МОДЕЛЮВАННЯ ВПЛИВУ ІНТЕГРАЦІЇ THREAT INTELLIGENCE НА ТОЧНІСТЬ ВИЯВЛЕННЯ АТАК У SOC-СЕРЕДОВИЩІ

Федюшин О.І., Вербицький А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах постійно зростаючої кількості кіберзагроз і складності атак ефективна діяльність Центрів оперативного реагування на інциденти безпеки (SOC) неможлива без використання систем Threat Intelligence (TI). Розвідка кіберзагроз виступає стратегічним компонентом кіберзахисту, який забезпечує не лише виявлення відомих індикаторів компрометації (IoC), але й формування контексту, необхідного для глибокого розуміння тактик, технік і процедур зловмисників (TTP) [1, 2].

Важливу роль відіграють також комерційні постачальники TI-фідів, які формують високоякісну, перевірену інформацію про актуальні загрози. Серед них виділяються Mandiant, Recorded Future, CrowdStrike Falcon Intelligence і Flashpoint. Ці сервіси надають глибокі аналітичні звіти про діяльність APT-груп, досліджують темні сегменти мережі (Dark Web), виявляють нові індикатори атак і забезпечують прогнозування ризиків. Отримані дані дозволяють SOC не лише реагувати на відомі інциденти, але й передбачати майбутні сценарії атак, що є важливим кроком у побудові адаптивної оборони.

Не менш значущою є роль інтегрованих сервісів і фреймворків, які підтримують застосування TI у повсякденних процесах SOC. Зокрема, MITRE ATT&CK Framework забезпечує методологічну основу для класифікації дій зловмисників і моделювання атак, допомагаючи аналітикам співвідносити реальні інциденти з відомими техніками. SIEM-системи, такі як Splunk чи Microsoft Sentinel, завдяки підтримці форматів STIX/TAXII, автоматично збагачують журнали подій TI-даними, що підвищує точність кореляції та зменшує кількість хибних спрацьовувань [3]. Крім того, сучасні EDR/XDR-рішення використовують TI для автоматичного пошуку загроз (Threat Hunting) у реальному часі, дозволяючи виявляти компрометації на ранніх етапах.

Отже, використання TI у діяльності SOC стає ключовим чинником підвищення ефективності кіберзахисту. Це дозволяє не лише виявляти відомі загрози, але й передбачати нові, забезпечуючи комплексну ситуаційну обізнаність і стійкість інформаційної інфраструктури до сучасних кібератак.

Список літератури

1. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). Information and cyber security of the enterprise. Textbook. Lviv: Publisher Marchenko T. V.

2. Sievierinov, O., Ovcharenko, M., & Vlasov, A. (2021). Enterprise Security Operations Center. Computer and information systems and technologies.

3. Li, X., Wang, Z., Leung, V. C. M., Ji, H., Liu, Y., & Zhang, H. (2021). Blockchain-empowered data-driven networks. ACM Computing Surveys, 54(3), 1-38.