УДК 004

В.Ковальчук, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПОВЕДІНКОВОГО АНАЛІЗУ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ КОНЦЕПЦІЇ UEBA

У статті розроблено програмне забезпечення, яке призначено для системи поведінкового аналізу користувачів за допомогою концепції UEBA. Метою розробки є дослідження та принципи побудови системи поведінкового аналізу користувачів за допомогою концепції UEBA. Об'єктом дослідження є процес поведінкового аналізу користувачів за допомогою концепції UEBA. Предметом дослідження є методи поведінкового аналізу користувачів за допомогою концепції UEBA. Методи дослідження базуються на методах машинного навчання, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи поведінкового аналізу користувачів за допомогою концепції UEBA. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

поведінковий аналіз користувачів, UEBA

Постановка проблеми. UEBA, що розшифровується як User and Entity Behavior Analytics (аналіз поведінки користувачів та сутностей), – це технологія кібербезпеки, яка аналізує поведінку користувачів та сутностей для виявлення аномальної та потенційно шкідливої діяльності. Вона виходить за рамки традиційних заходів безпеки, зосереджуючись на моделях поведінки, а не лише на відомих загрозах, використовуючи машинне навчання та розширену аналітику для виявлення відхилень від звичайної активності. Це допомагає організаціям виявляти внутрішні загрози, скомпрометовані облікові дані та інші складні атаки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи поведінкового аналізу користувачів за допомогою концепції UEBA.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи поведінкового аналізу користувачів за допомогою концепції UEBA.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем поведінкового аналізу користувачів за допомогою концепції UEBA.

– Дослідження системи поведінкового аналізу користувачів за допомогою концепції UEBA.

– Програмна реалізація системи поведінкового аналізу користувачів за допомогою концепції UEBA.

Об'єктом дослідження є процес поведінкового аналізу користувачів за допомогою концепції UEBA.

Предметом дослідження є методи поведінкового аналізу користувачів за допомогою концепції UEBA.

Методи дослідження базуються на методах машинного навчання, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Ключові характеристики інструментів UEBA

Хоча UEBA як категорія безпеки зараз часто вписується в рамки більших платформ, кілька ключових можливостей є однаковими для всієї галузі. Основні функції UEBA включають моніторинг інфраструктури, аналітику, сповіщення та керування користувачами.

Моніторинг

В інфраструктурі безпеки мережі, пристрої та програми повинні контролюватися. Інструменти UEBA постійно спостерігають за IT-системами та повідомляють адміністраторів, коли мережевий трафік та поведінка пристроїв або програм не відповідають попередньо налаштованим стандартам.

Аналітика

У рішеннях UEBA поведінкова аналітика базується на технології машинного навчання. ML ідентифікує поведінку користувачів, щоб визначити, чи відповідає вона заздалегідь визначеним критеріям типових дій. Якщо інструмент UEBA вирішує, що нестабільна поведінка користувача є небезпечною, він виділяє цю закономірність на панелі інструментів, щоб адміністратори безпеки могли її переглянути.

Сповіщення та пріоритетність

Інструменти UEBA запускають сповіщення, коли виникає достатньо значна аномалія. Оскільки ці інструменти вивчають типові моделі поведінки користувачів і програм протягом певного часу, вони помічають, коли відбувається щось неочікуване. Інструменти UEBA часто надають пріоритет сповіщенням – ранжуючи рівень ризику, щоб IT-персонал та співробітники служби безпеки могли вирішити, з чим боротися в першу чергу.

Керування користувачами та об'єктами

Рішення UEBA контролюють дозволи користувачів і визначають, чи суперечить поведінка певного користувача призначеним йому правам. Це допомагає зменшити використання привілейованого доступу, а також може виявити зловмисну інсайдерську діяльність. Рішення UEBA також часто контролюють об'єкти або активи, такі як ноутбуки чи сервери, щоб визначити, чи є їхня поведінка аномальною та чи потребує карантину або вимкнення.

Розширена ідентифікація загроз

Коли інструменти UEBA моніторять системи та виявляють аномалії, вони часто визначають, який саме тип проблеми виникає. До них належать такі загрози, як горизонтальне переміщення та витік даних, а рішення UEBA також можуть повідомити вам, чи є загроза внутрішньою чи зовнішньою по відношенню до вашої організації. Ця інформація корисна для боротьби зі зловмисниками, особливо якщо це ваші власні співробітники.

Основна функція UEBA включає:

– Поведінковий аналіз: Системи UEBA аналізують поведінку користувачів та сутностей, включаючи такі дії, як спроби входу, доступ до файлів, мережевий трафік та використання програм.

