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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту організації від інсайдерських атак»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Владислав ІГНАТЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
ІГНАТЕНКО Владислав
(прізвище, ім'я)

Керівник д.ф., МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

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

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
“___” жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

ІГНАТЕНКУ Владиславу Олександровичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Технологія захисту організації від інсайдерських атак»

керівник кваліфікаційної роботи МАРЧЕНКО Віталій Вікторович, д.ф.
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» жовтня 2024 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
UEBA ActivTrak;
ідентифікатори інсайдерських атак;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз необхідності захисту організації від інсайдерських атак.
2. Методи та засоби захисту від інсайдерських атак.
3. Розроблення варіанта технології захисту організації від інсайдерських атак на базі рішення UEBA ActivTrak.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми	01.10.2024 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	12.10.2024 р.	
3.	Аналіз необхідності захисту організації від інсайдерських атак	27.10.2024 р.	
4.	Методи та засоби захисту від інсайдерських атак	03.11.2024 р.	
5.	Розроблення варіанта технології захисту організації від інсайдерських атак на базі рішення UEBA ActivTrak	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Владислав ІГНАТЕНКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ІГНАТЕНКА Владислава
на тему: Технологія захисту організації від інсайдерських атак

Актуальність:
Технології відіграють ключову роль у запобіганні та виявленні інсайдерських загроз. Наприклад, системи автентифікації та управління ідентифікацією (IAM) дозволяють контролювати доступ до ресурсів, забезпечуючи, що користувачі мають лише той доступ, який їм потрібен. Інструменти запобігання втраті даних (DLP) можуть відстежувати та блокувати несанкціоновану передачу конфіденційної інформації. Сегментація мережі обмежує доступ до різних сегментів інфраструктури, зменшуючи ризики для важливих активів. Моніторинг активності та ведення журналів дозволяють збирати інформацію про дії користувачів, а плани реагування на інциденти готують організацію до швидкого реагування на виявлені загрози. Одним із таких рішень є ActivTrak UEBA (User and Entity Behavior Analytics) — це потужна платформа, яка дозволяє аналізувати поведінку користувачів, щоб виявити аномалії, пов'язані з потенційними інсайдерськими загрозами. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:
1. На основі проведеного аналізу, в роботі встановлено зміст проблеми забезпечення захисту організації від інсайдерських атак.
2. Досліджено методи та засоби захисту організації від інсайдерських атак.
3. Запропоновано варіант технології захисту організації від інсайдерських атак на базі рішення ActivTrak.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:
1. У кваліфікаційній роботі доцільно було б проаналізувати ActivTrak у порівнянні з іншими рішеннями UEBA та привести порівняльну таблицю переваг та недоліків.
2. Доцільно б було продемонструвати інтеграцію даного рішення до інших систем таких як: SIEM, DLP, IAM і відобразити результати їх взаємодії.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **ІГНАТЕНКО Владислав** - присвоєння кваліфікації магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач ІГНАТЕНКО Владислав до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: на тему: «Технологія захисту організації від інсайдерських атак».
Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ІГНАТЕНКО Владислав*** обрав тему роботи, метою якої було розробити варіант технології захисту організації від інсайдерських атак на базі рішення ActivTrak та рекомендації щодо її застосування. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ІГНАТЕНКО Владислав*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ІГНАТЕНКА Владислава*** на оцінку **"добре"** та присвоїти йому кваліфікацію магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ІГНАТЕНКО Владислав** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 60 сторінок, 36 рисунків, 1 таблиця, 20 джерел.

Об'єкт дослідження – захист організації від інсайдерських атак.

Предмет дослідження – технологія захисту організації від інсайдерських атак на базі рішення ActivTrak.

Мета роботи – розробити варіант технології захисту організації від інсайдерських атак на базі рішення ActivTrak та рекомендації щодо її застосування.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів, аналіз ризиків та загроз, тестування технології захисту організації від інсайдерських атак на базі рішення ActivTrak.

В роботі проведено аналіз необхідності захисту організації від інсайдерських атак. Класифіковано типи інсайдерських загроз та приведені основні ідентифікатори.

Досліджено методи та засоби захисту організації від інсайдерських атак.

Запропоновано варіант технології захисту організації від інсайдерських атак на базі рішення ActivTrak UEBA. Визначено призначення, основні функції та склад компонентів даної технології.

На основі проведених досліджень, в роботі отримано варіант технології захисту організації від інсайдерських атак на базі рішення ActivTrak UEBA

Галузь використання – кібербезпека організації.

ІНСАЙДЕРСЬКА ЗАГРОЗА, UEBA, КОНФІДЕНЦІЙНІСТЬ, МЕТОДИ ТА ЗАСОБИ, РЕКОМЕНДАЦІЇ, АРХІТЕКТУРА, ФУНКЦІЇ, ЗАХИСТ, ВНУТРІШНІ ЗАГРОЗИ

ABSTRACT

Text part of the master's qualification work: 60 pages, 36 figures, 1 table, 20 sources.

Object of research is to protect the organization from insider attacks.

Subject of research is the technology of protecting an organization from insider attacks based on the ActivTrak solution.

The purpose of the work is to develop a variant of the technology for protecting the organization from insider attacks based on the ActivTrak solution and recommendations for its use.

Research methods - studying the literature on this topic, analyzing operational documentation, international standards, analyzing risks and threats, testing the technology of protecting the organization from insider attacks based on the ActivTrak solution.

The paper analyzes the problem of protect an organization from insider attacks. The types of insider threats are classified and the main identifiers are given.

The methods and means of protecting the organization from insider attacks are studied.

A variant of the technology for protecting an organization from insider attacks based on the ActivTrak UEBA solution is proposed. The purpose, main functions and composition of the components of this technology are determined.

Based on the research, the paper presents a variant of the technology for protecting an organization from insider attacks based on the ActivTrak UEBA solution.

The field of use is cybersecurity of the organization.

INSIDER THREAT, UEBA, PRIVACY, METHODS AND TOOLS, RECOMMENDATIONS, ARCHITECTURE, FUNCTIONS, PROTECTION, INSIDER THREATS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІА	—	інсайдерська атака
ІЗ	—	інсайдерська загроза
VPN	—	Virtual Private Network
DLP	—	Data Loss Prevention
PAM	—	Privileged Access Management
IAM	—	Identity and Access Management
SIEM	—	Security Information and Event Management
GDPR	—	General Data Protection Regulation
CCPA	—	California Consumer Privacy Act
UEBA	—	User and Entity Behavior Analytics
ML	—	Machine Learning
URL	—	Uniform Resource Locator

ВСТУП

Актуальність дослідження. Інсайдерські загрози є одним із найнебезпечніших видів кібератак, адже вони походять від осіб, які мають доступ до внутрішніх ресурсів організації, таких як співробітники, підрядники або партнери. Сучасні інсайдерські атаки можуть мати значні наслідки: витік конфіденційної інформації, фінансові втрати, порушення операцій та шкоду репутації. Згідно [1-2], витрати на інциденти інсайдерських загроз зростають, оскільки організації стають більш вразливими через збільшення кількості віддалених працівників та комплексніші інфраструктури.

Інсайдерські загрози стали реальністю для цивільних компаній, таких як Tesla, яка зазнала саботажу та крадіжки інтелектуальної власності, та Capital One, яка постраждала від шахрайства. Ще більший суспільний резонанс викликав витік даних у Міністерстві оборони США, здійснений відомими зловмисниками Челсі Меннінг та Едвардом Сноуденом, чия шпигунська та хактивістська діяльність широко відома. Різке збільшення кількості подібних інцидентів в останні роки і незліченна шкода, завдана інсайдерами, повинні служити застереженням для всіх членів спільноти кібербезпеки [1].

Оскільки нормативно-правові вимоги, такі як GDPR, HIPAA і CCPA, зобов’язують організації захищати дані та забезпечувати контроль доступу до конфіденційної інформації. Технології, які застосовуються для запобігання інсайдерським атакам, мають сприяти відповідності цим вимогам, забезпечуючи комплексний контроль та прозорість дій користувачів.

Таким чином, поведінкова аналітика є ефективним для ідентифікації інсайдерських загроз. Впровадження цієї технології захисту організації від інсайдерських атак, UEBA, встановлює базові профілі поведінки та виявляє відхилення від них, що вказує на можливі інсайдерські дії, відповідає нормативно-правовим вимогам і допомагає організаціям захищати свою інформацію. Тому тема кваліфікаційної роботи «Технологія захисту організації від інсайдерських атак» є актуальною.

Об'єкт дослідження – захист організації від інсайдерських атак.

Предмет дослідження – технологія захисту організації від інсайдерських атак на базі рішення ActivTrak.

Мета роботи – розробити варіант технології захисту організації від інсайдерських атак на базі рішення ActivTrak та рекомендації щодо її застосування.

Наукові завдання:

- провести аналіз питання щодо необхідності захисту організації від інсайдерських атак;
- проаналізувати основні типи інсайдерських загроз та основні ідентифікатори;
- дослідити методи та засоби захисту організації від інсайдерських атак;
- розробити варіант технології захисту організації від інсайдерських атак на базі рішення ActivTrak UEBA та рекомендації щодо застосування даної технології. Визначити призначення, основні функції та склад компонентів даної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів, аналіз ризиків та загроз, тестування технології захисту організації від інсайдерських атак на базі рішення ActivTrak.

Практичне значення одержаних результатів полягає в розробці технології захисту організації від інсайдерських атак на базі рішення ActivTrak UEBA та рекомендації щодо застосування даної технології не тільки до віддалених працівників, але й до гібридної праці чи в офісі.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки» [1].

1 АНАЛІЗ НЕОБХІДНОСТІ ЗАХИСТУ ОРГАНІЗАЦІЇ ВІД ІНСАЙДЕРСЬКИХ АТАК

1.1. Аналіз необхідності захисту від інсайдерських атак

Інсайдерські загрози, зумовлені особистими мотивами, а також швидким розвитком технологій і гібридним робочим середовищем, становлять серйозний виклик для безпеки організації. Протидія цим загрозам вимагає складного, багатогранного підходу, який поєднує в собі передові технології виявлення, постійний моніторинг і сильний акцент на навчанні та обізнаності співробітників.

Новий звіт Cybersecurity Insiders і Securonix [2], заснований на опитуванні 467 фахівців з кібербезпеки, розкриває природу внутрішніх загроз, з якими стикаються організації, зосереджуючись на розумінні факторів, що зумовлюють ці загрози, складнощів їх виявлення і пом'якшення, а також на ефективності програм протидії внутрішнім загрозам. Звіт дає уявлення про те, як компанії адаптують свої стратегії і рішення для ефективної боротьби з внутрішніми ризиками безпеки:

Зростання кількості інсайдерських атак: З 2019 по 2024 рік кількість організацій, які повідомили про інсайдерські атаки, зросла з 66% до 76%, що свідчить про значне збільшення кількості виявлених внутрішніх загроз. Зокрема, зросла кількість інцидентів з кількома атаками на рік, що підкреслює нагальну потребу в удосконаленні стратегій виявлення та пом'якшення наслідків, включаючи постійний моніторинг та проактивний захист [2].

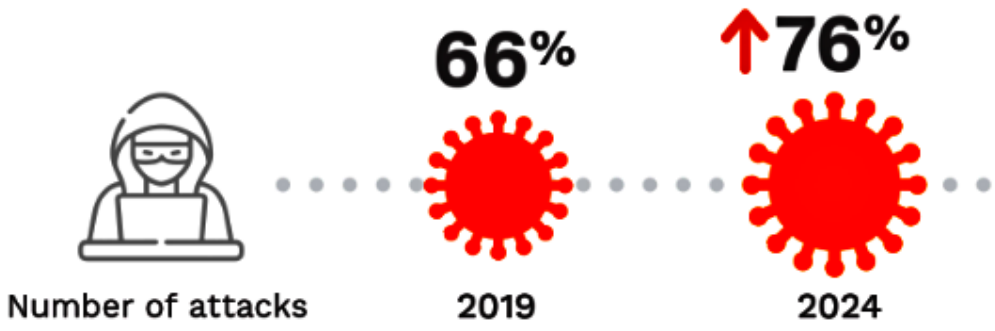


Рис. 1.1. Статистика зростання Інсайдерських атак з 2019 по 2024 роки [2]

Інсайдери з високим рівнем ризику та їхні мотиви: Помітно зросла стурбованість зловмисними діями інсайдерів - з 60% у 2019 році до 74% у 2024 році, що свідчить про підвищену обізнаність або досвід навмисних інсайдерських атак.

Виявлення внутрішніх та зовнішніх атак: 90% респондентів повідомляють, що виявити внутрішні атаки так само або навіть складніше, ніж зовнішні, що підкреслює складність внутрішніх загроз. Лише 16% організацій вважають, що вони надзвичайно ефективно протидіють внутрішнім загрозам, що є покращенням у порівнянні з 11% у 2019 році, але все ще існує значний простір для вдосконалення стратегій управління загрозами [2].

Загроза програм-вимагачів: 76% організацій повідомляють про зростаючу поширеність програм-вимагачів і методів потрійного вимагання в їхніх середовищах, що підкреслює зростаюче занепокоєння з приводу кібербезпеки. Розголошення інформації (56%) та несанкціоновані операції з даними (48%) також викликають найбільше занепокоєння, що підкреслює важливість заходів безпеки, орієнтованих на дані, та надійних засобів управління ідентифікацією та доступом.

Рис. 1.2. Відсоткове відношення організацій, що повідомляють про поширеність програм-вимагачів [2]

Гібридна робота та технології, що розвиваються: 70% респондентів висловлюють занепокоєння щодо інсайдерських ризиків в умовах гібридної

роботи, що відображає проблеми захисту розподілених, менш контрольованих середовищ. Більшість (75%) стурбовані впливом нових технологій, таких як штучний інтелект, метапростір і квантові обчислення, на внутрішні загрози, що свідчить про занепокоєння щодо їх зловживань і потенціалу посилення загроз.

Зрілість програм протидії внутрішнім загрозам: Хоча 66% організацій відчувають вразливість до внутрішніх атак, 41% організацій лише частково впровадили програми протидії внутрішнім загрозам, що вказує на відсутність комплексного моніторингу діяльності та передового управління загрозами. Лише 29% респондентів вважають, що вони повністю забезпечені необхідними інструментами для захисту від внутрішніх загроз, що свідчить про значну прогалину в можливостях безпеки багатьох організацій.

1.2. Класифікація інсайдерських загроз та основні ідентифікатори інсайдерських атак

Внутрішні загрози являють собою складний і динамічний ризик, що впливає на державні та приватні сфери всіх секторів критичної інфраструктури. Визначення цих загроз є 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 використає свій санкціонований доступ, навмисно чи ненавмисно, щоб завдати шкоди місії, ресурсам, персоналу, об'єктам, інформації, обладнанню, мережам або системам відомства. Внутрішні загрози проявляються по-різному: насильство, шпигунство, саботаж, крадіжки та кібератаки.

Інсайдер — це будь-яка особа, яка має або мала санкціонований доступ до ресурсів організації, включно з персоналом, приміщеннями, інформацією, обладнанням, мережами та системами, або володіє знаннями про них [3].

Прикладами інсайдерів можуть бути:

- особа, якій організація довіряє, включно з працівниками, членами організації та тими, кому організація надала конфіденційну інформацію та доступ;

- особа, якій видали бейдж або пристрій доступу, що ідентифікує її як особу з постійним (напр., працівник або член організації, підрядник, постачальник, зберігач або ремонтник);

- особа, якій організація надала комп'ютер та/або доступ до мережі;

- особа, яка розробляє продукти та послуги організації; до цієї групи належать ті, хто знає секрети продуктів, що створюють цінність для організації;

- особа, яка обізнана з основами діяльності організації, включно з ціноутворенням, витратами, а також сильними та слабкими сторонами організації;

- особа, яка обізнана з бізнес-стратегією та цілями організації, якій довірені плани на майбутнє або засоби підтримки організації та забезпечення добробуту її працівників;

- у контексті державних функцій інсайдером може бути особа, яка має доступ до інформації з обмеженим доступом, що, у разі компрометації, може завдати шкоди національній та громадській безпеці [3].

Інсайдерська загроза (ІЗ) – ризик заподіяння шкоди організації людьми, які знаходяться всередині контуру організації. До таких людей – їх називають інсайдерами – можуть бути як колишні, так і нинішні співробітники самої компанії, і фахівці підрядників або партнерів, тобто кожен, хто має доступ до конфіденційної інформації і критичної інфраструктури компанії.

Інсайдерська атака (ІА) – це зловмисна атака, здійснена в мережі чи комп’ютерній системі особою, яка має дозвіл на доступ до системи.

Зловмисні інсайдерські загрози часто з'являються через навмисне зловживання співробітниками інформацією, додатками або базами даних компанії. Вони мають привілеї перед іншими зловмисниками, оскільки знайомі з політиками та процедурами безпеки компанії та її вразливими місцями. Зазвичай вони мають намір використати свій доступ для крадіжки інформації або виведення системи з ладу з особистих, грошових або деструктивних міркувань. Прикладом внутрішньої загрози кібербезпеки може бути продаж співробітником конфіденційної інформації конкуренту.

Зловмисні або навмисні загрози поділяються [4]:

1. Колаборантів (Collaborators).

Зазвичай, колаборанти - це авторизовані користувачі в організації, які таємно співпрацюють з третьою стороною, щоб навмисно завдати шкоди організації. Вони схильні до витоку, обміну та продажу конфіденційних даних третім особам, тим самим порушуючи бізнес-операції. Третіми сторонами можуть бути конкуренти, національні держави, злочинні організації або навіть окремі особи.

2. Вовки-одинаки (Lone wolves).

Вони працюють незалежно і діють без зовнішньої підтримки або впливу. Вовки-одинаки особливо шкідливі, оскільки мають привілейований доступ до системи. Наприклад, колишній працівник, який затаїв образу, може зловживати активами.

