ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Кваліфікаційна робота
на тему:

«Технологія управління користувачами в інформаційній системі організації на прикладі IBM QRadar SIEM»

Виконав: КОЛОМІЄЦЬ Олексій, БСДМ-63
Керівник: КУЗНЕЦОВ Олександр Олександрович, д.т.н., професор

Актуальність. Сучасні підприємства широко застосовують різноманітні інформаційні системи задля підвищення ефективності бізнес-процесів. Забезпечення безпеки корпоративних інформаційних систем являє собою складне і багатовекторне завдання. Одне з ключових його напрямків – управління користувачами інформаційних систем підприємства.

Об'єкт дослідження – процес управління користувачами інформаційних систем

Предмет дослідження – технологія управління користувачами SIEM-системи

Мета роботи – розробити порядок застосування технології управління користувачами в інформаційній системі підприємства та рекомендації щодо її реалізації

Наукові завдання:

- дослідити структуру та функції центру управління кібербезпекою підприємства;
- дослідити середовище користувачів SIEM-системи центру управління кібербезпекою підприємства;
- проаналізувати існуючі методи та засоби управління користувачами в SIEM-системі;
- розробити порядок застосування технології управління користувачами в інформаційній системі підприємства;
- розробити рекомендації щодо застосування технології управління користувачами інформаційної системи підприємства.

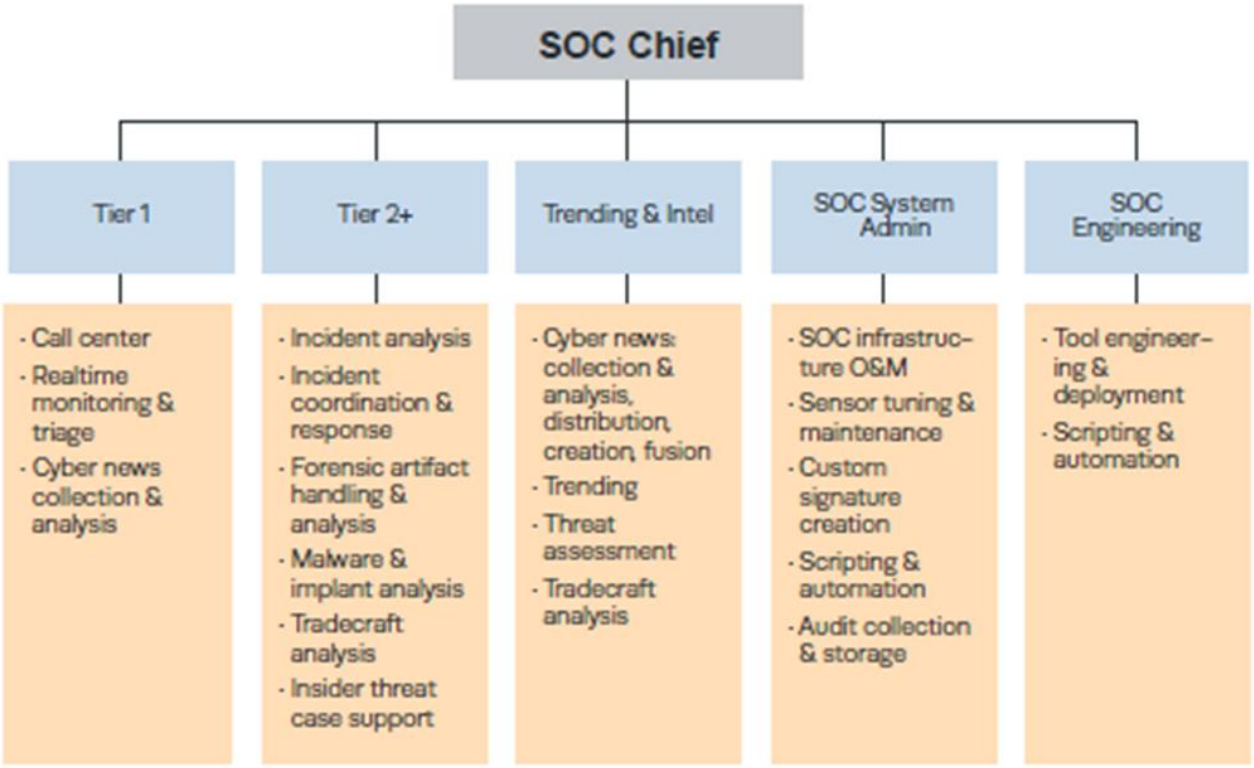
Призначення та основні функції SOC підприємства

Security Operation Centre визначається перш за все через своє основне завдання – захист комп'ютерних мереж (computer network defense, CND). CND означає дії по захисту від несанкціонованої діяльності в комп'ютерних мережах, включаючи моніторинг, виявлення, аналіз (наприклад, аналіз трендів і патернів), реагування та відновлення