– Виявлення аномалій: встановлює базовий рівень нормальної поведінки для кожного користувача та сутності, а потім позначає відхилення від цього базового рівня як потенційні загрози.

– Машинне навчання: UEBA використовує алгоритми машинного навчання для виявлення тонких закономірностей та аномалій, які можуть бути пропущені традиційними методами безпеки.

Ключові переваги включають:

– Покращене виявлення загроз: UEBA може виявляти ширший спектр загроз, включаючи внутрішні загрози, скомпрометовані облікові записи та розширені постійні загрози (APT).

– Покращений рівень безпеки: Завдяки проактивному виявленню підозрілої активності, UEBA допомагає організаціям покращити загальний рівень безпеки та зменшити ризик витоків даних.

– Зменшення кількості хибних спрацьовувань: здатність UEBA аналізувати контекст і поведінку допомагає мінімізувати кількість хибних спрацьовувань, дозволяючи командам безпеки зосередитися на справжніх загрозах.

– Швидше реагування на інциденти: Завдяки швидкому виявленню та сповіщенню про аномальну поведінку, UEBA забезпечує швидше реагування на інциденти та їх локалізацію.

– Повна видимість: UEBA надає повне уявлення про активність користувачів та організацій, допомагаючи організаціям зрозуміти, як використовуються їхні системи, та виявити потенційні слабкі місця в безпеці.

Інструменти UEBA використовують інноваційні алгоритми, засновані на традиційному машинному навчанні та глибокому навчанні, для виявлення аномальної та ризикованої поведінки користувачів, машин та інших об'єктів у корпоративній мережі, часто у поєднанні з рішенням для управління інцидентами та подіями безпеки (SIEM).

Зростаюча потреба в UEBA: внутрішні ризики перевищують зовнішні загрози

Згідно з нашим нещодавнім звітом «Від людини до гібрида: як штучний інтелект та розрив в аналітиці підживлюють внутрішні ризики» , внутрішні ризики вже перевершили зовнішні загрози як головну проблему для команд безпеки. У нашому опитуванні 64% фахівців з кібербезпеки визначили зловмисних або скомпрометованих інсайдерів як більшу небезпеку, ніж зовнішніх нападників, порівняно з 36%, які вказали на зовнішніх суб'єктів.

З цих 64% 42% вважали зловмисних інсайдерів основною проблемою, а 22% – скомпрометованих інсайдерів. Понад половина (53%) повідомила, що кількість інсайдерських інцидентів зросла за останній рік, а 54% очікують, що їхня кількість зростатиме ще більше протягом наступних 12 місяців.

Можливості виявлення залишаються недостатньо розвиненими. Лише 44% організацій використовують аналітику поведінки користувачів та об'єктів (UEBA), яка є критично важливою для виявлення аномальної активності. Хоча 88% кажуть, що мають програму боротьби з внутрішніми загрозами, багато з них є неформальними, недостатньо фінансованими або мають недостатню прозорість у системах. Узгодженість керівництва також є прогалиною: 74% фахівців з безпеки вважають, що керівники недооцінюють внутрішні ризики.

Генеративний штучний інтелект (ШІ) посилює проблему. 76% організацій стикалися з несанкціонованим використанням інструментів GenAI співробітниками. Фішинг та соціальна інженерія за допомогою ШІ (27%), а також несанкціоноване використання GenAI (22%) входять до числа основних векторів внутрішніх загроз, поряд із зловживанням привілеями (18%).

Керівники служб безпеки визнають необхідність кращого аналізу поведінки, але стикаються з технічними та організаційними перешкодами. Опір конфіденційності (20%), відсутність прозорості (16%) та фрагментовані інструменти (10%) створюють сліпі зони у зусиллях з виявлення.

Як працює UEBA

Аналіз поведінки користувачів та сутностей (UEBA) – це категорія рішень або можливостей кібербезпеки, які аналізують поведінку користувачів та сутностей і застосовують розширену аналітику та моделювання поведінки для визначення аномальної поведінки. UEBA використовується для виявлення розширених загроз безпеці, таких як зловмисні інсайдери та компрометація привілейованих облікових записів, які традиційні інструменти безпеки на основі правил не можуть побачити. Рішення UEBA отримують операційні дані з багатьох джерел та визначають, яка нормальна поведінка будь-якого користувача або нелюдської сутності. Суб'єкти можуть включати IT-активи, такі як хости, програми, мережевий трафік, облікові записи служб та сховища даних. З часом рішення створює стандартні профілі поведінки для користувачів та сутностей у різних групах рівних, щоб створити базовий рівень для того, що є нормальним в організації. Коли виявляється

аномальна активність, їй присвоюється оцінка ризику. Оцінка зростає зі збільшенням кількості аномальної поведінки, доки вона не перетне визначений поріг, що спрацьовує для аналітиків безпеки. Деякі рішення можуть автоматизувати дії реагування.

