КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.118128
УДК 004.056.53:519.171

Косогов Олександр Миколайович
к.військ.н., старший науковий співробітник, доцент
Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0001-6691-273X
olmykos@gmail.com

СИНЕРГЕТИЧНА АРХІТЕКТУРА ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ЦІЛЕСПРЯМОВАНИХ ІНФОРМАЦІЙНИХ АТАК

Анотація. Виявлення цілеспрямованих атак з метою своєчасної протидії їм потребує оперативного аналізу інформаційного простору з використанням спеціалізованих систем моніторингу. Такі системи мають забезпечувати не тільки апаратний аналіз інформаційних атак, а й кількісний аналіз динаміки проявів цих атак з урахуванням їх специфіки. У разі здійснення атаки інтенсивність інцидентів потоку атак, яка являє собою часовий ряд за кількістю інформаційних інцидентів за певний проміжок часу (як правило, за добу), може містити інформацію як про сам факт цілеспрямованої атаки, так і про фазу сценарію, за яким вона здійснюється. Відмічено, що сучасне виявлення загроз інформаційній безпеці — це переважно ручний процес, в якому команди аналітиків відстежують підозрілі події, використовуючи допоміжні інструменти. Здатність аналітиків розпізнавати підозрілу активність і повноваження приймати рішення щодо загроз ставлять людей на центральну роль у процесі виявлення загроз. Зазначено, що надмірне покладання на людські здібності може призвести до великої кількості невиявлених загроз. Обґрунтовано потребу в новій парадигмі виявлення, яка була б значною мірою автоматизованою, але в якій аналітики зберігали б ситуативну обізнаність і контроль над процесом. У статті запропоновано синергетичний процес виявлення, який раціонально використовує переваги людського пізнання і машинних обчислень, пом'якшуючи при цьому їх слабкі сторони. Представлено структуру виявлення аналітика в циклі і надано опис типів необхідних взаємодій між системою збору доказів, механізмом виводу і аналітиком. представлено структуру виявлення аналітика в циклі і надано опис типів необхідних взаємодій між системою збору доказів, механізмом виводу і аналітиком. Продемонстровано використання запитів та операцій для покращення виявлення і закладено основи для більш детального операційного визначення взаємодій.

Ключові слова: інформаційна загроза; синергетична архітектура; автоматизоване виявлення; цілеспрямована інформаційна атака; аналітик; збір доказів.

ВСТУП

Управління різними технологічними процесами в авіації базується на використанні інформаційно-телекомунікаційних систем (ІТС), до яких відносяться джерела інформації, засоби її передавання, оброблення, відображення, зберігання, загальносистемне та спеціальне програмне забезпечення. У всіх інформаційних технологічних процесах, а також процесах управління, важливу роль відіграє людський фактор.

Незважаючи на постійний прогрес в автоматизованому виявленні загроз, люди-аналітики та особи, які приймають рішення, продовжують відігравати вирішальну роль у боротьбі за безпеку ІТС [1]. Типовий процес виявлення загроз, як показано на рис. 1, починається зі спостереження за активністю дій в інформаційному просторі, яка потім фільтрується за допомогою набору інструментів виявлення [2]. Аналітик використовує

ці інструменти та їхні результати (наприклад, інформаційні зведення та попередження) для прийняття остаточного рішення про те, які загрози присутні в мережі та їхній можливий вплив на місію.

Багато особливостей кіберсередовища кидають виклик можливостям і здатності людського пізнання, в тому числі постійно зростаючий обсяг мережевих даних, широке розмаїття джерел даних, а також часті і несподівані зміни в мережі. Аналітик бере на себе велику відповідальність за прийняття якісних рішень в рамках поточного процесу виявлення. Як наслідок, велика увага приділяється підвищенню кваліфікації та досвіду аналітиків. Хоча основна роль людини-аналітика полягає у виявленні реальних загроз у великому обсязі оповіщень, аналітики також зобов'язані отримувати і підтримувати обізнаність про кіберситуацію [3].

