УДК 004.056
DOI: 10.31673/2409-7292.2021.031723

Ішметов І.С., Гуляєва О.І., Нечипуренко К.О.

УДОСКОНАЛЕНА ТЕХНОЛОГІЯ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ РІШЕННЯ IBM QRADAR INCIDENT FORENSICS

В роботі зроблено аналіз проблеми забезпечення кібербезпеки корпоративної інформаційної системи та визначено місце, мета та завдання розслідування кіберінцидентів корпоративної інформаційної системи. Проведено аналіз існуючих технологій розслідування кіберінцидентів корпоративної інформаційної системи. Досліджено методи та засоби розслідування кіберінцидентів корпоративної інформаційної системи на базі рішення IBM QRadar Incident Forensics. Визначено призначення, основні функції та склад комплексу IBM QRadar Incident Forensics. На основі досліджень проведених в роботі розроблено варіант технології розслідування кіберінцидентів корпоративної інформаційної системи та рекомендації щодо застосування цієї технології на підприємстві. Досліджено технологію інтеграції IBM QRadar SIEM та IBM QRadar Incident Forensics, застосування якої підвищує ефективність діяльності фахівців Центру управління кібербезпекою корпоративної інформаційної системи.

Ключові слова: корпоративна інформаційна система, кібербезпека, кіберінцидент, розслідування кіберінцидентів.

Вступ

За даними IBM X-Force [1] у 2019 було здійснено витік 8,5 мільярда записів, що дало зловмисникам доступ до більшої кількості вкрадених облікових даних. На сьогоднішній день виявлено більше ніж 150 000 вразливостей апаратного та програмного забезпечення. У четвертому кварталі 2019 року кількість атак програм-вимагачів збільшилася на 67% в порівнянні з аналогічним періодом минулого року. Кількість атак на операційні технології (OT) зросла в двадцять разів у порівнянні з минулим роком. Це визначає актуальність дослідження щодо розслідування кіберінцидентів у корпоративних інформаційних системах.

Аналіз проблеми

Цільові атаки (Advanced Persistent Threat) є серйозною проблемою в сфері інформаційної та кібербезпеки, яка турбує не тільки великі корпорації. Під прицілом хакерів знаходяться також підприємства середнього і малого бізнесу. Організовані угрупування вибирають цілями кібератак компанії в різноманітних сферах таких, як охорона здоров'я, IT, освіта та інші. Виділяються три основні канали проникнення шкідливого програмного забезпечення в корпоративні інформаційні системи. Перший – підбір пароля до сервісів VPN та/або RDP, другий – перехід користувача по зараженим посиланнях в будь-яких браузерах і третій, найбільш поширений, – через фішинговий лист.

Сучасні організації та підприємства зіштовхуються з хакерськими атаками, відмовою в обслуговуванні, шахрайством або з крадіжкою конфіденційних даних. Надійно захищені, цілісні логи дій користувачів не тільки забезпечують важливі докази в разі розслідування інцидентів, а й дають впевненість в тому, що можна точно визначити причину інциденту, навіть якщо вона лежить за межами області моніторингу. Використовуючи зібрані логи разом з поведінкової аналітикою, компанії можуть значно зменшити час розслідування, знизити витрати і при цьому реагувати на новітні загрози в режимі реального часу.

Мета роботи – розробити варіант технології розслідування кіберінцидентів корпоративної інформаційної системи та рекомендації щодо застосування цієї технології на підприємстві.

Можливості IBM QRadar Incident Forensics для розслідування кіберінцидентів

Необхідно підкреслити, що фахівцям з кібербезпеки гостро потрібні технології, методи та засоби, які б підвищили ефективність їх діяльності, у тому числі, з реагування, розслідування інцидентів та відновлення після них.

На наш погляд таким засобом є рішення IBM QRadar Incident Forensics.

Особливостями рішення IBM QRadar Incident Forensics є [2]:

розслідування інцидентів безпеки за допомогою пакетів, захоплених з корпоративної мережі;

простий процес запиту за допомогою інтерфейсу, подібний будь-якій пошуковій системі;

інтеграція з рішеннями IBM QRadar і існуючими форматами захоплення пакетів (PCAP) для декодування, індексації, відновлення і аналізу даних;

створення декількох уявлень даних, включаючи взаємозв'язки, часові рамки, джерело і категорію загроз;

створення нових інтелектуальних можливостей, виділяючи підозрілий контент, додаючи категоризації URL-адрес і візуально відображаючи цифрові враження користувачів або додатків;

надання допомоги у вирішенні виявлених інцидентів, в більшості випадків за хвилини або години, а не за дні або тижні.

