

Онлайн-курс

Основи кібербезпеки для бізнесу

Перші кроки та типові інструменти
для побудови системи кіберзахисту



Юрій Самохвалов

Інструктор, методолог та автор курсів, ISSP

Досвід:

- 20+ років в IT
- 17+ років навчання та викладання

Спеціалізація:

- мережева інфраструктура
- інформаційна безпека та кібербезпека
- етичний хакінг
- розслідування комп'ютерних злочинів



LinkedIn: Yuriy Samokhvalov



Київ

Програма

- 1 Побудова системи кіберзахисту
- 2 Безпекові практики МСБ* в Україні
- 3 Впровадження системи моніторингу захисту
- 4 Перевірка системи безпеки
- 5 Практика та наступні кроки

*МСБ – малі та середні бізнеси; група підприємств, які не перевищують визначені показники (наприклад: <250 співробітників)

1 Побудова системи кіберзахисту



80%

світових компаній
обробляють
важливу
інформацію, яка
потребує захисту

Джерело: ENISA (глобальна статистика)

Система кіберзахисту

Система кіберзахисту – це комплексний набір технологій, процедур, політик та практик, призначених для захисту інформаційних систем, комп'ютерних мереж, даних та інших цифрових ресурсів від різноманітних кіберзагроз і кібератак

Мета системи кіберзахисту:

- забезпечення конфіденційності, цілісності та доступності даних
- забезпечення нормальної роботи цифрових інфраструктур



Крок №1 в побудові системи
кіберзахисту – зрозуміти, що
потрібно захистити

Компоненти

Процеси

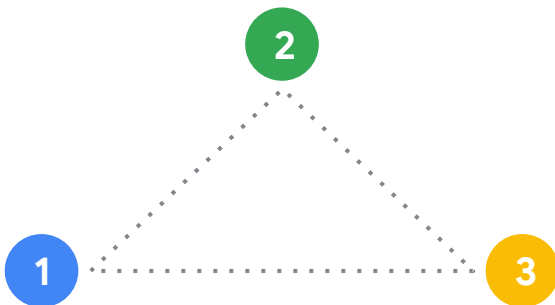
набір послідовних дій, спрямованих на досягнення певної мети або результату

Люди

всі співробітники, від робітників до вищого керівництва

Технології

інструменти, обладнання, програмне забезпечення



План для забезпечення захисту МСБ:

розпізнавання та класифікація важливих активів (дані, інформаційні системи тощо)

визначення потенційних загроз втрати або пошкодження активів

визначення відповідальної команди або відділу за реалізацію стратегії захисту

створення процедур щодо захисту та взаємодії з активами

1 Ідентифікація + класифікація активів

2 Оцінка ризиків

3 Призначення відповідальних осіб

4 Розробка та впровадження політик + процедур

визначає що саме потребує захисту

визначає важливість конкретних ризиків

забезпечує контроль над процесами захисту

допомагає створити основу для внутрішнього контролю та дотримання вимог

План для забезпечення захисту МСБ:

реалізація технічних заходів (встановлення брандмауерів, антивірусного ПЗ*)

організація тренінгів та інформаційних кампаній для співробітників щодо кібербезпеки

регулярне створення резервних копій даних та розробка планів відновлення

встановлення систем моніторингу безпеки для виявлення підозрілої активності

5 Технічні заходи захисту

6 Навчання та підвищення обізнаності співробітників

7 Резервне копіювання та відновлення даних

8 Моніторинг та виявлення інцидентів

допомагає зменшити
технічні ризики

зменшує ризик
внутрішнього порушення безпеки через соціальний інжиніринг

допомагає забезпечити
доступність даних після атак або втрати

допомагає вчасно
виявляти кіберзагрози та реагувати на них

*ПЗ – програмне забезпечення

План для забезпечення захисту МСБ:

регулярне оновлення програмного забезпечення, операційних систем та апаратного забезпечення для закриття вразливостей

регулярне проведення тестів на проникнення та аудитів безпеки для виявлення потенційних слабких місць

звіряння стратегії з результатами, аналіз недоліків і вдосконалення підходів для підвищення рівня захисту

9 Оновлення та патчінг*

10 Тестування та аудит безпеки

11 Неперервне підвищення рівня захисту

*патчінг – це процес оновлення програмного забезпечення, після офіційного сповіщення від вендора

2

Безпекові практики МСБ в Україні

Безпекові практики

Оцінка й управління ризиками*

Проведення аналізу ризиків для визначення потенційних загроз та вразливостей.

Ризик = вірогідність × вплив

Приклад: визначення пріоритетів активів і чітке розуміння ресурсів для захисту найважливіших.

Навчання та підвищення обізнаності

Організація регулярних навчальних сесій для співробітників щодо потенційних загроз та способів їх уникнення.

Приклад: симуляції фішингу* для навчання співробітників розпізнаванню шахрайських атак.

Захист мережі

Використання фаєрволів* та систем виявлення проникнення для захисту мережі від несанкціонованого доступу.

