МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
Доктор економічних наук, професор	Доктор економічних наук, професор
_____ С.В. Легомінова	_____ С.В. Легомінова
«__» _____ 2022 р.	«__» _____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

другого магістерського рівня вищої освіти

на тему:

ВИЗНАЧЕННЯ ДОЦІЛЬНОГО СПОСОБУ МОНІТОРИНГУ ЗОВНІШНІХ І ВНУТРІШНІХ ПРОЦЕСІВ В ІНТЕРЕСАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА (УСТАНОВИ, ОРГАНІЗАЦІЇ)

СТУДЕНТ:	Ющенко Матвій Олександрович	_____ (підпис)
КЕРІВНИК:	к.т.н., доцент Рабчун Дмитро Ігорович	_____ (підпис)
НОРМОКОНТРОЛЕР:	_____	_____ (підпис)

КИЇВ — 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Спеціальність «Кібербезпека»
Спеціалізація «Управління інформаційною безпекою»
Другого магістерського рівня вищої освіти

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
(підпис)
«___»_____ 2022 р.

ЗАВДАННЯ
на кваліфікаційну роботу
студенту Ющенку Матвію Олександровичу

1. Тема роботи «Визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації)», затверджена наказом по університету № 122 від “12” жовтня 2022 р.

2. Термін здачі студентом оформленої роботи «22» грудня 2022 р.

3. Об’єкт дослідження: забезпечення моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації).

4. Предмет дослідження: способи моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації).

5. Мета дослідження: визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації).

6. Перелік питань, які мають бути розроблені:

6.1. Проаналізувати моніторинг внутрішніх та зовнішніх процесів при управлінні безпекою інформаційних ресурсів підприємства (установи, організації).

6.2. Дослідити сучасні рішення інформаційної безпеки для визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства.

6.3. Визначити доцільний спосіб моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства методом експертних оцінок.

7. Дата видачі завдання «19» вересня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: «19» вересня 2022 року

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	26.09.2022	
2.	Збір та аналіз літератури.	03.10.2022	
3.	Аналіз моніторингу внутрішніх та зовнішніх процесів при управлінні безпекою інформаційних ресурсів підприємства (установи, організації).	17.10.2022	
4.	Дослідження сучасних рішень інформаційної безпеки для визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства.	31.10.2022	
5.	Визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства методом експертних оцінок.	14.11.2022	
6.	Формулювання висновків за результатами проведеного дослідження.	01.12.2022	
7.	Оформлення роботи.	08.12.2022	
8.	Оформлення презентації.	15.12.2022	
9.	Отримання рецензії на роботу.	23.12.2022	
10.	Захист в ДЕК.	17.01.2023	

Студент: _____ М.О. Ющенко
(підпис)

Науковий керівник: _____ Д.І. Рабчун
(підпис)

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню проблеми визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства. Робота складається зі вступу, трьох розділів, що містять 21 рисунок, висновків та списку використаних джерел, що містить 22 найменування. Загальний обсяг роботи становить 86 аркушів, з яких 2 аркуша займає список використаних джерел.

Об'єктом дослідження є забезпечення моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації).

Метою роботи є визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації). Для цього у роботі використовуються методи системного аналізу, метод експертних оцінок, теорія інформаційної безпеки, теорія моніторингу інформаційної безпеки та теорія проведення кібератак.

Як результат у роботі проведено аналіз моніторингу внутрішніх та зовнішніх процесів при управлінні безпекою інформаційних ресурсів підприємства (установи, організації); досліджено сучасні рішення інформаційної безпеки для визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства; визначено доцільний спосіб моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства методом експертних оцінок.

Галузь застосування. Визначений спосіб моніторингу зовнішніх і внутрішніх процесів інформаційної безпеки може бути використаний підприємством для захисту від кібератак та підвищення їх рівня інформаційної безпеки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, МОНІТОРИНГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЗОВНІШНІ ТА ВНУТРІШНІ ПРОЦЕСИ, СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ПРОВЕДЕННЯ КІБЕРАТАК.

ЗМІСТ

ВСТУП

Актуальність теми. Застосування сучасних інформаційних технологій створює умови для економічного розвитку та визначає інформаційну інфраструктуру державних органів, організацій, наукових установ, компаній, підприємств тощо. Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої організації. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку підприємства, в основі якого мають бути найновіші автоматизовані технічні засоби та практики інформаційної безпеки. Це пов'язано з постійно зростаючою кількістю загроз, кібератак та інших факторів, які можуть негативно впливати на інформаційну інфраструктуру підприємств, установ та організацій.

На даному етапі механізми моніторингу відіграють дуже важливу роль в системах захисту інформації підприємств, установ та організацій. Переважна більшість вдалих кібератак скоюються через некоректну організацію моніторингу інформаційної безпеки в межах мережевого обладнання, пошти, месенджерів та роботи персоналу. Наслідками кібератак зазвичай є порушення конфіденційності корпоративної інформації підприємств і організацій, що призводить до колосальних збитків та втрати репутації. Доволі часто моніторинг інформаційної безпеки недооцінюють в процесі розробки організаційних заходів та комплексних систем захисту інформації, а також і у процесі діяльності підприємства. На людський чинник через стрімкий прогрес ІТ також звертають дедалі менше уваги. При розробці систем захисту акцентують увагу саме захисті від неавторизованого вторгнення в систему зловмисника власноруч. Не всі підприємства усвідомлюють, що зловмиснику не обов’язково потрібно знешкоджувати систему захисту, якщо можливі інші шляхи – наприклад, використання працівників персоналу методами соціальної інженерії через їх людські якості, як позитивні, так і негативні. Зазвичай використання такого шляху є ключем до вдалої кібератаки.

Тож незахищеність інформації може дуже дорого обійтися для будь-якої компанії. Дуже важливо вчасно отримувати дані про загрози, уразливості, порушення, інциденти та інші події в корпоративній інформаційній системі. Це дозволить своєчасно відреагувати і усунути їх.

Тому політика забезпечення інформаційної безпеки підприємства має бути побудована з урахуванням потреб організації моніторингу зовнішніх та внутрішніх процесів підприємств, захисту чутливої інформації, інфраструктури та, зокрема, персоналу як стратегічних ресурсів підприємства. Необхідно впроваджувати автоматизовані засоби, які допоможуть проводити моніторинг зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства. Одним з кращим типів рішень на даний момент є клас рішень SIEM (Security Information and Event Management).

З огляду на зазначене тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня захисту підприємств, установ та організацій від кібератак.

Мета і завдання дослідження. Мета роботи полягає у визначенні доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації).

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати моніторинг внутрішніх та зовнішніх процесів при управлінні безпекою інформаційних ресурсів підприємства (установи, організації).

2. Дослідити сучасні рішення інформаційної безпеки для визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства.

3. Визначити доцільний спосіб моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства методом експертних оцінок.

Об’єкт дослідження – забезпечення моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації).

Предмет дослідження – способи моніторингу зовнішніх і внутрішніх процесів підприємства (установи, організації).

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, метод експертних оцінок, теорія інформаційної безпеки, теорія моніторингу інформаційної безпеки та теорія проведення кібератак.

Наукова новизна одержаних результатів. Визначений спосіб моніторингу зовнішніх і внутрішніх процесів інформаційної безпеки може бути використаний підприємством (установою, організацією) для захисту від кібератак та підвищення їх рівня інформаційної безпеки.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір способу моніторингу ініформаційної безпеки для захисту інформації, інфраструктури та персоналу підприємства від кібератак.

Розділ 1 АНАЛІЗ МОНІТОРИНГУ ВНУТРІШНІХ ТА ЗОВНІШНІХ ПРОЦЕСІВ ПРИ УПРАВЛІННІ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА (УСТАНОВИ, ОРГАНІЗАЦІЇ)

1.1 Управління безпекою інформаційних ресурсів підприємства

Управління безпекою інформаційних ресурсів описує засоби управління, які організація повинна впровадити, щоб забезпечити захист конфіденційності, доступності та цілісності активів від загроз та вразливостей [1]. Крім того, управління ІБ включає управління інформаційними ризиками, процес, який включає оцінку ризиків, з якими організація повинна мати справу при управлінні та захисті активів, а також розповсюдження ризиків серед всіх відповідних зацікавлених сторін. Для цього необхідна належна ідентифікація активів та етапів оцінки, включаючи оцінку цінності конфіденційності, цілісності, доступності і заміни активів.

По суті, управління ІБ означає управління і зменшення різних загроз і вразливостей для активів з одночасним балансуванням зусиль по управлінню, затрачених на потенційні загрози та вразливості, шляхом вимірювання імовірності їх фактичного виникнення.

Після відповідної ідентифікації і оцінки активів, управління ризиками і їх зменшення по відношенню до активів включають аналіз наступних питань [2]:

- Загрози. Небажані події, які можуть призвести до навмисної або випадкової втрати, пошкодження або неправильному використанню інформаційних активів.

- Вразливості. Наскільки інформаційні активи та пов’язані з ними засоби управління схильні до експлуатації однієї чи декількох загроз

- Вплив та ймовірність. Величина потенційної шкоди інформаційним активам від загроз та вразливостей, а також серйозність ризику, який вони

представляють для активу; аналіз затрат і вигоди також можуть бути частиною оцінки впливу чи окремо від неї

- Зменшення. Пропоновані методи для мінімізації впливу та ймовірності потенційних загроз і вразливостей

Після того, як загрози та вразливості були виявлені та оцінені як такі, які надають достатній вплив на інформаційні активи, може бути прийнятий план зменшення. Вибраний метод зменшення в значній мірі залежить від того, в якому домені інформаційних технологій знаходиться загроза або вразливість [2]. Управління ІБ забезпечує інтегрований підхід до управління послугами, виконуючи наступні дії [1]:

- Виявлення та визначення внутрішніх та зовнішніх вимог безпеки

- Планування процедур безпеки

- Створення розділу ІБ в SLA та Service Description

- Управління виконанням заходів безпеки

- Оцінка процедур безпеки і заходів безпеки

- Звіти про безпеку

- Вдосконалення безпеки

Одним з ключових понять в управлінні інформаційною безпекою є система управління інформаційною безпекою, що представляє собою сукупність усіх взаємопов’язаних/взаємодіючих елементів інформаційної безпеки організації, для гарантії того, що політики, процедури і цілі могли бути створені, впроваджені, передані та оцінені, для забезпечення загальної ІБ організації. Система управління інформаційною безпекою може бути інтерпретована як системний підхід для встановлення, реалізації, експлуатації, моніторингу, аналізу, підтримки та вдосконалення інформаційної безпеки організації. Така система зазвичай залежить від потреб, цілей, вимог безпеки, а

також розміру та процесів організації. СУІБ включає та надає ефективні стратегії управління ризиками та їх зниження. Крім того, прийняття організацією СУІБ вказує на те, що вона систематично виявляє, оцінює і управляє ризиками ІБ, а також буде здатна успішно задовольняти вимогам конфіденційності, цілісності і доступності інформації. Незважаючи на важливість створення та обслуговування СУІБ, навчання персоналу СУІБ та забезпечення відповідності щоденним процесам та діям в організації - є один із основних пріоритетів для кінцевого адекватного захисту даних. Пов’язані з розробкою, впровадженням та практикою СУІБ людські фактори також повинні враховуватись, для забезпечення кінцевого успіху СУІБ найкращим чином. Ключовими елементами функціонування СУІБ є процеси. Однак, незважаючи на свою важливість, структура процесу СУІБ з описом процесів СУІБ та їх взаємодія, а також взаємодія з іншими процесами відсутня в літературі [2].

Для ідентифікації процесів у СУІБ, застосовуються наступні методи [2]:

- аналіз серії стандартів ISO 27000;

- аналіз стандартів ITIL та COBIT відносно уже ідентифікованих процесів в ISO 27000, а також відносно можливих додаткових процесів СУІБ.

Внаслідок співставлення результатів ідентифікуються наступні ключові процеси СУІБ [1]:

- процес оцінки ризиків інформаційної безпеки;

- процес усунення ризиків інформаційної безпеки;

- процес управління ресурсами;

- процес забезпечення обізнаності та компетентності;

- процес зв’язку;

- процес контролю контролю документації та записів;

- процес управління вимогами;

- процес управління змінами інформаційної безпеки;

- процес управління зовнішніми процесами;

- процес управління внутрішніми процесами;

- процес оцінки продуктивності;

- процес внутрішнього аудиту;

- процес управління інцидентами інформаційної безпеки;

- процес вдосконалення інформаційної безпеки;

- процес управління відносинами і споживачем інформаційної безпеки;

- процес управління конфігураціями.

Оскільки поняття безпека не є кінцевим станом, якого необхідно досягти, а відповідає процесам, направленим на забезпечення захищеності певної інфраструктури, поняття “управління інформаційною безпекою” розглядається як управління процесами безпеки або управління процесами забезпечення безпеки.

Як уже було згадано раніше, інструменти, які доступні для допомоги організаціям в реалізації відповідних програм та засобів управління для зменшення загроз та вразливостей включають сімейство стандартів ISO 27000, структуру ITIL, структуру COBIT, а також велику кількість методологій, бібліотек та фреймворків.

Одним з перспективних напрямків щодо моніторингу внутрішнії та зовнішніх процесів, що активно розвиваються та впроваджуються на сьогодні - операційні центри безпеки, які є комплексним підходом до управління інформаційною безпекою (причому як і в контексті власне внутрішньої безпеки організації, так і безпеки інших організацій, залежно від призначення SOC). Така структура може визначатись як система управління інформаційною безпекою з орієнтацією на процеси ІБ із власною специфікою, характерною

саме SOC.

1.2 Аналіз процесів і засобів при моніторингу та протидії загроз

Загрози інформаційній безпеці (information security threat) — сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи [3]:

- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);

- загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації;

- праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т. ін.

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні як показано на рисунку 1.2.1.

Рис. 1.2.1. Класифікація загроз інформаційній безпеці

Варто одразу відзначити, що потрібен комплексний підхід до захисту інформаційних ресурсів підприємства. Використання одного-двох методів фактично не дасть позитивного результату.

Захист здійснюється програмним і адміністративним шляхом. До останнього відноситься [4]:

- створення внутрішніх нормативно-правових актів та підписання договорів з усіма співробітниками про “нерозголошення” та правила використання, передачі отриманої інформації;

- забезпечення контролю за виконанням локальних нормативних документів;

- наявність ефективного методу аутентифікації, з розмежуванням рівнів доступу до масивів інформації;

- регулярна перевірка працездатності, ефективності та своєчасне

оновлення систем управління інформаційною безпекою підприємства;

- постійне резервне копіювання для відновлення інформаційної системи в випадку збою, атаки або падіння.

Що стосується програмного забезпечення, то зараз існує велика кількість спеціалізованого ПЗ [4]:

- стаціонарне антивірусне ПЗ. Здатне перевіряти комп'ютер на "зараження" за встановленим графіком або запускатися адміністратором. У разі підозрілих дій окремої програми, може повідомити про це адміністратора, користувача або автоматично блокувати її. Також більшість антивірусів має функцію знезараження і відновлення постраждалих файлів;

- CloudAV. Оптимальне рішення для боротьби з вірусами, коли робочі станції, ПК і мають нестачу обчислювальних потужностей. На сам пристрій встановлюється легкий "Клієнт", що забезпечує зв'язок з "хмарою", де і проходить весь аналіз;

- впровадження DLP. Ці програми вирішують проблему основної загрози інформаційній безпеці підприємств – "витік" даних. Метод відноситься до складних і фінансово витратних, але є максимально ефективним;

- шифрування (криптографія). Може працювати по системі з одним або двома ключами. Останній варіант більш надійний, бо передбачає наявність різних ключів для шифрування і дешифрування;

- захист бездротових / дротових і локальних мереж за новітніми протоколами;

- блокування або фільтрація трафіку брандмауером, міжмережевим екраном. Це може бути мережевий фаєрвол або хост-серверний. Таким чином корпоративна мережа буде відокремлена від глобальної, з можливістю виходу в інтернет тільки в об'ємі встановлених обмежень;

- використання VPN. рішення для забезпечення інформаційної безпеки організації з розгалуженою системою філій, коли існує необхідність виходу в інтернет або віддалене підключення до локальної мережі;

- застосування проксі-сервера. Це значно прискорює відгук найбільш затребуваних ресурсів;

- фільтрація вмісту електронної пошти. Спеціальні фільтри переглядають вміст вхідної / вихідної кореспонденції, відсікають спам, заражені вірусом листи і блокують відсилання файлів/даних з конфіденційною інформацією;

- моніторинг електронної пошти, месенджерів та соціальних мереж працівників;

- SIEM моніторинг. Один з основних методів моніторингу процесів на підприємстві. Він фіксує і зберігає всі логи систем для подальшого їх аналізу на предмет виявлення несанкціонованих або шкідливих дій як ззовні, так і зсередини.

- моніторинг дій користувачів (UAM, User Activity Monitoring).

1.3 Моніторинг процесів за допомогою SIEM

SIEM (Security Information and Event Management) системи – це засоби, призначені для управління інформаційною безпекою в організаціях в цілому та управління подіями, отриманими з різних джерел (як зовнішніх, так і внутрішніх). SIEM системи здатні в режимі реального часу аналізувати події, що надходять від мережевих пристроїв та інших програм. Термін SIEM вперше з'явився в 2005 році і мав на увазі систему збору даних від пристроїв, розміщених у мережі підприємства, пристроїв безпеки, різних сервісів, призначених для управління обліковою інформацією та управління доступом, а також операційних систем, баз даних та встановлених у мережі додатків для

відстеження вразливостей та подальшого аналізу отриманих відомостей [5].

Таким чином, функції SIEM систем зводяться до наступного [5]:

Агрегація даних. Вся інформація про роботу мережевих пристроїв, серверів, датчиків від систем безпеки, різних програм надходить до журналів даних. SIEM системи керують такими журналами та допомагають співробітникам відділу інформаційної безпеки знаходити найбільш критичні події в інфраструктурі.

Кореляція. SIEM системи проводять пошук загальних значень і атрибутів і пов'язують між собою події, що надходять. Таким чином дані, що надходять від пристроїв та сервісів, приводяться до єдиного виду для подальшого аналізу.

Оповіщення. Після того, як система здійснила аналіз схожих між собою подій, вона повідомляє адміністратора безпеки про існуючі проблеми в інфраструктурі. Способи оповіщення можуть бути різними, включаючи виведення тривоги на панель моніторингу SIEM системи та сповіщення електронною поштою.

Панелі моніторингу, або інформаційні панелі, які надають інформацію про події у вигляді діаграм та графіків. Можливість візуалізації дозволяє визначити відхилення у поведінці, які різняться з типовою поведінкою різних систем.

Сумісність. SIEM системи впроваджуються в існуючу інфраструктуру підприємства та дозволяють автоматично збирати інформацію про події, формувати звіти для зібраних даних та застосовувати їх з метою управління безпекою та проведення аудиту.

Зберігання подій. Системи містять у собі сховища інформації, у яких зберігаються події безпеки. Ці події можуть сортуватися за часом, що дозволяє проводити експертизи та розслідування інцидентів.

Експертний аналіз. SIEM системи дозволяють шукати та аналізувати збережені події інформаційної безпеки, що також дає можливість проводити розслідування інцидентів інформаційної безпеки.

