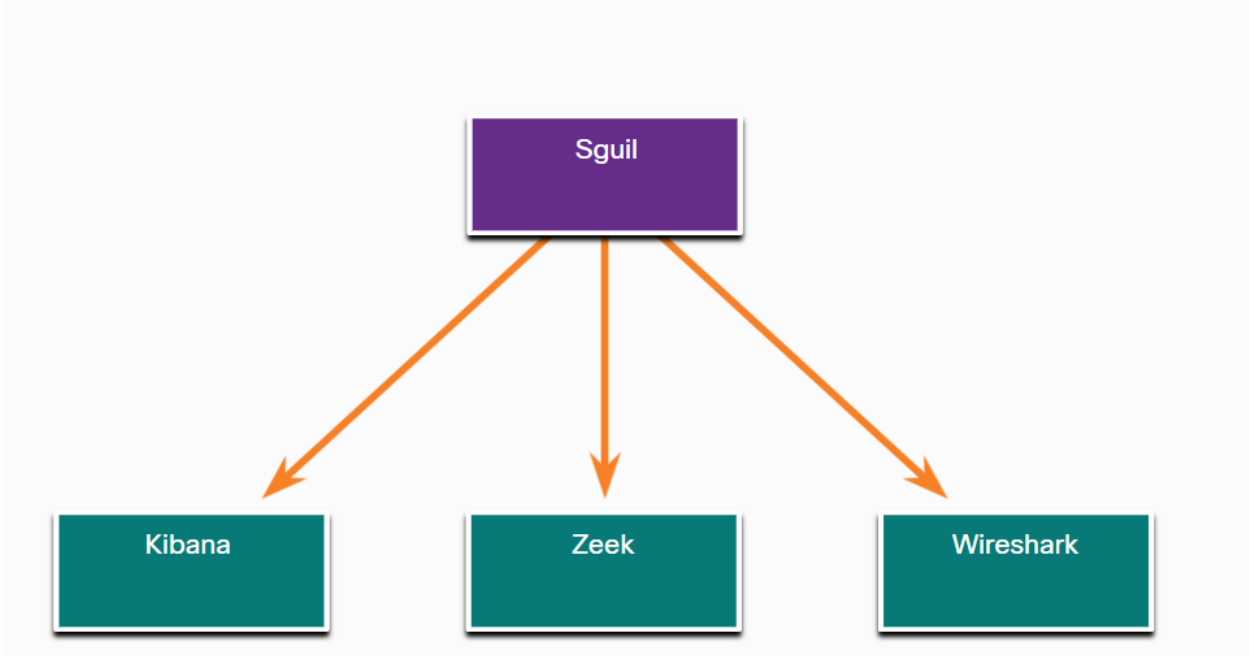
Потреба в оцінці сповіщень

Ландшафт загрози постійно змінюється у міру виявлення останніх вразливостей та розвитку нових загроз. Зі зміною потреб користувача та організацій, так змінюється і вигляд атаки. Зловмисники навчилися швидко змінювати особливості своїх експлойтів, щоб уникнути виявлення.

Неможливо розробити заходи для запобігання всім експлойтам. Експлойти неминуче уникатимуть заходів захисту, незалежно від того, наскільки складними вони можуть бути. Іноді найкраще, що можна зробити, це виявити експлойти під час або після того, як напад відбувся. Правила виявлення повинні бути надто консервативними. Інакше кажучи, краще мати сповіщення, які іноді генеруються невинним трафіком, ніж правила, які пропускають шкідливий трафік. З цієї причини необхідно, щоб кваліфіковані аналітики з кібербезпеки досліджували сповіщення, щоб визначити, чи дійсно трапилося вторгнення експлойту.

Аналітики кібербезпеки 1-го рівня зазвичай опрацьовують черги сповіщень у такому інструменті, як Sguil, звертаючись до таких засобів, як Zeek, Wireshark та Kibana, щоб переконатись чи сповіщення насправді є експлойтом.