Ненавмисні (Careless) загрози — вони виникають через людські помилки, коли людина може випадково піддати систему атакам шкідливого програмного забезпечення. Помилками можна вважати брак розсудливості, ненавмисну допомогу та підтримку, фішинг, шкідливе програмне забезпечення та викрадену ліцензію. Ненавмисні загрози також бувають різних типів [4]:

1) Пішаки (Pawn).

Користувачі, які мають офіційний контроль над системами організації, спроектовані так, щоб діяти зловмисно і ненавмисно завдати шкоди системі організації, називаються пішаками. Зазвичай це робиться за допомогою методів соціальної інженерії, таких як фішинг зі списом, щоб завантажити шкідливе програмне забезпечення на комп'ютер або розкрити конфіденційні дані з метою шахрайства.

2) Дурень (Goof).

На відміну від пішака, який ненавмисно завдає шкоди системі, дурень навмисно вчиняє деструктивні дії. Це можуть бути зарозумілі, недосвідчені та неефективні користувачі, які не вважають за потрібне дотримуватися правил і норм безпеки. Приклад користувач, який зберігає приватні дані клієнтів на власному пристрої, навіть якщо це суперечить політиці безпеки.

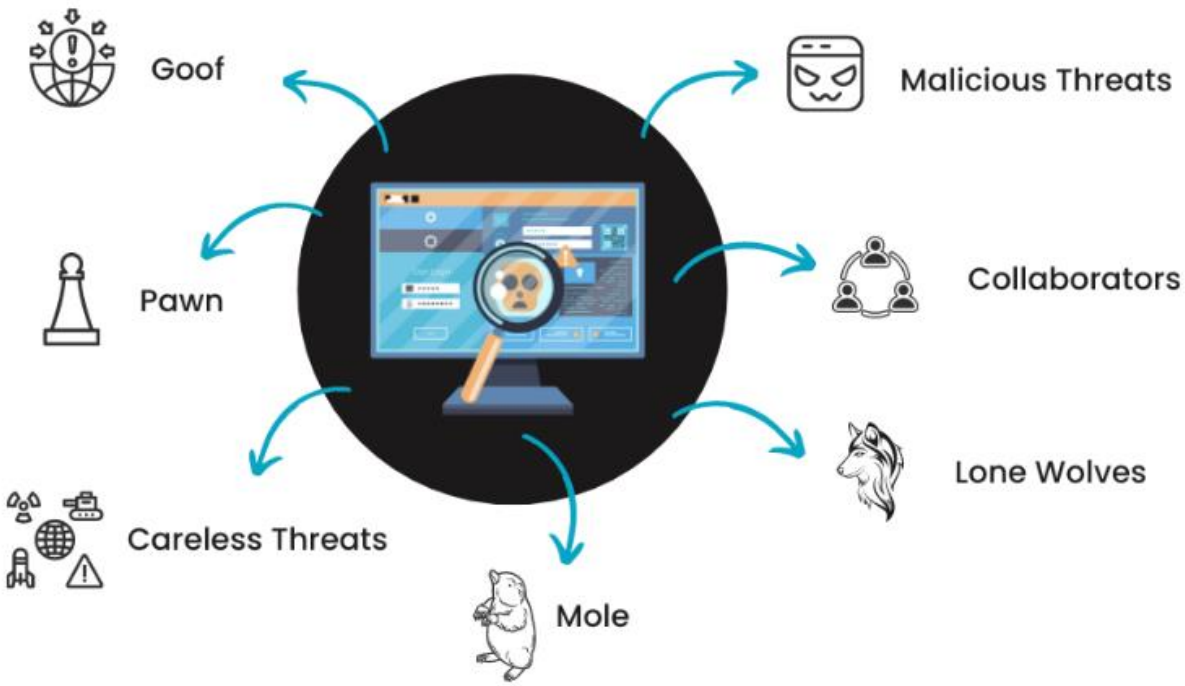


Рис. 1.3. Різновиди інсайдерських загроз [4]

Шпигун (A mole) - це стороння особа, яка отримала внутрішній доступ до систем організації. Це може бути постачальник, партнер, трейдер або працівник. Таким чином, вони отримують переважний контроль, який вони не змогли б отримати в інший спосіб.

Існує дві основні категорії індикаторів: поведінкові та цифрові. Обидва типи активності можуть вказувати на потенційно зловмисну діяльність, яку потрібно розслідувати (таблиця 1.1).

Таблиця 1.1.

Індикатори інсайдерських атак

Поведінкові	**Цифрові**
Нещасний або незадоволений працівник, трейдер, постачальник або партнер	Нетиповий вхід у додатки та мережі компанії
Ті що очікують відставку	Раптове зростання обсягу мережевого трафіку
Неприязнь до колег	Використання несанкціонованих пристроїв, таких як USB-накопичувачі
Постійно працює в неробочий час	Доступ до ресурсів, до яких вони не мають права доступу
Спроби перешкоджання безпеці	Проникнення в мережу та цілеспрямований пошук конфіденційних даних
Регулярне порушення організаційної політики	Пошук даних, які не стосуються їхніх посадових обов'язків
	Надсилання важливих даних електронною поштою за межі організації

1.3. Типи критичних даних та потенційні наслідки від інсайдерських загроз

Типи даних, які найбільше піддаються ризику інсайдерських атак, відображають як цінність, так і доступність цієї інформації в організації.

Фінансові дані вважаються найбільш вразливими, 44% респондентів відзначили їх, ймовірно, через їхній потенціал прямої монетизації. За ними йдуть дані про клієнтів (41%), що вказує на занепокоєння щодо втрати інформації, яка дозволяє ідентифікувати особу (PII). Дані про співробітників також викликають значне занепокоєння (37%), що свідчить про усвідомлення ризиків, пов'язаних з неналежним поводженням з конфіденційною інформацією про персонал [2]. Варто зазначити, що 31% респондентів вважають, що всі конфіденційні дані компанії є вразливими, що відображає більш широке занепокоєння щодо безпеки організаційних даних.

Проактивні заходи, такі як контроль доступу до даних, шифрування та навчання співробітників, можуть зменшити ризик інсайдерських атак та загрози конфіденційності, цілісності та доступності даних. Наголос на захисті найбільш вразливих фінансових даних, даних про клієнтів і співробітників в рамках комплексної стратегії безпеки даних є обов'язковим.

Найбільший вплив на організації мала крадіжка та витік даних, на які припадає 32% інцидентів, на які реагувала X-Force, що становить 19% від загальної кількості інцидентів у 2022 році. Це зростання відповідає зростанню активності інфозлодіїв та використанню законних інструментів для витоку даних. Крім того, у 2023 році кількість інцидентів з вимаганням зросла більш ніж удвічі, а частка всіх інцидентів, які були пов'язані з вимаганням, збільшилася з 21% у 2022 році до 24% у 2023 році.

Рис. 1.4. Типи даних під загрозою інсайдерських атак

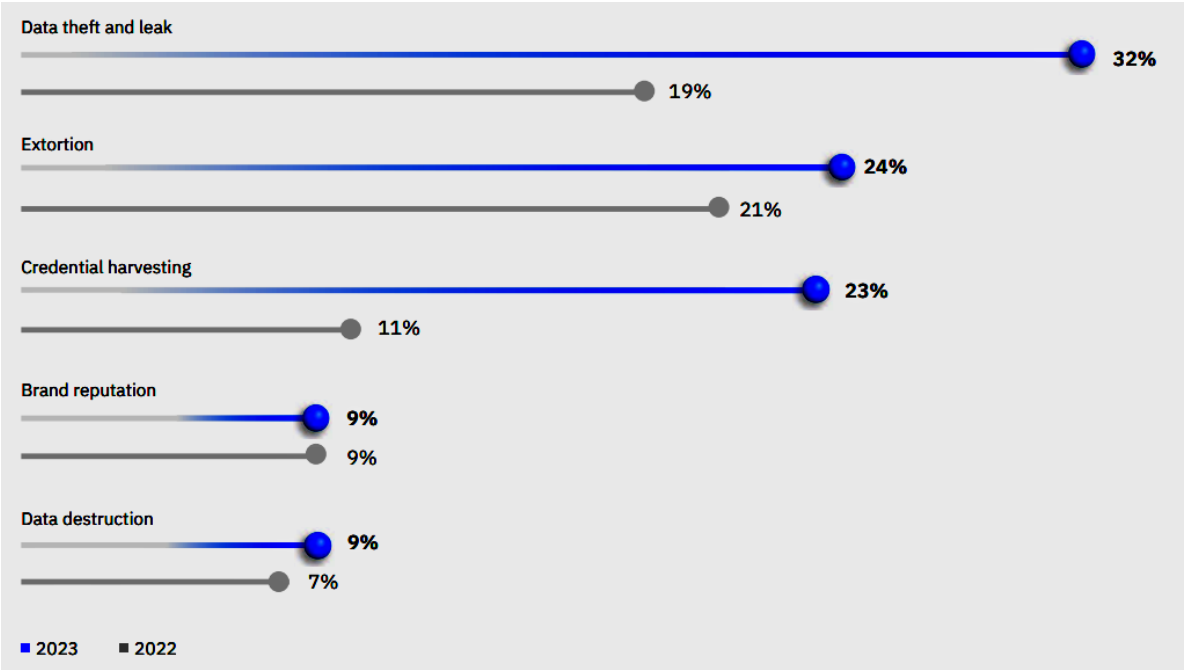


Рис. 1.5. Основні наслідки, які X-Force спостерігали під час операцій з реагування на інциденти у 2023 році [5]

Як уже згадувалося, у 2023 році атаки з вимаганням залишалися однією з рушійних сил кіберзлочинності, причому зловмисники використовували різні типи атак для досягнення своїх цілей з вимагання [5].

Висновки до розділу 1

1. Проведено аналіз необхідності захисту організацій від інсайдерських атак з приведенням статистики стрімкого зростання.

2. Проведено класифікацію інсайдерських загроз та наведені основні ідентифікатори інсайдерських атак.

3. Проведено типи критичних даних та потенційні наслідки від інсайдерських атак на основі звіту IBM X-Force.

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ВІД ІНСАЙДЕРСЬКИХ АТАК

2.1. Методи та засоби захисту від інсайдерських загроз

Інсайдерські атаки становлять серйозну загрозу для будь-якої організації. На відміну від зовнішніх загроз, інсайдери мають глибоке розуміння внутрішніх систем та процесів, що ускладнює їх виявлення. Для ефективного захисту від таких атак необхідно розглянемо основні методи та засоби захисту від ІА [6]:

1. Автентифікація — підтверджує особу користувача, який намагається отримати доступ до ресурсів компанії. Вона буває однофакторною (наприклад, пароль) або багатофакторною (пароль, біометричні дані, одноразові паролі тощо).

2. Контроль доступу — визначає, до яких ресурсів кожен користувач має право доступу, і базується на принципі мінімальних привілеїв, коли працівник має доступ тільки до тих даних, які йому необхідні для роботи.

3. UEBA (User and Entity Behavior Analytics)— дозволяє виявляти аномальну поведінку співробітників, яка може свідчити про ІА. Технології UEBA та SIEM аналізують дії користувачів, шукаючи відхилення від типових шаблонів активності.

4. Реагування на інциденти — процес реагування на інциденти включає виявлення, оцінку, обмеження наслідків, розслідування та усунення інцидентів безпеки. Цей процес повинен бути формалізованим і відомим усім працівникам, відповідальним за безпеку.

5. Навчання та підвищення обізнаності персоналу з питань безпеки включає інструктажі про політики безпеки, методи виявлення та запобігання ІА, а також про те, як поводитися в разі підозри на інцидент.

6. VPN (Virtual Private Network) створює зашифрований тунель для передавання даних через публічні або небезпечні мережі, дозволяючи працівникам безпечно підключатися до ресурсів компанії з віддалених локацій. VPN шифрує весь трафік, що передається, захищаючи дані від перехоплення або несанкціонованого доступу.

7. DLP (Data Loss Prevention) — системи призначені для захисту конфіденційної інформації від витоку або втрати. Вони контролюють та обмежують передачу, доступ і копіювання чутливих даних як всередині організації, так і під час передавання даних за її межі.

8. PAM (Privileged Access Management) — системи дозволяють управляти доступом до критично важливих ресурсів, призначаючи особливий контроль за привілейованими обліковими записами. Вони забезпечують моніторинг і аудит активності користувачів з розширеними правами доступу, обмежують їхні дії та автоматично виявляють підозрілі операції.

9. IAM (Identity and Access Management) — системи відповідають за управління ідентифікацією користувачів, а також за розподіл і контроль їхніх прав доступу до ресурсів. Ці системи автоматизують процес надання і скасування доступу, а також управління ролями в організації на основі правил і привілеїв.

10. SIEM (Security Information and Event Management) — системи збирають і аналізують інформацію з різних систем безпеки та журналів подій, допомагаючи виявляти аномалії та підозрілу активність у режимі реального часу. Вони забезпечують централізовану платформу для моніторингу, реагування на інциденти, створення звітів і аналізу подій безпеки.

2.2. Архітектура рішення ActivTrak UEBA

Аналіз поведінки користувачів та об'єктів (UEBA) — це тип кібербезпеки, який використовує машинне навчання (ML) для моніторингу та аналізу поведінки користувачів та об'єктів (таких як пристрої, додатки, сервери тощо) в мережі. UEBA виявляє аномальні або зловмисні дії в режимі реального часу та сповіщає команди безпеки або вживає автоматизованих заходів. Рішення UEBA можуть доповнювати або інтегруватися з іншими інструментами безпеки, такими як системи управління інформацією та подіями безпеки (SIEM), щоб забезпечити більш комплексний і проактивний підхід до безпеки UEBA. UEBA може допомогти організаціям запобігти витоку даних, внутрішнім загрозам, шахрайству,

скомпрометованим обліковим записам та іншим кібератакам шляхом виявлення та реагування на відхилення від нормальних моделей поведінки.

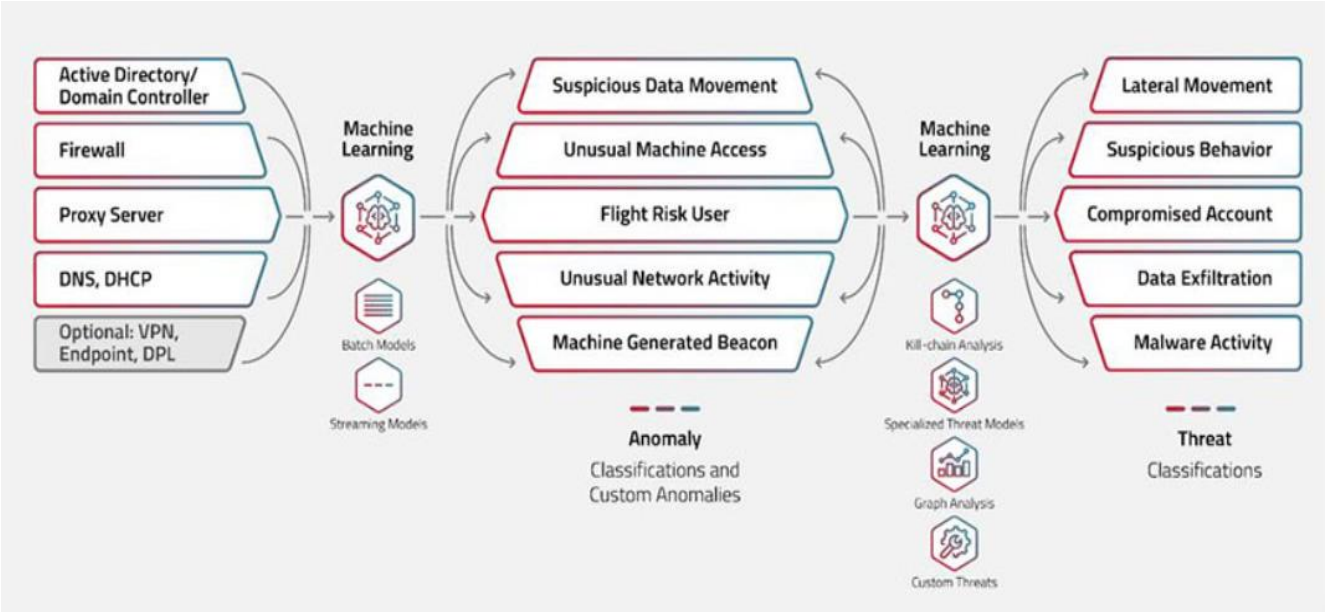


Рис. 2.1. Принцип роботи UEBA [7]

Архітектура та компоненти UEBA Архітектура UEBA базується на підході "ззовні-всередину", який натхненний парадигмою Gartner для рішень UEBA. Він базується на трьох системах координат: варіанти використання, джерела даних та аналітика.

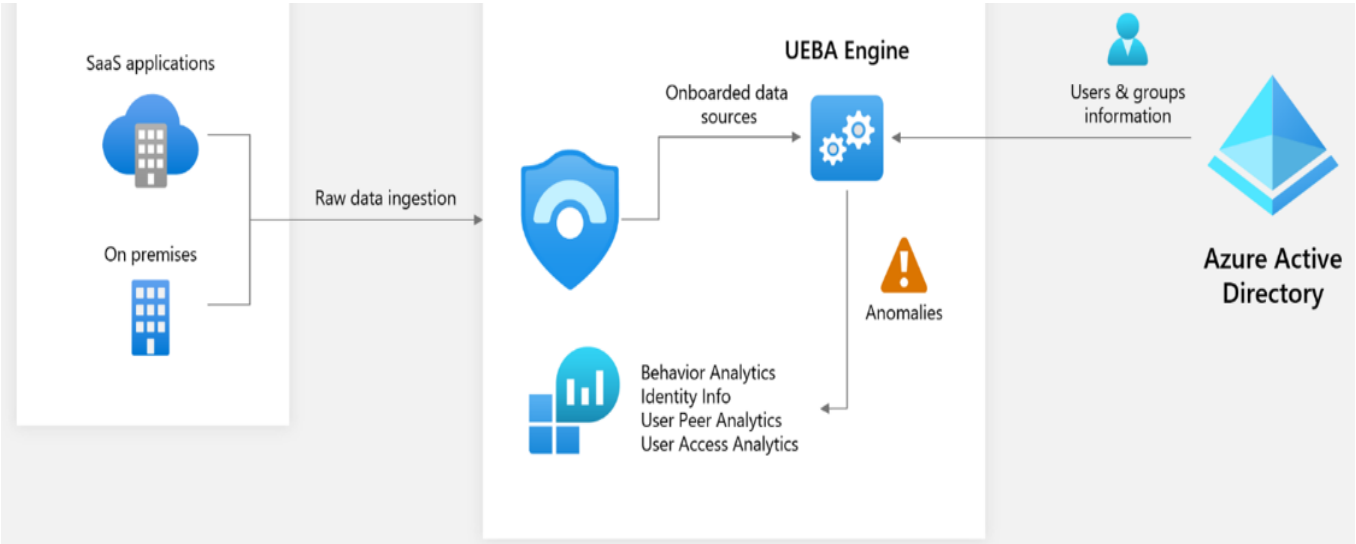


Рис. 2.2. Типова архітектура UEBA [8]

1. **Варіанти використання** визначають пріоритетність відповідних векторів і сценаріїв атак на основі досліджень безпеки, узгоджених із системою тактик, методів і підходів MITRE ATT&CK, яка визначає різні об'єкти як жертви, зловмисники або ключові точки в ланцюжку порушень. Аналітика використовує різні алгоритми машинного навчання для виявлення аномальних дій і представляє докази чітко і лаконічно у вигляді контекстних доповнень.

