УДК 004.056.5

Алладін МАБРОУК

Західноукраїнський національний університет

СИСТЕМА ВИЯВЛЕННЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ SECURITY ONION

Вступ. Кожен рік кіберзагрози стають дедалі складнішими, число атак на комп'ютерні мережі неухильно збільшується, тим самим створює нові виклики для системних адміністраторів та фахівців з інформаційної безпеки, тож тепер їхнє завдання не лише запобігти можливим атакам, але й уміти швидко виявити і проаналізувати загрози, аби мінімізувати шкоду від потенційних ризиків. В таких умовах стає особливо важливо використовувати ефективні інструменти для моніторингу та аналізу мережевого трафіку.

Один з таких інструментів це Security Onion, він пропонує потужний набір засобів виявлення, моніторингу та аналізу інцидентів мережевих трафіків. Завдяки Security Onion можна збирати і аналізувати інформацію про активність у мережі, які допомагають виявляти атаки на ранніх етапах, щоб швидше реагувати. SecurityOnion дозволяє організаціям будувати надійні механізми захисту, які знижують ризики й підвищують рівень безпеки мережевих ресурсів.

Мета: розкрити процес виявлення та аналізу кіберзагроз за допомогою системи Security Onion.

Основні етапи роботи Security Onion

Security Onion - це дистрибутив Linux, розроблений для виявлення вторгнень, моніторингу безпеки мережі та управління журналами.

Security Onion складається з кількох основних етапів (рисунок 1), кожен з яких відповідає за виконання окремих завдань у процесі моніторингу кібербезпеки.

1. Sensor - слідкує за мережевим трафіком і фіксує події, які відбуваються в мережі. Система отримує дані з різних джерел, таких як мережеві пристрої, сервери чи інші елементи інфраструктури. В результаті, збирається вся інформація про активність в мережі, що допомагає аналізувати потенційні загрози чи аномалію. Основні типи зібраних даних включають:

- журнали подій (Syslog), які містять записи про діяльність систем та інциденти безпеки;
- мережевий трафік, включаючи пакети даних, які можуть бути перевірені на наявність аномальної активності.

2. Обробка та фільтрація трафіку. Після збору дані направляються для обробки за допомогою інструментів, таких як Suricata та Zeek. Ці інструменти виконують наступні функції:

- Suricata аналізує мережеві пакети та шукає підозрілі шаблони, що можуть вказувати на атаки;
- Zeek здійснює аналіз мережевих сесій, виділяючи деталі про HTTP-запити, FTP-сеанси, DNS-запити тощо.

Таким чином, на цьому етапі відбувається початкове виявлення загроз через аналіз мережевого трафіку, що дозволяє виявити можливі інциденти кібербезпеки.

3. Генерація попереджень (Alerts). Якщо оброблені дані містять підозрілу активність, Security Onion створює попередження, яке записується в систему та відображається аналітикам. Попередження формуються в базі даних Elasticsearch, що дозволяє швидко та ефективно здійснювати пошук і фільтрацію інформації про загрози. Попередження можуть включати:

- інформацію про тип загрози (наприклад, DDoS-атака, спроба несанкціонованого доступу тощо);
- відомості про джерело і ціль атаки, що дозволяє оперативно реагувати на загрозу.

4. Аналіз та візуалізація даних. Аналітики кібербезпеки використовують Kibana та інші інструменти для візуалізації та пошуку за даними. Цей етап є важливим для ідентифікації тенденцій та детального аналізу кожного інциденту. Візуалізація даних допомагає швидко виявляти аномалії і спрощує процес аналізу, що дозволяє:

- швидко ідентифікувати джерела загроз;
- оцінювати, як певні події впливають на загальну безпеку мережі.

5. Зберігання даних (Storage Nodes). Всі зібрані та оброблені дані зберігаються на спеціальних серверах. Це важливо для детального розслідування минулих інцидентів і формування профілів загроз. Збереження даних дозволяє:

- проводити ретроспективний аналіз для виявлення схожих інцидентів;
- оцінювати поведінку кіберзлочинців і визначати нові тактики, техніки і процедури, що використовуються під час атак.

6. Планування та управління інцидентами. Необхідно спланувати процес на реагування інцидентів для миттєвої реакції загроз, цей процес допомагає:

- швидко реагувати на інцидент та зупинити загрозу;
- зменшити час на відновлення після інциденту.

7. Індексація даних в Elasticsearch. Компонент seraElasticsearch Index відіграє важливу роль у зберіганні та індексації даних про безпеку, що надходять з різних джерел. Його основні завдання включають:

- збирання даних: Отримання інформації з різних систем моніторингу та безпеки, таких як IDS/IPS, мережевий трафік і журнали подій;
- індексація в Elasticsearch: Дані індексуються для того, щоб їх можна було швидко знайти та проаналізувати. Це дозволяє зберігати велику кількість інформації та ефективно працювати з нею;
- зберігання та пошук: Індексовані дані зберігаються в Elasticsearch, що забезпечує швидкий доступ до них через пошукові запити. Це допомагає оперативно знаходити необхідні відомості за конкретними параметрами, такими як час або тип події;
- візуалізація та аналіз: Дані, що зберігаються в Elasticsearch, можна візуалізувати у Kibana, що полегшує їх аналіз і виявлення можливих інцидентів безпеки.