Основні інструменти для аналітика з безпеки 1-го рівня



Оцінка повідомлень

Порушення безпеки класифікують за схемою, запозиченою з медичної діагностики. Ця схема класифікації використовується для керування діями та оцінювання діагностичних процедур. Наприклад, коли пацієнт відвідує лікаря для проведення звичайного обстеження, одним з завдань лікаря є визначення того, чи пацієнт хворий. Як результат може бути правильне виявлення ознак захворювання та недуги пацієнта. Інший результат може показати, що хвороби немає і пацієнт здоровий.

Занепокоєння полягає в тому, що діагноз може бути точним, правильним, неточним або помилковим. Наприклад, лікар міг пропустити ознаки захворювання і зробити неправильний висновок, що пацієнт здоровий, коли він фактично хворий. Інша можлива помилка вважати пацієнта хворим, коли він насправді здоровий. Помилкові діагнози або дорогі, або небезпечні.

Під час аналізу мережної безпеки аналітик з кібербезпеки працює зі сповіщеннями. Це схоже на пацієнта, який йде до лікаря і каже: "Я хворий". Аналітик з кібербезпеки, як і лікар, повинен визначити, чи цей діагноз істинний. Аналітик з кібербезпеки запитує: "Система повідомляє, що стався експлойт. Це правда?"

Повідомлення можна класифікувати таким чином:

- **Дійсно позитивне:** підтверджено, що сповіщення є фактичним інцидентом безпеки.
- **Помилково позитивне:** сповіщення не вказує на фактичний інцидент безпеки. Сприятлива активність, яка призводить до помилково позитивного результату, іноді називають доброякісним тригером.

Альтернативна ситуація полягає в тому, що попередження не було створено. Відсутність сповіщення можна класифікувати як:

- **Дійсно негативні:** жодних інцидентів безпеки не сталося. Активність є доброякісною.
- **Помилково негативні:** стався невиявлений інцидент.

Коли надходить сповіщення, воно отримує одну з чотирьох можливих класифікацій.

	дійсно	помилковий
Позитивний (сповіщення існує)	Стався інцидент	Жодного інциденту не сталося
Негативний (сповіщення не існує)	Жодного інциденту не сталося	Стався інцидент

Дійсно позитивні (True positives) є бажаним типом сповіщення. Вони означають, що правила, які генерують сповіщення, спрацювали правильно.

Помилково позитивні(False positives) є небажаними. Такі сповіщення хоча й не вказують на появу невиявленого експлойта, проте є затратними, оскільки аналітики з кібербезпеки повинні розслідувати помилкові тривоги за рахунок часу, який мав би йти на дослідження сповіщень, викликаних справжніми порушеннями.

Дійсно негативні (True negatives) також бажані. Вони вказують на те, що нормальний трафік коректно ігнорується та помилкові сповіщення не видаються.

Помилково негативні (False negatives) небезпечні. Вони вказують на те, що впроваджені системи безпеки не виявляють експлойтів. Ці інциденти можуть залишатися невиявленими тривалий час, що може призвести до втрати та пошкодження даних.

Сприятливі події – це події, які не повинні викликати попередження. Надлишок сприятливих подій вказує на те, що деякі правила чи інші детектори необхідно покращити або усунути.

У разі виникнення підозри щодо появи дійсно позитивних сповіщень аналітику з кібербезпеки іноді потрібно передати таке попередження на вищий рівень для дослідження. Слідчий продовжить вивчення аби підтвердити цей інцидент і виявити потенційну шкоду, яку він міг завдати. Цю інформацію буде використано більш висококваліфікованим персоналом з питань безпеки, який працюватиме над ізоляцією шкоди, усуненням вразливостей, пом'якшенням загрози та формуванням звіту.

Аналітик з кібербезпеки також може нести відповідальність за інформування персоналу служби безпеки про те, що помилкові позитивні

трапляються з такою частотою, що це серйозно впливає на час його розслідувань. Ця ситуація вказує на те, що системи безпеки повинні бути налаштовані таким чином, щоб стати більш ефективними. Легітимні зміни у конфігурації мережі або нещодавно завантажені правила виявлення можуть призвести до раптового спалаху помилково позитивних.

