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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія реагування на інциденти внутрішньої безпеки на базі UAM Syteca»

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

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

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

_____ Євгеній НЕЧИПОРЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
НЕЧИПОРЕНКО Євгеній
(прізвище, ім'я)

Керівник д-р техн. наук, проф., САВЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 3
ВСТУП 4
1 АНАЛІЗ ІНЦИДЕНТІВ ВНУТРІШНЬОЇ БЕЗПЕКИ ТА ЗАСОБІВ ЇХ РЕАГУВАННЯ 6
1.1. Поняття та класифікація інцидентів внутрішньої інформаційної безпеки 6
1.2. Огляд сучасних підходів та технологій реагування на інсайдерські загрози 10
1.3. Аналіз існуючих рішень UAM та їх порівняльна характеристика 14
2 ДОСЛІДЖЕННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ UAM SYTECA 16
2.1. Архітектура системи UAM Syteca та її компоненти 16
2.2. Механізми моніторингу, збору та аналізу подій у Syteca 19
2.3. Інтеграція Syteca з іншими системами кібербезпеки підприємства 21
3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ РЕАГУВАННЯ НА ІНЦИДЕНТИ ВНУТРІШНЬОЇ БЕЗПЕКИ НА БАЗІ UAM SYTECA 25
3.1. Розгортання та налаштування UAM Syteca 25
3.2. Застосування технології з реагування на інциденти внутрішньої безпеки на базі UAM Syteca 36
3.3. Розроблення рекомендацій щодо застосування технології реагування на інциденти внутрішньої безпеки на базі UAM Syteca 46
ВИСНОВКИ 49
ПЕРЕЛІК ПОСИЛАНЬ 50
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 53

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IB	—	інтелектуальна власність
PII	—	Personally Identifiable Information
DLP	—	Data Loss Prevention
GDPR	—	General Data Protection Regulation
PAM	—	Privileged Access Management
SIEM	—	Security Incident and Event Management
UBA	—	User Behavior Analytics
IoC	—	Indicator of Compromise
OSINT	—	Open source intelligence
ISAC	—	Information Sharing and Analysis Center
NTA	—	Network Traffic Intelligence
NDA	—	Non-disclosure agreement
UAM	—	User Activity Monitoring
SDK	—	Software Development Kit
API	—	Application Programming Interface
URL	—	Uniform Resource Locator
SSO	—	Single sign-on
IAM	—	Identity and Access Management
SOC	—	Security Operations Center
SQL	—	Structured Query Language
MS	—	Microsoft

ВСТУП

Актуальність дослідження.

Статистика провідних аналітичних агентств свідчить, що значна частина інцидентів внутрішньої безпеки пов'язана з діями інсайдерів — легітимних користувачів, які мають санкціонований доступ до інформаційних ресурсів. Виявлення таких загроз ускладнюється тим, що дії внутрішнього зловмисника технічно часто не відрізняються від штатної роботи співробітника, що робить класичні засоби захисту (антивіруси, міжмережеві екрани) неефективними проти них.

Витік конфіденційної інформації, технологічних секретів або клієнтських баз через дії невідповідальних співробітників чи промислове шпигунство може завдати організації великих фінансових та репутаційних збитків, аж до повної втрати конкурентоспроможності. Крім того, в умовах сучасних гібридних загроз «людський фактор» залишається найслабшою ланкою: навіть відповідальні співробітники можуть стати ненавмисними інсайдерами внаслідок фішингових атак або низької обізнаності з правилами кібергігієни, що вимагає переходу від простого блокування до глибокого поведінкового аналізу дій персоналу.

Водночас, існуючі традиційні системи моніторингу подій часто надають лише фрагментарні дані у вигляді технічних логів, які не дозволяють однозначно трактувати наміри користувача та контекст інциденту. Це створює суттєві перешкоди при проведенні службових розслідувань та зборі доказової бази. Тому критично важливим стає впровадження комплексних технологій з UAM, таких як Syteca, що поєднують відеофіксацію дій, кейлоггінг та аналітику поведінки. Тому тема «Технологія реагування на інциденти внутрішньої безпеки на базі UAM Syteca».

Об'єкт дослідження – забезпечення захисту корпоративних інформаційних систем від внутрішніх загроз.

Предмет дослідження – технологія реагування на інциденти внутрішньої безпеки на базі UAM Syteca.

Мета роботи – розробити варіант технології реагування на інциденти внутрішньої безпеки на базі UAM Syteca та рекомендації, щодо її застосування.

Наукові завдання:

- проаналізувати інциденти внутрішньої безпеки та засобів реагування на них;

- дослідити функціональні можливості UAM Syteca;

- розгорнути та налаштувати UAM Syteca;

- застосування технології з реагування на інциденти внутрішньої безпеки на базі UAM Syteca;

- розробити варіант технології реагування на інциденти внутрішньої безпеки на базі UAM Syteca.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, експериментальний метод.

Практичне значення одержаних результатів: запропоновано застосування технології з реагування на інциденти внутрішньої безпеки на базі UAM Syteca, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Апробація результатів. Результати кваліфікаційної роботи апробовані на Всеукраїнській науково-практичній конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ІНЦИДЕНТІВ ВНУТРІШНЬОЇ БЕЗПЕКИ ТА ЗАСОБІВ ЇХ РЕАГУВАННЯ

1.1. Поняття та класифікація інцидентів внутрішньої інформаційної безпеки

Більшість організацій зосереджують свої зусилля на захисті від зовнішніх кібератак, статистика та практика незмінно підтверджують, що одна з найсерйозніших загроз інформаційній безпеці походить зсередини. Внутрішні інциденти, спричинені інсайдерами — чи то зловмисними, чи недбалими діями співробітників, підрядників або партнерів — часто завдають найбільшої шкоди. Ці загрози оперують за межами традиційного периметра безпеки, маючи легітимний доступ до систем, що робить їх виявлення та нейтралізацію значно складнішими, ніж протидію зовнішньому зловмиснику.

Розуміння поточного стану внутрішніх загроз у кібербезпеці є важливим для будь-якої організації, яка прагне зміцнити свою безпеку. Оскільки характер внутрішніх ризиків розвивається, відстеження останніх тенденцій дає керівникам відділів безпеки можливість приймати розумніші та проактивніші рішення [1].

Інцидент внутрішньої інформаційної безпеки — це будь-яка подія або дія, що походить зсередини організації та порушує її політики безпеки, ставлячи під загрозу конфіденційність, цілісність або доступність (так звану "тріада CIA") її інформаційних активів.

У Звіті про внутрішні загрози за 2024 рік [2], підготовленому Cybersecurity Insiders, зазначається, що 71% організацій є принаймні помірно вразливими до внутрішніх загроз. 51% організацій повідомили про шість або більше атак у 2023 році. Компанії продовжують стикатися з внутрішніми загрозами, які можна простежити за цими трьома типами суб'єктів зображеному на Рис. 1.1.

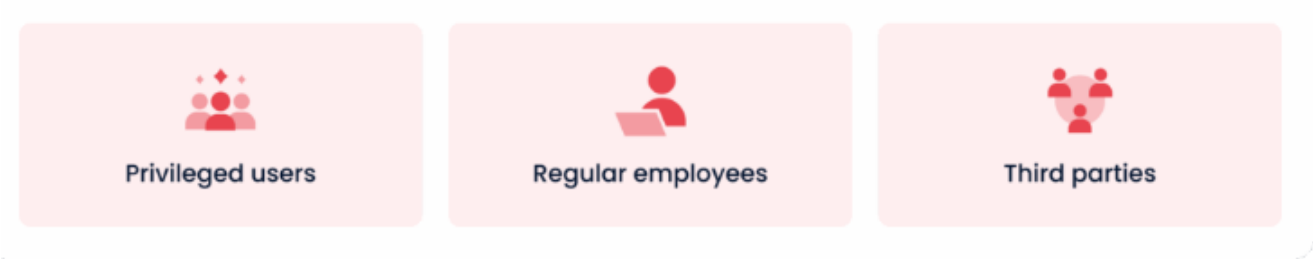

Рис. 1.1. Три основні категорії інсайдерів

1. Привілейовані користувачі (Privileged users)

Це користувачі, які мають підвищений, або привілейований, рівень доступу до критичних систем, даних та інфраструктури. До них належать системні адміністратори, адміністратори баз даних, мережеві інженери та топ-менеджмент.

2. Звичайні співробітники (Regular employees)

Це більшість персоналу організації. Вони мають стандартний рівень доступу, необхідний для виконання їхніх повсякденних робочих обов'язків (наприклад, доступ до електронної пошти, спільних дисків, CRM-системи тощо).

Це найчисельніша група, і саме вона найчастіше стає джерелом ненавмисних інцидентів (через недбалість, фішинг, помилкове відправлення даних). Вони також можуть бути зловмисними інсайдерами, наприклад, копіюючи клієнтську базу перед звільненням.

3. Треті сторони (Third parties)

Це не співробітники компанії, але вони мають легітимний, хоча й тимчасовий або обмежений, доступ до внутрішніх ресурсів. Це можуть бути підрядники, фрилансери, консультанти, аудитори або навіть представники компаній-постачальників (наприклад, для обслуговування обладнання).

У звіті Ponemon Institute «Вартість інсайдерських ризиків» за 2025 рік аналізується частота інцидентів, спричинених інсайдерами, та обсяг їхніх витрат. Для класифікації у звіті використовуються три профілі ризику: недбалість інсайдерів, злий намір та крадіжка облікових даних зовнішніми сторонами [1].

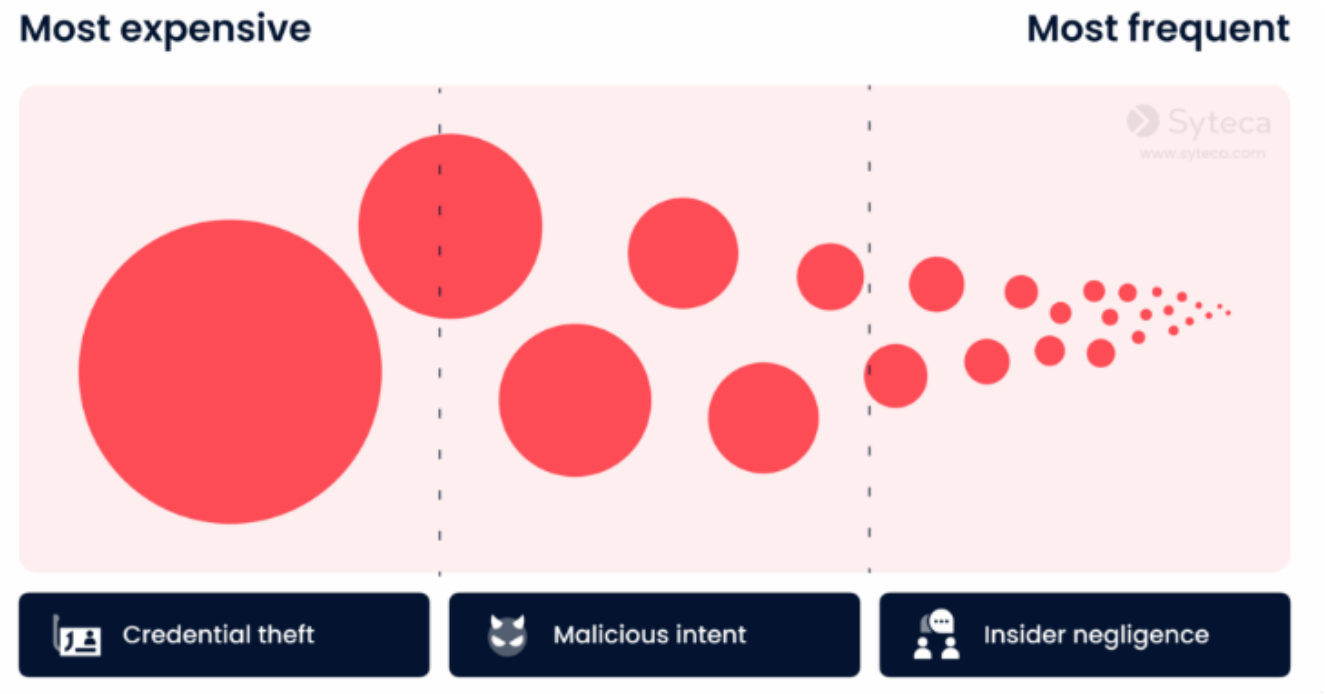

Рис. 1.2. Вартість та частота інцидентів внутрішніх загроз за профілем ризику [1]

Insider negligence

Недбалість внутрішніх осіб є причиною більшості інцидентів, пов'язаних з ризиками для безпеки внутрішніх осіб, що підкреслює необхідність моніторингу активності користувачів. Загалом у звіті проаналізовано 4321 такий інцидент, при цьому в середньому в організації у 2024 році сталося 13,5 таких випадків. Загальні річні витрати зросли до 8,8 мільйона доларів, порівняно з 7,2 мільйона доларів у 2023 році. Аналогічно, середня вартість одного інциденту зросла до 676 517 доларів, що є значним стрибком порівняно з 505 113 доларів у 2023 році [1].

Malicious intent

Інсайдерів зі зловмисними намірами важче виявити, ніж зовнішніх зловмисників чи хакерів, оскільки вони знайомі із заходами кібербезпеки вашої організації та конфіденційними даними. Згідно зі звітом, у 2024 році було зареєстровано 1995 таких інцидентів, причому кожна постраждала організація зазнала в середньому 6,3 події [1].

Вартість одного зловмисного інсайдерського інциденту досягла 715 366 доларів США у 2025 році, порівняно з 701 500 доларів США у 2023 році, що робить їх найдорожчими типами інсайдерських загроз у розрахунку на один інцидент.

Однак загальні річні витрати знизилися до 3,7 мільйона доларів США порівняно з 4,8 мільйона доларів США у попередньому році [1].

Credential theft

Крадіжка облікових даних – один із найпоширеніших методів, який зовнішні зловмисники використовують для проникнення через захищений периметр організації. Використовуючи легітимні облікові дані, зловмисники можуть непомітно діяти в системі протягом тривалого часу. Щоб отримати логіни та паролі користувачів, зловмисники використовують соціальну інженерію , атаки методом грубої сили , заповнення облікових даних та інші вектори атаки [1].

У звіті Ponemon наведено інформацію про 1552 такі інциденти, причому кожна організація стикається в середньому з 4,8 щорічно. Середні витрати на один інцидент зросли до 779 797 доларів США порівняно з 679 621 доларом США у 2023 році, що робить їх найвищими серед усіх трьох категорій внутрішніх загроз. Загальні річні витрати також зросли до 4,8 мільйона доларів США [1].

У посібнику Common Sense Guide to Mitigating Insider Threats (Посібник зі зменшення внутрішніх загроз від Common Sense) CERT класифікує діяльність зловмисних інсайдерів наступним чином [3, 4]:

Крадіжка інтелектуальної власності (ІВ) – це несанкціоноване отримання конфіденційної бізнес-інформації, такої як комерційна таємниця, вихідний код, наукові дослідження або запатентовані розробки. За даними дослідників CERT, понад половина випадків крадіжки ІВ стосується технічного персоналу – розробників, дослідників, інженерів – чиї навички та рівень доступу дозволяють їм непомітно витягувати великі обсяги даних. Поширеними причинами є фінансова потреба, незадоволення роботою, бажання допомогти новому роботодавцю або переконання, що вкрадена робота належить їм [3, 5].

ІТ-саботаж — це зловживання інформаційними технологіями з метою завдання конкретної шкоди організації чи окремій особі. Ці атаки також зазвичай здійснюють системні адміністратори, програмісти або інші технічно підковані співробітники, які можуть приховати свої зловмисні дії та порушити роботу організації. Цих людей зазвичай мотивує бажання помститися за негативний досвід

роботи, і вони зазвичай здійснюють свої атаки під час роботи або невдовзі після звільнення.

Шахрайство передбачає отримання несанкціонованого доступу до даних організації або їх зміну. Зазвичай мотивацією шахрайства є особиста вигода або крадіжка даних з метою крадіжки особистих даних або шахрайства з кредитними картками. Ці атаки зазвичай скоюють працівники фінансових, бухгалтерських або керівних посад, які можуть маніпулювати записами, здійснювати несанкціоновані платежі або отримувати доступ до особистої інформації (PII). У більшості випадків цими людьми мотивує жадібність або фінансовий тиск [3, 6].

Промислове шпигунство — це несанкціонований збір та передача конфіденційної інформації організації, такої як комерційна таємниця, дані клієнтів або стратегічні плани, на користь іноземного уряду або конкуруючої організації. Шпигунство зазвичай здійснюється довіреними інсайдерами з законним доступом, такими як інженери, дослідники або керівники проектів, і може бути мотивовано ідеологією, тиском або метою отримання прибутку [3, 7].

1.2. Огляд сучасних підходів та технологій реагування на інсайдерські загрози

З огляду на таку велику кількість інструментів кібербезпеки на ринку, важко звузити їх до однієї конкретної лінії захисту та вибрати програмне забезпечення для управління внутрішніми загрозами , яке забезпечує найкращий результат з мінімальними зусиллями. Згідно зі звітом про вартість інсайдерських ризиків за 2025 рік, опублікованим Інститутом Ponemon [8], п'ятьма головними інструментами та методами, які організації використовують для управління внутрішніми ризиками, є запобігання втраті даних, навчання та обізнаність користувачів, управління привілейованим доступом (PAM), моніторинг та спостереження за співробітниками, а також управління безпекою та подіями (SIEM) [1].

