КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1273
УДК 004.056

Гордієнко Мілан Парвез
аспірант кафедри інформаційної безпеки
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID:0009-0004-2226-2391
hordienko.m.p.-fb51f@edu.kpi.ua

МОДЕЛЬ ДИНАМІЧНОГО ОЦІНЮВАННЯ ІНДИКАТОРІВ КОМПРОМЕТАЦІЇ НА ОСНОВІ ЧАСОВОГО ЗГАСАННЯ ЧЕРЕЗ РОЗШИРЕННЯ STIX 2.1

Анотація. У цій статті запропоновано модель динамічного оцінювання індикаторів компрометації (Indicators of Compromise, IoC) на основі часового згасання – Temporal Decay Dynamic Scoring (TDDS), формалізовану у вигляді розширення стандарту STIX 2.1 за допомогою механізму Extension Definition. В основі моделі лежить комбінована математична формула, яка об'єднує чотири складові: початкову оцінку актуальності, що визначається типом індикатора відповідно до ієрархії Піраміди болю (Pyramid of Pain, PoP), репутацією джерела та ступенем підтвердження; адаптивний коефіцієнт згасання, що залежить від характерного часу напіврозпаду для відповідного типу індикатора, коефіцієнта масштабування, похідного від репутації джерела та контексту кампанії; функцію сповільнення згасання на основі спостережень та коригувальний доданок збагачення даними розвідки з відкритих джерел (OSINT). У роботі, шляхом використання механізму розширень STIX 2.1, формалізовано структуру даних, яка забезпечує передачу параметрів моделі TDDS. На відміну від наявних реалізацій – MISP та OpenCTI, – де параметри згасання є внутрішньою логікою платформи й не зберігаються під час експорту, запропонований підхід інкапсулює обчислені параметри моделі та проміжні результати розрахунків безпосередньо в структуру об'єкта STIX 2.1, забезпечуючи автономне обчислення актуальності IoC в системах-отримувачах без залежності від інфраструктури платформи-відправника.

Ключові слова: STIX 2.1; CTI; IoC; SIEM; динамічне оцінювання; часове згасання; репутація джерела; OSINT-збагачення; життєвий цикл CTI.

ВСТУП

Постійне зростання масштабу та серйозності інцидентів робить операційну ефективність центрів керування безпекою (Security Operations Center, SOC) першочерговим завданням. Згідно зі звітом IBM Security Cost of a Data Breach Report за 2025 рік, середня вартість витоку даних досягла 4,44 млн доларів США, а повний життєвий цикл інциденту – від початку проникнення до локалізації – тепер у середньому становить 241 день. З цього інтервалу 181 день припадає на середній час виявлення (mean time to identify, MTTI), а 60 днів – на середній час локалізації (mean time to contain, MTTC) [1]. Настільки тривалий час перебування загрози в системі демонструє структурну недосконаліть того, як здійснюється керування релевантними для безпеки даними після їхнього надходження до системи керування інформацією та подіями безпеки (Security Information and Event Management, SIEM).

Постановка проблеми. Опитування SANS SOC Survey 2025 свідчить, що 42% SOC імпортують усі вхідні дані у свої SIEM, зазвичай не дбаючи про те, як потім шукати їх та керувати їхнім життєвим циклом, а 18% аналітиків називають брак контексту або надмірну кількість сповіщень своєю головною проблемою [2]. Втома від помилкових сповіщень, зумовлена дубльованими та застарілими індикаторами компрометації (Indicators of Compromise, IoC), лише збільшує затримку виявлення інцидентів. Застаріла IP-адреса, яка була шкідливою місяць тому, але з того часу була перепризначена легітимному хосту, функціонально нічим не відрізняється від безпечної адреси в правилах кореляції SIEM, якщо релевантність індикатора не контролюється динамічно з плином часу. Незважаючи на те, що 69% SOC використовують дані розвідки кіберзагроз (Cyber Threat Intelligence, CTI) для реагування на інциденти [2], відсутність автоматизованих механізмів для керування життєвим циклом IoC призводить до затримки опрацювання подій та неможливості пріоритезації загроз на основі їхньої поточної актуальності.

Вирішення цієї проблеми та побудова ефективних засобів автоматизації неможливі без використання уніфікованих форматів представлення інформації про загрози. Structured Threat Information eXpression (STIX) – це мова та формат серіалізації, що використовується для обміну даними CTI. Модель даних STIX має графову структуру, в якій інформація розподіляється між трьома основними категоріями: доменними об'єктами (STIX Domain Objects, SDO), які є високорівневими сутностями розвідки, що описують поведінку та конструкції (Attack Pattern, Indicator, Malware, Threat Actor тощо); кіберспостережуваними об'єктами (STIX Cyber-observable Objects, SCO), які фіксують спостережувані факти про стан мережі або хоста (IPv4-Address, Domain Name, File, URL тощо) й можуть пов'язуватися з SDO; та об'єктами зв'язків (STIX Relationship Objects, SRO), які визначають відносини між SDO та SCO для формування цілісного розуміння ландшафту загроз.

