ВИКОРИСТАННЯ CYBER THREAT INTELLIGENCE ПРИ ПОБУДОВІ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Пічієнко М. Г., Данилюк А.О.

Кафедра «Інфокомунікаційної інженерії ім. В.В. Поповського»,
Харківський національний університет радіоелектроніки, Україна

E-mail: mariia.pichiienko@nure.ua,
andrii.danyliuk@nure.ua

Abstract

Threat intelligence plays an important role in the organization's risk management process and in the future information security management system. Leveraging cyber threat can improve an organization's cybersecurity posture by monitoring the problem landscape and facilitating decision-making. The knowledge provided by CTI can be used to implement new security controls and make changes to existing processes.

Cyber Threat Intelligence (CTI, розвідка про загрози) – це дані, які збираються, обробляються та аналізуються, щоб зрозуміти мотиви, цілі та поведінку атаки суб'єкта загрози. CTI дає змогу приймати швидші й обґрунтованіші рішення щодо безпеки на основі даних і змінювати їхню поведінку з реактивної на проактивну в боротьбі із загрозливими суб'єктами.

Переваги CTI значною мірою залежать від організаційної ієрархії. Надаючи стратегічну інформацію для керівників і ради директорів, CTI може вплинути на зміни політики та довгострокові стратегічні рішення в організації. Оскільки CTI надає ситуаційну картину ландшафту загроз і ситуаційну обізнаність, ці знання можуть впливати на прийняття рішень на високому рівні в організації. Операційний CTI може надати контекст TTP (tactics, techniques, procedures) і назвати потенційних супротивників, які можуть загрожувати організації. Організаційний CTI також підтримує SOC (Security Operational Center) для покращення безпеки. Тактичну розвідку, яка надає необхідні дані для блокування та необхідні знання про індикатори компрометації (IoC), можна використовувати для попереднього блокування зловмисника, що теж значно зменшить обсяг роботи для SOC [1].

Першим кроком у розумінні того, як найкраще використовувати аналіз загроз, є усвідомлення, які дані вам потрібні. Тобто, це найнеобхідніші для організації знання, що можуть включати будь-яку кількість тем, починаючи від розуміння груп загроз і закінчуючи інформацією про новий тип зловмисного програмного забезпечення. Визначення своїх вимог до розвідки допоможе краще зрозуміти, як використовувати CTI у організації для досягнення конкретних цілей. Може виявитися, що найпростіший шлях до зрілого використання аналізу загроз є лінійним. Тобто, можна почати з оперативної інформації та застосувати надані рекомендації в існуючих організаційних практиках або процесах, а потім поступово включити більш детальні способи використання. Тобто, першим етапом повинно бути створювання своєї бази знань за допомогою CTI. Перш ніж подумати про те, як отримати IOC або реалізувати захисні рекомендації, варто використати звіти про загрози, щоб краще зрозуміти ландшафт загроз вашої організації. Ця базова інформація містить інформацію про те, які групи загроз націлені на вашу галузь, географічне положення, технології, що використовуються. Маючи краще базове розуміння загроз, характерних для вашої компанії та галузі, ви можете почати звужувати коло рекомендації, і краще зрозуміти, на чому зосередити свій час, енергію та засоби захисту.

Логічним наступним кроком є отримання опублікованих IoC від постачальника розвідувальних даних. Це стане фундамент для виявлення загроз. Індикатори компрометації надають обчислювальні артефакти, які аналітики використовують для ідентифікації зловмисної діяльності. Це може бути хеш-значення, IP-адреса, зловмисне доменне ім'я, IP-адреси, URL-адреси або зловмисне програмне забезпечення. Фахівці з промислової кібербезпеки використовують IoC, щоб виявити зараження зло-

вмисним програмним забезпеченням, витік даних або іншу зловмисну діяльність. Відстежуючи індикатори компрометації, організації можуть виявляти атаки або спроби атак і швидко на них зреагувати, мінімізуючи можливість критичних порушень.

