SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #6. Аналіз та візуалізація даних мережевого моніторингу..*

План лекції . Тема 6. Аналіз та візуалізація даних мережевого моніторингу.

- Методи аналізу даних мережевого моніторингу та їх застосування для виявлення аномалій та проблем в мережі.
- Типові інструменти мережевого моніторингу
- Використання інструментів візуалізації даних для створення графіків, діаграм та звітів.
- Розробка звітів та дашбордів для ефективного моніторингу мережі..

Вступ.

Моніторинг мережі — це використання системи, яка постійно відстежує комп'ютерну мережу на наявність повільних або несправних компонентів і сповіщає адміністратора мережі (через електронну пошту , SMS або інші сигнали тривоги) у разі збоїв або інших проблем. Моніторинг мережі є частиною керування мережею .

Сучасна мережева інфраструктура зростає в розмірах і складності з кожним днем. Збільшення обсягів даних, різноманіття платформ і сервісів, а також зростання кількості користувачів ставлять перед адміністраторами мережі низку викликів. Одним з ключових інструментів для ефективного управління та забезпечення надійності мережі є мережевий моніторинг. Але просто збирати дані не достатньо. Не менш важливо аналізувати ці дані для виявлення аномалій, проблем, а також для прогнозування та усунення можливих ризиків.

Сьогодні ми розглянемо методи аналізу даних мережевого моніторингу та їх застосування для виявлення аномалій та проблем в мережі. Також поговоримо про використання інструментів візуалізації даних для створення графіків, діаграм та звітів, які дозволяють нам краще зрозуміти стан мережі та вчасно реагувати на будь-які зміни.
Поглибивши розуміння методів аналізу та візуалізації даних мережевого моніторингу, ми зможемо забезпечити більш ефективне управління та надійність мережі, що є критично важливим у сучасному світі цифрових технологій.

Методи аналізу даних мережевого моніторингу та їх застосування для виявлення аномалій та проблем в мережі.

Мережевий моніторинг - важливий елемент для забезпечення стабільності, продуктивності та безпеки вашої мережі:

- **Виявлення кіберзагроз та злочинної діяльності.** Дозволяє виявляти кіберзагрози та злочинну діяльність, такі як вторгнення, спам, фішинг та інші. Це допомагає запобігти можливим кібератакам та захистити мережу від шкідливих дій.

- **Підвищення ефективності мережі.** Дозволяє знайти проблеми з пропускною здатністю, визначити трафік, який споживає більше ресурсів мережі, та забезпечити оптимальне використання ресурсів мережі.

- **Відновлення роботи мережі.** Може допомогти відновити роботу мережі після виникнення проблем, таких як відмова обладнання чи програмного забезпечення.

- **Покращення безпеки мережі.** Може допомогти виявити вразливості в мережі та допомогти виправити їх, щоб уникнути можливих кібератак.

- **Підтримка рішень.** Може допомогти приймати обґрунтовані рішення щодо конфігурації мережі, вибору обладнання та відповідності вимогам безпеки.

Чому моніторинг мережі важливий для бізнесу?

Мережевий моніторинг **(NM)** має вирішальне значення з кількох причин. Це важливий компонент керування мережею, що дозволяє організаціям оптимізувати продуктивність мережі, мінімізувати час простою та забезпечити безпеку та відповідність своїх мереж.
NM особливо важливий для бізнесу, який займається належним функціонуванням своєї мережі та покладається на хмарні програми, веб-сервіси Інтернету або критичні програми, які здійснюють транзакції через мережу. NM обов'язковий для підприємств із мережами MPLS і SD-WAN і кількома інтернет-ланцюгами та з'єднаннями.

Ось кілька ключових причин, чому моніторинг мережі важливий для бізнесу:

1. **Підвищення продуктивності мережі:** NM є важливим для підтримки високопродуктивної мережі - це головна причина. Це дозволяє виявляти та усувати проблеми для покращення продуктивності мережі .
2. **Завчасне виявлення проблеми з мережею:** проблеми з мережею, як проблеми з доступністю мережі , так і проблеми з продуктивністю, можуть траплятися і трапляються, і вони можуть мати значний вплив на роботу. Тому важливо завчасно виявляти всі проблеми з мережею, перш ніж вони спричинять хаос:
   - ✓ **Проблеми з доступністю:** проблеми з доступністю характеризуються повною втратою з'єднання. Ці типи збоїв у мережі можуть бути спричинені різними факторами, зокрема фізичними пошкодженнями мережевої інфраструктури, обривами оптоволокна та перебоями в електропостачанні. Хоча проблеми з доступністю є поганою новиною для надійності мережі , їх найпростіше визначити та усунути.
   - ✓ **Проблеми з продуктивністю:** проблеми з продуктивністю мережі важче виявити та усунути, ніж проблеми з доступністю. Мережа функціонує менш ефективно, ніж очікувалося або потрібно. Це може включати в себе затримки в передачі даних, втрату пакетів, низьку швидкість передачі, або будь-які інші обмеження, які впливають на продуктивність і ефективність мережі.Ці збої можуть бути постійними або періодичними, причому останні є найважчими для виявлення та усунення несправностей. Проблеми з продуктивністю можуть виникнути будь-де, і вони можуть залишатися непоміченими роками.

3. **Оптимізація взаємодії з кінцевим користувачем:** відстежується робота кінцевого користувача під час використання мережевих програм і служб, а також завчасно виявляються та усуваються проблеми з мережею, перш ніж вони розчарують користувачів.
   - ✓ **Швидше вирішуються проблеми кінцевих користувачів**
   - ✓ **Підвищується рівень задоволеності кінцевих користувачів**

4. **Підвищення безпеки мережі:** підвищення безпеки мережі шляхом виявлення потенційних загроз безпеці, таких як незвичайна мережева активність або спроби неавторизованого доступу.

- ✓ **Виявлення потенційних порушенньь безпеки**
- ✓ **Зведення до мінімуму ризику втрати даних**
- ✓ **Поліпшення дотримання галузевих стандартів і правил**

5. **Планування пропускної здатності та оптимізація мережі**. Аналізуючи мережевий трафік і використання ресурсів, мережеві адміністратори можуть визначити потенційні вузькі місця для:
   - ✓ **Планування оновлення потужностей для підтримки майбутнього зростання**
   - ✓ **Оптимізації продуктивності мережі для задоволення зростаючих вимог**
   - ✓ **Зменшення витрат на інфраструктуру в майбутньому**

6. **Зниження витрат і покращення рентабельності інвестицій:** моніторинг мережі може допомогти знизити витрати та покращити рентабельність інвестицій шляхом виявлення неефективності та оптимізації мережевих ресурсів.
   - ✓ Визначення місць з **надмірним або недостатнім використанням ресурсів** і внесення коректив.
   - ✓ **Підвищення рентабельності інвестицій**, забезпечивши максимальну продуктивність мережі, що може підвищити продуктивність і задоволеність користувачів.
   - ✓ **Зменшення витрат, пов'язаних з простоєм мережі** та незапланованими відключеннями.

7. **Підвищення безперервності бізнесу:** нарешті, покращення продуктивності мережі (і взаємодії з користувачем) призведе до загального позитивного впливу на бізнес.
   - ✓ **Мінімізується час простою та збої в обслуговуванні**, що впливають на продуктивність
   - ✓ **Зменшиться кількість збоїв мережі** та проблем із продуктивністю, які можуть коштувати часу та грошей підприємствам
   - ✓ **Швидко вирішуватимуться проблеми з мережею**, не потребуючи додаткових IT-ресурсів

Основні завдання мережевого моніторингу

- **Аналіз трафіку (Traffic Analysis).** Інструменти мережевого моніторингу збирають і аналізують дані про мережевий трафік, включаючи обсяг даних, типи трафіку (наприклад, Інтернет, електронна пошта, відео), а також джерела та призначення трафіку. Це допомагає визначити шаблони та аномалії, які можуть вплинути на продуктивність мережі.

- **Вимірювання затримки (Latency measurement).** Затримка означає затримку передачі даних через мережу. Відстеження затримки допомагає забезпечити швидку передачу даних без значних затримок, що особливо важливо для додатків у реальному часі, таких як відеоконференції та онлайн-ігри.

- **Втрата пакетів (Packet Loss).** Втрата пакетів відбувається, коли пакети даних скидаються або не досягають місця призначення. Відстеження втрати пакетів допомагає точно визначити проблеми з мережею, які можуть призвести до втрати даних і низької продуктивності програми.

- **Використання пропускної здатності (Bandwidth Utilization).** Інструменти моніторингу відстежують, як використовується пропускна здатність мережі, визначаючи, які програми чи пристрої споживають найбільшу пропускну здатність. Ця інформація є цінною для планування потужності та оптимізації мережі.

- **Справність пристрою (Device Health).** Моніторинг працездатності та стану мережевих пристроїв (маршрутизаторів, комутаторів, брандмауерів, серверів тощо) допомагає виявити проблеми з обладнанням або конфігурацією, які можуть вплинути на продуктивність мережі.

- **Безпека (Security).** Моніторинг може відігравати певну роль у безпеці мережі, відстежуючи незвичайну або підозрілу мережеву активність, яка може свідчити про порушення безпеки або кібератаку.

- **Попередження та звітування (Alerting and Reporting)**. Інструментарій моніторингу генерує сповіщення, коли перевищуються попередньо визначені порогові значення продуктивності або коли виявляються аномалії. Вони також надають звіти та інформаційні панелі, щоб допомогти мережевим адміністраторам і IT-командам візуалізувати й проаналізувати дані про продуктивність мережі.

- **Аналіз історичних даних (Historical Data Analysis).** Зберігання історичних даних про продуктивність мережі дає змогу організаціям визначати тенденції та закономірності з часом, забезпечуючи ефективніше прийняття рішень і проактивне керування мережею.