Рис. 1.3. Інструменти та методи управління ризиками, пов'язаними з інцидентами внутрішньої безпеки [1, 8]

Data Loss Prevention (DLP)

Запобігання втраті даних – це рішення безпеки, яке виявляє та допомагає запобігти небезпечному або неналежному обміну, передачі чи використанню конфіденційних даних. Воно допомагає організаціям контролювати та захищати конфіденційну інформацію в локальних системах, хмарних середовищах та кінцевих пристроях. Також допомагає досягти відповідності таким нормативним актам, як «Закон про портативність та підзвітність медичного страхування» (HIPAA) та «Загальний регламент захисту персональних даних» (GDPR) [9].

User Training and Awareness (Навчання та Обізнаність Користувачів)

Це безперервний процес навчання співробітників правилам кібергігієни та політикам безпеки компанії.

Це головний захист від ненавмисних інцидентів. Регулярні тренінги, імітаційні фішингові атаки та чіткі інструкції вчать співробітників розпізнавати загрози, не переходити за підозрілими посиланнями та правильно поводитися з конфіденційною інформацією [10].

Privileged Access Management (PAM)

Керування привілейованим доступом – це рішення для захисту ідентифікаційних даних, яке допомагає захистити організації від кіберзагроз шляхом моніторингу, виявлення та запобігання несанкціонованому привілейованому доступу до критично важливих ресурсів. PAM працює через поєднання людей, процесів і технологій і надає вам уявлення про те, хто використовує привілейовані облікові записи та що вони роблять, коли ввійшли в систему. Обмеження кількості користувачів, які мають доступ до адміністративних функцій, підвищує безпеку системи, а додаткові рівні захисту зменшують ризики витоків даних з боку зловмисників [11].

PAM-системи реалізують принцип найменших привілеїв. Вони можуть видавати підвищені права лише на короткий час, вимагати додаткового схвалення для доступу та записувати всі дії, виконані під привілейованим обліковим записом. Це критично важливо для захисту від найбільш небезпечного типу інсайдерів.

Employee Monitoring and Surveillance

Моніторинг та Нагляд за Співробітниками — практика спостереження за діями співробітників на робочих комп'ютерах, включаючи моніторинг електронної пошти, відвіданих веб-сайтів, використання програм та файлових операцій [12].

Ці системи (часто у поєднанні з DLP) допомагають збирати докази та виявляти підозрілу активність у реальному часі. Наприклад, вони можуть попередити, якщо співробітник раптом починає копіювати великі обсяги даних, з якими він зазвичай не працює.

Security Incident and Event Management (SIEM)

Управління Інцидентами та Подіями Безпеки — збирають, агрегують та аналізують великі обсяги даних з програм, пристроїв, серверів та користувачів усієї організації в режимі реального часу. Об'єднуючи цей величезний масив даних в

єдину уніфіковану платформу, рішення SIEM забезпечують комплексне уявлення про стан безпеки організації, надаючи центрам операцій безпеки (SOC) можливість швидко та ефективно виявляти, розслідувати та реагувати на інциденти безпеки [13].

User Behavior Analytics (UBA)

Аналіз поведінки користувачів – це практика збору та аналізу даних про активність користувачів для створення базової лінії їхніх звичайних моделей поведінки та уподобань. Розробляючи ці базові лінії для кожного користувача та відстежуючи його активність у режимі реального часу, UBA допомагає організаціям виявляти порушення. Коли виникає підозріла поведінка, команди можуть ідентифікувати потенційні загрози безпеці, спроби несанкціонованого доступу та витоки даних [14].

Це більш просунутий метод, який використовує машинне навчання для створення «базового профілю» (baseline) нормальної поведінки для кожного користувача.

Threat Intelligence Sharing (Обмін Інформацією про Загрози)

Обмін інформацією про загрози – це спільний процес, який дозволяє організаціям обмінюватися інформацією, такою як індикатори компрометації (IoC), тактики, методи та процедури (TTP), а також вразливості між собою. Він включає збір інформації про загрози з різних джерел, таких як внутрішні мережеві журнали, інструменти безпеки, розвідка з відкритим кодом (OSINT), комерційні канали інформації про загрози та галузеві спільноти обміну інформацією, такі як Центри обміну та аналізу інформації (ISAC) [15].

Incident Response Management

Управління Реагуванням на Інциденти – це систематична стратегія, яка дозволяє організації реагувати на інциденти кібербезпеки та порушення безпеки. Метою реагування на інциденти є виявлення реальних інцидентів безпеки, контроль над ситуацією, обмеження шкоди, завданої зловмисником, а також скорочення часу та витрат на відновлення [16].

Управління реагуванням на інциденти зазвичай включає офіційну документацію, що описує процедури реагування на інциденти. Ці процедури повинні охоплювати весь процес реагування на інциденти, включаючи підготовку, виявлення, аналіз, локалізацію та ліквідацію наслідків після інциденту. Дотримуючись цих процедур, організації можуть обмежити збитки, запобігти подальшим втратам та дотримуватися чинних норм відповідності [16].

Network Traffic Intelligence (NTA)

Аналіз Мережевого Трафіку – це систематичний процес захоплення, моніторингу та інтерпретації мережевого зв'язку для виявлення аномалій, загроз та оптимізації продуктивності. Він виходить далеко за рамки простих перевірок статусу «вгору/вниз» або перехоплення пакетів.

Замість того, щоб перевіряти кожен пакет, аналіз мережевого трафіку зосереджується на метаданих, таких як IP-адреси, порти, протоколи та обсяг трафіку, а також використовує аналітику та машинне навчання для виявлення незвичайних закономірностей [17].

Strict Third-Party Vetting Procedures

Суворі Процедури Перевірки Третіх Сторін — це процес ретельної перевірки та управління ризиками, пов'язаними з підрядниками, партнерами та постачальниками, які мають доступ до ваших систем.

Це прямий захист від загрози "Третіх сторін". Він включає перевірку безпеки підрядника, підписання угод про нерозголошення (NDA) та надання їм лише мінімально необхідного доступу на строго обмежений час [18].

1.3. Аналіз існуючих рішень UAM та їх порівняльна характеристика

User Activity Monitoring (UAM). Моніторинг Активності Користувачів — це процес збору, аналізу та звітування про дії користувачів у корпоративній мережі та на кінцевих точках (комп'ютерах, серверах). Це технологія, що дозволяє відділам безпеки та IT бачити, що саме роблять співробітники, які мають легітимний доступ.

Ключові завдання UAM:

Виявлення інсайдерських загроз: Моніторинг нетипової поведінки, що може вказувати на крадіжку даних або саботаж.

Розслідування інцидентів: Надання детальних доказів (аж до відеозапису екрана) того, що сталося до, під час і після інциденту.

Забезпечення комплаєнсу (Compliance): Демонстрація аудиторам (наприклад, для PCI DSS або GDPR), що доступ до чутливих даних контролюється.

Ринок UAM є різноманітним. Деякі рішення зосереджені виключно на безпеці, інші — на продуктивності співробітників.

Таблиця 1.1.

Порівняльна характеристика UAM рішень

Критерій	Proofpoint (ObserveIT)	Teramind	Forcepoint	Syteca (Ekran System)	ActivTrak
Основний фокус	Безпека (Insider Threat)	Безпека + Продуктивність	Безпека (Data-First)	Безпека + Продуктивність (Insider Risk, PAM + UAM)	Продуктивність (Workforce Analytics)
Моніторинг екрана	Так	Так.	Так	Так	Так.
Моніторинг клавіатури	Ні	Так (Повний).	Так (Частково).	Так (Повний)..	Ні.
Аналітика (UBA)	Висока..	Середня/Висока.	Дуже висока..	Висока.	Низька
Блокування дій (DLP)	Обмежено. Фокус на виявленні.	Так	Так.	Так	Ні.
Розгортання	Хмара / Локальне	Хмара / Локальне	Хмара / Локальне	Хмара / Локальне	Хмара (SaaS)

Висновки до розділу 1

Отже, у розділі було проведено комплексний аналіз проблеми інцидентів внутрішньої інформаційної безпеки та засобів реагування на них, а саме: приведено класифікацію інцидентів внутрішньої безпеки; розглянуто сучасні підходи та технології реагування на дані порушення; проаналізовано існуючі рішення UAM та приведена порівняльна характеристика в таблиці 1.3.

2 ДОСЛІДЖЕННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ UAM SYTECA

2.1. Архітектура системи UAM Syteca та її компоненти

Завдяки UAM організації отримують повну прозорість у тому, як саме користувачі взаємодіють із критичними системами та даними, що дозволяє оперативно реагувати на інциденти. Одним із таких потужних інструментів є Syteca, яка забезпечує глибокий аналіз поведінки користувачів у корпоративному середовищі. Ця система дозволяє виявляти потенційно небезпечну активність у реальному часі та створювати детальні звіти для подальшого розслідування інцидентів.

Комбінуючи різні типи клієнтів Syteca, захищає та підвищує видимість кожної частини конкретної IT-інфраструктури. Для великих розгортань команда Syteca забезпечує високу доступність і аварійне відновлення для покращення стабільності системи для задоволення вимог сегментації та ізоляції даних [19-22].

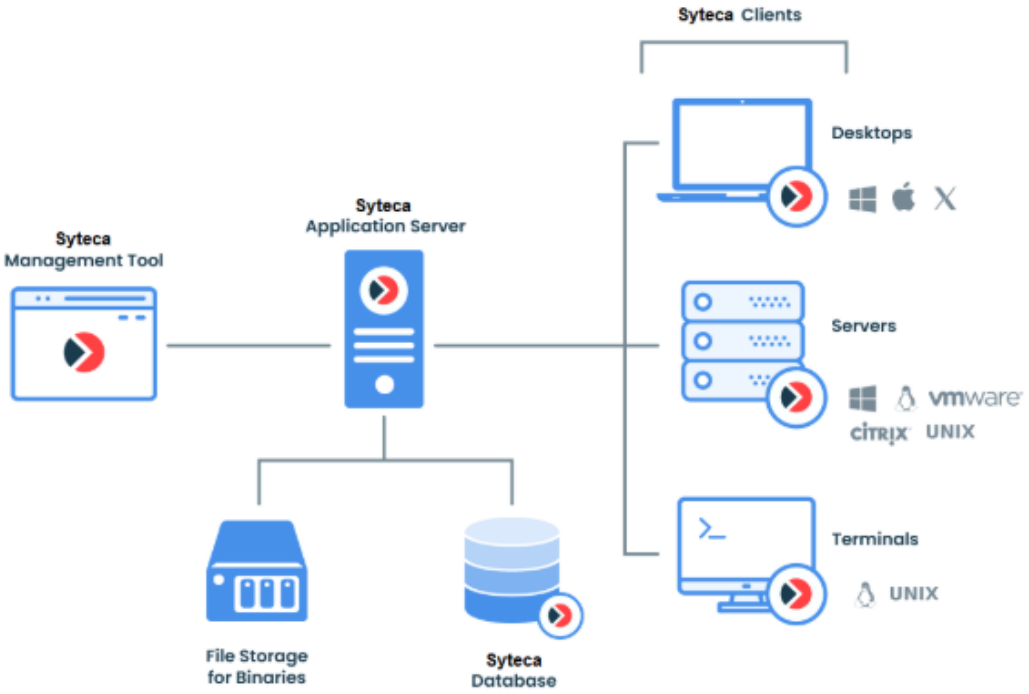

Рис. 2.1. Базова схема розгортання [20]

Завдяки такому розгортанню (рис. 2.1) досягається максимальна видимість та контроль будь-якої діяльності, що виконується в інфраструктурі, встановивши клієнт відповідного типу на кожну кінцеву точку.

В основі ефективності Syteca лежить комплексний підхід, що поєднує моніторинг, аналітику та контроль дій користувачів. Розглянемо ключові можливості платформи [19-22].

1. Низькорівневе логування подій.

Агент системи фіксує широкий спектр подій, що включає: 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 журнал 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, а саме: 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 і застосовує певні дії згідно налаштованих політик: сповіщення (email, Telegram, Slack тощо); блокування сесії користувача; ізоляція ПК від мережі; запуск скриптів для локального реагування.

Це забезпечує як пасивний нагляд, так і активну протидію загрозам у реальному часі.

6. Формування звітів та експорт даних.

Для звітування та подальшого аналізу доступні шаблони звітів (інциденти, активність користувачів, порушення політик). Можливість експортувати дані у PDF, XLSX, CSV та відеоформати. Підтримує збереження даних для цифрової експертизи (форензики) [19-22].

Основні компоненти системи

Система включає наступні основні програмні компоненти:

— Syteca Application Server (не доступний в SAAS): 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).

— 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..

— Syteca Clients, що встановлюються на кінцевих точках:

- Клієнти Syteca для Windows;
- Клієнти Syteca macOS;
- Клієнти Syteca Linux/Unix;

- Syteca Tray Notifications (не доступне в SAAS).

Додаткові компоненти системи

— Syteca Master Panel: 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) та інших даних між ними.

2.2. Механізми моніторингу, збору та аналізу подій у Syteca

Платформа Syteca використовує комплексний, агент-орієнтований підхід для забезпечення моніторингу, збору та аналізу активності користувачів. Процес можна розділити на три основні етапи.

1. Механізми моніторингу та збору подій.

Основою системи є легкі агенти (agents), які встановлюються безпосередньо на кінцеві точки (endpoints), що підлягають моніторингу:

— робочі станції (Windows, macOS, Linux);

— сервери (Windows, Linux);

— сервери термінального доступу (Citrix, VMware Horizon).

Для систем, де встановлення агентів неможливе або небажане (наприклад, мережеве обладнання), Syteca використовує проксі-сервер або Jump Server для моніторингу сесій, що проходять крізь нього [19-22].

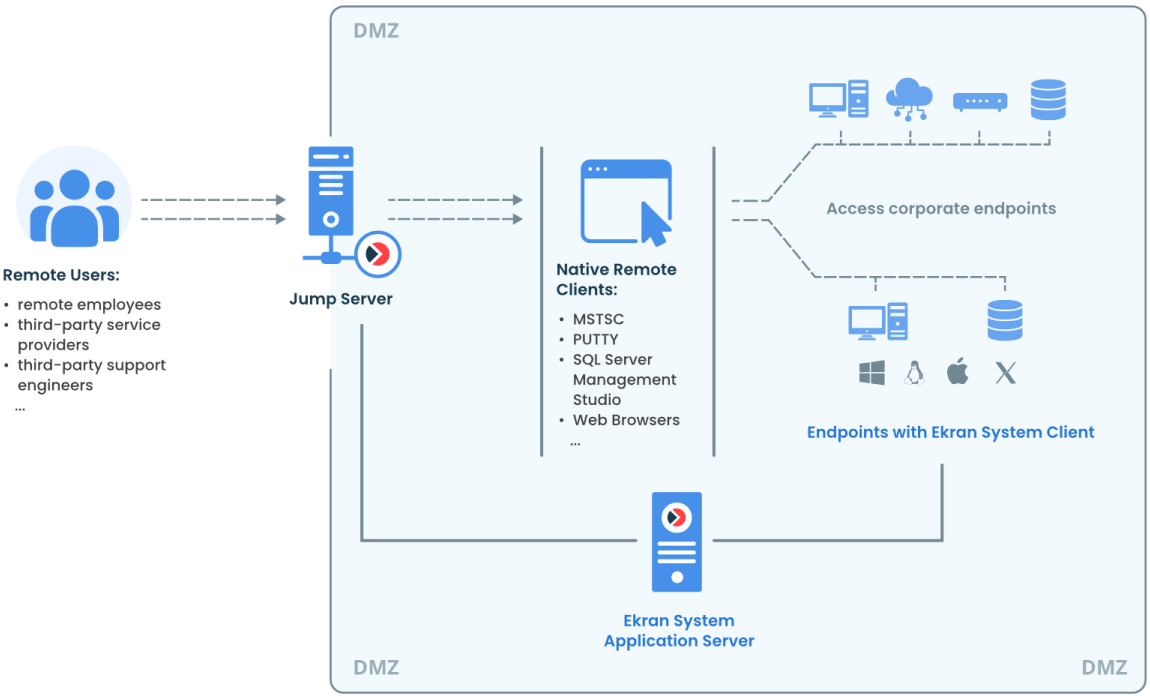

Рис. 2.2. Розгортання сервера Jump

Агенти збирають:

Відеозапис сесій: Syteca записує активність екрана користувача у форматі індексованого відео. Це головна особливість де кожна дія користувача (клік миші, відкриття вікна) прив'язується до таймкоду на відео.

Метадані сесій: разом з відео збирається текстовий контекст:

Натискання клавіш (Keystrokes): фіксуються всі натиснуті клавіші, включаючи буфер обміну (copy-paste).

Запущені програми: Ім'я процесу (наприклад, chrome.exe) та заголовок вікна ("Gmail - Новий лист").

Відвідані URL: запис усіх веб-сайтів, які відвідує користувач.

Підключені пристрої: моніторинг та ідентифікація USB-пристроїв (флешки, зовнішні диски) [19-22].

Файлові операції: відстеження доступу, створення, зміни чи видалення файлів (особливо на мережевих дисках).

2. Механізми аналізу подій.

Зібрані дані передаються на центральний сервер Syteca, де вони обробляються та аналізуються в реальному часі та для подальшого розслідування.

Базовий рівень аналізу, що базується на заздалегідь налаштованих правилах безпеки, тобто аналізу у реальному часі. Система перевіряє потік подій (метаданих) на відповідність правилам і при порушенні видає сповіщення (Alerts).

