ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В ІНФОРМАЦІЙНІЙ СИСТЕМІ НА БАЗІ PRIVILEGED BEHAVIOR ANALYTICS»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Бойчук Л.Я.
(прізвище та ініціали)
Керівник Чумак Н.С.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

РЕФЕРАТ

Текстова частина магістерської роботи: 60 сторінок, 14 джерел.

Об'єкт дослідження – процес виявлення вразливостей інформаційної системи.

Предмет дослідження – технологія виявлення вразливостей інформаційної системи.

Мета роботи – розробити варіант системи виявлення вразливостей інформаційної системи та рекомендації щодо застосування технології в організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу виявлення вразливостей інформаційної системи.

В роботі проведено аналіз проблеми виявлення вразливостей інформаційної системи та проаналізовано основні загрози. Було проведено аналіз існуючих технологій виявлення вразливостей інформаційної системи.

Досліджено методи за засоби виявлення вразливостей на прикладі рішення Gurucul User and Entity Behavior Analytics. Визначено основні характеристики, функції, можливості та принцип роботи Gurucul User and Entity Behavior Analytics.

На основі проведених досліджень в роботі представлено варіант системи виявлення вразливостей інформаційної системи.

Галузь використання – кібербезпека корпоративної інформаційної системи.

ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ВРАЗЛИВОСТІ, ЗАГРОЗИ, АНОМАЛІЇ, АНАЛІЗ, АНАЛІТИКА

ABSTRACT

The text part of the master's work: 60 pages, 14 sources.

The object of research is the process of identifying information system vulnerabilities.

The subject of research is the technology of detecting vulnerabilities of the information system.

The purpose of the work is to develop a variant of the information system vulnerability detection system and recommendations for the use of technology in the organization.

Research methods – study of the literature on this topic, analysis of operational documentation, international standards and their comparison, modeling of the process of identifying information system vulnerabilities.

The paper analyzes the problem of identifying information system vulnerabilities and analyzes the main threats. An analysis of existing technologies for detecting information system vulnerabilities was carried out.

Methods for vulnerability detection were studied using the Gurucul User and Entity Behavior Analytics solution as an example. The main characteristics, functions, capabilities and working principle of Gurucul User and Entity Behavior Analytics are defined.

On the basis of the conducted research, the work presents a variant of the information system vulnerability detection system.

The field of use is cyber security of the corporate information system.

INFORMATION SYSTEM, CYBER SECURITY, VULNERABILITIES, THREATS, ANOMALIES, ANALYSIS, ANALYTICS

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІС — інформаційна система

NGFW — Next-generation firewall

NGIPS — Next Generation Intrution Prevention System

CASB — Cloud Access Security Broker

SIEM — Security information and event management

ML — Machine Learning

VPN — Virtual Private Network

ВСТУП

Актуальність дослідження. Виявлення загроз – це практика аналізу всієї екосистеми безпеки для виявлення будь-якої зловмисної діяльності, яка може скомпрометувати мережу. Якщо загрозу виявлено, необхідно вжити заходів для її пом’якшення, щоб належним чином нейтралізувати загрозу, перш ніж вона зможе використати будь-яку наявну вразливість.

Коли справа доходить до виявлення та подолання загроз, швидкість має вирішальне значення. Програми безпеки повинні бути в змозі швидко й ефективно виявляти загрози, щоб зловмисники не мали достатньо часу для пошуку конфіденційних даних. Оборонні програми бізнесу ідеально можуть зупинити більшість загроз, оскільки вони часто були помічені раніше, а це означає, що вони повинні знати, як з ними боротися. Ці загрози вважаються «відомими». Однак існують додаткові «невідомі» загрози, які організація прагне виявити. Це означає, що організація раніше з ними не стикалася, можливо тому, що зловмисник використовує абсолютно нові методи чи технології.

Відомі загрози іноді можуть пройти повз навіть найкращі засоби захисту, тому більшість організацій безпеки активно шукають як відомі, так і невідомі загрози у своєму середовищі.

За допомогою аналітики поведінки користувачів організація може отримати базове розуміння того, якою буде нормальна поведінка співробітника: наприклад, до яких даних вони мають доступ, коли вони входять у систему та де вони фізично знаходяться.

Вищенаведені аргументи актуалізують тему даної магістерської роботи, зміст якої становлять дослідження щодо технології виявлення вразливостей на базі Gurucul User and Entity Behavior Analytics .

Об'єкт дослідження – процес виявлення вразливостей інформаційної системи.

Предмет дослідження – технологія виявлення вразливостей інформаційної системи.

Мета роботи – розробити варіант системи виявлення вразливостей інформаційної системи та рекомендації щодо застосування технології в організації.

Наукові завдання:

дослідити сутність проблеми виявлення вразливостей;

встановити сутність завдань захисту;

проаналізувати існуючі технології виявлення вразливостей;

проаналізувати методи та засоби виявлення вразливостей;

проаналізувати основні функції та принципи реалізації виявлення вразливостей.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу виявлення вразливостей інформаційної системи.

Практичне значення одержаних результатів полягає в розробці варіанта виявлення вразливостей на базі рішення Gurucul User and Entity Behavior Analytics, а також у розробці рекомендацій щодо застосування технології виявлення вразливостей в інформаційній системі.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1 Аналіз основних вразливостей інформаційних систем

Забезпечення захищеності інформаційної системи є одним із найважливіших етапів її розробки та підтримки. Очевидно, що інформаційна система, віддана у виробництво без будь-яких засобів захисту від загроз, не несе жодної практичної та матеріальної цінності. Наприклад, система здійснення та обробки торгових угод, реалізована без використання алгоритмів шифрування, не може гарантувати цілісність даних, що обробляються. Звичайно, така система не повинна і не використовуватиметься в реальних торгових операціях.

При проектуванні будь-якої нової інформаційної системи, а також при використанні вже реалізованої системи стоїть проблема гарантії її захищеності від компрометації. Гарантія потрібна не тільки для кінцевого користувача, а й, наприклад, для особи, яка виділяє кошти на розробку інформаційної системи. Аналіз захищеності системи, що розробляється, рекомендується проводити за допомогою моделювання потенційних загроз. Останнім часом нові вразливості з'являються щодня, тому важливо вміти класифікувати загрози та оцінювати їх за рівнем ризику. Інформаційна безпека визначається всіма аспектами, пов'язаними з досягненням та підтриманням конфіденційності, цілісності, доступності, невідмовності, підзвітності, автентичності та достовірності інформації чи засобів її обробки. Захист інформації має мати комплексний характер, проте, необхідно враховувати можливість виникнення загроз, специфічних для даної інформаційної системи. На етапі проектування системи захисту важливо не упустити істотних деталей і, водночас, не переоцінити деякі з них. Необхідно знати про характер можливих небезпек, класифікувати загрози та проводити заходи щодо їх усунення.

Основний принцип забезпечення безпеки інформаційної системи полягає в аналізі потенційних загроз, проведенні заходів щодо їх усунення та подальшому

аналізі стану безпеки системи. Моделювання загроз дозволяє структурувати процес забезпечення безпеки інформаційної системи та позначити загрози, які здатні завдати найбільших збитків та які необхідно усунути насамперед. Не можна забезпечити безпеку інформаційної системи без належного розуміння специфіки та походження загроз. Зазвичай уразливості усуваються в міру їх виявлення, часто випадковим чином. Використовуючи цей підхід, неможливо відповісти на запитання: «Досить безпечна інформаційна система?». Моделювання загроз не є одноразовим процесом. Це ітеративний підхід, який починається з ранніх стадій розробки системи та продовжується протягом усього її життєвого циклу.

Необхідність ітеративного підходу обумовлена двома причинами. По-перше, фізично неможливо виявити та зафіксувати всі потенційні для системи загрози за один раз. По-друге, додаток (інформаційна система), що розробляється, неодмінно адаптується під постійно змінюються користувальницькі і функціональні вимоги. Тому моделювання загроз необхідно повторювати протягом усього розвитку інформаційної системи.

Фахівці з безпеки компанії Microsoft запропонували процес моделювання загроз, що складається з шести етапів:

1. Визначення ресурсів, що захищаються.
2. Огляд архітектури.
3. Декомпозиція системи.
4. Визначення загроз.
5. Документація загроз.
6. Пріоритезація загроз.

На першому етапі визначаються всі ресурси, які необхідно захищати. Це можуть бути конфіденційні дані, бази даних, веб-сторінки тощо. Далі проводиться документація функцій інформаційної системи, її архітектури, фізичної конфігурації та технологій, використаних для її реалізації. Можливий пошук уразливостей у дизайні інформаційної системи. Визначення використовуваних у реалізації технологій допоможе не прогаяти специфічних для них уразливостей і надалі сконцентруватися на їх усуненні. На етапі декомпозиції система

розбивається на компоненти створення профілю безпеки (який описує реалізацію аутентифікації, авторизації, криптографії та інших аспектів безпеки у системі). Перевіряються основні питання безпеки, виділяються межі довіри, потоки даних та їх вхідні точки. Система аналізується виконання таких свойств: перевірка даних користувача, аутентифікація та авторизація, криптографічний захист передачі даних, управління винятками, аудит та ін. Профіль безпеки описує реалізацію аутентифікації, авторизації, криптографії та інших аспектів безпеки в системі. Далі визначаються потенційні загрози всім компонент системи. Компанія Microsoft пропонує методику STRIDE визначення та категоризації загроз. Моделювання за допомогою STRIDE допоможе забезпечити виконання в інформаційній системі всіх властивостей безпеки. STRIDE – абревіатура від: Далі визначаються потенційні загрози всім компонент системи. STRIDE – абревіатура від:

- Spoofing Identity (підміна особистості).
- Tampering with Data (зміна даних).
- Repudiation (відмова від досконалої операції).
- Information Disclosure (розголошення відомостей).
- Denial of Service (відмова в обслуговуванні).
- Elevation of Privilege (підвищення прав доступу).

За цією методикою визначаються загрози кожному компоненту інформаційної системи залежно від категорії загрози. Загрози типу «Підміна особистості» є актуальними для систем, в яких реалізуються різні рівні доступу користувачів. Користувач не повинен мати можливість вдаватися іншим користувачем або прочитати атрибути іншого користувача. Загрози типу Зміна даних реалізують можливість користувача вплинути на логіку роботи системи через доступні інтерфейси. Система повинна ретельно перевіряти всі дані, що виходять від користувача, в процесі їх використання і аж до моменту їх збереження в системі. При недостатньому аудиті транзакцій у системі загрози типу «Відмова від досконалої операції» реалізують можливість користувача відмовитися від виконаних ним будь-яких дій у системі, що може вплинути на достовірність

інформації, що циркулює за системою. Наприклад, користувач може заявити «Я не перераховував кошти з цього приводу». При недостатньому аудиті операцій неможливо перевірити цю заяву. Загрози типу «Розголошення даних» реалізують можливість публікації конфіденційних даних у системі. Можливо, у системі виявиться витік інформації. Дизайнери системи також повинні враховувати той факт, що на неї проводитимуться атаки типу DoS (відмова в обслуговуванні). Необхідно переконатися, що ресурсомісткі процеси будуть недоступні неавторизованим користувачам. Такими процесами можуть бути: читання великих файлів, складні обчислення, виконання довгих запитів до бази даних тощо. Якщо в системі розрізняються користувальницькі та адміністративні ролі, необхідно переконатися у неможливості підвищення прав доступу.

Усі дії у системі повинні перевірятися за матрицею доступу. На наступному етапі моделювання всі певні погрози необхідно зафіксувати у наступному вигляді:

- Опис небезпеки.
- Об'єкт можливої атаки.
- Ризик.
- Можливий сценарій атаки.
- Вжиті заходи щодо усунення загрози.

На останньому етапі процесу розставляються пріоритети щодо усунення загроз залежно від їхнього ризику. Це дозволить зайнятися насамперед загрозами, які можуть завдати системі найбільшої шкоди. Економічно невигідно усувати абсолютно всі певні загрози, тому можливо опустити загрози, ймовірність реалізації яких прагне нуля і збитки яких мінімальний. У результаті для розробників інформаційної системи представляється документ, що дозволяє їм сформувати чітке розуміння потенційних загроз і ризиків.

Безліч нових загроз, що розвиваються, кібербезпеки тримають галузь інформаційної безпеки в стані підвищеної готовності. Все більш витончені кібератаки з використанням шкідливих програм, фішингу, машинного навчання та штучного інтелекту, криптовалюти та багато іншого піддають дані та активи корпорацій, урядів та приватних осіб постійному ризику [1].

1.2 Аналіз загроз та тенденцій забезпечення безпеки інформаційних систем

Фішинг. Фішингові атаки, в яких ретельно націлені цифрові повідомлення передаються, щоб змусити людей клацнути посилання, яке потім може встановити шкідливе програмне забезпечення або розкрити конфіденційні дані, стають все більш витонченими.

Тепер, коли співробітники більшості організацій краще обізнані про небезпеки фішингу електронною поштою або переходу за підозрілими посиланнями, хакери підвищують ставки — наприклад, використовують машинне навчання для більш швидкого створення та поширення переконливих підроблених повідомлень, сподіваючись, що одержувачі ненавмисно скомпрометують мережі та системи організації. Такі атаки дозволяють хакерам красти логіни користувачів, облікові дані кредитних карток та іншу особисту фінансову інформацію, а також отримувати доступ до приватних баз даних.

Програми-вимагачі. Вважається, що хакери щорічно обходяться жертвам у мільярди доларів, оскільки хакери впроваджують технології, які дозволяють їм буквально викрадати бази даних окремих осіб чи організацій та зберігати всю інформацію з метою отримання викупу. Вважається, що зростання криптовалют, таких як біткойн, допомагає розпалювати атаки програм-вимагачів, дозволяючи анонімно оплачувати вимоги про викуп.

