MITM-АТАКИ ТА ЇХ ВИЯВЛЕННЯ ЗАСОБАМИ SECURITY OPERATIONS CENTER (SOC)

Федюшин О.І., Федосенко А.М.
Харківський національний університет радіоелектроніки, Харків, Україна
Сухотеплий В.М.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба, Харків, Україна

В епоху тотальної цифровізації, коли особисті та корпоративні дані стали найціннішим активом, питання захисту інформації від несанкціонованого доступу набуває вищого рівня. Кожна людина повинна критично оцінювати ситуації, коли її просять надати конфіденційні дані, і бути впевненою, що взаємодіє з легітимною системою, а не зі зловмисником.

Саме тому виникає гостра необхідність у потужних, централізованих системах моніторингу, здатних виявляти приховані атаки на рівні мережевого трафіку та аномалій у поведінці систем. Це і визначає критичну роль Security Operations Center (SOC) [1, 2], який виступає як технологічний захист, що аналізує потоки даних і виявляє ознаки компрометації, непомітні для звичайного користувача. Дослідження методів виявлення MITM-атак [3] засобами SOC є не просто актуальним, а життєво необхідним для побудови надійної системи кіберзахисту в сучасних умовах. Традиційно модель SOC є централізованою, всі ресурси та персонал розташовані в одному місці, що забезпечує фізичний захист даних та оптимізоване управління. Однак сучасні SOC також можуть бути розподілені між географічно розрізненими локаціями, що забезпечує глобальне розповсюдження ресурсів та цілодобовий аналіз загроз безпеки в режимі реального часу. SOC служать центральним вузлом для оцінки ситуації з безпекою в режимі реального часу, а їх основні функції включають постійний моніторинг, виявлення загроз, аналіз інцидентів та скоординовану реакцію на події, пов'язані з безпекою. Вони отримують різноманітні дані, інформацію та розвіддані, які надходять до сховища, яке використовується аналітиками для інтерпретації, кореляції, відображення, зберігання, архівування та прийняття рішень. Ключова роль у протидії загрозам MITM належить Security Operations Center. Як показав аналіз, SOC є не просто набором інструментів, а цілісним процесом, що поєднує технології та експертизу. За допомогою таких інструментів, як SIEM та IDS/IPS аналітики можуть ідентифікувати аномалії, що свідчать про MITM-атаку.

Список літератури

1.What is a security operations center (SOC)? [Електронний ресурс] / Режим доступу: https://www.ibm.com/think/topics/security-operations-center.

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

3. What is a Man-in-the-Middle Attack (MitM)? Definition and Prevention. [Електронний ресурс] / Режим доступу: https://jetpack.com/blog/what-is-a-man-in-the-middle-attack/.