ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо розслідування інцидентів критичної інфраструктури України на базі QRadar Incident Forensics»

зі спеціальності 125 Кібербезпека
(код, найменування спеціальності)

освітньо-професійної програми Інформаційна та кібернетична безпека
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Марина ЧЕЧИК
(підпис)

Виконала: здобувач вищої освіти групи БСД-42
ЧЕЧИК Марина
(прізвище, ім'я)

Керівник к.т.н., доцент БОРСУКОВСЬКИЙ Юрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ВСТУП

Актуальність дослідження. 14 січня 2022 року вважається початком повномасштабного кібервторгнення в Україну з боку Росії. Раніше, протягом тривалого періоду, Україна займала друге місце у світі за кількістю кібератак, одразу після Сполучених Штатів, однак починаючи з 14 січня, Україна стала лідером за кількістю кібератак і продовжує утримувати це перше місце. Від початку 2022 року відбулося орієнтовно 10 тис. кібератак та критичних інцидентів, значна кількість з яких припала на критичну інфраструктуру України. Енергетичні мережі, транспортні системи та комунікаційна інфраструктура відіграють стратегічну роль у функціонуванні країни, тому забезпечення їхнього надійного функціонування та захисту від кіберзагроз є критично важливим завданням для національної безпеки.

Ефективне опрацювання кібератак та інцидентів, разом із подальшим їх розслідуванням, сприяє зміцненню безпеки і зниженню ризику подібних атак у майбутньому. Система QRadar Incident Forensics - це інструмент, призначений для розслідування кіберінцидентів і аналізу подій в інформаційно-технологічних середовищах. Вона розроблена спеціально для виявлення, аналізу та відновлення дій, пов'язаних з кібератаками, що стало можливим завдяки використанню різноманітних джерел даних. По-перше, система є унікальним продуктом, адже дозволяє побудовувати ланцюгии подій (Event Chains) з використанням часових міток та залежностей між подіями й об’єктами подій, це допомагає в розумінні хронології кібератаки та дій зловмисників. По-друге, система чудово співпрацює з QRadar SIEM (а також інформацією з інших SIEM систем), що дозволяє інтегрувати дані з різних джерел, наприклад журнали подій, мережевий трафік та інші, для глибокого аналізу інциденту. Завдяки такій великій кількості джерел, система має можливість відновлення послідовності подій та дій, що сталися в системі, допомагаючи виявити точку вторгнення, методи та інструменти, використані зловмисниками. По-третє, QRadar Incident Forensics включає інструменти для аналізу зловмисних загроз та їхніх характеристик, що дозволяє виявляти патерни та типи атак для підвищення ефективності захисту мережі в майбутньому.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження шляхів та розробка рекомендацій щодо розслідування інцидентів критичної інфраструктури України на базі QRadar Incident Forensics.

Об'єкт дослідження - розслідування інцидентів.

Предмет дослідження - шляхи та методи розслідування інцидентів критичної інфраструктури України на базі QRadar Incident Forensics.

Мета роботи - розробка рекомендацій розробка рекомендацій щодо розслідування інцидентів критичної інфраструктури України на базі QRadar Incident Forensics.

Наукові завдання:

- проаналізувати основні шляхи та методи розслідування інцидентів;
- проаналізувати існуючі рішення для розслідування кіберінцидентів;
- проаналізувати шляхи та методи розслідування інцидентів на базі QRadar Incident Forensics;
- розробити рекомендацій щодо застосування шляхи та методи розслідування інцидентів в критичній інфраструктурі.

Методи дослідження – опрацювання літератури за даною темою, державних статистик та аналіз документації продуктів.

Практичне значення одержаних результатів - розроблено рекомендації фахівцям з кібербезпеки щодо налаштувань QRadar Incident Forensics, метрик аналізу доказів при проведенні розслідувань інцидентів.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

1.1 Аналіз проблеми захисту критичної інфраструктури України

Додано примітку [1]: (описуєш поняття, класифікацю, призначення, закони нормативні документи (процес проведення розслідування) і плавно переходиш до інцидентів , а потм на 1.2.)

Дослідження проблеми розслідування інцидентів критичної інфраструктури України вимагає ретельного розуміння сутності та класифікації цієї інфраструктури, а також засобів та методів розслідування інцидентів, що виникають у ній. Перед тим як розглядати основні аспекти розслідування, розглянемо поняття та класифікацію критичної інфраструктури.

Об’єкти критичної інфраструктури — це стратегічно важливі підприємства та установи, необхідні для функціонування суспільства країни та її економіки. До життєво важливих функцій та/або послуг належать, зокрема енергозабезпечення, продовольче забезпечення, охорона здоров’я, фармацевтична промисловість, інформаційні послуги, електронні комунікації, фінансові послуги тощо. Їх незапланована зупинка, виведення з ладу чи повне руйнування призводить до негативних наслідків для національної безпеки України.

Згідно Закону України (Далі - ЗУ) про критичну інфраструктуру, відповідальність за її захист несуть суб’єкти національної системи захисту критичної інфраструктури, визначення, повноваження та засади відповідальності яких визначаються державною політикою у сфері захисту критичної інфраструктури. Цими суб’єктами є, наприклад, усі підприємства, установи та організації, які провадять діяльність, пов’язану із забезпеченням безпеки критичної інфраструктури, Держспецзв’язку, Кабінет Міністрів України, оператори критичної інфраструктури, та інші (рисунок 1.1). Разом з тим, згідно з Постановою КМУ від 12.07.2022 № 787 «Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України», був визначений Уповноважений орган у сфері захисту критичної інфраструктури — Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості України (ДЗКІ).

Рис.1

Згідно статті 15 вищезгаданого закону, забезпечення захисту та стійкості критичної інфраструктури здійснюється в таких режимах її функціонування:

1. Штатний режим: оцінка та інформування про можливі загрози, функціонування згідно з проектним цільовим призначенням.
2. Режим готовності та запобігання: перевірка та підготовка системи захисту, функціонування згідно з проектним цільовим призначенням.
3. Режим реагування на кризову ситуацію: застосування заходів реагування, обмеження у роботі та доступі до об'єктів.
4. Режим відновлення: повернення до штатного функціонування з обмеженнями до ліквідації наслідків кризи.

Кібербезпека - це процес, який ніколи не закінчується, тому розглянемо його детальніше. Згідно постанови Кабінету Міністрів України від 29 грудня 2021 р. № 1426 “положення про організаційно-технічну модель кіберзахисту”, здійснення заходів з кіберзахисту системами кіберзахисту передбачає такі дії:

ідентифікацію - виявлення реальних і потенційних кіберзагроз для запобігання їм і їх нейтралізації;

захист - розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталості і надійності функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних та технологічних систем;

виявлення - проведення моніторингу визначення, збору та обробки нетипових подій у кіберпросторі;

реагування - вжиття заходів, спрямованих на запобігання кіберінцидентам, кібератакам, мінімізації їх можливих наслідків (запобігання виникненню загроз життю або здоров'ю людей та заподіяння шкоди майну), удосконалення систем кіберзахисту, з урахуванням необхідності забезпечення пропорційності та/або співрозмірності можливостей таких систем реальним та потенційним ризикам;

відновлення - поновлення штатного режиму функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних, технологічних систем після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення умов для проведення розслідування кібератаки.

Тема цієї дипломної роботи детально розглядає останній пункт, а саме розслідування кіберінцидентів. Національна стратегія забезпечення кібербезпеки та Закон України «Про основні засади забезпечення кібербезпеки України» встановлюють загальні принципи та основи забезпечення кібербезпеки в Україні, включаючи процедури реагування на кіберінциденти.

Однак, безпосередньо порядок розслідування кіберінцидентів детально регламентується не тільки цими документами, але й іншими правовими актами, такими як закони про правопорядок, кримінальний кодекс та процесуальні кодекси, які визначають процедури та механізми розслідування злочинів, включаючи кіберзлочини. Зокрема, в Україні існує Кримінально-процесуальний кодекс, що встановлює процедури та правила розслідування кіберзлочинів. Крім того, існують нормативно-правові акти, які можуть встановлювати особливі вимоги до розслідування кіберінцидентів, наприклад, у сфері захисту персональних даних або кібербезпеки державних органів та критичної інфраструктури.

Зважаючи на відсутність одного єдиного законодавчого акту, що регулює процедуру розслідування кіберінцидентів в Україні, визначення цього процесу потребує уваги до комплексу різноманітних правових норм. Наразі процедура розслідування кіберзлочинів базується на різних законах, постановах та інструкціях, які стосуються кібербезпеки, правил ведення слідства, технічних аспектів збору доказів і співпраці зі спеціалізованими установами. Однак відсутність єдиного регламенту, який би чітко визначав послідовність дій та відповідальність сторін у процесі розслідування, створює складнощі як для правоохоронних органів, що проводять розслідування, так і для потерпілих. Така ситуація може призвести до непрозорості та відсутності єдиної стратегії у боротьбі з кіберзлочинністю, що робить цей процес більш складним та менш ефективним.

1.2 Статистика інцидентів для критично важливої інфраструктури України

Статистика кібератак на об'єкти критичної інфраструктури та банківський сектор України показує тенденцію зростання активності. У 2020 році було зафіксовано 800 кібератак, у 2021 — 1400, у 2022 — 4500, а у 2023 році також 4500. У минулому 2023 році кількість зареєстрованих в Україні кіберінцидентів зросла на 62,5% у порівнянні з попереднім, 2022 роком, і наразі тенденція стає все гірше. Щоб мати уяву про типи атак, розглянемо статистику подій з останнього звіту SCPC (рисунок 1.2), яку представлено згідно офіційного Переліку категорій кіберінцидентів CERT-UA.