IBM QRadar Incident Forensics це рішення на основі програмного і апаратного забезпечення, розроблене для того, щоб надати фахівцям з кібербезпеки підприємства кращу видимість і ясність в мережевих діях, пов'язаних з інцидентами безпеки. Потім це розуміння може бути використано, щоб допомогти у виявленні в повній мірі інциденту мережевої безпеки, усунення пошкоджень і зниження ймовірності крадіжки даних або повторення минулих порушень [2].

Простий інтерфейс (рис. 1), схожий на пошукову систему, дозволяє здійснювати інтуїтивний пошук даних, пов'язаних з порушенням безпеки, включаючи дані в стані спокою (документи) або в русі (захоплення пакетів), структуровані або неструктуровані дані, а також документи і файли, починаючи від повідомлень електронної пошти, голосових – телефонні дзвінки по IP (VoIP), відвідування веб-сайтів, повідомлення в блогах і навіть вкладення в повідомленнях, такі як файли або зображення.

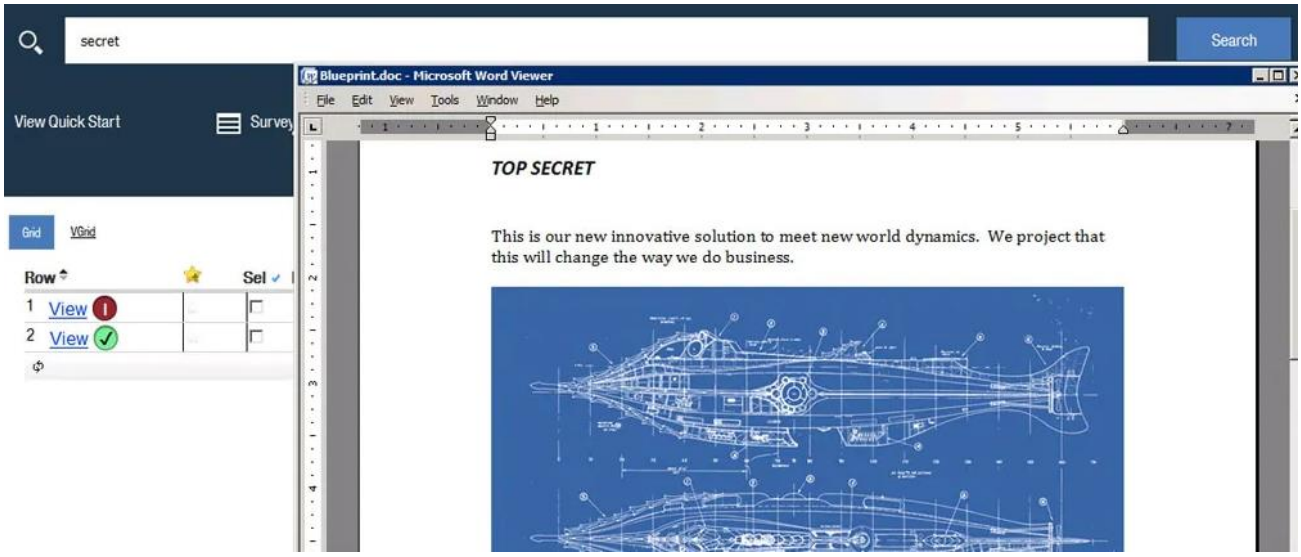

Рис. 1. Приклад інтерфейсу як результату функціонування QRadar Incident Forensics

QRadar Incident Forensics індексує і корелює всі ці дані, віддаючи пріоритет продуктивності пошуку, щоб допомогти швидко відрізнити справжні загрози від хибно-позитивних результатів, що генеруються існуючим правилом кореляції SIEM. Відновлюючи необроблені мережеві дані назад в їх первісну форму і відстежуючи інциденти безпеки, рішення QRadar Incident Forensics надає цінну інформацію, яка допомагає підтримувати безпеку мережі, аналізувати і запобігати зовнішні атаки і внутрішні загрози, а також документувати свідчення, пов'язані з інцидентами.