Джерелами даних для SIEM систем зазвичай служать системи виявлення і запобігання вторгнень, журнали серверів і комп'ютерів, комутатори, маршрутизатори, СУБД, антивірусні платформи, системи віддаленого доступу, DLP-системи, системи моніторингу дій користувачів, а також файлові сервери.

Враховуючи різноманітність можливих джерел подій у компанії, при виборі SIEM необхідно враховувати, від яких джерел система здатна приймати та обробляти дані. В даний час SIEM системи повинні проводити поведінковий аналіз та порівняння даних у режимі реального часу. Крім цього платформа повинна володіти функціями нормалізації та можливістю фільтрації інцидентів.

Даний функціонал найбільше підходить для моніторингу внутрішніх та зовнішніх процесів підприємства. Тому доцільно розглянути SIEM, як основний метод моніторингу процесів та управління безпекою інформаційних ресурсів на підприємстві та досвід його використання.

1.4 Моніторинг дій користувачів за допомогою систем UAM

Рішення моніторингу активності користувачів (UAM) — це програмні інструменти, які контролюють і відстежують поведінку користувачів на пристроях, у мережі та на інших IT-ресурсах підприємства. Багато організацій впроваджують інструменти моніторингу активності користувачів, щоб допомогти виявити та зупинити внутрішні загрози, ненавмисні чи зі зловмисними намірами. Діапазон моніторингу та використовуваних методів залежить від цілей компанії [6].

Запровадивши моніторинг активності користувачів, підприємства можуть легше виявляти підозрілу поведінку та зменшувати ризики ще до того, як вони призведуть до витоку даних, щоб мінімізувати збитки. Моніторинг активності користувачів, який іноді також називають моніторингом дій користувача, є формою стеження, але служить для проактивного перегляду активності кінцевого користувача, щоб визначити зловживання привілеями доступу або

політикою захисту даних через незнання чи зловмисний намір.

Метою моніторингу активності користувачів є захист інформації, забезпечуючи при цьому доступність і дотримання правил конфіденційності та безпеки даних. UAM виходить за рамки простого моніторингу мережевої активності. Натомість він може відстежувати всі типи дій користувачів, включаючи дії в системі, з даними, в програмах і мережі, наприклад, активність при веб-перегляді, чи мають користувачі доступ до несанкціонованих або конфіденційних файлів тощо.

Існують різні методи моніторингу та керування діями користувачів, наприклад [6]:

- відеозапис сесій;
- збір та аналіз журналів подій;
- перевірка мережевих пакетів;
- журнал натискань клавіш;
- моніторинг ядра;
- захоплення файлів/скріншотів;
- моніторинг пошти;
- моніторинг месенджерів;
- моніторинг соціальних мереж;
- моніторинг використання додатків та перегляд URL посилань.

Усю зібрану інформацію необхідно розглядати в межах політики компанії та ролі користувача, щоб з’ясувати, чи має місце невідповідна діяльність. Що вважати «неналежною діяльністю користувача» залежить від компанії, яка розгортає рішення UAM, і може включати будь-що: від відвідування особистих сайтів або покупок у робочий час до крадіжки конфіденційних даних компанії, таких як інтелектуальна власність або фінансова інформація.

Будь-який рівень моніторингу може накопичувати великі обсяги даних. Метою рішення моніторингу активності користувачів має бути пошук і відфільтрування корисної інформації, яка є цінною для захисту даних. За

допомогою ефективних процесів можливо негайно виявляти та досліджувати підозрілу активність користувачів. Можливо дізнатися, чи завантажують користувачі конфіденційні дані в загальнодоступні хмари, чи використовують несанкціоновані служби та програми, чи беруть участь у будь-якій іншій ризикованій діяльності під час використання мережі та інших ресурсів підприємства. Рішення моніторингу активності користувачів також допомагають гарантувати, що працівники не заволодіють конфіденційною інформацією підприємства при звільненні.

Рішення моніторингу активності користувачів також допомагають проводити моніторинг в реальному часі разом із детальним звітом про історичну діяльність. Моніторинг активності користувачів допомагає виявити зловживання привілеями, щоб зменшити ризик неналежних дій, які можуть призвести до зараження зловмисним програмним забезпеченням або витоку даних. Це також допомагає зменшити вартість відповідності стандартам безпеки, водночас пропонуючи інтелектуальні дані, необхідні для покращення заходів безпеки.

Існує безліч рішень, які можна використовувати для моніторингу активності користувачів. Ці рішення варіюються від загальних програм безпеки до цільових інструментів, призначених для відстеження сеансів і активності, створюючи повний контроль для кожного користувача. Існують також інструменти, відомі як рішення безпеки використання привілейованих облікових записів, які спрямовані на моніторинг і захист активності привілейованих облікових записів та їх централізованого керування [6].

Найкращі інструменти моніторингу активності користувачів включають системи оповіщення в реальному часі. Ці інструменти відстежують активність користувачів у фоновому режимі в режимі реального часу та сповіщають службу безпеки, коли виникає підозріла активність. Без елемента відстеження в реальному часі ризики можуть залишитися непоміченими, поки IT-відділ вирішує інші відомі проблеми. Завдяки сучасним рішенням немає необхідності

мати цілі IT-команди, які займаються моніторингом активності користувачів у реальному часі; хороше рішення безпеки, яке підтримує моніторинг активності користувачів, може виконати більшу частину важкої роботи.

Висновки до розділу 1

Отже, в першому розділі було проведено аналіз моніторингу внутрішніх та зовнішніх процесів при управлінні безпекою інформаційних ресурсів підприємства (установи, організації). Також було проаналізовано управління безпекою інформаційних ресурсів підприємства; процеси і засоби при моніторингу та протидії загроз; моніторинг процесів за допомогою SIEM; моніторинг дій користувачів за допомогою систем UAM.

Аналіз показав, що функціонал цих класів рішень найбільше підходить для вирішення проблеми моніторингу внутрішніх та зовнішніх процесів підприємства. Тому доцільно розглянути SIEM, як основний метод моніторингу процесів та управління безпекою інформаційних ресурсів на підприємстві та досвід його використання, та UAM як основне рішення для моніторингу зовнішніх процесів, активності користувачів, пошти, месенджерів та соціальних мереж.

Розділ 2 ДОСЛІДЖЕННЯ СУЧАСНИХ РІШЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ВИЗНАЧЕННЯ ДОЦІЛЬНОГО СПОСОБУ МОНІТОРИНГУ ЗОВНІШНІХ І ВНУТРІШНІХ ПРОЦЕСІВ В ІНТЕРЕСАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1 SIEM IBM QRadar

2.1.1 Опис та функціональні можливості IBM QRadar

SIEM – це система управління подіями інформаційної безпеки, яка може заздалегідь виявити атаки, загрози, слабкі і вразливі місця в інфраструктурі компанії. QRadar SIEM від компанії IBM використовує дані, що надходять від IT інфраструктури у вигляді потоку подій, далі проводить кореляцію подій і оцінку уразливостей, загроз, та виявлення інцидентів (порушень) інформаційної безпеки [7].

В QRadar включено кілька модулів: SIEM, Log Manager (управління журналами), Risk Manager (управління ризиками), Vulnerability Manager (управління уразливостями), колектори QFlow і VFlow та Incident Forensics.

Згідно зі звітом Gartner за 2021 рік (Рис. 2.1.1), одним з лідерів на ринку SIEM є IBM QRadar [8].

Source: Gartner (June 2021)

Рис. 2.1.1. Магічний квадрант Gartner для SIEM за 2021 рік

На рисунку 2.1.2 нижче представлені основні можливості модулів IBM QRadar:

Рис. 2.1.2. Основні можливості модулів IBM QRadar

Основний модуль IBM QRadar – QRadar SIEM. Даний модуль являє собою систему, яка збирає, аналізує і управляє подіями і потоками мережі з пристроїв, кінцевих точок, серверів, антивірусів, брандмауерів і різних систем запобігання вторгнень.

QRadar SIEM централізовано аналізує і консолідує зібрані дані за допомогою технології Sense Analytics, щоб виявити відхилення і складні загрози безпеки. Цей модуль збирає всі пов'язані між собою події в один інцидент для того, щоб надати IT-фахівцям розгорнуті дані про атаку, а саме час, мету, уразливості системи, облікові дані користувачів, відомості про

попередні загрози і вторгнення.

QRadar SIEM може автоматично виявляти джерела даних, а також має вбудовані шаблони. Ця функціональність дає можливість впровадити систему в найкоротші терміни. Консоль управління проста у використанні і дозволяє в консолідованому вигляді отримувати важливу інформацію з питань загроз і вразливостей для подальшого виявлення інцидентів інформаційної безпеки. Перевагою є те, що панель управління надається як функціонал, тому користувачі можуть самі створювати і налаштовувати свій робочий простір, як показано на рисунку 2.1.3. Деталізація функціоналу дозволяє набагато простіше виявляти, вибирати і аналізувати події і мережеві потоки, які безпосередньо пов'язані з порушеннями (інцидентами).

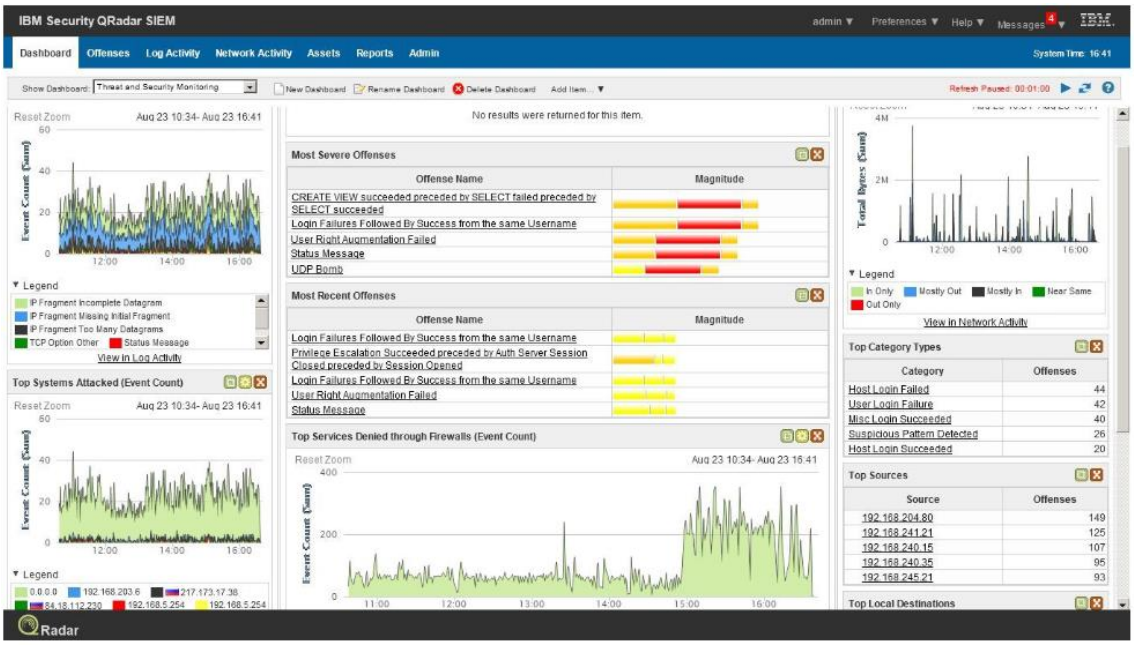


Рис. 2.1.3. Панель управління IBM QRadar

Основний елемент IBM QRadar SIEM – база даних, яка зберігає інформацію про події і потоки в мережі. Система оснащена технологією DPI (deep packet inspection), яка збирає події з брандмауерів і інших мережевих ресурсів і виконує глибокий аналіз мережевих пакетів.

Функціонал QRadar SIEM також забезпечує збір інформації про несанкціоновані дії користувачів (наприклад, доступ до недозволених ресурсів, розсилка спаму, перехід по фішингових посилань) і активності мережі на рівні додатків.

Більш того, IBM також надає підписку на IBM X-Force Threat Intelligence [9]. Дана опція надає список IP-адрес, які можуть нести загрозу і є потенційно шкідливими.

Функціональні можливості багато в чому визначають основні переваги для впровадження IBM QRadar на підприємстві. Слід виділити наступні переваги [7]:

1) проста конфігурація і розгортання на локальних ресурсах і в хмарному середовищі;

2) можливість відображення подій в реальному часі або за результатами минулих періодів;

3) комплексне виявлення інцидентів і управління уразливостями;

4) сильні аналітичні можливості завдяки яким IBM QRadar використовує контекст для підозрілих інцидентів, що призводить до зменшення великої кількості даних і більш високої швидкості виявлення інцидентів;

5) можливість надавати аналіз поведінки і відхилень даних мережевого потоку і журналів;

6) дані потоку (мережевий трафік) і дані подій об'єднані в єдину панель, що дозволяє користувачам точно визначати пріоритети даних про інциденти, зменшуючи кількість помилкових спрацьовувань;

7) IBM Security App Exchange дозволяє клієнтам, партнерам та іншим розробникам створювати додатки, що розширюють можливості QRadar;

8) інтегрується з усіма відповідними продуктами IBM і багатьма сторонніми

постачальниками.

З моменту своєї появи система QRadar стала популярним рішенням для фінансової та телекомунікаційної сфери. На сьогоднішній день QRadar широко використовується і в інших областях, в першу чергу в компаніях, у яких є безліч цінних даних, які необхідно захищати від різних загроз. Сюди входять і урядові органи, фінансові, медичні, торговельні, комунікаційні та транспортні компанії, які прагнуть зберегти свої дані для безперервності бізнесу.

Щоб впровадження IBM QRadar було успішним, компаніям необхідно розуміти, в яких ситуаціях вони можуть використовувати дане рішення. Тому краще всього змоделювати варіанти можливих загроз і порушень.

Що стосується термінів впровадження, то вони залежать від масштабу проекту. Наприклад, базову установку для збору даних про події та потоки можна виконати за кілька днів. А більші проекти, де обов'язково потрібно провести проектування з розрахунком можливих загроз, можуть тривати кілька місяців.

Вартість впровадження IBM QRadar залежить від кількості подій в секунду та вартості обраних ліцензій.

2.1.2 Аналізатор подій та процесів IBM QRadar SIEM

Система збору та аналізу подій IBM QRadar SIEM консолідує інформацію з журналів подій, що надходить від пристроїв, кінцевих точок і додатків в мережі, як показано на рисунку 2.1.4. QRadar SIEM нормалізує, аналізує та корелює події для виявлення загроз безпеки, а також використовує передовий механізм Sense Analytics для виявлення нормальної поведінки, аномалій, розкриття передових загроз і видалення хибно-позитивних результатів. Цей програмний модуль дає можливість зібрати всі пов'язані події в один інцидент [7].

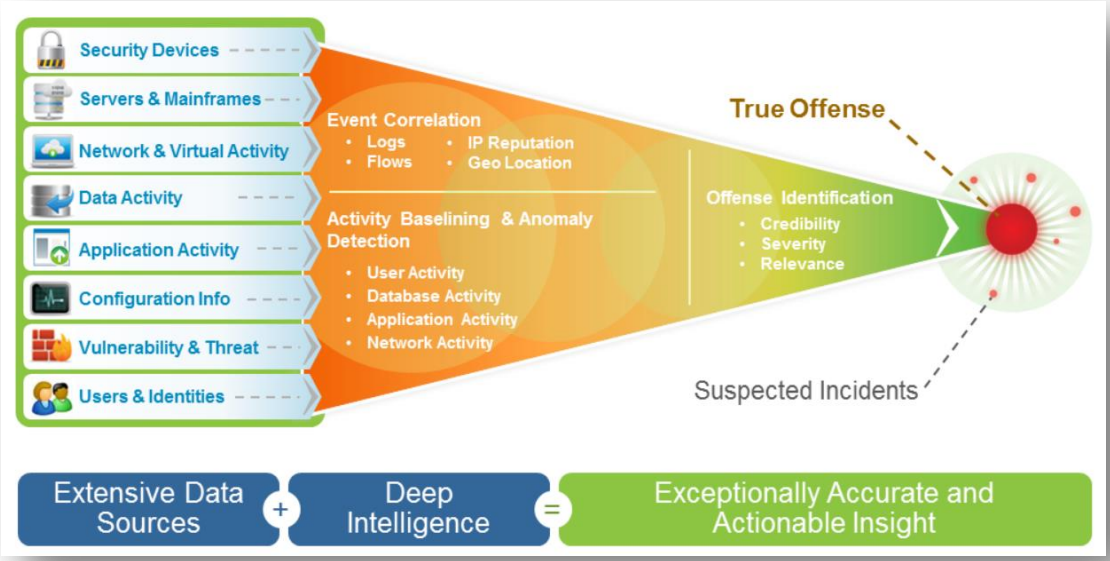


Рис. 2.1.4. Система збору та аналізу подій IBM QRadar SIEM

QRadar SIEM може включати в себе можливості аналізу загроз IBM X-Force Threat Intelligence зі списком потенційно шкідливих IP-адрес, адрес комп'ютерів з шкідливим ПЗ, джерел спаму та інших загроз, що дозволяє впровадити попереджувальний підхід до забезпечення безпеки. Крім того, для визначення пріоритетів продукт вміє зпівставляти загрози з подіями і даними з мережі [7].

Можливість створювати докладні звіти щодо доступу до даних і дій користувачів забезпечує більш ефективне управління загрозами і відповідність інформаційних систем стандартам.

Варто також згадати, що QRadar SIEM можна використовувати в локальних і хмарних середовищах.

Крім того, варто відзначити, що найближчим часом IBM планує використовувати платформу штучного інтелекту Watson в сфері безпеки, інтегрувавши її з програмним забезпеченням QRadar і базою даних X-Force. Це дозволить підвищити рівень аналітики для визначення характеру загроз, а також компенсувати брак IT-персоналу в сфері інформаційної безпеки [10].

Розглянемо зазначені вище можливості IBM QRadar SIEM більш детально. Забезпечення прозорості в реальному часі дозволяє виявити неправильне використання додатків, внутрішнє шахрайство та інші загрози, які можна було б випустити з уваги серед мільйонів подій, що відбуваються щодня. Рішення дозволяє забезпечити збір журналів і подій з різних джерел, включаючи пристрої безпеки, операційні системи, програми, бази даних та системи управління доступом і ідентифікацією.

Дані мережевих потоків надходять від комутаторів і маршрутизаторів, включаючи дані рівня 7 (рівень додатків). Передбачено отримання інформації від систем управління доступом та ідентифікацією і таких служб інфраструктури, як протокол динамічної настройки вузла (DHCP), а також від сканерів уразливості мереж і додатків.

QRadar SIEM виконує миттєву нормалізацію подій і зіставлення з іншими даними для виявлення загроз і створення нормативних звітів.

Рішення визначає пріоритети подій, виділяючи невелику кількість реальних порушень, які несуть найбільш серйозну загрозу для бізнесу. Виявлені аномалії дають можливість виявити зміни в поведінці, пов'язані з додатками, комп'ютерами, користувачами і сегментами мережі. При використанні ПЗ IBM X-Force Threat Intelligence також визначаються дії, пов'язані з підозрілими IP-адресами [9].

QRadar дає можливість більш ефективно управляти загрозами, відстежуючи серйозні інциденти та надаючи посилання на всі необхідні дані для проведення аналізу. Це дозволяє виявити дії в неробочий час або незвичайне використання додатків і хмарних сервісів, а також мережеву активність, яка не відповідає збереженим шаблонам використання.