Оскільки компанії продовжують зосереджуватися на створенні більш надійних засобів захисту від програм-вимагачів, деякі експерти вважають, що хакери все частіше націлюватимуться на інших потенційно прибуткових жертв програм-вимагачів, таких як заможні люди.

Криптоджекінг. Рух криптовалют також впливає на кібербезпеку іншими способами. Наприклад, криптоджекінг — це тенденція, коли кіберзлочинці захоплюють сторонні домашні чи робочі комп'ютери для «майнінгу» криптовалюти. Оскільки видобуток криптовалюти (наприклад, біткойна) вимагає величезної обчислювальної потужності комп'ютера, хакери можуть заробляти

гроші, таємно використовуючи чужі системи. Для підприємств системи з криптоджектом можуть викликати серйозні проблеми з продуктивністю та дорогі простої, оскільки IT-відділ працює над відстеженням та вирішенням проблеми [3].

Кібер-фізичні атаки. Та сама технологія, яка дозволила модернізувати та комп'ютеризувати критичну інфраструктуру, також пов'язана з ризиком. Постійна загроза злому електричних мереж, транспортних систем, водоочисних споруд і т.д. є серйозною вразливістю в майбутньому. Згідно з нещодавнім повідомленням The New York Times, навіть багатомільярдні військові системи Америки перебувають під загрозою високотехнологічної нечесної гри.

Атаки, спонсоровані державою. Крім хакерів, які прагнуть отримати прибуток за рахунок крадіжки особистих та корпоративних даних, цілі держави тепер використовують свої кібер-навички для проникнення в інші уряди та проведення атак на критично важливу інфраструктуру. Кіберзлочинність сьогодні є серйозною загрозою не тільки для приватного сектору та окремих осіб, а й для уряду та нації в цілому. Очікується, що з наближенням до кінця 2022 року кількість атак, спонсорованих державою, збільшуватиметься, причому атаки на критично важливу інфраструктуру викликатимуть особливе занепокоєння.

Багато таких атак націлені на державні системи та інфраструктуру, але організації приватного сектора також ризикують. Згідно з звітом Thomson Reuters Labs: «Кібератаки, спонсоровані державою, є новим і значним ризиком для приватного підприємства, який все більше кидатиме виклик тим секторам ділового світу, які надають зручні цілі для врегулювання геополітичних невдоволень» [2].

Атаки на Інтернет речей. Інтернет речей з кожним днем стає все більш поширеним (згідно з статистикою очікується, що до 2025 року кількість пристроїв, підключених до IoT, сягне 75 мільярдів). Це, звичайно, ноутбуки та планшети, а також маршрутизатори, веб-камери, побутова техніка, розумний годинник, медичні пристрої, виробниче обладнання, автомобілі та навіть системи домашньої безпеки.

Підключені пристрої зручні для споживачів, і багато компаній тепер використовують їх, щоб заощадити гроші, збираючи величезну кількість корисних

даних та оптимізуючи бізнес-процеси. Однак більша кількість підключених пристроїв означає більший ризик, що робить мережі IoT вразливішими для кібервторгнень та інфекцій. Потрапивши під контроль хакерів, пристрої IoT можуть використовуватися для створення хаосу, навантаження мереж або блокування основного обладнання з метою отримання фінансової вигоди.

Розумні медичні пристрої та електронні медичні карти (EMR). Індустрія охорони здоров'я все ще переживає серйозну еволюцію, оскільки більшість медичних карток пацієнтів наразі перенесено в онлайн, а медичні працівники усвідомлюють переваги досягнень у галузі інтелектуальних медичних пристроїв. Однак у міру того, як галузь охорони здоров'я адаптується до цифрового віку, виникає низка проблем, пов'язаних із загрозами конфіденційності, безпеки та кібербезпеки.

За даними Інституту розробки програмного забезпечення Університету Карнегі-Меллона, «у міру того, як все більше пристроїв підключається до мереж лікарень та клінік, дані та інформація про пацієнтів стають дедалі вразливішими. Ще більшу стурбованість викликає ризик віддаленої компрометації пристрою, безпосередньо підключеного до пацієнта. Зловмисник теоретично може збільшувати або зменшувати дози, надсилати електричні сигнали пацієнту або відключати моніторинг показників життєдіяльності».

Оскільки лікарні та медичні установи все ще адаптуються до оцифрування медичних карток пацієнтів, хакери використовують безліч уразливостей у їхніх засобах захисту. І тепер, коли медичні карти пацієнтів майже повністю розміщені в Інтернеті, вони є головною метою для хакерів через конфіденційну інформацію, що міститься в них.

Треті сторони. Треті сторони, такі як постачальники та підрядники, мають величезний ризик для корпорацій, більшість з яких не мають безпечної системи або спеціальної команди для управління цими сторонніми співробітниками.

У міру того, як кіберзлочинці стають все більш витонченими, а загрози кібербезпеки продовжують зростати, організації все більше усвідомлюють потенційну загрозу, що походить від третіх осіб. Однак ризик, як і раніше, високий.

Звіт про "Ризики безпеки, пов'язані з відносинами зі сторонніми постачальниками" опублікований RiskManagementMonitor.com, включає інфографіку, згідно з якою 60% витоків даних пов'язані з третьою стороною і що лише 52% компаній мають стандарти безпеки щодо сторонніх постачальників та підрядників.

Соціальна інженерія. Хакери постійно стають дедалі витонченішими не лише у використанні технологій, а й у психології. Tripwire описує соціальних інженерів як «хакери, які використовують одну слабкість, яка є у кожній організації: людську психологію. Використовуючи різні засоби масової інформації, у тому числі телефонні дзвінки та соціальні мережі, ці зловмисники обманом змушують людей пропонувати їм доступ до конфіденційної інформації» [2].

Гостра нестача фахівців з кібербезпеки. В останні роки епідемія кіберзлочинності швидко загострилася, тоді як компанії та уряди щосили намагалися найняти достатньо кваліфікованих фахівців для захисту від зростаючої загрози.

Гостра нестача кваліфікованих фахівців з кібербезпеки продовжує викликати тривогу, оскільки сильна, розумна цифрова робоча сила необхідна боротьби з більш частими і витонченими загрозами кібербезпеки, які з усього світу [3].

1.3 Аналіз основних методів запобіганням загрозам інформаційної системи

Убезпечити периметр

Перша складова, яку слід звернути увагу, — це периметр. Традиційних брандмауерів та антивірусних рішень вже недостатньо. Проте брандмауери наступного покоління (NGFW) поєднують розширений захист від шкідливих програм (AMP), систему запобігання вторгнень нового покоління (NGIPS), видимість і контроль додатків (AVC) та фільтрацію URL-адрес, щоб забезпечити багаторівневий підхід.

NGFW - це важливий перший крок до захисту периметра та впровадження інтегрованого рішення.

Захист користувачів

Сьогодні понад 50 відсотків працівників є мобільними. У міру того, як співробітники змінюють методи своєї роботи, IT-підрозділи повинні адаптуватися. Рішення IT-безпеки мають бути спрямовані на захист співробітників, де б вони не працювали. Співробітники можуть працювати в центральному офісі, філії або будь-якому іншому місці за допомогою мобільного пристрою.

Для більшості IT-відділів безпека мобільних пристроїв було найбільшою проблемою. Незважаючи на складність, важливо забезпечити безпеку мобільних пристроїв, оскільки підприємства продовжуватимуть збільшувати кількість мобільних пристроїв. Такі технології, як віртуальні приватні мережі (VPN), а також перевірка користувачів та довіра пристроїв можуть негайно підвищити безпеку мобільних пристроїв.

Розумна сегментація мережі

Програмна сегментація розділяє мережу, тому погрози можна легко ізолювати. Зі збільшенням числа бізнес-додатків та користувачів стає важко виявити взаємозалежність. Для достатнього запобігання загрозам підприємства повинні мати передову аналітика мережної безпеки і видимість визначення всіх взаємозалежностей мережі.

Надмірна сегментація мережі може уповільнити роботу. Недостатнє сегментування може призвести до поширення атак. Бізнес має бути розумним та ефективним при сегментуванні.

Швидке виявлення та усунення проблем

Порушення безпеки будуть. Найважливішим елементом запобігання загрозам є виявлення та усунення проблем. Це вимагає широкої видимості та контролю. Також потрібний добре підготовлений IT-персонал. Щоб допомогти підготуватись, часто рекомендують підприємствам розробитиплан реагування на інцидентита тестувати поточні мережеві рішення за допомогою перевірки на проникність.

Типи рішень для запобігання та виявлення загроз

NGFW

Як згадувалося вище, NGFW є важливим першим кроком до запобігання загрозам. Традиційні брандмауери просто надають чи забороняють доступ. Хоча це здається інтуїтивно зрозумілим, його ефективність залежить від точності запрограмованих політик та обмежень. Наприклад, якщо загроза нова та невідома, IT-відділ, швидше за все, ще не встановив політики, що забороняють їй доступ.

Однак NGFW інтегруються з додатковими програмними рішеннями, такими як NGIPS та AMP. Якщо невідома загроза обходить політики, що автоматично застосовуються, ці додаткові рішення надають засоби виявлення та виправлення для захисту вашої мережі. З усіма цими додатковими інструментами NGFW забезпечує покращену видимість, автоматизацію та контроль над вашою мережею.

NGIPS

NGIPS забезпечує чудове запобігання загрозам при виявленні вторгнень, сегментації внутрішньої мережі, загальнодоступній хмарі, а також управлінні вразливістю та виправленнями.

Для виявлення вторгнень потрібна технологія, яка не відстає від мінливих загроз. NGIPS забезпечує узгоджений захист та аналіз користувачів, програм, пристроїв та вразливостей у вашій мережі. Завдяки перевірці на основі файлів та вбудованому ізольованому програмному середовищу NGIPS може швидко виявляти загрози. Якщо загроза обходить засоби захисту, NGIPS забезпечує ретроспективний аналіз для видалення та усунення загроз на більш пізніх етапах їхнього існування.

Сегментація внутрішньої мережі дозволяє корпоративним організаціям забезпечити узгоджений механізм застосування, що охоплює вимоги кількох внутрішніх організацій. Сегментація може легко задовольнити різні вимоги мережі та різні робочі навантаження.

NGIPS забезпечує постійну ефективність безпеки як у загальнодоступних, так і приватних хмарах. NGIPS повинен підтримувати кілька гіпервізорів, включаючи Azure, AWS та VMWare. Ці програми не залежать від віртуальних

комутаторів. NGIPS дозволяє застосовувати політики в мережі на локальних пристроях, загальнодоступній хмарній інфраструктурі та звичайних гіпервізорах, проводячи глибоку перевірку пакетів між контейнерними середовищами.

Завдяки управлінню вразливістю та виправленням є можливість бути більш вибірковим на основі інформації, отриманої від NGIPS. Часто процес тестування та/або середовище організації можуть затримувати виправлення високопріоритетних уразливостей.

AMP

Розширений захист від шкідливих програм є найважливішим компонентом рішень нового покоління. Шкідливе ПЗ продовжує розвиватися та адаптуватися. З цієї причини шкідливе програмне забезпечення може бути надзвичайно важко виявити на периметрі мережі. Комбінуючи NGFW з AMP та аналітикою загроз, мережі можуть виявляти набагато більше раніше невідомих шкідливих програм.

Хоча аналіз загроз може виявляти більше загроз, мережа, як і раніше, буде наражатися на загрозу з боку нових, небачених раніше шкідливих програм. Деякі з цих шкідливих програм можуть мати таймери та інші приховані атрибути, які маскують шкідливу поведінку, доки вони не проникнуть у мережу. Однак існують рішення AMP, які безперервно аналізують файли протягом усього їхнього життєвого циклу. Це дуже важливо. Завдяки цим можливостям AMP негайно відзначить шкідливе програмне забезпечення, яке почне проявляти зловмисну поведінку в майбутньому.

AVC

Компанії використовують більше програм, ніж будь-коли раніше. З AVC, організації можуть створити справжню мережу за допомогою додатків. Глибока перевірка пакетів (DPI) може класифікувати програми, а у поєднанні зі статистичною класифікацією, кешуванням сокетів, виявленням сервісів, автоматичним навчанням та DNS-AS, AVC може забезпечити прозорість та контроль над мережними додатками.

Завдяки покращеній видимості організації можуть набагато швидше усувати загрози. Іноді програми можуть бути мережевими вразливими. Якщо організація не

може повністю бачити всі свої програми, вона не може їх захистити. Аналітика додатків та моніторинг дають негайне уявлення про продуктивність додатків. Низька продуктивність може бути ознакою того, що слід досліджувати загрози.

Аналітика загроз

Аналітика зароз підвищує чинність всіх цих розчинів. Аналітика загроз світового класу перетворює ці технології з хороших на відмінні. Захист мережі та видимість збільшують здатність організації зупиняти загрози. Однак це передбачає, що організація може визначити, чи є файл шкідливим чи безпечним. Це малоймовірно. Більшість загроз невідомі у мережі.

Аналітика загроз може попередити вашу мережу, якщо невідома загроза буде визнана шкідливою десь у земній кулі. Раптом значна кількість невідомих загроз стає повністю відомою та зрозумілою завдяки аналізу загроз.

Перевірка користувача та довіра до пристрою

Контроль доступу до мережі є обов'язковою умовою безпеки. За допомогою рішень для перевірки користувачів та довіри до пристроїв мережі можуть встановлювати довірчі стосунки з посвідченнями користувачів та пристроями та застосовувати політики доступу до програм. Двофакторна автентифікація може перевіряти право доступу користувача перед доступом до корпоративної інформації та ресурсів. Крім перевірки користувача, рішення для перевірки довіри пристроїв можуть перевіряти пристрої під час доступу, щоб визначити рівень їхньої безпеки та надійність [4].

