ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТАЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту віддалених користувачів інформаційної системи організації на базі рішення Sentinel ONE»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Кирил БЕРЕЗОВСЬКИЙ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
БЕРЕЗОВСЬКИЙ Кирил
(прізвище, ім'я)

Керівник д.т.н., професор ГАЙДУР Галина
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПК – Персональний комп’ютер

EPP – Endpoint Protection Platforms

EDR – Endpoint detection and response

XDR – extended detection and response

VPN – virtual private network

MFA – multi-factor authentication

ВСТУП

Останнім часом, все більша кількість організацій використовують для своїх бізнес–потреб віддалених працівників. Це створює нові виклики для забезпечення кібербезпеки інформаційних систем організацій, оскільки працівники використовують особисті пристрої та домашні мережі, що можуть бути менш захищеними.

Віддалений доступ може бути шляхом втручання в інформаційну мережу з використанням вразливостей, які активно використовують кіберзлочинці но основі нових методів проведення атак. Тому захист кінцевих точок стає критично важливим для виявлення та запобігання цим загрозам інформаційної системи організації.

Віддалені користувачі можуть підключатися до корпоративних мереж з різних пристроїв — ноутбуків, смартфонів, планшетів. Це вимагає комплексного підходу до захисту, щоб забезпечити безпечний доступ до ресурсів інформаційної системи. У сучасному світі дані компанії є її найціннішим активом. Недостатній захист може призвести до витоків даних, фінансових збитків та шкоди репутації.

Таким чином, дослідження питань захисту кінцевих точок в контексті віддалених користувачів має важливе значення для забезпечення стабільності та безпеки організацій у сучасному інформаційному середовищі.

Об'єкт дослідження –з ахист віддалених користувачів інформаційної системи організації.

Предмет дослідження – технологія захисту віддалених користувачів інформаційної системи на базі рішення Sentinel ONE.

Метою роботи – роботи є впровадження технології захисту віддалених користувачів інформаційної системи на базі рішення Sentinel ONE та розробка рекомендації щодо її застосування.

Наукові завдання:

дослідити сутність проблеми захисту віддалених користувачів;

проаналізувати підходи до вирішення проблеми віддаленої роботи користувачів інформаційної системи організації;

проаналізувати існуючі технології захисту віддалених користувачів на основі Endpoint Protection;

проаналізувати методи та засоби захисту віддалених користувачів на прикладі Sentinel Ones Endpoint Protection;

розкрити порядок реалізації технології захисту віддалених користувачів на прикладі Sentinel Ones Endpoint Protection.

Методи дослідження: опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, практичне використання засобів захисту віддалених користувачів.

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту віддалених користувачів на прикладі Sentinel Ones Endpoint Protection, а також розроблено рекомендації фахівцям з кібербезпеки щодо застосування даної технології.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Аналіз роботи віддалених користувачів інформаційної системи організації

Віддалена робота користувачів інформаційної системи організацій перетворилася з рідкісної переваги на нову норму. У дослідницькому звіті DigitalOcean Currents за 2023 рік зазначено, що 39% опитаних компаній працюють повністю віддалено, тоді як 23% дотримуються гібридної моделі з обов'язковими днями перебування в офісі (23%) або відкритими віддаленими варіантами (25%). Лише 14% компаній залишаються повністю в офісі [1].

Хоча привабливість гнучкості й уникнення щоденних поїздок на роботу й на роботу очевидна, перехід до віддаленої роботи не обійшовся без проблем. Успішна віддалена робота потребує зміни мислення та цифрових інструментів для спілкування в різних часових поясах, співпраці за кордоном і зв'язку між розподіленими командами. Розподілені команди все більше покладаються на віртуальний інструментарій, щоб втілити свої найкращі ідеї в життя.

Особливість такої роботи полягає, незалежно від того, чи в організації розподілені робочої сили чи віддалені команди , мати під рукою належне програмне забезпечення та платформи, які є важливими для максимальної продуктивності та підтримки культури компанії на відстані.

Перехід до віддаленої роботи користувачів інформаційної системи вимагає правильних цифрових інструментів для спілкування, співпраці та організації між віддаленими користувачами.

Щоб забезпечити ефективність, співпрацю, продуктивність і захист даних у розподіленому робочому місці, необхідно зважати на такі категорії інструментів віддаленої роботи: керування проектами, обмін файлами, зв'язок, відлік часу та безпека (рис 1.1).

Рис.1.1. Основні категорії засобів віддаленої роботи

Оцінюючи інструменти для віддаленої роботи, варто звернути увагу на різні категорії інструментів. Деякі програми підтримують командну роботу та спілкування, інші можуть увімкнути керування завданнями в розподілених місцях, тоді як інші інструменти сприяють безпеці в мережі ноутбуків по всьому світу. Розглянемо основні категорії засобів віддаленої роботи:

Управління проектами

Ефективні інструменти керування проектами дозволяють віддаленим командам надсилати нові функції, запускати нові продукти та досягати ширших бізнес-цілей. Такі інструменти пропонують інтуїтивно зрозумілий інтерфейс для призначення завдань, установлення термінів виконання, відстеження прогресу та підтримки видимості ініціатив вашої команди. Це дозволяє віддаленим користувачам залишатися налагодженою командою, гарантувати, що нічого не провалиться, і продовжуватиме рух проектів.

Обмін файлами та хмарне сховище

Віддалені співробітники постійно отримують доступ до файлів і документів з різних місць і пристроїв. Централізована хмарна платформа обміну файлами є обов'язковим інструментом віддаленої роботи. Тут застосовуються інструменти, які забезпечують великий простір для зберігання, організацію папок і детальні засоби керування дозволами. Це допомагає віддаленим користувачам співпрацювати над вмістом, отримувати доступ до важливих файлів і захищати конфіденційні дані.

Спілкування та співпраця

Незалежно від того, яка задача виконується, відбувається обговорення різниз професійних завдань. Інструменти комунікації та координації підтримують розмови у віддаленій команді. Це можуть бути інструменти з функціями відеоконференцій, як-от спільне використання екрана, віртуальні дошки та кімнати для сеансів, які допоможуть віддаленим колегам відчувати себе більш зв'язаними та згуртованими. Звичайний інструмент командного обміну повідомленнями або миттєвого чату також важливий для полегшення швидкої реєстрації, імпровізованих обговорень і доступності.

Облік часу та управління завданнями

Віддаленим співробітникам потрібні інтуїтивно зрозумілі способи відстеження свого часу. Правильні інструменти відстеження часу та керування завданнями матимуть такі функції, як реєстрація робочого часу, керування списками справ і моніторинг стану роботи. Це допоможе віддаленим користувачам не відставати від дедлайнів і отримати видимість загального рівня продуктивності. Він також підтримує підзвітність, звітність про прогрес і ефективне керування робочим процесом.

Безпека

Впровадження правильних інструментів безпеки може допомогти захистити конфіденційну інформацію вашої компанії та запобігти несанкціонованому доступу. Тут необхідно застосовувати інструменти, які пропонують такі функції, як багатофакторна автентифікація, шифрування та безпечний обмін файлами. Ці інструменти також мають бути простими у використанні та бездоганно

інтегруватися з наявним робочим процесом. Визначивши безпеку пріоритетом, користувачі інформаційної системи організації можуть спокійно зосередитися на своїй роботі, не турбуючись про потенційні порушення безпеки.

Отже, питання щодо захисту віддалених користувачів, є ключовим питанням, яке дозволить учасникам бізнес-процесів в інформаційній системі організації бути захищеними від впливів різноманітних атак та несанкціонованому доступу і як наслідок витоку конфіденційної інформації.

1.2. Аналіз загроз роботи віддалених користувачів інформаційної системи організації

Розвиток віддаленої роботи створив нові проблеми для компаній, які хочуть захистити свою конфіденційну інформацію. Оскільки все більше співробітників працюють за межами традиційного офісного середовища, компанії повинні знайти нові способи керування та моніторингу доступу до даних. Пристрої співробітників, домашні мережі Wi-Fi і невідомі програми сторонніх розробників становлять потенційну загрозу безпеці. У цій публікації блогу ми досліджуємо 10 основних ризиків віддаленої роботи та те, як можна захистити свій бізнес від кібератак [3].

1. Незахищені з’єднання: однією з найбільш суттєвих проблем віддаленої роботи є використання незахищених з’єднань для доступу до даних компанії. Загальнодоступні мережі Wi-Fi не є захищеними, і якщо співробітник входить у незахищену мережу, дані компанії, що передаються між його пристроєм і сервером, стають уразливими. Щоб зменшити ризик незахищених з’єднань, переконайтеся, що всі співробітники використовують VPN під час віддаленого доступу до даних компанії.

2. Фішингові шахрайства: віддалені працівники можуть стати жертвами фішингових шахраїв, які надсилають шахрайські електронні листи з наміром викрасти конфіденційні дані компанії. Шахрай може обманом змусити співробітника відкрити облікові дані для входу або завантажити зловмисне програмне забезпечення, яке заражає систему. Щоб зменшити ризик фішингового

шахрайства, проводите регулярні тренінги для співробітників, щоб навчити їх виявляти підозрілі електронні листи та дії.

3. Недостатня обізнаність щодо кібербезпеки. Іншим ризиком віддаленої роботи є недостатня обізнаність працівників щодо кібербезпеки. Віддалені співробітники можуть бути не настільки пильними щодо ризиків безпеки, як ті, хто працює в офісі. Щоб переконатися, що віддалені співробітники підтримують високий рівень обізнаності з кібербезпеки, забезпечуйте регулярне навчання та забезпечуйте дотримання політики компанії щодо найкращих практик кібербезпеки.

4. Керування пристроями: віддалені працівники можуть використовувати некеровані персональні пристрої для доступу до даних компанії, що може становити ризик для організаційних даних. Без належного керування пристроєм може бути складно відстежувати, які пристрої отримують доступ до інформації компанії, що може призвести до витоку даних. Встановіть системи, які контролюють пристрої, які використовуються для доступу до даних компанії.

5. Недостатня кількість оновлень системи: щоразу, коли стає доступним оновлення операційної системи, програмного забезпечення чи програми, важливо оновити систему останніми виправленнями безпеки. Багато віддалених працівників можуть не оновлювати свої пристрої регулярно, що робить їх уразливими до зловмисного програмного забезпечення та інших ризиків кібербезпеки. Надавайте регулярні нагадування віддаленим співробітникам про оновлення своїх пристроїв і вживайте всіх необхідних заходів для забезпечення своєчасного встановлення всіх оновлень системи.

6. Зберігання даних: під час віддаленої роботи конфіденційні дані можуть зберігатися на персональних комп’ютерах, які можуть не мати належних заходів безпеки. Якщо ці пристрої викрадено або зламано, може статися витік конфіденційних даних компанії, що призведе до порушення безпеки. Заохочуйте віддалених працівників зберігати дані в схваленому компанією хмарному сховищі або впровадити заходи для забезпечення шифрування даних на їхніх особистих пристроях.

7. Плинність кадрів. Плинність кадрів є ще одним ризиком віддаленої роботи, оскільки працівники можуть залишити компанію з конфіденційними даними. Важливо мати належні процедури для негайного скасування доступу до конфіденційних даних після звільнення працівника з організації.

8. Відсутність моніторингу: віддалені працівники фізично не присутні в офісі, що ускладнює моніторинг їхньої кібер-активності. Без необхідних моніторингових перевірок виявити потенційні загрози чи атаки стає складно. Встановіть належні заходи моніторингу, щоб гарантувати, що всі системи та мережі захищені та постійно контролюються.

9. Проблеми відповідності: якщо ваша організація має суворі нормативні вимоги, віддалена робота може становити ризик для відповідності. Оскільки віддалені працівники отримують доступ до конфіденційних даних зі своїх особистих пристроїв, може бути важко забезпечити повну відповідність. Важливо впровадити суворі заходи безпеки з використанням VPN, обмеження прав доступу до мереж, пристроїв і даних компанії.

10. Хмарна безпека. Хмарна безпека є ще однією важливою проблемою для віддалених працівників. Постачальники хмарних послуг зазвичай пропонують кілька функцій безпеки та протоколів, але важливо переконатися, що ці функції відповідають вашим стандартам безпеки даних. Оцініть постачальників хмарних послуг, перш ніж зробити вибір, щоб переконатися, що вони мають необхідні протоколи безпеки.