Ось більш детальний огляд основної функції UEBA:

– Машинне навчання: UEBA застосовує методи машинного навчання з вчителем та без вчителя для виявлення ледь помітних аномалій, які статичні правила не можуть вловлювати. Алгоритми можуть адаптуватися до зміни поведінки користувача, зменшуючи потребу в постійних ручних оновленнях. Це дозволяє системі виявляти приховані моделі атак, такі як повільне витікання даних або зловживання привілеями, які розгортаються поступово та в іншому випадку могли б уникнути виявлення.

– Поведінковий аналіз: UEBA збирає та зіставляє дані з кількох джерел, таких як журнали автентифікації, файлові системи, електронна пошта та хмарні додатки, для створення комплексного уявлення про активність. Він відстежує не лише окремі події, а й послідовності дій з плином часу, що дозволяє виявляти незвичайні робочі процеси, спроби доступу або моделі використання, які можуть свідчити про неправильне використання або компрометацію.

– Виявлення аномалій: Після встановлення профілів нормальної поведінки UEBA постійно порівнює нову активність з цими базовими показниками. Відхилення, такі як спроби входу з незвичайних місць, надмірне завантаження файлів або неочікуваний доступ до конфіденційних ресурсів, позначаються. Система призначає контекст цим аномаліям, допомагаючи аналітикам розрізняти нешкідливі відхилення та справжні загрози.

Цілісний аналіз з використанням кількох джерел даних

Справжня сила рішення UEBA полягає в його здатності долати організаційні кордони, IT-системи та джерела даних й аналізувати всі дані, доступні для конкретного користувача чи організації.

Рішення UEBA повинно аналізувати якомога більше джерел даних, деякі приклади джерел даних включають:

– Системи автентифікації, такі як Active Directory.

– Системи доступу, такі як VPN та проксі-сервери.

– Бази даних керування конфігурацією.

– Дані про людські ресурси – нові співробітники, співробітники, що звільнилися, та будь-які дані, що надають додатковий контекст про користувачів.

– Брандмауер, системи виявлення та запобігання вторгненням (IDPS).

– Антивірусні та антивірусні системи.

– Системи виявлення та реагування на кінцеві точки.

– Аналіз мережевого трафіку.

– Стрічки інформації про загрози.

Наприклад, рішення UEBA повинно мати можливість ідентифікувати незвичний вхід через Active Directory, зіставляти його з критичністю пристрою, на який здійснюється вхід, конфіденційністю файлів, до яких здійснювався доступ, та нещодавньою незвичайною мережевою або шкідливою активністю, яка могла призвести до компрометації.

Поведінкове базове дослідження та оцінки ризику

Рішення UEBA вивчає нормальну поведінку, щоб виявити аномальну. Воно аналізує широкий набір даних, щоб визначити базовий або поведінковий профіль користувача.

Наприклад, система відстежує користувача та бачить, як він використовує VPN, о котрій годині приходить на роботу та в які системи входить, який принтер використовує, як часто та якого розміру файли надсилає електронною поштою або завантажує на USB-накопичувач, а також багато інших даних, що визначають «нормальну поведінку» користувача. Те саме стосується серверів, баз даних або будь-якої значної IT-системи.

Коли відбувається відхилення від базового рівня, система додає до оцінки ризику цього користувача або машини. Чим незвичайніша поведінка, тим вищий бал ризику. Зі збільшенням кількості підозрілих випадків накопичення бал ризику збільшується, доки не досягне певного порогу, що призводить до передачі інформації аналітику для розслідування.

Такий аналітичний підхід має кілька переваг:

– Агрегація – оцінка ризику складається з численних подій, тому аналітикам не потрібно вручну переглядати велику кількість окремих сповіщень та подумки об'єднувати їх для виявлення загрози.

– Зменшення кількості хибнопозитивних результатів – одна незначна аномальна подія сама по собі не призведе до спрацювання сповіщення системи безпеки. Для створення сповіщення системі потрібні кілька ознак аномальної поведінки, що зменшує кількість хибнопозитивних результатів та заощаджує час аналітиків.

Більше контексту – традиційні правила кореляції, визначені адміністраторами безпеки, могли бути правильними для однієї групи користувачів або систем, але не для інших. Наприклад, якщо відділ починає наймати працівників, що працюють позмінно, або працівників, що працюють за кордоном, вони почнуть входити в систему в незвичний час, що постійно призводитиме до спрацьовування сповіщень на основі правил. UEBA розумніша, оскільки встановлює контекстно-залежний базовий рівень для кожної групи користувачів. Вхід працівника, що працює за кордоном, о 3:00 ранку за місцевим часом не вважатиметься аномальною подією.

