Сударіков С. О.[1] студент
Шелуха О. О.[1,2] к.т.н., доцент
[1.]Національний авіаційний університет
[2.]Державний університет «Житомирська Політехніка»

АНАЛІЗ РОБОТИ ПЛАТФОРМ THREAT INTELLIGENCE

На сьогодні ландшафт кібербезпеки вирізняється кількома загальними проблемами – масивними обсягами даних, невеликою кількістю аналітиків та все більш складними змагальними нападами. Існуючі інфраструктури безпеки пропонують багато інструментів для управління цією інформацією, але більшість з них мало піддаються взаємоінтеграції. Це призводить до не адекватного обсягу інженерних зусиль, спрямованих на управління системами та неминучими витратами при обмежених ресурсах і часі.

Щоб боротися з зазначеними проблемами, можуть застосовуватися платформи розвідки загроз (Threat Intelligence Platforms – TIP). TIP можуть бути розгорнуті в якості програмного забезпечення, як послуги або на основі припущених рішень для полегшення управління кіберрозвідкою та пов'язаними з нею об'єктами [1]. Це визначається її здатністю виконувати чотири ключові функції:

1. агрегація інтелекту з декількох джерел;
2. коригування, нормалізація, збагачення та оцінка ризиків;
3. інтеграція з існуючими системами безпеки;
4. аналіз і обмін інформацією про загрози.

Розвідка – знання загрози, накопиченої аналітиками або визначеними подіями в системі. «Розвідка» це широкий термін, але TIP представляє аналітики з конкретними видами розвідки, які можуть бути автоматизовані, зокрема:

- технічні знання про атаки, включаючи індикатори;
- готова розвідка – висновок людей, які шукають доступну інформацію та роблять висновки про ситуаційну обізнаність, прогнозують потенційні результати або майбутні атаки або оцінюють можливості противника;
- людська розвідка – будь-які розвідувальні дані, зібрані людьми, наприклад, приховані в форумі для перевірки підозрілої діяльності.

Платформа розвідки – продукт, який об'єднується з існуючими інструментами і продуктами, являє собою систему управління розвідки загрозами, яка автоматизує і спрощує роботу аналітиків, яку вони традиційно виконували самостійно [2].

Дані, які були нормалізовані, перевірені та накопичені, повинні потім бути доставлені до систем, які можуть використовувати його для автоматичного виконання та моніторингу. Платформа розвідки загроз працює з SIEM-системами та постачальниками систем управління журналами за кадром, знижуючи показники, щоб перейти до рішень безпеки в інфраструктурі мереж клієнтів. Варто відзначити, що навіть у своїй мінімальний формі кіберрозвідка може принести суттєву користь в захисті від кіберзлочинців, адже одна з її важливих завдань – дати фахівцям з інформаційної безпеки актуальні дані і контекст для пріоритетзації своїх дій і прийняття рішень.

В даний час критично не вистачає не тільки ресурсів, що дозволяють обробити всі інциденти, але і загальних систем, завдяки яким стало б можливим реагувати на них на ранніх стадіях кібератак, а також накопичувати розподілені знання про загрози, обмінюватися отриманими даними, розслідувати причини загроз, реагувати на них та знаходити зловмисників. Для більш швидкого накопичення інформації про можливі загрози слід використовувати корисні дані ширшого кола джерел. Окреслимо основні платформи кіберрозвідки, які виконують ці завдання, та визначимо можливості роботи даних платформ згідно рівнів Threat Intelligence (табл. 1).

Таблиця 1. Порівняння основних TIP

Платформа	Тип	Рівні Threat Intelligence		
		Тактич-ний	Оператив-ний	Стратегіч-ний
MISP	відкрита	+	+	-
CRIT	відкрита	+	+	-
TheHeroic	відкрита	+	+	+
YETI	відкрита	+	+	-
GOSINT Framework	відкрита	+	+	+
R-Vision	відкрита	+	+	+
ThreatStream	комерційна	+	+	+
IBM QRadar Security Intelligence Platform	комерційна	+	+	-

Список використаних джерел

1. What is a Threat Intelligence Platform (TIP)? [Електронний ресурс] // ANOMALI. – 2018. – Режим доступу до ресурсу: https://www.anomali.com/ resources/what-is-a-tip.
2. Разбираемся в Threat Intelligence: платформы, сервисы, фиды… [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://rvision.pro/blog-posts/razbiraemsya-v-threat-intelligence-platformy-servisy-feedy/.