У версії STIX 2.1 було впроваджено тип об'єкта Extension Definition, що дає змогу створювати формально визначені розширення: додавати нові властивості до будь-яких наявних об'єктів STIX (SDO, SCO, SRO) або визначати абсолютно нові типи об'єктів [3]. Практичним прикладом використання механізму розширень є онтологія Grid-STIX, яка адаптує стандарт під специфічні сутності кіберфізичних систем в енергетиці та середовищ операційних технологій (OT) [4]. Іншим вектором розвитку є впровадження сценаріїв реагування CACAO в об'єкти Course of Action SDO [5]. Обидва підходи доводять, що STIX 2.1 здатний інкапсулювати як складні галузеві структури даних, так і алгоритми реагування завдяки використанню механізму розширень. Проте досі цей механізм не використовувався для формалізації параметрів динамічного часового згасання IoC безпосередньо в структурі об'єкта Indicator SDO.

Сучасні платформи вирішують проблему старіння індикаторів за допомогою власних моделей згасання: MISP використовує гнучку модель оцінювання [6], а в OpenCTI правила згасання з'явилися у версії 6.x [7]. Обидва підходи мають спільне структурне обмеження: логіка згасання належить виключно рівню бази даних конкретної платформи та вилучається під час експорту об'єктів. Коли пакет даних (STIX Bundle) передається до SIEM за допомогою протоколу TAXII 2.1, система-отримувач бачить лише статичне значення рівня довіри (confidence), зафіксоване на момент експорту, не маючи жодної інформації про майбутню траєкторію згасання індикатора.

Аналіз останніх досліджень і публікацій. Фундаментальним дослідженням у сфері старіння індикаторів є робота [6], у якій формалізовано загальну модель оцінювання для згасання IoC у межах платформи MISP. Їхня архітектура визначає події спостереження (sighting) як основний сигнал для оновлення оцінки і впроваджує принцип, згідно з яким параметри згасання мають налаштовуватися окремо для кожного типу індикатора, а не глобально. Основним обмеженням є прив'язка до конкретної платформи: модель функціонує на рівні платформи MISP і не серіалізується в експортований формат даних, замість цього надається статичне значення рівня довіри (confidence) або заповнюються лише поля «valid_from» та «valid_until».

У роботі [8] було проведено першу емпіричну оцінку порогів часу життя (TTL) на основі аналізу реального мережевого трафіку за понад рік. У роботі визначено оптимальні з погляду витрат пороги TTL шляхом мінімізації суми витрат на пропуск загроз та витрат на моніторинг. Їхні висновки – зокрема те, що IoC на базі IP-адрес потребують значно менших значень TTL через свою ефемерну природу, тоді як хеші файлів можуть зберігати актуальність місяцями – є емпіричною основою для визначення значень коефіцієнту згасання λ. Проте автори не запропонували механізму для кодування цих значень TTL у транспортний формат даних CTI.

Часова динаміка швидкості публікації IoC, задокументована у роботі [9], показує, що нові IoC, пов'язані з певною вразливістю, описуються епідеміологічною кривою: низька інтенсивність на етапі первинного оприлюднення, різкий пік і тривалий спад. Цей висновок обґрунтовує впровадження контекстно-залежного коригувального коефіцієнта у формулу λ.

У роботі [10] запропонували першу систему оцінювання критичності та довіри до IoC, що інтегрована в структуру графа STIX. Вона розкладає якість індикатора на п'ять вимірів: точність, повноту, релевантність, своєчасність та узгодженість. Їхня реалізація дозволила знизити середню дисперсію оцінки довіри на 25.18% порівняно з базовою лінією OpenCTI. Попри впровадження багатовимірного оцінювання, у цій роботі немає методології визначення початкової ваги W_0 як функції від типу індикатора, а компонент згасання реалізовано неявно.

Концептуальна модель Піраміди болю (Pyramid of Pain, PoP) [11] – хоча спочатку створювалася як модель оцінки витрат супротивника на зміну своєї інфраструктури, а не як інструмент оцінювання IoC – пропонує логічну ієрархію для диференціації початкової релевантності індикаторів. Елементи TTP (тактики, техніки та процедури) на вершині піраміди супротивнику вкрай складно та дорого змінювати після виявлення; IP-адреси на базі піраміди змінюються тривіально. Ця ієрархія взята за основу для розрахунку базової ваги.

У роботі [5] продемонстровано, що об'єкти Extension Definition у STIX 2.1 здатні нести виконувану логіку (зокрема, сценарії реагування на інциденти стандарту CACAO) шляхом розширення об'єкта Course of Action SDO. Їхня робота заклала шаблон проектування з використанням вкладених розширень властивостей (property extensions) замість розширень верхнього рівня для збереження семантичної цілісності. Онтологія Grid-STIX [4] розширює STIX 2.1 для кіберфізичних середовищ, підтверджуючи можливість успішної валідації специфічних для предметної області розширень схем без порушення базової сумісності зі стандартом.

У роботі [12] пропонують метод автоматизованої динамічної оцінки якості джерел CTI, оцінюючи довіру до джерела через показники його оригінальності та крос-джерельної кореляції. Їхня модель передає оцінку джерела у формулу перезважування для визначення загальної якості, однак ця логіка не інтегрована безпосередньо в об'єкт STIX. Крім того, у поширених практиках оцінювання CTI, зокрема при використанні адміралтейської шкали в MISP [13], показники довіри або репутації джерела зазвичай застосовуються для визначення достовірності індикатора та формування його початкової оцінки. Водночас у проаналізованих роботах та платформах не виявлено підходів, у яких репутація джерела безпосередньо впливає на швидкість часового згасання індикатора.

