УДК 004.056
DOI: 10.31673/2409-7292.2018.040611

С.О. Гахов
https://orcid.org/0000-0001-9011-8210

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ПОДІЙ ТА ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ SIEM-СИСТЕМАМИ

У статті досліджуються методи автоматичного виявлення подій та інцидентів інформаційної та кібернетичної безпеки SIEM-системами. Розглянуто принципи кореляції вхідних даних та правил, які реалізуються в SIEM-системах. Встановлено перспективний напрямок подальшого розвитку теорії захищених інформаційних систем.

Ключові слова: SIEM-система, кореляційні правила, виявлення подій та інцидентів інформаційної та кібернетичної безпеки.

Постановка проблеми. Аналіз останніх повідомлень Computer Emergency Response Team of Ukraine (CERT-UA) [1-4] показав, що методи та інструменти реалізації Advanced Persistent Threat (APT) продовжують розвиватися, удосконалюватися та нарощувати свій функціонал.

Так, CERT-UA спільно зі Службою зовнішньої розвідки України було виявлено нові модифікації шкідливого програмного забезпечення типу Pterodo на комп'ютерах державних органів України, яке ймовірно є підготовчим етапом для проведення кібератаки. Дане шкідливе програмне забезпечення може збирати дані про комп'ютерну систему, регулярно відправляти їх на командно-контрольні сервери та чекати подальших команд [1].

Повідомляється, що шкідливе програмне забезпечення бекдор-завантажувача Sonoko/Propagate надає зловмисникам віддалений доступ до ураженого комп'ютера. Воно може змінювати мережеві налаштування, збирати дані історії веб-браузера, завантажувати інші шкідливі програми та змінювати значення реєстру [2].

Особливістю шкідливого програмного забезпечення Troldesh є те, що після його завантаження та запуску шифруються всі файли користувача, які є в комп'ютерній системі. Після шифрування файлів відображається повідомлення з вимогою викупу [3].

Дослідники компанії ESET виявили та проаналізували нове складне шкідливе програмне забезпечення, яке було використано для цілеспрямованих атак на інформаційно-комунікаційні системи об'єктів критичної інфраструктури в Центральній та Східній Європі. Шкідливе програмне забезпечення, яке дослідники компанії ESET назвали GreyEnergy, має багато концептуальних схожих ознак із BlackEnergy – шкідливим програмним забезпеченням, яке використовувалося під час кібернетичної атаки на українську енергосистему в грудні 2015 року [4, 5]. Шкідливе програмне забезпечення GreyEnergy має складний функціонал, який завантажується та застосовується в залежності від цілей певного етапу APT-атаки.

Складне шкідливе програмне забезпечення, так звані APBs (Advanced Persistent Bots), реалізує методи та технології, які дозволяють уникати виявлення при збереженні наполегливості у зламі цільових систем. Вони, як правило, можуть випадково змінювати IP-адреси, використовувати анонімні проксі-сервери та однорангові мережі для втілення, змінювати свої користувальницькі агенти тощо [6].

Це тільки деякі відомості, які говорять про гостру актуальність проблеми забезпечення кібернетичної безпеки корпоративних інформаційних систем, зокрема, попередження, виявлення та реагування на APT.

Аналіз останніх досліджень і публікацій за темою статті. Зловмисники стають більш компетентними в інформаційних технологіях і психології людини. Кібератаки стають усе більш цілеспрямованими, просунутими, наполегливими і тривалими.

Характерною ознакою сьогодення є автоматизація діяльності зловмисників, використання передових методів та інструментів виявлення вразливостей інформаційних систем і технологій, а також широке застосування автономно функціонуючого шкідливого програмного забезпечення та реалізація автоматичних атак інформаційних ресурсів [7].

Сьогодні передові підходи до забезпечення кібербезпеки корпоративних інформаційних систем базуються на широкому застосуванні засобів автоматизації діяльності фахівців з кібербезпеки. Для сучасного етапу розвитку систем забезпечення кібербезпеки характерно застосування інформаційних систем класу SIEM (Security information and event management), які складають базис сучасного SOC (Security operations center), але прийняття рішення щодо відповіді на виникаючі кіберінциденти залишається за людиною – адміністратором безпеки [8].