Приклад: встановлення систем моніторингу мереж для виявлення підозрілих активностей.

SIEM системи*

Впровадження системи виявлення і реагування на інциденти (SIEM) для ефективного реагування на зловмисні дії.

Приклад: встановлення систем Splunk, ArcSight, QRadar.

***ризик** – можливість виникнення негативних подій або втрат у результаті кібератак, кіберзагроз чи інших кібернетичних подій

***фішинг** - вид атаки, під час якої зловмисник намагається ввести в оману користувача з метою видобування конфіденційної інформації або інфікування користувачської системи

***фаєрвол** (англ. firewall) - програмний або апаратний засіб для захисту систем та мереж від зловмисних атак

***SIEM** (Security Information and Event Management) - комплексна система управління інформацією та безпековими подіями

Безпекові практики

Тестування на проникнення

Регулярне проведення тестувань на проникнення, допомагає виявити слабкі місця і ризики у системі кіберзахисту.

Приклад: перевірка вебсайту компанії на наявність нових вразливостей

Оцінювання стану безпеки

Регулярне проведення оцінювання надає впевненість в актуальності наявних політик та практик компанії.

Приклад: співробітник звільнився, його функціонал має виконувати інший співробітник – потрібно внести відповідні зміни до внутрішніх політик

Співпраця з експертами

Співпраця із зовнішніми консультантами або фахівцями з кібербезпеки дозволяє підвищити ефективність загальної системи захисту.

Приклад: консультант надасть рекомендації з додаткових налаштувань та продуктів, які можуть покращити моніторингову систему безпеки

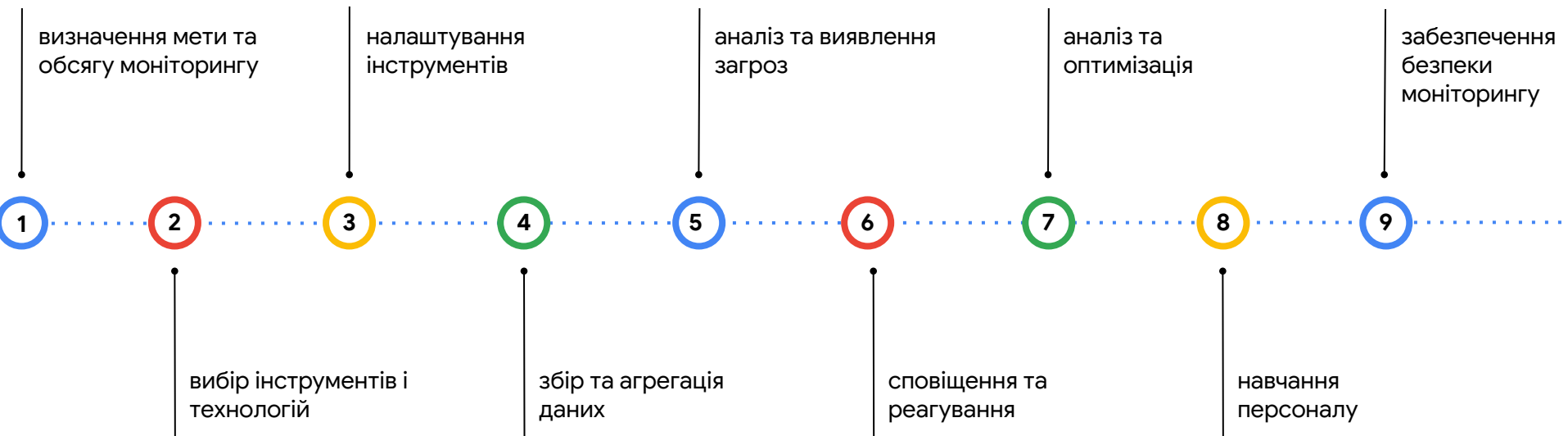
3

Впровадження системи моніторингу захисту

Моніторинг системи захисту – постійний процес



Складові реалізації моніторингу системи захисту



Як реалізувати моніторинг системи захисту?

Процедура варіативна і залежить від потреб організації та її можливостей.

1 Мета та обсяг

- Визначте, що саме ви хочете відстежувати: **події, вразливості, аномалії** тощо
- Встановіть обсяг та ресурси, які ви готові вкласти у моніторинг

2 Інструменти й технології

- Виберіть відповідні **інструменти для збору, агрегації та аналізу даних**
- При потребі виберіть інструменти для моніторингу мережі та серверів

3 Налаштування інструментів

- Встановіть та налаштуйте обрані інструменти відповідно до ваших **потреб та оточення**
- Задайте правила та порогові значення для сповіщень про аномалії чи загрози

Як реалізувати моніторинг системи захисту?

4 Збір та агрегація даних

- Налаштуйте інструменти для збору даних з різних джерел: логи*, сенсори*, мережевий трафік тощо
- Встановіть централізовану систему агрегації* для обробки та зберігання даних.