Процес передачі CTI через конвеєр STIX/TAXII для збагачення SIEM детально описано в багатьох операційних посібниках. Базовий шаблон – коли платформа розвідки загроз (Threat Intelligence Platform, TIP) публікує STIX-пакети в колекцію TAXII 2.1, а SIEM періодично опитує її та звіряє події безпеки з імпортованими індикаторами – підтримується в таких комерційних системах, як ArcSight, Splunk Enterprise Security, IBM QRadar [14], а також нативно в Elastic Security [15]. Головна проблема полягає в тому, що всі ці інтеграції розглядають індикатор STIX як статичний запис на момент імпорту, повністю ігноруючи будь-який динамічний контекст його життєвого циклу [14].

На основі огляду пов’язаних робіт, можна зробити висновок, що жодне з існуючих досліджень не формалізує параметри часового згасання, методологію розрахунку специфічного для типу індикатора W_0, адаптивний коефіцієнт згасання λ з урахуванням довіри до джерела та коригування через OSINT-збагачення в межах єдиного портативного розширення STIX 2.1 із можливістю валідації схеми під час передачі між платформами.

Мета статті. Метою статті є розробка моделі динамічного оцінювання IoC на основі часового згасання з інтеграцією в стандарт STIX 2.1, яка дозволяє вирішити проблему втрати контексту життєвого циклу IoC у гетерогенних середовищах обміну CTI.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Нехай $I = \{i_1, i_2, i_3, \dots i_n\}$ – множина гетерогенних IoC, де кожен індикатор i_k характеризується типом $T_k \in \{IP, Domain, URL, Hash, NetworkArtefact, Tool,\ TTP\}$, часом створення $t_{0,k}$ та множиною джерел $S_k = \{s_1, s_2, \dots, s_m\}$ із відповідними оцінками репутації $r_j \in [0, 1]$. Актуальність індикатора i_k у момент часу t є оцінкою $W_k(t) \in [0, 1]$, яка кількісно визначає ймовірність того, що цей індикатор усе ще пов'язаний з активною шкідливою діяльністю. Надалі для стислості позначення $W_k(t)$ буде записуватись як $W(t)$, оскільки вимоги формулюються для довільного індикатора i_k.

Система має відповідати трьом ключовим вимогам:

1. Диференціація. Значення $W(t)$ має зменшуватися зі швидкістю, що відображає характерну динаміку змін актуальності для конкретного типу індикатора. Динамічно змінювана IP-адреса повинна втрачати актуальність швидше, ніж хеш файлу;

2. Портативність. Параметри, що визначають траєкторію $W(t)$, мають передаватися разом з індикатором у машиночитаному форматі з підтримкою валідації схеми, незалежно від інфраструктури початкової платформи;

3. Адаптивність. Оцінка $W(t)$ повинна реагувати на нову інформацію – спостереження (sightings) та події OSINT-збагачення – без необхідності централізованого втручання в базу даних на стороні системи-отримувача.

Сучасний стан практики не задовольняє всі три вимоги одночасно. MISP та OpenCTI задовольняють вимогу (1), але не задовольняють вимоги (2) або (3). Базовий стандарт STIX 2.1 задовольняє вимогу (2), але не підтримує вимоги (1) або (3). Таким чином, виникає задача побудови моделі оцінювання, яка покликана одночасно забезпечити диференціацію, портативність та адаптивність.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

1. Комбінована формула запропонованої моделі.

1.1 Структура комбінованої формули.

Динамічне оцінювання індикатора *i* на основі часового згасання (Temporal Decay Dynamic Scoring, TDDS) в момент часу *t* визначається як:

$$W(t) = W_0 \cdot e^{-\lambda \cdot g(t,N_{sight})} + \sum_h E_h \cdot e^{-\mu \cdot (t-t_h)}, \quad (1)$$

де: W_0 – початкова оцінка актуальності індикатора; λ – адаптивний коефіцієнт згасання; $g(t, N_{sight})$ – функція часу, скоригована на кількість спостережень; E_h – коригування OSINT-збагачення в моменті події t_h; μ – швидкість згасання впливу OSINT-збагачення.

1.2 Початкова оцінка актуальності.

Початкова оцінка актуальності W_0 визначається як:

$$W_0 = w_{type} \cdot r_{src} \cdot c_{corr}, \quad (2)$$

де: w_{type} – базова вага за типом індикатора; r_{src} – агрегована репутація джерела; c_{corr} – коефіцієнт багатоджерельного підтвердження.

Базова вага за типом індикатора w_{type} базується на концепції Піраміди болю [11] та відображає складність заміни індикатора для супротивника.

Агрегована репутація джерела, що є операціоналізацією поняття довіра до джерела, обчислюється як зважене середнє:

$$r_{src} = \frac{\sum_j (w_j \cdot r_j)}{\sum_j w_j}, \quad (3)$$

де: $r_j \in [0, 1]$ – репутація джерела; w_j – нормована вага відповідного джерела.