2. **Збір та аналіз даних**. Система UEBA збирає дані про діяльність користувачів та організацій із системних журналів. Вона застосовує передові аналітичні методи для аналізу даних і встановлює базову лінію поведінки користувачів. UEBA постійно відстежує поведінку суб'єкта і порівнює її з базовою поведінкою того ж суб'єкта або подібних суб'єктів, щоб виявити аномальну поведінку. Система створює профілі того, як кожен суб'єкт зазвичай діє щодо використання додатків, активності спілкування та завантаження, а також мережевого підключення. Потім формулюються статистичні моделі, які застосовуються для виявлення незвичної поведінки [8].

3. **Алгоритми та моделі машинного навчання** (ML) UEBA можна розділити на дві основні категорії: контрольовані та неконтрольовані. Алгоритми керованого навчання вимагають маркованих даних для навчання та тестування моделей, тоді як алгоритми некерованого навчання не потребують міток і можуть виявляти закономірності та кластери на основі самих даних. Прикладами алгоритмів керованого навчання для UEBA є логістична регресія, дерева рішень, машини опорних векторів і нейронні мережі. Деякі приклади алгоритмів неконтрольованого навчання для UEBA - це кластеризація за методом k-середніх, аналіз головних компонент, виявлення аномалій та автокодери.

Згідно з дослідженнями Expert Insights на рис. 2.3 приведено Топ-10 рішень UEBA.

Рис. 2.3. Топ-10 рішень UEBA згідно Expert Insights [9]

Рис. 2.4. Відповідність ActivTrak до стандартів

Рішення «ActivTrak» демонструє відповідність наступним стандартам:

AICPA SOC – стандарт аудиту та контролю внутрішніх процесів у сфері безпеки, конфіденційності та доступності.

GDPR (General Data Protection Regulation) – Загальний регламент захисту даних Європейського Союзу, який визначає суворі вимоги до обробки персональних даних.

HIPAA – Закон США про перенесення та підзвітність медичного страхування, який регулює захист конфіденційності медичних даних.

CCPA Compliance – відповідність закону Каліфорнії про захист споживчих даних (California Consumer Privacy Act), що передбачає права споживачів на контроль за персональною інформацією.

Таким чином, рішення «ActivTrak» відповідає ключовим стандартам захисту даних та конфіденційності, що робить його надійним для використання у сферах, де важлива конфіденційність та відповідність регуляторним вимогам.

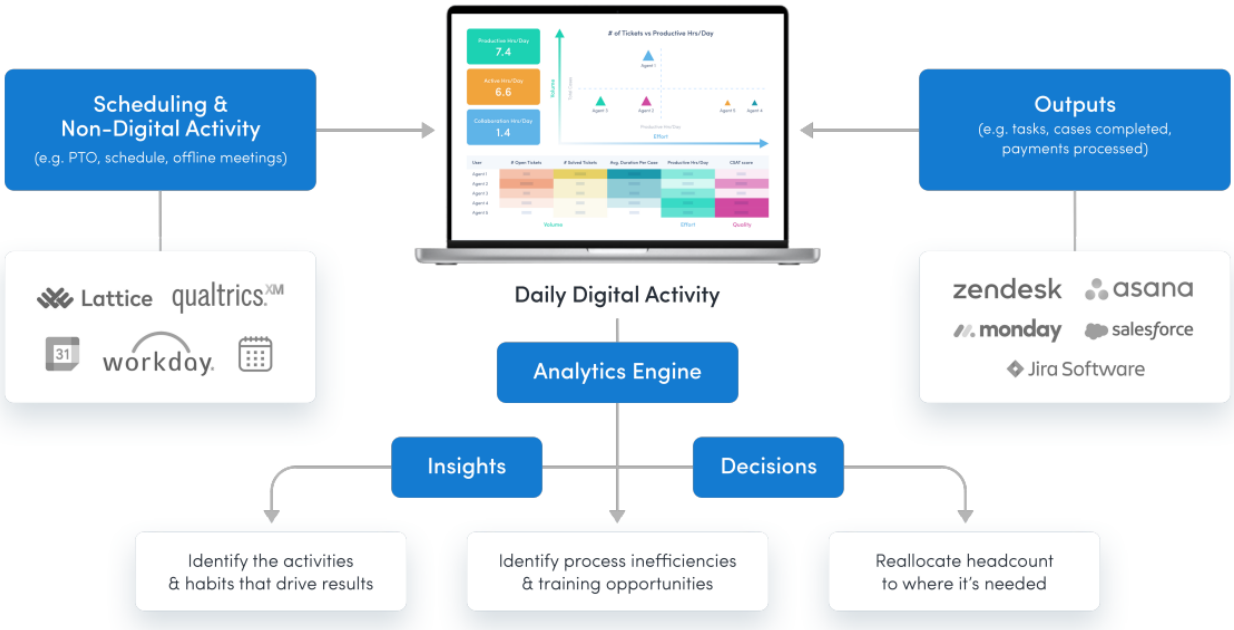


Рис.2.5. Схема аналітичної системи ActivTrak

Дана схема використовується для аналізу продуктивності та ефективності роботи організації.

Scheduling & Non-Digital Activity — відображає інформацію щодо розкладу та не цифрових активностей (наприклад, PTO, графік роботи, офлайн-зустрічі), які обробляються через системи, такі як Lattice, Qualtrics, Workday, Google Calendar.

Daily Digital Activity — відображає щоденну цифрову активність, яка збирається та аналізується аналітичною системою Analytics Engine для генерації Insights (інсайтів) та прийняття Decisions (рішень).

Insights — використовуються для виявлення діяльності та звичок, що приносять результати, а також для визначення неефективності процесів чи заборонених дій політикою організації.

Decisions — на основі аналітики приймаються рішення, зокрема перерозподіл кадрів відповідно до потреб організації.

Outputs — включають результати діяльності, такі як виконані завдання, завершені кейси та оброблені платежі. Вихідні дані зберігаються та обробляються через такі системи, як Zendesk, Asana, Monday, Salesforce, Jira Software.

Ця схема показує, як інформація про роботу працівників (як цифрова, так і не цифрова) збирається та обробляється для покращення продуктивності, оптимізації процесів і прийняття обґрунтованих рішень у межах організації на відповідні ідентифікатори дій.

2.3. Призначення та функції ActivTrak

Виходячи з попереднього дослідження в роботі було використано ActivTrak UEBA. ActivTrak - це хмарний інструмент моніторингу робочого часу та продуктивності співробітників, який дозволяє відстежувати веб-сайти та додатки, якими користуються працівники. ActivTrak збирає інформацію про URL-адреси, назви веб-сайтів та скріншоти всього, що працівники роблять у своїх системах. Окрім каталогу сайтів і додатків, він також показує час, який користувачі проводять на цих сайтах і додатках.

Функції ActivTrak:

1. Знімки екрану ActivTrak можна робити через певні проміжки часу, щоб точно знати, що відбувається на екранах співробітників. Тривалість інтервалів встановлюється відповідно до потреб [10,11].

2. Класифікація продуктивних/непродуктивних. За допомогою ActivTrak ви можете позначати певні сайти та програми як продуктивні або непродуктивні. Це можна зробити по-різному для різних типів співробітників. Наприклад, сайти соціальних мереж можуть бути позначені як продуктивні для менеджера соціальних мереж і непродуктивні для програміста.

3. Використання веб-сайтів і додатків. Окрім того, що ActivTrak надає вам URL-адресу та/або рядок заголовка сайту чи додатку, він також фіксує час, витрачений на кожну дію. Це дає уявлення про те, над чим працювали співробітники і як довго.

4. Автоматична фіксація часу. Вся діяльність співробітників відстежується в реальному часі за допомогою міток часу в ActivTrak. Можна створювати різні типи звітів із зазначенням URL-адреси сайту, часу та тривалості перебування на ньому.

5. Запланований моніторинг. Це важлива функція, якщо співробітники повинні використовувати свої ноутбуки з особистих причин або для моніторингу фрілансерів. Використовуючи ActivTrak, ви можете запланувати моніторинг системи тільки в робочий час. Таким чином, поважається конфіденційність працівників/фрілансерів. Це також полегшує оцінку звітів, оскільки вони складаються лише з даних про робочий час [10,11].

6. Блокування веб-сайтів. ActivTrak дозволяє блокувати певні веб-сайти для певних користувачів одночасно. Це допоможе заблокувати відволікаючі фактори, такі як соціальні мережі, розважальні платформи, сайти з пошуку роботи тощо. Не маючи можливості відволіктися, співробітники автоматично стануть більш продуктивними в робочий час. Більшість компаній блокують потокові платформи, такі як Netflix, Youtube, соціальні мережі, такі як Facebook, Instagram, та сайти з пошуку роботи, такі як LinkedIn та Indeed.

7. Нагадування про продуктивність ActivTrak - це дуже практичний інструмент для мінімізації відволікань працівників на роботі. Якщо працівник відволікається на соціальні мережі або інші непродуктивні сайти, можна налаштувати спливаючі сповіщення, які нагадають йому про те, що він робить, і повернуть його в потрібне русло.

8. Моніторинг активності клавіатури та миші. Активність клавіатури та миші є також корисним показником продуктивності. ActivTrak відстежує активність клавіатури і миші, щоб знайти час простою. Але він не реєструє точне натискання клавіш, тобто ActivTrak відстежує, чи використовуєте ви клавіатуру, чи ні. Але не записує, які саме клавіші натискаються на клавіатурі. Вони не збирають паролі або будь-які інші дані, що вводяться, таким чином зберігаючи конфіденційність співробітників [10,11].

Це дозволяє мати загальний огляд усіх даних. Можна бачити інформацію для різних користувачів і за різні періоди часу (дні, тижні, місяці, роки). Рішення показує буквально все, що відбувається на комп'ютері під час роботи. Якщо хочете побачити більше деталей, можна отримати доступ до лівої бічної панелі з більшою кількістю опцій.

Висновки до розділу 2

1. У розділі було проведено аналіз методів та засобів захисту від інсайдерських атак, а також представлено архітектуру UEBA в якій розкрито призначення, основні можливості та функції рішення ActivTrak UEBA, що займає перше місце серед інших UEBA рішень згідно [9].

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ЗАХИСТУ ОРГАНІЗАЦІЇ ВІД ІНСАЙДЕРСЬКИХ АТАК НА БАЗІ РІШЕННЯ ACTIVTRAK UEBA

3.1. Розроблення варіанта розгортання технології захисту організації від інсайдерських атак

В другому розділі було розглянуто архітектуру, складові та функції ActivTrak UEBA.

В даному розділі буде розглянуто питання щодо розгортання ActivTrak UEBA.

Незалежно від того, чи ви користуєтеся безкоштовною пробною версією або платним тарифним планом, налаштувати свій обліковий запис ActivTrak дуже просто слідуючи наступним крокам [12]:

1. Увійдіть до ActivTrak

Щоб увійти до ActivTrak, відвідайте app.activtrak.com і введіть свої облікові дані. Також можна увімкнути SSO та MFA. Дізнайтеся більше.

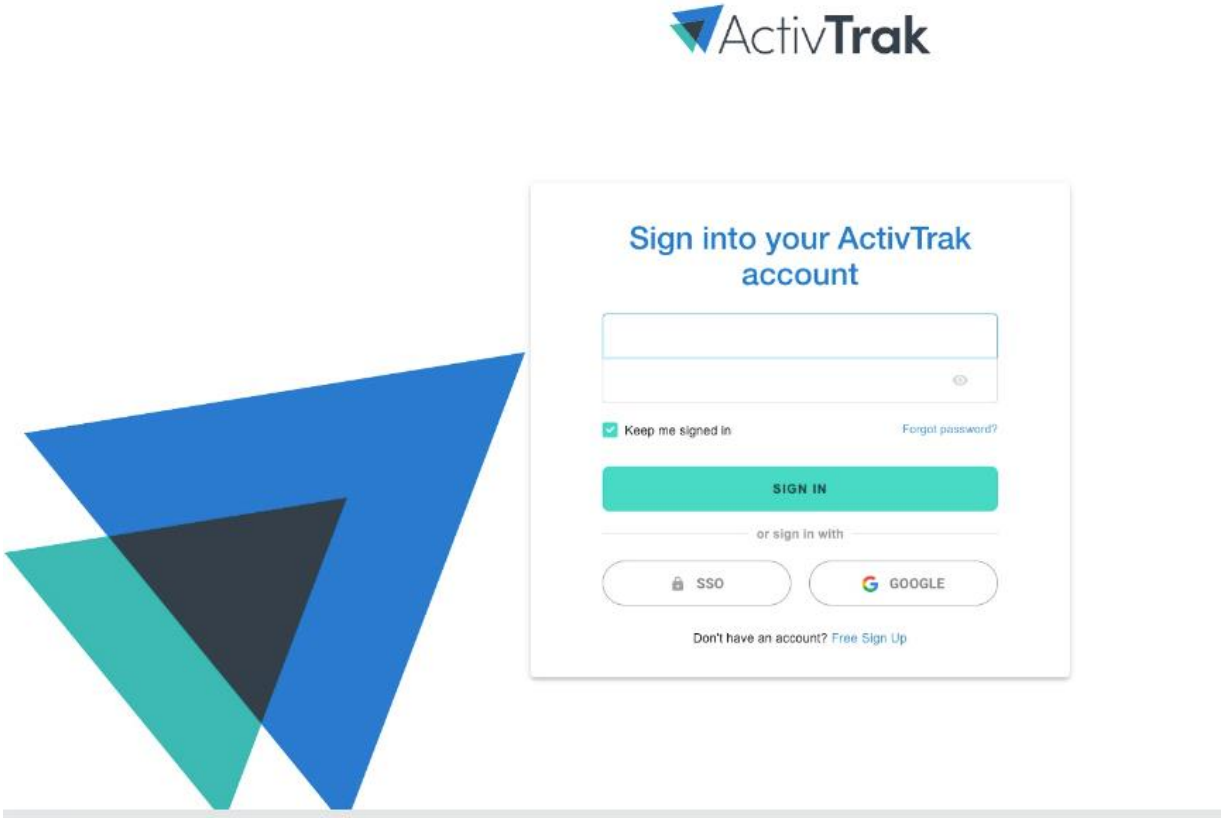


Рис. 3.1. Сторінка логування ActivTrak

2. Завершити кероване налаштування акаунта.

Під час першого входу до акаунта вам буде запропоновано завершити кероване налаштування акаунта. Ця функція дозволяє налаштувати обліковий запис відповідно до сценаріїв використання та налаштувань конфіденційності вашої організації. Ваш вибір визначатиме, які дашборди та звіти відображатимуться в лівій навігації програми, а також рівень даних, що відображатимуться у звітах та дашбордах [12].

Кероване налаштування облікового запису визначає, як виглядатиме ваш обліковий запис ActivTrak, включаючи приховування або відображення певних функцій. Ваші налаштування можна будь-коли оновити, відвідавши Налаштування > Доступ > Доступ до ролей, щоб перезапустити кероване налаштування облікового запису або зробити індивідуальний вибір. Якщо кероване налаштування облікового запису не запускається, це може бути пов'язано з тим, що інший адміністратор облікового запису вже завершив цей крок.

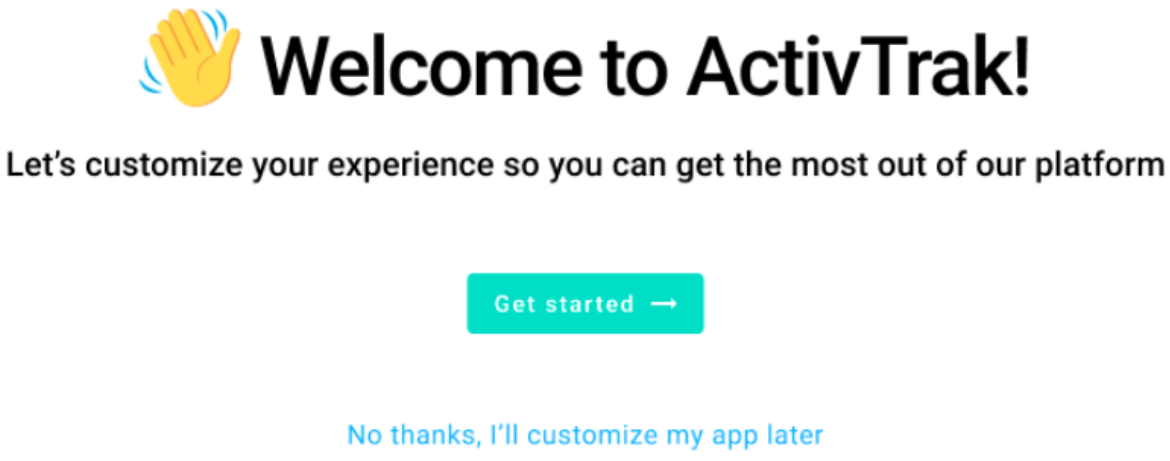


Рис. 3.2. Початок керованого налаштування

3. Розгортання агентів ActivTrak [12].

