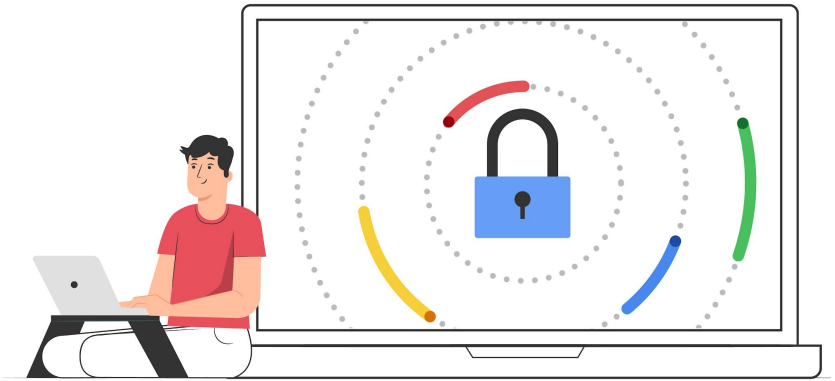
Безпечніше з Google

Google | ISSP | kitsoft

Онлайн-курс

Основи кібербезпеки для бізнесу

Кейс-стаді: кібербезпека та кібератака очима підприємця



Ярослав Беззубець

QA Team Lead/Cyber Security Engineer, Kitsoft

Досвід:

- 7 років в тестуванні програмного забезпечення
- 2 роки в тестуванні безпеки програмного забезпечення

Спеціалізація:

- налагодження процесу тестування ПЗ
- керування командою QA
- впровадження кібербезпеки

Київ

Yaroslav Bezzubets

kitsoft

Цифрова трансформація для держави

50+
веб-порталів

150+
цифрових послуг

17
років досвіду

20M+
користувачів продуктів

100
професіоналів в команді

120
інтеграцій із зовнішніми системами

Портал Дія

єМалятко

ЕкоСистема

Politdata

kitsoft.ua

Експертні консультації

1. **Безкоштовна 30-хвилинна сесія** з експертом із кібербезпеки ISSP
2. **Безпечне** та **конфіденційне середовище** для запитань стосовно кіберзахисту свого бізнесу
3. Можливість отримати **персоналізовану пораду** на свій запит
4. **Кількість консультацій обмежена**, відбір учасників на основі заповненої форми запиту
5. **Рівень попередніх знань не є критерієм відбору**

Програма

1 Кейс-стаді: досвід Kitsoft

1.1 Кібератаки та подолання їх наслідків

1.2 Безпечний життєвий цикл розробки програмного забезпечення

1.3 Інвентаризація активів, оцінка та зменшення ризиків

1.4 Створення та впровадження політик, і процедур з кібербезпеки

1.5 Навчання кібербезпеки співробітників

1.6 Корисні ресурси та висновки

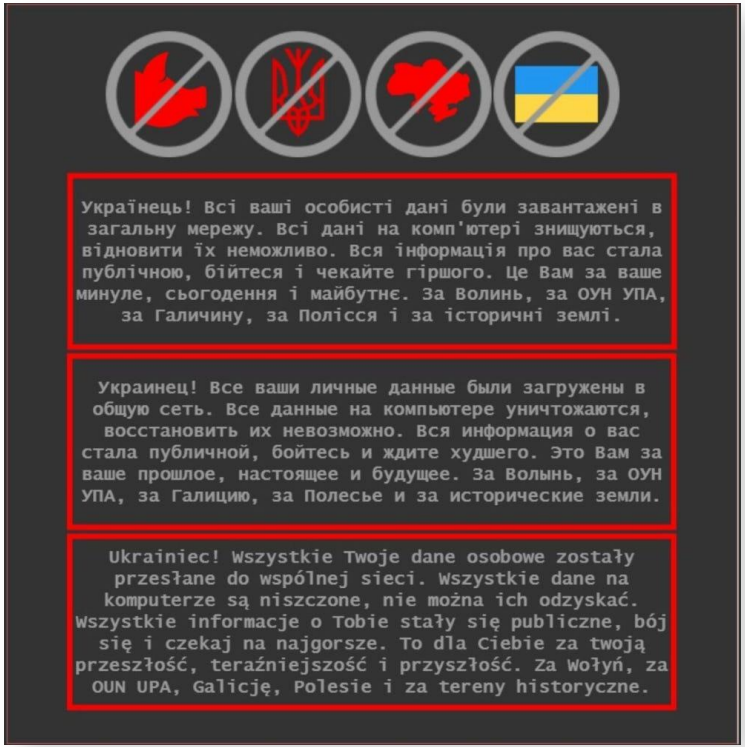
2 Сесія запитань-відповідей з модератором

