План лекції . Тема 8. Застосування моніторингу для виявлення загроз безпеці.

- Застосування моніторингу для виявлення загроз безпеці.
- Використання системного та мережевого моніторингу для виявлення вторгнень, зламів та інших загроз безпеці.
- Аналіз логів, виявлення аномалій та паттернів, пов'язаних із зловмисними діями.
- Розробка стратегій реагування та відновлення після виявлення загроз.
- Компроміси безпеки

Вступ.

Сьогодні ми з вами поговоримо про те, як моніторинг може допомогти нам виявляти загрози безпеці.
У сучасному світі кібербезпека є однією з найважливіших проблем для будь-якої організації. Кіберзлочинці постійно вдосконалюють свої методи, і традиційних методів захисту вже недостатньо. Моніторинг - це потужний інструмент, який може допомогти:

- **Виявити загрози на ранній стадії**, перш ніж вони завдадуть шкоди інформаційній системі.
- **Швидко відреагувати на інциденти**, швидко визначити масштаби інциденту та вжити заходів для його усунення.
- **Запобігти майбутнім атакам** шляхом виявлення вразливостей у інформаційній системі та вжити заходів для їх усунення.

У цій лекції ми обговоримо такі теми:

- Різні типи моніторингу, які можна використовувати для виявлення загроз безпеці.
- Як візуалізація даних моніторингу може допомогти вам краще їх зрозуміти.
- Як використовувати системний та мережевий моніторинг для виявлення вторгнень, зломів та інших загроз безпеці.
- Як аналізувати журнали, щоб виявити аномалії та паттерни, пов'язані з зловмисними діями.
- Як розробити стратегії реагування та відновлення після виявлення загроз.

Застосування моніторингу для виявлення загроз безпеці.

Що ж таке моніторинг для виявлення загроз? Коли мова заходить про застосування моніторингу для виявлення загроз безпеці, мови про розділення типів моніторингу не може бути, бо для цієї благородної цілі застосовуються всі допустимі типи моніторингу, крім заборонених законом ☺
Моніторинг – це, по суті, процес отримання інформації про події, які вже відбулися. Таким чином, коли ми говоримо про застосування моніторингу для виявлення загроз безпеці потрібно розуміти, що доводити можливі загрози безпеці до здійснення не потрібно. Потрібно передбачити за результатами моніторингу ці загрози чи навіть їх можливість.

Моніторинг безпеки – це практика збору інформації на різних рівнях робочого навантаження (інфраструктура, програми, операції) для отримання інформації про підозрілу діяльність . Мета полягає в тому, щоб передбачити інциденти та вивчити минулі події. Дані моніторингу є основою для аналізу того, що сталося після інциденту, щоб допомогти реагувати на інциденти та провести розслідування.

- **Ключові стратегії дизайну моніторингу безпеки.**
  Основною метою моніторингу безпеки є виявлення загроз . Необхідно запобігти потенційним порушенням безпеки та підтримувати безпечне середовище. Однак не менш важливо визнати, що не всі загрози можливо запобіжно заблокувати. У таких випадках моніторинг також слугує механізмом для визначення причини інциденту безпеки, який стався, незважаючи на зусилля із запобігання.
  До моніторингу необхідно підходити з різних точок зору:

  - ✓ **Моніторинг на різних рівнях.** Спостереження з різних рівнів — це процес отримання інформації про
    - потоки користувачів: як користувачі взаємодіють з додатком, веб-сайтом, хостом. Може включати дані про те, які сторінки вони відвідують, на які кнопки натискають, скільки часу вони проводять на кожній сторінці тощо.
    - доступ до даних: отримання доступу до даних. Може включати дані про те,
      - які користувачі отримують доступ до яких даних,
      - коли вони отримують доступ до даних і
      - як вони отримують доступ до даних (наприклад, через веб-інтерфейс або API).
    - ідентичність: співставлення користувача з конкретною людиною або службово-функціональним обліковим записом. Може включати дані про те,
      - як користувачі аутентифікуються у системі,
      - які у них ролі та дозволи, а також
      - їхню контактну інформацію.
    - мережу: як працює мережа. Може включати дані про те,
      - які пристрої підключені до мережі,
      - який трафік проходить через мережу та
      - як мережа використовується.
    - операційну систему: робота операційних систем всіх рівнів. Може включати дані про те,
      - які процеси запущені,
      - які ресурси використовуються та
      - які помилки виникають.

    Це лише кілька базових прикладів, що моніториться на різних рівнях. Іншими словами – моніторинг на різних рівнях це - процес збору даних про різні аспекти середовища Кожна зі згаданих областей пропонує унікальну інформацію, яка може допомогти визначити відхилення від очікуваної поведінки, встановленої порівняно з базовим рівнем безпеки. І навпаки, безперервний моніторинг системи та додатків протягом тривалого часу може допомогти встановити цю базову позицію. Наприклад, спостерігається близько 1000 спроб входу у систему ідентифікації щогодини. Якщо Ваш моніторинг виявляє сплеск 50 000 спроб входу протягом короткого періоду, можливо, зловмисник намагається отримати доступ до системи і цей сплеск активності - прояви спроби злому.

  - ✓ **Моніторинг при різних масштабах впливу.** Припустімо, що користувач випадково отримав підвищені привілеї, або сталося порушення безпеки. Якщо користувач виконує дії, що виходять за межі його визначеної сфери, вплив може обмежуватися діями, які можуть виконувати інші користувачі.

Однак, якщо будь яка внутрішня сутність (користувач чи криво написаний тригер) скомпрометує базу даних, ступінь потенційної шкоди залишається невизначеним. Якщо компрометація виникає на стороні ресурсу ядра системи (наприклад MS AD чи AWS AD), вплив може бути глобальним і розповсюдиться на всі сутності, які взаємодіють із ресурсом. Радіус заподіяної компроментацією шкоди, або масштаб удару можуть значно відрізнятися залежно від того, який із сценаріїв має місце.

Додаткові поради:

- Використовуйте принцип найменших привілеїв, щоб надати користувачам лише ті права, які їм дійсно потрібні.
- Регулярно проводьте аудит безпеки для виявлення та усунення вразливостей.
- Впровадьте систему раннього виявлення та реагування на інциденти (EDR).

Визначення різних масштабів впливу:

- **Локальний:** Вплив обмежується одним компонентом, модулем або підсистемою. Наприклад - несанкціонований доступ до однієї таблиці в базі даних.
- **Регіональний:** поширюється на кілька компонентів, модулів або підсистем, але не на всю систему. Приклад: несанкціонований доступ до одного сервера в кластері.
- **Глобальний:** поширюється на всю систему або на кілька систем. Приклад: несанкціонований доступ до центральної бази даних або доменного контролера.
- **Катастрофічний:** призводить до повної або часткової втрати працездатності системи, що може мати значні фінансові та репутаційні наслідки. Приклад: шифрування даних зловмисним програмним забезпеченням.
- **Невизначений:** у даний момент неможливо визначити масштаб впливу. Приклад: початкова фаза розслідування інциденту кібербезпеки.

Важливо зазначити, що масштаб впливу може змінюватися з часом. Наприклад, локальний інцидент може перерости в регіональний або глобальний, якщо його не буде вчасно виявлено та усунено.

- ✓ **Використання спеціалізованих засобів моніторингу.** Дуже важливо налаштувати та підтримувати у «бойовому стані» спеціалізовані інструменти, що постійно сканують аномальну поведінку, яка може свідчити про атаку. Більшість із цих інструментів мають можливості аналізу загроз, які можуть виконувати прогнозний аналіз на основі великого обсягу даних і відомих загроз. Інструменти моніторингу зазвичай не обмежуються простим збором даних, а також мають глибоке розуміння того, що ці дані означають з точки зору безпеки. Вони можуть виявляти аномалії, аналізувати загрози та навіть робити прогнози на основі цих даних.
  Інструменти мають бути інтегровані в платформу або принаймні відповідати платформі, щоб отримувати глибокі сигнали від платформи та робити прогнози з високою точністю. Вони повинні мати можливість своєчасно генерувати сповіщення з достатньою інформацією для проведення належного сортування. І навпаки, використання занадто великої кількості різноманітних інструментів може призвести до ускладнень та перевантаження мережі.

- ✓ **Використання моніторингу для реагування на інциденти.** Зведені та нормалізовані дані, перетворені на оперативну розвідку, дозволяють швидко й ефективно реагувати на інциденти. Моніторинг також допомагає діяти після інциденту. Мета — зібрати достатньо даних, щоб проаналізувати та зрозуміти, що сталося. Процес моніторингу фіксує інформацію про минулі події, щоб покращити можливості реагування та потенційно передбачити майбутні інциденти.

- ➢ **Збирання та зберігання даних, щоб відслідковувати діяльність.**

Мета полягає в тому, щоб підтримувати повний контрольний слід подій, важливих з точки зору безпеки. Логування є найпоширенішим способом фіксації шаблонів доступу. Реєстрацію потрібно виконувати для програми, платформи з прив'язкою до конкретного хосту чи ресурсу.
Для контрольного сліду необхідно встановити, *коли та хто пов'язаний з певними діями*. Необхідно визначити конкретні терміни виконання дій. Зробіть цю оцінку у своєму моделюванні загроз. Щоб протистояти загрозі відмови, слід створити надійні системи журналювання та аудиту, які призведуть до запису дій і транзакцій.

- ✓ **Потоки користувача програми.** Кожна критична з безпекової точки програма (додаток) має бути розроблена так, щоб забезпечити видимість під час важливих чи критичних подій. Визначте критичні точки у програмі та створіть журнал для цих точок. Наприклад, коли користувач входить у програму, зафіксуйте особу користувача, джерело розташування та іншу відповідну інформацію. Важливо підтверджувати будь-яке підвищення привілеїв користувача, дії, які виконує користувач, і чи отримував користувач доступ до конфіденційної інформації в безпечному сховищі даних. Відстежуйте дії користувача та сеанс користувача.
  Щоб полегшити це відстеження, логування виконується за допомогою *структурованого журналювання*. Це дає змогу легко стандартизовано виконувати запити та фільтрувати журнали.

Потрібно забезпечити відповідальне ведення журналу, щоб зберегти конфіденційність і цілісність інформаційної системи. Секрети та конфіденційні дані не повинні відображатися в журналах. Пам'ятайте про витік особистих даних та інші вимоги відповідності, коли збираєте дані журналу.

