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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо захисту інформації від інсайдерських загроз на основі UAM Syteca»

зі спеціальності *125 Кібербезпека*
(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

_____ Антоніна КОРЖ
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
КОРЖ Антоніна
(прізвище, ім'я)

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

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

Київ 2025

ВСТУП

В умовах активного використання цифрових технологій все більше організацій стикаються з необхідністю захищати внутрішню інформацію не лише від зовнішніх атак, а й від дій власних співробітників. Інсайдерські загрози стають дедалі поширенішими, а традиційні методи контролю часто не дають змоги своєчасно їх виявити. Це підвищує актуальність впровадження систем моніторингу дій користувачів, таких як UAM Syteca, які дають змогу контролювати активність у межах корпоративної мережі та запобігати витоку критичних даних. Упродовж останнього десятиліття спостерігається зростання інцидентів, пов’язаних з інсайдерськими загрозами. Класичні засоби інформаційної безпеки, такі як антивірусні програми чи міжмережеві екрани, не завжди здатні своєчасно виявити дії внутрішніх зловмисників, оскільки ті діють у рамках дозволених повноважень. Це потребує застосування спеціалізованих засобів моніторингу та аналізу поведінки користувачів, до яких належать системи класу UAM (User Activity Monitoring).

Ця кваліфікаційна робота присвячена дослідженню інсайдерських загроз, огляду існуючих методів виявлення та протидії цим загрозам, а також аналізу можливостей сучасних систем UAM для підвищення рівня захисту інформації. Особливу увагу приділено системі UAM Syteca, яка надає широкі можливості щодо моніторингу, запису та аналізу дій користувачів у корпоративній IT-інфраструктурі.

Таким чином, ця робота має на меті обґрунтувати доцільність використання сучасних технологій моніторингу активності користувачів як ефективного інструмента забезпечення інформаційної безпеки в умовах зростаючої складності та динаміки кіберзагроз з боку інсайдерів.

1 АНАЛІЗ ПРОБЛЕМИ ІНСАЙДЕРСЬКИХ ЗАГРОЗ В ОРГАНІЗАЦІЇ

1.1. Аналіз інсайдерських загроз та їх наслідки

Інсайдер — це будь-яка особа, яка має або мала авторизований доступ або знання ресурсів організації, включаючи персонал, приміщення, інформацію, обладнання, мережі та системи. Інсайдерська загроза — це можливість для інсайдера використовувати свій авторизований доступ або розуміння організації, щоб завдати їй шкоди. Ця шкода може включати навмисні чи ненавмисні дії, які негативно впливають на цілісність, конфіденційність і доступність організації, її даних, персоналу чи засобів.

Приклади інсайдера можуть включати:

- особа, якій організація довіряє, включаючи співробітників, членів організації та тих, кому організація надала конфіденційну інформацію, таку як фінансові дані, бізнес-стратегія, сильні та слабкі сторони організації. У контексті функцій уряду це також може включати секретну інформацію. Ця особа також може мати як фізичний, так і цифровий доступ до конфіденційних просторів.
- особа, якій надано бейдж або пристрій доступу, який ідентифікує її як особу з регулярним або постійним доступом (наприклад, працівник або член організації, підрядник, постачальник, зберігач або ремонтник).
- особа, якій організація надала комп’ютер та/або доступ до мережі.
- особа, яка має глибокі знання та, можливо, допомагає розвивати продукти та послуги організації; до цієї групи входять ті, хто знає секрети продуктів, які забезпечують цінність організації.

Інциденти внутрішньої загрози можливі в будь-якому секторі чи організації.

Кібератака – це навмисна спроба зловмисника або групи зловмисників проникнути в інформаційну систему, отримати несанкціонований доступ до її

ресурсів, порушити її працездатність, викрасти, пошкодити або знищити дані. Іншими словами, це будь-яка дія, спрямована на порушення одного або кількох принципів інформаційної безпеки:

- конфіденційність: Запобігання несанкціонованому розкриттю інформації.
- цілісність: Забезпечення точності та повноти інформації, а також її захист від несанкціонованої модифікації.
- доступність: Забезпечення того, що авторизовані користувачі мають своєчасний та надійний доступ до інформації та пов'язаних з нею ресурсів.

Кібератаки можуть бути різноманітними за складністю, метою та використовуваними методами. Вони можуть здійснюватися як окремими хакерами, так і організованими злочинними групами або навіть державними структурами. Інсайдерська загроза — це потенційна небезпека для інформаційної безпеки організації, яка виникає з боку осіб, що мають легітимний доступ до її інформаційних систем, даних або приміщень. Ці особи можуть бути співробітниками (поточними або колишніми), підрядниками, партнерами або іншими авторизованими користувачами. Кібератака та інсайдерська загроза є двома різними типами загроз для інформаційної безпеки, хоча вони можуть мати спільні наслідки. Основні відмінності наведено в таблиці 1.1.

Таблиця 1.1

Різниця кібератаки та інсайдерської загрози

Характеристика	**Кібератака**	**Інсайдерська загроза**
Джерело	Зовнішнє (неавторизовані особи)	Внутрішнє (авторизовані особи)
Початковий доступ	Потрібно отримати несанкціонований доступ	Вже існує легітимний доступ
Основні методи	Технічні (шкідливе ПЗ, експлойти, фішинг)	Технічні та нетехнічні (зловживання доступом, розголошення)
Мотивація	Різна (фінанси, шпигунство, ідеологія)	Різна (фінанси, помста, недбалість)

Інсайдерська загроза — це можливість для інсайдера використовувати свій авторизований доступ або розуміння організації, щоб завдати їй шкоди. 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 внутрішню загрозу як загрозу того, що інсайдер використовує свій авторизований доступ, свідомо чи мимоволі, щоб завдати шкоди місії відділу, ресурсам, персоналу, об'єктам, інформації, обладнанню, мережам або системам. Ця загроза може проявлятися як збиток відділу через такі дії внутрішньої особи:

- Шпигунство
- Тероризм
- Несанкціоноване розголошення інформації
- Корупція, в тому числі участь у транснаціональній організованій злочинності
- Саботаж
- Насильство на робочому місці
- Навмисна чи ненавмисна втрата чи деградація ресурсів чи можливостей відділу

Типи внутрішніх загроз:

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 [1].

- Випадковий – інсайдер такого типу помилково створює ненавмисний ризик для організації. Приклади включають неправильне введення адреси електронної пошти та випадкове надсилання конфіденційного ділового документа конкуренту, несвідоме чи випадкове клацання гіперпосилання, відкриття вкладення у фішинговому електронному листі, яке містить вірус, або неналежну утилізацію конфіденційних документів.

Навмисні загрози.

Навмисного інсайдера часто називають «зловмисним інсайдером». Навмисні погрози – це дії, вжиті з метою завдати шкоди організації заради особистої вигоди або діяти на підставі особистої скарги. Наприклад, багато інсайдерів мотивовані «поквитатися» 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 в помилковій надії просунутися по кар'єрі.

Інші загрози:

- Змовні загрози. Підгрупа зловмисних внутрішніх загроз називається змовними загрозами, коли один або кілька інсайдерів співпрацюють із зовнішнім учасником загрози, щоб скомпрометувати організацію. У цих інцидентах часто кіберзлочинці вербують інсайдера або кількох інсайдерів для шахрайства, крадіжки інтелектуальної власності, шпигунства або комбінації цих трьох.

- Загрози від третіх осіб . Крім того, до загроз від третіх сторін зазвичай відносяться підрядники або постачальники, які офіційно не є членами організації, але яким надано певний рівень доступу до засобів, систем, мереж або людей для виконання своєї роботи. Ці загрози можуть бути прямими або непрямими.

Як виникає внутрішня загроза? Внутрішні загрози проявляються різними способами: насильство, шпигунство, диверсії, крадіжки та кіберактивності. Вирази внутрішньої загрози детально визначені нижче.

Вираження внутрішньої загрози:

Насильство – ця дія включає загрозу насильства, а також іншу загрозливу поведінку, яка створює залякувальне, вороже чи образливе середовище.

- Насильство на робочому місці/в організації – це будь-яка дія або загроза фізичного насильства, переслідування, сексуальних домагань, залякування, знущань, образливих жартів або іншої загрозливої поведінки з боку колеги чи партнера, яка відбувається на місці роботи особи або під час роботи.
- Тероризм як внутрішня загроза — це незаконне використання або загроза насильства співробітниками, членами чи іншими особами, тісно пов'язаними з організацією, проти цієї організації. Метою тероризму є досягнення політичних або соціальних цілей.

Шпигунство – це таємна або незаконна практика шпигунства за іноземним урядом, організацією, юридичною особою 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 методів, методів, процесів, процедур, програм або кодів для виробництва).
- Урядове шпигунство — це таємна 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 розвідувальної інформації.
- Злочинне шпигунство.

Саботаж – саботаж описує навмисні дії з метою завдати шкоди фізичній або віртуальній інфраструктурі організації, включаючи недотримання процедур

технічного обслуговування або IT-процедур, забруднення чистих приміщень, фізичне пошкодження об’єктів або видалення коду для запобігання регулярним операціям.

- Фізичний саботаж — це вчинення навмисних дій, спрямованих на заподіяння шкоди фізичній інфраструктурі організації (наприклад, приміщенням або обладнанню).
- Віртуальний саботаж — це вчинення зловмисних дій за допомогою технічних засобів, щоб порушити або зупинити звичайні бізнес-операції організації.

Крадіжка – крадіжка – це викрадення грошей чи інтелектуальної власності.

- Фінансовий злочин — це несанкціоноване заволодіння або незаконне використання грошей або майна особи, підприємства чи організації з наміром отримати від цього вигоду.
- Крадіжка інтелектуальної власності — це викрадення або пограбування ідей, винаходів або творчих проявів особи чи організації, включно з комерційними таємницями та запатентованими продуктами, навіть якщо викрадені концепції чи предмети походять від злодія.

Кібернетична загроза включає в себе крадіжку, шпигунство, насильство та саботаж усього, що стосується технологій, віртуальної реальності, комп’ютерів, пристроїв або Інтернету.

- Ненавмисні загрози – це незловмисне (часто випадкове чи ненавмисне) розкриття IT-інфраструктури, систем і даних організації, яке завдає ненавмисної шкоди організації. Приклади включають фішингові електронні листи, шахрайське програмне забезпечення та «зловмисну рекламу» (вбудовування шкідливого вмісту в законну онлайн-рекламу).
- Навмисні загрози — це зловмисні дії, вчинені зловмисними інсайдерами, які використовують технічні засоби, щоб порушити або зупинити регулярні бізнес-операції організації, виявити слабкі місця в IT, отримати захищену інформацію або іншим чином просувати план атаки через доступ до IT-систем. Ця дія може включати

зміну даних або вставлення зловмисного програмного забезпечення чи іншого образливого програмного забезпечення для порушення роботи систем і мереж.

Індикатори внутрішніх загроз

Розуміння ознак внутрішніх загроз є важливим для організацій, щоб захистити свою конфіденційну інформацію та підтримувати безпечне робоче середовище. Ось деякі загальні ознаки внутрішніх загроз, на які організації повинні звернути увагу:

- Незвичайні моделі доступу: працівники, які отримують доступ до конфіденційних даних або систем, з якими вони зазвичай не взаємодіють, особливо в неробочий час.
- Збільшене завантаження або обмін даними: незрозумілі стрибки завантажень даних або передачі файлів, особливо якщо вони стосуються великої кількості конфіденційної інформації.
- Обхід протоколів безпеки: працівники, які часто намагаються обійти встановлені заходи безпеки, такі як вимкнення програмного забезпечення безпеки або використання неавторизованих пристроїв.
- Негативні зміни в поведінці: раптові зміни у ставленні співробітника, такі як зростання розчарування, незалученості або конфлікти з колегами.
- Часті запити на конфіденційну інформацію: працівники просять надати доступ до інформації, яка не стосується їхніх посад чи обов’язків.
- Використання неавторизованого програмного забезпечення: встановлення або використання несанкціонованого програмного забезпечення чи програм, які можуть поставити під загрозу безпеку.
- Непослідовний робочий час: працівники, які часто працюють у нерегулярний час або часто відсутні без пояснення причин, що викликає занепокоєння щодо їх діяльності.
- Недотримання протоколів: зразок ігнорування політики компанії щодо обробки даних, безпеки та зв’язку.

- Публічний обмін конфіденційною інформацією: співробітники обговорюють конфіденційні питання компанії на публічних форумах або в соціальних мережах.
- Звіти інших співробітників: занепокоєння колег щодо поведінки або дій особи, які здаються підозрілими або незвичайними [2].

Згідно з даними групи кібербезпеки SafetyDetectives , контейнер AWS S3, що містить інформацію про «електронну сумку для польотів» (EFB) Pegasus Airlines, залишився без захисту паролем, що призвело до витоку низки конфіденційних даних про польоти. Інформація про ковш була пов’язана з програмним забезпеченням EFB, розробленим PegasusEFB, яке пілоти використовують для навігації літака, зльоту/посадки, дозаправки, процедур безпеки та різних інших процесів у польоті. У відкритому сегменті PegasusEFB усі дані, зокрема карти польотів, навігаційні матеріали та ідентифікаційна інформація екіпажу, були доступні кожному. Відро також виявило вихідний код програмного забезпечення EFB, який містив звичайні текстові паролі та секретні ключі, які хтось міг використати для підробки надзвичайно конфіденційних файлів. Ми не перевіряли ці облікові дані з етичних міркувань. Майже 23 мільйони файлів було знайдено у відрі, загальним обсягом близько 6,5 ТБ даних. Це опромінення може вплинути на безпеку кожного пасажира та члена екіпажу Pegasus у всьому світі. Афілійовані авіакомпанії, які використовують PegasusEFB, також можуть постраждати.

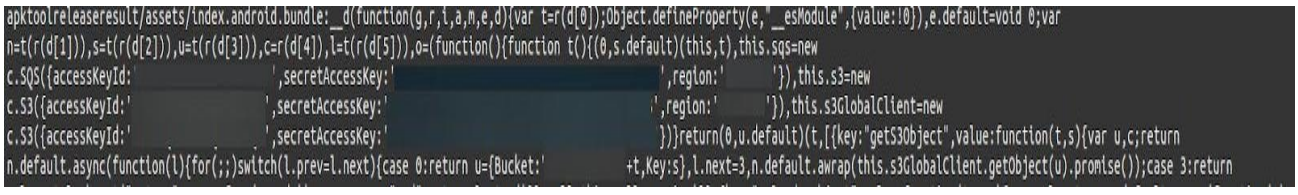


Рис. 1.1. Паролі та секретні ключі

Паролі та секретні ключі, які зазначено на рис.1 можуть надати доступ до надзвичайно конфіденційних файлів. Відкрите відро PegasusEFB було виявлено 28 лютого 2022 року в рамках масштабного проекту веб-картографії команди кібербезпеки SafetyDetectives. Дослідники SafetyDetectives використовують веб-

сканери для пошуку незахищених сховищ даних. Після виявлення відра наші дослідники перевірили відкриті дані PegasusEFB. урецька авіакомпанія Pegasus Airlines, заснована в 1990 році, спеціалізується на недорогих внутрішніх і міжнародних рейсах. Турецька приватна інвестиційна компанія Esas Holding AS володіє контрольним пакетом акцій компанії. Штаб-квартира Pegasus розташована в Стамбулі, і у 2021 році вона отримала 620 мільйонів доларів США доходу. PegasusEFB, компанія, дочірня з Pegasus Airlines, володіє відкритим відром, що містить інформацію про Pegasus EFB. Кілька авіакомпаній використовують програмне забезпечення PegasusEFB, включаючи Pegasus, IZairi Air Manas згідно з їх веб-сайтом. PegasusEFB володіє Electronic Flight Bag це стало відомо завдяки посиланням у вмісті відра.