Наступним механізмом є поведінковий аналіз (UBA) — механізм, що використовує машинне навчання для виявлення аномалій.

3. Механізм реакції додатково до механізму аналізу.

На основі аналізу Syteca може не лише сповіщати, але й активно реагувати на сповіщення, а саме:

Блокування сесії: примусове завершення сесії користувача при виявленні критичної загрози.

Блокування пристроїв/процесів: автоматичне блокування USB-порту або "kill" неавторизованого процесу.

Попереджувальні повідомлення: виведення на екран користувача повідомлення ("Ви намагаєтеся отримати доступ до конфіденційного файлу. Ця дія записується.") [19-22].

2.3. Інтеграція Syteca з іншими системами кібербезпеки підприємства

Syteca інтегрована та може бути налаштована для роботи з широким спектром сторонніх продуктів, інструментів та послуг, таких як постачальники SSO та SIEM-системи тощо.

Syteca також надає розробникам комплект розробки програмного забезпечення (SDK) , включаючи API та інші інструменти для інтеграції з інформаційними системами клієнтів.

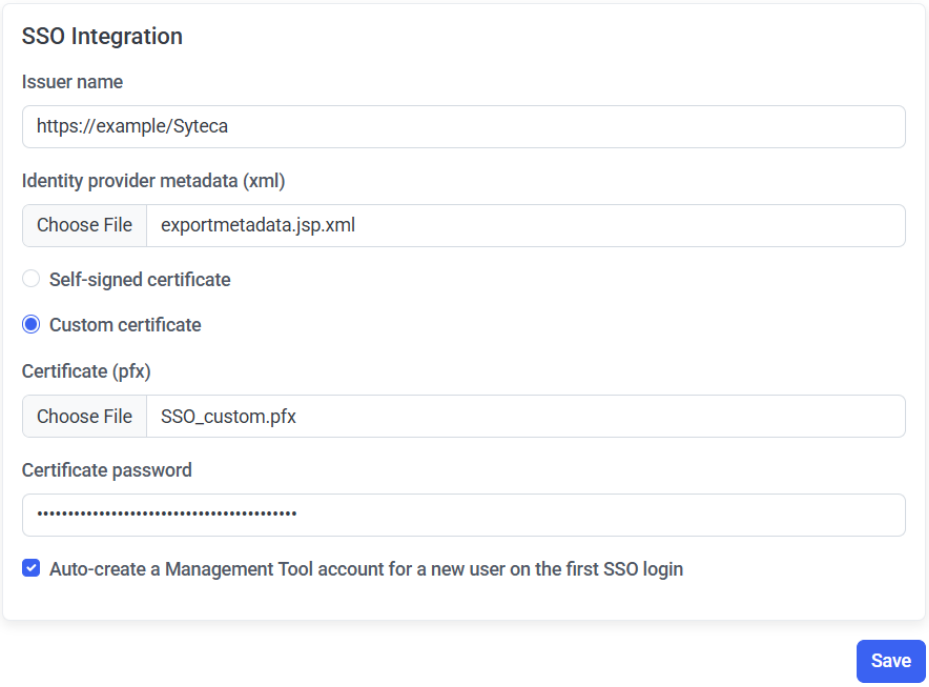

Рис. 2.3. Інтеграція Syteca з SSO [23]

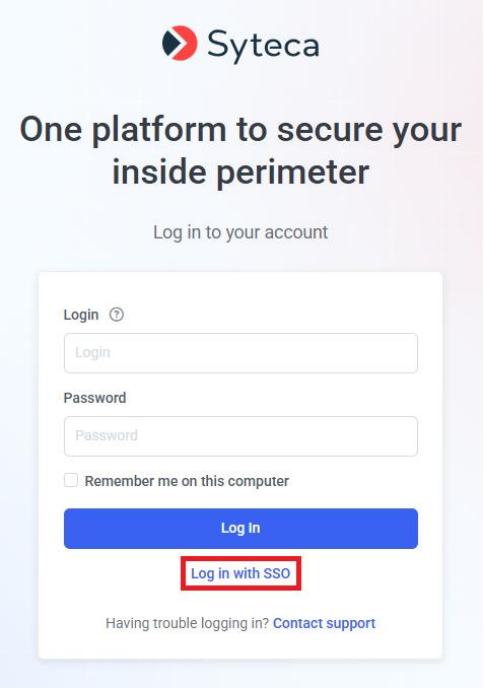

Рис. 2.4. Вікно після інтеграції SSO [23]

Інтеграція Syteca із засобом запуску програм Venn рис. 2.5, що дозволяє відстежувати лише активність користувачів у програмах, відкритих у робочому просторі Venn на клієнтських комп’ютерах Windows та macOS.

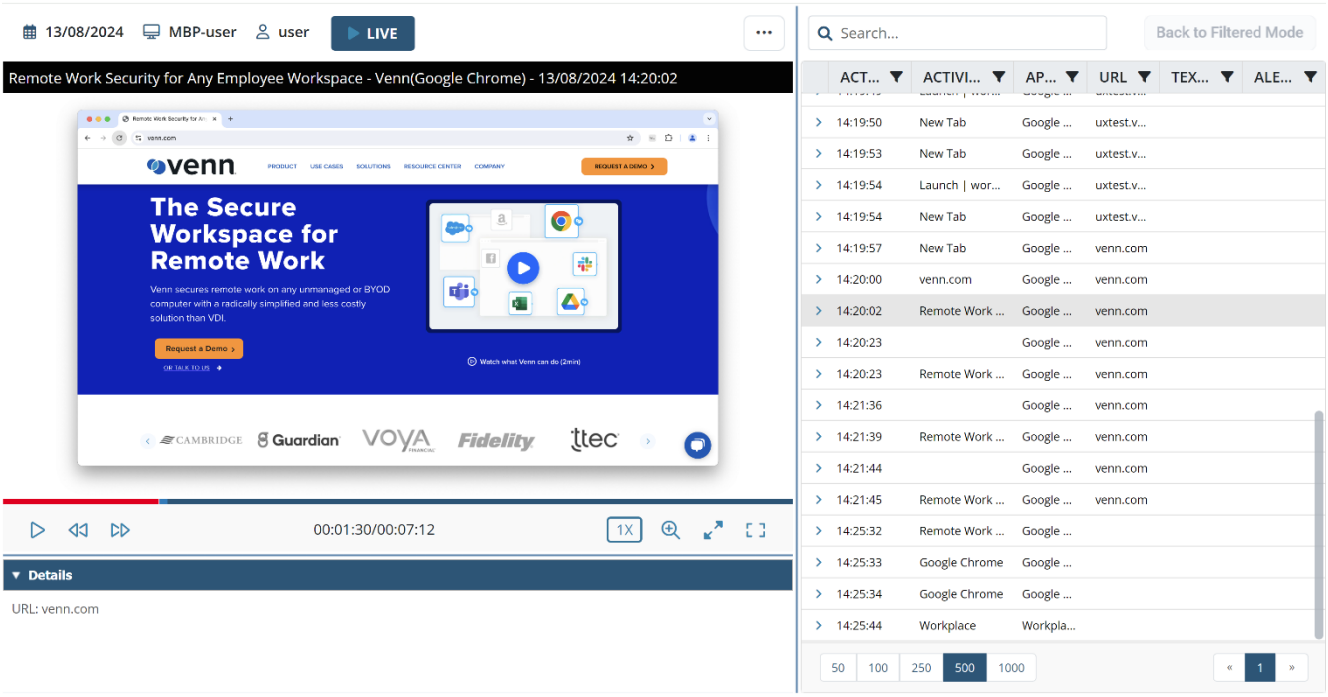

Рис. 2.5. Інтеграція з Venn

Venn — безпечний робочий простір для віддаленої роботи.

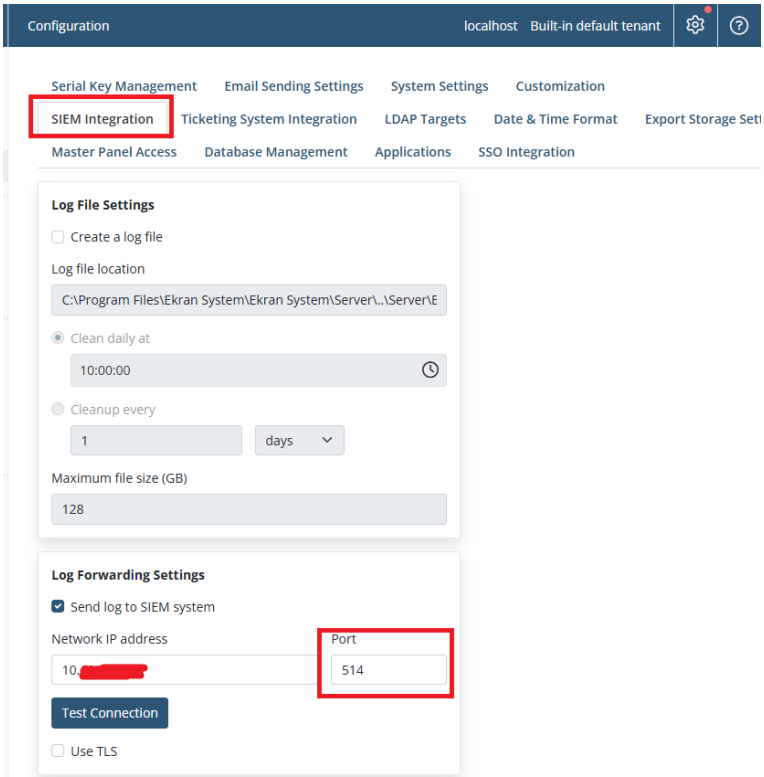

Рис. 2.6. Інтеграція з SIEM IBMQRadar

Таким чином, Syteca UAM як комплексне рішення рис. 2.7, яке не лише відстежує активність, але й виявляє загрози, автоматично реагує на них та надає інструменти для подальшого розслідування й аналізу продуктивності.

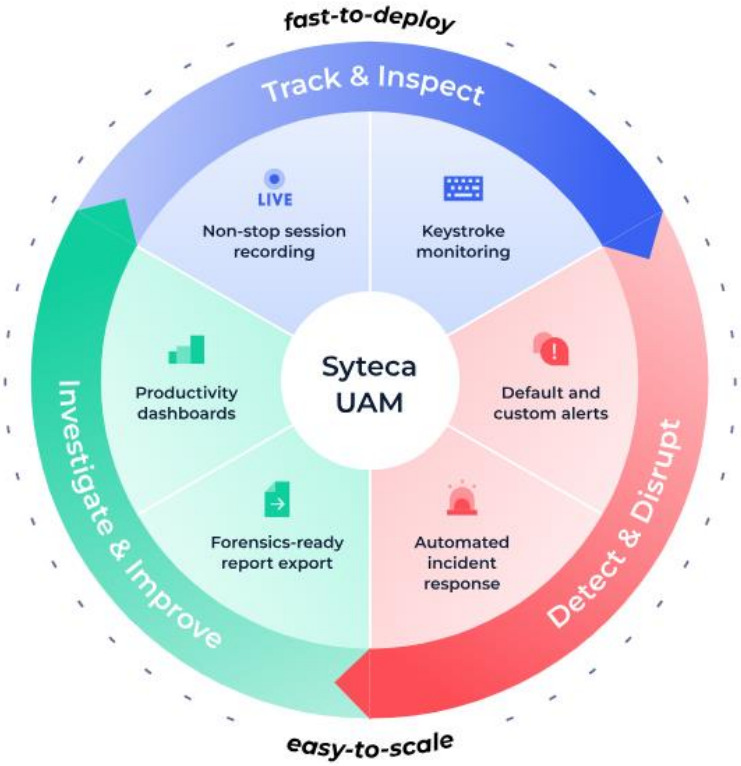

Рис. 2.7. Функціональний цикл Syteca

Отже, UAM Syteca підтримує взаємодію з іншими рішеннями у сфері кібербезпеки, такими як SIEM, DLP, IAM та SOC-платформи. Це забезпечує комплексний підхід до захисту даних і дозволяє об’єднати події з різних джерел у єдину систему моніторингу.

Висновки до розділу 2

У розділі було досліджено функціональні можливості UAM Syteca, приведена архітектура з основними компонентами системи. Реалізовано приклади інтеграції з різними системами та описані механізми моніторингу, збору та аналізу подій.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ РЕАГУВАННЯ НА ІНЦИДЕНТИ ВНУТРІШНЬОЇ БЕЗПЕКИ НА БАЗІ UAM SYTECA

3.1. Розгортання та налаштування UAM Syteca

Встановлення системи інтуїтивно зрозуміле для користувачів і тим паче для адміністраторів.

В першу чергу необхідно задовольнити умови для встановлення сервера застосунків, а саме [24]:

1. Встановлення бази даних.

Syteca підтримує два типи баз даних:

• PostgreSQL.

• MS SQL.

2. Встановлення .NET Framework

.NET Framework 4.8 включено до складу Windows 10 (версія 1903).

Наступним кроком запуск Installation Wizard (рис. 3.1.), прийняти ліцензійні умови користування і слідувати крокам встановлення.