5 Аналіз та виявлення загроз

- Налаштуйте правила та сценарії аналізу для виявлення аномалій, вразливостей та можливих атак
- Використовуйте аналітичні можливості для визначення незвичайних патернів чи поведінки

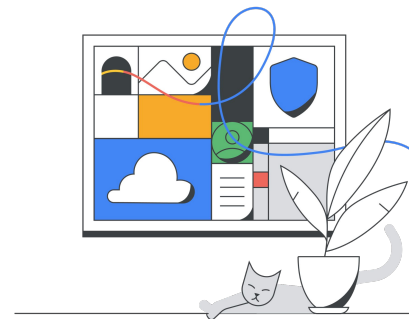
6 Сповіщення та реагування

- Налаштуйте систему сповіщень для інформування адміністраторів про виявлені загрози або аномалії
- Розробіть плани реагування на різні сценарії загроз

*логи – записи про події, які відбуваються в системі, програмі або мережі

*сенсори – компоненти або системи для виявлення та моніторингу подій

*централізована система агрегації – програмне або апаратне рішення, для збирання, обробки і агрегації даних з різних джерел в одному центральному місці для подальшого аналізу, моніторингу та звітування



Як реалізувати моніторинг системи захисту?

7 Аналіз та оптимізація

- Періодично аналізуйте ефективність моніторингу та аналізуйте зібрані дані для виявлення трендів та слабких місць
- Вносьте зміни у правила, порогові значення та конфігурацію інструментів для покращення результатів

8 Навчання персоналу

- Навчіть адміністраторів та безпековий персонал працювати з обраними інструментами та ефективно реагувати на сповіщення

9 Забезпечення безпеки моніторингу

- Захистіть систему моніторингу від несанкціонованого доступу, бо це може бути цільовою точкою для атак

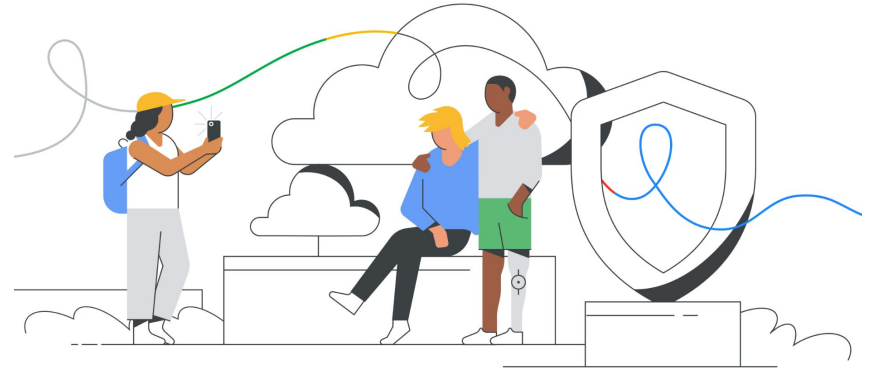


Хто бере участь у процесі моніторингу?

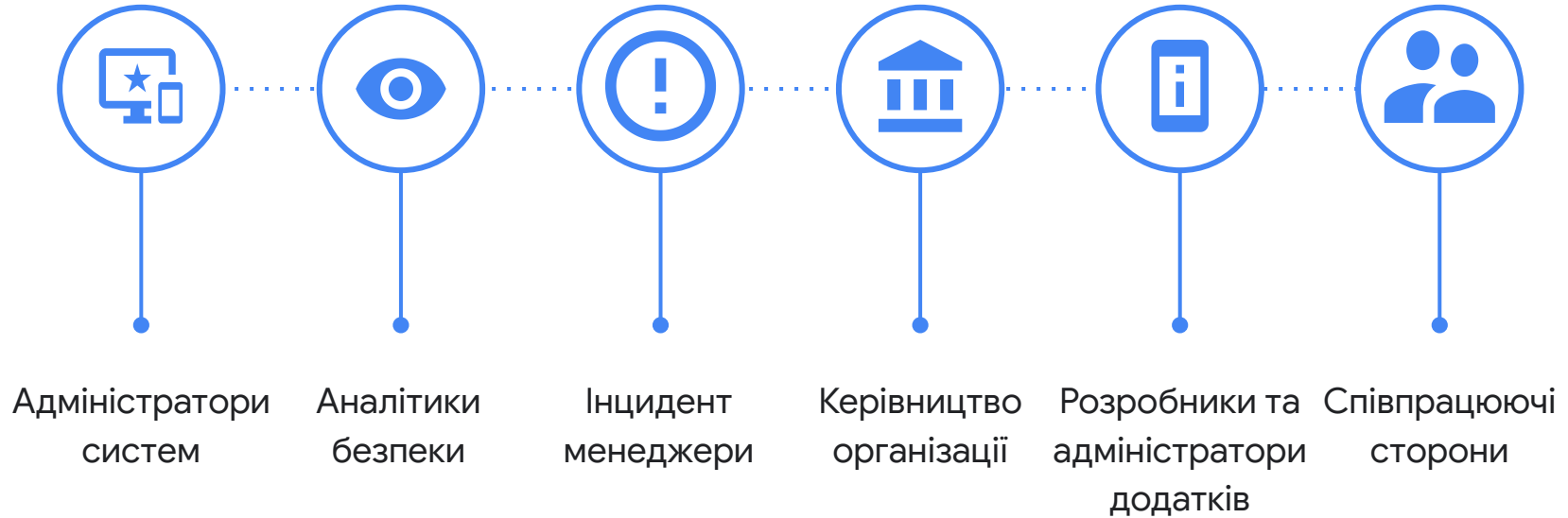
Моніторинг системи безпеки - це **спільний процес**, в якому беруть участь декілька співробітників і відділів компанії, з чітким розподілом ролей.

