ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту інформаційної системи від інсайдерських атак»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Дімітрій ДЕНИСЕНКО

Виконав: здобувач вищої освіти групи БСДМ-62
ДЕНИСЕНКО Дімітрій
(ПРІЗВИЩЕ, Ім'я)

Керівник: МАРЧЕНКО Віталій
д.ф., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CISA	—	Certified Information Systems Auditor
PAM	—	Privileged Access Management
UEBA	—	User and Entity Behavior Analytics
DLP	—	Data Loss Prevention
ПЗ	—	програмне забезпечення
ІТ	—	інформаційні технології
ІЗ	—	інсайдерська загроза
FUEBA	—	Forcepoint UEBA
SIEM	—	Security Information and Event Management
EDR	—	Endpoint Detection and Response
ITM	—	Insider Threat Management
CERT-UA	—	Computer Emergency Response Team of Ukraine
ТВР	—	Trusted Business Partner
RIM	—	Regional Information Model
CASB	—	Cloud Access Security Broker
API	—	Application Programming Interface

ВСТУП

Актуальність дослідження. Сучасний світ переживає еру цифрових технологій, де величезний обсяг інформації зберігається та обробляється в мережі Інтернет. Це робить комп'ютерні системи інтегральною частиною практично всіх сфер життя - від бізнесу і освіти до медицини та національної безпеки. Однак разом із підвищенням залежності суспільства від цифрових технологій, збільшується і загроза кібербезпеки. Серед різноманітних атак на інформаційні системи особливе місце займають інсайдерські атаки, що викликають серйозні загрози для безпеки організацій і держав.

Захист інформаційних систем від інсайдерських загроз стає надзвичайно актуальним завданням в умовах постійного розвитку технологій та зростання кількості та складності кіберзагроз. Інсайдерські атаки можуть призвести до значних втрат даних, порушення конфіденційності, а також завдати шкоди репутації організації. Враховуючи той факт, що працівники організації мають унікальний доступ до важливих ресурсів, виявлення та ефективний контроль над інсайдерськими загрозами стає критично важливим завданням для забезпечення кібербезпеки.

Таким чином, технологія захисту інформаційної системи від інсайдерських атак є важливою складовою інфраструктури інформаційної безпеки організацій і сприяє забезпеченню конфіденційності, цілісності та доступності даних та інших ресурсів. Впровадження цієї технології допомагає організаціям захищати свою інформацію. Тому тема кваліфікаційної роботи є актуальною.

Об’єкт дослідження – процес забезпечення захисту інформаційної системи від інсайдерських атак.

Предмет дослідження – технологія захисту інформаційної системи від інсайдерських атак на базі рішення Forcepoint UEBA.

Мета роботи – розробити варіанти технології захисту інформаційної системи від інсайдерських атак на базі рішення Forcepoint UEBA та рекомендації щодо застосування технології..

Наукові завдання:

- провести аналіз проблеми забезпечення захисту інформаційної системи від інсайдерських атак. Визначити типи інсайдерських атак та їх наслідки.
- дослідити методи захисту від інсайдерських атак.
- розробити варіант розгортання технології захисту інформаційної системи від інсайдерських атак на базі рішення Forcepoint UEBA та рекомендації щодо застосування даної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, вивчення реальних кейсів та практичних випадків застосування Forcepoint UEBA від захисту інсайдерських атак.

Практичне значення одержаних результатів полягає в розробці технології захисту інформаційної системи від інсайдерських атак на базі рішення Forcepoint UEBA та розробка рекомендацій щодо застосування даної технології.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВІД ІНСАЙДЕРСЬКИХ АТАК

1.1. Актуальність проблеми інсайдерських атак у сфері кібербезпеки

Інсайдерські загрози представляють складний і динамічний ризик, що впливає на державні та приватні домени всіх секторів критичної інфраструктури. Визначення цих загроз є критично важливим кроком у розумінні та створенні програми пом’якшення внутрішніх загроз. Агентство з кібербезпеки та безпеки інфраструктури (CISA) визначає внутрішню загрозу як загрозу того, що інсайдер навмисно чи ненавмисно використає свій авторизований доступ, щоб завдати шкоди місії, ресурсам, персоналу, об’єктам, інформації, обладнанню, мережам або системам департаменту. Внутрішні загрози проявляються різними способами: насильство, шпигунство, диверсії, крадіжки та кіберактивності [2].

Що таке Інсайдер?

Інсайдер — це будь-яка особа, яка має або мала авторизований доступ або знання ресурсів організації, включаючи персонал, приміщення, інформацію, обладнання, мережі та системи.

Приклади інсайдера можуть включати:

- особа, якій організація довіряє, включаючи співробітників, членів організації та тих, кому організація надала конфіденційну інформацію та доступ.
- особа, якій надано бейдж або пристрій доступу, який ідентифікує її як особу з регулярним або постійним доступом (наприклад, працівник або член організації, підрядник, постачальник, охоронець або ремонтник).
- особа, якій організація надала комп’ютер та/або доступ до мережі.
- особа, яка розробляє продукти та послуги організації; до цієї групи входять ті, хто знає секрети продуктів, які забезпечують цінність організації.

- людина, яка має знання про основи організації, включаючи ціни, витрати, а також сильні та слабкі сторони організації.
- особа, яка добре обізнана з бізнес-стратегією та цілями організації, їй довірено плани на майбутнє або засоби для підтримки організації та забезпечення добробуту її людей.
- у контексті державних функцій інсайдером може бути особа, яка має доступ до захищеної інформації, якщо її зламано, то інсайдер може завдати шкоди національній та громадській безпеці.

Що таке внутрішня загроза?

Інсайдерська загроза – це можливість внутрішньої особи використовувати свій авторизований доступ або розуміння організації, щоб завдати їй шкоди [2].

Ця шкода може включати зловмисні, самовдоволені або ненавмисні дії, які негативно впливають на цілісність, конфіденційність і доступність організації, її даних, персоналу або засобів. Зовнішні зацікавлені сторони та клієнти Агентства з кібербезпеки та безпеки інфраструктури (CISA) можуть вважати, що це загальне визначення краще підходить і адаптується для використання в їхніх організаціях.

CISA визначає інсайдерську загрозу як загрозу того, що інсайдер скористається своїм авторизованим доступом, свідомо чи мимоволі, щоб завдати шкоди місії департаменту, ресурсам, персоналу, об’єктам, інформації, обладнанню, мережам або системам. Ця загроза може проявлятися як збиток відділу через такі дії внутрішньої особи:

1. Шпигунство.
2. Тероризм.
3. Несанкціоноване розголошення інформації.
4. Корупція, в тому числі участь у транснаціональній організованій злочинності.
5. Саботаж.
6. Насильство на робочому місці.

7. Навмисна чи ненавмисна втрата чи деградація ресурсів чи можливостей відділу.

Розглянемо дослідження інсайдерських загроз за 2023 рік рис. 1.1 та ключові вектори атаки.

Рис. 1.1. Статистика інсайдерських загроз за травень 2023 року [3]

Рис. 1.2. Ключові вектори інсайдерських атак [4]

Зловживання привілеями Зловживання привілеями означає використання привілейованого доступу неналежним чином. У звіті Verizon про розслідування витоків даних за 2023 рік йдеться, що 78% усіх випадків зловживання привілеями є фінансовими мотивами [5]. Два найпоширеніші типи зловживання привілеями – це зловживання привілеями та неправильна обробка даних. Зловживання привілеями становить до 80% усіх випадків зловживання привілеями та стосується шахрайської або зловмисної діяльності з привілейованими правами доступу. Неправильне поводження з даними є причиною до 20% інцидентів зловживання привілеями та передбачає недбале поводження інсайдерів з конфіденційними даними. На відміну від зловживання привілеями, випадки неправильної обробки даних зазвичай не мають зловмисного наміру.

Рис. 1.3. Основні дії при зловживанні привілеями [4]

Різні помилки Відповідно до звіту Verizon про розслідування витоку даних за 2023 рік [5], різноманітні помилки вчиняються ненавмисно внутрішніми особами. Головні інсайдерські групи, які допускають такі помилки, зазвичай є привілейованими користувачами (системними адміністраторами та розробниками) та іншими кінцевими користувачами. Їхні найпоширеніші помилки:

Рис. 1.4. Найпоширеніші помилки [4]

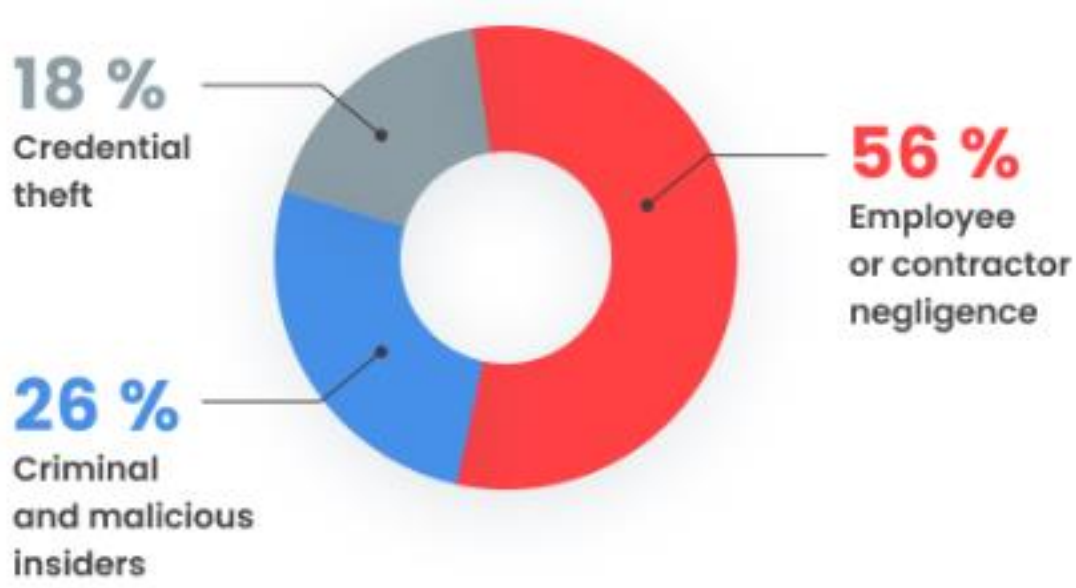

Рис. 1.5. Основні причини інцидентів [4]

Крадіжка облікових даних

Крадіжка облікових даних є одним із найпоширеніших способів потрапити всередину захищеного периметра організації. Використовуючи законні облікові дані, хакери можуть працювати непоміченими всередині системи протягом досить тривалого часу. Щоб отримати логіни та паролі користувачів, зловмисники використовують соціальну інженерію, Brute Force, введення облікових даних та інші вектори атак.