Компоненти SIEM-системи збирають, агрегують, фільтрують, зберігають, нормалізують, корелюють та візуалізують дані, які характеризують стан безпеки, як у реальному часі, так і в часовому огляді та аналізу [8].

Постановка завдання. Побудова захищеної інформаційної системи та реалізація захищеної інформаційної технології є необхідної умовою забезпечення кібернетичної безпеки корпоративних інформаційних систем.

Однак, складність APT-атак, що полягає в розмаїтті цілей, використовуваних методів та технологій, часовій рознесенності етапів досягнення часткових цілей тощо, вимагає застосування та розвитку засобів автоматизації діяльності фахівців щодо забезпечення інформаційної та кібернетичної безпеки.

Тому, метою даної статті є дослідження методів автоматичного виявлення подій та інцидентів інформаційної та кібернетичної безпеки в корпоративних інформаційних системах.

Основний матеріалу дослідження. Для сучасних корпоративних інформаційних систем характерні: структурна масштабованість; територіальна і часова рознесенність; функціональна розширюваність; розмаїття цілей створення, користувачів, інформаційних ресурсів і технологій, що визначає все зростаючу їх складність.

Необхідно підкреслити, що корпоративну інформаційну систему необхідно розглядати як цілісну систему – окрему сутність в кіберпросторі (середовищі існування процесів інформаційно-комунікаційних систем), яка повинна виконувати функції за призначенням та проявляти властивості функціональної стійкості в умовах деструктивних кібернетичних впливів.

Аналіз показав, що основними причинами виникнення деструктивних процесів функціонування інформаційних систем є:

властивості функціональних компонентів даної інформаційної системи;

властивості впроваджених зловмисником функціональних компонентів в дану інформаційну систему;

переходи інформаційної системи в небезпечний стан внаслідок ненавмисних дій користувачів тощо.

Необхідно зазначити, що при вирішенні проблеми забезпечення кібербезпеки на передній план виходять не цілі забезпечення прояву властивостей інформації, яка захищається, а цілі забезпечення безпеки процесів функціонування інформаційних систем. Необхідно забезпечувати функціонування корпоративної інформаційної системи в умовах кібернетичних впливів таким чином, щоб у ній виникали тільки ті процеси (функціональні системи), які відповідають цілям створення даної системи. Звідси, основними принципами побудови захищених інформаційних систем слід вважати принцип “захищеного периметра” і принцип “захищеного внутрішнього середовища”.

Сучасні підходи до забезпечення кібернетичної безпеки корпоративних інформаційних систем базуються на функціональних системах, які виникають в середовищі “людина – SIEM-система – компоненти та процеси інформаційної системи”. Основним змістом роботи фахівців SOC (архітекторів, аналітиків та адміністраторів безпеки) є запобігання переходу інформаційної системи в небезпечний стан шляхом реалізації захищеної інформаційної

технології, виявлення та встановлення індикаторів компрометації; виявлення подій та інцидентів безпеки в інформаційній системі; реагування на інциденти безпеки.

Під індикаторами компрометації розуміються ознаки та характеристики функціональних компонентів та процесів, що спостерігаються в інформаційній системі та можуть свідчити про її компрометацію. Прикладами індикаторів компрометації можуть бути певні IP-адреси, URL-адреси, хеш-суми файлів тощо.

Під подією безпеки вважається будь-який ідентифікований процес, який змінює або може змінити стан безпеки інформаційної системи. Під інцидентом безпеки вважається перехід інформаційної системи в небезпечний стан.

Застосування SIEM-системи має за мету підвищення ефективності діяльності людини щодо забезпечення кібернетичної безпеки корпоративної інформаційної системи. Відмінною ознакою сучасних SIEM-систем є реалізація механізму інтелектуальної обробки даних безпеки на основі контекстної, поведінкової і часової аналітики.

Так, наприклад, в IBM QRadar SIEM функція кореляції зібраних даних та правил реалізується механізмом правил, які створюються (Custom Rules Engine (CRE)) [9]. Кожне з типів правил (правила події, потоку, загальне, порушення) виступає образом, який застосовується для кореляції вхідних даних, зібраних із різних джерел різних функціональних рівнів інформаційних систем в реальному часі, для моніторингу стану безпеки інформаційної системи.