Склад команди залежить від:

- Розміру й складності організації
- Обсягу й складності моніторингу



Ключові учасники команди



Завдання інструментів моніторингу системи захисту



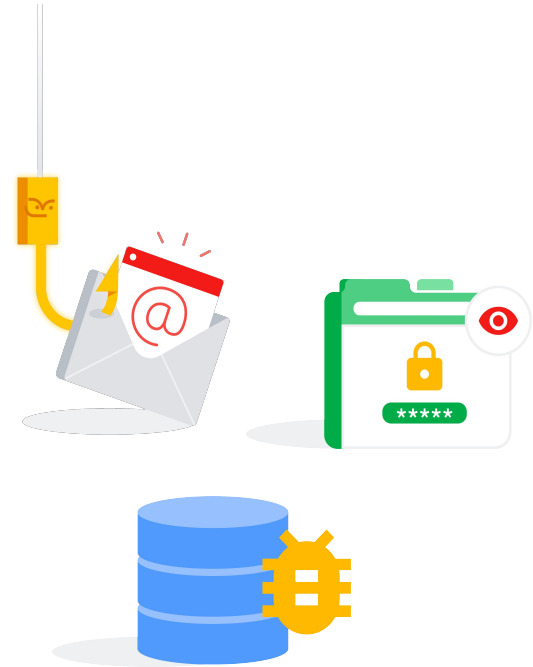
Виявлення вразливостей



Виявлення аномалій

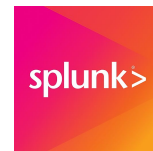


Виявлення загроз



Інструменти моніторингу системи захисту

- SIEM (Security Information and Event Management) – системи управління інформаційною безпекою



- IDS/IPS (Intrusion Detection/Prevention Systems) – системи детектування та запобігання проникненню



- DLP (Data Leak Prevention) – системи запобігання витоку даних



Інструменти моніторингу системи захисту

- Системи аналізу логів



- Мережеві аналізатори



- WAF (Web Application Firewall) - вебфаєрволи



Інструменти моніторингу системи захисту

- Vulnerability Scanners - сканери вразливостей
- UEBA (User and Entity Behavior Analytics) - аналізатори поведінки користувачів та сутностей



Бізнесам необхідно мати
комплексну стратегію
моніторингу, яка враховує
потреби компанії, її розмір,
галузь та наявні ресурси

Приклади рішень

Малий бізнес (наприклад, магазин малої роздрібної торгівлі) 

Системи виявлення вторгнень (IDS) і мережевий моніторинг: встановлення базових IDS, які виявляють аномалії в мережевому трафіку та сповіщають про них.

Антивіруси: використання антивірусів на кожному комп'ютері та регулярне оновлення вірусних баз даних.

Систематичне оновлення програмного забезпечення: використовуйте сервіси, щоб відстежувати доступність вебсайту та виявляти атаки DDoS.

Середній бізнес (наприклад, інтернет-магазин) 

SIEM-система: впровадження централізованої системи моніторингу та аналізу подій для збору та обробки даних безпеки.

Управління доступом і аутентифікація: використання двофакторної аутентифікації та ролей для обмеження доступу до важливих ресурсів.

Регулярні внутрішні та зовнішні оцінювання безпеки: проведення аудитів для виявлення вразливостей та слабких місць.

4 Перевірка системи безпеки

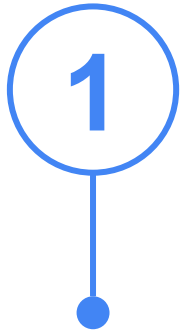
Чи потрібна перевірка системи кібербезпеки?

Перевірка системи кіберзахисту необхідна щоб:

- Виявляти вразливості
- Аналізувати аномалії
- Підтримувати стандарти відповідності
- Захищатись від атак
- Покращувати рівень кібербезпеки
- Мінімізувати існуючі ризики
- Оцінювати адекватність безпекових заходів
- Покращувати реагування на інциденти



Ключові фактори для вибору методу перевірки



Цілі та обсяг
перевірки



Тип системи та
інфраструктури



Обсяг
ресурсів



Вимоги
відповідності



Часові
обмеження

Вибір методу перевірки

Аудит кібербезпеки

Аудит - це всебічний перегляд системи кібербезпеки, щоб переконатися, що вона дотримується встановлених міжнародних або локальних стандартів та політик.

