МЕТОД ПОБУДОВИ ГРАФУ АТАКИ В SIEM-СИСТЕМАХ НА ОСНОВІ КОНТЕКСТУ ІДЕНТИЧНОСТІ

Москвін К.С., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні центри моніторингу безпеки (SOC) стикаються з експоненційним зростанням обсягів даних. Впровадження ешелонованого захисту, що включає системи EDR, NGFW та IAM, генерує мільйони окремих подій. Це створює фундаментальну проблему: традиційні SIEM-системи, хоч і агрегують ці дані, часто не здатні автоматично зв'язати їх у єдиний, зрозумілий ланцюжок інциденту. Як наслідок, аналітики перевантажені сповіщеннями, що призводить до "втоми від сповіщень" та збільшення часу виявлення загроз [1, 2]. Зі збільшенням складності атак зростає і їхня прихованість. Зловмисники активно використовують вкрадені облікові дані для легітимного, на перший погляд, просування всередині мережі. Існуючі механізми кореляції, що покладаються на зіставлення IP-адрес, хешів або статичних сигнатур, виявляються неефективними. Вони не можуть надійно відрізнити легітимну дію привілейованого користувача від дій зловмисника, що заволодів його акаунтом [3].

Тема даної доповіді присвячена розробці методу, що вирішує цю проблему шляхом використання контексту ідентичності як центрального вузла для кореляції подій. На відміну від підходів, де IAM є лише одним із джерел логів, запропонований метод використовує дані про користувачів, їхні ролі, привілеї та поведінкові патерни для автоматичного зв'язування розрізнених подій з EDR та NGFW. Це дозволяє в режимі реального часу формувати динамічний, орієнтований на користувача граф атаки, що є ключовим для реалізації сучасних стратегій безпеки, таких як Zero Trust [4].

Метою доповіді є дослідження та обґрунтування методу побудови графу атаки, який автоматично корелює події з різних систем захисту навколо сутності користувача. Такий підхід дозволяє миттєво візуалізувати повний ланцюжок атаки (Kill Chain), об'єднуючи мережеву активність, запуски процесів на хостах та спроби доступу. У рамках доповіді буде розглянуто запропоновану архітектуру інтеграції, алгоритм збагачення подій та побудови графу кореляції, а також представлено результати тестування методу на змодельованих сценаріях багатоетапних атак.

Список літератури

1. Cissec, J. The Challenge of Alert Overload in Modern Security Operations [Електронний ресурс] / Режим доповідей: https://securityboulevard.com
2. Sievierinov, O., Ovcharenko, M., & Vlasov, A. (2021). Enterprise Security Operations Center. Computer and information systems and technologies.
3. Microsoft. Identity is the new security perimeter [Електронний ресурс] / Режим доступу: https://www.microsoft.com
4. NIST. Special Publication 800-207: Zero Trust Architecture [Електронний ресурс] / Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-207/final