Основні функції SOC

- Аналіз в режимі реального часу
- Розвідка та виявлення трендів
- Аналіз інциденту та реагування
- Аналіз криміналістичних зразків
- Підтримка життєвого циклу інструментарію SOC
- Сканування і оцінка
- Профілактика

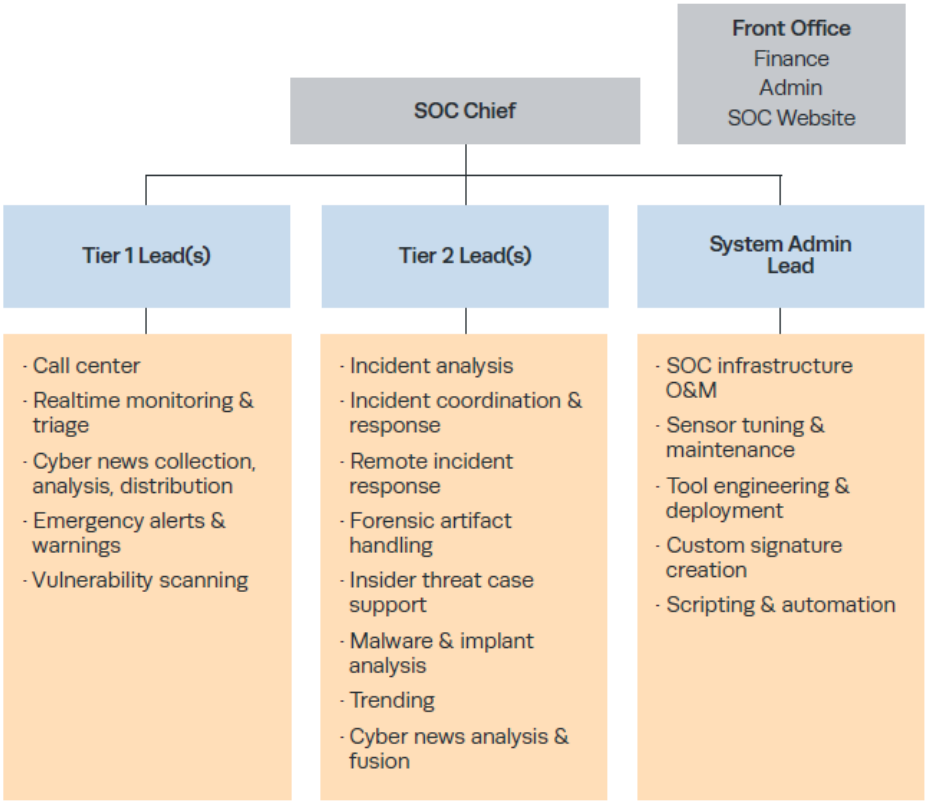
Аналіз середовища користувачів на прикладі SIEM-системи SOC підприємства



В результаті, виділяється п'ять нерозривних складових забезпечення захисту комп'ютерних мереж, які повинні знаходитися під однією командною структурою:

- моніторинг і пріоритизація в реальному часі (лінія 1);
- аналіз інцидентів, координація та реагування (лінія 2 і вище);
- збір і аналіз даних кіберрозвідки;
- налагодження та управління сенсорами, використання і підтримка інфраструктури SOC;
- Розробка та розгортання інструментарію SOC.

Мета та завдання управління користувачами в SIEM-системі

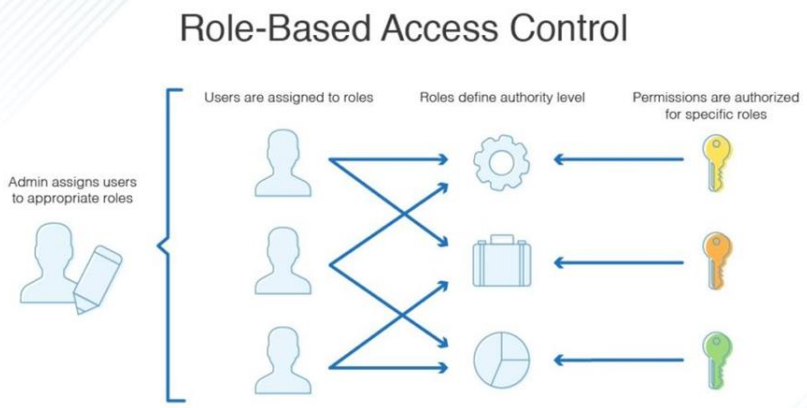


Малі SOC, в межах від п'яти до 20 осіб, часто мають просту організаційну модель. Це пов'язано з тим, що для невеликої кількості співробітників потрібна невелика диверсифікація ролей і є кілька позицій, для яких не потрібно робота аналітика на повний робочий день.