Після завершення керованого налаштування облікового запису потрапляємо на сторінку активації агента, яка містить посилання для розгортання агента на власному комп'ютері, а також для надання доступу до інсталяційного файлу та розгортання агентів на інших пристроях. Існує кілька методів розгортання агентів ActivTrak.

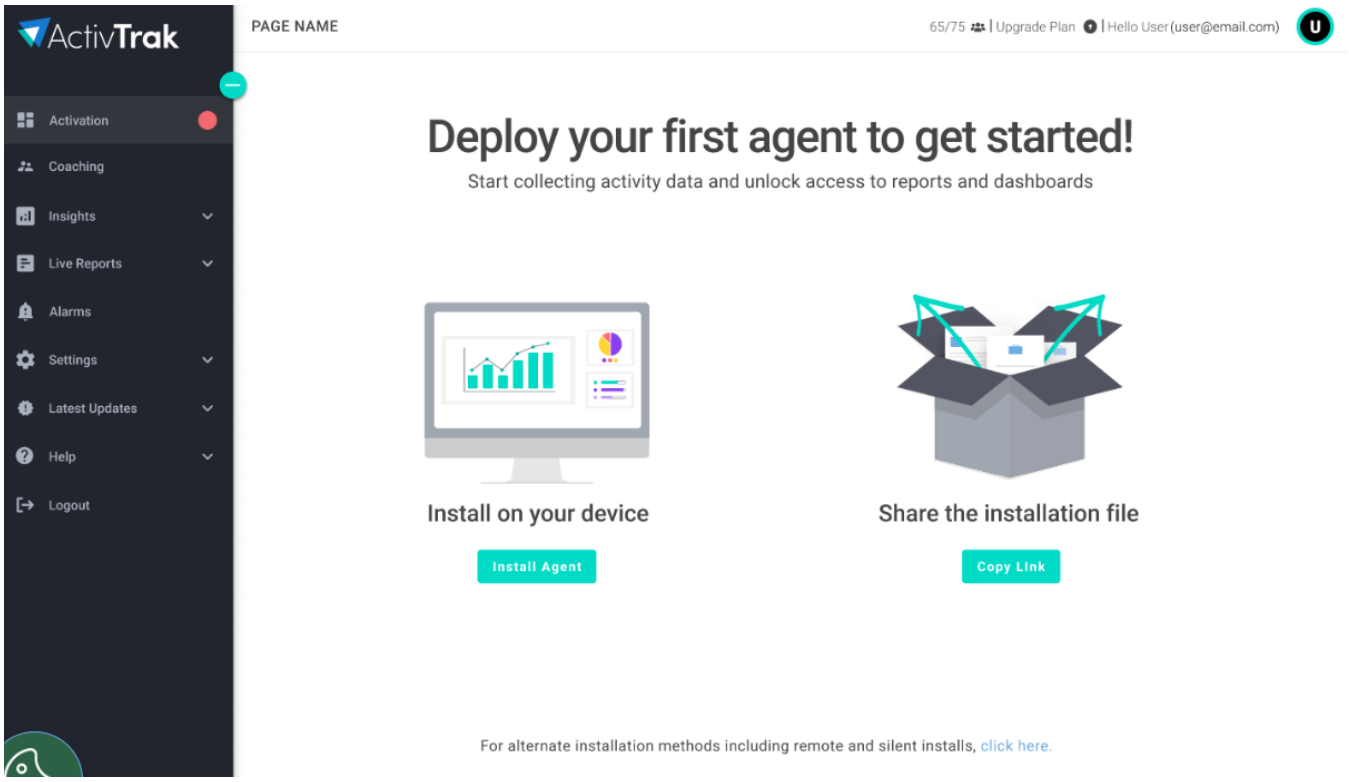


Рис. 3.3. Сторінка активації агента

При встановленні агента на власний пристрій програма визначає операційну систему робочої станції і автоматично завантажує відповідну версію агента. При наданні спільного доступу до інсталяційного файлу буде запропоновано вибрати операційну систему для пристрою, на якому буде встановлено агент. Ви будете бачити сторінку активації агента при кожному вході в систему, поки не розгорнете хоча б один агент. Ви також можете завантажити та встановити агент в будь-який час з Панелі адміністратора, натиснувши кнопку "Встановити/надати спільний доступ до файлу агента" в розділі "Швидкі дії" у верхній частині інформаційної панелі, як показано на знімку екрана нижче [12].

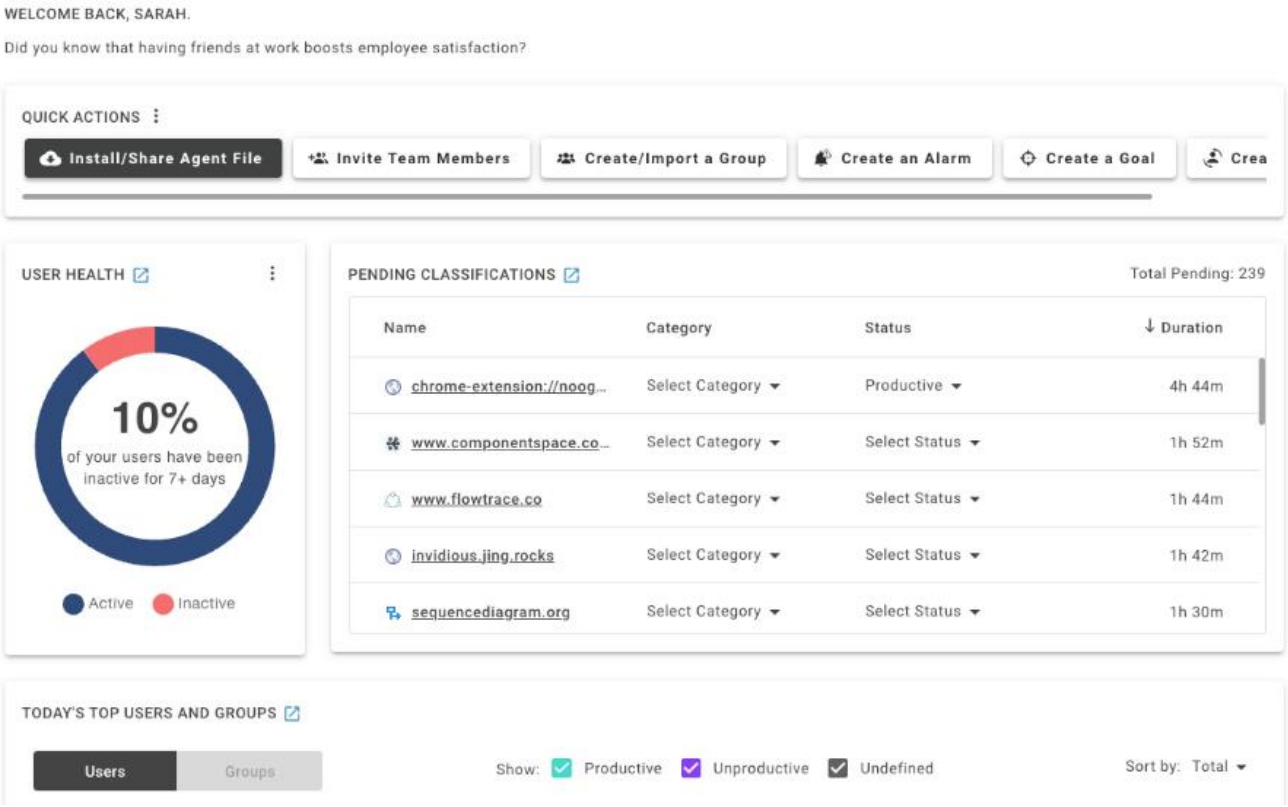


Рис. 3.4. Адмін панель

4. Створення псевдонімів користувачів і комп'ютерів.

Зміна видимого імені комп'ютера або користувача з псевдонімом. Коли Агент встановлено на комп'ютері, він відображає зареєстроване ім'я комп'ютера в усіх пов'язаних з ним даних. Ви також можете використовувати псевдоніми для зміни імен користувачів на інформаційних панелях і в звітах, а також об'єднувати різні варіанти імен користувачів в один псевдонім [12].

5. Об'єднання користувачів у групи.

Об'єднання користувачів у групи має важливе значення для забезпечення точної звітності та відповідального обміну даними про працівників. Зазвичай групи відповідають командам в організації, що дозволяє менеджерам визначати, які дії слід класифікувати як продуктивні, а які - як непродуктивні, встановлювати цілі та оцінювати стан здоров'я і продуктивність команди. Запрошуючи користувачів отримати доступ до вашого облікового запису ActivTrak (див. 7), ви обираєте їхні Групи для перегляду, щоб визначити, до чиїх даних вони зможуть отримати доступ.

Це гарантує, що дані про активність співробітників будуть видимі лише відповідним особам - як правило, їхньому безпосередньому керівнику.

6. Класифікація додатків і веб-сайтів.

Класифікація активності має важливе значення для того, щоб ваші звіти та інформаційні панелі точно відображали те, як користувачі проводять свій час. Інтелектуальна функція автоматичної класифікації ActivTrak використовує дані з відкритих джерел для автоматичного розподілу часто використовуваних веб-сайтів і додатків на продуктивні і непродуктивні. Ви можете скасувати автоматичну класифікацію продуктивності і створити власні категорії (наприклад, чат і обмін повідомленнями, управління проектами, бухгалтерські інструменти), щоб задовольнити унікальні вимоги вашої організації. Класифікації можна призначати на рівні групи, щоб врахувати відмінності в ролях і обов'язках - наприклад, соціальні мережі можуть бути непродуктивними для бухгалтерії, але продуктивними для команди маркетингу [12-15].

7. Налаштування параметрів активного і пасивного часу.

В ActivTrak час активності фіксується і класифікується як активний або пасивний. Активний час включає дії, які передбачають активні рухи мишею і клавіатурою (наприклад, створення електронного листа). Пасивний час включає дії, які не передбачають рухів мишею і клавіатурою (наприклад, перегляд відео).

Рис. 3.5. Типи часу в ActivTrak

Тривалість активного та пасивного часу встановлені за замовчуванням, однак можна налаштувати ці параметри відповідно до потреб організації [12].

8. Запрошуйте користувачів програми та призначайте їм ролі та дозволи.

Багато людей у організації - від керівників команд до керівників відділів кадрів та IT - можуть скористатися аналітичними даними про персонал в ActivTrak. Завдяки налаштованим ролям користувачів і групам перегляду можна надати кожному користувачеві програми доступ до конкретних даних, які йому потрібні, не порушуючи конфіденційність співробітників і не надаючи доступ до адміністративних налаштувань у обліковому записі.

- Ролі користувачів: Запрошуючи нових користувачів програми до облікового запису, ви призначаєте їм одну з чотирьох ролей: Адміністратор, Конфігуратор, Досвідчений користувач або Переглядач. Кожну роль можна налаштувати так, щоб надати доступ до відповідних дашбордів і налаштувань [12-15].

- Групи перегляду: Призначте групи для перегляду кожному користувачеві програми, щоб визначити, чиї дані він зможе бачити в дашбордах і звітах. Користувачі можуть бути членами кількох груп, тому легко створювати когорти для задоволення різноманітних потреб. Наприклад, можна створити групу для кожного відділу вашої організації (інженерії, продажів, фінансів), доступ до якої матиме керівник відділу, а також окремі групи для менших команд всередині відділу, доступ до яких матиме керівник відповідної команди.

9. Визначення власних робочих годин [12].

Можна визначити власні розклади, щоб запобігти збору даних про активність користувачів у неробочий час. Унікальні розклади можна застосувати до окремих користувачів, щоб узгодити їх зі стандартним робочим часом кожного співробітника.

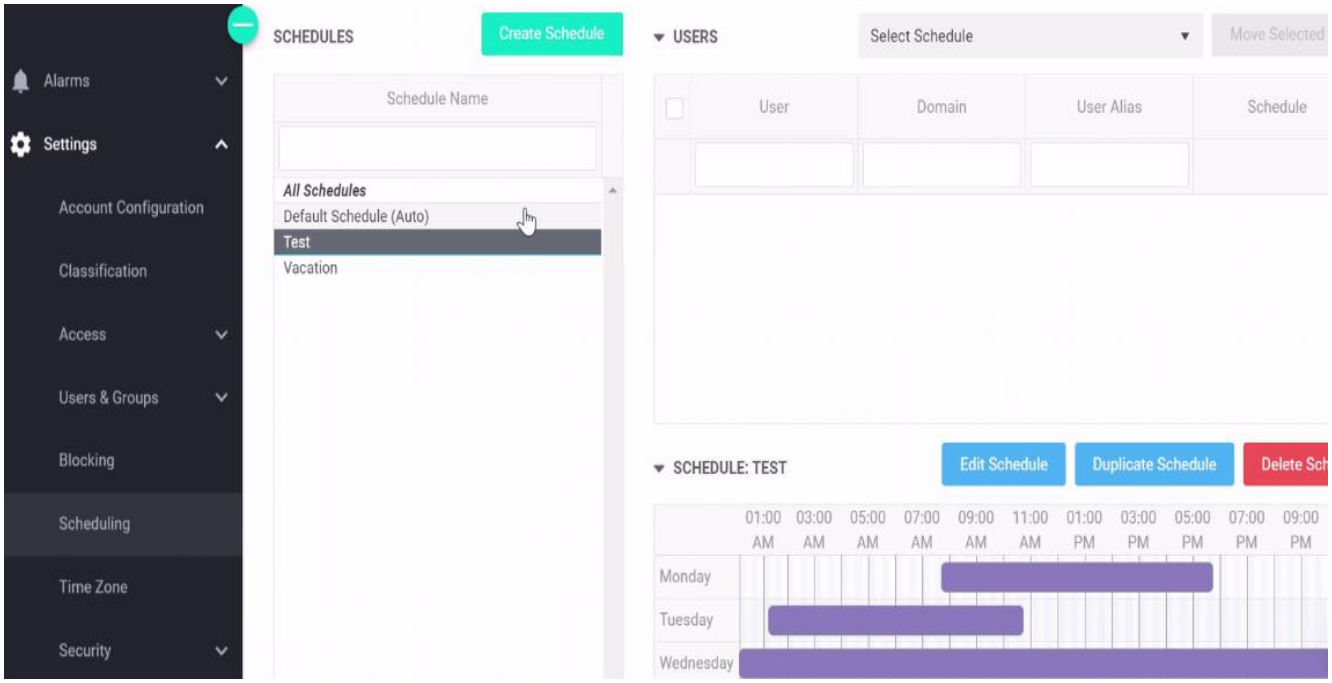


Рис. 3.6. Налаштування розкладу робочих годин

10. Дослідження дашбордів, функцій та звіти.

Домашні сторіноки - оптимізованих дашбордів, які спрощують робочі процеси і надають ключову інформацію з першого погляду для користувачів програми ActivTrak: Панель адміністратора Огляд організації Управління командою Панель активності Примітка: Панель адміністратора, Огляд організації та Панель активності доступні в усіх платних планах і Професійних пробних версіях. Керування командами доступне лише в окремих планах.

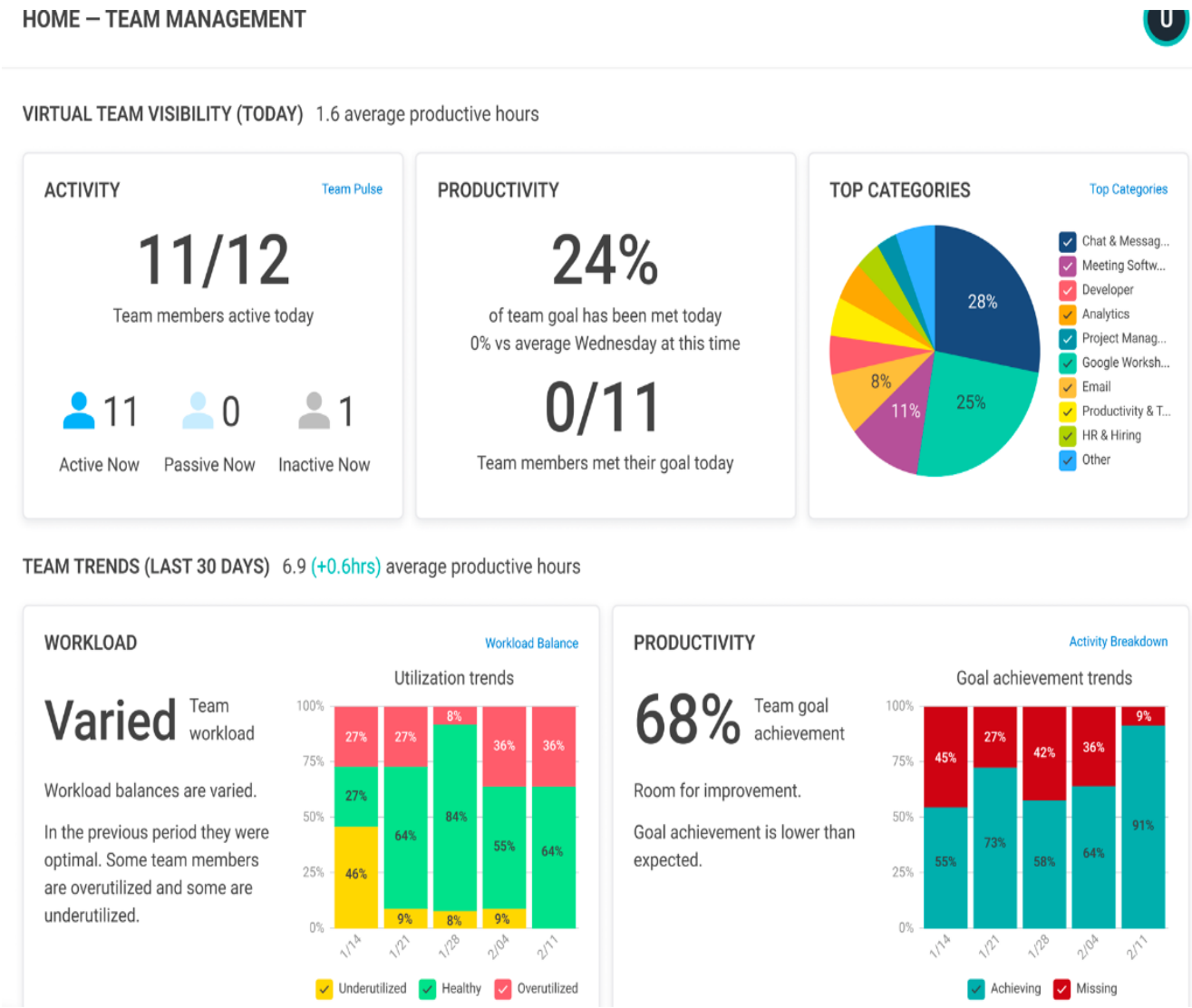


Рис. 3.7. Домашня сторінка управління командою

Далі, ActivTrak Coach [12-15] аналізує робочі звички команди, щоб виявити ранні ознаки роз'єднаності, вигорання та зниження продуктивності, а також надає поради, щоб менеджери могли вжити заходів і запобігти негативному впливу на продуктивність. Щоб менеджери не пропустили жодної можливості для коучингу, рекомендується підписатися на електронні звіти всіх вкладок Coach. Коуч - це функція Insights, доступна в окремих планах.