Кореляційне правило представляє собою регулярний вираз (речення), яке містить змінні, які можуть налаштовуватися. Для виявлення складних подій та порушень безпеки є можливість створення системи кореляційних правил за допомогою використання логічних операторів ТА, АБО чи НІ.

Саме індикатори компрометації виступають у ролі змінних кореляційних правил (див. рис. 1). Кореляційні правила надають змогу виявляти надмірні відмови брандмауера, множинні невдалі спроби входу в систему, потенційну активність ботнету тощо.

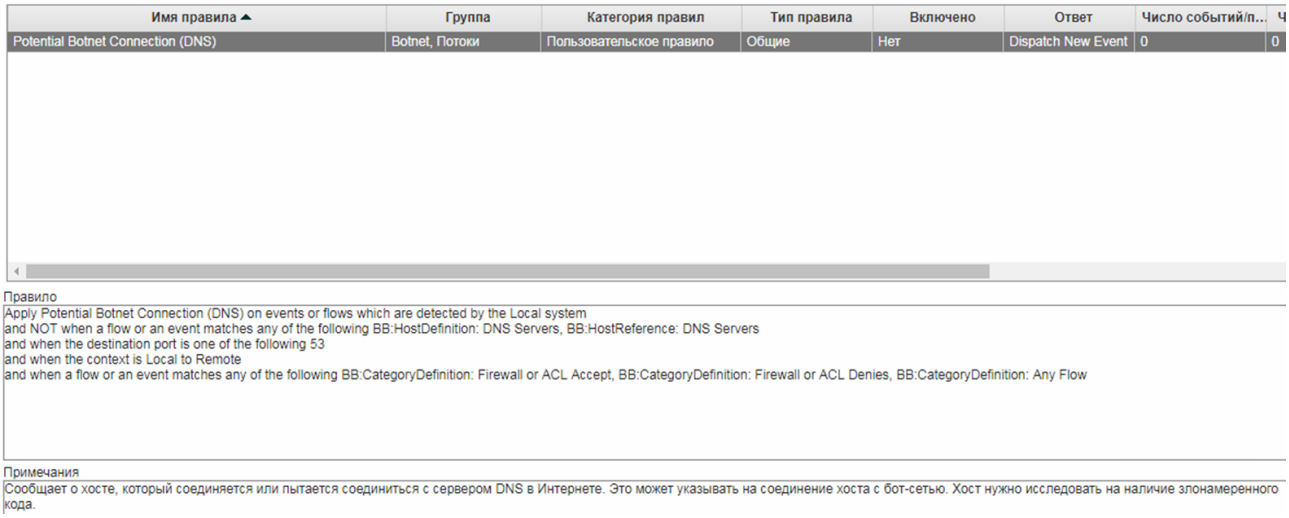

Рис. 1. Приклад змісту системи кореляційних правил в IBM QRadar SIEM

Кожне з типів правил (події, потоку, загальне та порушення) застосовується для реалізації функції кореляції вхідних даних з різних джерел у режимі реального часу. Існує кілька типів тестів правил. Деякі перевіряють наявність простих властивостей з набору даних. Інші тести правил більш складні. Вони відстежують кілька подій, потоків і порушень протягом певного періоду часу і використовують “лічильник” визначених параметрів до того, як спрацьовує відповідь правила.

Правила подій беруть участь у тестуванні вхідних даних журналів, які обробляються в режимі реального часу процесором подій QRadar. Правило події створюється для виявлення однієї події або послідовності подій за визначеною ознакою. Наприклад, щоб відстежувати інформаційну систему на предмет невдалих спроб входу до неї, виявлення сканування портів кількох хостів, за яким слідує експлуатація виявленої вразливості тощо.

Правила потоку беруть участь у тестуванні вхідних даних щодо потоків, які обробляються процесором потоку QRadar. Правило потоку створюється для визначення одного потоку або послідовності потоків за певною ознакою.

Загальні правила беруть участь у тестуванні вхідних даних подій і потоків. Загальне правило створюється для виявлення подій і потоків за визначеними ознаками, наприклад, за певною IP-адресою джерела.

Правила порушення беруть участь у тестуванні вхідних даних щодо порушень, наприклад, коли порушення відбувається протягом конкретної дати та часу. Правило порушення спрацьовує тільки в разі внесення змін до ознак та параметрів порушення, наприклад, коли додаються нові ознаки події або система призначає порушення для переоцінки.

