ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія розширеного виявлення загроз кінцевим точкам та реагування на них на базі Sophos Intercept X Endpoint»

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

_____ Володимир СИДОРЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
СИДОРЕНКО Володимир
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій кібербезпеки
_____ Галина ГАЙДУР
"___" жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

СИДОРЕНКУ Володимиру Дмитровичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія розширеного виявлення загроз кінцевим точкам та реагування на них на базі Sophos Intercept X Endpoint»

керівник кваліфікаційної роботи Гахов Сергій Олександрович, к.військ.н., доц.
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024 року № 320.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Sophos Intercept X Endpoint;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми технології розширеного виявлення загроз кінцевим точкам.
2. Аналіз методів та засобів розширеного виявлення загроз кінцевим точкам та реагування на них на базі Sophos Intercept X Endpoint.

3. Розроблення варіанта технології розширеного виявлення загроз кінцевим точкам та реагування на них на базі Sophos Intercept X Endpoint.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми виявлення загроз кінцевим точкам.	01.10.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	12.10.2024 р.	
3.	Аналіз методів та засобів розширеного виявлення загроз кінцевим точкам та реагування на них на базі Sophos Intercept X Endpoint.	27.10.2024 р.	
4.	Технологія застосування рішення Sophos Intercept X Endpoint.	03.11.2024 р.	
5.	Рекомендації щодо розширеного виявлення загроз кінцевим точкам та реагування на них.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Володимир СИДОРЕНКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Сергій ГАХОВ
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 71 сторінка, 37 рисунків, 14 джерел.

Об'єкт дослідження – розширене виявлення загроз кінцевим точкам.

Предмет дослідження – технології розширеного виявлення загроз кінцевим точкам та реагування на них на базі Sophos Intercept X Endpoint.

Мета роботи – розробити рекомендації щодо розширеного виявлення загроз кінцевим точкам та реагування на них.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Технологія розширеного виявлення загроз кінцевим точкам та реагування на них (EDR) на базі Sophos Intercept X Endpoint забезпечує інтегровану систему захисту кінцевих точок від складних кіберзагроз. Sophos Intercept X Endpoint використовує штучний інтелект для виявлення атак, таких як експлойти та програми-здирники, та надає автоматизовані інструменти для реагування на інциденти.

У роботі було проаналізовано проблему захисту кінцевих точок в умовах сучасних загроз, визначено мету та завдання впровадження EDR-рішень. Проведено дослідження можливостей Sophos Intercept X Endpoint, включаючи такі функції, як аналіз загроз у режимі реального часу, запобігання експлойтам, відновлення систем після атак та автоматизація реагування.

На основі отриманих результатів запропоновано порядок впровадження Sophos Intercept X Endpoint у корпоративне середовище, спрямований на забезпечення високого рівня безпеки. Надано практичні рекомендації для фахівців з кібербезпеки щодо інтеграції та використання цієї технології в умовах реальних організацій.

Галузь використання: розширене виявлення загроз кінцевим точкам та реагування на них.

КЛЮЧОВІ СЛОВА: ЗАХИСТ КІНЦЕВИХ ТОЧОК, розширене виявлення загроз, технологія розширеного виявлення загроз.

ABSTRACT

Text part of the qualification work: 71 pages, 37 figures, 14 sources.

Object of research – advanced endpoint threat detection.

Subject of research – advanced endpoint threat detection and response technologies based on Sophos Intercept X Endpoint.

The aim of research – to develop recommendations for advanced endpoint threat detection and response.

Research methods – study of the literature on the topic, analysis of operational documentation, international standards, and their comparison.

The technology of extended detection and response (EDR) for endpoints based on Sophos Intercept X Endpoint ensures an integrated protection system for endpoints against advanced cyber threats. Sophos Intercept X Endpoint uses artificial intelligence to detect attacks such as exploits and ransomware and provides automated tools for incident response.

The research analyzes the problem of endpoint protection in the context of modern threats and defines the objectives and goals of implementing EDR solutions. The capabilities of Sophos Intercept X Endpoint are investigated, including functions such as real-time threat analysis, exploit prevention, system recovery after attacks, and response automation.

Based on the obtained results, a procedure for implementing Sophos Intercept X Endpoint in a corporate environment aimed at ensuring a high level of security is proposed. Practical recommendations for cybersecurity specialists are provided regarding the integration and application of this technology in real organizational conditions.

Field of application – advanced threat detection and response for endpoints.

ENDPOINT PROTECTION, ADVANCED THREAT DETECTION, ADVANCED DETECTION TECHNOLOGY.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CVE – Common Vulnerabilities and Exposures

EDR – Endpoint Detection and Response

MaaS – Malware as a Service

MTTD – Mean Time to Detect

MTTR – Mean Time to Respond

SaaS – Software as a Service

SCCM – System Center Configuration Manager

SEO – Search Engine Optimization

SIEM – Security Information and Event Management

SOAR – Security Orchestration, Automation, and Response

TTPs – Tactics, Techniques, and Procedures

TVM – Threat and Vulnerability Management

VBA – Visual Basic for Applications

XDR – Extended Detection and Response

ВСТУП

Актуальність дослідження. У сучасному світі зростаюча залежність від цифрових технологій і активне використання інформаційних систем створюють нові виклики в сфері кібербезпеки. Одним із головних ризиків для організацій і приватних осіб є кіберзагрози, які постійно еволюціонують, стають складнішими та дедалі важче піддаються виявленню. У цьому контексті забезпечення захисту кінцевих точок – комп'ютерів, серверів, мобільних пристроїв та інших підключених до мережі систем – набуває особливої важливості.

Традиційні антивірусні рішення поступово втрачають ефективність перед новими видами атак, такими як складні багаторівневі зловмисні програми програми-вимагачі та експлойти нульового дня. Це вимагає впровадження сучасних підходів, зокрема технологій розширеного виявлення загроз і реагування.

Sophos Intercept X Endpoint є однією з провідних платформ у цій сфері, яка поєднує технології на основі штучного інтелекту, аналіз поведінки та автоматизоване реагування на інциденти. Її використання дозволяє виявляти й нейтралізувати складні загрози ще до того, як вони завдають шкоди інфраструктурі.

Актуальність дослідження зумовлена необхідністю розробки та вдосконалення підходів до захисту кінцевих точок, які враховують сучасні кіберзагрози та підвищують рівень інформаційної безпеки. Вивчення технологій Sophos Intercept X Endpoint дозволяє оцінити їхню ефективність, виявити переваги й недоліки, а також адаптувати ці інструменти до специфічних потреб організацій.

Результати дослідження можуть сприяти підвищенню обізнаності фахівців у сфері кібербезпеки, оптимізації захисту інформаційних систем та розробці нових стратегій реагування на загрози в реальному часі. Це, у свою чергу, є важливим кроком до створення більш безпечного цифрового середовища.

Об’єкт дослідження – розширене виявлення загроз кінцевим точкам.

Предмет дослідження – технології розширеного виявлення загроз кінцевим

точкам та реагування на них на базі Sophos Intercept X Endpoint.

Мета роботи – розробити порядок застосування технології розширеного виявлення загроз кінцевим точкам.

