УДК 004.056.57

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЙ EDR ТА XDR, частина 1

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.

Протягом багатьох років головним бар'єром для шкідливого програмного забезпечення були антивірусні програми. Вони перевіряли файли, які відкривав, копіював чи запускав користувач, на наявність характерної для вірусів послідовності байт – сигнатури. Бази сигнатур регулярно поповнювалися з сайту розробника антивірусу, удосконалювалися методи поведінкового аналізу програм, що запускалися, впроваджувалися евристичні методи для виявлення невідомих загроз, проте все це стосувалося виключно локального комп'ютера.

Для великих мереж впроваджувалися антивірусні комплекси із централізованою консоллю. Локальні антивіруси отримували налаштування від центру управління і відправляли туди всі попередження про виявлені погрози, виконуючи вказані в налаштуваннях дії (переміщали до карантину, видаляли файли або дозволяли роботу з ними).

З розвитком технологій та кіберзагроз можливостей традиційних антивірусів, що захищають кінцеві пристрої (Endpoint Protection Suite, EPP), перестало вистачати, оскільки для атак тепер використовуються цілком легітимні утиліти, наприклад, reg, wmic та powershell.

Самі атаки стали багатоетапними, і в цьому випадку кожна окрема шкідлива дія не викликає питань з боку антивірусу.

Отже, з'явилася гостра необхідність у рішеннях, які можуть не тільки відреагувати на загрозу відповідно до заданих правил, але й діяти проактивно, тобто не просто повідомити про інцидент, а заблокувати потенційно шкідливі операції, а також зібрати інформацію, необхідну для аналізу кібератаки. Такі рішення стосуються класу EDR – Endpoint Detection and Response, системи виявлення та реагування на загрози кінцевих пристроїв.

Системи EDR розширюють функціональність традиційних антивірусів модулем детального збирання даних. Це дозволяє аналітикам SOC (Security Operations Center – центр забезпечення інформаційної безпеки) у разі інциденту відповісти на такі запитання:

1) який пристрій став "нульовим пацієнтом", допустивши виконання шкідливої програми;

2) яким сином хакеру вдалося проникнути в систему і закріпитися в ній;

3) у якому файлі містився шкідливий код;

4) скільки систем було вражено;

5) які дані викрадено;

6) скільки часу зайняла атака;

7) які дії необхідно вжити.

Велика кількість інформації, що збирається EDR, призводить до того, що навіть у компанії середнього розміру команда SOC виявляється перевантаженою попередженнями, через що:

1) стає складно виявити кореляції між різними подіями;

2) витрачається багато часу на виявлення атак;

3) реакція відбувається надто пізно та в недостатньому обсязі;

4) розслідування інциденту не дає повної картини того, що сталося, оскільки якісь деталі залишаються нерозглянутими.

За даними дослідження Verizon 2019 Data Breach Investigations Report, середній час виявлення інцидентів становить 197 днів. В сучасних умовах це неприпустимо довгий термін: за півроку зловмисники встигнуть не тільки викрасти дані, що їх цікавлять, а й глибоко проникнути в мережу, детально вивчивши все, що відбувається в ній.

Логічним рішенням цієї проблеми є спільне застосування систем SIEM (Security Information and Event Management – системи управління інформацією та подіями безпеки) та EDR, що дозволить виявляти інциденти та реагувати на них оперативніше, проте це не так. SIEM системи збирають оповіщення від усіх пристроїв, підключених до мережі, але ці оповіщення, як і в EDR, ізольовані один від одного. Налаштування правил кореляції вирішує цю проблему лише частково, оскільки критично важливі повідомлення можуть загубитися серед інших повідомлень. Щоб виявити атаку за допомогою SIEM, потрібно виконати багато ручної роботи навіть за настроєних кореляцій, адже одна атака може бути представлена кількома тисячами подій.

EDR-рішення мають ще один істотний в контексті сучасних загроз недолік: вони працюють виключно з "кінцевими точками"– комп'ютерами, серверами та мобільними пристроями. Однак у мережі будь-якої організації є й інші компоненти, наприклад, принтери, маршрутизатори, пристрої IoT та IIoT, мережеве обладнання та компоненти хмарної інфраструктури (контейнери та віртуальні машини). З точки зору EDR їх не існує, хоча захоплений зловмисниками мережевий принтер чи маршрутизатор можуть стати серйозною загрозою для компанії.