Ефективний моніторинг продуктивності мережі може призвести до кількох переваг, зокрема підвищення надійності мережі, швидшого вирішення проблем, кращого розподілу ресурсів, покращення взаємодії з користувачем та економії коштів за рахунок ефективного використання мережевих ресурсів. Це важлива практика для підтримки загальної працездатності та функціональності сучасних комп'ютерних мереж, особливо на великих підприємствах і в середовищах з інтенсивним об'ємом даних.

Перелічимо загальні методи аналізу даних мережевого моніторингу:

Таблиця 06.01.

Метод	Опис	Застосування
Прослуховування пакетів (Packet sniffing).	Метод полягає в перехопленні і аналізі мережевих пакетів, що проходять через мережеві пристрої. Інструменти, такі як Wireshark, дозволяють вам переглядати, аналізувати і фільтрувати ці пакети для виявлення аномалій, витрат ресурсів або зловмисних атак.	Перехоплення та аналіз мережевих пакетів може допомогти виявити аномальні патерни трафіку, які можуть свідчити про зловживання або атаки на мережу. Наприклад, велика кількість запитів до певного вузла чи сервісу може свідчити про DDoS-атаку.

Трошки більше конкретики про метод прослуховування пакетів (Packet sniffing) — це комп'ютерна програма або комп'ютерне обладнання , наприклад пристрій захоплення пакетів, який може аналізувати та реєструвати трафік, що проходить через комп'ютерну мережу

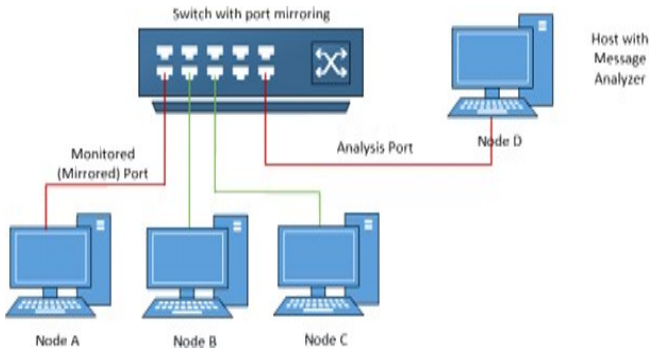
або частину мережі. Перехоплення пакетів — це процес перехоплення та реєстрації трафіку. Коли потоки даних проходять мережею, аналізатор фіксує кожен пакет і, якщо необхідно, декодує необроблені дані пакета, показуючи значення різних полів у пакеті, і аналізує його вміст відповідно до відповідних RFC або інших специфікацій.

Аналізатор пакетів, який використовується для перехоплення трафіку в бездротових мережах, називається бездротовим аналізатором або аналізатором WiFi . Хоча аналізатор пакетів також можна називати мережевим аналізатором або аналізатором протоколів, ці терміни також можуть мати інші значення. Технічно аналізатор протоколу може бути ширшим, загальнішим класом, який включає аналізатори/аналізатори пакетів і ми повернемося до цього методу аналізу даних мережевого моніторингу пізніше.

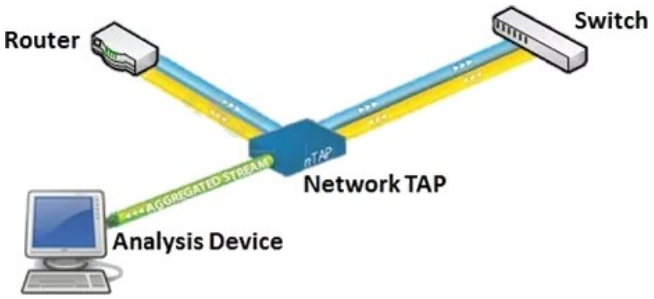
У дротових мережах, таких як Ethernet , Token Ring і FDDI , залежно від структури мережі (концентратор або комутатор), може перехопити весь трафік у мережі з однієї машини. У сучасних мережах трафік може бути захоплений за допомогою мережевого комутатора за допомогою **віддзеркалення портів** (**Port mirroring**), або за допомогою **мережевого крана** (**Network tap**), що є навіть більш надійним рішенням, ніж використання моніторингового порту для віддзеркалення портів, оскільки мережевий кран з меншою ймовірністю скидає пакети під час високого трафіку.

Прозвучало два, можливо незнайомих Вам терміни. Поясню.

Віддзеркалення портів (Port mirroring) використовується на мережевому комутаторі для надсилання копії мережевих пакетів , які бачать один порт комутатора (або весь VLAN), до з'єднання для моніторингу мережі на іншому порту комутатора. Це зазвичай використовується для мережевих пристроїв, які потребують моніторингу мережевого трафіку, наприклад системи виявлення вторгнень, пасивного зондування або технології моніторингу реального користувача (RUM), яка використовується для підтримки керування продуктивністю додатків (APM). Віддзеркалення портів на комутаторі Cisco Systems зазвичай називають аналізатором комутованих портів (SPAN) або аналізатором віддаленого комутованого порту (RSPAN). Інші постачальники мають різні назви для нього, наприклад, Roving Analysis Port (RAP) на комутаторах 3Com .



Мережевий кран (Network tap) - це система, яка відстежує події в локальній мережі. Кран зазвичай є спеціальним апаратним пристроєм, який забезпечує спосіб доступу до даних, що передаються через комп'ютерну мережу . Мережевий кран має (принаймні) три порти: порт A , порт B і порт монітора . Кран, вставлений між A і B, пропускає весь трафік (вхідний та вихідний потоки даних) безперешкодно в режимі реального часу, але також копіює ті самі дані на порт свого монітора, дозволяючи третій стороні слухати.



Мережеві крани у деяких джерелах мають назву мережеві відводи, зазвичай використовуються для систем виявлення вторгнень у мережу, запису VoIP, мережевого зондування, аналізаторів пакетів та інших пристроїв моніторингу та збору та програмного забезпечення, яким потрібен доступ до сегмента мережі. Мережеві крани використовуються в програмах безпеки, тому що вони ненав'язливі, не виявляються в мережі (не мають фізичної чи логічної адреси).

У бездротових локальних мережах трафік можна захоплювати по одному каналу за раз або за допомогою кількох адаптерів по кількох каналах одночасно. Зрозуміло, що 100% трафіку у таких мережах захопити проблематично, хоча теоретично можливо.

У дротових широкомовних і бездротових локальних мережах для захоплення одноадресного трафіку між іншими машинами мережевий адаптер , який захоплює трафік, має бути в безладному режимі (promiscuous mode).

У комп'ютерних мережах безладний режим (promiscuous mode) — це режим для контролера інтерфейсу дротової мережі (NIC) або контролера інтерфейсу бездротової мережі (WNIC), який змушує контролер пропускати весь трафік, який він отримує, до центрального процесора (CPU), а не пропускати лише кадри. на отримання яких контролер спеціально запрограмований.

У бездротових локальних мережах, навіть якщо адаптер працює в безладному режимі (promiscuous mode), пакети, які не відповідають набору послуг, для якого налаштовано адаптер, зазвичай ігноруються. Щоб побачити ці пакети, адаптер має бути в режимі моніторингу. Не потрібно ніяких спеціальних налаштувань для захоплення багатоадресного трафіку до групи багатоадресної розсилки, або широкомовного трафіку.

Під час захоплення трафіку записується або весь вміст пакетів, або лише заголовки . Запис лише заголовків зменшує вимоги до пам'яті та дозволяє уникнути деяких юридичних проблем щодо конфіденційності, але часто надає достатньо інформації для діагностики проблем.

Зібрана інформація декодується з необробленої цифрової форми в формат, зрозумілий людині, що дозволяє переглянути інформацію обміну. Аналізатори протоколів відрізняються за своїми можливостями відображення та аналізу даних.

Деякі аналізатори протоколів також можуть генерувати трафік. Вони можуть виконувати функції тестувальників протоколів. Такі тестери генерують трафік з правильним протоколом для функціонального тестування, а також можуть мати можливість навмисно вводити помилки, щоб перевірити здатність тестованого пристрою обробляти помилки.

Аналізатори протоколів також можуть бути апаратними у форматі зонда, або, що більш поширене, у поєднанні з дисковим масивом. Ці пристрої записують пакети або заголовки пакетів на дисковий масив. Перелічувати їх – нудна справа, згадаю лише всім Вам знайомий Wireshark.

Наступні методи аналізу даних мережевого моніторингу це:

Таблиця 06.01. Продовження.

Метод	Опис	Застосування
Протокольний аналіз (Protocol Analysis).	Аналіз структури та змісту мережевих протоколів для виявлення аномалій або проблем у спілкуванні між пристроями. Це включає в себе перевірку правильності даних, обмінюваних між пристроями, та виявлення будь-яких відхилень від стандартів.	Шляхом аналізу мережевих протоколів можна виявити аномальні зміни в структурі або змісті пакетів, що можуть вказувати на потенційні проблеми в мережі, такі як несправності обладнання або атаки.
Аналіз трафіку (Traffic Analysis).	Аналіз трафіку передбачає вивчення та аналіз мережевого трафіку для виявлення та діагностики проблем, пов'язаних із продуктивністю мережі, безпекою та відповідністю. Він передбачає моніторинг і аналіз потоку пакетів даних у мережі, обсягу, швидкості та напрямку мережевого трафіку для виявлення потенційних вузьких місць, перевантажень та інших проблем із продуктивністю, які можуть вплинути на продуктивність мережі. Аналіз трафіку може включати аналіз таких показників, як використання пропускної здатності, втрату пакетів, затримку та пропускну здатність. Метод дозволяє виявляти зміни в патернах трафіку, незвичайні обсяги або швидкості, а також потенційні точки перенапруження.	Моніторинг обсягу, швидкості та напрямку трафіку дозволяє виявляти аномальні збільшення чи зменшення трафіку, що можуть бути наслідком проблем у мережі або зловмисних дій.
Виявлення зловмисних дій (Intrusion Detection).	Використання спеціалізованих систем виявлення вторгнень (IDS) або систем виявлення вразливостей (Vulnerability Detection Systems) для виявлення незвичайної або потенційно шкідливої активності в мережі.	Системи виявлення вторгнень використовуються для пошуку підозрілих дій або патернів, які можуть свідчити про зловмисні атаки в мережі, такі як намагання несанкціонованого доступу до системи чи ресурсів.