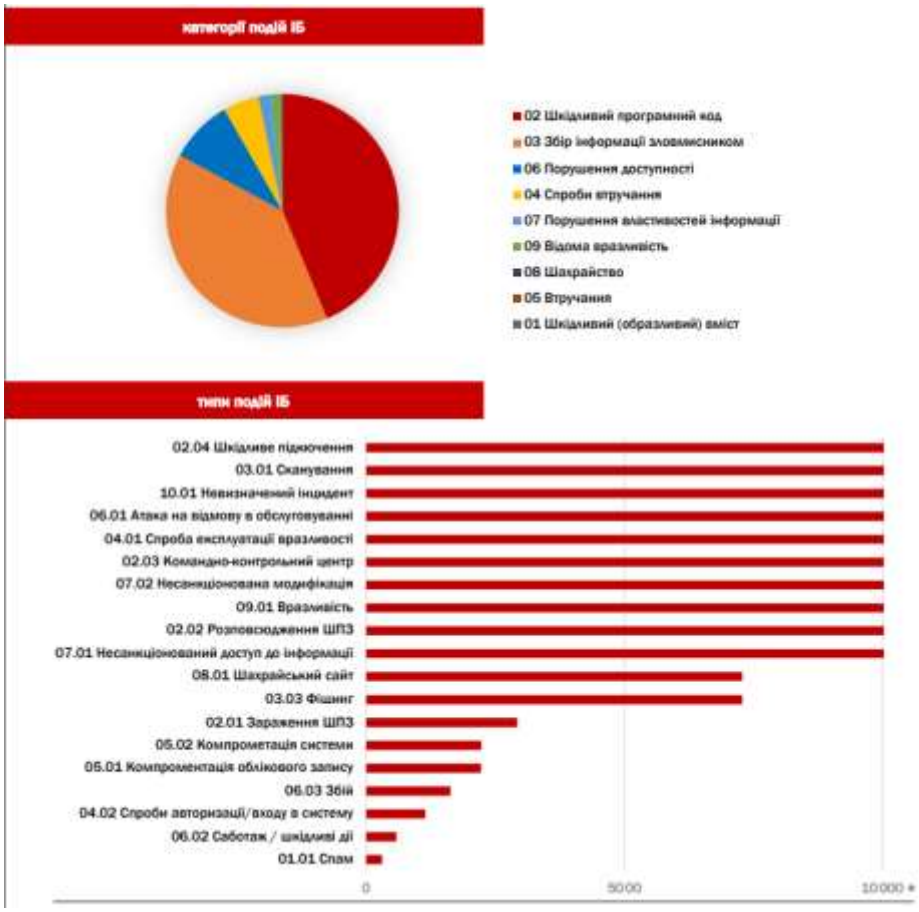


Рис. 1.2 - статистика подій ІБ

Для ефективної протидії цим загрозам, Служба безпеки України використовує платформу MISP-UA (Malware Information Sharing Platform Ukrainian Advantage), яка забезпечує обмін даними щодо кіберзагроз між об'єктами критичної інфраструктури та державними установами. MISP-UA, яка була впроваджена у 2018 році, налагоджує ефективний обмін інформацією між 1900 користувачами та 950 організаціями щодо понад 5 млн індикаторів компрометації. Фахівці СБУ також можуть бути залучені до заходів кібербезпеки, щоб ліквідувати наслідки кібератак, як це було у разі нападу на оператора зв'язку «Київстар».

Щоб надати огляд сучасних практик захисту критичних інфраструктур, ми розглядаємо найпрогресивніші підходи з Австралії, Америки (США) та Європи (Євросоюз).

В Австралії кібербезпека критичної інфраструктури регулюється Законом про безпеку критично важливої інфраструктури №29, 2018. Варто звернути увагу на деякі положення, що стануть у пригоді при розслідуванні інцидентів. Наприклад введення реєстру об'єктів критичної інфраструктури, який не буде оприлюднений. Це дозволить швидко визначити обсяг імовірного впливу атаки на критичні об'єкти та організувати відповідні заходи з ліквідації наслідків, зокрема при розслідуванні. Це в свою чергу покращить ефективність розслідування кіберінцидентів, забезпечивши систематизацію та координацію заходів безпеки. Також можна приділити увагу пункту про обов'язкове сповіщення про інциденти кібербезпеки, адже це також дозволить не зволікати і оперативно зреагувати на інцидент. Сюди ж можна віднести вимоги до певних організацій надавати інформацію про критичну інфраструктуру та повідомляти про події, що стосуються об'єктів.

У США, Агентство кібербезпеки та безпеки інфраструктури відповідає за загальне керівництво в цій сфері, а Закон про інформацію критичної інфраструктури надає правову основу для обміну інформацією між власниками та операторами критичних інфраструктур. З цікавого, цей закон стимулює широкий обмін інформацією про критичні інфраструктури між власниками та операторами цих інфраструктур, а також державними органами, що в свою чергу сприяє виявленню загроз та вразливостей та підвищує швидкість реагування на кіберінциденти.

У Євросоюзі щодо захисту мережевих та інформаційних систем значну увагу приділяє Директива ЄС, що створює рамки для забезпечення високого рівня безпеки в цих секторах. Один з пунктів - створення національних стратегій безпеки мереж та інформаційних систем дозволяє державам-членам Євросоюзу визначати конкретні заходи та політику з кібербезпеки для ефективного реагування на кіберінциденти. Також цьому сприяє створення мережі груп реагування на інциденти комп'ютерної безпеки (CSIRT). Один з найважливіших пунктів -

встановлення вимог безпеки та сповіщення для операторів основних послуг та постачальників цифрових послуг створює стандарти безпеки для певних секторів, що забезпечує захист від кіберзагроз і допомагає у попередженні кібератак.

Згідно Державної політики у сфері захисту критичної інфраструктури, українські служби активно співпрацюють з закордонними колегами, які допомагають зміцнити стійкість та захист українських інфраструктур.

1.3 Аналіз засобів щодо розслідування інцидентів критичної інфраструктури України

Додано примітку [2]: · ESET Inspect
· QRadar Incident Forensics
· Splunk Enterprise Security

Щоб знати на що звертати увагу при аналізі засобів розслідування, розберемося, які етапи розслідувань взагалі існують. Для цього звернемося до міжнародних стандартів NIST SP 800-61 та ISO/IEC 27035 і дізнаємось, які кроки і етапи розслідувань вони нам пропонують. Хоча кроки розслідування кіберінцидентів, рекомендовані цими стандартами, спрямовані на виявлення, аналіз та відновлення після інцидентів кібербезпеки, їх методи та акценти можуть трохи відрізнятися. Ось деякі з цих відмінностей:

Збір та аналіз доказів. У NIST SP 800-61 акцент здебільшого робиться на зборі та аналізі доказів, що дозволяє визначити природу та обсяг інциденту, а також встановити методи атаки та точки входу зловмисників. В свою чергу у ISO/IEC 27035 кроки збору та аналізу доказів також присутні, проте більший акцент робиться все ж на виявленні й управлінні вразливостями, та можливостях для подальшого вдосконалення систем безпеки.

Виправлення та відновлення. В NIST SP 800-61 виправлення та відновлення описуються як окремий етап, що включає в себе заходи для виправлення вразливостей та відновлення нормального функціонування інформаційної системи. У ISO/IEC 27035 ці кроки можуть бути включені до більш широкого етапу "процесу виправлення", який додадково може включати й інші заходи з підвищення рівня захисту.

Закон/Регулювання	Область застосування	Основні положення	Застосування
GDPR	Європейський Союз	Захист та конфіденційність даних, згода, повідомлення про порушення даних	Застосовується до суб'єктів, що обробляють дані громадян ЄС
NIST SP 800-53	Сполучені Штати	Контроль безпеки та конфіденційності для федеральних інформаційних систем	Федеральні агентства та підрядники
PCI DSS	Глобальний	Стандарти безпеки для даних платіжних карт	Організації, що обробляють платежі
Кібербезпекова стратегія України	Україна	Національна політика кібербезпеки, захист критичної інфраструктури	Державні установи та сектори КІ
Закон України про захист персональних даних	Україна	Регулювання обробки та захисту персональних даних	Усі суб'єкти, що обробляють персональні дані в Україні

Параметр	Україна	США	ЄС
Основний законодавчий акт	Закон про критичну інфраструктуру	Закон про кібербезпеку	Директива NIS
Уповноважений орган	Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості України	Агентство кібербезпеки та безпеки інфраструктури	Група реагування на інциденти комп'ютерної безпеки (CSIRT)

Оголошення про інциденти	Обов'язкове сповіщення	Обов'язкове сповіщення	Обов'язкове сповіщення
Реєстр об'єктів критичної інфраструктури	Відкритий	Закритий	Закритий
Співпраця між власниками і державою	Висока	Висока	Висока
Вимоги до захисту	Високі	Високі	Високі
Санкції за порушення	Є	Є	Є

З метою забезпечення ефективних збору, аналізу, виправлення, відновлення, звітності та документування інцидентів кібербезпеки, розглянемо спеціалізовані засоби реагування на кіберінциденти. Для такого аналізу було обрано три відомих міжнародних рішення - ESET Inspect, Splunk Enterprise Security та QRadar Incident Forensics.

ESET Inspect - це інструмент виявлення та реагування на загрози для кінцевих точок, який збирає системні дані про те, що відбувається у режимі реального часу. Що найважливіше, завдяки потужному механізму баз даних ESET Inspect дозволяє проводити криміналістичне розслідування минулих інцидентів і має можливості реагування для зменшення або блокування подальшого поширення виявлених складних постійних загроз у мережі шляхом ізоляції уражених ресурсів, блокування виконання та інших дій. Щоб розібратись чим корисний ESET Inspect в розслідуваннях, потрібно аналізувати його роботу. Спершу проводиться збір даних з різних джерел у мережі, загалом системні журнали подій, за допомогою окремого модулю - ESET Inspect Connector. Ці дані аналізуються на місці, а далі

передаються ESET Inspect для подальшого більш детального аналізу та розслідування, також з них збирається статистика (рисунок 1.3)

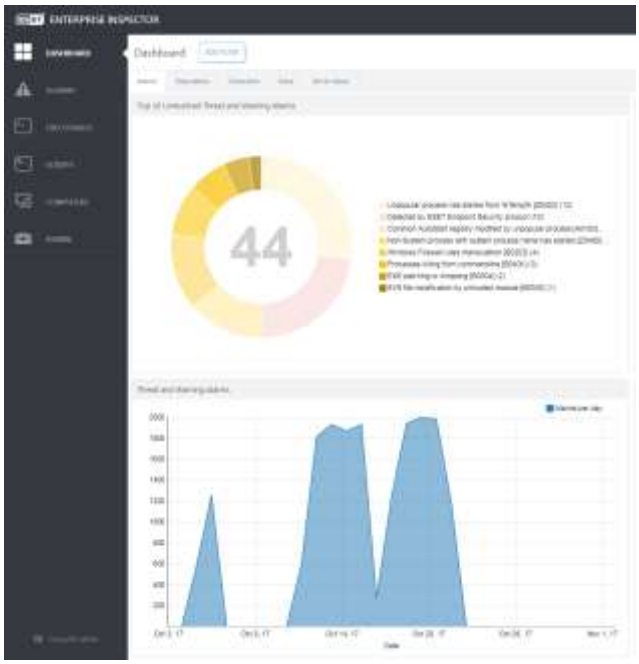


Рис. 1.3. - Приклад графіку з зібраних даних

Після збору даних ESET Inspect використовує відомі методи та алгоритми для виявлення аномальної активності у мережі, такі як сигнатурний аналіз евристичний або кореляція. Результатом може стати істинна (true positive) або хибна (false positive) спроба доступу, незвичайний обсяг трафіку, несподівані зміни в системних параметрах тощо (рисунок 1.4).