Постановка проблеми. За останні роки характер кібератак зазнав значних змін, про що свідчить поява все більшої кількості випадків деструктивних просунутих перманентних загроз (Advanced Persistent Threats, APT). Провідні урядові установи та організації зазнали все більш витончених атак, які мають відмінні характеристики порівняно з більш традиційними кіберзагрозами. APT, як правило, є добре спонсорованими та організованими кіберкампаніями з дуже конкретними та цілеспрямованими цілями. Однією з ключових цілей APT є досягнення стійкого закріплення в системі на тривалий період часу шляхом використання експлойтів «нульового дня», обережного розповсюдження і невеликого сліду. Все це залежить від якості інформації, що надається аналітику, і від здатності достатньою мірою обробити цю інформацію. Аналітик може навіть перешкоджати виявленню, оскільки основні людські можливості, такі як обсяг пам'яті та швидкість обробки, не можуть бути легко збільшені, щоб відповідати постійно зростаючому обсягу мережевого трафіку. Крім того, зміна моделей прийняття рішень аналітиком вимагає цілеспрямованих зусиль, які можуть відбуватися повільніше, ніж з'являються нові моделі кібератак.

Аналіз останніх досліджень і публікацій. У цьому підрозділі здійснюється аналіз робіт, у яких започатковано розв'язання даної проблеми, і на які спирається автор. Як результат аналізу джерел обов'язково виокремлюються раніше невирішені частини загальної проблеми, яким присвячена стаття:

Аналіз спеціалізованої літератури [2] – [5] свідчить про те, що процес забезпечення безпеки інформації повинен носити комплексний характер і має ґрунтуватися на глибокому аналізі можливих негативних наслідків (логіко-евристичний аналіз). Такий аналіз припускає обов'язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їхньому прояву (уразливостей) і, як наслідок, визначення актуальних загроз інформаційній безпеці [2].

Зокрема, аналітики розкривають значення поведінки мережі, що спостерігається (наприклад, яка її природа і походження?), і прогнозують, як ця поведінка може розвиватися і вплинути на місію (наприклад, що зловмисник буде робити далі?). Ця інформація формує рішення аналітика про те, як реагувати на ситуацію і який захист буде ефективним [4], [5].

У ході аналізу необхідно переконатися, що всі можливі загрози та їх джерела ідентифіковані, всі можливі уразливості ідентифіковані та зіставлені з ідентифікованими джерелами загроз, всім ідентифікованим джерелам загроз і уразливостям (факторам) зіставлені методи реалізації.

При цьому важливо мати можливість, у разі потреби, не міняючи самого методичного інструментарію, вводити нові види джерел загроз, методів їх реалізації, уразливостей, які стануть відомі в результаті подальшого отримання знань у цій сфері.

Виявлення та аналіз загроз інформаційній безпеці є першим етапом у розробці стратегії протидії інформаційних загроз (політики безпеки). При цьому процес виявлення та аналізу загроз слід розглядати в органічному зв'язку з процесом протидії загрозам.

Мета статті. Викладення структури адаптивного процесу виявлення загроз, в якому система моніторингу, механізм виявлення та людина-аналітик працюють разом для обміну інформацією та прийняття більш точних рішень. Ця структура має на меті забезпечити ефективне інвестування цінних, хоча і обмежених, когнітивних ресурсів аналітика в процеси виявлення шляхом створення основи для протоколу між компонентами виявлення.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Виявлення APT вимагає значної людської участі та зусиль при проведенні ретельного аналізу [6].

Протягом усього робочого процесу виявлення аналітик повинен мати можливість використовувати різні інструменти підтримки прийняття рішень. Ці інструменти допомагають аналітику фільтрувати, видобувати, узагальнювати та візуалізувати дані для прискорення аналізу. У деяких випадках, коли є достатня впевненість в автоматизованій діагностиці, інструменти можуть навіть визначати загрозу і ініціювати відповідне реагування. Однак у поточному лінійному робочому процесі виявлення загроз (рис. 1) аналітик не має впливу на спосіб збору або обробки доказів, і в кінцевому підсумку змушений приймати рішення на основі нав'язаного ззовні інформаційного потоку. Відсутність контролю і прозорості може перешкоджати обміну інформацією між аналітиками для того, щоб мати адаптивний процес, здатний виявляти нові загрози. На відміну від робочого процесу виявлення загроз, який значною мірою залежить від людини, пропонована структура описує процес, в якому компоненти підтримують і доповнюють один одного. Ми представляємо в рамках нашої концепції:

- різні рівні залучення аналітиків до процесу виявлення;
- адаптація виявлення відповідно до життєвого циклу загрози;
- характеризуючи типи взаємодії між компонентами виявлення, аналітик може швидко і точно виявляти загрози.