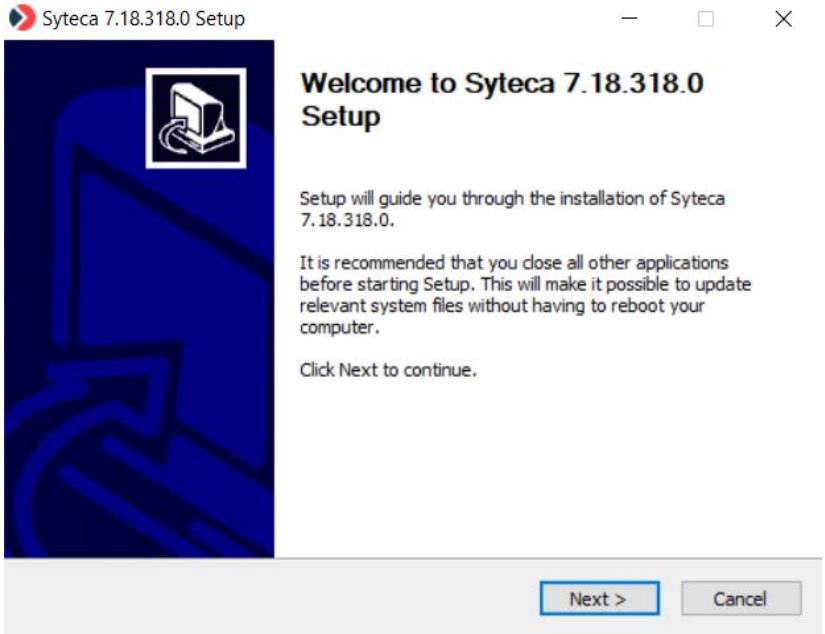

Рис. 3.1. Installation Wizard

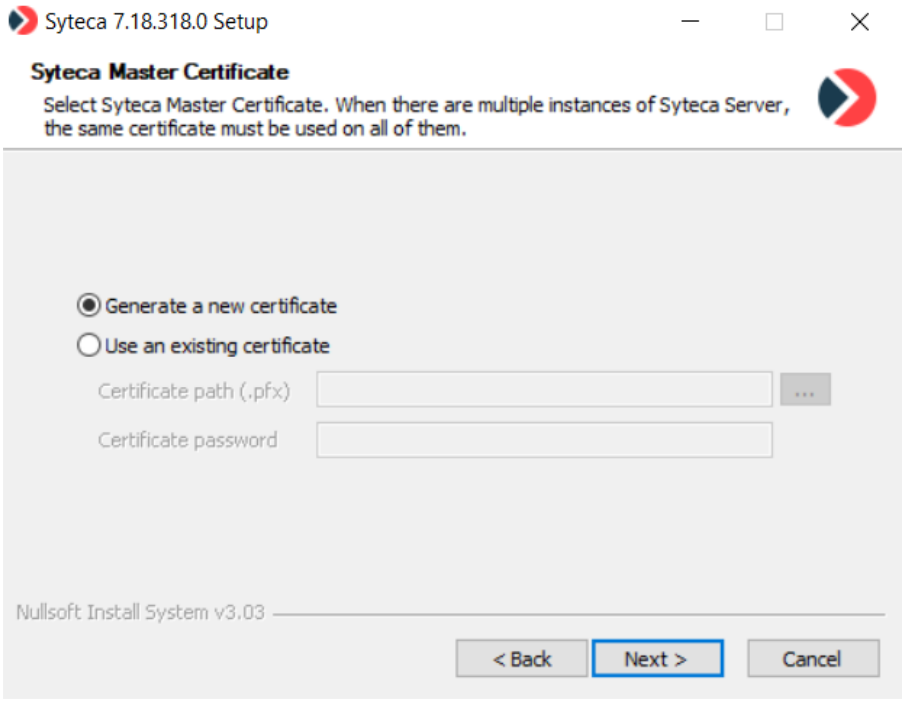

Рис. 3.2. Генерація сертифікату

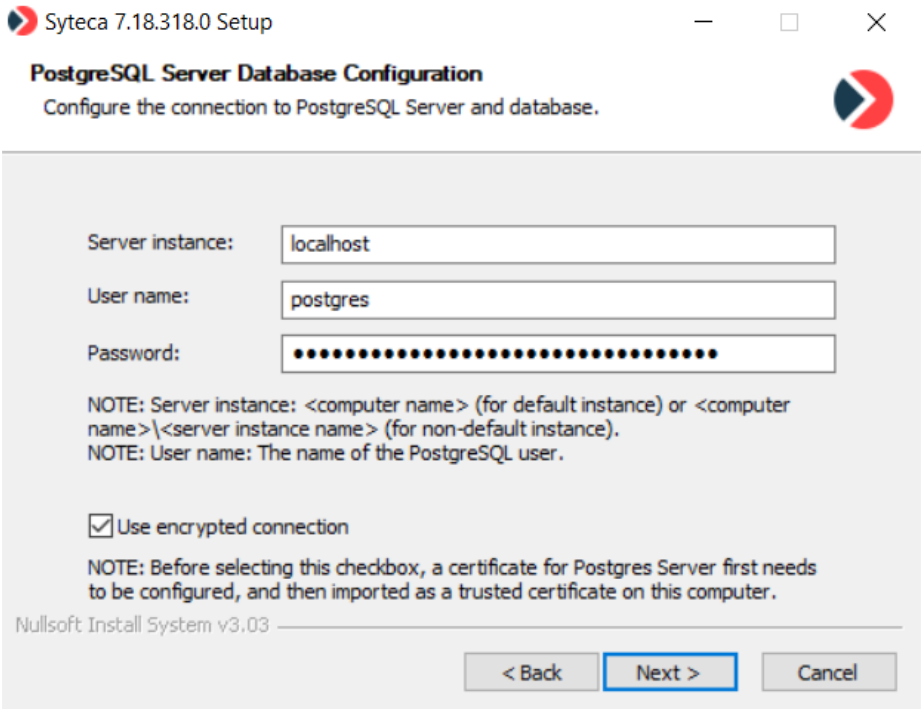

Рис. 3.3. Підключення до БД

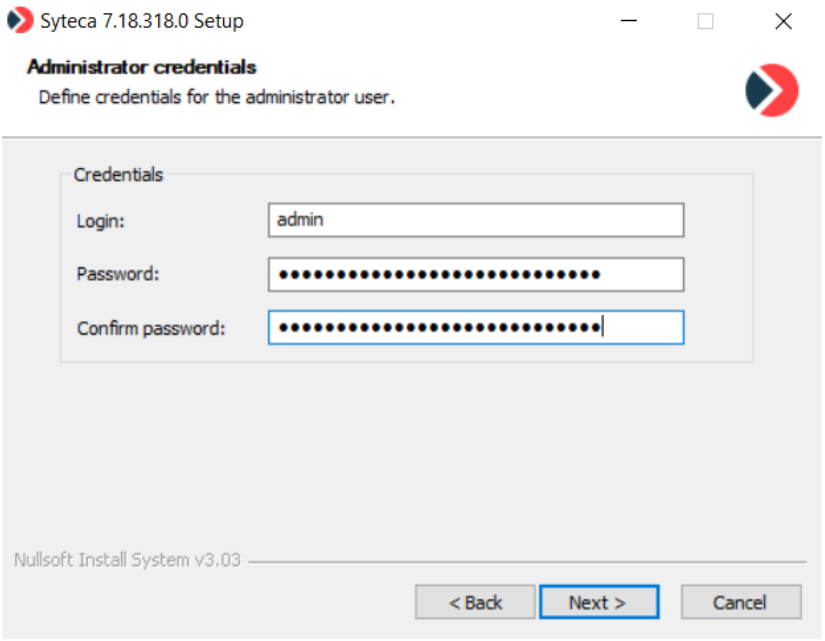

Рис. 3.4. Створення admin користувача

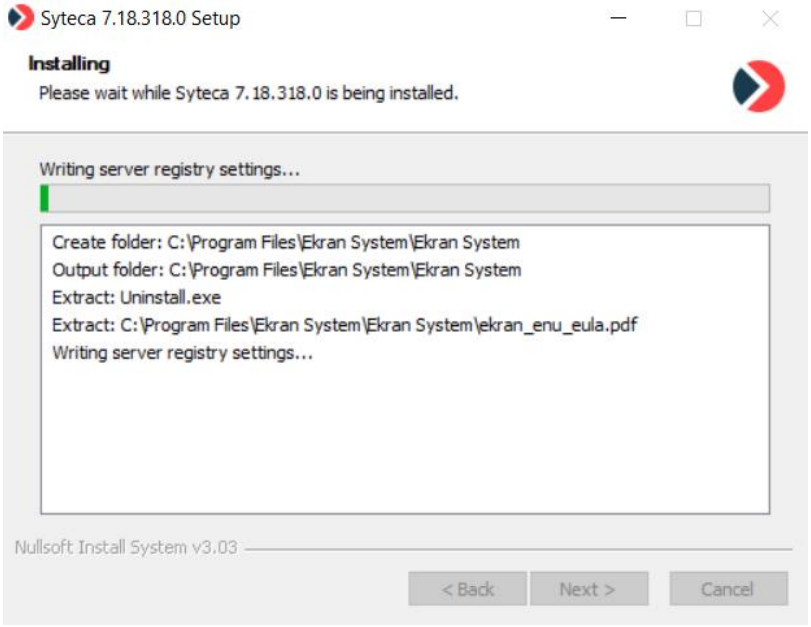

Рис. 3.5. Процес встановлення

Наступним етапом необхідні умови для встановлення засобу керування це увімкнення служби IIS та створення довіреного самопідписаного сертифіката та його експорт [24].

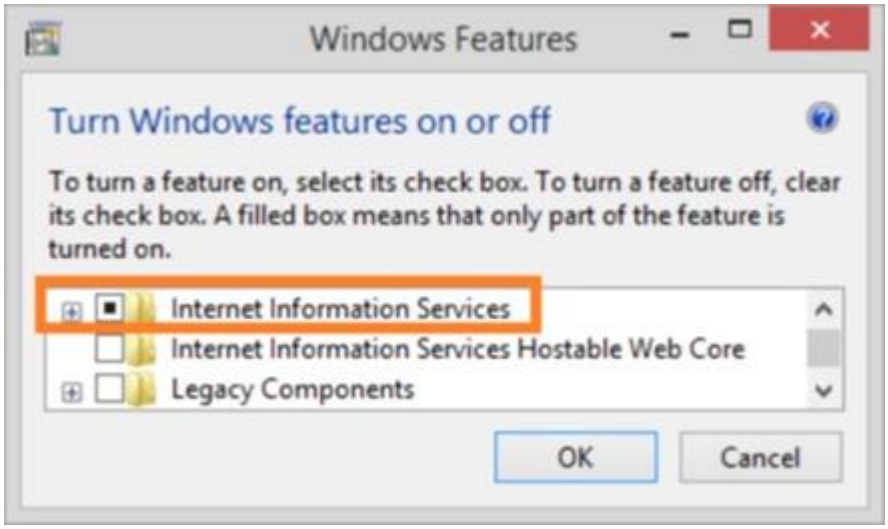

Рис. 3.6. Увімкнення служби IIS

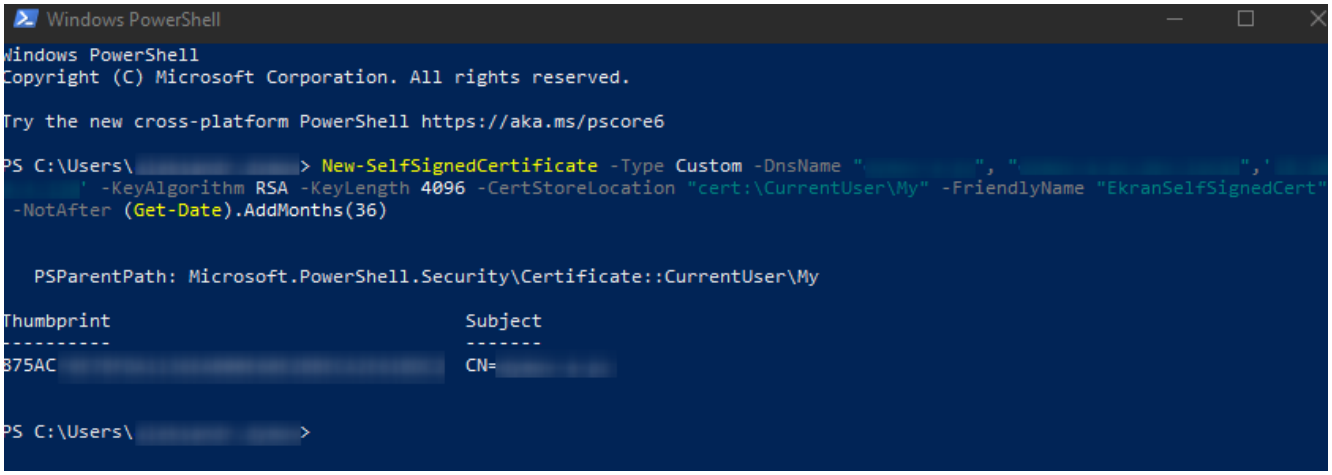

Рис. 3.7. Створення довіреного самопідписаного сертифіката

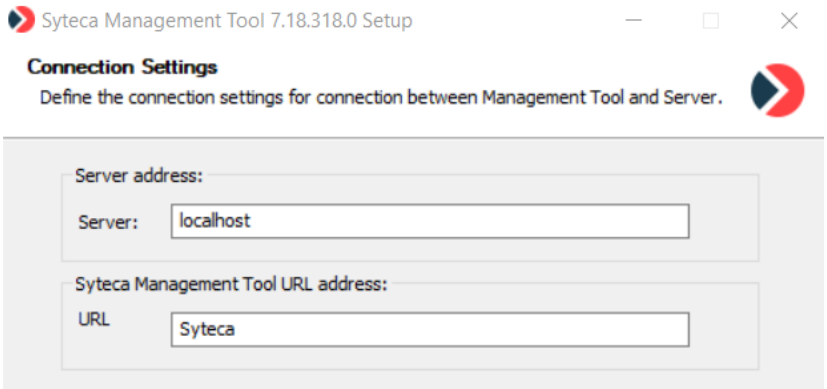

Рис. 3.8. Встановлення інструменту керування

У полі URL-адреси введіть назву папки, де потрібно розмістити Інструмент керування в IIS (назва за замовчуванням — Syteca , і ця назва папки буде

частиною URL-адреси, яка використовується для відкриття Інструмента керування) [24].

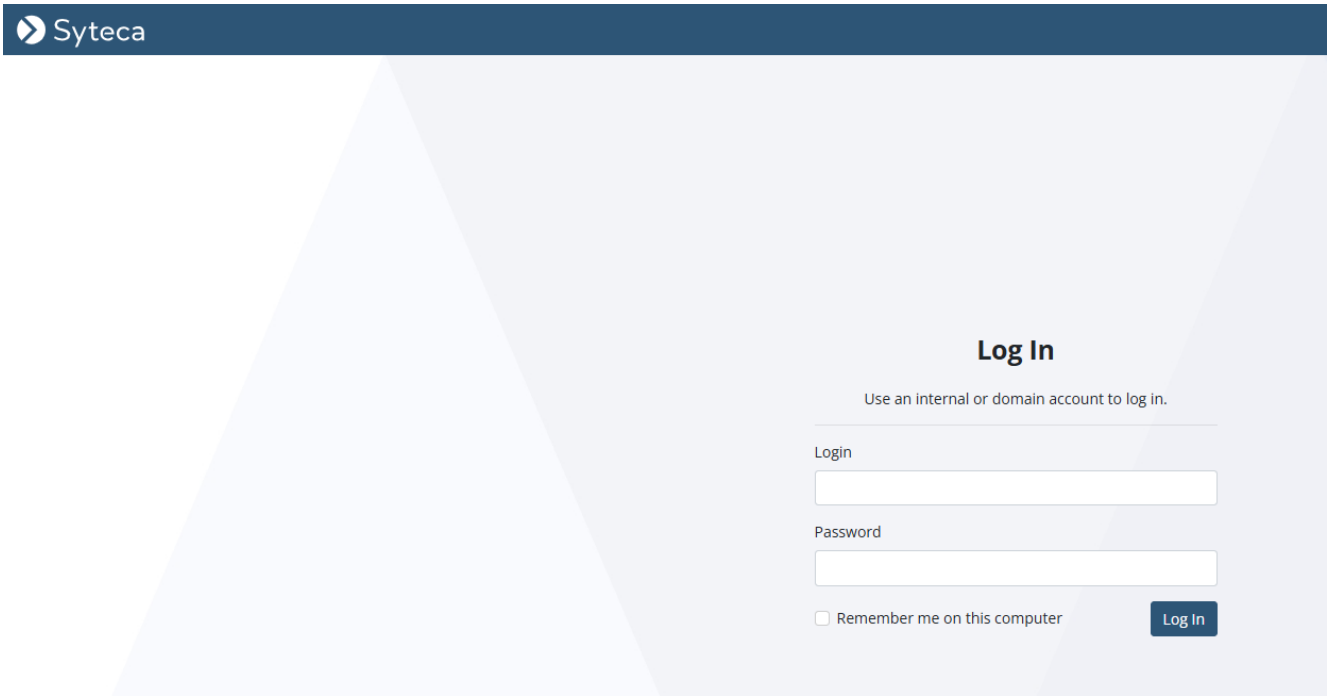

Рис. 3.9. Syteca Management Tool

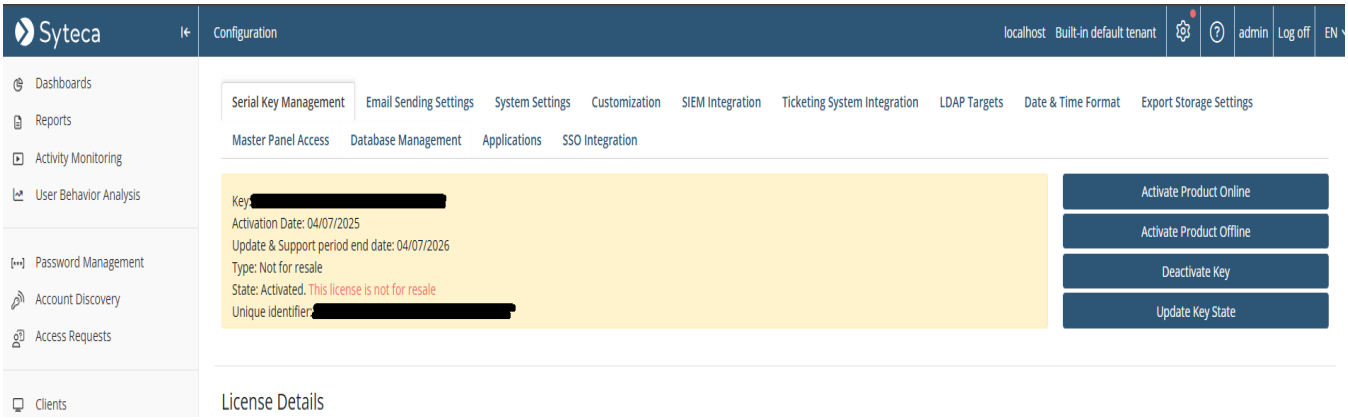

Рис. 3.10. Налаштування, доступні для адміністратора

Адміністративні налаштування складаються:

- параметрів надсилання електронної пошти;
- системні налаштування;
- параметри налаштування;
- інтеграція SIEM;

- параметри інтеграції системи обробки тікетів;
- об'єкти LDAP;
- формат дати та часу;
- параметри сховища експорту;
- параметри керування базою даних;
- доступ до майстер панелі;
- додатки;
- інтеграція SSO.

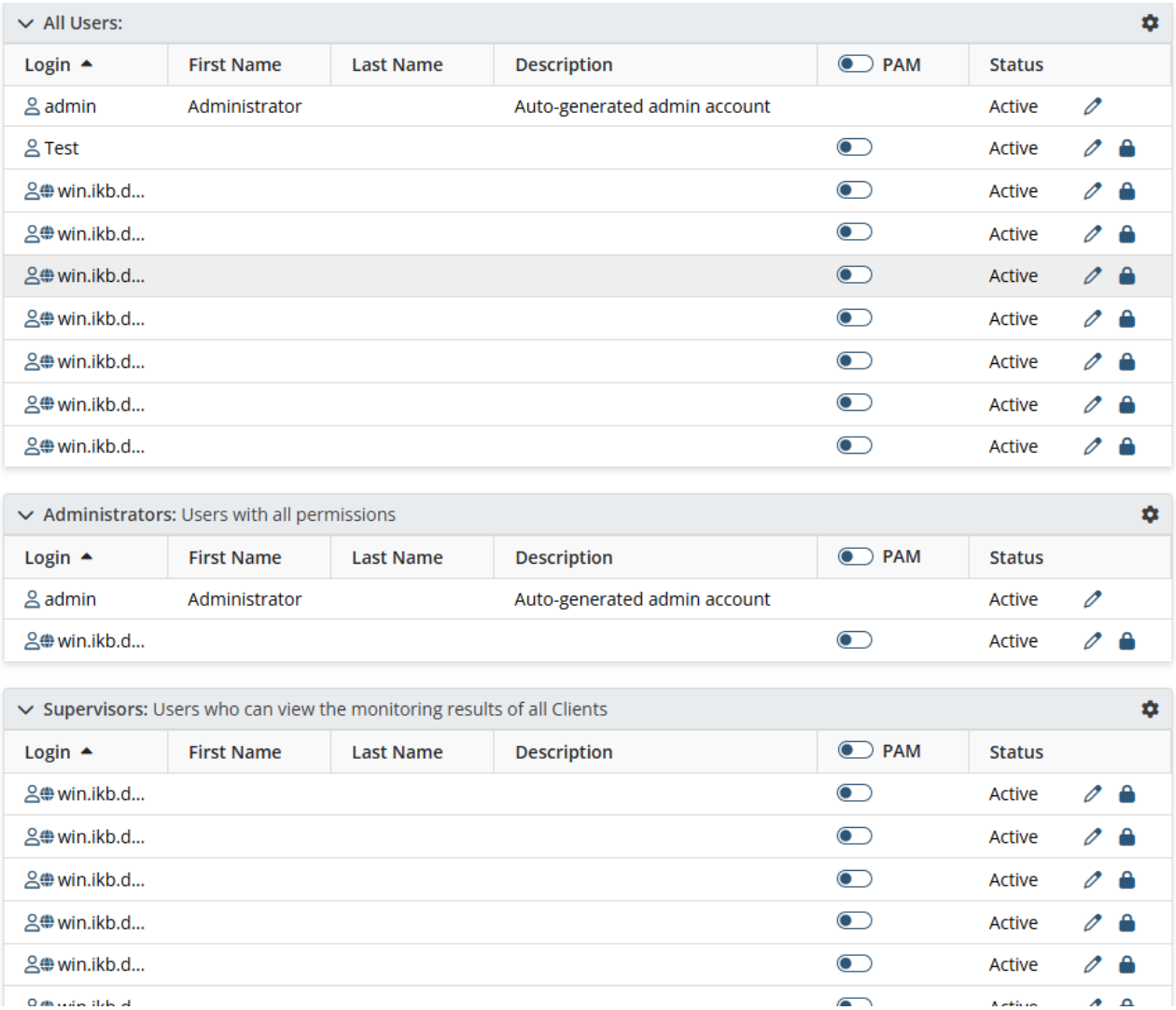

Рис. 3.11. Налаштування груп користувачів

У системі є кілька груп користувачів за замовчуванням, зокрема [24]:

• Усі користувачі: група користувачів, яка містить усіх створених користувачів.