Рис. 1.2. Вікно інсталяції адміністративної панелі PegasusEFB

Було викрито Відкритий сегмент AWS S3 PegasusEFB відкрив конфіденційні дані польоту, ідентифікаційну інформацію екіпажу та вихідний код програмного

забезпечення EFB. Amazon не несе відповідальності за неправильну конфігурацію сегмента PegasusEFB. Конфіденційні дані про рейс. Понад 3,2 мільйона файлів містили конфіденційні дані про польоти. Електронні таблиці (близько 2,9 мільйона файлів) і форми прийняття (понад 290 000 файлів) були двома найпоширенішими наборами даних, що містять цю інформацію:

- Форми приймання з детальним описом незначних проблем, виявлених під час передпольотних перевірок
- Польотні карти та редакції, які використовуються для допомоги в навігації та посадці
- Електронні таблиці, що містять інформацію про аеропорти, рейси, зміни екіпажу тощо.
- Документи та меморандуми, в т.ч. Страхові документи, дозволи та інструкції з техніки безпеки
- SIL – рівень цілісності безпеки, журнали, що містять правила та вихідний код

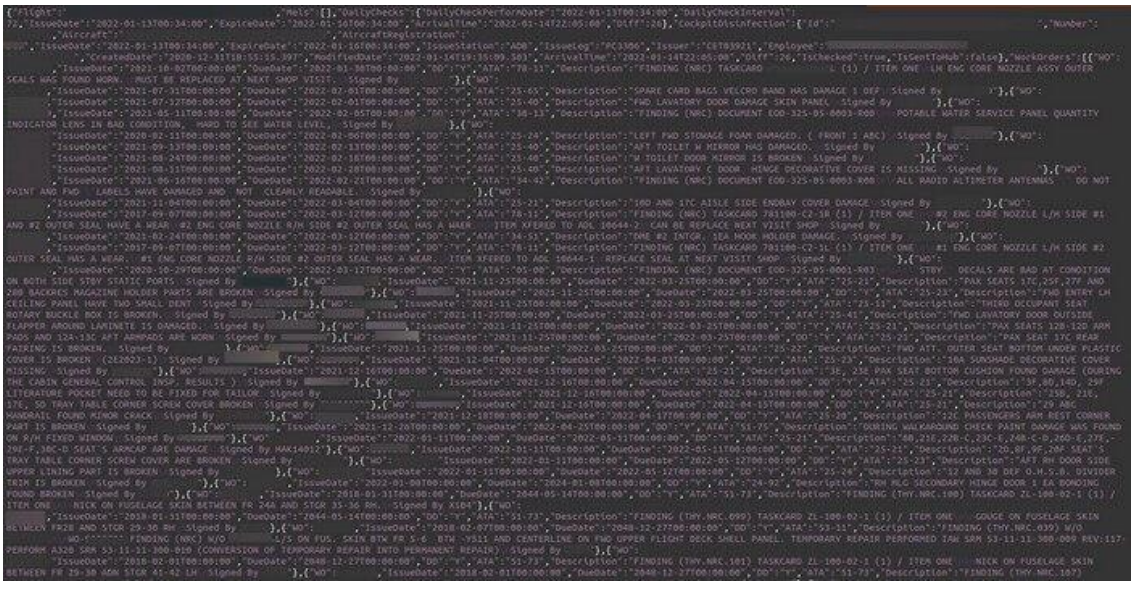


Рис. 1.3. Приймальні форми детальні передпольотні перевірки

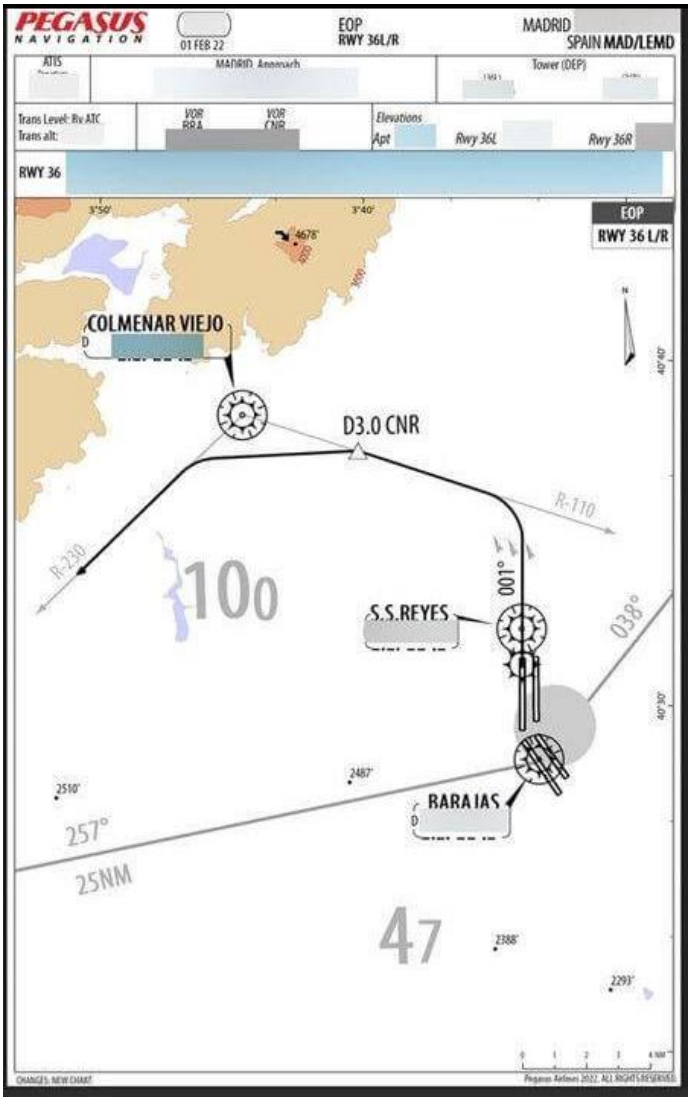


Рис. 1.4. Польотні карти містять навігаційну інформацію

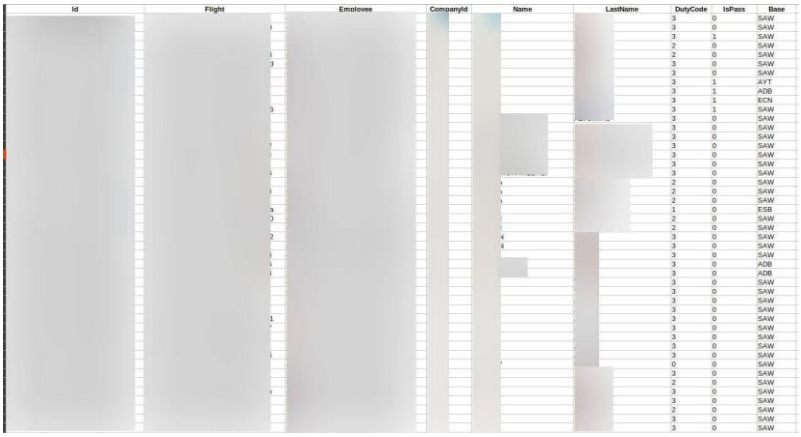
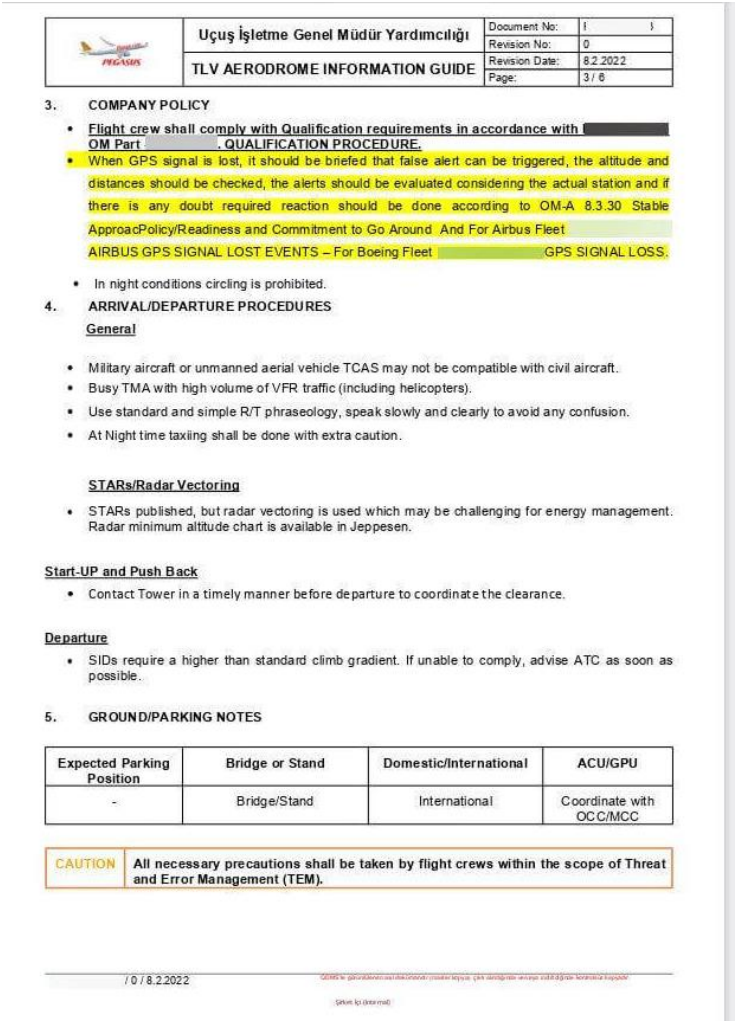


Рис. 1.5. Файли .CSV показували інформацію про рейс і екіпаж



	Uçuş İşletme Genel Müdür Yardımcılığı	Document No:	I
		Revision No:	0
	TLV AERODROME INFORMATION GUIDE	Revision Date:	8.2.2022
		Page:	3 / 6

3. **COMPANY POLICY**

- **Flight crew shall comply with Qualification requirements in accordance with [redacted] OM Part [redacted]. QUALIFICATION PROCEDURE.**
- When GPS signal is lost, it should be briefed that false alert can be triggered, the altitude and distances should be checked, the alerts should be evaluated considering the actual station and if there is any doubt required reaction should be done according to OM-A 8.3.30 Stable ApproacPolicy/Readiness and Commitment to Go Around And For Airbus Fleet AIRBUS GPS SIGNAL LOST EVENTS – For Boeing Fleet [redacted] GPS SIGNAL LOSS.
- In night conditions circling is prohibited.

4. **ARRIVAL/DEPARTURE PROCEDURES**

General

- Military aircraft or unmanned aerial vehicle TCAS may not be compatible with civil aircraft.
- Busy TMA with high volume of VFR traffic (including helicopters).
- Use standard and simple R/T phraseology, speak slowly and clearly to avoid any confusion.
- At Night time taxiing shall be done with extra caution.

STARs/Radar Vectoring

- STARs published, but radar vectoring is used which may be challenging for energy management. Radar minimum altitude chart is available in Jeppesen.

Start-UP and Push Back

- Contact Tower in a timely manner before departure to coordinate the clearance.

Departure

- SIDs require a higher than standard climb gradient. If unable to comply, advise ATC as soon as possible.

5. **GROUND/PARKING NOTES**

Expected Parking Position	Bridge or Stand	Domestic/International	ACU/GPU
-	Bridge/Stand	International	Coordinate with OCC/MCC

CAUTION	**All necessary precautions shall be taken by flight crews within the scope of Threat and Error Management (TEM).**

/ 0 / 8.2.2022

Рис. 1.6. Деякі файли містили інструкції з безпеки

Також було викрито персональну інформацію екіпажу. Понад 1,6 мільйона файлів у кошику містять ідентифікаційну інформацію екіпажу . Переважна більшість цих файлів містила наступне:

- Фотографії персоналу
- Підписи

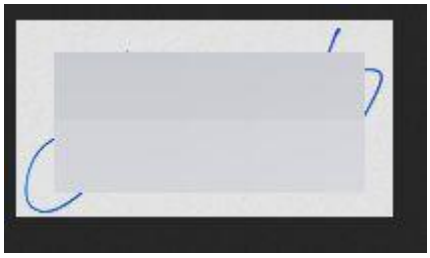


Рис. 1.7. Підпис члена екіпажу

Рис. 1.8. Фото одного члена екіпажу

Вихідний код програмного забезпечення PegasusEFB також було знайдено у відрі. Майже 400 файлів (у форматах .apk, .exe, .dll, .msi та інших) містили звичайні текстові паролі та секретні ключі. Ці файли залишилися доступними, і вони могли дозволити будь-кому видаляти, змінювати або завантажувати дані до додаткових зашифрованих або захищених паролем баз даних, файлів і папок у відрі.

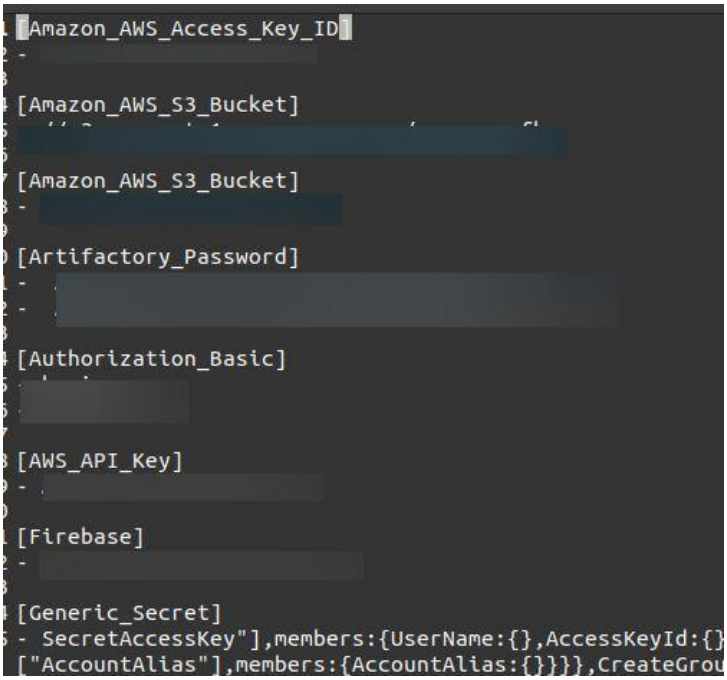


Рис. 1.9. Відра та ключі, зазначені в журналах

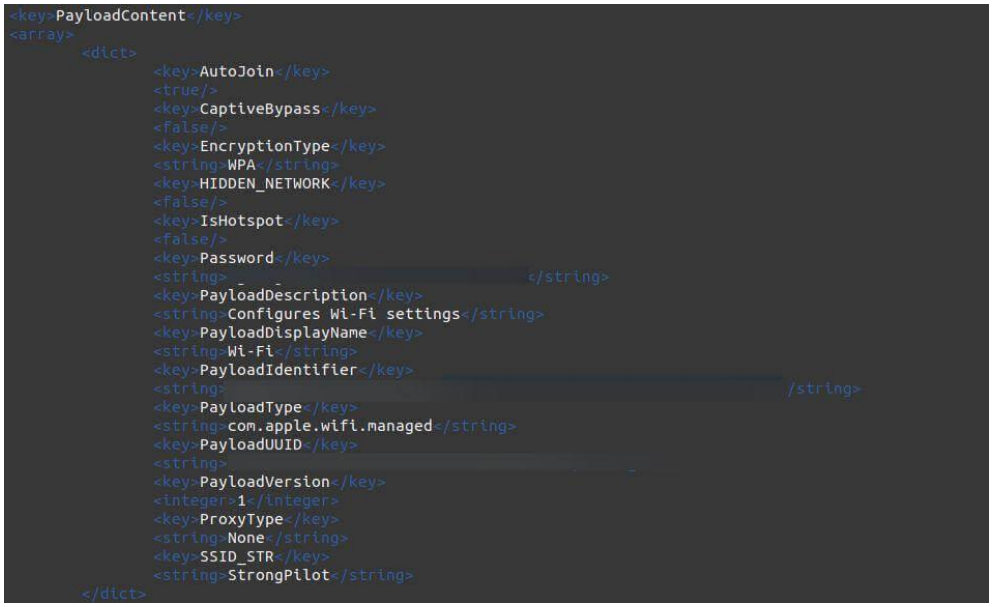


Рис. 1.10. Паролі для приватних підключень WiFi

Тож, підбиваючи підсумки можна зазначити наступне:

Таблиця 1.2

Характеристики інциденту з витоком даних

Кількість відкритих файлів	Майже 23 мільйони файлів
Кількість постраждалих користувачів	Тисячі (екіпаж авіакомпанії)
Розмір пролому	Близько 6,5 ТБ
Розташування компанії	Стамбул, Туреччина

Достовірно невідомо, чи зловмисники отримували доступ до незахищеного сегмента AWS S3 PegasusEFB. Якщо хтось прочитав або завантажив файли корзини, мільйони людей можуть зіткнутися з потенційно катастрофічними загрозами. Зловмисники можуть підробити конфіденційні дані про польоти та надзвичайно конфіденційні файли, використовуючи паролі та секретні ключі, знайдені у відрі PegasusEFB. Хоча ми не можемо бути впевнені, що пілоти використовуватимуть файли сегмента для майбутніх рейсів, зміна вмісту файлів потенційно може заблокувати важливу інформацію EFB від доступу до персоналу авіакомпанії та поставити під загрозу пасажирів і членів екіпажу. З мільйонами файлів, що містять

нещодавні та, можливо, релевантні дані про польоти, на жаль, зловмисник може мати багато варіантів завдати шкоди, якщо знайде відро PegasusEFB. Відкрите відро Пегаса могло сприяти іншим злочинам. Зловмисники можуть підробити конфіденційні дані про польоти та надзвичайно конфіденційні файли за допомогою паролів і секретних ключів, знайдених у відрі PegasusEFB. Більше того, зловмисники можуть використовувати інструкції з безпеки, щоб виявити слабкі місця в безпеці аеропорту чи літака. Співробітники повинні звернутися за допомогою до правоохоронних органів, якщо до них звертаються зловмисники або контактують з ними. PegasusEFB може перевіряти точність важливих документів, тоді як авіакомпанії та аеропорти повинні змінити протоколи безпеки, де це можливо. Щонайменше, відкрите відро PegasusEFB порушило конфіденційність персоналу літака. Зважаючи на це, PegasusEFB, можливо, порушив положення про захист даних Туреччини, Закон про захист персональних даних (LPPD). Таким чином, Управління із захисту персональних даних Туреччини може накласти максимальний штраф у розмірі приблизно 183 000 доларів США [3].

Інсайдерська загроза становить один із найнебезпечніших векторів атак у сфері кібербезпеки через легітимний доступ зловмисника до критичних ресурсів. Вона може мати як навмисний, так і ненавмисний характер і часто пов’язана з людським фактором, помилками конфігурації або умисними діями. Випадок із Pegasus Airlines, де помилка одного співробітника відкрила публічний доступ до 6,5 ТБ конфіденційних даних, чітко демонструє потенційні масштаби шкоди. Інсайдери мають різну мотивацію — від фінансової вигоди до помсти — і можуть діяти самостійно або у змові з третіми сторонами. Найефективніший захист — це впровадження чітких політик доступу, постійний моніторинг аномальної активності та підвищення обізнаності персоналу щодо загроз.

1.2. Методи виявлення та запобігання інсайдерським загрозам

Виявлення та ідентифікація загроз - це процес, за допомогою якого особи, які можуть становити ризик внутрішньої загрози, потрапляють до уваги організації або команди з протидії внутрішнім загрозам, часто в результаті спостережуваної поведінки, що викликає занепокоєння. Оскільки обсяг знань про виявлення та ідентифікацію внутрішніх загроз продовжує зростати, дослідники з Дослідницького центру персоналу і безпеки оборони визначили чотири основні поведінкові принципи, які слід враховувати:

1. Ризик стати інсайдером не розподіляється випадковим чином серед будь-якої групи населення. Певні особи з більшою ймовірністю становитимуть загрозу.
2. Інсайдерські загрози виникають у соціальному контексті. Певні середовище з більшою ймовірністю сприятиме внутрішнім загрозам поведінці інсайдерів.
3. Перетворення особи з інсайдера, якому довіряють, на зловмисника - це процес, а не подія.
4. Низькочастотна поведінка інсайдерської загрози з високим рівнем впливу корелює з загальними показниками і передує їм які можна спостерігати, моделювати та зменшувати.