У таких критично важливих ситуаціях, як виявлення загроз, аналітик повинен довіряти допоміжним інструментам, а також мати доступ до аргументації рекомендацій або сповіщень, які вони генерують, щоб правильно визначити, чи варто акцептору відхиляти рекомендацію [7].

Для виявлення ATP і забезпечення високого рівня виконання місії шляхом встановлення довіри до інструменту підтримки прийняття рішень і дотримання рекомендацій, які він генерує, аналітик повинен мати можливість взаємодіяти з основними механізмами виявлення протягом усього процесу виявлення (як показано на рис. 2), а не тільки в самому кінці [8]. Крім того, за допомогою такої взаємодії аналітик може надавати контекстну інформацію, яка може підтримати і підвищити точність і швидкість виявлення. Аналітик також може безперервно налаштовувати процеси виявлення у відповідь на нові загрози і надавати інструкції щодо того, як процеси виявлення повинні адаптуватися до змін у поверхні атаки і можливостях зловмисників.

Нещодавні дослідження взаємодії людини з даними (HDI) пропонують людиноцентричний підхід до розуміння і розвитку взаємодії з даними, динамічними

ISSN 2663 - 4023

потоками даних, алгоритмами, автоматизованими механізмами міркувань і візуалізацій [9]. Основні характеристики взаємодії HDI можуть бути адаптовані до сфери виявлення кібервторгнень шляхом визначення аналітика як впливового компонента в кожній частині процесу виявлення. Відповідно, в нашій синергетичній концепції аналітика в циклі ми виділяємо три високорівневі аспекти взаємодії аналітика з системою виявлення. Перший аспект — це зрозумілість, яка полягає в тому, що як механізми збору даних, так і алгоритми аналітики повинні бути прозорими і зрозумілими для аналітика. Другий аспект — повноваження — полягає в тому, що аналітик повинен мати можливість контролювати і впливати на процеси збору даних та управління ними.

І, нарешті, оборотність стосується здатності аналітика впливати на обробку даних та аналітику, щоб дані могли оброблятися різними методами, для різних цілей і в різних контекстах.

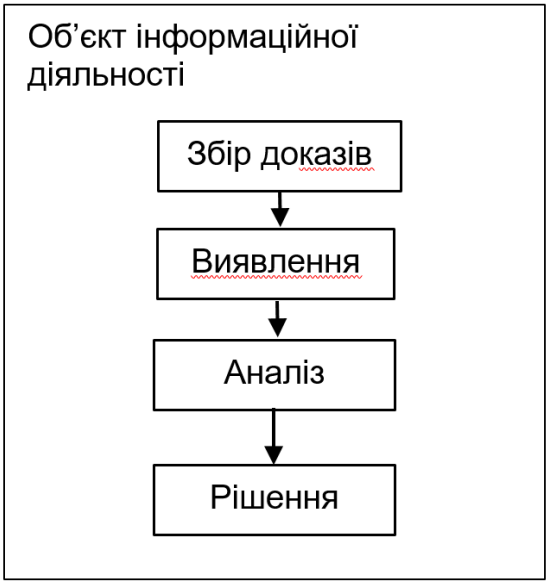

Рис. 1. Лінійний процес виявлення

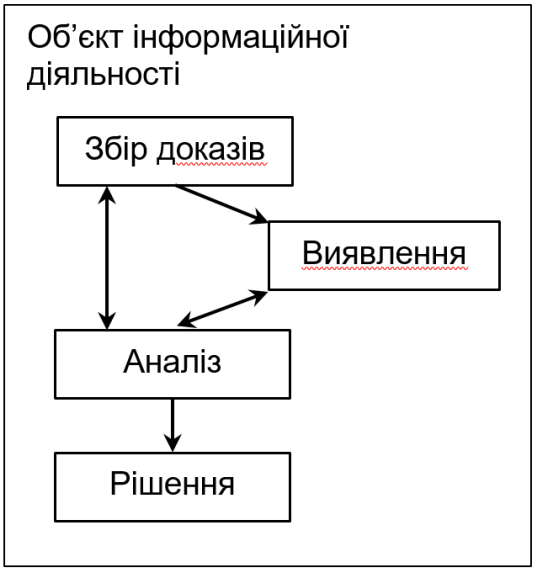

Рис. 2: Синергетичний процес виявлення

Рівні залучення аналітиків до виявлення

Увага людини-аналітика є цінним і дефіцитним ресурсом. Тому увагу та когнітивні здібності людини слід розподіляти таким чином, щоб вони були спрямовані на виконання найбільш важливих завдань. Інші завдання, які не отримують значної користі від людських аналітичних здібностей або відіграють менш важливу роль, можуть бути частково або повністю автоматизовані. У [10] пропонується модель типів та рівнів взаємодії людини із засобами автоматизації.