Злочинні та зловмисні інсайдери

Злочинці та зловмисники становлять значну загрозу, оскільки вони знають про заходи кібербезпеки вашої організації та конфіденційні дані. Використовуючи ці знання, вони можуть викрасти або злити дані, саботувати операції або надати зовнішнім зловмисникам доступ до ваших ресурсів.

Недбалість працівника або підрядника

Недбалість співробітників або підрядників є причиною більшості інцидентів, пов'язаних із внутрішньою загрозою безпеці, але наслідки таких інцидентів, як правило, коштують найменше для пом'якшення. Прикладами людської помилки є надсилання конфіденційних даних не тому одержувачу, неправильне налаштування середовища та використання небезпечних методів роботи.

1.2. Типи інсайдерських атак та їх наслідки

- **Ненавмисна загроза**
  - **недбалість** – Інсайдер такого типу наражає організацію на загрозу через необережність. Недбалі інсайдери, як правило, знайомі з політикою безпеки та/або IT-політики, але вирішили ігнорувати їх, створюючи ризик для організації. Приклади включають дозвіл комусь «перейти» через захищену точку входу, неправильне розміщення або втрату портативного пристрою зберігання, що містить конфіденційну інформацію, та ігнорування повідомлень про встановлення нових оновлень і виправлень безпеки [2].
  - **випадковий** – інсайдер такого типу помилково створює ненавмисну небезпеку для організації. Приклади включають неправильне введення адреси електронної пошти та випадкове надсилання конфіденційного ділового документа конкуренту, несвідоме чи випадкове натискання гіперпосилання, відкриття вкладення у фішинговому електронному листі, яке містить вірус, або неналежну утилізацію конфіденційних документів.

- **навмисні загрози** – навмисний інсайдер часто згадується як «зловмисний інсайдер». Навмисні погрози – це дії, вжиті з метою завдати шкоди організації заради особистої вигоди або діяти на підставі особистої скарги. Наприклад, багато інсайдерів мотивовані «відплатитися» через уявну відсутність визнання (наприклад, підвищення по службі, бонуси, бажана подорож) або звільнення. Їхні дії можуть включати витік конфіденційної інформації, переслідування партнерів, саботування обладнання, вчинення насильства або викрадення конфіденційних даних чи інтелектуальної власності з помилковою надією просунути свою кар'єру [2].
- **інші загрози**
  - **змовні загрози** – Підмножина зловмисних інсайдерських загроз називається змовними загрозами, коли один або кілька інсайдерів співпрацюють із зовнішнім загрозливим учасником скомпрометувати організацію. У цих інцидентах часто кіберзлочинці вербують інсайдера або кількох інсайдерів, щоб уможливити шахрайство, крадіжку інтелектуальної власності, шпигунство чи комбінацію цих трьох [2].
  - **загрози третіх сторін** – крім того, загрози третіх сторін зазвичай становлять підрядники або постачальники, які офіційно не є членами організації, але яким надано певний рівень доступу до об'єктів , систем, мереж або людей для завершення своєї роботи. Ці загрози можуть бути прямими чи непрямими.

Як виникає внутрішня загроза?

Внутрішні загрози проявляються різними способами: насильство, шпигунство, диверсії, крадіжки та кіберактивності. Вирази внутрішньої загрози детально визначені нижче [2].

<u>Вираження внутрішньої загрози</u>

- **насильство** – ця дія включає погрозу насильства, а також іншу загрозливу поведінку, яка створює залякувальне, вороже чи образливе середовище.
  - **насильство на робочому місці/організація** – це будь-яка дія чи загроза фізичного насильства, переслідувань, сексуальних домагань, залякування, знущань,

образливих жартів чи іншої загрозливої поведінки з боку колеги чи товариша що відбувається на місці роботи або під час роботи особи.

- **Тероризм** як внутрішня загроза – це незаконне використання насильства або погроза застосування насильства співробітниками, членами чи іншими особами, тісно пов'язаними з організацією, проти цієї організації. Метою тероризму є просування політичних або соціальних цілей.

- **шпигунство** – шпигунство – це прихована чи незаконна практика шпигунства за іноземним урядом, організацією, організацією чи особою з метою отримання конфіденційної інформації для військової, політичної, стратегічної чи фінансової вигоди .

- **економічне шпигунство** – це таємна практика отримання комерційної таємниці від іноземної держави (наприклад, усіх форм і типів фінансової, ділової, наукової, технічної, економічної чи інженерної інформації та методи, техніки, процеси, процедури, програми або коди для виробництва) [2].

- **урядове шпигунство** – це прихована діяльність одного уряду зі збору розвідувальних даних проти іншого з метою отримання політичної чи військової переваги. Це також може включати шпигунство уряду (урядів) за корпоративними організаціями, такими як авіаційні фірми, консалтингові фірми, аналітичні центри або компанії, що займаються виробництвом боєприпасів. Урядове шпигунство також називають збором розвідувальних даних.

- **злочинне шпигунство** включає громадянина США, який видає урядові таємниці США іноземним державам.

- **саботаж** – саботаж описує навмисні дії, спрямовані на заподіяння шкоди фізичній або віртуальній інфраструктурі організації, зокрема недотримання процедур технічного обслуговування чи IT, забруднення чистих приміщень, фізичне пошкодження об'єктів або видалення коду для запобігання регулярні операції.

- **фізичний саботаж** – це навмисні дії, спрямовані на заподіяння шкоди фізичній інфраструктурі організації (наприклад, приміщенням або обладнанню).

- **віртуальний саботаж** – це вчинення зловмисних дій за допомогою технічних засобів, щоб порушити або припинити звичайні бізнес-операції організації.

- **крадіжка** – крадіжка – це крадіжка грошей чи інтелектуальної власності.
  - **фінансовий злочин** – це несанкціоноване заволодіння або незаконне використання грошей чи власності особи, підприємства чи організації з наміром отримати від цього вигоду [2].
  - **крадіжка інтелектуальної власності** – це викрадення чи пограбування ідей, винаходів чи творчих проявів особи чи організації, зокрема комерційних таємниць і запатентованих продуктів, навіть якщо концепції чи елементи викрадаються походить від злодія.

- **кібер** – кіберзагроза включає крадіжки, шпигунство, насильство та саботаж усього, що стосується технологій, віртуальної реальності, комп'ютерів, пристроїв чи Інтернету.
  - **ненавмисні загрози** – це незловмисне (часто випадкове чи ненавмисне) розкриття ІТ-інфраструктури, систем і даних організації, яке завдає ненавмисної шкоди організації. Приклади включають фішингові електронні листи, шахрайське програмне забезпечення та «шкідливу рекламу» (вбудовування шкідливого вмісту в законну онлайн-рекламу) [2].
  - **навмисні загрози** – це зловмисні дії, вчинені зловмисними інсайдерами, які використовують технічні засоби, щоб порушити або зупинити звичайні бізнес-операції організації, виявити недоліки ІТ, отримати захищену інформацію або іншим чином сприяти атаці планувати через доступ до ІТ-систем. Ця дія може передбачати зміну даних або вставлення зловмисного програмного забезпечення чи іншого образливого програмного забезпечення для порушення роботи систем і мереж.

1.3. Визначення потенційних індикаторів ризику

Оцінка загрози інсайдерів – це процес збирання та аналізу інформації про відповідну особу, яка може мати інтерес, мотиви, наміри та здатність завдати шкоди організації чи особам. Оцінка загроз інсайдерів — це унікальна дисципліна, яка вимагає від команди людей оцінити особу, що викликає занепокоєння, і визначити масштаб, інтенсивність і наслідки потенційної загрози.

Ці оцінки базуються на поведінці, а не на профілях, а поведінка є змінною за своєю природою. Метою оцінки є запобігання внутрішньому інциденту, навмисному чи ненавмисному. Універсального підходу до оцінки не існує. Кожне оцінювання має бути точним, ретельним і проводитися відповідно до організаційних інструкцій і чинного законодавства. Стратегії втручання мають бути зосереджені на допомозі особі, що викликає занепокоєння, одночасно працюючи над пом’якшенням потенційних наслідків ворожої дії.

Проте існують певні індикатори ризику, які допомагають виявити можливі загрози та прийняти заходи забезпечення безпеки.

До потенційних індикаторів ризику відносяться:

1. Зміни в робочому звичаї:

— збільшення або зменшення активності: різке збільшення або, навпаки, зменшення активності працівника може бути ознакою аномальної поведінки.

— незвичайний доступ до систем: якщо спостерігаються несподівані спроби доступу до ресурсів або систем, це свідчить про неправомірні дії.