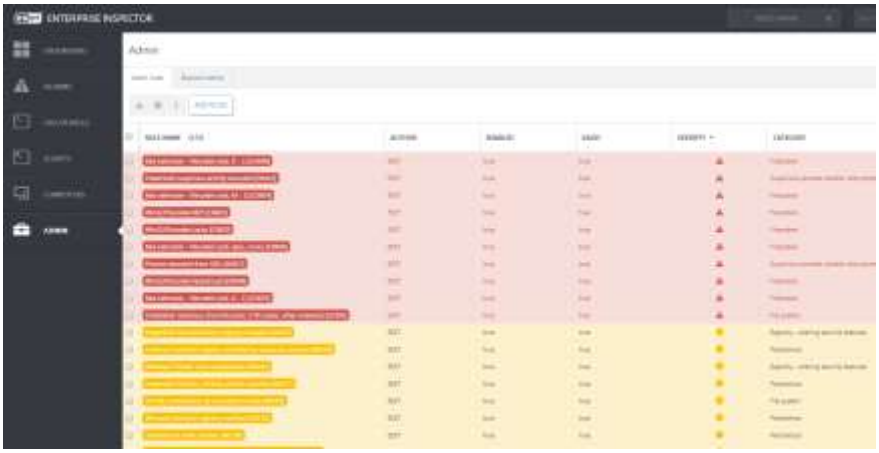


Рис. 1.4. - Приклад проаналізованих зібраних даних (подій безпеки)

Інструмент аналізує виявлені аномалії та спробує з'єднати їх з іншими подіями або взаємозв'язками у мережі (звертаючись також до своїх хмарних баз даних). Додатково, якщо в програмі виникне хибне спрацювання, але програма визнає його як істинне, адміністратор може змінити цю подію на хибне спрацювання, і програма автоматично враховуватиме цю корекцію у своїх подальших аналізах і оцінках. В якості прикладу на рисунку 1.5 показано кореляцію сутностей, створених за допомогою Incident Creator. На ньому адміністратор може швидко визначити зв'язок між виявленням шкідливого програмного забезпечення Filecoder (Ransomware) та іншими інцидентами, виявленими ESET Inspect. У цьому випадку адміністратор, який переглядає інформаційну панель, отримає загальне уявлення про те, що відбувається або вже відбулося. Залежно від рівня підготовки адміністратора, він може пропустити методи і процедури, пов'язані з тактикою MITRE ATT&CK, і натомість звернути увагу на кількість уражених комп'ютерів або виявлених виконуваних файлів.

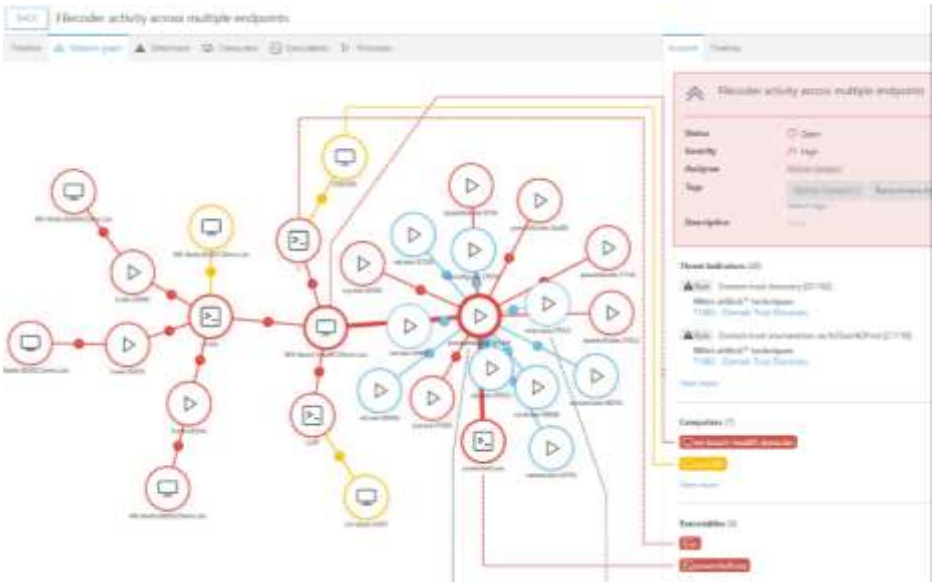


Рис. 1.5. - Кореляція сутностей Incident Inspect

У центрі ми бачимо конкретний комп'ютер, оточений червоним колом, що позначає ступінь серйозності (червоний = загроза, жовтий = попередження, синій = інформація) виявлення. Адміністратор може швидко визначити ряд виконуваних файлів і пов'язаних з ними пріоритетних процесів на роботі.

Розглянемо наступне рішення, що, на відміну від попереднього, за статистикою зустрічається частіше у корпоративних середовищах. Splunk Enterprise - це, в першу чергу, SIEM система, що вирішує широкий спектр аналітичних та операційних завдань, включаючи безперервний моніторинг безпеки, розширене виявлення загроз, дотримання нормативних вимог, розслідування інцидентів, криміналістику та реагування на інциденти. Splunk Enterprise Security надає наскрізний огляд стану безпеки організації та розслідувань. По аналогією з ESET Inspect, Splunk Enterprise Security проводить постійний аналіз мережі і у реальному часі виявляє підозрілі події безпеки. Також Splunk ES створює графіки статистики на основі отриманих даних у реальному часі (рисунок 1.6)

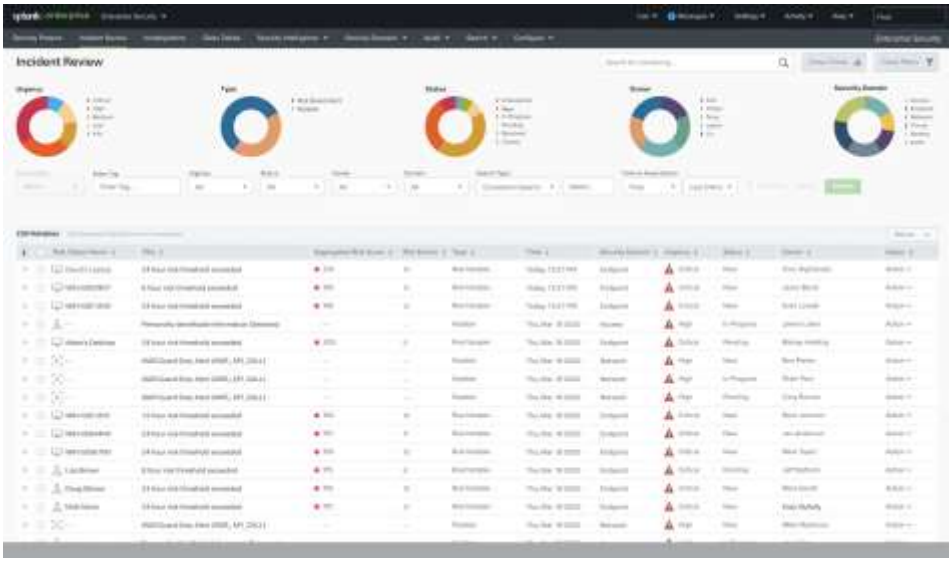


Рис. 1.6. - Результати сканування Splunk Enterprise Security

Варто зазначити, що Splunk ES, як і ESET Protect, корелює дані інциденту з іншими подіями та загрозами, що допомагає зрозуміти повну картину загрози та виявити зв'язки між різними подіями.

Перевага Splunk ES в тому, що він досить зручно інтегрується в будь-яких розмірів систему, також маючи одну з найзручніших пошуково-фільтруючих систем, за допомогою якої можна відфільтрувати дані як буде зручно. Також інтеграція користувачів в систему Splunk ES відбувається легко, але надійно, завдяки чому SIEM система отримує максимум корисної інформації. Особливо ефективно Splunk працює з Active Directory (AD) - підключається до контролерів доменів та інших серверів AD для збору журналів подій (Event Log), які містять інформацію про автентифікацію, авторизацію, аудит інформацію тощо. Зазвичай Splunk використовує LDAP для взаємодії з AD, однак також деякі розширені функції AD можуть бути доступні через API. Splunk ES може використовувати ці API для отримання специфічних даних з AD, які можуть бути корисними для виявлення загроз. Завдяки всьому цьому система дуже швидко ідентифікує та реагує на інциденти (рисунок 1.7).

Рис. 1.7. - Результати сканування Splunk Enterprise Security, виявлені події

Останнє рішення, яке ми сьогодні розглянемо - це IBM Security QRadar Incident Forensics. Програмно-апаратне рішення, призначене для надання командам IT-безпеки підприємств кращої видимості і ясності в мережевих діях, пов'язаних з інцидентами безпеки. Це розуміння може бути використане, щоб допомогти виявити повний масштаб мережевого інциденту інциденту безпеки, усунути пошкодження та зменшити ймовірність витоку даних. витоку даних або повторення минулих порушень. У сучасних корпоративних середовищах, де існує занадто багато вразливостей і занадто мало робочих годин, щоб вручну розслідувати і усунення інцидентів, QRadar Incident Forensics забезпечує розуміння і аналіз, якого неможливо досягти, використовуючи тільки події з журналів і деталі мережевого і деталі мережевого потоку.