- ✓ **Моніторинг ідентифікації та доступу.** Ведіть ретельний облік шаблонів доступу до програм та змін до ресурсів платформи. Майте надійні журнали активності та механізми виявлення загроз, особливо для дій, пов'язаних із ідентифікацією, оскільки зловмисники часто намагаються маніпулювати ідентифікацією, щоб отримати неавторизований доступ.
  Реалізуйте комплексне журналювання, використовуючи всі доступні точки даних. Наприклад, додайте IP-адресу клієнта, щоб відрізнити звичайну активність користувача від потенційних загроз із неочікуваних місць. Усі події журналювання повинні бути позначені часом з надійного серверу часу, а не часом користувача.
  Фіксуйте всі дії з доступом до ресурсів: хто що і коли робить з ресурсами. Випадки підвищення привілеїв є важливою точкою даних, яку слід реєструвати. Дії, пов'язані зі створенням або видаленням облікового запису, також повинні бути зафіксовані. Ця рекомендація поширюється на паролі, логіни, сертифікати, підписи. Слідкуйте за тим, хто має доступ до секретів і коли вони змінюються. Доступ до паролів, логінів, сертифікатів та підписів користувача має бути лише у цього користувача.
  Хоча протоколювання успішних дій є важливим, записування помилок також необхідне з точки зору безпеки. Документуйте будь-які порушення:
  - користувач, який намагається виконати дію, але зіткнувся з помилкою авторизації
  - спроби доступу до неіснуючих ресурсів
  - будь які інші дії, які здаються підозрілими.

SNM. #3. Інструменти моніторингу та аналізу даних ***

Системний *та мережевий моніторинг. Лекція #8. Застосування моніторингу для виявлення загроз безпеці.*

- ✓ **Моніторинг мережі.** Відстежуючи мережеві пакети та потоки, їх джерела, призначення та структури, отримуємо видимість шаблонів доступу на рівні мережі. Дизайн сегментації мережі має дозволяти точки спостереження на межі кожної мережі. Простіше це пояснюється так:

  Уявіть, що ваша мережа - це велика дорога.
  - Мережеві пакети та потоки - це як автомобілі, що їздять по ній.
  - Джерела - це місця, звідки виїжджають автомобілі.
  - Призначення - це місця, куди їдуть автомобілі.
  - Структури - це маршрути, якими їдуть автомобілі.

  Моніторинг мережі - це як спостереження за цією дорогою.

  Ви хочете знати:
  - Хто їздить по цій дорозі (які джерела та призначення)?
  - Куди вони їдуть (які маршрути)?
  - Як часто вони їздять (які шаблони доступу)?

  Для цього ви можете:
  - Встановити камери на кордонах (точки спостереження).
  - Записувати все, що їде через кордони (реєструвати дані).
  - Аналізувати записи, щоб бачити, що відбувається.

  Наприклад:
  - Ви можете відстежувати підмережі (групи автомобілів)
  - Ви можете відстежувати журнали брандмауера (записи про те, кому дозволено або заборонено їздити)

  Це допоможе вам:
  - Виявити підозрілу активність (наприклад, несанкціонований доступ)
  - Вирішити проблеми з мережею (наприклад, затори)
  - Забезпечити безпеку вашої мережі (наприклад, запобігти аваріям)

  Чим краще ви моніторите свою мережу, тим краще ви можете її захистити.

  Існують журнали доступу для вхідних запитів на підключення. У цих журналах записуються IP-адреси джерела, які ініціюють запити, тип запиту (GET, POST) та вся інша інформація, яка є частиною запитів.

  Захоплення потоків DNS є важливою вимогою для багатьох організацій. Наприклад, *журнали DNS можуть допомогти визначити, який користувач або пристрій ініціював певний запит DNS*. Співвідносячи діяльність DNS із журналами автентифікації користувача/пристрою, можливо відстежувати дії окремих клієнтів. Ця відповідальність часто поширюється на робочу групу, особливо якщо вони розгортають щось, що робить запити DNS частиною їхньої роботи. Аналіз трафіку DNS є ключовим аспектом безпеки платформи.

  Важливо відстежувати неочікувані DNS-запити або DNS-запити, спрямовані на відомі командні та контрольні кінцеві точки.

  Компроміс: реєстрація всіх мережевих дій може призвести до великого обсягу даних. Кожен запит із рівня 3 можна записати в журнал потоків, включаючи кожну транзакцію, яка перетинає межу підмережі. На жаль, неможливо зафіксувати лише несприятливі події, оскільки їх можна ідентифікувати лише після їх виникнення.

  Приймайте стратегічні рішення щодо типу подій, які потрібно зафіксувати, і тривалості їх зберігання. Якщо ви не будете обережні, керування даними може виявитися непосильним. Існує також компроміс щодо вартості зберігання цих даних.

  Зважаючи на компроміси, слід розглянути, чи вигода від мережевого моніторингу робочого навантаження є достатньою для виправдання витрат. Якщо у вас експлуатуються рішення з великим обсягом запитів і ваша система широко використовує керовані хмарні ресурси, вартість може переважити переваги. З іншого боку, якщо у вас є рішення, розроблене для використання віртуальних машин із різними портами та програмами, може бути важливо збирати та аналізувати журнали мережі.

- ➢ **Фіксація змін системи.**

  Щоб підтримувати цілісність системи, необхідно мати точний і актуальний запис про стан системи. Якщо є зміни, цей запис може бути використаний для оперативного вирішення будь-яких проблем, що виникли.

  Процеси сканування мережі також повинні видавати телеметрію. Ключовим є розуміння контексту безпеки подій. Знання того, що ініціювало процес сканування, хто його ініціював і коли він був ініційований, може дати цінну інформацію.

  Відстежуйте, *коли ресурси створюються та коли вони виводяться з експлуатації*. Ця інформація надає цінну інформацію для управління ресурсами та підзвітності.

  Також *необхідно моніторити переміщення (дрейф) ресурсів*. Документуйте будь-які зміни в існуючому ресурсі. Також слідкуйте за змінами, які не завершуються в рамках розгортання на парку ресурсів. Журнали мають фіксувати деталі зміни та точний час, коли вони відбулися.

  Отримайте всебічне уявлення, з точки зору виправлення, про те, чи є система актуальною та безпечною. Відстежуйте регулярні процеси оновлення, щоб переконатися, що вони завершуються за планом. Процес апдейту безпеки, який не завершується, слід вважати вразливістю. Також слід вести інвентаризацію, у якій записуються рівні виправлень та будь-які інші необхідні деталі.

  Виявлення змін також стосується операційної системи. Це передбачає відстеження того, додаються чи вимикаються служби. Він також включає моніторинг додавання нових користувачів до системи. Існують інструменти, призначені для націлювання на операційну систему. Вони допомагають у безконтекстному моніторингу в тому сенсі, що вони не націлені на функціональність робочого навантаження. Наприклад, моніторинг цілісності файлів є критично важливим інструментом, який дозволяє відстежувати зміни в системних файлах.

  Слід налаштувати сповіщення про ці зміни, особливо якщо ви не очікуєте, що вони відбуватимуться часто.

  Коли ви розгортаєте робочу версію елементу інформаційної мережі, переконайтеся, що сповіщення налаштовано для виявлення аномальної активності. А аномальну активність важливо передбачити у процесі тестування елементу мережі.

  Включіть перевірку журналювання та попередження як пріоритетні тестові випадки у плани тестування. Гарна практика – мати полігон інформаційної мережі. Хай навіть «іграшковий», але він повинен бути. Тим більше, що знайти ресурси для кількох віртуальних, або хмарних серверів не так вже і важко, маючи під адмініструванням продакт інформаційної мережі.

- ➢ **Збереження, агрегація та аналіз даних**

  Дані, які збираються під час моніторингу, повинні бути збережені в безпечних, надійних та доступних системах зберігання.

Дані повинні бути оброблені таким чином, щоб їх можна було *коректно ідентифікувати та порівнювати між собою*. Це включає *нормалізацію* (перетворення даних у стандартизований формат) та *кореляцію* (встановлення зв'язків між різними наборами даних) для отримання повної картини подій.

Дані, пов'язані з безпекою, повинні бути збережені в окремих сховищах даних, щоб уникнути можливості впливу на їх цілісність або зміну зловмисниками.

Сховища моніторингу, які отримують та обробляють ці дані, повинні існувати довше за джерела даних, щоб забезпечити постійність процесу моніторингу.

Системи зберігання даних повинні бути стійкими та надійними, щоб забезпечити неперервну роботу систем виявлення вторгнень.

Мережеві журнали можуть бути докладними та займати дуже великі об'єми. Впровадьте різні рівні систем зберігання. З часом дані переносяться до так званого холодного зберігання (повільні дискові сховища або інші, дешевші носії). Цей підхід є вигідним, оскільки старіші журнали потоку зазвичай не використовуються активно і потрібні лише на вимогу. Цей метод забезпечує ефективне керування сховищами, а також забезпечує доступ до історичних даних, коли вам це потрібно.

Потоки робочого навантаження зазвичай складаються з кількох джерел журналювання. Дані моніторингу необхідно ретельно аналізувати з усіх цих джерел. Наприклад, брандмауер блокуватиме лише трафік, який досягає його. Якщо у вас є група безпеки мережі, яка вже заблокувала певний трафік, цей трафік невидимий для брандмауера. Щоб реконструювати послідовність подій, потрібно агрегувати дані з усіх компонентів, які перебувають у потоці, а потім агрегувати дані з усіх потоків. Ці дані особливо корисні в сценарії реагування після інциденту, коли потрібно зрозуміти, що сталося. Дуже важливий точний відлік часу. З міркувань безпеки всі системи мають використовувати єдине мережеве джерело часу, щоб вони завжди були синхронізовані.

- ✓ **Централізоване виявлення загроз із корельованими журналами.** Гарна практика, використання Security information and event management (SIEM), щоб консолідувати дані безпеки в центральному сховищі – базі даних, де їх можна корелювати між різними службами. Ці системи мають вбудовані механізми виявлення загроз. Вони можуть підключатися до зовнішніх каналів для отримання даних розвідки про загрози. Microsoft Defender Threat Intelligence, наприклад, публікує дані аналізу загроз, які можуть бути використані. Також можливо придбати канали аналізу загроз від інших постачальників, як-от Anomali ThreatStream та FireEye Helix. Ці канали можуть надати цінну інформацію та підвищити вашу безпеку.

  Крім SIEM ще деякі класи спеціалізованих систем з розвідки загроз та моніторингу, призначені саме для агрегації, аналізу та використання інформації з таких джерел.
  - Threat Intelligence Platforms
  - EDR (Endpoint Detection and Response).
  - Firewalls та IDS/IPS (Intrusion Detection/Prevention Systems)
  - SOAR (Security Orchestration, Automation, and Response)

  Система SIEM може генерувати сповіщення на основі корельованих і нормалізованих даних. Ці сповіщення є значним ресурсом під час процесу реагування на інциденти.