Для поліпшення аналітики QRadar підтримує можливість пошуку в подіях і потоках даних в режимі близькому до реального часу, а також по збережених

даних. Можливе виконання об'єднаного пошуку у великих розподілених середовищах. Для більш глибокого розуміння і кращого відображення додатків, баз даних, продуктів для спільної роботи і соціальних мереж можна використовувати пристрої IBM QRadar QFlow і IBM QRadar VFlow Collector, які дозволяють проводити детальний аналіз мережевих потоків на рівні 7 моделі OSI [7].

Можливість установки в хмарі SoftLayer дозволяє QRadar SIEM отримувати оперативну інформацію про безпеку в хмарних середовищах. Причому збір подій і потоків даних від програм виконується як в хмарі, так і на локальних ресурсах [11].

QRadar має інтуїтивно зрозумілий модуль звітів, що не вимагає спеціальних баз даних або особливих навичок від IT-адміністраторів. Створення звітів про доступ до даних і активності користувачів з можливістю відстеження інформації по імені і IP-адресою гарантує дотримання політик безпеки, а також відповідність нормативним вимогам.

З інструментом QRadar SIEM інтегрується ряд модулів, що підвищують його ефективність. Одним з найбільш важливих є QRadar Risk Manager, який зіставляє інформацію про уразливість з даними про топологію мережі і з'єднання. Цей модуль виявляє уразливості в мережі компанії та додатках, оцінивши ризики і мінімізувавши їх. Risk Manager відстежує конфігурацію комутаторів, маршрутизаторів, мережевих екранів і систем запобігання вторгнень (IPS), розпізнаючи умови, що можуть представляти загрозу безпеці. Крім того, він дозволяє моделювати мережеві атаки та інші сценарії вторгнень, вносити в конфігурацію мережі зміни, які дають можливість оцінити масштаб загрози.

Ще один цікавий інструмент – модуль QRadar Log Manager. Він збирає і обробляє дані про події в режимі реального часу, що надходять від маршрутизаторів, комутаторів, брандмауерів, мереж VPN, систем виявлення і

запобігання вторгнень (IDS / IPS), антивірусних програм та інших джерел. Log Manager дає можливість спростити ведення необхідної звітності та контроль за дотриманням нормативно-правових вимог.

2.2 SIEM Splunk

2.2.1 Опис та функціональні можливості Splunk

Splunk — це аналітичний інструмент SIEM, який збирає, аналізує та корелює великі обсяги мережевих та інших машинних даних (мережа, кінцеві точки, доступ, шкідливі програми, вразливості) у режимі реального часу. Splunk, який керується через веб-браузер, надає командам безпеки відповідну та дієву інформацію, необхідну для більш ефективного реагування на загрози та підтримки безпеки в корпоративному масштабі [12].

Завдяки Splunk Enterprise Security фахівці з безпеки можуть швидко виявляти внутрішні та зовнішні атаки та вживати відповідні заходи. Це дозволяє спростити операції захисту від загроз, мінімізувати ризики та забезпечити безпеку бізнесу. Splunk Enterprise Security оптимізує всі аспекти захисту та підходить для організацій будь-якого масштабу та професійного рівня.

Згідно зі звітом Gartner за 2021 рік [13], Splunk є одним з лідерів на ринку SIEM, як показано на рисунку 2.2.1:

Рис. 2.2.1. Магічний квадрант Gartner для SIEM за 2021 рік

Далі розглянемо функціональні можливості Splunk більш детально. Серед основних функцій та особливостей Splunk можна виділити наступні [14]:

Швидке реагування на інциденти. Splunk дозволяє адміністраторам безпеки аналізувати великі набори даних, виявляти зловмисну мережеву активність і реагувати на загрози.

Інтелектуальний аналіз подій. Splunk автоматично збирає, зберігає та співвідносить мережеву та користувацьку активність в режимі реального часу, забезпечуючи команду безпеки актуальними даними, які можуть використовуватись для значного покращення рівня безпеки.

Повна видимість. Splunk надає аналітикам безпеки та іншим ключовим зацікавленим сторонам детальне розуміння продуктивності та активності мережі на пристроях, програмах тощо.

Покращені операції безпеки. Розширені можливості машинного навчання Splunk оптимізують операції безпеки шляхом автоматизації завдань і робочих процесів, зменшуючи необхідність виділяти велику кількість годин ручної праці та людського нагляду.

Splunk безперервно відстежує всі мережеві ресурси та їх активність, щоб виявити аномальну поведінку ще до того, як вона стане серйозною загрозою для організації. Використовуючи інформацію, яку надає Splunk, аналітики безпеки можуть отримати докладне, кероване даними уявлення про продуктивність, стан і вразливість мережі в будь-який момент часу. При виявленні шкідливих або високоризикових подій, Splunk має можливість автоматично сповістити адміністраторів з детальним описом загрози.

Виявлення загроз. Інтелектуальний моніторинг інфраструктури, програм, користувачів та інших мережевих ресурсів у різних середовищах дозволяє Splunk виявляти активні загрози або аномальну поведінку в реальному часі. Splunk проводить кореляцію журналів подій, щоб виявити індикатори компрометації або зловмисні зв’язків, щоб аналітики безпеки могли негайно впоратися з потенційними загрозами до того, як мережі буде завдано будь-якої значної шкоди. До виявлення загроз входить [14]:

- видимість та аналітика мережі;
- інтелектуальна класифікація загроз;
- кореляція журналу подій між пристроями та середовищами;
- методологія блокування Cyber Kill Chain;
- аналітика поведінки користувачів (UBA) для виявлення поведінкових та статистичних аномалій.

Аналітика поведінки користувачів. Використовуючи алгоритми машинного навчання, Splunk визначає поведінку мережі, а також корелює поведінку користувачів між джерелами даних і середовищами, щоб виявити загрози безпеці. Адміністратори безпеки автоматично повідомляються про

будь-які відхилення від звичайної мережевої активності, щоб мати можливість швидко відреагувати на загрози та за потреби провести багатоетапне розслідування інциденту.

Реагування на інциденти. Adaptive Response Framework від Splunk надає можливість контекстуалізувати дані подій у різних середовищах і автоматизувати процеси реагування на інциденти, щоб мати можливісь швидко підтвердити, визначити пріоритет та відреагувати на загрози.

Криміналістика інцидентів. Splunk щодня відстежує та реєструє величезні набори інформації про безпеку, отримані з різноманітних джерел. Команда служби безпеки може використовувати це джерело даних для проведення ретельних судових розслідувань щодо походження злому або перевірки нових загроз, щоб отримати глибше розуміння ефективності своїх заходів безпеки (і внести відповідні покращення).

2.2.2 Компоненти та архітектура Splunk

Архітектурно Splunk складається з декількох компонентів як показано на рисунку 2.2.2 [15]:

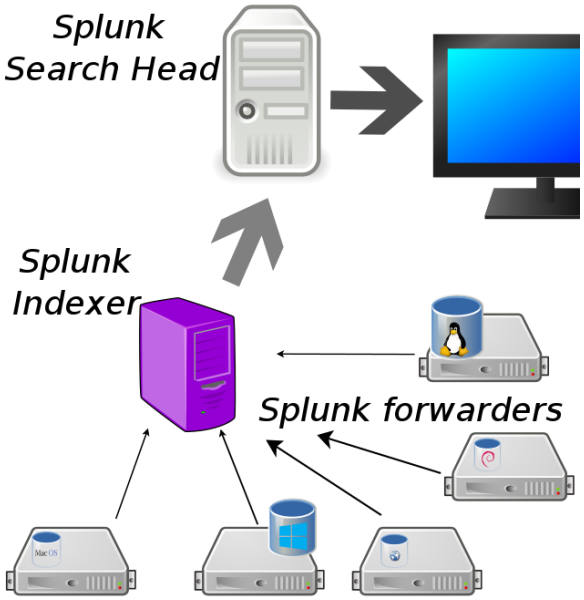


Рис. 2.2.2. Архітектура Splunk

1) Splunk Indexer (індексатор) – використовується для зберігання та індексування даних для покращення ефективності пошуків Splunk. Перетворює сирі дані в події, зберігає їх на диску та додає до індексу, що забезпечує можливість швидкого пошуку. Індексатор створює такі файли, розділяючи їх на каталоги, які називаються сегментами:

- стиснуті сирі дані;

- індекси, що вказують на необроблені дані (файли .TSIDX);

- файли метаданих.

Індексатор виконує загальну обробку подій для даних журналу, наприклад, застосування мітки часу та додавання джерела, а також може виконувати визначені користувачем дії перетворення, щоб отримати певну інформацію або застосувати спеціальні правила, наприклад фільтрацію небажаних подій.

У Splunk є можливість налаштувати кластер індексаторів із реплікацією між ними, щоб уникнути втрати даних і надати більше системних ресурсів і місця для зберігання та обробки великих обсягів даних.

2) Splunk Search Head – виконує роль звітування та допомагає отримати розвідувальні дані. Надає користувацький інтерфейс, який використовується для взаємодії з Splunk як показано на рисунку 2.2.3. Дозволяє користувачам шукати та запитувати дані Splunk, а також взаємодіє з індексаторами, щоб отримати доступ до конкретних даних.

Splunk надає архітектуру розподіленого пошуку, яка дозволяє масштабувати роботу з великими обсягами даних, а також щоб краще контролювати доступ і географічно розподілені дані. За сценарію розподіленого пошуку адміністратор надсилає пошукові запити групі індексаторів, які також називаються одноранговими пошуковими вузлами. Індексатори виконують пошук локально та повертають результати до Splunk

Search Head, який об’єднує результати та повертає їх користувачеві.

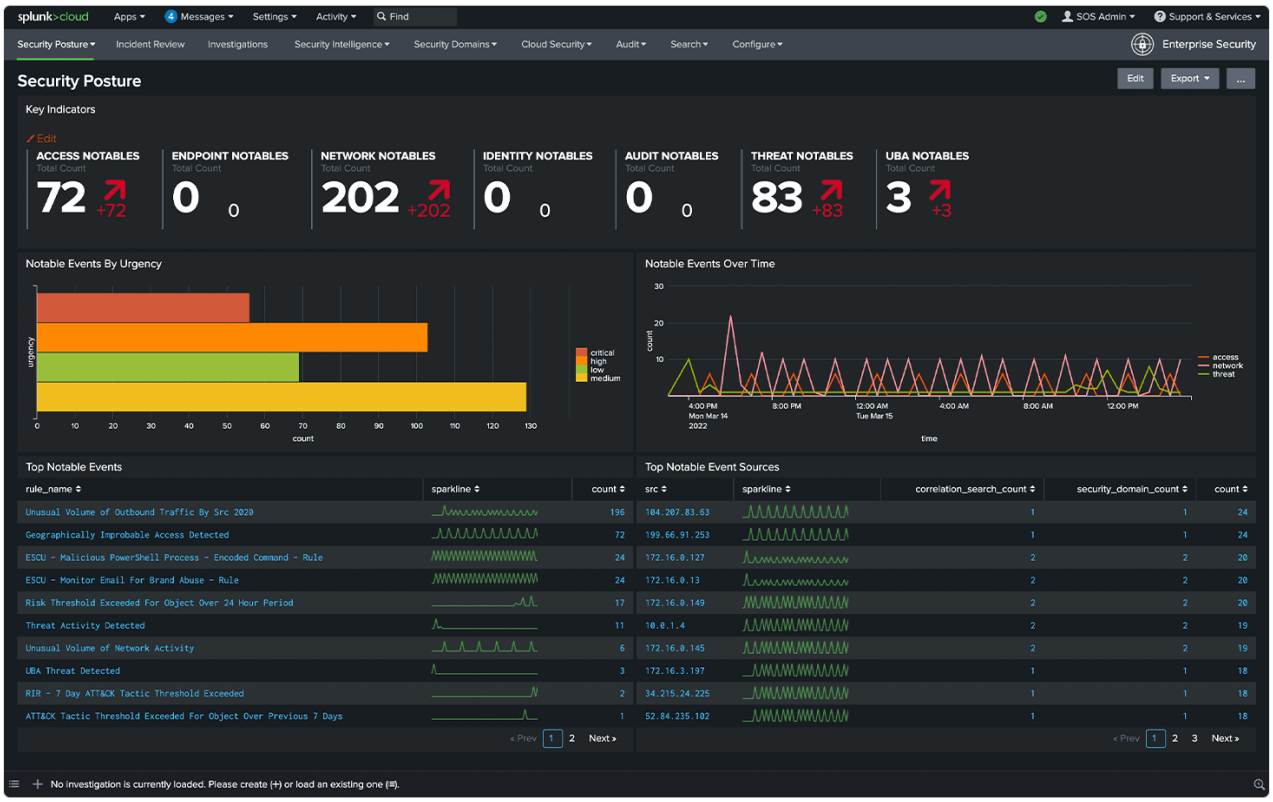


Рис. 2.2.3. Інтерфейс адміністратора Splunk

3) Splunk Forwarder – це агент, який ви розгортається в IT-системах для збору журналів. Надсилає зібрані журнали до Splunk Indexer. Splunk має два типи форвардерів:

- Universal Forwarder – пересилає сирі дані без попередньої обробки. Це швидше та потребує менше ресурсів на хості, але призводить до надсилання величезної кількості даних до індексатора;

- Heavy Forwarder – перед відправкою даних до індексатора, виконує їх синтаксичний аналіз та індексування. Надсилає лише проаналізовані події до індексатора.

4) Сервер розгортання (опціанально) – використовується для розгортання конфігурацій Splunk.

5) Менеджер ліцензій (опціонально) – перевіряє інформацію про ліцензію користувача. Ліцензування здійснюється на основі використання та обсягу.

2.3 SIEM ArcSight

2.3.1 Опис та функціональні можливості ArcSight

Microfocus — це компанія з кібербезпеки, яка у 2000 році випустила продукт під назвою «SIEM ArcSight». Основною метою цього продукту є забезпечення аналітики та безпеки даних і програмного забезпечення та аналізу роботи пристроїв і систем. На підприємствах цей продукт також використовується як метод керування журналами подій. SIEM ArcSight забезпечує чудовий і безпечний досвід споживача з дружнім інтерфейсом. Однією з важливих функцій SIEM ArcSight є захист підключених пристроїв і потоків даних. Багато додатків використовують цей інструмент, наприклад уряд організації, охорона здоров’я, роздрібна торгівля, фінанси, соціальні мережі та комунікації. ArcSight також допомагає споживачам ідентифікувати та захистити себе від загроз безпеки. Тепер ArcSight став дочірнім продуктом HP (Hewlett-Packard) [16].

ArcSight — це корпоративний менеджер безпеки (Enterprise Security Manager) або ESM, який виконує функції прийому та інтерпретації системних журналів, встановлення підключень до каналів аналітики загроз, кореляції пристроїв у реальному часі, аналітики даних, попередження про інциденти безпеки та представлення даних користувачам через інформаційні панелі та інші едементи користувацького інтерфейсу, звітність. ESM також підтримує побудову базового профілю безпеки та механізм сповіщень, якого можна досягти за допомогою інтеграції з різними аналітичними продуктами, такими як аналітика поведінки користувачів ArcSight або UBA. ArcSight також включає функції збагачення даних, такі як оцінка даних, моделювання мережі,

геолокації, моделювання користувачів і пошук вразливостей [17].

Далі розглянемо функціональні можливості системи ArcSight більш детально. Нижче наведено основні функціональні можливості SIEM ArcSight [16]:

1. Відслідковування загроз: це одна з важливих функцій керування безпекою. Він включає доступ до даних у структурі загроз ArcSight, а також допомагає отримувати оновлення для елементів безпеки, таких як правила, звіти, випадки використання та інформаційні панелі.

2. Моніторинг подій та процесів: найважливіша функція інструменту SIEM ArcSight, яка допомагає аналізувати дані з різних пристроїв, а також включає аналіз даних про кіберзагрози через стандартні інформаційні панелі STIX і CIF. Отримання даних з джерела складається з розумних конекторів, які підтримують формат подій, API, журнали, сирі файли, журнали брандмауера, Net flow, XML/JSON і підключення до баз даних.

3. Високий рівень продуктивності: 100 000 подій за секунду або EPS.

4. Реалізація: відповідно до звіту Gartner, ArcSight — це гнучко налаштовуваний інструмент для підтримки різноманітних випадків керування загрозами та відповідності стандартів. ArcSight API забезпечує широку інтеграцію даних у кількох середовищах SOC.

5. Керування: це популярна та найкраща функція інструменту ArcSight. За допомогою цієї функції модульні пакети налаштувань надають можливість експортувати різноманітні користувацькі правила, інший вміст і інформаційні панелі SIEM, які спільно використовуватимуться між клієнтами, пристроями та системами. Ця функція також включає централізоване керування, звітування про події безпеки підприємства та аналіз даних.

6. Підтримка: надійне керування даними та підтримка безпеки.

7. Масштабованість: можливість масштабувати систему до 100 000 EPS

разом із розподіленою кореляцією.

2.3.2 Компоненти та архітектура SIEM ArcSight

Архітектурно ArcSight складається з декількох компонентів як показано на рисунку 2.3.1 [16]:

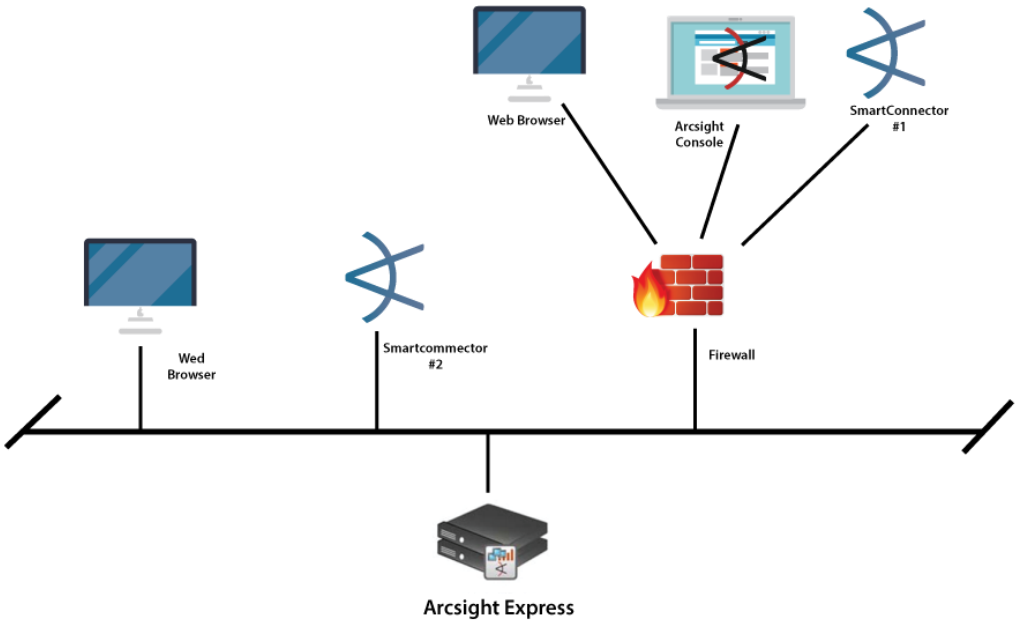


Рис. 2.3.1. Архітектура ArcSight

В процесі роботи з ArcSight аналітики використовуватимуть консоль ArcSight або веб-браузер для доступу до ESM, Logger і CA. Події з усіх Smart Connector направлятимуться до ESM для збагачення та кореляції в реальному часі, і після того будуть перенаправлені знову до Logger для тривалого зберігання. Всі Smart Connector керуються віддалено за допомогою диспетчера ESM. Події з усіх Smart Connector можуть пересилатися до окремих Logger з ціллю балансування навантаження.

