УДК 004.056
DOI: 10.31673/2409-7292.2021.031216

Дорохін О.О., Марченко В.В., Семенова І.Д.

ТЕХНОЛОГІЯ THREAT INTELLIGENCE ТА МЕТОДИ ЇЇ ВИКОРИСТАННЯ ДЛЯ ЗАХИСТУ КОМПАНІЇ ВІД КІБЕРЗАГРОЗ

Статтю присвячено розгляду методів застосування технології Threat Intelligence («розвідка загроз» або «кіберрозвідка» в перекладі з англійської) у компаніях що потребують побудови захищеної IT-інфраструктури та механізмів протидії загрозам інформаційній безпеці за допомогою даної технології. Досліджено питання цінності Threat Intelligence на фоні існуючих кіберзагроз. Описано шляхи впровадження технології Threat Intelligence. Поетапно описаний процес роботи з Threat Intelligence, дані рекомендації з отримання максимальної користі від кіберрозвідки .

Ключові слова: Threat Intelligence, SOC, моніторинг, кіберрозвідка, загрози інформаційній безпеці, кіберзагрози, індикатори компрометації, OWASP Top-10.

Вступ

Наразі кіберпростір охоплює найвіддаленіші куточки світу, а там де проводовий Інтернет недосяжний популярністю користуються смартфони з мобільним Інтернет працюючим по технологіям зв'язку GSM, CDMA, UMTS, WiMAX, взятих за основу в EDGE, 3G, LTE та багато інших [1]. Так чи інакше кількість Інтернет трафіку стрімко зростає, як і кількість веб-сайтів, платформ потокового аудіо- та відео-контенту. Для бізнесу важливо бути представленим в кіберпросторі щоб залучати більше чи навіть всю аудиторію користувачів та покупців товарів та сервісів. В такому світі відстеження загроз кібербезпеці перетворюється на один із важливих процесів забезпечення ефективного захисту бізнесу.

Постановка проблеми

Потреба розвідувальних даних виникла не відразу. Довгий час галузь інформаційної безпеки реагувала реактивно на дії зловмисників. Але при сучасних технологіях і стрімкій швидкості кібератак виникає гостра потреба передбачати атаки і розпізнавати їх за ранніми ознаками. Threat Intelligence – одна з таких технік, що дозволяє дізнаватися про загрози до того, як вони реалізувалися та спричинили шкоду. Саме тому, створення технічних та програмних засобів для виявлення та протидії кіберзагрозам, в тому числі завдяки Threat Intelligence є надзвичайно актуальною проблемою сьогодення.

Мета дослідження: розгляд методів застосування технології Threat Intelligence у компаніях що потребують побудови захищеної IT-інфраструктури та механізмів протидії загрозам інформаційній безпеці за допомогою даної технології й опис шляхів впровадження даної технології.

Для досягнення цієї мети в роботі необхідно вирішити такі **завдання**:

1) проаналізувати методи застосування технології Threat Intelligence у компаніях що потребують побудови захищеної IT-інфраструктури та механізми протидії загрозам інформаційній безпеці за допомогою даної технології;

2) сформувати шляхів впровадження даної технології.

Аналіз списку загроз Топ-10 від OWASP

OWASP Топ-10 - це список з десяти найпоширеніших наразі вразливостей веб-додатків. Завдяки цьому списку користувачі будуть обізнані про найбільш критичні ризики та загрози, їх наслідки та заходи протидії. Оновлюється список OWASP кожні три-чотири роки. Востаннє він був випущений у 2021 році, який і буде розглянуто далі [2].

Порівняння списку OWASP Top-10 2017 та 2021 років:

A01:2021- Broken Access Control піднявся з п'ятої позиції до категорії з найсерйознішим ризиком безпеки веб-додатків; Надані дані вказують на те, що в середньому 3,81% тестованих додатків мали одну або кілька загальних перерахувань слабкості (CWE) з понад 318 тисячами випадків CWE в цій категорії ризику. 34 CWE, зіставлені з порушенням контролю доступу, мали більше випадків у додатках, ніж будь-яка інша категорія.

A02:2021- Cryptographic Failures зміщуються на одну позицію вгору до №2, раніше

відомого як A3:2017- Sensitive Data Exposure, що було скоріше поширеним симптомом, ніж першопричиною. Оновлена назва зосереджена на збоях, пов'язаних із криптографією, як це було неявно раніше. Ця категорія часто призводить до розкриття конфіденційних даних або компрометації системи.