Рішення надає потужні можливості індексування, пошуку, обробки даних і звітності, які підтримують прийняття більш розумних і швидких рішень командою IT-безпеки. Простий інтерфейс, схожий на пошукову систему, дозволяє здійснювати інтуїтивний пошук даних пов'язаних з інцидентом безпеки, включаючи дані в стані спокою (документи) або в русі (PCAP), починаючи від повідомлень електронної пошти, телефонних дзвінків через IP-телефонію (VoIP), відвідування веб-сайтів, дописи в блогах і навіть вкладення повідомлень, такі як файли або зображення. QRadar Incident Forensics індексує і співвідносить всі ці дані, визначаючи пріоритетність пошуку, щоб допомогти швидко відрізнити

справжні загрози від false positive результатів, згенерованих існуючим правилом кореляції SIEM.

Як фахівець з криміналістики, ми маємо аналізувати крок за кроком дії кіберзлочинців та відтворювати початкові мережеві дані, пов'язані з інцидентом безпеки. IBM QRadar Incident Forensics в різноманітних сценаріях розслідувань, таких як мережева безпека, внутрішній аналіз, виявлення шахрайства та зловживань, а також збір доказів включає:

1. відновлення та реконструкція мережевих сесій з використанням IP-адрес;
2. за допомогою створених інцидентів ви можете отримувати атрибути для збору доказів;
3. створюється інцидент при відновленні дій;
4. використання фільтрів пошуку для отримання важливої інформації.

Шляхом візуалізації мережевих зв'язків QRadar Incident Forensics дозволяє виявляти зв'язки між різними пристроями та активностями, за допомогою цього аналітики виявляють потенційно шкідливу поведінку. Наприклад, виявлення підозрілих запитів від конкретного пристрою до кількох віддалених хостів може вказувати на витік даних або атаку (рисунок 1.8).

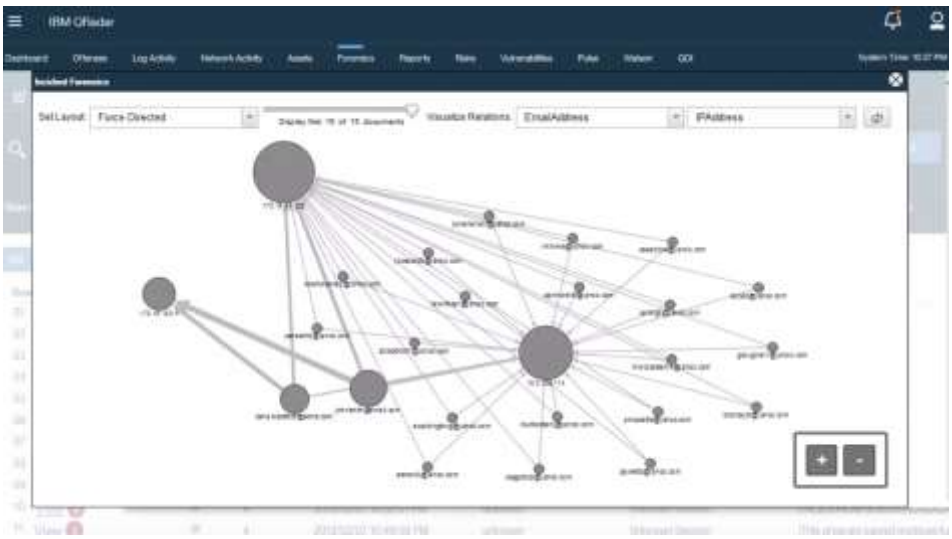


Рис. 1.8. - Приклад візуалізації даних інструментом VGrid

Однією з продаючих можливостей QRadar Incident Forensics є інструмент об'єднання даних (Data pivoting), який передбачає перетворення знайденого контенту з результатів пошуку на гіперпосилання (яке зберігає в собі всі зв’язки об’єкта). Наприклад, за запитом “Марина” результати пошуку можуть включати електронні листи, написані Мариною (включаючи вкладення), журнали чату за участю Марини та додаткові контекстні деталі. Клікнувши на її електронну пошту, буде відображено кожен ресурс або елемент, пов'язаний з ім’ям “Марина”, наприклад, вкладення або ідентифікатори комп'ютера, представлені у вигляді посилань, на які можна натиснути. По аналогією з двома описаними рішеннями вище, QRadar Incident Forensics найкраще співпрацює з однойменною SIEM системою - QRadar, завдяки якій можливості Data pivoting розширяються в декілька разів.

Висновок

Додано примітку [3]: (Порівняння результатів і висновки, обираємо найкраще рішення, для якого буду давати рекомендації)

Розглянемо підсумки про ці три рішення. Повертаючись до ESET Inspect, можна впевнено сказати, що завдяки потужному механізму баз даних, цей інструмент дозволяє проводити криміналістичне розслідування минулих інцидентів та реагувати на складні загрози шляхом ізоляції уражених ресурсів. Інструмент агрегує дані з різних джерел для аналізу аномальної активності, використовуючи сигнатурний аналіз, евристику та кореляцію, а адміністратор може коригувати хибні спрацювання, що враховується в подальшому аналізі. Однак в порівнянні з іншим інструментами, ESET Inspect має менш розвинені аналітичні функції, адже ESET Inspect це більше EDR ніж XDR. ESET Inspect в першу чергу націлений на швидке і автономне реагування на інциденти, ніж їхнє подальше глибоке розслідування.

Splunk Enterprise Security (ES) має свої переваги у проведенні розслідувань інцидентів, таких як детальний аналіз у реальному часі, виявлення аномалій і структурних зв'язків, а також надання рекомендацій щодо відповіді на інцидент. Однак, звідси також можна виокремити кілька потенційних недоліків. У великих

організаціях, де немає або недостатньо спеціалістів з глибокими навичками у роботі зі Splunk ES, інструмент не зможе ефективно масштабуватися для збору чи обробки великих обсягів даних. Це може призвести до затримок у виявленні та реагуванні на інциденти в обсягових середовищах. Splunk складний у реалізації, однак його впровадження і нормальне адміністрування забезпечують найкраще реагування, проте не розслідування.

QRadar Incident Forensics виділяється серед інших рішень у кількох аспектах. По-перше, він володіє потужним механізмом обробки даних, здатним агрегувати і аналізувати інформацію з різних джерел. Це дозволяє ефективно проводити криміналістичне розслідування минулих інцидентів та реагувати на поточні загрози шляхом ізоляції уражених ресурсів. По-друге, QRadar Incident Forensics володіє потужним інструментом Data pivoting, який дозволяє легко відстежувати всі зв'язки об'єктів, це значно полегшує розуміння ситуації та реагування на загрози. По-третє, як і попередні рішення, QRadar Incident Forensics інтегрується зі своєю власною SIEM системою - QRadar, що забезпечує ще більшу ефективність та розширює можливості того ж Data pivoting. Incident Forensics так само є корпоративним рішенням, яке підходить великим компаніям з великою кількістю мереж та підмереж, проте орієнтований він саме на розслідування інцидентів. З цих причин можна зробити висновок, що QRadar Incident Forensics є найбільш оптимальним рішенням для проведення розслідувань.

Параметр	QRadar Incident Forensics	Splunk Enterprise Security	ESET Inspect
Моніторинг в реальному часі	Так	Так	Так
Відновлення мережевих сесій	Так	Ні	Ні
Аналіз ентропії файлів	Так	Ні	Так
Інтеграція з SIEM	Так (з QRadar SIEM)	Так (з Splunk SIEM)	Обмежено

Можливість розшифрування SSL	Так	Ні	Ні
Data pivoting	Так	Ні	Ні
Аналіз підозрілих вмістів	Так	Так	Так
Візуалізація зв'язків та асоціацій	Так	Так	Так
Підтримка розслідувань на основі MITRE ATT&CK	Так	Так	Так
Підтримка аналізу на основі YARA-правил	Так	Так	Ні

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

2.1 Аналіз QRadar Incident Forensics як інструменту аналізу і розслідування інцидентів критичної інфраструктури

Розглянемо Incident Forensics більш детально, починаючи з його архітектури (рисунок 2.1). Функції безпеки, пропоновані IBM QRadar Incident Forensics, залежать від типу установки. З одного боку, можна використати, автономний сценарій розгортання (Stand-alone deployment), тобто коли встановлюється лише один сервер, який працює самостійно. В такому разі один пристрій Incident Forensics Standalone забезпечує виключно можливості мережевої криміналістики і нічого більше. А з іншого боку, можна реалізувати розподілене розгортання (Distributed deployment), коли сервер QRadar Incident Forensics взаємодіє з іншими серверами та компонентами QRadar, такими як консоль або обробник. Цей тип установки дозволяє розширити функціональні можливості, так як кожен компонент

може виконувати специфічні завдання і зменшити навантаження на один компонент. Пристрій Incident Forensics Processor підключається до консолі Console в якості керованого хоста, розширюючи можливості безпеки, що виходять за рамки автономних установок. Цей тип розгортання включає управління подіями і журналами, виявлення аномалій, управління ризиками, управління вразливостями, а також надає можливість розподілити робоче навантаження для відновлення даних. Програмне забезпечення QRadar Incident Forensics може бути встановлене як на виділеному обладнанні, так і на віртуальному пристрої (але варто зазначити, що Incident Forensics вимагає встановлення на операційну систему Red Hat Enterprise Linux).

На наведеній нижче схемі представлено огляд функцій безпеки та архітектурної структури платформи IBM QRadar Security Intelligence Platform. Це візуальне представлення інкапсулює комплексні можливості і варіанти розгортання, доступні в екосистемі QRadar.