Аналіз часової шкали та зшивання сесій

Під час аналізу інцидентів безпеки часова шкала є критично важливим поняттям, яке може пов'язати, здавалося б, не пов'язані між собою дії. Сучасні атаки – це процеси, а не ізольовані події.

Передові рішення UEBA можуть «зшивати» дані з різних систем та потоків подій, щоб побудувати повну часову шкалу інциденту безпеки.

Наприклад, розглянемо користувача, який увійшов у систему, виконав підозрілу активність, а потім зник із журналів. Чи була та сама IP-адреса використана для підключення до інших організаційних систем невдовзі після цього? Якщо так, це може бути частиною того самого інциденту, коли той самий користувач продовжував спроби проникнення в систему. Додатковим прикладом може бути вхід зловмисника в систему на одному комп'ютері кілька разів, використовуючи різні облікові дані. Це також вимагає «зшивання» даних про різні спроби входу та позначення їх як одного інциденту.

Після того, як рішення UEBA об'єднає всі відповідні дані, воно може призначити оцінки ризику будь-якій діяльності вздовж часової шкали події. Засвоюється нормальна поведінка для всіх користувачів і машин. Оцінка ризику додається для високоризикової та аномальної поведінки.

Внутрішні загрози

Існує три типи внутрішніх загроз:

1. Недбалий інсайдер – недбалий інсайдер – це працівник або підрядник із привілейованим доступом до IT-систем, який ненавмисно наражає свою організацію на небезпеку, не дотримуючись належних IT-процедур. Наприклад, той, хто залишає свій комп'ютер, не вийшовши з системи, або адміністратор, який не змінив пароль за замовчуванням або не встановив патч безпеки. Визначення нормальної та аномальної активності користувача є ключовим для виявлення користувача, який був скомпрометований через недбалість.

2. Зловмисний інсайдер – Зловмисний інсайдер – це співробітник або підрядник із привілейованим доступом до IT-систем, який має намір здійснити кібератаку на організацію. Важко виміряти зловмисний намір або виявити його за допомогою лог-файлів або регулярних подій безпеки. Рішення UEBA допомагають, встановлюючи базову лінію типової поведінки користувача та виявляючи аномальну активність.

3. Скомпрометований інсайдер – Зловмисники часто проникають в організацію та компрометують обліковий запис привілейованого користувача або довірений хост у мережі, а потім продовжують атаку звідти. Рішення UEBA можуть допомогти швидко виявити та проаналізувати шкідливу діяльність, яку зловмисник здійснює через скомпрометований обліковий запис.

Традиційним засобам безпеки важко виявити скомпрометованого інсайдера, якщо схема атаки або ланцюжок знищення наразі невідомі (наприклад, під час атаки нульового дня), або якщо атака поширюється латерально через організацію, змінюючи облікові дані, IP-адреси або машини. Однак технологія UEBA може виявляти ці типи атак, оскільки вони майже завжди змушують активи поводитися інакше, ніж встановлені базові показники.

Пріоритетність інцидентів

SIEM збирає події та журнали з кількох інструментів безпеки та критично важливих систем, а також генерує велику кількість сповіщень, які мають розслідувати співробітники служби безпеки. Це призводить до втоми від сповіщень, що є поширеною проблемою Центрів операцій безпеки (SOC).

Рішення UEBA можуть допомогти зрозуміти, які інциденти є особливо ненормальними, підозрілими або потенційно небезпечними в контексті вашої організації. UEBA може вийти за рамки базових показників та моделей загроз, додаючи дані про організаційну структуру, наприклад, критичність активів, ролі та рівні доступу до певних функцій організації. Невелике відхилення від норми для критично захищеної системи або адміністратора вищого рівня може бути вартим уваги для слідчого; для звичайного співробітника лише значне відхилення отримає високий пріоритет.

Запобігання втраті даних (DLP) та запобігання витоку даних

Інструменти запобігання втраті даних (DLP) використовуються для запобігання витоку даних або незаконній передачі даних за межі організації. Традиційні інструменти DLP повідомляють про будь-яку незвичайну активність, що здійснюється з конфіденційними даними, – вони створюють велику кількість сповіщень, з якими може бути важко впоратися командам безпеки.

Рішення UEBA можуть приймати сповіщення DLP, визначати їх пріоритети та консолідувати, розуміючи, які події являють собою аномальну поведінку порівняно з відомими базовими показниками. Це заощаджує час слідчим та допомагає їм швидше виявляти реальні інциденти безпеки.