Розслідування, що виходять за рамки простого захоплення пакетів

QRadar Incident Forensics легко інтегрується з IBM QRadar Security Intelligence Platform (рис. 2), використовуючи інтерфейс управління з однієї консоллю. Сумісне зі стандартними форматами PCAP, рішення дозволяє проводити спрямований аналіз з метою виявлення порушень QRadar або можливих умов атаки, виявлених зовнішніми джерелами інформації про загрози, такими як IBM X-Force. Він забезпечує видимість і розслідування інцидентів безпеки в усій мережевій інфраструктурі організації або підприємства.

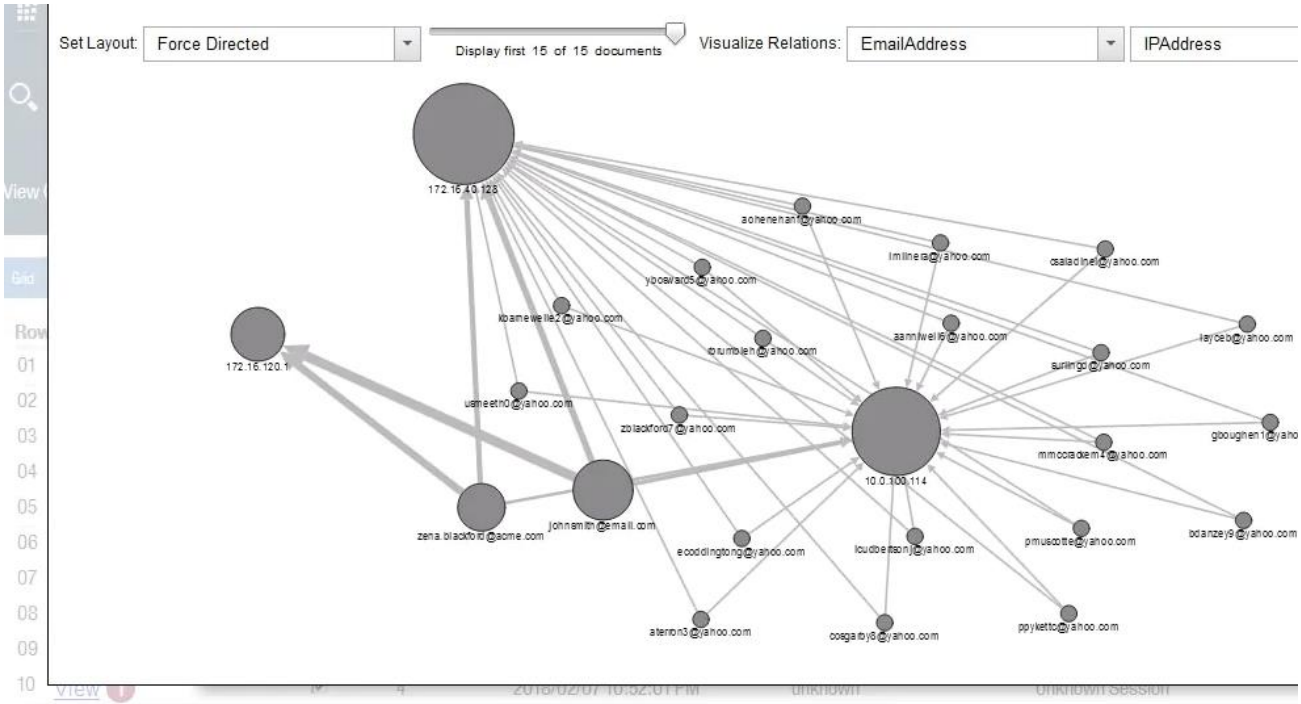

Рис. 2. Приклад інтерфейсу як результату інтеграції рішень IBM QRadar Security Intelligence Platform

QRadar Incident Forensics, на відміну від менш комплексних рішень, не тільки витягує більш придатні для використання дані з PCAP, але також може імпортувати пов'язані документи і файли і робити всі ці матеріали доступними для дослідження даних на основі пошуку. Дане рішення підвищує продуктивність пошуку за рахунок потужної функції індексування, яка індексує метадані та фактичне корисне навантаження PCAP або файлових документів. Це дозволяє аналітику виконувати пошук на основі тексту, який може включати числа, дати або ключові слова. Рішення підтримує як розслідування підозрілої активності в режимі реального часу, так і реконструкцію попередніх дій, повертаючи результати пошуку в більшості випадків за секунди.

