів даних має однаковий рівень важливості, то значуща для прийняття рішень інформація може залишитися непоміченою. За відсутності пріоритету інцидентів система безпеки може генерувати значну кількість попереджень, які вимагають уваги співробітників служби безпеки. Велика проблема, з якою стикається багато компаній, полягає в тому, що аналітики отримують занадто багато попереджень. Величезна кількість нерелевантних попереджень призводить до втоми, притуплює увагу, що може призвести до пропуску аналітиком реальної загрози.

Навіть якщо повідомлення доповнюються контекстними даними, не всі підозрілі дії однакові. Ефективний UEBA постійно ранжує підозрілу діяльність за рівнем ризику. Доповнення контексту конкретної організації, що описує критичність активів та рівні доступу до конкретних функцій та користувачів, дозволяє більш ефективно виявляти серйозні відхилення від нормальної поведінки.

Запобігання витоку даних.

Авторизовані користувачі повинні обробляти, зберігати та передавати різні корпоративні дані практично щодня. Передача великих обсягів даних може бути індикатором витоку даних. Багато шкідливих дій, пов'язаних з втратою даних, можуть бути не настільки помітними. Рішення UEBA використовують відомі базові показники користувачів та сутностей, щоб відстежувати та проводити класифікацію подій, що становлять аномальну поведінку.

Цільове навчання користувачів.

Аналіз поведінки користувачів є невід'ємною частиною ефективної безпеки. Часто співробітники організації не мають належного уявлення про культуру інформаційної безпеки – не розуміють, як необхідно захищати конфіденційні дані, чи не усвідомлюють, що ті чи інші їхні дії наражають компанію на ризик і можуть призвести до несприятливих наслідків, існує проблема компетентності у правових та технічних питаннях використання інформаційно-комунікаційних технологій [4].

UEBA відстежує дії користувачів, виявляє поведінку людини, пов'язану з фішингом, передачею даних, контролем доступу, використання неправильних паролів та може коригувати його за допомогою додаткового навчання. Коли роботодавці знають, які користувачі потребують додаткового навчання, вони можуть забезпечити цільове навчання для усунення конкретних моделей поведінки та запобігання майбутнім діям, які можуть

призвести до успішних атак.

Аудит поведінки дистанційних працівників.

UEBA може підвищити безпеку бізнесу, який використовує віддалені та гібридні схеми роботи співробітників, встановивши базову поведінку для віддалених співробітників та пристроїв. Інструменти геолокації можуть надавати оповіщення про входи до системи, що відбуваються в нетиповому місці, про потенційні ризики, такі як скомпрометовані облікові дані. Віддалені пристрої більш схильні до атак. UEBA може забезпечити критично важливий додатковий рівень захисту для запуску попереджень про атаки, витоки даних та зміни дозволів. Побудова моделі користувача також дозволяє аналізувати, потім співробітники витрачають свій робочий час, що дозволяє менеджерам оцінити ситуацію для своєчасної коригування і мотивації персоналу [5].

Висновки

Сучасні зловмисники використовують у своїх атаках значну кількість різноманітних підходів, технологій та інструментів, які можуть завдати серйозної шкоди мережам великих організацій. Це потребує більше ресурсів для аналізу поведінки порушників та формування правил, здатних детектувати їхню поведінку. Синергія спільного застосування SIEM з UEBA дозволяє помітно підвищити швидкість реакції та якість виявлення та розслідування інцидентів інформаційної безпеки, що, у свою чергу, значно підвищує рівень інформаційної безпеки організації.

Список використаних джерел:

1. Cinque M., Cotroneo D., Pecchia A., Challenges and Directions in Security Information and Event Management (SIEM), in: 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2018, pp. 95–99.

2. Muhammad Zunair Ahmed Khan, Muhammad Mubashir Khan & Junaid Arshad. Anomaly Detection and Enterprise Security using User and Entity Behavior Analytics (UEBA). Conference: 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS)

3. K. Singh. Application of SIEM/UEBA/SOAR/SOC (Cyber SUSS) Concepts on MSCS 6560 Computer Lab. p. 82

4. Alhogail A. Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study // International Journal of Security And Its Applications, 9 (7), 163–178. DOI: 10.14257/ijsia.2015.9.7.15.

5. The Best Employee Monitoring Software for 2024. URL: https://www.businessnewsdaily.com/11143-best-employee-monitoring-software.html (дата звернення: 20.12.2023).

6. Грицаненко Я. Ю. UBA-аналіз як засіб підвищення інформаційної безпеки автоматизованих систем / Я. Ю. Грицаненко // Радіоелектроніка та молодь у XXI столітті : тези доповідей 27-го Міжнародного молодіжного форуму, 10–12 травня 2023 р. – Харків : ХНУРЕ, 2023. – Т. 3. – С. 233–234.