Ekran system

# БОРОТЬБА З ІНСАЙДЕРАМИ

# Навіщо керувати внутрішніми загрозами: актуальна статистика

**72%**

**більше інцидентів, пов'язаних із внутрішніми загрозами, сталося у 2021 році, ніж у 2020 році**

згідно зі звітом про інсайдерські ризики DTEX 2022

**74%**

**витоків даних у 2022 році були пов'язані з людським фактором**

згідно зі Звітом про розслідування витоків даних за 2023 рік від Verizon

**83%**

**організацій мали більше одного витоку даних у 2021-2022 роках**

згідно зі звітом IBM Security "Вартість витоку даних у 2022 році

**$15.4 M**

**середньорічна вартість інсайдерських загроз у 2021 році**

згідно зі звітом "Вартість інсайдерських загроз у світі за 2022 рік", підготовленим Ponemon Institute

# 5 ключових типів інсайдерів

**1**

### Зовнішній агент

Фіктивний співробітник, який викрадає дані для інших компаній або урядів

**2**

### Зловмисний працівник

Співробітник, який незаконно отримує доступ до конфіденційних даних для особистої вигоди

**3**

### Недбалий працівник

Співробітник, який встановлює неавторизовані програми, нехтує рекомендаціями щодо пароля та не дотримується інших заходів безпеки

**4**

### Незадоволений працівник

Звичай колишній працівник, який хоче завдати шкоди репутації компанії

**5**

### Необережна третя сторона

Ділові партнери або зацікавлені особи, які ставлять під загрозу безпеку через недбалість, неправильне використання або неавторизований доступ

# Інсайдерські загрози для організації

1. Тіньові IT

2. Ненавмисна інсайдерська діяльність

3. Навмисна інсайдерська діяльність

4. Доступ користувачів до корпоративних додатків та інфраструктури

5. Відсутність видимості робочого процесу

# Шляхи компанії

## 1. Не звертати увагу

Покладатись на долю та не звертати уваги на ризики, пов’язані з інсайдерами

## 2. Використовувати спеціалізоване ПО для захисту

Різнорідні рішення для контролю файлів, ПО, інфраструктури.

## 3. Сфокусуватись на боротьбі з інсайдерами

Рішення, заточені на виявлення аномалій в поведінці і контролю злонаміренних дій користувачів

# Вирішення

✓ **Alerts**
Налаштувати правила та використовувати вбудовані шаблони і сповіщення для розповсюджених **додатків, вебсайтів та програм**, які можуть бути використанні для зловмисницької діяльності

✓ **Education**
Налаштувати правила сповіщення користувачів згідно бізнес-процесів для більш прозорої робити співробітників і подальшого **навчання по використанню саме корпоративних правил і ПЗ**

