ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Кваліфікаційна робота
на тему:

«Технологія виявлення зловмисної активності в інформаційній системи організації на базі IBM QRadar DNS Analyzer»

Виконав: КАРПЕНКО Владислав, БСДМ-61
Керівник: ГАХОВ Сергій Олександрович, к.військ.н., доц.

Актуальність. Виявлення зловмисної активності є важливим компонентом комплексної стратегії кібербезпеки, що дозволяє організаціям виявляти загрози на ранніх стадіях і вживати заходів для запобігання шкоди, яку вони можуть завдати.

Об'єкт дослідження – процес виявлення зловмисної активності в інформаційній системі організації

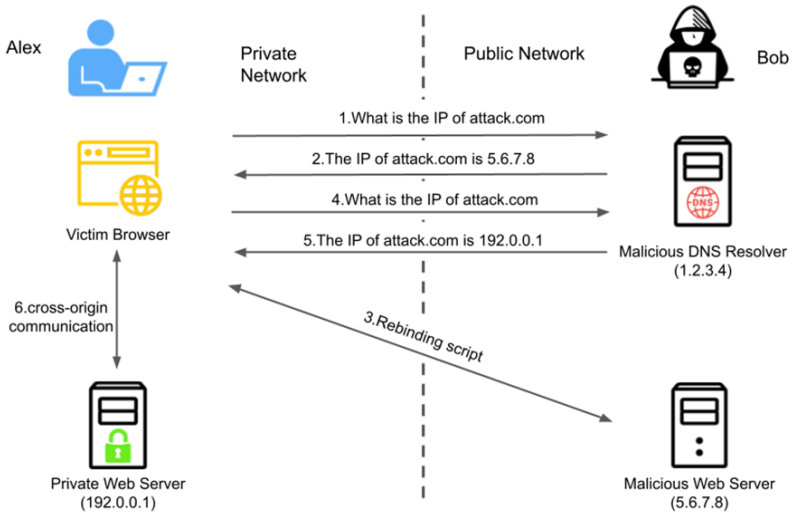
Предмет дослідження – технологія виявлення зловмисної активності в інформаційній системі організації на базі IBM QRadar DNS Analyzer

Мета роботи – розробити порядок застосування технології виявлення зловмисної активності в інформаційній системі організації та рекомендації щодо її реалізації

Наукові завдання:

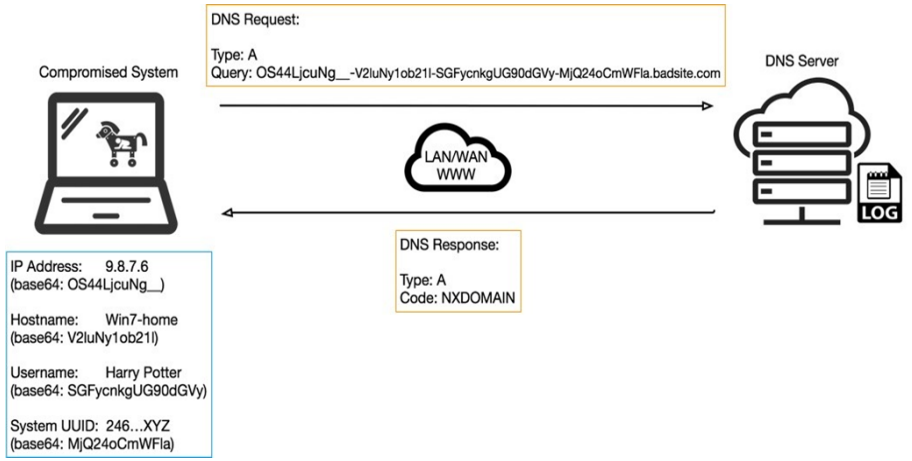
- дослідити проблему виявлення зловмисної активності в інформаційній системі організації;
- проаналізувати існуючі підходи до виявлення зловмисної активності в інформаційних системах;
- проаналізувати методи та засоби виявлення зловмисної активності в інформаційній системі організації на базі IBM QRadar DNS Analyzer;
- розглянути порядок застосування IBM QRadar DNS Analyzer для виявлення зловмисної активності в інформаційній системі організації;
- запропонувати рекомендації щодо застосування технології виявлення зловмисної активності в інформаційній системі організації.