Серед інших практичних реалізацій, ця модель може бути використана для призначення різних рівнів автоматизації для чотирьох етапів обробки інформації (збір інформації, аналіз інформації, вибір рішення і реалізація дій). Виявлення атаки ґрунтується на обробці інформації, де збір ознак є еквівалентом збору інформації, робота механізму виявлення еквівалентна аналізу інформації, а етапи прийняття рішення аналітиком і реагування відповідають етапам вибору рішення і реалізації дій. Таким чином, на кожному з етапів виявлення участь аналітика може варіюватися від високої до низької. Висока участь аналітика відповідає низькому рівню автоматизації, коли аналітик повинен приймати всі рішення і дії, в той час як низька участь аналітика відповідає високому рівню автоматизації, коли процеси виявлення працюють автономно. Що стосується рішення аналітика про наявність чи відсутність кібератаки, ми розглядаємо чотири рівні взаємодії. На найнижчому рівні взаємодії аналітик працює без сторонньої допомоги і виявляє загрози в необроблених даних на рівні повідомлень. Рівень автоматизації можна підвищити, додавши механізми виявлення, які надають аналітику рекомендації (тобто оповіщення). Фактичний рівень автоматизації залежить від визначення ролі аналітика при реагуванні на ці оповіщення. Аналітики можуть підтверджувати правильність виявлених загроз і виявляти додаткові загрози, які були пропущені автоматизованим виявленням. З іншого боку, якщо автоматизація є більш широкою і надійною, роль аналітика може бути обмежена виявленням пропущених загроз і скасуванням помилкових тривог. На найвищому рівні всі аспекти виявлення автоматизовані, і аналітик може зосередити всю свою увагу на виборі найкращої реакції на виявлені загрози.

Адаптація виявлення до життєвого циклу загрози

Загрози можна охарактеризувати тим, наскільки ефективно їх можна виявити за допомогою автоматизованих методів, що, як правило, тісно пов'язано з розумінням загрози. З точки зору аналітика, загрози проходять певну стадію розуміння, яка також відображається в життєвому циклі загрози [11].

Спочатку загроза невідома аналітику; така невідома загроза часто націлена на невідому вразливість, її називають загрозою нульового дня (zero-day exploit). Виявлення такої загрози вимагає значного обсягу експертних досліджень та вивчення нормальної та аномальної поведінки системи, щоб ізолювати загрозу та отримати попереднє уявлення про її існування. На цьому етапі може значною мірою залучатися участь людини — від визначення (тобто маркування) активності як зловмисної, до виявлення доказів, що вказують на наявність загрози, і визначення її впливу. Чим більше прикладів загрози спостерігається, тим більше інформації відкривається людині. Зрештою, знання про загрозу покращується до такої міри, що точні механізми виявлення можуть бути автоматизовані і запрограмовані в системах виявлення вторгнень. Ця автоматизація, паралельно з виправленням (наприклад, виправленням) вразливостей, знімає навантаження з аналітика. Дуже важливо забезпечити підтримку аналітика за допомогою

автоматизації на цьому етапі життєвого циклу загрози, оскільки після розкриття обсяг кібератак, що використовують конкретну загрозу, може збільшитися на 5 порядків [12].

На цьому етапі виявлення вже добре зрозумілої загрози можна сміливо передати переважно автоматизованим механізмам. Аналітик залишається відповідальним за прийняття остаточного рішення на основі результатів автоматизованого виявлення. Однак більша частина обробки даних для визначення ймовірності загрози відбувається без участі людини.

Динаміка життєвого циклу загрози і виявлення вказує на необхідність забезпечення різних рівнів автоматизації процесів виявлення. Ця можливість тісно пов'язана зі здатністю аналітика взаємодіяти з процесами виявлення, розуміти, як вони працюють, і впливати на їхню роботу. Зрештою, потреби і роль людини-аналітика можуть постійно змінюватися, і тому процеси виявлення повинні бути достатньо гнучкими, щоб полегшити роботу аналітика в умовах постійних змін рівня розуміння і обізнаності про загрози інформаційному простору.