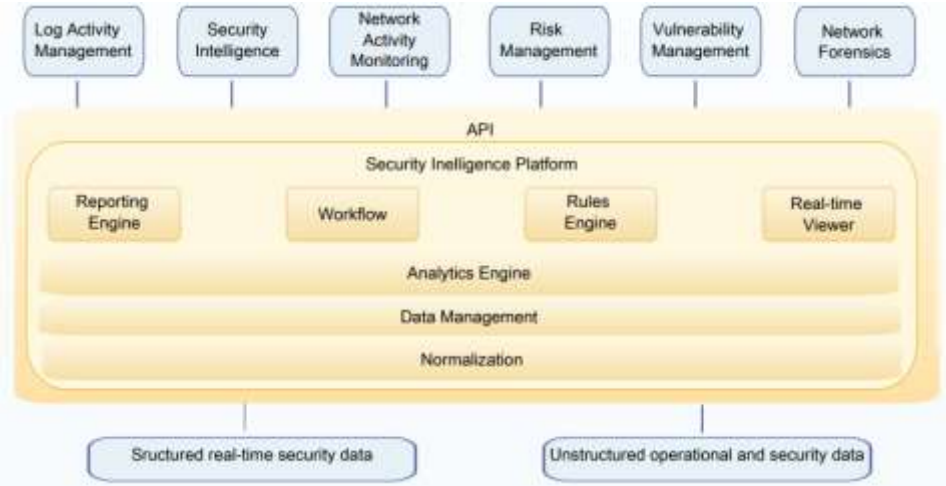


Рис. 2.1. - Огляд архітектури системи охоронної розвідки QRadar

Як ми можемо побачити, QRadar Incident Forensics інтегровано в масштабовану архітектуру IBM QRadar Security Intelligence Platform. Розглянемо

детальніше компоненти цієї архітектури, щоб зрозуміти, що з чим співпрацює і які функції задовольняє.

Перший компонент - це *QRadar Flow Collector*. Він збирає потоки, підключаючись до порту SPAN або мережевого TAP, також підтримує збір зовнішніх джерел даних на основі потоків, таких як NetFlow від маршрутизаторів.

Далі всі зібрані дані переходять до *QRadar Flow Processor*. Він обробляє потоки від одного або декількох пристроїв QRadar Flow Collector, хоча пристрій Flow Processor також може збирати зовнішні мережеві потоки, такі як NetFlow, J-Flow і sFlow, безпосередньо з маршрутизаторів у мережі. Flow Processor також використовується для масштабування розгортання QRadar, щоб управляти більш високими показниками FPM.

Data Node (вузли даних) дозволяють новим і існуючим розгортанням QRadar додавати ємність для зберігання і обробки даних, коли це необхідно. Вузли даних також збільшують швидкість пошуку у вашому розгортанні, надаючи більше апаратних ресурсів для запуску пошукових запитів.

Далі вся інформація потрапляє в *QRadar Console*. Загалом вона забезпечує користувацький інтерфейс для взаємодії з продуктом, у тому числі перегляд подій та потоків у реальному часі, генерацію звітів, адміністрування та інші адміністративні функції. У розподілених розгортаннях QRadar використовується для адміністрування інших хостів, які керуються QRadar.

І, нарешті, *QRadar Incident Forensics Processor*, він забезпечує основний користувальницький інтерфейс продукту QRadar Incident Forensics. Інтерфейс надає інструменти для відстеження покрокових дій кіберзлочинців, реконструкції необроблених мережевих даних, пов'язаних з інцидентом безпеки, пошуку в доступних неструктурованих даних і візуальної реконструкції сеансів і подій.

Також можна розглянути два опційні рішення, що не потребують обов’язкового встановлення. *Network Packet Capture* пропонує додаткове рішення для зберігання і управління даними, які використовуються QRadar Incident Forensics, при відсутності інших пристроїв захоплення пакетів у вашій інфраструктурі. Ці пристрої можуть бути розгорнуті як мережеві відгалужувачі або

підмережі для збору необроблених пакетних даних. У випадках, коли пристрій захоплення пакетів не підключено, користувачі мають можливість вручну завантажувати файли захоплення пакетів через інтерфейс користувача або по FTP. Також є додатковий інструмент *QRadar Network Insights* забезпечує аналіз мережевих даних в режимі реального часу і пропонує розширені можливості виявлення загроз. Це дозволяє користувачам виявляти і оцінювати різні загрози, включаючи шкідливе програмне забезпечення, спроби фішингу, інсайдерські загрози, атаки бокового переміщення, витік даних і невідповідності стандартам.

2.2 Основні складові та функції багатофункціонального програмного засобу QRadar Incident Forensics

IBM QRadar Incident Forensics розроблено для покращення безпеки та захисту даних у компаніях. Основна мета цього інструменту полягає у вдосконаленні розслідування інцидентів мережевої безпеки, надаючи засоби для аналізу та з'ясування причин подій. Спробуємо розібратись в основному функціоналі програми.

Почнемо з головної вкладки, Offenses (Злочини), де можна почати пошук слідчих дій. Якщо праворуч клацнути на злочин або будь-яку IP-адресу та запустити “відновлення слідчих дій”, то програма витягне сирі дані за вказаними часовими діапазонами з пристрою захоплення та відновить документи, а потім додасть результати до репозиторію слідчих дій. Якщо запустити “пошук слідчих дій”, репозиторій фільтрується та шукається лише для цієї IP-адреси. Результати потім показуються в основній таблиці на вкладці Offenses. Ви можете уточнити свій пошук, будуючи запити.

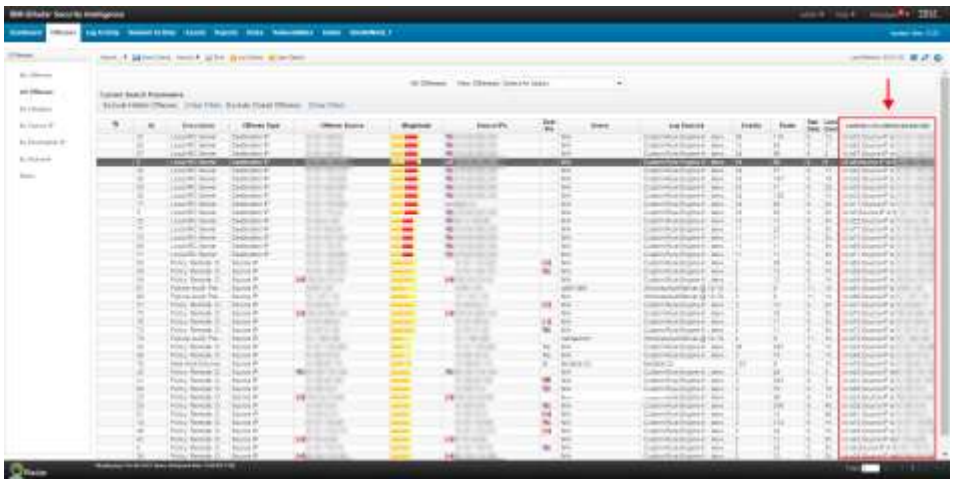


Рисунок 2.2 - Основна таблиця вкладки Offenses

Варто зазначити, що коли програма отримує запит на пошук, вона обробляє дані перехоплення пакетів та повертає їх у вихідний формат, в якому вони були у

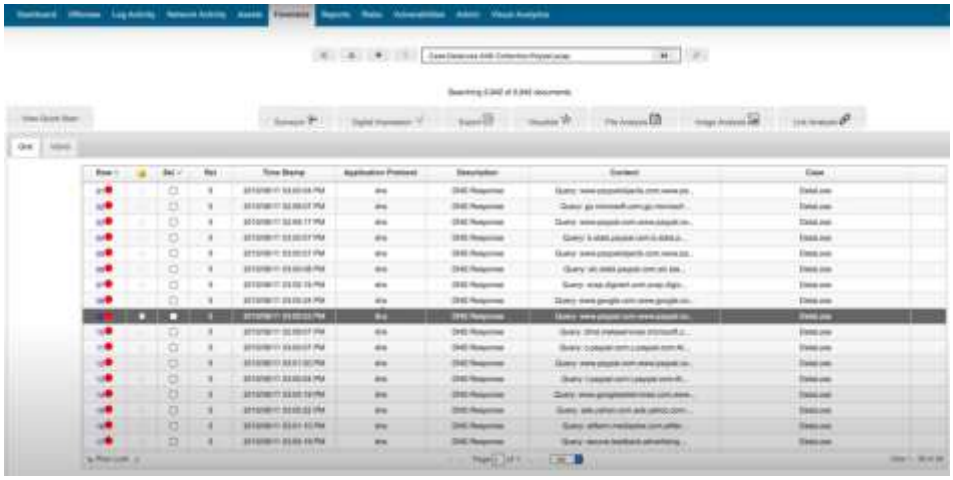
їхньому початковому вигляді. Наприклад, документи MS Word відтворюються у форматі файлів .word, а телефонні дзвінки через VoIP перетворюються на аудіофайли. Отримані файли індексуються з використанням метаданих та вмісту, щоб забезпечити їх доступність для подальшого пошуку. Після того, як ми виконали відновлення або пошук, ми можемо розпочати своє дослідження у тій же вкладці Forensics.

Переглянемо категорію Suspect Content (Підозрілий контент) та запустимо один з запитів, наприклад entity alert (попередження сутності), який визначає можливу зловмисну сутність, що залучена до порушення політик безпеки. Suspect Content базується на визначеному наборі правил щодо вмісту, що вказує на підозрілу діяльність. QRadar Incident Forensics повертає впорядковані результати пошуку, це навіть схоже на пошукову оптимізацію, яка пріоритизує сайти у пошуку в Інтернеті, коли найбільш часті випадки з'являються найвище.

Далі можемо почати аналіз даних, переходячи за посиланнями та шукаючи метадані, що пов'язані з, наприклад, певним документом. Можливості аналізу всіх цих даних надають різні види та підсумки пошукових переглядів і даних. Щоб дослідити взаємозв'язки між усіма діями та інцидентом безпеки, у перегляді документа праворуч треба натиснути "Отримати відносини для" і нам з’явиться вся знайдена інформація. Після цього вже можна відфільтрувати зібрану інформацію, з'єднуючи сутності.