Перевага – цілісний підхід до оцінки кібербезпеки з організаційного боку

Оцінка вразливостей

Оцінка вразливостей – це технічний аналіз і виявлення слабких місць в інформаційних системах та інфраструктурі компанії.

Факт – може бути виконана автоматизованими засобами або вручну експертами

Тестування на проникнення

Тестування на проникнення (пентест) - це активне випробування системи на наявність вразливостей та спробу проникнення зломисників.

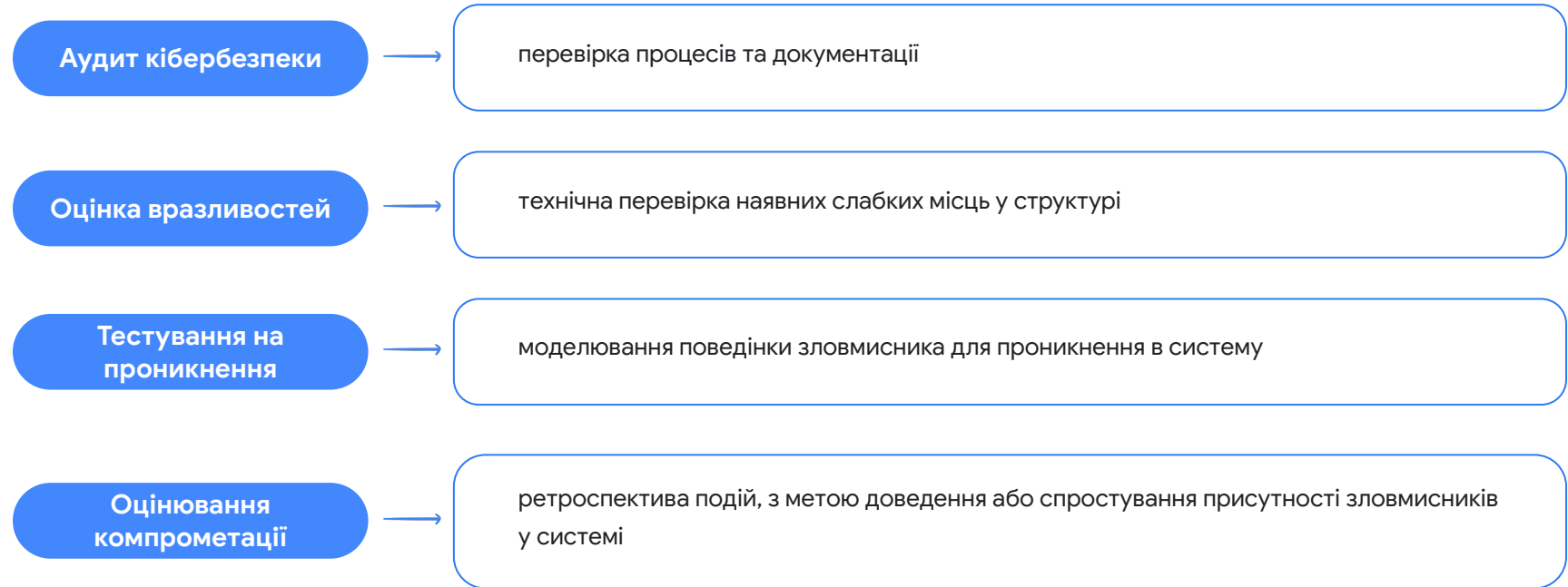
Перевага – може надати більш реалістичне уявлення про реальні ризики та наслідки атаки

Оцінювання компрометації

Оцінювання компрометації - це технічне дослідження цільової структури, яке дозволяє виявляти підозрілі або незвичні активності та можливу наявність чи потенційну можливість проникнення.

Факт – допомагає вчасно виявляти й аналізувати можливі порушення та атаки

Вибір методу перевірки



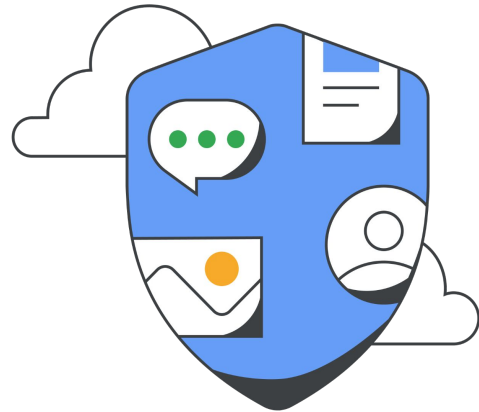
Аудит кібербезпеки –
періодичність і реальна цінність

Як часто проводити аудит?

Регулярно: Безпековий аудит повинен проводитися регулярно, оскільки загрози та вразливості змінюються з часом.