Трошки більше конкретики про метод виявлення зловмисних дій (Intrusion Detection) — це пристрій або програмне забезпечення, яке відстежує мережу чи системи на наявність зловмисної активності чи порушень політики. Інформація про будь-яке вторгнення або порушення зазвичай повідомляється адміністратору або збирається централізовано за допомогою системи керування інформацією та подіями безпеки (SIEM) . Система SIEM поєднує вихідні дані з кількох джерел і використовує методи фільтрації критичних та некритичних подій, щоб відрізнити зловмисну активність від помилкових спрацювань.

Типи **Intrusion Detection** варіюються від окремих комп'ютерів до великих мереж.

IDS можна класифікувати за місцем виявлення (мережа чи хост) або методом виявлення, який використовується (сигнатурний або на основі аномалії).

<u>За місцем виявлення класифікація наступна:</u>

Найпоширенішими класифікаціями є системи виявлення вторгнень у мережу (NIDS) і системи виявлення вторгнень на основі хосту (HIDS). Система, яка відстежує важливі файли операційної системи, є прикладом HIDS, тоді як система, яка аналізує вхідний мережевий трафік, є прикладом NIDS.

- **Системи виявлення мережевих вторгнень (NIDS)** розміщуються в стратегічній точці або точках у мережі для моніторингу трафіку до та від усіх пристроїв у мережі. NIDS виконує аналіз трафіку, що проходить у всій підмережі , і зіставляє трафік, який передається підмережами, з бібліотекою відомих атак. Після виявлення атаки або виявлення ненормальної поведінки надсилається сповіщення. Прикладом NIDS може бути встановлення його в підмережі, де розташовані брандмауери, щоб побачити, чи хтось намагається зламати брандмауер. В ідеалі можна сканувати весь вхідний і вихідний трафік, однак це може створити вузьке місце, яке погіршить загальну швидкість мережі. OPNET і NetSim є широко використовуваними інструментами для імітації мережевих систем виявлення вторгнень. Системи NID також здатні порівнювати сигнатури подібних пакетів, щоб зв'язувати та видаляти виявлені шкідливі пакети, які мають підпис, що відповідає записам у NIDS. Коли ми класифікуємо дизайн NIDS відповідно до властивості інтерактивності системи, існує два типи: он-лайн і офлайн NIDS, які часто називають вбудованим і кран-режимом відповідно. Он-лайн NIDS працює з мережею в режимі реального часу та аналізує пакети Ethernet і застосовує деякі правила, щоб вирішити, чи це атака чи ні. Off-line NIDS працює зі збереженими даними та пропускає їх через аналітичні процеси для визначення атаки.

- **Системи виявлення вторгнень (HIDS)** працюють на окремих хостах або пристроях у мережі. HIDS відстежує вхідні та вихідні пакети лише з пристрою та сповіщатиме користувача або адміністратора, якщо буде виявлено підозрілу активність. Він робить знімок існуючих системних файлів і порівнює його з попереднім знімком. Якщо критичні системні файли були змінені або видалені, сповіщення надсилається адміністратору для дослідження. Приклад використання HIDS можна побачити на критично важливих машинах, на яких не очікується зміна конфігурацій.

<u>За методом виявлення аномалій існує наступна класифікація:</u>

Класифікація IDS за методом виявлення:

- ✓ виявлення на основі сигнатур (розпізнавання поганих шаблонів, наприклад шкідливих програм).
- ✓ виявлення на основі аномалій (виявлення відхилень від моделі «хорошого» трафіку, яка часто покладається на машинне навчання).
- ✓ виявлення на основі репутації (розпізнавання потенційної загрози за балами репутації) Цей клас фактично є підкласом виявлення на основі аномалій. .

Трошки детальніше про цю класифікацію:

- **На основі підпису**, або друга назва — **IDS на основі сигнатур** — це виявлення атак шляхом пошуку певних шаблонів, наприклад послідовностей байтів у мережевому трафіку або відомих зловмисних інструкцій, які використовуються шкідливим програмним забезпеченням. Ця технологія та термінологія походить від антивірусного програмного забезпечення , яке називає ці виявлені шаблони сигнатурами. Хоча IDS на основі сигнатур може легко виявити відомі атаки, важко виявити нові атаки, для яких відсутні шаблони.

- **Системи виявлення вторгнень на основі аномалій** були введені в першу чергу для виявлення невідомих атак, частково через швидкий розвиток шкідливого програмного забезпечення. Основний підхід полягає у використанні машинного навчання для створення моделі надійної діяльності, а потім порівняння нової поведінки з цією моделлю. Оскільки ці моделі можна навчити відповідно до програм і апаратних конфігурацій, метод на основі машинного навчання має кращу узагальнену властивість порівняно з традиційними IDS на основі підпису. Хоча цей підхід дозволяє виявляти раніше невідомі атаки, він дає доволі високий відсоток хибних спрацьовувань: раніше невідомі законні дії можуть бути класифіковані як зловмисні. Більшість існуючих IDS страждають від того, що процес виявлення займає багато часу, що погіршує продуктивність IDS. Ефективний алгоритм вибору ознак робить процес класифікації, що використовується для виявлення, більш надійним.

На майбутнє, як перспективні теми для обрання дипломної роботи – зверніть увагу на клас безкоштовних систем виявлення атак (англ. Intrusion Detection System, IDS) для захисту MS AD та іншої інфраструктури. Найбільш перспективні в цьому плані:

- **Suricata** є відкритою і доступною для безкоштовного використання - ліцензія GPLv2. Основні характеристики Suricata включають:
  - ***Швидкість та масштабованість.*** Побудована для ефективної обробки великого обсягу мережевого трафіку та може використовувати багатопоточність для оптимізації продуктивності на системах з багатьма ядрами.
  - ***Підтримка великої кількості протоколів.*** Розпізнає і аналізує різні мережеві протоколи, включаючи TCP, UDP, ICMP, IPv4, IPv6, HTTP, TLS, DNS і багато інших.
  - ***Підтримка правил для виявлення загроз.*** Використовує мову правил для виявлення аномального або підозрілого мережевого трафіку. Ці правила можуть бути розроблені спільнотою або створені користувачем, враховуючи конкретні потреби мережі.
  - **Багатофункціональність і логування.** Забезпечує широкі можливості логування подій, які можуть бути використані для аналізу та виявлення потенційних загроз.
  - ***Оптимізація для використання в хмарних середовищах***. Легко інтегрується з хмарними платформами, що робить інтсурмент практичним для застосування в різноманітних хмарних і гібридних середовищах.

- **Splunk** це платформа для аналізу та моніторингу даних у реальному часі. Використовує ліцензію, яка базується на обсязі оброблених даних (дані, які імпортуються та обробляються Splunk). Це може бути обмеження обсягу даних на день або на місяць, в залежності від типу ліцензії (Free, Enterprise, Cloud, тощо). Основні характеристики та напрямки використання Splunk включають:
  - ***Збір та індексація даних***. Збирає дані з різноманітних джерел, включаючи журнали подій, тексти логів, дані метрик та інші джерела. Після цього він індексує ці дані, щоб забезпечити швидкий пошук та аналіз.
  - ***Пошук та аналіз даних***. Має потужний інтерфейс для пошуку, фільтрації та аналізу даних. Користувачі можуть використовувати власні запити та доповнення для вивчення великих обсягів даних.
  - ***Візуалізація даних.*** Дозволяє створювати графіки, діаграми та інші візуальні елементи для представлення результатів аналізу даних.
  - ***Моніторинг безпеки***. Може використовуватися для моніторингу та виявлення інцидентів безпеки. Здатен агрегувати дані з різних джерел, що дозволяє виявляти аномалії та потенційні загрози.
  - ***Моніторинг та аналіз Active Directory***. Використовується для моніторингу та аналізу подій у середовищі Active Directory та може агрегувати дані з лог-файлів AD та інших джерел для виявлення аномалій, атак та інших проблем.
  - ***Дозволяє налаштовувати запити та дашборди*** відповідно до конкретних потреб користувача, забезпечуючи гнучкість та масштабованість для різних використань, включаючи моніторинг та захист Active Directory.

- **ELK Stack (Elasticsearch, Logstash, Kibana)** це набір відкритих інструментів для агрегації, аналізу та візуалізації лог-файлів та інших даних. Функціонал та напрямки використання ELK Stack:
  - ***Elasticsearch функціонал:***
    - ***Пошук та індексація:*** використовує механізм індексації, щоб швидко забезпечити пошук та аналіз даних.
    - ***Розподілена архітектура:*** забезпечує розподілену обробку та зберігання даних для масштабованості.
    - ***RESTful API:*** надає простий RESTful API для запитів до даних та використання власних додатків.
  - ***Elasticsearch напрямок використання:***
    - ***Пошук та аналіз лог-файлів***: використовується для швидкого та ефективного пошуку лог-файлів та інших даних.
    - ***Моніторинг та аналіз продуктивност***і: використовується для моніторингу систем, мереж та інших аспектів продуктивності.
  - ***Logstash функціонал:***
    - Потоковий обробник даних: Logstash призначений для обробки, трансформації та вивантаження даних.
    - Підтримка різних входів та виходів: Підтримує велику кількість вхідних джерел даних та можливостей виведення.
  - ***Напрямок використання Logstash:***
    - ***Збір та нормалізація лог-файлів***: Logstash дозволяє збирати дані з різних джерел та нормалізувати їх для подальшого аналізу.
    - ***Передавання даних в Elasticsearch***: Logstash інтегрується з Elasticsearch, щоб ефективно пересилати оброблені дані для індексації.
  - ***Kibana. Функціонал:***
    - Візуалізація даних: Kibana дозволяє створювати графіки, діаграми та інші візуальні елементи на основі даних в Elasticsearch.
    - Дашборди та звіти: Надає можливості створення і керування дашбордами для моніторингу та аналізу даних.
  - ***Напрямок використання Kibana:***
    - ***Моніторинг та аналіз лог-файлів***: Kibana є потужним інструментом для вивчення лог-даних та створення звітів.
    - ***Візуалізація даних безпеки***: Використовується для відображення статистики та графіків, пов'язаних з безпекою, такими як аналіз входів/виходів, аномалії та інше.
  - ***IDS в MS AD з ELK Stack:***
    - ELK Stack може ефективно використовуватися для виявлення інтрузій у середовищі Active Directory. Logstash може збирати та нормалізувати журнали подій AD, а потім передавати їх до Elasticsearch для індексації. Kibana дозволяє створювати дашборди та візуалізації для моніторингу безпеки, виявлення аномалій та аналізу подій. ELK Stack може бути налаштований для інтеграції з різними іншими інструментами безпеки та IDS, що робить його ефективним для цілей безпеки в AD.