Аналітика сутностей (IoT)

UEBA може бути особливо важливим у боротьбі з ризиками безпеки Інтернету речей (IoT). Організації розгортають великі парки підключених пристроїв, часто з мінімальними заходами безпеки або без них. Зловмисники можуть скомпрометувати пристрої IoT, використовувати їх для крадіжки даних або отримання доступу до інших IT-систем, або, що ще гірше, використовувати їх для DDoS-атаки чи інших атак на третіх осіб.

Дві чутливі категорії Інтернету речей – це медичні прилади та виробниче обладнання. Підключені медичні прилади можуть містити критично важливі дані та можуть становити загрозу для життя, якщо їх використовувати безпосередньо для догляду за пацієнтами. Виробниче обладнання може спричинити великі фінансові втрати у разі його збою, а в деяких випадках може загрожувати безпеці працівників.

UEBA може відстежувати підключені пристрої, встановлювати базову поведінку для кожного пристрою або групи подібних пристроїв і негайно виявляти, чи пристрій поводиться поза межами своїх звичайних меж. Наприклад:

- Підключення до або з незвичайних адрес чи пристроїв.
- Активність у незвичний час.
- Активовані функції пристрою, які зазвичай не використовуються.

Конвергенція UEBA та SIEM

Існує тісний зв'язок між технологіями UEBA та SIEM, оскільки UEBA спирається на міжорганізаційні дані безпеки для виконання свого аналізу, і ці дані зазвичай збираються та зберігаються SIEM.

Gartner розглядає UEBA як функцію, інтегровану в SIEM. Аналіз поведінки – це одна з можливостей, за допомогою якої Gartner оцінює постачальників у Магічному квадранті для управління інформацією та подіями безпеки. Gartner окреслює такі можливості для SIEM:

– Сукупні дані про події, що генеруються пристроями безпеки, мережевою інфраструктурою, системами та програмами.

– Поєднуйте дані про події з контекстною інформацією про користувачів, активи, загрози та вразливості з метою оцінювання, визначення пріоритетів та пришвидшення розслідувань.

– Нормалізуйте дані для ефективнішого аналізу.

– Пропонуйте аналіз подій у режимі реального часу для моніторингу безпеки, розширений аналіз поведінки користувачів та об'єктів, аналітику запитів, підтримку розслідування та управління інцидентами, а також звітність.

UEBA проти аналогічних технологій

UEBA проти NTA

Аналіз мережевого трафіку (NTA) зосереджений на моніторингу та аналізі мережевого зв'язку для виявлення аномалій або ознак компрометації. Хоча UEBA та NTA виявляють аномальну поведінку, їхні області застосування відрізняються.

UEBA досліджує поведінку користувачів та об'єктів у різних системах, включаючи кінцеві точки, програми та каталоги, а не лише мережеву активність. NTA обмежується мережевими даними та чудово справляється з виявленням таких загроз, як горизонтальне переміщення та витік даних. Натомість UEBA може виявляти загрози, пов'язані з зловживанням привілейованим доступом, незвичайною поведінкою під час входу або змінами в шаблонах доступу до файлів. NTA зазвичай підтримує аналіз трафіку в режимі реального часу, тоді як UEBA працює як з даними в реальному часі, так і з історичними даними для довгострокового моделювання поведінки.

Разом UEBA та NTA можуть доповнювати один одного: NTA виділяє підозрілі мережеві шляхи, тоді як UEBA надає поведінковий контекст щодо того, хто або що задіяно.

UBA проти UEBA

Аналітика поведінки користувачів (UBA) – це попереднє покоління технологій, орієнтованих виключно на користувачів-людей. Вона аналізує поведінку користувачів для виявлення таких ризиків, як неправомірне використання облікових даних, внутрішні загрози або підозрілі моделі доступу.

UEBA (аналітика поведінки користувачів та об'єктів) розширює цю концепцію, включаючи нелюдські об'єкти, такі як сервери, програми та пристрої Інтернету речей. Цей ширший охоплення є критично важливим, оскільки багато атак спрямовані на об'єкти, що не є користувачами-людьми, або походять від них. UEBA також зазвичай включає більш просунуту аналітику, таку як моделі машинного навчання, здатні виявляти складні поведінкові аномалії в гібридних середовищах.

Коротше кажучи, UEBA базується на UBA, надаючи більш повне уявлення про всі сутності в IT-середовищі та взаємозв'язки між ними.