Аналітика поведінки користувачів та об'єктів (UEBA), також відома як аналітика поведінки користувачів (UBA), є процесом збору інформації про мережеві події, які користувачі генерують щодня. Після збирання та аналізу його можна використовувати для виявлення використання скомпрометованих облікових даних, горизонтального переміщення та інших шкідливих дій.

У Gartner Market Guide додано «Сутність» у User Behavior Analytics через зростаючі загрози з боку зовнішніх сил, а не лише окремих користувачів. Ці зовнішні сили включають, крім іншого, маршрутизатори, сервери, програми та інші мережні пристрої, які можуть бути скомпрометовані.

Таким чином, ці інші типи аналітики поведінки відхиляються від традиційної аналітики поведінки споживачів, щоб зосередитися на поведінці систем та облікових записах користувачів у них [1].

На основі досліджень Gartner наведено приклади застосування UEBA до конкретних випадків використання або реалізації функцій UEBA для доповнення базової аналітики в інших інструментах.

Моніторинг співробітників за допомогою агентів

Інструменти, орієнтовані моніторинг співробітників, вимагають дуже специфічних даних, які часто вимагають розгортання спеціальних агентів до створення необхідних необроблених даних. Наприклад, рішенням з моніторингу співробітників іноді потрібні агенти, що знаходяться на кінцевих точках для відстеження клацань мишею та натискання клавіш з метою судової експертизи. Крім того, до такої поведінки застосовуватимуться функції UEBA для виявлення аномалій.

Приклади репрезентативних постачальників моніторингу співробітників, які заявляють про функції UEBA, включають:

- Dtex Systems
- e-Safe Systems
- Forcepoint (formerly RedOwl, a UEBA solution)
- Haystax Technology
- ObserveIT
- Raytheon SureView

Veriato (formerly SpectorSoft)

Захист кінцевих точок на основі агентів

Витонченість атак на кінцеву точку і можливість виявляти неправомірну поведінку зловмисників або скомпрометованих користувачів усередині кінцевої точки вимагають від постачальників EPP/EDR доступу до локальних даних, які зазвичай не надаються базовими журналами та видимістю з базової ОС. Отже, вони розгортатимуть агенти в кінцевих точках для створення необхідних точок телеметрії та даних. У майбутньому провідні постачальники засобів захисту

кінцевих точок (EPP/EDR) можуть застосовувати методи UEBA до цих точок даних, щоб надати розширені аналітичні можливості для виявлення аномалій як користувачів, так і об'єктів.

Приклади репрезентативних постачальників EPP/EDR, які мають функції UEBA:

- Carbon Black
- Cisco
- CounterTack
- CrowdStrike
- Cybereason
- Cylance
- Rapid7
- SentinelOne

CASB

Декілька постачальників CASB заявляють про різний ступінь можливостей UEBA, застосовуючи методи аналітики для спостереження за тим, як користувачі взаємодіють з програмами SaaS, і виявляючи ризиковану або ненормальну поведінку, яка вказує на можливі атаки.

- Bitglass
- Forcepoint CASB
- Microsoft
- Netskope
- Oracle CASB
- McAfee
- Symantec CloudSOC

SIEM

Природним розширенням інструментів SIEM є постійне надання якіснішої аналітики, тому не дивно, що постачальники SIEM впроваджують функції UEBA, як описано в розділі «Конвергенція SIEM та UEBA».

Приклади репрезентативних постачальників SIEM, які заявляють про можливості UEBA, включають:

- Dell Technologies
- Exabeam (також є автономним постачальником рішення UEBA)
- IBM
- FireEye
- LogRhythm (також є автономним постачальником рішення UEBA)
- FireEye
- Micro Focus ArcSight (через OEM Securonix)
- Rapid7
- Securonix (також є автономним постачальником рішення UEBA)
- Splunk (також є автономним постачальником рішення UEBA після придбання Caspida)
- VENUSTECH [5].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ НА БАЗІ РІШЕННЯ GURUCUL UEBA

2.1. Аналіз властивостей, функцій та характеристик UEBA

Аналіз поведінки користувачів та об'єктів (UEBA) – це рішення для забезпечення безпеки, яке часто використовує алгоритми ШІ та машинного навчання для виявлення аномальної поведінки в мережах та комп'ютерних системах. Він аналізує моделі поведінки користувачів та інших об'єктів у корпоративних мережах, серверах, маршрутизаторах та кінцевих точках.

UEBA відрізняється від більш простого аналізу поведінки користувачів (UBA) тим, що він охоплює всі об'єкти, включаючи пристрої та програми, а не лише користувачів. Таким чином, UEBA є складнішою формою UBA. Він має спеціалізований моніторинг нелюдських (машинних) об'єктів та процесів, таких як керовані та некеровані кінцеві точки, хмарні та мобільні програми, а також автоматизовані шкідливі процеси.

У 2017 році Gartner додали букву "E" до UEBA. Мета полягала в тому, щоб допомогти індустрії безпеки покращити профільування некористувальних об'єктів, щоб забезпечити точніше виявлення погроз[5].

Функції

Рішення UEBA відстежують поведінку всіх користувачів та об'єктів у мережі організації. Вони обробляють поведінкові дані, щоб визначити, чи може конкретна дія або тенденція поведінки вказувати або сприяти атаці. Технологія UEBA може визначити, що являє собою нормальну діяльність, а що може становити загрозу.

Зловмисники можуть проникнути в мережу, використовуючи вкрадені облікові дані співробітників, але шкідлива активність зловмисника відрізняється від звичайних моделей поведінки, що дозволяє UEBA виявити її як аномалію.

Дані, що обробляються UEBA, можуть надходити з репозиторію даних (тобто озера даних) або рішення SIEM, яке збирає дані з кількох джерел. UEBA інтегрує

різні типи інформації, включаючи дані захоплення пакетів, журнали та інші дані із платформ моніторингу безпеки. Багато організацій об'єднують UEBA з SIEM для збору та обробки даних.

Аналітичний компонент UEBA може виявляти аномалії за допомогою різних аналітичних методів, включаючи моделі на основі правил, сигнатур, статистичні моделі та моделі машинного навчання. Окрім відстеження пристроїв та подій, UEBA відстежує потенційні внутрішні загрози за допомогою машинного навчання. Він працює, встановлюючи базовий рівень нормальної активності для порівняння підозрілої поведінки.

Якщо користувач входить до системи з незвичайного місця, отримує доступ до незвичайних файлів або намагається отримати доступ до файлів занадто часто або в незвичайний час, це може вказувати на неправильне використання прав доступу. Можливості розширеної аналітики повинні доповнювати традиційну аналітику SIEM на основі правил, дозволяючи UEBA виявляти безліч складних та простих типів атак, на відміну від спеціалізованого інструменту, який фокусується на моніторингу одного об'єкта (наприклад, співробітників).

Здатність UEBA виявляти аномальну поведінку в режимі реального часу дозволяє негайно надсилати попередження. Таким чином, аналітики безпеки можуть швидко реагувати на загрози та запобігати серйозним порушенням. Без UEBA груп безпеки необхідно фільтрувати оповіщення, щоб визначити, які ознаки становлять реальну загрозу. UEBA автоматизує цей аналітичний процес для визначення пріоритетів реальних загроз.

Варіанти використання UEBA

Рішення UEBA та безпека на основі поведінки корисні для різних сценаріїв. Деякі складні загрози можуть уникнути і уникнути виявлення за допомогою звичайних інструментів безпеки, але система UEBA виявить та заблокує їх. До них відносяться:

Вкрадені облікові дані – зловмисники можуть отримати облікові дані законного користувача. Будь-яка шкідлива активність, що виконується з використанням законних облікових даних, може бути звичайною для традиційного

інструменту моніторингу, але UEBA ідентифікує нетипову активність в обліковому записі користувача.

Цільові пристрої та облікові записи — просунуті зловмисники можуть безпосередньо атакувати кінцевий пристрій або обліковий запис, який використовують керівники, такі як генеральний директор або фінансовий директор. UEBA допомагає виявляти незвичну поведінку на привілейованих ресурсах.

Скомпрометовані хости. Зловмисники можуть залишатися непоміченими протягом багатьох місяців або років після отримання контролю над системою чи сервером у корпоративній мережі. UEBA допомагає виявляти зміни у поведінці системи та досліджувати, чи не відбувається шкідлива активність.

Внутрішні небезпеки. Зловмисні інсайдери є серйозною проблемою безпеки, враховуючи їхню здатність уникати виявлення традиційними рішеннями безпеки. UEBA може бачити, коли користувач виконує небезпечні або підозрілі дії, включаючи передачу великих обсягів даних, підвищення привілеїв та доступ до несподіваної програми або системи, що може вказувати на зловмисну поведінку.

Бокове переміщення — зловмисник може скомпрометувати кінцеву точку або систему та використовувати її як базу для отримання доступу до інших облікових записів користувачів та систем. UEBA забезпечує комплексне представлення кількох систем виявлення аномальної активності у мережі.

Крадіжка даних – якщо хтось передає дані організації у зовнішнє джерело, це може вказувати на атаку ексфільтрації. У деяких випадках передача даних є законною, коли користувачі використовують зовнішню службу, але в інших випадках зловмисники налаштовують зловмисне програмне забезпечення для крадіжки конфіденційної інформації. UEBA аналізує передачу даних, щоб визначити, чи є пункт призначення законним, і оцінює відповідність переданих даних ролі та контексту користувача [6].

Можливості

UEBA відстежує поведінку користувачів та об'єктів організації. Він обробляє цю інформацію і вирішує, чи конкретна дія або поведінка може призвести до кібератаки. Він може знати, що таке загроза або атака і що є нормальним

використанням, тому що хоча хакер може вкрасти пароль співробітника для входу в систему, опинившись усередині, хакер не зможе імітувати «нормальну» поведінку, а UEBA може виявити цю аномальну поведінку.

UEBA може обробляти дані із загальних сховищ даних, таких як озеро даних або сховище даних, або через SIEM, який об'єднує дані з різних джерел. Він інтегрує таку інформацію, як журнали, дані захоплення пакетів та інші набори даних з існуючими системами моніторингу безпеки. Тому UEBA та SIEM часто використовуються разом, оскільки UEBA спирається на міжорганізаційні дані безпеки, які зазвичай збираються та зберігаються у SIEM.

Компонент аналітики виявляє аномалії, використовуючи різні аналітичні підходи, включаючи статистичні моделі, машинне навчання, правила та сигнатури загроз. UEBA не тільки відстежує події та пристрої, але й використовує машинне навчання для відстеження можливих загроз з боку інсайдерів. Це робиться шляхом створення «базового рівня»: звідки кінцевий користувач входить в систему, файли та сервери, які він часто використовує, привілеї, які він має, частота і час доступу, а також пристрої, що використовуються для доступу. Розширену аналітику слід використовувати у тандемі з традиційною аналітикою на основі правил та кореляції, доступною у традиційних SIEM.

Таким чином, UEBA може виявляти широкий спектр типів атак, від простих до складних, на відміну від спеціалізованих інструментів для моніторингу співробітників, моніторингу довірених хостів та шахрайства.

Оскільки UEBA може виявляти аномальну поведінку в режимі реального часу, вона може швидко видавати попередження та запитувати відповідь у аналітиків безпеки, дозволяючи їм реагувати на потенційні загрози до того, як вони стануть порушеннями. Зазвичай групам безпеки доводиться просівати оповіщення, щоб побачити, які з них є реальними загрозами, але з UEBA цей аналіз автоматизовано, і пріоритет надається лише реальним загрозам.

Існує тісний зв'язок між технологіями UEBA та SIEM, оскільки UEBA використовує для аналізу міжорганізаційні дані про безпеку, і ці дані зазвичай збираються та зберігаються у SIEM.

UEBA проти SIEM

Security Information and Event Management (SIEM) – це комплексний набір технологій, що забезпечують всебічне уявлення про профіль безпеки організації. Він використовує дані про загрози та інформацію про події, щоб допомогти групам безпеки ідентифікувати нормальні моделі та аномальні події чи тенденції. UEBA використовує аналогічний підхід, попереджаючи групи безпеки про аномалії, але додає активність користувачів та організацій у набір даних.

Коротше кажучи, SIEM фокусується на подіях безпеки, а UEBA на поведінкових шаблонах. Ще одна важлива відмінність полягає в тому, що SIEM – це рішення, яке ґрунтується на правилах. Зловмисники можуть ідентифікувати та обходити правила SIEM, щоб уникнути виявлення. Правила SIEM зазвичай спрямовані на негайне виявлення загроз, але розширені атаки можуть відбуватися протягом тривалого часу.

З іншого боку, UEBA використовує складні алгоритми та оцінку ризиків замість правил. Ці методи дозволяють UEBA виявляти підозрілу активність, якщо вона розподілена у часі. Передовою практикою IT-безпеки є об'єднання UEBA та SIEM для всебічного виявлення загроз.

Як UEBA працює з SIEM

SIEM означає безпеку інформації та управління подіями та надає організаціям засоби виявлення, аналітики та реагування нового покоління. Програмне забезпечення SIEM поєднує в собі управління інформацією про безпеку (SIM) та управління подіями безпеки (SEM), щоб забезпечити аналіз попереджень про безпеку, що генеруються програмами та мережевим обладнанням, в режимі реального часу.

Застарілі SIEM не включали аналітику поведінки, що означало, що вони не могли відстежувати загрози в режимі реального часу. І тому UEBA була розроблена для вирішення цієї проблеми. З додаванням UEBA SIEM дозволяє групам безпеки відстежувати загрози в режимі реального часу та швидко реагувати, щоб уникнути атак та усувати вразливості, що робить його набагато ефективнішим при виявленні

та аналізі загроз. Це дає групам безпеки можливість використовувати складні кількісні методи отримання інформації та визначення пріоритетів зусиль[7].