Нижче наведено основні компоненти Arcsight [16]:

1. Smart Connector. Використовується для: збору журналів подій з

мережевих пристроїв та їх агрегації; фільтрації даних для заощадження пам’яті і пропускної здатності; нормалізації загальної схеми подій; класифікації подій в загальному форматі для установки правил та фільтрів.

2. ArcSight Manager: Загальні функції включають: оцінку подій відповідно до моделі мережі та вразливостей; створення звітів про загрози в реальному часі; запис подій до механізму CORR.

3. Механізм подій CORR або механізм збереження та пошуку, оптимізований кореляцією. Основні функції: впорядковування даних та збереження їх для довготривалого зберігання.

Компоненти інтерфейсу користувача ArcSight [17]:

1. Командний центр ArcSight. Основні функції: керування користувачами, даними про події та сховищем; створення звітів і оновлення ліцензії.

2. Консоль ArcSight. Основні функції: створення фільтрів, звітів, шаблонів, правил та інформаційних панелей; моніторинг даних безпеки; адміністрування користувачів і робочих процесів.

3. ArcSight web – це веб-інтерфейс ArcSight, який допомагає стежити за подіями; використовується для перегляду інформаційних панелей, звітів і повідомлень аналітиків безпеки.

4.ArcSight risk insight – допомагає оцінити вплив на бізнес конкретних загроз для визначення правил.

2.4 Система моніторингу дій користувачів Ekran System

2.4.1 Опис та функціональні можливості Ekran System

Ekran System – це універсальна програмна платформа для моніторингу активності користувачів, виявлення та мінімізації внутрішніх загроз в корпоративних мережах.

Ekran дозволяє виявляти, розслідувати та запобігати потенційним інсайдерським загрозам шляхом контролювання дій користувачів та миттєвих сповіщень при відхиленні дій користувачів від встановлених внутрішніх політик безпеки.

Цілі Ekran System [18]:

- Detection: проактивний захист від небезпечних дій звичайних та привілейованих користувачів, що були скоєні свідомо або несвідомо;
- investigation: забезпечення спеціалістів з інформаційної безпеки детальними матеріалами щодо інциденту з метою проведення подальшого розслідування;
- prevention: зниження кількості інцидентів шляхом стримування небезпечної поведінки користувачів у поєднанні із записом екрану.

Далі розглянемо функціональні можливості Ekran System більш детально. Серед основних функцій та особливостей Ekran System можна виділити наступні [18]:

- запис метаданих, логування і відеозапис дій користувача – вікна або всього екрану його сесії незалежно від протоколу або додатка, діючи подібно камері відеоспостереження;
- моніторинг та блокування USB-пристроїв;
- персоніфікація облікових записів у випадку, якщо ними користується більше однієї особи;
- вбудований перелік правил сповіщень, що охоплюють найпоширеніші сценарії небезпечної діяльності користувачів;

- примусове дотримання встановлених політик інформаційної безпеки користувачами шляхом попередження та блокування дій, що порушують ці правила;
- відстеження змін в поведінці користувачів: спеціалісти з інформаційної безпеки можуть відслідковувати спрацювання правил поведінки, а також виявляти користувачів, які продовжують їх порушувати;
- аналіз поведінки користувачів з метою виявлення дій, які є підозрілими, або порушують політику інформаційної безпеки;
- підтримка всіх основних ОС;
- віддалена установка Клієнтів на Windows системи;
- інтеграція з Active Directory, SIEM, Ticketing System;
- багатофакторна автентифікація користувачів;
- наявність PAM (Privileged Access Management) модулю, що дозволяє забезпечити безпечний віддалений доступ до критичних кінцевих точок.

2.4.2 Компоненти та архітектура Ekran System

Архітектурно рішення Ekran System складається з декількох компонентів як показано на рисунку 2.4.1 [19]:

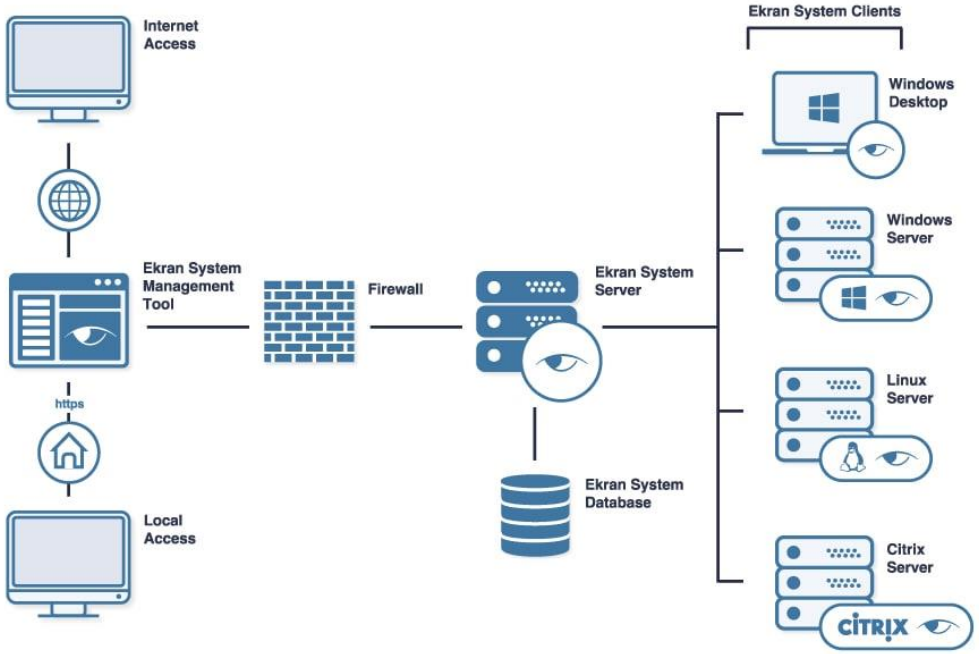


Рис. 2.4.1. Архітектура Ekran System

1. Клієнти (Ekran System Clients) – агенти Ekran System, допомагають контролювати активність користувачів, керувати доступом та запобігати шкідливим діям на будь-яких типах настільних ПК та серверів:

- сервери інфраструктури;
- термінальні сервери;
- фізичні та віртуальні ПК.

Підтримувані платформи:

- Windows;
- Linux;
- UNIX;
- Citrix;
- VMware;
- Mac OS.

2. Сервер (Ekran System Server) – агенти надсилають дані моніторингу на системний сервер Ekran, який аналізує дані та зберігає їх у центральній базі даних. Якщо дані моніторингу містять події, які відповідають визначеним користувачем правилам, Сервер згенерує миттєві сповіщення та за потреби ініціює автоматизовану реакцію на інцидент. Сервер також відповідає за збереження даних конфігурації, надсилання пакетів оновлень Клієнтам, проведення очищення бази даних, створення звітів та відповідної статистики.

3. Веб-консоль управління (Ekran System Management Tool) – це основний інтерфейс адміністратора Ekran System. Вона дозволяє керувати Клієнтами, налаштовувати сповіщення про потенційні інциденти, визначати та призначати дозволи користувачам Ekran, керувати доступом до кінцевих точок, а також переглядати та аналізувати дані моніторингу, отримані від Клієнтів.

4. База даних (Ekran System Database) – сховище даних Ekran System (MS SQL або PostgreSQL), що забезпечує гнучкий вибір залежно від потреб у безпеці, економічності та швидкості обробки.

5. Файлове сховище (Ekran System File share, опціонально) – необов’язковий компонент Системи, який використовується для зберігання скріншотів (цифрових даних).

Кожен з серверних компонентів (Ekran System Server, Веб-консоль управління та База даних) можуть бути встановлені на одній платформі («All-in-One» розгортання).

Процес взаємодії компонентів Ekran System між собою:

1. На робочих станціях та серверах, що контролюються, працює Клієнт (Ekran Client).

2. Клієнт збирає інформацію про діяльність користувача та відправляє на Ekran System Server.

3. Ekran System Server обробляє, стискає та зберігає отриману інформацію в базу даних.

4. Спеціалісти з інформаційної безпеки оперують даними, реагують на внутрішні загрози та адмініструють Ekran System за допомогою Management Tool.

Веб-інтерфейс Ekran System Management Tool зображено на рисунку 2.4.2:

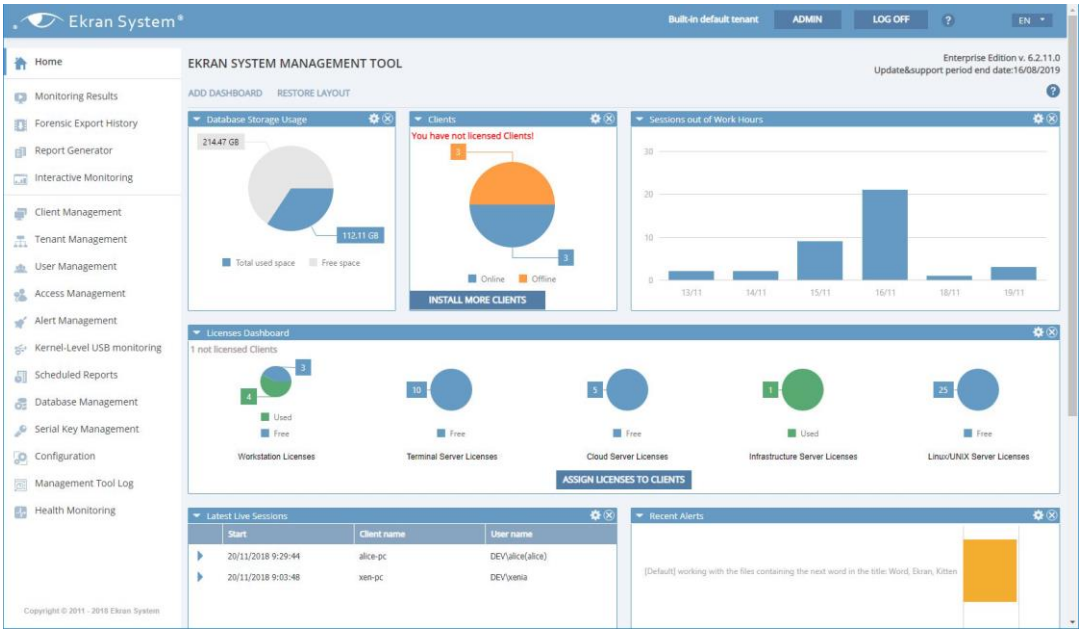


Рис. 2.4.2. Веб-інтерфейс системи Ekran System

2.5 Система моніторингу дій користувачів Mirobase

2.5.1 Опис та функціональні можливості Mirobase

Mirobase – це система контролю активності працівників на ПК, планшетах та мобільних пристрояї у робочий час. Mirobase призначений для визначення ефективності дій персоналу, моніторингу використовуваних програм, інтернет-ресурсів та месенджерів, блокування витоку конфіденційної інформації. Особливостями програмного комплексу є такі функції, як розпізнавання дій співробітника по «клавіатурному почерку» та голосове DLP (Data Loss Prevention) – розпізнавання, переклад та запис розмови у текстові файли та реагування на ключові фрази. Додаткові можливості – облік робочого часу працівників, контроль витрат паперу на принтерах, облік змін у апаратній

частині ПК. Для економії обчислювальних потужностей підприємства рекомендується використовується SaaS версію Mirobase [20].

Далі розглянемо функціональні можливості системи Mirobase більш детально. Серед основних функцій та особливостей можна виділити наступні [20]:

1) Прогноз ризиків та аналізатор ефективності роботи кожного співробітника. За алгоритмом дій співробітників Mirobase розпізнає «шкідливу» та «корисну» активність. Наприклад, для менеджера з продажу час, проведений у LinkedIn або на спеціалізованому форумі, розцінюватиметься системою як корисний: він вивчає профіль компанії-клієнта та шукає виходи на осіб, які приймають рішення. Водночас, аномально висока активність будь-якого представника колективу на розважальних сайтах буде розцінена як нецільове витрачання робочого часу та сприйнята як ризик.

Mirobase також виявляє безпосередні бізнес-ризики, пов'язані з витоком важливої для компанії інформації. Наприклад, якщо програма визначає, що з робочого комп'ютера з особистої адреси співробітника відправляється лист, де фігурує словосполучення «клієнтська база» чи «фінансові показники», вона розцінює це як шкідливу активність. Оповіщення про неї буде негайно надіслано керівнику.

2) Моніторинг активного часу комп'ютера співробітника (скільки робочого часу працівник витрачає на активну роботу з комп'ютером, а скільки його немає на робочому місці):

- час першого увімкнення та останнього вимикання комп'ютера співробітника;

- загальна кількість часу роботи комп'ютера у відсотках від тривалості робочого дня;

- час активного використання комп'ютера протягом усього робочого дня (графічно).

3) Моніторинг програм (якими програмами співробітник користується в робочий час, і з якими цілями):

- перелік усіх програм, з якими працював співробітник, включаючи Skype, ICQ, Lync та інші;

- запис назви програми, шляху до файлу, заголовоку вікна, загального часу роботи з програмою, тексту, введеного користувачем;

- можливість фільтрування даних за заданими ознаками.

4) Моніторинг відвідуваних веб-сайтів (скільки часу працівник витрачає на використання мережі інтернет у робочих цілях, а скільки – в особистих):

- url-адреси відвідуваних веб-сайтів;

- час, протягом якого сторінку було просто відкрито і час фактичної роботи з нею;

- текст, що вводиться в браузері, включаючи текст у поштових сервісах;

- запити в пошукових системах;

- можливість фільтрування даних за заданими ознаками;

- повідомлення про відвідування небажаних сайтів (наприклад, соціальні мережі, сайти з пошуку роботи).

5) Моніторинг тексту, що вводиться (яка, а також куди і кому повідомляється або пересилається важлива комерційна інформація):

- зміст повідомлень користувача з поштових додатків, онлайн-клієнтів, e-mail та інших програмах;

- перегляд тексту запитів у пошукових системах;

- перехоплення вхідних та вихідних повідомлень у поштових клієнтах Outlook, Outlook Express, Bat, Windows Live, Mozilla Thunderbird;

- контроль листування співробітників у месенджерах – Skype, Lync, ICQ, QIP, RnQ, Spark;

- повідомлення про використання підозрілих словосполучень, наприклад, «зарплата», «начальник» тощо;

6) Моніторинг файлових операцій (чи були видалені або відправлені важливі файли і чи не була важлива база даних скопійована на флеш накопичувач):

- усі операції з файлами, ініційовані співробітниками - копіювання, перенесення, видалення, копіювання в буфер обміну;

- вміст буфера обміну - текстова/графічна інформація, яка копіюється для подальшої вставки;

- перехоплення файлів, що надсилаються через поштові програми, файлообмінні сервери, месенджери (Skype, ICQ, QIP);

- перехоплення підписаних цифровим підписом та зашифрованих повідомлень (тільки в MS Outlook);

- можливість заборони відправки файлів через інтернет, запису на USB-накопичувач або заборона будь-якого використання USB-накопичувачів.

7) Моніторинг голосових розмов:

- фіксація факту дзвінка та його тривалості;

- автоматичний запис голосових розмов Skype, Lync;

- автоматичний запис голосових розмов телефоном;

- автоматичний запис із мікрофона комп'ютера співробітника;

- аналіз аудіофайлів.

8) Моніторинг знімків з екрану (перегляд робочого столу на комп'ютері співробітника. Частота знімків екрану, а також їх якість налаштовуються).

9) Контроль друку та перехоплення роздрукованих документів (30% випадків витоку конфіденційної комерційної інформації трапляються у вигляді винесення роздрукованої документації):

- можливість встановлення різних тарифів на друк для кожного принтера індивідуально;

- хто, що, коли, на якому принтері та скільки інформації роздрукував;

- перехоплення роздрукованих документів за допомогою функції тіньового копіювання.

10) Моніторинг підозрілих дій та контроль обладнання (завдяки контролю обладнання на комп'ютерах співробітників є можливість вчасно дізнатися про можливі крадіжки обладнання з комп'ютерів):

- оповіщення про крадіжку чи заміну на менш потужну деталь робочого комп'ютера співробітника;

- список всього обладнання та встановлених програм на комп'ютері співробітника;

- повідомлення про запуск небажаних або шкідливих програм на комп'ютері співробітника (ігри, відео, шпигунське програмне забезпечення тощо);

11) Загальний звіт – аналітичний звіт, що містить узагальнену інформацію щодо співробітника/співробітників, а саме:

- запізнення, ранні відходи з роботи та прогули;

- характеристики ефективності;

- кількість тексту, що роздруковується;

- наявність підозрілої активності;

- найбільш використовувані програми та веб-сайти.

12) Пошук співробітника за критерієм (за допомогою спеціальної форми здійснюється пошук співробітника, який задовольняє певні характеристики, наприклад, використання певних програм, відвідування конкретних веб-сайтів, використання характерних слів).

13) Майстер звітів (майстер звітів формує звіти за співробітником або групою співробітників за заданими параметрами у будь-яких інформаційних розрізах).

14) Експорт звітів до Excel (дана можливість дозволяє експортувати звіти в Microsoft Excel або OpenOffice Calc. Підтримуються формати XLS та CSV).

2.5.2 Компоненти та архітектура Mirobase

Архітектурно Mirobase складається з декількох компонентів як показано на рисунку 2.5.1 [21]:

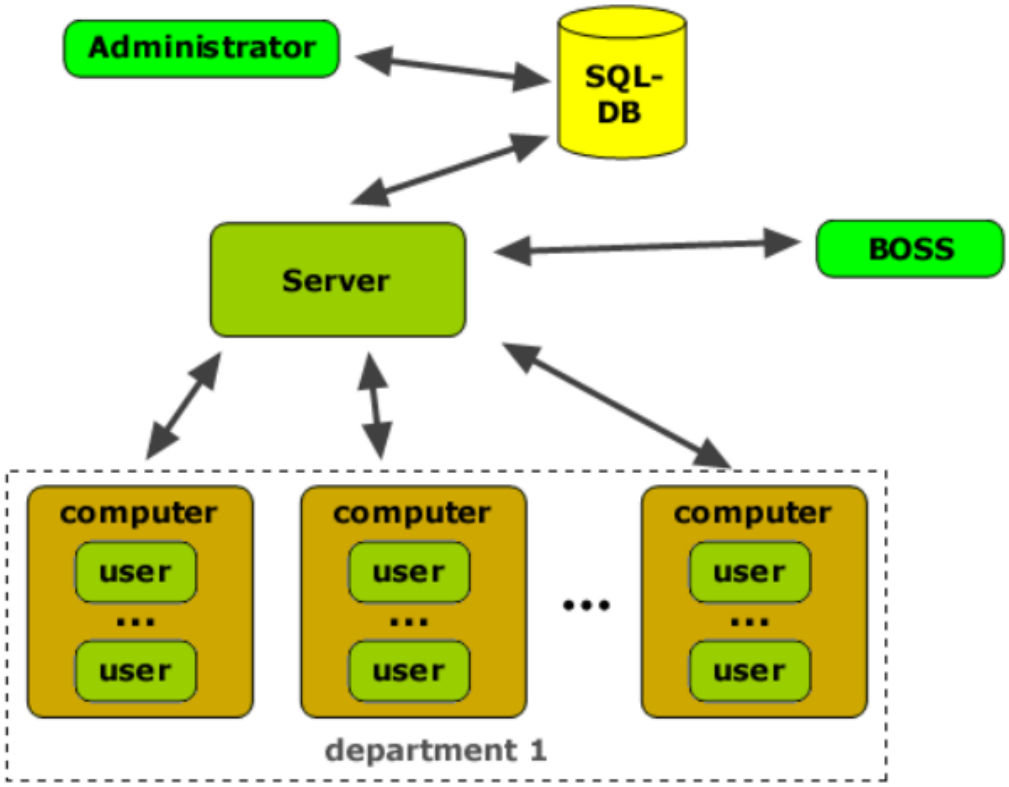


Рис. 2.5.1. Архітектура Mirobase

1. Mirobase Agent – агенти системи, які встановлюються на ПК. Допомогають контролювати активність користувачів та запобігати шкідливим діям на ПК.