Дослідження проблеми виявлення зловмисної активності в інформаційних системах



Зловмисники щодня реєструють тисячі нових доменів, готуючись до майбутніх зловмисних дій, таких як обслуговування серверів C2, розміщення шкідливих програм і доставка оманливого вмісту. Більшість існуючих детекторів зловживань доменом зосереджені на пошуку шаблонів DNS – пошуку поточних атак і активному скануванні веб-контенту на наявність шкідливих індикаторів. На рисунку наведено приклад механізму атаки переприв'язування DNS.

Розглянемо інший приклад, де клієнтську систему скомпрометовано зловмисним програмним забезпеченням, яке створює дивні рядки запиту для надсилання через DNS. Подібні запити все ще діють як серцеві сигнали, що вказують зловмиснику, що його корисне навантаження все ще активне, однак вони також надають деякі основні метадані про жертву і, що важливо, способи унікального визначення однієї жертви від іншої.



Аналіз існуючих підходів до виявлення зловмисної активності в DNS інформаційної системи організації

Необхідно відмітити, що існують хробаки та шкідливі програми для створення DNS-пакетів, які порушують формат дійсного заголовка DNS. Це можна виявити на рівні мережі, а також у добре відформатованому сценарії на основі хоста, який має можливість аналізувати пакети та декодувати трафік DNS для перевірки. Коли ми виявимо аномалії, ми зможемо переглянути елементи дій для вихідних IP-адрес.

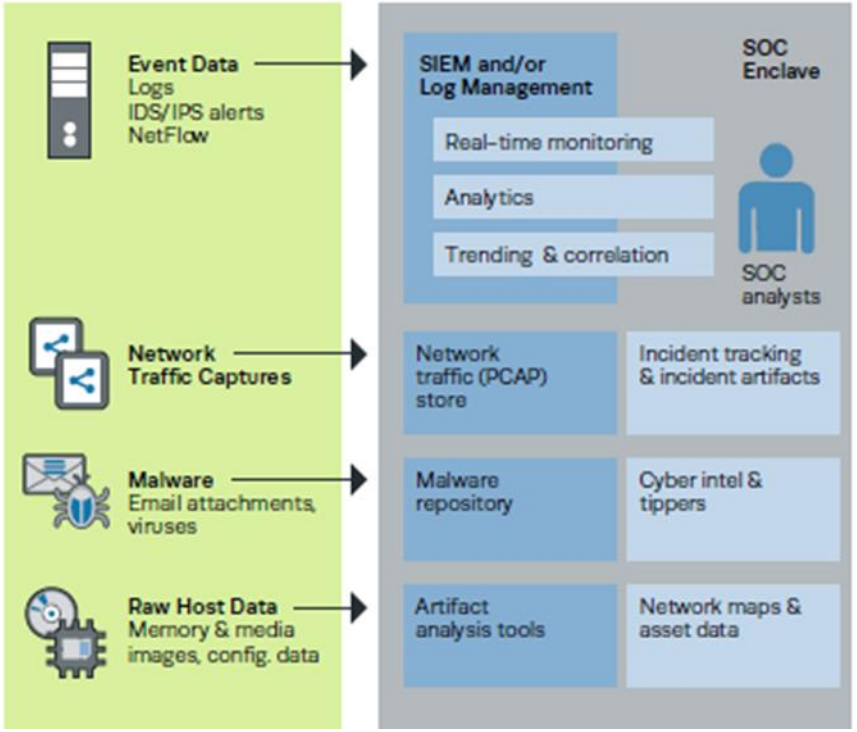
Для виявлення аномалій DNS є *дві групи методів*. Перша група методів аналізує пакети на наявність аномалій DNS у даних, які вони містять. Ці методи виявлення можна виконувати в режимі реального часу в міру надходження пакетів. Друга група методів виконує статистичний аналіз великої кількості даних. Це дозволяє нам виявляти аномалії в обсягах запитів або відповідях на запити з часом.