1 Кейс-стаді: досвід Kitsoft

1.1 Кібератаки та подолання їх наслідків

Кібератака на державні сайти 14 січня 2022 року

- Постраждали близько 70 державних сайтів
- Мета зловмисників: заблокування доступу до ключових інформаційних державних ресурсів
- Атака CVE-2021-32648



Кібератака CVE-2021-32648

👨‍💼👩‍💼🏢

- Відбулась через **вразливість в функціоналі відновлення пароля**
- Зловмисники отримали **доступ до адміністративної панелі** застарілих ресурсів

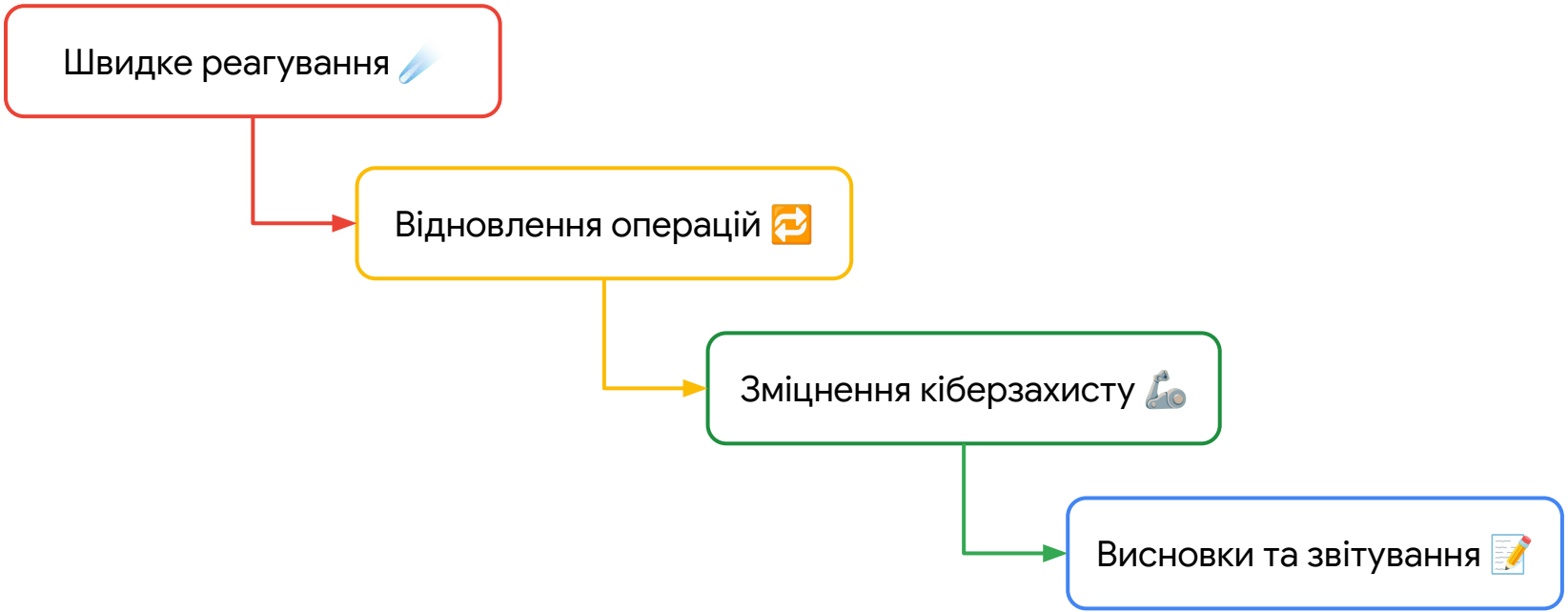
👩‍💻👨‍💻

- **Не** була здійснена через **ланцюжок постачання**
- Процеси неперервної інтеграції та неперервного розгортання **(CI/CD) не були скомпрометовані**
- Шкідливе ПЗ не було розповсюджене через ці процеси