• Адміністратори: група користувачів, які можуть виконувати адміністративні функції в системі. Якщо користувача додано до цієї групи, він матиме всі адміністративні та клієнтські дозволи для системи.

• Керівники: група користувачів, чиїм завданням є виконання основної слідчої роботи шляхом аналізу Клієнтів. Якщо користувача додано до цієї групи, він матиме дозвіл на перегляд результатів моніторингу для всіх Клієнтів.

• Користувачі PAM: група користувачів, які не мають дозволу на доступ до Інструмента керування.

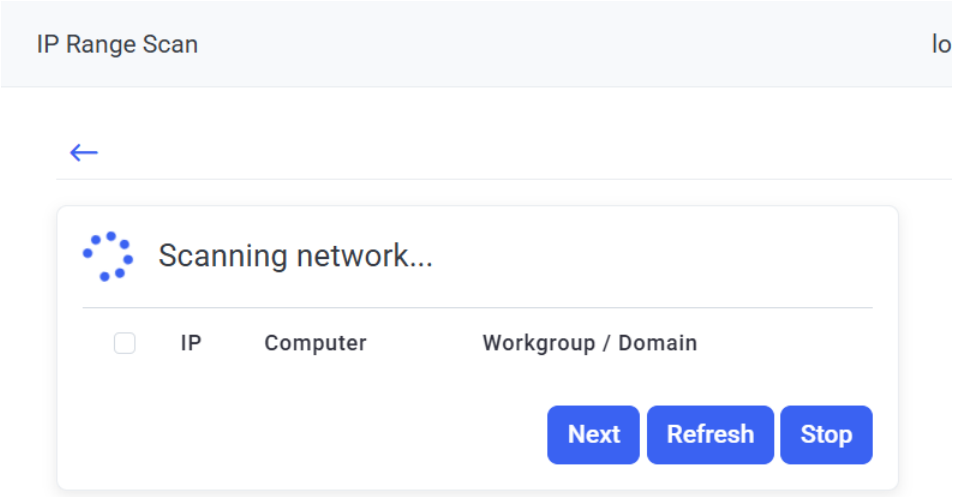

Рис. 3.12. Сканування мережі для встановлення клієнтів

Рис. 3.13. Вибираємо клієнтів на які буде встановлено клієнтську частину

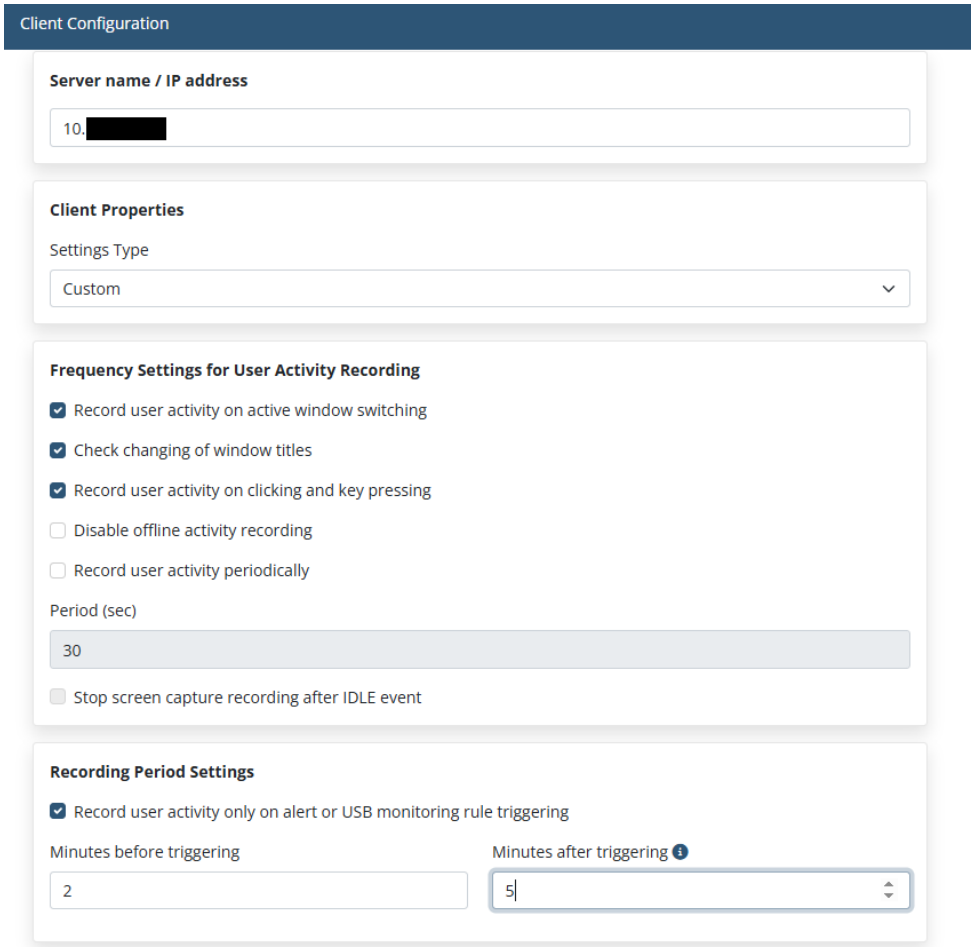

Рис. 3.14. Конфігурація клієнтів

Конфігурація клієнтів включає:

- IP адресу/Ім’я сервера до якого буде застосовуватися конфігурація попереджень;

- тип налаштування (Custom налаштування одного клієнта, застосування для всіх клієнтів або до конкретної групи клієнтів);

- налаштування частоти запису (Record user activity on active window switching – записувати активність при перемиканні вікон; Check changing of window titles – відстежувати зміну заголовків вікон; Record user activity on clicking and key pressing – фіксувати натискання клавіш; Disable offline activity recording – вимкнути запис офлайн-активності; Record user activity periodically – записувати активність періодично, Period (sec) інтервал періодичного запису; Stop screen capture recording after IDLE event – зупинити запис після IDLE (бездіяльності системи) події.

Комп'ютер	Робоча група \ Домен	Стан	Деталі
421-10	WIN	В процесі...	
421-03	WIN	В процесі...	
421-02	WIN	В процесі...	
421-21	WIN	В процесі...	
421-17	WIN	В процесі...	
421-18	WIN	В процесі...	
421-01	WIN	В процесі...	

Рис. 3.15. Віддалене встановлення клієнтів

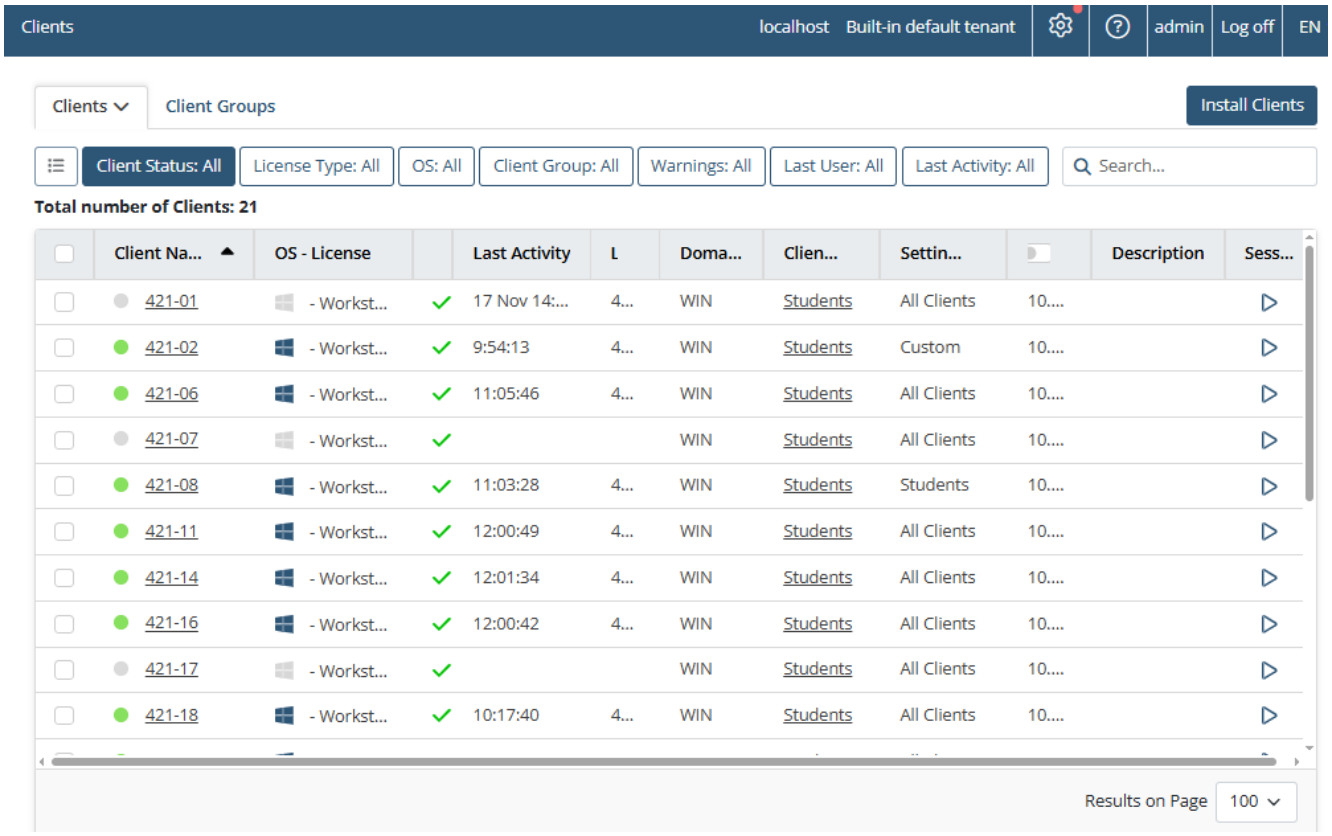

Рис. 3.16. Панель керування клієнтами

Панель керування містить список клієнтських пристроїв. Для кожного запису відображені поля, зокрема:

Client Name — ім’я клієнта;

OS – License — піктограми операційної системи (Windows) та активована ліцензія;

Last Activity — час останньої активності, наприклад;

Domain — до якого домену належить;

Client Group — до якої групи користувачів відносяться;

Settings —профіль налаштування;

IP-адреси;

Description - опис і Session відкриття сесії/деталей.

Біля кожного клієнта є індикатор стану: зелені кола — активні/онлайн. Сірі — неактивні/офлайн.

[Default] Running a cloud backup application	This is an alert on running a cloud backup software that can copy files/folders to a remote location.	Enabled	None
[Default] Running CD or DVD burning tools	This is an alert on running a CD/DVD burning software.	Enabled	None
[Default] Synchronizing MS-Office document with another Microsoft account	This is an alert on opening the Switch Account window in Microsoft Office applications.	Enabled	None
[Default] Running steganography tools	This is an alert on running one of the predefined stenography tools that are usually used to conceal text information within images.	Enabled	None
[Default] Password protecting Excel file	This is an alert on opening the General Options screen in Microsoft Excel to potentially set a password protection upon saving a file.	Enabled	None
[Default] Password protecting Word file	This is an alert on opening the General Options screen in Microsoft Word to potentially set a password protection upon saving a file.	Enabled	None

Рис. 3.17. Застосування попереджень до кінцевих точок

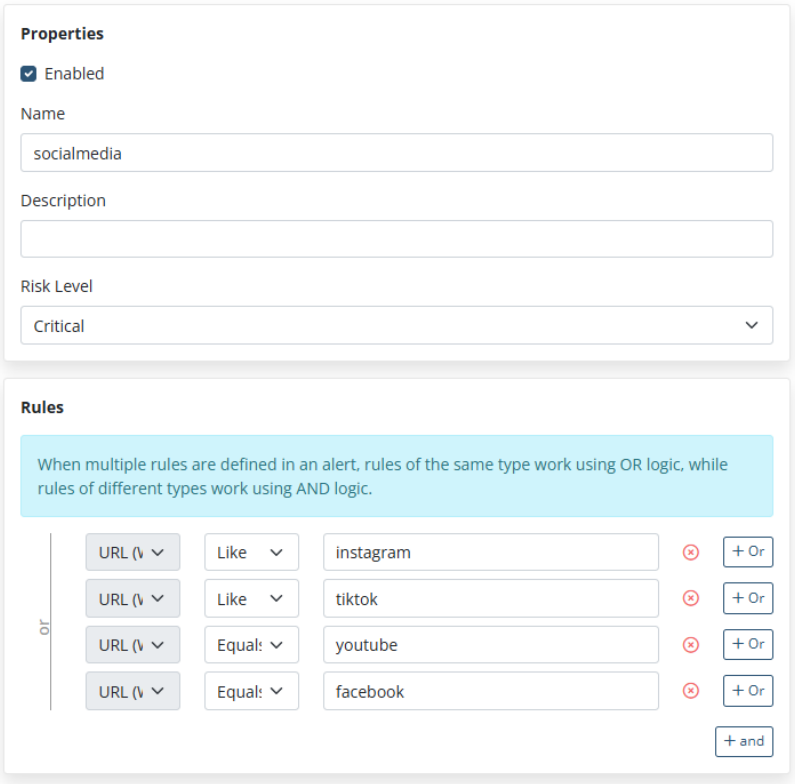

Рис. 3.18. Створення нових попереджень

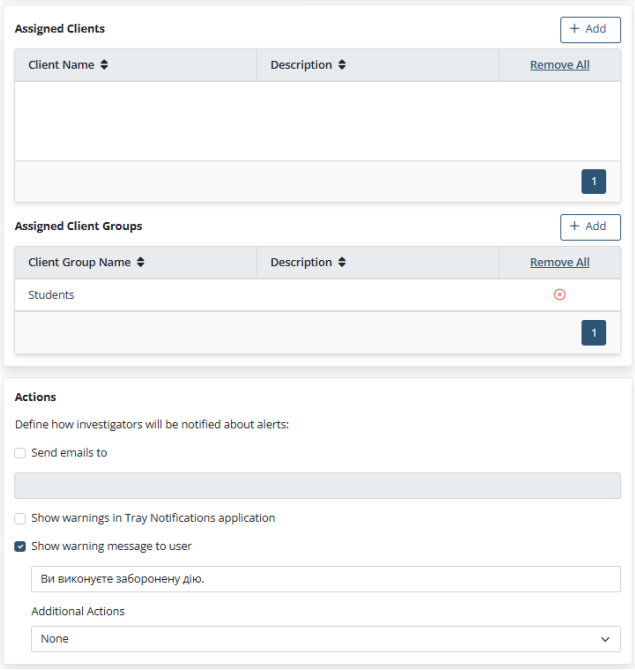

Рис. 3.19. Створення нових попереджень

Створення нових попереджень включає [24]:

- властивості, які містять активність правила; назву; опис; рівень ризику;

- логіку спрацювання правила «Коли в одному алерті визначено декілька правил, правила одного типу працюють за логікою АБО (OR), тоді як правила різних типів працюють за логікою І (AND)»

- застосування правила до окремого клієнта або до групи;

- дії при спрацюванні попередження.