Для оцінювання r_j можуть використовуватися наявні механізми довіри платформ кіберрозвідки, зокрема репутаційні оцінки спільноти, історична точність джерела або шкали достовірності інформації.

Коефіцієнт багатоджерельного підтвердження визначається як:

$$c_{corr} = 1 + \alpha \cdot \ln(1 + M), \quad (4)$$

де: M – кількість незалежних підтверджень індикатора; α – коефіцієнт чутливості до додаткових підтверджень.

Логарифмічна форма функції забезпечує ефект насичення: кожне нове незалежне підтвердження підвищує довіру до індикатора, однак величина приросту поступово зменшується. Це знижує ризик штучного завищення оцінки внаслідок багаторазового дублювання однакової інформації у різних відкритих джерелах.

1.3 Адаптивний коефіцієнт згасання.

Адаптивний коефіцієнт згасання λ визначає швидкість, з якою зменшується актуальність індикатора. Розширюючи класичну залежність періоду напіврозпаду з роботи [6], λ визначається як добуток трьох компонентів:

$$\lambda = \lambda_{base} \cdot f_{trust} \cdot f_{camp}, \quad (5)$$

де: λ_{base} – базова швидкість згасання, отримана на основі характерного періоду напіврозпаду для відповідного типу індикатора, який задається політикою організації або параметрами конкретної реалізації моделі; f_{trust} – коефіцієнт масштабування швидкості згасання, похідний від репутації джерела; f_{camp} – коефіцієнт контексту кампанії.

Базова швидкість згасання λ_{base} визначається через характерний період напіврозпаду для відповідного типу індикатора:

$$\lambda_{base} = \frac{\ln(2)}{t_{1/2}(T_k)}, \quad (6)$$

де: $t_{1/2}(T_k)$ – характерний період напіврозпаду для індикатора типу T_k.

Вплив репутації джерела на швидкість згасання визначається за допомогою коефіцієнта f_{trust}:

$$f_{trust} = \frac{1}{0.5 + r_{src}}, \quad (7)$$

де: r_{src} – агрегована репутація джерела, визначена за формулою (3).

Висока репутація джерела уповільнює згасання індикатора. Якщо $r_{src} = 1.0$ (абсолютно надійне джерело), то $f_{trust} = 0.67$ – індикатор згасає зі швидкістю, що становить 67% від базової. Якщо $r_{src} = 0.0$ (абсолютно ненадійне джерело), $f_{trust} = 2.0$ – індикатор згасає вдвічі швидше. Така залежність відображає якісні рекомендації з роботи [12] щодо врахування довіри до джерела і практичну логіку: дані, отримані з верифікованих закритих спільнот обміну інформацією про загрози, мають залишатися актуальними довше, ніж анонімні публікації на OSINT-ресурсах.

Виходячи зі спостережуваної епідеміологічної динаміки публікації IoC, описаної в роботі [9], у запропонованій моделі припускається, що стадія розвитку кампанії може впливати на швидкість втрати актуальності індикатора. Для формалізації цього припущення вводиться логістична функція:

$$f_{camp} = \frac{1}{1+e^{-\nu(\tau-\tau_{mean})}}, \tag{8}$$

де: τ – параметр, який характеризує поточне положення індикатора на часовій шкалі кампанії; τ_{mean} – центр розподілу публікацій IoC; ν – параметр, який визначає крутизну логістичної кривої. У межах запропонованої моделі менші значення f_{camp} відповідають повільнішому згасанню актуальності, тоді як значення, близькі до 1, наближають швидкість згасання до базового рівня. За відсутності метаданих про кампанію приймається $f_{camp} = 1.0$.

1.4 Функція сповільнення згасання на основі спостережень.

Факт спостереження індикатора (sighting) – підтверджена фіксація активності IoC у реальному мережевому трафіку – є найсильнішим сигналом його актуальності. Спеціальна функція стискає ефективний час, що минув, за наявності нових спостережень:

$$g(t, N_{sight}) = t \cdot (1 - \beta \cdot \ln(1 + N_{sight})), \tag{9}$$

де: N_{sight} – кількість підтверджених спостережень індикатора; β – параметр чутливості моделі до нових спостережень.

При фіксованому значенні β збільшення кількості спостережень зменшує ефективний час $g(t, N_{sight})$, що призводить до повільнішого згасання оцінки актуальності. Параметр β обирається таким чином, щоб виконувалась умова $1 - \beta \cdot \ln(1 + N_{sight}) \geq 0$, яка гарантує невід'ємність функції $g(t, N_{sight})$. За цієї умови функція не відновлює оцінку актуальності та не допускає її неконтрольованого зростання вище початкової оцінки W_0, а лише сповільнює її згасання.

1.5 Коригування через OSINT-збагачення.

Події OSINT-збагачення виникають у випадках отримання нової інформації щодо індикатора з зовнішніх джерел кіберрозвідки. Такі події можуть як підтверджувати актуальність індикатора, так і знижувати рівень довіри до нього. Коригування, пов'язане з подією збагачення у момент часу t_h, визначається як:

$$E_h = \varepsilon \cdot v_h \cdot c_h, \tag{10}$$

де: $v_h \in \{-1, +1\}$ – знак коригування; $c_h \in [0,1]$ – оцінка довіри до результату збагачення; ε – параметр, що визначає максимальну силу впливу події збагачення.