2. Mirobase Server – серверний компонент системи, який аналізує дані та зберігає їх у SQL-DB. Якщо дані моніторингу містять події, які відповідають визначеним адміністратором правилам, сервер згенерує сповіщення та за потреби ініціює автоматичну реакцію на інцидент. Також відповідає за збереження даних конфігурацій, створення звітів та відповідної статистики.

3. Mirobase BOSS – основний інтерфейс адміністраторів для моніторингу активності користувачів. Інтерфейс адміністратора показано на рисунку 2.5.2.

4. Mirobase SQL-DB – сховище даних Mirobase.

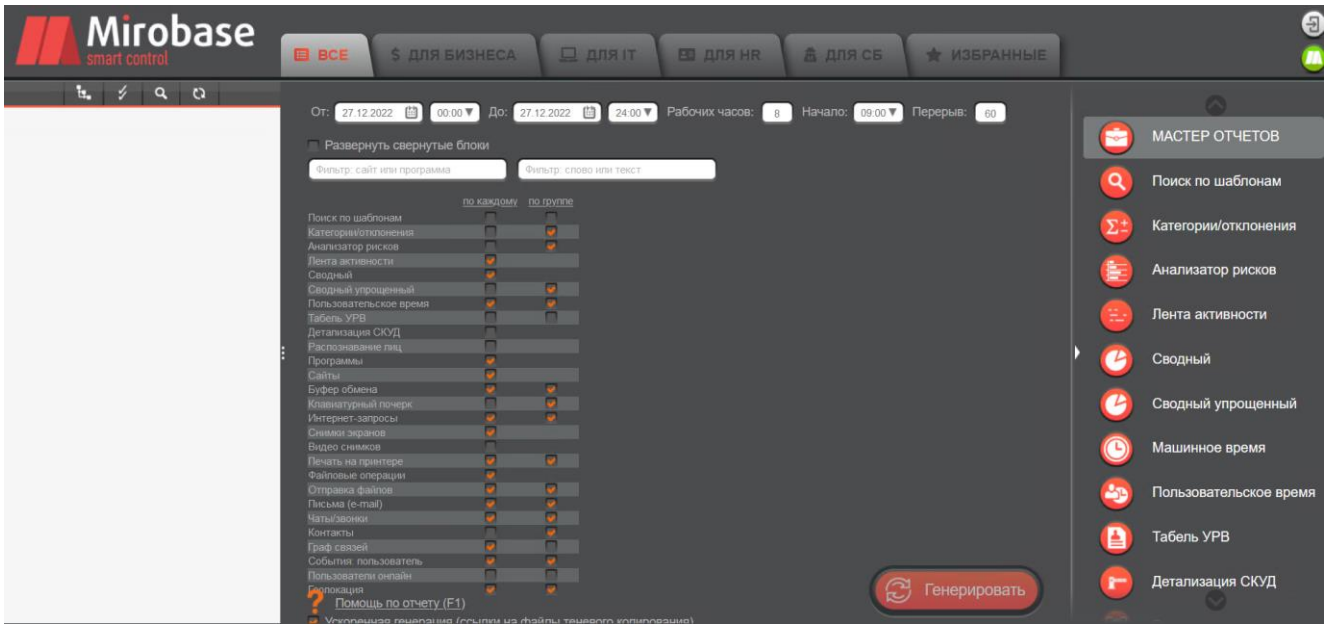


Рис. 2.5.2. Веб-інтерфейс системи Mirobase

2.6 Система моніторингу дій користувачів Teramind UAM

2.6.1 Опис та функціональні можливості Teramind UAM

Компанія Teramind була заснована в 2014 році. Вона є провідним постачальником рішень моніторингу працівників, аналітики поведінки користувачів, виявлення інсайдерських загроз і постачальником програмного забезпечення для запобігання втрати даних.

Велика кількість компаній по всьому світу працюють з Teramind. Це компанії з галузі фінансів, юридичної, роздрібної торгівлі, виробництва, енергетики, охорони здоров'я і навіть урядові організації. Штаб-квартира Teramind знаходиться в Маямі, штат Флорида, з відділами з продажу та підтримки по всьому світу.

Teramind UAM – це система моніторингу дій користувачів, яка надає

підприємствам при її використанні наступні можливості:

- можливість відслідковування будь-яких дій працівників на персональному комп’ютері як в режимі реального часу (в live), так і по історії;
- відеозапис всього, що відбувається на екрані працівника;
- моніторинг пошти;
- моніторинг месенджерів;
- моніторинг соціальних мереж;
- моніторинг додатків, які використовують працівники під час роботи на ПК;
- моніторинг команд, які використовують працівники в терміналах cmd та PowerShell;
- моніторинг URL-посилань, які використовують працівники під час роботи на ПК;
- налаштування правил поведінки працівників та автоматичне застосування відповідних дій при порушенні цих правил;
- моніторинг продуктивності працівників;
- використання вбудованої системи захисту від витоку конфіденційних даних (Data Loss Prevention, DLP);
- надання доказової бази при розслідуванні інцидентів інформаційної безпеки.

2.6.2 Компоненти та архітектура системи Teramind UAM

Архітектурно рішення Teramind UAM складається з декількох компонентів як показано на рисунку 2.6.1 [22]:

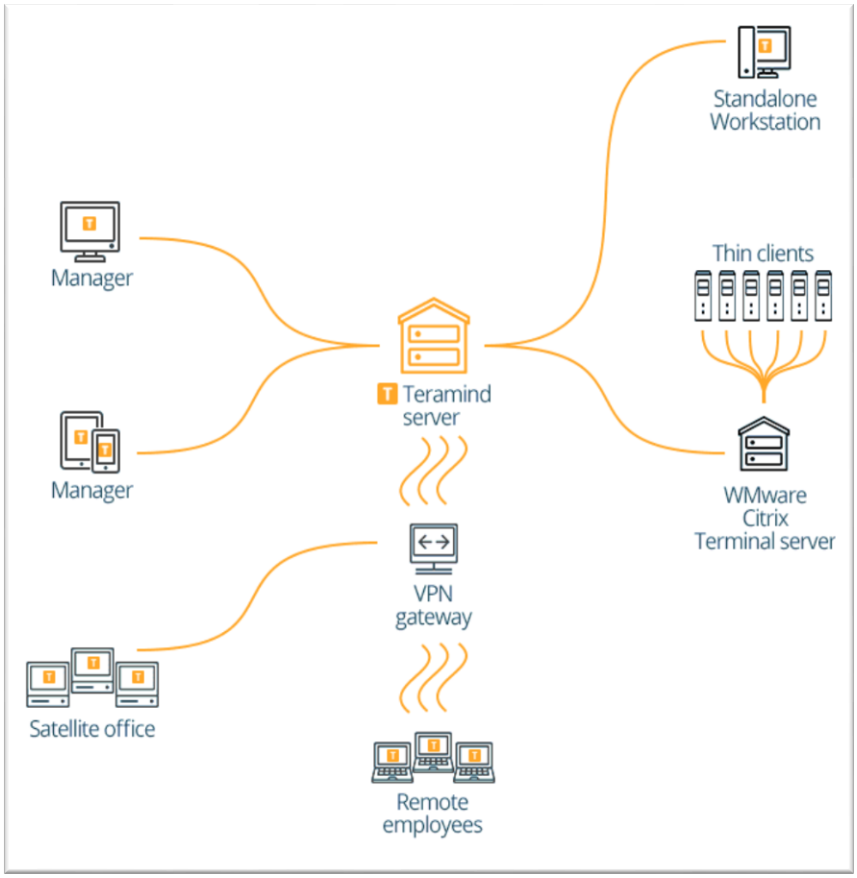


Рис. 2.6.1. Архітектура системи Teramind UAM

1) Агенти (Agents) – це програмні засоби, які встановлюються на персональних комп’ютерах працівників, і призначені для запису будь-яких дій працівників на ПК. Після запису такої інформації, агенти передають її на сервер Teramind. Агенти потребують невелику кількість ресурсів (30-50 МБ оперативної пам’яті (RAM) та 1-3% CPU) та для проведення моніторингу можуть бути встановлені на такі типи систем:

- Windows 7, 8, 10 (32&64 bit);
- Windows Server 2008, 2012, 2016, 2019 (32&64 bit);
- MacOS 10.15 (Catalina), MacOS 10.4 (Mojave);
- Citrix;
- VMware Horizon.

2) Teramind Server – це серверний компонент системи, який приймає зібрану інформацію моніторингу з агентів та проводить її аналіз, обробку, зберігання і видачу адміністраторам безпеки за допомогою веб-інтерфейсу. Веб-інтерфейс системи Teramind UAM зображено на рисунку 2.6.2:

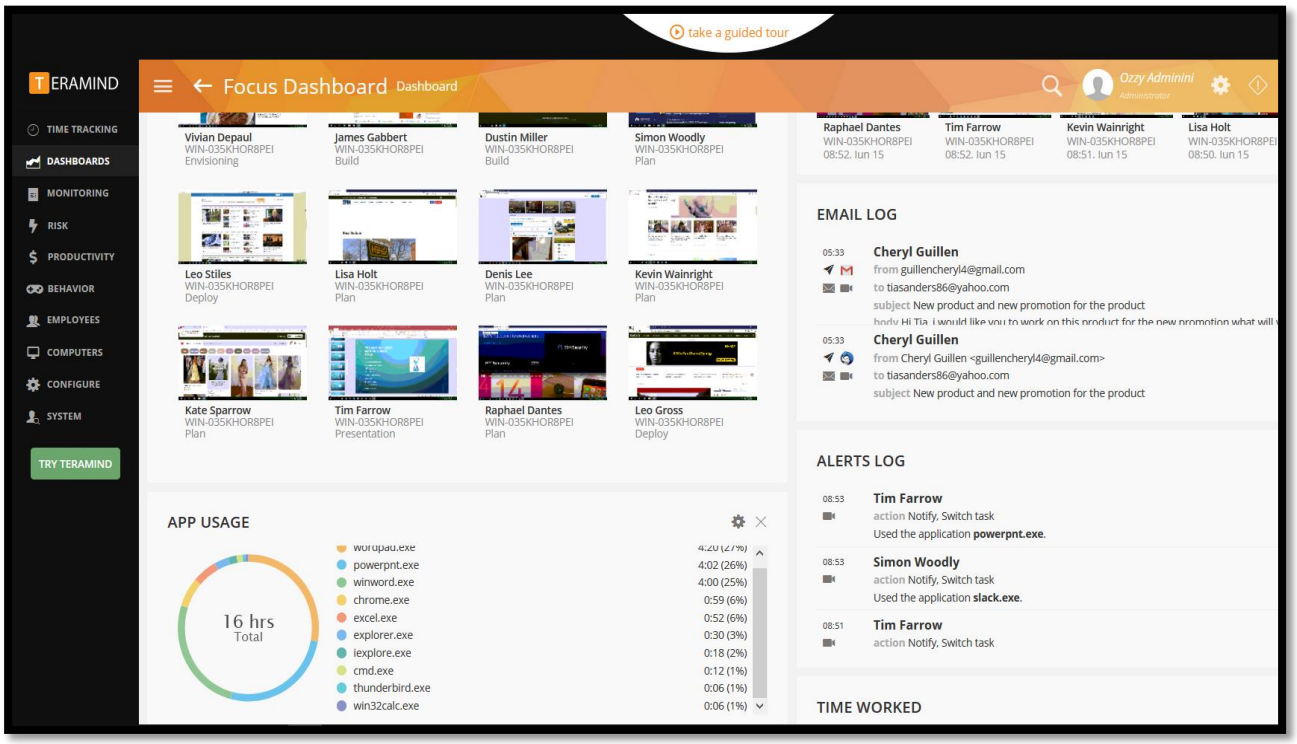


Рис. 2.6.2. Веб-інтерфейс системи Teramind UAM

Є три основні способи розгортання сервера Teramind:

1) Установка власного серверу Teramind (On-premise Deployment). У такому випадку підприємство матиме повний контроль над усією системою, як над агентською частиною, так і над серверною, але для установки серверу потрібно буде виділити необхідні ресурси в залежності від кількості робочих станцій працівників, на які планується встановити агент [22]:

- До 100 агентів – CPU: 4 ядра, RAM: 6 ГБ;
- До 500 агентів – CPU: 8 ядер, RAM: 16 ГБ;
- До 1000 агентів – CPU: 16 ядер, RAM: 24 ГБ

2) Використання хмарного середовища розробника системи (Cloud Deployment). У такому випадку серверна частина системи Teramind UAM буде підтримуватись розробником. Це рішення найкраще підходить для малого бізнесу, коли у складі компанії немає повноцінної IT-команди.

3) Використання приватного хмарного середовища (Private Cloud). У даному випадку серверна частина система буде підтримуватись приватною хмарою (наприклад, Amazon AWS, Microsoft Azure).

2.6.3 Модулі моніторингу системи Teramind UAM

Система Teramind UAM має декілька модулів, які можна використовувати як механізми моніторингу внутрішніх та зовнішніх процесів підприємства [22]:

1) Модуль моніторингу пошти. Надає можливість адміністраторам безпеки переглядати в режимі реального часу або по історії будь-які листи, які приходять працівникам підприємства як показано на рисунку 2.6.3:

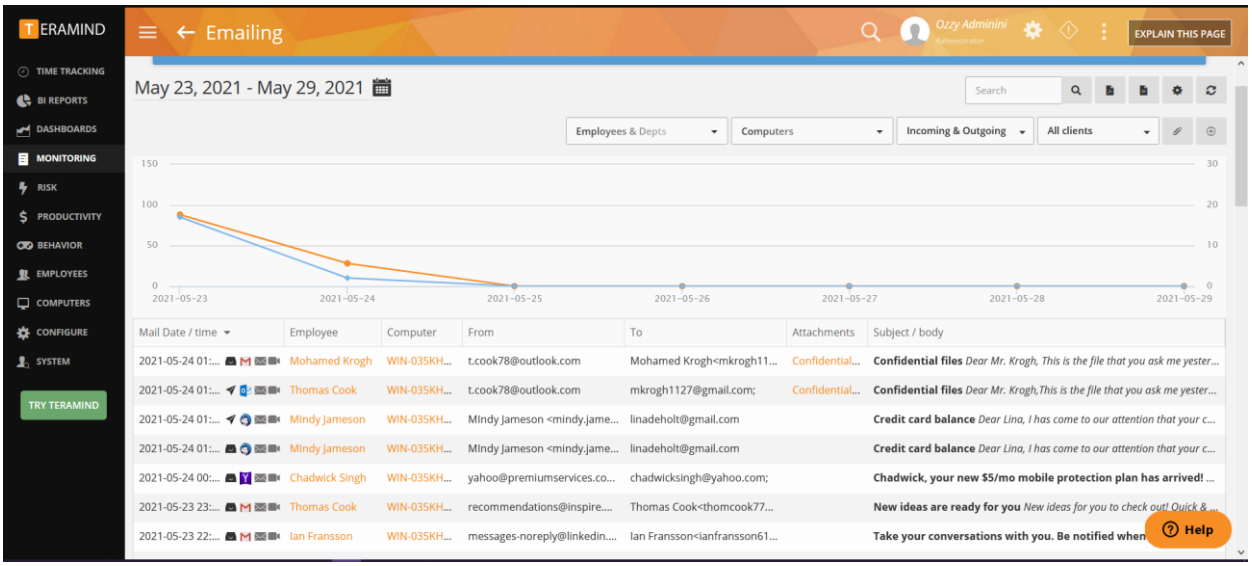
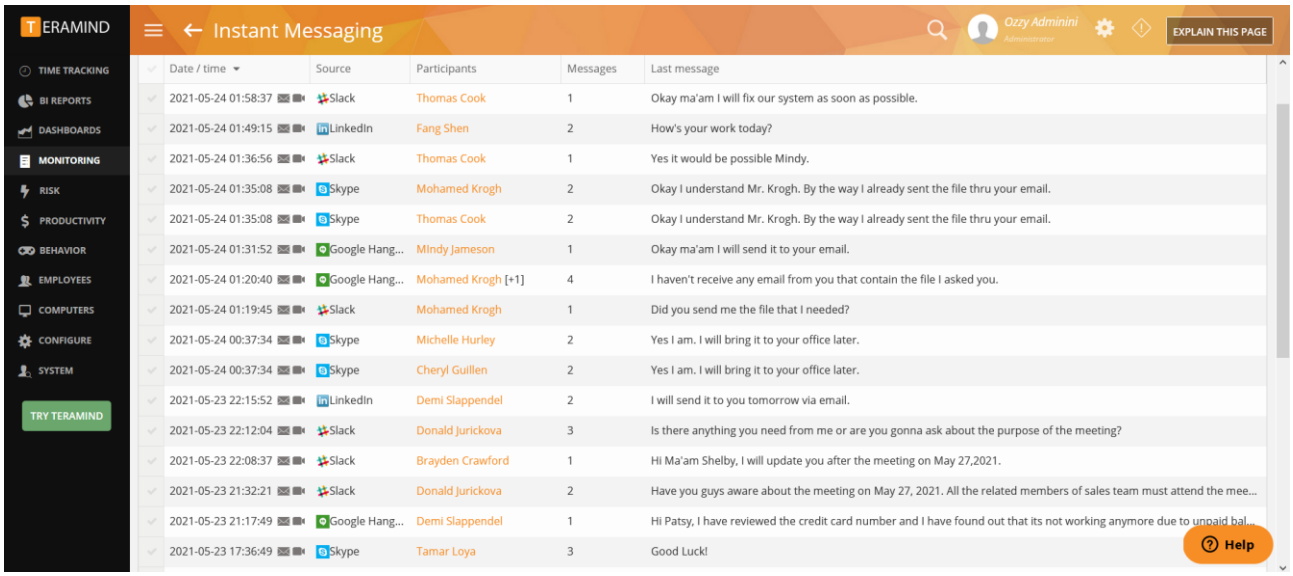


Рис. 2.6.3. Модуль моніторингу пошти

Адміністратор може переглядати вміст електронного листа, від кого та кому даний лист було відправлено, а також, прикріплені файли. Крім цього, є можливість автоматично повідомляти адміністратора про надходження

підозрілих листів но основі попередньо налаштованих правил безпеки. Підтримується велика кількість поштових клієнтів. Серед основних можна виділити наступні: Mozilla Thunderbird, Yandex Mail, Desktop Outlook, Gmail, Web Outlook та інші.