Дослідження з оцінки ризику цілеспрямованого насильства показало, що більшість кривдників не погрожували своїм жертвам безпосередньо, але демонстрували жертвам безпосередньо, але демонструють поведінку, яку можна ідентифікувати і яка відображає потенційну внутрішню загрозу, що робить виявлення реалістичною та досяжною метою. Виявлення та ідентифікація будуть відрізнятися залежно від вираження та прояву загрози. Наприклад, ненасильницькі прояви внутрішньої загрози в першу чергу виявляються за допомогою технологічних індикаторів, а колеги та сторонні спостерігачі в другу чергу виявляють відповідну поведінку або надають контекст, такий як стресові фактори або схильності, для підтримки оцінки загрози. І навпаки, насильницькі прояви загрози, як правило,

виявляються та ідентифікуються через прямі повідомлення про відповідну поведінку від колег та сторонніх осіб, а технології слугують додатковим засобом виявлення - у вигляді у вигляді ворожих електронних листів або інших повідомлень [4].

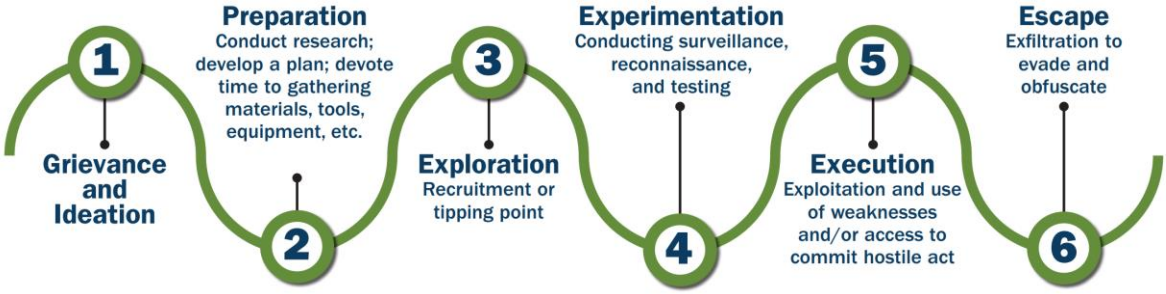


Рис. 1.11. Прогрес інсайдера до зловмисного інциденту

Еволюція внутрішньої загрози до зловмисного інциденту

Хоча практично кожна людина переживає стресові події у своєму житті, переважна більшість з них не вдається до підривних чи деструктивних дій. Щодо тих інсайдерів, які вдаються до зловмисних дій, дослідники встановили, що вони рідко бувають спонтанними; натомість, вони зазвичай є результатом свідомого рішення діяти. Дослідники інсайдерських загроз описують еволюцію від довіреного інсайдера до інсайдерської загрози як критичний шлях, на якому особисті схильності та досвід суб'єкта, що роблять його вразливим до спокуси зловмисних дій, взаємодіють з особистими стресами та організаційним середовищем, рухаючи його вниз по шляху до зловмисного інциденту. Часто зловмисник затає образу, демонструючи поведінку, яку можуть помітити і повідомити про неї колеги та колеги по роботі. Цей шлях може бути швидким або повільним, і в різних людей він проходить по-різному. Попереджувальні знаки, стресові фактори та поведінка можуть бути очевидними на шляху до дії. Глибока образа або приниження, реальне чи уявне, часто є першим кроком на шляху до запланованого насильства. Як показано на рисунку 1.2.1, Просування інсайдера до зловмисного інциденту, сукупність факторів, представлених

нижче, призводить до того, що шлях, який часто можна ідентифікувати через поведінку людини, може бути визначений через її поведінку. Важливо зазначити, що сама лише демонстрація поведінки, яка може становити загрозу для інсайдера, не гарантує, що особа вчинить зловмисну дію. Але як тільки особа починає рухатися цим шляхом, вона з більшою ймовірністю буде діяти. Особливу увагу слід приділяти особам, які можуть бути близькими до відставки, відмежування або звільнення. За особами, які були звільнені з організації чи асоціації без їхньої згоди, слід уважно спостерігати та оцінювати ризик насильства, оскільки їхнє перебування на посаді добігає кінця.

Скарга та ідея (Grievance and Ideation)

Першим кроком на цьому шляху є первинне вираження чийогось страждання або причини для скарги чи обурення - реальна або уявна кривда, яка набуває для людини дуже персоналізованого значення. Або це може бути стресовий фактор, пов'язаний із соціальними, фінансовими чи ідеологічними проблемами. Незалежно від причини, це є відправною точкою, з якої людина починає переходити від ідеї до дії, навмисного вибору порушити довіру організації. З точки зору оцінки загроз, ці скарги можуть перетворитися на поведінку, пов'язану з відчуттям місії, долі, призначення з почуттям місії, долі, втрати або бажання помститися. Незалежно від того, чи є це об'єктивно раціональним, чи ні, важливо те, що інсайдер відчуває бажання діяти, щоб задовольнити свої почуття або відчуття несправедливості, приниження, гніву чи іншого усвідомленого дефіциту. Якщо інсайдер не відмовляє себе від цієї концептуальної потреби, або організація ігнорує ознаки його дистресу чи не реагує адекватно, коли йому стає відомо про них, ці образи чи стреси можуть зростати і розширюватися, підштовхуючи його до зловмисного інциденту [5].

Підготовка (Preparation)

Ідея або образа проявляється в поведінці, коли інсайдер починає обмірковувати, як він хоче реалізувати свій план вчинення інсайдерської або ворожої дії. Поведінка відображає чиїсь переконання, почуття та емоції, що проявляються в діях, які можна

спостерігати. Підготовчі заходи можуть включати дослідження та розробку плану. Особа також може почати купувати предмети, необхідні для здійснення запланованої дії - саботажу, крадіжки, шпигунства або насильства. Для кібератак підготовка може мати форму логічних бомб (наприклад, шкідливого коду), крадіжки паролів, отримання привілеїв або інших технологічних інструментів. Для насильницьких загроз підготовка може включати придбання вогнепальної зброї, боєприпасів, вибухівки або інших засобів ураження. Така поведінка може дати перехожим, колегам, друзям, родичам або іншим особам першу можливість спостерігати за поведінкою, що викликає занепокоєння і може допомогти ідентифікувати особу, яка перебуває на шляху до вчинення злочину. Більшість людей не просуваються далі фази підготовки на цьому шляху до дії. Часто активної фантазії про помсту буває достатньо, щоб задовольнити своє невдоволення. Інші можуть відмовити себе від задуманого вчинку завдяки втручанню з боку особистих мереж підтримки або внаслідок змін у ситуації чи оточенні, які пом'якшують їхні стресові фактори. Їх може стримувати загроза затримання або притягнення до відповідальності, або ж вони знаходять здорові способи виплеснути свої проблеми [5].

Вивчення (Exploration)

До цього етапу підопічна особа може бути безініціативною, вагаючись між дією або мовчазною згодою. Однак на цьому етапі відбувається щось, що змушує підопічну особу почати діяти, що є відправною точкою. Це може бути додатковий стресовий фактор, наприклад, наближення терміну виплати кредиту, брак уваги з боку жертви або зневажлива реакція на її скаргу з боку організації, в якій вона працює. На цьому етапі зловмисник може почати шукати слабкі місця в системі безпеки, знаходити нові точки доступу або вирішувати, які дані він хоче знищити, використати не за призначенням або викрасти. Зловмисник може також намагатися залучити до співпраці інших однодумців, щоб допомогти йому в його діях.

Експеримент (Experimentation)

Спостереження, розвідка, тестування та репетиції плану відкривають небезпечну фазу на шляху до дії. На цьому етапі зловмисники переглядають і вдосконалюють плани. Інсайдер може спробувати розпочати спостереження за певними місцями, проникнути в будівлю або технологічну систему, з'явитися в місцях, які йому не належать, або іншим чином випробувати межі своєї організації. Експериментальна поведінка може тривати протягом тривалого часу, при цьому інсайдери маскують свої наміри і намагаються притупити обізнаність інших або занепокоєння з приводу їхнього зондування або проникнення, тобто дій, спрямованих на обхід системи безпеки для отримання доступу до цілі. Важливо зазначити, що якщо організація виявляє такий тип експериментальної поведінки, дозволяючи інсайдеру продовжувати неприйнятну поведінку без виправлення, наслідків або навіть повідомлення керівництву, може заохотити інсайдера продовжувати неприйнятну поведінку.

Виконання (Execution)

Сформулювавши, спланувавши і відрепетирувавши ворожу атаку або порушення, інсайдер може скористатися своїм доступом і знаннями, щоб реалізувати свій план. Якщо не зупинити інсайдерський інцидент, він може призвести до крадіжки інформації, саботажу обладнання або насильства над колегами чи іншими особами.

Втеча (Escape)

Інсайдерські загрози часто розробляють стратегію втечі перед тим, як здійснити інцидент. Залежно від типу вчиненої дії, втеча може передбачати уникнення виявлення та спотворення доказів злочину, наприклад, перекладання вини, зміну записів, приховування переміщення або зловмисних дій. У разі вчинення насильницьких дій інсайдер може спробувати уникнути затримання та арешту або покінчити життя самогубством - або власною рукою, або через навмисну провокацію озброєних осіб, які надають допомогу. Деякі інсайдерські загрози можуть бути зосереджені на розголосі зловмисних дій шляхом трансляції викрадених даних, інформації або інтелектуальної власності для загального огляду. Дії, що вживаються

на цьому етапі, можуть бути адаптовані до цілого ряду можливих варіацій. Після інциденту інсайдер може діяти самостійно або залучати інших причетних і непричетних осіб, щоб уникнути або перенаправити безпосередні наслідки інциденту. Хоча це потенційно припиняє активну загрозу з боку інсайдера, наслідки його дій часто є значними і можуть тривати протягом тривалого періоду часу. Це може бути особливо актуально, якщо діяння пов'язане з постійною крадіжкою або неправомірним використанням службових даних, поки особа, що викликає занепокоєння, залишається на своєму робочому місці.

Детектори загроз

Люди як сенсори

Співробітники, колеги, друзі, сусіди, члени сім'ї або випадкові спостерігачі - це людський компонент для виявлення та ідентифікації внутрішньої загрози. Вони часто можуть мати уявлення про схильності, стресові фактори та поведінку інсайдерів, які можуть планувати зловмисні дії, а також бути обізнаними про них. Часто ті, хто вчиняє насильство, і ті, хто викрадає дані або секрети, перед тим, як діяти, розповідають про свої плани або скарги іншим. Деякі особи самоідентифікуються. Вони телефонують, пишуть, надсилають електронні листи, підходять до державного службовця чи діяча або виявляють незвичний чи неналежний інтерес до організації. Такі особи часто називають свої імена або надають іншу інформацію, яка дозволяє їх ідентифікувати. Як показано на рисунку 14 нижче, зловмисники часто повідомляють про свої наміри заздалегідь.

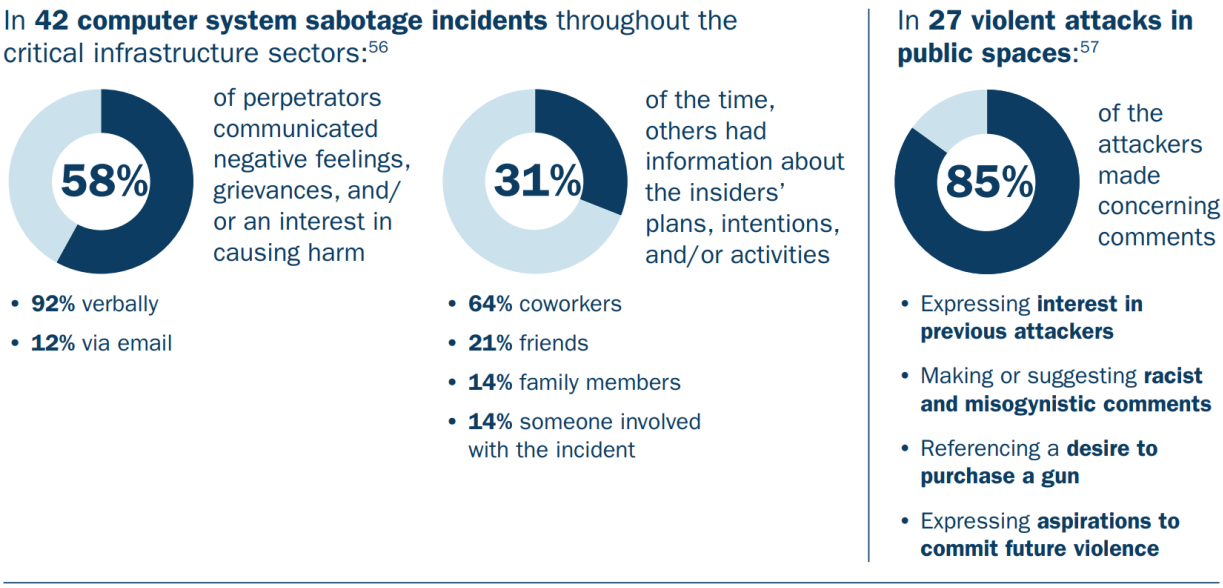


Рис. 1.12. Дослідження Секретної служби США та Національного центру внутрішніх загроз CERT

Програми мінімізації внутрішніх загроз можуть підвищити обізнаність працівників щодо індикаторів, які викликають занепокоєння, та цінності їхніх спостережень у виявленні загроз. Працівників та членів організації слід ознайомити з різними індикаторами загрози, такими як тривожна поведінка та стресові фактори, а також з даними про витоки, щоб допомогти їм зрозуміти, яку роль може відігравати кожна людина у виявленні та ідентифікації тривожних ознак. Наголошуйте на слуханні на більш глибокому рівні, включаючи спостереження за мовою тіла. Контекст є ключовим елементом в оцінці того, чи становить загрозу особа, яка викликає занепокоєння [6].

Дві важливі якості, про які слід пам'ятати, спостерігаючи за поведінкою людини пам'ятати, спостерігаючи за поведінкою людини:

- Слухайте очима. Поведінка та комунікація людини часто розкривається за допомогою невербальних засобів. Звертайте увагу на те, що люди говорять за допомогою виразу обличчя, емоцій та мови тіла.

- Слухайте через систему координат співрозмовника. Люди різні і, швидше за все, не будуть обговорювати свої наміри чи потреби так само, як інші. Поведінка, яку одні люди вважають тривожною чи загрозливою, для інших може бути способом прохання про допомогу.

Існує кілька потенційних варіантів втручання для пом'якшення внутрішньої загрози, але найважливіша дія, яку може зробити особа, – це передати те, що вона знає, спостерігає або боїться, що може статися. Особи, які чують коментарі, погрози, плани, витік або бачать публікації в соціальних мережах, повинні сприймати їх серйозно та належним чином повідомляти керівникам, керівництву організації, вищому менеджеру, відділу кадрів або правоохоронним органам, залежно від обставин.

Моніторинг інсайдерської діяльності

Спеціалізовані технології слід використовувати разом із людськими датчиками для виявлення та запобігання внутрішнім загрозам. Технологічні інструменти виявлення виявляють різноманітні набори даних для виявлення аномалій, таких як записи фізичного чи комп'ютерного доступу, натискання клавіш або клацання мишею або записи спілкування. Ці інструменти можуть допомогти у виявленні аномальної поведінки:

Функції виявлення:

- Забезпечення безперервного моніторингу, який автоматизований і не потребує активного втручання.
- Повідомлення користувачів, коли їхні облікові дані використовуються для входу в систему.
- Порівняння прав доступу користувача з його фактичними діями для виявлення аномальної поведінки.
- Використання прогнозної аналітики для виявлення потенційних порушників.

- Виявлення відхиляючої поведінки, наприклад, активність одного користувача, коли інші неактивні.
- Фіксація, коли і ким отримано доступ до конфіденційних даних.
- Позначення великих завантажень, передавання файлів або інших форм витоку даних.
- Формування портфелів ризику для пріоритезації захисту найбільш важливих або цінних даних.
- Виявлення користувачів, які отримують або змінюють інформацію поза межами своїх повноважень, доступу або потреби.
- Виявлення шкідливого ПЗ або скомпрометованих облікових записів.
- Аналіз ключових слів і психолінгвістичний моніторинг комунікацій.

Інструменти виявлення

- Програмне забезпечення UAM
- Програмне забезпечення UBA
- Система контролю доступу до об'єктів
- Відеоспостереження
- Інструменти веб-моніторингу
- Інструменти SIEM
- Інструменти DLP

Індикатори загрози

Індикатори загрози – це поведінка людини, фактори стресу, схильності та минуле, які можуть вказувати на підвищену ймовірність того, що вона вчинить ворожу чи зловмисну дію. Важливим для цього процесу є розуміння того, що найбільше значення має поведінка, а не мотивація, будь то політична, релігійна, ідеологічна, фінансова чи помста. Хоча мотивація важлива для розуміння того, що рухає злочинцем, саме поведінка та показники особи можуть допомогти позначити особу для додаткового розгляду, моніторингу чи оцінки. Раннє виявлення внутрішньої

загрози залишається складним. Підтвердження будь-якого показника загрози вимагає чіткого розуміння контексту та цілісного уявлення про особу, про яку йдеться. Важливо розуміти, що людина може демонструвати поведінку, характерну для певного періоду її життя, яка може не призводити до прямого вираження загрози. Однак особу, яка демонструє кілька показників, слід позначити повідомлення для додаткового моніторингу або розслідування. Постійна пильність необхідна для своєчасного виявлення індикаторів загрози та реагування на них, а також у відповідному контексті, щоб уможливити втручання для запобігання інциденту. Наступні параграфи представляють репрезентативну вибірку можливих показників; це не все включено.