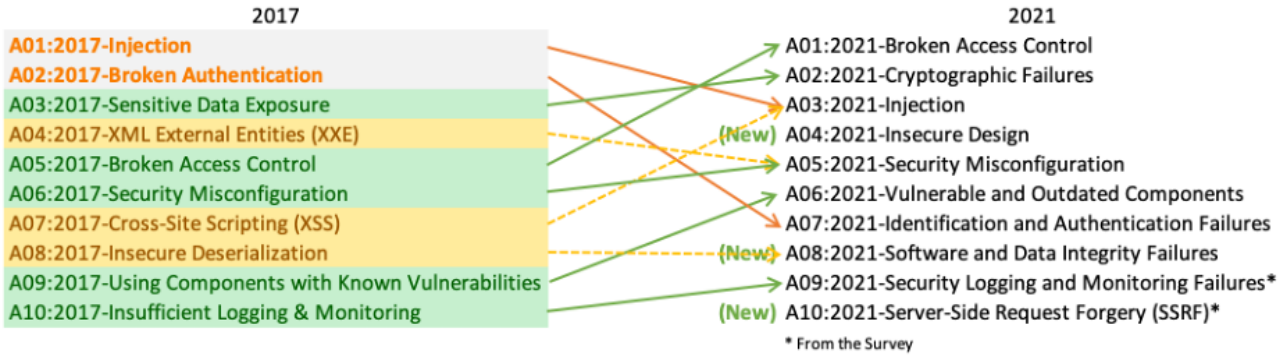

Рис. 1. Порівняння списку OWASP Top-10 2017 та 2021 років

A03:2021- Injection ковзає вниз до третьої позиції. 94% додатків були перевірені на певну форму ін'єкції з максимальним рівнем зараження 19%, середнім рівнем зараження 3,37%, а 33 CWE, віднесені до цієї категорії, займають друге місце за кількістю випадків у додатках із 274 тисячами випадків. XSS тепер є частиною цієї категорії в цьому виданні.

A04:2021- Insecure Design – це нова категорія для 2021 року, зосереджена на ризиках, пов'язаних із недоліками дизайну. Якщо ми справді хочемо «рухатися вліво» як галузь, нам потрібно більше моделювання загроз, безпечних шаблонів і принципів проектування та еталонних архітектур. Небезпечний дизайн не може бути виправлений ідеальною реалізацією, оскільки за визначенням необхідні засоби контролю безпеки ніколи не створювалися для захисту від конкретних атак.

A05:2021- Security Misconfiguration змінюється з №6 у попередньому виданні; 90% додатків були перевірені на певну форму неправильної конфігурації, із середнім рівнем зараження 4,5%, і понад 208 тисяч випадків CWE віднесено до цієї категорії ризику. Колишня категорія XXE A4:2017-XML (XXE) тепер є частиною цієї категорії ризику.

A06:2021- Vulnerable and Outdated Components категорія раніше називалася «Using Components with Known Vulnerabilities» і займала 2-е місце в опитуванні спільноти «Top-10», але також мала достатньо даних, щоб увійти до топ-10 за допомогою аналізу даних. Ця категорія піднялася з 9 у 2017 році і є відомою проблемою, яку нам важко перевірити та оцінити ризики. Це єдина категорія, яка не має жодних загальних вразливостей та ризиків (CVE), які зіставлені з включеними CWE, тому в їхні оцінки враховуються значення експлойту та впливу за замовчуванням 5,0.

A07:2021- Identification and Authentication Failures раніше були порушеною автентифікацією і сповзали з другої позиції, а тепер включають CWE, які більше пов'язані з помилками ідентифікації. Ця категорія все ще є невід'ємною частиною ТОП-10, але збільшення доступності стандартизованих фреймворків, здається, допомагає.

A08:2021- Software and Data Integrity Failures – це нова категорія для 2021 року, яка зосереджена на створенні припущень, пов'язаних із оновленнями програмного забезпечення, критично важливими даними та конвеєрами CI/CD без перевірки цілісності. Один із найбільш зважених впливів даних загальної вразливості та ризиків/системи оцінки загальної вразливості (CVE/CVSS), зіставлених з 10 CWE в цій категорії. A8:2017- Insecure Deserialization тепер є частиною цієї більшої категорії.

A09:2021- Security Logging and Monitoring Failures раніше був A10:2017-Недостатнє ведення журналу та моніторингу та додано з опитування 10 найкращих спільнот (№3), перейшовши з №10 раніше. Ця категорія розширена, щоб охопити більше типів збоїв, її складно перевірити, і вона погано представлена в даних CVE/CVSS. Однак збої в цій

категорії можуть безпосередньо вплинути на видимість, оповіщення про інциденти та криміналістичну експертизу.

A10:2021- Server-Side Request Forgery. Дані показують відносно низький рівень зараження з охопленням тестуванням вище середнього, а також вищими за середні оцінки щодо потенціалу експлуатації та впливу. Ця категорія представляє сценарій, коли члени спільноти безпеки говорять нам, що це важливо, хоча наразі це не показано в даних.