Таким чином, у рішенні IBM QRadar Incident Forensics реалізована потужна інформаційна технологія, застосування якої забезпечить ефективність діяльності фахівців з кібербезпеки щодо розслідування інцидентів інформаційної та кібербезпеки. Даний момент обґрунтовує необхідність подальшого дослідження можливостей даного рішення та шляхів удосконалення діяльності фахівців з кібербезпеки.

Варіант архітектури рішення IBM QRadar Incident Forensics та її розгортання

Програмне забезпечення QRadar Incident Forensics встановлюється на власний фізичний або віртуальний пристрій. QRadar Incident Forensics повинен бути встановлений в операційній системі Red Hat Enterprise Linux [3].

На рис. 3. показано основні компоненти архітектури IBM QRadar Security Intelligence Platform.

Для більшості розгортань встановлюється консоль QRadar, принаймні один процесор QRadar Incident Forensics і один або кілька пристроїв QRadar Network Packet Capture.

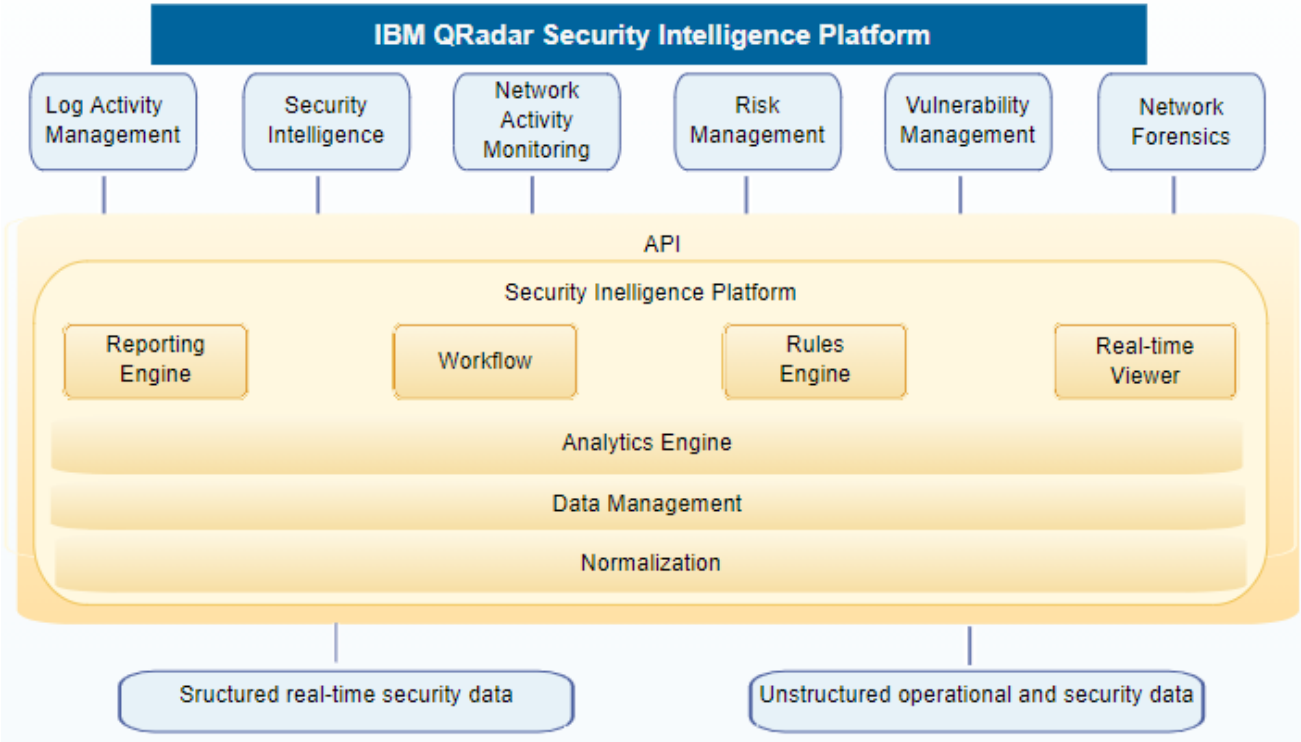

Рис. 3. Основні компоненти архітектури IBM QRadar Security Intelligence Platform [3]

Автономне розгортання IBM QRadar Incident Forensics

IBM QRadar Incident Forensics Standalone це розгортання одного пристрою, який аналогічно розгортанню консолі QRadar і керованого хоста QRadar Incident Forensics на одному пристрої. Це рішення для мережевої криміналістики, що зазвичай називають розгортанням «все в одному», не включає в себе можливості управління журналами або моніторингу мережевої активності. Для цього встановлюється QRadar Incident Forensics Standalone (ідентифікатор пристрою 6100) з ISO-образу QRadar Incident Forensics.