- **Snort** це система виявлення і запобігання інтрузійним діям (Intrusion Detection and Prevention System, IDS/IPS), що використовується для моніторингу та аналізу мережевого трафіку з метою виявлення потенційних загроз безпеці та розповсюджується під GNU General Public License (GPL)
  - Snort може бути успішно використаний для виявлення атак та моніторингу безпеки в середовищі Active Directory (AD). Він аналізує мережевий трафік і виявляє потенційно шкідливі або небезпечні дії.
  - Щоб налаштувати Snort для роботи з AD, вам слід визначити специфічні правила для виявлення аномалій та загроз, що можуть виникнути в середовищі AD, хоча існують і набори шаблонів визначення правил.
  - Використання Snort у поєднанні з іншими інструментами аналізу та збору лог-файлів може забезпечити комплексний підхід до моніторингу та захисту AD.
  - Популярний та ефективний інструмент для IDS/IPS та моніторингу безпеки Відкрита ліцензія робить Snort доступним для різних типів організацій, включаючи ті, які використовують середовище Active Directory.

Наступні методи аналізу даних мережевого моніторингу це:

Таблиця 06.01. Продовження.

Метод	Опис	Застосування
Побудова та аналіз графіків (Graph Analysis).	Використання графіків для візуалізації зв'язків між різними мережевими вузлами та їх активністю. Це може допомогти виявити аномальні мережеві зв'язки або патерни спілкування.	Дозволяє візуалізувати зв'язки між мережевими вузлами та активністю. Наприклад, зміни в графіку можуть вказувати на аномальні зв'язки між вузлами, що може свідчити про атаки або несправності.
Моделювання мережі (Network Modeling).	Використання математичних моделей для аналізу різних аспектів мережі, таких як її структура, пропускна здатність та вразливості. Це дозволяє прогнозувати поведінку мережі та виявляти можливі проблеми заздалегідь.	Дозволяє створити математичні моделі її структури, пропускної здатності та поведінки. Ці моделі можуть використовуватися для симуляції різних сценаріїв та виявлення можливих проблем або вразливостей. Наприклад, можна моделювати вплив відмови певних вузлів чи ліній на загальну пропускну здатність мережі або виявити точки перенапруження.
Статистичний аналіз (Statistical Analysis).	Використання статистичних методів для виявлення патернів, аномалій або важливих змін в мережевих даних. Це може включати аналіз розподілу даних, кореляційні аналізи та інші методи.	Застосування статистичних методів дозволяє виявляти аномалії у мережевих даних на основі їх розподілу, кореляцій та інших параметрів.
Історичний аналіз даних про продуктивність мережі (Historical analysis of NPD).	Аналіз історичних даних є ключовим компонентом у вирішенні минулих проблем із продуктивністю мережі, особливо періодичних. Він передбачає збір і аналіз історичних даних продуктивності за певний період часу для виявлення тенденцій і закономірностей, пов'язаних з продуктивністю мережі.	Дані історичного аналізу можуть бути використані для виявлення закономірностей і тенденцій, пов'язаних з продуктивністю мережі, таких як зміни в моделях трафіку, періоди пікового використання та повторювані або періодичні проблеми. Це також дозволяє IT-командам вирішувати проблеми, які виникли в минулому, а також передбачати майбутні проблеми з продуктивністю мережі та планувати оновлення потужності або інші покращення мережі.
Відображення топології мережі (Network topology display)	Відображення топології мережі забезпечує створення та підтримку карти або діаграми, яка представляє фізичне та логічне розташування мережі. Відображення топології мережі дає можливість IT-командам візуалізувати та розуміти зв'язки між мережевими засобами, програмами та користувачами, що може допомогти IT-командам виявити поточні проблеми з продуктивною мережею, загрози безпеки та ризики відповідальності.	Після створення карти топології мережі IT-спеціалісти можуть використовувати її для виявлення продуктивності наявних вузьких місць, таких як перевантажені комутатори або маршрутизатори, і для оптимізації продуктивності мережі.
Моніторинг продуктивності додатків (Application Performance Monitoring) (APM)	Моніторинг продуктивності додатків (APM) зосереджується на моніторингу та аналізі продуктивності конкретних програм, що працюють у мережі. Він передбачає моніторинг і аналіз показників продуктивності додатків, таких як час відгук, затримка, пропускна здатність і частота помилок, щоб виявити проблеми, пов'язані з продуктивністю додатків, доступністю та взаємодією з користувачем.	APM передбачає збір даних із різних джерел, включаючи журнали додатків, журнали серверів, мережевий трафік і взаємодію користувачів, щоб забезпечити цілісне уявлення про продуктивність додатків.
Моніторинг мережевих пристроїв SNMP (Simple Network Management Protocol) SNMP.	SNMP дозволяє IT-командам контролювати продуктивність і стан мережевих пристроїв/обладнання.	Пристрої з увімкненням SNMP можна налаштувати для зв'язку з сервером SNMP, який відповідатиме за збір цінних даних про працездатність і використання ресурсів мережевого пристрою.
Машинне навчання та штучний інтелект (Machine Learning and Artificial Intelligence).	Використання алгоритмів машинного навчання та штучного інтелекту для автоматизованого аналізу мережевих даних. Це може включати виявлення аномалій, класифікацію трафіку та передбачення подій в мережі.	Використання алгоритмів машинного навчання для автоматизованого виявлення аномалій у мережі на основі історичних даних та патернів поведінки.

Методи моніторингу мережі ми розглянули, переходимо до

SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #6. Аналіз та візуалізація даних мережевого моніторингу..*

Типи інструментів моніторингу мережі

Для моніторингу мережі використовуються різноманітні інструменти для моніторингу й аналізу мережевого трафіку, виявлення вузьких місць і усунення проблем.

Одним із найважливіших аспектів моніторингу продуктивності мережі є використання спеціалізованих інструментів, призначених для збору та аналізу мережевих даних у режимі реального часу, оскільки ви не можете стежити за всім самостійно. Ці інструменти мають багато форм і використовуються мережевими адміністраторами, інженерами та IT-фахівцями для моніторингу стану мережі , усунення проблем і оптимізації продуктивності.

З різних типів інструментів моніторингу мережі , які зазвичай використовуються в сучасних мережах виділяють кілька класів інструментів. Розглянемо їх детальніше.

- **Інструменти пасивного моніторингу мережі**

Інструменти пасивного моніторингу мережі збирають і аналізують дані про мережевий трафік під час його проходження через мережу.

На відміну від інструментів активного моніторингу, які генерують синтетичний трафік, інструменти пасивного моніторингу фіксують і аналізують трафік, який уже проходить через мережу.
Інструменти пасивного моніторингу мережі зазвичай використовуються для захоплення мережевого трафіку, вимірювання показників продуктивності мережі та забезпечення видимості моделей використання мережі .
Інструменти пасивного моніторингу мережі зазвичай включають:

- ✓ **Збір і аналіз реального трафіку** користувачів.
- ✓ **Аналіз заголовків пакетів**.
- ✓ **Аналіз корисного навантаження** для вимірювання показників продуктивності мережі, таких як затримка, тремтіння та пропускна здатність.
- ✓ Забезпечення детальної **видимості шаблонів мережевого трафіку**, які можна використовувати для визначення тенденцій, усунення проблем і моніторингу продуктивності додатків.
- ✓ **Виявлення програм, які потребують великої пропускної здатності.**
- ✓ **Аналіз моделей трафіку**
- ✓ **Визначення точок перевантаження** мережі або загального перевантаження мережі .

Переваги пасивного моніторингу

- ✓ Не створює додаткового навантаження на мережеві пристрої.
- ✓ Простий у налаштуванні та підтримці.
- ✓ Підходить для моніторингу великих мереж.

Інструменти пасивного моніторингу продуктивності мережі мають кілька недоліків, тому їх все частіше замінюють рішеннями для активного моніторингу. **Ось деякі з недоліків**:

- ✓ **Нездатність генерувати трафік**. Вони можуть бути не в змозі визначити проблеми, які присутні лише в періоди інтенсивного трафіку.
- ✓ **Обмежений обсяг аналізу**. Оскільки вони можуть аналізувати лише зафіксований трафік, це може не надати повної картини продуктивності мережі.
- ✓ **Ресурсовитратні**. Вимагають значних ресурсів для захоплення та зберігання мережевого трафіку, що може призвести до проблем із продуктивністю в контрольованій мережі.
- ✓ **Потенційні проблеми з конфіденційністю**. Оскільки вони захоплюють увесь мережевий трафік, включаючи конфіденційну інформацію, таку як паролі та конфіденційні дані. Це може викликати проблеми з конфіденційністю, якщо отримані дані не захищені належним чином.
- ✓ **Складність**. Складно використовувати, бо для інтерпретації зібраних даних потрібен високий рівень технічної експертизи.

- **Інструменти активного моніторингу мережі**

Інструменти активного моніторингу мережі відстежують продуктивність мережі, надсилаючи пакети даних через мережу для імітації трафіку користувача та тестування продуктивності мережі.