  Компроміс: системи SIEM можуть бути дорогими, складними та вимагати спеціальних навичок. Однак, якщо у вас відсутні такі навички, потрібно буде обробляти та аналізувати дані SIEM самостійно. Це може бути трудомістким і складним процесом.

  Системами SIEM зазвичай керують центральні команди організації. Якщо у вашій організації немає таких фахівців, подумайте про сторонню підтримку. Це може полегшити тягар ручного аналізу та кореляції журналів, щоб забезпечити більш ефективне та ефективне керування безпекою.

  Комбінуючи кілька менших інструментів, ви можете емулювати деякі функції системи SIEM. Однак вам потрібно знати, що ці тимчасові рішення можуть не виконувати кореляційний аналіз. Ці альтернативи можуть бути корисними, але вони не можуть повністю замінити функціональність спеціальної системи SIEM, яка «заточена» під
  - виявлення загроз,
  - розслідування інцидентів,
  - оцінку ризиків,
  - управління кібербезпекою

- ➢ **Постійне виявлення та фіксація зловживань.**
  - ✓ **Будьте проактивними щодо виявлення загроз** і будьте пильні щодо ознак зловживань, як-от атаки методом (brute force) грубої обробки даних на компонент SSH або кінцеву точку RDP. Хоча зовнішні загрози можуть створювати багато шуму, особливо якщо програма працює в Інтернеті, внутрішні загрози повинні викликати більше занепокоєння. Несподівана атака грубої сили (brute force) з надійного мережевого джерела або ненавмисна неправильна конфігурація, наприклад, повинні бути розслідувані негайно.

    Моніторинг не замінить проактивне зміцнення середовища. *Більша площа поверхні схильна до більшої кількості атак.* У міру практики посильте контроль. Наприклад
    - **виявляйте та вимикайте невикористовувані облікові записи**
    - **видаляйте невикористовувані порти**
    - **використовуйте брандмауер веб-додатків.**

    До цих базових правил проактивних дій щодо виявлення загроз також відносяться наступні "the best practical":
    - **встановлюйте складні паролі**
      Вимагайте від користувачів встановлювати складні паролі з комбінацією великих і малих літер, цифр і спеціальних символів. Це зробить атаку методом грубої сили набагато складнішою.
    - **забороніть використання стандартних портів**
      Забороніть користувачам використовувати стандартні порти для з'єднань, такі як порт 22 для SSH. Використання нестандартних портів може зменшити ймовірність успішної атаки.
    - **аудит безпеки**
      Регулярно проводьте аудит безпеки системи для виявлення можливих слабких місць і потенційних загроз. Це допоможе забезпечити, що ваша система захищена від нових видів атак.
    - **встановіть двофакторну автентифікацію**

Встановіть двофакторну аутентифікацію для важливих облікових записів, щоб ускладнити заволодіння ними зловмисниками. Це дозволить захистити систему навіть у випадку, якщо пароль викрадений.

- **регулярно оновлюйте ПЗ**
  Важливо регулярно оновлювати всі програми та операційну систему до останніх версій, оскільки вони містять патчі безпеки, які закривають відомі уразливості.

✓ **Виявлення на основі сигнатур може детально перевірити систему.** Це передбачає пошук ознак або кореляції між діями, які можуть вказувати на потенційну атаку. Механізм виявлення може ідентифікувати певні характеристики, які вказують на конкретний тип атаки. Не завжди можливо безпосередньо виявити командний механізм атаки. Однак часто існують підказки або шаблони, пов'язані з певним процесом керування. Наприклад, на атаку може вказувати певна швидкість потоку з точки зору запиту, або вона може часто звертатися до доменів, які мають певні закінчення.

✓ Виявляйте **аномальні моделі доступу користувачів**, щоб ви могли ідентифікувати та досліджувати відхилення від очікуваних моделей. Це передбачає порівняння поточної поведінки користувача з минулою, щоб виявити аномалії. Хоча виконати це завдання вручну може бути неможливим, для цього можна скористатися інструментами аналізу загроз. Інвестуйте в інструменти Analytics and Entity Behavior Analytics (UEBA), які збирають поведінку користувачів із даних моніторингу та аналізують її. Ці інструменти часто можуть виконувати прогнозний аналіз, який зіставляє підозрілу поведінку з потенційними типами атак.

Використання системного та мережевого моніторингу для виявлення вторгнень, зламів та інших загроз безпеці.

➢ **Типові загрози безпеці, які можна виявити за допомогою моніторингу:**

Таблиця 08.01

Загроза	Опис	Метод моніторингу	Спосіб виявлення
Вторгнення, або несанкціонований доступ до систем або мереж	Спроби отримати доступ до конфіденційної інформації, системних ресурсів або мережевих послуг без дозволу або авторизації. Моніторинг виявляє незвичайну або підозрілу активність, що пов'язана з спробами неавторизованого доступу до системних ресурсів, невдалими спробами аутентифікації, незвичайними мережеві пакети або активністю, що відхиляється від звичайного шаблону.	Системні журнали (логи)	❖ невдалі спроби входу ❖ спроби доступу до неприпустимих ресурсів ❖ виконання незвичайних команд
		Мережеві монітори	❖ невідомі підключення ❖ аномальний обсяг трафіку ❖ спроби перехоплення даних
		Системи виявлення вторгнень (IDS) і захисту від вторгнень (IPS)	Аналізують мережевий або системний трафік для виявлення ознак атак або незвичайної активності і можуть автоматично вживати заходи для запобігання вторгненням
		Моніторинг користувацьких активностей	Відстежують активність користувачів і сповіщають про незвичайні дії, які можуть вказувати на компрометацію акаунтів або систем.
Моніторинг вторгнень допомагає виявляти атаки на ранніх етапах, що дозволяє забезпечити вчасну реакцію та запобігти серйозним наслідкам для безпеки систем та мереж.			
Злам, або отримання несанкціонованого доступу до даних або систем	Одна з найбільш руйнівних загроз для безпеки IT. Передбачає отримання зловмисником доступу до конфіденційної інформації, системних ресурсів або програм без належних авторизаційних прав. Моніторинг системи і даних може допомогти виявити підозрілу або незвичайну активність, що може свідчити про можливі спроби злому.	Системні журнали (логи)	❖ спроби незаконного доступу до системних ресурсів ❖ невдалі спроби авторизації
		Моніторинг доступу до даних	дозволяє виявити незвичайні або неповноважні спроби доступу.
		Системи виявлення вторгнень (IDS) і захисту від вторгнень (IPS)	Виявляють незвичайну мережеву активність, що може свідчити про спроби злому або компрометацію систем.
		Моніторинг активності користувачів	виявлення незвичайних патернів поведінки може допомогти виявити компрометацію облікових записів або систем.
		Аналіз зловмисного ПЗ	Допомагає виявити спроби злому або компрометації систем.
Моніторинг зламів допомагає виявляти незаконні або зловмисні дії на ранніх етапах, що дозволяє приймати заходи для захисту систем і даних від потенційної компрометації.			
Шкідливе програмне забезпечення, таке як віруси, трояни, шпигунські програми та ботнети	Наносять значну шкоду системам і даним, а також порушують їхню конфіденційність, цілісність та доступність. Моніторинг системи та мережі допомагає виявляти наявність шкідливого ПЗ шляхом аналізу різноманітних параметрів і показників активності	Антивірусні програми	Дозволяють виявляти віруси, трояни та інші шкідливі програми, які можуть впливати на безпеку системи
		Мережевий моніторинг	Виявляє підозрілі з'єднання або активність, пов'язану зі шкідливим ПЗ - спроби з'єднання з відомими командними і серверними центрами управління ботнетами
		Журнали подій	Виявлення незвичайних або підозрілих дій, що пов'язані з інфікуванням шкідливим ПЗ
		Засоби виявлення вторгнень (IDS)	Виявляють підозрілу мережеву активність, яка свідчить про наявність шкідливого ПЗ у системі
		Системи моніторингу виконання коду (HIDS)	Виявляє незвичайну або підозрілу активність, що свідчить про присутність шкідливих програм
Моніторинг шкідливого програмного забезпечення дозволяє виявляти і реагувати на загрози на ранніх етапах, що допомагає запобігти серйозним наслідкам для безпеки систем та даних.			

SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #8. Застосування моніторингу для виявлення загроз безпеці.*

Фішингові атаки для обману користувачів і отримання їхніх особистих даних або конфіденційної інформації	Передбачають використання підроблених електронних листів, веб-сайтів або повідомлень, які намагаються виглядати як офіційні комунікації від надійних джерел. Моніторинг може допомогти виявити фішингові атаки, спостереженням за певними ознаками та індикаторами, які вказують на шахрайство.	Фільтрація електронних листів	виявлення підозрілих або небезпечних електронних листів за допомогою систем фільтрації спаму та антивірусних програм
		Аналіз вмісту електронних листів	моніторинг наявності підозрілих посилань, вкладень або запитів на особисту інформацію у вмісті електронних листів
		Моніторинг мережевого трафіку	виявлення спроб з'єднання з підробними веб-сайтами або веб-сторінками, що імітують офіційні ресурси
		Системи фішингового виявлення	Виявлення індикаторів фішингових атак у вмісті електронних листів або на веб-сторінках
		Інформаційна освіта користувачів	Навчання користувачів розпізнавати підозрілі електронні листи та уникати небезпечних дій
Моніторинг фішингових атак допомагає виявляти шахрайські спроби на ранніх етапах та запобігає втратам особистої інформації та конфіденційності.			
DDoS-атаки спрямовані на перевантаження серверів або мережевих ресурсів шляхом надмірного навантаження	Призводять до відмови в обслуговуванні легітимних користувачів. Моніторинг може допомогти виявити DDoS-атаки, аналізуючи та виявляючи аномальну мережеву активність та поведінку.	Моніторинг мережевого трафіку	аналіз обсягу мережевого трафіку і виявлення незвичайно великої кількості запитів з одного або декількох джерел, що може свідчити про DDoS-атаку
		Системи виявлення вторгнень (IDS) і захисту від вторгнень (IPS)	виявлення аномальної мережевої активності та блокування небезпечних пакетів, що може бути зв'язано з DDoS-атакою.
		Моніторинг доступності веб-сайту або сервісу	Спостереження за доступністю та швидкістю реакції веб-сайту або сервісу, що дозволяє вчасно виявити відмови в обслуговуванні.
		Аналіз поведінки мережі	Виявлення аномальних патернів мережевої активності, таких як надмірне навантаження на конкретні ресурси або підвищений обсяг запитів.
		Системи миттєвого реагування	можуть реагувати на DDoS-атаки шляхом блокування зловмисницької мережевої активності або перенаправлення трафіку.
Моніторинг DDoS-атак дозволяє оперативно реагувати на загрози і вживати заходів для забезпечення доступності та безпеки веб-сайтів та онлайн-сервісів.			