2. Надмірні права доступу:

— надання занадто великої кількості прав доступу: інсайдерам необхідно здобути додаткові права для здійснення атаки.

3. Нагромадження конфіденційної інформації:

— необґрунтоване копіювання чи переміщення файлів: велика кількість непередбачуваних або незвичайних операцій з файлами може бути ознакою інсайдерської діяльності.

4. Неординарна активність на робочих системах:

— зміни у звичайному користуванні системами: наприклад, надмірна активність під час робочих годин, коли цього не очікується.

5. Зміни у спілкуванні:

— збільшення або зменшення комунікації з колегами: інсайдери можуть змінити свої звичайні зв'язки для уникнення виявлення.

6. Незвичайна поведінка в мережі:

— неординарна використання мережевих ресурсів: збільшення або зменшення трафіку, невиправдані великі обсяги передачі даних.

7. Історія конфліктів чи недовіри:

— ворожа поведінка або конфлікти: історія конфліктів або недовіри може бути попередженням про можливі інсайдерські мотивації.

8. Зміни у корпоративних правилах та політиках:

— обхід або порушення внутрішніх правил і політик: інсайдер може спробувати обійти чи порушити внутрішні правила для досягнення своїх цілей.

Визначення цих індикаторів ризику та їх систематичний моніторинг допомагає вчасно виявляти інсайдерські загрози та реагувати на них, зменшуючи можливість серйозних наслідків для безпеки інформації та організаційних ресурсів.

Висновок до розділу 1

В розділі проаналізовано актуальність проблеми інсайдерських атак, приведено статистику дослідницьких інститутів за 2023 рік. Представлено типи інсайдерських атак та їх наслідків, а також визначено потенційні індикатори ризику інсайдерських атак.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВІД ІНСАЙДЕРСЬКИХ АТАК

2.1. Дослідження програмних методів захисту інформаційної системи від інсайдерських атак

Інструменти, які компанії використовують для виявлення та запобігання внутрішньому шахрайству, викраденню даних співробітниками та інших загроз базуються на уніфікованій видимості, що означає, що всю діяльність користувача можна побачити з одного місця.

З такою кількістю інструментів кібербезпеки на ринку важко зосередитися на певній лінії захисту та вибрати програмне забезпечення для керування внутрішніми загрозами, яке забезпечує найкращий результат із мінімальними зусиллями. Керування привілейованим доступом (PAM), аналітика поведінки користувачів і об’єктів (UEBA) і запобігання втраті даних (DLP) є трьома найкращими технологіями для запобігання внутрішнім загрозам з запобігання втраті даних.

Рис. 2.1. Інструменти та заходи для зниження інсайдерських ризиків [6]

Запобігання втраті даних (Data Loss Prevention — DLP) — це набір інструментів і процесів, які використовуються для запобігання втраті конфіденційних даних, їх неналежному використанню чи доступу неавторизованих користувачів.

DLP класифікує регульовані, конфіденційні та критично важливі для бізнесу дані та виявляє порушення політик, визначених організаціями або в рамках попередньо визначеного пакету політик, як правило, керуючись нормативними вимогами, такими як HIPAA, PCI-DSS або GDPR [7].

Після виявлення цих порушень DLP примусово виправляє їх за допомогою сповіщень, шифрування та інших захисних дій, щоб запобігти випадковому чи зловмисному обміну кінцевими користувачами дані, які можуть створити організаційні ризики.

Управління привілейованим доступом (Privileged access management — PAM) — це рішення безпеки ідентифікації, яке допомагає захистити організації від кіберзагроз шляхом моніторингу, виявлення та запобігання несанкціонованому привілейованому доступу до критично важливих ресурсів. PAM працює через поєднання людей, процесів і технологій і дає змогу бачити, хто використовує привілейовані облікові записи та що вони роблять під час входу в систему. Обмеження кількості користувачів, які мають доступ до адміністративних функцій, підвищує безпеку системи, а додаткові рівні захисту пом'якшити випадки витоку даних з боку загрозливих суб'єктів [8].

Аналітика поведінки користувачів і об’єктів (User and entity behavior analytics — UEBA) – це рішення для кібербезпеки, яке використовує алгоритми та машинне навчання для виявлення аномалій у поведінці не лише користувачів у корпоративній мережі, а також маршрутизаторів, серверів і кінцевих точок у цій мережі.

UEBA прагне розпізнавати будь-яку особливу або підозрілу поведінку — випадки, коли є відхилення від звичайних повсякденних моделей або використання. Наприклад, якщо певний користувач у мережі регулярно завантажує файли розміром

20 МБ щодня, але починає завантажувати файли розміром 4 ГБ, система UEBA вважатиме це аномалією та або сповістить IT-адміністратора, або, якщо є автоматизація, автоматично від'єднається. цього користувача з мережі [9].

UEBA йде далі, ніж просто стежить за поведінкою людей — вона стежить за машинами. Сервер в одній філії одного дня може раптово отримати тисячі запитів більше, ніж зазвичай, сигналізуючи про початок потенційної розподіленої атаки на відмову в обслуговуванні (DDoS). Існує ймовірність, що IT-адміністратори можуть не помітити такого типу діяльності, але UEBA розпізнає це та вживає подальших заходів.

Інформація про безпеку та керування подіями (Security information and event management — SIEM) — це рішення безпеки, яке допомагає організаціям розпізнавати й усунути потенційні загрози безпеці й уразливості, перш ніж у них з'явиться шанс порушити бізнес-операції. Системи SIEM допомагають групам безпеки підприємства виявляти аномалії поведінки користувачів і використовувати штучний інтелект (AI) для автоматизації багатьох ручних процесів, пов'язаних із виявленням загроз та реагування на інцидент.

Оригінальні платформи SIEM були інструментами керування журналами, які поєднували керування інформацією про безпеку (SIM) і керування подіями безпеки (SEM), щоб забезпечити моніторинг у реальному часі та аналіз подій, пов'язаних із безпекою, а також відстеження та реєстрацію даних безпеки для відповідності чи аудиту цілей. Gartner ввів термін SIEM для поєднання технологій SIM і SEM у 2005 році [10].

Виявлення кінцевих точок і реагування на них (Endpoint Detection and Response — EDR), також відоме як виявлення кінцевих точок і реагування на загрози (endpoint detection and threat response — EDTR), — це рішення безпеки кінцевих точок, яке постійно відстежує пристрої кінцевих користувачів для виявлення та реагувати на кіберзагрози, як-от програми-вимагачі та шкідливі програми [11].

Створений Антоном Чувакіним із Gartner, EDR визначається як рішення, яке «записує та зберігає поведінку на рівні кінцевої системи, використовує різні методи

аналізу даних для виявлення підозрілої поведінки системи, забезпечує контекстну інформацію, блокує зловмисну активність і надає пропозиції щодо відновлення уражених систем» [11].

Gartner визначає **управління внутрішніми загрозами (insider threat management — ITM)** як методологію, що включає інструменти та можливості для вимірювання, виявлення та стримування небажаної поведінки довірених облікових записів в організації. Вона включає рішення, які відстежують поведінку працівників, сервісних партнерів і ключових постачальників, що працюють всередині організації. Потім ці інструменти оцінюють, чи відповідає поведінка очікуванням ролі та корпоративній толерантності до ризиків. Для IT-директорів і керівників служб кібербезпеки управління внутрішніми ризиками означає використання технічних рішень для вирішення суто людської проблеми. Управління інсайдерськими ризиками вимагає співпраці між багатьма міжфункціональними партнерами. Компонентами методології управління інсайдерськими ризиками є політики, інструкції та слідчі дії, які виходять за рамки типової організації з кібербезпеки. Для наших цілей ринок управління інсайдерськими ризиками складається з інструментів і рішень, які відстежують поведінку співробітників, сервісних партнерів і ключових постачальників, що працюють всередині організації. Вони оцінюють, чи відповідає ця поведінка очікуванням ролі та корпоративній толерантності до ризиків [12].

2.2. Порівняння програмних методів захисту інформаційної системи від інсайдерських атак

Кожне рішення в тому чи іншому сенсі має свої переваги та недоліки порівняємо розглянуті вище методи та засоби захисту від інсайдерських атак.

1. DLP (Data Loss Prevention):

Переваги:

DLP дозволяє виявляти, моніторити та блокувати спроби втрати конфіденційної інформації.

Надає можливість налаштовувати та впроваджувати політики безпеки щодо обробки даних.

Відстежує порушення внутрішніх правил щодо обробки та обміну інформацією.

Недоліки:

Може призводити до блокування законних операцій через високий рівень чутливості.

Вимагає часу та ресурсів для правильної конфігурації та налаштування [7-12].

2. PAM (Privileged Access Management):

Переваги:

Зменшення можливості несанкціонованого доступу до привілейованих облікових записів.

Ведення журналів та аудиту всіх привілейованих дій для виявлення підозрілих активностей.

Забезпечує автоматизацію процесів надання та забирання привілеїв.

Недоліки:

Впровадження PAM складне завдання, особливо в комплексних інформаційних середовищах.

Забезпечення безпеки вимагає від адміністраторів суворого дотримання політик безпеки.

3. UEBA (User and Entity Behavior Analytics):

Переваги:

Аналізує поведінку користувачів та сутностей для виявлення відхилень від звичайної активності.

Допомагає вчасно виявляти підозрілі дії інсайдерів та інших загроз безпеці.

Недоліки:

Щоб аналіз був ефективним, необхідна велика кількість даних для навчання моделі аналізу поведінки.

Може викликати тривожні повідомлення на підставі нормальної, але незвичайної активності користувачів [7-12].

4. SIEM (Security Information and Event Management):

Переваги:

Забезпечує централізований погляд на події в системі для швидкого виявлення загроз.