Отримане коригування враховується у формулі (1) через суму доданків $E_h \cdot e^{-\mu \cdot (t-t_h)}$, де параметр μ визначає швидкість поступового зменшення впливу події збагачення з часом. Такий підхід забезпечує більший вплив нових відомостей порівняно із застарілими та запобігає довготривалому домінуванню окремих подій збагачення в оцінці актуальності індикатора.

2. Визначення розширення STIX 2.1.

2.1 Схема розширення.

Для забезпечення портативності запропонованої моделі параметри оцінювання актуальності індикаторів передаються разом з об'єктом Indicator SDO за допомогою механізму Extension Definition стандарту STIX 2.1. Тип розширення визначається як property-extension та застосовується безпосередньо до об'єкта Indicator. Такий підхід відповідає рекомендаціям специфікації STIX 2.1 та забезпечує сумісність із наявними реалізаціями платформ розвідки загроз (Threat Intelligence Platform, TIP).

Запропонована модель передбачає логічне розділення обчислень між TIP та системою-отримувачем. Платформа TIP або пов'язаний з нею модуль обчислення параметрів виконує розрахунок значень W_0 та λ відповідно до формул (2)-(8), після чого результати серіалізуються у вигляді розширення STIX 2.1. Система-отримувач використовує передані параметри для локального обчислення поточної

оцінки актуальності індикатора без необхідності звернення до внутрішньої бази даних платформи-відправника.

Мінімальний набір властивостей розширення включає:

- w0 – початкова оцінка актуальності індикатора;
- lambda – адаптивний коефіцієнт згасання λ;
- last_recalculated – мітка часу останнього розрахунку оцінки;
- current_score – значення $W(t)$ на момент last_recalculated;

Для підтримки адаптивних механізмів моделі можуть додатково передаватися:

- sightings – кількість спостережень N_{sight};
- enrichment_events – масив об'єктів подій OSINT-збагачення, кожен з яких містить інформацію про джерело (source), час отримання (timestamp), вердикт (verdict) та рівень довіри до результату збагачення (confidence).

Параметри β, μ та ε розглядаються як параметри реалізації моделі та визначаються специфікацією розширення. Їх значення не залежать від конкретного індикатора, тому вони не передаються всередині кожного об'єкта STIX 2.1.

Компонент контексту кампанії f_{camp}, визначений формулою (8), є необов'язковим розширенням моделі. За наявності відповідних метаданих він може бути розрахований на стороні платформи TIP та врахований під час формування коефіцієнта λ. За відсутності таких даних приймається $f_{camp} = 1.0$, що не впливає на базову працездатність моделі.

Поле sightings містить агреговане значення N_{sight} розраховане на стороні TIP на основі одного або декількох об'єктів Sighting SRO. Його передача у складі розширення дозволяє системі-отримувачу виконувати обчислення без необхідності отримання та обробки всіх пов'язаних об'єктів Sighting.

Таким чином, усі параметри, необхідні для подальшого обчислення актуальності індикатора, передаються разом із самим об'єктом STIX 2.1, що забезпечує виконання вимоги портативності.

2.2 Приклад доповненого об’єкта індикатора.

Для демонстрації способу інтеграції параметрів моделі до стандарту STIX 2.1 наведено фрагмент схеми JSON відповідно до об'єкта Indicator SDO із застосуванням розширення. Основу прикладу становить структура об'єкта Indicator, наведена у специфікації OASIS STIX 2.1 [3], яка була доповнена полями, необхідними для передачі параметрів запропонованої моделі.

Конкретні значення параметрів W_0, λ та подій збагачення визначаються відповідно до вхідних даних, політик організації та особливостей конкретної реалізації моделі. Позначення у квадратних дужках ([...]) використовуються як заповнювачі значень і мають бути замінені фактичними даними під час формування STIX-об'єкта. Наприклад, [extension-id] позначає ідентифікатор об'єкта Extension Definition, який має бути визначений відповідно до специфікації STIX 2.1 [3] та пов'язаний із запропонованим розширенням.

```
{
"type": "indicator",
"spec_version": "2.1",
"id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
"created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
"created": "2016-04-06T20:03:48.000Z",
"modified": "2016-04-06T20:03:48.000Z",
"indicator_types": ["malicious-activity"],
"name": "Poison Ivy Malware",
"description": "This file is part of Poison Ivy",
"pattern": "[ file:hashes.'SHA-256' =
'4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877' ]",
"pattern_type": "stix",
"valid_from": "2016-01-01T00:00:00Z",
"extensions": {
  "extension-definition--[extension-id]": {
      "extension_type": "property-extension",
      "w0": [w0_value],
      "lambda":[lambda_value],
      "current_score": [current_score_value],
      "last_recalculated": "[last_recalculated_value]",
      "sightings": [sightings_value],
      "enrichment_events": [
        {
```

```
            "source": "[source_value]",
            "timestamp": "[timestamp_value]",
            "verdict": "[verdict_value]",
            "confidence": [confidence_value]
          }
        ]
      }
    }
  }
```

3. Теоретичний аналіз поведінки моделі.

Виконання вимоги диференціації. Оскільки базова швидкість згасання визначається у формулі (6), модель забезпечує різну швидкість втрати актуальності для різних типів індикаторів. Менші значення $t_{1/2}$ призводять до швидшого згасання оцінки актуальності, тоді як більші значення забезпечують її довготривале збереження. Таким чином виконується вимога диференціації.