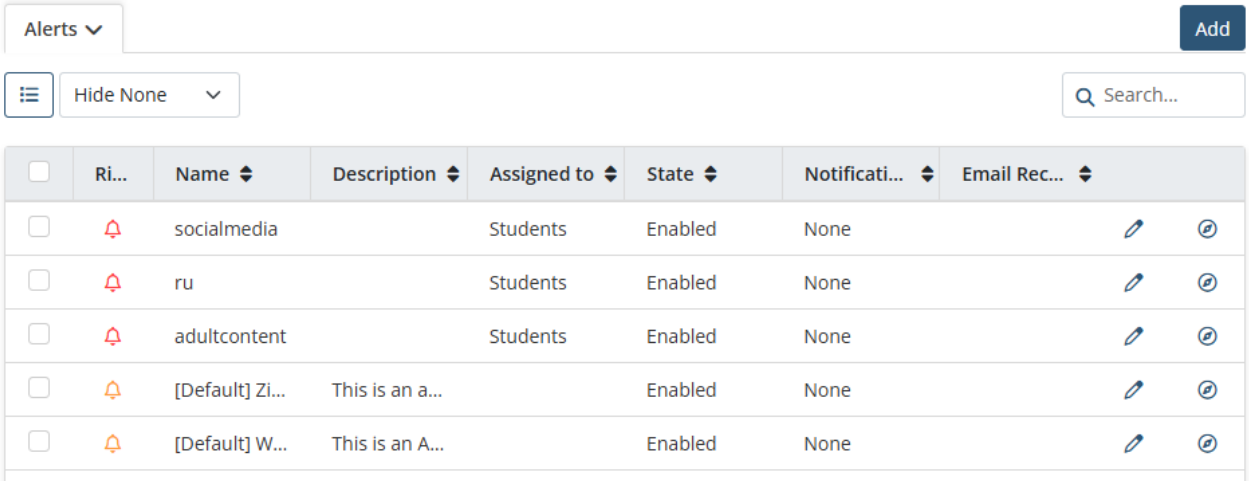

Рис. 3.20. Вікно застосованих правил попереджень

Вікно застосованих правил попереджень дозволяє переглянути створені правила, визначити їх активність, до яких клієнтів/груп застосовано та редагувати правила.

3.2. Застосування технології з реагування на інциденти внутрішньої безпеки на базі UAM Syteca

У даному розділі розглянемо процес практичного застосування технології Syteca UAM для захисту від інсайдерських загроз. Основна увага приділяється у виявленні підозрілої активності (на прикладі контролю доступу до соціальних мереж та інших ресурсів).

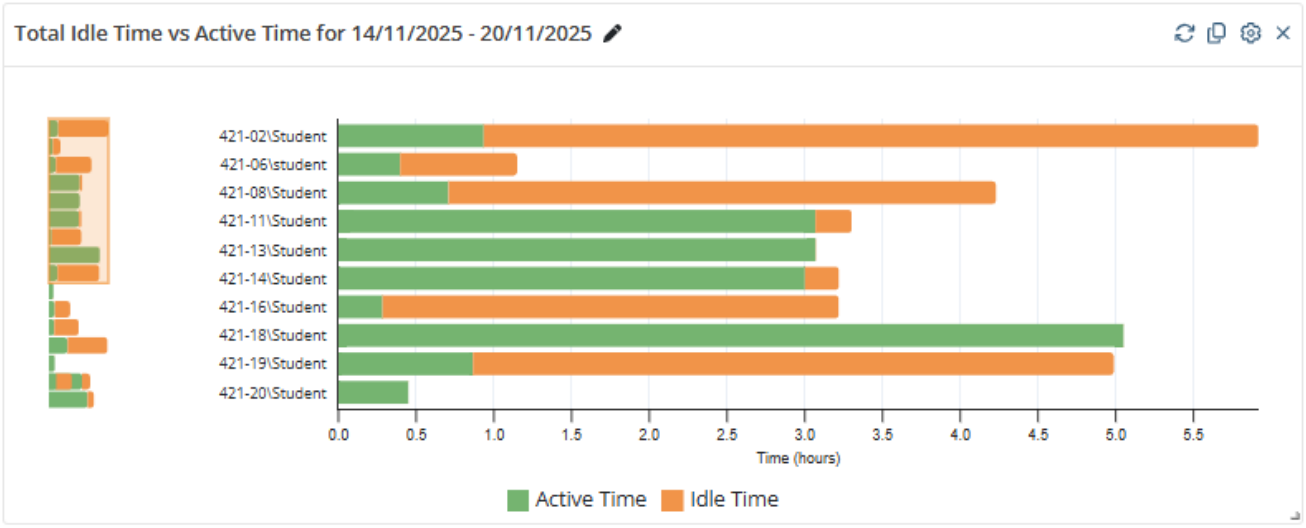

Рис. 3.21. Загальний час простою та активного часу

Рис. 3.21 демонструє нам стовбчасту діаграму загального часу використання кінцевих точок (далі - КТ) користувачами та часом простою.

Вісь Y демонструє список користувачів, які використовували КТ.

Вісь X — час у годинах.

Active Time (Зелені стовпчики): Час активної роботи (рух мишею, натискання клавіш, тощо).

Idle Time (Помаранчеві): Час простою (комп'ютер увімкнений, сесія активна, але користувач не виконує жодних дій).

Діаграма дозволяє миттєво порівняти ефективність роботи різних користувачів, а з точки зору інформаційної безпеки — велика кількість Idle Time (як у КТ 421-02) є потенційним інцидентом безпеки. Це означає, що розблокований комп'ютер був залишений без нагляду, що створює ризик несанкціонованого доступу третіх осіб (наприклад, інший студент міг підійти і скопіювати дані).

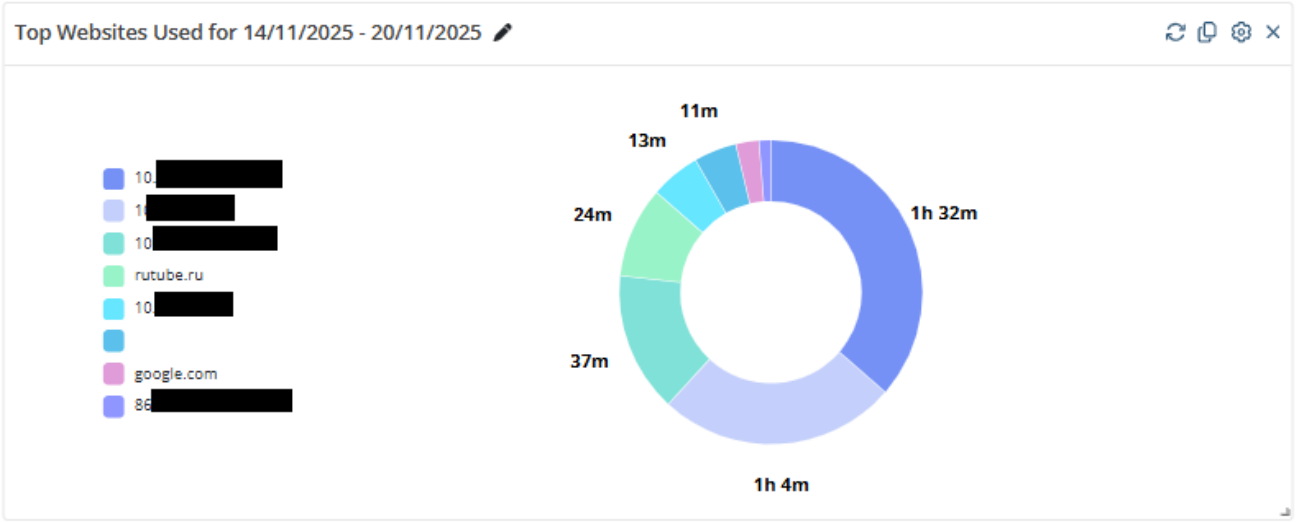

Рис. 3.22. Найпопулярніші відвідувані веб-сайти

Рис. 3.22 Допомагає виявити відвідування підозрілих або заборонених ресурсів, що можуть стати джерелом зловмисного ПЗ або витоку інформації.

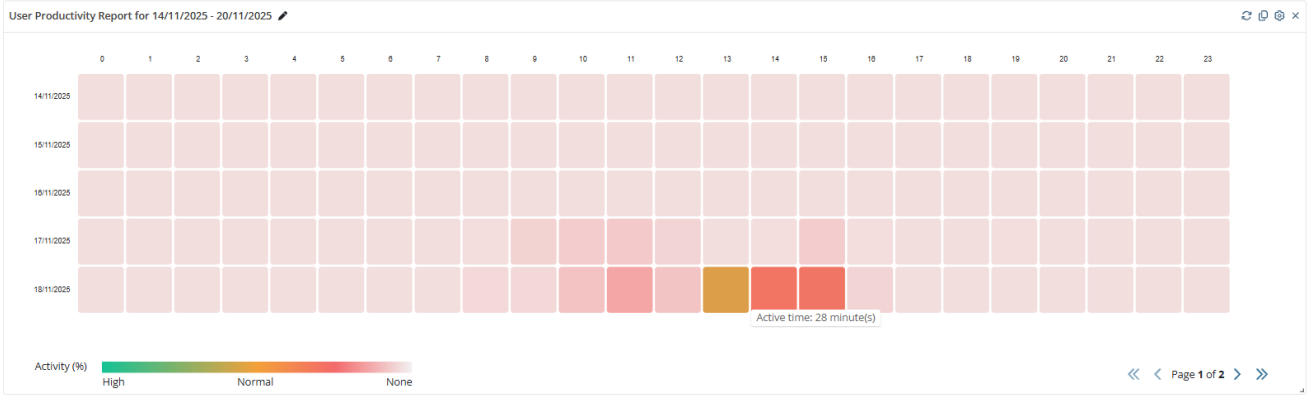

Рис. 3.23. Звіт про продуктивність користувача

Рис. 3.23 допомагає виявляти аномалії, наприклад: якби активність (зелений або жовтий квадрат) з'явилася о 3-й годині ночі, це було б індикатором інциденту безпеки (злам акаунта або інсайдерська діяльність у неробочий час).

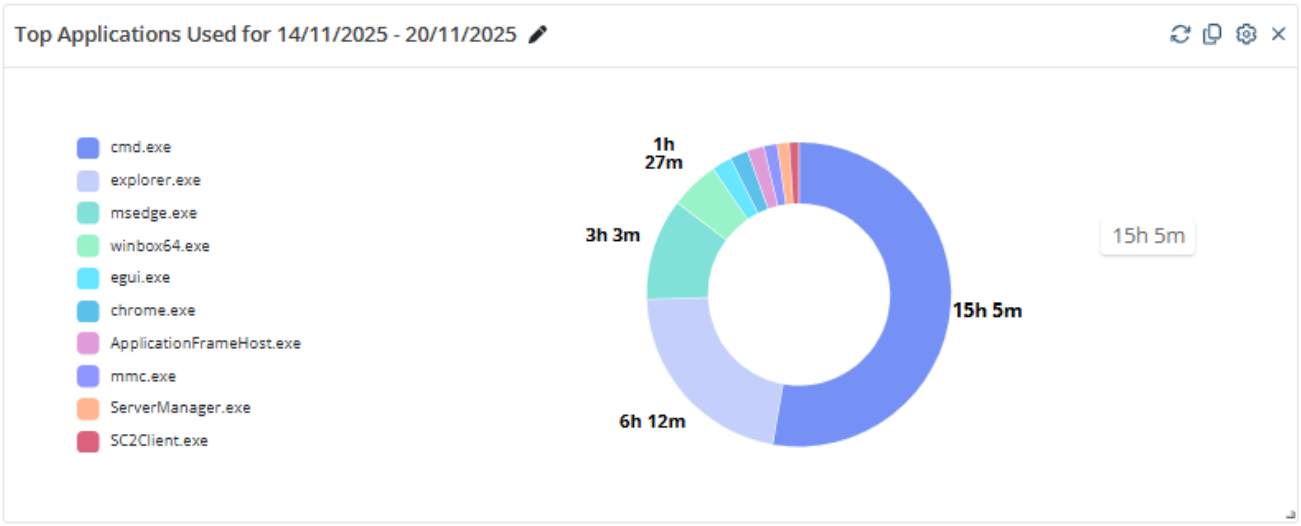

Рис. 3.24. Найпопулярніші використані додатки

На рис. 3.24 виявлено інцидент запуску розважального ПЗ (SC2Client.exe), що неприпустимо для корпоративного середовища.

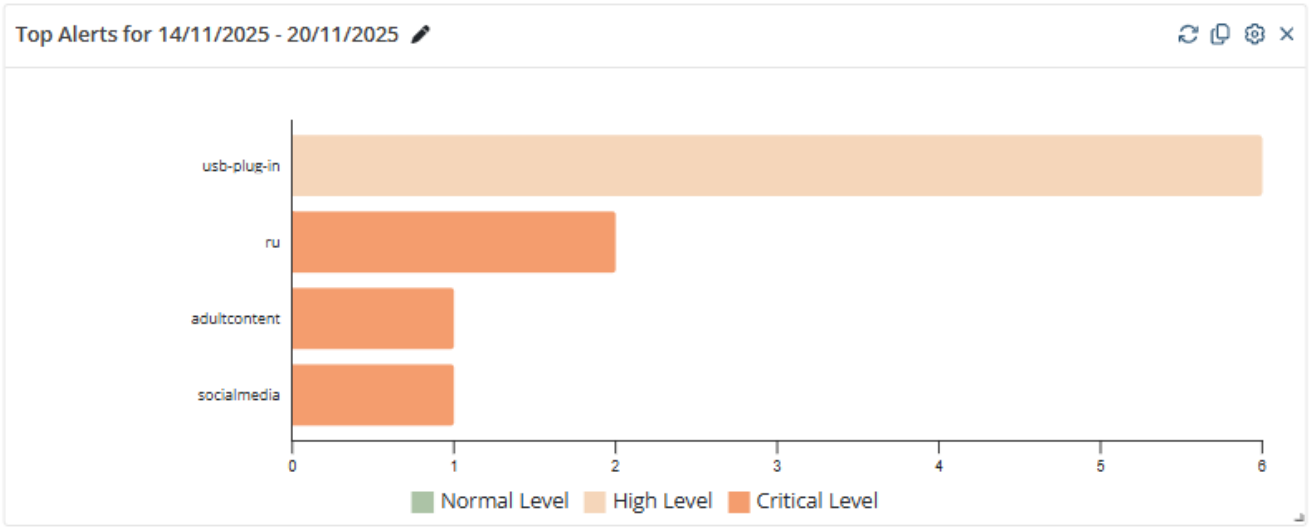

Рис. 3.25. Топ спрацювань порушень політик безпеки

Рис. 3.25 є одним із найважливіших, оскільки він показує не просто статистику, а конкретні інциденти порушення політик.

Проаналізуємо спрацювання інцидентів:

usb-plug-in (6 спрацювань) — High Level. Це класичний вектор для витоку даних (співробітник копіює документи на флешку) або зараження системи шкідливим ПЗ (віруси з принесеної флешки).

ru (2 спрацювання) — Critical Level.

Спрацювання правила, яке, налаштоване на детекцію відвідування сайтів агресора у доменній зоні .ru. В умовах України це розглядається як критичний інцидент, що може свідчити про зв'язок з країною-агресором, споживання ворожої пропаганди або використання забороненого російського ПЗ.

adultcontent (1 спрацювання) — Critical Level. Спроба доступу до ресурсів "для дорослих". Свідчить про грубе порушення етики та трудової дисципліни, а також високий ризик «підхопити» віруси, які часто поширюються через такі сайти.

socialmedia (1 спрацювання) — Critical Level. Нецільове використання робочого часу та потенційний канал витоку інформації через месенджери соцмереж.

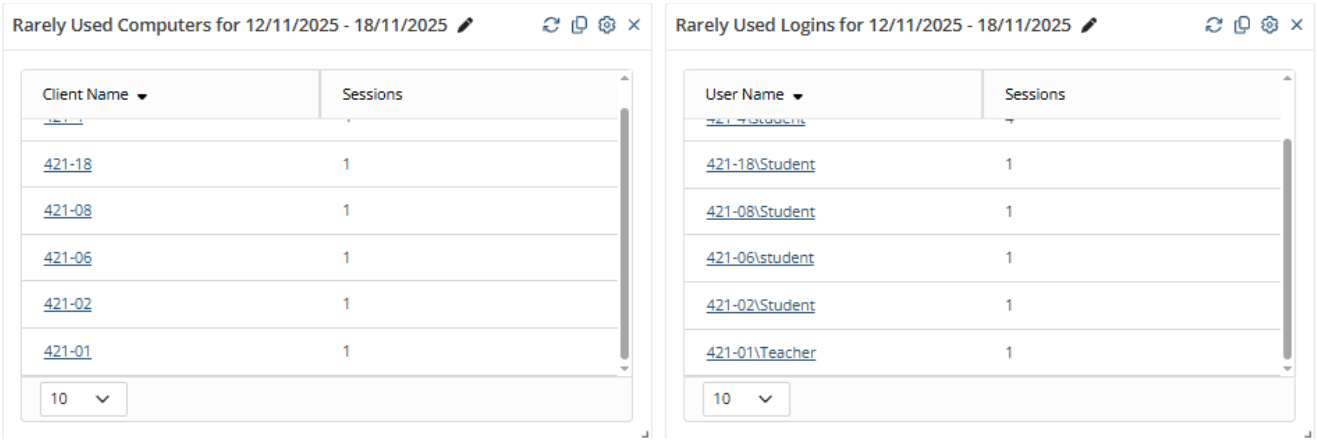

Рис. 3.26. Рідко використовувані комп'ютери та облікові записи

Допомагає виявленню «Dormant Accounts» (Сплячих акаунтів). Оскільки облікові записи, якими рідко користуються, є улюбленою ціллю хакерів. Якщо зловмисник зламає акаунт, яким ніхто не користується, його вхід може залишитися непоміченим довгий час. Системний адміністратор повинен відключати або видаляти такі акаунти.