Синергетичне аналітичне виявлення кібератак

Для того, щоб сформулювати та продемонструвати синергетичну архітектуру виявлення вторгнень, розглянемо спрощений процес виявлення. Кіберактивність впливає на навколишнє середовище. Стан середовища вимірюється засобами моніторингу і містить ознаки.

Отримані ознаки надходять до системи виявлення (Inference), яка перевіряє гіпотези, присвоюючи їм вагу.

Ґрунтуючись на наявних дослідженнях щодо виявлення загроз та взаємодії інформації про загрозу, гіпотеза полягає в тому, що кожен компонент взаємодіє та обмінюється відповідною інформацією з іншими компонентами. Це дає змогу швидше приймати кращі рішення щодо нових та існуючих загроз. Спочатку представляються компоненти процесу виявлення, а потім обговорюється взаємодія між ними.

Компоненти

Трьома центральними компонентами системи виявлення є Механізм збору фактичних даних (позначається **C**), Механізм виявлення/висновків (**D**) і людина-аналітик (**A**) (див. рис. 3). Остаточне рішення щодо загроз приймає **A** за підтримки **D** та **C**.

C, система збору інформації, керує засобами моніторингу, які передають інформацію про поведінку спостережуваної активності для використання механізмом виявлення. Вони можуть розміщуватися на локальному рівні мережі для перевірки трафіку (наприклад, глибока перевірка пакетів) або на рівні хоста для моніторингу процесів. Отримана інформація перетворюється на підтвердження, яке необхідне **D** або **A**.

C володіє інформацією про типи підтверджень, які він може зібрати, а також про вартість їх збору. Відомості мають багато властивостей, таких як частота оновлення, швидкість передачі, дисперсія, достовірність тощо.

Ці можливості уможливлюють різноманітну поведінку. Наприклад, вона може розрахувати вартість розгортання запропонованого набору засобів моніторингу або повідомити аналітика, коли надійність зібраних даних погіршилася.

D, система виявлення, обробляє наявні спостереження і генерує ймовірності можливих загроз. Важливою здатністю **D** є робота з великими обсягами інформації. Вона здатна вдосконалювати своє виявлення та адаптуватися до змін у навколишньому середовищі завдяки взаємодії з людиною (наприклад, кероване машинне навчання [13]).

Для конкретної загрози **D** певною мірою розуміє взаємозв’язок між ймовірністю та фактами, наприклад, як необхідними або достатніми умовами для загрози. Вона здатна

надати людині розуміння того, як обчислюється ймовірність загрози. Це означає, що її внутрішня логіка може бути надана людині в зрозумілому форматі.

Людина-аналітик вирішує, які загрози мають місце, як правило, беручи до уваги ймовірності, обчислені механізмом виявлення.

Замість того, щоб зосередитися на структурі **D** і **C**, ця стаття зосереджується на тому, як людина-аналітик може взаємодіяти з **D** і **C**. Далі наведено допоміжну структуру для цих взаємодій.

Інтерактивний процес виявлення

На рис. 3 зображено процес виявлення загроз, де суцільні стрілки вказують на напрямок руху інформації від джерела до отримувача. Потік виявлення починається з подій у мережі та на хості, за якими спостерігають засоби моніторингу. Система збору інформації **C** розгортає монітори і перетворює зібрану інформацію на докази. Механізм виявлення **D** робить висновки про те, які загрози є ймовірними з огляду на надані докази. Ймовірності представляються аналітику у вигляді набору вагових коефіцієнтів.

Мета аналітика **A** — спостерігати за набором гіпотез і вагових коефіцієнтів та вирішувати, які види діяльності відбуваються. Для того, щоб покращити продуктивність (точність, ефективність і т.д.) загального потоку виявлення, аналітик може взаємодіяти з **C** і **D**, як показано пунктирними лініями на рис. 3. **C** і **D** також можуть взаємодіяти безпосередньо. Така взаємодія може бути поширенням взаємодії аналітика з одним компонентом на інший або результатом поточного виконання процесу. Формалізуємо взаємодію між компонентами процесів виявлення в термінах запитів та операцій.