Аналізує та корелює події з різних джерел для виявлення зв'язків та визначення загроз.

Підтримує інтеграцію з різноманітними джерелами журналів для комплексного аналізу.

Недоліки:

Вимагає досвіду та ресурсів для ефективного конфігурування та підтримки.

Залежно від налаштувань та об'єму даних, час виявлення загроз може суттєво затримуватися.

5. EDR (Endpoint Detection and Response):

Переваги:

Забезпечує захист на рівні кінцевих точок (комп'ютерів, серверів) в режимі реального часу.

Дозволяє виявляти та ізолювати компрометовані системи або процеси.

Недоліки:

EDR фокусується на захисті кінцевих точок і може не мати повноцінного огляду всієї системи.

Реалізація та управління EDR ускладнюється через велику кількість точок, якими потрібно керувати [7-12].

6. ITM (Insider Threat Management)

Переваги:

Спрямована на ідентифікацію та вирішення інсайдерських загроз та дій.

Система для виявлення нормальної та ненормальної активності працівників [7-12].

Недоліки:

Невизначеність меж між нормальною та ненормальною поведінкою.

Інсайдерські загрози залишаються невиявленими, якщо система не покриває всі аспекти діяльності працівників.

Таблиця 2.1.

Узагальнена порівняльна таблиця методів та засобів захисту від інсайдерських загроз

Параметр	**DLP**	**PAM**	**UEBA**	**SIEM**	**EDR**	**ITM**
Захист конфіденційної інформації	+	+	-	-	-	+
Моніторинг та аудит доступу	-	+	-	+	+	+
Виявлення незвичайної поведінки	-	-	+	+	+	+
Автоматизація управління доступом	-	+	-	-	-	-
Централізована система моніторингу	-	-	+	+	-	-
Виявлення та ізоляція загроз	-	-	-	-	+	-
Обмежені можливості в аналізі ситуації	-	-	+	+	-	-
Моніторинг та реагування на кінцевих точках	-	-	-	-	+	-
Виявлення внутрішніх загроз	+	-	+	+	-	+

Виходячи з проведеного порівняльного аналізу для більш надійного захисту від інсайдерських загроз необхідно комбінувати методи та засоби між собою одного ідеалу не існує.

2.3. Рекомендації протидії інсайдерським загрозам згідно CERT-UA

Ключові компоненти протидії інсайдерським загрозам CERT використовуються перед тим, як створити захист від інсайдерської загрози (ІЗ) в організації, спершу потрібно зрозуміти необхідні компоненти такої програми. В центрі інсайдерських загроз CERT виділяють наступні ключові компоненти, для створення повністю функціонуючої програми захисту від ІЗ.

Для ефективного зменшення загроз, викликаних інсайдерами, необхідно розуміти сприйнятливість організації до загроз [13]. Оцінка вразливості загрози CERT допомагає визначити, наскільки організації чи підприємства готові запобігти, виявити та реагувати на ІЗ, якщо вони з’являться в організації.

Основні рекомендації:

1. Врахування досвіду попередніх інцидентів. Для організацій ІЗ майже однакові і про способи протидії інсайдерам можна знайти багато, наприклад, у рекомендаціях на цю тему. Якщо була здійснена атака, впровадьте відповідні засоби захисту. Деякі організації створюють команди з вивчення та протидії інсайдерським загрозам (Security Operations Center), розбору випадків і методик протидії їм.

2. Концентрація на захисті критично важливих ресурсів. Більше третини інцидентів, пов'язаних з інсайдерами, за даними команд швидкого реагування, мають відношення до іноземних державних організацій. Проведення аудиту критично важливих цінностей організації, впровадження надлишкових та посилених заходів та засобів для захисту.

3. Використання різноманітних способів захисту. Ефективніший багаторівневий та різнотипний захист — DLP, SIEM, IDS, log management and analisys тощо, він значно ускладнить побудову вектору атаки на організацію. Введення та аналіз журнальних файлів пристроїв захисту організації на предмет виявлення підозрілої активності.

4. Реагування на загрози від партнерів. Довірені бізнес-партнери (Trusted Business Partner, TBP), якими можуть бути контрактори або аутсорсингові компанії, можуть нести інсайдерську загрозу, не меншу за конкурентів. Визначення заходів з інформаційної безпеки у контракті з TBP.

5. Зважайте на взаємовідносини, як на індикатор інсайдерської загрози. Напружені взаємовідносини між організаціями — 4 місце серед причин інсайдерських випадків згідно CERT Insider Threat Database . Погані відносини між співробітниками організації — 8 місце. Коли негаразди у колективі —найчастіше це стає причиною IT-саботажу через інсайдерів. Деякі організації, також, навчають персонал, як виявляти типові індикатори інсайдера, впроваджують HR-менеджмент та вводять посади відповідальних за внутрішню безпеку.

6. Навчання персоналу згідно потенційної посади.

7. Приділення особливої уваги перепризначенням та звільненням. Кадрові зміни — перше місце у CERT Insider Threat Database, тому необхідно робити цільовий моніторинг співробітників, які звільняються та змінюють посади у організації.

8. Формалізуйте та узгодьте питання приватності в організації. Приватність співробітників — важлива та щоб вона не стала інструментом інсайдера, треба приділяти їй увагу [13].

9. Комплексна робота з організацією. IT-персонал не може вирішити проблему інсайдерів власними зусиллями. Потрібні зусилля менеджменту, IT-персоналу, співробітників з інформаційної безпеки, власників даних, розробників програмних продуктів, керівництва та співробітників. Іноді, для того щоб виявити інсайдера, треба провести велику роботу всередині підрозділу організації та налагодити ефективні відносини між підрозділами.

10. Створення програми протидії ІЗ. У перші три місяці необхідно:

- створити та заповнити вакансію топ-менеджера, що займеться інсайдерською проблематикою;
- сформувати команду з протидії ІЗ;

- створити та погодити політику безпеки, яка включатиме ІЗ;
- розробити процеси та впровадити засоби протидії інсайдерам.

У перші шість місяців потрібно:

- повністю переробити та значно покращити політику безпеки;
- регулярно перевіряти контрольні параметри для виявлення інсайдерів;
- налагодити заняття з персоналом стосовно інсайдерських загроз, моделюючи типові ІЗ у вигляді практичних занять.

Висновок до розділу 2

В розділі було досліджено програмні методи захисту від інсайдерських атак, а саме Data Loss Prevention, Privileged Access Management, User and Entity Behavior Analytics, Security Information and Event Management, Endpoint Detection and Response, Insider Threat Management, проведений їх аналіз в якому виділені переваги та недоліки кожного з них. Систематизовано дані переваги та недоліки в узагальнену порівняльну таблицю. Приведені рекомендації протидії інсайдерським загрозам згідно CERT-UA (Computer Emergency Response Team of Ukraine) спеціалізованого структурного підрозділу Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВІД ІНСАЙДЕРСЬКИХ АТАК НА БАЗІ РІШЕННЯ FORCEPOINT UEBA

3.1. Можливості та архітектура Forcepoint UEBA

Forcepoint (укр. «Форспоінт») - американська багатонаціональна корпорація, що займається розробкою програмного забезпечення, зі штаб-квартирою в Остіні, штат Техас США. Компанія є дочірньою компанією Raytheon Technologies, яка наразі займається розробкою програмного забезпечення для комп'ютерної безпеки та запобігання витокам персональних даних, CASB, міжмережевого екрану та міждоменних рішень, компанія також відома як Websense, Raytheon|Websense.

Forcepoint UEBA отримує та аналізує сценарії, засновані на активності користувачів (події, такі як вхід в систему, завдання на друк тощо), а також сценарії, не пов'язані з активністю (інформація про організації, наприклад, дані про персонал) в межах компанії. Потім Forcepoint UEBA застосовує багаторівневий набір функцій оцінювання та аналітики, щоб отримати інформацію про те, що люди роблять і ким вони є [14].

Ці дані в кінцевому підсумку готуються і візуалізуються, щоб надати командам по боротьбі з внутрішніми загрозами потужний поведінковий аналіз для виявлення і пом'якшення внутрішніх ризиків. Цінність Forcepoint UEBA полягає не тільки в його аналітичних можливостях, але і в спрощеній та інтуїтивно зрозумілій візуалізації даних. Інформаційна модель (RIM) Forcepoint UEBA відображає дані з різних джерел у послідовну модель даних, яку можна легко зрозуміти та проаналізувати.