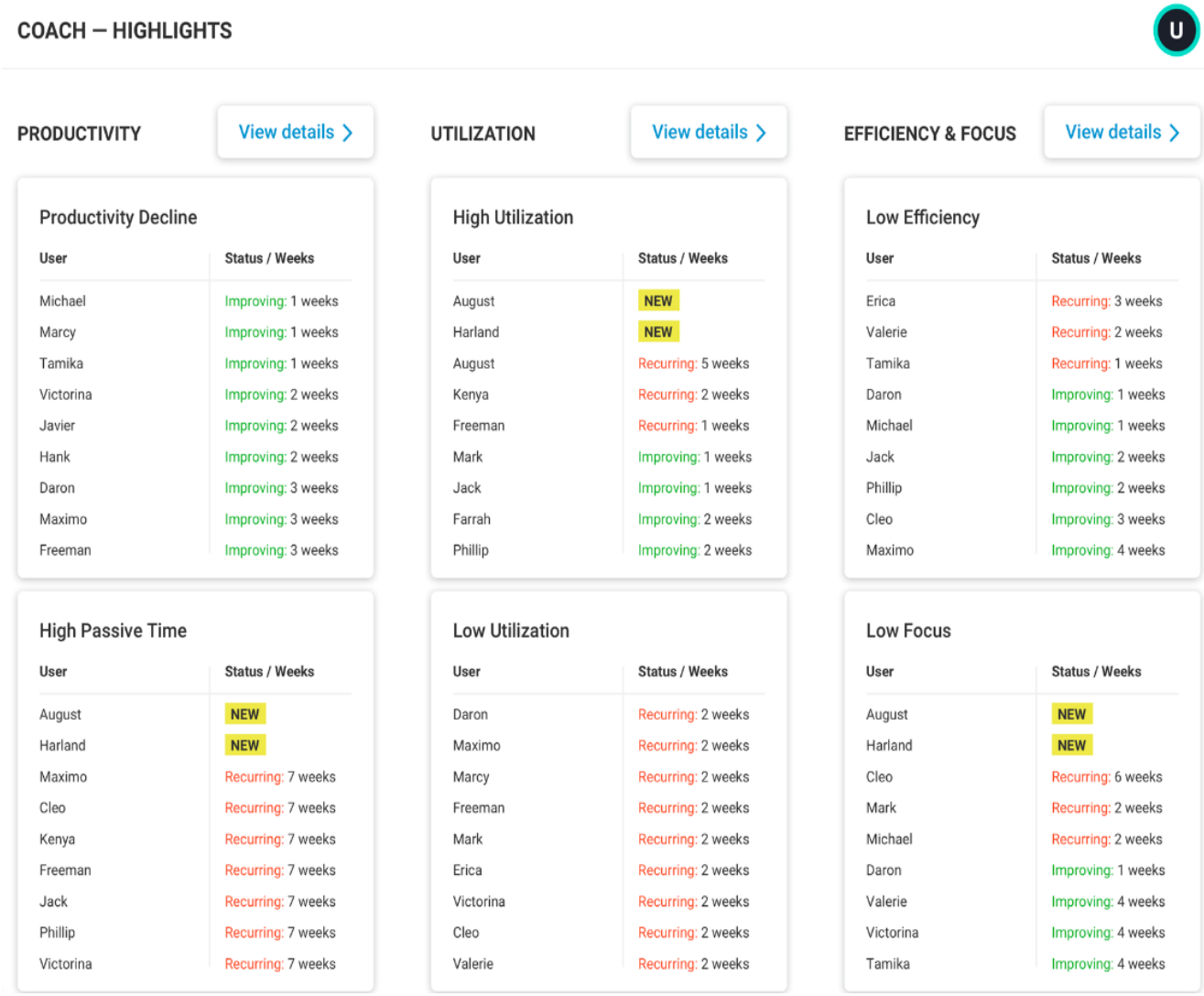
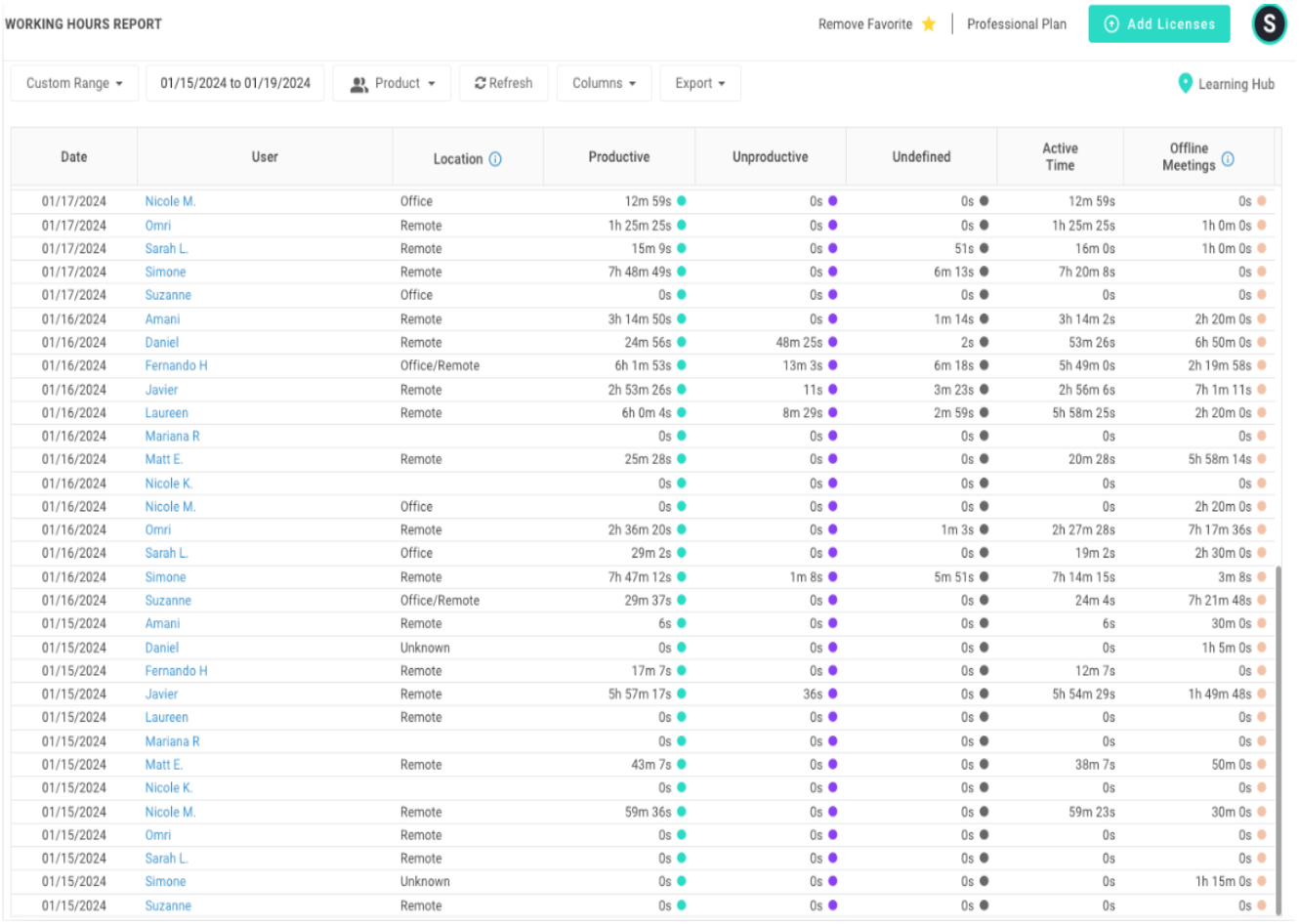


Рис. 3.8. Коуч ActivTrak

Ознайомлення зі звітами в реальному часі та інформаційними панелями. Звіти в реальному часі - це набір звітів, які надають цінні дані про персонал майже в реальному часі та короткострокові історичні дані, щоб відповісти на питання: "Чи працює моя команда так, як очікувалося?". Дізнайтися про всі звіти в реальному часі можна у меня Огляді звітів в реальному часі [12-15].



Date	User	Location	Productive	Unproductive	Undefined	Active Time	Offline Meetings
01/17/2024	Nicole M.	Office	12m 59s	0s	0s	12m 59s	0s
01/17/2024	Omri	Remote	1h 25m 25s	0s	0s	1h 25m 25s	1h 0m 0s
01/17/2024	Sarah L.	Remote	15m 9s	0s	51s	16m 0s	1h 0m 0s
01/17/2024	Simone	Remote	7h 48m 49s	0s	6m 13s	7h 20m 8s	0s
01/17/2024	Suzanne	Office	0s	0s	0s	0s	0s
01/16/2024	Amani	Remote	3h 14m 50s	0s	1m 14s	3h 14m 2s	2h 20m 0s
01/16/2024	Daniel	Remote	24m 56s	48m 25s	2s	53m 26s	6h 50m 0s
01/16/2024	Fernando H	Office/Remote	6h 1m 53s	13m 3s	6m 18s	5h 49m 0s	2h 19m 58s
01/16/2024	Javier	Remote	2h 53m 26s	11s	3m 23s	2h 56m 6s	7h 1m 11s
01/16/2024	Laureen	Remote	6h 0m 4s	8m 29s	2m 59s	5h 58m 25s	2h 20m 0s
01/16/2024	Mariana R		0s	0s	0s	0s	0s
01/16/2024	Matt E.	Remote	25m 28s	0s	0s	20m 28s	5h 58m 14s
01/16/2024	Nicole K.		0s	0s	0s	0s	0s
01/16/2024	Nicole M.	Office	0s	0s	0s	0s	2h 20m 0s
01/16/2024	Omri	Remote	2h 36m 20s	0s	1m 3s	2h 27m 28s	7h 17m 36s
01/16/2024	Sarah L.	Office	29m 2s	0s	0s	19m 2s	2h 30m 0s
01/16/2024	Simone	Remote	7h 47m 12s	1m 8s	5m 51s	7h 14m 15s	3m 8s
01/16/2024	Suzanne	Office/Remote	29m 37s	0s	0s	24m 4s	7h 21m 48s
01/15/2024	Amani	Remote	6s	0s	0s	6s	30m 0s
01/15/2024	Daniel	Unknown	0s	0s	0s	0s	1h 5m 0s
01/15/2024	Fernando H	Remote	17m 7s	0s	0s	12m 7s	0s
01/15/2024	Javier	Remote	5h 57m 17s	36s	0s	5h 54m 29s	1h 49m 48s
01/15/2024	Laureen	Remote	0s	0s	0s	0s	0s
01/15/2024	Mariana R		0s	0s	0s	0s	0s
01/15/2024	Matt E.	Remote	43m 7s	0s	0s	38m 7s	50m 0s
01/15/2024	Nicole K.		0s	0s	0s	0s	0s
01/15/2024	Nicole M.	Remote	59m 36s	0s	0s	59m 23s	30m 0s
01/15/2024	Omri	Remote	0s	0s	0s	0s	0s
01/15/2024	Sarah L.	Remote	0s	0s	0s	0s	0s
01/15/2024	Simone	Unknown	0s	0s	0s	0s	1h 15m 0s
01/15/2024	Suzanne	Remote	0s	0s	0s	0s	0s

Рис. 3.9. Звіт про робочий час (Live Report)

Інформаційні панелі та функції Insights (рис. 3.10) надають розширену аналітику на основі штучного інтелекту та виявлення закономірностей, щоб відповісти на питання: "Чи працює моя команда для досягнення максимальних результатів?". Важливо, що на відміну від звітів у реальному часі [12-15], Insights дозволяють організаціям: встановлювати цілі та вимірювати прогрес у досягненні цілей.

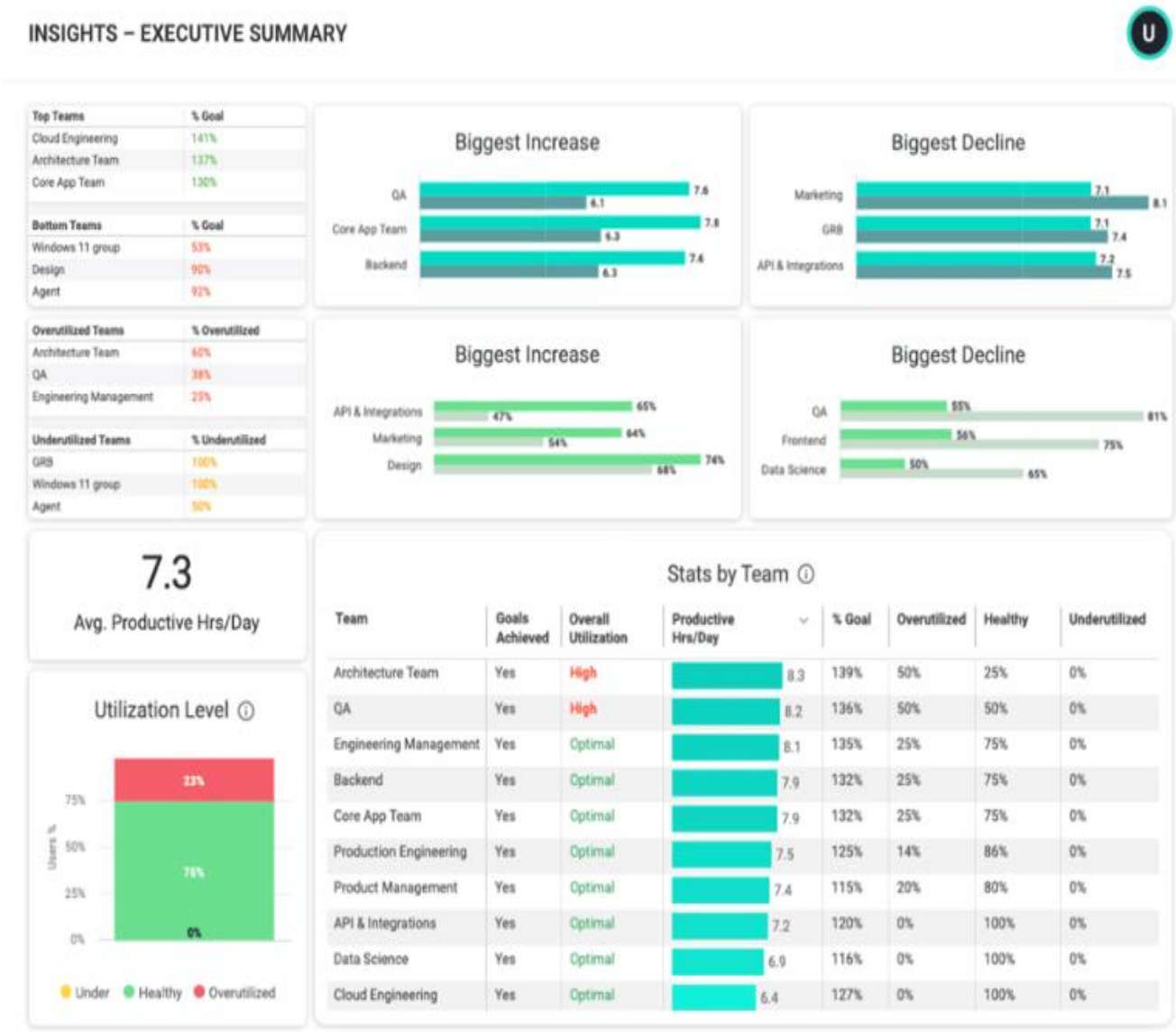


Рис. 3.10. Інформаційна панель резюме (Insights Dashboard)

11. Створення ярликів за допомогою меню Вибраного.

Заощаджуйте час на доступ до найуживаніших звітів, інформаційних панелей, функцій і сторінок за допомогою Вибраного в навігації. Вибране - це чудовий спосіб для всіх користувачів створювати свої робочі процеси та налаштовувати роботу в додатку [12-15]. Додайте Вибране, навівши курсор на назву сторінки в лівій навігації і натиснувши іконку зірочки праворуч від назви сторінки АБО натисніть "Додати до вибраного" у верхній частині будь-якої сторінки. Кожен користувач може створити власний список Вибраного - зроблений вами вибір не вплине на Вибране інших користувачів.