Наукові завдання:

дослідити сутність проблеми виявлення загроз кінцевим точкам;

проаналізувати підходи до розширеного виявлення загроз кінцевим точкам;

проаналізувати існуючі рішення із розширеного виявлення загроз кінцевим точкам;

проаналізувати методи та засоби розширеного виявлення кінцевим точкам;

розкрити порядок реалізації технології розширеного виявлення кінцевим точкам та реагування на них.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології розширеного виявлення загроз кінецим точкам та реагування на них на базі Sophos Intercept X Endpoint.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИМ ТОЧКАМ

1.1 Дослідження проблеми виявлення загроз кінцевим точкам

Згідно зі звітом Sophos 2024 Threat Report, організації стикаються з дедалі більшою складністю управління системами виявлення загроз на кінцевих точках. Це пов'язано із зростанням кількості кібератак, особливо на гібридні та віддалені робочі середовища [1].

Дослідження акцентує увагу на важливості використання інтегрованих рішень, які поєднують штучний інтелект із традиційними методами виявлення загроз, для ефективної протидії все більш складним атакам. Крім того, зростання кількості атак із використанням програм-вимагачів спонукає компанії приділяти пріоритетну увагу захисту кінцевих точок, оскільки ці загрози стають не лише більш поширеними, але й виходять за межі своїх звичних цілей.

Атаки програм-вимагачів стають складнішими і частіше спрямовані на викрадення та шифрування даних. Зловмисники також використовують методи подвійного і навіть потрійного здирництва, коли погрожують публікацією викрадених даних [1].

Кіберзлочинність вражає людей різних професій, але особливо сильно впливає на малі підприємства. Незважаючи на те, що кібернапади на великі компанії та державні установи привертають більше уваги медіа, малі підприємства (зазвичай, організації з менш ніж 500 працівниками) вразливіші до атак з боку кіберзлочинців і страждають від наслідків таких атак у більшій пропорції. Відсутність досвідчених фахівців з безпеки, недостатні інвестиції в кібербезпеку та обмежені бюджети на інформаційні технології сприяють

цій вразливості. А якщо вони зазнають атаки, витрати на відновлення можуть призвести до закриття багатьох малих підприємств.

Малі підприємства відіграють важливу роль. За даними Світового банку, понад 90% світового бізнесу складають малі та середні організації, які забезпечують більше 50% зайнятості у світі. У США вони становлять понад 40% економічної діяльності. У 2023 році понад 75% випадків реагування на інциденти, які обробляла служба реагування Sophos X-Ops, стосувалися малих підприємств. Дані, зібрані з цих випадків, надають унікальне розуміння загроз, які щоденно націлені на ці організації [1].

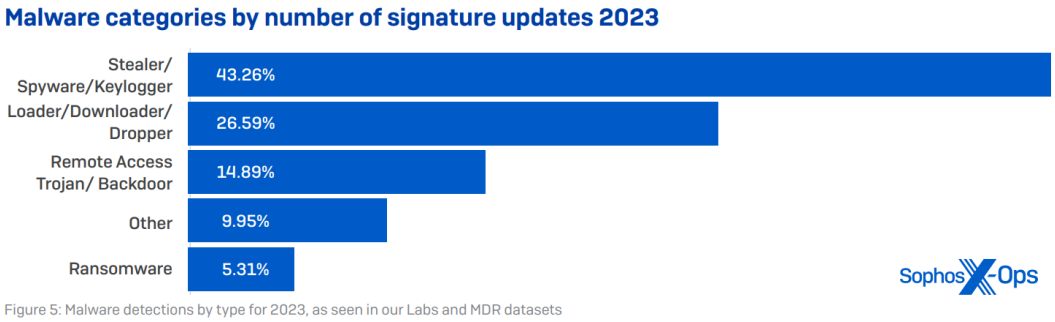


Рис. 1.1. Категорії шкідливих програм за кількістю оновлень сигнатур 2023 [1]

Близько 10% виявлених зловмисних програм не підпадають під основні категорії. Ця "інша" категорія включає ПЗ, яке націлене на веб-браузери для розміщення реклами або зміни результатів пошуку з метою отримання прибутку. Деякі викрадачі, такі як "токен" Discord, спеціалізуються на крадіжці облікових даних, а інші, такі як Strela, Raccoon Stealer і RedLine, активно збирають паролі, файли cookie та інші дані. Raccoon Stealer також використовує "кліпери" для зміни адрес криптовалютних гаманців у буфері обміну [2].

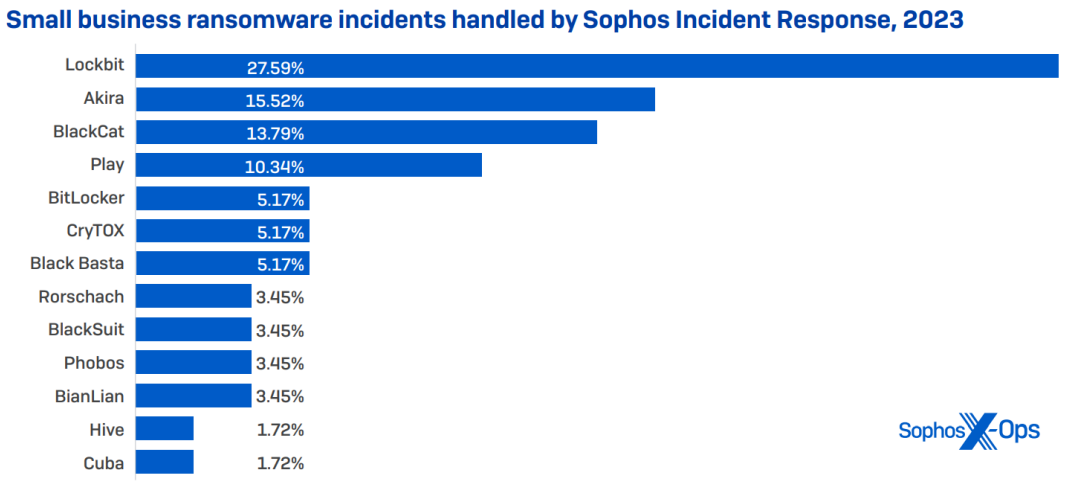


Рис. 1.2. Інциденти програм-вимагачів для малого бізнесу, оброблені Sophos Incident Response, 2023 [2]

Програми-вимагачі продовжують залишатися однією з основних загроз для малого бізнесу. Хоча вони складають відносно невелику частку серед усіх виявлених зловмисних програм, їхній вплив залишається найзначнішим. Такі атаки зачіпають підприємства будь-якого розміру та галузі, проте найчастіше вони спрямовані саме на малі та середні компанії.

У 2021 році робоча група з програм-вимагачів Інституту безпеки та технологій виявила, що 70% атак програм-вимагачів були спрямовані на малий бізнес. Хоча загальна кількість атак програм-вимагачів змінюється щороку, цей відсоток підтверджується нашими власними показниками. Програмне забезпечення-вимагач LockBit було найпоширенішою загрозою в справах безпеки малого бізнесу, які взяло на себе Sophos Incident Response у 2023 році. LockBit – це програмне забезпечення-вимагач як послуга, надане кількома дочірніми компаніями, яке було найбільш поширеним програмним забезпеченням-вимагачем у 2022 році згідно з рисунком 1.1 [2].