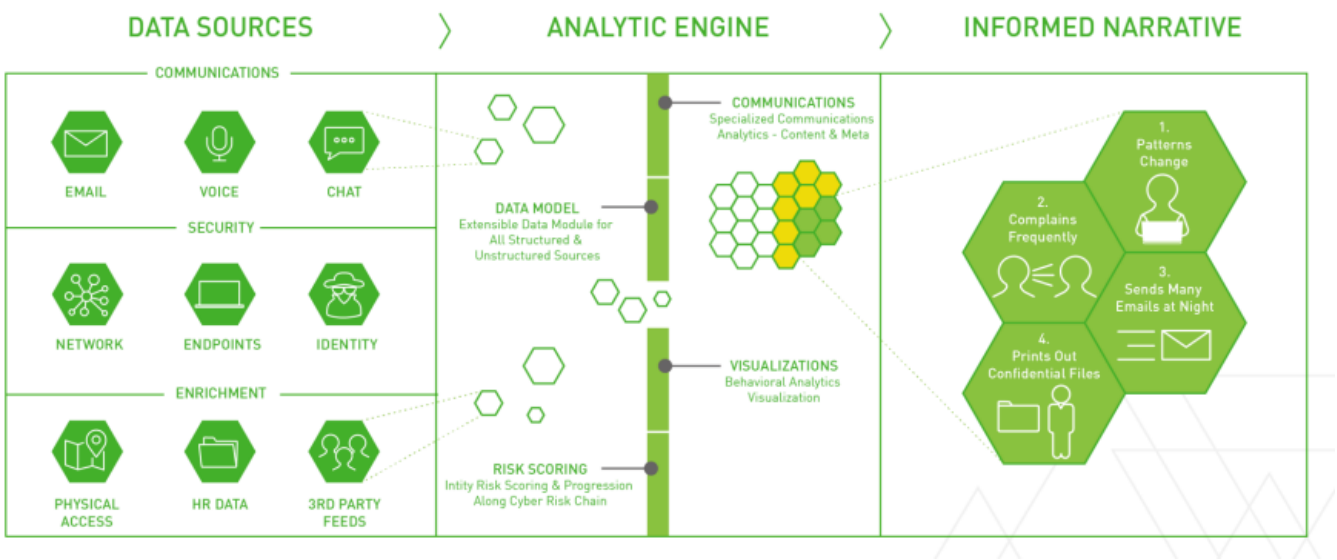

Рис. 3.1. Процес, який Forcepoint UEBA використовує для побудови обґрунтованої поведінки про користувачів з високим рівнем ризику [15]

Архітектура Forcepoint UEBA складається з 3-х рівнів, а саме:

→ Рівень I: Дані > Forcepoint збирає необроблені дані з широкого спектру каналів даних підприємства, включаючи комунікації, фізичний доступ, кінцеві точки і мережеву активність. Forcepoint DLP і Forcepoint Insider Threat є рекомендованими, але не обов'язковими джерелами даних.

→ Рівень II: Поглинання (Ingest) > На рівні «Поглинання» потоки необроблених даних перетворюються і готуються до аналізу. Використовуючи гнучку платформу збору даних (наприклад, TCP-listener, FTP-download), Forcepoint збирає необроблені дані, перетворює їх у формат подій і пропускає через конвеєр поглинання та аналітичний механізм.

→ Рівень III: Додаток > Рівень додатку забезпечує маштабоване зберігання даних і можливості запитів аналітику поведінки під час виконання, інтерфейс аналітика і адміністратора, а також вихідний API.

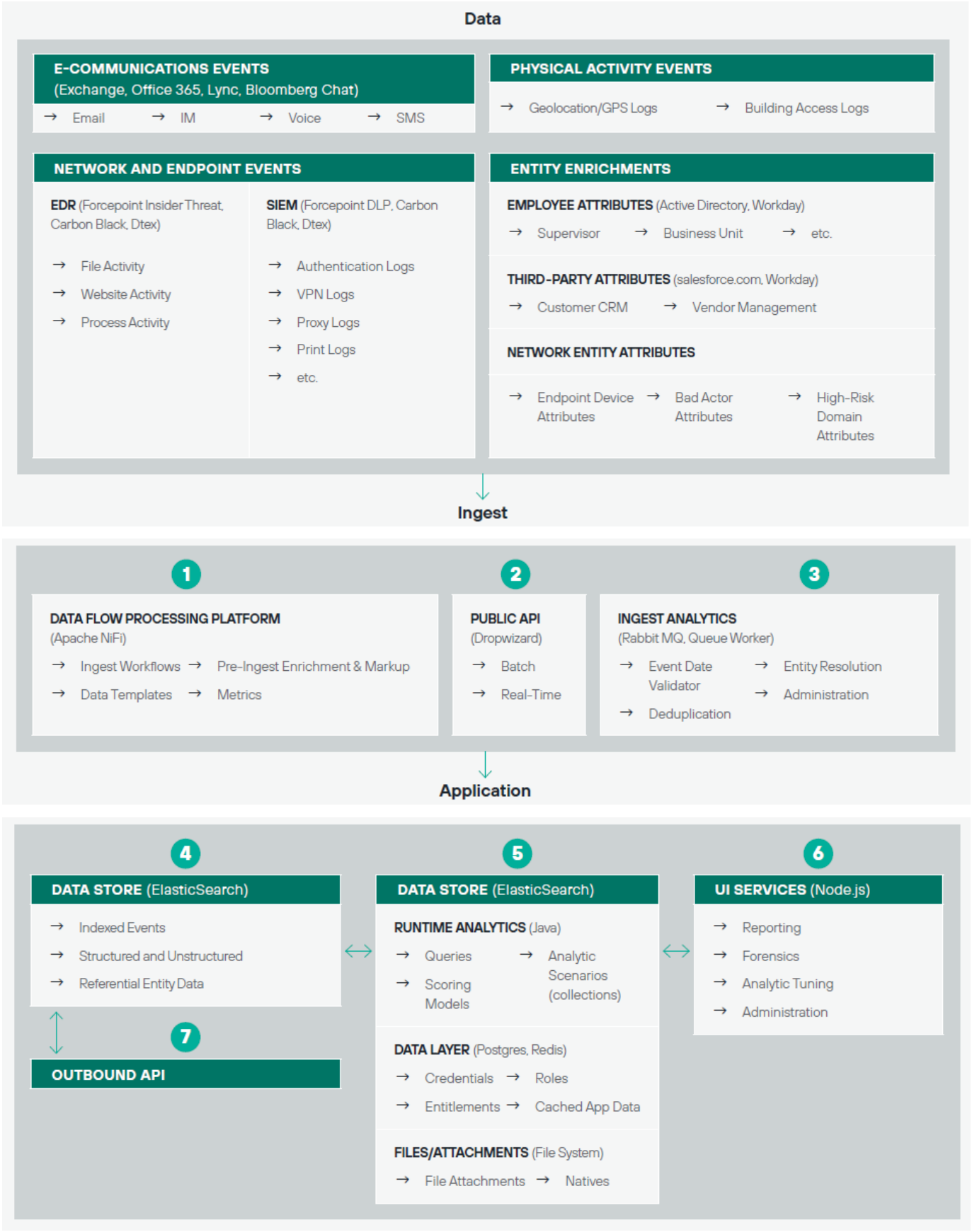

Рис. 3.2. Рівні архітектури Forcepoint Behavioral Analytics [16]

Як описано і проілюстровано вище на рис. 3.2, необроблені дані з безлічі джерел надходять в архітектуру Ingest (поглинання) і, нарешті, в прикладний рівень, де збагачені події Forcepoint Behavioral Analytics корелюються, аналізуються і представляються аналітикам для проведення розслідування [16].

Поглинання даних - це процес отримання та імпорту даних для негайного використання або зберігання.

Рівень I: Платформа обробки даних

Поведінкова аналітика Forcepoint покладається на дані, отримані від існуючих датчиків, журналів і системи мережевої безпеки організації, щоб надавати поведінкову аналітику внутрішніх загроз. Для отримання необроблених даних платформа обробки даних Forcepoint використовує ряд механізмів збору, які можуть включати прослуховування вхідних потоків TCP або UDP (наприклад, syslog), запити API (наприклад, Splunk API) або пакетне витягування даних за допомогою FTP, доступу до файлового ресурсу тощо.

Рівень II: Поглинання

Перший набір компонентів платформи відповідає за отримання та збагачення даних. Після визначення типів даних, що підлягають аналізу, як це передбачено Керівництвом з аудиту, ці джерела даних зіставляються з інформаційною моделлю в платформі обробки потоку даних перед завантаженням [16]. Потім вони отримуються через публічний API і, нарешті, проходять через низку процесів збагачення та аналізу.

Компоненти другого рівня:

1. Платформа для обробки потоку даних перед завантаженням — Forcepoint в основному використовує фреймворк Apache NiFi для обробки даних перед завантаженням на платформу. Ключові концепції фреймворку NiFi - походження даних, трансформація, слабкий зв'язок, висока паралельність, метрики - тісно пов'язані з цілями Forcepoint, а готове рішення Forcepoint надає клієнтам набір робочих процесів, шаблонів і процесорів, які є стандартизованими, надійними і відмовостійкими, для консолідації джерел даних і публікації в публічному інтерфейсі

API Forcepoint. Платформа обробки потоків даних також дозволяє клієнтам розробляти і впроваджувати специфічні для середовища процесори збагачення для маркування подій перед їх надходженням. Це дозволяє налаштовувати потоки даних без додаткових витрат на професійні послуги Forcepoint. Таким чином, платформа обробки потоків даних перед завантаженням забезпечує додаткову розширюваність і гнучкість без додаткових витрат і складнощів [16].

2. Потоковий публічний API — Forcepoint Behavioral Analytics Public API - це RESTful API, який використовується для отримання інформації про події та об'єкти в додатку, або в режимі реального часу, або шляхом масового завантаження в API. API містить безліч зручних кінцевих точок, які узгоджуються з відображеннями інформаційної моделі (також використовується в платформі обробки потоку даних перед поглинанням), а також пропонує стандартизований набір метрик, які вимірюють затримки запитів. Зручність і наочність під час поглинання - дві основні переваги публічного API. (Деякі джерела даних можуть бути розміщені безпосередньо в конвеєрі поглинання, описаному нижче, але Forcepoint настійно рекомендує використовувати публічний API) [16].

3. Конвеєр поглинання (перевірка > збагачення > аналітика) — після того, як інформація про події та об'єкти поглинається через публічний API, вона поміщається в чергу повідомлень і в обробник черги для подальшої обробки і збагачення. Кожен з процесорів в Queue Worker в кінцевому підсумку надає переваги для аналітики та розслідування.

Розглянемо кожен з них:

→ **Валідатор дати події** — дозволяє Forcepoint отримувати тільки ті події, які мають відношення до налаштованого аналітичного часового вікна.

