АНАЛІЗ СИСТЕМ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ВІД СКЛАДНИХ ЗАГРОЗ EDR (ENDPOINT DETECTION AND RESPONSE)

Баклан Я. А., Сєвєрінов О. В.
Харківський національний університет радіоелектроніки, Харків, Україна

Дослідження багатьох аналітичних фірм показують, що нинішній рівень захисту інформації у багатьох випадках є низьким через покращення тактики маскування через кінцевих користувачів, які працюють поза периметром (наприклад, від аеропортів, кафе, магазинів або з додому), заражених USB, безфайлових атак і так далі. Звичайні рішення безпеки хоч і корисні та забезпечують захист від більшості загроз - різні антивіруси, брандмауери, веб-шлюзи, системи контролю інцидентів та заходів безпеки (SIEM), хмарні інструменти безпеки тощо, проте захист розпочинається з кінцевих точок, і все більше організацій розгортають рішення EDR як доповнення до існуючої системи безпеки [1]. У числі важливих переваг EDR - безперервний моніторинг кінцевих точок усередині і поза корпоративною мережею. Крім того, ці засоби використовують штучний інтелект для виявлення активності шкідливого коду, а також забезпечують попереджуюче полювання за індикаторами атак, щоб побачити ознаки, які ще не виявлені.

Метою доповіді є огляд та аналіз функціональних можливостях сучасних рішень Endpoint Detection and Response (EDR) для забезпеченні безпеки робочих місць організацій.

Наводяться результати аналізу функціональних можливостей сучасних рішень EDR. Популярні системи класу Endpoint Protection Platform (EPP) не орієнтовані на протидію складним і комплексним загрозам на кінцевих точках, що свідчить про необхідність додаткових інвестицій в спеціалізовані продукти класу Endpoint Detection and Response (EDR) для розширеного виявлення на базі передових технологій і подальшого реагування на знайдені складні загрози [2]. Дійшли висновку, що тільки спільне використання цих двох технологій і балансу між власною експертизою і використанням сторонніх сервісів дозволить організаціям добитися дійсно високих показників захисту своїх кінцевих пристроїв і тим самим підвищити безпеку компанії в цілому в епоху швидко зростаючого числа і складності передових загроз і цілеспрямованих атак.

Список літератури

1. Ушатов В. В., Сєвєрінов О. В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. - Харків.: ХНУРЕ, 2019. – С. 104–105.
2. Harmionee Kaur and Richa Tiwari. Endpoint detection and response using machine learning 2021. DOI: 10.1088/1742-6596/2062/1/012013/
3. Сєвєрінов О. В., Хрєнов А. Г., Поляков А. О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі // Системи обробки інформації, 9 (2015): 101-104.