2) Модуль моніторингу месенджерів. Надає можливість адміністраторам безпеки переглядати в режимі реального часу або по історії будь-які повідомлення в месенджерах, які приходять працівникам підприємства як показано на рисунку 2.6.4:



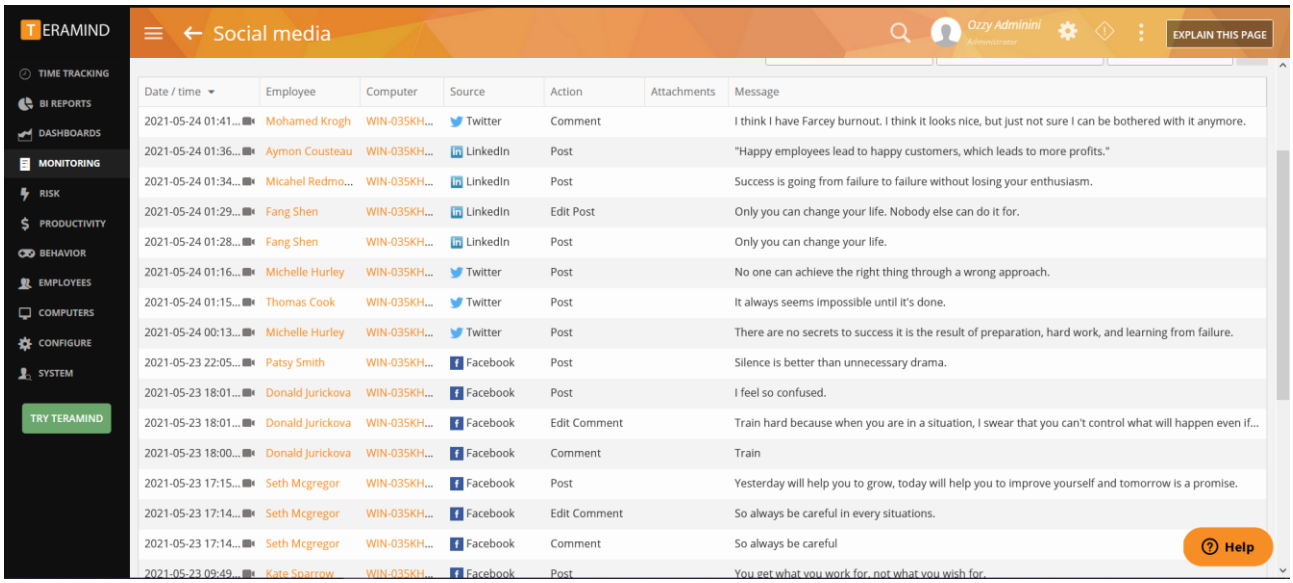
Date / time	Source	Participants	Messages	Last message
2021-05-24 01:58:37	Slack	Thomas Cook	1	Okay ma'am I will fix our system as soon as possible.
2021-05-24 01:49:15	LinkedIn	Fang Shen	2	How's your work today?
2021-05-24 01:36:56	Slack	Thomas Cook	1	Yes it would be possible Mindy.
2021-05-24 01:35:08	Skype	Mohamed Krogh	2	Okay I understand Mr. Krogh. By the way I already sent the file thru your email.
2021-05-24 01:35:08	Skype	Thomas Cook	2	Okay I understand Mr. Krogh. By the way I already sent the file thru your email.
2021-05-24 01:31:52	Google Hang...	MIndy Jameson	1	Okay ma'am I will send it to your email.
2021-05-24 01:20:40	Google Hang...	Mohamed Krogh [+1]	4	I haven't receive any email from you that contain the file I asked you.
2021-05-24 01:19:45	Slack	Mohamed Krogh	1	Did you send me the file that I needed?
2021-05-24 00:37:34	Skype	Michelle Hurley	2	Yes I am. I will bring it to your office later.
2021-05-24 00:37:34	Skype	Cheryl Guillen	2	Yes I am. I will bring it to your office later.
2021-05-23 22:15:52	LinkedIn	Demi Slappendel	2	I will send it to you tomorrow via email.
2021-05-23 22:12:04	Slack	Donald Jurickova	3	Is there anything you need from me or are you gonna ask about the purpose of the meeting?
2021-05-23 22:08:37	Slack	Brayden Crawford	1	Hi Ma'am Shelby, I will update you after the meeting on May 27,2021.
2021-05-23 21:32:21	Slack	Donald Jurickova	2	Have you guys aware about the meeting on May 27, 2021. All the related members of sales team must attend the mee...
2021-05-23 21:17:49	Google Hang...	Demi Slappendel	1	Hi Patsy, I have reviewed the credit card number and I have found out that its not working anymore due to unpaid bal...
2021-05-23 17:36:49	Skype	Tamar Loya	3	Good Luck!

Рис. 2.6.4. Модуль моніторингу месенджерів

Адміністратор може переглядати вміст повідомлення, від кого та кому його було відправлено. Крім цього, є можливість автоматично повідомляти адміністратора про надходження в месенджерах підозрілих повідомлень на основі попередньо налаштованих правил безпеки. Підтримуються наступні месенджери: Facebook, Skype, Skype Web, Skype for Business, Google Hangouts, WhatsApp, Slack, Slack Web, LinkedIn, Microsoft Teams, Microsoft Teams Web.

Окрім цього адміністратор може виявити витік конфіденційних даних або іншу небажану активність працівників.

3) Модуль моніторингу соціальних мереж. Надає можливість адміністраторам безпеки переглядати в режимі реального часу активність працівників в соціальних мережах, як показано на рисунку 2.6.5:



Date / time	Employee	Computer	Source	Action	Attachments	Message
2021-05-24 01:41...	Mohamed Krogh	WIN-035KH...	Twitter	Comment		I think I have Farcey burnout. I think it looks nice, but just not sure I can be bothered with it anymore.
2021-05-24 01:36...	Aymon Cousteau	WIN-035KH...	LinkedIn	Post		"Happy employees lead to happy customers, which leads to more profits."
2021-05-24 01:34...	Micahel Redmo...	WIN-035KH...	LinkedIn	Post		Success is going from failure to failure without losing your enthusiasm.
2021-05-24 01:29...	Fang Shen	WIN-035KH...	LinkedIn	Edit Post		Only you can change your life. Nobody else can do it for.
2021-05-24 01:28...	Fang Shen	WIN-035KH...	LinkedIn	Post		Only you can change your life.
2021-05-24 01:16...	Michelle Hurley	WIN-035KH...	Twitter	Post		No one can achieve the right thing through a wrong approach.
2021-05-24 01:15...	Thomas Cook	WIN-035KH...	Twitter	Post		It always seems impossible until it's done.
2021-05-24 00:13...	Michelle Hurley	WIN-035KH...	Twitter	Post		There are no secrets to success it is the result of preparation, hard work, and learning from failure.
2021-05-23 22:05...	Patsy Smith	WIN-035KH...	Facebook	Post		Silence is better than unnecessary drama.
2021-05-23 18:01...	Donald Jurickova	WIN-035KH...	Facebook	Post		I feel so confused.
2021-05-23 18:01...	Donald Jurickova	WIN-035KH...	Facebook	Edit Comment		Train hard because when you are in a situation, I swear that you can't control what will happen even if...
2021-05-23 18:00...	Donald Jurickova	WIN-035KH...	Facebook	Comment		Train
2021-05-23 17:15...	Seth Mcgregor	WIN-035KH...	Facebook	Post		Yesterday will help you to grow, today will help you to improve yourself and tomorrow is a promise.
2021-05-23 17:14...	Seth Mcgregor	WIN-035KH...	Facebook	Edit Comment		So always be careful in every situations.
2021-05-23 17:14...	Seth Mcgregor	WIN-035KH...	Facebook	Comment		So always be careful
2021-05-23 09:49...	Kate Sparrow	WIN-035KH...	Facebook	Post		You get what you work for, not what you wish for.

Рис. 2.6.5. Модуль моніторингу соціальних мереж

Адміністратор може переглядати вміст постів та коментарів в соціальних мережах. Крім цього, є можливість автоматично повідомляти адміністратора про виявлення підозрілих постів чи коментарів но основі попередньо налаштованих правил безпеки.

Система підтримує наступні соціальні мережі: Facebook, Twitter, LinkedIn.

4) Модуль захисту від витоку конфіденційних даних (Data Loss Prevention, DLP). Навіть якщо соціальному інженеру вдасться обманути працівника та змусити передати чутливі дані, модуль DLP системи Teramind може допомогти адміністраторам безпеки виявити таку передачу даних та не дати їй відбутися. Для цього адміністратори повинні визначити, які дані вважаються чутливими та розробити на їх основі правила контенту.

Правила налаштовуються на блокування та оповіщення адміністратора безпеки у тому разі, якщо системою буде виявлено факт передачі працівником

номерів банківських карток в електронному листі або повідомленні месенджера. Подібні правила можна налаштувати і на інші типи даних.

Висновки до розділу 2

Отже, в другому розділі було досліджено сучасні рішення інформаційної безпеки для визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства, установи чи організації.

Досліджено основні сучасні рішення SIEM, як основний метод моніторингу процесів та управління безпекою інформаційних ресурсів на підприємстві та досвід їх використання, та UAM як основне рішення для моніторингу зовнішніх процесів, активності користувачів, пошти, месенджерів та соціальних мереж. Проаналізовано функціональні можливості та переваги таких сучасних SIEM систем, як IBM QRadar, Splunk, ArcSight та систем моніторингу дій користувачів Ekran System, Mirobase та Teramind UAM.

Дослідження показало, що описані вище рішення SIEM та UAM є практично рівними по функціоналу, можливостям та ефективності роботи, хоч вони є і передовими на ринку. На перший погляд дуже важко оцінити, яке з рішень є лідером серед інших в своєму класі. Тому доцільно провести визначення кращих з них методом експертних оцінок.

Розділ 3 ВИЗНАЧЕННЯ ДОЦІЛЬНОГО СПОСОБУ МОНІТОРИНГУ ЗОВНІШНІХ І ВНУТРІШНІХ ПРОЦЕСІВ В ІНТЕРЕСАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА МЕТОДОМ ЕКСПЕРТНИХ ОЦІНОК

В результаті проведеного дослідження систем інформаційної безпеки в розділі 2 доцільно провести визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства методом експертних оцінок. Далі проводиться визначення необхідних рішень SIEM (Security Information and Event Management) та UAM (User Activity Monitoring).

3.1 Визначення системи SIEM методом експертних оцінок

Незважаючи на свою відносну зрілість, ринок SIEM все ще зростає двозначними темпами. Основною тенденцією є все більш широке використання поведінкової аналітики та автоматизації для фільтрації менш нагальних попереджень, щоб групи безпеки могли зосередитись на найбільших загрозах та подіях.

Програмне забезпечення Security Information and Event Management (SIEM) надає спеціалістам інформаційної безпеки підприємства можливість відстежувати події, які відбуваються в їхньому IT-середовищі.

Технологія існує вже більше десяти років. Вона поєднує в собі управління подіями безпеки (SEM) – аналіз даних журналу та подій у режимі реального часу, щоб забезпечити моніторинг загроз, кореляцію подій, реагування на інциденти, та управлінням інформаційною безпекою (SIM), яка збирає, аналізує та звітує про дані журналу.

SIEM збирає та агрегує дані журналу, згенеровані на всій технологічній інфраструктурі організації, від хостових систем і додатків до мережевих та захисних пристроїв, таких як брандмауери та антивірусні фільтри.

Після цього програмне забезпечення визначає та класифікує інциденти та події, а також аналізує їх. SIEM забезпечує дві основні цілі, які мають бути досягнуті:

1) надавати звіти про інциденти та події, пов'язані з безпекою, такі як успішні та невдалі входи в систему, активність зловмисного програмного забезпечення та інші можливі зловмисні дії; та

2) надсилати сповіщення, якщо аналіз показує, що будь-яка діяльність виконується проти заздалегідь визначених наборів правил і, таким чином, вказує на потенційну проблему безпеки.

SIEM в основному використовується великими організаціями та державними компаніями, де дотримання правил залишається найважливішим фактором використання цієї технології.

На ринку SIEM є декілька домінуючих постачальників на основі продажів у всьому світі, зокрема IBM, Splunk та HPE. Є щонайменше ще кілька основних гравців, а саме: Alert Logic, Intel, LogRhythm, ManageEngine, Micro Focus, Solar Winds і Trustwave.

Аналіз тенденцій розвитку сучасних SIEM систем дозволяють визначити, що головними потребами з боку споживачів є забезпечення повної видимості подій безпеки, кількість інтеграцій, надійність, доступність (ціна) та простота у використанні.

При здійсненні як вибору методу експертних оцінок, так і показників, за яким він виконувався, не будемо робити розподіл на постачальник – споживач. Тому сам метод вважається уніфікованим, але увагу звернено на стратегію і доступність для недостатньо підготованих учасників ринку кібербезпеки. Крім того, застосовуючи принцип зваженості, кожен з користувачів цього методу може адаптувати його з урахуванням власних можливостей та потреб.

Головним при оцінці ефективності є той факт, що показники теж можуть змінювати свій стан, тобто підлаштовуватись під застосований математичний апарат методом інверсії. Наприклад, зміна станів мобільність – стаціонарність, безпека – доступність, складність – простота і т.д. для спрощення об’єктивного визначення переваг та недоліків кожної з SIEM систем. Як приклад пропонується порівняльна таблиця 3.1.1 для кількох найпопулярніших SIEM. Для покращення ефективності оцінки передбачена можливість розподілу показників за групами, що складають індивідуальну пріоритетність за потребами. Таким чином в таблиці 3.1.1 наведено базові показники, за якими достатньо проводити оцінку. Але при необхідності кожну з груп можна поширити чи зменшити за бажанням, порівняно з базовою.

Базове порівняння проводилося за наступними основними показниками (чинниками):

- Архітектура (On-premise, Cloud, SaaS)
- Складність впровадження
- Зручність функціоналу розслідування інцидентів
- Деталізація відображення даних
- Автоматичне виявлення джерел подій
- Оповіщення про інциденти
- Можливість задання або імпорту інформації про активи
- Кількість підтримуваних джерел подій
- Можливість підключення нестандартних джерел подій
- Наявність готових правил кореляції
- Наявність готових графічних панелей (Dashboards)
- Наявність готових звітів
- Наявність панелей візуалізації та звітів щодо відповідності стандартам (Compliance)
- Можливість пошуку по «сирим» подіям
- Робота з фільтрами

- Можливість побудови графів мережевої взаємодії
- Можливість формування звітів у вигляді документів (формати експорту)
- Інтерактивна робота з графічними панелями
- Наявність HA (High Availability) та DR (Disaster Recovery)
- Можливість відновлення БД після збоїв
- Агрегація подій за типом
- Нормалізація подій
- Методи збору подій з джерел
- Підтримувані формати збору подій
- Можливість збору даних про мережевий трафік
- Поведінкова аналітика (UBA)
- Інтеграція з ITSM/CMDB
- Підключення репутаційних баз
- Наявність API
- Інтеграція зі сканерами уразливостей

Наведені в таблиці значення параметрів SIEM не дозволяє однозначно прорахувати ефективність та зробити вибір, що повинен задовольнити конкретного споживача. Для більш обґрунтованого визначення доцільно використати один з методів експертних оцінок. Сутність методу полягає в порівнянні об’єктів за прорахованими оцінками.

Таблиця 3.1.1

Порівняння сучасних SIEM систем

№	Параметр	IBM QRadar	Splunk	HPE ArcSight
1.	Архітектура (On-premise, Cloud, SaaS)	On-prem Cloud SaaS	On-prem SaaS	On-prem Cloud
2.	Складність впровадження	Складно	Складно	Дуже складно

3.	Зручність функціоналу розслідування інцидентів	++	+	+
4.	Деталізація відображення даних	+	+	+
5.	Автоматичне виявлення джерел подій	+	+	+
6.	Оповіщення про інциденти	SMTP	SMTP Месенджер	SMTP SMS
7.	Можливість задання або імпорту інформації про активи	Сканери безпеки CSV-файл API	-	ArcSight Asset Import Connector
8.	Кількість підтримуваних джерел подій	300+	2000+	300+
9.	Можливість підключення нестандартних джерел подій	Розробка парсера	Розробка парсера	ArcSight Flex Connector
10.	Наявність готових правил кореляції	+	+	+
11.	Наявність готових графічних панелей (Dashboards)	+ QRadar Pulse	+	+
12.	Наявність готових звітів	110+ Content Extension Pack	500+	80+
13.	Наявність панелей візуалізації та звітів щодо відповідності стандартам (Compliance)	PCI DSS COBIT FISMA GLBA HIPAA NERC SOX	GDRP HIPAA FISMA PCI DSS	PCI DSS HIPAA SOX NERC FISMA
14.	Можливість пошуку по «сирим» подіям	+	+	+
15.	Робота з фільтрами	Фільтри по полям Regex AQL	Фільтри по полям SPL	Фільтри по полям Повнотекстовий пошук
16.	Можливість побудови графів мережевої взаємодії	+	+	Між 3 хостами
17.	Можливість формування звітів у вигляді документів (формати експорту)	PDF HTML RTF XML XLS	Raw PDF CSV XML JSON	PDF HTML XLS RTF CSV
18.	Інтерактивна робота з	+	+	+

	графічними панелями			
19.	Наявність HA (High Availability) та DR (Disaster Recovery)	HA DR	HA DR	HA
20.	Можливість відновлення БД після збоїв	+	+	+
21.	Агрегація подій за типом	++	+	+
22.	Нормалізація подій	+	+	+
23.	Методи збору подій з джерел	Агентний Безагентний	Агентний Безагентний	Агентний Безагентний
24.	Підтримувані формати збору подій	Syslog TLS Syslog Log File SNMP JDBC WinRPC OPSEC HTTP FTP SCP	Syslog Wineventlog Perfmon WMI OPSEC SNMP JDBC SDEE SQL	Syslog TLS Syslog Log File SNMP JDBC WinRPC OPSEC HTTP SCP
25.	Можливість збору даних про мережевий трафік	SPAN Netflow J-flow sFlow	Netflow J-flow sFlow IPFIX HTTP XMPP	Netflow J-flow IPFIX
26.	Поведінкова аналітика (UBA)	+	+	+
27.	Інтеграція з ITSM/CMDB	+	+	+
28.	Підключення репутаційних баз	+	IBM X-force	ArcSight RepSM
29.	Наявність API	REST API	REST API	WebAPI
30.	Інтеграція зі сканерами уразливостей	+	+	+

Для більш обґрунтованого визначення, по перше, доцільності використання будь-якої з обраних для аналізу SIEM систем, а по друге отримання кількісної характеристики ефективності, використаємо метод експертних оцінок. Сутність методу полягає в порівнянні об’єктів за прорахованими оцінками.

Спочатку необхідно визначити ваговий коефіцієнт кожного з показників. Якщо застосовувати прямі та інверсні показники, то значення коефіцієнту

розташовано в межах від 0 до 1. Але при такому підході доцільно використовувати дрібний комплексний показник ефективності, де прямі показники розташовані у чисельнику, а інверсні в знаменнику. Це, по-перше, ускладнює розрахунки, а по-друге, зменшує рівень розрізненості технологій, тобто нівелює межу прийняття рішення. Для спрощеної оцінки при використанні тільки прямих показників та заміні на інверсні, може застосовуватись комплексний показник на основі суми окремих показників, що помножені на коефіцієнти, які мають межу від 1 до 10 або до 100 за бажанням споживача та його здатності визначити пріоритетні властивості показників.