Плюси та мінуси UEBA

UEBA допомагає зміцнити систему безпеки організації, закриваючи сліпі зони, недоступні традиційним рішенням безпеки, включаючи SIEM, моніторинг користувачів та управління доступом на основі правил (RBAC). Впровадження UEBA разом з іншими інструментами безпеки допомагає підвищити їхню гнучкість, звести до мінімуму помилкові спрацьовування та виявити більш складні загрози.

Організації можуть значно підвищити рівень безпеки завдяки наступним перевагам рішення UEBA:

Автоматизований аналіз даних — інструменти UEBA збирають та обробляють великі обсяги журналів активності користувачів та об'єктів в інфраструктурі організації. Ці журнали дозволяють оцінювати ризики різних подій безпеки, заощаджуючи час та зусилля групи безпеки. Аналітики безпеки можуть пріоритизувати події безпеки з високим рівнем ризику замість того, щоб вручну аналізувати все.

Розширене виявлення загроз у режимі реального часу — звичайні інструменти моніторингу безпеки не можуть виявляти загрози так само швидко, як UEBA, що дозволяє зловмисникам завдати більших збитків організації, перш ніж вони будуть ідентифіковані та заблоковані. UEBA ідентифікує ледь помітні зміни в поведінці користувача або об'єкта до того, як вони явно порушать правила безпеки організації. Раннє виявлення може допомогти запобігти переростанню події в серйозний інцидент.

Автоматичне реагування — інструменти UEBA зазвичай сповіщають служби безпеки при виявленні підозрілої поведінки, але вони можуть автоматично блокувати загрози. Якщо це настроєно, UEBA може ініціювати автоматичну відповідь на загрозу, щоб стримати підозрілого користувача або об'єкт і зупинити атаку до того, як вона завдасть шкоди. Аналітики безпеки виграють час для розслідування інциденту.

Низькі експлуатаційні витрати — незважаючи на те, що налаштування інструменту UEBA може бути складним, після початкового налаштування потрібне мінімальне обслуговування. Як тільки рішення UEBA отримає необхідні дані, базові моделі поведінки та навчені алгоритми, воно зможе працювати автономно з мінімальним контролем з боку IT-фахівців та служби безпеки. Крім періодичного тонкого налаштування або додавання базового рівня, інструмент може автоматично адаптуватися до середовища безпеки, використовуючи свої алгоритми машинного навчання.

Розгортання та налаштування інструментів UEBA може включати кілька проблем:

Побудова базових поведінкових показників. Рішення UEBA не є готовими та потребують ретельного навчання та налаштування. Алгоритм повинен вивчити базові моделі поведінки на основі даних щодо поведінки користувачів, перш ніж виявляти загрози в реальному світі. Цей процес потребує часу (до трьох місяців), тому організаціям слід зважати на це при впровадженні рішення UEBA. UEBA ефективна як довгострокова стратегія, але не для термінових покращень.

Менш ефективне виявлення повільних атак — UEBA є найбільш ефективним, коли користувачі або об'єкти швидко змінюють свою звичайну поведінку. Наприклад, він може відразу ідентифікувати зловмисника, який скомпрометував обліковий запис або викрав дані як разового. Однак деякі атаки розвиваються повільно, особливо якщо в них беруть участь зловмисники або внутрішні зловмисники, які готують та проводять свої атаки протягом тривалого часу. Іноді ці атаки включають дуже невеликі дії, що повторюються щодня протягом декількох місяців, наприклад, передачу невеликих обсягів конфіденційних даних. Інструменти UEBA можуть розглядати такі дії як підозрілі, оскільки вони стають частиною звичайної поведінки користувача.

Необхідний досвід — навчання UEBA вимагає спеціальних навичок і знань, оскільки кожній організації потрібні набори даних, що настроюються, про поведінку користувачів. Загальні набори даних є неефективними, враховуючи відмінності в обов'язках користувачів та суб'єктів у різних організаціях. Підготовка

цих наборів даних є складною і вимагає навчання машинного навчання. Організації повинні навчати власних експертів або наймати третіх осіб для створення своїх наборів даних.

Розгортання з великими інвестиціями — використання UEBA потребує значного часу та зусиль, і кожна частина установки (конфігурація, навчання, інтеграція) пов'язана з витратами. Враховуючи складність технологій UEBA, організаціям необхідно наймати фахівців з ІІ, що збільшує вартість інструменту UEBA.

Рекомендації щодо UEBA

Після того, як організація налаштує та активує свою систему UEBA, вона може застосувати декілька принципів, щоб забезпечити хорошу роботу системи. Наведені нижче рекомендації щодо безпеки застосовуються до різних інструментів безпеки, включаючи UEBA. Те, як організація використовує ці системи, є важливим фактором підвищення безпеки, оскільки всі співробітники мають необхідні знання для забезпечення безпеки.

Навчання співробітників

Важливим фактором правильного використання систем UEBA є забезпечення того, щоб співробітники мали знання та навички, необхідні для роботи з цими системами. Організації можуть використовувати шаблон безпеки, щоб допомогти співробітникам зрозуміти важливість безпеки. Також важливо підвищувати поінформованість про безпеку та передовий досвід протягом року — це стосується систем UEBA та інших типів програмного забезпечення для безпеки.

Базовий рівень UEBA

Цілі безпеки бізнесу та належна активність користувачів є важливими міркуваннями для базового періоду. Цей період не повинен бути занадто довгим або занадто коротким — якщо базовий період закінчується занадто рано, може не вистачити часу для збору точної інформації, і кількість хибно-позитивних результатів може зрости. З іншого боку, якщо організації потрібно багато часу для отримання базової інформації, деякі шкідливі дії можуть вважатися нормальною поведінкою.

Оскільки дії користувачів та об'єктів постійно змінюються, базові дані можуть вимагати періодичного оновлення. Співробітники можуть перемикатися між ролями, проектами та рівнями привілеїв, що дозволяє їм виконувати нові дії. Організації можуть налаштувати свою систему UEBA для автоматичного збору даних та коригування базових показників у міру виникнення змін.

Передбачення внутрішніх загроз

Ця передова практика є більш специфічною для рішень UEBA — організації повинні враховувати свій загальний профіль загроз при створенні правил та політик для виявлення атак. Однією з основних переваг UEBA є його здатність ефективно виявляти внутрішні загрози так само, як і зовнішні. Однак виявлення внутрішніх загроз можливе лише в тому випадку, якщо система налаштована на пошук.

Обмеження доступу

Щоб захистити свої системи UEBA, організації повинні надати відповідному персоналу відповідні привілеї. Не всі повинні мати доступ до системи UEBA. Тільки певні члени команди повинні мати дозвіл на перегляд даних безпеки, і система повинна повідомляти лише цих осіб.

Підготовка до підвищення привілеїв

Багато організацій недооцінюють загрозу, яку становлять непривілейовані облікові записи користувачів. Зловмисники часто націлені на облікові записи з низьким рівнем доступу та використовують їх для підвищення своїх привілеїв та злому конфіденційних систем. Система UEBA допомагає виявляти несанкціоновані спроби підвищення привілеїв. Програмне забезпечення має бути налаштоване на оповіщення групи безпеки у разі виникнення інцидентів з підвищенням привілеїв[6].

2.2 Порівняльна характеристика рішень UEBA

UEBA використовує сучасні технології, такі як машинне навчання, алгоритми та статистичний аналіз, щоб створити основу для нормальної поведінки

кожного користувача. Він постійно вивчає та аналізує різні моделі поведінки користувачів та порівнює їх зі стандартними або нормальними. Як тільки він виявляє відхилення від норми, він попереджає адміністратора про аномалію. Наприклад, користувач завантажує в середньому 10 МБ даних щодня на певну робочу станцію. Якщо цей користувач раптово завантажить сотні або більше мегабайт або використовує іншу робочу станцію для виконання операції, яка зазвичай не виконується, персонал служби IT-безпеки буде повідомлено про це.

Крім аналітики поведінки користувачів, інструменти UEBA відстежують користувачів та ресурси, а не пристрої чи пристрої. подій безпеки. Він також може об'єднувати дані у звіти та журнали, які стосуються дій користувачів. Вони аналізують файли, робочі процеси та інформацію про пакети та можуть інтегруватися з іншими системами безпеки, такими як програмне забезпечення для реагування на інциденти.

Найкращі інструменти аналізу поведінки користувачів та об'єктів (UEBA)

Безпека UEBA не призначена для заміни існуючих заходів безпеки IT, а скоріше доповнює та розширює їх для більш повного охоплення. Деякі експерти вважають, що найслабшою ланкою комп'ютерної безпеки є людський чинник. Були повідомлення про те, що колишні чи нинішні співробітники крадуть дані компанії для отримання фінансової вигоди. Деякі ненавмисно встановлюють шкідливі програми або стають жертвами фішингових атак. Інструменти UEBA – це компоненти безпеки, які зменшують загрози та запобігають порушенням безпеки. Нижче наведено список рішень безпеки UEBA від провідних постачальників з помітними відгуками, сучасними функціями, можливостями інтеграції, хорошими відгуками користувачів та високим рейтингом компанії.

ActivTrak реалізує безпеку UEBA за допомогою програмного забезпечення для аналітики персоналу та моніторингу працівників. Використання глибокого аналізу даних, він розкриває, як співробітники та команди працюють, щоб надати користувачам інформацію, необхідну їм для допомоги робочій силі та організації робочого процесу. Він аналізує продуктивність робочої сили в тому числі

продуктивну поведінку, щоб встановити базовий рівень максимальної продуктивності.

Teramind – це програмне забезпечення для моніторингу комп'ютерів, яке забезпечує моніторинг активності користувачів, запобігання втраті даних та аналітику поведінки користувачів. Користувачі можуть відстежувати та контролювати дії користувачів, щоб забезпечити дотримання політик та правил. Його інструменти аналізу поведінки користувачів виявляють аномалії поведінки та виявляють потенційні загрози у режимі реального часу. Адміністратори можуть налаштовувати оповіщення та отримувати повний контрольний журнал із відеозаписом усіх дій користувача. Інші функції включають OCR, зняття відбитків пальців, виявлення контенту, автоматичне виявлення ризиків та блокування небажаної поведінки [8].

InsightIDR від Rapid7 - це комплексне рішення для забезпечення безпеки, яке включає в себе аналітику поведінки користувачів та інші функції. InsightIDR постійно відстежує здорову активність користувачів, щоб надійно виявляти зловмисників, які видають себе за співробітників компанії. Він автоматично зіставляє мережну активність з користувачами та об'єктами, щоб легко виявляти ризиковану поведінку. Інші функції включають базовий рівень машинного навчання, автоматичні оповіщення з контекстом користувача, візуальний пошук в журналах, попередньо створені карти відповідності, аналітику поведінки зловмисників, виявлення і видимість кінцевих точок, а також централізоване управління журналами.

Varonis – постачальник програмного забезпечення для забезпечення безпеки даних та виявлення внутрішніх загроз. Рішення включає інструменти для захисту даних, відповідності вимогам, виявлення загроз та реагування на них. UEBA є важливою частиною інструментів виявлення загроз. Він використовує прогностичні моделі загроз для аналізу поведінки на кількох платформах. Все це робиться автоматично, включаючи оповіщення адміністратора про потенційну атаку. Він може виявляти зараження CryptoLocker, скомпрометовані облікові записи служб та поведінку незадоволених співробітників на локальних та хмарних

платформах, таких як AD, Windows, SharePoint, Exchange, Office365, Unix/Linux, Dell EMC, HPE та Box.

Forcepoint – постачальник рішень безпеки для динамічного захисту даних, динамічного захисту кордонів та динамічного захисту користувачів. Його продукти працюють разом і можуть інтегруватися з різними існуючими середовищами. Його динамічний захист користувачів має хмарний моніторинг активності користувачів для виявлення та зупинення компрометованих користувачів. Поведінкова аналітика забезпечує контекстно-залежну оцінку ризику, яка допомагає виявляти та досліджувати ризик об'єкта майже у реальному часі. Інструмент внутрішніх загроз – це інструмент захисту та моніторингу робочої сили, який використовує глибокий збір даних та криміналістичну експертизу для підвищення прозорості дій користувачів.

Splunk User Behavior Analytics (UBA) – це інструмент UEBA, який проводить різницю між поведінкою користувача та об'єкта. Він виявляє невідомі погрози та аномальну поведінку за допомогою машинного навчання. Це дозволяє програмному забезпеченню UEBA виявляти аномалії та загрози, пропущені традиційними інструментами безпеки. Він автоматизує об'єднання кількох аномалій на єдину загрозу, щоб спростити завдання аналітиків безпеки. Глибокі можливості розслідування та базові моделі поведінки допомагають прискорити пошук загроз. UBA використовується у сфері фінансових послуг, державного сектору та охорони здоров'я [9].

Prisma Cloud – продукт Palo Alto Networks. Це комплексне рішення для забезпечення безпеки у хмарі, яке пропонує управління станом безпеки, захист робочих навантажень, управління правами на інфраструктуру та безпеку мережі. Система включає різні модулі, у тому числі виявлення мережевих аномалій і UEBA, що допомагають виявляти загрози і реагувати на них. Він поєднує в собі аналітику на основі правил та поведінки та доповнює дані з більш ніж 30 унікальних джерел для аналізу загроз. Швидко відстежуйте та відстежуйте дії користувачів, а потім отримуйте сповіщення про будь-які відхилення від встановленої нормальної поведінки за допомогою механізму UEBA на основі машинного навчання.