Останнім часом дистанційна робота, безсумнівно, різко зросла, і компанії повинні змиритися з потенційними ризиками, пов’язаними з цим новим режимом роботи. Ризики кібербезпеки впливають на репутацію, фінансову стабільність і юридичний статус компанії. Оскільки підприємства продовжують використовувати віддалену роботу, важливо вжити всіх необхідних заходів для запобігання кібератакам. Організації повинні інвестувати в адекватні заходи кібербезпеки, навчання співробітників, регулярні оновлення пристроїв і належні системи моніторингу. Таким чином вони можуть захистити свій бізнес і підтримувати високий рівень безпеки даних.

Сьогодні співробітники на 85% частіше розкривають файли, ніж до COVID-19 [4].

59% керівників IT-безпеки кажуть, що загрози від інсайдерів зростуть або «значно» зростуть протягом наступних двох років.

Більше половини організацій не мають плану реагування на внутрішні ризики.

40% організацій не оцінюють, наскільки ефективно їхні технології пом'якшують внутрішні загрози.

Незважаючи на те, що вони знають ризики, пов'язані з інсайдерами, більше половини організацій не мають плану реагування на інсайдерські ризики. Згідно з новим звітом, трохи менше половини компаній не мають звички оцінювати, наскільки ефективно їхні технології пом'якшують внутрішні загрози.

Згідно з дослідженням, проведеним на замовлення Code42 The Ponemon Institute, лідери бізнесу та безпеки допускають масові внутрішні загрози після раптового переходу до віддаленої роботи минулого року [4].

Вектор атак згідно звіту [5] кібератаки, яких зазнали віддалені користувачі, мають різний діапазон цілі. Більшість rjhbcnedfxsd (53%) вважають, що використовували для встановлення шпигунського програмного забезпечення, при цьому була фінансова вигода майже в половині нападів (48%). 48% повідомили про поширення програм-вимагачів наших респондентів.

Щодо типів кібератак (рис 1.2) найпоширенішим є фішинг, а потім веб-атаки.

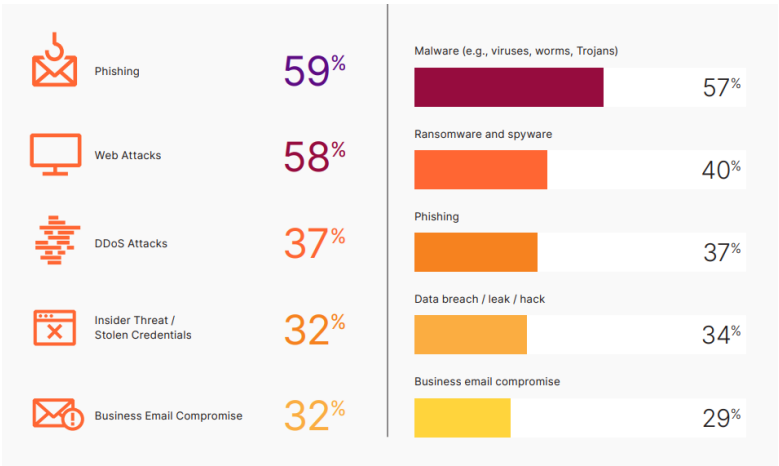

Рис. 1.2. Поширені атаки на віддалених користувачів

Що стосується загроз, зловмисного програмного забезпечення, як віруси, хробаки і трояни — входять до трійки лідерів ризики для 57% користувачів. Інші поширені загрози є програми-вимагачі та шпигунські програми (40%), фішинг (37%), виток даних (34%) та компроментація корпоративної електронної пошти (29%).

1.3. Підходи до вирішення проблеми віддаленої роботи користувачів інформаційної системи організацій

Ризики для безпеки даних віддаленої роботи та як їх пом’якшити і вирішити проблеми віддалених користувачів інформаційної системи організації розглянемо надалі, щоб не завдати кібервпливів інформаційній системі організацій. Необхідно зважати на такі ключові моменти, Після пандемії зростання дистанційної роботи дозволило працівникам використовувати балансом між роботою та особистим життям і свободою працювати, де завгодно.

У той час як компанії скористалися перевагами зменшення накладних витрат, віддалена робота підняла питання про нові ризики та загрози кібербезпеці, які можуть завдати шкоди їх бізнесу.

Невідповідна безпека даних у сценаріях віддаленої роботи може призвести до витоку даних, коли хакери можуть використовувати вразливості, ставлячи під загрозу конфіденційність даних. Такі порушення можуть мати серйозні наслідки, зокрема атаки програм-вимагачів і репутаційну шкоду.

Щоб вирішити ці проблеми, компанії можуть створювати комплексні політики безпеки даних, забезпечувати постійне навчання з питань безпеки, запроваджувати VPN для безпечної передачі даних, зробити багатофакторну автентифікацію (MFA) обов’язковою та заохочувати використання менеджерів паролів.

Завдяки сповіщенням співробітників у режимі реального часу, автоматичним редагуванням і політикам збереження, а також повній видимості хмарні технології можуть допомогти організаціям виявити та захистити найбільш конфіденційні дані.

Оскільки випадки витоку даних продовжують зростати, лише в березні 2023 року було скомпрометовано 41,9 мільйона записів у всьому світі, вкрай важливо, щоб команди безпеки були готові до віддаленої роботи та нових загроз, які вона може принести.

Виділемо кілька загроз для безпеки даних, коли мова йде про віддалену роботу:

1. Пропущені зв'язки

Працюючи вдома, без товариства в офісі, працівники можуть виявитися зкомпроментованими. Досить легко повідомити всіх про потенційну фішингову атаку, коли всі знаходяться в одному місці, але до того часу, коли ви зможете надіслати потрібне повідомлення людям, які працюють наодинці, може бути надто пізно.

2. Тіньові питання IT

Команди безпеки також можуть не мати повної видимості того, як співробітники використовують конфіденційні дані, де вони зберігаються та чи видаляються дані після використання. Відсутність контролю над конфіденційними даними може призвести до того, що конфіденційна інформація буде розповсюджена в багатьох програмах SaaS, таких як Slack , Google Drive і Jira .

3. Співробітники залишають свої пристрої відкритими в громадських місцях

Віддалена робота може не означати роботу вдома. Ваші співробітники можуть працювати в кав’ярнях, коворкінгах або в будь-якому іншому місці, де вони можуть отримати з’єднання Wi-Fi. Проблема, яка у вас може виникнути тут, більше стосується конфіденційності. Співробітники залишають свої ноутбуки без нагляду, щоб піти випити кави, чи проводять приватні дискусії в громадському місці? Ви повинні повідомити їм, чого очікує компанія з точки зору конфіденційності та безпеки, коли вони працюють поза домом чи офісом.

4. Незахищені мережі

Співробітники, які працюють у громадських місцях, можуть підключатися до незахищених мереж Wi-Fi, що може збільшити ризик перехоплення даних неавторизованими користувачами. Дані, перехоплені між пристроєм вашого

співробітника та мережею компанії, можуть стати золотим пилом для хакера. Наприклад, атаки «людина посередині» можуть бути активовані за допомогою віддаленої роботи, особливо якщо ваші співробітники покладаються на незахищені з'єднання для виконання своєї роботи.

5. Безпека кінцевої точки

Віддалені співробітники можуть використовувати власні пристрої або незахищені пристрої компанії, які можуть бути скомпрометовані, якщо вони не захищені належним чином. Дані, що зберігаються на незахищених пристроях, можуть бути більш сприйнятливими до крадіжки або доступу неавторизованих користувачів до конфіденційних файлів.

6 Проблеми відповідності

Команди безпеки повинні будуть переконатися, що вони дотримуються галузевих норм, таких як HIPAA , GDPR або PCI DSS , незважаючи на домовленості про віддалену роботу. Це може бути важко, оскільки працівники можуть ділитися інформацією більш вільно, ніж вони могли б в офісі, порушуючи вимоги дотримання.

Без справжньої видимості конфіденційних даних організації піддаються більшому ризику витоку чи порушення даних. Наприклад, якщо хакер проник в обліковий запис Google Workspace одного співробітника, він може знайти всі інші дані, які він зможе зберегти, щоб отримати викуп або продати іншим.

Дані надто легко потрапляють у чужі руки, якщо працівники не повністю обізнані з політикою безпеки та набувають поганих звичок, коли йдеться про обробку конфіденційної інформації.

Офіс проти віддаленої роботи: які унікальні виклики для команд безпеки?

Команди безпеки зіткнуться з багатьма проблемами, коли справа доходить до віддаленої роботи, наприклад:

1. Відсутність контролю над пристроями

У той час як раніше корпоративні ноутбуки роздавали в офісі, попередньо ретельно підготувавши службу безпеки, тепер більше співробітників використовують свої особисті пристрої або отримують пристрої, які їм

доставляють безпосередньо. Без встановленого належного програмного забезпечення служби безпеки повинні покладатися на співробітників, які запровадять власні засоби захисту – це нелегке завдання.

Оскільки люди працюють із власних домівок, використовуючи власні з'єднання Wi-Fi, захисну мережу брандмауера компанії також було видалено, наражаючи їх на ризики, з якими в іншому випадку їм не довелося б зіткнутися.

2. Співробітники, які стають жертвами фішингових атак

Без регулярного контакту з фахівцями з безпеки та колегами, які можуть допомогти перевірити, чи є щось законним чи ні, співробітників може бути легше обманом змусити надати конфіденційні дані або завантажити зловмисне програмне забезпечення.

Службі безпеки доведеться наполегливо попрацювати, щоб переконатися, що їхні співробітники правильно ідентифікують фішинговий аферист і не припускатимуть автоматично, що особисту інформацію запитує їх справжній начальник.

3. Труднощі з моніторингом віддалених працівників

Якщо у вас немає відповідних можливостей, може бути важко контролювати, що роблять співробітники та чи дотримуються вони протоколу. Наприклад, вони відкладають важливі оновлення, через які ви могли б їх ознайомити, якби ви були разом в офісі?

Віддалених співробітників необхідно довіряти правильному дотриманню процедур безпеки.

4. Більше хмарних даних

Незахищені хмарні сервіси можуть стати пригодою для витоку даних. З великою кількістю різних пристроїв, які отримують доступ до однієї інформації через багато різних пристроїв, може бути дуже легко дозволити комусь випадково отримати доступ до ваших хмарних даних.

Для фахівців із безпеки важливо мати правильні процеси автентифікації, щоб уберегти зловмисників від рівняння.

Є кілька способів забезпечити дотримання та ефективне управління безпекою, якими служби безпеки можуть переконатися, що їхні співробітники дотримуються їх політики:

1. Створіть комплексну політику безпеки даних

Розробка політики безпеки даних , яка описує інструменти, які будуть використовуватися, і процедури, які ви матимете для захисту своїх даних, означає, що ви можете отримати всіх на одній сторінці. Наприклад, окресліть свою політику збереження та чи є у вас автоматичне редагування, щоб співробітники знали, чого очікувати.

Ви також повинні надати ресурси, які чітко описують політику, щоб співробітники могли швидко та легко знайти потрібну інформацію.

2. Проводьте регулярне навчання з питань безпеки

Щорічного навчання з питань безпеки недостатньо, щоб дати співробітникам гарне уявлення про те, що вони повинні робити, щоб захистити свої конфіденційні дані.

Натомість спробуйте безперервне навчання для навчання працівників (наприклад, сповіщення співробітників у режимі реального часу), яке допоможе їм побачити політику безпеки в дії та в контексті їх ролі.

3. Використовуйте VPN, щоб захистити своє з’єднання

Замість того, щоб ризикувати передаванням даних через незахищені мережі, використовуйте VPN (віртуальні приватні мережі), щоб захистити свої дані, зашифрувавши їх під час передачі. Наявність їх на місці додасть додатковий рівень безпеки, коли мова йде про роботу ваших співробітників з дому.