Після цього йде визначення ступеню важливості параметра для побудови системи моніторингу з використанням SIEM систем та внесення його до належної групи. Розподіл на групи може бути проведено за належністю до стану: технічні, економічні, ергономічні, фінансові або інші, але для спрощення достатньо обмежитись групами; наприклад, придатності, переваги та оптимальності.

Третій крок – уточнення значення коефіцієнту вагомості, що поєднує перші два кроки. Він також може мати два напрямки:

Перший полягає у виборі меж між групами:

- 0-3 бали – не задовольняє умовам, не найкращий варіант, але належить до групи придатності, хоча і з обмеженнями;
- 4-7 бали – кращий в порівнянні з іншими та на скільки – це ступінь переваги;
- 8-10 бали – найкращий, квазіоптимальний або оптимальний.

Другий базується на спрощенні і визначає фіксовані значення коефіцієнтів. Наприклад:

- 10 – задовольняє умовам та є оптимальним;
- 5 – не найкращий варіант, але підходить для побудови – придатність;
- 1 – не задовольняє умовам.

Крок четвертий – коефіцієнти або оцінка за параметром проставляється для кожної системи окремо. Для наглядності це може бути таблиця порівняння сучасних SIEM систем з урахуванням важливості параметрів – таблиця 3.1.2.

Крок п’ятий – розрахунок суми кількості балів для кожної системи як суми добутків відповідної оцінки параметру на його ваговий коефіцієнт за формулою 3.1.1:

$$S_i = \sum_{i=1}^{n} a_i \cdot M_i \,, \qquad (3.1.1)$$

де

- S_i – сумарна кількість балів для стандарту;
- a_i – i оцінка параметру;
- M_i – ваговий коефіцієнт i параметра системи.

Крок останній – вибір за найбільшим значенням найкращого з розглянутих чи тих, що порівнюються.

Далі зображена таблиця порівняння найпопулярніших SIEM систем з врахуванням важливості параметрів, з максимальним коефіцієнтом важливості 10.

Таблиця 3.1.2

Порівняння SIEM систем з урахуванням важливості параметрів

№	Параметр	IBM QRadar	Splunk	HPE ArcSight	M
1.	Архітектура (On-premise, Cloud, SaaS)	10	7	7	7
2.	Складність впровадження	8	7	5	10
3.	Зручність функціоналу розслідування інцидентів	9	8	8	10
4.	Деталізація відображення даних	10	10	10	9
5.	Автоматичне виявлення джерел подій	10	10	10	7
6.	Оповіщення про інциденти	8	10	10	8
7.	Можливість задання або імпорту інформації про активи	10	0	9	8
8.	Кількість підтримуваних джерел подій	7	10	7	10

9.	Можливість підключення нестандартних джерел подій	8	8	9	8
10.	Наявність готових правил кореляції	10	10	10	10
11.	Наявність готових графічних панелей (Dashboards)	10	9	9	10
12.	Наявність готових звітів	9	10	8	8
13.	Наявність панелей візуалізації та звітів щодо відповідності стандартам (Compliance)	10	7	9	10
14.	Можливість пошуку по «сирим» подіям	10	10	10	9
15.	Робота з фільтрами	10	7	5	10
16.	Можливість побудови графів мережевої взаємодії	10	10	6	10
17.	Можливість формування звітів у вигляді документів (формати експорту)	9	9	9	6
18.	Інтерактивна робота з графічними панелями	10	10	10	9
19.	Наявність HA (High Availability) та DR (Disaster Recovery)	10	10	7	9
20.	Можливість відновлення БД після збоїв	10	10	10	10
21.	Агрегація подій за типом	8	7	7	7
22.	Нормалізація подій	10	10	10	10
23.	Методи збору подій з джерел	10	10	10	7
24.	Підтримувані формати збору подій	10	8	9	10
25.	Можливість збору даних про мережевий трафік	8	10	7	10
26.	Поведінкова аналітика (UBA)	10	10	10	9
27.	Інтеграція з ITSM/CMDB	10	10	10	7
28.	Підключення репутаційних баз	10	7	9	10
29.	Наявність API	9	9	8	8
30.	Інтеграція зі сканерами уразливостей	10	10	10	10
Максимальна кількість балів з урахуванням коефіцієнтів важливості				2660	
Сумарна кількість балів для систем		2512	2338	2277	

Розрахунок максимальної кількості балів з урахуванням коефіцієнтів важливості за формулою 3.1.1:

$$A = \sum_{i=1}^{n} a_i \cdot M_i$$

$$= 10 * 7 + 10 * 10 + 10 * 10 + 10 * 9 + 10 * 7 + 10 * 8 + 10 * 8 + 10 * 10 + 10 * 8 + 10 * 10 + 10 * 10 + 10 * 8 + 10 * 10 + 10 * 9 + 10 * 10 + 10 * 10 + 10 * 6 + 10 * 9 + 10 * 9 + 10 * 10 + 10 * 7 + 10 * 10 + 10 * 7 + 10 * 10 + 10 * 10 + 10 * 9 + 10 * 7 + 10 * 10 + 10 * 8 + 10 * 10 = 2660$$

Розрахунок суми кількості балів для IBM QRadar за формулою 3.1.1:

$$S_i = \sum_{i=1}^{n} a_i \cdot M_i$$

$$= 10 * 7 + 8 * 10 + 9 * 10 + 10 * 9 + 10 * 7 + 8 * 8 + 10 * 8 + 7 * 10 + 8 * 8 + 10 * 10 + 10 * 10 + 9 * 8 + 10 * 10 + 10 * 9 + 10 * 10 + 10 * 10 + 9 * 6 + 10 * 9 + 10 * 9 + 10 * 10 + 8 * 7 + 10 * 10 + 10 * 7 + 10 * 10 + 8 * 10 + 10 * 9 + 10 * 7 + 10 * 10 + 9 * 8 + 10 * 10 = 2512$$

Розрахунок суми кількості балів для Splunk за формулою 3.1.1:

$$S_i = \sum_{i=1}^{n} a_i \cdot M_i = 7 * 7 + 7 * 10 + 8 * 10 + 10 * 9 + 10 * 7 + 10 * 8 + 0 * 8 + 10 * 10 + 8 * 8 + 10 * 10 + 9 * 10 + 10 * 8 + 7 * 10 + 10 * 9 + 7 * 10 + 10 * 10 + 9 * 6 + 10 * 9 + 10 * 9 + 10 * 10 + 7 * 7 + 10 * 10 + 10 * 7 + 8 * 10 + 10 * 10 + 10 * 9 + 10 * 7 + 7 * 10 + 9 * 8 + 10 * 10 = 2338$$

Розрахунок суми кількості балів для HPE ArcSight за формулою 3.1.1:

$$S_i = \sum_{i=1}^{n} a_i \cdot M_i$$

$$= 7 * 7 + 5 * 10 + 8 * 10 + 10 * 9 + 10 * 7 + 10 * 8 + 9 * 8 + 7 * 10 + 9 * 8 + 10 * 10 + 9 * 10 + 8 * 8 + 9 * 10 + 10 * 9 + 5 * 10 + 6 * 10 + 9 * 6 + 10 * 9 + 7 * 9 + 10 * 10 + 7 * 7 + 10 * 10 + 10 * 7 + 9 * 10 + 7 * 10 + 10 * 9 + 10 * 7 + 9 * 10 + 8 * 8 + 10 * 10$$

$$= 2277$$

Враховуючи, що виконання останнього кроку потребує чисельної аргументації, визначаємо середню оцінку кожної SIEM за формулою 3.1.2:

$$S = 10 \cdot \frac{S_i}{A} \quad , \qquad (3.1.2)$$

де

- S_i – сумарна кількість балів для SIEM системи;
- A – максимальна кількість балів.

Розрахунок середньої оцінки для IBM QRadar за формулою 3.1.2:

$$S_{IBM\ QRadar} = 10 \cdot \frac{S_i}{A} = 10 * \frac{2512}{2660} = 9{,}44$$

Розрахунок середньої оцінки для Splunk за формулою 3.1.2:

$$S_{Splunk} = 10 \cdot \frac{S_i}{A} = 10 * \frac{2338}{2660} = 8{,}79$$

Розрахунок середньої оцінки для HPE ArcSight за формулою 3.1.2:

$$S_{HPE\ ArcSight} = 10 \cdot \frac{S_i}{A} = 10 * \frac{2277}{2660} = 8{,}56$$

Таким чином, висновком по аналізу вибору технології SIEM слід вважати порівняння результатів, що зведені в таблицю 3.1.3.

Згідно розглянутого прикладу, що не претендує на загальну оцінку в цілому, а базується на введених обмеженнях і є більш абстрактним, як наслідок використання спрощеної методики є висновок. Серед сучасних SIEM систем перевагу по обраних параметрах має система IBM QRadar. По головним

показникам та за загальною оцінкою до неї наближається система Splunk (Рис. 3.1.1).

Таблиця 3.1.3

Загальна оцінка SIEM систем

SIEM система	Загальна оцінка SIEM систем (S)
IBM QRadar	9,44
Splunk	8,79
HPE ArcSight	8,56

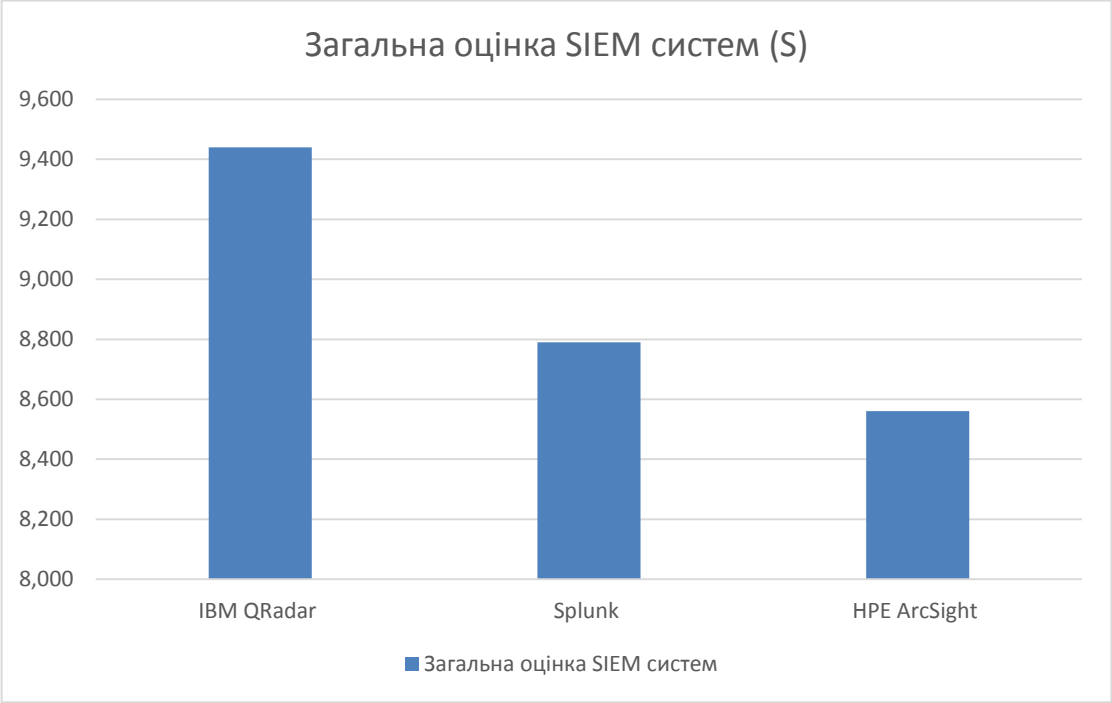


Рис. 3.1.1. Результат оцінки сучасних SIEM систем

3.2 Визначення системи моніторингу дій користувачів UAM методом експертних оцінок

Проаналізувавши сучасні методи зловмисників можна виділити декілька основних шляхів, які використовуються для реалізації кібератак з застосуванням методів соціальної інженерії:

1) Електронна пошта;

2) Соціальні мережі;

3) Месенджери.

Дані шляхи підлягають більш ретельному моніторингу, так як вони можуть в додачу бути використані інсайдерами для викрадення конфіденційних даних. Для реалізації вищевказаних задач доцільно використовувати системи моніторингу дій користувачів (User Activity Monitoring, UAM). В українських підприємствах такі системи застосовуються достатньо часто. До систем моніторингу дій користувачів можна віднести наступні (найбільш поширені):

1) Teramind User Activity Monitoring (UAM);

2) Ekran System Enterprise Edition;

3) Proofpoint ObserveIT (зазначимо, що в Україні дана система наразі не є доступною, тому порівнювати її з іншими системами даного класу рішень недоцільно);

4) Mirobase.

За версією відомого сайту business.com, Teramind User Activity Monitoring вважається передовим рішенням моніторингу користувачів в 2021 році, але це джерело не враховує таких представників як Ekran System та Mirobase.

В результаці цього маємо необхідність проведення обґрунтованого вибору технології моніторингу дій працівників, електронної пошти пошти та месенджерів. Аналіз тенденцій розвитку сучасних систем моніторингу дій користувачів дозволяє визначити, що головними потребами з боку споживачів є забезпечення запису робочої сесії у відео форматі, можливість моніторингу

пошти, месенджерів та соціальних мереж, надійність системи, доступність, простота у використанні, можливість генерації аналітичних звітів та інтеграція з SIEM.

При здійсненні як вибору методу експертних оцінок, так і показників, за яким він виконувався, не будемо робити розподіл на постачальник – споживач. Тому сам метод вважається уніфікованим, але увагу звернено на стратегію і доступність для недостатньо підготованих учасників ринку кібербезпеки. Крім того, застосовуючи принцип зваженості, кожен з користувачів цього методу може адаптувати його з урахуванням власних можливостей та потреб. Головним при оцінці ефективності є той факт, що показники теж можуть змінювати свій стан, тобто підлаштовуватись під застосований математичний апарат методом інверсії. Наприклад, зміна станів мобільність – стаціонарність, безпека – доступність, складність – простота і т.д. Як приклад пропонується порівняльна таблиця 3.2.1 для кількох популярних систем моніторингу дій користувачів. Для покращення ефективності оцінки передбачена можливість розподілу показників за групами, що складають індивідуальну пріоритетність за потребами. Таким чином в таблиці 3.2.1 наведено базові показники, за якими достатньо проводити оцінку. Але при необхідності групу можна поширити чи зменшити за бажанням, порівняно з базовою.

Базове порівняння проводилося за наступними основними показниками (чинниками):

- Повнота підтримки ОС (Windows, Linux, MacOS)
- Архітектура (On-premise, Private Cloud, SaaS)
- Забезпечення запису робочої сесії у відео форматі
- Можливість запису сесій в offline режимі
- Прив’язка логу подій до кожного скріншота
- Перегляд сесій в Live режимі
- Гнучке налаштування параметрів моніторингу для кожної машини
- Моніторинг додатків та веб-сторінок (URL)

- Моніторинг буферу обміну (копіювання/вставка)
- Моніторинг підключень USB-пристроїв
- Моніторинг пошти
- Моніторинг месенджерів
- Моніторинг соціальних мереж
- Моніторинг консольних команд та їх параметрів
- Віддалена установка/видалення/оновлення агентів
- Захист агентів від модифікацій
- Фільтрація моніторингу та пошук ключових слів у сесіях
- Наявність модулю OCR (Optical Character Recognition)
- Надійність системи
- Доступність системи
- Простота у використанні
- Можливість генерації аналітичних звітів
- Інтеграція з SIEM
- Повідомлення адміністратора про порушення поведінкових правил

Наведені значеня параметрів не дозволяють однозначно прорахувати ефективність та зробити вибір рішення UAM, що повинно задовольнити конкретного споживача. Для більш обґрунтованого визначення доцільно використати метод експертних оцінок. Сутність методу полягає в порівнянні об’єктів за прорахованими оцінками.

Таблиця 3.2.1

Порівняння сучасних систем моніторингу дій користувачів UAM

№	Параметр	Ekran System	Mirobase	Teramind
1.	Повнота підтримки ОС (Windows, Linux, MacOS)	Windows Linux MacOS	Windows Linux	Windows MacOS

2.	Архітектура (On-premise, Cloud, SaaS)	On-prem Cloud	On-prem	On-prem Cloud SaaS
3.	Забезпечення запису робочої сесії у відео форматі	+	+	+
4.	Можливість запису сесій в offline режимі	+	-	-
5.	Прив’язка логу подій до кожного скріншота	+	+	+
6.	Перегляд сесій в Live режимі	+	+	+
7.	Гнучке налаштування параметрів моніторингу для кожної машини	++	+	++
8.	Моніторинг додатків та веб-сторінок (URL)	+	+	+
9.	Моніторинг буферу обміну (копіювання/вставка)	+	+	+
10.	Моніторинг підключень USB-пристроїв	+	+	+
11.	Моніторинг пошти	-	+	+
12.	Моніторинг месенджерів	-	+	+
13.	Моніторинг соціальних мереж	-	-	+
14.	Моніторинг консольних команд та їх параметрів	-	-	+
15.	Віддалена установка/видалення/оновлення агентів	+	-	+
16.	Захист агентів від модифікацій	+	-	-
17.	Фільтрація моніторингу та пошук ключових слів у сесіях	++	+	++
18.	Наявність модулю OCR (Optical Character Recognition)	-	-	+
19.	Надійність системи	+	-	+
20.	Доступність системи	$$$	$	$$
21.	Простота у використанні	+	-	++
22.	Можливість генерації аналітичних звітів	+	+	+
23.	Інтеграція з SIEM	+	-	+
24.	Повідомлення адміністратора про порушення поведінкових правил	+	+	++

Для більш обґрунтованого визначення, по перше, доцільності використання будь-якої з обраних для аналізу систем моніторингу дій користувачів, а по друге для отримання кількісної характеристики ефективності, використаємо метод експертних оцінок. Сутність методу полягає в порівнянні об’єктів за прорахованими оцінками.

Першим кроком необхідно визначити ваговий коефіцієнта кожного з показників. Якщо застосовувати прямі та інверсні показники, то значення коефіцієнту розташовано в межах від 0 до 1. Але при такому підході доцільно використовувати дрібний комплексний показник ефективності, де прямі показники розташовані у чисельнику, а інверсні в знаменнику. Це, по-перше, ускладнює розрахунки, а по-друге, зменшує рівень розрізненості технологій, тобто нівелює межу прийняття рішення. Для спрощеної оцінки при використанні тільки прямих показників та заміні на інверсні, може застосовуватись комплексний показник на основі суми окремих показників, що помножені на коефіцієнти, які мають межу від 1 до 10 або до 100 за бажанням споживача та його здатності визначити пріоритетні властивості показників.

Другий крок – визначення ступеню важливості параметра для побудови системи захисту з використанням систем моніторингу дій користувачів та внесення його до належної групи. Розподіл на групи може бути проведено за належністю до стану: технічні, економічні, ергономічні, фінансові або інші, але для спрощення достатньо обмежитись групами; наприклад, придатності, переваги та оптимальності.