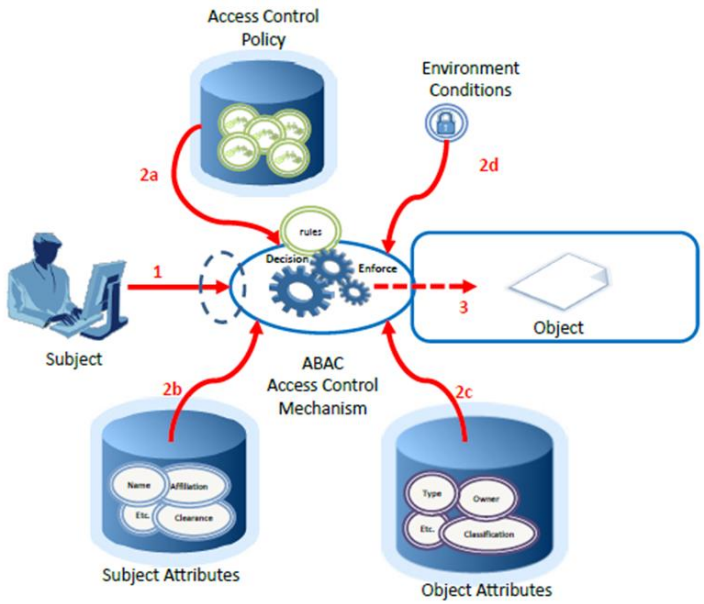
Класичний малий SOC буде включати два або три підрозділи:

- Лінія 1. Включає аналітиків, які виконують рутинні обов'язки, такі як перегляд консолей IDS або SIEM, збір даних кіберрозвідки і прийом запитів від клієнтів.
- Лінія 2. Виконує всебічний аналіз інцидентів, переданих йому з Лінії 1 (наприклад, аналіз журналу та даних PCAP) і координує процес реагування на інциденти з клієнтами.
- Системне адміністрування. Підтримує системи і сенсори SOC, що може включати в себе розробку і впровадження нових можливостей.