→ **Дедуплікація** — дозволяє видаляти повторювані події, щоб вони не створювали шум і непотрібну роботу для користувачів програми.

→ **Розв'язання сутностей** — забезпечує розв'язання ідентифікаторів події до певної сутності, так що одна сутність може бути легко прив'язана до декількох ідентифікаторів та режимів діяльності.

→ **Виявлення застережень** — видаляє нецікавий з аналітичної точки зору текст, а саме застереження, з комунікаційних подій, щоб вони не створювали шуму в системі.

→ **Маркування** — сприяє маркуванню подій на основі визначеного набору політик.

→ **Оцінювання характеристик** — являє собою перший фундаментальний блок у аналітичному процесі, оцінюючи кожну подію на основі налаштованого набору базових аналітичних моделей, завантажених у систему [16].

Рівень ІІІ: Додаток Forcepoint

Після того, як події та сутності потрапляють до системи, вони зберігаються для використання в додатку. Опишемо функції та переваги кожного компонента в самому додатку.

1. Сховище даних — Forcepoint Behavioral Analytics використовує ElasticSearch (ES) як основне сховище даних для інформації про події та сутності. ElasticSearch добре зарекомендував себе в масштабах і надає значні переваги кінцевим користувачам для текстового пошуку, аналітики та агрегації, які інші технології баз даних просто не можуть забезпечити [16].

2. Служба основних даних (MDS) — власна служба основних даних Forcepoint забезпечує більшу частину аналітичних можливостей програми, а також співвідносить дані зі сховища даних ElasticSearch з іншими допоміжними технологіями (наприклад, Postgres і Redis використовуються для зберігання реляційних і транзакційних даних). Однією з переваг такого поділу сховищ даних є можливість їх масштабування незалежно один від одного, що дозволяє більше контролювати конфігурацію розгортання на основі моніторингу користувачів та отриманих даних, і, в кінцевому рахунку, знизити операційні витрати наших клієнтів.

— аналітика в реальному часі — ця аналітика дозволяє виконувати спеціальні аналітичні запити в реальному часі, розраховувати оцінки ризиків, орієнтовані на організацію, та аналізувати поведінку користувачів на основі сценаріїв (наприклад, витік даних, зловживання привілейованими користувачами, а також аналітичні згортки на основі сценаріїв ризику витоку).

— рівень даних — облікові дані користувачів, права та ролі зберігаються в службі основних даних. Крім того, тут зберігаються кешовані дані програми, що пришвидшує час відповіді на запити [16].

— файли/вкладення — для тих стрічок подій, які містять файли та вкладення, Служба основних даних індексує вміст цих файлів для вкладень і, за бажанням, зберігає оригінальні вкладення для полегшення доступу кінцевого користувача та деталізації з інтерфейсу користувача. Це значно підвищує продуктивність аналітиків, дозволяючи інтегроване глибоке занурення в криміналістику безпосередньо з події, що отримала оцінку.

3. Служби користувацького інтерфейсу — рівень користувацького інтерфейсу Forcepoint - це веб-додаток, тоді як клієнтом є браузер. Сервер, на якому працює node.js HTTPS, використовується для всіх взаємодій між браузером і сервером, Redis - для кешування даних додатку, а також для сесій користувачів [16].

4. Вихідний API — Forcepoint надає послугу вихідного API, яка дозволяє зовнішнім програмам отримувати оброблені події та пов'язані з ними аналітичні метадані (наприклад, функції та моделі). Це дозволяє клієнтам використовувати аналітику Forcepoint в інших системах (наприклад, в оркестровці безпеки або робочому процесі).

3.2. Технологія захисту інформаційної системи від інсайдерських атак на базі рішення Forcepoint UEBA

Вимоги до кінцевого користувача [17]

Для використання Forcepoint UEBA потрібен сучасний веб-браузер.

- Chrome 65+
- Firefox 59 +
- Internet Explorer 11+

Вхід до користувацького інтерфейсу Forcepoint UEBA

Щоб увійти до Forcepoint UEBA:

1. Необхідно перейти за URL-адресою для входу в Forcepoint UEBA, яку надає адміністратор Forcepoint UEBA.
2. У вікні для входу ввести свою адресу електронної пошти та пароль.
3. Натиснути «Увійти» [17].

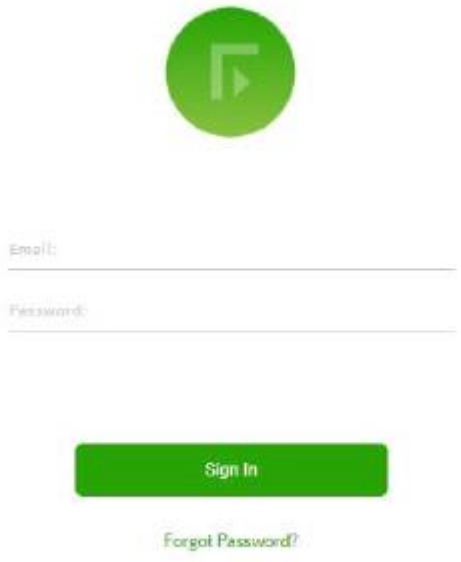

Рис. 3.3. Вікно логування

Навігація

Інтерфейс користувача (UI) Forcepoint UEBA складається з декількох сторінок, які використовуються для моніторингу та налаштування різних типів даних. Перехід на кожну сторінку здійснюється шляхом наведення курсору на піктограму шестерні та клацнувши на панелі навігації.

Рис. 3.4. Вікно навігації

Панель навігації забезпечує швидкий доступ до найбільш часто використовуваних частин програми [17].

Аналітика

Навігаційне посилання "Аналітика" містить 4 варіанти меню, що випадають при наведенні на нього.

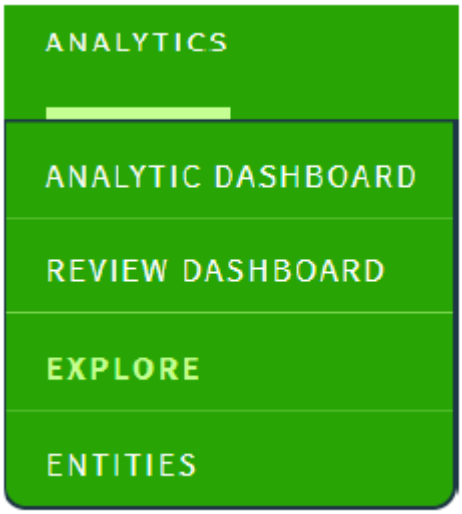

Рис. 3.5. Вкладка аналітики

Аналітична панель

Узагальнює дані про поведінку компаній і представляє 50 найцікавіших організацій, відсортованих за рівнем ризику, а також надає початкову інформацію про останні тенденції та поведінку з високим рівнем ризику.

Інформаційна панель

Перераховує всі події, відібрані для подальшого аналізу аналітиками Forcepoint UEBA. Ця сторінка дозволяє аналітикам легко переглядати, коментувати, позначати, закривати або ескалувати події в ефективний спосіб [17].

Дослідити

— надає вичерпний огляд подій на високому рівні.

— надає аналітикам можливість вільно шукати і досліджувати свої дані. сторінка Explore пропонує можливості пошуку за базовими (вибір попередньо налаштованих опцій) або розширеними (RQL-запит) критеріями пошуку по всіх даних Forcepoint UEBA Event.

— забезпечує детальний огляд подій та активності за допомогою різноманітних інформаційних карток.

— пропонує деталізацію безпосередньо до конкретних подій за допомогою засобу перегляду подій. Апертура може бути звужена за допомогою фільтрів пошуку або різних карток, щоб вибрати певні групи подій (ті, що відповідають певним аналітичним критеріям або включають певні дії) для заповнення Переглядача подій. Потім користувачі можуть знову розширити апертуру від конкретної події, показавши контекст і повторно заповнивши пошукові події на сторінці "Дослідити".

Сутності

— дозволяє користувачам ідентифікувати та перевіряти всі організації в Forcepoint UEBA.

— надає можливість досліджувати профілі окремих суб'єктів, включаючи розбивку їхніх псевдонімів, атрибутів суб'єкта, історичної активності та головних суб'єктів, з якими вони взаємодіють.

— вибір суб'єкта перенаправляє користувачів на сторінку з деталями про суб'єкта. На цій сторінці можна заглибитися в конкретну діяльність вибраної сутності, а також додати і відредагувати її функції та атрибути [17].

Сторінка Поведінки

— використовується для глибокого занурення в сценарій і вивчення об'єктів, чия діяльність у цьому сценарії відзначена найвищою мірою. Діяльність об'єкта для кожного сценарію далі розбивається на моделі та події, які можна дослідити у вікні перегляду подій.

— надає візуальну аналітичну інформацію у вигляді теплових карт поведінки, які відображаються на конфігурованій часовій шкалі. Рядки цих теплових карт позначені кольором відповідних моделей, а кожній інтервальній матриці присвоюється колірна непрозорість на основі оцінки інтервалу.