4. Зробіть MFA (багатофакторну автентифікацію) обов’язковою

Багатофакторна автентифікація означає, що ви не покладаєтеся лише на паролі, коли справа доходить до входу, що ускладнює доступ хакерам до ваших конфіденційних даних.

Якщо це ще не є обов’язковим у вашому бізнесі, було б гарною ідеєю встановити це на місце, щоб, якщо ваші співробітники використовують слабкі

паролі, ви могли бути спокійні, знаючи, що існує додатковий рівень безпеки, який потрібно пройти.

5. Використовуйте менеджери паролів

65% співробітників «просто запам’ятовують» свій пароль, показуючи, що пароль, швидше за все, використовувався ними на кількох платформах і його легко запам’ятати. Ці паролі зазвичай слабкі, оскільки вони коротші та містять справжні слова. Зрештою, хто запам’ятає випадковий рядок цифр і цифр із 16 символів, які лежать у голові?

Менеджери паролів можуть сприяти розвитку хороших звичок, зберігаючи складні та унікальні паролі для багатьох різних платформ.

Отже, для захисту віддалених користувачів, необхідно використовувати технологію, яка зможе комплексно управляти віддаленими користувачіами, які будуть відповідати політиці безпеки організації.

1.4. Аналіз технологій захисту віддалених користувачів на основі Endpoint Protection

Захист віддалених користувачів найкраще проводити застосовуючи технології Endpoint Protection від провідних постачальників послуг. Для порівняння будуть використовуватись технології кращих провайдерів, які видзначив Gartner у своєму дослідженні [7].

Отже, рішення, які будуть порівнюватись є:

SentinelOne;

CrowdStrike;

Microsoft;

Софос;

Trend Micro;

Palo Alto Networks;

Bitdefender;

Фортінет;

Cisco Systems.

Оцінюючи різні рішення, будемо порівнювати компетенції в таких категоріях, як оцінка та укладення контрактів, інтеграція та розгортання, обслуговування та підтримка, а також конкретні можливості продукту.

Для аналізу використовуються, підтверджені значення Gartner, щоб дізнатися, наскільки SentinelOne порівнює своїх конкурентів, і знайти найкраще програмне забезпечення чи послугу для вашої організації.

Crowdstrike Falcon забезпечує видимість у режимі реального часу під час виявлення загроз, його можливості швидкого реагування допомагають вживати ефективних заходів проти цих загроз, а його всебічна розвідка про загрози допомагає забезпечити глибоке розуміння загроз. Легкий агент працює ефективно Він також постійно відстежує дії кінцевих точок і використовує алгоритми машинного навчання для виявлення та блокування цих зловмисних дій, обробляючи дані про загрози в режимі реального часу, забезпечуючи негайне їх виявлення та реагування на них Він забезпечує централізоване керування та видимість для всіх кінцевих точок у великих організаціях. Він ефективно працює з інтеграцією аналізу загроз, включаючи безперервний збір та аналіз даних із різних глобальних джерел, з яких falcon надає ефективну інформацію організаціям, щоб тримати середовище попереду. нові загрози » .

Microsoft Defender for Endpoint рішення яке має потужні можливості машинного навчання та гарантують, що віно виявляє та блокує складні атаки, перш ніж вони можуть завдати будь-якої шкоди. Він також має можливість виявлення кінцевої точки та реагування, що дозволяє користувачеві швидко досліджувати будь-які випадки безпеки та реагувати на них. Крім того, він надає дуже детальну інформацію про графік будь-якої атаки.

Використання рішення Sophos Intercept як антивірусного рішення – чудовий рішення для організацій. Воно дозволяє захистити кінцеві точки організації від зовнішніх загроз і атак зловмисного програмного забезпечення. перехід від існуючих рішень до Sophos також є плавним і завершеним у заплановані терміни

без впливу на продуктивність. Рішення дозволяє отримувати звіти, наданими на інформаційній панелі Sophos.

Palo Alto Networks Cortex XDR забезпечує повну видимість безпеки нашої організації в кінцевих точках і мережах. Cortex XDR постійно виявляє та зупиняє складні атаки загроз, а також адаптує механізми захисту для запобігання майбутнім атакам. Cortex XDR дуже корисний, оскільки він оптимізує наші операції безпеки.

Bitdefender. Налаштування продукту легкт: хмарна консоль дозволила негайно розпочати розгортання агентів. Документація містить багато корисної інформації та добре організована. На етапі налаштування було виявлено дуже мало хибних спрацьовувань, і завдяки функціям звітування та експорту є можливість дуже швидко їх визначити та вирішити, додавши кілька виключень.

Cisco Systems поєднує поведінкову аналітику та штучний інтелект, щоб зупинити загрози від компрометації наших кінцевих точок. Це спрощує розслідування, і є можливість ідентифікації атаки в реальному часі для швидшого виявлення загроз.

SentinelOne користується великою повагою в індустрії мережевої безпеки за високий рівень забезпечення кінцевої точки. Ось кілька ключових точок зору, які можна виділити:

1. Простота використання: етап відомий інсталювання взаємодії та простота використання робить його доступним як для маленьких, так і для великих організацій.

2. Розширене виявлення небезпеки: SentinelOne використовує симуляцію інтелекту та ШІ для поступового визначення небезпек і відповіді на них

3. Автоматизація: роботизовані можливості реагування, включаючи відокремлення заражених пристроїв і відновлення, навчені для зменшення ваги в групах IT і прискорення часу реакції на загрозу.

4. Продуктивність: Користувачі часто визнають незначний вплив на виконання фреймворку, що дає змогу працювати успішно, не звертаючись до гаджетів.

5. Підтримка та спільнота: клієнтська служба Sentinel Ones і локальні активи зазвичай користуються повагою, надаючи своєчасну допомогу та важливий досвід для оптимізації роботи.

При прийнятті рішення про використеання будь-якого програмного забезпечення чи послуги важливу роль відіграють кілька факторів. Для компаній вибір продукту безпеки кінцевої точки стає дуже складним, оскільки від цього аспекту залежить майбутнє стану безпеки організації. Тому проведемо порівняння п’яти найкращих продуктів безпеки кінцевих точок, які допоможуть захистити віддалених користувачів інформаційної системи організації.

Таблиця 1.1.

Порівняння рішень безпеки кінцевих точок

Продукт	Ключові характеристики	Ціноутворення	Безкоштовна пробна версія	Рейтинги (G2, Gartner, Peerspot, Capterra)
SentinelOne	Виявлення загроз на основі штучного інтелекту, автономне реагування, хмарна архітектура, централізоване керування, зручний інтерфейс	За запитом	так	• G2: 4,7/5 • Gartner: 4,7/5 • Peerspot: 4,4/5 • Capterra: 4,8/5
CrowdStrike Falcon	Хмарна платформа, розвідка загроз у реальному часі, поведінкова аналітика	Від 99,99 доларів США/пристрій/рік	так	• G2: 4,7/5 • Gartner: 4,8/5 • Peerspot: 4,6/5 • Capterra: 4,7/5

Symantec Endpoint Security	Розширене машинне навчання, виявлення кінцевих точок і відповідь (EDR), інтегрований кіберзахист	Індивідуальне ціноутворення для підприємств	так	• G2: 4,4/5 • Gartner: 4,3/5 • Peerspot: 4./5 • Capterra: 4,4/5
Microsoft Defender для кінцевої точки	Хмарний захист, керування загрозами та вразливістю, автоматизоване розслідування та виправлення	Зв'яжіться з нами для ціноутворення	так	• G2: 4,4/5 • Gartner: 4,5/5 • Peerspot: 4,0/5 • Capterra: 4,6/5
Trend Micro Vision One	Безпека XGen™, підключений захист від загроз, віртуальне оновлення	Індивідуальне ціноутворення для підприємств	так	• G2: 4,7/5 • Gartner Peer Insights: 4,7/5 • Peerspot: 4,0/5 • Capterra: 4,4/5

SentinelOne пропонує захист кінцевих точок нового покоління за допомогою штучного інтелекту та машинного навчання для захисту ноутбуків, настільних ПК і мобільних пристроїв. Він забезпечить автоматичне запобігання, виявлення та реагування на широкий спектр кіберзагроз, забезпечуючи захист для кожної кінцевої точки організації.

Ключові характеристики SentinelOne [7]:

Виявлення та реагування на загрози на основі штучного інтелекту: він використовує машинне навчання для визначення та видалення загроз кінцевих точок у режимі реального часу, незалежно від того, чи це програми-вимагачі, чи

атаки нульового дня. Це миттєво розпізнає зловмисне програмне забезпечення, щоб мінімізувати ризик злому до того, як може бути завдано значної шкоди [7].

Автономна реакція кінцевої точки: Singularity™ Cloud Security негайно автоматизує реакцію на загрозу кінцевої точки шляхом стримування та усунення атак за лічені секунди без участі людини. Він зменшує час відповіді, оскільки містить атаку, щоб зменшити поверхню атаки, таким чином мінімізуючи вплив, який може мати атака. Це дає змогу групам безпеки зосередитися на діяльності вищого рівня, а не на ручному управлінні інцидентами [7].

Централізоване керування кінцевими точками: забезпечує єдину консоль для керування безпекою всіх кінцевих точок, за допомогою якої адміністратори можуть бачити стан пристроїв, застосовувати політики безпеки та переглядати звіти з однієї інформаційної панелі. Це спрощує керування кінцевими точками як у хмарі, так і в локальному середовищі [7].

Безпека робочого навантаження в хмарі: Singularity™ пропонує безпеку робочого навантаження в хмарі, поширюючи захист на кінцеві точки, які взаємодіють з хмарою. Захист кінцевих точок від загроз програм-вимагачів, безфайлових атак і атак нульового дня захищає всі ваші кінцеві точки в хмарі та локально від загроз нового покоління.

Безпека даних кінцевої точки: Платформа Singularity™ пропонує безпеку даних, керовану штучним інтелектом, щоб захистити дані кінцевої точки від таких загроз, як зловмисне програмне забезпечення та несанкціонований доступ. Таким чином, автоматизація, карантин і шифрування шкідливих файлів захищають конфіденційні дані на всіх підключених пристроях [7].

Основні проблеми, які SentinelOne усуває:

Загрози нульового дня: SentinelOne, керуючись своїм підходом на основі штучного інтелекту, також має можливість виявляти та нейтралізувати раніше невідомі загрози проти організацій, які можуть мати слабкі місця у вразливостях нульового дня [7].

Стримування загроз вручну: SentinelOne автоматизує виявлення та усунення загроз, звільняючи команду безпеки для роботи над стратегічними ініціативами замість того, щоб витрачати час на втручання вручну.

Уніфіковане керування безпекою : уніфікована консоль значно спрощує операції безпеки. Це зменшує складність, пов’язану з відстеженням кількох різних інструментів безпеки, і загалом підвищує ефективність.

Обмежена видимість: забезпечує глибоку видимість діяльності кінцевих точок і, таким чином, дає змогу організації зрозуміти та виправити всі потенційні прогалини в безпеці в мережі.

Проаналізувавши рішення (таблю1.1) та отримавши відгуки від фахівців з кібербезпеки (Рис.1.3), можна відзначити, що кращим вибором рішення захисту віддалених користувачів інформаційної системи Endpoint Protection є Sentinel Ones.

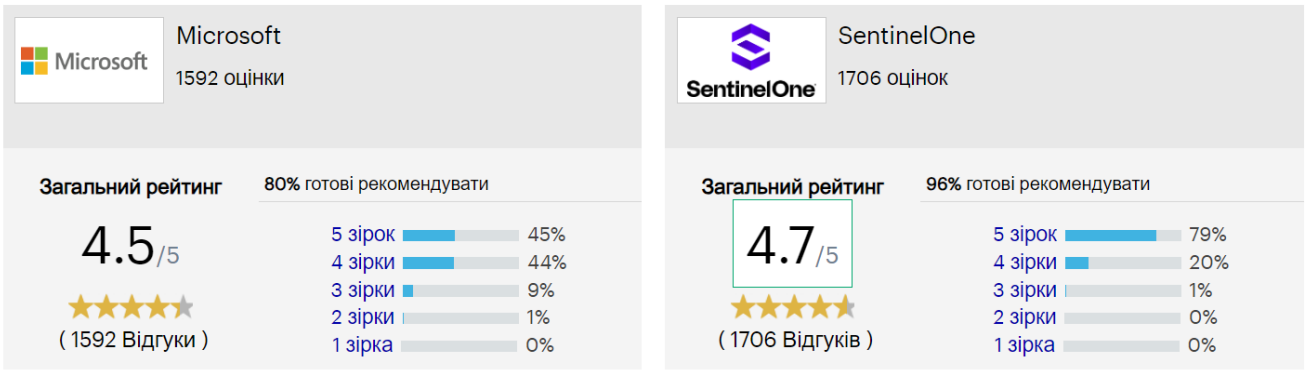

Рис.1.3. Порівняння рішень класу Endpoint Protection [7]

Отже, для розробки варіанту захисту віддалених користувачів інформаційної системи організації буде використовуватись рішення Sentinel Ones.