Аналіз існуючих підходів до управління користувачами інформаційних систем

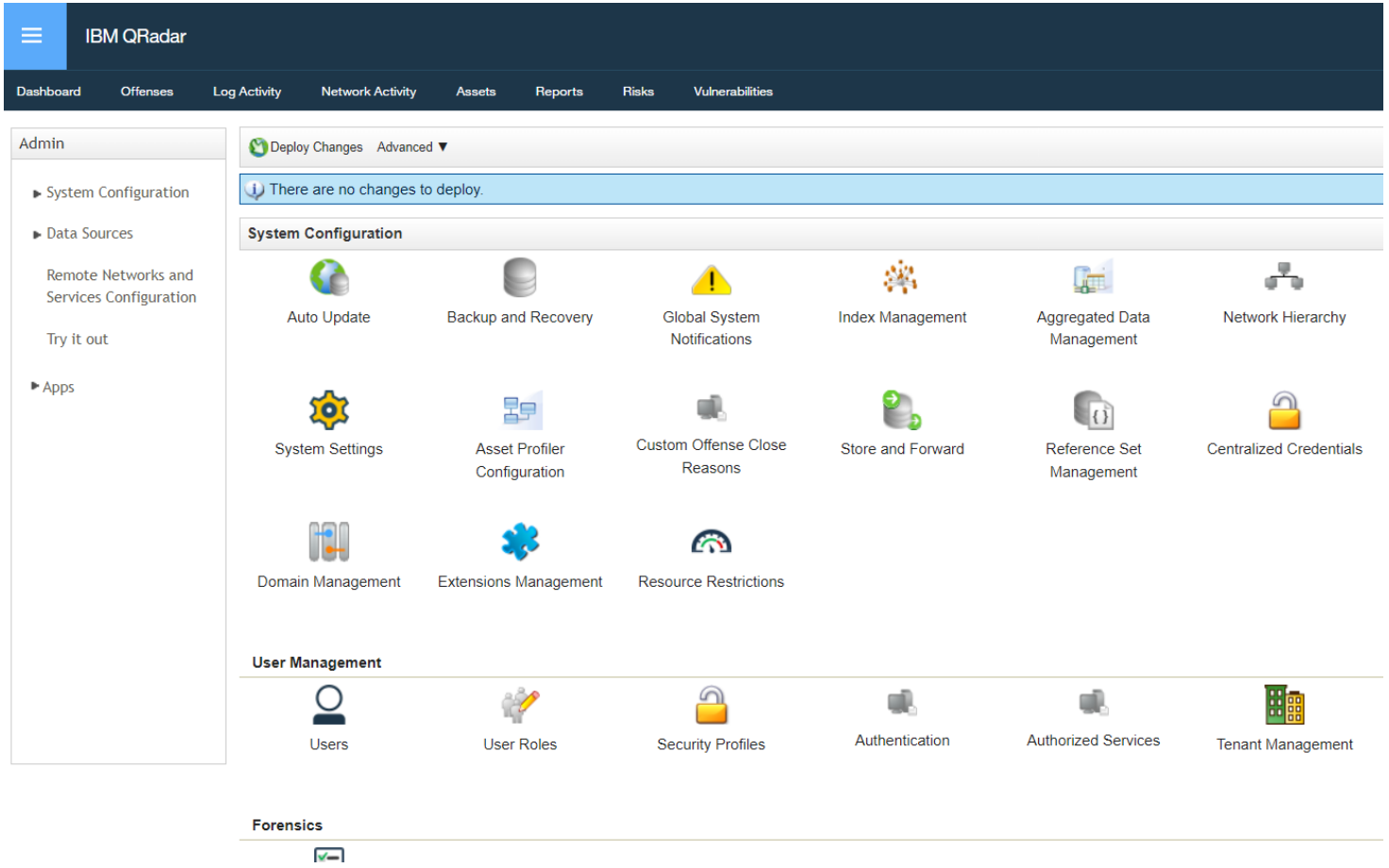


Контроль доступу на основі ролей користувача (role-based access control (RBAC)) – тобто, набір дозволів доступу, який користувач отримує на основі явного або неявного припущення про певну роль. Дозволи на роль можуть бути успадковані через ієрархію ролей і, як правило, відображають дозволи, необхідні для виконання визначених функцій в організації. Дана роль може стосуватися однієї особи або декількох осіб



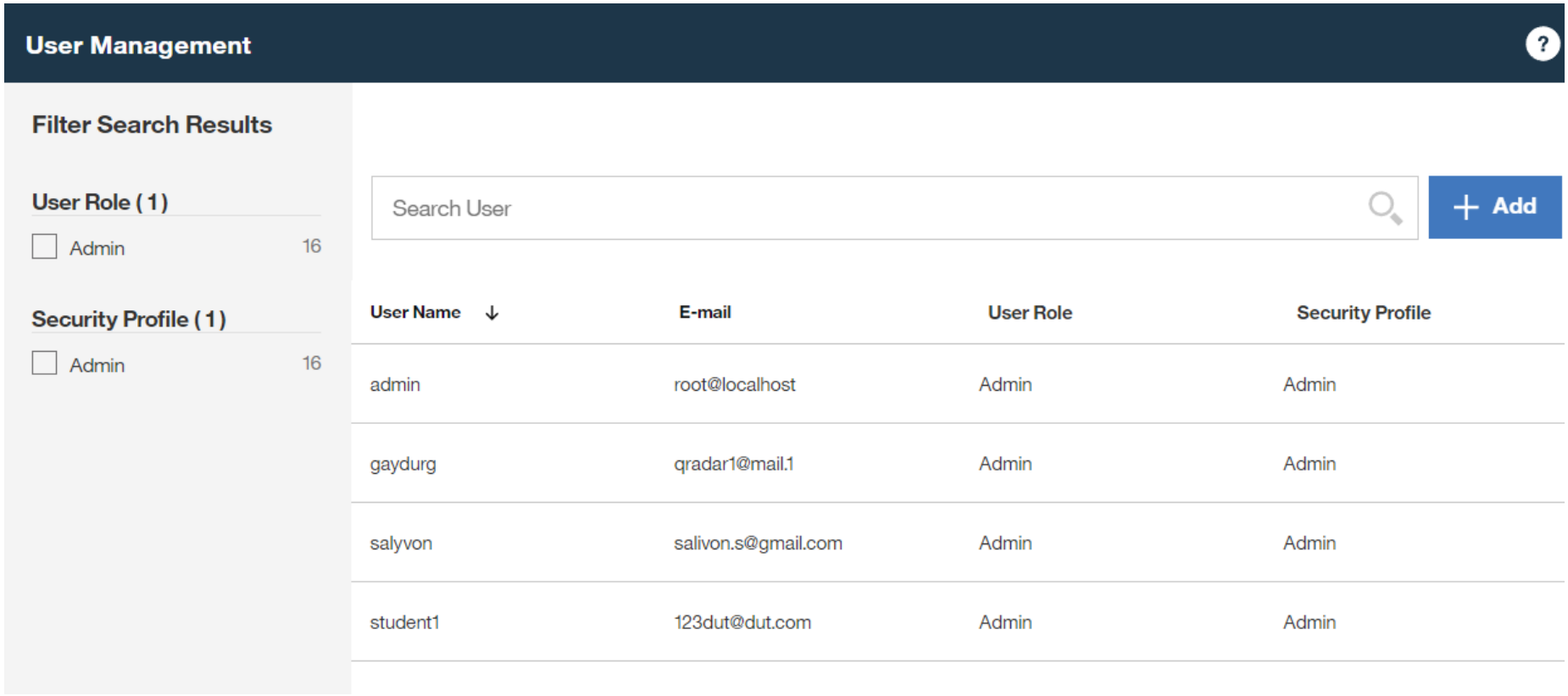
Контроль доступу на основі атрибутів (Attribute Based Access Control (ABAC)) – метод контролю доступу, коли запити суб'єкта на виконання операцій над об'єктами надаються або відхиляються на основі присвоєних атрибутів суб'єкта, призначених атрибутів об'єкта, умов середовища та набору політик, визначених у умови цих ознак та умов