- **Конкретні приклади того, як моніторинг може допомогти виявити ці загрози:**

  - Таблиця 08.02

Моніторинг аномального завантаження процесора або використання пам'яті	Моніторинг ресурсів системи	виявляє несподівано велике навантаження на систему, що може свідчити про активну діяльність шкідливого програмного забезпечення або ботнета
	Автоматичні попередження	автоматичне сповіщення адміністраторів про значне збільшення використання ресурсів, дозволяє оперативно реагувати на можливі загрози
	Аналіз активності процесів	допомагає виявити незвичайні або підозрілі дії, які можуть бути пов'язані з шкідливим програмним забезпеченням або ботнетами
	Виявлення аномального мережевого трафіку	шкідливе ПЗ або ботнети спричиняють значний обсяг мережевого трафіку, що може бути виявлено за допомогою мережевого моніторингу
	Системи виявлення вторгнень (IDS)	використання IDS для аналізу мережевої активності та виявлення незвичайних патернів, що можуть вказувати на наявність шкідливого ПЗ або ботнетів
Моніторинг підозрілої мережевої активності	Моніторинг мережевого трафіку	аналіз загального обсягу мережевого трафіку і виявлення незвичайних піків або спадів може свідчити про атаки або іншу підозрілу мережеву активність
	Системи виявлення вторгнень (IDS)	використання IDS для аналізу мережевої активності та виявлення незвичайних патернів, таких як сканування портів або атаки на протоколи
	Моніторинг журналів подій мережевих пристроїв	аналіз логів маршрутизаторів, комутаторів та інших мережевих пристроїв для виявлення незвичайних або підозрілих активностей
	Виявлення аномальних підключень	моніторинг незвичайних підключень до мережевих ресурсів або систем, які можуть свідчити про недозволені дії або сканування мережі
	Моніторинг протоколів мережі	аналіз використання мережевих протоколів і виявлення незвичайних або підозрілих патернів комунікації, що можуть вказувати на атаки на протоколи або спроби експлойтації вразливостей
Допомагає оперативно виявляти потенційні загрози мережевої безпеки та приймати відповідні заходи для їх усунення.		
Моніторинг несанкціонованого доступу до файлів або систем	Моніторинг змін у файлах	виявляє незвичайні модифікації, які можуть свідчити про несанкціонований доступ або втручання у систему
	Моніторинг журналів подій	виявляє незвичайну активність, таку як невдалі спроби входу або виконання непередбачуваних операцій, що можуть свідчити про спроби несанкціонованого доступу

	Автоматичне сповіщення про підозрілі дії	сповіщення про незвичайні дії або події, такі як зміна прав доступу до файлів чи невдалі спроби авторизації
	Виявлення незвичайних патернів активності користувачів	моніторинг звітів про активність користувачів дозволяє виявляти незвичайну або підозрілу активність, таку як несподівані спроби доступу до конфіденційних файлів чи каталогів
	Використання систем виявлення вторгнень (IDS)	Використання IDS для аналізу мережевої активності та виявлення спроб несанкціонованого доступу до системи
Дозволяє оперативно виявляти порушення безпеки та приймати відповідні заходи для їх усунення.		
Моніторинг зловживання правами доступу користувачів з адміністративними правами	Журнали подій системи	ведення журналів подій, які відображають всі дії користувачів з адміністративними правами, такі як зміна налаштувань, створення чи видалення облікових записів, зміни прав доступу тощо
	Моніторинг змін в системі	незвичайні зміни в конфігурації системи, файловій структурі або правах доступу, що може свідчити про можливі зловживання
	Сповіщення про незвичайну активність	автоматичне сповіщення адміністраторів про незвичайні або підозрілі дії користувачів з адміністративними правами
	Моніторинг дій з адміністративними привілеями	спостереження за активністю користувачів з адміністративними правами, такою як спроби доступу до обмежених ресурсів або виконання критичних команд
	Аудит доступу до системних ресурсів	встановлення систем аудиту, які відстежують всі спроби доступу до системних ресурсів користувачами з адміністративними правами
Допомагає оперативно виявляти можливі загрози безпеці та забезпечує ефективний контроль над доступом до системних ресурсів.		
Моніторинг поширення шкідливого програмного забезпечення	Моніторинг завантаження та запуску файлів	відстеження процесів завантаження та запуску файлів на системі, що дозволяє виявити незвичайні або підозрілі файли, які можуть бути шкідливим програмним забезпеченням
	Системи виявлення загроз (IDS/IPS)	використання спеціалізованих систем для виявлення аномальної або підозрілої мережевої активності, яка може бути пов'язана з поширенням шкідливого програмного забезпечення
	Моніторинг мережевого трафіку	виявлення незвичайних або підозрілих патернів, таких як спроби з'єднання з небезпечними доменами або серверами, які можуть вказувати на поширення шкідливого програмного забезпечення
	Системи антивірусного захисту	сканування файлів на наявність відомих шкідливих програм та блокування їх запуску
	Моніторинг системних ресурсів	CPU, пам'ять, диск та інші для виявлення незвичайних або підозрілих активностей, які можуть бути пов'язані з роботою шкідливого ПЗ
Допомагає оперативно виявляти та усувати цю загрозу, що забезпечує надійний рівень безпеки для систем та даних		
Моніторинг фішингових атак	Моніторинг URL-адрес	постійне відстеження та аналіз URL-адрес, що надходять до системи електронної пошти чи інших комунікаційних каналів. Деякі системи можуть автоматично розпізнавати підозрілі або фішингові URL-адреси за допомогою евристичних методів аналізу
	Аналіз електронних листів	сканування та аналіз вмісту електронних листів, для виявлення ознак фішингу, такі як надмірна пропозиція, небезпечні вкладення чи посилання, надання конфіденційної інформації тощо
	Використання спеціалізованих фільтрів	встановлення фільтрів та правил для виявлення та блокування фішингових спроб, що грунтуються на аналізі вмісту електронних листів та URL-адрес
	Сповіщення про підозрілі листи	автоматичне сповіщення користувачів про підозрілі або небезпечні електронні листи, що може збільшити обізнаність та усвідомленість користувачів щодо потенційних загроз
	Моніторинг поведінки користувачів	аналіз поведінки користувачів та виявлення аномалій у їхньому споживанні електронної пошти, що може вказувати на спроби фішингу чи недбале ставлення до безпеки
Моніторинг URL-адрес та електронних листів дозволяє ефективно виявляти фішингові атаки та запобігати їхньому успішному використанню, що забезпечує підвищення рівня безпеки для організації та користувачів		
Моніторинг DDoS-атак	Моніторинг доступності сервісів	постійна перевірка доступності ключових сервісів, таких як веб-сайти, сервери електронної пошти чи додатки, і сповіщення про будь-які відмови у доступі
	Аналіз аномального трафіку	виявлення аномальних патернів або збільшення обсягу трафіку, які можуть бути ознакою DDoS-атаки
	Використання систем виявлення вторгнень (IDS/IPS)	виявлення та блокування атак, що спрямовані на виведення з ладу сервісів шляхом перевантаження мережевого трафіку
	Спостереження за аномальними запитами	аналіз логів серверів та мережевих пристроїв для виявлення незвичайно великої кількості запитів від певних джерел, що може свідчити про DDoS-атаку
	Моніторинг споживання ресурсів	❖ пропускна здатність мережі ❖ обсяг використання процесора ❖ обсяг використання пам'яті

Дозволяє оперативно виявляти DDoS-атаки та приймати необхідні заходи для їх усунення, що забезпечує надійну захист від цієї форми кібератак.

- **Рекомендації щодо налаштування моніторингу для виявлення загроз:**

  - **Критичні системи** - це ті, без яких неможливо нормально функціонувати організації або іншій сутності. Це можуть бути системи управління базами даних, сервери електронної пошти, системи зберігання даних, мережеві інфраструктури, системи моніторингу безпеки тощо.
    Критичні системи можуть також включати ті, які забезпечують забезпечення здоров'я та безпеку людей, наприклад, системи медичного обладнання, системи безпеки виробництва тощо.
  - **Критичні дані** - це дані, які є найважливішими для діяльності організації або мають велику цінність для її функціонування. Це може бути конфіденційна інформація про клієнтів, фінансові дані, інтелектуальна власність, розробки, а також дані, які підлягають регулюванню законами про конфіденційність, такі як персональні дані.

  - **Рекомендації щодо налаштування моніторингу**.
    - ✓ **Ідентифікація критичних активів**. Почніть з ідентифікації всіх критичних систем та даних в вашій організації. Це допоможе зосередити зусилля на захисті найважливішого.
    - ✓ **Налаштування моніторингу безпеки**. Встановіть системи моніторингу безпеки для постійного відстеження активності в мережі та на серверах. Це включає виявлення незвичайних патернів трафіку, спроби несанкціонованого доступу, аномальні активності користувачів тощо.
    - ✓ **Реагування на виявлені загрози**. Розробіть процедури та плани реагування на виявлені загрози. Це може включати автоматичні заходи безпеки, які активуються при виявленні підозрілих дій, а також ручні процедури для виявлення та усунення загроз вручну.
    - ✓ **Регулярне оновлення моніторингових систем**. Забезпечте, що ваші системи моніторингу постійно оновлюються та налаштовуються для виявлення нових видів загроз, оскільки кіберзлочинці постійно вдосконалюють свої методи.
    - ✓ **Навчання персоналу**. Проводьте навчання персоналу з питань кібербезпеки та впроваджуйте свідомість про безпеку в організації, щоб уникнути людських помилок, які можуть стати витоком для загроз безпеці.

  Деякі рекомендації щодо вибору інструментів моніторингу з урахуванням потреб та бюджету:

  - **Оцінка потреб**. Почніть з оцінки потреб вашої організації щодо моніторингу. Які типи систем і даних вам потрібно моніторити? Які загрози ви хочете виявляти? Які функції та можливості вам необхідні для ефективного моніторингу?

  - **Аналіз бюджету.** Визначте ваш бюджет на моніторинг і безпеку. Розгляньте, скільки ви готові і можливі витратити на придбання та підтримку інструментів моніторингу.