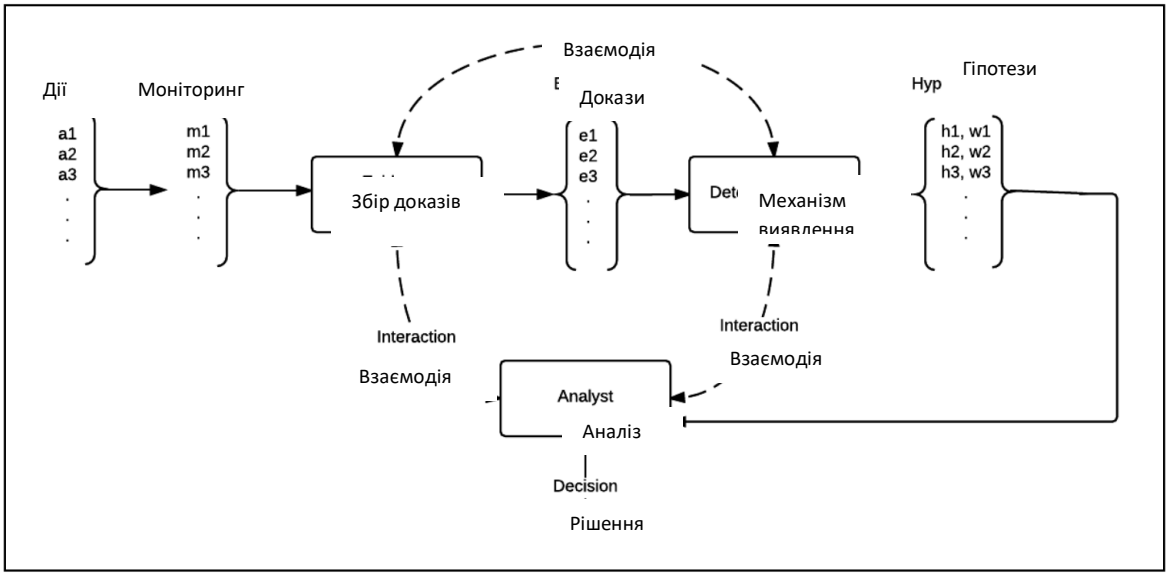

Рис. 3: Потік інформації (суцільні лінії) та взаємодії в процесі синергетичного виявлення (пунктирні лінії)

Взаємодія

Взаємодія між процесами виявлення підпадає під одну з двох можливих категорій:

1. Запити — будь-який тип запиту на інформацію (тобто запит), який не змінює роботу процесу. За запитом завжди слідує відповідь.

2. Операція — будь-який тип запиту, який змінює роботу процесу. Операція завжди супроводжується зворотним зв'язком, який вказує, принаймні, на те, чи була операція успішно завершена чи ні.

В рамках синергетичного виявлення запити та операції можуть приймати різні форми. Замість того, щоб перераховувати всі можливі запити і операції, для ілюстрації потоку взаємодії і деяких з найбільш важливих запитів і операцій ми використовуємо наступний спрощений приклад.

1. **C** розгортає комплект пристроїв для відслідковування мережевої активності.

2. На основі зібраних доказів **D** надає **A** попередження про те, що дії a1, a2 є ймовірними, а дія a3 є малоймовірною. Тут ми вважаємо, що a1 — це несанкціоноване підвищення привілеїв, a2 — поточна атака SYN-флуду, коли **C** спостерігає велику кількість SYN-пакетів, а a3 — маячок шкідливого програмного забезпечення на керуючий сервер.

3. **(a1).** Виходячи з досвіду, **A** знає, що **D** генерує точні попередження для a1 і, таким чином, підтверджує, що a1 є вірним. Цей тип взаємодії з оновлення забезпечує зворотній зв'язок з **D**, що підсилює використання механізму, який з високою ймовірністю дав результат a1.

4. **(a2). A** знає про поточний стан мережі та ефемерні завдання, які вона підтримує. Таким чином, A може використовувати цю контекстну інформацію, щоб відкинути тривогу щодо a2. Знову ж таки, ця взаємодія забезпечує зворотній зв'язок з **D** і впливає на його подальшу роботу.