Виконання вимоги портативності. Усі параметри, необхідні для подальшого обчислення актуальності індикатора, передаються разом із об'єктом STIX 2.1 через механізм Extension Definition. Система-отримувач не потребує доступу до внутрішньої бази даних платформи-відправника для подальшого оцінювання актуальності індикатора.

Виконання вимоги адаптивності. Функція $g(t, N_{sight})$, яка визначається за формулою (9), забезпечує врахування нових спостережень, а компонент E_h, який визначається за формулою (10), дозволяє враховувати результати OSINT-збагачення. Унаслідок цього оцінка актуальності індикатора може адаптуватися до нової інформації без зміни базової структури моделі.

Ефективність моделі залежить від коректності вибору параметрів w_{type}, $t_{1/2}(T_k)$, α, β, μ, ε та, за використання контексту кампанії, параметрів v і τ_{mean}. Крім того, результати оцінювання залежать від якості вхідних даних, зокрема репутаційних оцінок джерел r_j, їх ваг w_j та кількості незалежних підтверджень M. Оптимальні значення цих параметрів потребують окремої емпіричної валідації на репрезентативних наборах даних CTI.

4. Архітектура інтеграції

Запропонована модель не потребує внесення змін до специфікації STIX 2.1, оскільки використовує стандартний механізм Extension Definition для розширення об'єкта Indicator додатковими властивостями. Для демонстрації можливого способу практичного використання моделі пропонується концептуальна трирівнева архітектура, яка складається з TIP, модуля оцінювання актуальності індикаторів (TDDS Engine) та системи SIEM.

Запропонована архітектура має концептуальний характер і призначена для демонстрації можливого розподілу функцій між компонентами системи відповідно до запропонованої математичної моделі. Загальну структуру взаємодії компонентів наведено на рисунку 1.

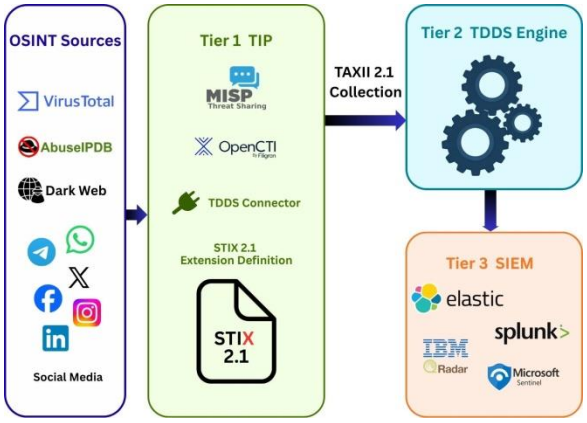

Рис. 1. Концептуальна архітектура інтеграції моделі TDDS

Рівень 1 – TIP. TIP виконує функції збору, нормалізації та поширення CTI. У межах запропонованої моделі передбачається використання додаткового програмного компонента (TDDS Connector), який може бути реалізований у вигляді плагіна або зовнішнього сервісу, інтегрованого з платформою.

Основним завданням цього компонента є обчислення параметрів моделі згідно з формулами, наведеними вище. Зокрема, на стороні TIP можуть визначатися:

- початкова оцінка актуальності W_0 за формулою (2);
- агрегована репутація джерела r_{src} за формулою (3);
- коефіцієнт багатоджерельного підтвердження c_{corr} за формулою (4);
- базова швидкість згасання λ_{base} за формулою (6);
- коефіцієнт масштабування швидкості згасання f_{trust} за формулою (7);
- коефіцієнт контексту кампанії f_{camp} за формулою (8).

Після обчислення параметрів результати серіалізуються у розширення STIX та публікуються разом з об'єктом Indicator через TAXII.

Рівень 2 – TDDS Engine. TDDS Engine є логічним компонентом, відповідальним за реалізацію математичної моделі згасання. На відміну від TIP, цей модуль не потребує доступу до історичних даних платформи-відправника. Для оцінювання актуальності індикатора використовуються лише параметри, передані всередині STIX-об'єкта.

Функції модуля включають:

- обчислення поточної оцінки актуальності $W(t)$ за формулою (1);
- врахування впливу повторних спостережень $g(t, N_{sight})$ за формулою (9);
- врахування результатів OSINT-збагачення E_h за формулою (10);
- формування актуальної оцінки індикатора для подальшого використання системою-отримувачем.

Рівень 3 – SIEM. Система SIEM виконує традиційні функції збору подій безпеки, кореляції та виявлення загроз. У межах запропонованої архітектури SIEM не виконує розрахунок параметрів моделі та не потребує доступу до внутрішньої бази даних TIP. Вона використовує результати роботи TDDS Engine як додатковий контекст під час обробки IoC. Такий підхід дозволяє уникнути жорсткої залежності між платформою-відправником та системою-отримувачем і забезпечує перенесення логіки життєвого циклу індикатора разом із самим об'єктом STIX.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі запропоновано формалізовану модель динамічного оцінювання IoC на основі часового згасання, орієнтовану на використання в екосистемі стандартів STIX 2.1 та TAXII 2.1. На відміну від підходів, що використовують фіксовані часові пороги або однакові параметри згасання для всіх категорій індикаторів, запропонована модель враховує тип індикатора, рівень довіри до джерела, повторні спостереження та результати OSINT-збагачення.