  - **Вибір відповідних інструментів.**

    - ✓ **Відкриті рішення.** Розгляньте використання відкритих рішень, таких як Nagios, Zabbix, OpenNMS для системного та мережевого моніторингу. Вони зазвичай безкоштовні або мають відкритий код, що знижує витрати на ліцензії.
    - ✓ **Комерційні рішення**. Якщо ви готові витратити більше коштів, розгляньте комерційні рішення, такі як SolarWinds, Splunk, IBM QRadar. Вони можуть мати більше функціональності та підтримку, але можуть бути дорожчими.
    - ✓ **Спеціалізовані інструменти**. Для виявлення конкретних загроз, таких як DDoS-атаки або фішинг, ви можете розглянути використання спеціалізованих інструментів, таких як Cloudflare для захисту від DDoS-атак або PhishMe для виявлення фішингових спроб.
  - **Управління ризиками.** Приймайте рішення про вибір інструментів, враховуючи рівень ризику вашої організації. Пам'ятайте про баланс між витратами та рівнем захисту, який вони забезпечують.

  - **Тестування і оцінка.** Перед повним впровадженням інструментів проведіть тестування та оцінку їх ефективності. Впевніться, що вони відповідають вашим потребам і вимогам безпеки перед прийняттям остаточного рішення.

Необхідно згадати про таку річ, як налаштування правил та тригерів моніторингу для кожного типу загрози. Про більшість типів загроз ми вже говорили це

- **Вторгнення (не санкціонований доступ до систем або мереж).**
- **Зломи (отримання не санкціонованого доступу до даних або систем).**
- **Поширення шкідливого програмного забезпечення.**
- **Фішингові атаки.**
- **DDoS-атаки.**

Не згадували ще у цьому переліку такі неприємні речі, що дуже важко або навіть неможливо передбачити як

- **Вихід з ладу обладнання**
- **Стихійне лихо**.

Тут можливо лише рекомендувати використання систем моніторингу стану обладнання для виявлення незвичайних або непередбачених змін у функціонуванні та налаштування тригерів для сповіщень про великі зміни в енергоспоживанні або температурі обладнання, що може свідчити про проблеми з обладнанням або його виходом з ладу.

Не забуваємо, що процес моніторингу має бути безперервним, цілодобовим та супроводжуватися швидким реагуванням на інциденти.
Програмне забезпечення та бази даних загроз мають регулярно оновлюватися.

Аналіз логів, виявлення аномалій та паттернів, пов'язаних із зловмисними діями.

SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #8. Застосування моніторингу для виявлення загроз безпеці.*

1. **Фільтрація та збір та лог-даних (Collection of Log Data).** На цьому етапі відбувається пошук даних (в даному випадку – лог даних) з відповідних джерел. Велике значення має репрезентативність інформації, оскільки на цих даних буде оснований результат. Зважаючи на цей фактор велике значення має реальність та непошкодженість інформації. Зібрані дані мають бути поміщенні у деяке сховище (наприклад – база даних) та відфільтровані за відповідними критеріями використовуючи застосунки. Фільтрація даних має велике значення так як це впливає на репрезентативність даних.

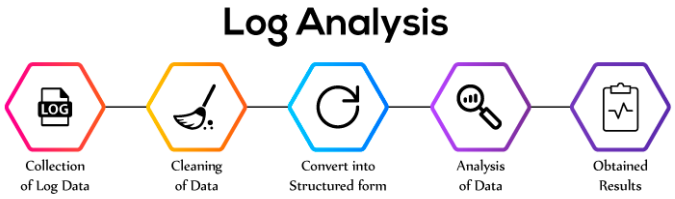


Рис. 08.01. Класичні етапи аналізу логів

2. **Структурування даних (Cleaning and Convert of Data into Structured form).** Дані логів можуть мати великий об'єм а також складну структуру. Для полегшення розуміння їх слід структурувати у зручному для користувача вигляді. Слід зважати на те, що логи можуть мати зв'язок з даними, що були отримані з інших джерел.
3. **Аналіз даних (Analysis of Data).** Завершаючим етапом є аналіз оброблених даних. На цьому етапі можуть бути залученні різні відомі методи аналізу даних. Вибір методу напряму залежить від типу задачі а також навиків розробника.

➢ **Аномалії та методики їх виявлення**

Виявлення аномалій відноситься до пошуку непередбачених значень (патернів) в потоках даних. Аномалія (викид, помилка, відхилення або виключення) - це відхилення поведінки системи від стандартного (очікуваного). Аномалії поділяються на три наступні категорії:

1. **Точкові аномалії** - виникають в ситуації, коли окремий екземпляр даних може розглядатися як аномальний по відношенню до решти даних. Даний вид аномалій є найбільш легко розпізнаваним, більшість існуючих методів створено для розпізнавання точкових аномалій.
2. **Контекстні аномалії**, також відомі як «умовні аномалії» – спостерігаються, якщо екземпляр даних є аномальним лише в певному контексті. Аномальна поведінка визначається за допомогою значень поведінкових атрибутів виходячи з конкретного контексту. Таким чином, екземпляр даних може бути контекстуальної аномалією за даних умов, але при таких же поведінкових атрибутах вважатися нормальним в іншому контексті.
3. **Колективні аномалії** – виникають, коли послідовність пов'язаних примірників даних (наприклад, ділянка часового ряду) є аномальною по відношенню до цілого набору даних. Окремий екземпляр даних в такій послідовності може не бути відхиленням, проте спільна поява таких екземплярів є колективною аномалією.

➢ **Режими виявлення аномалій**

Для вирішення завдання пошуку аномалій потребується набір даних, що описують систему. Кожен екземпляр в ньому описується міткою, яка вказує, чи є він нормальним або аномальним. Таким чином, безліч екземплярів з однаковими тегами формують відповідний клас.
Створення подібної промаркованної вибірки зазвичай проводиться вручну і є трудомістким і дорогим процесом. У деяких випадках отримати екземпляри аномального класу неможливо в силу відсутності даних про можливі відхилення в системі, в інших можуть бути відсутні мітки обох класів. Залежно від того, які класи даних використовуються для реалізації алгоритму, методи пошуку аномалій можуть виконуватися в одному з трьох перерахованих нижче режимів:

✓ **Supervised anomaly detection (режим розпізнавання з учителем).** Дана методика вимагає наявності навчальної вибірки, що повноцінно представляє систему і включає екземпляри даних нормального і аномального класів. Робота алгоритму відбувається в два етапи: навчання та розпізнавання. На першому етапі будується модель, з якою будуть порівнюються екземпляри, які не мають мітки. У більшості випадків покладається, що дані не змінюють свої статистичні характеристики, інакше виникає необхідність змінювати класифікатор. Основною складністю алгоритмів, що працюють в режимі розпізнавання з учителем, є формування даних для навчання. Часто аномальний клас представлений значно меншою кількістю примірників, ніж нормальний, що може призводити до неточностей в отриманій моделі. У таких випадках застосовується штучна генерація аномалій.

✓ **Semi-Supervised anomaly detection (режим розпізнавання частково з учителем).** Вихідні дані при цьому підході представляють тільки нормальний клас. Навчившись на одному класі, система може визначати приналежність нових даних до нього, таким чином, визначаючи протилежний. Алгоритми, що працюють в режимі розпізнавання частково з учителем, не вимагають інформації про аномальний клас примірників, внаслідок чого вони ширше застосовуються й дозволяють розпізнавати відхилення за відсутності заздалегідь певної інформації про них.

✓ **Unsupervised anomaly detection (режим розпізнавання без учителя).** Застосовується при відсутності апріорної інформації про дані. Алгоритми розпізнавання в режимі без вчителя базуються на припущенні про те, що аномальні екземпляри зустрічаються набагато рідше нормальних. Дані обробляються, найбільш віддалені визначаються як аномалії. Для застосування цієї методики має бути доступний весь набір даних, тобто вона не може застосовуватися в режимі реального часу.

➢ **Системи моніторингу, що використовують аналіз логів.** Існує багато систем моніторингу, які використовують аналіз логів для виявлення аномалій та патернів, пов'язаних із зловмисними діями. Яскраві приклади таких систем:

❖ **ELK Stack (Elasticsearch, Logstash, Kibana)**
ELK Stack - це популярний набір інструментів з відкритим кодом для збору, зберігання, аналізу та візуалізації даних логів.
Elasticsearch використовується для зберігання та пошуку даних логів.
Logstash використовується для збору та перетворення даних логів.
Kibana використовується для візуалізації даних логів та виявлення аномалій.
❖ **Graylog**
❖ **Splunk**
❖ **SolarWinds Log & Event Manager (LEM)**
❖ **IBM QRadar**

Перелічені системи моніторингу можуть збирати дані логів з різних джерел, включаючи системи, додатки та мережеві пристрої та мають вбудовані панелі моніторингу та звіти для візуалізації даних логів.
Splunk - це єдиний продукт з перелічених, який має безкоштовний рівень ліцензування, щообмежується об'ємом даних логів 500 МБ на день, без обмежень за функціональністю. **ELK Stack** – повністю безкоштовний продукт, але його потрібно самостійно встановити та налаштувати. Інші продукти (**Graylog, SolarWinds LEM, IBM QRadar**) є платними.
Важливо зазначити, що це лише декілька прикладів систем моніторингу, які використовують аналіз логів.

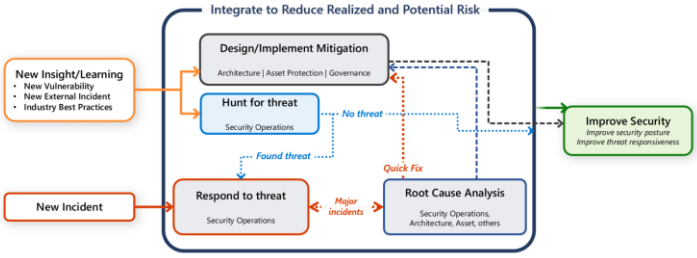
SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #8. Застосування моніторингу для виявлення загроз безпеці.*
При виборі системи моніторингу важливо враховувати конкретні потреби та бюджет.

Розробка стратегій реагування та відновлення після виявлення загроз.

Більшість підприємств мають центральну групу безпеки (також відому як Security Operations Center (SOC) або SecOps). Відповідальність робочої групи безпеки полягає в тому, щоб швидко виявляти, визначати пріоритети та сортувати потенційні атаки. Команда також відстежує пов'язані з безпекою телеметричні дані та розслідує порушення безпеки.