2 МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

2.1. Архітектура Sentinel Ones Endpoint Protection

Кінцеві точки стосуються різних пристроїв, підключених до мережі організації, наприклад ноутбуків, смартфонів і серверів. Архітектура безпеки кінцевих точок спрямована на захист цих кінцевих точок. Зазвичай це перша стіна безпеки, яку зловмисник повинен зламати, щоб проникнути всередину.

Зі змінами в технології також відбулися зміни в природі безпеки кінцевих точок. Був час, коли традиційне антивірусне програмне забезпечення вважалося найвищим рівнем безпеки для настільних ПК. Але з часом у системах знайшли набагато досконаліші рішення безпеки. Кінцеві точки містять не лише настільні комп’ютери, а й мобільні телефони, пристрої IoT і хмарні системи. Таким чином, для компаній важливо мати кращі рішення безпеки кінцевих точок, які важко зламати зловмисникам.

У цьому розділі дослідимо, що таке архітектура безпеки кінцевих точок і як вона захищає кінцеві точки.

Архітектура безпеки кінцевих точок — це структура, яка допомагає організаціям захистити свої кінцеві точки від будь-яких видів кібератак, які можуть призвести до порушень безпеки. Щоб забезпечити безпеку кінцевих точок, архітектура безпеки кінцевих точок повинна складатися з різних типів стратегій, технологій, політик і процесів, які мають бути реалізовані. Запропонована архітектура безпеки кінцевих точок вважається успішною лише тоді, коли вона може забезпечити активний підхід до захисту кінцевих точок, на які зловмисникам найлегше націлити.

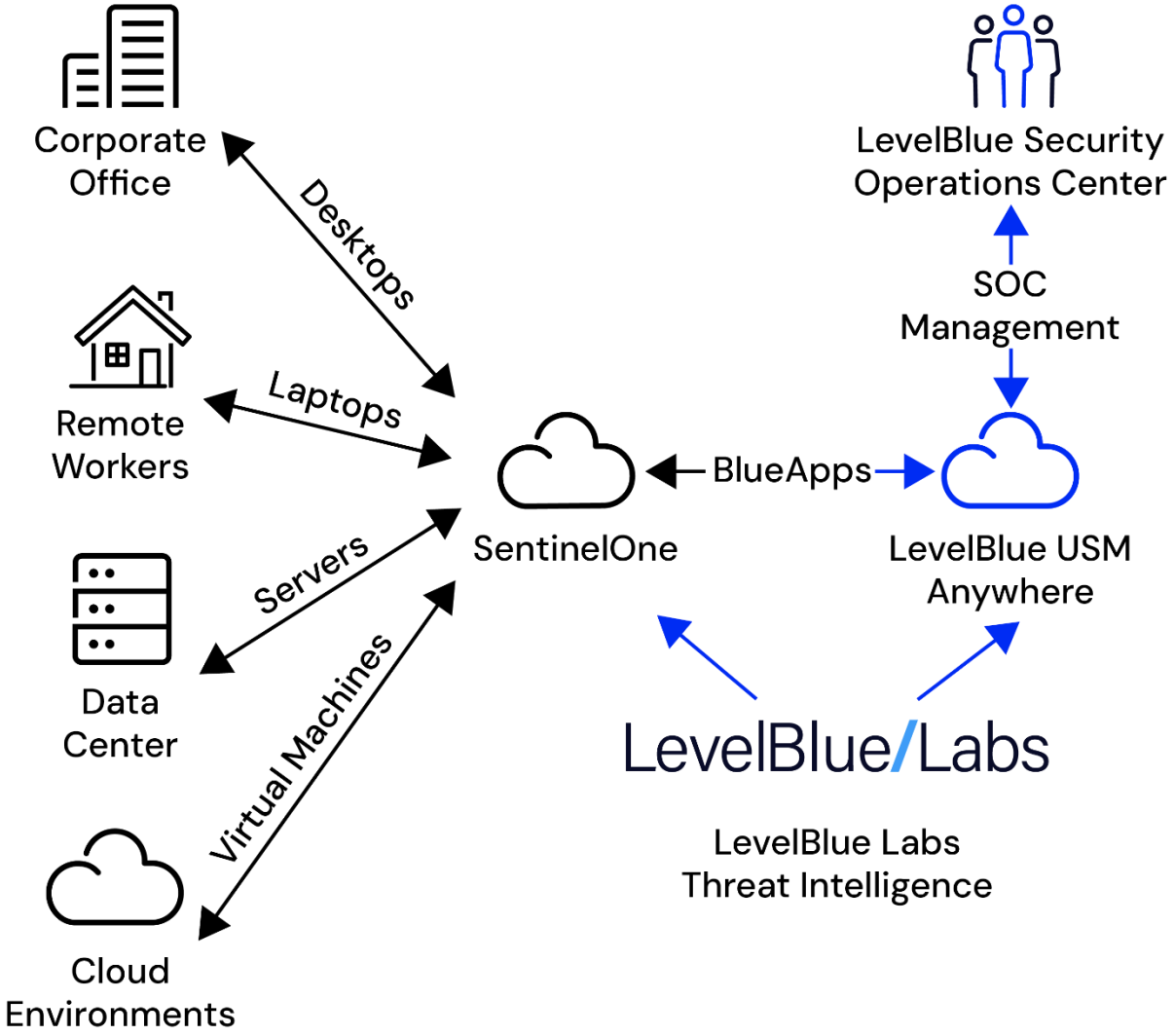

Рис. 2.1. Архітектура безпеки кінцевих точок Sentinel Ones

Архітектура безпеки кінцевих точок містить кілька рівнів безпеки, що гарантує, що кожен рівень може допомогти подолати різні вразливості кінцевих точок. Ці рівні складаються з рішень для захисту від вірусів і зловмисного програмного забезпечення, брандмауерів, систем виявлення та запобігання вторгненням (IDS і IPS), засобів запобігання втраті даних (DLP) і виявлення кінцевих точок і відповіді (EDR) для захисту кінцевих точок.

Ця архітектура має бути на крок попереду зловмисника, реалізуючи керування політикою, автентифікацію користувачів і контроль доступу. Ці кроки гарантують, що лише авторизований користувач і пристрої мають доступ для підключення до мережі. Він також включає методи шифрування та дистанційне

стирання втрачених або викрадених пристроїв. Щоб керувати всім цим в одному місці, надається централізована консоль керування для моніторингу та керування всіма кінцевими точками в організації.

2.2. Компоненти архітектури безпеки кінцевої точки

Сьогодні багаторівнева безпека є єдиним рішенням для складних атак зловмисників. Архітектура безпеки кінцевої точки забезпечує кілька рівнів безпеки, гарантуючи, що кожен рівень допомагає організаціям захистити кінцеву точку від різних видів загроз.

Нижче наведено різні компоненти, які забезпечують роботу архітектури безпеки кінцевої точки.

Платформи захисту кінцевих точок (EPP)

Це основний компонент архітектури безпеки кінцевої точки. EPP поєднує в собі потужність антивірусів, захисту від зловмисного програмного забезпечення, шифрування даних і брандмауерів для забезпечення безпеки. EPP використовує виявлення на основі сигнатур і машинне навчання, щоб блокувати загрози, перш ніж вони використають будь-яку вразливість кінцевої точки.

Виявлення кінцевої точки та відповідь (EDR)

EDR працює разом з EPP, виявляючи загрози та вказуючи, як діяти після виявлення загрози. EDR допомагає контролювати кінцеві точки та мережевий трафік, що входить і виходить з кінцевої точки. Потім EDR проводить аналіз поведінки, щоб виявити будь-яку підозрілу поведінку, і надає сповіщення в режимі реального часу, коли виявляється будь-яка проблема. Це допомагає групі безпеки швидко дослідити проблему та зупинити поширення загрози.

Запобігання втраті даних (DLP)

Цей компонент допомагає організації захистити свою конфіденційну інформацію від витоку даних, пошкодження та викрадання. Рішення DLP відстежують дані, щоб виявляти та блокувати передачу конфіденційних даних через кінцеві точки, мережі та хмарні служби. Вони використовують алгоритми

зіставлення шаблонів для ідентифікації та захисту будь-якої конфіденційної інформації. Це допомагає організаціям дотримуватися законів про захист даних.

Захист на рівні мережі

Цей рівень допомагає переконатися, що зв'язок між кінцевими точками та мережею безпечний. Він використовує брандмауери, системи виявлення та запобігання вторгненням (IDS/IPS) і захищені веб-шлюзи. Мережевий захист забезпечує виконання політик безпеки та допомагає стримувати загрозу, якщо вона виникає в одній кінцевій точці, від поширення по мережі.

2.3. Ключові аспекти архітектури безпеки кінцевої точки Sentinel Ones

Для організацій важливо розуміти важливість архітектури безпеки кінцевих точок для захисту від будь-яких загроз, які можуть виникнути на кінцевих точках.

1. Комплексне запобігання загрозам

Важливо, щоб архітектура безпеки кінцевої точки була багаторівневою, щоб вона могла захистити організації від різних типів кіберзагроз. Для цього в архітектурі безпеки кінцевої точки використовуються різні компоненти, такі як EPP, EDR і засоби захисту на рівні мережі. Ці компоненти захищають організації від зловмисного програмного забезпечення, експлойтів нульового дня та атак без файлів. Це допомагає зменшити ризик порушення безпеки.

2. Покращена видимість і контроль

Архітектура безпеки кінцевої точки допомагає забезпечити повну видимість на всіх пристроях у мережі організації. Це допомагає групам безпеки відстежувати кожну активність, яка відбувається з кінцевою точкою, щоб будь-які аномалії були негайно виявлені та усунені. За допомогою централізованої консолі можна примусово застосовувати всі політики безпеки, а також надсилати оновлення, коли вони надходять раз і назавжди, безпосередньо на всі кінцеві точки.

3. Адаптивний захист від загроз, що розвиваються

Середовище кібербезпеки дуже динамічне, оскільки зловмисники винаходять нові підходи, щоб обійти традиційні заходи безпеки. Архітектура безпеки кінцевої

точки є адаптивною та гнучкою. Така гнучка конструкція дозволяє інтегрувати нові технології, методи або механізми захисту. Крім того, сучасні рішення безпеки кінцевих точок також використовують штучний інтелект і машинне навчання, що означає, що система безпеки вивчає нові шаблони атак і, таким чином, коригує заходи безпеки, роблячи кібербезпеку організації набагато більш динамічною та проактивною.

4. Відповідність і захист даних

Організації повинні дотримуватися законів про захист даних. Архітектура безпеки кінцевої точки гарантує, що організації зможуть це зробити. Він реалізує засоби запобігання втраті даних (DLP) і засоби шифрування для захисту даних у стані спокою та під час передачі. Це гарантує відповідність організацій вимогам. Однак це також дає організаціям можливість перевіряти моделі використання даних і зменшувати ризик неправильного використання даних або їх втрати.

5. Підтримка сучасних робочих середовищ

Сьогодні, коли все більше підприємств і роботи працюють віддалено. Сучасні організації повинні впроваджувати сучасні рішення для архітектури безпеки кінцевих точок, щоб забезпечити гнучкість і в той же час дотримуватися основних стандартів безпеки. Це не повинно залежати від розташування кінцевої точки, але захищати кожну кінцеву точку будь-якого пристрою в будь-якому місці.