Виходячи з загроз: Якщо ви опинились під загрозою або відбулися зміни в інфраструктурі, може бути доцільним провести аудит негайно для визначення потенційних проблем.

Після інцидентів: Після кіберінциденту, навіть якщо він був не критичним, важливо провести аудит для виявлення недоліків та можливих слабких місць у захисті



Реальна цінність аудиту кібербезпеки



Потреби Вашої компанії та
вимоги галузі є основою для
вибору періодичності та
формату аудиту

Оцінювання вразливостей чи
тестування на проникнення, що
обрати?

Особливості

Оцінювання вразливостей

- ✓ **Сканування та аналіз:** полягає в ідентифікації та аналізі можливих вразливостей, шляхом сканування системи або мережі
- ✓ **Фокус на вразливостях:** акцент на виявленні вразливостей та вирішенні їх, а не на симуляції атаки
- ✓ **Менше ризиків для продуктивності:** оцінка вразливостей не включає активних атак

Тест на проникнення (пентест)

- ✓ **Активне тестування:** активна та реалістична атака на систему або мережу з метою виявлення вразливостей та інших слабких місць
- ✓ **Симуляція атаки:** використовуються техніки, схожі на ті, які можуть використовувати зловмисники
- ✓ **Виявлення вразливостей і експлойтів*:** пентест може виявити вразливості та використати їх для демонстрації можливих наслідків.

*експлойти – це програмний код або техніка, яка використовується зловмисниками для виконання різних типів атак або отримання несанкціонованого доступу до системи чи даних.

Підготовка до пентесту

Крок 1: Визначте, **що саме** ви хочете **перевірити** та обговоріть, які **види атак** дозволені, а які ні

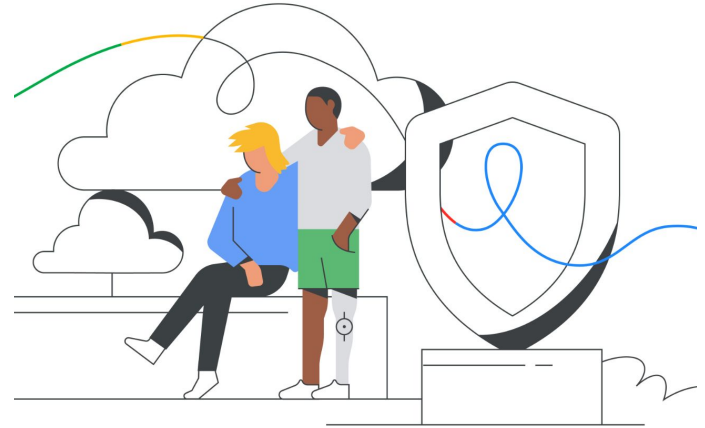
Приклад: вебдодаток, мережа, програмне забезпечення, сервери тощо



Підготовка до пентесту

Крок 2: Вибір команди

Знайдіть **внутрішніх фахівців** або **зовнішніх спеціалістів** з відповідним досвідом та знаннями в області **кібербезпеки**, які проводитимуть пентест