Ці інструменти використовуються для активного моніторингу та вимірювання продуктивності мережі, виявлення проблем у режимі реального часу та створення сповіщень, коли продуктивність мережі падає нижче прийнятного рівня.
Інструменти активного моніторингу мережі зазвичай включають:

- ✓ **Розгортання агентів моніторингу** або зондів у ключових місцях мережі для наскрізного моніторингу.
- ✓ **Агенти або зонди безперервно надсилають синтетичні пакети даних через мережу** для вимірювання затримки мережі, пропускної здатності та втрати пакетів.
- ✓ **Дозволяють** мережевим адміністраторам **імітувати поведінку користувачів** і перевіряти, як мережа реагує за різних навантажень і умов.

Інструменти активного моніторингу мережі також все частіше замінюють старі рішення пасивного моніторингу з різних причин, таких як:

- ✓ **Проактивний моніторинг**. Імітують трафік користувачів і постійно відстежують мережу на предмет потенційних проблем, що дозволяє IT-командам виявляти та вирішувати проблеми до того, як вони вплинуть на кінцевих користувачів.
- ✓ **Немає захоплення пакетів**. Інструменти активного моніторингу не фіксують трафік реального користувача, що означає, що немає проблем із конфіденційністю даних реального користувача. Це також означає, що вони можуть контролювати продуктивність навіть у періоди низького трафіку.
- ✓ **Точні вимірювання.** Активні інструменти можуть забезпечити точні вимірювання показників продуктивності мережі, таких як затримка, використання пропускної здатності та втрати пакетів, оскільки вони генерують власний трафік і вимірюють відповідь.
- ✓ **Повна видимість.** Можуть контролювати всі компоненти мережі, включаючи сервери, комутатори, маршрутизатори та програми, надаючи IT-командам повну видимість продуктивності всієї мережі.
- ✓ **Гнучкість.** Можна налаштувати відповідно до конкретних потреб моніторингу та розгортати в різних місцях, включаючи хмару, локальні та віддалені місця.
- ✓ **Масштабованість.** Можуть масштабуватися для моніторингу великих і складних мереж із кількома розташуваннями, що робить їх ідеальними для організацій корпоративного рівня.

SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #6. Аналіз та візуалізація даних мережевого моніторингу.*.

Недоліки активного моніторингу:

- ✓ Може створювати додаткове навантаження на мережеві пристрої.
- ✓ Може бути складним налаштувати та підтримувати.
- ✓ Може не підходити для моніторингу великих мереж.

Найбільш поширені приклади активних інструментів моніторингу мережі Вам знайомі. Це Ping, Traceroute. Вони є вбудованими інструментами, доступними в більшості операційних систем та систем моніторингу. Існують більш просунуті комерційні інструменти, що відстежують продуктивність мережі за допомогою агентів моніторингу, які надсилають синтетичний TCP/UDP-трафік з певною періодичністю між хостами-агентами через ключові місця мережі

- **Засоби моніторингу мережі на основі SNMP**

Інструменти моніторингу мережі на основі SNMP використовують простий протокол керування мережею (SNMP) для моніторингу та керування мережевими пристроями .

SNMP — це протокол, який використовується для керування мережевими пристроями та дозволяє відстежувати та контролювати мережеві пристрої. Інструменти моніторингу мережі на основі SNMP можуть збирати інформацію про мережеві пристрої, як-от використання ЦП, пам'яті, статистику трафіку та інші параметри.
Інструменти моніторингу на основі SNMP можуть бути як активними, так і пасивними, і їх можна використовувати для моніторингу дротових і бездротових мереж.

- **Інструменти моніторингу продуктивності додатків (APM).**

Інструменти моніторингу продуктивності додатків - Application Performance Monitoring (APM) — це програми, призначені для моніторингу продуктивності та доступності програм у режимі реального часу.

Інструменти APM використовуються для виявлення, діагностики та вирішення проблем продуктивності, які впливають на продуктивність програми та взаємодію з користувачем.

Інструменти APM забезпечують видимість усього стеку додатків, включаючи код додатків, веб-сервери, бази даних та інші компоненти інфраструктури, збираючи різноманітні показники, пов'язані з продуктивністю додатків, наприклад час відповіді, пропускну спроможність, частоту помилок і використання ресурсів, щоб надати розуміння поведінки додатків і оптимізації продуктивності. Вони також мають такі функції, як зіставлення додатків, відстеження транзакцій і діагностика на рівні коду, щоб допомогти виявити та діагностувати проблеми продуктивності.

- **Інструменти моніторингу роботи кінцевого користувача**

Інструменти моніторингу взаємодії з кінцевим користувачем - End-User Experience Monitoring Tools (EUEM) призначені для відстеження досвіду роботи кінцевих користувачів під час використання ними програми або доступу до веб-сайту .

Вони забезпечують видимість того, як програми та служби працюють для кінцевих користувачів, незалежно від того, звідки вони до них звертаються, і можуть допомогти виявити та усунути проблеми, пов'язані з продуктивністю мережі.

Інструменти EUEM збирають дані про різноманітні показники взаємодії з користувачем, включаючи час завантаження сторінки, час відповіді та частоту помилок, серед іншого. Деякі інструменти EUEM також пропонують можливість імітувати взаємодію користувача з додатками, що дозволяє IT-командам виявляти потенційні проблеми, перш ніж вони вплинуть на кінцевих користувачів.

- **Синтетичні засоби моніторингу продуктивності мережі**

Інструменти синтетичного моніторингу продуктивності мережі призначені для імітації поведінки користувача в мережі для вимірювання продуктивності мережі. Ці інструменти генерують синтетичний трафік, який надсилається через мережу, і вимірюють різні показники продуктивності, такі як затримка, втрата пакетів і тремтіння.

Інструменти синтетичного моніторингу використовуються для тестування продуктивності нової мережевої інфраструктури, а також виявлення та діагностики проблем у існуючій мережевій інфраструктурі. Вони також можуть бути використані для моделювання реальних сценаріїв, таких як велике навантаження користувачів або певні типи мережевого трафіку, щоб перевірити продуктивність мережі за різних умов.

Інструменти активного моніторингу продуктивності мережі часто також є синтетичними інструментами моніторингу.
Загалом синтетичні інструменти моніторингу продуктивності мережі забезпечують спосіб проактивного моніторингу та тестування продуктивності мережі для забезпечення оптимальної роботи мережі.

- **Інструменти аналізатора мережевих пакетів**

Аналізатори мережевих пакетів, також відомі як аналізатори пакетів, аналізатори протоколів або мережеві аналізатори, збирають і аналізують пакети даних, надіслані та отримані через мережу.

Інструмент дозволяє мережевим адміністраторам і фахівцям із безпеки перевіряти мережевий трафік, визначати джерело й призначення пакетів, а також аналізувати вміст пакетів, щоб усунути проблеми з мережею, оптимізувати продуктивність мережі, а також виявити й запобігти загрозам безпеки.

Аналізатори пакетів можна використовувати в дротових і бездротових мережах, і вони підтримують різноманітні мережеві протоколи та інтерфейси, такі як Ethernet, Wi-Fi, TCP/IP і HTTP.

- **Інструменти моніторингу мережі на основі потоку**

Інструменти моніторингу мережі на основі потоку збирають інформацію про мережевий трафік, аналізуючи дані потоку. Дані потоку — це метадані, які описують характеристики мережевого трафіку, наприклад IP-адреси джерела та призначення, номери портів і обсяг переданих даних.

Ми вже вивчали основи використання протоколів NetFlow та sFlow у мережевому моніторингу та пам'ятаємо, що моніторинг на основі потоку використовується для визначення типів трафіку, який проходить мережею, а також кінцевих точок, які генерують і отримують трафік.

- **Хмарні інструменти моніторингу мережі**

Хмарні інструменти моніторингу мережі дозволяють контролювати продуктивність мережі з віддаленого місця . Вони розміщені в хмарі та використовують мережу серверів для збору та аналізу даних про мережевий трафік, продуктивність програм та інші відповідні показники.

Доступ до хмарних інструментів моніторингу мережі можна отримати через веб-інтерфейс, що полегшує IT-фахівцям моніторинг продуктивності своєї мережі з будь-якого місця, де є підключення до Інтернету. Вони також часто засновані на підписці та можуть пропонувати такі функції, як моніторинг у реальному часі, сповіщення та звітування. Вони також можуть легко масштабуватися для мереж, що ростуть, запропонувати високу доступність і надійність і допомогти організаціям зменшити витрати на IT-інфраструктуру, усуваючи необхідність купувати та обслуговувати обладнання та програмне забезпечення на місці.

- **Інструменти моніторингу продуктивності Wi-Fi**

Інструменти моніторингу продуктивності Wi-Fi відстежують і аналізують продуктивність мереж Wi-Fi . Вони збирають і аналізують дані з пристроїв Wi-Fi і точок доступу, надаючи інформацію про різні показники продуктивності Wi-Fi, такі як потужність сигналу, пропускна здатність, затримка та втрата пакетів.

Інструменти моніторингу продуктивності Wi-Fi допомагають виявити та усунути проблеми з продуктивністю Wi-Fi, оптимізувати роботу мережі Wi-Fi та забезпечити високу якість надання послуг Wi-Fi кінцевим користувачам.

Використання інструментів візуалізації даних для створення графіків, діаграм та звітів.

Графічне відображення інформації допомагає донести потрібну думку, підкріпити сформульований висновок або підкреслити акцент
Одна з труднощів, яка істотно сповільнює та ускладнює сприйняття звітів та аналітичну роботу, полягає в підборі правильного типу діаграми. Невірний її вибір може викликати плутанину в голові у користувача, або системного адміністратора, чи призвести до помилкової інтерпретації даних.
Щоб створити діаграму, яка пояснює та демонструє точну аналітику, спочатку потрібно зрозуміти причини, через які взагалі вона може знадобитися. Розглянемо п'ять типових питань, що виникають при виборі типу діаграми. Потім ми дамо огляд основних видів діаграм, що використовуються для відображення результатів моніторингу.