Розглянемо основні особливості безпеки керованої точки корпоративного рівня у вигляді в таблиці 2.2.

Таблиця 2.2.

Безпека керованої кінцевої точки корпоративного рівня

Особливості	Опис
Автономний агент кінцевої точки	Кінцеві точки посилені захистом від несанкціонованого доступу та запатентованими алгоритмами штучного інтелекту, які живуть на пристроях, відловлюючи зловмисну активність у режимі реального часу, а також

	автономно вживаючи заходів для відновлення, щоб підтримувати кінцеві точки в постійному чистому стані
Відповідь і відкат	Можливості SentinelOne поширюються не тільки на захист, але й на автономні реакції. Завдяки автоматичному відображенню та відстеженню активності всіх кінцевих точок платформа вживає чітких дій, щоб реагувати, виправляти та навіть повертати активність до попередніх безпечних станів.
Виявлення та контроль IoT	Виявлення шахрайських пристроїв і пристроїв Інтернету речей у мережі отримує ще більше переваг від кібербезпеки кінцевих точок. Виявляє та сегментує активи, щоб забезпечити захист, відповідно вимогам і заходам контролю – без додаткового програмного забезпечення, мережевого обладнання та консолей.
Хмарний захист	Допомагає захистити робочі навантаження хмарних і динамічних контейнерів у AWS і Azure, включаючи повну підтримку Kubernetes і Docker.
Цілодобова команда SOC	Моніторинг, керування та підтримка безпеки кінцевих точок, включаючи активний пошук загроз, цифрова криміналістика та постійне дослідження, сортування та реагування на загрози.
Надання високоякісних послуг	Забезпечує налаштування політики, план реагування на інциденти (IRP), поточне налаштування системи та навчання на платформі.
Глибока інтеграція	Покращене виявлення та реагування завдяки інтеграції платформи та LevelBlue Labs Threat Intelligence та Open Threat Exchange (OTX).

При впровадження архітектури безпеки кінцевих точок треба звернути на основні проблеми інформаційних систем організації для успішної реалізації технології захисту віддалених користувачів ІС. До таких проблем відноситься:

1. Віддалена робота та BYOD

Політика дистанційної роботи та використання власного пристрою стає все більш популярною за останні кілька років. Однак ці політики призводять до збільшення поверхні атаки організації. Кінцеві точки майже завжди скомпрометовані, тому що люди використовують свої пристрої вдома або в загальнодоступному Wi-Fi, що робить ці кінцеві точки дуже незахищеними. Команди безпеки відповідають за безпеку цих віддалених кінцевих точок. Ці пристрої мають відповідати тим самим стандартам і політикам, що й їхні локальні кінцеві точки.

2. Витончені загрози

Складні загрози стосуються того, що зловмисники створюють дуже складні методи. Вони включають розширені постійні загрози, використання безфайлового зловмисного програмного забезпечення або експлойтів нульового дня, відомих тим, що порушують традиційні заходи безпеки. Тому ще одним заходом безпеки, який необхідно вжити організаціям, є вивчення та впровадження нових методів.

3. Відповідність і нормативні вимоги

Деякі галузі, як-от охорона здоров’я, мають дотримуватися певних суворих правил і норм, як-от GDPR, HIPAA або PCI DSS. Організації повинні створити архітектуру безпеки кінцевої точки таким чином, щоб вона могла задовольнити ці вимоги відповідності. Вони також повинні переконатися, що існує правильний баланс між потребами безпеки та правилами, оскільки для цього часто потрібні додаткові ресурси та досвід.

4. Вразливості застарілої системи

Є ще деякі організації, які не перейшли від застарілих систем. Таким організаціям стає важко інтегрувати сучасні рішення безпеки кінцевих точок у свої системи. Застарілі системи містять уразливості, які важко видалити без оновлення

системи. Таким чином, реалізація архітектури безпеки кінцевих точок без зміни їх функціональності стає дещо складною.

5. Обмеження ресурсів

Це вимагає фінансових і людських ресурсів для впровадження архітектури безпеки кінцевої точки. Від організацій вимагається інвестувати в кращі рішення безпеки та або навчати наявний персонал, або залучати нових кваліфікованих співробітників.

Основні функції SentinelOne, які допомагають організаціям забезпечити безпеку віддалених користуачів включають в себе:

Автономний захист на основі ШІ

SentinelOne використовує ШІ та машинне навчання для забезпечення безпеки. Він використовує поведінковий штучний інтелект для виявлення загроз, що робить його вільним від людських помилок. ШІ має унікальну здатність, яка продовжує вивчати нові шаблони атак, що також допомагає забезпечити захист від невідомих загроз. SentinelOne також пропонує автоматичне реагування на загрози за допомогою ШІ.

Можливості EDR

Платформа SentinelOne надає можливості виявлення та реагування кінцевих точок (EDR) для кращого захисту кінцевих точок. Це допомагає організаціям мати повну видимість діяльності на кінцевій точці. EDR надає детальний судовий звіт про атаку, що містить усю інформацію, як-от місце виникнення атаки, як вона поширилася та вплив атаки на кінцеву точку. SentinelOne EDR також забезпечує автоматичні реакції, такі як ізоляція мережі та відкат шкідливих змін.

Хмарна рідна архітектура

Хмарна архітектура SentinelOne забезпечує легке розгортання та керування захистом кінцевої точки. Цей підхід також допомагає організаціям вирішувати потреби в масштабованості. Хмарна архітектура підтримує віддалену роботу, забезпечуючи захист незалежно від розташування кінцевої точки.

Отже, архітектура безпеки кінцевої точки є важливою для кібербезпеки інформаційної системи організації. Існують різні компоненти безпеки кінцевих

точок, такі як платформи захисту кінцевих точок (EPP) і системи виявлення та реагування на кінцеві точки (EDR). Однак існують певні проблеми, з якими організація може зіткнутися під час впровадження безпеки кінцевих точок, наприклад зростання віддаленої роботи та постійна загроза кібератак. Щоб переконатися, що архітектура безпеки кінцевої точки є ефективною, організації повинні впроваджувати найкращі практики, такі як навчання користувачів, регулярне встановлення виправлень і впровадження архітектур нульової довіри .

3 ТЕХНОЛОГІЯ ЗАХИСТУ ВІДДАЛЕНИХ КОРИСТУВАЧІВ

3.1 Технологія захисту віддалених користувачів на прикладі Sentinel Ones Endpoint Protection

Платформа Singularity SentinelOne розширює можливості SOC та IT-операцій, надає більш ефективний спосіб захисту інформаційних систем від сучасних складних загроз.

SentinelOne Singularity об’єднує та розширює можливості виявлення та реагування на багато рівнів безпеки, включаючи кінцеву точку, хмару, ідентифікацію, мережу та мобільний зв’язок, що забезпечує безпеку команди з централізованою наскрізною корпоративною видимістю, потужною аналітикою та автоматизованими відповідями у великому перетині технологічного стека.

Управління агентами Sentinel здійснюється за допомогою глобально доступної багатокористувацької консолі SaaS, яка простою у використанні та має гнучке керування. [8, 9]

Для впровадження віддаленого доступу до інформаційної системи організації буде використано архітектуру безпеки на основі якої буде створено технологію, яка забезпечить захист віддаленого доступу від сучасних атак відповідно до вимог захисту конфіденційної інформації, GDRP та іншим нормативно-правовим актам.

Для впровадження технології, необхідно визначитись з платформою, яку буде обрано в залежності від розміру організації. На рис.3.1. показано які платформи пропонує Sentinel Ones Endpoint Protection та які функції вона буде виконувати. Чим складніші задачі буде виконувати платформа для захисту інформаційної системи організації – тим більше функцій вона буде виконувати. Тому важливим етапом для початку впровадження технології захисту віддаленого доступу користувачів буде визначення основних функцій захисту, які необхідні організації.

Рис 3.1. Платформа Singularity SentinelOne [9]

Singularity Complete

Singularity Complete забезпечує найкращі у своєму класі можливості EPP і EDR на одній платформі, консолі керування та агенті. Singularity Complete, розроблений для організацій, використовує технологію для масштабованої системи запобігання, виявлення та реагування на інциденти на корпоративному рівні, у поєднанні з користувальницькою автоматизацією, дозволяє командам безпеки легко ідентифікувати та захищати кожну кінцеву точку користувача в їхній мережі.

Забезпечує повна видимість як безпечних, так і шкідливих даних;

Надає варіанти збереження даних для будь-яких потреб, можливість оновлення до 3 років;

Використовує техніку MITRE ATT&CK;

Визначає сюжетні лінії як загрози для примусового виконання функціями EPP;

Використовує спеціальні виявлення та автоматичні правила полювання за допомогою Storyline Active Response (STAR™);

Має вбудовані сценарії збору даних для покращення видимості та розслідування інцидентів;

Застосовується хронологія.

Singularity Core

Singularity Core є основою всіх пропозицій захисту кінцевих точок SentinelOne для заміни застарілих AV або NGAV більш ефективним і простим у керуванні EPP. Core містить статичний і поведінковий механізми ШІ для виявлення широкого спектру атак. Автономний агент Sentinel застосовує захист і виявлення безпосередньо на кінцевій точці, з підключенням до хмари чи без нього.

Singularity Control

Singularity Control пропонує найкращий захист кінцевих точок у поєднанні з функціями «набору безпеки» для керування кінцевими точками. Керування включає всі основні функції, а також: керування брандмауером для контролю мережевого підключення до/з пристроїв, включаючи інформацію про місцезнаходження. Контроль пристроїв USB і периферійних пристроїв Bluetooth/BLE. Управління вразливістю та інвентаризація додатків, щоб надати інформацію про програми сторонніх розробників із відомими вразливими місцями, зіставлені з базою даних MITER ATT&CK CVE.

На рис.3.2. зображено технологію, яка є основою для організації захисту віддалених користувачів і представляє собою узагальнену схему порядку розгортання Sentinel Ones Endpoint Protection.

Кількість кінцевих точок зростає завдяки таким факторам, як широке впровадження моделей віддаленої та гібридної роботи та політики Bring Your Own

Device (BYOD). Збільшення кількості точок входу в мережу створює більше можливостей для вразливостей, оскільки персональні пристрої, які використовуються в сценаріях BYOD, часто не мають конфігурацій безпеки, які мають внутрішні офісні пристрої. Ця різниця в стандартах безпеки спонукає компанії застосовувати захист кінцевих точок підприємства для функцій безпеки, які захищають усі пристрої в мережі. Ці функції часто включають засоби запобігання загрозам, такі як антивірусне програмне забезпечення та програмне забезпечення для захисту від шкідливих програм, а також захист брандмауером для сканування та активного блокування шкідливого коду.

У корпоративних умовах кінцеві точки можуть включати різні обчислювальні пристрої, які виконують такі функції, як зв'язок, обробка даних і віддалений доступ. Ці кінцеві точки включають традиційні елементи, такі як настільні комп'ютери та ноутбуки, мобільні пристрої, сервери або пристрої Інтернету речей (IoT). Але в той же час їх використання створює ризики для безпеки. Найпоширеніші типи кінцевих точок включають:

Настільні комп'ютери та ноутбуки. Настільні комп'ютери та ноутбуки вразливі до зловмисного програмного забезпечення, програм-вимагачів, фішингових електронних листів і несанкціонованого доступу, часто через уразливості системи безпеки або соціальну інженерію. Зламаний пристрій може призвести до витоку даних, а також надати зловмисникам доступ до великої мережі, що означає, що бізнес-операції порушуються, а гроші втрачаються.

Мобільні пристрої: мобільні пристрої стикаються з такими загрозами, як зловмисне програмне забезпечення, фішингові повідомлення, а також незахищені мережеві з'єднання. Зламаний мобільний пристрій може розкрити конфіденційні корпоративні дані або потрапити на несанкціоновані ресурси на рівні компанії. Це призведе до витоку даних, часткових порушень відповідності з боку державних і приватних організацій і навіть призведе до збою всієї мережі.

Сервери: Сервери, можливо, вразливі до таких атак, як DDoS-атаки, віруси-вимагачі та злом оборотної проникнення. Пошкоджений сервер може поширювати втрату даних і простої програм, а також розкривати важливу бізнес-інформацію

назовні, що, ймовірно, призведе до блокування будь-якої бізнес-активності, завдаючи значної фінансової шкоди.