🏛️☑️👀

- Було використано **відому вразливість**
- Уражені сайти **не були оновлені** до версії, в якій ця вразливість була виправлена

Кібератака та подолання наслідків



Кібератака та подолання наслідків

- ідентифікація джерела та методу атаки
- аналіз і сканування ураженої зони

- аналіз уражених систем та втрат даних
- застосування резервних копій

- вдосконалення політик безпеки
- перевірка ефективності заходів безпеки
- тренінги для персоналу

- документування хронології подій + вжитих заходів + результатів
- аналіз причин

1.2 Безпечний життєвий цикл розробки програмного забезпечення

Життєвий цикл розробки програмного забезпечення (SDLC*)

*SDLC (англ. Software Development Life Cycle) – Життєвий цикл розробки програмного забезпечення - це фреймворк, який визначає кроки, пов'язані з розробкою програмного забезпечення на кожному етапі.

Безпечний життєвий цикл розробки в Kitsoft

Визначення безпекових вимог: Інтеграція безпекових вимог, таких як автентифікація, авторизація, шифрування, і захист даних від самого початку

Оцінка ризиків: Проведення оцінки ризиків для ідентифікації потенційних загроз та вразливостей

Життєвий цикл розробки в Kitsoft

Кодування з урахуванням безпеки: Застосування найкращих практик безпечного кодування та використання стандартів, наприклад, OWASP*

Код-рев'ю: Регулярне проведення перевірок коду на відповідність безпековим стандартам

SAST*: Використання статичних аналізаторів коду

*OWASP – онлайн-спільнота, яка створює вільно доступні статті, методології, документацію, інструменти та технології в галузі безпеки вебзастосунків
*SAST – статичне тестування безпеки програми використовується для захисту програмного забезпечення шляхом перегляду вихідного коду програмного забезпечення для виявлення джерел уразливостей.

Життєвий цикл розробки в Kitsoft

Автоматизоване тестування безпеки: Використання інструментів для автоматичного виявлення вразливостей, наприклад, динамічного аналізу коду

Ручне тестування безпеки: Тестування на проникнення і емуляції атак

Життєвий цикл розробки в Kitsoft

Перевірка конфігурації: Забезпечення, що конфігурації серверів, баз даних та інших компонентів безпечні

Управління змінами: Контроль змін у продуктовому середовищі для забезпечення стабільності і безпеки

Життєвий цикл розробки в Kitsoft

Моніторинг та логування: Відстеження подій безпеки у реальному часі й зберігання логів* для аналізу

Оновлення і патчі*: Регулярне оновлення систем та застосування патчів для усунення виявлених вразливостей

*логи доступу – програмні журнали подій успішного або безуспішного доступу до середовища
*патчі – оновлення або виправлення програмного забезпечення, яке виправляє помилки, закриває вразливості безпеки або покращує функціональність програми.

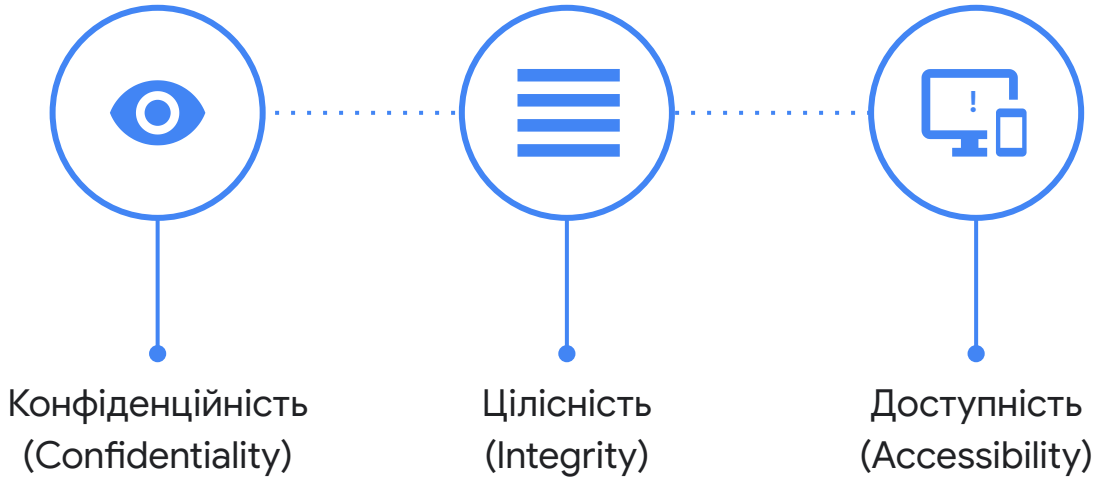
1.3 Інвентаризація активів, оцінка та зменшення ризиків