FortiInsight — це програмне забезпечення для аналізу поведінки користувачів та організацій, призначене для виявлення та запобігання внутрішнім загрозам. Він захищає користувачів, постійно відстежуючи користувачів та кінцеві точки з можливостями автоматичного виявлення та реагування. Машинне навчання та розширена аналітика автоматично виявляють невідповідну, підозрілу чи аномальну поведінку. Система швидко повідомляє адміністраторів про будь-які скомпрометовані облікові записи користувачів. Він може захистити конфіденційні та цінні дані від втрати, крадіжки та неправильного поводження внаслідок навмисних чи випадкових дій.

IBM QRadar User Behavior Analytics аналізує дії користувачів для виявлення внутрішніх зловмисників. Програмне забезпечення визначає, чи скомпрометовано облікові дані користувача. Це інтегрований компонент платформи QRadar Security Intelligence Platform, який дозволяє аналітикам безпеки бачити небезпечних користувачів та їх аномальні дії з можливістю деталізації для реєстрації та передачі даних. Поведінкові правила та моделі машинного навчання надають додатковий контекст користувача для мережі, журналів, даних про вразливості та загрози для швидкого відображення та виявлення атак [8].

Azure Advanced Threat Protection (ATP) включає функції для моніторингу користувачів, поведінки сутностей та дій за допомогою аналітики на основі навчання. Він захищає ідентифікаційні дані користувачів та облікові дані, які зберігаються, зокрема, в Active Directory. Програмне забезпечення виявляє та розслідує підозрілі дії користувачів та складні атаки, а потім надає чітку інформацію про інциденти на тимчасовій шкалі для швидкого сортування та виправлення. За словами Microsoft, імена можуть змінитися в найближчому майбутньому, але ATP - це рішення для захисту локальних посвідчень для запобігання, виявлення та розслідування загроз.

Gurucul User and Entity Behavior Analytics (UEBA) використовує моделі машинного навчання на великих даних із відкритим вибором для виявлення невідомих загроз на ранніх етапах ланцюжка знищення. UEBA забезпечує реалістичний підхід до всебічного управління та моніторингу ризиків, пов'язаних з

користувачами та об'єктами. UEBA виявляє аномальну активність, максимізуючи своєчасну реакцію на інцидент або автоматизоване реагування на ризики. Діапазон варіантів використання Gurucul UEBA робить рішення розширюваним та цінним. Основна увага приділяється виявленню ризиків та загроз, що виходять за рамки можливостей сигнатур, правил та шаблонів.

Використовуючи великі дані, Gurucul надає поведінкову аналітику на основі ризиків, надаючи оперативну інформацію для груп безпеки з низьким рівнем помилкових спрацьовувань. Ми використовуємо більшість готових джерел даних та використовуємо найбільшу бібліотеку машинного навчання. Крім того, він забезпечує єдину уніфіковану оцінку ризику з пріоритетом для кожного користувача та об'єкта. Зрештою, рішення призначене для того, щоб допомогти користувачам знаходити погрози – невідомі невідомі – швидко, без ручного пошуку погроз та налаштування, та отримувати результати без написання запитів, правил чи підписів [9].

2.3 Особливості роботи з GURUCUL UEBA

Оскільки кібератаки продовжують зростати як за кількістю, так і складністю, а ставки зростають у міру розширення поверхонь загроз, організації знаходяться під сильним тиском, щоб захистити себе від компрометації. Лідери безпеки стикаються з постійною проблемою, пов'язаною з хакерською тактикою, що постійно розвивається, яка легко вислизає від сигнатур, правил і шаблонів у традиційних системах кіберзахисту. Ще більше ускладнює завдання необхідність захисту гібридних середовищ на підприємстві та у хмарі.

У відповідь компанії збільшили свої бюджети на безпеку та впровадили досконаліші засоби захисту. Одним із компонентів цих захисних маневрів є створення репозиторію великих даних, що містить агреговані дані з численних джерел усередині підприємства та за його межами. Серед джерел - журнали пристроїв, дані про дії користувачів, дані про конфігурацію пристроїв, системи керування ідентифікацією, канали аналізу загроз та багато іншого. Часто у цьому

величезному сховищі даних приховані критично важливі індикатори доступу та активності потенційного зловмисника.

Зростаючий масштаб цього комплексного озера даних з повною прозорістю підприємства далеко затьмарив здатність людей досліджувати його будь-яким реалістичним способом. Тим не менш, це ідеальне джерело для моделей машинного навчання (ML), які невпинно аналізують дані та шукають кореляції та аномалії, які можуть свідчити про зловмисну діяльність.

Саме в цій галузі розширеної аналітики безпеки UEBA як частина програми виявлення загроз, розслідування та реагування стала найбільш ефективним підходом до всебічного управління та моніторингу ризиків, пов'язаних з ідентифікацією, та невідомих загроз у всіх середовищах організації. UEBA спирається на контекст великих даних і спирається на моделі машинного навчання, а не на сигнатури чи правила, щоб забезпечити неоціненну прозорість та оцінку ризику підозрілої активності.

User and Entity Behavior Analytics швидко виявляє аномальну активність, максимізуючи своєчасну реакцію на інцидент або автоматизоване реагування на ризики. Діапазон варіантів використання — те, що робить рішення UEBA розширюваним і цінним. Щоб організації могли ефективно справлятися зі своїми проблемами кібербезпеки, вони повинні переконатися, що варіанти використання відповідають їхнім конкретним потребам та різноманітним вимогам сьогодні та в майбутньому.

Gurucul надає повний набір варіантів використання для аналітики поведінки користувачів та організацій, включаючи:

– Раннє виявлення програм-вимагачів
– Виявлення фішингу
– Запобігання зловживанням привілейованим доступом
– 3-й партнер та моніторинг загроз ланцюжка поставок
– Ексфільтрація даних, DLP та захист IP
– Виявлення компрометації облікового запису, захоплення та спільного використання

- Інсайдерський моніторинг ризиків та загроз
- Моніторинг аномальної активності
- Виявлення компрометації хоста/пристрою
- Виявлення бічного руху
- Розвідувальний моніторинг
- Ідентифікація неправильної конфігурації безпеки

Хоча розгортання UEBA зазвичай починається з одного або двох варіантів використання, рекомендується розробити план майбутніх проектів для різних відділів. Сьогодні аналітики Центру управління безпекою (SOC) можуть переважно займатися аналізом інцидентів, проте завтра переваги автоматизованого реагування на ризики між рішеннями безпеки можуть стати основною вимогою.

Хоча розрізнені рішення щодо безпеки можуть мати власні аналітичні можливості, агрегування даних у великому озері даних має велике значення для підтримки кореляції інформації між джерелами даних. У міру того, як поточні інновації розширюватимуться завдяки більш широкому впровадженню, лідери в галузі безпеки поглиблюватимуть своє розуміння того, як розширена аналітика безпеки покращує виявлення та реагування. У цьому технічному документі розглядається комплексний та оптимальний набір сценаріїв використання UEBA [10].

3 ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ GURUCUL UEBA

3.1 Розроблення рекомендацій щодо застосування GURUCUL UEBA для виявлення вразливостей

Для UEBA аналітика — це науковий процес перетворення даних щодо поведінки користувачів та об'єктів в аналітику з пріоритетом ризику для стимулювання ділових дій. Ця програма науки про дані для створення базових показників поведінки користувачів та об'єктів на основі історії доступу та активності. Після встановлення базових показників поведінки (на основі історичних даних щонайменше за 3 місяці) він починає використовувати аналітику для моніторингу поведінки користувачів та об'єктів у режимі реального часу з метою прогнозування та виявлення аномальної активності. Ключовим моментом тут є режим реального часу: аналітика опрацьовує величезні обсяги даних і дає уявлення про те, що насправді відбувається з користувачами та об'єктами у вашій організації, як це відбувається. Результатом аналітики безпеки є єдина оцінка ризику кожного користувача та об'єкта.

Приклад. Користувач входить до системи о 9-й ранку в понеділок. Оцінка ризику цього користувача дорівнює 10. Оцінки ризику варіюються від 1 до 100, де 100 – найвищий рівень ризику. Оскільки цей користувач повторює вхід в систему щодня о 9-й ранку, його оцінка ризику змінюється з 10 до 9 і 8, оскільки він демонструє послідовну поведінку. Але коли він входить в систему опівночі, його оцінка ризику підскакує, тому що це аномальна поведінка для цього користувача. Зважаючи на всю його іншу онлайн-активність — додатки, до яких він зазвичай звертається, файли, з якими він працює, людей, яким він надсилає електронні листи, що роблять його колеги і т. д. — аналітика може почати малювати картину того, наскільки ризикованою є ця діяльність цього користувача. Аналітика отримує

потоки даних про доступ та дії з кількох джерел для кожного користувача та об'єкта та генерує оцінки ризику для кожного в режимі реального часу на основі поведінки.

Вхідними даними для UEBA-аналітики є дані про доступ та активність. Обчислювальна потужність для аналітики UEBA – це моделі машинного навчання та наука про дані. Результатом аналітики UEBA є аналітика із пріоритетом ризику (оцінка ризику).

Чим більше даних проаналізовано, тим краще. Ключ у тому, щоб переглянути всі можливі канали доступу та активності, щоб ви могли з'єднати точки. Отже, з'єднання між додатками, системами, групами, пристроями тощо для ефективного викорінення дійсно ризикованої аномальної поведінки. Якщо хтось входить у систему опівночі, чи виконує ця людина оновлення системи? Чи його обліковий запис було скомпрометовано, і це спроба крадіжки даних? Вивчення контексту у всьому середовищі — єдиний спосіб виявити справді аномальну поведінку.

Нижче наведено деякі типи даних, які Gurucul UEBA може приймати: репозиторій документів, захист від втрати даних (DLP), автентифікація, системи управління вихідним кодом, дані системи управління персоналом та адміністрування, дані мобільних обчислень, дані мережі та інфраструктури, дані з інформаційної події безпеки. Системи управління (SIEM), системи контролю доступу (бейджинг), дані з хмарних додатків, дані із систем баз даних, дані каталогів та LDAP, дані VPN, дані із файлових систем зберігання, дані із систем управління ідентифікацією, дані із систем управління привілейованим доступом , системи загроз та вразливостей, дані соціальних мереж, системи управління справами, дані EMR та HER, а також фінансові дані.

Машинне навчання.У міру надходження даних аналітика використовує алгоритми машинного навчання обробки даних у режимі реального часу. Gurucul UEBA використовує ряд аналітичних методів та моделей машинного навчання для прогнозування та виявлення загроз, у тому числі: аналіз посилань (Soundex, Fuzzy Logic), аналіз ознак (аналіз основних компонентів), аналіз поведінки (контрольований, неконтрольований, напівконтрольований, глибоке навчання). , байєсовська мережа, аналіз настроїв, класифікація), аналіз однорангових груп

(кластер, K-середні), аналіз викидів (LOF, K-NN) та оцінка ризику (розпад, базельський індекс).

Результатом аналітики є інформація, яка орієнтована на ризик. Аналітика – це математика та наука, які дозволяють приймати виважені рішення на основі даних. І ці рішення можуть бути автоматизовані та організовані задля досягнення оптимального ефекту в середовищі, де переглядаються мільйони подій (або дій) за секунду [11].

Механізм управління ризиками Gurucul використовує різні фактори для розрахунку оцінок ризику, включаючи історичну поведінку, контекст користувача на декількох ресурсах, тип аномалії, рівень доступу, рейтинги ризику ресурсів і моделей і т. д., щоб агрегувати оцінки і забезпечити раннє вказівку ризику, що забезпечує можливість прогнозування. .

Вся справа в управлінні ризиками та ухваленні рішень з урахуванням ризиків у світі, де загрози нульового дня можуть вивести з ладу цілі мережі за лічені секунди. Машинне навчання та розширена аналітика безпеки дозволяють аналізувати великі обсяги даних. Крім того, прогнозувати аномальну поведінку, яка може допомогти запобігти великомасштабному шахрайству та виявити невідомі погрози

Ключем до прогнозування загроз, особливо невідомих загроз, є моніторинг поведінки користувачів та об'єктів, щоб розпізнати, коли ця поведінка починає бути аномальною.

Якщо для офісу або будівлі потрібен доступ з перепусткою, створюється контрольний журнал щоразу, коли проводите перепусткою. Моделі машинного навчання, що лежать в основі UEBA, здатні виявляти зміни у часі прибуття та відправлення. Так само час, проведений в офісі або за обідом, навіть перерви, якщо офіс захищений системою доступу за допомогою карти-ключа. Крім того, якщо використовується ключ-карта для входу до офісу, а потім здійснюється вхід з віддаленого місця з невизнаною IP-адресою, UEBA пов'язує ці дії та позначає їх як аномалію. Користувач не можете одночасно перебувати в офісі та працювати віддалено.

Зв'язування даних про поведінку користувачів з фізичної системи бейджів та журналу безпеки Windows – єдиний спосіб встановити цю конкретну аномалію, тому найкращі продукти UEBA приймають найрізноманітніші потоки даних.

Щоб передбачити невідомі загрози, UEBA досліджує все, що роблять користувачі та об'єкти в режимі реального часу, потім збирає, зіставляє та пов'язує ці дані для виявлення аномалій. До цих об'єднаних та нормалізованих даних застосовується ціла бібліотека алгоритмів машинного навчання та аналітики, тому що люди не можуть виявити зміни в моделях поведінки в такому масштабі [12].

Gurucul UEBA створює поведінковий базовий рівень, використовуючи атрибути профілювання з різних джерел даних, таких як HR-записи, події, репозиторії доступу, рішення для управління журналами, NetFlow та багато іншого. Gurucul UEBA виявляє відхилення від встановлених шаблонів. В результаті він може швидко сповіщати про внутрішні загрози, скомпрометовані облікові записи, атаки грубої сили, зміни дозволів, витоки даних тощо.