Основним результатом дослідження є математична формалізація процесу оцінювання актуальності IoC. Побудована модель об'єднує початкову оцінку актуальності W_0, адаптивний коефіцієнт згасання λ, функцію сповільнення згасання на основі спостережень, коригування через OSINT-збагачення та механізм інтеграції результатів в єдину систему оцінювання життєвого циклу IoC.

У роботі також запропоновано спосіб серіалізації параметрів моделі за допомогою механізму Extension Definition стандарту STIX 2.1. Такий підхід дозволяє передавати параметри оцінювання разом із самим об'єктом Indicator SDO та усуває залежність системи-отримувача від внутрішньої бази даних платформи-відправника. У результаті забезпечується виконання вимоги портативності моделі та можливість її використання в гетерогенних середовищах обміну CTI.

Запропонована архітектура інтеграції демонструє один із можливих способів практичного використання моделі TDDS у середовищах обміну CTI. Теоретично вона забезпечує виконання сформульованої вимоги портативності, оскільки всі параметри, необхідні для подальшого оцінювання актуальності індикатора, передаються всередині STIX-об'єкта та не потребують

звернення до внутрішньої інфраструктури платформи-відправника. Водночас низка питань залишається відкритою та потребує подальших досліджень.

Подальші дослідження будуть спрямовані на експериментальну перевірку запропонованої моделі на реальних наборах даних CTI та визначення оптимальних значень її параметрів. Таке дослідження має встановити вплив моделі на покращення якості детектування порівняно із статичними підходами. Окремим напрямом є дослідження механізму врахування контексту кампаній. У роботі запропоновано математичну основу для врахування часового положення індикатора відносно життєвого циклу кампанії. Подальші дослідження мають визначити можливість автоматичного вилучення таких параметрів із даних CTI. Крім того, перспективним напрямом є розроблення еталонної реалізації TDDS Connector для платформ MISP та OpenCTI. Така реалізація дозволить перевірити практичну застосовність запропонованого розширення STIX 2.1, оцінити накладні витрати на обробку даних та сформувати рекомендації щодо інтеграції моделі до існуючих платформ обміну CTI.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IBM Security. (2025). *Cost of a data breach report 2025*. IBM. https://www.ibm.com/reports/data-breach
2. Crowley, C. (2025). *SANS 2025 SOC survey*. SANS Institute. https://www.sans.org/white-papers/sans-2025-soc-survey
3. OASIS Cyber Threat Intelligence Technical Committee. (2021). *STIX™ Version 2.1*. OASIS Open. https://www.oasis-open.org/standard/stix-version-2-1/
4. Blakely, B., & Karcz, D. (2025). *Grid-STIX: A STIX 2.1-compliant cyber-physical security ontology for power grid* (arXiv:2511.11366). arXiv. https://doi.org/10.48550/arXiv.2511.11366
5. Mavroeidis, V., & Zych, M. (2022). *Cybersecurity playbook sharing with STIX 2.1* (arXiv:2203.04136). arXiv. https://doi.org/10.48550/arXiv.2203.04136
6. Iklody, A., Wagener, G., Dulaunoy, A., Mokaddem, S., & Wagner, C. (2018). *Decaying indicators of compromise* (arXiv:1803.11052). arXiv. https://doi.org/10.48550/arXiv.1803.11052
7. Jard, A., & Hadjiat, S. (2024). *Introducing decay rules implementation for indicators in OpenCTI*. Filigran Blog. https://filigran.io/blog/introducing-decay-rules-implementation-for-indicators-in-opencti/
8. Tostes, B., Ventura, L., Lovat, E., Martins, M., & Menasché, D. S. (2023). *Learning when to say goodbye: What should be the shelf life of an indicator of compromise?* (arXiv:2307.16852). arXiv. https://doi.org/10.48550/arXiv.2307.16852
9. Kodituwakku, A., Xu, C., Rogers, D., Ahn, D. K., & Fulp, E. W. (2024). *Investigating the temporal dynamics of cyber threat intelligence* (arXiv:2412.19086). arXiv. https://doi.org/10.48550/arXiv.2412.19086
10. Chen, S.-S., Hwang, R.-H., Ali, A., Lin, Y.-D., Wei, Y.-C., & Pai, T.-W. (2024). Improving quality of indicators of compromise using STIX graphs. *Computers & Security*, Article 103972. https://doi.org/10.1016/j.cose.2024.103972
11. Bianco, D. J. (2013). *The Pyramid of Pain*. Enterprise Detection & Response. https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
12. Yang, L., Wang, M., & Lou, W. (2024). An automated dynamic quality assessment method for cyber threat intelligence. *Computers & Security*, Article 104079. https://doi.org/10.1016/j.cose.2024.104079
13. MISP Project. (2019). *Best practices in threat intelligence*. https://www.misp-project.org/best-practices-in-threat-intelligence.html
14. Siam, A. A., Hassan, M. M., Masum, A. K. M., & Bhuiyan, T. (2025). Automating malware detection and response via real-time threat feed integration with Wazuh SIEM. In *Proceedings of the IEEE Conference* (IEEE Xplore). https://ieeexplore.ieee.org/document/11381876/
15. Elastic. (2024). *Elastic's new custom threat intelligence integration*. Elastic Blog. https://www.elastic.co/blog/custom-threat-intelligence-integration