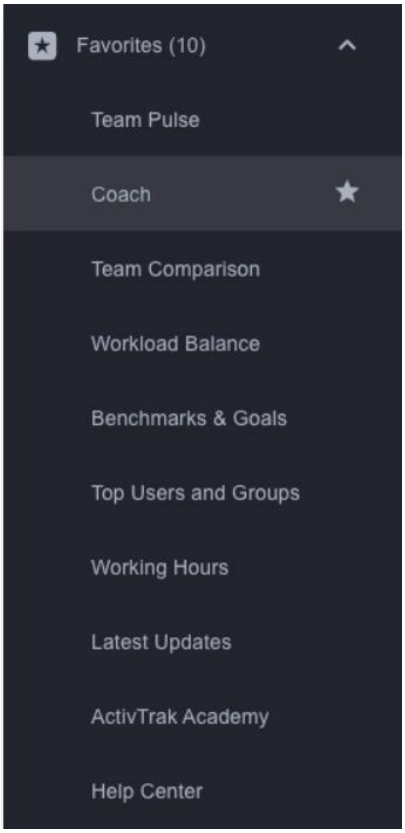


Рис. 3.11. Приклад списку обраного

12. Отримайте додаткове навчання та підтримку.

В ActivTrak є багато цікавого для вивчення! Вам потрібно прискорити процес використання ActivTrak для досягнення ваших цілей? Отримайте доступ до поєднання курсів для самостійного вивчення та навчання в реальному часі в Академії ActivTrak [12-17].

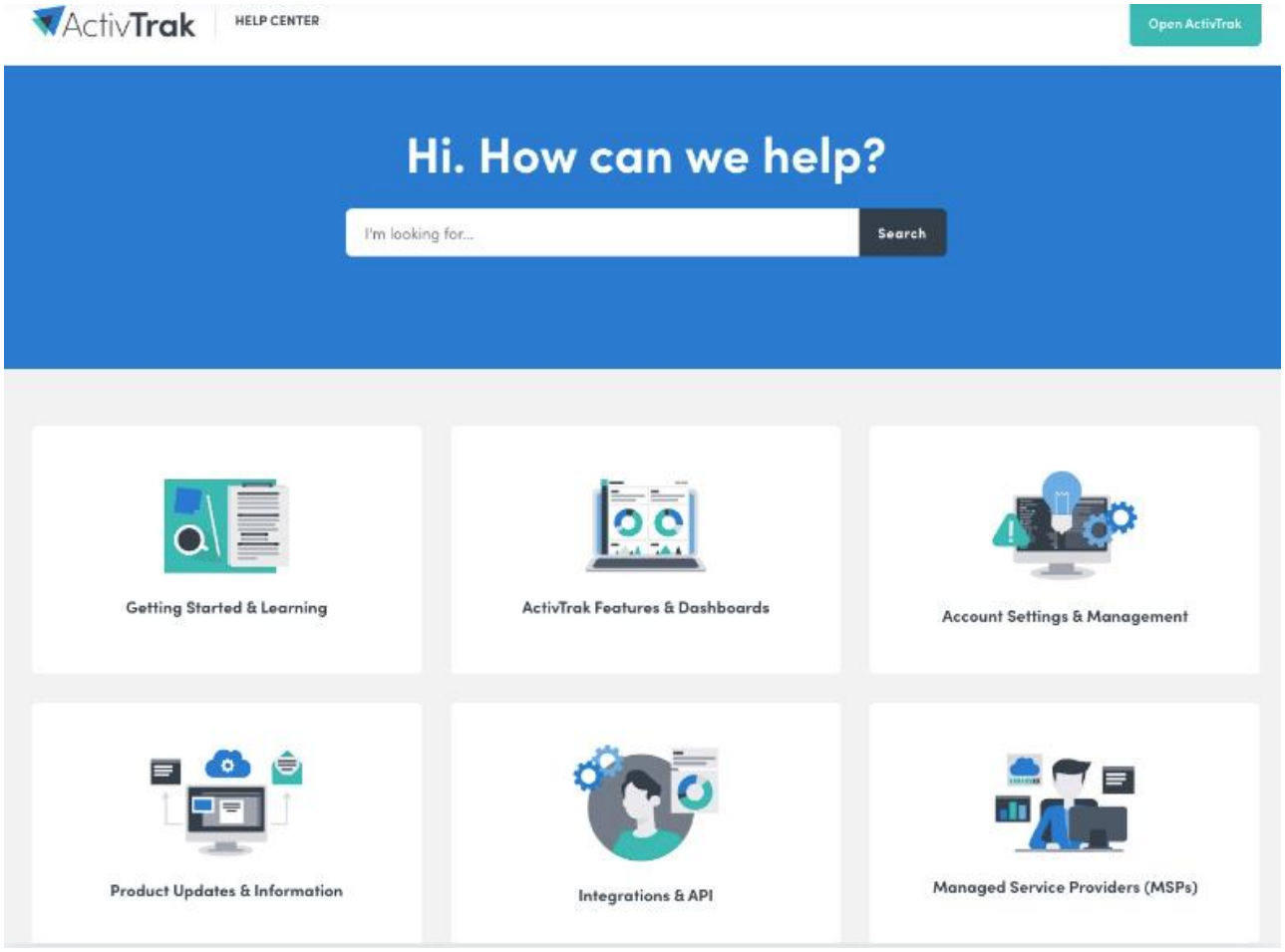


Рис. 3.12. Довідковий центр ActivTrak

3.2. Технологія захисту організації від інсайдерських атак на базі рішення ActivTrak UEBA

Після етапів розгортання та налаштування перейдемо до тестування технології.

На рис. 3.13-3.14 зображено всі дані про активність за дні, тижні, місяці, роки або користувацький час, а також про користувачів. Як і в розділі «Реальний час», тут відображається тип активності (продуктивна чи непродуктивна), скріншоти, дані, час, комп'ютер, користувач, тривалість активності, додаток, веб-сайт. Крім того, є можливість експортувати звіти у CSV-файл або зберегти їх на Google Диску.

Але є ще одна важлива функція – оповіщення [15-20].

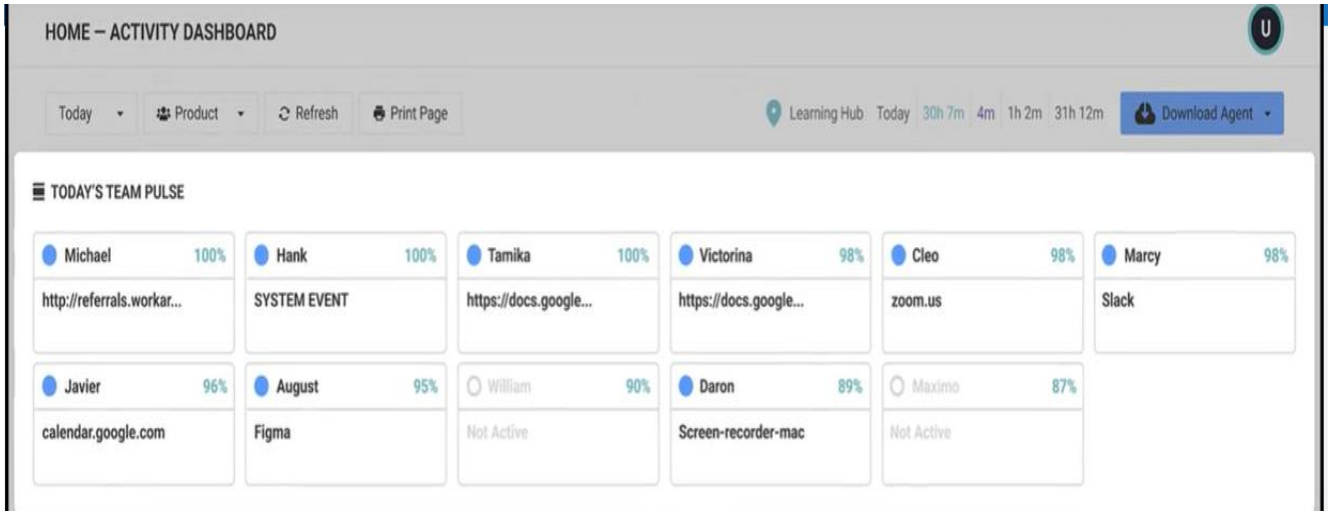


Рис. 3.13. Активність користувачів за поточний день

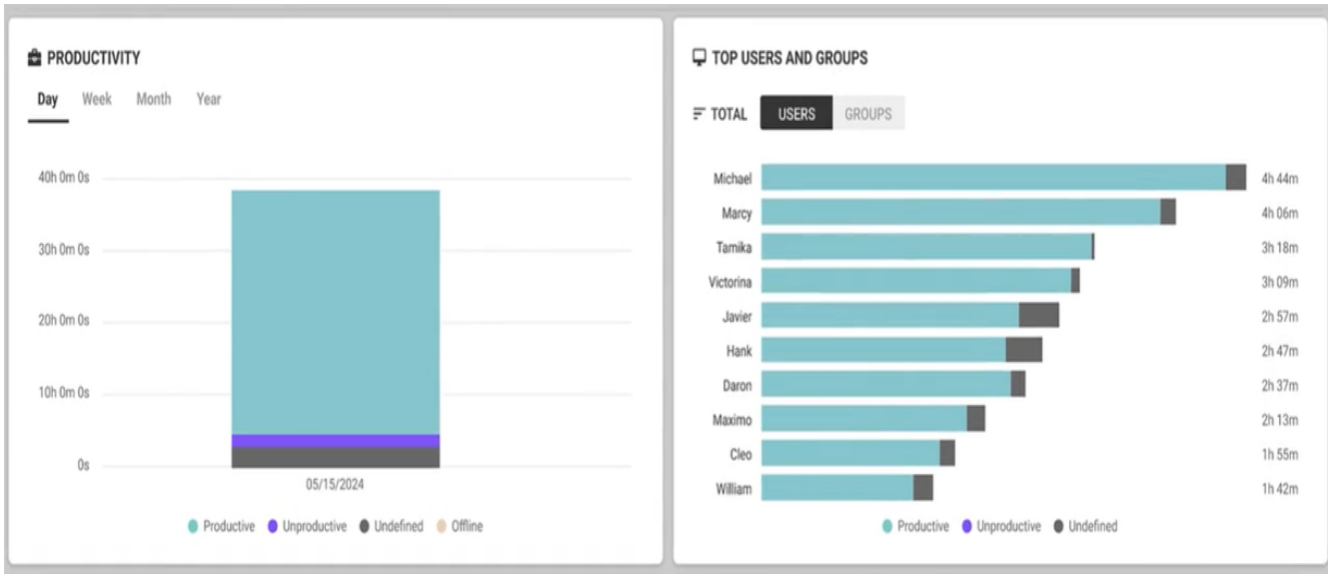


Рис. 3.14. Часова продуктивність

На рис. 3.15-3.17 зображено з деталями активності працівників протягом робочого дня. Таблиця містить такі стовпці:

User — Ім'я користувача або працівника.

Location — Місце роботи працівника (офіс або дистанційно).

First Activity — Час початку першої активності.

Last Activity — Час завершення останньої активності.

Productive — Час, витрачений на продуктивну роботу.

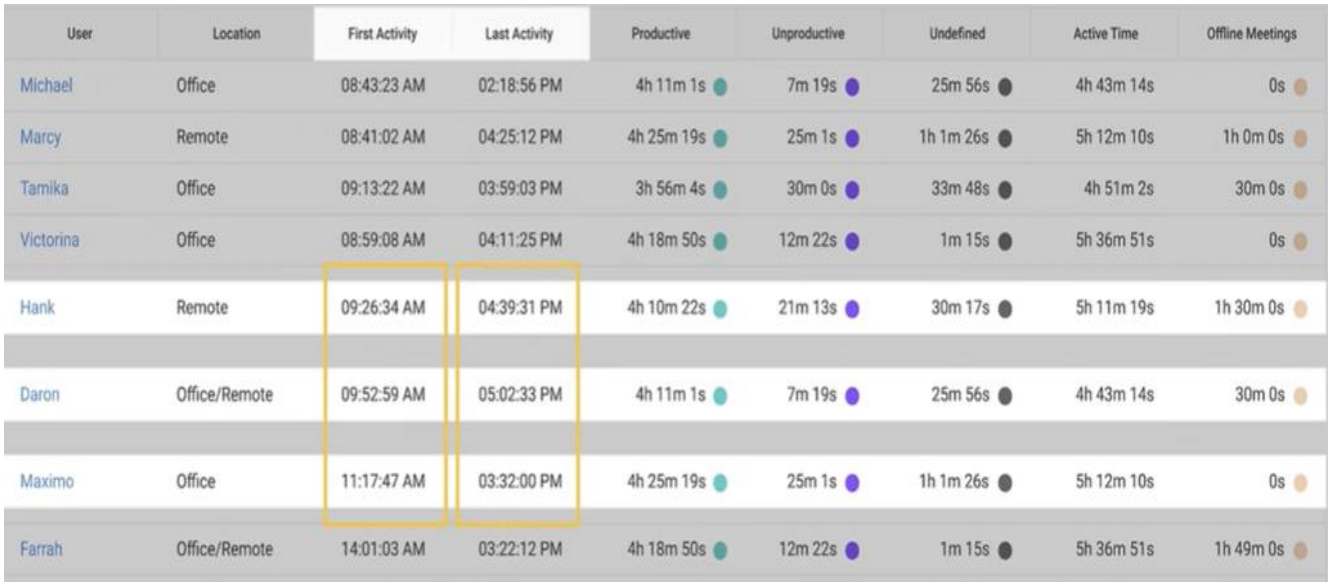
Unproductive — Час, витрачений на непродуктивну роботу.

Undefined — Час, позначений як невизначений.

Active Time — Загальний активний час протягом дня.

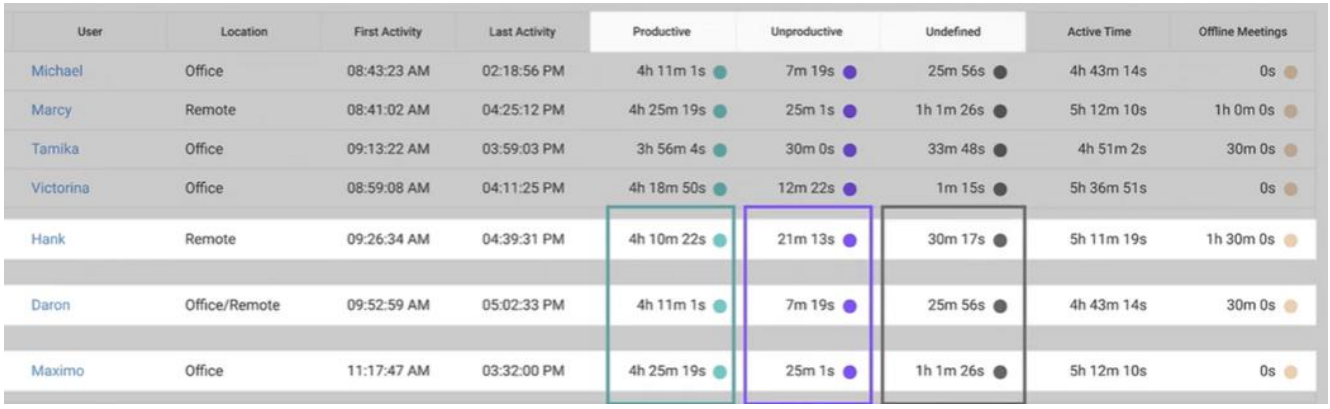
Offline Meetings — Час, витрачений на офлайн-зустрічі [15-20]..

У таблиці видно, скільки часу кожен працівник провів у різних типах активностей. Виділені жовтими рамками рядки (наприклад, Hank, Daron, Maximo) підкреслюють дані по активності цих користувачів. Це дозволяє оцінити продуктивність, час, витрачений на зустрічі, та загальну ефективність роботи впродовж дня, а також хто звідки працює і має доступ.



User	Location	First Activity	Last Activity	Productive	Unproductive	Undefined	Active Time	Offline Meetings
Michael	Office	08:43:23 AM	02:18:56 PM	4h 11m 1s	7m 19s	25m 56s	4h 43m 14s	0s
Marcy	Remote	08:41:02 AM	04:25:12 PM	4h 25m 19s	25m 1s	1h 1m 26s	5h 12m 10s	1h 0m 0s
Tamika	Office	09:13:22 AM	03:59:03 PM	3h 56m 4s	30m 0s	33m 48s	4h 51m 2s	30m 0s
Victorina	Office	08:59:08 AM	04:11:25 PM	4h 18m 50s	12m 22s	1m 15s	5h 36m 51s	0s
Hank	Remote	09:26:34 AM	04:39:31 PM	4h 10m 22s	21m 13s	30m 17s	5h 11m 19s	1h 30m 0s
Daron	Office/Remote	09:52:59 AM	05:02:33 PM	4h 11m 1s	7m 19s	25m 56s	4h 43m 14s	30m 0s
Maximo	Office	11:17:47 AM	03:32:00 PM	4h 25m 19s	25m 1s	1h 1m 26s	5h 12m 10s	0s
Farrah	Office/Remote	14:01:03 AM	03:22:12 PM	4h 18m 50s	12m 22s	1m 15s	5h 36m 51s	1h 49m 0s

Рис. 3.15. Активність користувачів



User	Location	First Activity	Last Activity	Productive	Unproductive	Undefined	Active Time	Offline Meetings
Michael	Office	08:43:23 AM	02:18:56 PM	4h 11m 1s	7m 19s	25m 56s	4h 43m 14s	0s
Marcy	Remote	08:41:02 AM	04:25:12 PM	4h 25m 19s	25m 1s	1h 1m 26s	5h 12m 10s	1h 0m 0s
Tamika	Office	09:13:22 AM	03:59:03 PM	3h 56m 4s	30m 0s	33m 48s	4h 51m 2s	30m 0s
Victorina	Office	08:59:08 AM	04:11:25 PM	4h 18m 50s	12m 22s	1m 15s	5h 36m 51s	0s
Hank	Remote	09:26:34 AM	04:39:31 PM	4h 10m 22s	21m 13s	30m 17s	5h 11m 19s	1h 30m 0s
Daron	Office/Remote	09:52:59 AM	05:02:33 PM	4h 11m 1s	7m 19s	25m 56s	4h 43m 14s	30m 0s
Maximo	Office	11:17:47 AM	03:32:00 PM	4h 25m 19s	25m 1s	1h 1m 26s	5h 12m 10s	0s

Рис. 3.16. Часова продуктивність

Рис. 3.17. Звідки вони працюють

Рис.3.18 представляє діаграму, яка відображає відсоток використання різних додатків та сайтів, згрупованих за активністю користувачів.