Завдання Threat Intelligence

Є безліч підходів до визначення поняття threat intelligence, причому вони змінюються з часом. Threat Intelligence являє собою знаннями про загрози, отримані в результаті аналізу та інтерпретації даних [3].

Threat Intelligence поєднує три взаємопов'язані елементи:

1) контекст
2) індикатори компрометації
3) взаємозв'язки та збагачення

Кожен елемент не несе цінності сам по собі, але в сукупності вони утворюють саме ці цінні знання.

Процес обробки Threat Intelligence (TI) починається зі збирання сирих даних – потоку інформації, яку необхідно нормалізувати, збагатити контекстом та виявити взаємозв'язки. Після цього ми отримаємо якийсь профіль або «картку» загрози, з якою згодом буде працювати аналітик і аналізувати в розрізі конкретної організації. Після аналізу контексту зловмисника та контексту компанії аналітик видасть рішення, яке вже можна назвати «знанням». Процес TI дуже схожий на класичну розвідку, в якій команда отримує завдання, збирає розвіддані, виводить їх на командира, який аналізує ризики, пов'язані з поточною ситуацією, приймає рішення та діє. Аналогічно працює кіберрозвідка. З контексту конкретної організації, необхідно зібрати дані, проаналізувати, обробити, збагатити їх. В результаті вони перетворюються на знання, які передаються директору з інформаційної безпеки (CISO) або особі, яка приймає рішення, після чого він аналізує відповідні ризики та приймає це рішення. Тому якість даних TI безпосередньо впливає швидкість і якість прийняття рішень.

Дані кіберрозвідки прийнято поділяти на три рівні (рис. 2):

1) Операційний чи технічний рівень. До нього належать індикатори компрометації, тобто ознаки, за якими можна розпізнати потенційну загрозу (наприклад, хеші шкідливих файлів, IP-адреси, домени, пов'язані зі злочинною активністю тощо) та здійснити технічні заходи щодо її блокування.

Рис. 2. Рівні Threat Intelligence

2) Тактичний рівень. На цьому рівні проводиться аналіз поведінки порушників, спираючись на інформацію про техніку, тактику та процедури зловмисника (TTP), та виробляється розуміння, хто, що і навіщо може здійснити проти організації. В результаті у неї з'являється можливість передбачати атаки та прогнозувати свою подальшу діяльність.

3) Стратегічний рівень. Сюди можна віднести аналітичні дані щодо тенденцій загроз у світі з метою вироблення подальшої стратегії розвитку системи інформаційної безпеки організації. Спираючись на інформацію з попередніх рівнів, здійснюється подання актуальних загроз та необхідних заходів перед топ-менеджментом організації, планування завдань та потреб (у нових людях, процесах, інструментах).

Робота з даними кіберрозвідки має забезпечуватись на всіх трьох рівнях. За втрати одного з них вся концепція знижує відчутну користь для організації.

Цінність Threat Intelligence

Threat Intelligence знаходиться у тісному взаємозв'язку з іншими процесами інформаційної безпеки – реагуванням на інциденти, управлінням ризиками, управлінням уразливістю, виявленням шахрайства та операційною діяльністю ІБ підрозділу. Підвищити ефективність даних процесів, якість та швидкість прийняття рішень у рамках цих процесів – це і є, по суті, головне завдання роботи з TI.

У першу чергу, використання threat intelligence в рази підвищує якість та швидкість реагування на інциденти. Коли надходить інформація про нову загрозу, можна оперативно поставити її на моніторинг, паралельно блокуючи деякі індикатори компрометації. Знаючи контекст, розуміючи, яким чином відбуватиметься кібератака, всі можливі варіанти її розвитку та яким чином ця загроза могла потрапити в інфраструктуру, можна вчасно її виявити, опрацювати в рамках конкретного інциденту, побудувати для неї відповідні сценарії реагування. У плані управління вразливістю дані про загрози допомагають у розстановці пріоритетів та визначенні критичності вразливостей. Threat intelligence дає необхідну фактуру для аналізу та оцінки ризиків - інформацію про актуальні загрози, отриману на тактичному та стратегічному рівні TI. В результаті процес ризик-менеджменту стає більш практичним та якісним. Threat intelligence дозволяє вибудовувати операційну діяльність ІБ-підрозділу, діяти проактивно, планувати, впроваджувати та реалізовувати захисні заходи, орієнтуючись на актуальний ландшафт загроз, а не наосліп.

Чому TI мало хто використовує?