Однак ви також несете відповідальність за збереження свого робочого навантаження. Важливо, щоб будь-які комунікації, розслідування та пошукові дії були спільними зусиллями команди робочого навантаження та команди SecOps.

Розглянемо рекомендації для робочої групи, які допоможуть швидко виявити, сортувати та розслідувати атаки.



Розглянемо термінологію, яка буде використовуватися у цій частині лекції:

Попередження	Повідомлення, що містить інформацію про інцидент.
Вірність попередження	Точність даних, які визначають сповіщення. Сповіщення високої точності містять контекст безпеки, необхідний для вжиття негайних дій. Сповіщення низької точності містять брак інформації або шум.
Хибно позитивний	Сповіщення, яке вказує на інцидент, якого не сталося.
Інцидент	Подія, яка вказує на неавторизований доступ до системи.
Реагування на інцидент	Процес, який виявляє ризики, пов'язані з інцидентом, реагує на них і пом'якшує їх.
Сортування	Операція з реагування на інциденти, яка аналізує проблеми безпеки та визначає пріоритетність їх пом'якшення.

- **Стратегія дизайну оповіщень.**
  Операції з реагування на інциденти виконуються, коли є сигнал або сповіщення про потенційну компрометацію. Сповіщення високої точності містять широкий контекст безпеки, який полегшує аналітикам прийняття рішень. Сповіщення високої точності призводять до низької кількості помилкових спрацьовувань. Необхідно передбачити, що система сповіщень фільтрує сигнали низької точності та зосереджується на сповіщеннях високої точності, які можуть вказувати на реальний інцидент.

- **Налаштування сповіщень про інцидент.**
  Сповіщення безпеки мають охопити відповідних людей у вашій команді та організації. Встановіть призначену контактну інформацію у вашій робочій групі, щоб отримувати повідомлення про інциденти. Ці сповіщення мають містити якомога більше інформації про ресурс, який зламано, і систему. Сповіщення має містити наступні дії, щоб ваша команда могла пришвидшити дії.
  Рекомендується реєструвати сповіщення про інциденти та дії та керувати ними за допомогою спеціальних інструментів, які зберігають контрольний слід. Використовуючи стандартні інструменти, ви можете зберегти докази, які можуть знадобитися для потенційних судових розслідувань. Шукайте можливості впровадження автоматизації, яка може надсилати сповіщення на основі обов'язків відповідальних сторін. Зберігайте чіткий ланцюжок зв'язку та звітування під час інциденту.
  Скористайтеся перевагами рішень для управління подіями безпеки (SIEM) і рішень для автоматизованого реагування оркестровки безпеки (SOAR), які надає ваша організація. Крім того, ви можете придбати інструменти керування інцидентами та заохотити свою організацію стандартизувати їх для всіх робочих груп.

- **Розслідування інцидентів за допомогою групи реагування.**
  Після виявлення загрози найважливіше провести ретельне розслідування, щоб зрозуміти її масштаби та наслідки. У цьому вам допоможе **група реагування на інциденти** (її ще називають **командою оцінки**).
  Перший крок - створення групи реагування.
  - ✓ Людина, яка отримала сповіщення про інцидент, повинна зібрати групу фахівців, виходячи з отриманої інформації.
  - ✓ Цій групі потрібно **узгодити методи та канали комунікації**. Чи потрібні асинхронні обговорення (наприклад, листування) або термінові дзвінки? Як відстежуватимуть та повідомлятимуть про хід розслідування? Де знайти необхідні матеріали, пов'язані з інцидентом?

  Ефективність розслідування залежить від актуальності документації.
  - ✓ Важливо мати **останні версії документів**, що описують архітектуру системи, інформацію про компоненти, рівень конфіденційності та безпеки, власників компонентів та контактні особи. Застаріла інформація змусить групу витрачати дорогоцінний час на розуміння того, як працює система, хто відповідає за кожну її частину та які можуть бути наслідки інциденту.

  До розслідування залучайте необхідних фахівців.
  - ✓ Це може бути керівник реагування на інциденти, співробітник служби безпеки або відповідальні за окремі робочі навантаження.
  - ✓ Не варто залучати людей, чиї обов'язки не стосуються конкретної проблеми. Іноді розслідування проводять окремі команди. Одна команда може первинно досліджувати проблему та намагатися її мінімізувати, а інша, більш спеціалізована, може проводити детальний цифровий аналіз для виявлення глибинних проблем. Для такої команди можна тимчасово ізолювати робоче середовище. В інших випадках усе розслідування може проводити одна команда.

  На початковому етапі група реагування повинна визначити:
  - ✓ **Можливий вектор атаки** та його вплив на **конфіденційність, цілісність та доступність (confidentiality, integrity, and availability - CIA)** системи.
  - ✓ **Початковий рівень серйозності** інциденту, який враховує масштаби шкоди та терміновість виправлення. Цей рівень, ймовірно, змінюватиметься в міру отримання нових даних під час розслідування.

  Під час розслідування потрібно визначити:
  - ✓ **Необхідні дії та план інформування.** Чи потрібно змінити стан роботи системи? Як зупинити подальшу експлуатацію вразливості? Чи потрібно інформувати внутрішні або зовнішні структури, наприклад, провести публічне розкриття інформації про вразливість?

- ✓ **Час виявлення та реагування.** Іноді законодавство зобов'язує вас повідомити про певні типи порушень регуляторні органи протягом певного часу (зазвичай годин або днів).

Якщо прийнято рішення зупинити роботу системи, наступним кроком буде відновлення її працездатності за допомогою процедур аварійного відновлення. Якщо зупиняти роботу системи не потрібно, визначте, як усунути інцидент без впливу на її функціональність.

- **Відновлення після інциденту.**

Ставтесь до інцидентів кібербезпеки, як до стихійного лиха. Якщо відновлення потребує повного перезапуску системи, використовуйте належні механізми відновлення після аварій (DR) з урахуванням безпеки.

Процес відновлення повинен запобігти повторному виникненню проблеми.

- ✓ Відновлення із зараженої резервної копії призведе до повторного зараження.
- ✓ Повторне розгортання системи з тією ж самою вразливістю призведе до того ж інциденту.
- ✓ Обов'язково перевірте кроки та процеси переходу на резервну систему та повернення до основної.

Якщо система продовжує працювати:

- ✓ Оцініть вплив інциденту на її функціонування.
- ✓ Продовжуйте моніторинг системи, щоб переконатися, що інші показники надійності та продуктивності відповідають вимогам, або відкоригуйте їх за допомогою належних процедур зниження впливу.
- ✓ Не дозволяйте заходам реагування порушувати конфіденційність даних.

Діагностика - це інтерактивний процес.
Вона триває доти, доки не буде визначено вектор атаки, потенційне виправлення та відкат системи. Після діагностики команда працює над **виправленням**, яке полягає у визначенні та застосуванні необхідного рішення протягом допустимого часу.
Показники відновлення вимірюють, скільки часу потрібно, щоб виправити проблему. У випадку зупинки системи, терміни виправлення можуть бути критичними. Для стабілізації системи потрібен час на застосування виправлень, патчів, тестування та розгортання оновлень.
Розробіть стратегії стримування для запобігання подальшій шкоді та поширенню інциденту.
Розробіть процедури повного видалення загрози із системи.

Компроміс: під час інциденту ви, ймовірно, не зможете дотримуватися інших функціональних або нефункціональних вимог. Наприклад, вам може знадобитися тимчасово відключити частини системи під час розслідування або навіть повністю зупинити її роботу, поки не буде визначено масштаби інциденту. Керівництво повинно чітко визначити прийнятні цілі під час інциденту та призначити відповідальну за це рішення особу.

- **Навчання на інцидентах.**

Інцидент кібербезпеки розкриває недоліки або вразливі місця в проєктуванні чи реалізації системи. Це можливість для покращення за рахунок уроків, отриманих з технічних аспектів проєктування, автоматизації, процесів розробки продуктів, що включають тестування, та ефективності реагування на інциденти.
Зберігайте детальні записи про інциденти, включаючи вжиті дії, хронологію та висновки.
Настійно рекомендується проводити структуровані огляди після інцидентів, такі як аналіз корінних причин та ретроспективи. Відстежуйте та пріоритезуйте результати цих оглядів і розгляньте можливість використання отриманих знань у майбутньому проєктуванні робочих навантажень.
Плани покращення повинні включати оновлення навчальних заходів з безпеки та тестування, наприклад, навчання з безперервності бізнесу та відновлення після аварій (BCDR). Використовуйте компрометацію безпеки як сценарій для проведення навчань з BCDR. Навчання можуть підтвердити, як працюють задокументовані процеси.
Не повинно бути кількох сценаріїв реагування на інциденти. Використовуйте єдине джерело, яке можна адаптувати залежно від масштабу інциденту та його поширення. Навчання базуються на гіпотетичних ситуаціях. Проводьте навчання в середовищі з низьким рівнем ризику та включайте фазу навчання до самих навчань.
Проводьте огляди після інцидентів, або пост-mortem аналіз, щоб визначити слабкі місця в процесі реагування та сфери для покращення. На основі уроків, отриманих з інциденту, оновіть план реагування на інциденти (IRP) та засоби безпеки.

- **Інформування після інциденту**

Реагування на інцидент включає інформування.
Необхідно повідомити користувачів про збій у роботі системи та поінформувати внутрішніх зацікавлених осіб про дії з відновлення та покращення.
Також потрібно повідомити інших співробітників вашої організації про будь-які зміни в базових засобах безпеки робочого навантаження, щоб запобігти інцидентам у майбутньому.
Створіть план інформування для різних цілей:

- ✓ **Звіти про інциденти для внутрішнього користування:** ці звіти документують події інциденту та дії, вжиті для його вирішення.
- ✓ **Звіти для регуляторного або юридичного дотримання:** якщо законодавство або юридичні обставини вимагають звітності, потрібно підготувати відповідний документ.

Для ефективного інформування:

- ✓ Використовуйте **стандартний формат звіту** із визначеними розділами. Це дозволить команді центру безпеки (SOC) швидко готувати звіти для всіх інцидентів.
- ✓ Переконайтесь, що **кожен інцидент має пов'язаний звіт**, перш ніж закривати розслідування.

- **Рекомендації щодо інформування про небезпеки в інформаційних мережах**

Інформаційні мережі, як і будь-яка інша система, можуть бути вразливими до кіберзагроз. **Системи моніторингу**, такі як SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation, and Response), відіграють важливу роль у виявленні та реагуванні на ці загрози.

SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation, and Response) - це обидва важливі інструменти для кібербезпеки, але вони мають різні функції та підходи.