Визначення можливостей щодо управління користувачами в IBM QRadar SIEM



Управління користувачами в IBM QRadar SIEM передбачає визначення ролі користувачів, профілів безпеки і облікових записів користувачів, щоб контролювати, хто має доступ до системи, які завдання вони можуть виконувати і до яких даних вони мають доступ. Реалізовано модель RBAC

Аналіз методів управління обліковими записами користувачів в IBM QRadar SIEM

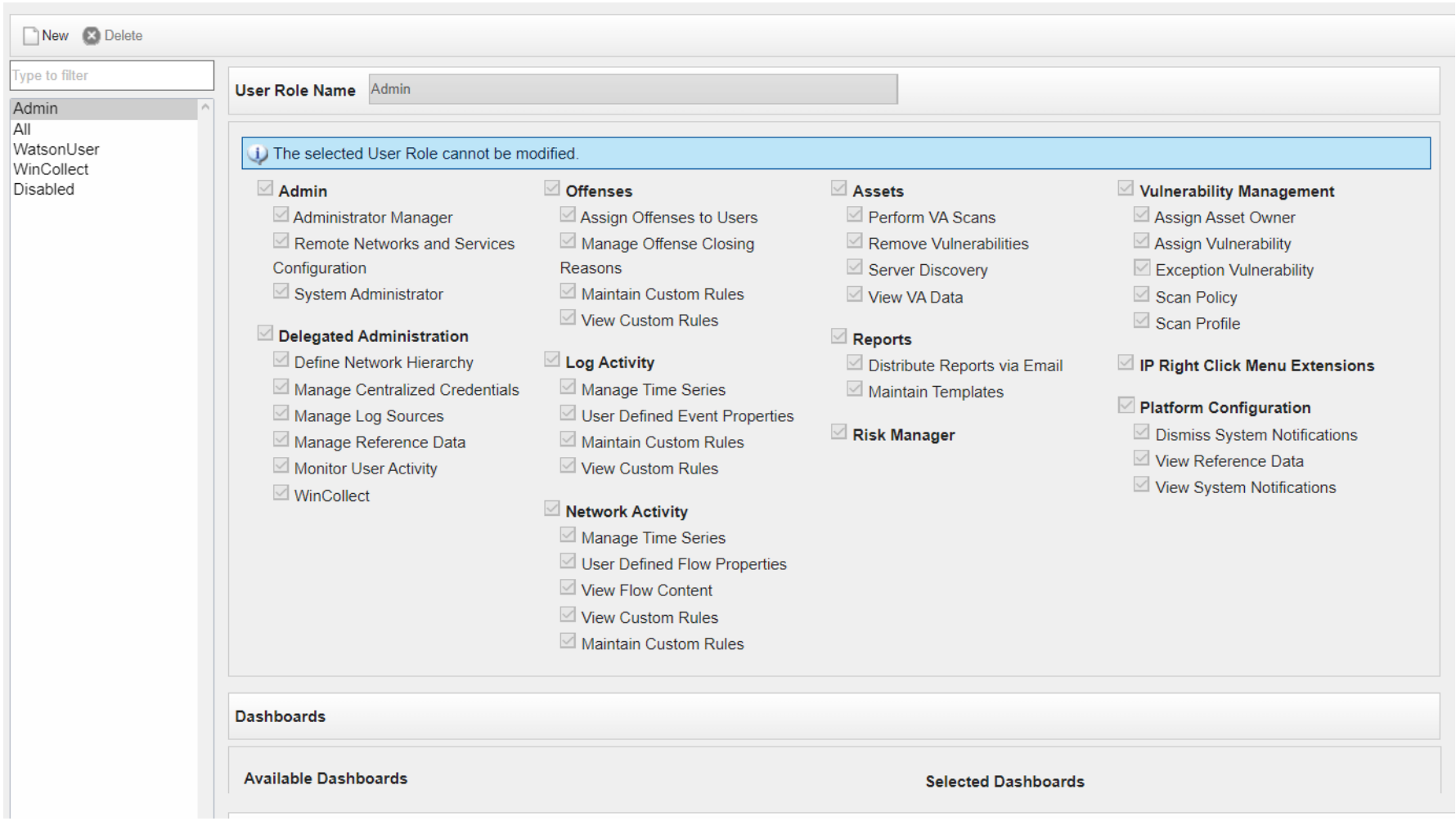


Створення облікового запису користувача

При створенні нового облікового запису користувача необхідно призначити користувачеві облікові дані для отримання доступу, роль користувача і профіль захисту. Ролі користувачів вказують, на виконання яких дій у користувача є дозвіл. Профілі захисту вказують, на доступ до яких даних у користувача є дозвіл.