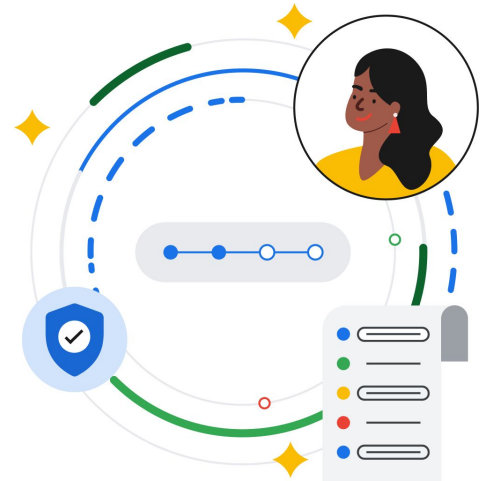
Підготовка до пентесту

Крок 3: Узгодження плану та методології

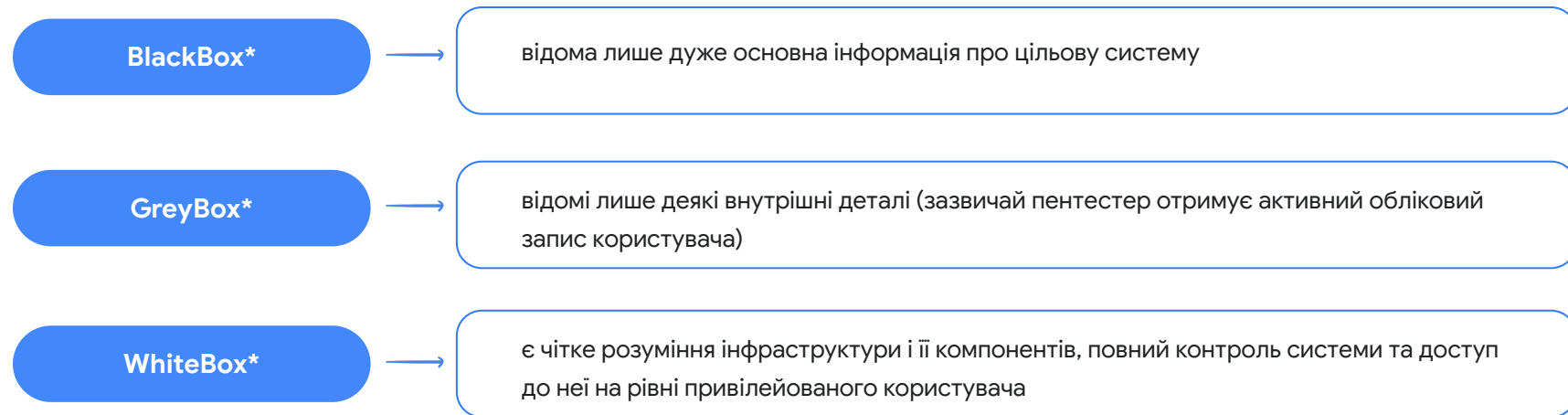
Команда тестування повинна узгодити із замовником план перевірки, який буде включати різні типи тестів та методологію

Приклади тестів: сканування портів, виявлення вразливостей, тестування аутентифікації тощо

Приклад методології: OWASP Testing Guide або NIST SP 800-115



Визначення типу пентесту



***BlackBox** – чорний ящик.

***GreyBox** – сірий ящик.

***WhiteBox** – білий ящик.

Виконання пентесту

1. Збір інформації

Використовуються публічно доступні інструменти для збору інформації про цільову систему

2. Аналіз вразливостей

Використовуються не тільки автоматизовані інструменти, але й ручний аналіз для виявлення вразливостей

3. Експлуатація вразливостей

Використовуються знайдені вразливості для здійснення атак і отримання доступу до системи

4. Тестування аутентифікації та авторизації

Перевіряється можливість обходу механізмів автентифікації та отримання несанкціонованого доступу

Результати пентесту

1

Оцінка наслідків атак

Визначте, які можливі наслідки атак для вашої організації.

Якщо атака була успішною, які дані можуть бути скомпрометовані або які системи можуть бути пошкоджені

2

Отримання звіту

Після завершення тестування створюється детальний звіт, з описом знайдених вразливостей, проведених атак і їх результатів, а також рекомендації з їх виправлення

3

Подальші дії

Після отримання результатів пентесту, важливо вжити заходів для виправлення знайдених вразливостей та покращення кібербезпеки

Що обрати?

Вибір залежить від потреб і спроможностей організації:

- Оцінка вразливостей – для **ідентифікації** та **мінімізації** або **усунення** вразливостей
- Пентест – для **оцінки витривалості** всієї системи або її складової (наприклад, мережі) до реальної атаки



Оцінювання компрометації
інфраструктури – перевірка чи
не пропустили ми хакера
всередину

Оцінювання компрометації інфраструктури

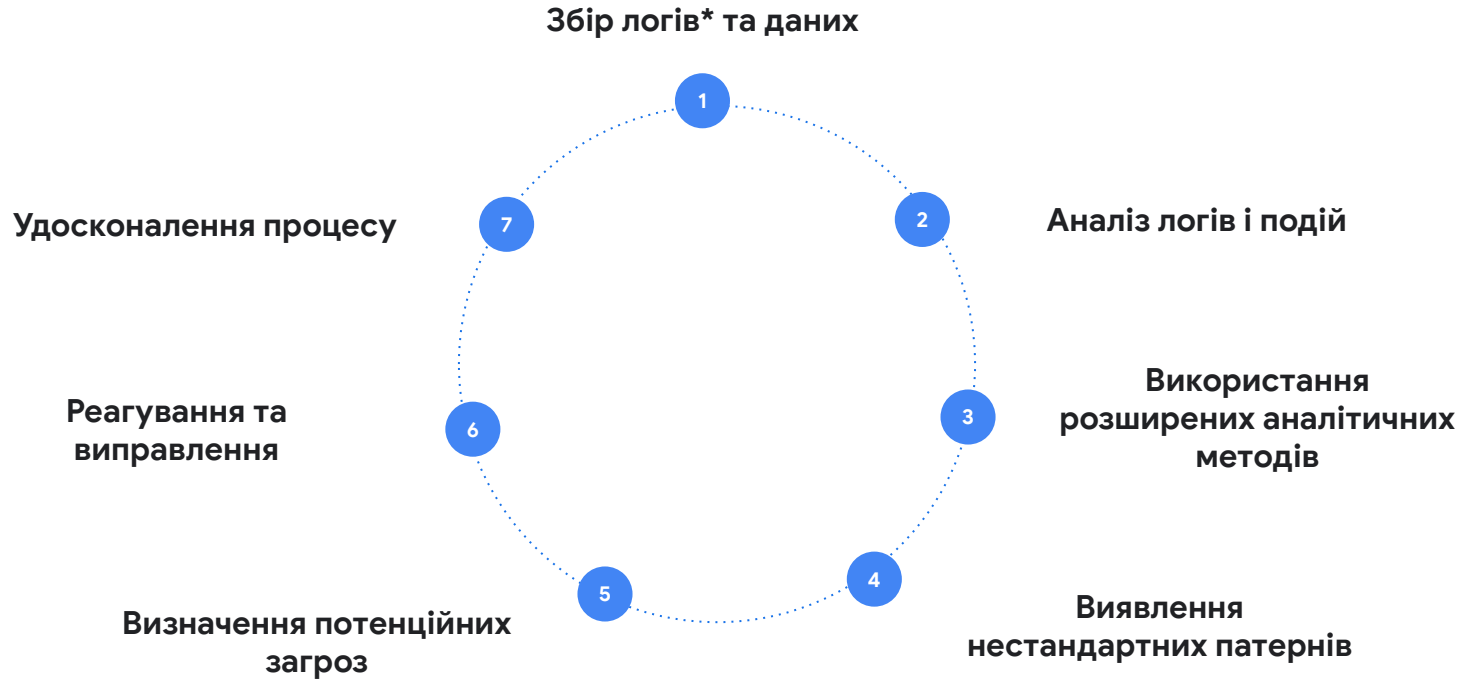
Оцінювання компрометації інфраструктури (англ. Compromise Assessment) – практика в кібербезпеці для виявлення присутності в інфраструктурі зломисників після того, як атака або компрометація могла відбутися

