УДК 004.056.5
Т. Маслянка; Ю. Олійник; Н. Загородна, к. т. н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОБМЕЖЕННЯ СТАНДАРТНИХ МЕТРИК ЕФЕКТИВНОСТІ XDR-СИСТЕМ ПРИ АНАЛІЗІ ФІШИНГОВИХ КАМПАНІЙ

UDC 004.056.5
T. Maslianka; Yu. Oliinyk; N. Zagorodna, PhD., Assoc. Prof.

LIMITATIONS OF STANDARD EFFICIENCY METRICS OF XDR SYSTEM IN ANALYZING PHISHING CAMPAIGNS

У сучасному ландшафті кіберзагроз фішинг залишається домінуючим вектором первинного доступу зловмисників до корпоративних мереж. Згідно зі звітом Microsoft Digital Defense Report, лише за останній рік обсяг атак на основі паролів зріс у десять разів, а складність методів обходу фільтрації, таких як Adversary-in-the-Middle (AiTM), значно підвищилася [1]. У відповідь на це організації впроваджують платформи розширеного виявлення та реагування, зокрема Microsoft Defender XDR, які консолідують захист пошти, кінцевих точок та ідентичності. Однак, покладання виключно на автоматизовані засоби блокування та стандартні звіти створює хибне відчуття безпеки.

Проблематика стандартних інструментів звітності полягає у використанні обмеженого набору кількісних показників, які можуть не враховувати критичних факторів контексту та хронології інцидентів. Типові дашборди демонструють кількість заблокованих листів, але часто не дають відповіді на питання про час перебування фішингового листа у поштовій скриньці до моменту його видалення або про дії користувача, які не призвели до негайного спрацювання сигнатур. Як зазначають дослідники SANS Institute, перехід до проактивного захисту вимагає зміни парадигми від пасивного моніторингу до активного пошуку загроз [2].

Для об’єктивної оцінки ефективності контрзаходів необхідний перехід до аналізу «сирих» даних. У екосистемі Microsoft Defender XDR ключовим інструментом для цього є Advanced Hunting, що базується на мові запитів Kusto Query Language (KQL). На відміну від статичних звітів, KQL дозволяє корелювати події з різних доменів безпеки. Наприклад, поєднання даних з таблиць EmailEvents, EmailUrlInfo та DeviceNetworkEvents дозволяє виявити ланцюжки атак, де користувач перейшов за посиланням, яке на момент доставки вважалося безпечним [3].

Аналіз функціональних можливостей XDR-систем свідчить про необхідність застосування спеціалізованих метрик аудиту, які виходять за межі стандартних звітів. Використання певних запитів, таких як Advanced Hunting в Microsoft Defender XDR, дозволяє вирахувати такі критичні показники, як середній час між доставкою листа та кліком користувача та ефективність пост-детекції. Такий підхід дозволяє трансформувати механізми пошуку загроз у засіб верифікації надійності системи захисту та виявляти слабкі місця в політиках безпеки, які залишаються непоміченими при використанні стандартних інструментів моніторингу.

Література

1. Microsoft Digital Defense Report 2024 [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2024.
2. Lee R. M. The Who, What, Where, When, Why and How of Effective Threat Hunting / R. M. Lee, D. Wolpoff. – SANS Institute, 2016. – 18 p.
3. Advanced hunting schema [Електронний ресурс] // Microsoft Learn. – 2024. – Режим доступу: https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-schema-tables.