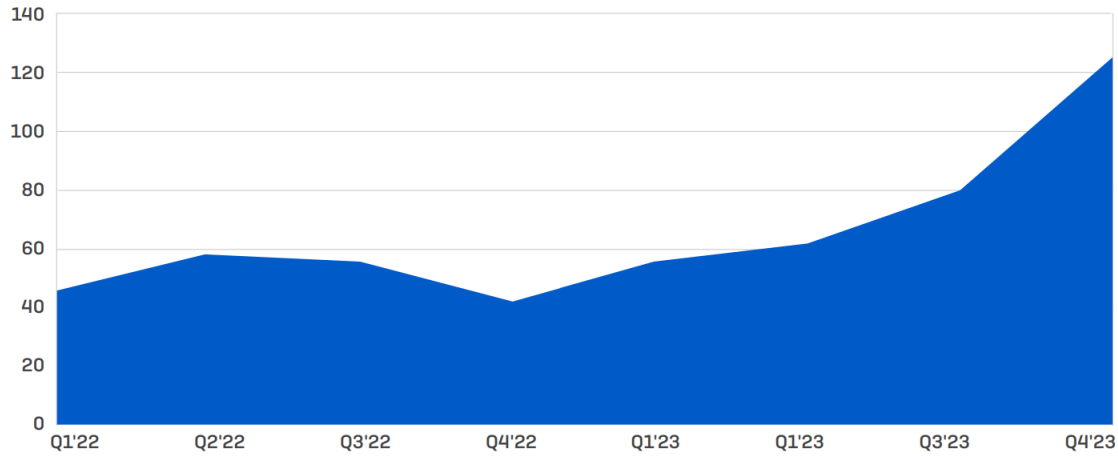


Рис. 1.3. Віддалені випадки програм-вимагачів, 2022-2023 [2]

У сучасному світі продовжує домінувати концепція «зловмисне програмне забезпечення як послуга» (MaaS), що передбачає використання інфраструктури доставки шкідливого ПЗ, яку кіберзлочинці надають через підпільні ринки своїм спільникам. Однак підвищення рівня безпеки платформ, а також дії з ліквідації таких сервісів з боку індустрії та правоохоронних органів певною мірою змінили характер ландшафту MaaS.

Після десятиліття домінування в бізнесі розповсюдження зловмисного програмного забезпечення Emotet пішов на спад після того, як його ліквідували Європол і Євроюст у січні 2021 року. Так само, меншою мірою, Qakbot і Trickbot, після того, як у серпні 2023 року їх зламали правоохоронні органи. Тоді як Qakbot повернувся в певній обмеженій формі, він був значною мірою витіснений його майбутніми наступниками, Pikabot і DarkGate. Ніщо з цього не вплинуло на відомий троян віддаленого доступу AgentTesla, який перемістився на вершину ринку MaaS. Це було зловмисне програмне забезпечення, яке найчастіше виявлялося засобами захисту кінцевих точок у 2023 році загалом у кінцевих точках і становило 51% виявлення зловмисного програмного забезпечення в загальній телеметрії минулого року [2].

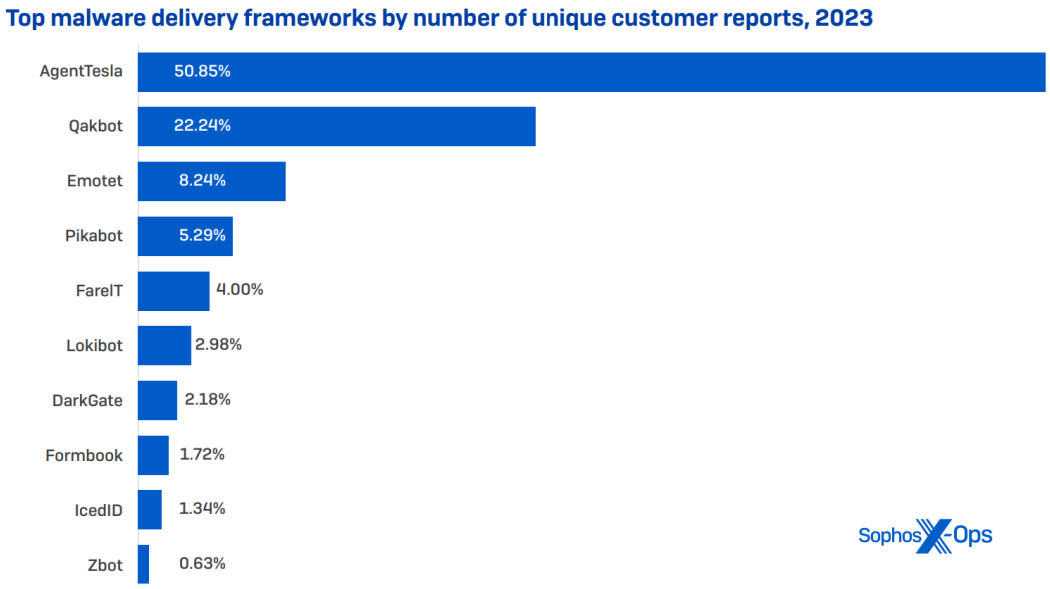


Рис. 1.4. Найкращі фреймворки доставки зловмисного програмного забезпечення за кількістю унікальних повідомлень клієнтів, 2023 рік [2]

Розбивка загальних інфраструктур, які використовуються зловмисниками для доставки шкідливого програмного забезпечення, на основі кількості виявлень кінцевих точок із захищених Sophos мереж клієнтів числа Qakbot відображають виявлення до серпневої дії міжнародних правоохоронних органів проти його інфраструктури [2].

Атаки зловмисного програмного забезпечення потребують певної форми початкового доступу. Як правило, це стосується наступного [2]:

фішингові листи;

шкідливі вкладення електронної пошти;

використання вразливостей в операційних системах і програмах;

підроблені оновлення програмного забезпечення;

використання та зловживання протоколом віддаленого робочого столу;

крадіжка облікових даних.

Основним методом операторів MaaS у минулому було закладення шкідливого ПЗ у вкладення електронної пошти. Але гігант ринку платформа Microsoft Office змінила політику безпеки за замовчуванням, що значною

мірою вплинуло на ринок MaaS. Оскільки Microsoft внесла зміни в програми Office, які за замовчуванням блокують макроси VBA у документах, завантажених з Інтернету, операторам MaaS стало важче використовувати улюблений метод розповсюдження шкідливих програм. Результатом цього стала зміна типів вкладених файлів і повний перехід на вкладені файли PDF формату.

Проте були деякі помітні винятки. На початку 2023 року оператори Qakbot почали використовувати шкідливі документи OneNote, щоб обійти зміни, які надсилаються до Excel і Word, приховуючи в документі посилання на файли сценаріїв, які активувалися, коли натискали кнопку у файлі блокнота OneNote [2].

У 2021 році стало помітно, що пропозиції «зловмисне програмне забезпечення як послуга», такі як бекдор RaccoonStealer, почали значною мірою покладатися на веб-доставку, часто використовуючи трюки пошукової оптимізації (SEO), щоб обдурити цілі, щоб вони завантажили їх шкідливе програмне забезпечення. Ці методи знову набувають популярності, а хакери, які стоять за ними, стали більш досконалими. Також є відомі кампанії які використовували шкідливу рекламу на просторах Інтернета та пошукову оптимізацію для пошуку нових незахищених користувачів. Одна з цих кампаній була організована групою, яка використовує шкідливе програмне забезпечення, яке назвали «Nitrogen». Ця група мала у використанні рекламу Google і Bing, прив’язану до конкретних ключових слів, щоб обманом завантажити потрібному, на думку жертви, програму з фейкового веб-сайту, використовуючи фірмовий знак законного розробника програмного забезпечення. Така ж техніка зловмисної реклами була використана у зв’язку з низкою інших зловмисних програм для початкового доступу, включаючи ботнет-агент Pikabot, викрадач інформації IcedID і родини зловмисних програм для бекдорів Gozi [2].