Персональні показники

Особистісні показники — це комбінація ознак схильності та особистих стресових факторів, що відображають події, що зараз впливають на інсайдера. Індикатори схильності можуть включати психіатричні або медичні розлади, зокрема ті, що впливають на судження та самоконтроль, такі як алкоголізм або компульсивна поведінка, відсутність соціальних навичок, нездатність ладити з іншими, а також порушення правил, злочинна поведінка чи судимості в анамнезі. Інші показники схильності, такі як нарцисизм, історія агресії чи насильства, психопатія або самоушкодження, можуть підвищити ризик ворожості, гніву, насильства або самогубства. Незважаючи на те, що особисті показники можуть вимагати дослідження життя людини, колеги та колеги можуть мати підозри щодо особистого благополуччя інсайдера, що може свідчити про загрозу, що з’являється або продовжується. Через делікатну природу цього типу індикатора загрози важливо бути делікатним і забезпечити дотримання всіх законів про конфіденційність, працю та зайнятість, положення, правила та політики. Ця вимога буде розглянута більш детально пізніше в цьому посібнику. Особисті стресори – це, як правило, ситуації, які викликають напругу в особистому чи професійному житті людини. Слід зазначити, що як негативні, так і позитивні події (наприклад, пониження в посаді чи підвищення по

службі) можуть спричинити напругу чи напругу в особистості. Хоча несподівані події можуть статися з будь-ким у будь-який час, стресори можуть діяти як тригери для людей, які потенційно можуть стати внутрішньою загрозою. Це особливо вірно, коли подія передбачає невиправдані очікування, наприклад невдачу виграти очікувану нагороду чи підвищення.

Фонові індикатори

Фонові індикатори – це події, які відбуваються до того, як особу наймають в організацію або до того, як особа отримує доступ. Зазвичай їх не можуть спостерігати колеги, керівники чи відділ кадрів, але вони визначаються шляхом об'єктивного перегляду історичних записів особи. Ці перевірки є звичайними перед приєднанням особи до організації, особливо якщо інсайдери отримають доступ до конфіденційної інформації чи систем. Важливо зазначити, що особи можуть і будуть приховувати особисту та довідкову інформацію, навіть якщо її розголошення є обов'язковим для їх зв'язку або роботи в організації. Для отримання інформації, необхідної для виявлення потенційної внутрішньої загрози, може знадобитися поглиблена перевірка. Організації не повинні уникати всебічної підготовки перевірки на страх сприйняття, правові проблеми чи проблеми профспілки, особливо ті, які включають перегляд записів про психічне здоров'я відповідної особи або публічних профілів у соціальних мережах. Дані, зібрані під час цих перевірок, можуть дати зрозуміти, який тип загрози може висловити інсайдер, а також потенційні контрзаходи, які слід застосувати, якщо така загроза все-таки виявиться. Організаціям настійно рекомендується залучати юридичних консультантів, коли запитують довідкові записи, щоб забезпечити дотримання конфіденційності.

Поведінкові показники

Поведінка особи відображає моделі нормальної або доброякісної діяльності, засновані на тому, як інсайдер взаємодіє всередині організації або в її мережі. З часом така поведінка створює базову лінію діяльності, зміни якої можна вважати індикатором загрози. На відміну від особистого і фонові показники, які зазвичай

вимагають перевірки життя особи, що стосується, поведінкові показники безпосередньо спостерігаються колегами, персоналом відділу кадрів, керівниками та технологіями.

Технічні індикатори

Технічні індикатори – це ті, які вимагають безпосереднього застосування IT-систем та інструментів для виявлення. Ці індикатори включають діяльність у мережі та хості, наприклад дії на комп'ютері, терміналі або стаціонарному/мобільному пристрої, а також інциденти, що відбуваються в основній IT-інфраструктурі організації. Одним із найбільш часто використовуваних додатків для виявлення індикаторів внутрішньої загрози є UAM, можливість, яка використовується аналітиками для спостереження за поведінкою людини в IT-сфері. Більшість інцидентів з інсайдерськими загрозами вимагають невеликої технічної складності для виконання. Дослідження в банківському та фінансовому секторі показали, що більшість атак не були ані складними, ані вимагали особливих технологічних навичок і були скоєні особами, які не працювали в IT-сфері та не мали великого досвіду в технологіях. Натомість ці особи використовували вразливі місця в системах і процесах для вчинення крадіжки. Ці приклади призначені для представлення загальної структури індикаторів потенційної внутрішньої загрози. Наведені нижче приклади не є остаточним списком. Натомість вони забезпечують загальну структуру індикаторів потенційної внутрішньої загрози та відправної точки для організації для визначення індикаторів загрози, які відповідають її конкретним унікальним характеристикам і проблемам.

Приклади технічних індикаторів

- Пряме листування з конкурентами;
- Повідомлення електронної пошти з надто великими вкладеннями або обсягом даних;
- Запити системи доменних імен (DNS), пов'язані з діяльністю Dark Web;

- Використання інструментів маскування активності (наприклад, віртуальних приватних мереж [VPN] або Onion Router [Tor]);
- Виконання наступальних засобів;
- Запуск шкідливих програм;
- Підключення неавторизованого пристрою до мережі;
- Завантаження або встановлення забороненого програмного забезпечення;
- Несподівана діяльність поза звичайним робочим часом;
- Спроби обійти або вимкнути інструменти захисту від зловмисного програмного забезпечення або елементи керування безпекою;
- Несанкціоновані спроби підвищити дозволи або привілеї, особливо без необхідності знати;
- Спроба надрукувати або скопіювати захищені або обмежені документи;
- Надмірно велика кількість помилок програмного забезпечення або операційної системи;
- Підключення невідомого пристрою до робочої станції (USB, зовнішній жорсткий диск);
- Збереження доступу до конфіденційних даних після повідомлення про розірвання;
- Різні користувачі намагаються увійти з однієї робочої станції чи пристрою;
- Відсутність повідомлень журналу або даних моніторингу;
- Несанкціонована зміна файлів, що зберігаються в централізованому файлі;
- Копіювання великої кількості документів на локальний диск;
- Помилки автентифікації або невдалі спроби входу;
- Несанкціоновані зміни конфігураційного файлу або зміни дозволів;
- Несанкціоновані зміни вмісту бази даних;
- Безвідповідальні звички в соціальних мережах;

- Інсайдер намагається отримати доступ до ресурсів, не пов’язаних зі звичайною роллю цього інсайдера;
- Обліковий запис користувача, який використовується з кількох пристроїв;
- Для одного користувача визначено кілька облікових записів;
- Запуск ключових слів або фраз в електронних листах, текстових повідомленнях або телефонних дзвінках.

Інститут розробки програмного забезпечення (SEI) при Університеті Карнегі-Меллона надає додаткові докази на підтримку концепції людського та технічного моніторингу. На основі свого обширного дослідження внутрішньої загрози SEI розробив 10 найбільш часто спостережуваних потенційних кіберіндикаторів внутрішньої загрози:

- Відсутність засобів контролю для запобігання неавторизованій модифікації важливих даних
- «Невдоволений» працівник
- Використання надмірних привілеїв доступу
- Зламані паролі
- Електронна пошта/чат із зовнішніми конкурентами/змовниками
- Збій захисту критичних файлів
- Порушення політики необхідності знати
- Несанкціоноване завантаження даних до/з дому
- Несанкціонований експорт даних
- Можливість користувачів з правами системного адміністратора саботувати системи або дані

Співробітники або члени організації, як правило, становлять більший ризик внутрішньої загрози, якщо їх звільнили, виключили або отримали нову посаду. У цих випадках інсайдери, як правило, викрадають інформацію, з якою вони працюють або з якою стикаються найчастіше. Деякі вважають, що вони мають право на цю

інформацію і що вона належить їм, а не організації. У цих випадках, які стосуються інформації та даних, з якими інсайдер має частий контакт, попереджувальні ознаки крадіжки можуть бути не такими помітними. Деякі працівники можуть бути найняті конкуруючими корпораціями чи національними державами та можуть вступати в змову з колегами, які також почуваються позбавленими прав або ображеними. Цей тип взаємодії може ускладнити виявлення крадіжки чи саботажу, особливо якщо співпраця відбувається з користувачами, які є наглядачами або мають права адміністратора в системах, що містять інформацію. Крім того, інсайдери, які є керівниками, наглядачами чи адміністраторами, можуть увімкнути та навіть приховати індикатори внутрішньої загрози, змінюючи інформацію, яка відстежує та реєструє переміщення користувачів, що означає, що ідентифікація винуватця крадіжки чи саботажу може зайняти ще більше часу [7].

Успішна стратегія управління загрозами

Щоб оптимізувати можливості для досягнення успіху, стратегії управління загрозами повинні досягти ретельного балансу між захистом організації та турботою про особу, про яку йдеться. Навіть при пильній увазі стратегії все одно можуть зазнати невдачі, а деякі можуть навіть погіршити ситуацію. Успішна стратегія управління загрозами може зменшити ризик, спричинений особою, про яку йдеться, запобігти внутрішньому інциденту та захистити організацію та її працівників. Якщо початкові стратегії зазнають невдачі, організації повинні продовжувати шукати правильний варіант, який дозволить запобігти внутрішньому інциденту та знизити ризики для організації, навіть якщо відповідну особу було вилучено з організації. У цьому прикладі роботодавець дотримувався визначеного процесу управління загрозами після визначення особи, яка викликає занепокоєння, і оцінки цих проблем як потенційної загрози для організації. У міру розвитку загрози організація коригувала свій підхід, посилюючи втручання, дотримуючись чинних законів, правил і норм. Коли можливості організації були перевищені, організація залучила стороннього органу, щоб допомогти їм продовжувати оцінювати загрозу та керувати нею.

Таблиця 1.3.

Профіль інсайдера та індикатори ризикової поведінки

Інсайдер	**Індикатори**
37-річний автоматник Технік і фахівець з безпеки та контролю на нафтопереробному заводі на півдні США, який відповідав за технічне обслуговування та ремонт усіх пневматичних, електронних, комп'ютерних засобів керування процесами та кріогенних онлайн-систем заводу.	Розслідування та подальша оцінка виявили технік мав: • Схильність до насильства • Словесно ображав і залякував своїх колег і керівника • Неодноразово піддавався сексуальним домаганням і переслідував жінку-колегу • Вчинив фізичний розтин зі своїм керівником • Словесно та фізично знущався над своєю невиліковно хворою дружиною

Стратегія почтакового втручання

На підставі їх початкової оцінки організація застосувала до техніка прогресивну дисциплінарну відповідальність, написала попередження про незадовільне виконання роботи та відсторонила його від роботи на чотири дні. Крім того, організація доручила йому розробити план під час його відсторонення, щоб покращити свою продуктивність і змінити поведінку, викладену в його звіті про результати. На жаль, ця початкова стратегія не мала видимого ефекту, оскільки його продуктивність не покращилася, а після його повернення на роботу виникли додаткові проблеми.

Друга стратегія втручання

Технік став більш войовничим, порушував накази та відмовлявся покращувати стан безпеки, що збільшувало ризик нещасного випадку для організації та її персоналу. Організація вирішила видати останнє письмове попередження про

незадовільну роботу та відсторонити його без збереження заробітної плати на один тиждень. Крім того, вони наказали йому утримуватися від будь-яких контактів із персоналом заводу чи робочою діяльністю та попередили його, що будь-які подальші проблеми призведуть до негайного звільнення. Незважаючи на ці два управлінські втручання, занепокоєна поведінка людини загострилася. Під час відсторонення він став більш загрозливим і небезпечним для безпеки організації та своїх колег. Протягом цього часу, перебуваючи на вечірці з колегами, він, як повідомляється, використав штурмову гвинтівку, щоб вистрілити в опудало свого керівника. Коли працівники, які займалися його посадою, попросили пароль до автоматизованої системи безпеки заводу, він відмовився його надати. Що ще гірше, він двічі намагався віддалено маніпулювати системами безпеки, щоб створити кризу, яку, як він припускав, його керівник не зможе виправити без його допомоги. На щастя, ці спроби диверсії йому не вдалися. Погрозлива поведінка техніка, його відмова надати пароль для систем контролю безпеки та його спроби саботувати механізми контролю безпеки заводу змусили його організацію побоюватися його звільнення через страх насильницької помсти. Поки технік був відсторонений, служби безпеки, кадри та операційні підрозділи компанії провели спільне розслідування його поведінки та її впливу на членів команди та продуктивність підприємства. Ця перевірка включала консультацію із зовнішнім спеціалістом із безпеки/психічного здоров’я, кваліфікованим у сфері ризику внутрішньої загрози; спроба допомогти групі управління загрозами оцінити та керувати загрозою, що розвивається та, очевидно, нерозв’язною.

Третя стратегія втручання

Після ретельної оцінки ситуації, що розвивається, організація розробила третю стратегію управління. Цей новий підхід спрямований на те, щоб вирішити проблеми та скарги людини, а також допомогти йому впоратися зі своїм гнівом і поведінкою, що викликає занепокоєння. Стратегія передбачала отримання медичної допомоги для техніка та його хворої дружини (яка була в термінальній стадії раку та була активним

суїцидалом), відправлення його в оплачувану відпустку, продовження зусиль щодо його реабілітації через Програму допомоги працівникам, постійне лікування та оцінку, а також моніторинг третьої сторони. Через деякий час організація вирішила, що звільнення техніка є необхідним, але на той час вони розглянули проблеми особи та були впевнені, що звільнення може відбутися без ризику насильства. Крім того, примітно, що організація не закрила справу щодо внутрішньої погрози щодо цієї особи. Натомість команда управління загрозами продовжувала моніторинг, а організація продовжувала надавати допомогу, доки клінічний психолог не вирішив, що колишній технік більше не становить загрози для організації [7].

Вплив успішної стратегії

Організація вважає заслугою своїх постійних зусиль із застосування ефективної стратегії втручання для запобігання акту саботажу чи насильства, які могло спровокувати раптове припинення роботи.

Типи засобів виявлення інсайдерів

Інструменти виявлення внутрішніх загроз виявляють зловмисну поведінку та дії в організації. Вони шукають загальні індикатори внутрішньої загрози, як-от незвичайний час входу чи передачі файлів, і виявляють підозрілі дії, які можуть свідчити про спроби крадіжки або розгортання зловмисного програмного забезпечення. Деякі інструменти сповіщають команди кібербезпеки в режимі реального часу, а інші можуть автоматично вживати заходів до ескалації загроз.

SIEM — Рішення для керування інформацією та подіями безпеки (SIEM) збирають дані журналів із пристроїв і мереж у IT-середовищі організації. Якщо правильно налаштувати платформу SIEM, вона може сповіщати команди безпеки про дії пристроїв і користувачів, які можуть свідчити про наявність внутрішньої загрози, як-от викрадання конфіденційних даних або раптові надмірні дозволи для непривілейованих користувачів. Недоліком рішень SIEM є те, що вони можуть створювати надмірну кількість помилкових спрацьовувань. SIEM часто плутають нормальну поведінку користувача зі зловмисною діяльністю.

EDR — Рішення для виявлення та реагування на кінцеві точки (EDR) збирають дані з кінцевих точок, аналізують їх і автоматично вживають заздалегідь визначених дій. EDR корисні для запобігання внутрішнім загрозам, оскільки вони можуть виявляти незвичне використання облікових даних користувача в мережі. Наприклад, рішення EDR може виявляти інциденти, коли доступ до облікових записів користувачів здійснюється зі сторонніх IP-адрес, а потім вживати заходів для припинення з'єднань. Щоб розгорнути EDR як інструмент пом'якшення внутрішніх загроз, його потрібно ретельно налаштувати, щоб оцінювати та сортувати незвичайну поведінку, не викликаючи збоїв.

Інструменти керування журналами — Інструменти керування журналами збирають журнали використання пристрою з кінцевих точок і програм, таких як облікові записи користувачів, сервери та принтери. Команди безпеки можуть налаштувати інструменти керування журналами для надсилання сповіщень електронною поштою, коли відбувається певна дія, як-от використання принтера для друку конфіденційного документа. Інструменти керування журналюванням можуть допомогти у реагуванні на інциденти та криміналістичному розслідуванні внутрішніх загроз.

UEBA — Аналітика поведінки користувачів і об'єктів (UEBA), — це рішення для моніторингу, які використовують штучний інтелект і машинне навчання для виявлення та припинення поведінки користувачів і пристроїв, які можуть сигналізувати про внутрішню атаку. Наприклад, інструмент UEBA може виявити та відключити користувача, який зазвичай завантажує лише кілька мегабайт даних протягом звичайного робочого дня, але раптово завантажує кілька гігабайт.

ITM — Програмне забезпечення Insider Threat Management (ITM) — це тип рішення безпеки, що продається явно як спосіб для компаній керувати внутрішніми загрозами. Функціональність рішення ITM буде відрізнятися залежно від того, який постачальник його пропонує. Рішення ITM часто використовують ті самі можливості,

що й у рішеннях SIEM, EDR або UEBA, але мають спеціальну інформаційну панель внутрішніх загроз [8].

Автоматизація безпеки — Автоматизація безпеки – це технологія, яка дозволяє групам безпеки автоматизувати рутинні елементи збору, аналізу та реагування на дані безпеки. Автоматизація безпеки є потужним методом раннього виявлення та припинення ланцюжків атак інсайдерської загрози. Такі технології, як XDR, SOAR і автономний кіберзахист, використовують автоматизацію безпеки, щоб знаходити й реагувати на потенційну внутрішню загрозу набагато швидше й ефективніше, ніж це можливо за допомогою ручного аналізу чи попередньо визначених правил. Автоматизація безпеки також може зменшити кількість хибних спрацьовуючих сповіщень , які створюють заходи із запобігання внутрішнім загрозам.