Вибудовуючи процес кіберрозвідки, кожна організація стикається з певними складнощами. По-перше, дані складно отримувати. Джерел інформації кіберрозвідки безліч, при цьому немає єдиного стандарту - кожен постачальник або канал надає їх у своєму вигляді. Частина даних поставляється в машиночитаній формі, інша - у вигляді звітів, розрахованих на читання аналітиком. В результаті, перш ніж почати аналізувати дані, навіть якщо використовується лише 2-3 джерела, їх потрібно привести до єдиної моделі уявлення, нормалізувати. Для правильної інтерпретації та прийняття рішень сирих даних з джерел недостатньо, потрібно їх збагатити контекстом, додатковою інформацією, яка допоможе підібрати найбільш правильну тактику дій у відповідь. Якщо джерел занадто багато, виникає складність у їх практичному застосуванні. Потрібно проводити фільтрацію та відбір, щоб не захлинутися в потоці інформації.

Ще один важливий момент полягає в тому, що користь TI складно оцінювати, немає об'єктивних метрик. Її ефективність можна вимірювати опосередковано через підвищення ефективності тих процесів, із якими пов'язана. Тому найчастіше threat intelligence використовується в ІБ-підрозділах або SOC, які досягли певного рівня зрілості.

Як зробити TI по-справжньому робочим інструментом?

Для початку необхідно визначити мету та завдання, які планується вирішувати за допомогою TI та як оцінюватимуться результати виконання цих завдань. Не варто розпочинати роботу з інструментами threat intelligence, якщо немає розуміння, навіщо це потрібно.

Якщо рішення про необхідність використання threat intelligence прийнято, має сенс відразу використовувати для цього спеціалізовану платформу управління даними кіберрозвідки. Це може бути open-source або комерційне рішення, що дозволяє автоматизувати всі рутинні операції. Якщо використовується хоча б кілька джерел, без автоматизації неможливо якісно працювати з ними, здійснювати нормалізацію та зберігання в єдиній базі, а також працювати з відкритими загрозами.

Важливо на регулярній основі проводити оцінку якості та кількості джерел даних (фідів), позбавляючись тих, які ненадійні, дають велику кількість хибнопозитивних спрацьовувань, скорочуючи потік даних і підвищуючи його якість.

Етапи роботи з TI

Поетапно процес роботи з TI виглядає так:

1. Збір даних із різних джерел, який передбачає заклад всіх наявних джерел по фідам на одну платформу для роботи з ними в одному вікні. Це можуть бути будь-які джерела про загрози, що надходять у SOC, зовнішні дані від провайдерів, відкриті джерела, від партнерів, регуляторів, дані мережевої телеметрії (маршрутизаторів, міжмережевих екранів, пісочниці, SIEM-систем тощо).
2. Обробка зібраних фідів передбачає їхню нормалізацію та стандартизацію для того, щоб усі вони були приведені до єдиного формату, до єдиної «картки».
3. Збагачення додатковим контекстом, якщо даних недостатньо. Для збагачення даних існують універсальні сервіси (наприклад, VirusTotal, whois та інші) та вузькоспеціалізовані джерела. Зазвичай аналітик знає, бачачи дані про загрозу, з якого вузькоспеціального фіда необхідно збагатити цю інформацію. Зручно, коли вибрана платформа threat intelligence інтегрована з необхідною добіркою сервісів збагачення.
4. Виявлення індикаторів компрометації у власній інфраструктурі. Наприклад, R-Vision TIP дозволяє завести потік даних із SIEM-системи та перевірити конкретний набір індикаторів у цьому потоці подій.
5. Поширення індикаторів на засоби захисту та моніторингу.

Висновки

Threat intelligence – це важливий інструмент для прийняття рішень у сфері інформаційної безпеки. Він дає розуміння ландшафту загроз для прогнозування можливих атак та реалізації адекватних заходів захисту; підвищує якість та швидкість реагування на інциденти, тим самим дозволяючи мінімізувати можливі збитки. Інформація про актуальні загрози допомагає в більш точній оцінці ІБ-ризиків та плануванні необхідних заходів щодо їх обробки. Як показує практика, зазвичай організації починають цікавитися роботою з даними кіберрозвідки з побудови власного центру реагування на інциденти (security operations center, SOC). І якщо ви вже зрозуміли, що вам потрібна кіберрозвідка, варто відразу вибудовувати цей процес на базі автоматизованої платформи.

Перелік посилань

1. NIST SP 800-82 [Електронний ресурс] – Режим доступу до ресурсу: World Wide Web. – URL: https://csrc.nist.gov/publications/detail/sp/800-82/archive/2011-06-09 . Дата звернення: 26.07.2021
2. Організація OWASP. OWASP Top-10, головна сторінка [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/Top10/ . Дата звернення: 26.07.2021.
3. Блог компанії R-Vision. Что такое threat intelligence и как применять? [Електронний ресурс] – Режим доступу до ресурсу: https://rvision.pro/blog-posts/chto-takoe-threat-intelligence-i-v-chem-ego-tsennost/ . Дата звернення: 26.07.2021.

Надійшла: 23.06.2021 Рецензент: д.т.н., професор Савченко В.А.