- **5 питань, які потрібно задати собі при виборі діаграми**

1. ***Вам потрібно порівнювати величини?***
   Графіки ідеально підходять для порівняння одного або декількох наборів величин, і вони можуть легко відображати самі низькі і високі показники. Для створення порівняльної діаграми використовуйте наступні типи: гістограма, кругова діаграма, точкова діаграма, шкала зі значеннями.

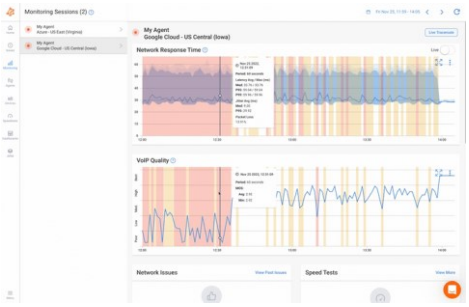
2. ***Ви хочете показати структуру чогось?***
   Наприклад, ви хочете отримати поточний стан CPUз прив'язкою до типів хостів, або загальний обсяг інтернет трафіку, розбитий на лінки від різних провайдерів. Щоб показати структуру, використовуйте наступні діаграми: кругова діаграма, гістограма з накопиченням, вертикальний стек, обласна діаграма, діаграма-водоспад.

3. ***Ви хочете зрозуміти, як розподіляються дані?***
   Таблиці з розподілом допомагають зрозуміти основні тенденції і відзначити, що виходить за рамки. Для відображення розподілу даних використовуйте ці діаграми: точкова діаграма, лінійна діаграма, гістограма.

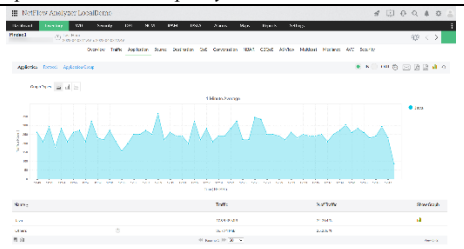
4. ***Ви зацікавлені в аналізі тенденцій у певному наборі даних?***
   Якщо ви хочете дізнатися більше про те, як дані поводяться протягом конкретного часового періоду, є типи діаграм, які дуже добре це відображають. Вам знадобляться: лінійна діаграма, подвійна вісь (стовпець і лінія), гістограма.

5. ***Хочете краще зрозуміти взаємозв'язок між встановленими значеннями?***
   Взаємопов'язані графіки підходять для того, щоб показати, як одна змінна відноситься до іншої або декількох різних змінних. Це можна використовувати, щоб показати позитивний, негативний або нульовий вплив на іншу цифру. Використовуйте для цього такі діаграми: точкова діаграма, бульбашкова діаграма, лінійна діаграма.

Розглянемо типи графіків та діаграм, які використовуються для візуалізації даних у мережевому моніторингу. Візуалізація даних є надзвичайно важливим етапом у розумінні стану мережі, виявленні аномалій, аналізі та прийнятті рішень. Ось деякі типи графіків та діаграм, які часто використовуються у мережевому моніторингу:

Часові графіки: Ці графіки показують зміну параметрів мережі в залежності від часу. Вони дозволяють виявити тенденції та циклічність у поведінці мережі, а також виявляти винятки та аномалії, які можуть виникнути протягом певного часового періоду. А ми пам'ятаємо, що моніторинг у режимі реального часу є критично важливим аспектом моніторингу мережі (NM), який стосується постійного моніторингу показників продуктивності мережі, таких як використання пропускної здатності, затримка, втрата пакетів та інші ключові показники ефективності (KPI) у режимі реального часу. Це дозволяє IT-командам завчасно виявляти проблеми з мережею до того, як вони вплинуть на кінцевих користувачів.	

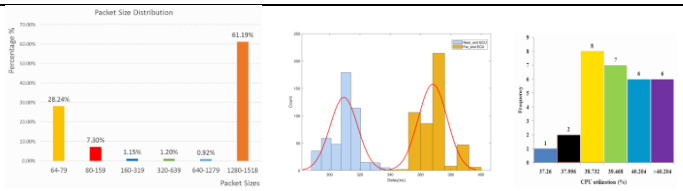
Лінійні графіки: Ці графіки використовуються для відображення залежності між двома змінними, такими як швидкість передачі даних, витрата пропускної здатності тощо. Вони часто використовуються для моніторингу пропускної здатності та швидкості мережі.



Гістограми: Це графіки, які показують розподіл даних за певними параметрами. Наприклад, гістограми можуть бути використані для відображення розподілу величини пакетів за їхньою довжиною, що допомагає спостерігати за нормальністю процесу, або виявити незвичайні або аномальні значення.

Приклади:

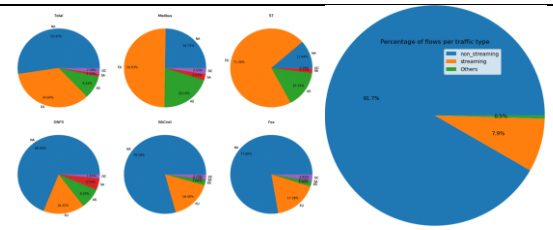
1. Гістограма розподілу розмірів пакетів
2. Гістограма розподілу затримки
3. Гістограма використання ЦП сервера



1 2 3

Кругові діаграми: Вони часто використовуються для відображення часток різних типів даних у загальному наборі даних. Наприклад, кругова діаграма може показати співвідношення різних протоколів, що використовуються у мережі. Для цього типу діаграм необхідно розуміти, що вони наглядні та прості у розумінні тільки при порівняно невеликій кількості показників, або порівнянні якихось домінуючих показників з залишком кола, що припадає на інші.

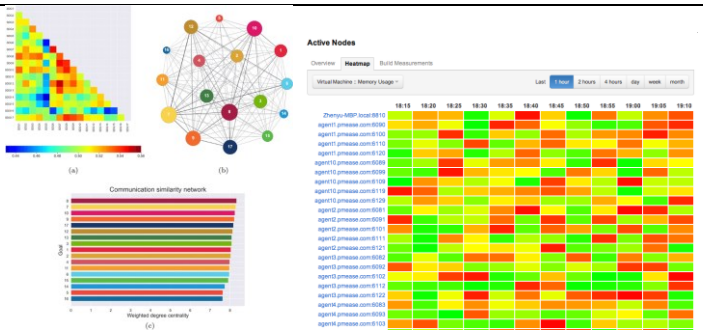
4. Розподіл мережевого трафіку за протоколом
5. Діаграма розподілу трафіку за адресою



4 5

Теплові карти: Ці графіки використовуються для візуалізації інтенсивності певного параметру на основі розташування у просторі. Наприклад, теплова карта може відображати рівень трафіку на різних ділянках мережі.

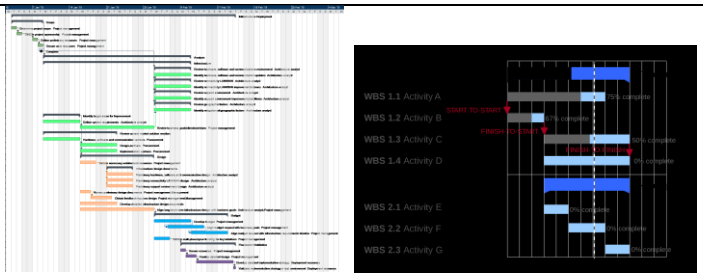
1. Теплова карта доступності мережі
2. Теплова карта, що показує використання пам'яті сервера на різних серверах



1 2

Діаграми Ганта: Вони використовуються для відображення розкладу різних подій або завдань у часі. Це може бути корисно для відстеження виконання певних мережевих проектів або технічних робіт.

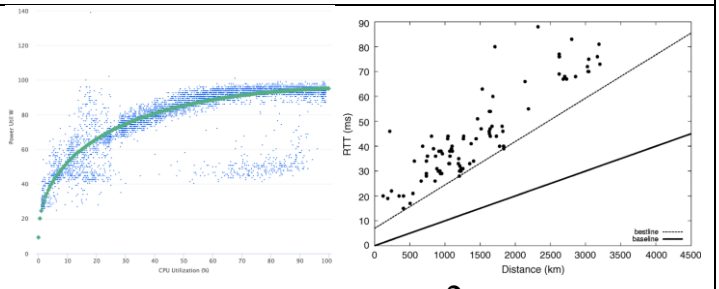
3. Діаграма Ганта розгортання нового маршрутизатора
4. Діаграма ГАнта усунення несправностей мережі



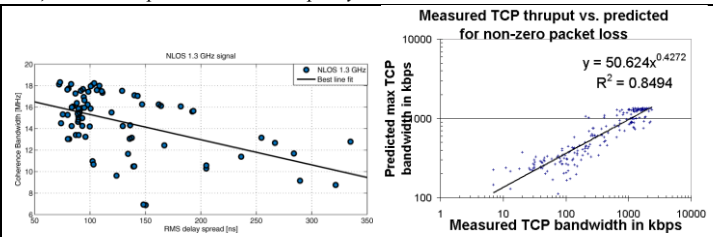
3 4

Скатерограми: Це графіки, що відображають взаємозв'язок між трьома або більше змінними. Вони дозволяють виявити кореляції або залежності між різними параметрами мережі.

1. Скатерограма залежності використання ЦП сервера від навантаження
2. Скатерограма залежності часу відгуку веб-сайту від затримки
3. Скатерограма залежності затримки від пропускної здатності
4. Скатерограма залежності втрати пакетів від пропускної здатності



2



3 4

Звичайно не всі ці типи графіків та діаграм підтримуються кожним інструментом моніторингу, але цей короткий опис має допомогти Вам при обранні типу, якщо він доступний.

Розробка звітів та дашбордів для ефективного моніторингу мережі..

