УДК 004.9 +343.1

НОСОВ ВІТАЛІЙ ВІКТОРОВИЧ

кандидат технічних наук, доцент,

професор кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ЧАЙКІН ТИМОФІЙ АНДРІЙОВИЧ

курсант факультету № 4

Харківського національного університету внутрішніх справ

АНАЛІЗ ФУНКЦІОНАЛЬНОСТІ ПОПУЛЯРНИХ ПЛАТФОРМ РОЗВІДКИ ЗАГРОЗ

Відомча комп'ютерна мережа Національної поліції України (НПУ) потребує впровадження сучасних рішень із забезпечення кібербезпеки.

Одним із засобів забезпечення кібербезпеки корпоративних комп'ютерних мереж є платформи розвідки загроз (Threat Intelligence Platforms, TIP), які є складовою платформ обміну інформацією про загрози (Malware Information Sharing Platform, MISP) (рис. 1) і призначені для збору, упорядкуванню, зберіганню, обміну та співвіднесенню показників компрометації (IoC) цілеспрямованих атак на комп'ютерні системи.

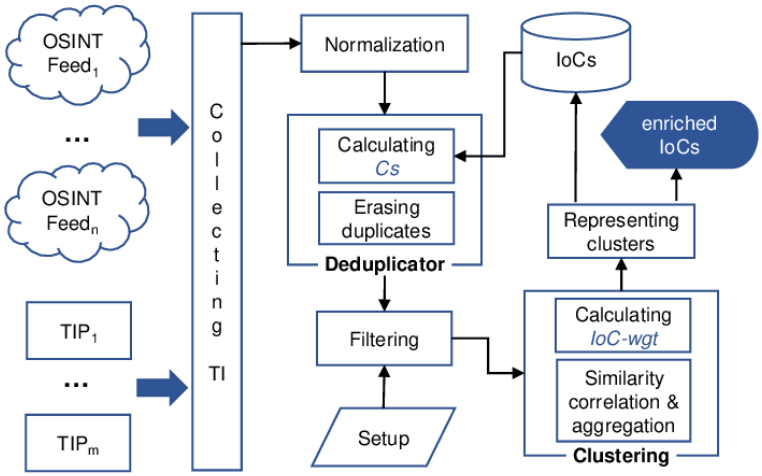

Рис. 1. Типова структура TIP-MIPS [1]

За даними [2] першою трійкою постачальників на ринку TIP за 2022 рік є компанії Fortinet (38,93%), Gigamon (7,1%) та SecureWorks (5,5%) (рис. 2).

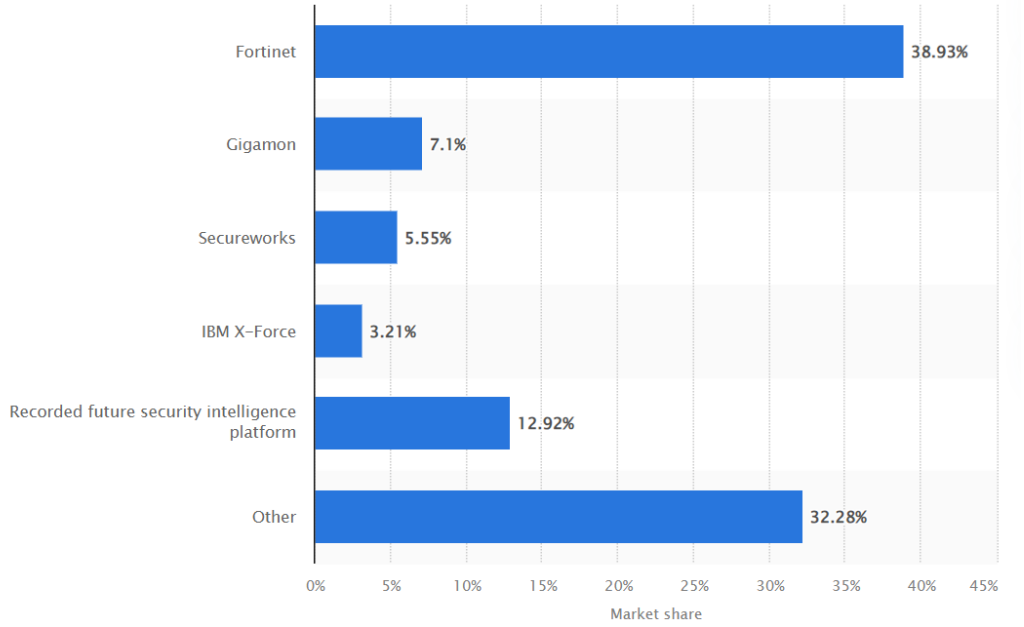

Рис. 2. Частка постачальників TIP на світовому ринку у 2022 році [2]

FortiEDR [3] від Fortinet має опції розгортання у хмарі, локально або гібридно. Основними особливостями є: виявлення та блокування загроз в реальному часі на основі політик мінімізації ризиків; наявність контекстних сценаріїв реагування на інциденти; реагування та відновлення безпеки без відключення систем для підтримки безперервності бізнесу.

GigaVUE Cloud Suite [4] від Gigamon є хмарним рішенням, орієнтована на глибокий аналіз трафіку публічної і приватної хмарної інфраструктури з метою проактивного пошуку загроз, має звичайний функціонал TIP.

Secureworks Taegis [5] є також хмарним рішенням, націлена на виявлення і реагування на загрози, має відкриту до масштабування архітектуру із інтеграцією продуктів від різних постачальників, пріорієтизацію сповіщень, застосовує технології штучного інтелекту для пошуку загроз.

Кожен вищезазначений продукт має свій унікальний функціонал, що дозволяє їх застосовувати в залежності від особливостей архітектури і призначення корпоративної комп'ютерної мережі. Але, з огляду на наявну тенденцію міграції корпоративних мереж у хмарну інфраструктуру і відповідну можливість створення приватної хмари НПУ, TIP Secureworks Taegis виглядає

більш функціональним, гнучким і потужним за рахунок впровадження технологій штучного інтелекту для впровадження його у відомчу комп'ютерну мережу НПУ.

Список використаних джерел:

1. Azevedo, Rui et al. "PURE: Generating Quality Threat Intelligence by Clustering and Correlating OSINT." *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (2019): 483-490.

2. Vendor share in the threat intelligence software market worldwide in 2022 // URL: https://www.statista.com/statistics/818165/threat-intelligence-security-services-spending-worldwide (дата звернення 24.11.2023).

3. Endpoint Detection and Response // URL: https://www.fortinet.com/products/endpoint-security/fortiedr (дата звернення 24.11.2023).

4. Migrate Workloads While Ensuring Security and Agility // URL: https://www.gigamon.com/products/access-traffic/cloud-suite.html (дата звернення 24.11.2023).

5. SECUREWORKS TAEGIS PLATFORM // URL: https://www.secureworks.com/products (дата звернення 24.11.2023).