Особливою групою кореляційних правил, які вимагають накопичення статистичних даних, є правила виявлення аномалій.

Під час застосування правил виявлення аномалій використовуються результати збережених даних потоків за певними параметрами та виявляються незвичайні зміни параметрів трафіку. Функція кореляції визначених даних параметрів потоків та правил виявлення аномалій реалізується механізмом виявлення аномалій (Anomaly Detection Engine (ADE)) [9].

Різновидами правил виявлення аномалій є правила порогів, правила аномалій та поведінкові правила.

Під час застосування правил порогів дані щодо подій або потоків перевіряються на відповідність заданому діапазону значення певного параметра (рис. 2). Ці правила корисні для виявлення змін використання смуги пропускання в додатках; служб, які невдало завершили роботу; користувачів, які використовують VPN; вихідного трафіку великого обсягу тощо.

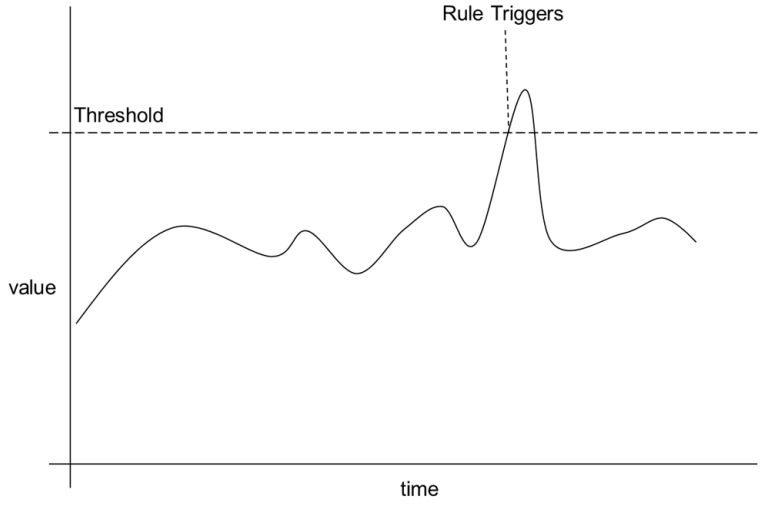

Рис. 2. Пояснення принципу правил порогів (за матеріалами IBM)

Під час застосування правил аномалій дані щодо подій або потоків перевіряється на наявність змін значення певного параметра протягом короткого часу по зрівнянню з більш тривалим періодом часу (рис. 3). Наприклад, різке зростання числа нових активів у системі,

аварійне завершення роботи веб-сервера, брандмауери, які починають масово відмовляти в трафіку тощо.

Під час застосування поведінкових правил дані щодо подій або потоків перевіряється на предмет зміни значень певних параметрів в звичайних шаблонах значень для подій або потоків, щоб виявити аномалії (рис. 4). Наприклад, у поштового сервера є відкрита ретрансляція і він раптово починає взаємодію з багатьма хостами або системи IPS починають генерувати численні сповіщення тощо.

Поведінкове правило містить змінні величини, які відображають швидкість зміни певного параметра або його об'єму протягом завчасно визначеного часового інтервалу. Даний часовий інтервал визначає базовий рівень для оцінювання.

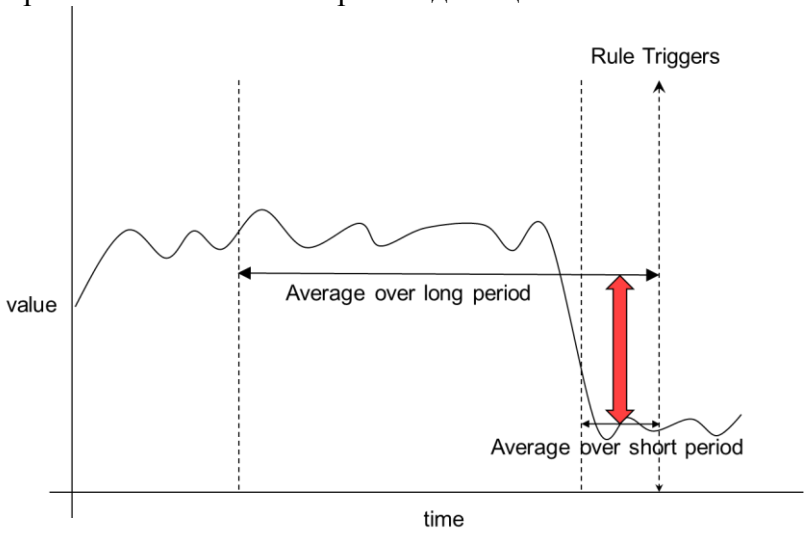

Рис. 3. Пояснення принципу правил аномалій (за матеріалами IBM)