Розподілене розгортання IBM QRadar Incident Forensics

Розподілене розгортання QRadar Incident Forensics включає консоль QRadar і один або кілька керованих хостів QRadar Incident Forensics. Цей тип розгортання включає в себе управління подіями і журналами, виявлення аномалій, управління ризиками, управління вразливостями, а також дає можливість розподіляти робоче навантаження для криміналістичних відновлень.

У розподіленому розгортанні є три види пристроїв рис. 4:

консоль QRadar;

керований хост QRadar Incident Forensics (Forensics processor);

QRadar Network Packet Capture (optional) – пристрій захоплення пакетів.

Версії програмного забезпечення для всіх пристроїв IBM QRadar в розгортанні повинні бути однією версією і рівня виправлень. Розгортання, що використовують різні версії програмного забезпечення, не підтримуються.

На рис. 4 показано, що до консолі QRadar можна підключити декілька керованих хостів QRadar Incident Forensics. Пристрої QRadar Network Packet Capture підєднуються до керованих хостів QRadar Incident Forensics (QRadar Incident Forensics Processor).

Основні компоненти QRadar Incident Forensics, які реалізують технологію розслідування інцидентів (рис. 5) [4]:

QRadar Console надає користувальницький інтерфейс продукту, а також уявлення в режимі реального часу щодо подій і потоків, звіти, порушення, інформацію щодо активів, а також забезпечує адміністрування.

У розподіленому розгортанні QRadar консоль QRadar використовується для адміністрування інших хостів, керованих QRadar.

