УДК 004.056.57

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЙ EDR ТА XDR, частина 2

Сєров І. О., Олефір О.О.
Науковий керівник – ст. викладач Медведєв Є.О.
Харківський національний університет радіоелектроніки,
каф. КРіСТЗІ, м. Харків, Україна
тел. +38(057) 702-14-30, e-mail: oleksandr.olefir@nure.ua

The purpose of the study is to analyze modern information security technologies (EDR and XDR) for solving the problems of protecting information in the corporate net infrastructure.

Наступним кроком у розвитку захисту корпоративних мереж стали рішення класу XDR, які охоплюють не тільки кінцеві точки, а й інші елементи типової мережної інфраструктури.

XDR поєднує в собі вже знайому по EDR функціональність виявлення та реагування на загрози кінцевих точок з можливостями виявлення сучасних кібератак, які виконуються через мережу, пошту чи хмарну інфраструктуру.

Нові джерела отримання відомостей про загрози – важлива відмінність XDR від рішень попереднього покоління, проте його головна перевага – у потужній системі збирання та обробки інформації.

Деталі реалізації XDR-систем можуть відрізнятися у різних вендорів, проте наступні модулі є базовими:

1) Deep Discovery Inspector – виконує глибокий аналіз мережевого трафіку та виявлення аномалій;

2) Cloud App Security – перевіряє поштові скриньки користувачів на предмет шкідливих листів та посилань;

3) Apex One SaaS – для захисту кінцевих точок;

4) Cloud One Workload Security – для перевірки контейнерів та компонентів хмарної інфраструктури.

Вся інформація про події, що надходить, збирається в єдиному сховищі, після чого виконується її обробка та аналіз за допомогою штучного інтелекту та інших технологій.

Вбудована в XDR система аналітики виявляє атаки як багатокомпонентні процеси, поєднуючи тисячі подій у кілька попереджень.

Система дозволяє візуалізувати атаку та подивитися, звідки прийшла загроза, як вона поширювалася по мережі та контейнерах у хмарах, кого заразила, як відбувалося переміщення між пристроями, які команди при цьому виконувались, і все це у вигляді таймлайну, який можна пройти покроково.

У XDR не використовується сигнатурний аналіз та правила кореляції, подібні до SIEM-систем. Натомість тут працюють поведінкові моделі, роз-

роблені аналітиками вендора на базі вивчення сотень тисяч виявлених атак. XDR автоматично об'єднує серії малозначимих дій у єдину значущу подію та розподіляє за пріоритетом відповідні оповіщення.

Завдяки зіставленню знайдених загроз по всій організації, вичерпній інформації про них, штучному інтелекту та аналітиці великих даних, при використанні XDR-аналітики SOC отримуватимуть лише значні сповіщення, відсортовані за рівнем серйозності.

У свою чергу, аналіз контексту незначних загроз від різних джерел дозволяє визначити значущі індикатори компрометації, що дозволяє проводити корисні дослідження, створювати єдину картину загроз, оперативно виявляти їх і блокувати. Автоматично аналізуючи величезні масиви даних, XDR усуває необхідність ручного втручання, дозволяючи фахівцям безпеки швидко відтворити розвиток атаки.

Таким чином, XDR системи безпеки дозволяють підвищити ефективність роботи аналітиків SOC та суттєво підвищити рівень захисту компанії від кіберзагроз.\

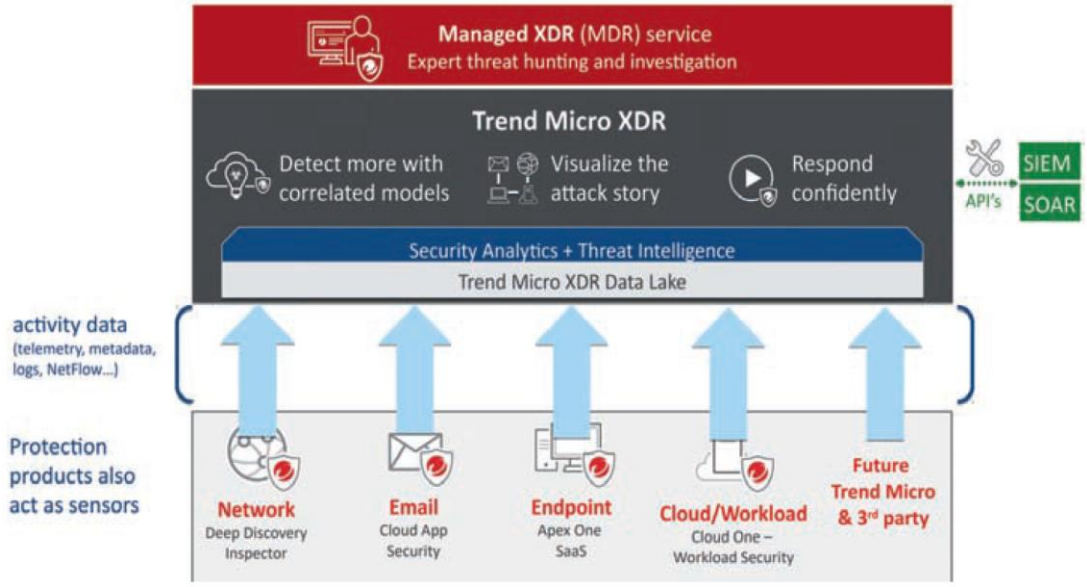

Рисунок 1 – Структура взаємодії компонентів XDR системи

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.

1. EDR, XDR And MDR: Understanding The Differences Behind The Acronyms. [Електронний ресурс] – Режим доступу: https://towerwall.com/wp-content/uploads/2021/05/Towerwall-EDR_XDR_MDR_Whitepaper-JD.pdf. Дата звернення: 15.03.2023.

2. From Endpoint Detection and Response to Proactive Cyber Defense with XDR. [Електронний ресурс] – Режим доступу: https://fidelissecurity.com/wp-content/uploads/2021/10/MITRE-WhitePaper_F-1021.pdf. Дата звернення: 15.03.2023.