Методи аналітики UEBA

Деякі рішення UEBA покладаються на традиційні методи виявлення підозрілої активності. До них можуть належати правила, визначені вручну, кореляції між подіями безпеки та відомими шаблонами атак. Обмеження традиційних методів полягає в тому, що вони ефективні лише настільки, наскільки ефективні правила, визначені адміністраторами безпеки, і не можуть адаптуватися до нових типів загроз або поведінки системи.

Розширена аналітика включає кілька сучасних технологій, які можуть допомогти виявити аномальну поведінку навіть за відсутності відомих закономірностей:

– Машинне навчання з вчителем – набори відомої хорошої та відомої поганої поведінки подаються в систему. Інструмент навчається аналізувати нову поведінку та визначати, чи є вона «схожою» на набір відомої хорошої чи відомої поганої поведінки.

– Баєсівські мережі – можуть поєднувати машинне навчання з вчителем та правила для створення поведінкових профілів.

– Самонавчання – система вивчає нормальну поведінку та здатна виявляти аномальну поведінку й попереджати про неї. Вона не зможе визначити, чи є аномальна поведінка хорошою чи поганою, лише те, що вона відхиляється від норми.

– Підсилене/напівавторизоване машинне навчання – гібридна модель, де основою є навчання без вчителя, а фактичні рішення щодо сповіщень передаються назад у систему, щоб забезпечити точне налаштування моделі та зменшити співвідношення сигнал/шум.

– Глибоке навчання – дозволяє проводити віртуальне сортування та розслідування тривог. Система навчається на наборах даних, що представляють тривоги безпеки та їх результати сортування, виконує самоідентифікацію ознак та здатна прогнозувати результати сортування для нових наборів тривог безпеки.

Традиційні методи аналітики є детермінованими в тому сенсі, що якщо певні умови були виконані, генерувалося сповіщення, а якщо ні, система вважала, що «все гаразд». Розширені методи аналітики, перелічені вище, відрізняються тим, що вони є евристичними. Вони обчислюють оцінку ризику, яка є ймовірністю того, що подія являє собою аномалію або інцидент безпеки. Коли оцінка ризику перевищує певний поріг, система створює сповіщення безпеки.

Проблеми розгортання UEBA

Інтеграція та масштабування даних

Однією з головних проблем розгортання UEBA є інтеграція різноманітних джерел даних. Системи UEBA покладаються на комплексні, високоякісні дані із систем керування ідентифікацією, журналів програм, мережевого трафіку, телеметрії кінцевих точок тощо. Інтеграція цих джерел – часто в різних форматах і обсягах – може бути складною та трудомісткою.

Масштабованість – ще одна проблема. Зі зростанням організацій та додаванням нових пристроїв, програм і користувачів обсяг даних зростає експоненціально. Рішення UEBA повинні обробляти ці дані майже в режимі реального часу, зберігаючи при цьому продуктивність. Без належного планування вузькі місця в продуктивності та збільшена затримка можуть погіршити можливості виявлення та робочі процеси аналітиків.

Хибнопозитивні результати

Незважаючи на розширену аналітику, хибнопозитивні результати залишаються значною проблемою в розгортанні UEBA. Якщо система генерує забагато сповіщень про нешкідливі аномалії, такі як робота легітимного користувача з нового місця розташування, аналітики безпеки можуть бути перевантажені або втратити чутливість.

Ця проблема часто пов'язана з незрілим базовим підходом або недостатнім контекстом у моделях поведінки. З часом, коли система навчається та налаштовує оцінку ризиків, кількість хибнопозитивних результатів може зменшитися. Однак на ранніх етапах розгортання або в динамічних середовищах підтримувати прийнятну якість сповіщень може бути складно.

Вимоги до навичок та ресурсів

Платформи UEBA потребують кваліфікованого персоналу для конфігурації, налаштування та обслуговування. Організаціям потрібні аналітики зі знаннями поведінкової аналітики, виявлення загроз та реагування на інциденти. Крім того, можуть знадобитися інженери обробки даних, щоб забезпечити належне отримання та нормалізацію даних. Меншим організаціям може бракувати досвіду або кількості персоналу для підтримки

повномасштабного впровадження UEBA. Навіть для великих підприємств інтеграція UEBA в існуючі операції безпеки може вимагати значних часових витрат та постійних зусиль для підтримки точності та ефективності моделей.

Ключові найкращі практики впровадження UEBA

1. Забезпечення комплексної та високоякісної інтеграції даних

Системи UEBA покладаються на багаті, різноманітні дані для точного моделювання поведінки. Почніть з визначення ключових джерел даних від постачальників ідентифікації (наприклад, Active Directory, LDAP), журналів кінцевих точок, хмарних додатків, VPN, проксі-серверів та мережевого трафіку. Отримуйте як структуровані, так і неструктуровані дані для створення повних профілів поведінки.