Крок 1: Інвентаризація активів

1. **Техніка:** Ноутбуки, стаціонарні ПК, сервери
2. **Мережева інфраструктура:** Маршрутизатори, точки доступу бездротового зв'язку та модеми
3. **Сервіси та ПЗ:** Платформи електронної пошти та комунікацій, CRM системи, системи таскмедженту та інші
4. **Об’єкти інтелектуальної власності тощо:** Власні алгоритми та програмний код

Крок 2: Оцінка ризиків

Для кожного з активів робимо оцінку трьох параметрів:

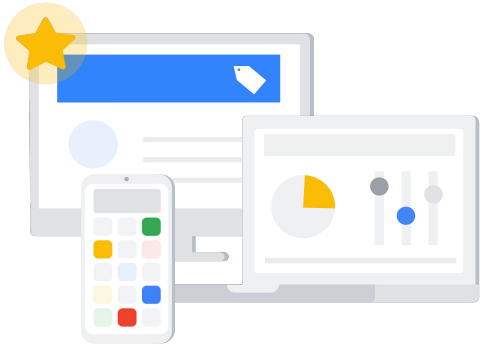


Крок 2: Оцінка ризиків

Оцінюємо кожен параметр за трибальною шкалою, де **3 - найвищий рівень** критичності наслідків кіберризиків для активу, **1 - найнижчий**. Далі – оцінюємо вірогідність настання ризику кожного з цих параметрів.

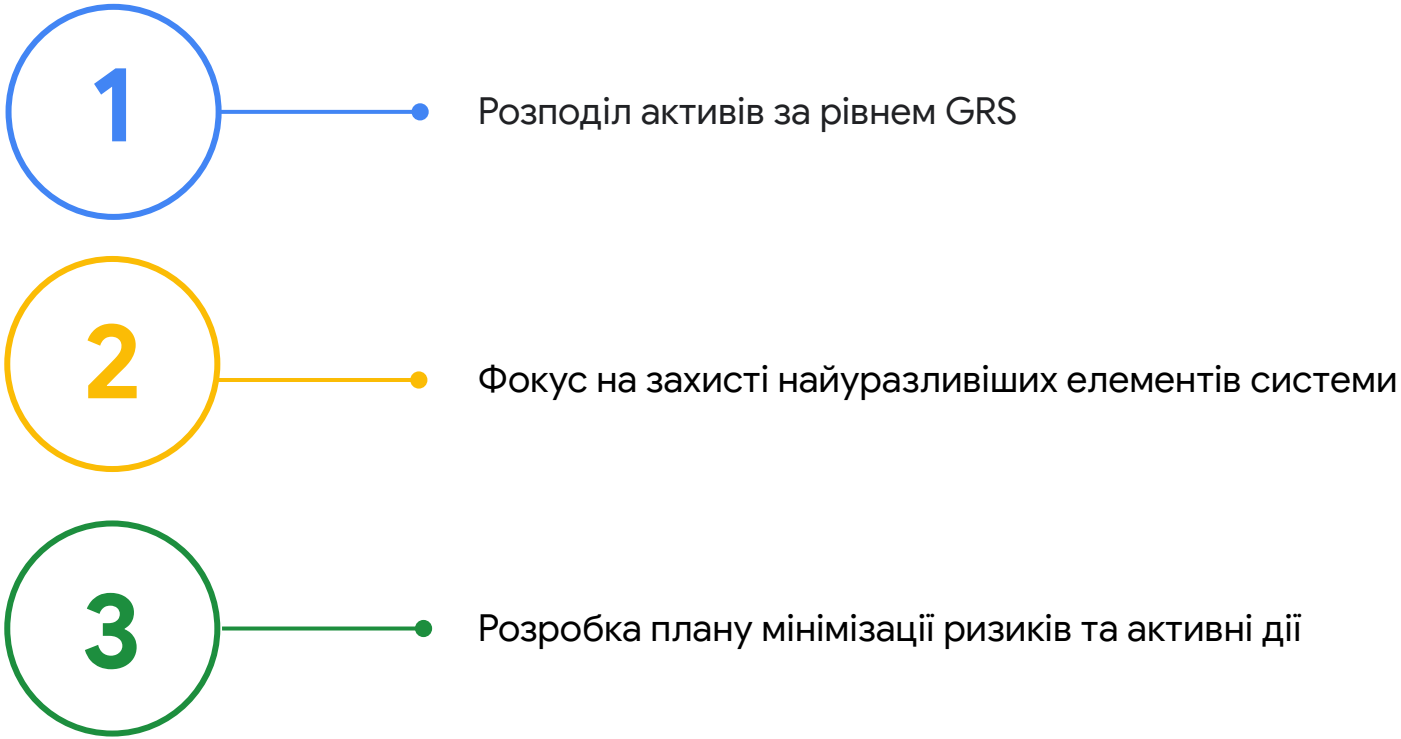
Рахуємо GRS* простим додаванням перемножених параметрів на вірогідність.

