УДК 004.7

Колощук М.С., ст. викладач
Дячук О. Ю., ст. викладач
Окунькова О.О., ст. викладач
Державний університет "Житомирська політехніка"

ВИКОРИСТАННЯ ADEM ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ ТА ПОТЕНЦІЙНИХ КІБЕРЗАГРОЗ У РОЗПОДІЛЕНИХ МЕРЕЖАХ

Сучасні корпоративні мережі зазнали фундаментальної трансформації: масовий перехід на гібридну модель роботи, міграція застосунків у хмарні середовища, розширення мережі філій та зростання кількості мобільних користувачів призвели до того, що мережевий периметр став розмитим, а поверхня атаки — значно ширшою. У таких умовах традиційні підходи до моніторингу мережевої безпеки, орієнтовані на контроль фіксованого периметра, втрачають ефективність. Зловмисники дедалі частіше використовують легітимні канали зв'язку, компрометовані облікові записи та методи латерального переміщення (lateral movement), які важко виявити за допомогою сигнатурних методів або статичних правил.

Традиційні системи моніторингу, зокрема SIEM, IDS/IPS та NMS, мають суттєві обмеження в умовах розподілених мереж. SIEM-системи забезпечують кореляцію подій безпеки, але працюють переважно реактивно, генерують значну кількість хибних спрацювань і потребують постійного ручного налаштування правил кореляції. IDS/IPS-рішення ефективні проти відомих сигнатур атак, проте безсилі перед новими або невідомими загрозами, що використовують легітимні протоколи. Системи мережевого моніторингу (NMS) зосереджені на стані інфраструктурних елементів, а не на користувацькому досвіді чи виявленні загроз, і не забезпечують наскрізної видимості від кінцевого пристрою до застосунку. У зв'язку з цим виникає потреба в проактивних, автономних рішеннях, здатних виявляти аномалії в реальному часі без постійного втручання людини. Саме таким рішенням є Autonomous Digital Experience Management (ADEM) — компонент платформи Prisma SASE від Palo Alto Networks, що використовує штучний інтелект та машинне навчання для безперервного моніторингу розподілених мереж.

На відміну від SIEM, IDS/IPS та NMS, ADEM забезпечує комплексний підхід: він не лише виявляє аномалії, але й автоматично визначає першопричину, оцінює вплив на користувачів та надає рекомендації щодо усунення. ADEM є нативно інтегрованим у SASE-архітектуру Prisma, що дозволяє отримувати телеметрію з усіх сегментів мережі без розгортання додаткових агентів або обладнання.

Порівняльний аналіз традиційних засобів моніторингу та ADEM наведено в таблиці 1.

Таблиця 1 – Порівняння ADEM з традиційними засобами моніторингу

Характеристика	SIEM	IDS/IPS	NMS	ADEM
Метод виявлення загроз	Кореляція подій за правилами	Сигнатурний аналіз	Порогові значення метрик	ML-моделі, аналіз відхилень від baseline
Видимість	Логи, події безпеки	Мережевий трафік	Інфраструктурні пристрої	Наскрізна: від пристрою до застосунку
Проактивність	Низька (реактивний)	Середня	Низька	Висока (прогнозування та автономне усунення)
Інтеграція з SASE	Відсутня або обмежена	Відсутня	Відсутня	Нативна
Автономне усунення	Ні	Частково (блокування)	Ні	Так (guided remediation playbooks)

В основі функціонування ADEM лежить адаптивне базування (adaptive ML baselining) — метод, за якого система безперервно навчається на історичних даних, формуючи динамічний базовий рівень «нормальної» поведінки для кожного сегмента мережі. На відміну від фіксованих порогових значень, ADEM застосовує сегментне оцінювання (segment-wise scoring), коли відхилення вимірюються відносно того, що є нормальним для конкретного сегмента (LAN, ISP, оверлейні тунелі) та конкретної групи користувачів. Крім того, ADEM використовує кластеризацію користувачів (user clustering) за спільними ознаками, такими як провайдер зв'язку, географічне розташування або шлях до шлюзу. Це дозволяє відрізнити локальну проблему одного користувача від системної деградації, що впливає на велику кількість осіб.