Загалом *чорний список* використовується для заборони доступу до певних хостів, оскільки вони відомі як шкідливі. Чорний список можна створити шляхом поєднання різних популярних чорних списків для перевірки запиту. Механізм перевірки чорного списку заснований на принципі: якщо він у списку, він шкідливий. Цей метод, ймовірно, визначить аномальний DNS-трафік, що викликається людиною.

Тунельне виявлення DNS. Оскільки дані DNS часто погано контролюються і часто пропускаються через брандмауер, це ідеальний кандидат для прихованого каналу. Пакети DNS можна використовувати для створення прихованого каналу даних. Існує велика кількість способів приховати дані в законних пакетах DNS

Існують й інші методи. Загалом, моніторинг DNS-трафіку є важливим компонентом комплексної стратегії кібербезпеки, що допомагає організаціям своєчасно виявляти потенційні загрози та реагувати на них.
Існують різні типи зловмисної активності, які можна виявити в DNS-трафіку організації: алгоритми генерації доменів (DGA), командно-контрольні (C2) комунікації, витік даних, атаки посилення DNS, шкідливі домени тощо.

Роль і місце виявлення зловмисної активності в інформаційній системі

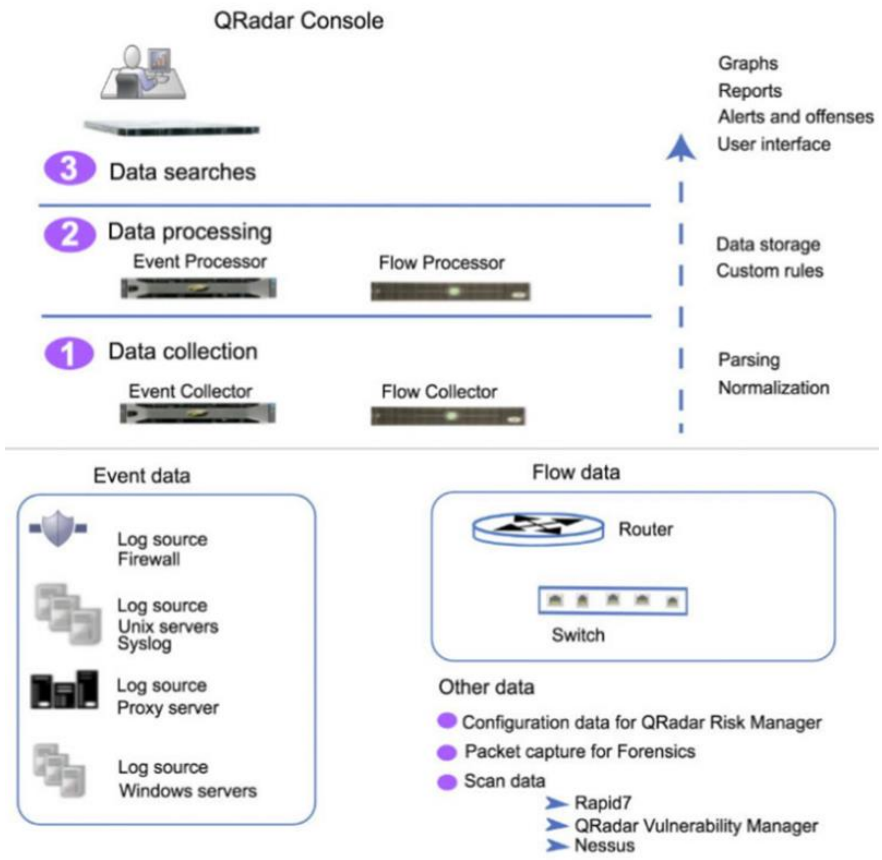


Необхідно відмітити, що успіх або невдача в забезпеченні кібербезпеки інформаційних ресурсів організації залежить від здатності фахівців SOC зібрати і зрозуміти потрібні дані в потрібний час та в потрібному контексті. Практично кожен зрілий SOC використовує набір технологій для створення, збору, аналізу, зберігання та подання величезної кількості даних для своєї команди. На рисунку зображено високорівнева архітектура використовуваних в SOC інструментів і технологій.