Третій крок – уточнення значення коефіцієнту вагомості, що поєднує перші два кроки. Він також може мати два напрямки:

Перший полягає у виборі меж між групами:

- 0-3 бали – не задовольняє умовам, не найкращий варіант, але належить до групи придатності, хоча і з обмеженнями;
- 4-7 бали – кращий в порівнянні з іншими та на скільки – це ступінь переваги;
- 8-10 бали – найкращий, квазіоптимальний або оптимальний.

Другий базується на спрощенні і визначає фіксовані значення коефіцієнтів. Наприклад:

- 10 – задовольняє умовам та є оптимальним;
- 5 – не найкращий варіант, але підходить для побудови – придатність;

- 1 – не задовольняє умовам.

Крок четвертий – коефіцієнти або оцінка за параметром проставляється для кожної системи окремо. Для наглядності це може бути таблиця порівняння сучасних систем моніторингу дій користувачів з урахуванням важливості параметрів – таблиця 3.2.2.

Крок п’ятий – розрахунок суми кількості балів для кожної системи як суми добутків відповідної оцінки параметру на його ваговий коефіцієнт за формулою 3.2.1:

$$S_i = \sum_{i=1}^{n} a_i \cdot M_i \,, \qquad (3.2.1)$$

де

- S_i – сумарна кількість балів для стандарту;
- a_i – i оцінка параметру;
- M_i – ваговий коефіцієнт i параметра системи.

Крок останній – вибір за найбільшим значенням найкращого з розглянутих чи тих, що порівнюються.

Далі зображена таблиця порівняння сучасних систем моніторингу дій користувачів з врахуванням важливості параметрів 3.2.2, з максимальним коефіцієнтом важливості 10.

Таблиця 3.2.2

Порівняння сучасних систем моніторингу дій користувачів з урахуванням важливості параметрів

№	Параметр	Ekran System	Mirobase	Teramind	M
1.	Повнота підтримки ОС (Windows, Linux, MacOS)	10	6	6	10
2.	Архітектура (On-premise, Cloud, SaaS)	7	5	10	8

3.	Забезпечення запису робочої сесії у відео форматі	10	8	10	10
4.	Можливість запису сесій в offline режимі	10	0	0	6
5.	Прив’язка логу подій до кожного скріншота	10	8	10	8
6.	Перегляд сесій в Live режимі	10	10	10	9
7.	Гнучке налаштування параметрів моніторингу для кожної машини	10	6	10	9
8.	Моніторинг додатків та веб-сторінок (URL)	10	10	10	10
9.	Моніторинг буферу обміну (копіювання/вставка)	10	10	10	8
10.	Моніторинг підключень USB-пристроїв	9	8	9	6
11.	Моніторинг пошти	0	8	10	10
12.	Моніторинг месенджерів	0	9	10	10
13.	Моніторинг соціальних мереж	0	0	8	10
14.	Моніторинг консольних команд та їх параметрів	0	0	8	7
15.	Віддалена установка/видалення/оновлення агентів	10	0	8	5
16.	Захист агентів від модифікацій	10	0	0	8
17.	Фільтрація моніторингу та пошук ключових слів у сесіях	10	7	10	9
18.	Наявність модулю OCR (Optical Character Recognition)	0	0	10	7
19.	Надійність системи	8	5	9	10
20.	Доступність системи	6	10	9	10
21.	Простота у використанні	8	6	10	10
22.	Можливість генерації аналітичних звітів	9	7	9	9
23.	Інтеграція з SIEM	10	0	10	10
24.	Повідомлення адміністратора про порушення поведінкових правил	8	7	10	8
Максимальна кількість балів з урахуванням коефіцієнтів важливості				2070	
Сумарна кількість балів для систем		1495	1178	1811	

Розрахунок максимальної кількості балів з урахуванням коефіцієнтів важливості за формулою 3.2.1:

$$A = \sum_{i=1}^{n} a_i \cdot M_i = 10 * 10 + 10 * 8 + 10 * 10 + 10 * 6 + 10 * 8 + 10 * 9 + 10 * 9 + 10 * 10 + 10 * 8 + 10 * 6 + 10 * 10 + 10 * 10 + 10 * 10 + 10 * 7 + 10 * 5 + 10 * 8 + 10 * 9 + 10 * 7 + 10 * 10 + 10 * 10 + 10 * 10 + 10 * 9 + 10 * 10 + 10 * 8 = 2070$$

Розрахунок суми кількості балів для Ekran System за формулою 3.2.1:

$$S_i = \sum_{i=1}^{n} a_i \cdot M_i = 10 * 10 + 7 * 8 + 10 * 10 + 10 * 6 + 10 * 8 + 10 * 9 + 10 * 9 + 10 * 10 + 10 * 8 + 9 * 6 + 0 * 10 + 0 * 10 + 0 * 10 + 0 * 7 + 10 * 5 + 10 * 8 + 10 * 9 + 0 * 7 + 8 * 10 + 6 * 10 + 8 * 10 + 9 * 9 + 10 * 10 + 8 * 8 = 1495$$

Розрахунок суми кількості балів для Mirobase за формулою 3.2.1:

$$S_i = \sum_{i=1}^{n} a_i \cdot M_i = 6 * 10 + 5 * 8 + 8 * 10 + 0 * 6 + 8 * 8 + 10 * 9 + 6 * 9 + 10 * 10 + 10 * 8 + 8 * 6 + 8 * 10 + 9 * 10 + 0 * 10 + 0 * 7 + 0 * 5 + 0 * 8 + 7 * 9 + 0 * 7 + 5 * 10 + 10 * 10 + 6 * 10 + 7 * 9 + 0 * 10 + 7 * 8 = 1178$$

Розрахунок суми кількості балів для Teramind за формулою 3.2.1:

$$S_i = \sum_{i=1}^{n} a_i \cdot M_i = 6 * 10 + 10 * 8 + 10 * 10 + 0 * 6 + 10 * 8 + 10 * 9 + 10 * 9 + 10 * 10 + 10 * 8 + 9 * 6 + 10 * 10 + 10 * 10 + 8 * 10 + 8 * 7 + 8 * 5 + 0 * 8 + 10 * 9 + 10 * 7 + 9 * 10 + 9 * 10 + 10 * 10 + 9 * 9 + 10 * 10 + 10 * 8 = 1811$$

Враховуючи що виконання останнього кроку потребує чисельної аргументації, визначаємо середню оцінку кожної системи моніторингу дій користувачів за формулою 3.2.2:

$$S = 10 \cdot \frac{S_i}{A} \quad , \qquad (3.2.2)$$

де

- S_i – сумарна кількість балів для системи моніторингу;
- A – максимальна кількість балів.

Розрахунок середньої оцінки для Ekran System за формулою 3.2.2:

$$S_{Ekran\ System} = 10 \cdot \frac{S_i}{A} = 10 * \frac{1495}{2070} = 7{,}22$$

Розрахунок середньої оцінки для Mirobase за формулою 3.2.2:

$$S_{Mirobase} = 10 \cdot \frac{S_i}{A} = 10 * \frac{1178}{2070} = 5{,}69$$

Розрахунок середньої оцінки для Teramind за формулою 3.2.2:

$$S_{Teramind} = 10 \cdot \frac{S_i}{A} = 10 * \frac{1811}{2070} = 8{,}75$$

Таким чином, висновком по аналізу вибору системи моніторингу дій користувачів слід вважати порівняння результатів, що зведені в таблицю 3.2.3.

Згідно розглянутого прикладу, що не претендує на загальну оцінку в цілому, а базується на введених обмеженнях і є більш абстрактним, як наслідок використання спрощеної методики є висновок. Серед сучасних систем моніторингу дій користувачів перевагу по обраних параметрах має система Teramind. По головним показникам та за загальною оцінкою до неї наближається система Ekran System (Рис. 3.2.1).

Таблиця 3.2.3

Загальна оцінка систем моніторингу дій користувачів

Система моніторингу дій користувачів (UAM)	**Загальна оцінка систем моніторингу дій користувачів (S)**
Ekran System	7,22
Mirobase	5,69
Teramind	8,75

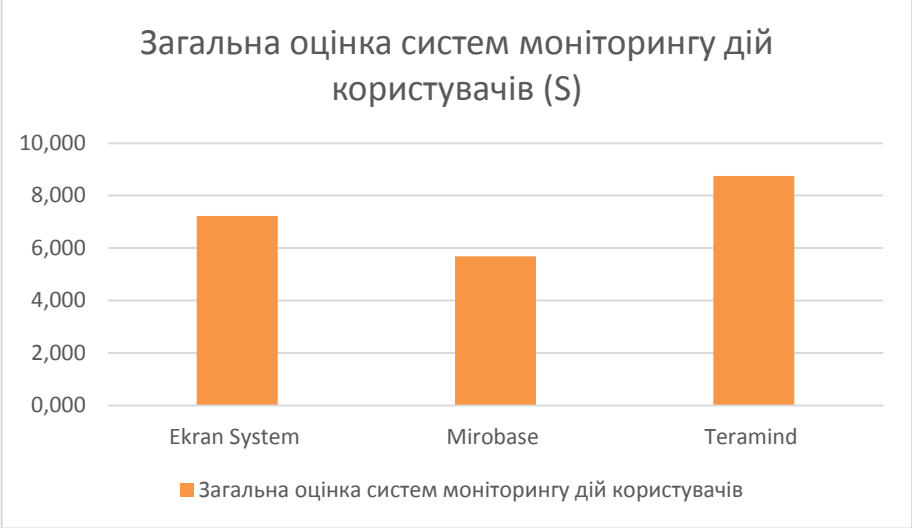


Рис. 3.2.1. Результат оцінки сучасних систем моніторингу дій користувачів

3.3 Загальна схема моніторингу внутрішніх та зовнішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації)

В результаті проведеного дослідження доцільно розробити загальну схему моніторингу внутрішніх та зовнішніх процесів в інтересах інформаційної безпеки підприємства, установи чи організації на основі SIEM IBM QRadar та системи моніторингу дій користувачів Teramind.

На рисунку 3.3.1 наведено загальну схему моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства на основі IBM QRadar та Teramind:

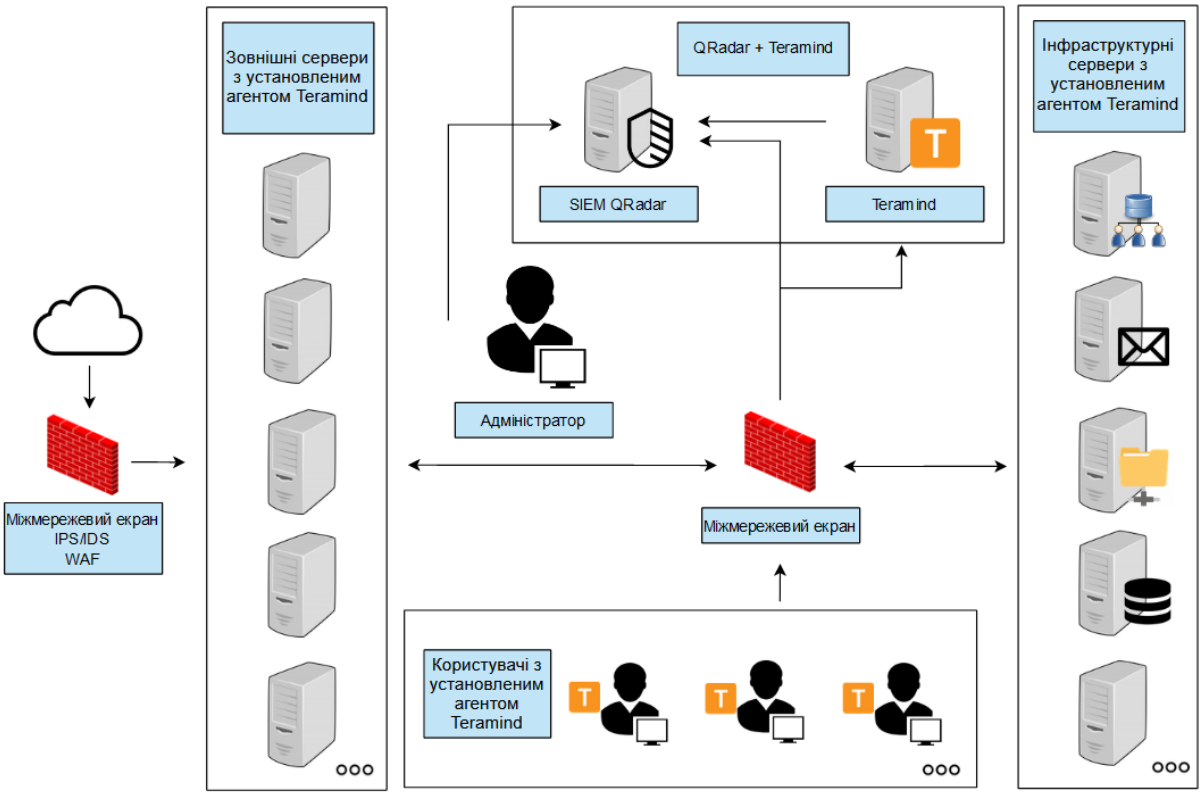


Рис. 3.3.1. Загальна схема моніторингу зовнішніх і внутрішніх процесів підприємства на основі IBM QRadar та Teramind

Висновки до розділу 3

Отже, в третьому розділі дипломної роботи було проведено визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства методом експертних оцінок.

По-перше, отримано оцінку сучасних рішень SIEM на прикладі вибірки з трьох представників, а саме IBM QRadar, Splunk, HPE ArcSight.

В ході реалізації підбору був використаний метод експертних оцінок, завдяки якому було визначено лідера серед трьох, практично рівних по функціоналу, можливостям та ефективності роботи рішень SIEM.

По-друге, отримано оцінку сучасних рішень моніторингу активності користувачів на прикладі вибірки з трьох представників, а саме Ekran System, Mirobase, Teramind. В ході реалізації підбору системи UAM був також

використаний метод експертних оцінок.

Серед сучасних SIEM систем перевагу по обраних параметрах має система IBM QRadar. По головним показникам та за загальною оцінкою до неї наближається система Splunk. Серед сучасних систем моніторингу дій користувачів перевагу по обраних параметрах має система Teramind. По головним показникам та за загальною оцінкою до неї наближається Ekran System.

В результаті отриманих даних щодо визначення систем безпеки було розроблено загальну схему моніторингу внутрішніх та зовнішніх процесів в інтересах інформаційної безпеки підприємства, установи чи організації на основі SIEM IBM QRadar та системи моніторингу дій користувачів Teramind.

ВИСНОВКИ

Отже, в ході виконання дипломної роботи було досягнуто поставленої мети та визначено доцільний спосіб моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства (установи, організації). Були отримані наступні наукові та практичні результати:

1. Проаналізовано моніторинг внутрішніх та зовнішніх процесів при управлінні безпекою інформаційних ресурсів підприємств; моніторинг процесів за допомогою SIEM та моніторинг дій користувачів за допомогою систем UAM. Аналіз показав, що функціонал цих класів рішень найбільше підходить для вирішення проблем моніторингу внутрішніх та зовнішніх процесів в інтересах інформаційної безпеки підприємства.

2. Тому було досліджено основні сучасні рішення SIEM, як основний метод моніторингу процесів та управління безпекою інформаційних ресурсів на підприємстві та досвід їх використання, та UAM як рішення для моніторингу зовнішніх процесів, активності користувачів, пошти, месенджерів та соціальних мереж. Досліджено функціональні можливості та переваги таких SIEM систем, як IBM QRadar, Splunk, ArcSight та систем моніторингу дій користувачів Ekran System, Mirobase та Teramind UAM.

3. Проведено визначення доцільного способу моніторингу зовнішніх і внутрішніх процесів в інтересах інформаційної безпеки підприємства методом експертних оцінок. По-перше, отримано оцінку сучасних рішень SIEM на прикладі вибірки з трьох представників, а саме IBM QRadar, Splunk, HPE ArcSight. По-друге, отримано оцінку сучасних рішень моніторингу активності користувачів на прикладі вибірки з трьох представників, а саме Ekran System, Mirobase, Teramind. Визначено, що серед сучасних SIEM систем перевагу по обраних параметрах має система IBM QRadar, а серед систем моніторингу дій користувачів перевагу має система Teramind.

В результаті отриманих даних щодо визначення систем безпеки було розроблено загальну схему моніторингу внутрішніх та зовнішніх процесів в інтересах інформаційної безпеки підприємства, установи чи організації на основі SIEM IBM QRadar та системи моніторингу дій користувачів Teramind.

Визначений спосіб моніторингу зовнішніх і внутрішніх процесів інформаційної безпеки може бути використаний підприємством, установою чи організацією для захисту від кібератак та підвищення рівня інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Information security management - definition & overview. URL: https://www.sumologic.com/glossary/information-security-management/

2. Information Security Management (ISM). URL: https://en.wikipedia.org/wiki/Information_security_management

3. Класифікація загроз інформаційній безпеці. URL: https://sites.google.com/site/informacijnabezpeka15/zagrozi-informacijnij-bezpeci/klasifikacia-zagroz-informacijnij-bezpeci

4. Інформаційна безпека підприємства: методи захисту від головних загроз. URL: https://group-fs.com/informaczijna-bezpeka-pidpryyemstva-metody-zahystu-vid-golovnyh-zagroz/

5. Security Information and Event Management, SIEM. URL: https://www.anti-malware.ru/security/siem

6. What is User Activity Monitoring? How It Works, Benefits, Best Practices. URL: https://digitalguardian.com/blog/what-user-activity-monitoring-how-it-works-benefits-best-practices-and-more

7. На страже безопасности: IBM QRadar SIEM. URL: https://habr.com/ru/company/muk/blog/325330/

8. The Gartner 2021 SIEM Magic Quadrant. URL: https://logrhythm.com/gartner-magic-quadrant-siem-report-2021/

9. IBM X-Force Exchange. URL: https://exchange.xforce.ibmcloud.com

10. QRadar Advisor with Watson. URL: https://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.Wat sonapp.doc/c_Qapps_advisor_intro.html

11. IBM QRadar SoftLayer. URL: https://www.ibm.com/cloud/info/softlayer-is-now-ibm-cloud

12. Security Information and Event Management with Splunk. URL: https://www.cprime.com/resources/blog/security-information-and-event-management-siem-splunk/

13. Gartner Peer Insights. SIEM. URL: https://www.gartner.com/reviews/market/security-information-event-management/compare/product/arcsight-enterprise-security-manager-esm-vs-qradar-siem-vs-splunk-enterprise

14. Splunk Analytics-driven Security Intelligence. URL: https://www.datashieldprotect.com/tools/splunk

15. Splunk Architecture: Data Flow, Components and Topologies. URL: https://cloudian.com/guides/splunk-big-data/splunk-architecture-data-flow-components-and-topologies/

16. SIEM ArcSight. URL: https://hkrtrainings.com/siem-arcsight

17. Microfocus. ArcSight Enterprise Security Manager (ESM). URL: https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm

18. Ekran System. URL: https://www.ekransystem.com/en/product/user-activity-monitoring

19. Ekran System Docs. URL: https://documentation.ekransystem.com

20. Mirobase. URL: http://www.infobezpeka.com/products/insider/Mirobase/

21. Mirobase Documentation. URL: https://mirobase.com/spravka/struktura-kompleksu-prostij-vipadok-odin-zal-ta-odin-server/

22. Teramind User Activity Monitoring (UAM). Teramind. URL: https://www.teramind.co/product/uam-user-activity-monitoring