У випадку з Nitrogen реклама була націлена на IT-спеціалістів широкого профілю, пропонуючи завантаження, включаючи добре відоме програмне забезпечення для віддаленого робочого столу для підтримки кінцевих користувачів і утиліти безпечної передачі файлів. Інсталятори встановили те, що рекламувалося, але вони також доставили шкідливе корисне навантаження Python, яке, запущене інсталятором, видаляло віддалену оболонку Meterpreter і маяки Cobalt Strike [2].

Малі підприємства мають постійні загрози і складність цих загроз не сильно відрізняється в порівнянні з загрозами на великі підприємства та уряди. Хоч і малі організації мають менший прибуток, зловмисників це не зупиняє і вони охоче викрадають те, що є, і компенсують це великим обсягом. Злочинні синдикати розраховують на те, що менші компанії будуть менш захищені та не розгорнуть сучасні, складні інструменти для захисту своїх користувачів і активів. Ключ до успішного захисту від цих загроз полягає в тому, щоб довести помилковість їхніх припущень, треба навчити свій персонал, розгорнути багатофакторну автентифікацію на всіх зовнішніх активах, виправленнях серверів і мережевих пристроїв із найвищим пріоритетом і подумати про перехід для керування активів, таких як сервери Microsoft Exchange, на SaaS платформи електронної пошти [2].

Основна відмінність між компаніями, які найбільше постраждали від кібератак, і тими, які постраждали найменше, полягає в часі на реагування. Наявність експертів із безпеки, які цілодобово контролюватимуть і реагуватимуть на них, є основним фактором для ефективного захисту у 2024 році. Залишатися в безпеці не неможливо, просто потрібно комплексне планування та багаторівневий захист, щоб виграти час на реагування та мінімізувати збитки [2]

1.2 Аналіз підходів до виявлення загроз кінцевих точок

EDR дає командам із безпеки змогу отримувати уніфіковану видимість і керування наявними кінцевими точками, а також виявляти некеровані кінцеві точки, підключені до мережі, які можуть бути джерелом типових вразливостей та недоліків (CVE). Вони також можуть використовувати EDR для зменшення можливостей для атак, позначаючи вразливості та неправильні конфігурації.

Завдяки EDR, фахівці з кібербезпеки можуть здійснювати моніторинг активностей на кінцевих точках у режимі реального часу. Це дозволяє виявляти підозрілу поведінку, а також будь-які відхилення від нормального стану системи. Після виявлення загрози система може автоматично або вручну блокувати або ізолювати підозрілу кінцеву точку, знижуючи ризик поширення загрози по всій мережі.

EDR включає в себе розширені аналітичні можливості та використовує методи машинного навчання для аналізу великих обсягів даних з кінцевих точок. Це дає можливість виявляти навіть найскладніші та найнепомітніші загрози, включаючи ті, що використовують тактики "безфайлових" атак або інші просунуті методи [3].

EDR може бути інтегрований з іншими засобами безпеки, такими як SIEM і SOAR. Це дозволяє командам кібербезпеки оптимально використовувати дані та автоматизувати процеси виявлення загроз і реагування на них. Завдяки такій інтеграції забезпечується скоординована взаємодія між різними системами, що суттєво підвищує ефективність як ідентифікації загроз, так і дій у відповідь.

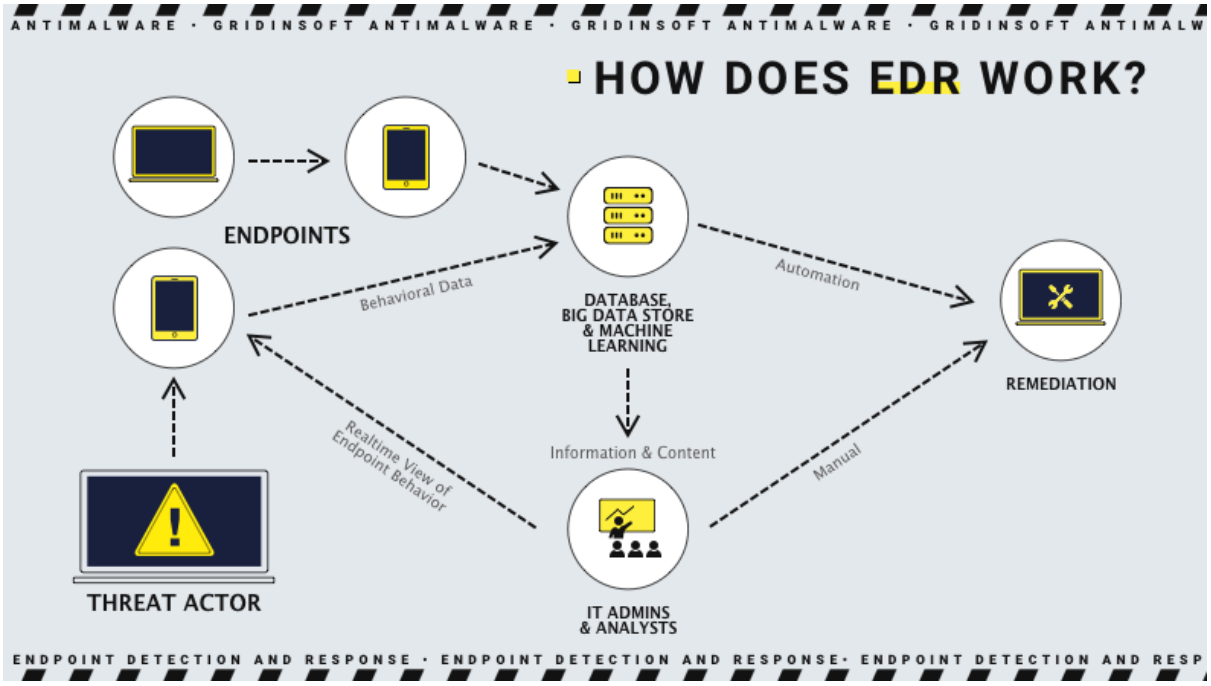


Рис. 1.5. Принцип роботи розширеного виявлення загроз на кінцеві точки [3]

Крім виявлення загроз, EDR пропонує функції автоматизації, які можуть включати автоматичне альтернативне врегулювання – наприклад, ізоляцію заражених кінцевих точок, видалення шкідливого ПЗ або виправлення конфігураційних помилок. Це дозволяє швидко нейтралізувати загрозу без залучення додаткових ресурсів [3].

Системи EDR надають потужні інструменти для проведення аналізу після інцидентів. Зібрані логи та події з кінцевих точок дозволяють дослідити, як саме загроза потрапила в систему, які дії виконувала, і як можна було уникнути її в майбутньому. Ця інформація сприяє вдосконаленню політик безпеки та захисних механізмів.

Завдяки автоматизації та аналітичним можливостям EDR значно скорочує середній час виявлення загроз та реагування на них. Це допомагає швидко нейтралізувати атаки й мінімізувати їхні наслідки.