Що таке дашборд: приклади і способи застосування

Термін «dashboard» з англійської на українську перекладається як інформаційна панель. А по суті, дашборд - це програмне рішення, що дозволяє створювати, одержувати, аналізувати дані в реальному часі. Видані інформаційною панеллю «розумні звіти» допомагають власнику, керівнику, менеджеру розуміти певні тенденції в конкретному сегменті діяльності та контролювати події, що відбуваються.

Актуально: Виграш від використання в роботі не класичного звіту, а дашборду в тому, що глобальні і просто важливі показники надаються до вивчення зрозуміло і наочно. Інформаційна панель істотно спрощує сприйняття користувачем складних і різносторонніх відомостей. Той, хто отримує дані за допомогою дашборда, може оцінити поточний стан справ на конкретний момент часу з першого погляду.

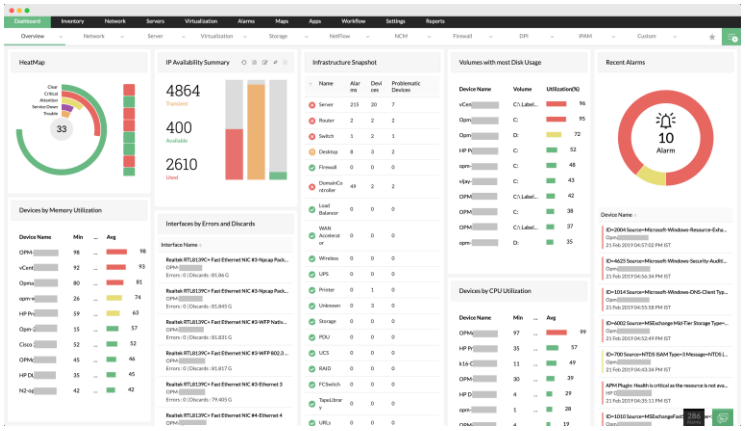
Щоб Вам було простіше зрозуміти, що таке дашборд, наведемо кілька прикладів використання подібного програмного рішення. Пригадуєте гігантські монітори з художніх фільмів про глобальні катастрофи або надпотужні випробування? На стіні-дисплеї з'являються зведення, важливі показники про чисельність, фактичне розташування і так далі. Подібні монітори з оперативною інформацією зустрічаються не тільки в кіно. У реальному житті безліч прикладів використання дашборду для своєчасного отримання та аналізу інформації. Це:

- ✓ пункти управління космічними польотами;
- ✓ військові бази;
- ✓ диспетчерські центри контролю над авіаперельотами;
- ✓ брокерські контори, звідки ведеться спостереження за рухом на ринку валют і цінних паперів.
- ✓ моніторингові кімнати провайдерів чи адміністрування ЦОДів

У світі бізнесу без подібного програмного рішення, яке в автоматичному режимі здійснює обробку що надходять відомостей і виводить їх у вигляді зрозумілих діаграм, стовпців, графіків, обійтися складно. Це очевидно. Але «ігри багатих» - далеко не єдина сфера застосування інформаційних панелей. Вони надзвичайно корисні не тільки міжконтинентальних корпораціям, фінансовим мережам, концернам. Працювати з даними за допомогою гарного та інформативного дашборда може будь-хто.

Найпростішим прикладом дашборду, зрозумілим будь-якій сучасній людині, є приладова панель автомобіля. На ній відображено кілька датчиків, які демонструють в зрозумілому вигляді важливу інформацію - швидкість, рівень масла і бензину, число обертів двигуна, температуру в салоні і «за бортом». Ефективність використання панелі досягається за рахунок групування та мінімізації інформації, що відображається в реальному часі. Другий приклад елементу дашборду, але вже з галузі моніторингу, це панель на яку виведена кругова діаграма п'яти максимальних навантажень на інтернет лінки, де всі навантаження, менші від певного порогу виведені одним значенням. На панелі буде лише 6 елементів, що дозволить легко сприйняти інформацію.

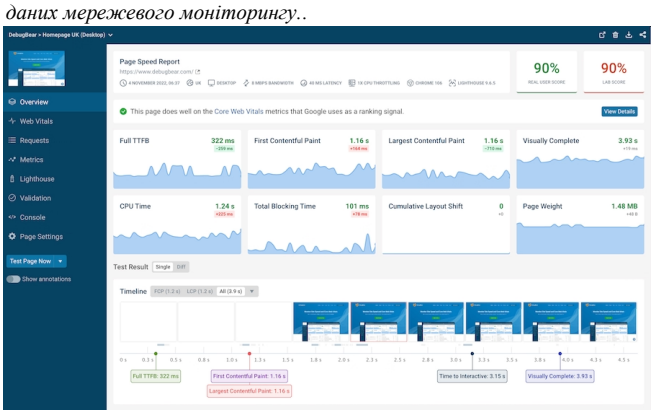
1



2

SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #6. Аналіз та візуалізація даних мережевого моніторингу.*.

3



4

1. **Дашборд моніторингу продуктивності сервера.** Показує ключові показники продуктивності сервера, такі як використання ЦП, використання пам'яті, дисковий ввід-вивід і мережевий трафік. Цю інформацію можна використовувати для виявлення проблем із продуктивністю сервера та їх усунення.
2. **Дашборд моніторингу доступності мережі.** Показує доступність мережевих пристроїв і зв'язків. Цю інформацію можна використовувати для виявлення проблем із доступністю мережі та їх усунення.
3. **Дашборд моніторингу безпеки мережі.** Показує активність мережевої безпеки, такі як спроби вторгнення та атаки шкідливих програм. Цю інформацію можна використовувати для виявлення та реагування на загрози безпеці мережі.
4. **Дашборд моніторингу продуктивності веб-сайту.** Показує ключові показники продуктивності веб-сайту, такі як час завантаження сторінки, частота відмов і кількість переглядів сторінок. Цю інформацію можна використовувати для виявлення проблем із продуктивністю веб-сайту та їх усунення.

Кожен з нас хоч раз користувався примітивним «родичем» дашборда. Найпростіші зразки - звіт в Excel, рахунок в магазині або кафе, зошит із записом витрат, звіт про рух складу. Від усіх цих прикладів дашборд відрізняється динамічністю, інтерактивністю візуалізації даних.

Візуальні особливості дашборду

Зрозумілість і читабельність аналізованих даних досягається в дашборді різноманітними інструментами. Це можуть бути стрілочні індикатори як в транспортних засобах або більш звичні таблиці. Зручний вид анімації програмується під завдання замовника і з урахуванням його особистих побажань.

З якими даними можна працювати

Будь-яка інформація зі змінними даними може стати джерелом для використання в дашборді - найпростіші таблички в Excel, статистика соцмережі, відвідуваності сайтів, спеціалізовані бази Data Warehouse, багатовимірні куби OLAP і MDX.

Які дії з даними здійснюються в дашборді

- ✓ **Групування.** Схожі відомості групуються за спільною ознакою - назвою, типом, видом дії, стандартністю події.
- ✓ **Агрегація.** Дані відображаються за фактом з вихідних даних, наприклад, сума, кількість, максимум. Ще більш зрозумілий приклад: унікальне число нових відвідувачів сайту за конкретний період часу.
- ✓ **Сортування.** Наприклад, відомості, які колись уже згруповані за конкретним запитом (середнє навантаження на CPU хоста гіпервізора) можна сортувати по висхідній для пошуку хосту з найбільшим навантаженням за період.
- ✓ **Фільтрація.** Відомості виключаються з візуального інструменту за потрібною ознакою або формулою.
- ✓ **Обчислюється колонка.** Нова інформація візуалізується за певними формулами. Наприклад, кількість трафіку за місяць по лінкам провайдера та його тариф дає рахунок, який ми маємо отримати.
- ✓ **Кращі параметри.** На дисплеї відображається число максимальних або мінімальних даних в групі.

Ця та інша інформація відображається на дисплеї у вигляді таблиць, діаграм, карт. Якщо Ви працювали з SQL (Structured query language — мова структурованих запитів) — декларативна мова програмування для взаємодії користувача з базами даних, що застосовується для формування запитів, оновлення і керування реляційними БД), то помітили схожість дій у дашборді та типових SQL-запитів.

Отже, чому для успішної роботи, контролю, аналізу у системі моніторингу потрібна така помічниця як інформаційна панель? Вона дозволяє:

- ✓ систематизувати і візуалізувати дані;
- ✓ представляти їх споживачеві у вигляді простої і наочної анімації;
- ✓ отримувати найостанніші зведення, оперативно спостерігати динаміку даних;
- ✓ видавати дані в потрібній ієрархії, проводити їх порівняння;
- ✓ виділити ключові відомості, щоб тримати їх під контролем;
- ✓ оптимізувати вивчення великих масивів даних, виділяти найважливіше за принципом: «з першого погляду ситуація прояснилася».
- ✓ порівнювати блоки інформації, швидко отримувати відомості в налаштованому для себе вигляді.

Як працює дашборд, які цілі цей сервіс допомагає досягати, ми вже обговорили. А які звіти можна отримати, використовуючи цей інструмент?

- ✓ Регулярну аналітику за заданими показниками. Такі звіти дозволять відстежити тренди, отримати звіт-аналіз по ситуації і на підставі цих графіків скорегувати тактику компанії.
- ✓ Оперативні звіти - це актуальна інформація, що подається споживачу постійно. Діаграма допоможе не пропустити важливі зміни даних.
- ✓ Довгострокові управлінські рішення складно приймати, не маючи «під рукою» стратегічні звіти. Дашборда допоможе у вирішенні цього завдання.

SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #6. Аналіз та візуалізація даних мережевого моніторингу..*
Принципи роботи з дашбордами
Ми дізналися багато про це програмне рішення. Ну а як конкретно працювати з dashboard? Найбільш ефективні аналітичні панелі розробляються і налаштовуються під потреби і запити конкретного користувача. Щоб замовнику було зручно працювати, інтерактивна система візуалізації даних повинна відрізнятися наступними характеристиками:

- ✓ Простота. Під час налаштування візуальних звітів важливо, щоб кожен показник читався однозначно. Наприклад, «Х» повинна означати число унікальних відвідувачів за добу, відвантаження товару за останню годину, суму надходжень в конкретній валюті.
- ✓ Порівняння. Дані, які підлягають порівнянню, повинні розташовуватися у вигляді схожих графіків на панелі поруч.
- ✓ Головне - першим рядком. Всі важливі відомості повинні бути доступні.
- ✓ Гнучкість налаштувань. Хороша програма дозволяє легко перебудовувати елементи панелі. Це важливо, тому що в ході роботи, на різних етапах бізнесу можуть вимагатися різні дані. Наприклад, спочатку дані про виробництво, далі - рух по складу, пізніше - звіт з продажу.
- ✓ Варіанти візуалізації одних і тих же даних. Наприклад, одна інформація може бути представлена на моніторі в графіку і діаграмі. Це дає можливість під іншим кутом вивчати відомості, по-новому аналізувати їх.
- ✓ Тільки найважливіше. Відмовляйтеся від непотрібних елементів, які будуть відволікати і перевантажувати увагу і монітор надлишковою інформацією.

Ті користувачі, хто вперше обирає програмне рішення, часто роблять типові помилки. Серед них хочеться виділити основні моменти:

- ✓ Занадто багато елементів. Коли починаючий користувач хоче одночасно відстежувати занадто багато даних, дашборд перетворюється на калейдоскоп. Дуже важливо на початковому етапі зрозуміти, які відомості дійсно важливі, і на яких не обов'язково фокусувати увагу.
- ✓ Якщо некоректно або незрозуміло обізвав метрики або осі графіків, розібратися в такому дашборді може тільки програміст. А ось користувачам буде складно прочитати діаграму і зрозуміти, що вона демонструє.
- ✓ Некоректна візуалізація. Дуже важливо вибрати вид віджета, який буде найкращим чином демонструвати дані. Наприклад, щоб показувати зміна даних у часі, не підійде кругова діаграма.

Як зробити дашборд?
Розробка персонального дашборду може коштувати дуже дорого. Набагато вигідніше купити готове програмне рішення, яке легко налаштовується на нового користувача. Існує багато сервісів для розробки таких рішень. Але ми звикли робити все самі, тому…

Основні інструменти створення дашбордів.

Інструмент	Опис	Ліцензія	
Grafana	Один з найпопулярніших інструментів для створення дашбордів та візуалізації даних з різноманітних джерел, таких як Prometheus, InfluxDB, Graphite, Elasticsearch тощо. Grafana надає широкий вибір графічних елементів та можливостей налаштування.	Відкрита ліцензія Apache 2.0, безкоштовна для використання.	
Kibana	Поставляється разом з Elasticsearch (ELK stack) і використовується для аналізу та візуалізації журналів, метрик та інших даних. Він дозволяє створювати різноманітні графіки, таблиці та інші візуальні елементи для моніторингу.	Відкрита ліцензія Apache 2.0, безкоштовна для використання.	
Kubernetes Dashboard	Вбудований інструмент для моніторингу та управління Kubernetes-кластерами. Він надає графіки та статистику щодо ресурсів, а також можливість відслідковувати стан роботи різних компонентів кластера.	Відкрита ліцензія Apache 2.0, безкоштовна для використання.	
Prometheus Dashboard	Prometheus поставляється зі своїм власним інструментом для візуалізації даних, що дозволяє створювати графіки та графи для метрик, зібраних Prometheus.	Відкрита ліцензія Apache 2.0, безкоштовна для використання.	
Splunk	Інструмент для аналізу та моніторингу журналів та даних. Він має широкий функціонал для створення дашбордів, включаючи графіки, таблиці, зведені дані тощо.	Використовує ліцензію, яка базується на обсязі обробленої даних (дані, які імпортуються та обробляються Splunk). Це може бути обмеження обсягу даних на день або на місяць, в залежності від типу ліцензії (Free, Enterprise, Cloud, тощо)	
MS SQL Server Reporting Services (SSRS)	За допомогою SSRS можна створювати різноманітні звіти та дашборди на основі даних, які зберігаються в базі даних, що підтримує SQL джерела даних. SSRS дозволяє створювати динамічні дашборди, які можуть включати графіки, таблиці, карти та інші візуальні елементи для представлення даних. Ці дашборди будуються на основі запитів до БД, а також можуть використовувати попередньо підготовлені власні набори даних.	Вартість ліцензії залежить від БД, що використовується.	

І як резюме хочеться відзначити, що дашборд тільки звучить складно. На практиці це зручне рішення.

Глобальні дашборди кіберзагроз.

Спостереження за тим, які зміни відбуваються на планеті в масштабах країн та континентів – справжнє джерело натхнення для аналітиків безпеки. Навіть якщо ви не пов'язані з ІБ, але годинами залипали в контурні карти глобальних стратегій або захоплювалися глобусом в центрі управління X-COM, ця добірка інструментів вам сподобається.
Сервісів у цій категорії виявилося чимало. Всі вони мають схожу функціональність, але спираються на різні джерела даних, так що немає однієї карти загроз, яка керує всім.

- shadowserver dashboard — команда Shadowserver збирає інформацію про різноманітні загрози, такі як DDoS-атаки, ботнети, сканування портів та виявлення CVE-уразливостей. На картах і діаграмах представлена статистика щодня оновлюється.
- Global ransomware attacks — глобальна карта інцидентів, що агрегує дані щодо атак програм-вимагачів з 2018 року. Тут можна дізнатися, які сектори економіки торкнулася конкретної атаки, типу програми-вимагача і навіть суми викупу. Оновлюється щодня.
- Live Threat Map — тут можна подивитися зведену статистику по кібератаках за останню годину, добу або місяць, а також виділити країни, що найбільш атакуються, топ векторів атак і порти, що найбільш скануються.
- Talos reputation center - дашборд із загальною інформацією про кіберзагрози, створений компанією Talos за підтримки Cisco.
- Cyber Attack Map - топ нанесених на карту серверів-розповсюджувачів спаму та шкідливого ПЗ.
- Sicherheitstacho – дашборд кібератак від Deutsche Telekom, який працює на базі опенсорсної мережі honeypot (дослівно "горщик з медом): T-Pot . Це система, спеціально розроблена для того, щоб бути скомпрометованою хакерами. Її мета - заманити зловмисників та збирати інформацію про їхні методи та інструменти.
- Cyber map - дашборд від європейської компанії HTTPCS, який агрегує дані про кіберзагрози, виявлені на території різних країн. Для перегляду більшості статистики потрібна реєстрація.
- Cyberthreat Heatmap – інформативний атлас кіберзагроз. Дещо вибивається із загального ряду представлених тут ресурсів, проте пропонує велику кількість аналітики по регіонах та «працюючих» за ними APT-угруповань.
- Sophos threat center — геолокує веб-загрози, джерела розповсюдження спаму та шкідливого ПЗ у міру того, як їх виявляють аналітики компанії Sophos. Сервіс показує поточний рівень небезпеки та дозволяє побачити базову статистику щодо деяких видів загроз.
- ddos-attack-map - Live-карта DDoS-атак з тимчасовою шкалою, фільтрами по країнах та галузям, а також вказівкою сили атак.
- Digital attack map — інтерактивна карта DDoS-атак, створена в результаті співпраці Google Ideas та Arbor Networks . Дозволяє вивчати історичні дані у звітах про збої в конкретний день із розбивкою країнами.
- DDoS Threat Intelligence Map – аналітична карта, яка, як стверджують творці, дозволяє передбачати джерела майбутніх DDoS-атак. Відображає IP-адреси, з яких велися відбиті атаки, виявляє ботнети, які активно використовувалися за останні 24 години. Надає фільтри за категоріями атакуючих агентів.
- Live botnet threats worldwide — показує розташування IP-адрес серверів, що використовуються для керування зараженими пристроями.
- app.any.run - Дашборд відомого сервісу для перевірки підозрілих файлів на віруси. Відображає статистику щодо малварі, виявленої в різних регіонах світу за останні 24 години.
- Threatbutt Internet Hacking Attack Attribution Map - ця карта виділяється тим, що візуалізує не самі погрози, а повідомлення про атаки. Для цього використовується інформація, знайдена у ЗМІ, соціальних мережах та на сайтах ІБ-компаній. Карта працює на опенсорсному фреймворку pewpew (саме з таким звуком з'являються нові повідомлення).

Глобальні дашборди інтернет-інфраструктури, протоколи та сервіси

- Submarine Cable Map – карта підводних інтернет кабелів. Безкоштовний і регулярно оновлюваний ресурс від TeleGeography
- Wigle – карта точок доступу Wi-Fi
- pingdom map – дашборд для моніторингу доступності сайтів, що оновлюється в Live-режимі.
- DomainTools Internet Statistics - агрегована і нанесена на карту Whois-статистика про IP-адреси і місцезнаходження серверів, їх власників, пов'язаних доменах і багато іншого.

Висновки.

Методи аналізу даних мережевого моніторингу є ключовими для виявлення аномалій та проблем в мережі. Вони дозволяють оперативно реагувати на потенційні проблеми та забезпечують безперервну роботу мережевої інфраструктури.
Типові інструменти мережевого моніторингу, такі як Nagios, Zabbix, PRTG та інші, надають широкий функціонал для збору, аналізу та візуалізації даних про стан мережевих пристроїв.

Використання інструментів візуалізації даних є важливим аспектом для розуміння та аналізу стану мережі. Створення графіків, діаграм та звітів дозволяє швидко виявляти та аналізувати тренди та аномалії.
Розробка звітів та дашбордів є ефективним способом візуалізації даних для моніторингу мережі. Ці інструменти дозволяють збирати ключову інформацію та представляти її у зручному та зрозумілому форматі для прийняття обґрунтованих рішень щодо управління мережею.

У підсумку, аналіз та візуалізація даних мережевого моніторингу є невід'ємною частиною ефективного управління мережею. Ці процеси допомагають забезпечувати стабільну та безперебійну роботу мережі, вчасно виявляти проблеми та оптимізувати її роботу.