Перевіряє чи вдалося атакуючому:

- проникнути в систему чи
- він вже знаходиться всередині

**Аналіз
компрометації
має бути
постійним
процесом**

Основні етапи аналізу компрометації інфраструктури включають:



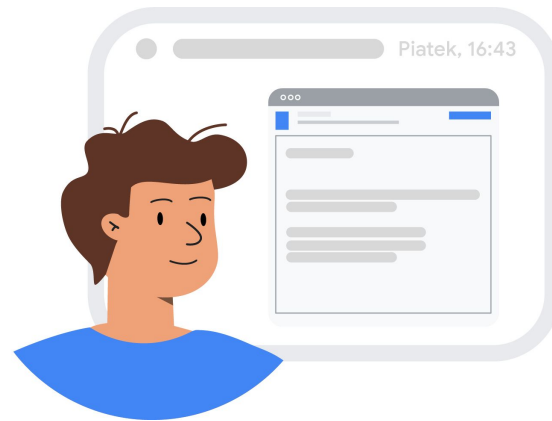
*логи - записи про події, які відбуваються в системі, програмі або мережі

5 Закріплюємо вивчене: Практика та наступні кроки

Практичне завдання: кейс

Ситуація:

- Ви - власник середнього бізнесу і додатково **запускаєте власний вебсайт** для більшого охоплення клієнтської бази
- Згодом, клієнти, які зареєстровані на сайті, звертаються з повідомленнями про **спам-розсилку** на їхні адреси, після процесу реєстрації на вашому сайті



Питання: Які безпекові моменти потрібно врахувати?



Головні кроки для побудови системи кіберзахисту

- Проведення критичного аналізу наявних активів (людей, процесів, технологій)
- Розробка політик кіберзахисту
- Побудова або адаптація інфраструктури з урахуванням безпекових критеріїв
- Систематичне навчання персоналу
- Вибір та проведення перевірок систем безпеки (як окремо, так і в комплексі)



Практичні питання на самостійне опрацювання



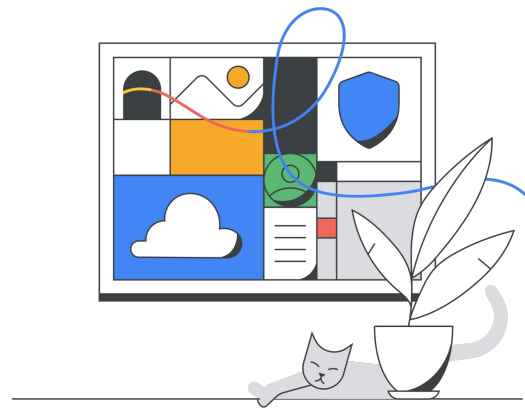
Завдання: Створіть власний **рейтинг пріоритетів активів компанії** залежно від особливостей вашої справи



Перевірка: Яку небезпеку можуть мати для компанії її загальнодоступні електронні ресурси?

Наступні кроки

- Заплануйте регулярні зустрічі з CISO* та представниками його команди
- Тримайте руку на пульсі подій безпекової команди шляхом звітів (не частіше 1 разу в місяць)
- Порадьтеся та визначте план подальших дій для підсилення поточного стану безпеки компанії



*CISO (англ. Chief Information Security Officer) – директор з інформаційної безпеки

Дякую за увагу!