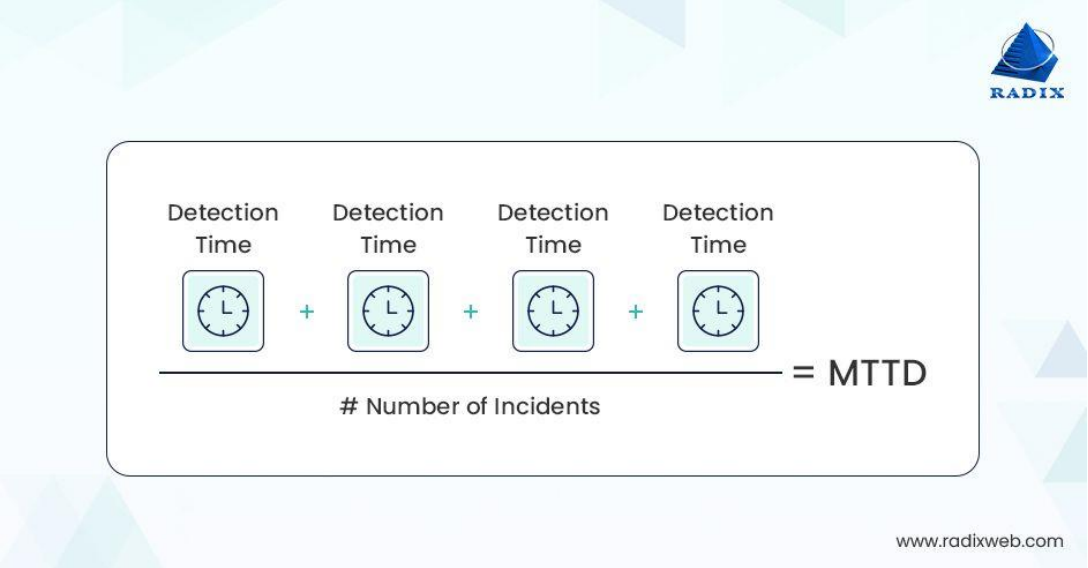


Рис. 1.6. MTTD (Mean Time to Detec) [4]

З огляду на постійну еволюцію кіберзагроз, системи EDR регулярно оновлюються відповідно до нових вразливостей і тактик зловмисників. Це забезпечує їхню актуальність і ефективність у боротьбі з сучасними загрозами.

У підсумку, EDR забезпечує проактивний підхід до кібербезпеки, дозволяючи організаціям не лише реагувати на інциденти, але й запобігати їхньому виникненню, підвищуючи загальний рівень захищеності мережі та кінцевих точок [4].

Технології розширеного виявлення загроз кінцевим точкам та реагування на них (EDR) є ключовим елементом сучасних систем кібербезпеки, і для їхнього впровадження та використання існує кілька стандартів і рекомендацій, які допомагають організаціям відповідати найкращим практикам. Вони охоплюють різні аспекти кібербезпеки, включаючи управління кінцевими точками, моніторинг, захист від загроз та реакцію на інциденти. Нижче наведено основні стандарти, які стосуються технологій EDR [4].

NIST Cybersecurity Framework (CSF) [5]. Національний інститут стандартів і технологій США (NIST) розробив NIST CSF як набір

рекомендацій щодо управління ризиками кібербезпеки. Він охоплює різні аспекти захисту кінцевих точок. Identify (Ідентифікація). Ця функція стосується розуміння ризиків, пов'язаних із безпекою кінцевих точок, а також активів та загроз.

Вимоги NIST CSF містить у собі управління активами (ID.AM). Організація повинна мати повний облік кінцевих точок, включаючи комп'ютери, сервери, мобільні пристрої та інші активи. EDR повинен допомагати в ідентифікації всіх кінцевих точок і контролювати некеровані або невідомі пристрої. Управління ризиками (ID.RA). Необхідно оцінювати ризики, пов'язані з кінцевими точками, враховуючи потенційні загрози. EDR сприяє оцінці ризиків, допомагаючи ідентифікувати уразливі кінцеві точки та оцінювати вплив потенційних атак.

Наступна функція називається Protect (Захист). Функція захисту охоплює механізми для забезпечення стійкості до кіберзагроз та зниження можливості атак на кінцеві точки.

Вимогами є управління ідентифікацією та доступом (PR.AC). Організація повинна обмежувати доступ до систем і кінцевих точок лише авторизованим користувачам і процесам. EDR повинен надавати можливості для моніторингу доступу до кінцевих точок і виявлення підозрілих спроб. Захист даних (PR.DS). Включає механізми шифрування та захисту даних, що передаються через кінцеві точки. EDR допомагає виявляти спроби несанкціонованого доступу до даних на кінцевих точках. Процедури безпеки (PR.PT). EDR повинен забезпечувати захист кінцевих точок через регулярні оновлення антивірусних програм, фаєрволів, і системних патчів для усунення вразливостей.

Третя функція захисту – це Detect (Виявлення). Функція виявлення включає здатність своєчасно ідентифікувати кіберзагрози.

Вимогами є аномалії та події (DE.AE). EDR повинен бути здатним виявляти аномальну активність на кінцевих точках, таку як незвичні процеси,

підозрілі мережеві запити або зміни в конфігураціях. Безперервний моніторинг (DE.CM). EDR системи повинні забезпечувати постійний моніторинг кінцевих точок, щоб вчасно виявляти загрози та активності, які можуть свідчити про потенційні інциденти безпеки. Моніторинг та аналіз журналів (DE.DP). EDR повинен збирати та аналізувати журнали подій на кінцевих точках для виявлення підозрілої активності і кіберзагроз.

Наступна функція є Respond (Реагування). Ця функція включає процеси і механізми для ефективного реагування на інциденти.

Вимоги NIST CSF – планування реагування на інциденти (RS.RP). EDR повинен підтримувати процеси швидкого реагування на інциденти, дозволяючи ізолювати скомпрометовані кінцеві точки або зупинити підозрілі процеси. Аналіз (RS.AN). Після виявлення загрози EDR повинен забезпечити аналіз інциденту, включаючи його джерело, вектори атаки та вплив. Реагування на інциденти (RS.CO). EDR повинен надавати засоби для координації реагування, автоматизації заходів щодо нейтралізації загроз та мінімізації їхнього впливу. Навчання після інциденту (RS.IM). EDR повинен надавати можливості для аналізу інциденту після його завершення, щоб визначити, які техніки були використані і як їх уникнути в майбутньому.

Одна з основних функцій є Recover (Відновлення). Ця функція охоплює здатність до відновлення після кіберінцидентів.

Вимоги NIST CSF є планування відновлення (RC.RP). EDR повинен забезпечити створення плану відновлення систем і кінцевих точок після атаки. Відновлення після інцидентів (RC.CO). Після усунення загрози EDR повинен сприяти поверненню кінцевих точок до нормальної роботи, включаючи виправлення пошкоджених або скомпрометованих компонентів. Поліпшення (RC.IM). EDR має бути частиною постійного циклу вдосконалення, надаючи інформацію для удосконалення майбутніх заходів безпеки та відновлення.

Розглянемо наступний стандарт – це *MITRE ATT&CK Framework* [6].

MITRE ATT&CK є глобально визнаною базою знань про тактики, методи та процедури, які використовуються зловмисниками. Вона забезпечує детальне описання поведінки атакуючих, що дозволяє ефективно використовувати EDR для виявлення та реагування на специфічні техніки атак. EDR технології часто інтегрують дані з ATT&CK Framework для підвищення точності виявлення загроз і формування відповідних реакцій.

Для технологій розширеного виявлення загроз кінцевим точкам та реагування (EDR), MITRE ATT&CK Framework вимагає та рекомендує наступні компоненти та функції.

Покриття тактик і технік (TTPs). MITRE ATT&CK організований навколо тактик (цілі зловмисника на кожному етапі атаки) та технік (специфічні методи, що використовуються для досягнення цих цілей). Технології EDR повинні виявляти різні техніки атак, зокрема ті, що використовуються для ініціації атак, ескалації привілеїв, переміщення по мережі та виконання зловмисних дій. Також охоплювати всі етапи атаки, починаючи від початкового доступу та закінчуючи діями після зламування (такі як збір даних, ексфільтрація або видалення слідів) [6].