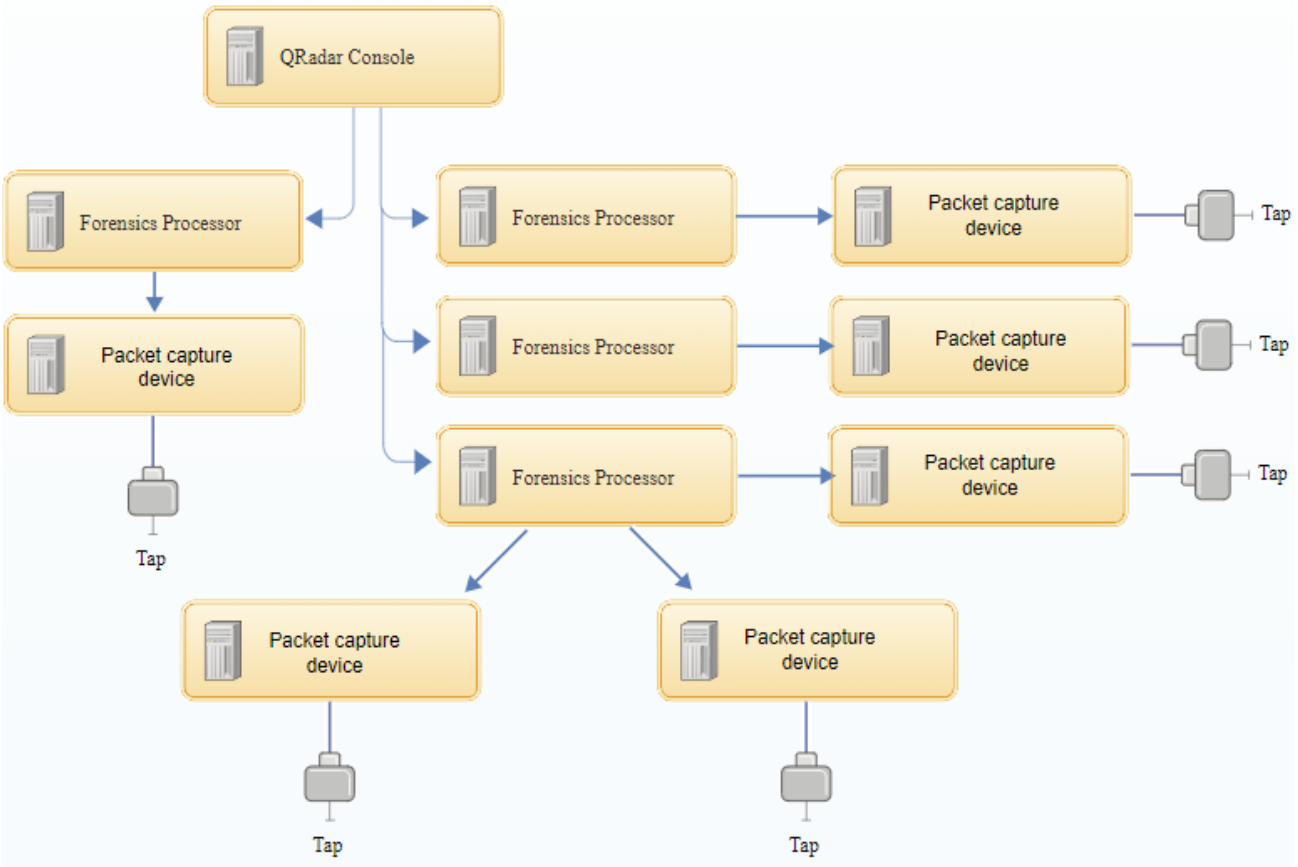

Рис. 4. Схема розподіленого розгортання IBM QRadar Incident Forensics [3]

QRadar Flow Processor – на нього надходять процеси від одного або декількох пристроїв QRadar QFlow Collector. Пристрій Flow Processor також може збирати зовнішні мережеві потоки, такі як NetFlow, J-Flow і sFlow, безпосередньо від маршрутизаторів у корпоративній мережі. Пристрій Flow Processor застосовується для масштабування розгортання QRadar для задоволення більш високих швидкостей потоку в хвилину.

QRadar Data Node – вузли даних дозволяють за необхідності новим та існуючим розгортанням QRadar додавати сховище і обчислювальну потужність. Вузли даних допомагають збільшити швидкість пошуку в корпоративному розгортанні, надаючи більше апаратних ресурсів для виконання пошукових запитів.

QRadar QFlow Collector – колектор збирає потоки шляхом підключення до порту SPAN або мережевого TAP. Пристрій також підтримує збір даних з зовнішніх джерел на основі потоків, таких як NetFlow з маршрутизаторів.

QRadar Incident Forensics Processor забезпечує даними користувальницький інтерфейс рішення QRadar Incident Forensics. Інтерфейс надає інструменти для покрокового відстеження дій кіберзлочинців, відновлення необроблених мережевих даних, пов'язаних з інцидентом безпеки, пошуку за доступними неструктурованими даними і візуального відновлення сеансів і подій.

QRadar Incident Forensics Processor під’єднується як керований хост до консолі QRadar для використання можливості дослідження аналітики безпеки для розслідування інцидентів. Є можливість підключення до п'яти пристроїв захоплення пакетів до QRadar Incident Forensics Processor або до автономного пристрою IBM QRadar Incident Forensics.

QRadar Network Packet Capture – додаткові пристрої захоплення пакетів застосовуються для зберігання і управління даними, які використовуються QRadar Incident

Forensics, коли у мережевому середовищі не розгорнуто інший пристрій захоплення пакетів. Можна встановити будь-яку кількість цих пристроїв в якості мережевого захоплювача для збору необроблених пакетних даних. Якщо пристрій захоплення пакетів не підключено, є можливість ручного завантаження файлів захоплення пакетів в інтерфейсі або за допомогою FTP.