GRS = Значення КЦД (Конфіденційність/Цілісність/Доступність) x Ймовірність



*GRS (англ. Gross Risk Score) – загальний рівень ризику

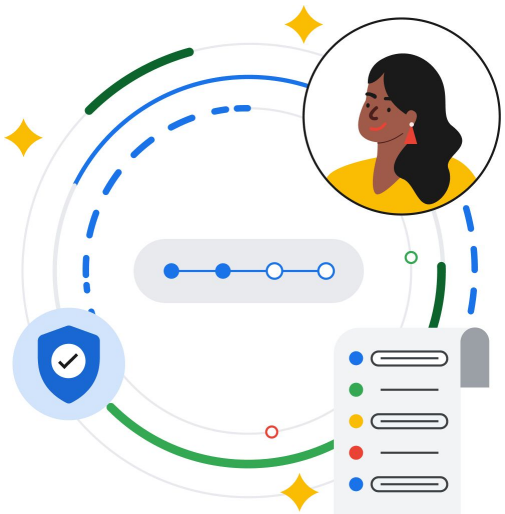
Крок 3: Зменшення ризиків



1.4 Створення та впровадження політик, і процедур з кібербезпеки

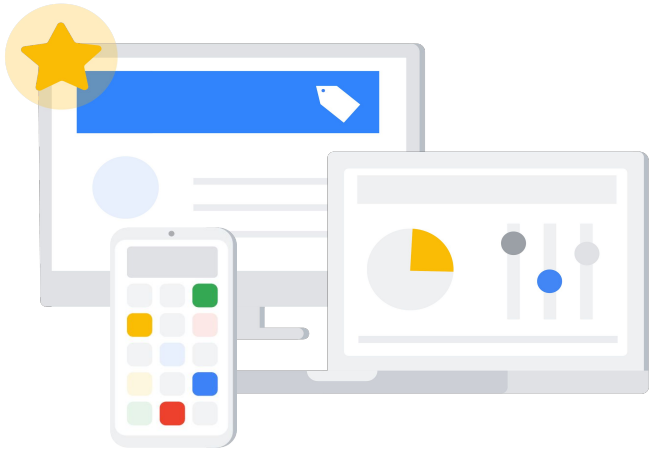
Політика паролів

1. **Вимоги до складності паролів:**
    - Мінімум вісім (8) символів у довжину
    - Англійські великі та малі літери (A-z)
    - Десяткові цифри (0-9)
    - Спеціальні символи (наприклад, !, $, #, %)
2. **Періодичність зміни паролів:** Паролі мають оновлюватись кожних три місяці
3. **Унікальність паролів:** Паролі до різних застосунків мають бути унікальними
4. **Зберігання паролів:** Паролі мають зберігатись в менеджерах паролів