Наостанок використаємо функцію Digital Impressions (Цифрові відбитки), щоб відслідкувати шлях сутності та отримати скомпільований набір асоціацій. Digital Impressions - це індекс метаданих, який може допомогти ідентифікувати підозрілих злочинців зсередини, вислідковуючи їхній шлях. З його допомогою криміналіст може відповісти на такі питання: що відомо про цього підозрілого атакувальника, комп'ютер або IP-адресу? З ким спілкувався цей підозрілий злочинець? Хто знаходиться у їх мережі контактів? Чи намагається підозрілий злочинець приховати свою ідентичність? При побудові цих взаємозв'язків QRadar Incident Forensics використовує дані з мережевих джерел, таких як IP-адреси, MAC-адреси та порти та протоколи TCP. Він знаходить інформацію, таку як

ідентифікатори чатів, і може читати інформацію, таку як ідентифікація автора з текстових процесорів або електронних таблиць. Digital Impressions може допомогти розкрити асоціації, з'єднуючи ідентичність сутності з ідентифікаційною інформацією для інших користувачів або сутностей.



Всі вищеперелічені інструменти аналітики використовують для керування даними різними способами. Як аналітик з безпеки, ми маємо виявляти загрози, які уникнули виявлення раніше, аналізуючи відновлені артефакти, такі як файли та зображення. Щоб зрозуміти зв'язки між співробітниками та артефактами, нам також треба досліджувати посилання на ці файли та зображення, а також вихідні посилання з них.

Розглянемо на прикладі аналіз артефактів (artifact analysis) для пошуку джерела атаки (patient zero). Декілька систем нашої компанії заражені, незважаючи на всі заходи безпеки, які були прийняті. Після того як ми ідентифікуємо та ізолюємо ці системи, потрібно виявити, як ці системи були заражені та чи залишились інші скомпрометовані активи. Починаючи з IP-адрес та приблизного часового проміжку, з якими маємо справу, використаємо Incident Forensics для відновлення відповідних даних пакетів.

Шукаємо виконавчий вміст, використовуючи можливості аналізу файлів QRadar Incident Forensics, що дозволяє побачити список всіх файлів та як часто вони відправлялися, чи містять вони вбудовані файли або скрипти, і їх оцінки ентропії.

Оцінка ентропії файлу (останній стовбець), яка вимірює випадковість даних і використовується для пошуку зашифрованих шкідливих програм, і розподіл ентропії також чітко показують, що частина файлу не відповідає вимогам. Подальший аналіз підтверджує, що цей файл містить новий вид шкідливого програмного забезпечення, яке пройшло існуючі заходи безпеки непоміченим і було відповідальним за заражені системи.

Розглянемо ентропію як метрику для аналізу файлів детальніше. Вона використовується як показник варіабельності (випадковості/непердбачуваності) бітів на байт. В основі цього поняття лежить ідея, що здатність стиснення даних залежить від ступеня впорядкування або непорядку даних. Якщо дані є більш непередбачуваними або випадковими, то їх складніше стиснути, і вони будуть мати

вищу ентропію. Таким чином, аналіз ентропії у файлі дозволяє виявити підозрілість. Висока ентропія може вказувати на те, що дані можуть бути зашифровані або стиснуті, що є характеристикою для багатьох типів шкідливих програм. Низька ентропія, навпаки, може свідчити про те, що дані легко стискаються або є впорядкованими, що може бути незвичайним для деяких типів файлів. Оскільки кожен символ в одиниці даних складається з 1 байта, значення ентропії вказує на варіацію символів і стисливість одиниці даних. Зміна значень ентропії у файлі може вказувати на те, що у файлах приховано підозрілий вміст.

Для визначення можливих впливів на інші системи Incident Forensics надає аналіз посилань для швидкої візуалізації всіх веб-сайтів, які були переглянуті. Незважаючи на зазвичай велику кількість трафіку на веб-сайтах компаній, можна чітко помітити невелику підмножину доступів до зараженого веб-хоста. Аналізуючи ці посилання, ми побачимо, які інші сервери в мережі використовувалися для доступу до цього веб-хоста.

Висновок

IBM QRadar Incident Forensics надає широкі можливості для аналізу кіберінцидентів, включаючи відновлення даних, аналіз контенту, візуалізацію комунікації та ідентифікацію злочинців. Ці можливості сприяють ефективному розслідуванню та виявленню потенційних загроз безпеці, а що найважливіше, розслідування не обмежене ніякими факторами, а зачіпає всю систему. Програма дозволяє візуалізувати комунікацію між веб-сайтами, що допомагає виявити зв'язки між різними системами та потенційно підозрілими діями., а під час аналізу посилань відображаються усі зв’язки (спільність) між веб-сайтами, які були переглянуті. Під час розслідування кіберінцидентів видно, де є “перекриття” точок зацікавленості і які люди з ними стикаються. Наприклад, якщо є підозра, що злочинець не один і їх ціла група, що співпрацює, але немає впевненості і доказів як саме, ми можемо переглянути набір документів від різних користувачів і використовувати аналіз посилань для виявлення спільних веб-сторінок, а після цього цього провести докладне дослідження конкретних веб-сайтів, на які вели

вивела програма. Для отримання можливості перегляду відповідного контенту в розмовах, які відбулися під час кіберінциденту, є можливість відновити весь мережевий трафік, що пов'язаний з конкретною IP-адресою чи ім’ям. Коли мережевий трафік відновлюється з IP-адреси, програма автоматично створює інцидент. IBM QRadar Incident Forensics індексує всі доступні мережеві дані, файли, метадані та текстові символи, що містяться в кожному відновленому файлі.

3 РЕКОМЕНДАЦІЇ ЩОДО РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ НА БАЗІ QRADAR INCIDENT FORENSICS

3.1 Рекомендації щодо налаштувань та конфігурації QRadar Incident Forensics

Перше, що потрібно налаштувати одразу після встановлення QRadar Incident Forensics - пристрої з перехоплення пакетів (package capture devices), про які статистично дуже часто забувають, або встановлюють їх некоректно. Перше, що потрібно запам’ятати - можна підключити до п'яти пристроїв з перехопленням пакетів до керованого (або іноді автономного) хоста IBM Security QRadar Incident Forensics. Якщо ж жоден пристрій з перехопленням пакетів не підключено, можна вручну завантажити файли перехоплення пакетів за допомогою користувацького інтерфейсу або за допомогою FTP. Обмеження: Використання Deployment Editor (Редактора розгортання) для додавання пристроїв з перехопленням пакетів не підтримується, для цього слід використовувати інструмент System and License Management (Управління системою та ліцензіями). До речі, процес встановлення такий самий для автономних розгортань, але керований хост не розгортається.

Крім того, необхідно забезпечити користувачів можливістю передавати файли самостійно (за допомогою безпечного протоколу FTP). Це робиться з метою розслідування інцидентів безпеки, виявлення порушень, аналізу подій та виявлення можливих загроз для системи. Надання цих даних на обробку дозволяє адміністраторам та аналітикам безпечно аналізувати інформацію та здійснювати необхідні кроки для виявлення та вирішення проблем безпеки. Для цього адміністратор має видати права на безпечний FTP доступ користувачу та управляти справою, до якої ці дані будуть віднесені. Користувачі можуть вибирати, який хост IBM QRadar Incident Forensics буде обробляти їхній запит FTP. Що зручно, користувач можуть завантажувати кілька файлів до справи, і адміністратор може надати доступ до справи кільком користувачам, тобто користувач може бути частиною розслідування і приймати в ньому участь.

Часто для виявлення прихованих загроз може бути необхідно розшифрувати SSL/TLS трафік, що обробляється IBM QRadar. Для розгортання IBM QRadar Incident Forensics разом з IBM QRadar Network Packet Capture рекомендується використовувати спеціальне рішення "man-in-the-middle", де результат розшифрування передається у відкритому тексті прямо в QRadar.

У разі відсутності QRadar Network Packet Capture або якщо не потрібно розгортати рішення "man-in-the-middle", в QRadar доступні обмежені можливості розшифрування, якщо необхідні ключі доступні. Варто зазначити, що у разі ввімкнення розшифрування відбувається погіршення продуктивності. Розшифрування підтримується для наступних протоколів: SSL v3, TLS v1.0/v1.1/v1.2. Застосовуються наступні обмеження:

• Трафік не може бути розшифрований, якщо використовується стиск SSL/TLS.

• Механізм обміну ключами Diffie Hellman не підтримується, коли зашифрований трафік розшифровується за допомогою приватного ключа. При використанні приватного ключа підтримуються інші методи обміну ключами, такі як RSA. Це обмеження не стосується випадку, коли трафік розшифровується за допомогою інформації, знайденої в журналі ключів.

Зростаюче використання шифрування мережевого трафіку, зокрема TLS, покращує безпеку даних. Однак це створює виклик для аналізу трафіку. Розгортання рішень "man-in-the-middle" з можливістю розшифрування трафіку дозволяє дублювати цей трафік до QRadar Network Insights (QNI). Але як зберегти видимість в мережі, якщо дані залишаються зашифрованими?

QRadar Network Insights підтримує видимість комунікацій, що не піддаються впливу шифрування, за допомогою потоків і QNI. Для незашифрованих протоколів або тих, що використовують шифрування рідко, зберігається можливість перегляду комунікацій. Для поліпшення аналізу зашифрованого трафіку, у випуску QRadar 7.3.3 додано генерацію хешів JA3/JA3S. Хеші JA3 та JA3S працюють шляхом створення унікальних відбитків TLS/SSL сесій, які дозволяють ідентифікувати і відстежувати специфічні характеристики зашифрованих мережевих сесій.

При встановленні зашифрованої сесії програма надсилає пакет Client Hello, що містить інформацію про версію протоколу, криптографічний набір, методи стискання та розширення. Сервер відповідає пакетом Server Hello, який містить відповідні параметри. Цей обмін дозволяє обом пристроям узгодити параметри зашифрованої комунікації. JA3/JA3S хеші створюються шляхом конкатенації версії TLS, криптографічних методів, списку розширень, еліптичних кривих та форматів еліптичних кривих, а потім застосування хешу MD5. Хеші JA3 базуються на Client Hello, а JA3S – на Server Hello. Вони забезпечують стандартизований спосіб представлення цих ключових елементів.