1.3. Аналіз та порівняння сучасних систем UAM для боротьби з інсайдерськими загрозами

Моніторинг активності користувачів (UAM) відстежує та аналізує дії користувачів у мережах, системах або програмах. Це в основному для підвищення безпеки, забезпечення відповідності та підвищення продуктивності. Спостерігаючи за діяльністю користувачів, підприємства можуть помічати незвичну поведінку, зменшувати загрози безпеці та підтримувати ефективність. Системи моніторингу активності користувачів використовують різні технології для збору та аналізу даних про дії користувачів. Вони записують детальну взаємодію з цифровими активами. Потім вони обробляють ці дані, щоб запропонувати розуміння. Ця інформація допомагає організаціям зрозуміти моделі поведінки, виявляти аномалії та застосовувати політики безпеки.

Ключові компоненти систем моніторингу активності користувачів

- Механізми збору даних: вони включають програмні агенти, встановлені на кінцевих точках, інструменти аналізу мережевого трафіку та журнали серверів. Вони

фіксують детальні дані про дії користувача, такі як натискання клавіш, рухи миші, використання програм тощо.

- Зберігання та керування даними: зібрані дані надійно зберігаються в базах даних, де ними можна керувати, отримувати та аналізувати. Ефективні рішення для зберігання даних забезпечують цілісність і доступність даних.
- Інструменти аналітики та звітності: ці інструменти обробляють зібрані дані для виявлення закономірностей і створення звітів. Розширена аналітика може виділити відхилення від нормальної поведінки, вказуючи на потенційні інциденти безпеки.
- Системи оповіщення та сповіщень: рішення UAM часто включають механізми сповіщень у реальному часі для сповіщення адміністраторів про підозрілу діяльність. Ці сповіщення можуть ініціювати автоматичні реакції для зменшення ризиків.

Типи зібраних даних

- Системи моніторингу активності користувачів збирають різні типи даних, кожна з яких служить певній меті для розуміння та захисту дій користувачів. Основні типи зібраних даних включають:
- Час входу: Запис, коли користувачі входять і виходять із систем, допомагає виявити незвичайні шаблони доступу та потенційні порушення безпеки.
- Відвідування веб-сайтів: відстеження веб-сайтів, до яких звертаються користувачі, дає змогу зрозуміти поведінку веб-переглядача та може запобігти доступу до шкідливих або не пов’язаних із роботою сайтів.
- Використання програм: відстеження того, які програми використовуються та як довго, може допомогти в оцінці продуктивності та виявленні неавторизованого використання програмного забезпечення.
- Доступ до файлів і їх модифікація: операції з записом файлів (наприклад, створення, видалення, модифікація) допомагають запобігти втраті даних і забезпечують цілісність даних.

Методи збору даних

Моніторинг активності користувачів використовує різні методи для ефективного збору даних:

- Програмні агенти: вони встановлюються на кінцевих точках (наприклад, настільних ПК, ноутбуках) і постійно збирають детальні дані про діяльність користувачів. Вони діють на системному рівні, забезпечуючи комплексний моніторинг.
- Аналіз мережевого трафіку: Аналізуючи мережеві пакети, системи UAM можуть контролювати дані, що проходять через мережу, ідентифікувати дії користувачів і виявляти аномалії, не покладаючись на встановлення кінцевих точок.
- Журнали сервера: журнали, створені серверами, містять велику кількість інформації про дії користувачів. Ці журнали можна аналізувати, щоб відстежувати дії користувачів, виявляти неавторизований доступ і гарантувати відповідність політикам безпеки.

Переваги моніторингу активності користувачів

1. Підвищення безпеки

Моніторинг активності користувачів (UAM) є життєво важливим для безпеки організації. Він відстежує дії користувачів, щоб негайно виявити несанкціонований доступ і порушення безпеки. Наприклад, якщо співробітник намагається отримати доступ до обмежених файлів, UAM сповіщає IT-групу. Це дозволяє їм діяти швидко та зменшувати ризики. Крім того, системи UAM виявляють незвичну поведінку, яка може сигналізувати про зламаний обліковий запис або внутрішню загрозу. Це допомагає запобігти витоку даних і захистити конфіденційну інформацію.

2. Підвищення продуктивності

Моніторинг активності користувачів (UAM) підвищує безпеку та продуктивність. Він відстежує продуктивність співробітників, показуючи, як використовуються час і ресурси. Це допомагає знайти проблеми робочого процесу. Потім менеджери можуть виправити це, щоб підвищити продуктивність. Наприклад,

якщо завдання затягується, вони можуть запропонувати додаткове навчання або ресурси. Це робить роботу більш ефективною. Отже, UAM допомагає організаціям працювати краще.

3. Відповідність та аудит

Моніторинг активності користувачів є життєво важливим для відповідності та аудитів. У багатьох секторах діють суворі правила. Ці правила часто вимагають відстеження дій користувачів, щоб відповідати стандартам безпеки та конфіденційності. Моніторинг активності користувачів (UAM) пропонує докладні записи, важливі для перевірок або розслідувань. Це допомагає організаціям дотримуватись таких законів, як GDPR, HIPAA або PCI-DSS. Це дозволяє уникнути штрафів або юридичних проблем. Крім того, ці записи є ключовими в суперечках або судових справах, пропонуючи чіткий звіт про дії користувачів.

Види моніторингу активності користувачів

1. Моніторинг співробітників проти моніторингу клієнтів

Моніторинг співробітників: це практика спостереження за працівниками на роботі. Його головні цілі — забезпечення продуктивності, безпеки та дотримання політики. Методи включають відстеження використання комп’ютера, моніторинг електронної пошти та використання відеоспостереження.

Мета полягає в тому, щоб виявити такі ризики, як витік даних або внутрішні загрози, і підвищити ефективність. Однак для підтримки позитивної робочої атмосфери важливо збалансувати моніторинг із правами на конфіденційність.

Моніторинг клієнтів: Моніторинг клієнтів зосереджується на аналізі поведінки клієнтів, щоб покращити надання послуг і задовольнити їх. Це передбачає відстеження взаємодії на веб-сайтах, у мобільних додатках та інших цифрових платформах, зокрема моделі веб-перегляду, поведінку кліків та історію покупок. Статистика цих заходів допомагає компаніям персоналізувати пропозиції, оптимізувати взаємодію з користувачами та підвищити утримання клієнтів. Етичні

міркування мають вирішальне значення для забезпечення конфіденційності даних і дотримання таких нормативних актів, як GDPR і CCPA [9].

2. Моніторинг у реальному часі проти історичного моніторингу

Моніторинг у реальному часі: цей метод постійно відстежує та записує дії користувачів. Він пропонує негайну інформацію та швидку відповідь на загрози. Наприклад, на робочому місці він попереджає IT-персонал про підозрілі входи або неавторизований доступ до файлів, що дозволяє швидко вжити заходів.
Подібним чином у моніторингу клієнтів він покращує досвід, надаючи миттєву підтримку або персоналізовані рекомендації на основі поточної поведінки.

Історичний моніторинг: цей процес збирає та аналізує дані з часом, щоб виявити тенденції. Це ключ до перевірок, розуміння поведінки та прийняття рішень. Наприклад, перегляд даних минулих працівників може виявити проблеми або загрози продуктивності. Подібним чином аналіз даних про клієнтів виявляє моделі купівлі та рівень залучення. Це розуміння допомагає у стратегічному плануванні та маркетингу. Популярні інструменти та програмне забезпечення для моніторингу активності користувачів Інструменти моніторингу активності користувачів (UAM) життєво важливі для бізнесу. Вони підвищують продуктивність, забезпечують відповідність і захищають конфіденційні дані. Деякі рішення UAM виділяються своїми функціями та простотою використання. У цьому розділі розглядаються найпопулярніші рішення UAM, порівнюються їхні функції та детально описується ціна та ліцензування.

3. Пасивний моніторинг проти активного

Пасивний моніторинг: цей метод спостерігає за користувачами без прямої взаємодії. Він тихо збирає дані, зводячи до мінімуму збої та залишаючи користувачів непомітними. Цей підхід ідеально підходить для автентичних даних. На робочих місцях він може відстежувати використання Інтернету або програмного забезпечення, не повідомляючи співробітників. Для клієнтів це передбачає аналіз використання веб-сайту чи додатка, щоб покращити їхній досвід.

Активний моніторинг: цей метод передбачає безпосередню взаємодію з користувачами або системами для збору даних або ініціювання дій. Це включає надсилання сповіщень, перевірку в режимі реального часу або запит на підтвердження користувача. Під час моніторингу співробітників це може включати реєстрацію натискань клавіш або надсилання сповіщень про порушення політики. Для клієнтів це може означати використання опитувань, форм зворотного зв'язку або підтримки в чаті. Хоча це більш нав'язливий процес, активний моніторинг пропонує детальну інформацію та швидкі реакції на конкретну поведінку.

Огляд провідних рішень

Hubstaff — популярний інструмент UAM, відомий своєю простотою та надійною функціональністю. Він пропонує відстеження робочого часу, моніторинг співробітників і аналіз продуктивності. Hubstaff широко використовується віддаленими командами та підприємствами, які прагнуть оптимізувати роботу та підвищити ефективність.

Teramind — це комплексне рішення UAM, розроблене для підприємств, яким потрібен детальний моніторинг і розширена аналітика. Він забезпечує відстеження активності користувачів у реальному часі, аналіз поведінки та запобігання втраті даних (DLP). Teramind ідеально підходить для організацій із суворими вимогами до безпеки та тих, хто потребує глибокого розуміння поведінки користувачів.

ActivTrak — це хмарний інструмент UAM, який зосереджується на моніторингу продуктивності та аналітиці робочої сили. Це допомагає компаніям зрозуміти, як співробітники витрачають свій час, і визначити сфери, які потрібно вдосконалити. Зручний інтерфейс і потужна аналітика ActivTrak роблять його улюбленим серед малих і середніх підприємств.

Syteca — це комплексне рішення для моніторингу, яке фіксує активність користувачів, дозволяє відтворювати сесії у вигляді відео та аналізувати ризиковану поведінку. Система відстежує дії як кінцевих користувачів, так і адміністраторів, забезпечуючи високий рівень прозорості та контроль над доступом до критичних

ресурсів. Syteca підтримує інтеграцію з існуючими системами кібербезпеки, зокрема DLP і SIEM, що робить її гнучким і масштабованим інструментом для великих підприємств і організацій з підвищеними вимогами до захисту інформації. Ключові функції: запис сесій користувачів із детальними метаданими, моніторинг у реальному часі з можливістю втручання, налаштування правил доступу за ролями, автоматичне формування звітів і журналів активності, підтримка сценаріїв інцидент-менеджменту, ціна та ліцензування. Ліцензія Syteca надається відповідно до кількості користувачів або серверів, що підлягають контролю. Доступні різні конфігурації — від базового моніторингу до розширених корпоративних рішень із повною інтеграцією в інфраструктуру безпеки підприємства.

Порівняння провідних рішень у сфері UAM продемонструвало, що сучасні системи значно розрізняються за функціональністю, підходами до моніторингу та гнучкістю налаштувань. Критеріями для оцінки стали: рівень деталізації даних, інтеграційні можливості, ефективність виявлення аномалій та підтримка політик безпеки. Обрана система — Syteca — відповідає всім цим вимогам і забезпечує високий рівень контролю над активністю як кінцевих користувачів, так і адміністраторів. Її функціональність, зокрема можливість запису сесій, аналітика ризикованої поведінки та підтримка сценаріїв реагування, забезпечує комплексний підхід до боротьби з інсайдерськими загрозами. Окрім технічних характеристик, важливу роль відіграла також локалізація продукту та його відповідність українським реаліям — це дозволяє ефективно впроваджувати систему без необхідності суттєвих адаптацій. Syteca — це не лише засіб контролю, а й інструмент забезпечення цифрової довіри в організації [10].

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ UAM SYTECA

2.1. Архітектура та функціональні можливості UAM Syteca

Клієнти Syteca допомагають запобігати, виявляти та знищувати внутрішні загрози на будь-якому типі настільних комп'ютерів і серверів: серверах інфраструктури, серверах терміналів, серверах Jump, фізичних і віртуальних настільних комп'ютерах. Найповніший набір підтримуваних платформ: Windows, Linux, macOS, X Window System, фізичні та віртуальні робочі столи. Citrix і VMware. Клієнт знімає екрани користувачів за допомогою рухів миші відповідно до налаштувань запису та одночасно записує важливі метадані, такі як назви програм, заголовки активних вікон, натискання клавіш тощо. Контрольовані дані надсилаються на сервер програм Syteca для зберігання та аналізу або, якщо немає підключення до мережі, зберігаються в захищеному кеші клієнта, доки з'єднання не буде відновлено. Ви можете налаштувати клієнт залежно від того, наскільки інтенсивним має бути моніторинг безпеки, аж до створення знімків екрана щосекунди або на основі кожного клацання миші чи натискання клавіші. Ви можете ввімкнути спеціальний Захищений режим, щоб забезпечити безпеку роботи Клієнта та цілісність відстежуваних даних. Syteca дозволяє легко розгортати рішення, надаючи можливості віддаленого встановлення клієнта.

Клієнти Syteca надсилають відстежувані дані на сервер прикладних програм Syteca, який аналізує дані та зберігає їх у центральній базі даних. Якщо відстежувані дані містять події, які відповідають правилам, визначеним користувачем, Сервер генерує миттєві сповіщення та за потреби ініціює автоматичне реагування на інцидент. Сервер також відповідає за зберігання конфігураційних даних, надсилання пакетів оновлень клієнтам, виконання очищення бази даних і створення звітів і

відповідної статистики. Syteca Application Server може додатково працювати зі сторонніми базами даних MS SQL або PostgreSQL, забезпечуючи гнучкий вибір залежно від ваших потреб у безпеці, економічності та швидкості обробки.

Інструмент керування є основним інтерфейсом користувача Syteca. Це дозволяє керувати клієнтами, налаштовувати сповіщення системи безпеки щодо потенційних інцидентів, визначати та призначати дозволи користувачам Syteca, керувати доступом до кінцевих точок, а також переглядати й аналізувати відстежувані дані безпеки, отримані від клієнтів.

Комбінуючи різні типи клієнтів Syteca, захищається та підвищується видимість кожної частини конкретної IT-інфраструктури. Для великих розгортань команда Syteca забезпечує високу доступність і аварійне відновлення для покращення стабільності системи та мультитенантний режим для задоволення вимог сегментації та ізоляції даних.

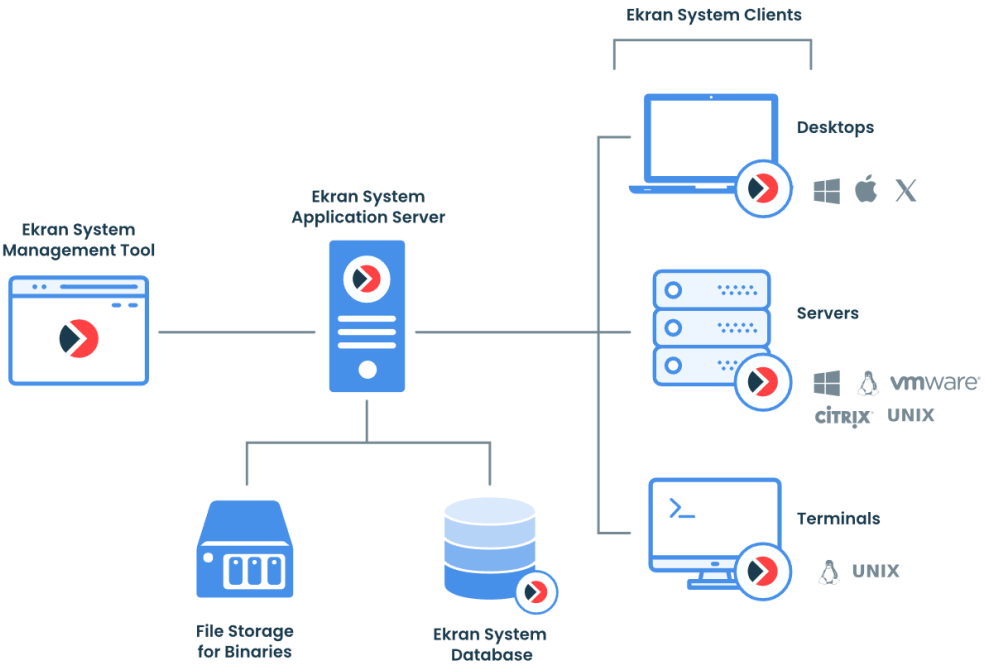


Рис. 2.1. Базова схема розгортання

Завдяки розгортанню типу рис. 2.1. можна досянути максимальної видимості та контролю будь-якої діяльності, що виконується в інфраструктурі, встановивши клієнт відповідного типу на кожну кінцеву точку.