Ключовим компонентом є кореляційний рушій (correlation engine), який пов'язує симптоми, підтверджувальні дані та ймовірну першопричину, автоматично формуючи інцидент із рекомендаціями щодо усунення. Такий підхід дозволяє скоротити час виявлення (MTTD) до 95% та час усунення (MTTR) до 77%.

Архітектура ADEM у контексті SASE. ADEM є нативно інтегрованим у три ключові компоненти платформи Prisma SASE. По-перше, агент GlobalProtect на кінцевих пристроях користувачів збирає телеметрію про стан Wi-Fi, завантаження CPU/пам'яті та якість з'єднання. По-друге, пристрої Prisma SD-WAN (ION) у філіях забезпечують моніторинг усіх активних і резервних WAN-шляхів до застосунків, визначаючи базові показники затримки, джиттера та втрат для кожного сегмента. По-третє, хмарні точки присутності Prisma Access виконують синтетичні тести та моніторинг реального трафіку користувачів, забезпечуючи видимість навіть тоді, коли користувачі та застосунки перебувають поза межами корпоративної мережі. Завдяки такій нативній інтеграції ADEM не потребує розгортання додаткових агентів або обладнання, що спрощує впровадження та знижує операційні витрати.

Важливо зазначити, що архітектура ADEM повністю відповідає принципам Zero Trust: система забезпечує повну видимість усього

трафіку, контроль доступу на основі контексту (користувач, пристрій, застосунок, місцезнаходження) та безперервну верифікацію кожного з'єднання. Такий підхід унеможливлює приховане латеральне переміщення зловмисника всередині мережі.

ADEM може бути використаний для виявлення низки потенційних кіберзагроз у розподілених мережах. Зокрема, латеральне переміщення (lateral movement) — техніка, за якої зловмисник після початкової компрометації переміщується між вузлами мережі в пошуках цінних активів, — може бути виявлене через аномальну зміну затримки або джиттера між внутрішніми сегментами, а також через нехарактерні патерни трафіку між вузлами, які зазвичай не взаємодіють між собою. Крім того, ADEM здатний виявляти аномальний трафік: різке зростання обсягу переданих даних, зміну типових протоколів або портів, підозрілі DNS-запити, що можуть свідчити про витік даних або командно-контрольний трафік (C2). Особливу цінність становить можливість використання відхилень у показниках затримки та джиттера як індикаторів атак: раптове погіршення якості з'єднання може свідчити про атаку типу «людина посередині» (MITM), DDoS-атаку або компрометацію кінцевого пристрою, що генерує аномальний трафік. ADEM дозволяє відстежувати ці показники на кожному сегменті мережі (LAN, інтернет, Prisma Access, застосунок) і виявляти відхилення від встановленого базового рівня.

ADEM є якісно новим підходом до виявлення аномалій у розподілених мережах завдяки поєднанню ML-моделей, адаптивного базування та наскрізної видимості. Інтеграція ADEM у SASE-архітектуру забезпечує безперервний моніторинг від кінцевого пристрою до застосунку, що повністю відповідає принципам Zero Trust та дозволяє виявляти загрози, які залишаються непоміченими традиційними засобами. Використання відхилень у показниках затримки та джиттера як індикаторів кіберзагроз відкриває нові можливості для проактивного виявлення атак типу lateral movement та MITM. Подальші дослідження можуть бути спрямовані на інтеграцію ADEM з XDR-платформами та розробку спеціалізованих моделей машинного навчання для виявлення складних APT-атак у розподілених мережах.

Список використаних джерел

1. Prisma SASE: Autonomous Digital Experience Manager (ADEM). The Network DNA. 2025. URL: https://www.thenetworkdna.com/2025/10/prisma-sase-autonomous-digital.html

2. Sharma M. Adaptive ML Baselining to Detect Network Performance Degradations. Palo Alto Networks Community Blog. 2025. URL: https://live.paloaltonetworks.com/t5/community-blogs/adaptive-ml-baselining-to-detect-network-performance/ba-p/1241203

3. Autonomous Digital Experience Management At a Glance. Palo Alto Networks. 2024. Autonomous DEM Administrator’s Guide. Palo Alto Networks. 2024. 28 лют. URL: https://origin-docs.paloaltonetworks.com/autonomous-dem/autonomous-dem-admin/adem-monitoring-and-tests