Використовуючи QRadar Network Insights (QNI), можна аналізувати зашифровані мережеві сесії, включаючи активність шкідливого ПЗ. На вкладці "Network Activity" в QRadar можна застосувати фільтри для перегляду трафіку, пов'язаного з певною IP-адресою та хешами JA3.

Dest IP	Destinatic Port	Protocol	Suspect Content Descriptions	Application	Protocol Name	Protocol Version	TLS JA3 Hash	TLS JA3S Hash
	443	tcp_ip	N/A	Web.SecureWeb	TLS	1.0	1d095e68489d3c535297cd8dffb06cb9	184d532a16876b78846ae6a03f654890
	443	tcp_ip	N/A	Web.SecureWeb	TLS	1.0	1d095e68489d3c535297cd8dffb06cb9	184d532a16876b78846ae6a03f654890
	443	tcp_ip	N/A	Web.SecureWeb	TLS	1.0	1d095e68489d3c535297cd8dffb06cb9	184d532a16876b78846ae6a03f654890
	443	tcp_ip	self signed certificate	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
	443	tcp_ip	self signed certificate	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
	447	tcp_ip	Multiple (2)	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
	447	tcp_ip	nonstandard port	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
	447	tcp_ip	Multiple (2)	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
	447	tcp_ip	nonstandard port	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
	443	tcp_ip	N/A	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
	447	tcp_ip	Multiple (2)	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
	443	tcp_ip	Multiple (2)	Web.SecureWeb	TLS	1.0	1d095e68489d3c535297cd8dffb06cb9	4192c0a946c5bd9b544b4656d9f624a4
	447	tcp_ip	nonstandard port	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf

Застосувавши ці фільтри, ми бачимо чітко визначений набір хешів JA3 в мережевих сесіях. Швидкий пошук в інтернеті показує, що ці хеші JA3 пов'язані з ботнетом Tofsee. Ми можемо шукати мережеву активність, щоб ідентифікувати всі сесії з цим самим хешем JA3, а також знайти інші випадки хешів JA3S незалежно від IP-адреси або домену.

Шкідливе ПЗ використовувало TLS 1.0 для шифрування, але створення хешів JA3 і JA3S працює однаково для всіх версій протоколу, включаючи TLS 1.3. Наприклад, аналіз додаткових PCAP файлів, що містять шкідливе ПЗ, через QNI показав хеші JA3 і JA3S для TLS 1.0 і TLS 1.2.

	447	tcp_ip	Multiple (2)	Web.SecureWeb	TLS	1.2	72a589da586844d7f0818ce684948eea	ec74a5c51106f0419184d0dd08fb05bc
	449	tcp_ip	nonstandard port	Web.SecureWeb	TLS	1.0	72a589da586844d7f0818ce684948eea	[illegible]

Пошук в інтернеті за хешем JA3 показує, що він пов'язаний з Metasploit і CobaltStrike. Цікаво, що версії TLS для цих сесій різні, хоча хеші JA3 однакові. Однак ми бачимо, що два хости відповіли різними Server Hello на основі різних хешів JA3S.Використовуючи QRadar Incident Forensics, можна побачити текст JA3 і JA3S до хешування. У обох випадках Client Hello вказує TLS 1.2 (номер версії 771 на початку поля TLSJA3Text).

Де сервер "Server Hello" вище відповідає версією 771 (TLS 1.2), сервер нижче відповідає версією 769 і знижує сесію до використання TLS 1.0.

Отже, використання хешів JA3 і JA3S дозволяє ефективно аналізувати зашифрований трафік, зберігаючи видимість і контроль над мережевою безпекою і якщо ви зацікавлені в аналізі відбитків JA3/JA3S для зашифрованого трафіку у ваших мережах, рекомендується завантажити QNI з IBM Fix Central і дослідити його самостійно.

3.2 Розробка метрик для аналізу на базі QRadar Incident Forensics

Метрики відіграють ключову роль в аналізі кіберінцидентів, надаючи кількісні показники для оцінки стану безпеки, виявлення аномалій та прийняття рішень. Основні метрики, які використовуються для аналізу кіберінцидентів на базі QRadar Incident Forensics, включають:

1. Кількість інцидентів за певний період, що дозволяє оцінити частоту та інтенсивність кіберзагроз. Відстеження загальної кількості інцидентів, що відбулися за тиждень, дозволяє оцінити інтенсивність кіберзагроз і швидкість їхнього виявлення та реагування.
2. Вимірювання часу від виявлення інциденту до початку його розслідування та вирішення. Вимірювання середнього часу від виявлення інциденту до початку його розслідування та вирішення дозволяє оцінити ефективність команд реагування.
3. Категоризація інцидентів за типами, такими як шкідливе ПЗ, фішинг, DoS атаки, витоки даних тощо.
4. Ідентифікація джерел загроз, включаючи IP-адреси, геолокації, та інші атрибути.
5. Оцінка критичності інциденту на основі його впливу на організацію або критичну інфраструктуру.
6. Вимірювання ефективності впроваджених заходів кібербезпеки. Відсоток виявлених загроз з числа всіх загроз, що пройшли через систему, дозволяє оцінити ефективність механізмів виявлення.

QRadar Incident Forensics використовує різні джерела даних, включаючи журнали подій, мережеві трафіки та пакети захоплення. Журнали подій можуть бути імпортовані загалом з серверів, маршрутизаторів, та кінцевих точкок. Ці журнали містять інформацію про всі події, що відбуваються в системі, включаючи успішні та невдалі спроби доступу, зміни конфігурацій та інші дії. Також QRadar Incident Forensics захоплює мережевий трафік у реальному часі, використовуючи пристрої захоплення пакетів. Це дозволяє отримати повну картину мережевої активності, включаючи деталі зашифрованих сесій за допомогою тих самих хешів

JA3/JA3S. Аналіз PCAP файлів дивиться, чи файли містять необроблені дані мережевих сесій, які можуть бути відновлені для детального аналізу.

Для коректної роботи цих метрик в QRadar Incident Forensics необхідно виконати такі кроки:

1. Створення правил кореляції. Вони визначають як різні події пов'язані між собою. Наприклад, якщо одна людина постійно логіниться в систему о 8:00 ранку, це нормально. Але якщо вона раптом зайшла в систему о третій ночі, це вже аномалія і спрацює правило кореляції.
2. Встановлення порогових значень. Варто пам’ятати, що не можна зводити певне правило в абсолют. Повертаючись до ситуації з дивним логіном, не можна спиратись лише на одну аномалію, адже так є ризик зростання false positive. Для кожної метрики мають бути встановлені порогові значення, які визначають, коли подія або набір подій стають інцидентом. Наприклад, логін о третій ночі - недостатня причина для формування інциденту, а от декілька невдалих спроб логіну о третій ночі вже причина для реагування.
3. Налаштування звітності. QRadar Incident Forensics дозволяє налаштовувати автоматичне генерування звітів за визначеними метриками. Це включає щоденні, тижневі та місячні звіти про стан безпеки, кількість інцидентів, ефективність заходів реагування тощо. Регулярні звіти про метрики дозволяють керівництву організації оцінювати стан кібербезпеки та ефективність вжитих заходів. Це також корисно для аудиту та дотримання нормативних вимог.

Постійний моніторинг метрик дозволяє виявляти аномалії та підозрілу активність у режимі реального часу, це забезпечує швидке реагування на потенційні загрози. Зібрані метрики дозволяють проводити ретроспективний аналіз інцидентів, вивчаючи їх причини та наслідки, що допомагає вдосконалювати заходи безпеки та запобігати повторенню подібних інцидентів у майбутньому.

Також розглянемо метрики, за якими слід аналізувати файли. Ці метрики обов’язково потрібно налаштовувати при роботі з QRadar Incident Forensics, якщо ми хочемо провести якісне розслідування.

Ентропія файлу. Як ми розглянули в пункті 3.1, в рамках регулярного аналізу, впроваджується метрика ентропії для виявлення підозрілих файлів. Ентропія файлу є важливою метрикою для аналізу кіберінцидентів, яка допомагає виявляти зашифровані або стиснені шкідливі файли. Впровадження цієї метрики в QRadar Incident Forensics дозволяє адміністраторам ефективно моніторити та аналізувати підозрілу активність у файловій системі, підвищуючи загальний рівень кібербезпеки критичної інфраструктури. В QRadar Incident Forensics налаштовується автоматичний розрахунок ентропії для всіх нових файлів, що з'являються в системі. Для кожного файлу розраховується ентропія. Наприклад, файли з ентропією вище 7.5 (з можливих 8) позначаються як 100% шкідливі. Ентропія 5 та вище свідчить про потребу в глибшому аналізі цього файлу, який не можна ігнорувати.

Аналіз розподілу байтів у файлі полягає у вивченні частотного розподілу байтів (0-255) у файлі. Це дозволяє виявляти невідповідності та аномалії, що можуть свідчити про компресію або шифрування даних. Файли, які мають високу ентропію або незвично розподілені байти, можуть бути зашифрованими, стисненими або містити приховану інформацію. Звичайні текстові файли або файли з відкритим кодом мають певний характерний розподіл байтів, де деякі байти зустрічаються частіше за інші. Наприклад, у текстовому файлі букви та пробіли будуть з'являтися частіше. Файли, які містять шкідливий код або є зашифрованими, часто мають рівномірний розподіл байтів, оскільки шифрування або компресія намагаються приховати структуру даних. Це може бути виявлено за допомогою аналізу частотного розподілу байтів.

Ідентифікація підписів файлів, також відомих як "magic numbers", полягає у виявленні унікальних байтових послідовностей на початку файлів, які визначають їх тип. Ці підписи допомагають розпізнати справжній формат файлу, навіть якщо його розширення було змінено для маскування. Використання підписів файлів дозволяє виявляти підозрілі файли, які маскуються під інші типи, що є важливим для забезпечення кібербезпеки. Наприклад .txt файл заявляє себе як текстовий файл, але його підпис вказує на виконуваний файл (наприклад, підпис "MZ" вказує

на виконуваний файл Windows). Система генерує попередження про можливу загрозу. Або .jpg айл заявляє себе як зображення, але його підпис вказує на архівний файл (наприклад, підпис "PK" вказує на ZIP-архів). Система позначає файл як підозрілий.