Політика використання пристроїв

1. **Захищений доступ до пристрою:** Акаунт пристрою має бути обов'язково захищений паролем
2. **Оновлення операційної системи:** Має бути активовано автоматичне оновлення, та встановлено актуальну версію операційної системи
3. **Контроль використання пристроїв:** Пристрій має використовуватись лише для робочих цілей, на пристрої має буди встановлено лише ліцензійне програмне забезпечення



Політика використання пристроїв

✅ Дозволено:

- Використання корпоративних пристроїв лише для робочих завдань
- Використання лише ліцензійного програмного забезпечення
- Використання пристрою для перегляду сайтів для навчання, та саморозвитку

🚫 Заборонено:

- Використання Android та iOS додатків, розроблених компаніями країни-агресора
- Встановлення неліцензійного програмного забезпечення на комп'ютери компанії
- На мобільних пристроях Android/iOS заборонено використовувати root-доступ* та JailBreak
- Відвідування ненадійних вебсайтів та встановлення сумнівного програмного забезпечення

*root-доступ – найвищий рівень доступу до операційної системи, який дозволяє користувачеві мати повний контроль над системою

Політика інцидентів безпеки

1. **Відповідальні особи:** Потрібно визначити відповідальних осіб, які будуть займатись реагуванням, та вирішенням інцидентів з безпеки
2. **Список типів інцидентів:** Має бути визначено перелік типів інцидентів на які має реагувати відповідальні особи
3. **Процедура реагування:** По кожному інциденту має бути прописана чітка процедура реагування на інцидент

Інші впроваджені політики

1. **Політика захисту персональних даних:** Якщо організація обробляє персональні дані, ця політика визначає як вони мають бути захищені
2. **Політика фізичної безпеки:** Визначає заходи для захисту фізичних активів організації та інформації
3. **Політика резервного копіювання:** Політика, яка встановлює вимоги до створення, зберігання та перевірки резервних копій важливих даних

Впровадження стандарту secure.txt

- Kitsoft використовує стандарт secure.txt*, щоб забезпечити безпечний і анонімний механізм для повідомлення про знайдені вразливості в системах безпеки
- Розміщення файлу secure.txt у корені нашого вебсайту дозволяє етичним хакерам знати, як і куди вони можуть відправити свої звіти

→ підвищує рівень кібербезпеки нашої компанії

→ захищає репутацію, уникаючи публічного розголошення інформації

```
Contact: mailto:secure@kitsoft.ua
Expires: 2025-04-23T22:59:00.000Z
Preferred-Languages: ua,en
-----BEGIN PGP SIGNATURE-----
xsBNBGYiU/gBCADU5QO/QSrX/uScoO9xi+pMougf19RZvIR8RMI0j9yWbyW8
VHnNfy+j8LsP0EGRrr7gXCHyoCa68piPRjpvZzVrAXQr9AU21pxvcjrE8MUq
7f/kQy0nhupDVMs03MUhkHZq6LaizzPcVTF7x3C0B6ba0Ai7Yxzsu6u6wdUt
w+xrj1SqKjWLcvwgfbrn3kQ7oMtGPq76jOFriao9G2DTtvqHRziFFS/HNbCw
nFH3+VyETHkNUe0rYBiuy66rPx0iFznx5ZztMif1UhWjpFJG3CnPk46KYg9t
tu8mvMgGB+g5qdeknFEwfVbuVBekh8mKF6iroLqJ805LYEG+2AfVNuH3ABEB
AAHNG0tpdHNvZnQgPHNlY3VyZUBraXRzb2Z0LnVhPsLAjQQQAQgAIAUCZiJT
+AYLCQcIAwIEFQgKAgQWAgEAAhkBAhsDAh4BACEJEMLhTAoXYj57FiEEQAVs
j4KD4KPhnrndwuFMChdiPnskwggA0kQR60aXFKuP7Gvk8QSWecRpMU6O1wZD
hyEFLZgU+x/KVUstj54RZsJPoaeWlCL8f5PqsLsigRctIAMUcMDJ03EY3vPj
B0jJiOFSOoqF59x+rRc86oY82GviUCrUfBqjx165WhySnXb69gUCYN3jzLY0
i8r7IXxyY+WqySMUvbBdlGEqIDCy37eYzx5RbEAykgVrLuAgnMYSb9sFlV0b
5tZ3i0fK9PIPjzmFMVUSggPAA6z3HqEaYWGXjH+TJuB+mHQaf3f595i7DNeN
7PNcCVkaLb4TNPstNVFO0aoh9gDw0kGmywzvoadaTsN85sRoyiPIY2QOQqmJ
YSoyR0GeU87ATQRmIlP4AQgArQO2LsVH5NBHJlppOfpM9/8YaIPyatpw4/Vz
lnB9W7U9G0ViVnIsWclUMahjqg7MysMF1GzUSqxYips15dWCcznl/g89dgo7
jjw6pIlgV62wPgzivB3XJVadFqunQSJIm5iRS88QKXTVDc/ZoBHeNKEbaiKO
wo3cfXcDqNo/QISrK+s7EWE+ZUiFa8BKpkY/zYY6Bp54Vltoexu/0xwmv3UC
1LHxS2jnhRI1o1IrK3HyNsY2EIOnykqfsn4YqUQKb5PCOfa2nrsnUqSQyS/W
ctYuB4g6MclYglwzzpye3QXKEcNLvXOiMdEPbdKT8/qcGiJ5F8GSLxlu+QnR
8z138QARAQABwsB2BBgBCAAJBQJmIlP4AhsMACEJEMLhTAoXYj57FiEEQAVs
j4KD4KPhnrndwuFMChdiPnv3iAf9HIh9m30i/u6Qhwu9awbI/panHa8tHxJ2
pXHHFDKphouWYvbT5rzRoe2YytIw3rKqW5DcG1XOPpSRKCrdX7pESnBu9bli
h8R2ssP9zq342fhJbLYecm5oXBlagUhmZJP6NbYu3jnPEv/njfBwGgptVgoy
t3/n6vu6KgFsopukiTX84QQflVUN/9gGhbdWAMWWocexTvj3y90g3wSbwy6L
dAffJKO4I2SLXk+/TPM6trBIRbNczCL1ETjptnq3WjmCO6S6P6RGJCvzNiJp
EQ4sIeD5rCTv/wiXcBx8wc/rUzgOYfJYI10EPOpyT89zmG4k5uoyvLmjOtZY
vywb7rWQJA==
```

