Чи достатньо просто захищати?

Що показав пілот

cynet



Cynet поєднує виявлення, аналіз та автоматизоване реагування на загрози.

Наявність антивірусу, систем моніторингу, політик доступу та інших засобів захисту ще не означає, що інфраструктура справді захищена. Частина ризиків може залишатися поза увагою: неврахований програмне забезпечення, застарілі компоненти, небезпечні налаштування або легітимні інструменти, які використовуються не за призначенням. Тому важливо перевіряти не лише те, що має працювати в системі, а й що в ній відбувається насправді.

NWU провела пілот Cynet у реальному IT-середовищі одного з комунальних медичних закладів Києва, щоб оцінити, які ризики можуть залишатися непомітними під час повсякденної роботи. Пілот тривав 17 днів і охопив сім робочих станцій. Проте навіть у такому невеликому сегменті було виявлено різні класи ризиків — від Shadow IT і неконтрольованих засобів віддаленого доступу до небезпечних конфігурацій та незакритих вразливостей.

Shadow IT: те, чого команда може не бачити

Одним із результатів пілоту стало виявлення програм та portable-інструментів, які використовувалися поза стандартним контролем IT-служби, зокрема засобів віддаленого адміністрування. Самі по собі такі інструменти можуть бути цілком легітимними, однак їх неконтрольоване використання створює додаткові ризики та потенційні канали віддаленого доступу до робочих станцій. Проблема Shadow IT — у відсутності повної видимості: IT-команда не завжди знає, які інструменти фактично працюють у середовищі, хто їх запускає та з якою метою.

Risk Score: від сигналу до розслідування

Під час пілоту були виявлені файли з максимальним рівнем Risk Score, скрипти та dual-use утиліти. Сама наявність такого ПЗ не обов'язково свідчить про атаку, тому критично важливим є контекст: звідки запущено файл, як він поводиться, з якими процесами взаємодіє та які дії виконує. Cynet аналізує події не ізольовано, а в контексті пов'язаної активності, формуючи граф зі зв'язками між пристроєм, процесами, файлами та джерелами їх запуску. В одному з випадків вдалося встановити, що portable-програму з високим Risk Score було запущено з USB-носія. Такий підхід допомагає швидше зрозуміти, що саме відбулося, визначити реальний рівень ризику та перейти від сповіщення до розслідування.

Конфігурації та вразливості як прихована поверхня атаки

Пілот показав, що частина ризиків пов'язана зі станом самої інфраструктури. Було виявлено потенційно ризикові мережеві та системні конфігурації: використання mDNS і LLMNR, налаштування Windows Installer, що допускають встановлення програм із підвищеними правами, а також відкритий RDP. Окремий напрям — незакриті CVE у програмному забезпеченні та браузерах. Навіть у межах невеликого тестового сегмента було виявлено десятки вразливостей різного рівня критичності, зокрема критичну вразливість у застарілій версії Adobe Acrobat. Це дозволило не лише зафіксувати наявні проблеми, а й визначити пріоритетність їх усунення.

Від виявлення — до дії

Cynet об'єднує аналіз, розслідування та реагування в межах однієї платформи. CyAI допомагає аналізувати та пов'язувати події, SOAR — автоматизувати типові сценарії реагування й усунення загроз, а MDR/CyOps — забезпечити цілодобовий моніторинг та експертну підтримку. Для організацій з обмеженими ресурсами IT-команди це дозволяє автоматизувати значну частину роботи без необхідності створювати власний SOC та окрему команду аналітиків.

Що показав пілот

Головний висновок тестування простий: фактичний стан інфраструктури може суттєво відрізнятися від того, що бачить команда під час повсякденного моніторингу. Практичний пілот дозволяє перевірити це безпосередньо в робочому середовищі, оцінити процеси безпеки та зрозуміти, наскільки швидко організація може переходити від виявлення потенційної проблеми до її аналізу та реагування.

Оцініть фактичний стан власної інфраструктури

NWU, офіційний дистриб'ютор Cynet в Україні, проводить пілотні проєкти безпосередньо в IT-середовищі замовника. Залиште заявку на пілот Cynet (*cynet.nwu.ua*) – експерти NWU допоможуть оцінити фактичний стан вашої IT-інфраструктури, виявити потенційні ризики та визначити пріоритети для їх усунення.

NWU

Більше про рішення з питань кібербезпеки за телефоном +38 044 359 01 31 або на сайті nwu.ua