Метрика	Опис	Приклад використання
Ентропія	Ступінь випадковості або хаотичності даних	Виявлення зашифрованих або стиснених файлів
Хеш-функції (MD5, SHA-1, SHA-256)	Унікальні підписи файлів	Виявлення змін у файлах та ідентифікація шкідливих файлів
Розподіл байтів	Аналіз частотного розподілу байтів	Виявлення аномалій та прихованої інформації
Підписи файлів	Виявлення унікальних байтових послідовностей на початку файлів	Визначення справжнього типу файлів та виявлення маскування

3.3 Розробка рекомендацій для фахівців щодо розслідування інцидентів критичної інфраструктури України

Розслідування інцидентів в критичній інфраструктурі вимагає системного підходу та використання надійних інструментів і метрик. На основі розділів 3.1 та 3.2 розроблено рекомендації для фахівців, працюючих працюють в критичній інфраструктурі України, які допоможуть ефективно проводити розслідування інцидентів та забезпечити високий рівень кібербезпеки. Рекомендації для фахівців з кібербезпеки в критичній інфраструктурі України включають використання ефективних метрик та інструментів для виявлення та розслідування інцидентів. Використання метрик, таких як ентропія, хеш-функції, розподіл байтів та підписи файлів, допомагає ідентифікувати аномалії та шкідливе ПЗ. А використовуючи їх в такому інструменті як QRadar Incident Forensics, вони надають можливість автоматизованого моніторингу, збору доказів, аналізу та візуалізації даних, що забезпечує високий рівень кібербезпеки та швидке реагування на загрози.

Спершу переконайтесь, що пристрої захоплення пакетів (Packet Capture Devices) встановлені (їх можна налаштувати та встановити до п'яти штук). Переконайтеся, що вони правильно підключені та налаштовані. Також використовуйте безпечний протокол FTP для завантаження файлів перехоплення пакетів. Налаштуйте права доступу для користувачів та адміністраторів для забезпечення безпеки даних.

Почати потрібно з коректного налаштування QRadar Incident Forensics, а саме - встановлення та налаштування рішення "man-in-the-middle".

1. Виберіть відповідне рішення MITM, яке підтримується QRadar Network Insights. Це може бути програмне забезпечення або апаратне рішення.
2. У налаштуваннях MITM вкажіть параметри розшифрування SSL/TLS, включаючи підтримувані версії протоколу (SSL v3, TLS v1.0/v1.1/v1.2).
3. Імпортуйте необхідні сертифікати та приватні ключі для розшифрування трафіку. Переконайтесь, що ці ключі зберігаються в безпечному місці.

Примітка: при розшифруванні зашифрованого трафіку необхідно враховувати певні обмеження, що можуть вплинути на процес розшифрування.

Трафік, який використовує стиск SSL/TLS, не може бути розшифрований за допомогою приватного ключа. Якщо використовується механізм обміну ключами Diffie Hellman, трафік не може бути розшифрований за допомогою приватного ключа. Інші методи обміну ключами, такі як RSA, підтримуються. Також переконайтеся, що ваші налаштування підтримують розшифрування протоколів SSL v3, TLS v1.0/v1.1/v1.2. Для TLS 1.3 можуть бути необхідні додаткові налаштування.

Після налаштування рішення "man-in-the-middle", переконайтесь, що у вас використовуються хеші JA3 і JA3S для аналізу зашифрованого трафіку. Вони дозволяють створювати унікальні відбитки TLS/SSL сесій, що допомагає ідентифікувати та відстежувати специфічні характеристики зашифрованих мережевих сесій.

Кроки для налаштування:

1. Генерація хешів JA3/JA3S: QRadar Incident Forensics підтримує генерацію хешів JA3/JA3S для аналізу зашифрованого трафіку. Ці хеші створюються шляхом конкатенації версії TLS, криптографічних методів, списку розширень, еліптичних кривих та форматів еліптичних кривих, а потім застосування хешу MD5.
2. Використовуйте хеші JA3/JA3S для аналізу мережевої активності. Застосовуйте фільтри для перегляду трафіку, пов'язаного з певною IP-адресою та хешами JA3.
3. Хеші JA3/JA3S допомагають ідентифікувати підозрілу активність, пов'язану зі шкідливим ПЗ, таким як ботнети Tofsee, Metasploit, CobaltStrike тощо. Аналіз додаткових PCAP файлів, що містять шкідливе ПЗ, допоможе виявити і розшифрувати зашифровані сесії.

Після коректного налаштування аналізу трафіку, правил кореляції, та коли ми впевнились, що вся необхідна інформація моніториться, розглянемо рекомендації для коректного аналізу доказів, а саме, наступні метрики для аналізу файлів:

1. Показник ентропії, для виявлення зашифрованих або стиснених файлів. Встановіть порогові значення ентропії, наприклад, ентропія вище 7 (з можливих 8) позначається як 100% шкідлива, а про показники вище 5 адміністратор має бути повідомлений для глибшого аналізу.
2. Хеш-функції (MD5, SHA-1, SHA-256), для виявлення змін у файлах та ідентифікації шкідливих файлів. Для кожного файлу обчислюються хеші MD5, SHA-1 і SHA-256, потім ці хеші зберігаються у безпечному місці як база для подальшого порівняння. Далі система автоматично обчислює хеші для файлів через певні інтервали часу або при кожній зміні файлу. Обчислені хеші порівнюються з базовими хешами, збереженими раніше, і якщо хеші не збігаються, це означає, що файл було змінено.
3. Розподіл байтів виявляє аномалії та приховану інформацію у файлах. Обчисліть кількість появ кожного байта (від 0 до 255) у підозрілому файлі та на основі цього створіть гістограму для візуалізації частотного розподілу байтів. Звичайні текстові файли або файли з відкритим кодом матимуть характерний розподіл байтів, де деякі байти зустрічаються частіше за інші. Якщо файл має рівномірний розподіл байтів, це може свідчити про компресію або шифрування, оскільки ці процеси прагнуть зробити дані більш випадковими.
4. Підписи файлів (Magic Numbers): Для визначення справжнього типу файлів та виявлення маскування. Витягніть перші кілька байтів файлу для визначення його підпису та порівняйте витягнутий підпис з базою даних відомих підписів файлів (magic numbers).Порівняйте визначений тип файлу з його розширенням. Якщо файл заявляє себе як один тип, але його підпис вказує на інший, файл визначається як підозрілий (наприклад розширення .pdf має підпис 25 50 44 46 2D, який відповідає PDF файлу).

Висновок

Розділ 3 розглядає комплексні рекомендації для розслідування інцидентів критичної інфраструктури України за допомогою QRadar Incident Forensics. Рекомендації спрямовані на ефективне налаштування та використання цього інструменту для забезпечення високого рівня кібербезпеки. На основі аналізу інцидентів та метрик, розроблено рекомендації для фахівців з кібербезпеки в критичній інфраструктурі України. Вони включають:

- Використання ефективних інструментів, таких як QRadar Incident Forensics, для автоматизованого моніторингу, збору доказів, аналізу та візуалізації даних.
- Налаштування пристроїв захоплення пакетів та забезпечення безпечного завантаження файлів.
- Використання хешів JA3 і JA3S для аналізу зашифрованого трафіку.
- Використання метрик, таких як ентропія, хеш-функції, розподіл байтів та підписи файлів для виявлення аномалій та шкідливого ПЗ.

Загалом, впровадження цих рекомендацій сприятиме покращенню кібербезпеки та ефективному розслідуванню інцидентів у критичній інфраструктурі України.

ВИСНОВКИ

В цій дипломній роботі було проведено всебічне дослідження проблеми розслідування інцидентів у критичній інфраструктурі України за допомогою QRadar Incident Forensics. Основними аспектами дослідження були налаштування та конфігурація системи QRadar Incident Forensics, розробка метрик для аналізу інцидентів та розробка рекомендацій для фахівців з кібербезпеки.

Було визначено, що ефективне налаштування пристроїв з перехоплення пакетів є критично важливим етапом для забезпечення повного охоплення мережевого трафіку. Крім того, розгортання рішень "man-in-the-middle" для розшифрування трафіку та використання хешів JA3/JA3S дозволяє ефективно аналізувати зашифровані сесії, що є важливим для виявлення підозрілої активності.

Розроблені метрики для аналізу файлів, такі як ентропія, хеш-функції, розподіл байтів та підписи файлів, забезпечують виявлення аномалій та шкідливого ПЗ. Використання цих метрик у QRadar Incident Forensics дозволяє адміністраторам ідентифікувати підозрілу активність, що підвищує рівень кібербезпеки критичної інфраструктури.

Рекомендації для фахівців з кібербезпеки в критичній інфраструктурі України включають:

- Налаштування та використання QRadar Incident Forensics.
- Використовувати безпечний FTP для завантаження файлів перехоплення пакетів.
- Розгорнути рішення "man-in-the-middle" для розшифрування SSL/TLS трафіку.
- Використовувати хеші JA3/JA3S для аналізу зашифрованого трафіку.
- Впровадити метрики ентропії для виявлення зашифрованих або стиснених файлів.
- Використовувати хеш-функції (MD5, SHA-1, SHA-256) для виявлення змін у файлах та ідентифікації шкідливих файлів.

- Аналізувати розподіл байтів для виявлення аномалій та прихованої інформації.
- Ідентифікувати підписи файлів (magic numbers) для визначення справжнього типу файлів та виявлення маскування.

Загалом, впровадження цих рекомендацій дозволить значно підвищити рівень кібербезпеки в критичній інфраструктурі України, забезпечити ефективний моніторинг, аналіз і розслідування кіберінцидентів, а також швидке реагування на загрози. Це створить умови для надійного захисту важливих інформаційних ресурсів та забезпечення стабільної роботи критичних інфраструктурних об'єктів країни.

Перелік використаних джерел