Рис. 3.2. Технологія захисту віддаленого доступу користувачів інформаційної системи

Пристрої Інтернету речей (IoT): пристрої в IoT можна легко зламати, оскільки вони часто не мають надійного захисту та не можуть протистояти атаці ботнету. Експлойти через налаштування за замовчуванням або застарілу мікропрограму можуть становити загрозу безпеці пристрою. За допомогою таких скомпрометованих пристроїв зловмисники можуть отримати доступ до критично важливих систем і порушити роботу, наприклад, системи контролю середовища/безпеки.

Принтери та сканери: у скомпрометованому стані файли принтерів і сканерів можуть бути перехоплені дистанційно, забезпечуючи доступ до мереж для атаки. Вони можуть призвести до витоку даних і розповсюдження зловмисного програмного забезпечення в багатьох системах, викликаючи масові проблеми з роботою.

Системи торгових точок (POS): системи POS є фінансово цільовими та часто використовуються для зберігання даних карток. Якщо ця інформація скомпрометована, це може призвести до фінансового шахрайства, а також наразити організацію на юридичну відповідальність і штрафи та завдати шкоди її суспільній репутації.

Після встановлення платформи Sentinel Ones Endpoint Protection адміністратор системи переходить у вікно Dashboard де показані основні вкладки щодо виявлення та налаштування кінцевих точок організації(Рис.3.3).

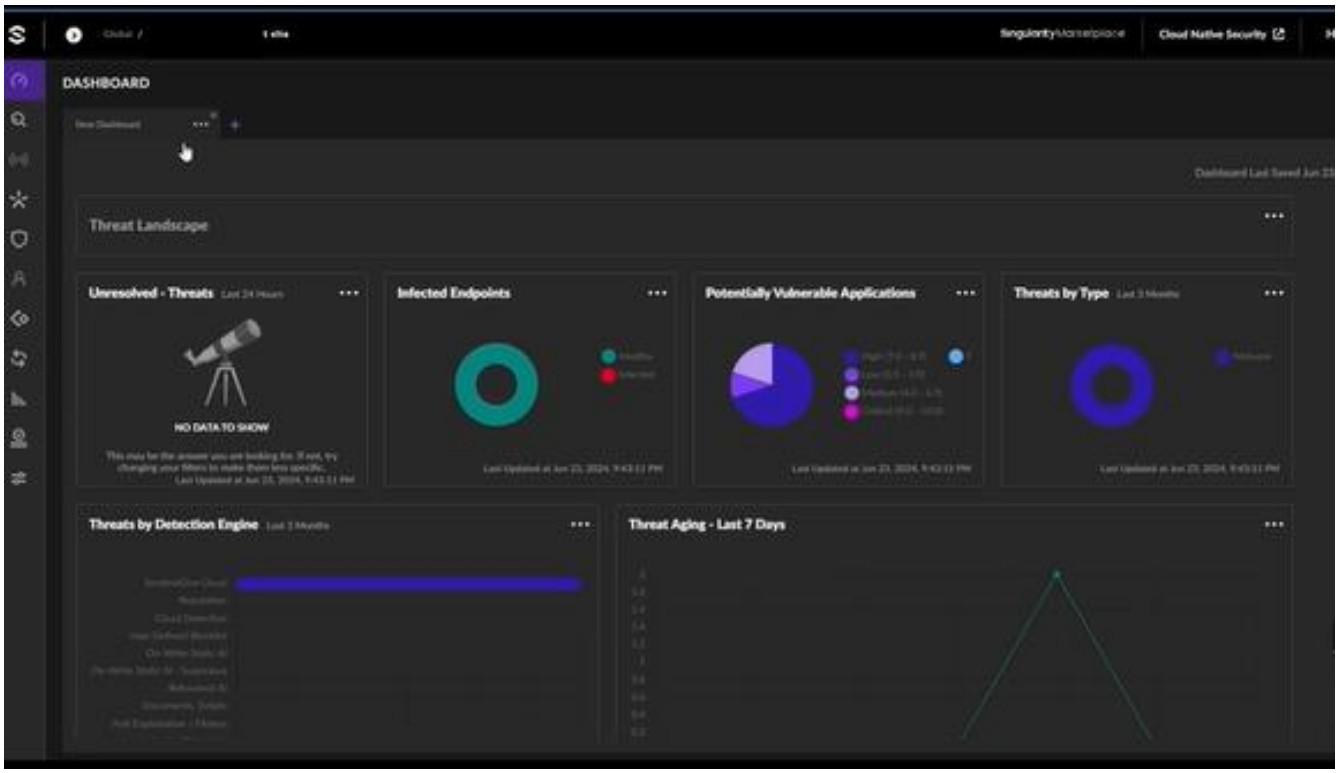

Рис.3.3. Вікно Dashboard

Однією з основних вкладок є вкладка Endpoint – де відбувається виявлення та підключення кінцевих точок(рис.3.4). На цій вкладці можна отримати всю інформацію кінцевої точки, яка підключена до інформаційної системи організації.

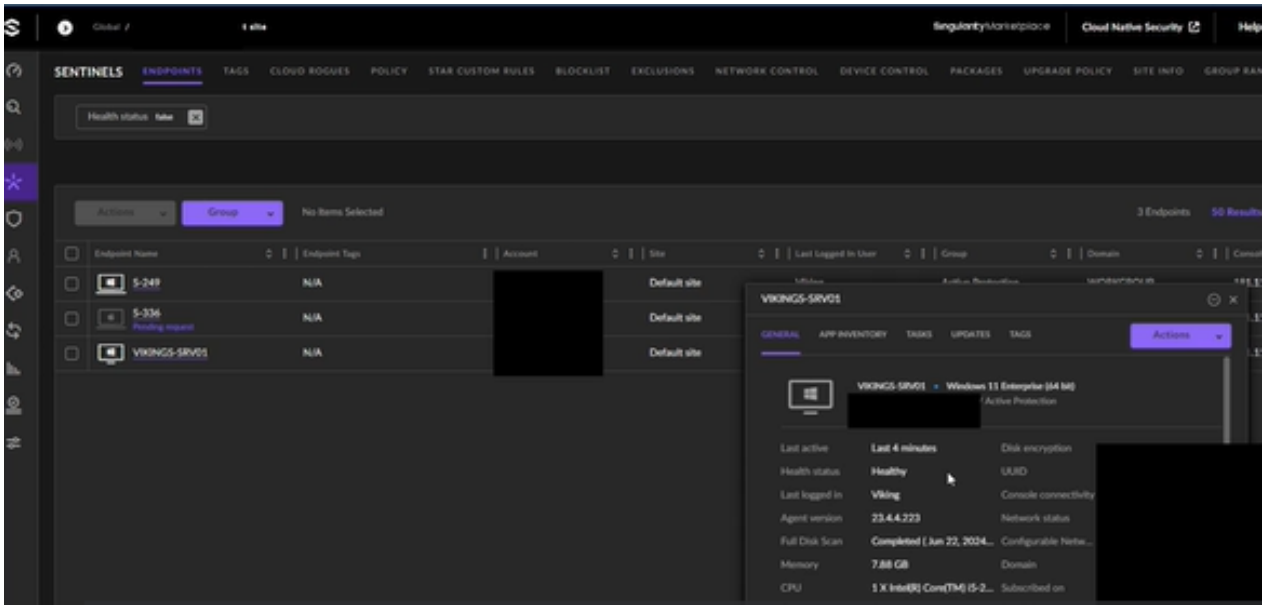

Рис.3.4. Вікно Endpoint

Наступним етапом після підключення кінцевої точки є вкладка Device control, яка відстежує місцезнаходження девайсу та контролює підключення до ІС (3.5).

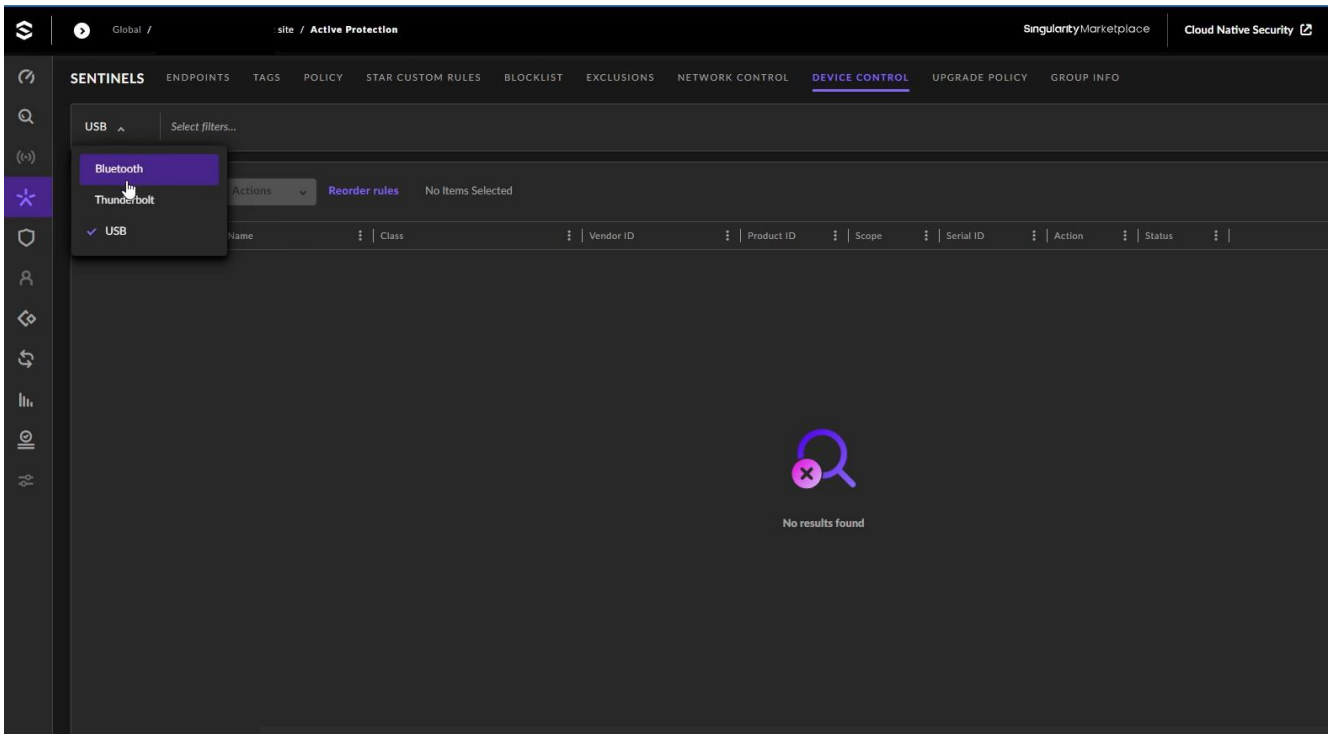

Рис.3.5. Вкладка Device control

Моніторинг підключених кінцевих пристроїв відбувається на вкладці Aplications management (Рис.3.6).