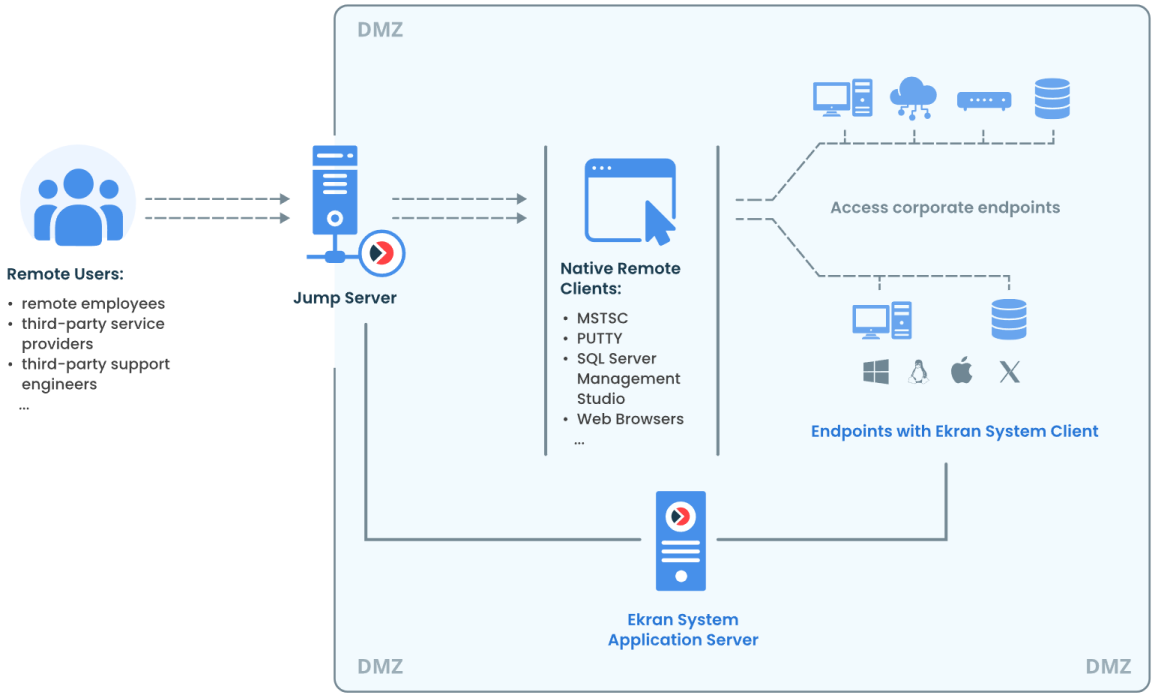


Рис. 2.2. Розгортання сервера Jump

Як показано на рис. 2.2. можна встановити лише один клієнт термінального сервера Syteca на сервер переходу, щоб відстежувати всі сеанси, які проходять через нього, і, якщо необхідно, керувати доступом до кінцевих точок у межах захищеного периметра за допомогою набору інструментів Syteca PAM.

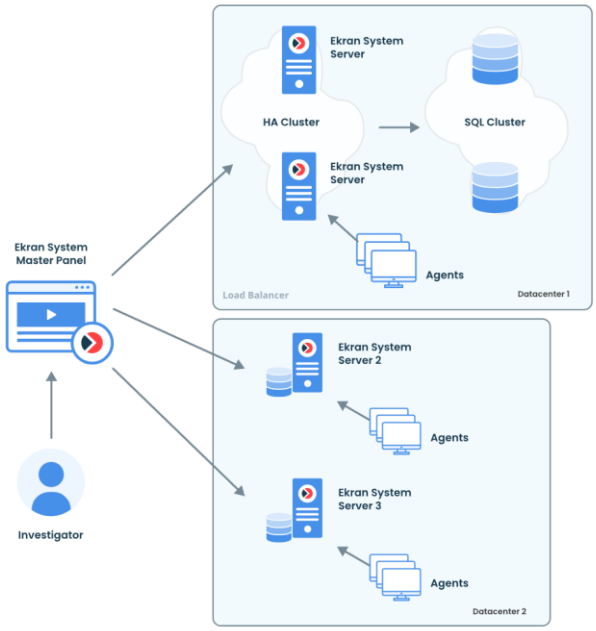


Рис. 2.3. Масштаб для зростання за допомогою панелі Master

У наші дні співробітники служби безпеки організацій, які мають центри обробки даних, розподілені в різних географічних місцях, стикаються з багатьма проблемами, керуючи ризиками внутрішніх загроз. Головна панель — це компонент Syteca, який використовується для перегляду сеансів усіх клієнтів організації. Цей компонент об'єднує дані з усіх ізольованих серверів програм Syteca або розгортань в єдиний інтерфейс користувача.

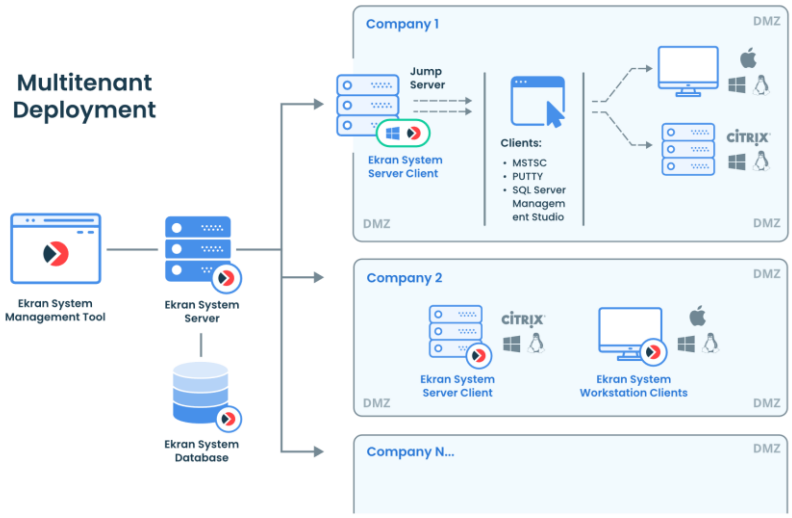


Рис. 2.4. Багатокористувацький режим

Багатокористувацький режим був розроблений для професійних сервісних компаній, які керують безпекою своїх клієнтів, а також для великих організацій із географічно розділеними офісами та незалежними відділами. Цей режим розгортання дозволяє кільком незалежним клієнтам працювати в середовищі Syteca. Дані кожного орендаря, включаючи відстежувані дані, облікові дані користувача, імена клієнтів, конфігурацію системи тощо, є повністю незалежними та недоступними для інших орендарів [11].

2.2. Основні компоненти системи та їх призначення

Основні компоненти системи

Система включає наступні основні програмні компоненти:

- NOT AVAILABLE IN SAAS Syteca Application Server: Це основний компонент Syteca, який отримує дані моніторингу (знімки екрану та пов'язані з ними метадані) від Клієнтів Syteca, аналізує дані (і генерує сповіщення про потенційні інциденти безпеки) та зберігає їх у центральній базі даних (з підтримкою сторонніх баз даних MS SQL або PostgreSQL). Сервер додатків також відповідає за зберігання даних конфігурації, надсилання пакетів оновлень клієнтам, очищення бази даних, створення звітів і відповідної статистики. Робота Сервера додатків може бути запущена або зупинена за допомогою іконки Syteca Server в треї, яка також включає в себе додаток Параметри бази даних (DbSetupToolUI), за допомогою якого можна перевипустити або перемістити Майстер-сертифікат Syteca, змінити параметри бази даних і т.д.

Syteca Management Tool: Це центральна адміністративна консоль зі зручним веб-інтерфейсом, яка дозволяє переглядати та аналізувати дані моніторингу безпеки від Клієнтів, а також керувати Клієнтами, користувачами, правилами моніторингу USB, оповіщеннями, базою даних, серійними ключами і т.д. Ви можете отримати доступ до Інструменту керування віддалено з будь-якого комп'ютера в мережі, без необхідності встановлювати його на цей комп'ютер. Інструмент управління включає

в себе Session Viewer, який надає зручний інтерфейс для швидкого перегляду даних моніторингу, отриманих від клієнтів Syteca, включаючи відтворення у вигляді відеозаписів знімків екрану, зроблених під час будь-якого обраного сеансу роботи клієнта [12].

Syteca Clients, що встановлюються на кінцевих точках:

- Клієнти Syteca для Windows (далі - Клієнти Windows): Розташовані на віддалених комп'ютерах, Клієнти Windows записують знімки екрану з рухами миші у вигляді відео з певною частотою і відправляють їх на Сервер додатків разом з метаданими, такими як ім'я користувача, ім'я хоста, час активності, заголовки активних вікон, назви додатків, URL-адреси, текстові дані буфера обміну, натискання клавіш і т.д. Керування конфігурацією та налаштуваннями віддалених Windows-клієнтів здійснюється за допомогою Інструменту керування.
- Клієнти Syteca macOS (далі - Клієнти macOS): Розміщені на віддалених комп'ютерах, клієнти macOS записують знімки екрану з рухами миші у вигляді відео із заданою частотою і відправляють їх на сервер додатків разом з метаданими, такими як ім'я користувача, ім'я хоста, час активності, заголовки активних вікон, назви додатків і т.д. Керування конфігурацією та налаштуваннями віддалених macOS-клієнтів здійснюється за допомогою Інструменту керування.
- Клієнти Syteca Linux/Unix (далі - Клієнти Linux): Розташовані на віддалених комп'ютерах, клієнти Linux записують знімки екрану і дані вводу/виводу терміналу (включаючи виконані команди) і надсилають ці інтерактивні дані на сервер додатків.
- NOT AVAILABLE IN SAAS Syteca Tray Notifications (далі - програма Tray Notifications): Ця програма дозволяє отримувати сповіщення від Клієнтів про тривожні події на них.

Інші компоненти системи

Також можна використовувати інші окремі програмні компоненти Syteca:

- NOT AVAILABLE IN SAAS Syteca Master Panel (далі - Майстер-панель): Цей додатковий автономний компонент Syteca може використовуватися для

великомасштабного розгортання в режимі високої доступності і об'єднує дані з усіх екземплярів Syteca Applications Servers на різних вузлах, дозволяючи переглядати всі клієнтські сесії в єдиному інтерфейсі користувача.

- Syteca SDK (для розробників): Syteca Software Development Kit складається з API та інших інструментів, які дозволяють розробникам інтегрувати Syteca з інформаційними системами клієнтів, щоб полегшити передачу бізнес-аналітики (BI) та інших даних між ними.

2.3. Механізми моніторингу та аналізу користувацької активності в UAM. Syteca

Syteca реалізує багаторівневий підхід до моніторингу активності користувачів, поєднуючи технічний нагляд, запис дій та аналітичну обробку даних. Це дозволяє не лише фіксувати події, але й виявляти загрози на основі поведінкових патернів та контексту дій.

1. Низькорівневе логування подій

Агент системи фіксує широкий спектр подій, включаючи:

- запуск і завершення програм;
- відкриття, редагування та копіювання файлів;
- доступ до зовнішніх носіїв (USB, CD/DVD);
- мережеву активність (веб-сайти, IP-з’єднання);
- натискання клавіш (keylogging);
- буфер обміну (clipboard activity).

Ці дані формують хронологічний лог активності, доступний для перегляду у вигляді таблиць або фільтрованих списків.

2. Відеозапис сесій користувача

Одна з ключових особливостей Syteca — створення відео-скрінкасту робочої сесії користувача. Запис включає:

- робочий стіл, активні вікна та взаємодію з інтерфейсом;
- одночасне відображення таймлайнів натискань клавіш та подій;
- можливість прискореного перегляду та переходу до підозрілих фрагментів.

Це дає змогу відтворити повну картину подій при розслідуванні інцидентів.

3. Поведенковий аналіз (User Behavior Analytics, UBA)

Syteca будує поведінкові профілі користувачів на основі:

- типових робочих годин;
- використовуваних програм;
- стандартних дій з файлами;
- обсягу даних, що передаються у мережу чи на носії.

Відхилення від звичного профілю автоматично позначаються як потенційно ризиковані.

4. Індикатори компрометації (Indicators of Compromise, IoC)

Система виявляє ознаки потенційної загрози:

- запуск інструментів адміністрування поза робочим контекстом;
- доступ до критичних директорій;
- масове копіювання файлів;
- спроби обходу політик безпеки.

Інциденти зберігаються в спеціальному журналі й супроводжуються тегами ризику.

5. Політики реагування та автоматичні тригери

Syteca підтримує створення правил, які реагують на виявлену активність:

- сповіщення (email, Telegram, Slack тощо);
- блокування сесії користувача;
- ізоляція ПК від мережі;
- запуск скриптів для локального реагування.

Це забезпечує як пасивний нагляд, так і активне протидіяння загрозам у реальному часі.

6. Формування звітів та експорту даних

Для звітування та подальшого аналізу:

- доступні шаблони звітів (інциденти, активність користувачів, порушення політик);
- дані експортуються у PDF, XLSX, CSV, відеоформати;
- підтримка збереження даних для судової експертизи (форензика) [12].

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ВІД ІНСАЙДЕРСЬКИХ НА ОСНОВІ UAM SYTECA

3.1. Встановлення, налаштування UAM Syteca в корпоративну IT-інфраструктуру

Для забезпечення контролю за активністю користувачів у корпоративному середовищі необхідно інтегрувати систему моніторингу до існуючої IT-інфраструктури. Одним із прикладів таких рішень є система User Activity Monitoring (UAM) Syteca, яка надає розширені можливості з відстеження дій користувачів, виявлення інцидентів безпеки та забезпечення відповідності політикам організації.

У цьому розділі розглядається поетапний процес встановлення та налаштування UAM Syteca, починаючи зі створення серверної частини, підключення до бази даних і конфігурування збереження даних, до встановлення агентів на кінцеві точки та організації доступу через веб-інтерфейс. Наведені ілюстрації демонструють ключові кроки впровадження системи в робоче середовище та її подальшу інтеграцію з клієнтськими пристроями [14].