Використовуйте конектори, API або відправники журналів для автоматизації збору даних та забезпечення узгодженої синхронізації часу між джерелами – розбіжності в часі можуть перешкоджати точному аналізу часової шкали. Інвестуйте в процеси нормалізації та збагачення даних, щоб стандартизувати формати, вирішувати неоднозначності та позначати відповідні метадані, такі як ролі користувачів або класифікації активів.

Високоякісні дані – це не просто технічна вимога, вони є основоположними для здатності UEBA генерувати змістовні та практичні висновки. Низька якість даних призводить до спотворення базових показників, неефективного виявлення аномалій та збільшення кількості хибнопозитивних результатів.

2. Встановлення надійних базових показників поведінки

Ефективність UEBA залежить від сили її поведінкових моделей. Почніть з надання системі періоду спостереження – зазвичай кілька тижнів – протягом якого вона відстежує активність без попереджень. Протягом цього періоду система встановлює базові показники для користувачів та об'єктів, вивчаючи моделі використання, час доступу, мережеву взаємодію та поведінку системи.

Для більшої точності базові показники повинні враховувати взаємодію з колегами, включаючи порівняння поведінки користувачів, які виконують схожі ролі або мають схожі системи в одній операційній категорії. Врахування організаційного контексту, такого як відділ або місцезнаходження, допомагає адаптувати базові показники та запобігти неправильній класифікації. Регулярно переглядайте та вдосконалюйте ці базові показники. Якщо бізнес-операції змінюються, наприклад, додавання віддалених команд або сезонний сплеск активності, переконайтеся, що система адаптується. Статичні базові показники в динамічному середовищі призводять до появи сліпих зон або втоми від оповіщень.

3. Ретельно налаштуйте порогові значення та оцінку ризику

Не всі аномалії заслуговують на однакову стурбованість. Системи UEBA використовують оцінки ризику для оцінки серйозності відхилень, але їх необхідно ретельно калібрувати. Почніть з консервативних порогових значень, щоб уникнути перевантаження аналітиків, і коригуйте їх на основі оперативного зворотного зв'язку та аналізу інцидентів.

Оцінка ризику повинна враховувати частоту аномалій, їх серйозність та критичність для ураженої системи чи користувача. Наприклад, незвичайний вхід адміністратора на цінний сервер повинен мати більшу вагу, ніж така сама дія на звичайній робочій станції.

Використовуйте динамічні порогові значення, де це можливо – адаптивні системи, які з часом вивчають прийнятну дисперсію, можуть забезпечити більш нюансовані сповіщення. Також визначте шляхи ескалації та автоматизуйте дії реагування на події з високою достовірністю та високим ризиком, щоб пришвидшити пом’якшення наслідків.

4. Збагачуйте сповіщення контекстом та інформацією про загрози

Контекст є важливим для скорочення часу сортування та покращення прийняття рішень. Збагачуйте сповіщення метаданими з HR-систем (наприклад, статус зайнятості, відділ), інвентаризації активів (наприклад, критичність системи) та історичних моделей поведінки. Включайте такі деталі, як час входу, ідентифікатори пристроїв, геолокацію та журнали доступу до даних.