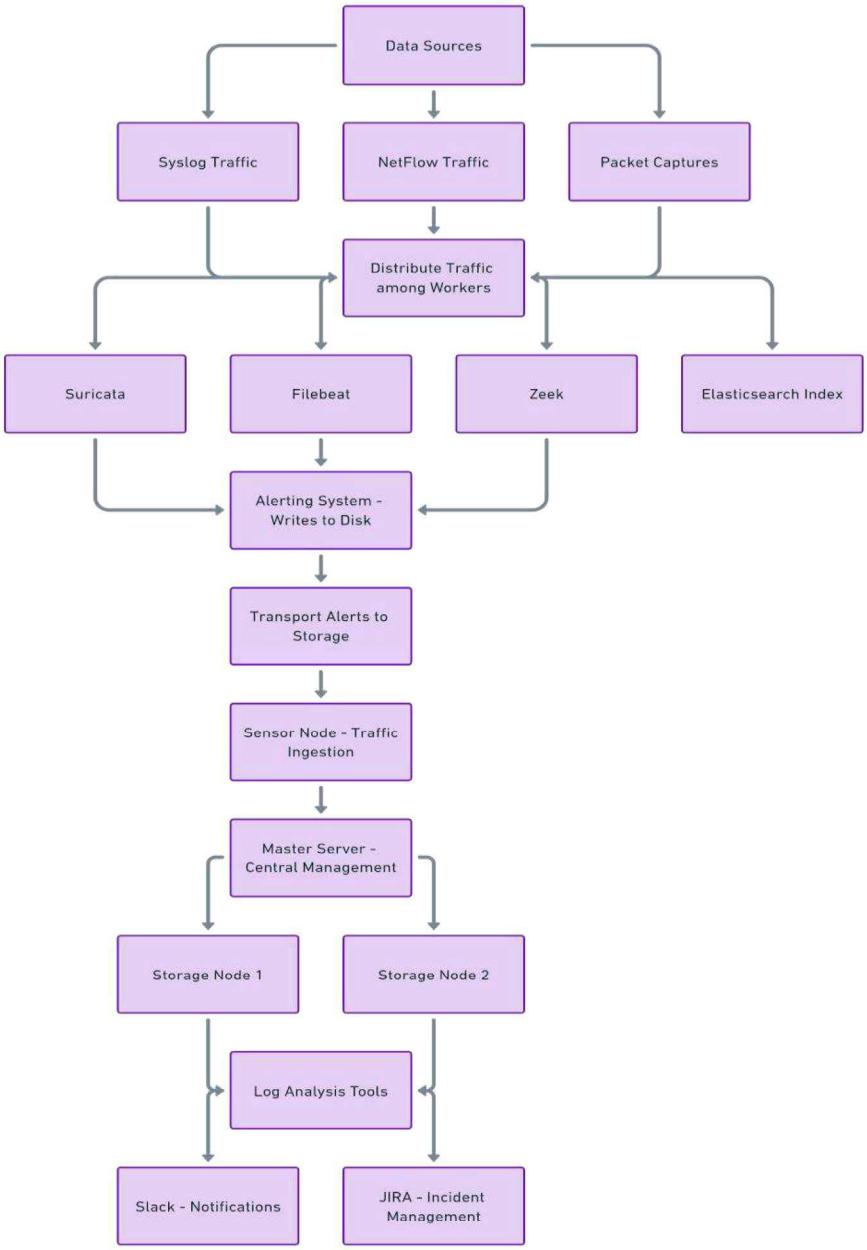

Рисунок 1 - Архітектура компонента в SecurityOnion

Висновок. Security Onion надає все необхідне для забезпечення моніторингу трафіку, надаючи системним адміністраторам та фахівцям інформаційної безпеки інструменти для швидкого виявлення та реагування на загрози. Це рішення допомагає організаціям забезпечити високий рівень безпеки у своїх мережевих ресурсів, запобігаючи та аналізуючи інциденти кібербезпеки в реальному часі та в довгостроковій перспективі. Завдяки структуруванню даних та їх візуалізації, система SecurityOnion є ефективним інструментом для забезпечення захисту в умовах сучасних кіберзагроз.

Перелік використаних джерел.

1. Security Onion Documentation [Електронний ресурс]. - Режим доступу: https://docs.securityonion.net/en/2.4/

2. Elastic Architecture [Електронний ресурс]. - Режим доступу: https://github.com/security-onion-solutions/security-onion/wiki/Elastic-Architecture