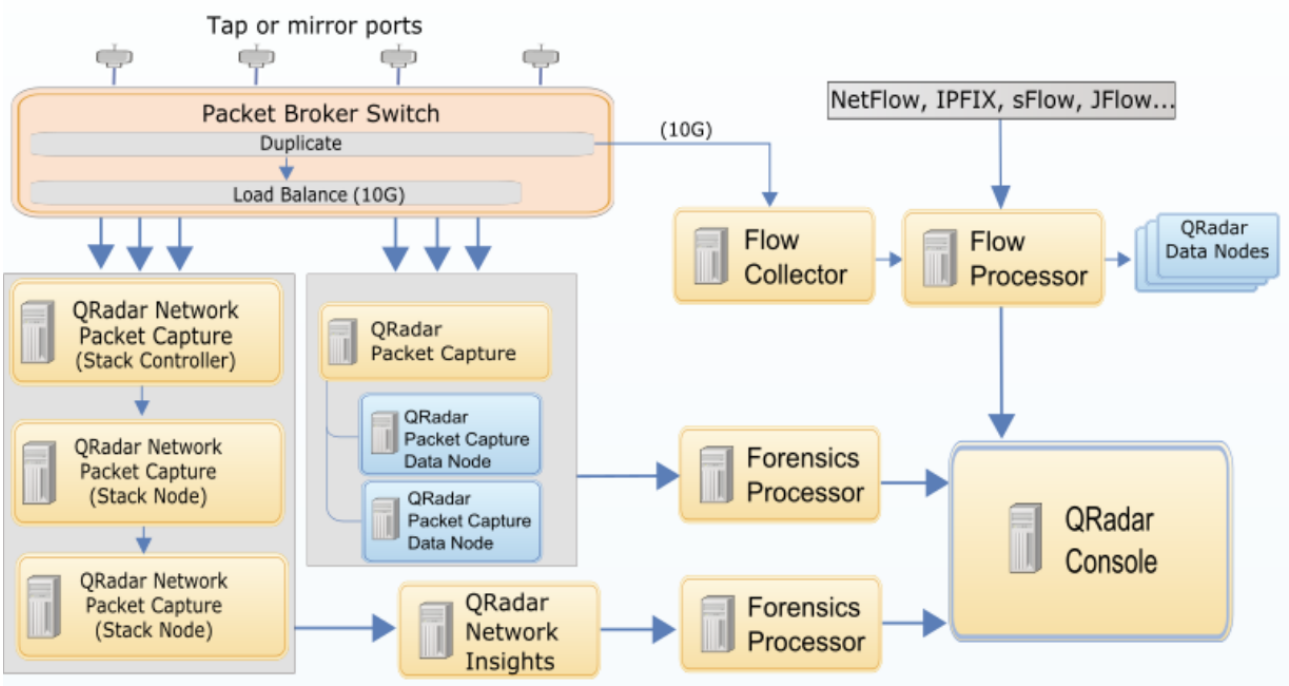

Рис. 5. Архітектура IBM QRadar Incident Forensics [4]

Є можливість розширити сховище, яке доступне для захоплення даних, з'єднавши кілька пристроїв QRadar Network Packet Capture разом в кільцеву топологію для створення стека. Стек дозволяє розподіляти дані захоплення по кожному з підключених пристроїв. Стек може включати до 16 пристроїв, але виглядає і поводиться як єдиний об'єкт, який збирає дані з одного TAP одного порту 10 ГБ.

QRadar Packet Capture є додатковими пристроями захоплення пакетів для зберігання і управління даними, які використовуються QRadar Incident Forensics, якщо у мережевому середовищі не розгорнуто інший пристрій захоплення пакетів. Можна встановити будь-яку кількість цих пристроїв в якості мережевого захоплювача для збору необроблених пакетних даних. Якщо пристрій захоплення пакетів не підключено, можна вручну завантажити файли захоплення пакетів в інтерфейсі або за допомогою FTP.

Є можливість розширити сховище даних, додавши пристрої QRadar Packet Capture Data Node. До кожної первинної системі QRadar Packet Capture можна підключити до двох пристроїв вузлів даних. Кожен вузол даних надає додатково 37 ТБ додаткового сховища.

QRadar Network Insights забезпечує аналіз мережевих даних в реальному часі і розширений рівень виявлення і аналізу загроз. QRadar Network Insights застосовується для виявлення і аналізу шкідливих програм, фішингу, внутрішніх загроз, атак бічного переміщення, крадіжки даних і прогалин в дотриманні нормативних вимог.

Технологія розслідування кіберінцидентів корпоративної інформаційної системи на базі IBM QRadar Incident Forensics

IBM QRadar Incident Forensics розроблений, щоб допомогти компаніям та організаціям поліпшити безпеку свого середовища і даних. Зокрема, IBM QRadar Incident Forensics має допомагати компаніям та організаціям розслідувати і краще розуміти, що сталося в інцидентах мережевої безпеки.

Цей інструмент дозволяє компаніям індексувати і шукати захоплені мережеві пакетні дані (PCAP) і включає функцію, яка може відновлювати такі дані назад в їх вихідну форму.