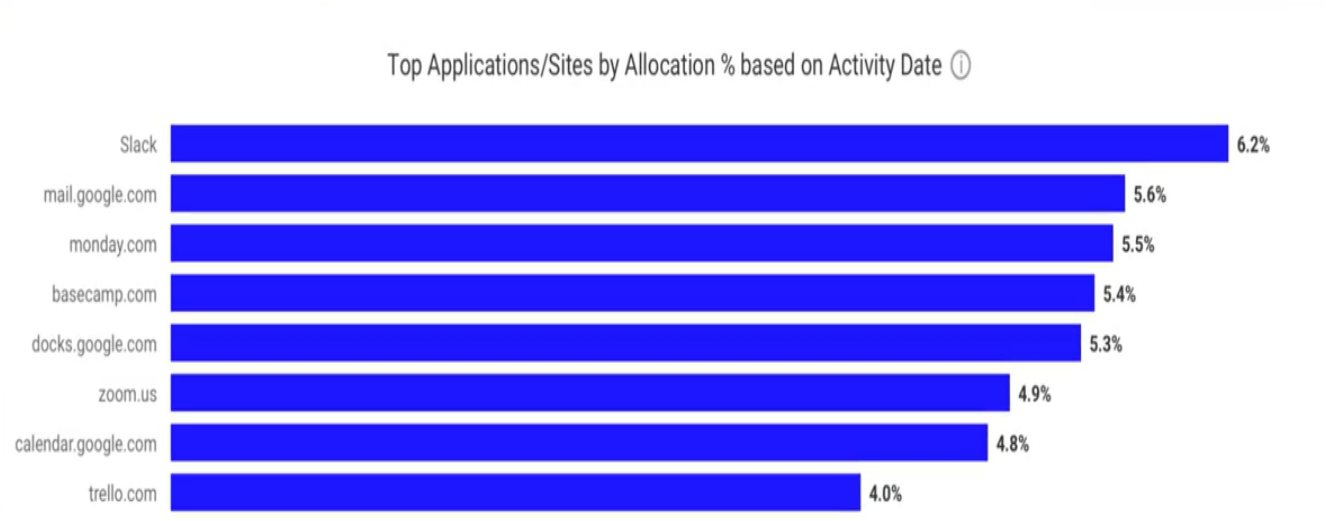


Рис. 3.18. Які адреси і ПЗ застосовувалося

Ця візуалізація дозволяє організаціям легко відслідковувати активність користувачів у різних додатках і швидко виявляти аномальні або підозрілі патерни. Наприклад [15-20].:

Виявлення аномальної активності: Якщо показник використання якогось додатку раптово зростає або значно відрізняється від стандартних показників, це

може вказувати на потенційну внутрішню загрозу або на те, що користувачі витрачають забагато часу на певні платформи, що не пов'язані з їх роботою.

Попередження про потенційні внутрішні загрози: Наприклад, якщо додатки для комунікації (як Slack чи mail.google.com) використовуються більше, ніж додатки для робочих завдань (як monday.com чи basecamp.com), це може свідчити про зниження продуктивності або потенційні порушення в роботі, такі як обмін конфіденційною інформацією поза межами контрольованих каналів.

Оцінка ефективності використання робочих ресурсів: Цей графік дозволяє оцінити, наскільки часто використовуються різні платформи для командної роботи (як Trello, Zoom або Google Calendar). Це допомагає виявити, які інструменти є найбільш ефективними, а які можливо мають низьку продуктивність.

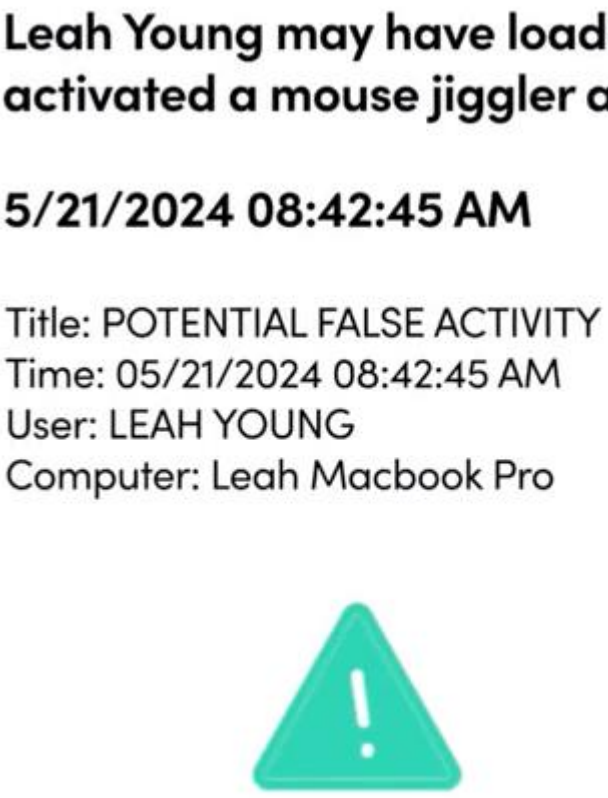


Рис. 3.19. Сповіщення потенційно негативної активності

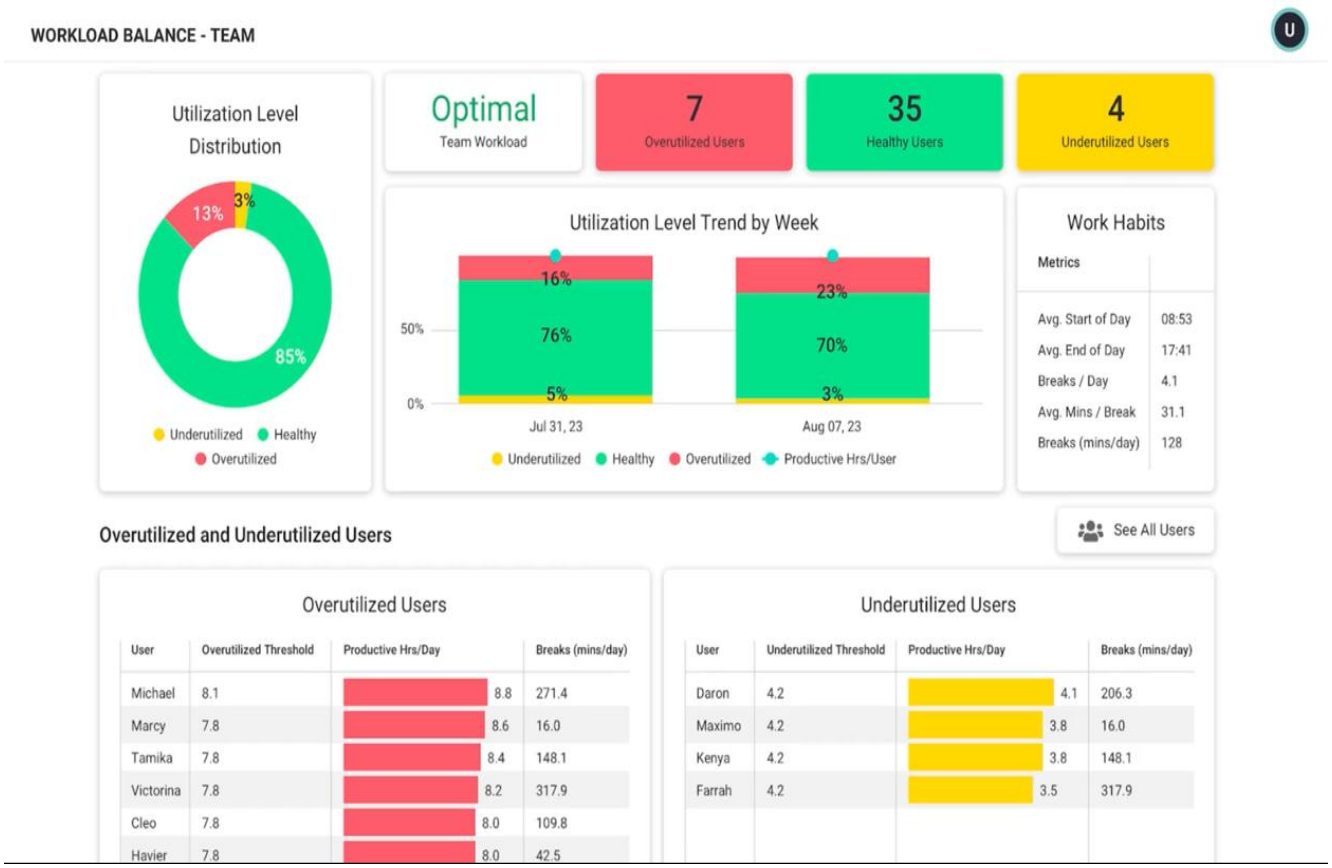


Рис. 3.20. Відображення інформації про рівень використання ресурсів командою

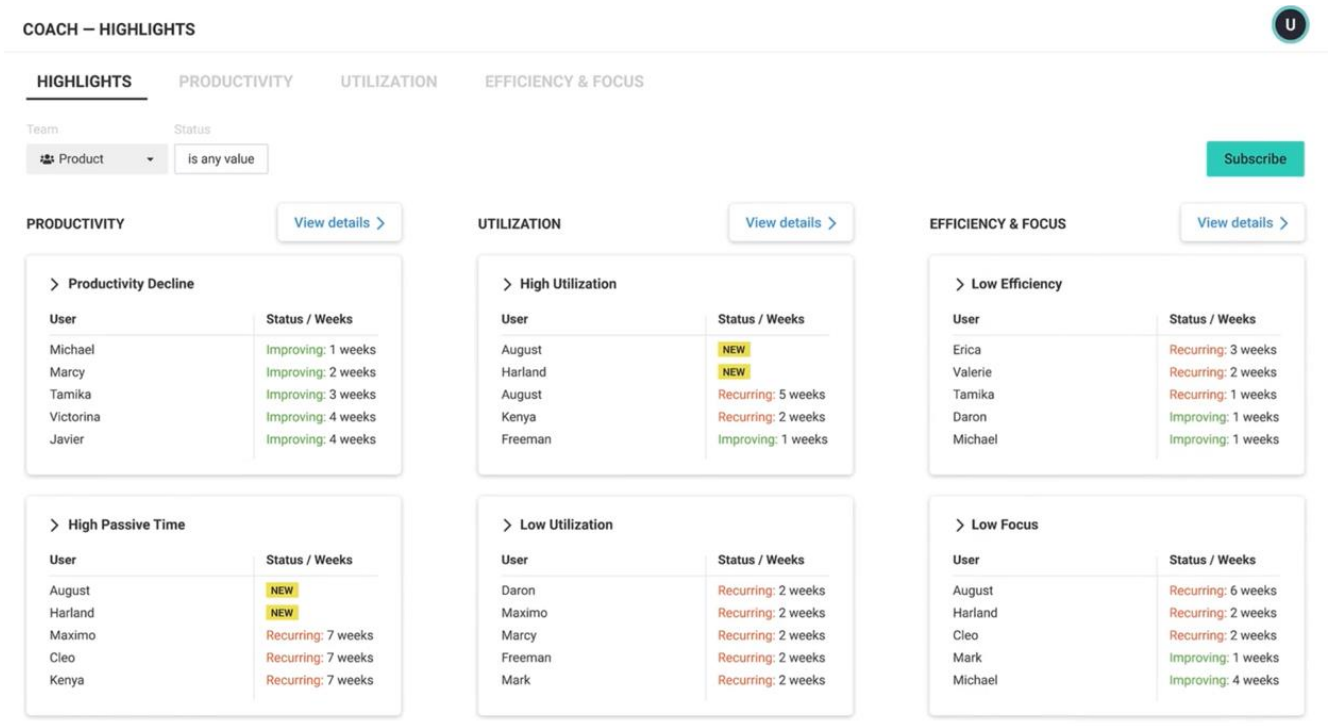


Рис. 3.21. Coach – Highlights

Рис.3.21 є частиною системи моніторингу доступу до сайтів, що попереджає користувача про порушення встановлених правил використання Інтернету.

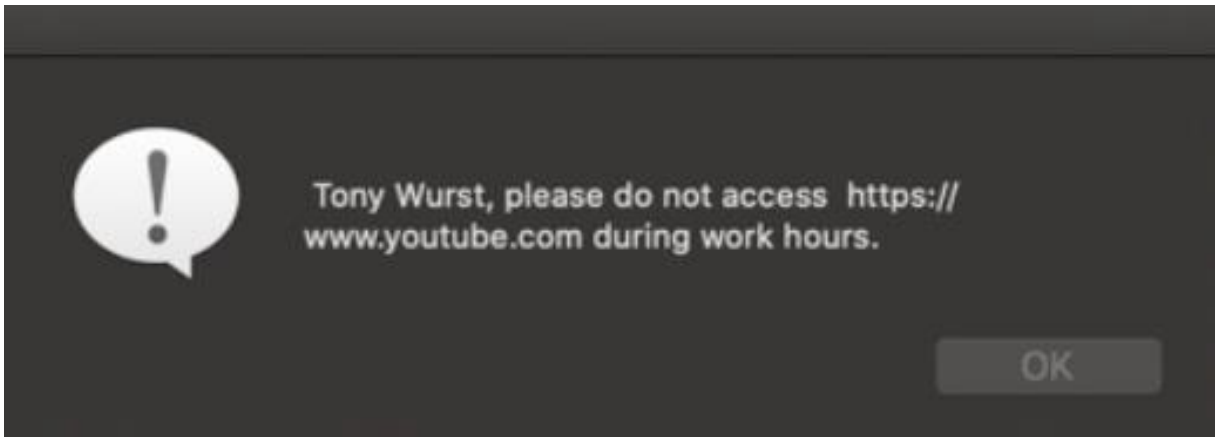


Рис. 3.21. порушення встановлених правил використання Інтернету

На рис.3.22 екран журналу сигналів тривоги в інтерфейсі моніторингового програмного забезпечення, для відстеження активності користувачів на комп'ютерах. Основні елементи цього інтерфейсу [15-20].:

Меню навігації зліва: Включає розділи:

"Live Reports" (Живі звіти)

"Integrations" (Інтеграції)

"Alarms" (Сигнали тривоги), з підпунктами

"Risk Level" (Рівень ризику) та "Alarm Log" (Журнал тривог)

"Configuration" (Конфігурація)

"Screenshots" (Скріншоти)

"Videos" (Відео)

"Notifications" (Сповіщення)

Журнал сигналів тривоги (Alarm Log):

У цьому розділі відображаються записи про події з тривогою. Кожен рядок представляє окремий сигнал тривоги і містить такі поля:

Prod - індикатор продуктивності або статусу.

Alarm Name (Назва сигналу тривоги)

Date/Time (Дата/Час): Дата і час виникнення тривоги

Computer (Комп'ютер): Ідентифікатор комп'ютера, з якого отримано сигнал (наприклад, LAPTOP-9L3N916H).

User (Користувач): Ім'я користувача, під яким було створено сигнал.

Session (Сесія): Номер сесії.

Duration (Тривалість): Тривалість події в секундах (наприклад, 9s, 7s, 3s, 10s).

Додаткові відомості: Наприклад, які програми чи сайти були.

Цей дозволяє адміністраторам переглядати та фільтрувати журнали тривог для відстеження активності користувачів, що допомагає ідентифікувати потенційно небажану активність.

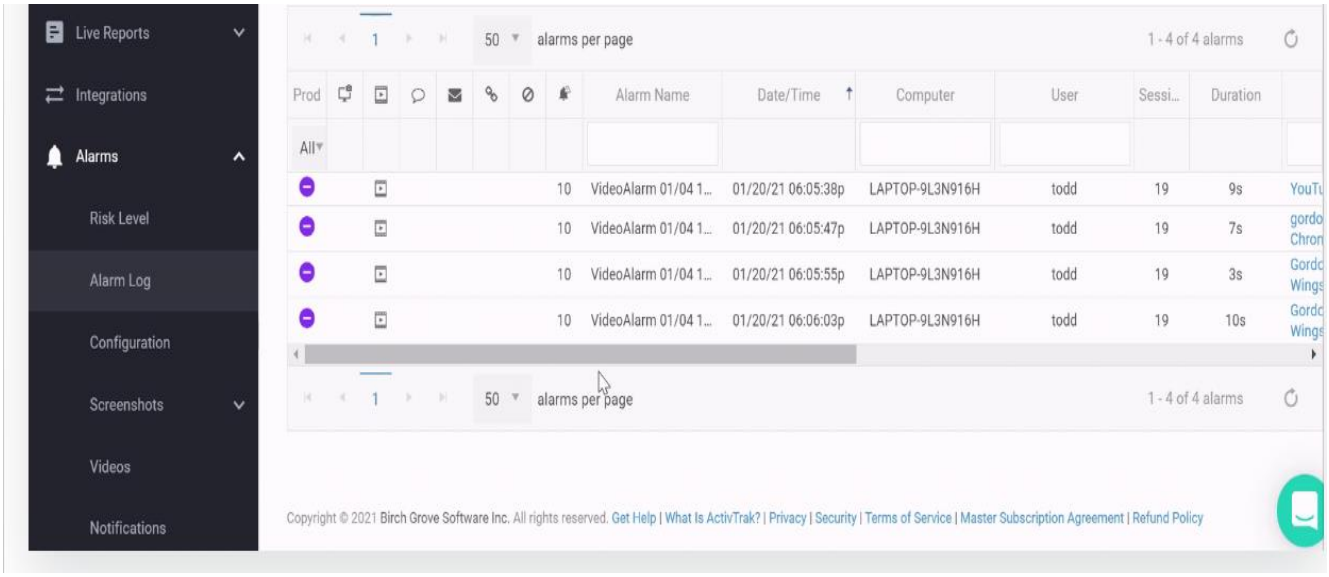


Рис.3.22. Екран журналу сигналів тривоги

На рис. 3.23 відображено дві панелі з графіками, що відображають розподіл та ранжування ризикових показників користувачів у системі. Нижче приведений детальний опис кожної панелі.