Gurucul UEBA може витягувати журнали з централізованих агрегаторів журналів, систем EDR, потокової передачі системних журналів, WMI, завантажувати файли з підключень NAS або агентів платформи, які збирають та пересилають журнали Gurucul UEBA. Він використовує різні елементи даних та події, такі як виконані команди, створені або запущені процеси, доступ до файлової системи, оповіщення IDS/IPS/AV/DLP і т. д., щоб виявити підозрілу/зловмисну поведінку, яка не є нормальною дією для користувача чи об'єкта (машини).) з урахуванням минулого поведінки. Gurucul UEBA надає оцінку ризику кожному користувачеві та об'єкту, для яких виникають аномалії. Оцінки ризиків разом із метаданими аномалій, такими як дані про ресурси та події, можна використовувати для ініціювання відповідних дій з виправлення. Gurucul UEBA підтримує інтеграцію на основі API із рішеннями превентивної безпеки. Тому, маючи можливість блокувати,

Gurucul UEBA надає понад 200 готових роз'ємів для більшості стандартних комерційних платформ. Він також надає власну платформу Flex-Connector Framework, яка дозволяє клієнтам швидко створювати та налаштовувати

універсальний з'єднувач. Gurucul підтримує потокові, плоскі файли (CSV, XML, JSON), бази даних, з'єднання LDAP та API. Таким чином, дозволяючи клієнтам підключатися практично до будь-якого джерела даних. Gurucul UEBA можна також налаштувати для отримання даних про активність у вигляді потоку в режимі реального часу. Це включає налаштування відповідних портів і прослуховувача для отримання потокових даних. Потім обробіть потік неструктурованих даних тим самим способом, що й обробки файлів неструктурованих даних.

Однією з найбільших проблем більшості сучасних організацій є їхня нездатність остаточно пов'язати подію з конкретним обліковим записом користувача. Gurucul вирішує цю проблему, роблячи метадані облікового запису користувача/пристрою найпершим входом до своїх систем. Профілі облікових записів користувачів та об'єктів можуть бути створені за допомогою журналів розрізнених систем, таких як брандмауери, антивіруси та DLP. Gurucul поєднує в собі ідентифікацію та мережеве сповіщення, щоб озброїти команди SOC комплексною картиною інциденту, щоб відповісти на основні питання, такі як:

Який обліковий запис користувача викликав інцидент?

Це від якого пристрою?

З якої частини мережі це було?

Хто є власником пристрою/підмережі?

Чи поведінка цього облікового запису користувача є нормальною порівняно з одноранговими обліковими записами?

На додаток до моніторингу того, як посвідчення використовуються та керуються, слід вивчити інші важливі джерела даних у обчислювальному середовищі організації, щоб надати більше контексту, крім того, хто та що. Приклади джерел даних включають доступ до мережі, дані про події та потоки, дані DLP, системні журнали, дані сканування вразливостей, файли журналів з IT-додатків, записи відділу кадрів тощо. У багатьох випадках ці дані вже можуть бути об'єднані в журнал управління подіями чи SIEM. Рішення. Цей великий масив даних у поєднанні з інформацією про те, як посвідчення використовуються як людьми, так і машинами, створює багате джерело контексту, яке можна отримати

за допомогою аналізу загроз та виявлення аномалій. Коли далі розглядається ідентичність як площина загроз, сотні атрибутів можуть стати моделями в алгоритмах машинного навчання для прогнозування та запобігання загрозам безпеці [12].

Злом облікового запису відбувається, коли адреса електронної пошти стає метою зловмисника. Потім хакер використовує скомпрометований обліковий запис електронної пошти, щоб видати себе за користувача, власника облікового запису. Обліковий запис електронної пошти пов'язаний із низкою онлайн-сервісів, включаючи соціальні мережі та банківські рахунки. Хакер використовує облікові дані для отримання особистої інформації та створення нових облікових записів з кінцевою метою виконання транзакцій для отримання фінансової вигоди. Це відбувається дуже швидко.

Найефективніший спосіб знайти зламані облікові записи – використовувати аналітику поведінки користувачів та організацій (UEBA), тому що можна вкрасти особистість, але не можна вкрасти поведінку.

Насамперед, найбільш поширеними методами, які хакери використовують для захоплення облікових записів, є фішинг, підбір пароля, шкідливе програмне забезпечення, шкідлива реклама та реєстрація натискань клавіш. Зловмисники також використовують уразливості за допомогою таких атак, як Pass-the-Hash (PtH), грубої сили та віддаленого виконання, щоб отримати доступ до облікових даних користувача. Неймовірно, але фішинг залишається одним з найпоширеніших методів крадіжки акаунтів.

Існує чотири типи фішингових тактик, що використовуються при захопленні облікового запису. Кожен з них є нетрадиційним елементом управління, який вселяє довіру до електронної пошти, а не знижує довіру, навчаючи користувачів не довіряти електронній пошті. Таксономія фішингових листів зазвичай включає:

Підміна домену: це включає відправлення електронної пошти, яке виглядає як вихідне від законного та надійного домену електронної пошти.

Схожі домени: це зареєстровані домени, які виглядають як популярні та відомі домени, але часто мають одну літеру, яку користувач не дізнається під час читання повідомлення електронної пошти.

Обман відображуваного імені: ця тактика включає створення повідомлень електронної пошти з підробленим ім'ям відправника, зазвичай це хтось, кого ви знаєте, наприклад, ваш бос або генеральний директор.

Скомпрометовані облікові записи електронної пошти: цей метод є найбільш швидкозростаючою тактикою на сьогоднішній день через мільярди скомпрометованих облікових даних від провайдерів електронної пошти, які були зламані. Фішингові електронні листи надходять із законних облікових записів електронної пошти та поштових доменів, яким довіряють фільтри спаму та фішингу, і, у свою чергу, електронна пошта доставляється нічого не підозрюючому кінцевому користувачеві. Ця тактика є найбільшою проблемою для підприємств сьогодні [11].

Важливість UEBA для виявлення злому облікового запису

Одна з 10 основних уразливостей OWASP (Open Web Application Security Project) пов'язана зі сценарієм «Порушена автентифікація та керування сеансом». В результаті саме тут хакери використовують Pass-the-Hash (PtH), Pass-the-Token (PtT), Brute Force та Remote Execution для отримання доступу до облікових даних користувача (паролі та хеш). Такі атаки можна знайти за допомогою базових алгоритмів машинного навчання UEBA. Вони забезпечують перевірку різних параметрів, таких як мітка часу, розташування, IP-адреса, пристрій, шаблони транзакцій, коди подій з високим рівнем ризику та мережні пакети. Налаштуйте їх, щоб визначити будь-яке відхилення від нормальної поведінки. Це може бути конкретний рахунок та відповідні транзакції.

Це полегшує виявлення будь-яких потенційних сценаріїв захоплення облікового запису або компрометації облікового запису на основі аномальних моделей поведінки, таких як: аномальний доступ до об'єктів з високим ризиком або конфіденційним об'єктам, аномальна кількість дій, запити в короткі терміни, активність з віддалених облікових записів користувачів або бездіяльних облікових

записів. , атаки PtH та атаки відтворення сеансу. Аномалії, виявлені за допомогою кластеризації моделей машинного навчання та аналізу викидів, несумісних із нормальною поведінкою користувача чи колег, отримують оцінки ризику на основі прогнозної аналітики для управління попередженнями, діями та запитами.

Переваги:

Виявляє аномальну поведінку, що виходить за рамки правил, шаблонів та сигнатур, для компрометації, захоплення та обміну обліковими записами.

Забезпечує 360-градусну видимість облікових записів користувачів, доступу та дій у локальних, хмарних та гібридних середовищах.

Варіант використання UEBA для відстеження сеансів з відстеження стану

У цьому випадку UEBA створює та відстежує стан сеансу користувача. Це відбувається навіть тоді, коли користувач переміщається різнорідними ресурсами. Це також стосується програм, які використовують різні облікові записи та пристрої в різний час. Використовуючи машинне навчання, UEBA динамічно створює атрибути кореляції сеансу, які використовуються для створення контексту сеансу, щоб зв'язати будь-які наступні дії на основі достовірності. Це дозволяє ідентифікувати дійсне перемикання IP-адрес через переходи між дротовими та бездротовими мережами, робочою станцією і портативним/мобільним пристроєм або доступу до корпоративних ресурсів з різних місць на місці або віддалено через VPN.

UEBA має можливість відстежувати сеанси користувачів за цими різними параметрами. Таким чином, забезпечується значне скорочення помилкових спрацьовувань при одночасному покращенні видимості послідовності подій. Він також надає можливість деталізувати конкретні дії, які виконує користувач або об'єкт під час проведення розслідування. Цей аналіз також прискорює виявлення повторів сеансів та атак перехоплення. Він починає виділяти будь-яку аномальну активність з сеансу користувача або одночасних сеансів з того ж облікового запису.

Забезпечує більшу видимість дій користувача в кількох ресурсах або програмах завдяки відстеженню сеансів з відстеженням стану.

Надає детальні та необроблені журнали для глибокого аналізу подій у джерелі.

Зменшує кількість помилкових спрацювань через поширені сценарії, такі як перемикання IP-адреси, облікового запису та пристрою під час виконання повсякденних дій.

Виявляє повтор сеансу та атаки перехоплення.

Компрометація хмарного облікового запису, злом та спільне використання UEBA.

Cloud Security Analytics усуває компрометацію хмарних облікових записів, зламування хмарних облікових записів та спільне використання хмарних облікових записів за допомогою інтеграції API з програмами SaaS, а також IaaS та PaaS. Прозорість хмарних програм Office 365 використовує видимість Microsoft Azure для інформації про хмарну інфраструктуру та платформу поряд з даними про активність хмарних програм. Те саме стосується й інших популярних хмарних програм у хмарних середовищах AWS. Більше того, управління ідентифікацією та доступом як послуга (IDaaS) також відіграє роль для хмарного середовища.

У гру входять переваги інфраструктури великих даних із гнучкою моделлю даних. Вони розробляють з'єднувачі даних API для прийому хмарних даних, які можуть багато в чому імітувати локальні функції. Крім того, використовуючи передові моделі поведінки машинного навчання, хмарна аналітика безпеки використовує цю можливість для хмарних середовищ для виявлення компрометації облікових записів, захоплення та спільного використання у локальному середовищі. Основні концепції алгоритмів кластеризації та викидів для пошуку аномалій на основі нормальних базових показників користувача та колег для оцінок прогнозованого ризику залишаються сумісними з поправками на різноманітність та якість даних. Джерела даних відрізняються, а прийом даних для хмарного середовища здійснюється на основі API.

Виявляє компрометацію облікових записів, захоплення та спільне використання облікових записів хмарних додатків та привілейованих облікових записів для IaaS, PaaS та IDaaS.

Виявляє аномальну поведінку крім правил, шаблонів та підписів для компрометації хмарного облікового запису, захоплення та обміну

Поєднує хмарну аналітику безпеки з локальною аналітикою безпеки для забезпечення видимості гібридного середовища на одній платформі UEBA.

Внутрішня загроза – це зловмисна загроза організації, що виходить зсередини: співробітники, колишні співробітники, ділові партнери чи підрядники. У цих осіб є внутрішня інформація про методи забезпечення безпеки, інфраструктуру та дані організації. Існує три типи внутрішніх загроз: помилка користувача, зловмисний інсайдер та скомпрометований обліковий запис. рішення UEBA надає моделі з прогнозуючими намірами виявлення зловмисних внутрішніх дій. Він виявить сценарії злому облікового запису, такі як атаки методом грубої сили, підозріле скидання пароля, спільне використання облікового запису, використання облікового запису з незвичайного пристрою або місця розташування тощо. або сканування файлів, коли зловмисник намагається отримати доступ до кількох ресурсів, щоб отримати доступ до коштовностей організації (IP, конфіденційна інформація, дані клієнтів тощо). Моделі також виявляють будь-який несанкціонований доступ до конфіденційних даних PII/PCI або незвичайні/надмірні завантаження даних, а також спроби ексфільтрації через друк, електронну пошту, хмарне сховище або USB-пристрій [12].

Реальна цінність рішення UEBA полягає у його здатності виявляти не тільки відомі загрози, але й невідомі загрози на основі поведінки користувача та об'єкта. UEBA реалізує інноваційні методи обробки даних та аналітики на основі машинного навчання, орієнтовані на виявлення загроз, які обходять традиційні системи виявлення та запобігання. Алгоритми машинного навчання дозволяють використовувати автоматичні та масштабовані способи отримання інформації з великих багатовимірних даних. UEBA використовує різні моделі з використанням контрольованих, неконтрольованих та напівконтрольованих алгоритмів. Він також використовує передові методи, такі як глибоке навчання та аналіз тексту для аналізу настроїв з метою виявлення внутрішніх загроз.

В рамках моделювання механізм аналітики створює базові профілі поведінки для кожного посвідчення (користувача та об'єкта), визначеного в системі, а потім запускається в режимі прогнозування для виявлення будь-яких відхилень від базового рівня або базового рівня групи однолітків. Виявлення викидів у поєднанні з контекстуальною інформацією, як-от канали Threat Intelligence та оповіщення, що генеруються зовнішніми системами, забезпечує загальну оцінку з пріоритетом ризику для кожного посвідчення, яку можна використовувати для подальшого розслідування інциденту.

Журнали

Джерела журналів надають контекст, необхідний алгоритмам машинного навчання створення інтелектуальних вихідних даних. І з'єднання точок у різних даних журналу – це те, як UEBA забезпечує цінність. Як спрощений приклад припустимо, що Джеррі Браун повинен використовувати сканер перепусток, щоб потрапити до свого офісу:

О 8:50 система сканування бейджів фіксує, що Джеррі використовує свій бейдж, щоб увійти до офісу.

Також о 8:50 журнали VPN показують, що Джеррі Браун входить до корпоративної мережі з віддаленого місця.