Ця функція реконструкції може відновлювати дані і файли, включаючи повідомлення електронної пошти, вкладення файлів і зображень, телефонні дзвінки VoIP і веб-сайти [5].

За допомогою IBM QRadar Incident Forensics фахівець з розслідування інцидентів безпеки може виявляти виникаючі загрози, визначати основну причину і запобігати повторенню. Використовуючи інструменти розслідування інцидентів безпеки фахівець з розслідування інцидентів безпеки може швидко сфокусувати свій аналіз на тому, хто ініціював загрозу, як вони це зробили і що було зламано [6].

Фахівець з розслідування інцидентів безпеки може простежити покрокові дії кіберзлочинців і відновити необроблені мережеві дані, пов'язані з інцидентом безпеки [6].

Коли організація вперше дізнається про загрозу, потенційний ризик безпеки або порушення нормативних вимог, то ставляться цілі для оцінки області, визначення залучених суб'єктів і розуміння мотивів [5].

Фахівець з розслідування інцидентів безпеки може використовувати інструменти IBM QRadar Incident Forensics в певних сценаріях в різних типах розслідувань, таких як мережева безпека, інсайдерський аналіз, шахрайство і зловживання, а також збір доказів [6].

Фахівець з розслідування інцидентів безпеки здійснює такі функції [6]:

відновлення і реконструкція мережевих сеансів на IP-адресу та з неї;

зі створених інцидентів є можливість запиту категорії атрибутів для збору доказів. Коли фахівець здійснює відновлення, створюється інцидент;

використання пошукових фільтрів для отримання бажаної інформації;

в залежності від типу розслідування обирання відповідного інструменту розслідування інциденту, який надасть необхідні докази.

Правильне застосування розглянутої технології розслідування кіберінцидентів корпоративної інформаційної системи на базі IBM QRadar Incident Forensics дозволяє ефективно встановлювати їх причини, дійових осіб та визначити шляхи усунення недоліків з метою неповторення їх у подальшому.

Висновки

Таким чином, сучасні підходи щодо розслідування кіберінцидентів корпоративної інформаційної системи базуються на застосуванні засобів автоматизації, які підвищують ефективність даної діяльності фахівців із кібербезпеки. Застосування IBM QRadar Incident Forensics скорочує час, необхідний для розслідування інцидентів безпеки і реагування на них. Його можливості збору даних виходять за рамки реєстрації подій і мережевих потоків і включають в себе повний захват пакетів, а також документи і елементи, що зберігаються в цифровому вигляді. Це допомагає забезпечити контекст і видимість того, хто, що, коли, де і як атакує.

Перелік посилань

1. X-Force Threat Intelligence Index 2020. Produced by IBM X-Force Incident Response and Intelligence Services (IRIS) [Електронний ресурс] – Режим доступу: https://www.ibm.com/security/digital-assets/xforce-threat-intelligence-index-map/#/.

2. IBM Security QRadar Incident Forensics Network visibility to help rapidly and thoroughly investigate malicious activity [Електронний ресурс] – Режим доступу: https://www.ibm.com/downloads/cas/AZ0KAOK5.

3. IBM QRadar Incident Forensics. Version 7.4.2. Installation Guide, 44 p. [Електронний ресурс] https://www.ibm.com/support/knowledgecenter/SS42VS_7.4/com.ibm.qradar.doc/b_forensics_ig.pdf?view=kc.

4. QRadar Incident Forensics installation components. IBM Knowledge Center [Електронний ресурс] – https://www.ibm.com/support/knowledgecenter/SS42VS_7.4/com.ibm.qradar.doc/c_qif_ig_cmpts.html.

5. IBM QRadar Incident Forensics. Version 7.4.2. User Guide, 54 p. [Електронний ресурс] https://www.ibm.com/support/knowledgecenter/SS42VS_7.4/com.ibm.qradar.doc/b_forensics_ug.pdf?view=kc.

6. Ішметов І.С. Технологія розслідування кіберінцидентів корпоративної інформаційної системи на базі рішення IBM QRadar Incident Forensics / І.С. Ішметов // Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Тези доповідей. 22 жовтня 2020 року, м. Київ – с. 46-49.

Надійшла: 26.06.2021 Рецензент: д.т.н., професор Гайдур Г.І.