Коли ви досягаєте зрілості та краще розумієте, як використовувати CTI, а також краще розумієте, що є «нормальним» у вашому середовищі, ви природним чином переходите від використання на основі індикаторів до більш проактивного підходу, наприклад пошуку загроз (або полювання на загрози, threat hunting). Хороший спосіб розпочати threat hunting або бути готовим до реагування на інцидент – переглянути звіти розвідки, які містять TTPs та інші технічні відомості про поведінку противника та його кампанії. Важливо звернути увагу на відповідні деталі звіту, наприклад інформацію про галузь або регіон. Наприклад, ви можете використовувати звіти про групи загроз і розвідувальні дані TTP, щоб припустити, які групи загроз будуть націлені на вашу компанію на основі звітів про історичне націлювання та використання TTP. Потім ви можете відслідковувати таку поведінку у своєму власному оточенні.

Ще один спосіб посилити захист інформаційної системи – це використовувати оцінки вразливостей, які можуть допомогти у визначенні пріоритетів та пом'якшенні вразливості. Найкращий спосіб зробити це — переглянути й оцінити відповідність повідомлених вразливостей щодо технологій, які ви використовуєте у своїх мережах і середовищах. Це допоможе вам спланувати та розставити пріоритети patch-менеджменту (що може бути громіздким процесом) і дотримуватися захисних рекомендацій, коли виправлення недоступне або його неможливо застосувати. Розуміння та впровадження цих захисних рекомендацій зменшить ризик для вашої інфраструктури і дозволить постійно вдосконалювати її на основі рекомендованих заходів пом'якшення, які можуть бути надані.

Наступним етапом може стати розповсюдження вже власних знань про загрози. Наприклад, це може бути доцільним для того щоб обґрунтувати керівникам необхідність інвестування в кібербезпеку. Розвідувальні звіти, що публікуються більшістю компаній, пов'язаних з кібербезпекою, чи постачальниками відповідного програмного забезпечення, в поєднанні з вашими експертними знаннями щодо проблем, характерних для вашої галузі та регіону, допоможуть вам легко побудувати аргументи щодо ландшафту загроз. Це дозволить вам визначити інвестиції в кібербезпеку, необхідні для ефективної боротьби із загрозами [2]. Також, ідеальним було б підтримування постійного зворотного зв'язку із постачальниками розвідувальних даних. Цикл розвідувальних даних працює найкраще, коли клієнти можуть визначити, які дані є дня ними пріоритетними. Тобто, чим більше ви можете розповісти своєму постачальнику розвідувальних даних, що вам потрібно, тим більша ймовірність, що ви побачите щось цікаве у звітах розвідки.

Отже, розвідка про загрози відіграє важливу роль у процесі управління ризиками організації та при будуванні системи менеджменту інформаційної безпеки. Використання аналізу кіберзагроз може покращити стан кібербезпеки організації, спостерігаючи за проблемним ландшафтом і допомагаючи в прийнятті рішень. Знання, які надає CTI, можна використовувати для впровадження нових засобів контролю безпеки та внесення змін до процесів. Оскільки CTI надасть рекомендації щодо дій, вони можуть виявитися цінними для протидії вхідним атакам. CTI можна використовувати для покращення обізнаності про ситуацію, щоб стежити за потенційними супротивниками та їхніми TTP. Розуміння того, як використовувати інформацію про загрози інформаційної безпеки (ІБ) і як реалізувати захисні рекомендації, є критичним кроком у створенні зрілої системи менеджменту інформаційної безпеки (СМІБ).

Література

1. Matilainen J. Using Cyber Threat Intelligence as a part of organisational cybersecurity. – Jyväskylä, 2020. – 55 с.

2. Warehime B. Using Threat Intelligence to Build a Mature OT Network Defense [Електронний ресурс] / B. Warehime, E. Wilfong. – 2022. – Режим доступу до ресурсу: https://www.dragos.com/blog/using-threat-intelligence-to-build-a-mature-ot-network-defense/.

3. Orchestrating Collaborative Cybersecurity: A Secure Framework for DistributedPrivacy-Preserving Threat Intelligence Sharing [Електронний ресурс] / [J. Trocoso-Pastoriza, A. Mermoud, R. Bouy та ін.]. – 2022. – Режим доступу до ресурсу:
https://www.researchgate.net/publication/363334807_Orchestrating_Collaborative_Cybersecurity_A_Secure_Framework_for_Distributed_Privacy-Preserving_Threat_Intelligence_Sharing.