*secure.txt — це запропонована чернетка стандарту Інтернету щодо інформування про безпеку вебсайтів, який повинен дозволяти дослідникам безпеки легко повідомляти про вразливості безпеки.

Чому ISO 27001 Важливий для Kitsoft?

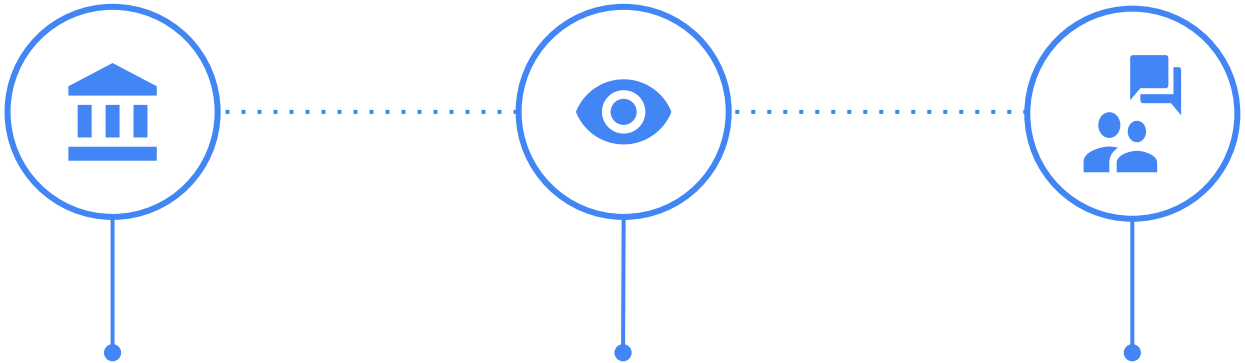
- **Забезпечення довіри клієнтів:** Сертифікація підтверджує відповідальність та надійність нашої системи управління інформаційною безпекою

- **Покращення управління ризиками:** Впровадження найкращих міжнародних практик управління ризиками та інформаційної безпеки

- **Оптимізація процесів:** Вдосконалення внутрішніх процесів та ефективність управління безпекою інформації