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Milan Hordiienko
PhD student of the Department of Information Security
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID:0009-0004-2226-2391
hordienko.m.p.-fb51f@edu.kpi.ua

TEMPORAL DECAY DYNAMIC SCORING MODEL FOR INDICATORS OF COMPROMISE VIA STIX 2.1 EXTENSION

Abstract. This article proposes a temporal decay dynamic scoring model (TDDS) for indicators of compromise (IoC), formalized as an extension of the STIX 2.1 standard using the Extension Definition mechanism. The model is based on a composite mathematical formula that combines four components: an initial relevance score, determined by the indicator type according to the Pyramid of Pain (PoP) hierarchy, source reputation, and the degree of corroboration; an adaptive decay coefficient, which depends on the characteristic half-life for the respective indicator type, a scaling factor derived from the source reputation, and the campaign context; a sighting-based decay-slowing function; and an enrichment adjustment term derived from Open-Source Intelligence (OSINT) data. Using the STIX 2.1 extension mechanism, the paper formalizes a data structure that enables the transfer of TDDS model parameters between cyber threat intelligence (CTI) systems. Unlike existing implementations such as MISP and OpenCTI, where decay-related parameters remain part of the platform's internal logic and are not preserved during export, the proposed approach encapsulates computed model parameters and intermediate calculation results directly within the STIX 2.1 object structure. This enables autonomous IoC relevance evaluation by receiving systems without dependence on the infrastructure of the originating platform.

Keywords: STIX 2.1; CTI; IoC; SIEM; dynamic scoring; temporal decay; source reputation; OSINT enrichment; CTI lifecycle.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. IBM Security. (2025). *Cost of a data breach report 2025*. IBM. https://www.ibm.com/reports/data-breach
2. Crowley, C. (2025). *SANS 2025 SOC survey*. SANS Institute. https://www.sans.org/white-papers/sans-2025-soc-survey
3. OASIS Cyber Threat Intelligence Technical Committee. (2021). *STIX™ Version 2.1*. OASIS Open. https://www.oasis-open.org/standard/stix-version-2-1/
4. Blakely, B., & Karcz, D. (2025). *Grid-STIX: A STIX 2.1-compliant cyber-physical security ontology for power grid* (arXiv:2511.11366). arXiv. https://doi.org/10.48550/arXiv.2511.11366
5. Mavroeidis, V., & Zych, M. (2022). *Cybersecurity playbook sharing with STIX 2.1* (arXiv:2203.04136). arXiv. https://doi.org/10.48550/arXiv.2203.04136
6. Iklody, A., Wagener, G., Dulaunoy, A., Mokaddem, S., & Wagner, C. (2018). *Decaying indicators of compromise* (arXiv:1803.11052). arXiv. https://doi.org/10.48550/arXiv.1803.11052
7. Jard, A., & Hadjiat, S. (2024). *Introducing decay rules implementation for indicators in OpenCTI*. Filigran Blog. https://filigran.io/blog/introducing-decay-rules-implementation-for-indicators-in-opencti/
8. Tostes, B., Ventura, L., Lovat, E., Martins, M., & Menasché, D. S. (2023). *Learning when to say goodbye: What should be the shelf life of an indicator of compromise?* (arXiv:2307.16852). arXiv. https://doi.org/10.48550/arXiv.2307.16852
9. Kodituwakku, A., Xu, C., Rogers, D., Ahn, D. K., & Fulp, E. W. (2024). *Investigating the temporal dynamics of cyber threat intelligence* (arXiv:2412.19086). arXiv. https://doi.org/10.48550/arXiv.2412.19086
10. Chen, S.-S., Hwang, R.-H., Ali, A., Lin, Y.-D., Wei, Y.-C., & Pai, T.-W. (2024). Improving quality of indicators of compromise using STIX graphs. *Computers & Security*, Article 103972. https://doi.org/10.1016/j.cose.2024.103972
11. Bianco, D. J. (2013). *The Pyramid of Pain*. Enterprise Detection & Response. https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
12. Yang, L., Wang, M., & Lou, W. (2024). An automated dynamic quality assessment method for cyber threat intelligence. *Computers & Security*, Article 104079. https://doi.org/10.1016/j.cose.2024.104079

13. MISP Project. (2019). *Best practices in threat intelligence*. https://www.misp-project.org/best-practices-in-threat-intelligence.html
14. Siam, A. A., Hassan, M. M., Masum, A. K. M., & Bhuiyan, T. (2025). Automating malware detection and response via real-time threat feed integration with Wazuh SIEM. In *Proceedings of the IEEE Conference* (IEEE Xplore). https://ieeexplore.ieee.org/document/11381876/
15. Elastic. (2024). *Elastic's new custom threat intelligence integration*. Elastic Blog. https://www.elastic.co/blog/custom-threat-intelligence-integration

Отримано редакцією журналу / Received: 22.01.26
Прорецензовано / Revised: 05.02.26
Схвалено до друку / Accepted: 24.09.26