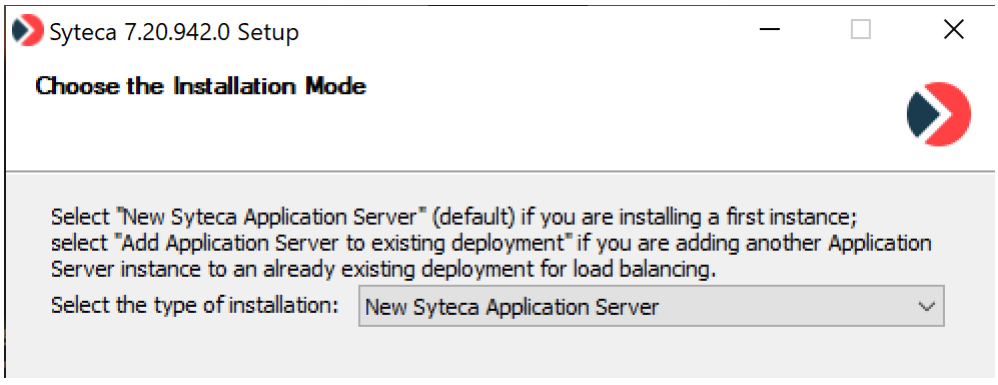


Рис. 3.1. Встановлення серверу Syteca

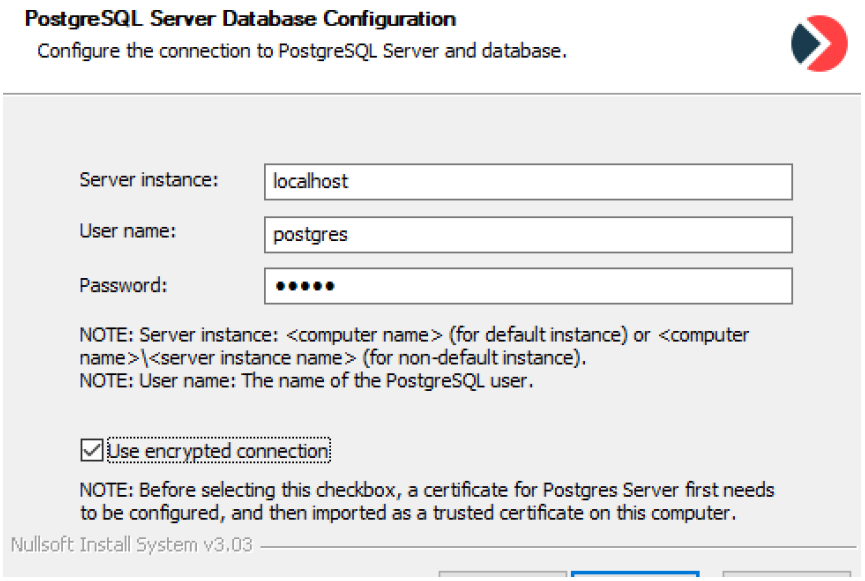


Рис. 3.2. Підключення серверу Syteca до бази PostgreSQL

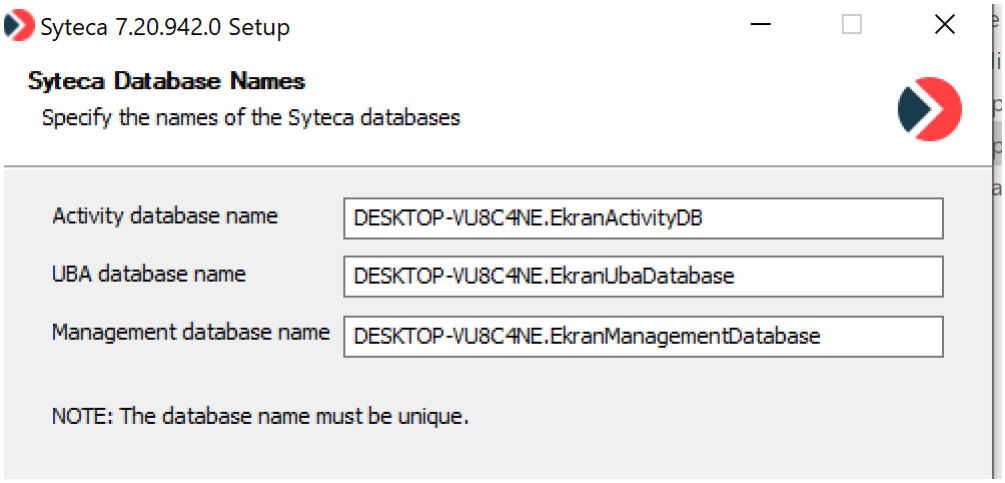


Рис. 3.3. Шлях зберігання даних Syteca

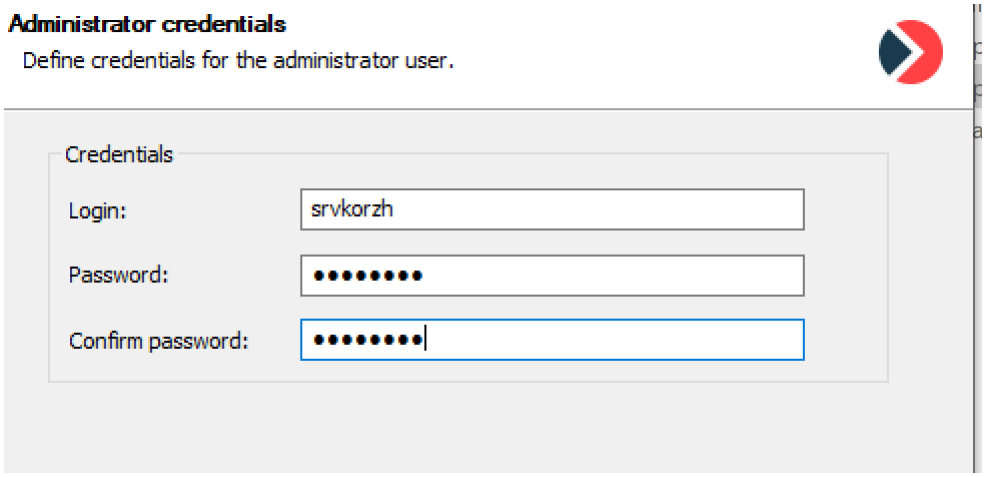


Рис. 3.4. Створення адміністратора серверу Syteca

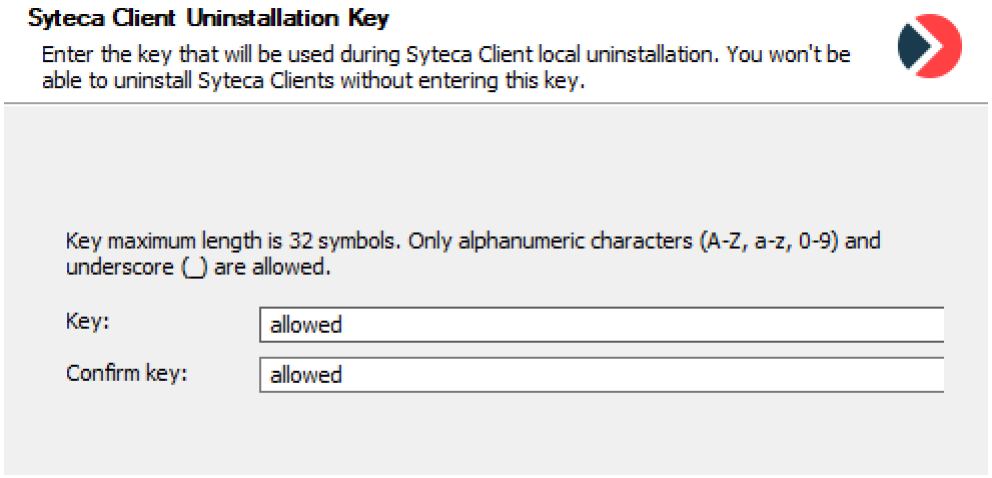


Рис. 3.5. Створення ключа деінсталяції

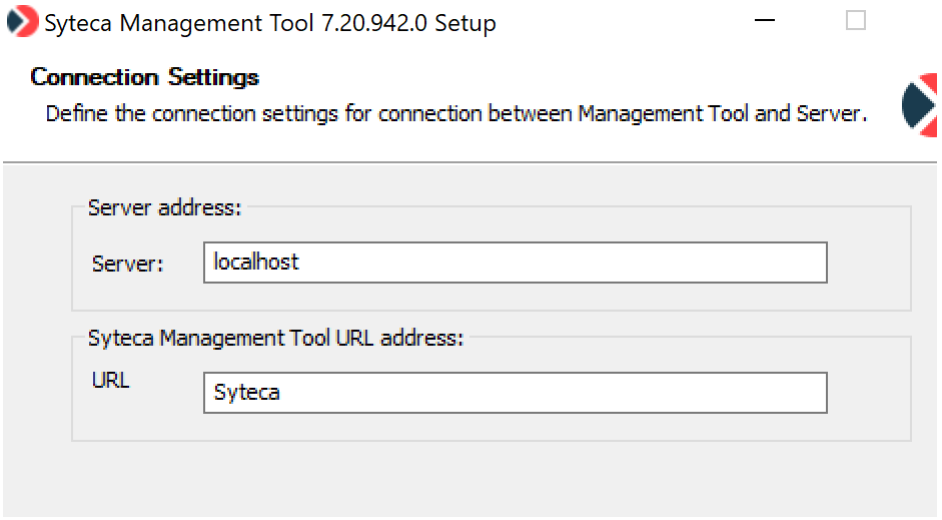


Рис. 3.6. Налаштування доступу з web-сторінки до утиліти керування Syteca

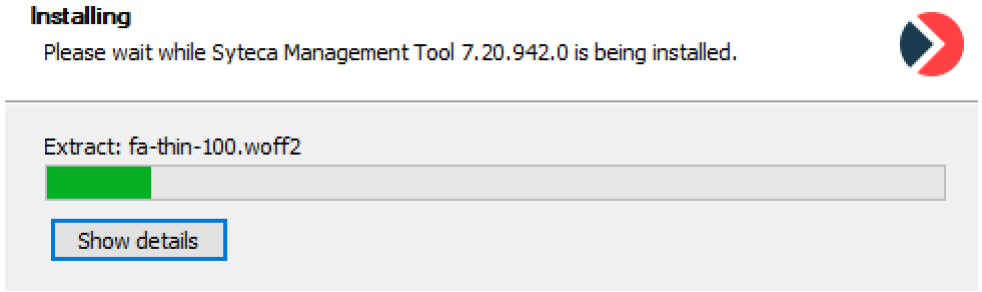


Рис. 3.7. Процес інсталяції Syteca

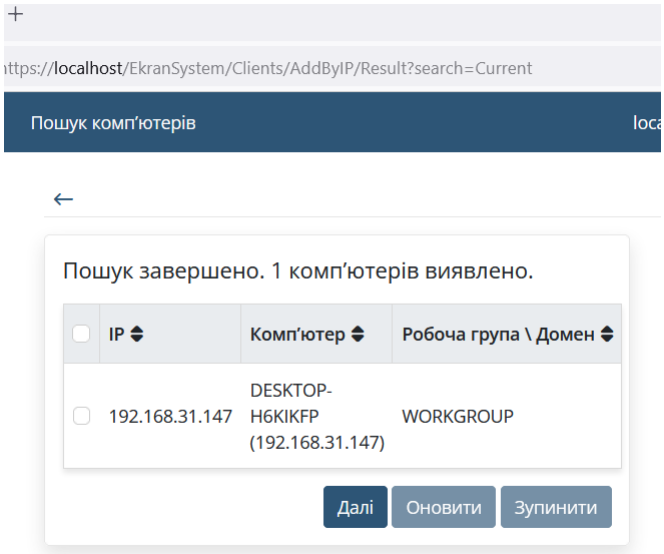


Рис. 3.8. Встановлення агента Syteca на кінцеву точку

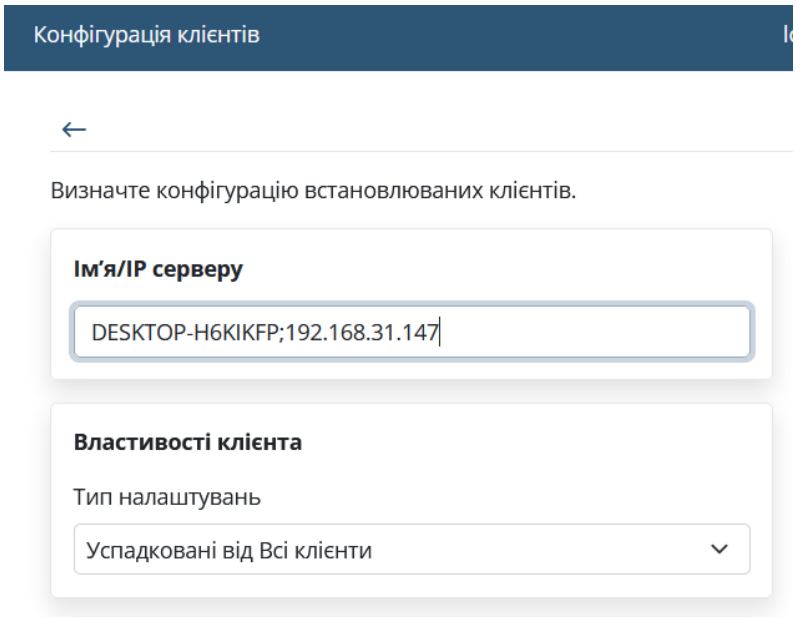


Рис. 3.9. Конфігурація клієнта

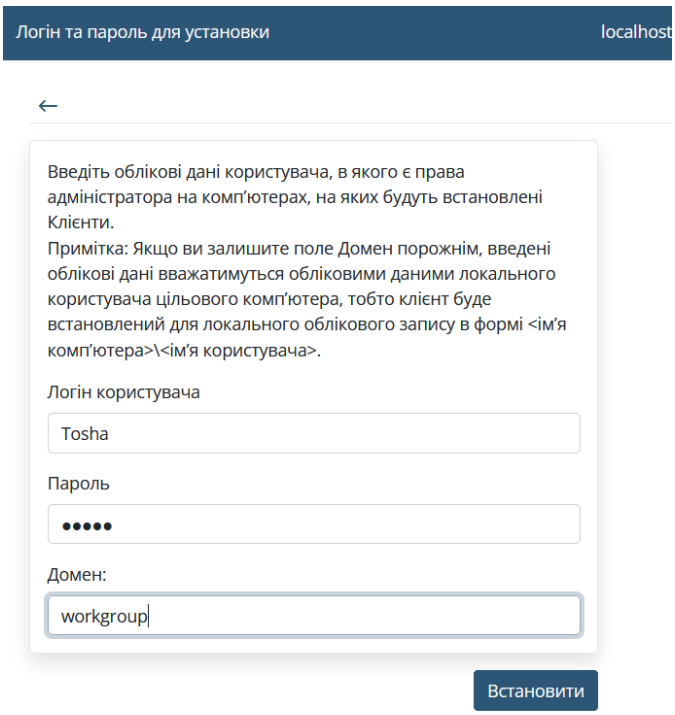


Рис. 3.10. Введення логіну та паролю для встановлення агента на кінцеву точку

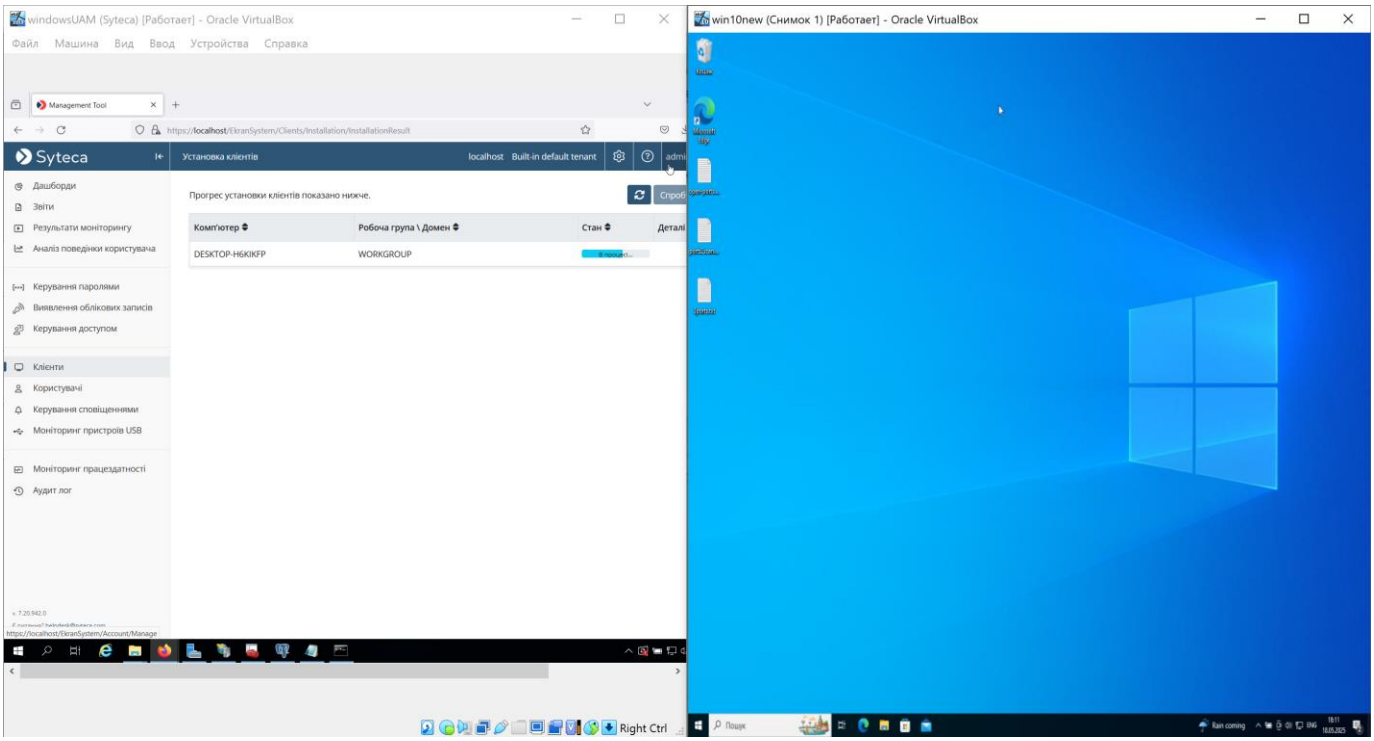


Рис. 3.11. Процес віддаленого встановлення агента на кінцеву точку

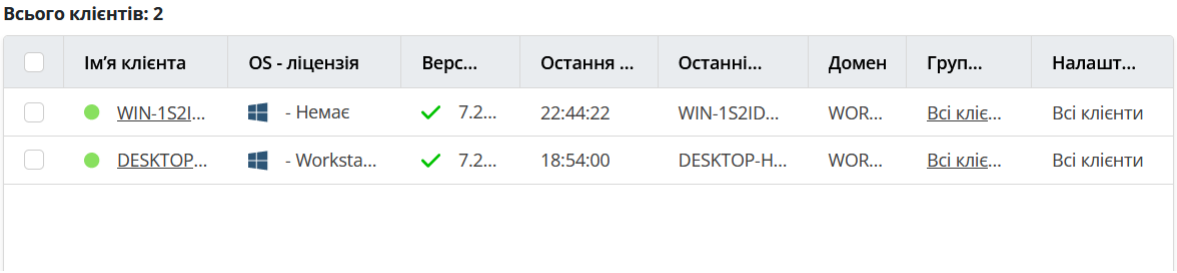


Рис. 3.12. Підключені клієнти до UAM Syteca

3.2. Результати моніторингу та робота з тригерами в UAM Syteca

Після успішного встановлення та налаштування системи UAM Syteca наступним кроком є аналіз результатів моніторингу та ефективне використання механізму тригерів для виявлення потенційно небезпечної або небажаної активності. Тригери в Syteca дозволяють автоматично реагувати на певні дії користувачів — наприклад, підключення зовнішніх носіїв, запуск виконуваних файлів чи використання визначених ключових слів.

У цьому розділі наведено приклади спрацювань тригерів і демонструється, як система фіксує такі події в інтерфейсі адміністратора. Це дає змогу швидко реагувати на порушення політик безпеки, формувати звітність та приймати обґрунтовані рішення щодо подальших дій.