1.5 Навчання кібербезпеки співробітників

Як Kitsoft навчає співробітників



Всередині компанії

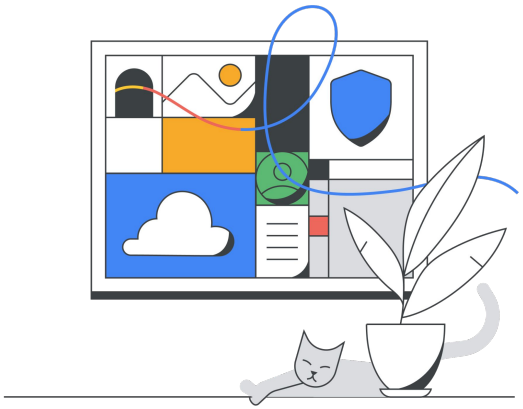
Тренінг центри та платформи з навчання

Зовнішні консультанти з кібербезпеки

1.6 Корисні ресурси та висновки

Корисні ресурси

- Курси для усіх співробітників – “Кіберняні”
- Курси для технічних спеціалістів – Cybersecurity fundamentals



Запрошуємо також переглянути короткий курс “Підвищуйте безпеку свого бізнесу в Інтернеті” від Google

Корисні інструменти

Google One

Mozilla Monitor

Keeper data breach scan

Перевірка компрометації акаунтів

Squarex

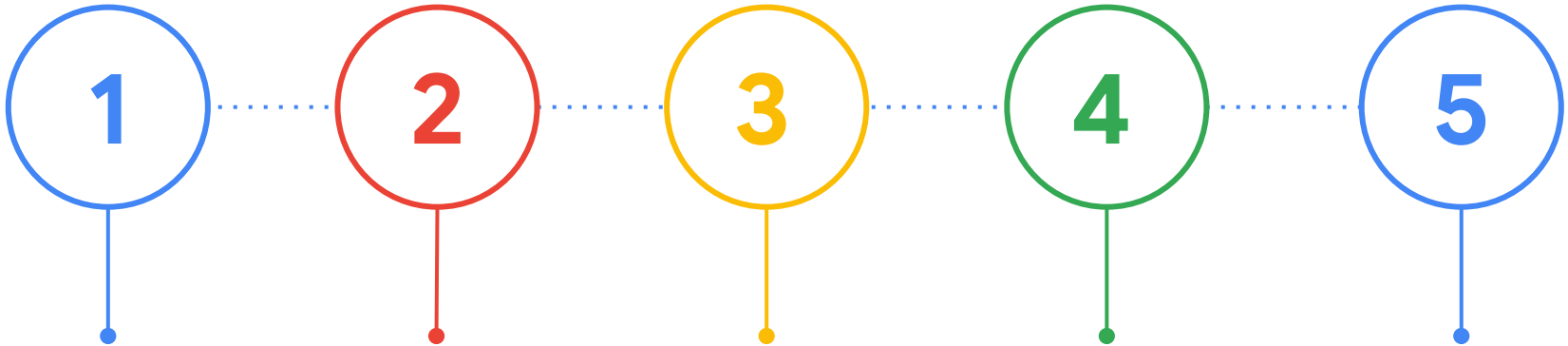
Безпечний перегляд підозрілих файлів та посилань

Висновки

Сьогодні ви дізнались, що:

- Інвентаризація активів, оцінка та зменшення ризиків є **ключовими компонентами ефективного управління кібербезпекою** в компанії
- Політики з кібербезпеки, допомагають **підготуватись до кібератак**, **описують процедуру реагування**, та **допомагають подолати їх наслідки**
- Регулярне навчання кібербезпеки **збільшує обізнаність і компетенції** співробітників, та є життєво важливим для **забезпечення стійкості та захищеності** організації від кіберзагроз

Загальні висновки онлайн-курсу “Основи кібербезпеки для бізнесу”



1. Визначте критичні бізнес-процеси та активи, це допоможе розставити пріоритети в розбудові кібербезпеки
2. Систематично навчайте персонал, люди - це “перший фаєрвол”
3. Розробіть, перевіряйте та оновлюйте політики та процедури інформаційної безпеки регулярно
4. Використовуйте AI для підсилення ваших можливостей кібербезпеки не надаючи доступ до конфіденційних даних
5. Зменшуйте ризики за допомогою впровадження контролів з інформаційної безпеки