- **SIEM (Security Information and Event Management)** - це система, яка збирає, аналізує та інтерпретує дані з різних джерел у реальному часі з метою виявлення потенційних загроз та ризиків для безпеки. SIEM зазвичай використовується для моніторингу подій, виявлення аномалій, аналізу журналів, зберігання даних та генерації звітів. Він може інтегруватись з іншими інструментами безпеки для покращення виявлення та реагування на загрози.
- **SOAR (Security Orchestration, Automation, and Response)** - це платформа, яка комбінує в собі засоби автоматизації, оркестрації та відповіді на події безпеки з метою ефективного управління інцидентами та зменшення часу реагування. SOAR допомагає організаціям у стандартизації та автоматизації процесів реагування на кіберзагрози. Це включає автоматизовану обробку інцидентів, інтеграцію з іншими інструментами безпеки, створення та виконання відповідних дій в разі інцидентів та відслідковування їх статусу.

Отже, основна різниця між SIEM і SOAR полягає в тому, що SIEM спрямований на моніторинг та аналіз подій безпеки, тоді як SOAR розвиває цей концепт, додаючи елементи автоматизації, оркестрації та відповіді на події.

✓ **Приклади SIEM (Security Information and Event Management) рішень:**
- ❖ **Splunk Enterprise Security:** Цей продукт використовується для збору даних з різних джерел, їх аналізу та кореляції для виявлення загроз.
- ❖ **ArcSight ESM:** Цей продукт використовується для централізованого моніторингу та управління журналами безпеки.
- ❖ **QRadar:** Цей продукт використовується для виявлення аномалій та кореляції подій для виявлення загроз.

✓ **Приклади SOAR (Security Orchestration, Automation, and Response) рішень:**
- ❖ **Demisto:** Цей продукт використовується для автоматизації завдань реагування на інциденти.
- ❖ **Palo Alto Networks Cortex XSOAR:** Цей продукт використовується для оркестрації та автоматизації завдань кібербезпеки.
- ❖ **IBM Resilient:** Цей продукт використовується для автоматизації та координації реагування на інциденти.

Ці рішення можуть бути використані для:
- ❖ Збору даних з різних джерел, таких як журнали безпеки, мережеві пристрої та агенти на кінцевих точках.
- ❖ Аналізу даних для виявлення загроз.
- ❖ Кореляції подій для визначення масштабу та впливу інциденту.
- ❖ Автоматизації завдань реагування на інциденти.
- ❖ Створення звітів про інциденти.

Вибір SIEM/SOAR рішення залежить від потреб вашої організації. Важливо враховувати такі фактори:
- ❖ Розмір вашої організації.
- ❖ Складність вашої мережі.
- ❖ Ваш бюджет.
- ❖ Ваші вимоги до безпеки.

Рекомендується проконсультуватися з фахівцем з кібербезпеки, щоб вибрати правильне рішення для вашої організації.

На основі даних моніторингу та рішень SIEM/SOAR можна сформувати наступні **рекомендації щодо інформування про небезпеки** в будь-якій інформаційній мережі:

1. **Створення та підтримка актуального плану інформування.**
   План повинен визначати, **хто** буде повідомлений про **які** інциденти, **коли** та **яким чином**.
   Необхідно чітко визначити **ролі та відповідальності** за інформування.
   План має бути регулярно **переглядатись та оновлюватись**, щоб враховувати зміни в мережі та загрозах.
2. **Використання каналів зв'язку, які відповідають потребам аудиторії.**
   Для **технічних фахівців** можуть бути більш корисними **детальні технічні звіти**.
   Керівництво може потребувати **коротких оглядів** з акцентом на **бізнес-ризики** та **дії, які потрібно вжити**.
   Для **широкої аудиторії** можуть бути корисними **прості та зрозумілі повідомлення**.
3. **Своєчасне інформування про всі інциденти.**
   Важливо **негайно** повідомити про **критичні інциденти**, щоб можна було вжити відповідних заходів для їхнього стримування.
   Про **менш серйозні інциденти** можна повідомляти **з меншою терміновістю**, але все ж таки вчасно, щоб дати можливість зацікавленим сторонам вжити заходів для захисту.
4. **Надання чіткої та лаконічної інформації.**
   Повідомлення про інциденти повинні містити **яку інформацію**:
   - Дата та час інциденту
   - Тип інциденту
   - Вплив на мережу та дані
   - Вжиті дії
   - Рекомендації для зацікавлених **сторін**
5. **Використання автоматизованих інструментів для інформування.**
   SIEM/SOAR рішення можуть **автоматизувати** процес надсилання повідомлень про інциденти.
   Це може **заощадити час** та **забезпечити своєчасне інформування** всіх зацікавлених сторін.
6. **Проведення навчання з кібербезпеки для користувачів мережі.**
   Навчання може допомогти користувачам **розпізнавати** та **повідомляти** про підозрілу активність.
   Це може **знизити ризик** успішної атаки.
7. **Регулярний перегляд та оновлення плану інформування.**
   Важливо **регулярно переглядати** план інформування, щоб **враховувати зміни** в мережі, загрозах та потребах аудиторії. Це допоможе **забезпечити ефективність** інформування про інциденти.

Важливо пам'ятати, що ефективне інформування про інциденти **є важливою складовою** кібербезпеки.

Компроміси безпеки

SNM. #3. Інструменти моніторингу та аналізу даних ***

Системний *та мережевий моніторинг. Лекція #8. Застосування моніторингу для виявлення загроз безпеці.*

Безпека повинна гарантувати конфіденційність, цілісність та доступність даних користувачів. Ніколи не можна йти на компроміси щодо заходів безпеки, але є моменти, що виглядають як компроміси безпеки, але насправді підвищують надійність мережі та її безпеку.

- **Компроміс безпеки з надійністю**

  Підвищена складність. Надійність це простота. Рекомендується звести до мінімуму точки відмови.
  - Деякі елементи керування безпекою можуть збільшити ризик неправильної конфігурації, що може призвести до збою служби. Приклади елементів керування безпекою, які можуть призвести до неправильної конфігурації, включають правила мережевого трафіку, постачальників ідентифікаційних даних, виключення сканування вірусів і призначення контролю доступу на основі ролей або атрибутів.
  - Збільшення сегментації зазвичай призводить до більш складного середовища з точки зору топології ресурсів і мережі та доступу оператора. Ця складність може призвести до збільшення кількості точок збою в процесах і виконанні робочого навантаження.
  - Інструменти безпеки часто включені в багато рівнів архітектури інфраструктури. Ці інструменти можуть впливати на стійкість, доступність і планування потужностей. Неврахування обмежень у інструментах може призвести до зниження надійності, як-от виснаження порту NAT на вихідному брандмауері.

- **Збільшення критичних залежностей.**

  Надійність: Важливо мінімізувати критичні залежності компонентів інфраструктури, щоб мати більше контролю над точками відмови.

  Безпека: Для верифікації особи та дій потрібні ключові компоненти інфраструктури. Якщо ці компоненти недоступні або не працюють, система не може гарантувати безпеку.

  Ризики: Недоступність або несправність компонентів інфраструктури може призвести до проблем з верифікацією та, як наслідок, до ризиків для безпеки.

  Приклади критичних залежностей:
  - Мережеві брандмауери
  - Списки відкликаних сертифікатів
  - Сервер NTP
  - Microsoft AD

- **Компроміси безпеки - складність відновлення після аварій.**

  Компоненти інфраструктури мають надійно відновлюватися після будь-яких катастроф.
  - Контроль безпеки може вплинути на цільовий час відновлення. Цей ефект може бути спричинений додатковими кроками, які необхідні для розшифровки резервних копій даних, або затримками оперативного доступу, створеними сортуванням надійності сайту.
  - Самі елементи керування безпекою, наприклад секретні сховища та їхній вміст або захист від DDoS, мають бути частиною плану аварійного відновлення компонентів інфраструктури та мають бути перевірені за допомогою вправ відновлення.
  - Вимоги щодо безпеки чи відповідності можуть обмежити варіанти розташування даних або доступ до резервних копій. Це може додатково ускладнити відновлення, оскільки навіть офлайн-копії можуть бути сегментовані.
- **Компроміси безпеки - підвищена швидкість змін.**

  Часті зміни в системі можуть вплинути на її надійність.

  .

  Суворіша політика оновлень та патчів призводить до більшої кількості змін у виробничому середовищі **системи**. Ці зміни можуть виникати з таких джерел:
  - Частіші оновлення коду додатків
  - Збільшення routine patchів операційних систем
  - Оновлення версій програмного забезпечення або платформ даних
  - Застосування патчів постачальників до програмного забезпечення в середовищі
  - Ротація ключів, облікових даних служб та сертифікатів

  Таким чином часті зміни можуть призвести до тимчасових проблем із надійністю, поки система адаптується до нових налаштувань.

  Порада:
  - Ретельно тестуйте оновлення та патчі перед їх застосуванням у product-середовищі.
  - Розгляньте можливість використання поетапного розгортання оновлень, щоб мінімізувати ризики.

- **Компроміси безпеки при оптимізації витрат**
  - **Збільшення інфраструктури**

    Оптимізація витрат:
    - Один із способів оптимізації витрат на **систему** полягає в пошуку шляхів зменшення кількості та різноманітності **компонентів інфраструктури** та підвищення щільності їх розміщення.

    Безпека vs. Витрати:
    - Деякі **компоненти інфраструктури** або проектні рішення існують тільки для захисту безпеки (конфіденційності, цілісності та доступності) систем та даних.
    - Хоча ці **компоненти** підвищують безпеку середовища, вони також збільшують витрати.
    - Їх вартість також підлягає оптимізації.

    Приклади додаткових витрат на безпеку:
    - Обчислювальні ресурси, та мережева сегментація даних для ізоляції, що іноді передбачає запуск окремих екземплярів, запобігання спільному розміщенню та зниження щільності.
    - Спеціалізовані засоби спостереження, такі як SIEM, здатні здійснювати агрегацію та аналіз загроз.
    - Спеціалізовані мережеві пристрої або функції, такі як брандмауери або засоби запобігання розподіленим атакам типу "відмова в обслуговуванні" (DDoS).
    - Засоби класифікації даних, необхідні для визначення рівня конфіденційності та типів інформації.
    - Спеціалізовані сховища або обчислювальні можливості для підтримки шифрування даних в стані спокою та під час передачі, наприклад, апаратний модуль безпеки (HSM) або функції конфіденційних обчислень.

- Окремі тестові середовища та інструменти тестування для перевірки функціонування засобів безпеки та виявлення раніше невиявлених прогалин у їхньому охопленні.
- Ці елементи часто також існують за межами виробничого середовища, в ресурсах попереднього виробництва та відновлення після аварій.