Моніторинг підозрілої активності. EDR повинен надавати можливості для безперервного моніторингу активності на кінцевих точках, включаючи виявлення аномальних процесів і активності, наприклад, підозрілі процеси, зміну конфігурацій, виконання команд через PowerShell або спроби доступу до критичних системних файлів. Також EDR повинен відстежувати спроби ескалації привілеїв, такі техніки, як "Privilege Escalation" або "Persistence", повинні бути легко ідентифіковані за допомогою моніторингу процесів і доступів. Технології EDR мають бути налаштовані на розпізнавання багатьох із цих технік, які документовані в MITRE ATT&CK, щоб вчасно ідентифікувати підозрілу активність.

Контекст і аналіз поведінки. MITRE ATT&CK вимагає від технологій розширеного виявлення загроз здатності аналізувати поведінку користувачів

та програм, щоб виявляти відхилення від норми. EDR має збирати та аналізувати великий обсяг даних з кінцевих точок (логів, процесів, мережевої активності). Використовувати контекстно-обізнану аналітику для розуміння типових шаблонів поведінки зловмисників (відповідно до технік з ATT&CK) і ідентифікації аномалій у поведінці системи або користувачів [6].

Аналіз після атаки. Стандарт визначає також важливість здатності до аналізу після атаки, що дозволяє зрозуміти, як саме була реалізована атака. Технології EDR мають забезпечувати повне логування дій на кінцевих точках, що дозволяє відстежити всі кроки зловмисника. Також надавати можливості для проведення форензичного аналізу, що дозволяє розслідувати інцидент та зрозуміти, які техніки були використані та який вектор атаки використовувався [6].

Ізоляція та реагування. EDR повинен забезпечувати засоби для ефективної реакції на інциденти. MITRE ATT&CK визначає, що технології мають містити в собі функціонал для ізоляції скомпрометованих кінцевих точок, що дозволяє запобігти подальшому поширенню загрози по мережі. Підтримувати автоматичну або ручну відповідь на загрози, зокрема через блокування шкідливих процесів або скидання налаштувань [6].

Інтеграція з іншими інструментами. MITRE ATT&CK підтримує інтеграцію технологій EDR з іншими системами безпеки, такими як SIEM (Security Information and Event Management) або SOAR (Security Orchestration, Automation, and Response). Вимоги включають в собі спільне використання даних та обмін інформацією між EDR і SIEM, що дозволяє створювати злагоджений процес моніторингу та реагування на загрози. Використання автоматизації для реагування на загрози, що допомагає пришвидшити процес реагування та зменшити час між виявленням і нейтралізацією загрози.

Пошук атак до ATT&CK матриці. EDR системи повинні вміти шукати свої виявлені загрози до відповідних тактик і технік у матриці MITRE ATT&CK. Це дозволяє швидше ідентифікувати тип атаки та техніки, що

використовувалися зловмисниками, та покращити аналітичний процес та розслідування інцидентів, допомагаючи зрозуміти повну картину атаки [6].

Адаптивність до нових загроз підкреслює MITRE ATT&CK, що технології EDR мають бути адаптивними, тобто повинні вміти навчатися нових технік, які використовують зловмисники, і вчасно реагувати на нові вектори атак. Це включає регулярне оновлення баз даних загроз та інтеграцію нових технік у систему виявлення, здатність до швидкої адаптації до нових методів атак, що дозволяє EDR залишатися ефективним у мінливому середовищі [6].

ISO/IEC 27001 [7] та ISO/IEC 27002 [8]. Міжнародний стандарт ISO/IEC 27001 є важливим для управління інформаційною безпекою в організаціях. Він визначає вимоги до системи управління інформаційною безпекою (ISMS) та містить контрольні заходи, які можуть бути реалізовані через EDR. Стандарт ISO/IEC 27002 надає рекомендації щодо впровадження засобів безпеки, зокрема виявлення та реагування на інциденти кібербезпеки.

Основні вимоги, що стосуються EDR [7]:

оцінка ризиків (розділ 6.1.2): організація повинна ідентифікувати загрози, пов'язані з кінцевими точками, та оцінювати ризики, які можуть виникнути через відсутність належного захисту. Використання EDR може стати одним із заходів для зменшення ризиків, які пов’язані з кінцевими точками;

контроль доступу (розділ 9.1): захист кінцевих точок пов'язаний із впровадженням ефективних заходів контролю доступу, щоб запобігти несанкціонованому доступу до інформаційних ресурсів. EDR системи можуть відстежувати активність користувачів і виявляти спроби несанкціонованого доступу;

реагування на інциденти безпеки (розділ 16): організація повинна мати процеси для швидкого виявлення, реагування на інциденти безпеки та їхньої ескалації. EDR забезпечує можливості виявлення загроз на кінцевих точках і

автоматичного або ручного реагування на ці загрози;

моніторинг та огляд безпеки (розділ 18.2): організація повинна постійно контролювати свої інформаційні системи та забезпечувати їх регулярний огляд на предмет інцидентів безпеки. EDR надає аналітичні дані, що допомагають у моніторингу та оцінці стану безпеки кінцевих точок.

Розглядаючи звіт Sophos 2024, який надає глибокий аналіз поточних загроз кібербезпеки, з особливим акцентом на проблемах малого бізнесу та викликах управління кінцевими точками в умовах зростаючої складності кібератак. Підкреслючи кілька ключових тенденцій і проблем, такі як – зростаюча складність кібератак, що у свою чергу малі та середні підприємства, стикаються з дедалі більш складними загрозами, зокрема програмами-вимагачами. Ці загрози стають більш витонченими через застосування подвійного і потрійного здирництва, коли зловмисники викрадають та шифрують дані, а потім погрожують їх публікацією.

Незважаючи на те, що кібератаки на великі організації привертають більше уваги, малі підприємства є більш вразливими через відсутність кваліфікованого персоналу з кібербезпеки, обмежені бюджети та недостатні інвестиції у захист. Малі підприємства, які становлять понад 90% глобального бізнесу, відчувають наслідки атак сильніше, і багато з них можуть збанкрутувати через витрати на відновлення.

Програми-вимагачі залишаються однією з головних загроз, особливо для малих підприємств. В 2023 році Sophos зафіксував, що переважна більшість випадків реагування на інциденти стосувалися саме малих підприємств. Програма-вимагач LockBit залишається найпоширенішою загрозою для цього сегменту бізнесу.

Кіберзлочинці активно використовують MaaS, коли інфраструктуру для розповсюдження шкідливих програм надають інші злочинці через підпільні ринки. Незважаючи на зусилля правоохоронних органів, деякі

зловмисні програми, як-от AgentTesla, продовжують активно діяти і домінувати на ринку.

Також, основними методами початкового доступу залишаються фішингові атаки, шкідливі вкладення електронної пошти та використання вразливостей у програмах. Особливу увагу привертає зміна тактик зловмисників через зміни у продуктах Microsoft, що змусило кіберзлочинців використовувати файли PDF та OneNote замість макросів VBA для зараження.

З наведеного вище неможливо виключати роль EDR системи, які в свою чергу забезпечують комплексний підхід до виявлення загроз і реагування на них. Завдяки можливостям моніторингу, аналітики та автоматизації, ці системи дозволяють організаціям не лише ефективніше виявляти загрози в реальному часі, але й швидко реагувати на них, знижуючи ризик поширення шкідливих програм. Такі системи значно скорочують середній час на виявлення (MTTD) та реагування (MTTR), що критично важливо для мінімізації шкоди. Ключові рекомендації: Звіт рекомендує малим підприємствам підвищувати обізнаність працівників, використовувати багатофакторну аутентифікацію, своєчасно оновлювати програмне забезпечення та розглядати перехід на SaaS-рішення для захисту своєї інфраструктури.