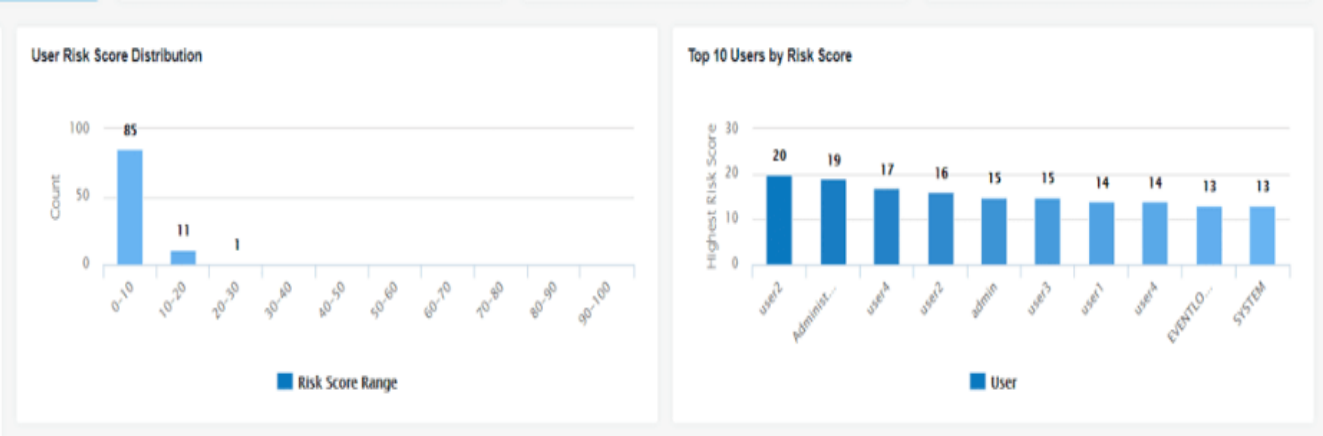


Рис. 3.23. Розподіл та ранжування ризикових показників користувачів у системі

1. **User Risk Score Distribution (Розподіл ризикових показників користувачів):**

- Це стовпчикова діаграма, яка відображає кількість користувачів у різних діапазонах ризикових показників.
- Основна частина користувачів (85 осіб) має низький ризик (показник від 0 до 10).
- Деякі користувачі (11 осіб) мають ризиковий показник у діапазоні 10-20, а ще один користувач — у діапазоні 20-30.
- Інші діапазони ризику (30-100) не мають користувачів, що свідчить про те, що більшість користувачів знаходяться в зоні низького ризику.

2. **Top 10 Users by Risk Score (Топ 10 користувачів за ризиковими показниками):**

- Це стовпчикова діаграма, яка показує 10 користувачів із найвищими ризиковими показниками.
- Найвищий ризиковий показник становить 20 для користувача "user2", за яким слідують інші користувачі з балами 19, 17, 16 і так далі.
- Останні два місця в цьому списку мають показник 13.
- Ця панель допомагає визначити користувачів із підвищеним ризиком, що дозволяє адміністраторам сфокусуватися на них для подальшого моніторингу чи аналізу [15-20]..

Дані графіки дозволяють адміністраторам ідентифікувати загальний рівень ризику серед користувачів та виділити найбільш ризикових для подальшої перевірки або дій.

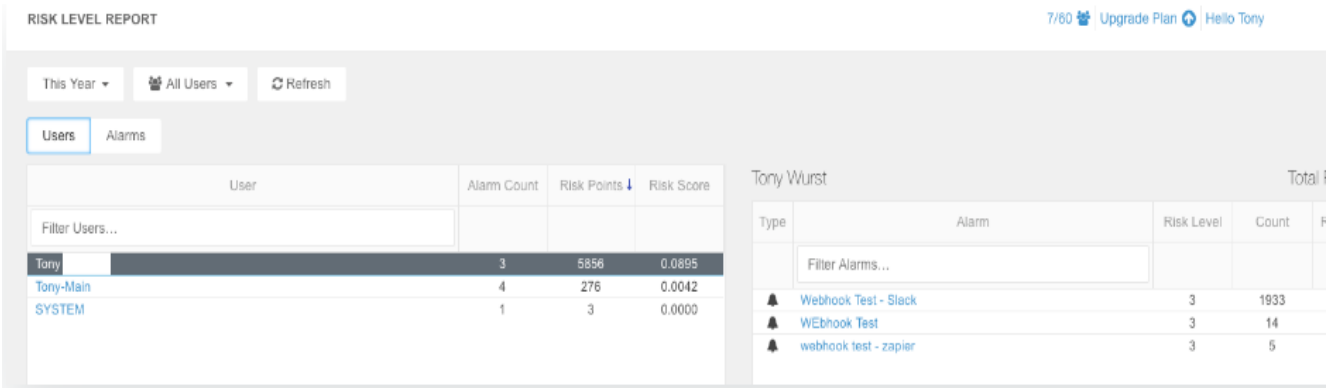


Рис.3.24. Рівень ризику

Оцінка ризику тривоги - це розрахунковий показник, який можна порівнювати від періоду до періоду, від групи до групи та від користувача до користувача. Оцінка базується на загальній кількості балів ризику користувача, поділеній на максимальну кількість записів у журналі активності для одного користувача в організації протягом певного періоду часу. Бали ризику - це сума рівнів ризику тривог, помножена на кількість разів, коли користувач активував тривогу протягом певного періоду часу [15-20].

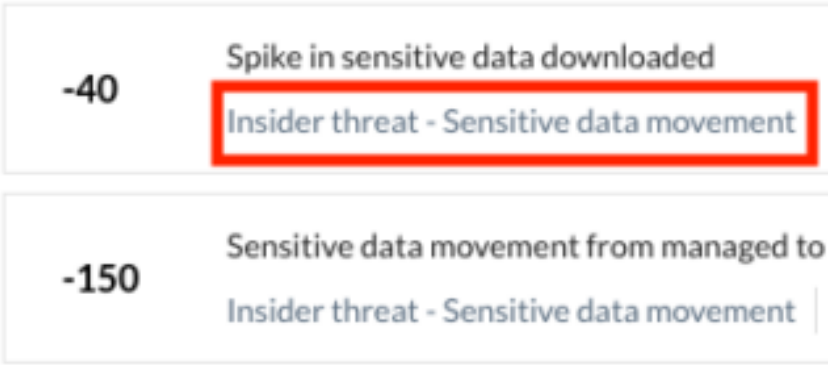


Рис. 3.25. Виявлення загрози

Перший запис має оцінку -40, що вказує на "Spike in sensitive data downloaded" (сплеск завантаження конфіденційних даних).

Другий запис має оцінку -150 і опис "Sensitive data movement from managed to unmanaged location" (переміщення конфіденційних даних з керованого на некероване місце).

Під кожним описом події є текстове посилання "Insider threat - Sensitive data movement" (Внутрішня загроза - Переміщення конфіденційних даних).

Ці записи відображають інформацію про потенційні інциденти, пов'язані з ризиком витоку конфіденційної інформації через дії всередині організації. Вони дозволяють адміністраторам швидко визначити серйозні події, пов'язані з внутрішніми загрозами, та вжити відповідних заходів для захисту даних [15-20]..

Employee	Computer	Policy	Rule	Action
Kate Sparrow	WIN-035KHOR8PER	Demo Policy	Block notepad that is opened by CLI	Block
MIndy Jameson		Anomalies	Webpages Anomalies	
Chadwick Singh		Anomalies	Excess time on unproductive site	
Raphael Dantes		Anomalies	File upload anomaly	
Raphael Dantes		Anomalies	Excess time on unproductive site	
Raphael Dantes		Anomalies	Excess time on unproductive site	

Рис. 3.26. Спрацювання політик безпеки

Policy (Політика): Назва політики, яка була активована під час події. Наприклад:

Rule (Правило): Опис правила, яке спрацювало у відповідності до політики. Серед прикладів:

"Block notepad that is opened by CLI" (Блокувати блокнот, відкритий через командний рядок)

"Webpages Anomalies" (Аномалії на веб-сторінках)

"Excess time on unproductive site" (Надмірний час на непродуктивному сайті)

"File upload anomaly" (Аномалія завантаження файлів)

Action (Дія): Опис дії, яку було виконано у відповідь на подію. Наприклад, "Block" (Блокувати) для першого запису [15-20]..

3.3. Розроблення рекомендацій щодо застосування технології захисту організації від інсайдерських атак на базі рішення ActivTrak UEBA

ActivTrak — це потужна платформа UEBA (User and Entity Behavior Analytics), яка дозволяє аналізувати поведінку користувачів, щоб виявити аномалії, пов’язані з потенційними інсайдерськими загрозами. Впровадження ActivTrak допомагає організаціям краще зрозуміти, як співробітники взаємодіють із системами та даними, і виявляти підозрілу поведінку.

Рекомендації щодо застосування технології захисту організації від інсайдерських атак на базі ActivTrak UEBA:

1. Виявлення внутрішніх загроз

- **Створення базових профілів поведінки**: Використання ActivTrak для формування звичайних моделей поведінки користувачів (робочих звичок, звичних годин активності, доступу до конкретних ресурсів).
- **Налаштування тригерів для підозрілої поведінки**: Встановлення автоматичних оповіщень для аномальної поведінки, наприклад, коли співробітник відкриває великий обсяг конфіденційних даних, намагається передати файли через зовнішні канали або виконує дії, що виходять за межі його звичайних обов'язків.
- **Відстеження аномалій у режимі реального часу**

2. **Запобігання внутрішнім загрозам**

- **Обмеження доступу за принципом мінімальних привілеїв**: встановлення обмеження на доступ до конфіденційних даних, забезпечуючи те, що співробітники мають лише той доступ, який необхідний для виконання їхніх обов'язків.
- **Регулярний аналіз та перегляд привілеїв**: Використовуючи аналітику, необхідно регулярно переглядати рівні доступу та вносити зміни, якщо співробітники більше не потребують доступу до певних систем або даних.
- **Навчання персоналу з питань безпеки**.

3. **Реагування на інциденти**

- **Автоматизовані звіти про підозрілу активність.**

- **Інтеграція з іншими системами безпеки**: Інтегруйте ActivTrak з SIEM-системами або іншими інструментами моніторингу безпеки для більш глибокого аналізу даних та кращої реакції на інциденти. Це допоможе забезпечити швидке реагування на потенційні інсайдерські загрози.
- **Розробка плану дій у разі інциденту**: На основі даних, зібраних через ActivTrak, створіть детальний план дій для реагування на підозрілі або шкідливі дії. Це має включати чіткі вказівки щодо того, як ізолювати порушника, обмежити його доступ до системи та провести розслідування.

4. Оптимізація продуктивності та процесів

- **Визначення неефективності процесів**: інсайтам, зібрані ActivTrak, дозволяє виявити повільні або неефективні процеси в організації, які потенційно можуть спричинити ризики (наприклад, затримки у виконанні критичних завдань).
- **Перерозподіл ресурсів**: ActivTrak допомагає оптимізувати використання ресурсів, забезпечуючи кращу роботу команди без зайвих ризиків для безпеки.
- **Забезпечення балансу між безпекою та продуктивністю**: Досліджуйте, як співробітники витрачають робочий час, щоб уникнути перешкод у продуктивності, але зберегти високий рівень безпеки. Важливо знайти оптимальний баланс між контролем і довірою до співробітників.

5. Оцінка ефективності впроваджених заходів

- **Регулярні аудити безпеки**: здійснення регулярних перевірок використання ActivTrak та оцінка ефективності заходів, спрямованих на захист від інсайдерських атак. Це допоможе організації визначити, наскільки система ефективно справляється з загрозами.
- **Моніторинг змін у поведінці**: постійне відстеження зміни у поведінці співробітників, особливо після впровадження нових політик або навчальних програм. Зміни у звичках можуть вказувати на ефективність навчання або, навпаки, підвищення рівня ризику.
- **Вдосконалення політик на основі даних**: використання даних ActivTrak для регулярного оновлення та вдосконалення політик безпеки, що дозволить

організації бути готовою до нових загроз і покращувати захист від інсайдерських атак.

Висновки до розділу 3

1. Розроблено варіант розгортання та налаштування технології захисту організації від ІА на базі рішення ActivTrak UEBA.

2. В практичній частині показано основні кроки щодо використання даного рішення, відповідно до раніше застосованих правил та налаштувань. Відображено результати реагування рішення ActivTrak UEBA на прикладі.

3. Розроблено рекомендацій щодо застосування технології захисту організації від інсайдерських атак на базі рішення ActivTrak UEBA, які покращують розуміння необхідності використання функцій та модулів даного рішення.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи отримано наступні результати:

1. Проведено аналіз необхідності захисту організацій від інсайдерських атак з приведенням статистики стрімкого зростання.

2. Проведено класифікацію інсайдерських загроз та наведені основні ідентифікатори інсайдерських атак.

3. Проведено типи критичних даних та потенційні наслідки від інсайдерських атак на основі звіту IBM X-Force.

4. проведено дослідження методів та засобів захисту від інсайдерських атак, а також представлено архітектуру UEBA в якій розкрито призначення, основні можливості та функції рішення ActivTrak UEBA, що займає перше місце серед інших UEBA рішень згідно.

5. Розроблено варіант розгортання та налаштування технології захисту організації від ІА на базі рішення ActivTrak UEBA.

6. В практичній частині показано основні кроки щодо використання даного рішення, відповідно до раніше застосованих правил та налаштувань. Відображено результати реагування рішення ActivTrak UEBA на прикладі.

7. Розроблено рекомендацій щодо застосування технології захисту організації від інсайдерських атак на базі рішення ActivTrak UEBA, які покращують розуміння необхідності використання функцій та модулів даного рішення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ігнатенко В. О. Технологія захисту організації від інсайдерських атак. «Актуальні проблеми кібербезпеки» : Всеукр. науково-практ. конф., м. Київ, 25 жовт. 2024 р. Київ, 2024. С. 74–76.

2. Schulze H. 2024 Insider Threat Report: Key Trends & Fixes. Cybersecurity Insiders. URL: https://www.cybersecurity-insiders.com/2024-insider-threat-report-trends-challenges-and-solutions/ (дата звернення: 01.11.2024).

3. 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: 01.11.2024).

4. Roberts S. Insider Threats in Cyber Security - All You Need to Know in 2024. theknowledgeacademy. URL:https://www.theknowledgeacademy.com/blog/insider-threats-in-cyber-security/ (дата звернення: 01.11.2024).

5. IBM Security X-Force Threat Intelligence Index 2024. IBM - United States. URL: https://www.ibm.com/reports/threat-intelligence (дата звернення: 01.11.2024).

6. Chin K. How to detect and prevent insider threats | upguard. Third-Party Risk and Attack Surface Management Software | UpGuard. URL: https://www.upguard.com/blog/how-to-detect-and-prevent-insider-threats (дата звернення: 01.11.2024).

7. UEBA: what is user and entity behavior analytics? | radware. Radware Captcha Page. URL: https://www.radware.com/cyberpedia/cloud-security/ueba/ (дата звернення: 01.11.2024).

8. Advanced threat detection with user and entity behavior analytics (UEBA) in microsoft sentinel. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics (дата звернення: 01.11.2024).

9. Harris C. The Top 10 User And Entity Behavior Analytics (UEBA) Solutions | Expert Insights. Expert Insights. URL: https://expertinsights.com/insights/top-user-and-entity-behavior-analytics-solutions/ (дата звернення: 01.11.2024).

10. Saleem. How activtrak works -pricing, features 2023. Desklog. URL: https://desklog.io/blog/how-activtrak-works/ (дата звернення: 01.11.2024).

11. ActivTrak Review - Employee Monitoring Software for More Demanding Users. SoftwareSupport - The Agency of the Future, on-demand. URL: https://softwaresupp.com/blog/activtrak-review (дата звернення: 01.11.2024).

12. ActivTrak Product Team. Guide to Getting Started with ActivTrak. ActivTrak | Help Center. URL: https://support.activtrak.com/hc/en-us/articles/360034996271-Guide-to-Getting-Started-with-ActivTrak (дата звернення: 01.11.2024).

13. 2. Help Center Team. ActivTrak Agent Deployment Guide. ActivTrak | Help Center. URL: https://support.activtrak.com/hc/en-us/articles/360039249211-ActivTrak-Agent-Deployment-Guide (дата звернення: 02.11.2024).

14. Help Center Team. Agent Whitelist Addresses for Antivirus and Firewall. ActivTrak | Help Center. URL: https://support.activtrak.com/hc/en-us/articles/360034165131-Agent-Whitelist-Addresses-for-Antivirus-and-Firewall (дата звернення: 01.11.2024).

15. Help Center Team. Create and Manage Groups in ActivTrak. ActivTrak | Help Center. URL: https://support.activtrak.com/hc/en-us/articles/360034995171-Create-and-Manage-Groups-in-ActivTrak (дата звернення: 01.11.2024).

16. ActivTrak Product Team. Active Time and Passive Time in ActivTrak. ActivTrak | Help Center. URL: https://support.activtrak.com/hc/en-us/articles/360026990372-Active-Time-and-Passive-Time-in-ActivTrak (дата звернення: 01.11.2024).

17. ActivTrak Review - Employee Monitoring Software for More Demanding Users. SoftwareSupport - The Agency of the Future, on-demand. URL: https://softwaresupp.com/blog/activtrak-review (дата звернення: 01.11.2024).

18. Location Insights. ActivTrak. URL: https://www.activtrak.com/product/location-insights/ (дата звернення: 01.11.2024).

19. ActivTrak Product Team. End of Sale: Risk Levels Report. ActivTrak | Help Center. URL: https://support.activtrak.com/hc/en-us/articles/360026521891-End-of-Sale-Risk-Levels-Report (дата звернення: 01.11.2024).

20. ActivTrak Overview, 2024. ActivTrak. URL: https://www.activtrak.com/resources/videos/activtrak-overview/ (дата звернення: 01.11.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)