Рис. 3.6. Вигляд Dashboard

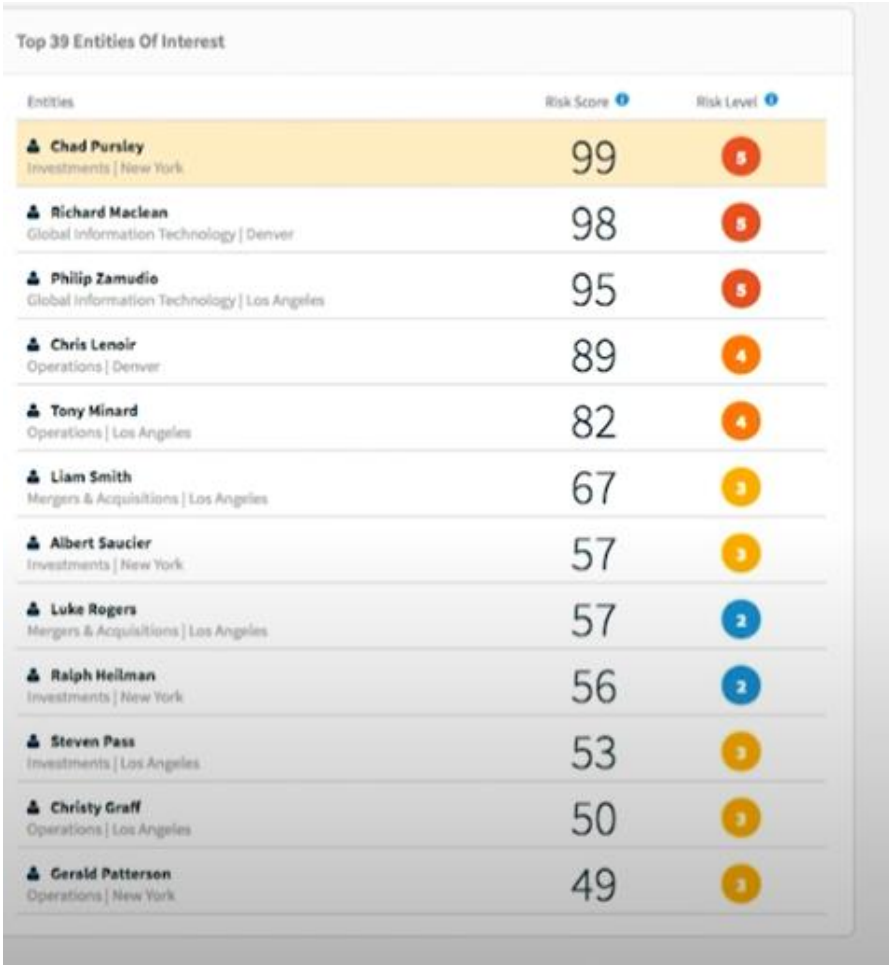

Рис. 3.7. Ліва частина Dashboard з рівнем та значенням ризику тієї чи іншої персони

Рис. 3.8. Права частина Dashboard графічна з застосованим сценарієм та порівняльним значенням

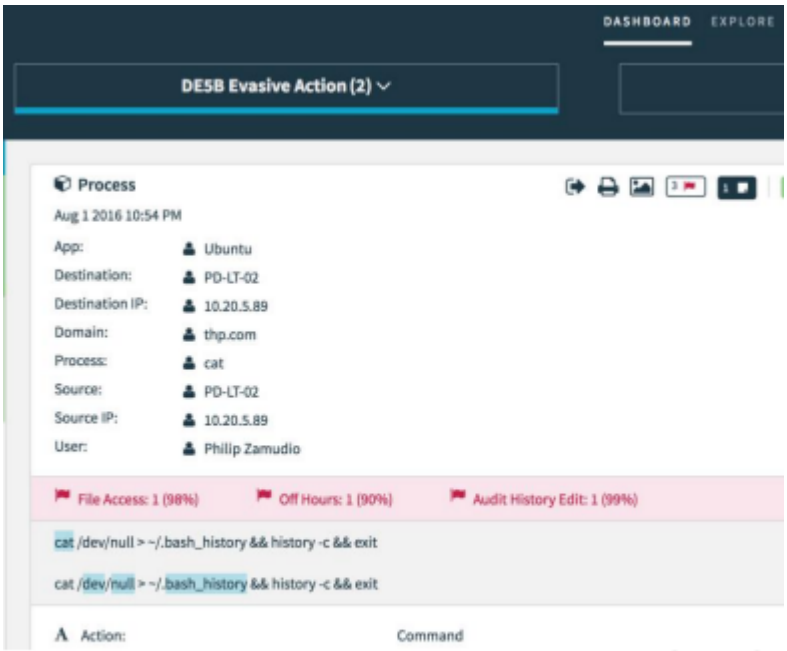

Рис. 3.9. Огляд події спрацювання процесу що є загрозою

Рис. 3.10. Часовий показник спрацювань із рівнем загрози

Вибравши відповідне спрацювання можна натиснути на нього і перейти до глибокого розслідування рис. 3.11.

Глибоке розслідування дозволяє переглянути які політики були порушені тим чи іншим користувачем, а також які зловмисні дії виконав інсайдер. Розглянемо приклад з нелегальним товаром рис. 3.12.

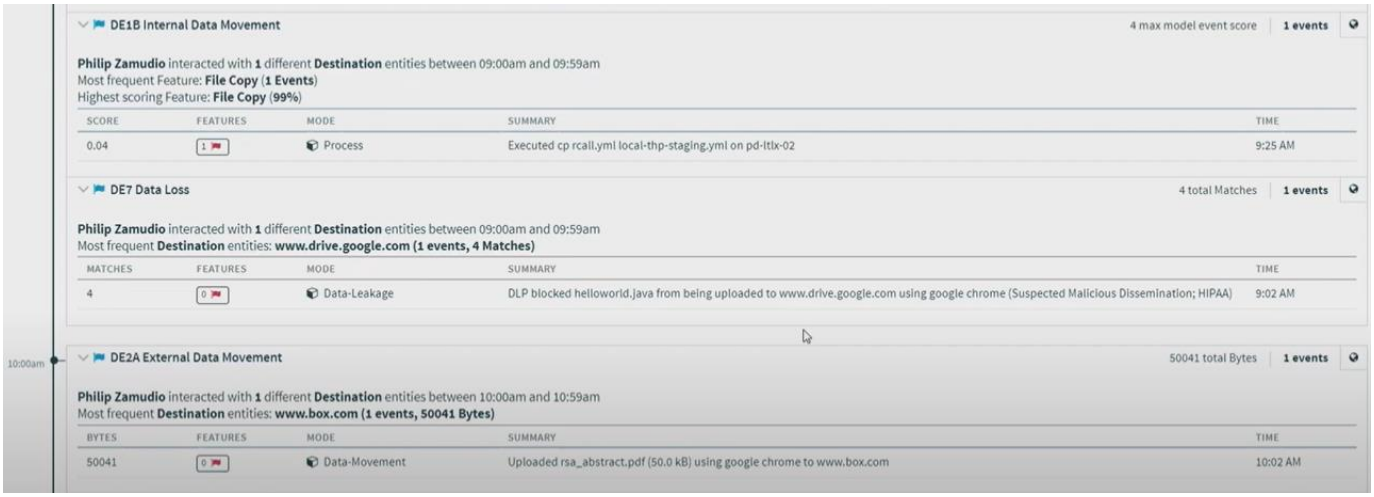

Рис. 3.11. Інформація про порушені політики UEBA

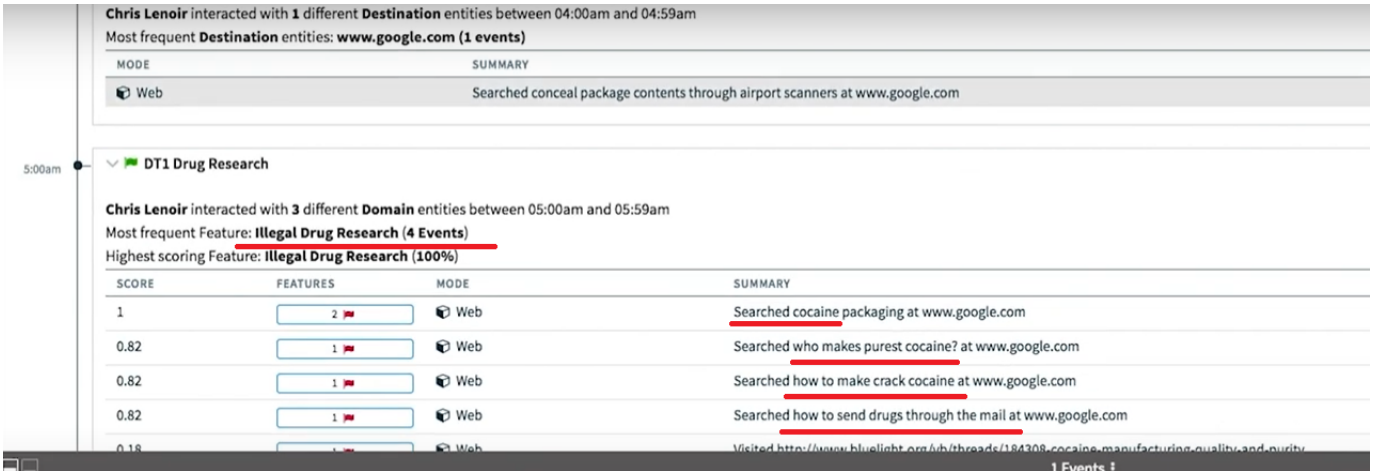

Рис. 3.12. Виявлення події пошуку наркотичних препаратів

З рис. 3.12 бачимо про пошук в системі google наркотичних препаратів з 5-ї ранку. Рівень небезпеки 100% все відбувалося з Web переглядача [17]. Натискаючи на особливості спрацювання (Features) переходимо до глибинного огляду події, в якій видно дані інсайдера та про, що йшла мова стосовно заборонених речовин рис. 3.13

Рис. 3.13. Вміст листування інсайдера

Нікому не таємниця, що один програмний засіб не забезпечить 100% захист організації. Тому обов'язково необхідна інтеграція з іншими технологіями захисту для надійнішого захисту наприклад як на рис. 3.14.