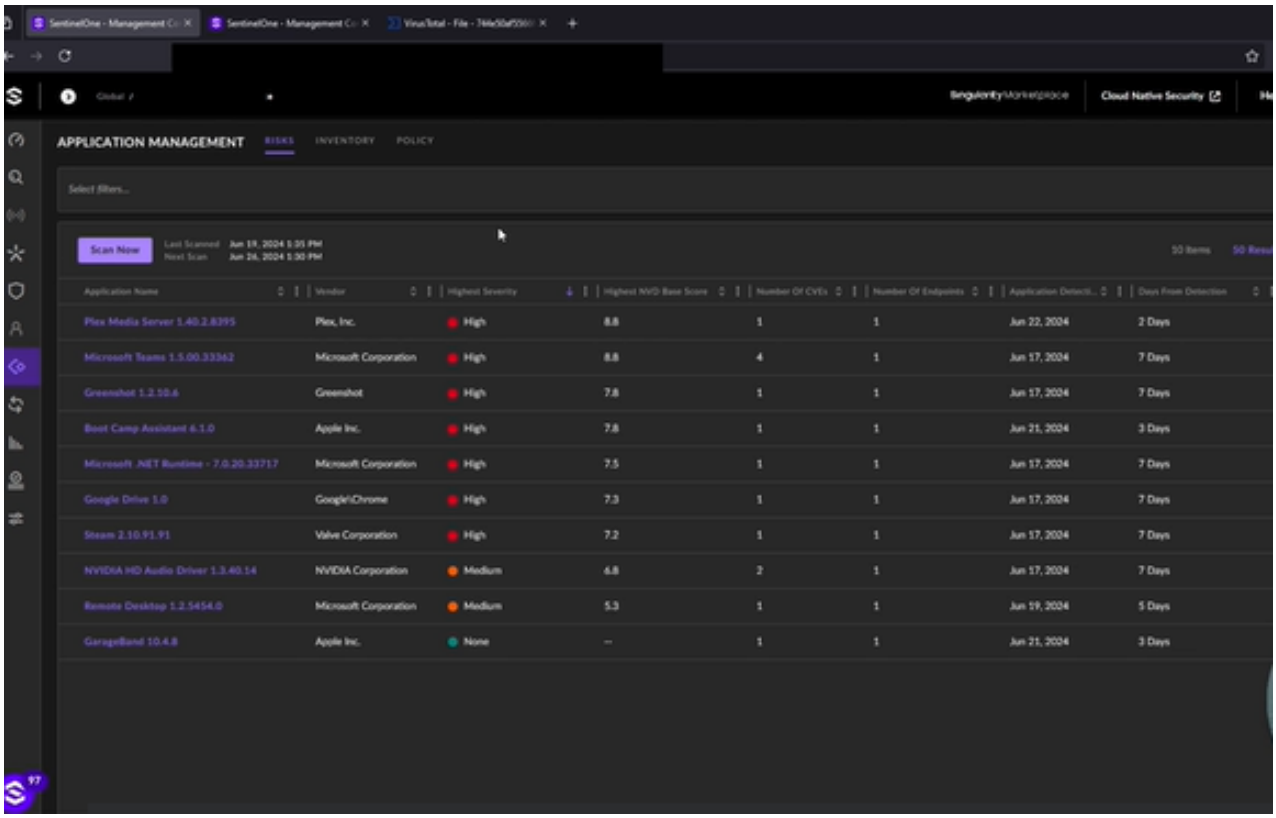

Рис.3.6. Вкладка Aplications management

На даній вкладці адміністратор безпеки може отримати інформацію щодо встановлених додатків за рівнем важливості вразливості. (рис.3.5). Якщо буде виявлено вразливість, є можливість отримати інформацію щодо CVE та отримати повну інформацію щодо виявленої вразливості (Рис. 3.7 та 3.8).

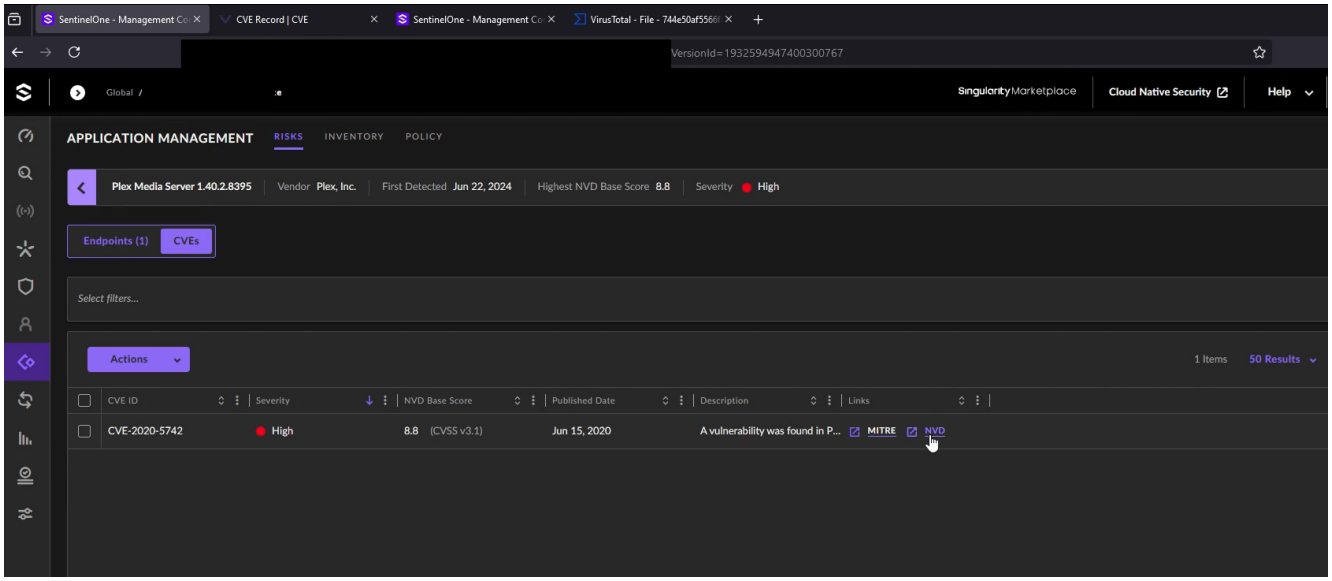

Рис. 3.7. Виявлена вразливість

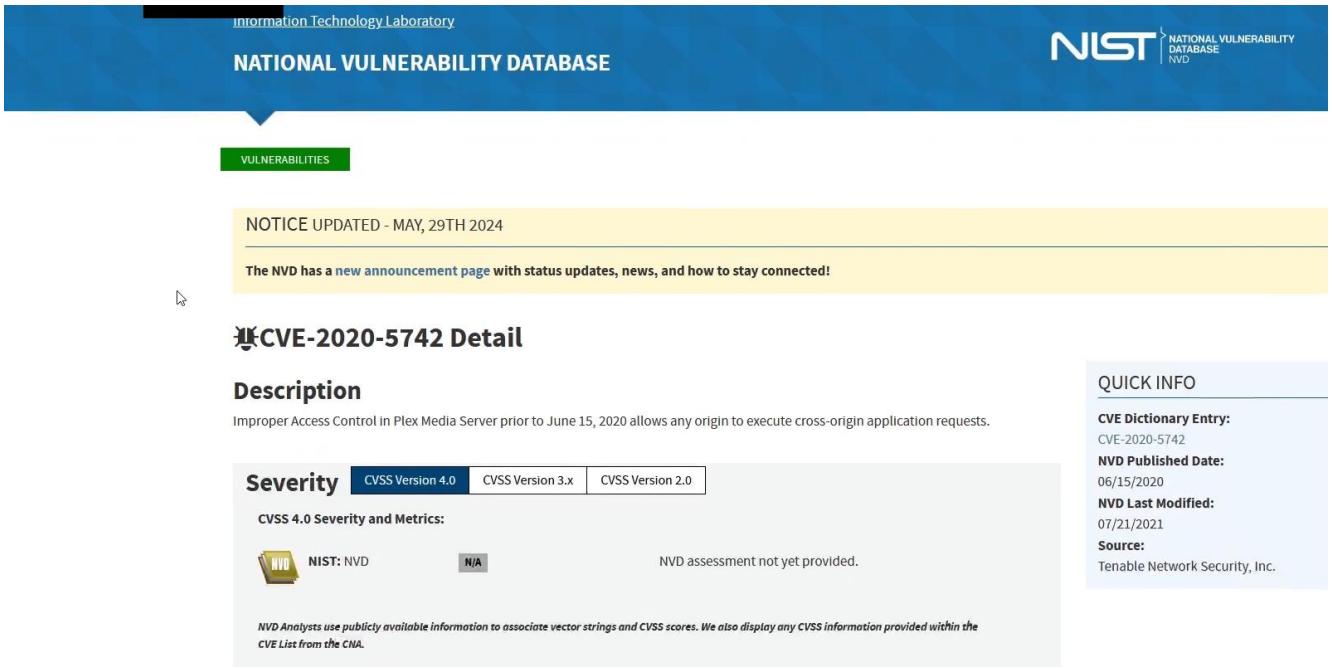

Рис.3.8. Опис вразливості

Для захисту віддалених користувачів, важливим питанням є реагування на інцидент після його виявлення. Виявлення інциденту може відбуватись різними шляхами, як це показано на рис.3.9.

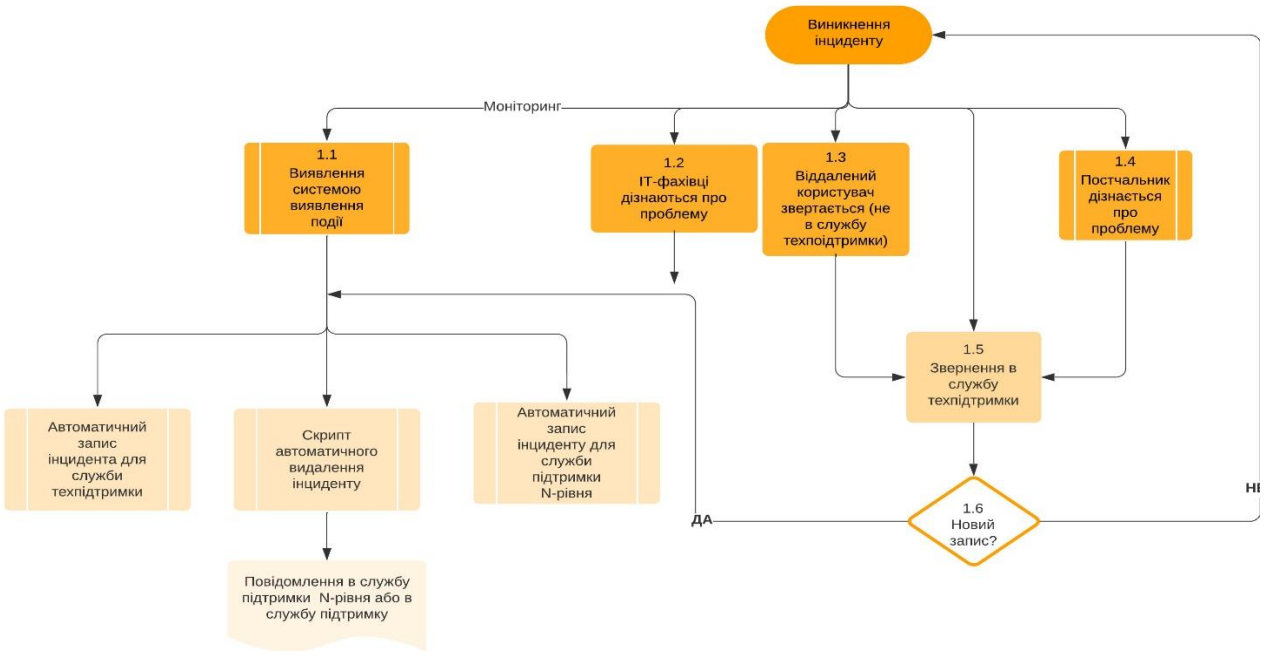

Рис.3.9. Алгоритм виявлення інциденту

Після виявлення інциденту вся інформація передається в службу підтримки або фахівцям з реагування на кіберінциденти. Такий підхід дозволяє вчасно реагувати та захищати інформаційну систему організації від кібервпливів, які можуть бути з боку віддалених користувачів.

3.2. Рекомендації використання технологій захисту віддалених користувачів на прикладі Sentinel Ones Endpoint Protection

Вибір відповідного продукту безпеки кінцевої точки для організації може бути одним із тих важливих, але складних рішень, які мають далекосяжний вплив на загальну кібербезпеку. До основних рекомендацій впровадження рішення Sentinel Ones Endpoint Protection для фахівців кібербезпеки можна виокремити наступне:

Оцініть потреби вашої організації: перший крок у виборі ідеального рішення вимагає від вас оцінити конкретні потреби вашої організації щодо безпеки. Необхідно врахувати розмір вашого бізнесу, типи кінцевих точок, галузеві вимоги

відповідності та поточну інфраструктуру безпеки. Це допоможе вам ранжувати найважливіші функції та можливості.