SOC може розміщувати інструменти моніторингу в різних точках інформаційної системи організації для пошуку зловмисної або аномальної активності на кожному етапі життєвого циклу кібератаки. Так, наприклад, особливий інтерес для аналітиків SOC можуть представляти ключові хости і «вузькі місця» мереж. Кожен інструмент генерує серію подій і контекстних даних, які після вивчення можуть бути доказом інциденту.

Відстежуючи та аналізуючи ці події, фахівці з кібербезпеки можуть виявляти потенційні загрози безпеці та реагувати на них до того, як вони завдадуть значної шкоди організації.

Призначення та можливості рішення IBM QRadar SIEM



У сфері кібербезпеки управління інформацією та подіями безпеки (Security Information and Event Management, SIEM) розглядається як серія технологій, що відповідають за аналіз, зменшення загроз і реєстрацію подій безпеки у визначеній мережі. SIEM надає загальне уявлення про всю технічну інфраструктуру, з конкретними даними про події безпеки, а також про пом'якшення наслідків для цих інфраструктур.

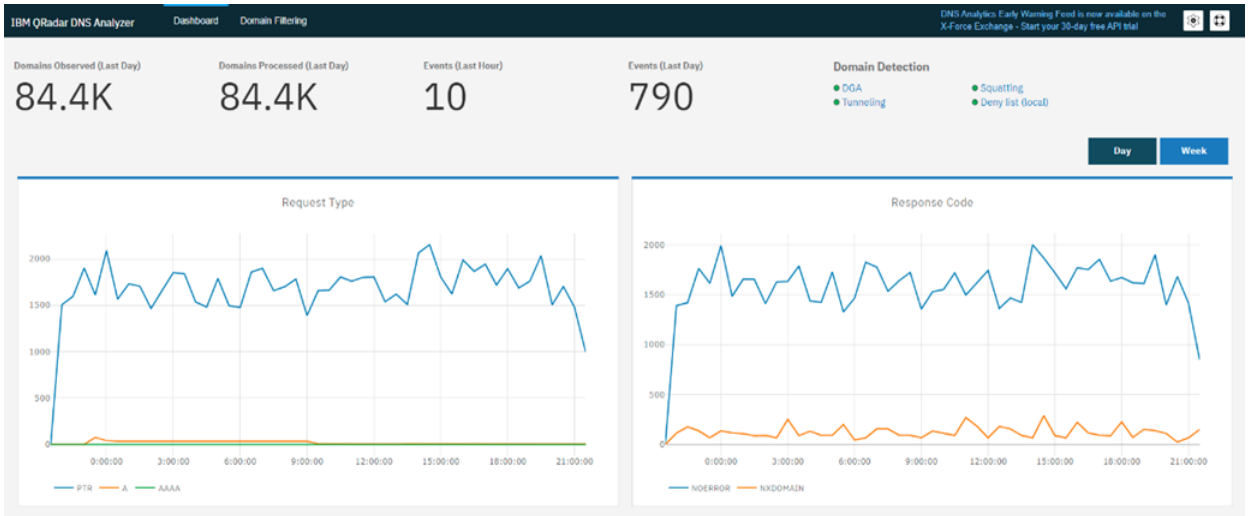
Рівні, представлені на рисунку, складають основну функціональність будь-якої системи IBM QRadar.
Збір даних – це перший рівень архітектури. На цьому рівні система IBM QRadar отримує дані, такі як події та потоки, які вона отримує від мережевих пристроїв.

Обробка даних. Після збору даних, другий рівень обробки даних полягає в тому, що система IBM QRadar обробляє ці дані за допомогою компонента Custom Rule Engine (CRE). Після того, як компонент CRE обробив дані, система може генерувати порушення і попередження, щоб потім записати або зберегти дані в сховище.

Пошук даних – на цьому рівні зберігаються дані, які були зібрані та оброблені системою, і вони доступні для використання в пошуках, звітах, оповіщеннях та розслідуванні порушень.

Призначення та можливості рішення IBM QRadar DNS Analyzer

IBM QRadar DNS Analyzer – це рішення для аналізу безпеки, призначене для аналізу DNS-трафіку і виявлення потенційних ризиків безпеки або зловмисної активності. Воно дозволяє організаціям виявляти і розслідувати інциденти безпеки, пов'язані з DNS, а також допомагає їм визначати пріоритети і більш ефективно реагувати на події безпеки.