Кіберзагрози стають дедалі складнішими та агресивнішими, особливо для малого бізнесу, який часто не має належних ресурсів для протидії таким атакам. Інтеграція технологій на основі штучного інтелекту та рішень EDR стає необхідністю для захисту кінцевих точок, а також для своєчасного виявлення та реагування на загрози. Організаціям потрібно впроваджувати багаторівневі системи захисту та постійно оновлювати свою кібербезпекову стратегію, щоб залишатися на крок попереду зловмисників.

1.3 Аналіз існуючих рішень щодо розширеного виявлення загроз кінцевим точкам та реагування на них

У сфері технологій розширеного виявлення загроз кінцевим точкам та реагування на них є кілька провідних рішень.

CrowdStrike

CrowdStrike Falcon є одним із найпопулярніших EDR-рішень на ринку. Компанія використовує хмарні технології та штучний інтелект для виявлення загроз і реагування на інциденти безпеки.

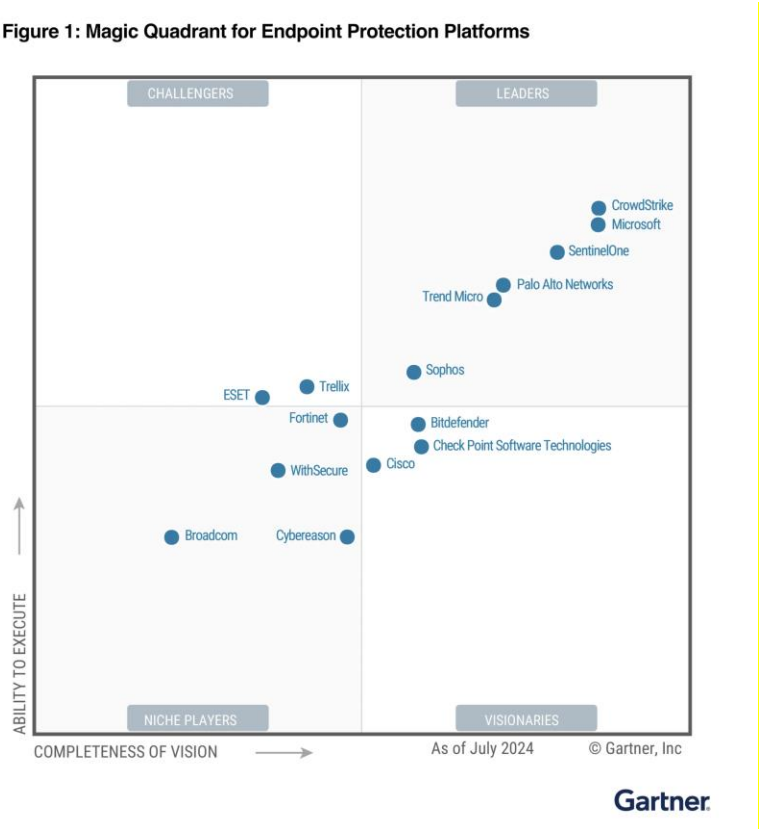


Рис. 1.7. Магічний квадрант Гартнера станом на 2024 рік [9]

Їхня платформа поєднує превентивний захист, автоматичне виявлення загроз і можливості розслідування інцидентів в реальному часі. Серед переваг – висока швидкість розгортання, мінімальний вплив на продуктивність кінцевих точок і постійне оновлення даних загроз завдяки хмарній інфраструктурі.

Основні характеристики CrowdStrike Falcon, які стосуються EDR [10]:

хмарна архітектура. CrowdStrike Falcon працює виключно в хмарному середовищі, що забезпечує оперативний збір, аналіз і обробку даних з кінцевих точок без необхідності у складній локальній інфраструктурі. Такий підхід гарантує масштабованість і високу продуктивність, дозволяючи системі швидко реагувати на загрози;

машинне навчання та штучний інтелект. Платформа використовує передові технології машинного навчання, щоб виявляти поведінкові аномалії та протидіяти складним атакам у реальному часі. Її алгоритми здатні розпізнавати нові та невідомі загрози, аналізуючи поведінку зловмисного коду навіть у випадках, коли він ще не каталогізований;

поглиблений аналіз загроз. Falcon надає детальну інформацію про атаки, включаючи контекст подій: механізми здійснення атак, використані вразливості та скомпрометовані системи. Це допомагає командам безпеки ефективніше усувати наслідки інцидентів;

швидка реакція на інциденти. Платформа дозволяє не лише виявляти, але й миттєво реагувати на загрози. Інструменти для ізоляції кінцевих точок, видалення шкідливих файлів та відновлення систем допомагають мінімізувати вплив атак на бізнес-процеси;

CrowdStrike Threat Graph. Завдяки системі Threat Graph платформа щодня аналізує трильйони подій. Інструмент збирає дані про поведінку кінцевих точок у глобальній мережі CrowdStrike, що дозволяє виявляти та попереджати загрози в реальному часі;

контекстний захист від загроз (Threat Intelligence). Falcon має вбудовану функціональність для аналізу загроз, яка надає розширену інформацію про потенційні атаки та зловмисні кампанії. Це допомагає командам безпеки розуміти природу загрози й оцінювати ризики для організації;

полегшена установка і низький вплив на систему. CrowdStrike Falcon потребує встановлення лише одного легкого агента на кінцевій точці, який споживає мінімум системних ресурсів. Це забезпечує непомітну роботу агента та мінімальний вплив на продуктивність пристроїв;

захист від атак без використання файлів (fileless attacks). Falcon здатний виявляти й блокувати атаки, які не використовують традиційні шкідливі файли, зокрема ті, що працюють лише в оперативній пам'яті, використовують легітимні процеси операційної системи або інструменти адміністративного управління (наприклад, PowerShell);

мобільний захист. Окрім захисту для традиційних кінцевих точок, CrowdStrike Falcon пропонує рішення для захисту мобільних пристроїв (Android та iOS), що робить його універсальним інструментом для різних типів кінцевих точок.

Переваги CrowdStrike Falcon [10]:

висока ефективність виявлення. Завдяки хмарним можливостям та передовим алгоритмам платформа може швидко виявляти та запобігати складним атакам;

масштабованість. Платформа підходить як для великих, так і для малих організацій завдяки своїй хмарній архітектурі та мінімальним вимогам до інфраструктури;

гобальна спільнота захисту. Використовуючи Threat Graph, Falcon постійно аналізує дані зі всієї своєї глобальної мережі, що дозволяє швидко адаптуватися до нових загроз;

простота у використанні. Falcon пропонує зручний інтерфейс, який дозволяє легко керувати захистом кінцевих точок та налаштовувати захисні політики.

Наступним рішенням, який надається до розгляду – це *SentinelOne.*

SentinelOne пропонує EDR-рішення, які поєднують автоматизоване виявлення загроз, реагування на інциденти та відновлення систем після атак.

Їхні технології, засновані на машинному навчанні, ефективно протидіють як новим, так і відомим загрозам у реальному часі. Завдяки автоматизації процесів реагування платформа забезпечує швидке усунення атак, що робить її оптимальним вибором для організацій, які прагнуть мінімізувати час реагування на інциденти.