Проаналізуйте основні функції: шукайте продукти безпеки кінцевих точок із широким набором функцій, які відповідають вашим потребам. Під час оцінювання враховуйте такі ключові характеристики, як розширене виявлення та запобігання загрозам, ШІ з машинним навчанням для ідентифікації загроз,

Функція EDR або виявлення та реагування кінцевих точок це важлива функція, яку повинні мати продукти безпеки кінцевих точок. Він також використовується для полювання на загрозу, реагування та розслідування інцидентів.

Інтеграція аналізу загроз у режимі реального часу: це те, що продовжує допомагати бути в курсі нових загроз.

Автоматичне реагування та усунення: це автоматизує нейтралізацію загроз без залучення людей.

Централізоване управління та звітність: це забезпечить видимість у всіх сферах з перевіркою нагляду та звітністю про відповідність.

Виберіть рішення, яке забезпечить вашому бізнесу збалансоване поєднання проактивного захисту, виявлення та реагування.

Особливу увагу приділяйте питанню про масштабованість і гнучкість. Масштабоване рішення може розвиватися разом із вашою організацією. Ймовірно, більшість хмарних продуктів захисту кінцевих точок є більш масштабованими та гнучкими, ніж інші. Тоді ви легко зможете додати або видалити кінцеві точки, коли ваш бізнес зміниться. Виберіть рішення, яке підходить для різних операційних систем і типів пристроїв.

Постійно проводьте аналіз продуктивності: Рішення безпеки кінцевої точки не повинно мати суттєвого впливу на продуктивність системи, але пропонуватиме всі переваги надійного захисту. Шукайте легких агентів і оптимізацію ресурсів. Продукт може полегшити його оцінку з точки зору очікуваного впливу на продуктивність.

Рішення повинно мати просте розгортання та керування. Простота процесу розгортання та постійного керування призведе до значної економії загальної вартості володіння. Продукти, які спрощують процес розгортання, мають зручні консолі керування та надають можливості для автоматичного оновлення, пройшли цей тест. Можливості централізованого керування можуть спростити адміністрування великих або розподілених середовищ.

Ефективна безпека кінцевої точки залежить від поточного аналізу загроз. Проаналізуйте як якість, так і ширину мережі аналізу загроз кожного постачальника. Рішення, які покладаються на машинне навчання та ШІ для аналізу глобальних даних, можуть запропонувати набагато кращий захист.

Використовуйте рішення, які можуть запропонувати розширені звіти та аналітику за допомогою настроюваних інформаційних панелей, журналів подій і звітів щодо відповідності.

Зверніть увагу на можливості інтеграції: переконайтеся, що всі інші елементи вашої інфраструктури безпеки бездоганно інтегруються з безпекою вашої кінцевої точки. Дізнайтеся, як кожен продукт інтегрується з SIEM, рішеннями для керування ідентифікаційним доступом або іншими інструментами безпеки.

Порівняйте підтримку та ресурси, які пропонує кожен постачальник. Постачальник рішення повинен забезпечити детальну документацію, швидку підтримку клієнтів і доступ до досліджень загроз і найкращих практик. Постачальники з широкими програмами навчання та сертифікації краще допоможуть вашим командам отримати максимальну рентабельність інвестицій від рішення.

Визначте, скільки коштуватиме володіння протягом певного періоду часу. Окрім ліцензійних зборів, враховуйте необхідні витрати на апаратне забезпечення, навчання персоналу та інші витрати на поточне обслуговування. Рішення можуть бути дорожчими на початку, але забезпечать довгострокову економію завдяки зменшенню витрат на керування або навіть кращому захисту.

Таким чином, оскільки загрози стають дедалі прогресивнішими та частішими, рішення безпеки кінцевих точок повинні бути доступними в основі

комплексної стратегії кібербезпеки організації. Рішення, яке було досліджено, є одними з найкращих продуктів безпеки кінцевих точок, доступних у 2024 році. Вибираючи правильний продукт безпеки кінцевих точок, бізнес повинен брати до уваги широкий спектр особливостей, будь то масштабованість, вплив на продуктивність, простота керування та можливості інтеграції. .

Суть полягає в тому, що ідеальний продукт безпеки кінцевої точки має відповідати вашій організації та інфраструктурі. Використовуйте якнайкраще безкоштовні пробні та демонстраційні версії від постачальників, щоб отримати практичний тест того, як кожне рішення працюватиме у вашому середовищі. Зрештою, ви повинні зробити крок зараз, щоб підвищити позицію безпеки вашої організації.

Організації повинні дотримуватися найкращих практик, щоб переконатися, що захист кінцевих точок є повністю ефективним. Перелік цих практик полягає у наступному:

1. Навчання користувачів

Для організації важливо навчити свої групи безпеки для впровадження архітектури безпеки кінцевої точки. Навчання має включати інформацію про те, як розпізнавати фішингові атаки, методи безпечного перегляду та необхідність політики безпеки. Навчання допоможе організаціям зменшити ризик людської помилки, яка часто призводить до порушень безпеки.

2. Регулярні виправлення та оновлення

Щодня в кінцевих точках виявляються нові вразливості. Таким чином, організаціям стає важливо підтримувати оновлене програмне забезпечення та надсилати виправлення на випадок уразливості в їхній системі. Організаціям слід використовувати автоматизовані засоби керування виправленнями, щоб зробити процес плавним і швидшим.

3. Архітектура нульової довіри

Модель нульової довіри стверджує принцип, що жодному користувачу, пристрою чи мережі не можна автоматично довіряти. У цій моделі кожен запит на доступ має бути автентифікований, авторизований і зашифрований перед наданням

доступу. Це можна зробити, лише якщо в організації реалізовано перевірку особи та контроль доступу з найменшими привілеями. Ця модель знижує ризик несанкціонованого доступу, що, у свою чергу, зменшує ризик порушення безпеки або витоку даних.

4. Комплексний план реагування на інциденти

Організації повинні завжди мати при собі план реагування на інциденти . Це планування допомагає зменшити поширення вразливості по всій системі, коли вона вперше виявлена. У цьому плані мають бути чітко визначені ролі та обов'язки кожної особи, яка буде залучена до цього, і, нарешті, що робити у разі виявлення загрози.

5. Багатофакторна автентифікація (MFA)

Багатофакторна автентифікація допомагає захистити кінцеву точку від небажаних зловмисників, які, якщо кінцеву точку скомпрометовано, можуть проникнути в мережу. MFA гарантує, що користувачі отримують доступ до ресурсів після проходження двох рівнів перевірки. Це діє як додатковий рівень безпеки, який ускладнює проникнення зловмисників у систему.

Вибір рішення безпеки кінцевої точки

Організації повинні подумати про свої потреби та інфраструктуру, щоб вибрати архітектуру безпеки кінцевої точки для своїх систем. Цей вибір має ґрунтуватися на різних факторах, як-от характер розгортання, керування та продуктивності.

Хмарні рішення проти локальних рішень

Хмарним рішенням слід віддавати перевагу та використовувати їх, коли організаціям потрібне простіше розгортання, автоматичне оновлення та висока масштабованість. Вони майже все забирають з рук організації. У хмарних рішеннях використовується принцип оплати за використання, що означає, що організації повинні платити лише за ті ресурси, які вони фактично використовують у даний момент. Основна проблема з цим рішенням полягає в тому, що організація не може безпосередньо контролювати свої дані, і це стає величезною проблемою, якщо підключення до Інтернету є поганим для користувача.

Локальні рішення надають організаціям контроль над своїми даними. Це рішення також дає їм гнучкість у впровадженні певних політик щодо відповідності. Однак це рішення вимагає високої вартості налаштування та внутрішніх ресурсів для керування й обслуговування, але може запропонувати кращу продуктивність і роботу без залежності від Інтернету.

Масштабованість і гнучкість

Організації також повинні враховувати свої потреби в масштабованості, перш ніж використовувати будь-яке рішення безпеки кінцевої точки. Це особливо важливо для організацій, які бачать підйоми та падіння свого мережевого трафіку, наприклад веб-сайти електронної комерції. Вибране рішення безпеки кінцевої точки має забезпечувати відсутність або мінімальне зниження продуктивності в разі збільшення кількості кінцевих точок.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

Проведено аналіз проблеми захисту віддалених користувачів інформаційної системи організації. На основі отриманих звітів було виявлено, що велика частка витоку інформації з інформаційної системи організації може бути через віддалених користувачів, які все частіше є в організаціях.

Щоб вирішити ці проблеми, компанії можуть створювати комплексні політики безпеки даних, забезпечувати постійне навчання з питань безпеки, запроваджувати VPN для безпечної передачі даних, зробити багатофакторну автентифікацію (MFA) обов'язковою та заохочувати використання менеджерів паролів.

Для захисту віддалених користувачів запропоновано використовувати методи та засоби рішення на основі Endpoint Protection.

В роботі проведено порівняння різних рішень Endpoint Protection. Для подальшого дослідження кращим рішенням щодо вирішення проблеми захисту віддалених користувачів обрано рішення SentinelOne.

Запропоновано архітектуру безпеки кінцевих точок SentinelOne, де кінцеві точки стосуються різних пристроїв, підключених до мережі організації, наприклад ноутбуків, смартфонів і серверів. Архітектура безпеки кінцевих точок спрямована на захист цих кінцевих точок. Зазвичай це перша ланка безпеки, яку зловмисник намагається пройти зламати, щоб проникнути до інформаційної системи.

Визначено компоненти платформи захисту кінцевих точок, яка поєднує в собі потужність антивірусів, захисту від зловмисного програмного забезпечення, шифрування даних і брандмауерів для забезпечення безпеки. EPP використовує виявлення на основі сигнатур і машинне навчання, щоб блокувати загрози, перш ніж вони використають будь-яку вразливість кінцевої точки.

Результатом даного дослідження була отримана технологія захисту віддалених користувачів інформаційної системи організації та запропоновано

алгоритм, для фахівців з реагування на інциденти щодо вирішення проблеми після виявлення інциденту.

Розроблені рекомендації щодо впровадження технологію Sentinel Ones Endpoint Protection для фахівців кібербезпеки, яке дозволяє сформувати і впровадити рішення в залежності від потреб їх організації.

ПЕРЕЛІК ПОСИЛАНЬ

1 10 Essential Remote Work Tools for Productivity and Communication | DigitalOcean. URL: https://www.digitalocean.com/resources/articles/remote-work-tools.

2. Errichiello, L., & Pianese, T. (2021). The Role of Organizational Support in Effective Remote Work Implementation in the Post-COVID Era. . doi: 10.4018/978-1-7998-6754-8.ch013

3. Davies, V. (2023). The Top 10 risks of remote working. Bizclik Media Ltd. URL: https://cybermagazine.com/articles/the-top-10-risks-of-remote-working

4.Truta, F. (2024, September 30). 61% of IT Security Leaders Say Remote Workers Have Caused a Data Breach This Year. URL: https://www.bitdefender.com/blog/businessinsights/61-of-it-security-leaders-say-remote-workers-have-caused-a-data-breach-this-year/?srsltid=AfmBOopLyEw-6Ycv67G2mU2ygeYq7HRTxmHHoH0s59yzo0S6uBXKc06i%2F

5. Europe Cybersecurity Report - Asset Thank You LP. (2024). URL: https://www.cloudflare.com/lp/2024europesurvey/download/assets

6. The Data Security Risks Of Remote Working and How To Mitigate Them | Metomic. (2024, September 30). Retrieved from https://www.metomic.io/resource-centre/the-challenges-of-dlp-for-remote-working-and-how-to-manage-it

7. SentinelOne Reviews, Ratings & Features 2024 | Gartner Peer Insights. URL: https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/sentinelone/alternatives?marketSeoName=endpoint-protection-platforms&vendorSeoName=sentinelone .

8. Top Endpoint Security Products for Business in 2024. URL: https://www.sentinelone.com/cybersecurity-101/endpoint-security/endpoint-security-products .

9. Enterprise Endpoint Protection. URL: https://www.sentinelone.com/cybersecurity-101/endpoint-security/enterprise-endpoint-protection/.

10. Березовський К.В., Рудомьотова М.А. Технологія захисту кінцевих точок організації. Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 25 жовтня 2024 року). Київ, 2024. С. 10-12 (дата звернення: 05.11.2024).