Деякі з ключових можливостей IBM QRadar DNS Analyzer включають:

- моніторинг і аналіз DNS-трафіку в режимі реального часу. Додаток може відстежувати DNS-запити і відповіді в режимі реального часу і надавати детальну інформацію про мережеву активність;

- додаток може виявляти різні загрози на основі DNS, такі як DNS-тунелювання, DNS-ексфільтрація та перехоплення DNS;
- IBM QRadar DNS Analyzer може інтегруватися з іншими інструментами безпеки, такими як брандмауери, системи виявлення вторгнень і SIEM, щоб забезпечити більш повне уявлення про загрози безпеки;
- додаток надає настроювані інформаційні панелі і звіти, які дозволяють командам безпеки швидко виявляти і розслідувати потенційні інциденти безпеки.

В цілому, IBM QRadar DNS Analyzer є потужним інструментом для організацій, які прагнуть поліпшити свою систему безпеки DNS і знизити ризик атак на основі DNS.

Порядок застосування додатка QRadar DNS Analyzer

Варіант	опис
Присідання	• **Обробка** . Виявляє доменні імена, тісно пов'язані з торговою маркою, брендом або популярним веб-сайтом. • **Місцеві події** - Створює події сквотінгу домену.
DGA	• **Обробка** – визначення доменного імені, створеного за допомогою алгоритму (DGA). DGA зазвичай використовується в наборах для фішингу для створення випадкового та унікального доменного імені. За замовчуванням він завжди ввімкнено. • **Локальні події** – увімкніть цей параметр, щоб створювати події DGA.
Список заборонених	• **Обробка** - Виявляє доменні імена з негативною репутацією. За замовчуванням він завжди ввімкнено. • **Локальні події** – створює події зі списку заборонених.
Тунелювання	• **Обробка** – Виявляє доменні імена за допомогою даних, закодованих у запитах і відповідях DNS. • **Локальні події** - створює події тунелювання.

QRadar DNS Analyzer безперервно відстежує DNS-трафік в режимі реального часу, що дозволяє йому швидко виявляти і реагувати на потенційні загрози безпеці.

Налаштування параметрів додатка включає в себе кілька кроків, які описані нижче:

- встановіть та увімкніть додаток QRadar DNS Analyzer у консолі QRadar;

- додайте DNS-сервери, які додаток повинен використовувати для пошуку DNS;
- налаштуйте мережеву ієрархію, щоб визначити сегменти мережі, які повинні контролюватися додатком QRadar DNS Analyzer;
- налаштуйте джерела даних для QRadar DNS Analyzer, вибравши джерела журналів, які повинні використовуватися для подій DNS;
- налаштуйте правила, які слід використовувати для виявлення загроз безпеці DNS;
- налаштуйте еталонні набори, які слід використовувати для виявлення відомих DNS-загроз;
- налаштуйте порушення, які слід створювати, коли виявлено загрозу безпеці DNS;
- протестуйте конфігурацію, згенерувавши тестовий DNS-трафік або використовуючи тестове середовище.

Рекомендації щодо застосування технології виявлення зловмисної активності в інформаційній системі організації

У роботі запропоновано такі основні рекомендації щодо виявлення та моніторингу зловмисної активності в DNS-трафіку організації:

- впроваджуйте протоколи безпеки DNS: розширення безпеки DNS (DNSSEC), безпека системи доменних імен (DNSSEC) і DNS через HTTPs (DoH) можуть допомогти захиститися від підміни DNS та інших атак;
- використовуйте канали розвідки загроз: інтеграція каналів розвідки загроз із журналами DNS може допомогти виявити зловмисні домени та IP-адреси. Ці канали можуть містити дані про відоме шкідливе програмне забезпечення, фішингові сайти та інші загрози;
- аналізуйте журнали DNS: аналіз журналів DNS може допомогти виявити аномальну поведінку та шаблони, наприклад, надмірну кількість DNS-запитів з одного пристрою або доменне ім'я, яке часто запитується;
- використовуйте машинне навчання: алгоритми машинного навчання можуть аналізувати DNS-трафік у режимі реального часу, виявляючи аномалії та шаблони, які можуть свідчити про зловмисну активність;
- відстежуйте DNS-тунелювання: тунелювання DNS – це метод, який використовується зловмисниками для обходу засобів захисту і витоку даних. Моніторинг цього типу активності може допомогти виявити і запобігти витоку даних;
- впровадження DNS-тунелю: DNS-тунель – це DNS-сервер, який налаштований на перенаправлення шкідливих доменних імен на неіснуючу IP-адресу. Це може запобігти зв'язку заражених пристроїв зі шкідливими доменами, а також забезпечити видимість активності цих пристроїв;
- регулярно оновлюйте та виправляйте DNS-сервери: оновлення та виправлення DNS-серверів може допомогти запобігти використанню відомих вразливостей.