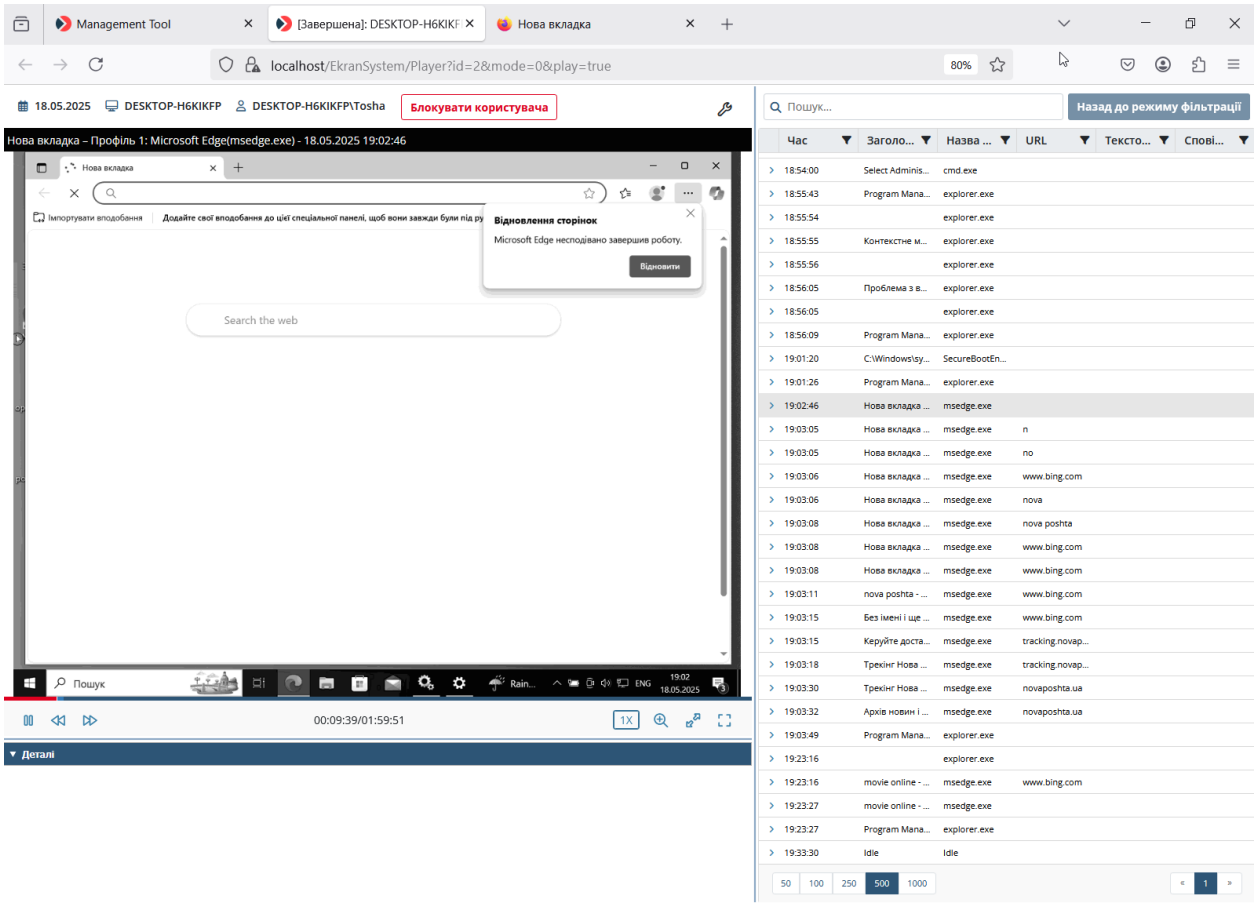


Рис. 3.13. Результати моніторингу та спрацювань на тригери

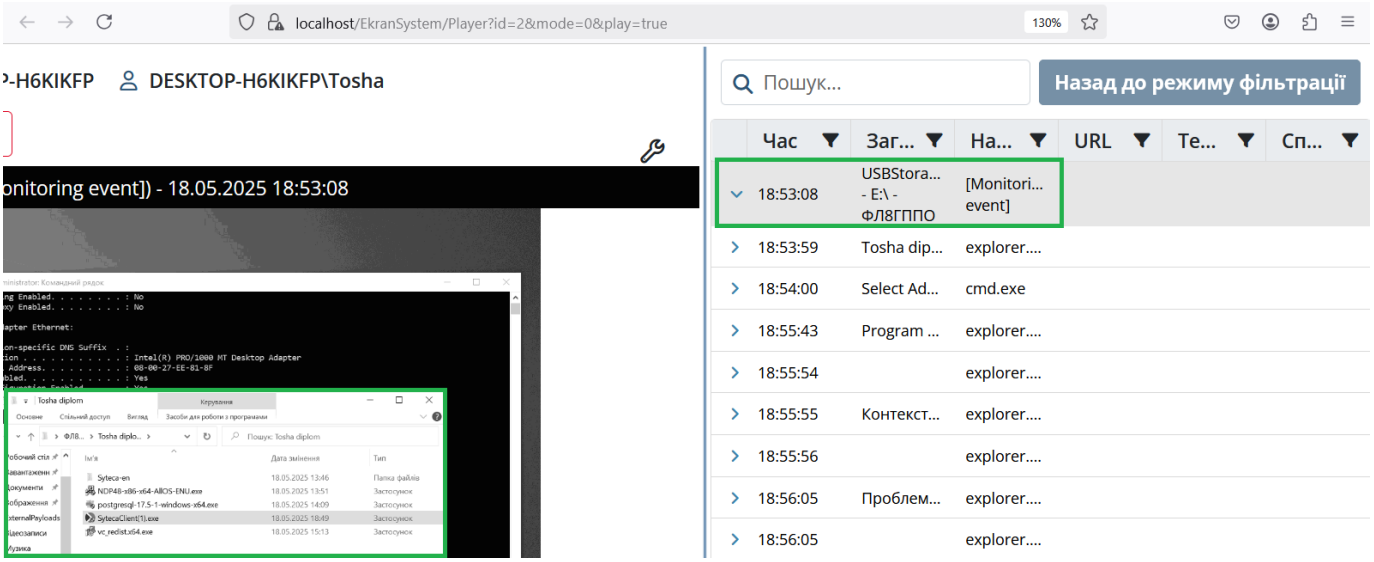


Рис. 3.14. Спрацювання на тригер підключення зовнішніх пристроїв

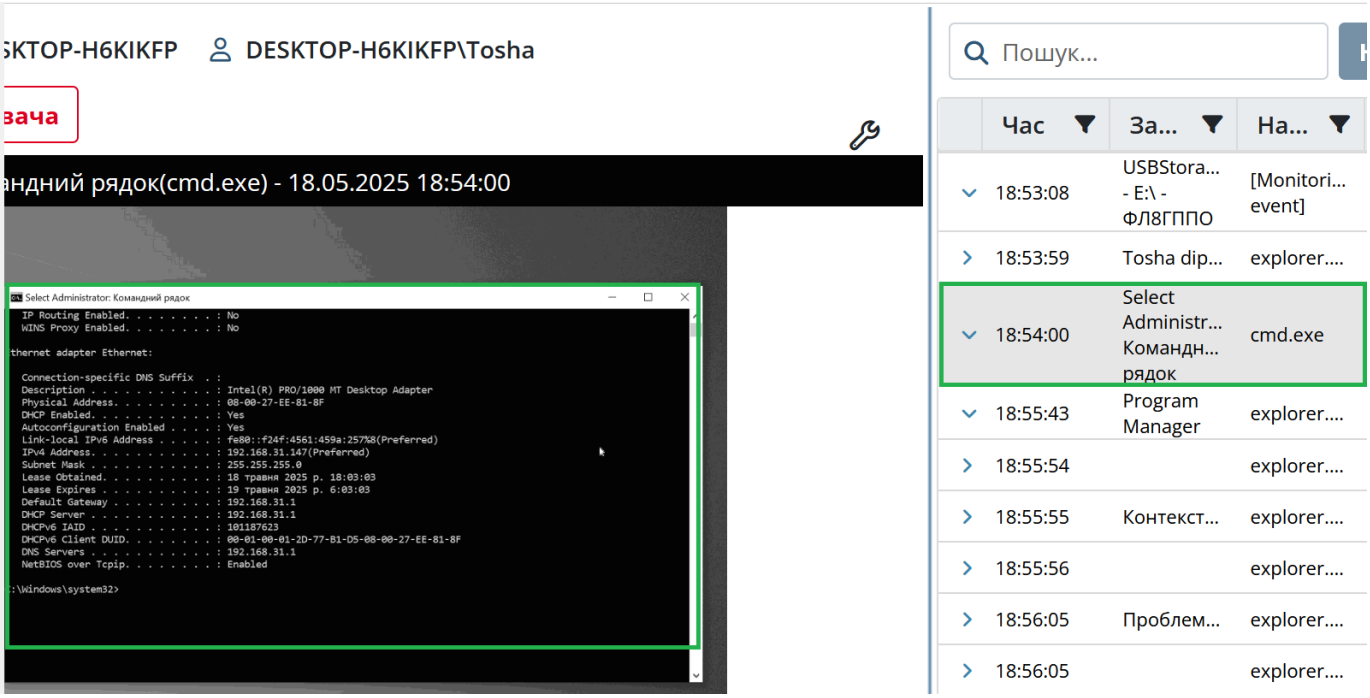


Рис. 3.15. Тригер запуску файлів розширення exe

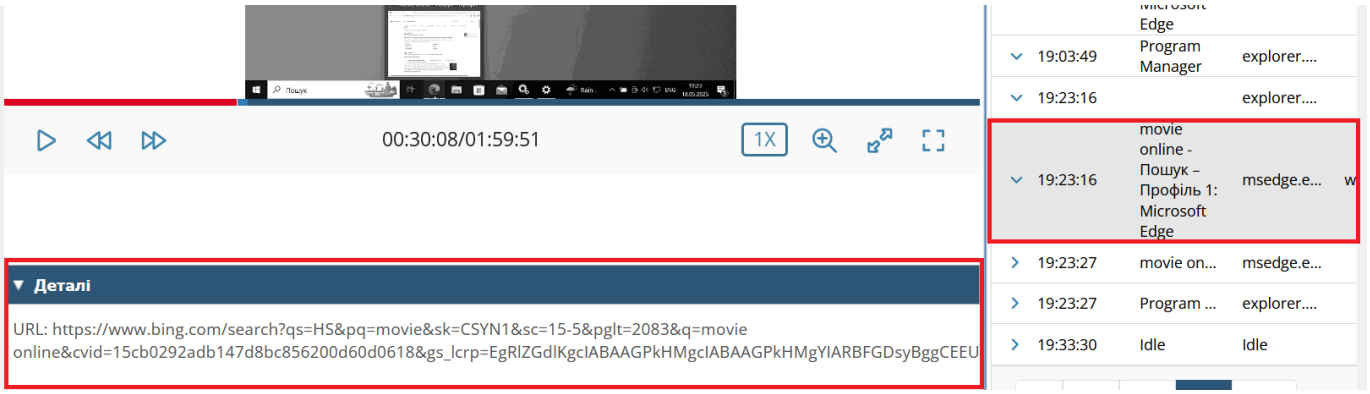


Рис. 3.16. Спрацювання тригера по ключовим словах

3.3.Рекомендації щодо захисту інформації від інсайдерських загроз на основі UAM Syteca

Ключ до виявлення інсайдерських загроз лежить у здатності системи фіксувати та аналізувати найдрібніші деталі поведінки користувача. Syteca надає для цього потужні інструменти [15].

- Моніторинг клавіатури (Keystroke Monitoring) та буфера обміну: Syteca дозволяє записувати кожне натискання клавіші, а також фіксувати вміст буфера обміну, що надає повний контекст дій користувача завдяки інтеграції з відеозаписом екрану.
- Фільтрація IP-адрес (Remote Host IP Filtering): Syteca дозволяє контролювати та обмежувати доступ до корпоративних ресурсів з певних IP-адрес.
- Моніторинг програм та веб-сайтів (Application and Website/URL Monitoring): Система дозволяє створювати "білі" та "чорні" списки програм та веб-сайтів, а також відстежувати час, проведений користувачами в певних додатках.
- Детальний моніторинг файлових операцій: Syteca фіксує всі операції з файлами – копіювання, переміщення, видалення, перейменування, завантаження та вивантаження – на локальних дисках, мережевих ресурсах, знімних носіях та у хмарних сховищах.
- Контроль USB-пристроїв та інших знімних носіїв: Система надає детальний контроль над підключенням та використанням USB-пристроїв, зовнішніх дисків та інших знімних носіїв.
- Налаштування сповіщень та автоматизованих реакцій на інциденти: Система дозволяє налаштовувати різноманітні правила для генерації сповіщень та автоматичних дій у відповідь на виявлену підозрілу активність.
- Звітування та аналіз даних: Система надає розширені можливості для формування звітів, пошуку та фільтрації даних у записах сесій.

Інші інтеграційні можливості та адміністративні аспекти:

Ефективність Syteca значно зростає при її інтеграції в загальну архітектуру інформаційної безпеки.

- Інтеграція з DLP-системами (Data Loss Prevention): Хоча Syteca сама по собі є потужним інструментом для запобігання витокам даних, її інтеграція з виділеними DLP-системами дозволить посилити контроль над вмістом та запобігти витоку даних на основі аналізу їхнього вмісту, що доповнює поведінковий моніторинг Syteca.

- Управління привілейованим доступом (PAM): Syteca (як частина EkranSystem) може виступати як компонент PAM-рішення. Детальний моніторинг привілейованих облікових записів (системних адміністраторів, розробників) є критично важливим, оскільки саме вони мають найбільший потенціал для зловживань. Це включає запис сесій, управління паролями та надання "Just-in-Time" доступу.
- Прозорість та навчання: Важливо інформувати співробітників про те, що їхня активність на корпоративних системах моніториться. Це не тільки відповідає законодавчим вимогам, але й діє як превентивний фактор, зменшуючи ймовірність зловживань. Регулярні тренінги з кібербезпеки повинні включати розділ про інсайдерські загрози та роль UAM-систем у їх запобіганні.

ВИСНОВКИ

Проведений аналіз проблеми інсайдерських загроз розкриває їх як одну з найбільш небезпечних та складних категорій ризиків для інформаційної безпеки будь-якої організації. Інсайдер, будучи особою з авторизованим доступом або знанням внутрішніх ресурсів, має унікальні можливості для нанесення шкоди, що може включати як навмисні зловмисні дії (шпигунство, саботаж, крадіжка, тероризм, корупція), так і ненавмисні помилки, спричинені недбалістю чи випадковістю. На відміну від зовнішніх кібератак, інсайдерська загроза походить зсередини, що робить традиційні засоби захисту периметра менш ефективними.

Ключовим аспектом розуміння та протидії інсайдерським загрозам є усвідомлення того, що перетворення довіреного співробітника на зловмисника – це часто не спонтанна подія, а процес, що включає етапи виникнення невдоволення чи стресу, підготовки, вивчення системи, експериментів та, зрештою, виконання деструктивних дій. На кожному з цих етапів особа може демонструвати поведінкові індикатори, такі як незвичайні моделі доступу до даних, спроби обійти заходи безпеки, зміни в поведінці чи несанкціоноване використання ресурсів. Приклад з Pegasus Airlines, де витік майже 6,5 ТБ конфіденційних даних стався через незахищений сегмент AWS S3, яскраво ілюструє, як навіть ненавмисна помилка може мати катастрофічні наслідки, підкреслюючи вразливість перед внутрішніми загрозами та необхідність постійного контролю за конфігураціями та доступом.

Ефективне виявлення та запобігання інсайдерським загрозам вимагає комплексного підходу. Важливу роль відіграють не лише технологічні рішення, такі як UAM, що дозволяють відстежувати та аналізувати поведінку, виявляючи аномалії. Критично важливим є також "людський фактор" – обізнаність співробітників та їх здатність розпізнавати тривожні ознаки в поведінці колег. Програми підвищення обізнаності серед персоналу, що навчають розпізнавати індикатори загрози та повідомляти про них, є невід'ємною частиною стратегії захисту.

ПЕРЕЛІК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Insider Threat Mitigation. cisa. URL: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation (дата звернення: 02.05.2025).
2. Insider Threat Protection Guide: 10 Best Practices to Follow | Syteca. Syteca. URL: https://www.syteca.com/en/blog/guide-to-insider-threat-protection (дата звернення: 20.05.2025).
3. Mitigating Insider Threats: 5 Simple and Effective Strategies for 2025. Sattrix. URL: https://www.sattrix.com/blog/insider-threats-mitigation-strategies-2025/ (дата звернення: 10.04.2025).
4. Mitigating Insider Threats: 5 Simple and Effective Strategies for 2025. Sattrix. URL: https://www.sattrix.com/blog/insider-threats-mitigation-strategies-2025/ (дата звернення: 10.04.2025).
5. Ananthanpillai R. Insider Threats: How companies can combat the rising risks from within. Home | Security Info Watch. URL: https://www.securityinfowatch.com/cybersecurity/article/55261438/insider-threats-how-companies-can-combat-the-rising-risks-from-within (дата звернення: 23.04.2025).
6. UAM Indicators | MITRE Insider Threat Research & Solutions™. MITRE Insider Threat Research & Solutions. URL: https://insiderthreat.mitre.org/uam-indicators/ (дата звернення: 03.05.2025).
7. Syteca to Exhibit at RSAC 2025 | Syteca. Syteca. URL: https://www.syteca.com/en/blog/rsac-2025 (дата звернення: 08.05.2025).
8. A Comprehensive Guide to User Activity Monitoring. EMB Blogs. URL: https://blog.emb.global/user-activity-monitoring-uam/ (дата звернення: 13.05.2025).
9. What is the difference between Teramind Starter, Teramind UAM, Teramind DLP and Teramind Enterprise? | Teramind Knowledge Base. Teramind Knowledge Base. URL: https://kb.teramind.co/en/articles/8790885-what-is-the-difference-between-teramind-starter-teramind-uam-teramind-dlp-and-teramind-enterprise (дата звернення: 12.05.2025).

10. What is UBA, UEBA, & SIEM? Security Management Terms Defined. exabeam. URL: https://www.exabeam.com/blog/siem-trends/what-is-uba-ueba-siem-security-management-terms-defined/ (дата звернення: 14.05.2025).

11. SIEM vs. SOAR vs. XDR vs. UEBA: How Are They Different?. Mimecast. URL: https://www.mimecast.com/blog/siem-vs-soar-vs-xdr-vs-ueba-how-are-they-different/ (дата звернення: 11.05.2025).

12. Лаптєв С. О. Удосконалення моделі протидії витоку інсайдерської інформації з урахуванням нестабільності функціонування окремих елементів системи захисту інформації. Google Scholar. URL: https://scholar.google.com/citations?view_op=view_citation&hl=uk&user=aD8ZHpkAAAAJ&citation_for_view=aD8ZHpkAAAAJ:KlAtU1dfN6UC (дата звернення: 09.05.2025).

13. UAM Security, Benefits, and Best Practices | ScreenConnect. ScreenConnect. URL: https://www.screenconnect.com/blog/uam-security (дата звернення: 10.05.2025).

14. AccessMatrix Universal Access Management (UAM). Cybersecurity Excellence Awards. URL: https://cybersecurity-excellence-awards.com/candidates/accessmatrix-universal-access-management-uam-2025/ (дата звернення: 14.05.2025).

15. Katz E. Top 7 User Activity Monitoring (UAM) Tools for 2024 | Memcyco. Memcyco. URL: https://www.memcyco.com/user-activity-monitoring-uam-tools/ (дата звернення: 14.05.2025).