5. **(a3).** Щодо a3, **A** запитує **D** про деталі щодо типу доказів, які **D** використовував при прийнятті рішення. Враховуючи високий ризик пропуску активності шкідливого програмного забезпечення, **A** може надіслати запит до **D** про те, які додаткові докази необхідні для того, щоб з більшою впевненістю стверджувати, що a3 має місце чи ні. На основі відповіді **A** може доручити **C** виконати операцію зі збору цільових доказів, щоб вирішити невизначеність щодо a3. **C** обробляє запит на операцію і модифікує монітори відповідно до нього. Після завершення операції **C** інформує **A** про успішне виконання запиту, а **D** — про зміни в потоці доказів. Тепер, маючи додаткові докази, **D** може надати **A** більш впевнене попередження щодо дії a3.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Наразі зловмисники мають асиметричну перевагу над захисниками. Ця несприятлива і вразлива позиція вимагає надійних та ефективних механізмів виявлення вторгнень. Хоча поточний робочий процес виявлення вторгнень передбачає залучення людей-захисників і покладається на їхні аналітичні можливості, ми стверджуємо, що для покращення виявлення та захисту мереж від складних атак необхідний нелінійний та інтерактивний підхід «аналітик в циклі». Цей підхід передбачає, що кіберзахисники повинні мати засоби для взаємодії та впливу на кожен компонент процесу виявлення.

Крім того, роль аналітика полягає в тому, щоб керувати і контролювати автоматизовані процеси виявлення, вирішувати неоднозначності і надавати контекстну інформацію, що стосується місії, а не обробляти великі обсяги інформації і відсіювати помилкові тривоги. Позиціонування захисника як контролера процесу виявлення, а не обробника тривог, дозволяє йому спрямовувати аналітичні можливості на завдання, де їхній внесок має максимальний вплив.

Ефективний розподіл аналітичних можливостей захисника підвищує точність і швидкість виявлення.

У цьому дослідженні представлено структуру виявлення аналітика в циклі і надано опис типів необхідних взаємодій між системою збору доказів, механізмом виводу і аналітиком. Продемонстровано використання запитів та операцій для покращення виявлення і закладено основи для більш детального операційного визначення взаємодій.

У перспективах подальших досліджень планується на основі запропонованої синергетичної архітектури розробити алгоритм виявлення та аналізування уразливостей об’єктів інформаційної діяльності до впливів цілеспрямованих інформаційних атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kosohov, O. (2024). Model of the dynamics of the intensity of information influence for detecting targeted information attacks. *Proceedings of the ICSU Conferences*, 184-189. https://doi.org/10.62731/mcnd-17.05.2024.007
2. Kosohov, O. M. (2023). Conceptual Bases For Evaluating The Efficiency Of Automation Of Production Processes At Aviation Enterprises. *Science and technology: problems, prospects and innovations. Proceedings of the 10th International scientific and practical conference*, 58–64.
3. Gonzalez, C., Ben-Asher, N., Oltramari, A., & Lebiere, C. (2014). Cognition and technology. *Cyber Defense and Situational Awareness*, 93–117.
4. Zhong, C., Yen, J., Liu, P., & Erbacher, R. F. (2016). Automate cybersecurity data triage by leveraging human analysts’ cognitive process. *IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 357–363.
5. Saydjari, O. S. (2004). Cyber defense: art to science. *Communications of the ACM, 47(3)*, 52–57.
6. Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013). Trusted computing vs. advanced persistent threats: Can a defender win this game? *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*, 396–403.
7. Ehrlich, K., Kirk, S. E., Patterson, J., Rasmussen, J. C., Ross, S. I., & Gruen, D. M. (2011). Taking advice from intelligent systems: the double-edged sword of explanations. *Proceedings of the 16th international conference on Intelligent user interfaces*, 125–134.
8. Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 46(1)*, 50–80.
9. Mortier, R., Haddadi, H., Henderson, T., McAuley, D., & Crowcroft, J. (2014). *Human-data interaction: the human face of the data-driven society*. https://dx.doi.org/10.2139/ssrn.2508051.
10. Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on systems, man, and cybernetics-Part A: Systems and Humans, 30(3)*, 286–297.
11. Arbaugh, W. A., Fithen, W. L., & McHugh, J. (2000). Windows of vulnerability: A case study analysis. *Computer, 33(12)*, 52–59.
12. Bilge, L., & Dumitras, T. (2012). Before we knew it: an empirical study of zero-day attacks in the real world. *Proceedings of the 2012 ACM conference on Computer and communications security*, 833–844.
13. Veeramachaneni, K., Arnaldo, I., Korrapati, V., Bassias, C., & Li, K. (2016). Ai2 Training a big data machine to defend. *IEEE International Conference on Intelligent Data and Security*, 49–54.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Oleksandr Kosohov
PhD Mil. Sci., Senior Research Fellow
Associate Professor, National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0001-6691-273X
olmykos@gmail.com