В цілому, моніторинг DNS-трафіку може надати цінну інформацію про потенційні загрози безпеці і допомогти організаціям проактивно виявляти і реагувати на зловмисну активність.

ВИСНОВКИ

- В роботі проведено дослідження та аналіз проблеми виявлення зловмисної активності в інформаційній системі організації. Виявлення зловмисної активності є важливим компонентом комплексної стратегії кібербезпеки, що дозволяє організаціям виявляти загрози на ранніх стадіях і вживати заходів для запобігання шкоди, яку вони можуть завдати. Так, атака повторного переприв'язування DNS може скомпрометувати браузери жертв як тунелі трафіку для використання приватних служб. За допомогою цієї техніки зловмисники можуть викрасти конфіденційну інформацію та надсилати підроблені запити на сервери жертв. Браузери, резолвери та веб-додатки застосовували різні стратегії для захисту від нього. Однак існують розширені експлойти, які можуть обійти традиційний захист. Крім того, важче забезпечити повний захист, оскільки внутрішнє мережеве середовище стає складнішим.
- Проаналізовано існуючі підходи до виявлення зловмисної активності в інформаційних системах. Так, моніторинг DNS-трафіку є важливим компонентом комплексної стратегії кібербезпеки, що допомагає організаціям своєчасно виявляти потенційні загрози та реагувати на них.
- Досліджено методи та засоби виявлення зловмисної активності в інформаційній системі організації на базі IBM QRadar DNS Analyzer. Моніторинг процесів функціонування інформаційної системи організації з точки зору кібербезпеки передбачає систематичне спостереження та аналіз подій і дій, пов'язаних з безпекою, для виявлення потенційних порушень безпеки та вразливостей в системі. Метою є своєчасне виявлення та реагування на інциденти безпеки для запобігання або мінімізації їх впливу на організацію.

ВИСНОВКИ

- IBM QRadar DNS Analyzer – це рішення для аналізу безпеки, призначене для аналізу DNS-трафіку і виявлення потенційних ризиків безпеки або зловмисної активності. Воно дозволяє організаціям виявляти і розслідувати інциденти безпеки, пов'язані з DNS, а також допомагає їм визначати пріоритети і більш ефективно реагувати на події безпеки.
- Додаток IBM QRadar DNS Analyzer надає інформацію про локальний DNS-трафік організації, виявляючи зловмисну активність і дозволяючи команді фахівців з безпеки виявляти алгоритм генерування доменів (DGA), тунелювання або самовільне захоплення доменів, до яких здійснюється доступ з корпоративної мережі.
- Розглянуто порядок застосування IBM QRadar DNS Analyzer для виявлення зловмисної активності в інформаційній системі організації. Додаток QRadar DNS Analyzer надає додаткові можливості щодо виявлення зловмисної активності в інформаційній системі організації. Правильне налаштування параметрів даного додатка забезпечить ефективне виявлення та своєчасне реагування на наявну зловмисну активність в мережі організації.
- Запропоновано рекомендації фахівцям з кібербезпеки щодо застосування технології виявлення зловмисної активності в інформаційній системі організації.

В цілому, моніторинг DNS-трафіку може надати цінну інформацію про потенційні загрози безпеці і допомогти організаціям проактивно виявляти і реагувати на зловмисну активність.

Тому, правильне застосування технології виявлення зловмисної активності в інформаційних системах має забезпечити ефективний захист інформаційних ресурсів організацій.

Дякую за увагу!
Доповідь закінчено