Перш ніж створювати обліковий запис користувача, треба впевнитися, що створена потрібна роль користувача і потрібний профіль захисту.

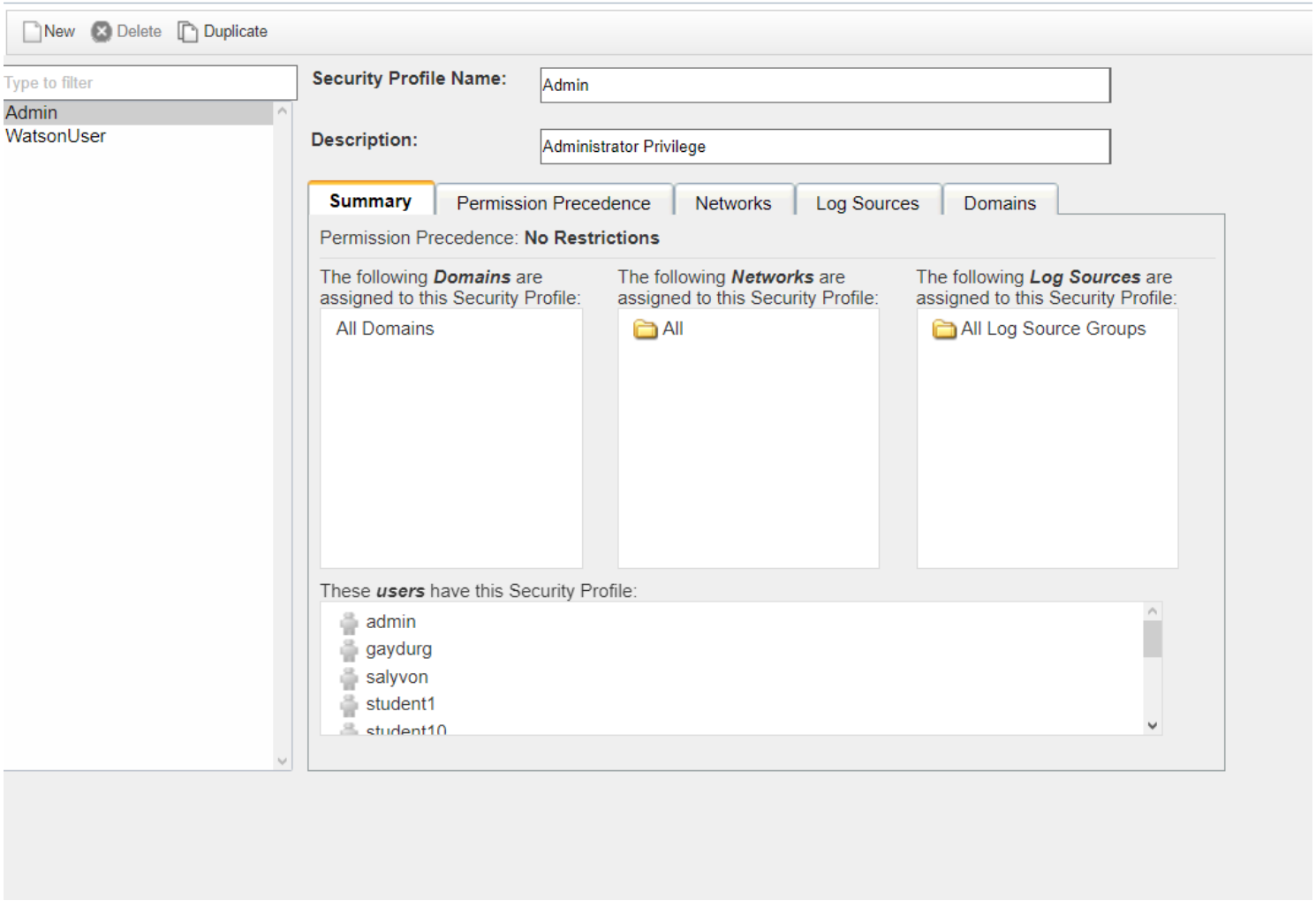
Аналіз методів управління ролями користувачів в IBM QRadar SIEM



Додавання ролі користувача

Використовуючи вікно Ролі користувачів, можна створювати ролі користувачів та керувати ними.