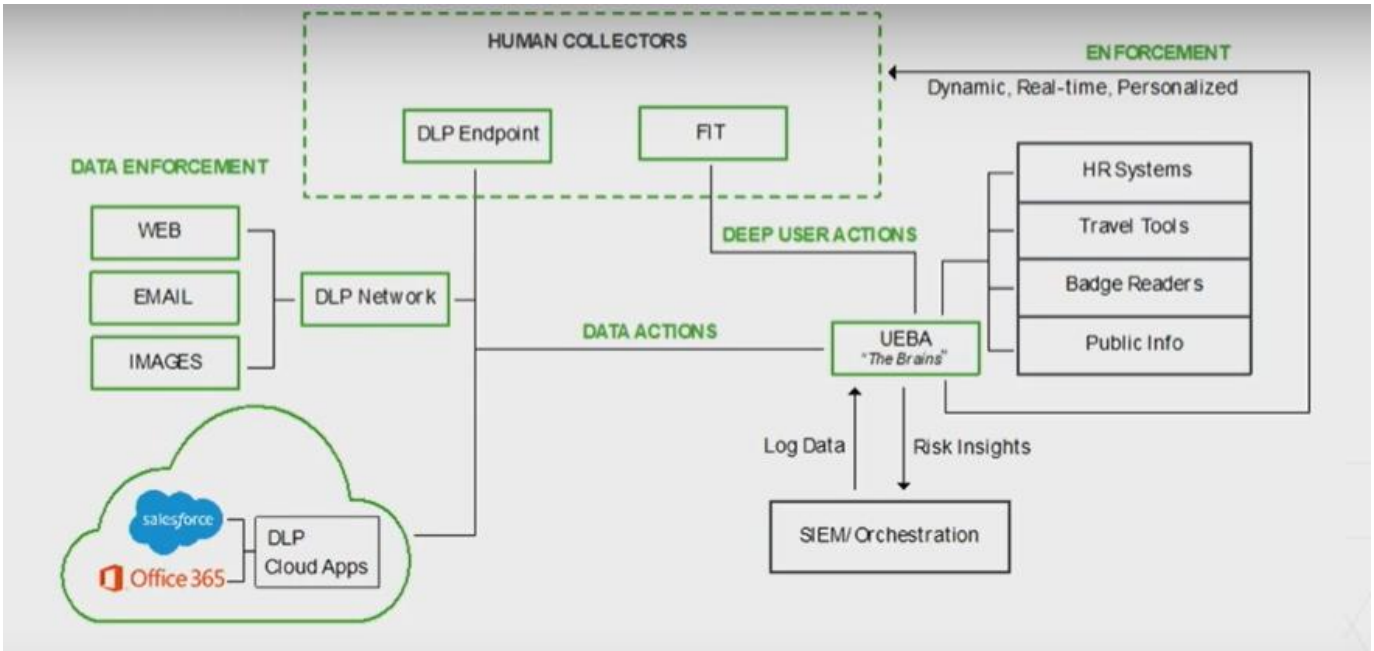

Рис. 3.14. Схема розміщення UEBA в ІС підприємства

Forcepoint легко інтегрується з комунікаційними, захисними та іншими корпоративними додатками, що використовуються в даний час. Вбудовані власні аналітичні моделі Forcepoint аналізують інформацію з усіх підрозділів підприємства, щоб сформувати цілісне уявлення про поведінкові ризики [17].

3.3. Розроблення рекомендацій щодо застосування технології захисту інформаційної системи від інсайдерських атак на базі рішення Forcepoint UEBA

Для забезпечення надійного захисту ІС від інсайдерських атак на базі рішення Forcepoint UEBA (FUEBA) необхідно дотримуватись наступних рекомендацій:

1. Врахування досвіду попередніх інцидентів при розгортанні та налаштуванні FUEBA.

2. Концентрація на захисті критично важливих ресурсів.

3. Інтеграція з іншими системами захисту таких як: DLP, SIEM, IDS, log management and analisys тощо.

4. Оптимізація аналізу поведінки при налаштуванні FUEBA для відстеження індивідуальних і групових активностей.

5. Регулярне навчання моделей аналізу поведінки для підтримання точності виявлення загроз.

6. Навчання персоналу згідно потенційної посади.

7. Приділення уваги перепризначенням та звільненням осіб, а також аналіз змін у звичайному графіку роботи, що свідчать про не притаманну активність.

8. Інтеграція з PAM для управління та моніторингу доступу до привілейованих облікових записів.

9. Автоматизація реагування на ІЗ за допомогою відповідних правил.

10. Активна співпраця з командою безпеки для постійного вдосконалення стратегій та заходів протидії інсайдерським загрозам.

Висновок до розділу 3

В розділі проаналізовано можливості та архітектура FUEBA. Розглянуто графічний інтерфейс та меню ПЗ. Додатково проведено аналіз спрацьованих подій щодо інсайдерської загрози на базі рішення FUEBA.

Розроблено рекомендації щодо застосування технології захисту інформаційної системи від інсайдерських атак на базі рішення Forcepoint UEBA.

ВИСНОВКИ

З урахуванням складнощів у виявленні та протидії інсайдерським атакам, важливо розробляти та впроваджувати ефективні стратегії забезпечення кібербезпеки.

В розділі 1 проаналізовано актуальність проблеми інсайдерських атак, приведено статистику дослідницьких інститутів за 2023 рік. Представлено типи інсайдерських атак та їх наслідків, а також визначено потенційні індикатори ризику інсайдерських атак.

В розділі 2 було досліджено програмні методи захисту від інсайдерських атак, а саме Data Loss Prevention, Privileged Access Management, User and Entity Behavior Analytics, Security Information and Event Management, Endpoint Detection and Response, Insider Threat Management, проведений їх аналіз в якому виділені переваги та недоліки кожного з них. Систематизовано дані переваги та недоліки в узагальнену порівняльну таблицю. Приведені рекомендації протидії інсайдерським загрозам згідно CERT-UA (Computer Emergency Response Team of Ukraine) спеціалізованого структурного підрозділу Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.

В розділі 3 проаналізовано можливості та архітектура FUEBA. Розглянуто графічний інтерфейс та меню ПЗ. Додатково проведено аналіз спрацьованих подій щодо інсайдерської загрози на базі рішення FUEBA.

Розроблено рекомендації щодо застосування технології захисту інформаційної системи від інсайдерських атак на базі рішення Forcepoint UEBA.

Ці рекомендації становлять комплексний підхід до захисту інформаційної системи від інсайдерських атак за допомогою технології Forcepoint UEBA.

ПЕРЕЛІК ПОСИЛАНЬ

1. Денисенко Д. Б. Захист інформаційної системи від інсайдерських атак. Актуальні проблеми кібербезпеки : Всеукр. науково-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 91–93.

2. Defining Insider Threats | CISA. Cybersecurity and Infrastructure Security Agency CISA. URL: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats (дата звернення: 04.10.2023).

3. Insider Threat: How to Identify, Prepare For, and Prevent Insider Threats. Flashpoint. URL: https://flashpoint.io/blog/insider-threat/ (дата звернення: 08.10.2023).

4. Insider Threat Statistics for 2023: Facts, Reports & Costs | Ekran System. Ekran System. URL: https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures (дата звернення: 10.10.2023).

5. 2023 Data Breach Investigations Report. Verizon Business. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 10.10.2023).

6. What is the best strategy for protecting against insider threats. Ekran System. URL: https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures#id-what-is-the-best-strategy-for-protecting-against-insider-threats (дата звернення: 01.11.2023).

7. What is Data Loss Prevention (DLP)? Definition, Types & Tips. Digital Guardian. URL: https://www.digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention (дата звернення: 01.11.2023).

8. What is privileged access management (PAM)?. microsoft. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam#:~:text=Privileged%20access%20management%20(PAM)%20is,privileged%20access%20to%20critical%20resources. (дата звернення: 02.11.2023).

9. What Is UEBA? Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/what-is-

ueba#:~:text=UEBA%20Definition,and%20endpoints%20in%20that%20network. (дата звернення: 02.11.2023).

10. What is Security Information and Event Management (SIEM)? | IBM. IBM in Deutschland, Österreich und der Schweiz | IBM. URL: https://www.ibm.com/topics/siem (date of access: 02.11.2023).

11. Aarness A. What is EDR? Endpoint Detection & Response Defined. crowdstrike.com. URL: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (дата звернення: 02.11.2023).

12. Best Insider Risk Management Solutions Reviews 2023 | Gartner Peer Insights. Gartner. URL: https://www.gartner.com/reviews/market/insider-risk-management-solutions (дата звернення: 02.11.2023).

13. CUA-15-04R Рекомендації CERT-UA з протидії загрозі інсайдера. cert. URL: https://cert.gov.ua/files/pdf/CUA-15-04R.pdf (дата звернення: 06.11.2023).

14. Forcepoint UEBA User Manual. forcepoint. URL: https://www.websense.com/content/support/library/ueba/v30/user_manual/user_manual.pdf (дата звернення: 22.11.2023).

15. GDPR Technology Mapping Guide - PDF Free Download. Enjoy free comfortable tools to publish, exchange, and share any kind of documents online!. URL: https://docplayer.net/76388838-Gdpr-technology-mapping-guide.html (дата звернення: 22.11.2023).

16. Forcepoint Behavioral Analytics Platform architecture overview: From data to behavior insights–functional architecture. forcepoint. URL: https://www.forcepoint.com/sites/default/files/resources/datasheets/ueba-platform-architecture-overview.pdf (дата звернення: 23.11.2023).

17. Forcepoint UEBA User Manual. websense. URL: https://www.websense.com/content/support/library/ueba/v30/user_manual/user_manual.pdf (дата звернення: 25.11.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)