Помилково негативні події можуть бути виявлені належним чином після настання експлойту. Це може відбутися через ретроспективний аналіз безпеки (Retrospective security analysis, RSA). RSA може мати ефект, коли для архівних даних про мережну безпеку застосовуються нові правила або інший аналіз розвідки загроз. З цієї причини важливо стежити за розслідуванням загроз, щоб дізнатися про нові вразливості та експлойти, а також оцінити ймовірність того, що мережа була вразливою до них у минулому. Окрім цього, втручання експлойту повинно бути оцінено стосовно потенційної шкоди, через яку підприємство може постраждати. Можна визначити, чи додавання нових технік пом'якшення наслідків є достатнім або необхідний більш детальний аналіз.

Коли надходить сповіщення, воно отримує одну з чотирьох можливих класифікацій.

	дійсно	**помилковий**
Позитивний (сповіщення існує)	Стався інцидент	Жодного інциденту не сталося
Негативний (сповіщення не існує)	Жодного інциденту не сталося	Стався інцидент

Примітка: «дійсні» події є бажаними. «Помилкові» події є небажаними та потенційно небезпечними.

Детермінований аналіз і ймовірний аналіз

Статистичні методи можуть бути використані для оцінки ризику того, що експлойти будуть успішними в певній мережі. Цей тип аналізу може допомогти керівництву краще оцінити витрати на пом'якшення загрози та мінімізацію збитків, які може спричинити втручання експлойту.

Для цього використовуються два загальні підходи: детермінований та ймовірнісний аналіз, як показано на малюнку. Детермінований аналіз оцінює ризик на основі відомостей про вразливість. Передбачається, що для успішного виконання експлойту всі попередні кроки в процесі його втручання

також повинні бути вдалими. Цей тип аналізу ризику може лише описати найгірший випадок. Попри те, що багатьом зловмисникам відомий процес проведення експлойту, вони можуть не мати достатньо знань або досвіду для результативного (ефективного) завершення кожного кроку на шляху до успішного використання. Це дозволяє аналітику з кібербезпеки можливість виявити цей експлойт та зупинити його до того, як він просунеться далі.

Ймовірнісний аналіз оцінює потенційний успіх втручання експлойту, оцінюючи ймовірність того, що, якщо один крок втручання експлойту буде успішно завершено, то наступний крок також буде вдалим. Ймовірний аналіз особливо корисний в аналізі мережної безпеки в реальному часі, у якому аналізуються численні змінні, і відповідна загроза може призвести до невідомих наслідків, якщо експлойт поширитьcя.

Ймовірнісний аналіз спирається на статистичні методи, які призначені для оцінки вірогідності того, що подія відбудеться на основі ймовірності настання попередніх подій. Використовуючи цей тип аналізу, можна оцінити найбільш вірогідні шляхи, які буде використано експлойтом. І увага персоналу з питань безпеки повинна бути спрямована на запобігання або виявлення найбільш ймовірної атаки.

У детермінованому аналізі передбачається, що вся інформація, яку потрібно знати для втручання експлойту, є відомою. Характеристики експлойту, такі як використання певних номерів портів, відомі з інших випадків втручання експлойту, або те, що використовуються стандартизовані порти . При ймовірнісному аналізі вважають, що номери портів, які підлягатимуть впливу, можна прогнозувати лише з певною мірою впевненості. У цій ситуації експлойт, що використовує, наприклад, динамічні номери портів, не може бути проаналізований детерміновано. Такі експлойти були оптимізовані, щоб уникнути виявлення брандмауерами, які використовують статичні правила.

Нижче наведено два підходи.

- **Детермінований аналіз–** для вдалої реалізації експлойту, усі його попередні кроки також мають бути успішними. Аналітик з кібербезпеки знає кроки для успішного експлойту.
- **Ймовірний аналіз –** для визначення ймовірності того, чи буде експлойт успішним, виходячи з імовірності вдалого виконання кожного його кроку.