SYNERGISTIC ARCHITECTURE FOR AUTOMATED DETECTION OF TARGETED INFORMATION ATTACKS

Abstract. Detecting targeted attacks in order to counteract them in a timely manner requires an operational analysis of the information space using specialized monitoring systems. Such systems should provide not only hardware analysis of information attacks, but also quantitative analysis of the dynamics of these attacks, taking into account their specifics. In the event of an attack, the intensity of incidents of the attack flow, which is a time series by the number of information incidents over a certain period of time (usually per day), may contain information both about the fact of a targeted attack and about the phase of the scenario in which it is carried out. It is noted that the current detection of information security threats is mainly a manual process in which teams of analysts monitor suspicious events using auxiliary tools. The ability of analysts to recognize suspicious activity and the authority to make decisions about threats put people at the centre of the threat detection process. It is noted that excessive reliance on human abilities can lead to a large number of undetected threats. The author substantiates the need for a new detection paradigm that would be largely automated, but in which analysts would retain situational awareness and control over the process. The article proposes a synergistic detection process that rationally uses the advantages of human cognition and machine computing, while mitigating their weaknesses. The paper presents the structure of analyst discovery in the cycle and describes the types of required interactions between the evidence collection system, inference engine, and analyst. the paper presents the structure of analyst discovery in the cycle and describes the types of required interactions between the evidence collection system, inference engine, and analyst. The use of queries and operations to improve detection is demonstrated and the basis for a more detailed operational definition of interactions is laid.

Keywords: information threat; synergistic architecture; automated detection; targeted information attack; analyst; evidence collection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kosohov, O. (2024). Model of the dynamics of the intensity of information influence for detecting targeted information attacks. *Proceedings of the ICSU Conferences*, 184-189. https://doi.org/10.62731/mcnd-17.05.2024.007
2. Kosohov, O. M. (2023). Conceptual Bases For Evaluating The Efficiency Of Automation Of Production Processes At Aviation Enterprises. *Science and technology: problems, prospects and innovations. Proceedings of the 10th International scientific and practical conference*, 58–64.
3. Gonzalez, C., Ben-Asher, N., Oltramari, A., & Lebiere, C. (2014). Cognition and technology. *Cyber Defense and Situational Awareness*, 93–117.
4. Zhong, C., Yen, J., Liu, P., & Erbacher, R. F. (2016). Automate cybersecurity data triage by leveraging human analysts' cognitive process. *IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 357–363.
5. Saydjari, O. S. (2004). Cyber defense: art to science. *Communications of the ACM, 47(3),* 52–57.
6. Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013). Trusted computing vs. advanced persistent threats: Can a defender win this game? *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*, 396–403.

7. Ehrlich, K., Kirk, S. E., Patterson, J., Rasmussen, J. C., Ross, S. I., & Gruen, D. M. (2011). Taking advice from intelligent systems: the double-edged sword of explanations. *Proceedings of the 16th international conference on Intelligent user interfaces*, 125–134.
8. Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 46(1),* 50–80.
9. Mortier, R., Haddadi, H., Henderson, T., McAuley, D., & Crowcroft, J. (2014). *Human-data interaction: the human face of the data-driven society*. https://dx.doi.org/10.2139/ssrn.2508051.
10. Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on systems, man, and cybernetics-Part A: Systems and Humans, 30(3),* 286–297.
11. Arbaugh, W. A., Fithen, W. L., & McHugh, J. (2000). Windows of vulnerability: A case study analysis. *Computer, 33(12),* 52–59.
12. Bilge, L., & Dumitras, T. (2012). Before we knew it: an empirical study of zero-day attacks in the real world. *Proceedings of the 2012 ACM conference on Computer and communications security,* 833–844.
13. Veeramachaneni, K., Arnaldo, I., Korrapati, V., Bassias, C., & Li, K. (2016). Ai2 Training a big data machine to defend. *IEEE International Conference on Intelligent Data and Security*, 49–54.