Activity Ti...	Activity Ti...	Applicatio...	URL	Text Data	Alert/USB
15:21:07	Program Manager	explorer.exe			
15:21:23	Program Manager	explorer.exe			
15:21:23	Program Manager	explorer.exe			usb-plug-in
15:21:24	Сповіщення - ESE...	egui.exe			
15:21:25	Флешка 8 Гб (D:)	explorer.exe			
15:21:25	USBStorage - D:\ - ...	[Monitoring event]			
15:21:25	Program Manager	explorer.exe			
15:21:29	Контекстне меню	explorer.exe			
15:22:18	Нова вкладка - Go...	chrome.exe	instagram		
15:22:18	Нова вкладка - Go...	chrome.exe	google.com		
15:22:18	Нова вкладка - Go...	chrome.exe	google.com		
15:22:20	instagram - Пошук...	chrome.exe	google.com		
15:22:20	instagram - Пошук...	chrome.exe	instagram.com		
15:22:24	Instagram - Google...	chrome.exe	instagram.com		
15:22:31	YouTube - Google ...	chrome.exe			
15:22:34	YouTube - Google ...	chrome.exe	youtube.com		

Рис. 3.27. Лог подій сесії користувача

Рис. 3.27 демонструє детальний перегляд Live сесії та тригерів спрацювання порушень політик безпеки.

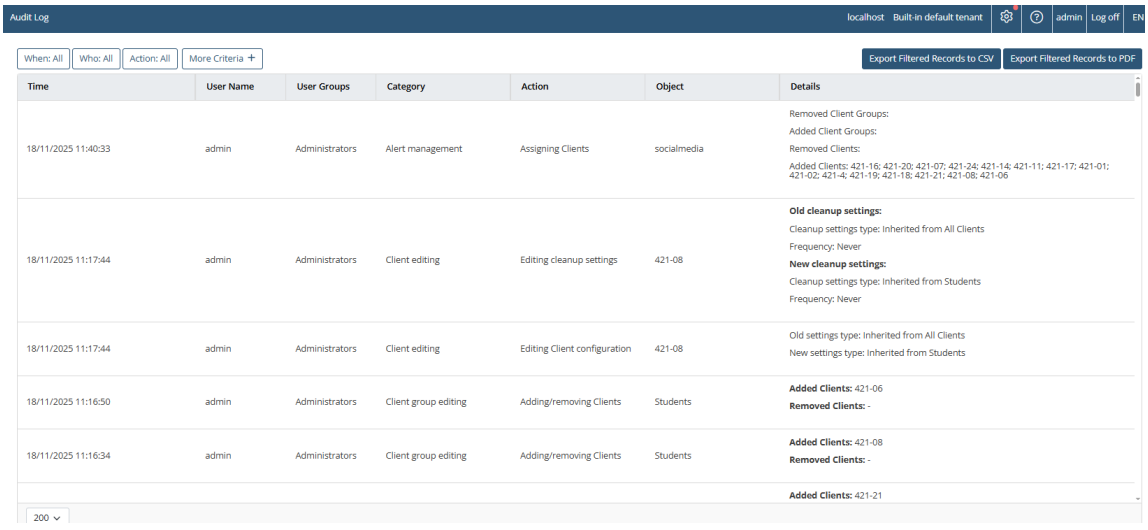

Рис. 3.28. Журнал системного аудиту

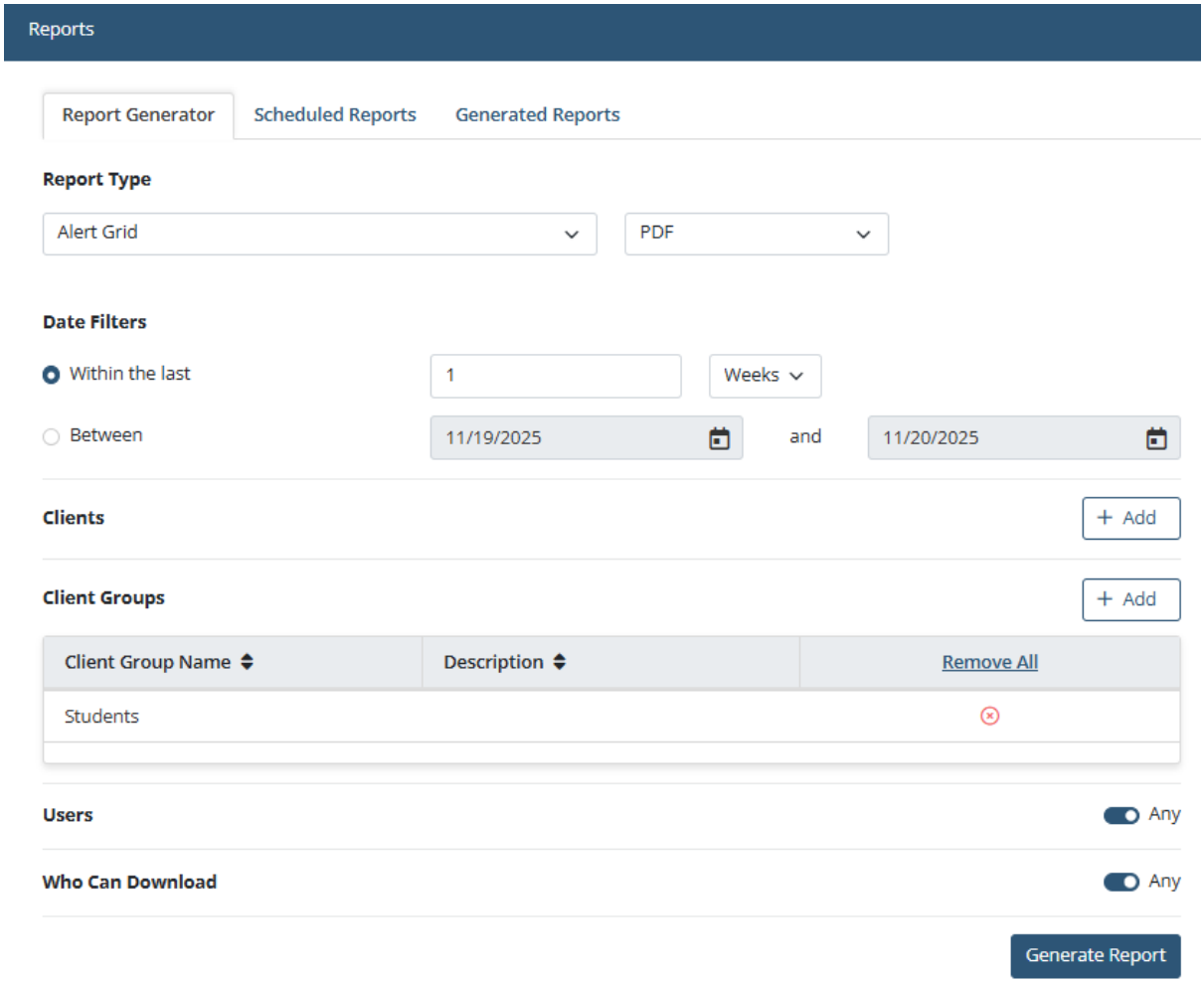

Рис. 3.29. Створення звіту подій

Рис. 3.29 демонструє параметри формування звіту системи UAM Syteca в консолі управління. На якому доступні наступні параметри:

1. Тип та Формат Звіту (Report Type) включає: тип "Alert Grid" (Сітка/Таблиця алертів). Це означає, що адміністратор хоче отримати зведений список усіх спрацювань політик безпеки (інцидентів). Format: формат PDF. Це зручний формат для передачі керівництву або долучення до матеріалів розслідування.

2. Часові Фільтри (Date Filters) — «Within the last 1 Weeks» (Протягом останнього 1 тижня).

3. Об'єкти моніторингу (Target): Clients (Клієнти) або Client Groups (Групи клієнтів).

4. Інші налаштування

Users: параметр «Any» (Будь-які). Звіт включає активність усіх користувачів, які працювали на машинах групи «Students».

Who Can Download будь хто.

5. Кнопка дії «Generate Report» генерація звіту.

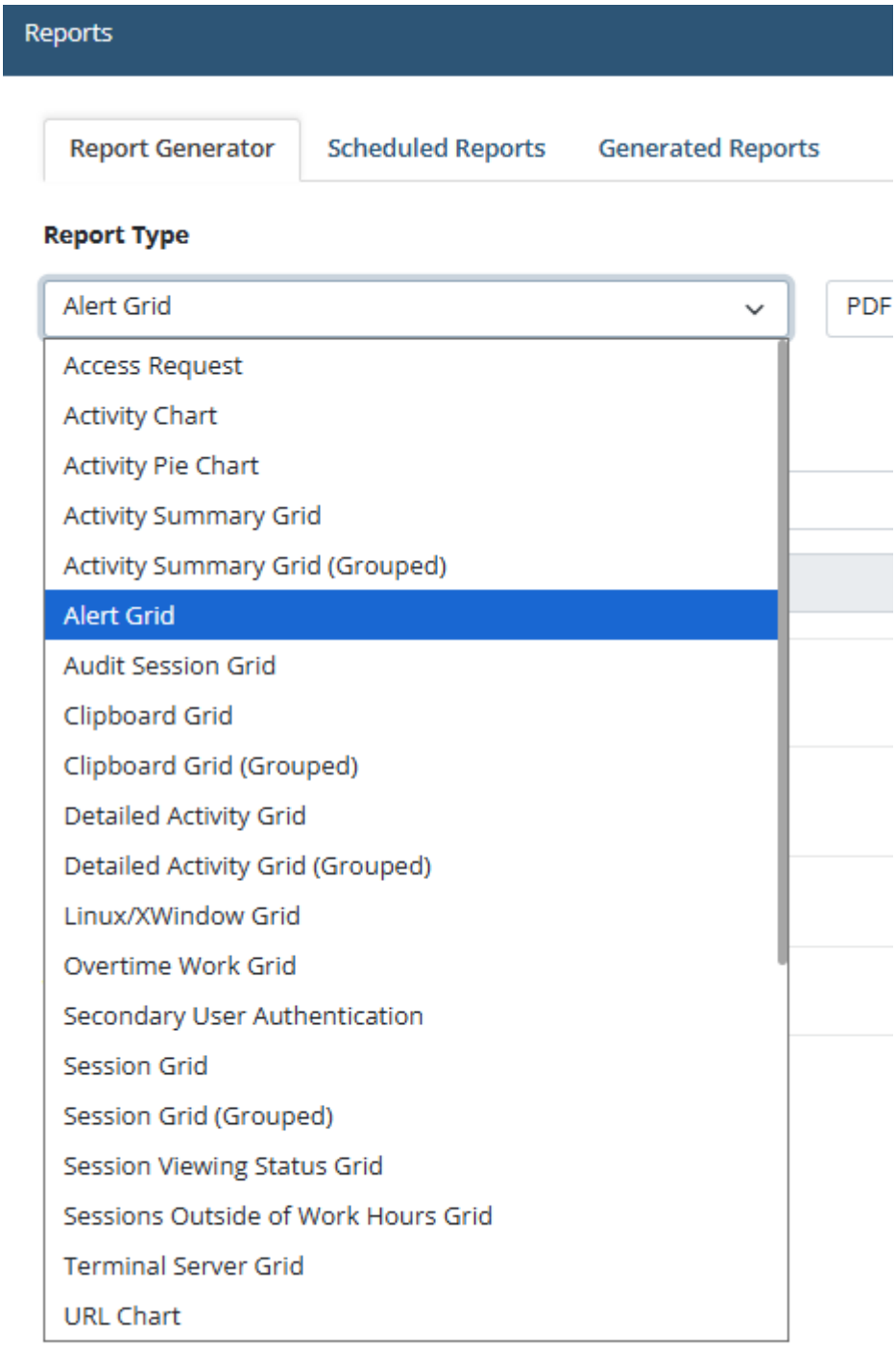

Рис. 3.30. Параметри типу та формату звіту (Report Type)

Аналіз доступних типів звітів представлений на рис. 3.30 демонструє глибину аналітики системи. Звіти можна умовно поділити на категорії:

1. Загальна активність:

Activity Chart / Pie Chart: графічні діаграми активності (лінійні та кругові).

Session Grid: детальний список усіх сесій користувачів.

URL Chart: статистика відвідування веб-сайтів.

2. Безпека та розслідування (Forensics):

Alert Grid: звіт по спрацюванню політик безпеки.

Clipboard Grid: дозволяє бачити історію буферу обміну (текст, який користувачі копіювали та вставляли). Це критично для виявлення витоку даних.

Audit Session Grid: аудит дій самих адміністраторів.

3. Специфічні платформи:

Linux/XWindow Grid: окремі звіти для Linux-систем, що підтверджує кросплатформеність Syteca.

Terminal Server Grid: звіти по термінальних серверах.

4. Human Resources (Людські ресурси, HR):

Overtime Work Grid: звіт про перепрацювання (хто працює більше норми).

Sessions Outside of Work Hours Grid: звіт про сесії у неробочий час. Це критичний маркер як для HR (вигорання), так і для безпеки (підозрілий нічний доступ).