❖ **Підвищений попит на інфраструктуру**

Оптимізація витрат:

- Оптимізація витрат має на меті зменшення попиту на ресурси для використання більш дешевих SKU (Stock Keeping Unit - унікальний код, який використовується для ідентифікації товару в системі інвентаризації), меншої кількості екземплярів або зниження споживання.

Безпека vs. Витрати:

- Преміум-SKU: Деякі заходи безпеки в хмарних та сервісах постачальників, які можуть покращити стан безпеки **системи**, можуть бути доступні лише в дорожчих SKU або рівнях.
- Зберігання журналів: Моніторинг безпеки високої точності та дані аудиту, що забезпечують широке охоплення, збільшують витрати на зберігання. Дані спостереження за безпекою також часто зберігаються протягом більш тривалого періоду, ніж це потрібно для звичайного оперативного аналізу.
- Збільшене споживання ресурсів: Вбудовані та локальні засоби безпеки можуть призвести до додаткової потреби в ресурсах. Шифрування даних в стані спокою та під час передачі також може збільшити попит. Обидва сценарії можуть потребувати більшої кількості екземплярів або більших SKU.

❖ **Підвищені витрати на процеси та експлуатацію**

Загальна вартість володіння:

- Витрати на робочі процеси персоналу є частиною загальної вартості володіння **системою** та враховуються при розрахунку рентабельності інвестицій. Оптимізація цих витрат є рекомендацією стовпа "Оптимізація витрат".

Безпека vs. Витрати:

- Більш комплексний та суворий режим управління патчами призводить до збільшення часу та коштів, витрачених на ці рутинні завдання. Це збільшення часто поєднується з очікуванням інвестування в готовність до позапланового застосування патчів для усунення вразливостей нульового дня.
- Суворіший контроль доступу для зниження ризику несанкціонованого доступу може призвести до більш складного управління користувачами та оперативного доступу.
- Навчання та обізнаність щодо інструментів та процесів безпеки займають час працівників, а також
- Витрати на матеріали, інструкторів та, можливо, навчальні середовища.
- Дотримання нормативних актів може потребувати додаткових інвестицій в аудит та генерацію звітів про відповідність.
- Планування та проведення навчань з реагування на інциденти безпеки потребує часу.
- Необхідно виділити час для проектування та виконання рутинних та позапланових процесів, пов'язаних з безпекою, таких як ротація ключів або сертифікатів.
- Перевірка безпеки SDLC зазвичай потребує спеціальних інструментів. Вашій організації може знадобитися платити за ці інструменти.
- Приоритизація та усунення проблем, виявлених під час тестування, також займають час.
- Залучення сторонніх фахівців з безпеки для проведення "білого" тестування або тестування, яке проводиться без знання внутрішньої роботи системи (іноді відомого як "чорне" тестування), включаючи тестування на проникнення, призводить до додаткових витрат.

➢ **Компроміси безпеки з операційною досконалістю**

❖ **Ускладнення прозорості та зручності обслуговування.**

Операційна досконалість:

Архітектура системи повинна бути легко обслуговуваною та мати належний рівень спостереження.

Найбільш зручними для обслуговування є **архітектури**, які максимально прозорі для всіх залучених осіб.

Безпека vs. прозорість:

Безпека залежить від детального ведення журналів, яке забезпечує високоточний аналіз **системи** для оповіщення про відхилення від базових показників та реагування на інциденти.

Ці журнали можуть генерувати значний обсяг даних, що може ускладнити отримання інформації, спрямованої на надійність або продуктивність.

Відповідність та конфіденційність:

При дотриманні керівних принципів відповідності щодо маскування даних певні фрагменти журналів або навіть великі обсяги табличних даних редагуються для захисту конфіденційності.

Команді необхідно оцінити, як цей пробіл у спостереженні може вплинути на оповіщення або перешкодити реагуванню на інциденти.

Сегментація та складність:

Надійна сегментація ресурсів збільшує складність спостереження, оскільки для захоплення трафіку потрібне додаткове розподілене трасування та кореляція між службами.

Сегментація також збільшує площу обчислювальних ресурсів та даних, які необхідно обслуговувати.

Контроль доступу та реагування на інциденти:

Деякі засоби безпеки за задумом обмежують доступ. Під час реагування на інциденти ці засоби можуть уповільнити екстрений доступ операторів **системи**.

Тому плани реагування на інциденти повинні більшою мірою робити акцент на плануванні та навчаннях для досягнення прийнятної ефективності.

❖ **Зниження швидкості та підвищення складності**

Гнучкість розробки:

Команди, що відповідають за **систему**, оцінюють її швидкість, щоб з часом покращувати якість, частоту та ефективність процесів доставки.

Складність **системи** впливає на зусилля та ризики, пов'язані з її експлуатацією.

Зміна та безпека:
Суворіший контроль змін та політика їх затвердження для зниження ризику появи вразливостей безпеки можуть уповільнити розробку та безпечне розгортання нових функцій.
Однак очікування щодо оновлень безпеки та застосування патчів може збільшити потребу в частіших розгортаннях.
Крім того, політика затвердження людьми в операційних процесах може ускладнити автоматизацію цих процесів.
Тестування безпеки:
Результати тестування безпеки можуть містити висновки, які потребують пріоритезації, що може блокувати заплановану роботу.
Ведення журналів та автоматизація:
Рутинні, позапланові та аварійні процеси можуть потребувати ведення журналів аудиту для дотримання вимог відповідності.
Це ведення журналів робить виконання процесів більш жорстким.
Керування користувачами та автоматизація:
Команди, що відповідають за **систему**, можуть збільшити складність керування користувачами зі зростанням деталізації визначення та призначення ролей.
Збільшення кількості рутинних операційних завдань, пов'язаних із безпекою, наприклад, керування сертифікатами, збільшує кількість процесів для автоматизації.

- **Координація зусиль**

Операційна автономія:
Команда, яка мінімізує зовнішні контакти та перевірки, може ефективніше контролювати свої операції та графік.
Зовнішні вимоги та координація:
Зі зростанням зовнішніх вимог до відповідності від більшої організації або від зовнішніх організацій також зростає складність досягнення та доведення відповідності аудиторам.
Спеціальні навички та координація:
Безпека потребує спеціальних навичок, яких зазвичай немає у команд, що відповідають за **систему**.
Ці навички часто отримують від більшої організації або від третіх сторін.
У обох випадках необхідно налагодити координацію зусиль, доступу та відповідальності.
Плани реагування на інциденти та координація:
Вимоги відповідності або організаційні вимоги часто потребують планів чіткої комунікації для відповідального розкриття порушень.
Ці плани повинні бути включені в координацію зусиль з забезпечення безпеки.

- **Компроміси безпеки з ефективністю продуктивності**
  - **Затримка та накладні витрати**

Ефективність продуктивності:
Система повинна працювати з мінімальними затримками та накладними витратами.
Безпека vs. Продуктивність:
Засоби інспекційного контролю безпеки, такі як брандмауери та фільтри вмісту, розміщуються в потоках, які вони захищають.
Тому ці потоки підлягають додатковій перевірці, що збільшує затримку запитів.
Керування доступом:
Кожен виклик керованого компонента потребує явної перевірки за допомогою засобів контролю ідентифікації.
Ця перевірка споживає обчислювальні цикли та може потребувати мережевого з'єднання для авторизації.
Шифрування:
Шифрування та розшифрування потребують виділених обчислювальних циклів.
Ці цикли збільшують час та ресурси, які споживаються цими потоками.
Це збільшення, як правило, корелюється зі складністю алгоритму та генерацією високоентропійних та різноманітних ініціалізаційних векторів (IV).
Ведення журналів:
Зі зростанням обсягу ведення журналів може також збільшуватися вплив на системні ресурси та пропускну здатність мережі для потокового передавання цих журналів.
Сегментація ресурсів:
Сегментація ресурсів часто призводить до додаткових мережевих переходів в архітектурі **системи**.

- **Збільшення ризику неправильної конфігурації**

Надійність продуктивності:
Стабільне досягнення цілей продуктивності залежить від передбачуваної реалізації проекту.
Безпека vs. Конфігурація:
Неправильна конфігурація або надмірне застосування засобів безпеки може вплинути на продуктивність через неефективну конфігурацію.
Ось деякі приклади конфігурацій засобів безпеки, які можуть вплинути на продуктивність:
Порядок, складність та кількість правил брандмауера (гранулярність).
Відсутність виключення ключових файлів з моніторів цілісності файлів або антивірусів.
Ігнорування цього кроку може призвести до конфліктів блокування.
Включення веб-брандмауерів для глибокої інспекції пакетів для мов або платформ, які не є релевантними для компонентів, що захищаються.

Висновки.

У сучасному світі кіберзагрози стають дедалі більш витонченими та небезпечними. Організаціям усіх розмірів важливо мати надійні системи безпеки для виявлення та реагування на ці загрози. Моніторинг є ключовим компонентом будь-якої стратегії кібербезпеки, оскільки він дозволяє організаціям відстежувати свою мережу та системи на наявність ознак компрометації.

- Системний та мережевий моніторинг може використовуватися для виявлення вторгнень, зламів та інших загроз безпеці.
- Аналіз журналів може допомогти виявити аномалії та патерни, пов'язані із зловмисними діями.
- Розробка стратегій реагування та відновлення є важливою для мінімізації впливу успішної кібератаки.
- Компроміси безпеки можуть мати серйозні наслідки для організацій, включаючи фінансові втрати, шкоду репутації та перерви в роботі.

SNM. #3. Інструменти моніторингу та аналізу даних ***

Системний *та мережевий моніторинг. Лекція #8. Застосування моніторингу для виявлення загроз безпеці.*

Моніторинг є важливим інструментом для виявлення та реагування на кіберзагрози. Організації повинні впровадити комплексні стратегії моніторингу, які включають системний та мережевий моніторинг, аналіз журналів та розробку планів реагування та відновлення.

- Інвестуйте в рішення для моніторингу безпеки, які відповідають вашим потребам.
- Налаштуйте свої системи моніторингу для виявлення підозрілої активності.
- Регулярно переглядайте свої журнали та шукайте аномалії.
- Розробіть план реагування на інциденти та регулярно його тестуйте.
- Підтримуйте свої системи та програмне забезпечення в актуальному стані.

Моніторинг - це не одноразова подія. Це постійний процес, який потребує постійної уваги та вдосконалення. Організації, які серйозно ставляться до кібербезпеки, повинні зробити моніторинг пріоритетом.