Джеррі не може одночасно перебувати в офісі та віддалено підключатися до мережі.

Об'єднання даних журналів з обох систем – єдиний спосіб виявити цю аномальну активність VPN.

Якби журнали системи фізичних перепусток були недоступні, ця подія компрометації облікового запису могла б залишитися непоміченою.

Кластеризація та модель K-Means ML

Модель машинного навчання Clustering and K-Means групує дані у кластери. Він переглядає різні змінні, щоб визначити, хто має до чого доступ. Він переглядає журнали активності, атрибути HR та моделі поведінки. Він також розглядає доступ: чого мають доступ користувачі? До чого повинні мати доступ? Gurucul UEBA використовує цю модель для виявлення стороннього доступу.

Gurucul використовує Clustering та K-Means для того, що ми ласкаво називаємо Dynamic Peer Grouping. Це механізм виявлення динамічних кластерів з використанням даних у реальному часі та короткострокових груп даних. Gurucul UEBA реалізує певні групи однорангових вузлів за допомогою машинного навчання для неконтрольованих та контрольованих алгоритмів. Це кластери користувачів, розміщені в декількох суміжних групах на основі атрибутів, отриманих за допомогою аналітики, а не просто на основі статичних атрибутів користувачів або облікових записів. Прикладом може бути: все у супермаркеті о 10:00 у суботу. Статичною групою будуть працівники супермаркету у суботу вранці, оскільки вони відомі як члени цієї групи. Динамічна однорангова група складатиметься з покупців та співробітників, оскільки покупці динамічно додаються до групи у міру здійснення покупок.

Gurucul обчислює базові показники поведінки для динамічних однорангових груп та використовує їх для порівняльного розрахунку викидів, коли член динамічної однорангової групи виконує аномальні події. Скажімо, хтось грабує супермаркет — це незвичайна та ризикована поведінка.

Кластеризація та метод K-Means можуть використовуватися для традиційного аналізу ролей – для очищення доступу шляхом забезпечення додаткової видимості використовуваного доступу. Середньостатистичний користувач має більше 100 дозволів, і управляти ними вручну може бути дуже складно. Завдяки використанню моделі машинного навчання Clustering та K-Means ми можемо виявляти викиди доступу, аналізуючи, що відбувається з динамічними одноранговими групами користувачів.

Приклад. Недільний день дані доступу компанії показують, що співробітник відділу IT працює над вашою системою виробничих фінансів. Це незвичайна дія для IT-співробітника, оскільки для людини в цій ролі нетипово отримувати доступ до системи виробничого фінансування, тим більше в неділю вдень. Чи це заняття є ризикованим? Допустимо, що є бізнес-аналітик, який працює з однією і тією ж системою виробничих фінансів в один і той же час.

Якщо розглянути ці дві дії окремо, можна помітити проблему. Проте, якщо динамічно поєднаєти ці дві точки доступу до даних, ситуація може виявитися менш ризикованою. Швидше за все, у цьому сценарії ці співробітники працюють разом, щоб виконати оновлення системи або вирішити проблему виробничої. З реальної точки зору, коли можна вивчити традиційні атрибути статичних даних, такі як посада чи номер відділу, ці співробітники не вважатимуться релевантною групою однолітків. З точки зору поведінкової аналітики, ці співробітники складають динамічно створювану групу однолітків, оскільки в систему записуються дані про їхні дії щодо одночасного доступу до однієї і тієї ж системи виробничих фінансів.

Динамічні однорангові групи - це кластери користувачів, які створюються у міру того, як Gurucul UEBA отримує дані журналів майже в реальному часі, і всі вони є внутрішніми для алгоритмів машинного навчання. Динамічні однорангові групи є досить тимчасовими, але їх можна зберегти для подальшого використання. Використовуючи машинне навчання Clustering та K-Means, а також застосовуючи технологію динамічного угруповання однорангових вузлів, Gurucul UEBA може вдесятеро зменшити кількість помилкових спрацьовувань порівняно з використанням статичних груп таких каталогів, як Active Directory.

Привілейовані облікові записи стають мішенню для кіберзлочинців, тому що вони надають ключі від королівства. Зловмисникам потрібні привілеї для отримання доступу до систем з конфіденційними даними, встановлення шкідливих програм, ексфільтрації даних та отримання контролю над системами та пристроями. Отримання привілейованого доступу — це сенс спроб корпоративного злому. Основним варіантом використання User and Entity Behavior Analytics (UEBA) є виявлення та запобігання зловживанням привілейованим доступом. Це може бути зловмисник, який отримує доступ до важливих систем зі скомпрометованим обліковим записом, або привілейований користувач, який зловживає наявним доступом. У будь-якому випадку моніторинг поведінки привілейованих облікових записів та користувачів є ключем до забезпечення безпеки цих цінних активів.

Щоб заборонити привілейованим користувачам переглядати та красти дані або IP-адреси, вам необхідно визначити їхню поведінку таким чином, щоб будь-яке відхилення піднімало червоний прапор — або, у випадку Гурукула, оцінку ризику користувача. Використовуючи комбінацію облікових записів, доступу та даних про активність, Gurucul UEBA може виявляти зловживання привілейованим доступом (HPA).

Gurucul отримує дані про діяльність із джерел аудиту чи журналів на рівні підприємства (наприклад, SIEM чи агрегаторів журналів) або отримує їх безпосередньо з цільових джерел даних. Як тільки облікові записи HPA ідентифіковані, UEBA може виявити підозрілу поведінку та неправомірне використання, наприклад: використання HPA для призначення особливих або підвищених привілеїв власного облікового запису користувача з подальшою дією. Він може виявляти транзакції, що відбуваються за межами вікна перевірки пароля привілейованого облікового запису та тимчасових рамок реєстрації. Він визначає, коли привілейовані користувачі отримують доступ до ресурсів і виконують транзакції за межами звичайних профілів поведінки, ненормально отримують доступ до секретних або конфіденційних документів або виконують кілька одночасних сеансів з одного і того ж облікового запису, з різних IP-адрес, пристроїв, розташування та т.д.

Gurucul UEBA може зловити системних адміністраторів у процесі підвищення привілеїв свого або чужого облікового запису в хмарі та визначити, де вони зловживають цими привілеями. Він може зловити адміністраторів Google G-Suite, які створюють облікові записи, підвищують привілеї та роблять загальнодоступними документи компанії, щоб вони були доступні для скачування будь-ким і будь-де.

Gurucul UEBA може ідентифікувати та надсилати оповіщення, коли системні адміністратори виявляють, що вони запускають незатверджені програми. Gurucul UEBA досліджує та класифікує веб-трафік. Коли незатверджена програма запускається під обліком неавторизованого користувача, ця подія позначається. За бажання можна надіслати повідомлення. Таким чином, Gurucul UEBA може

швидко визначити, коли системний адміністратор запускає незатверджену програму. Це може попередити вашу слідчу групу про необхідність вжити заходів для запобігання можливому пошкодженню критично важливих даних компанії [12].

3.2 Застосування технології Gurucul User and Entity Behavior Analytics

Раннє виявлення програм-вимагачів

Програми-вимагачі відомі тим, що шифрують файли користувачів, незалежно від того, мають ці файли сенс чи ні. Що ще важливіше, програми-вимагачі — це торговий інструмент супротивника, зброя, яку можна використати на будь-якому привабливому ресурсі. Розширені атаки програм-вимагачів здебільшого націлені на шифрування документів і ресурсів з високою ставкою, таких як MySQL dB, і зловмисники нерідко отримують доступ за допомогою таких тактик як фішинг або атаки з проїздом. Виробники NGAV випустили програмне забезпечення, що використовує канаркові файли, будь то загальносистемні файли фактичних даних або спеціальні неправдиві цілі. Більш інтелектуальне програмне забезпечення для захисту від програм-вимагачів перевіряє наявність змін, виявляє будь-які зміни заголовків файлів, зроблені за допомогою симетричного шифрування AES і вчасно знищує шкідливий процес. Однак це лише гонка з часом, і хто переможе в цій гонці програм-вимагачів?

Якщо поставити запитання, більшість директорів з інформаційної безпеки, як і раніше, мають серйозні проблеми з виявленням програм-вимагачів та захистом від них. Це з характером самої атаки. Наприклад, якщо зловмисник вирішить отримати ключ шифрування AES через той самий доступ, який він або вона спочатку ввели, і скопіює їх на хост-жертву, або якщо він має намір отримати ключі після того, як вони досягли певного ресурсу. Обидві ці дії будуть ключовою точкою виявлення, і в областях поведінкової аналітики обидві будуть ідентифіковані як неприродні моделі поведінки. Багато інших факторів також вступають у гру, наприклад, користувач, від якого було створено хост, нерегулярне використання

протоколів, незвичайну мережу та файлову активність — все це вказує на ненормальну поведінку.

Виявлення фішингу

Фішинг - це провідний метод соціальної інженерії, який зловмисники або кіберзлочинці використовують для отримання доступу до облікових даних законного користувача. Отримавши ім'я користувача та пароль співробітника, зловмисник може безпосередньо увійти до мережі та отримати ті самі привілеї, що і цей користувач. Щоб запобігти захопленню облікового запису, важливо зупинити фішинг у джерелі — у поштових скриньках законних користувачів або раніше.

UEBA аналізує активність вхідних повідомлень фішингової кампанії, щоб виявити незвичайну поведінку, що свідчить про шкідливу електронну пошту. UEBA шукає атрибути, такі як незвичайні домени електронної пошти відправника, вхідні електронні листи від схожих відправників велику кількість внутрішніх користувачів, незвичайну послідовність символів на основі інтелектуального аналізу тексту та попередньо навчене виявлення у довірених рядках теми. Оповіщення про ці дії, а також автоматичні відповіді, які ізолюють підозрілі повідомлення можуть допомогти обмежити фішинг в організації [13].

Запобігання зловживанням привілейованим доступом

Цей варіант використання виявляє зловживання високопривілейованим доступом (HPA) шляхом використання комбінації облікових записів, доступу та даних про активність. Як правило, облікові записи та дані доступу надходять з платформ управління ідентифікацією (IAM), управління привілейованим доступом (PAM) та/або служб каталогів для ідентифікації облікових записів HPA та виявлення будь-яких облікових записів, що не належать HPA, яким надано високі привілейовані права. Крім того, дані про діяльність приймаються із джерел аудиту чи журналів на рівні підприємства або виходять безпосередньо з цільових джерел даних.

Як тільки облікові записи HPA ідентифіковані, UEBA може виявити підозрілу поведінку та неправомірне використання, наприклад, використання HPA для призначення спеціальних або підвищених привілеїв власного облікового

запису користувача з подальшою дією або транзакціями за межами вікна перевірки значення пароля та часу перевірки. Це також включає доступ до ресурсів і транзакцій за межами звичайних профілів поведінки, ненормальний доступ до секретних або конфіденційних документів і кілька одночасних сеансів з одного і того ж облікового запису з використанням різних IP-адрес, пристроїв, розташування і т.д.

3-й партнер та моніторинг загроз ланцюжка поставок

Завдяки розумінню сторонніх засобів управління доступом, політик привілейованого доступу та аналізу мережевого трафіку UEBA може виявляти підозрілу поведінку та неправомірне використання. Це включає використання стороннього доступу для призначення спеціальних або підвищених привілеїв власного облікового запису користувача з подальшою дією або транзакціями за межами вікна перевірки значення пароля та тимчасових рамок реєстрації. Він також може знаходити незвичайні підключення та трафік від недіючих та рідко використовуваних або навіть сторонніх сторін, які вже навіть не є активними партнерами. UEBA – це найбільш ефективний спосіб виявити початкову компрометацію з боку третьої сторони або партнера з ланцюжка постачання. Крім того, наш повний набір аналітики посвідчень, мережі [14].

Ексфільтрація даних, DLP та захист IP

UEBA виявляє спроби крадіжки даних та захищає інтелектуальну власність, використовуючи такі джерела даних, як захист від втрати даних (DLP) та класифікація даних, щоб дізнатися про розташування важливих даних, доступ до них та активність додатків.

Основною перевагою машинного навчання UEBA є створення попереджень DLP з оцінкою ризиків, які допомагають знизити стомлюваність попереджень та розставити пріоритети щодо пошуку та усунення несправностей. Аналіз UEBA включає локальні та хмарні програми для всебічного огляду доступу до даних та активності. Цей підхід допомагає клієнтам розставляти пріоритети при розслідуванні попереджень DLP, а також виявляти і відстежувати навіть

попередження DLP з низьким рівнем серйозності, пов'язані з користувачами або користувачами з високим рівнем ризику.

Моделі неконтрольованого машинного навчання розробляють базові показники, що належать до типових схем доступу до даних, що дозволяє виявляти активність аномальних подій. Крім того, рішення UEBA традиційно надають готові моделі машинного навчання, які можуть ідентифікувати відомі шаблони, такі як завантаження та копіювання конфіденційних документів на USB-накопичувач, великі обсяги вихідного коду, вилучені з репозиторіїв вихідного коду, завантаження файлів у сховище хмари, електронні листи. до особистих кабінетів, доступ до сайтів конкурентів та/або вакансій тощо.

Організації також поширили оповіщення UEBA не тільки на аналітиків SOC, але й на менеджерів проектів, враховуючи їхню глибину контексту та актуальність щодо співробітників, даних та проектів.

Виявлення компрометації облікового запису, захоплення та спільного використання

Одна з 10 основних уразливостей OWASP (Open Web Application Security Project) пов'язана зі сценарієм «Порушена автентифікація та керування сеансом». Тут зловмисники використовують уразливості за допомогою таких атак, як Pass-the-Hash (PtH), Pass-the-Token (PtT), Brute Force та Remote Execution, щоб отримати доступ до облікових даних користувача (паролі або хеш).