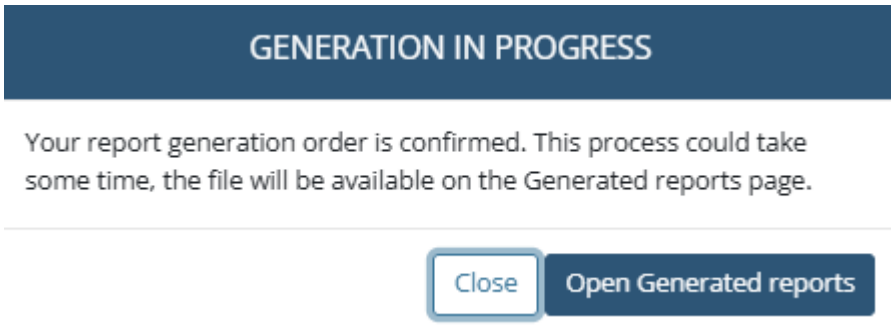

Рис. 3.31. Успішна генерація звітів

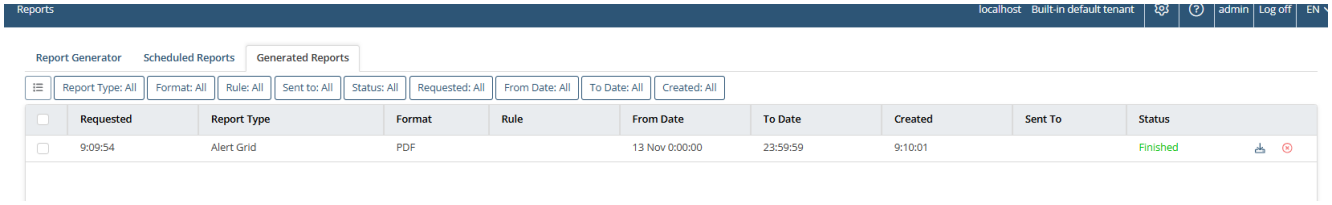

Рис. 3.32. Вікно створених звітів

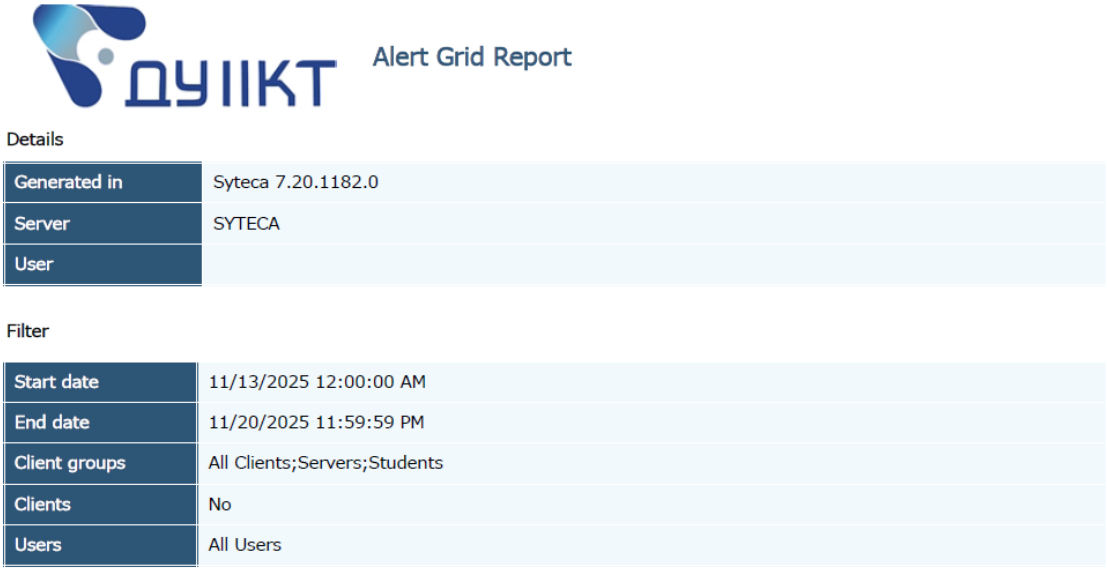

Рис. 3.33. Деталі згенерованого звіту про порушення політик безпеки

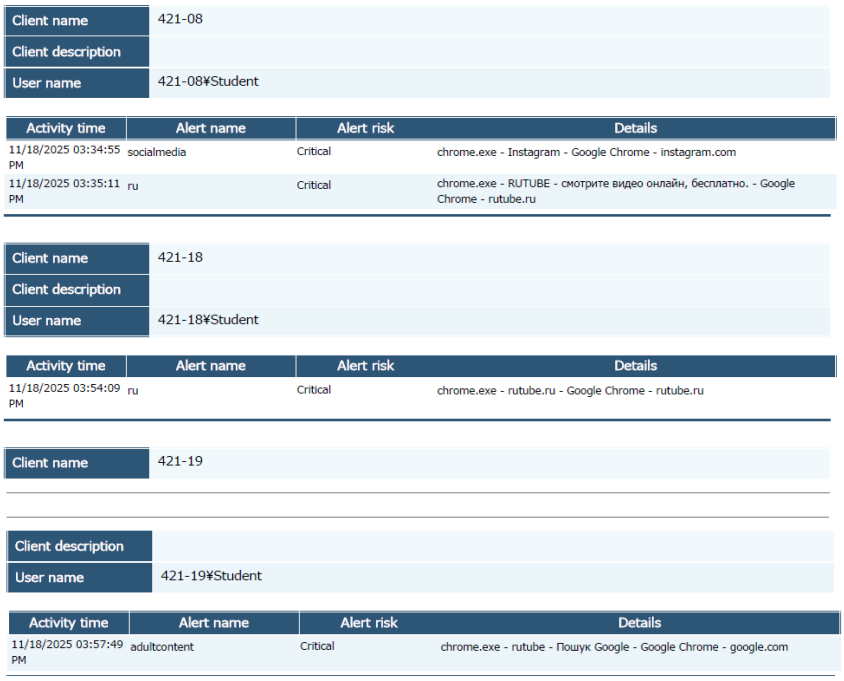

Рис. 3.34. Детальний опис у звіті інцидентів

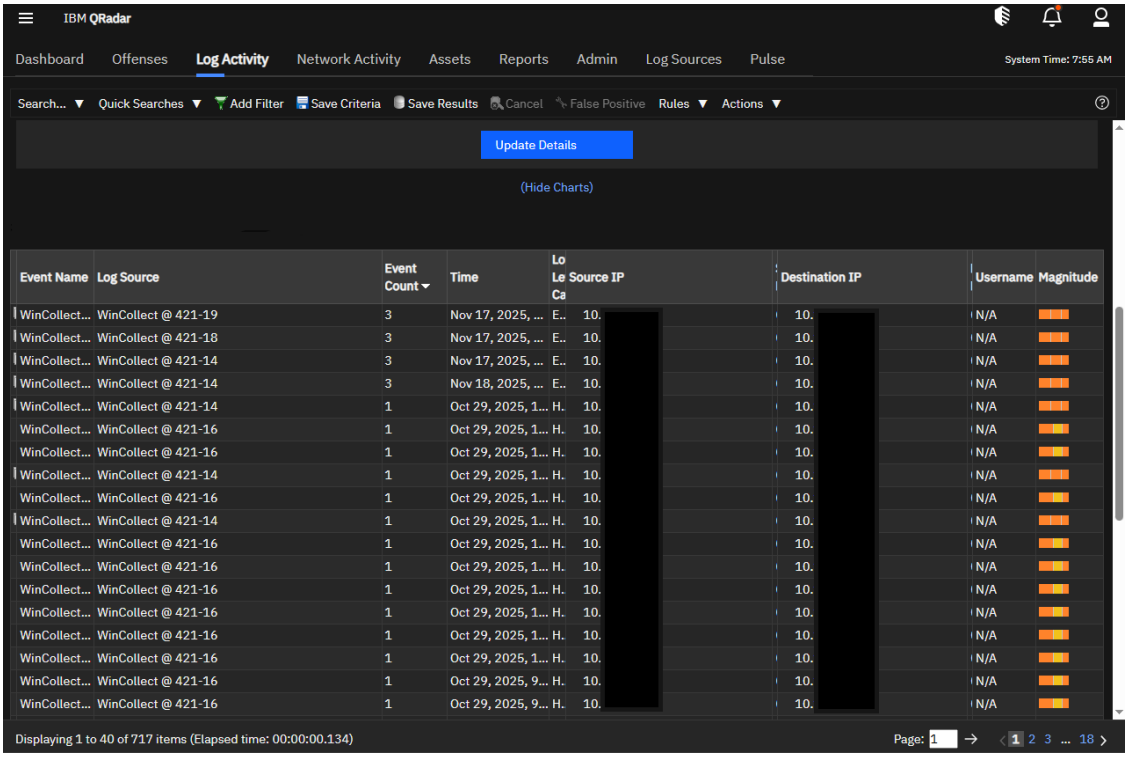

Рис. 3.35. Передані і зібрані логи в IBM QRadar

Рис. 3.34 демонструє детальний опис порушень політик безпеки у системі, а саме:

Клієнт: 421-08 (Користувач: 421-08\Student). Цей користувач є найбільш активним порушником. Зафіксовано два інциденти з різницею в 16 секунд:

Час: 15:34:55 (03:34:55 PM).

Порушення політики socialmedia (Соціальні мережі).

Ризик: Critical (Критичний).

Деталі: Запущено процес chrome.exe, заголовок вікна вказує на Instagram, URL — instagram.com.

Час: 15:35:11 (03:35:11 PM).

Порушення політики ru (Ресурси агресора).

Ризик: Critical (Критичний).

Деталі: Запущено chrome.exe, відкрито сайт RUTUBE (rutube.ru).

Користувач намагався отримати доступ до відеохостингу країни-агресора. Це підтверджує ефективність налаштованого правила «ru».

Клієнт: 421-18 (Користувач: 421-18\Student)

Ще один інцидент на іншій КТ:

Час: 15:54:09 (03:54:09 PM).

Порушення політики ru.

Ризик: Critical.

Клієнт 421-19\Student.

Час: 15:57:49 (03:57:49 PM).

Порушення політики adultcontent (контент для дорослих 18+)

Ризик: Critical (Критичний).

Це підтверджує факт спроби доступу до небажаних ресурсів, що було зафіксовано системою як критичне порушення.

У звіті чітко видно ХТО (ім'я користувача), КОЛИ (точний час до секунди), ЩО (URL та заголовок вікна) і ДЕ (на якій КТ) порушив політику.

Звіт доводить, що створені раніше алерти (socialmedia, ru, та adultcontent) працюють коректно і виявляють загрози в реальному часі.

3.3. Розроблення рекомендацій щодо застосування технології реагування на інциденти внутрішньої безпеки на базі UAM Syteca

На основі вищезазначеного матеріалу було розроблено рекомендацій щодо застосування технології реагування на інциденти внутрішньої безпеки на базі UAM Syteca. Рекомендації розділені на 4 логічні етапи життєвого циклу інциденту: Конфігурація, Виявлення, Реагування та Аналіз.

І. Налаштування політик та конфігурація.

- групування об'єктів моніторингу: розділення КТ на логічні групи. Політики безпеки повинні застосовуватися не до окремих ПК, а до груп відповідно до принципу мінімальних привілеїв.

- сегментація правил за типами загроз: створення окремих категорій алертів для різних векторів атак: окремо для USB (usb-plug-in), веб-активності (socialmedia, ru) та запуску ПЗ. Це спрощує аналітику.

- використання логічних операторів у правилах: При створенні складних алертів (наприклад, socialmedia) використовувати оператор "OR" для об'єднання однотипних ресурсів (Facebook OR Instagram OR TikTok) в одне правило, щоб уникнути дублювання налаштувань.

- пріоритезація ризиків: обов'язкове присвоювання рівнів ризику кожному алерту.

- налаштування «Чорних списків» ПЗ: внесення до списку заборонених програм виконувані файли ігор (наприклад, виявлений SC2Client.exe) та торент-клієнтів. Їх запуск має генерувати миттєвий алерт.

- контроль системних утиліт: налаштування підвищеного моніторингу для системних процесів, таких як cmd.exe, powershell.exe, mmc.exe. Тривала активність у них (як виявлені 15 годин у cmd.exe) для звичайних користувачів є аномалією.

- гео-блокування та контент-фільтрація: впровадити правило (на зразок алерта ru), що реагує на URL-адреси, які містять домени країн-агресорів або ключові слова, пов'язані з ворожою пропагандою.

II. Моніторинг та Виявлення.

- контроль підключення зовнішніх носіїв: активація моніторингу USB-пристроїв для всіх користувачів. Необхідно фіксувати не лише факт підключення, а й імена файлів, до яких здійснювався доступ.

- моніторинг у неробочий час: будь-яка активність (навіть легітимний вхід) у нічний час або вихідні має розглядатися як потенційний інцидент.

- аналіз співвідношення Active/Idle Time: регулярний перегляд звітів продуктивності. Користувачі з аномально високим часом простою (Idle Time > 80%) створюють ризик фізичного доступу до незаблокованої КТ третіх осіб.

- виявлення "Сплячих" акаунтів: регулярно генерувати звіт «Rarely Used Logins». Акаунти, які не використовувалися понад 30 днів (або мають 1 сесію за тиждень), повинні бути заблоковані або поставлені на особливий контроль.

- моніторинг буфера обміну: активувати перехоплення даних буфера обміну (Clipboard) для критичних груп користувачів, щоб виявляти спроби копіювання конфіденційних даних (номери карток, паролі, клієнтські бази).

- відеозапис за подією: для економії місця та ефективності налаштувати запис відео не в режимі 24/7, а лише при спрацюванні тригерів (відкриття певної теки, запуск браузера, під'єднання USB).

III. Реагування на інциденти.

- автоматичне блокування USB: Трансформувати правило usb-plug-in з режиму «тільки моніторинг» у режим «блокування пристрою» або «дозволити тільки читання» для всіх, крім адміністраторів.

- примусове завершення процесів: налаштувати автоматичну реакцію (Kill Process) на запуск критично небезпечного ПЗ (ігри, майнери, невідомі скрипти).

- повідомлення користувача: налаштувати виведення спливаючого вікна з попередженням при спробі доступу до заборонених ресурсів (наприклад, «Ваша дія зафіксована службою безпеки»). Це часто зупиняє ненавмисні порушення.

- живий перегляд (Live View): при отриманні алерта рівня "Critical", необхідно негайно підключитися до сесії в режимі реального часу для оцінки ситуації.

IV. Розслідування та Аналіз.

- аудит дій адміністраторів: регулярно переглядати «Audit Log» для контролю змін у конфігурації. Будь-яке відключення моніторингу або зміна політик (як було зафіксовано Assigning Clients до групи socialmedia) має бути санкціонованим.

- регулярна звітність: налаштувати автоматичну генерацію та відправку звітів «Alert Grid» та «Top Applications» керівництву та відповідній службі безпеки раз на тиждень для аналізу трендів (зростання кількості інцидентів, поява нових загроз).

Висновки до розділу 3

У розділі було розгорнуто та налаштовану систему UAM Syteca з інтеграцією до SIEM IBM QRadar CE, завантажено агенти на кінцеві точки та підключені до системи. Досліджено функціонування Syteca на реальних порушеннях внутрішньої безпеки. Та розроблено рекомендації щодо застосування технології реагування на інциденти внутрішньої безпеки на базі UAM Syteca.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було проведено комплексне дослідження та практичну реалізацію системи захисту від інцидентів внутрішньої інформаційної безпеки, а саме:

У першому розділі було проведено комплексний аналіз проблеми інцидентів внутрішньої інформаційної безпеки та засобів реагування на них, а саме: приведено класифікацію інцидентів внутрішньої безпеки; розглянуто сучасні підходи та технології реагування на дані порушення; проаналізовано існуючі рішення UAM та приведена порівняльна характеристика в таблиці 1.3.

У другому розділі було досліджено функціональні можливості UAM Syteca, приведена архітектура з основними компонентами системи. Реалізовано приклади інтеграції з різними системами та описані механізми моніторингу, збору та аналізу подій.

У третьому розділі було розгорнуто та налаштовану систему UAM Syteca з інтеграцією до SIEM IBM QRadar CE, завантажено агенти на кінцеві точки та підключені до системи. Досліджено функціонування Syteca на реальних порушеннях внутрішньої безпеки. Та розроблено рекомендації щодо застосування технології реагування на інциденти внутрішньої безпеки на базі UAM Syteca.

Проведене тестування на реальних сценаріях порушень довело ефективність обраного підходу у виявленні та реагуванні на інциденти. Розроблені рекомендації щодо налаштування та застосування UAM Syteca є готовим алгоритмом для мінімізації внутрішніх ризиків в інформаційній інфраструктурі підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Storchak Y. Insider Threat Statistics for 2025: Facts, Reports & Costs | Syteca. Syteca. URL: https://www.syteca.com/en/blog/insider-threat-statistics-facts-and-figures (дата звернення: 10.10.2025).

2. 2024 Insider Threat Report [Gurucul]. Cybersecurity Insiders. URL: https://www.cybersecurity-insiders.com/portfolio/2024-insider-threat-report-gurucul/ (дата звернення: 10.10.2025).

3. Shomonko O. What Is a ‘Malicious Insider’? Indicators and Examples | Syteca. Syteca. URL: https://www.syteca.com/en/blog/portrait-malicious-insiders (дата звернення: 10.10.2025).

4. Software Engineering Institute. Common Sense Guide to Mitigating Insider Threats, Seventh Edition. SEI Digital Library. URL: https://www.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/ (дата звернення: 11.10.2025).

5. Zhurer Y. Intellectual Property Theft: 7 Best Practices on How to Prevent It | Syteca. Syteca. URL: https://www.syteca.com/en/blog/best-practices-to-prevent-intellectual-property-theft (дата звернення: 12.10.2025).

6. Zhurer Y. Insider Fraud Prevention: Tips & Tricks to Prevent Insider Fraud | Syteca. Syteca. URL: https://www.syteca.com/en/blog/insider-fraud-prevention (дата звернення: 13.10.2025).

7. Zhurer Y. How to Detect and Prevent Industrial or Corporate Espionage | Syteca. Syteca. URL: https://www.syteca.com/en/blog/prevent-industrial-espionage (дата звернення: 13.10.2025).

8. 2025 Ponemon Cost of Insider Threats Global Report. DTEX Systems. URL: https://ponemon.dtexsystems.com/?team=board&wtime=%7Bseek_to_second_number%7D (дата звернення: 13.10.2025).

9. What is data loss prevention (DLP)? | Microsoft Security. Your request has been blocked. This could be due to several reasons. URL: https://www.microsoft.com/en-

us/security/business/security-101/what-is-data-loss-prevention-dlp (дата звернення: 13.10.2025).

10. Jensen S. L. What Is Awareness Training? And How To Implement It Effectively. CyberPilot | Awareness training & Phishing training. URL: https://www.cyberpilot.io/cyberpilot-blog/what-is-awareness-training-and-how-to-implement-it-effectively (дата звернення: 13.10.2025).

11. What is Privileged Access Management (PAM) | Microsoft Security. Your request has been blocked. This could be due to several reasons. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam (дата звернення: 13.10.2025).

12. Managing Workplace Monitoring and Surveillance. Welcome to SHRM | The Voice of All Things Work. URL: https://www.shrm.org/topics-tools/tools/toolkits/managing-workplace-monitoring-surveillance (дата звернення: 13.10.2025).

13. What Is SIEM? | Microsoft Security. Microsoft – AI, Cloud, Produktivität, Computing, Gaming und Apps. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem (дата звернення: 14.10.2025).

14. What is User Behavior Analytics (UBA)? | A Comprehensive UBA Guide. Elastic – The Search AI Company | Elastic. URL: https://www.elastic.co/what-is/user-behavior-analytics (дата звернення: 14.10.2025).

15. Thomas K. What is Cybersecurity threat intelligence sharing. Cybersecurity & Managed Security Service Provider | LevelBlue. URL: https://levelblue.com/blogs/security-essentials/what-is-cybersecurity-threat-intelligence-sharing (дата звернення14.10.2025).

16. Incident Response Management: Key Elements and Best Practices. Cynet. URL: https://www.cynet.com/incident-response/incident-response-management-key-elements-and-best-practices/ (дата звернення: 15.10.2025).

17. What is Network Traffic Analysis? A Complete Guide for Enterprise Security Leaders. NETWITNESS. URL: https://www.netwitness.com/blog/what-is-network-traffic-analysis/ (дата звернення: 15.10.2025).

18. Bell T. Third-party security vetting: Do it before you sign a contract. CSO Online. URL: https://www.csoonline.com/article/564777/third-party-security-vetting-do-it-before-you-sign-a-contract.html (дата звернення: 15.10.2025).

19. Нечипоренко Є.В. Можливості UAM Syteca для виявлення інцидентів внутрішньої безпеки: Всеукр. Науково-практ. Конф. тези доп., м. Київ, 29 жовт. 2025 р. Київ, 2025. С. 58–60. URL: https://duikt.edu.ua/uploads/p_2779_58326207.pdf.

20. Що таке Syteca?. Syteca | BAKOTECH. URL: https://syteca.bakotech.com/ua (дата звернення: 16.10.2025).

21. System Components. Syteca Knowledge Base of End-User Documentation. URL: https://docs.syteca.com/view/system-structure-and-architecture (дата звернення: 20.10.2025).

22. Liudmyla Pryimenko. 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: 05.11.2025).

23. Configuring Syteca Integration with ForgeRock SSO. Syteca Knowledge Base of End-User Documentation. URL: https://docs.syteca.com/view/integrating-forgerock-sso-with-the-ekran-system-ma (дата звернення: 14.11.2025).

24. Quick Start Deployment Guide. Syteca Knowledge Base of End-User Documentation. URL: https://docs.syteca.com/view/quick-start-deployment-guide (дата звернення: 28.11.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)