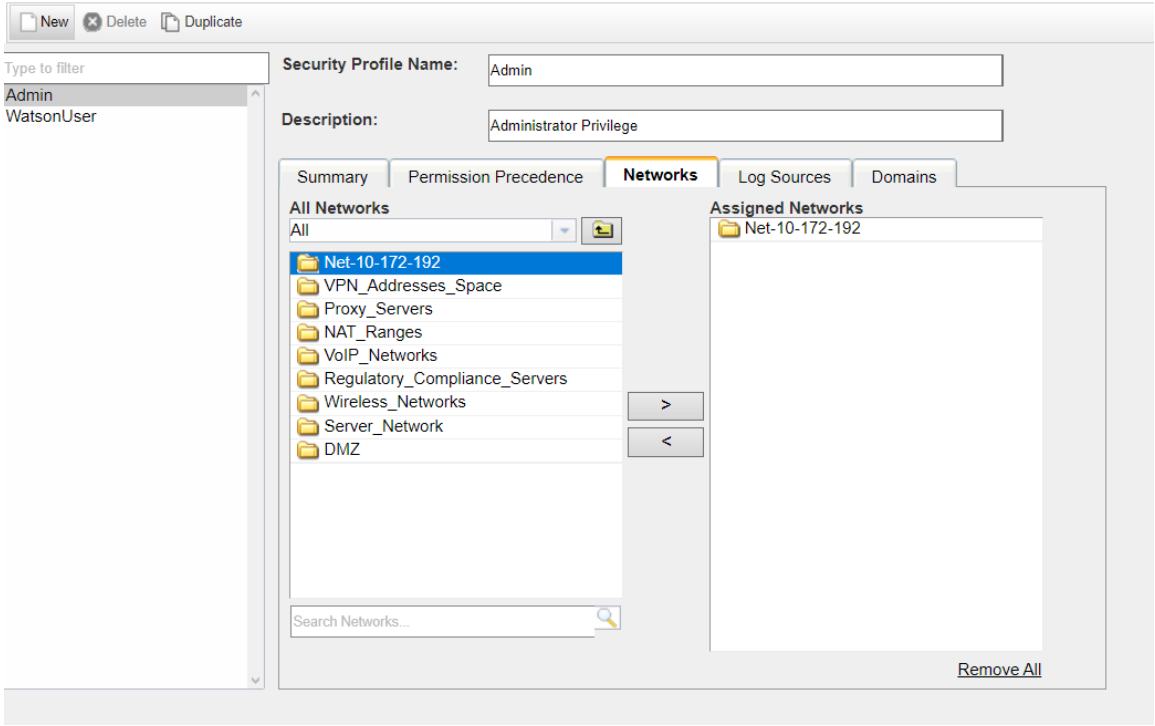
Аналіз управління профілем захисту в IBM QRadar SIEM



Створення профілю захисту

У вікні Управління профілями захисту зазначено, доступ до яких мереж, джерел журналів і доменів може отримати користувач

Технологія управління користувачами в IBM QRadar SIEM



Для правильного управління користувачами SIEM системи корпоративної інформаційної системи підприємства необхідно дотримуватися чіткого алгоритму дій, який складається з таких етапів:

- визначитися з ролями користувачів SIEM системи (посади фахівців з кібербезпеки);
- визначитися з графіком та порядком роботи SOC;

- визначитися з наявною кількістю фахівців, складом змін та порядком роботи фахівців;
- адміністратору системи за визначеними посадами створити ролі користувачів IBM QRadar SIEM;
- адміністратору системи створити облікові записи всім користувачам IBM QRadar SIEM;
- адміністратору системи створити профілі безпеки всім ролям користувачів IBM QRadar SIEM;
- адміністратору системи при необхідності (у разі змін серед користувачів системи, змін посадових інструкцій тощо) вробити відповідні налаштування сервісу управління користувачами IBM QRadar SIEM.

Результати застосування технології управління користувачами в IBM QRadar SIEM на прикладі обраного варіанту SOC підприємства