Такі атаки можуть бути виявлені за допомогою базових алгоритмів машинного навчання, налаштованих на перевірку різних параметрів, таких як мітка часу, місцезнаходження, IP-адреса, пристрій, шаблони транзакцій, коди подій з високим рівнем ризику та мережні пакети для виявлення будь-яких відхилень від нормального поведінки конкретного облікового запису та відповідні угоди. Це полегшує виявлення будь-яких потенційних сценаріїв компрометації або захоплення облікового запису на основі моделей аномальної поведінки, таких як ненормальний доступ до об'єктів з високим ризиком або конфіденційними об'єктами, ненормальна кількість дій, надмірні запити за короткий проміжок часу,

активність із закритих або бездіяльних облікових записів користувачів Атаки PtH та атаки відтворення сеансу.

Аномалії, виявлені за допомогою кластеризації моделей машинного навчання та аналізу викидів, несумісних із нормальною поведінкою користувача чи колег, отримують оцінку ризику на основі розширеної аналітики безпеки для управління попередженнями, діями та запитами.

Інсайдерський моніторинг ризиків та загроз

Розширений моніторинг інсайдерських ризиків та загроз UEBA використовує дослідження, засновані на великих базах даних інсайдерських загроз реальних інцидентів, для розробки, тестування та уточнення моделей поведінки машинного навчання. Базові профілі створюються з використанням атрибутів із записів відділу кадрів, подій, репозиторія доступу, рішень для управління журналами тощо. люди не могли б розпізнати чи виявити інакше. Як множник сили, машинне навчання набагато перевершує людські можливості та розробку програмного забезпечення для управління великими обсягами та різноманітністю даних.

Справжнє машинне навчання також знаходить високорівневі взаємодії та закономірності даних для вирішення складних проблем, таких як внутрішні загрози, скомпрометовані облікові записи та ексфільтрація даних. Він робить це, використовуючи корисні та прогностичні сигнали, які надто зашумлені та багатовимірні для виявлення експертами-людьми та традиційним програмним забезпеченням.

Панель моніторингу Gurucul забезпечує видимість облікових записів, доступу та дій посвідчення для локальних та хмарних гібридних середовищ. Як доступ, так і активність оцінюються за ризиком аномальних подій, результати помітні керівникам співробітників та аналітикам SOC [12].

Моніторинг аномальної активності

UEBA виявляє та відстежує аномальну активність людей або пристроїв за допомогою алгоритмів машинного навчання, налаштованих для перевірки різних параметрів, таких як мітка часу, місцезнаходження, IP-адреса, пристрій, шаблони транзакцій, коди подій з високим рівнем ризику та мережні пакети. Цей метод може

виявити будь-яке відхилення від нормальної поведінки, яка може свідчити про небезпеку.

Наприклад, адміністратор бази даних може створити сценарій, який щодня о 2 годині ночі запускає кілька команд, що впливають на безпеку. Цей користувач – новатор, який працює над підвищенням продуктивності підприємства. Проте моделі машинного навчання розглядатимуть ці конфіденційні команди у неробочий час як аномалію та відповідним чином оцінюватимуть ризик. Супервайзер може надати зворотний зв'язок моделям навчання, щоб відзначити, що поведінка є доброякісною, і не помічати її знову. Тим не менш, адміністратор бази даних може бути поміщений до списку спостереження на деякий час, щоб гарантувати, що його поведінка цілком доречна.

Списки спостереження попередньо визначені в UEBA для загальних груп високого ризику, таких як нові працівники, працівники, що звільняються, звільнені працівники та інші користувачі з високим ризиком. UEBA також підтримує явне додавання або видалення посвідчень у списках спостереження. У дуже чутливих середовищах, таких як державні установи, пристрої іноземного походження можуть бути внесені до списку спостереження, щоб гарантувати відсутність мерзенної прихованої комунікаційної активності.

Списки спостереження та інших підозрілих користувачів або об'єктів можна відслідковувати за допомогою меню панелі інструментів, що розкриваються, для аналізу показників ризику, аномалій, доступу, активності та термінів.

Виявлення компрометації хоста/пристрою

Добре відомо, що однією з тактик проведення кібератак, що широко використовуються, є компрометація довірених хостів, підключених до мережевої інфраструктури організації. На додаток до відстеження аномальної поведінки користувачів за допомогою UEBA для організацій дуже важливо уважно стежити за всіма кінцевими точками (пристроями та хостами), підключеними до мережі. UEBA будує тимчасову шкалу аномалій для об'єкта на основі аномальних подій та дій з високим ризиком, що виконуються з відповідного пристрою чи хоста. Організація може виявляти просунуті постійні загрози (APT) та вектори атак, а

також прогнозувати витік даних, виконуючи виявлення аномалій, орієнтованих на об'єкти.

UEBA зіставляє широкий спектр параметрів, пов'язаних з об'єктом, включаючи оповіщення безпеки кінцевих точок, результати сканування вразливостей (загальна система оцінки вразливостей або CVSS), рівні ризику користувачів та облікових записів, об'єкти, до яких здійснюється доступ, перевірка запитаних корисних даних на рівні пакетів и більше. Ця кореляція полегшує виявлення будь-яких аномальних дій чи подій визначення прогнозованих показників ризику [14].

Виявлення бічного руху

Бокове переміщення — це метод, який використовується зловмисником, при якому після отримання початкового доступу до мережі він намагається переміщатися всередині мережі, щоб знайти найкращі точки огляду для завантаження додаткових шкідливих програм, зв'язку із зовнішніми серверами і, зрештою, виявлення розташування конфіденційних даних. Щоб отримати початковий доступ, зловмисник часто використовує законні облікові дані користувача, які були вкрадені за допомогою соціальної інженерії (фішинг) або інших методів. Потім для бічного переміщення в мережі зазвичай потрібно, щоб зловмисник отримав підвищені привілеї користувача та використовував різні інструменти, щоб визначити, де він знаходиться в мережі та які засоби захисту знаходяться навколо нього. Ці інструменти часто використовуються для виконання таких дій,

Досвідчений зловмисник може використовувати «час очікування» у своїх інтересах, що означає, що його дії повільні та приховані, щоб уникнути виявлення до того, як станеться зловмисна активність, іноді через кілька тижнів або місяців після початкового злому мережі.

Незважаючи на те, що зловмисник видає себе за законного користувача в мережі, його дії та поведінка аномальні порівняно з діями реального користувача. UEBA виявляє ці аномалії, відправляє попередження та відповідним чином коригує

оцінку ризику для цього посвідчення, що допомагає виявити залишкову активність цього скомпрометованого облікового запису.

Розвідувальний моніторинг

Розвідка — це попередній етап кібератаки, при якому зловмисник намагається дізнатися якнайбільше про обчислювальне середовище організації та її засоби захисту. Щоб отримати інформацію без активної взаємодії з мережею, зловмисник використовує розвідувальні заходи для взаємодії з відкритими портами мережі, запущеними службами тощо. Наприклад, зловмисник може використовувати сканування портів, щоб визначити, які служби видно і де може бути проведена атака. В рамках сканування портів дані вилучаються з відкритих портів та аналізуються.

Аналізуючи поведінку об'єкта, UEBA може розпізнавати та попереджати про різні розвідувальні дії, включаючи сканування портів, перевірку зв'язку та зняття відбитків пальців; Виявлення таблиць та структур БД з логів веб-сервера; виявлення відкритих каталогів та сторінок в інтернеті; виявлення відкритих хмарних ресурсів, включаючи сегменти сховища, екземпляри та бази даних; і багато іншого.

Ідентифікація неправильної конфігурації безпеки

Показуючи незвичайну або ненормальну активність, у тому числі несподіваний доступ до мереж, кінцевих точок та серверів, а також додатків, UEBA може показати, де очікувані елементи керування безпекою не працюють або налаштовані неправильно. Це може включати неправильно налаштовані права доступу, обмежений доступ до певних мереж або мережевих сегментів і навіть несподіване або несанкціоноване використання програм, і це лише деякі приклади. UEBA також може виявляти несподівані канали зв'язку та активність для зовнішніх сторін, наприклад VPN-тунелі, залишені відкритими для попереднього партнера з ланцюжка поставок, які можуть бути використані в мерзотних цілях. Неточно налаштовані або незахищені елементи управління безпекою наражають на ризик системи та дані компанії. Це настільки поширена проблема,

Приклади використання Gurucul UEBA для конкретних галузей

Gurucul також пропонує кілька попередньо запакованих галузевих аналітичних матеріалів. Ці набори моделей орієнтовані рішення проблем і загроз, унікальних кожної галузевої вертикалі. Це допомагає скоротити будь-які зусилля для налаштування або впровадження для створення галузевих моделей з нуля. Ці моделі розробляються у співпраці з командою Gurucul Labs, технологічними та торговими партнерами, а також клієнтами з урахуванням телеметрії зі спеціалізованих систем, сценаріїв шахрайства/загроз та стандартів [13].

ВИСНОВКИ

В кваліфікаційній роботі було проаналізовано проблему виявлення вразливостей інформаційної системи. Було виявлено, що сучасні мережі збирають нескінченну кількість інформації, особливо коли користувачі плавно переміщуються між IP-адресами, активами, хмарними службами та мобільними пристроями. UBA зосереджується на активності користувачів, а не на статичних індикаторах загрози, тобто може виявляти атаки, які не були зіставлені з аналізом загроз, і попереджати про зловмисну поведінку на початку атаки.

Оскільки мережі стали складнішими, стало легше, ніж будь-коли, успішно проникнути в корпоративну мережу та маскуватися під внутрішнього співробітника, обходячи зовнішній захист. Якщо зловмиснику вдається проникнути в мережу й залишитися там непоміченим, він може неодноразово викрадати конфіденційні дані та завдати грошової шкоди.

В магістерській роботі було проаналізовано основні методи за засоби виявлення вразливосткй. Згідно з дослідженням, User Behavior Analytics виявляє приховану діяльність зловмисників, виявляючи шаблони поведінки користувачів, щоб визначити, що є «нормальною» поведінкою, а що може бути доказом компрометації зловмисників, внутрішніх загроз або ризикованої поведінки в мережі.

Аналітика поведінки користувачів і суб’єктів дає змогу легше визначити, чи є потенційна загроза сторонньою стороною, яка видає себе за працівника, чи справжнім працівником, який представляє певний ризик через недбалість чи зловмисний умисел. UEBA пов’язує діяльність у мережі з конкретним користувачем, а не з IP-адресою чи активом. Це означає, що якщо користувач починає поводитися незвичним або малоймовірним чином, навіть якщо це не помічено традиційними інструментами моніторингу периметра, ви зможете швидко помітити таку поведінку, визначити, чи є вона аномальною, і почати розслідування при необхідності.

Впровадження аналітики поведінки користувачів і об’єктів є обов’язковим для будь-якої організації, щоб гарантувати свою безпеку від внутрішньої шкоди. За останні роки UEBA зросла в геометричній прогресії завдяки поширенню Інтернету речей (IoT) і збільшення кількості пристроїв, які потенційно могли б використовувати вразливості мережі. Незалежно від того, намагаєтесь виявити підозрілі інсайдерські загрози чи відстежуються привілейовані облікові записи, UEBA надає оновлену лінію безпеки для IT-інфраструктури від вторгаючих атак.

ПЕРЕЛІК ПОСИЛАНЬ

1. User and Entity Behavior Analytics (UEBA) [Електронний ресурс] – режим доступу: https://www.rapid7.com/fundamentals/user-behavior-analytics/
2. Top Cybersecurity Threats in 2022) [Електронний ресурс] – режим доступу: https://onlinegrades.sandiego.edu/top-cyber-security-threats/
3. Top cybersecurity threats of 2022: report) [Електронний ресурс] – режим доступу: https://cybernews.com/security/top-cybersecurity-threats-of-2022-report/
4. What Is Threat Prevention?) [Електронний ресурс] – режим доступу: https://www.cisco.com/c/en/us/products/security/what-is-threat-prevention.html#~how-threat-prevention-works
5. Market Guide for User and Entity Behavior Analytics Gartner) [Електронний ресурс] – режим доступу: https://www.gartner.com/en/documents/3917096
6. What Is User Entity Behavior Analytics (UEBA)? Complete Guide) [Електронний ресурс] – режим доступу: https://www.cynet.com/ueba/
7. What Is UEBA?) [Електронний ресурс] – режим доступу: https://www.trellix.com/en-us/security-awareness/operations/what-is-ueba.html
8. Best User and Entity Behavior Analytics (UEBA) Tools for 2022) [Електронний ресурс] – режим доступу: https://www.esecurityplanet.com/products/best-user-and-entity-behavior-analytics-ueba-tools/
9. Best UEBA Tools for 2022) [Електронний ресурс] – режим доступу: https://project-management.com/ueba-tools/
10. User and Entity Behavior Analytics (UEBA)) [Електронний ресурс] – режим доступу: https://gurucul.com/products/user-entity-behavior-analytics-ueba
11. Gurucul User & Entity Behavior Analytics (UEBA) DATASHEET) [Електронний ресурс] – режим доступу: https://go1.gurucul.com/UEBA-Datasheet#_ga=2.242106562.1700617405.1671323161-328751094.1670330256

12. eBook: ABCs of UEBA) [Електронний ресурс] – режим доступу: https://gurucul.com/resources/whitepapers/abcs-of-ueba

13. Whitepaper: User and Entity Behavior Analytics (UEBA) Use Cases) [Електронний ресурс] – режим доступу: https://gurucul.com/resources/whitepapers/user-and-entity-behavior-analytics-use-cases

14. How Mature Behavior Analytics Accelerates Detection of Persistent Threats) [Електронний ресурс] – режим доступу: https://gurucul.com/resources/webinars/mature-behavior-analytics

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)