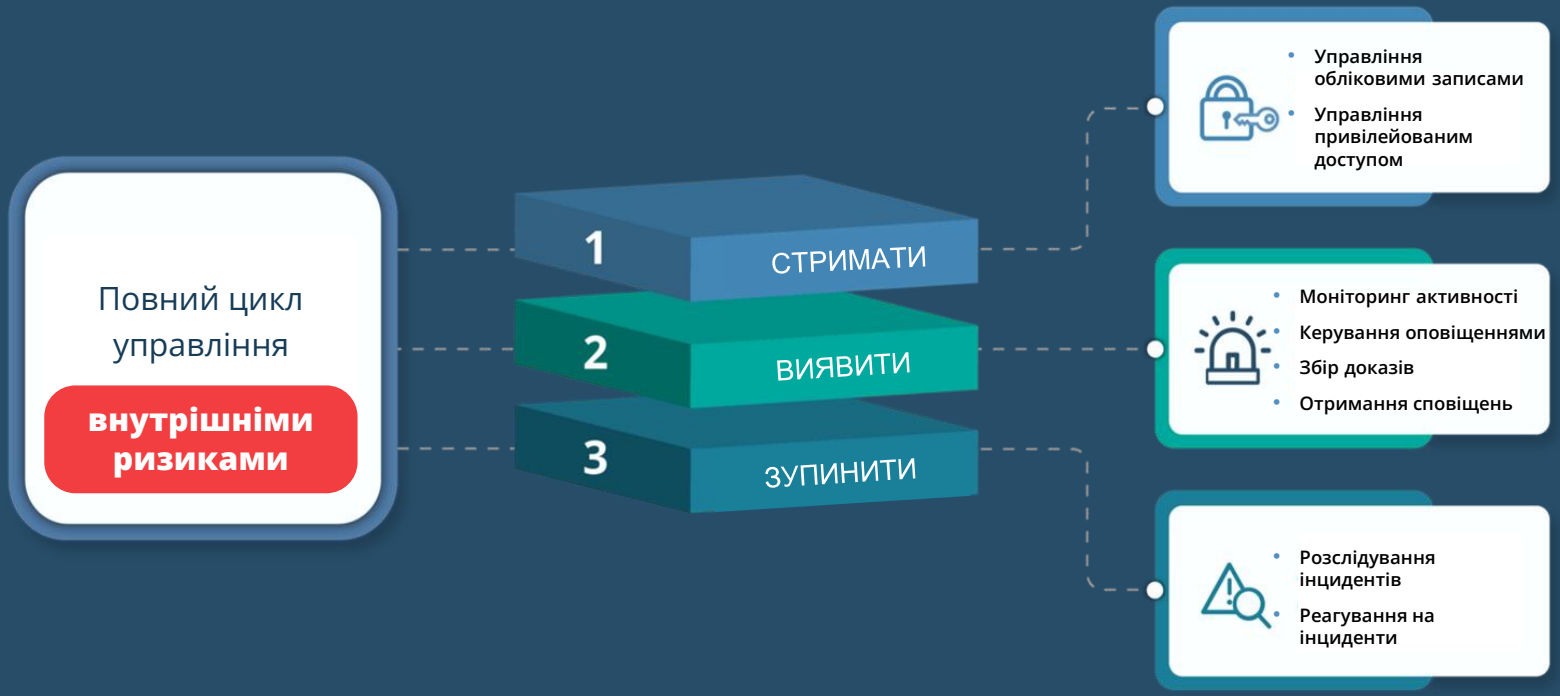
✓ **Monitoring**
Налаштувати правила для внутрішніх користувачів, підрядників для **оперативного реагування в реальному часі на підозрілі дії** і при необходності автоматично записувати сессії для виявлення інциденту і розслідування загроз

✓ **Access**
Налаштувати правила сповіщення користувачів та департаменту ІБ в модулі Ekran System PAM, які дозволяють **проходити аутентифікацію з гранульованим дозволом.** Допоможе вчасно сповіщати про несанкціоновані запити доступу до чутливої інформації або аккаунтів з привілейованим доступом

✓ **UEBA & Reports**
Створення поведінкових моделей з **аналізом активності користувачів під час робочих годин і формування відповідних звітів з піковою активністю або простоями.** З останнім оновленням **Ekran System інтегрується з MS Power BI**

# Управління інсайдерськими ризиками повного циклу

Ekran System – це платформа для управління інсайдерськими ризиками повного циклу, яка ефективно стримує, виявляє та усуває інсайдерські загрози.



# Про Ekran System

Ekran System допомагає організаціям по всьому світу посилити свою безпеку та забезпечити відповідність вимогам в рамках своєї IT-інфраструктури.

**Заснована**
**2013**

**Офіси**
**4 країни**
**Штаб-квартира: Needham, MA**

**Клієнти**
**2500+**

**Партнери**
**300+**

# Галузі з конфіденційною інформацією використовують Ekran System

Фінансові сервіси та страхування

Уряд та Збройні сили

Енергетика

Телекомунікації

Державне управління

Охорона здоров'я

# Американська оборонна організація посилює захист від інсайдерських загроз за допомогою Ekran System

Як військова організація, яка захищає стратегічні об’єкти, наш клієнт має безпечно обробляти великі обсяги конфіденційних даних і відповідати суворим вимогам кібербезпеки.

## Вимоги:

- ✓ Контролювати діяльність співробітників
- ✓ Зменшити ризик внутрішніх загроз
- ✓ Прискорити розслідування інцидентів кібербезпеки
- ✓ Легко інтегруйвати в існуючий робочий процес
- ✓ Забезпечити дотримання вимог кібербезпеки

## Результат:

- ✓ Повна видимість дій користувача
- ✓ Ефективне запобігання та пом’якшення внутрішніх загроз
- ✓ Зменшення часу розслідування та доступності доказів
- ✓ Нульовий негативний вплив на продуктивність мережі та робочі процеси співробітників
- ✓ Засоби для виконання вимог відповідності

Ekran system

# Дякую!