Анчис А. О., магістрант,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ВУЗЛІВ

Кібербезпека стала однією з найбільш актуальних і важливих проблем сучасного світу. Зростання кількості і складності кіберзагроз створює серйозні ризики для бізнесу, державних установ, та індивідуальних користувачів. Кібератаки можуть призвести до втрати конфіденційної інформації, фінансових втрат, порушення приватності, та навіть можуть загрожувати життям та безпеці людей.

Система EDR (Endpoint Detection and Response) є однією з ключових компонентів для забезпечення кібербезпеки. Вона надає можливість виявляти та реагувати на загрози, які спрямовані на кінцеві вузли в мережі. Система EDR включає в себе інструменти для виявлення аномальної активності, моніторингу та реагування на загрози [1].

EDR грає ключову роль у виявленні потенційних загроз для кінцевих вузлів. Вона аналізує активність в реальному часі і виявляє незвичайні або підозрілі дії, які можуть свідчити про наявність загрози. Це може включати в себе виявлення вторгнень, вірусів, шкідливого програмного забезпечення та інших загроз.

Після виявлення загрози, система EDR надає можливість реагувати швидко і ефективно. Це може включати в себе автоматизовані процеси для ізоляції заражених вузлів, блокування загрози та подальший аналіз інциденту для запобігання подібним інцидентам у майбутньому [3].

Моніторинг є ключовим аспектом роботи системи. Вона надає можливість постійно відслідковувати активність на кінцевих вузлах та надавати докладну звітність про події безпеки. Це допомагає вчасно реагувати на загрози та аналізувати їх для подальшого удосконалення заходів безпеки.

Інтеграція з іншими інструментами і технічними рішеннями кібербезпеки для досягнення максимальної ефективності є важливою складовою даного рішення захисту мережі. Інтеграція дозволяє обмінюватися інформацією та взаємодіяти з іншими засобами захисту: антивірусними системами, файрволами, системами моніторингу тощо.

Незважаючи на всі переваги, існують виклики, з якими можуть стикатися організації при її впровадженні. Це включає в себе складність налаштування, необхідність постійного оновлення і аналізу результатів. Проте з розвитком технологій і збільшенням обсягу кіберзагроз, система EDR залишається актуальною та важливою частиною стратегії кібербезпеки.

Існує численна кількість організацій, які успішно впровадили систему EDR та змогли значно підвищити рівень кібербезпеки. Такі успішні сценарії можуть надихати інші організації на вдосконалення своєї стратегії захисту [2]. Наприклад, міжнародний «Безпечний Банк» є однією з провідних фінансових установ в світі та обробляє великий обсяг фінансових транзакцій кожного дня. Зберігання конфіденційної інформації клієнтів та забезпечення безпеки фінансових операцій є найважливішим завданням банку. Фахівці провели докладний аналіз своїх потреб у сфері кібербезпеки та визначили, що для забезпечення безпеки кінцевих вузлів та виявлення загроз система EDR є обов'язковою.

В результаті впровадження, було збільшено безпеку операцій та досягнуто ефективне виявлення та реагування на кіберзагрози в реальному часі, що дозволило забезпечити безпеку фінансових операцій та конфіденційної інформації клієнтів.

В доповіді буде представлено технологію захисту кінцевих вузлів, а також програмне встановлення захисту та його можливості.

Список використаних джерел

1. Що таке Endpoint Detection and Response. URL: https://ua.softlist.com.ua/articles/chto-takoe-endpoint-detection/
2. Чому організації використовують EDR. URL: https://www.ibm.com/topics/edr
3. Що таке EDR та як він працює. URL: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html