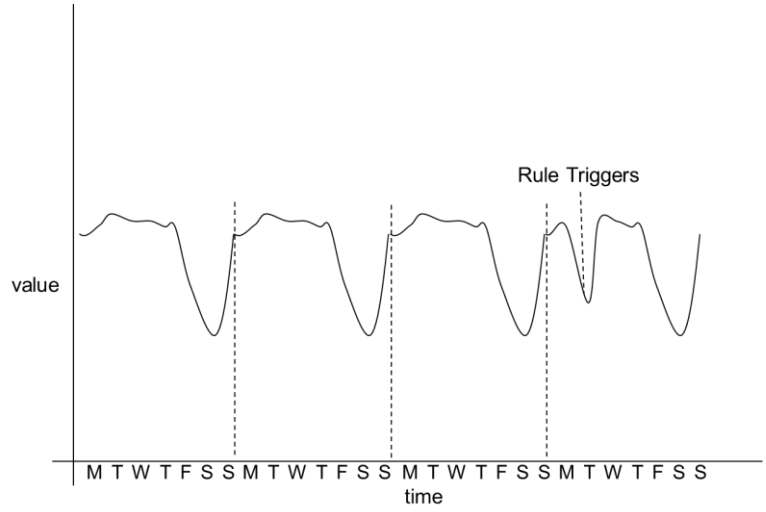

Рис. 4. Пояснення принципу поведінкових правил (за матеріалами IBM)

Висновки. Розглянуті методи автоматичного виявлення подій та інцидентів інформаційної та кібернетичної безпеки в корпоративних інформаційних системах, які застосовуються в SIEM-системах, дозволяють виявляти APT-атаки на будь-якому етапі їх життєвого циклу.

Знання напрямків і перспектив розвитку теорії та практики забезпечення кібернетичної безпеки корпоративних інформаційних систем необхідно для подальших наукових

досліджень у цій галузі, обґрунтування вимог до систем забезпечення кібербезпеки та їх створення, а також для підготовки майбутніх фахівців.

Список використаних джерел

1. Виявлена підготовка до проведення кібератаки з використанням ШПЗ типу Pterodo [Електронний ресурс] – Режим доступу: https://cert.gov.ua/news/46#.

2. Розсилка шкідливого програмного забезпечення бекдор-завантажувача Sonoko/Propagate [Електронний ресурс] – Режим доступу: https://cert.gov.ua/news/47.

3. Нові хвилі масових розсилок вірусу-шифрувальника Troldesh [Електронний ресурс] – Режим доступу: https://cert.gov.ua/news/48.

4. Виявлено нове шкідливе програмне забезпечення GreyEnergy [Електронний ресурс] – Режим доступу: https://cert.gov.ua/news/45.

5. GreyEnergy – наступник BlackEnergy [Електронний ресурс] – Режим доступу: https://eset.ua/download_files/marketing/Releases/GreyEnergy_final_ua.pdf.

6. Distil Networks. 2018 Bad Bot Report. The Year Bad Bots Went Mainstream [Електронний ресурс] – Режим доступу: http://www.gmi.com/wp-content/uploads/2018/04/General-Microsystems_2018-bad-bot-report.pdf.

7. OWASP Automated Threat Handbook Web Applications. Version 1.2 [Електронний ресурс] – Режим доступу: https://www.owasp.org/images/3/33/Automated-threat-handbook.pdf.

8. MITRE. Ten Strategies of a World-Class Cybersecurity Operations Center. Carson Zimmerman – The MITRE Corporation, 2014. – 346 p. [Електронний ресурс] – Режим доступу: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf.

9. Rules [Електронний ресурс] – Режим доступу: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_rul_mgt.html.