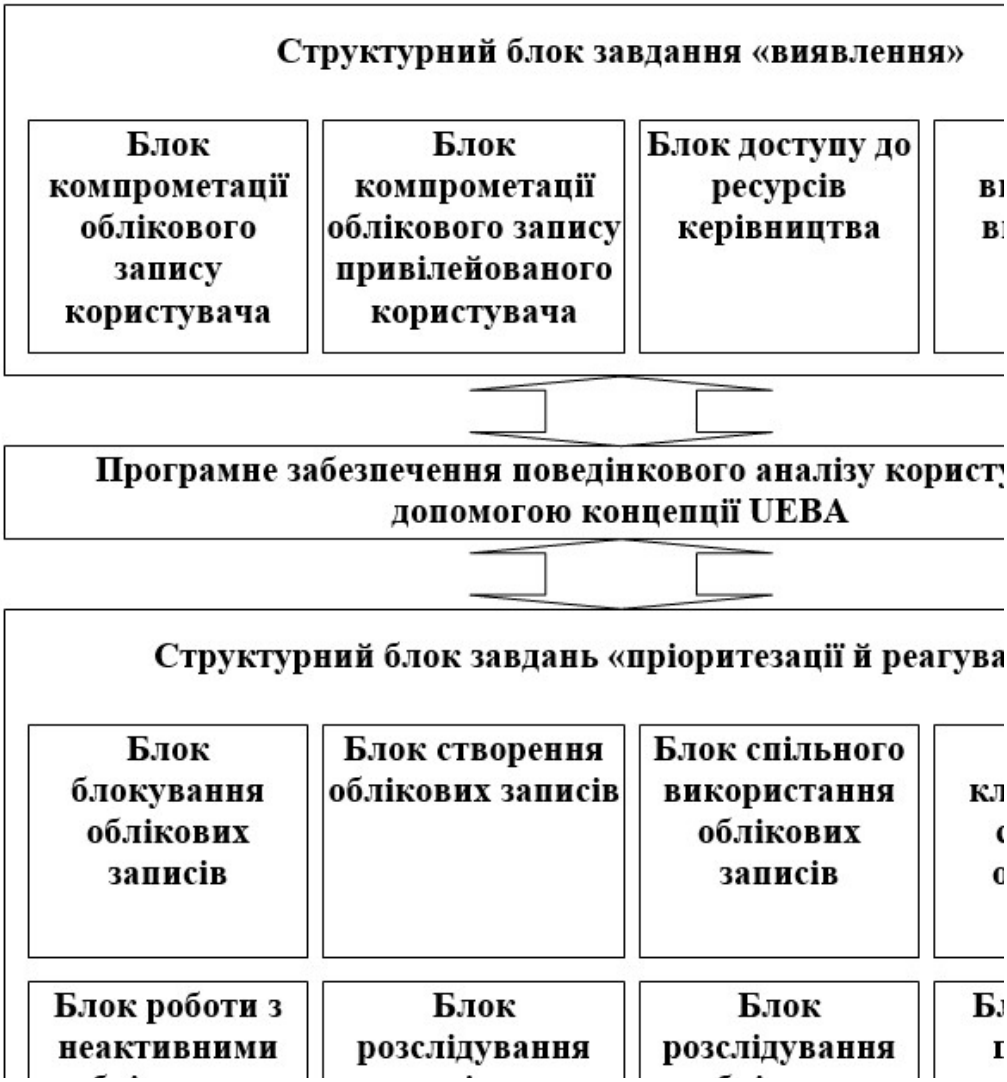

Рисунок 1 – Структурна схема системи

Інтегруйте канали аналітики загроз для зіставлення аномалій з відомими індикаторами компрометації (IOC) або тактиками, методами та процедурами зловмисників (TTP). Це допомагає розрізняти випадкові аномалії та цілеспрямовані загрози.

Представляйте збагачені сповіщення у зручному для аналітиків форматі, пов'язуючи їх із відповідними подіями в ланцюжку атаки. Це мінімізує час ручного розслідування та покращує якість дій реагування.

5. Інтеграція відповідно до стеку безпеки та робочих процесів

Щоб максимізувати цінність, UEBA має працювати в рамках ширшої екосистеми безпеки. Інтегруватися з платформами SIEM для використання існуючих можливостей збору та кореляції журналів. Передавати оцінки ризиків та сповіщення в системи SOAR, щоб забезпечити автоматизоване виконання сценаріїв, таких як ізоляція пристроїв або скидання облікових даних.

Забезпечте відповідність результатів UEBA вашим існуючим робочим процесам реагування на інциденти, системам видачі заявок та панелям звітності. Це забезпечує безперешкодну передачу між групами виявлення та розслідування та уникає дублювання зусиль.

Ретельно протестуйте інтеграції – системи UEBA повинні не лише надавати точні сповіщення, а й відповідати операційним реаліям. Обсяг сповіщень, час реагування та зручність використання так само важливі, як і точність виявлення. Прагніть до тісно

пов’язаної архітектури, де поведінкова аналітика стає природною частиною життєвого циклу ваших операцій безпеки.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів поведінкового аналізу користувачів за допомогою концепції UEBA. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем поведінкового аналізу користувачів за допомогою концепції UEBA.

– Досліджена система поведінкового аналізу користувачів за допомогою концепції UEBA.

– На основі отриманих результатів досліджень створена програмна реалізація системи поведінкового аналізу користувачів за допомогою концепції UEBA.

Розроблені алгоритми дозволяють успішно вирішувати завдання поведінкового аналізу користувачів за допомогою концепції UEBA. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
2. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
3. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
4. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
5. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
6. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56
7. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
8. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
9. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
10. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
11. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи ȟозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
12. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
13. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.

14. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 2(72), С. 170-178.
15. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
16. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
17. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
18. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
19. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
20. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
21. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
22. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
23. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.
24. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58.
25. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
26. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
27. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
28. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131.
29. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
30. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84.
31. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
32. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 166-171.