Создать | Изменить | Удалить | Поиск пользовател

Имя пользователя ▲	Описание	По электронной почте
admin	Admin	root@localhost
Alex	Адміністратор 2-ї зміни по моніторингу порушень	Alex1@ukr.net
Andrew	Адміністратор 1-ї зміни по моніторингу порушень	Andrew1988@ukr.net
Darina	Адміністратор 2-ї зміни по моніторингу подій (Log Maneger)	Nuinyan@yandex.ru
Diachenko	Адміністратор 1-ї зміни по моніторингу подій (Log Maneger)	maxd1686@gmail.com
Eve	Адміністратор 2-ї зміни по моніторингу трафіку (Network Activity)	eve3@ukr.net
Fred	Адміністратор 1-ї зміни по моніторингу трафіку (Network Activity)	fred@ukr.net
Genry	Головний адміністратор зміни (керує 1-ю зміною)	genry@ukr.net
Glen Jr	Адміністратор 2-ї зміни по моніторингу трафіку (Network Activity)	glen12@ukr.net
Helen	Головний адміністратор зміни (керує 2-ю зміною)	Helena.mim@ukr.net
Kovalenko	Адміністратор 4-ї зміни по моніторингу порушень	sasha2954441@gmail.com
KovalenkoN	Адміністратор 4-ї зміни по моніторингу подій (Log Maneger)	nazarkovalenko1@yandex.ru
KUCHER_sec_admin	Адміністратор 4-ї зміни по моніторингу трафіку (Network Activity)	student@dut.ua
Mickle	Адміністратор 1-ї зміни по моніторингу подій (Log Maneger)	mickle1@ukr.net
Naconecnuy	Администратор 2-й смены безопасности Центра управления кибербезопасностью	max3xzender@rambler.ru
Nazar	Головний адміністратор зміни (керує 3-ю зміною)	nazar@ukr.net
Nikita	Адміністратор 3-ї зміни по моніторингу подій (Log Maneger)	regenon1011@gmail.com
Pavel	Адміністратор 3-ї зміни по моніторингу порушень	Pavlik12@ukr.net
Serhii	Адміністратор 1-ї зміни по моніторингу порушень	kamikaze13@yahoo.com
Slava	Головний адміністратор зміни (керує 4-ю зміною)	zachet_na_5_@gmail.com
Slava2	Адміністратор 3-ї зміни по моніторингу трафіку (Network Activity)	qradar@gmail.com
student		123@dut.com
Аліна	Головний адміністратор зміни (керує 3-ю зміною)	qazwsx@gmail.com

Далі було створено ролі користувачів для кожної посади. Ми створили чотири профілі безпеки для кожної ролі у SIEM.

Центр управління кібербезпекою підприємства «IT-Solutions» працює за графіком 24/7 з тривалістю зміни 6 годин. Одночасно в інформаційній системі підприємства працює 4 людини на зміні. За 24 години на підприємстві змінюється чотири зміни. Враховуючи те, що кожен робітник працює по графіку «дві зміни, два дні відпочинку», було знайдено точну кількість користувачів. А саме 20.

Рекомендації щодо застосування технології управління користувачами інформаційної системи підприємства

Необхідно відмітити, що в більшості інформаційних систем підприємств – готових рішень, які постачаються вендорами, закладено функціонал саме контролю доступу на основі ролей користувача (RBAC). Як прикладі SIEM система IBM QRadar в нашій роботі. Тому, для правильної організації та здійснення User Management рекомендується:

- Ретельно визначати підрозділи та працівників, які будуть працювати з конкретною інформаційною системою.
- Ретельно визначати посадові обов'язки працівників та інформаційні ресурси, з якими їм надається право працювати за посадами та службовою необхідністю.
- Ретельно визначати коло працівників, які будуть виконувати функціональні обов'язки за конкретною посадою.
- Знати можливості функціоналу інформаційної системи та реалізованої моделі щодо управління користувачами та їх доступом до корпоративних даних.
- У разі відсутності такого функціонала в інформаційній системі необхідно приймати рішення щодо моделі управління користувачами та реалізовувати її організаційними заходами та технічними засобами.
- Адміністраторам безпеки правильно розробляти політику безпеки, що регламентує правила доступу користувачів до інформаційних систем підприємства та здійснювати керування ними та контроль за їх дотриманням.

ВИСНОВКИ

- В роботі проведено дослідження проблеми управління користувачами в інформаційних системах підприємства, встановлений його зміст та сутність завдань.
- Досліджено структуру та функції центру управління кібербезпекою підприємства, а також можливе середовище користувачів SIEM-системи центру управління кібербезпекою підприємства.
- Проаналізовано підходи до управління користувачами інформаційних систем та сучасні моделі керування доступом.
- Встановлено, що управління користувачами в SIEM-системі IBM QRadar базується на моделі RBAC. Технологію User Management складають налаштування облікових записів користувачів, ролей користувачів та профілів безпеки.
- Запропоновано варіант технології управління користувачами в IBM QRadar SIEM та здійснено її реалізацію на прикладі обраного варіанту SOC підприємства.
- Розроблено рекомендації керівникам підприємств та фахівцям з кібербезпеки щодо застосування технології управління користувачами інформаційних систем підприємства.
- Необхідно зазначити, що зміст захисту від несанкціонованого доступу (protection from unauthorized access) полягає в запобіганні або істотному утруднення несанкціонованого доступу до інформації. Тому виникає завдання керування доступом (access control) як сукупності заходів з визначення повноважень і прав доступу, контролю за додержанням правил розмежування доступу.

Таким чином, правильна реалізація політики управління користувачами інформаційних систем має забезпечити ефективний захист корпоративних даних та кібербезпеку корпоративної інформаційної системи підприємства в цілому.

Дякую за увагу!
Доповідь закінчено