Нижче наведено основні функції цього рішення [11]:

виявлення та реагування на загрози в реальному часі. SentinelOne EDR забезпечує виявлення загроз у режимі реального часу та реагування на них, що дозволяє командам безпеки швидко й ефективно виявляти складні загрози та реагувати на них. Рішення збирає та аналізує дані кінцевої точки, мережевий трафік і поведінку користувачів, щоб виявити аномальні дії, які можуть свідчити про порушення безпек;

автоматизоване реагування на інциденти. SentinelOne EDR автоматизує процеси реагування на інциденти, скорочуючи час для виявлення і реагування на інциденти безпеки. Коли виявляється потенційна загроза, рішення автоматично ініціює робочі процеси реагування на інциденти, такі як ізоляція постраждалої кінцевої точки, блокування зловмисного трафіку та сповіщення команд безпеки;

можливості судово-медичних розслідувань. SentinelOne EDR надає можливості судово-медичних розслідувань, дозволяючи командам безпеки проводити глибокі судові розслідування інцидентів безпеки. Рішення збирає детальні дані кінцевої точки, мережевий трафік і дані про поведінку користувачів, надаючи командам безпеки інформацію, необхідну для ефективного розслідування інцидентів безпеки та реагування на них;

простий у використанні та розгортанні. SentinelOne EDR простий у використанні та розгортанні, що робить його чудовим вибором для організацій, які хочуть швидко й ефективно підвищити безпеку кінцевих точок. Рішення розроблено для бездоганної інтеграції з існуючими

інструментами та процесами безпеки, що полегшує впровадження та використання;

комплексна безпека кінцевої точки. SentinelOne EDR забезпечує комплексну безпеку кінцевих точок, захищаючи кінцеві точки від широкого спектру кіберзагроз, включаючи шкідливі програми, програми-вимагачі та фішингові атаки. Рішення використовує машинне навчання та аналіз поведінки для виявлення та блокування розширених загроз, мінімізуючи ризик витоку даних та інших інцидентів кібербезпеки.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint (колишній Microsoft Defender ATP) інтегрується з екосистемою Microsoft і є потужним EDR-рішенням. Він забезпечує активне виявлення та захист від складних загроз на кінцевих точках за допомогою розширених аналітичних інструментів, таких як поведінковий аналіз та штучний інтелект. Перевагою є глибока інтеграція з іншими продуктами Microsoft, що дозволяє легко керувати безпекою в корпоративних середовищах з великою кількістю кінцевих точок.

Основні модулі Microsoft Defender for Endpoint [12]:

виявлення загроз в реальному часі. MDE використовує алгоритми штучного інтелекту та поведінковий аналіз для виявлення аномальної активності та загроз у реальному часі. Завдяки хмарним технологіям рішення отримує оновлення про нові загрози практично миттєво, що забезпечує постійний захист від нових типів атак.

автоматизація процесів реагування. Microsoft Defender for Endpoint дозволяє автоматизувати процес реагування на загрози, що допомагає зменшити час між виявленням атаки та вжиттям заходів. Автоматизовані дії можуть включати ізоляцію заражених кінцевих точок, видалення шкідливих файлів або блокування підозрілої активності.

поглиблений аналіз інцидентів. Рішення дозволяє командам безпеки здійснювати розслідування інцидентів, надаючи глибокий аналіз того, як і

звідки виникла загроза, що вона зачепила та які дії були здійснені шкідливим програмним забезпеченням. Це дає можливість оцінити повний цикл атаки та мінімізувати повторні загрози;

хмарна інтеграція. MDE використовує потужності Microsoft Azure для аналізу великих обсягів даних і їх обробки у хмарі. Це дозволяє обробляти події та лог-файли з багатьох кінцевих точок, не обтяжуючи локальні ресурси організації;

інтеграція з іншими продуктами Microsoft. Microsoft Defender for Endpoint інтегрується з іншими рішеннями Microsoft, зокрема Azure Security Center, Office 365, Azure Active Directory, що дозволяє забезпечити повну безпеку на всіх рівнях інфраструктури компанії. Це спрощує управління безпекою в організаціях, які використовують екосистему Microsoft;

підтримка різних операційних систем. Хоча MDE спочатку був орієнтований на захист пристроїв з Windows, зараз він також підтримує інші операційні системи, включаючи macOS, Linux та мобільні платформи (iOS і Android). Це робить його універсальним рішенням для захисту різних типів кінцевих точок;

Threat and Vulnerability Management (TVM). Одна з унікальних функцій MDE – це управління вразливостями (TVM), яке дозволяє виявляти та усувати вразливі місця у системах до того, як їх можуть використати зловмисники. Рішення автоматично оцінює стан безпеки кінцевих точок та пропонує кроки для виправлення ситуації.

Переваги Microsoft Defender for Endpoint [12]:

комплексний захист: MDE охоплює всі аспекти безпеки кінцевих точок, включаючи виявлення, реагування, аналіз та усунення наслідків;

інтеграція з Microsoft 365: Легко інтегрується з існуючими сервісами Microsoft, забезпечуючи узгодженість і зручність у використанні;

хмарні можливості: Завдяки хмарній архітектурі система може швидко адаптуватися до нових загроз і забезпечувати високий рівень продуктивності без втрати швидкодії;

зручний для великих компаній: Ідеальний для підприємств із великими IT-інфраструктурами завдяки можливості централізованого управління та широкому спектру аналітичних інструментів.

Загалом, Microsoft Defender for Endpoint є потужним інструментом для сучасних організацій, що дозволяє не лише захистити кінцеві точки, але й забезпечити повний цикл реагування на інциденти та управління вразливостями в реальному часі.

Наведені вище рішення є провідними (еталонними) у своїй сфері. Ці компанії є лідерами в галузі завдяки своїм інноваційним підходам до виявлення загроз і реагування на інциденти, а також постійному розвитку своїх технологій.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РОЗШИРЕНОГО ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИМ ТОЧКАМ ТА РЕАГУВАННЯ НА НИХ НА БАЗІ SOPHOS INTERCEPT X ENDPOINT

2.1 Призначення та основні функції Sophos Intercept X Endpoint

В цілому Intercept X Endpoint має багаторівневий захист завдяки поєднанню методів сигнатурного, поведінкового та евристичного аналізу; розширені функції EDR для ефективного розслідування інцидентів безпеки; синхронізація з іншими рішеннями Sophos для швидшого реагування на загрози; захист від сучасних видів атак на основі експлойтів, атак типу "нульового дня" та шифрувальників.

Захист від шкідливого ПЗ – це антивірусний модуль, який використовує традиційні методи для виявлення відомого шкідливого ПЗ. Додатково існує модуль глибокого вивчення (Deep Learning), який прогнозує загрози, аналізуючи файли до їх виконання, що дозволяє виявляти нові та невідомі загрози [13].

Anti-Ransomware – це функція виявляє та зупиняє шкідливі програми, що намагаються шифрувати файли з метою вимагання викупу. Зокрема, функція CryptoGuard захищає файли від несанкціонованого шифрування, допомагаючи уникнути втрат важливих даних [13].

Exploit Prevention (Запобігання експлойтам) – цей компонент захищає кінцеві точки від атак, що експлуатують вразливості в програмному забезпеченні, та блокує шкідливі дії, часто використовувані зловмисниками для обходу традиційних методів захисту [13].

Endpoint Detection and Response надає інструменти для моніторингу та аналізу підозрілої активності на пристроях, допомагаючи командам безпеки

розслідувати інциденти, аналізувати їхні причини, виявляти вразливості й оперативно реагувати на загрози [13].

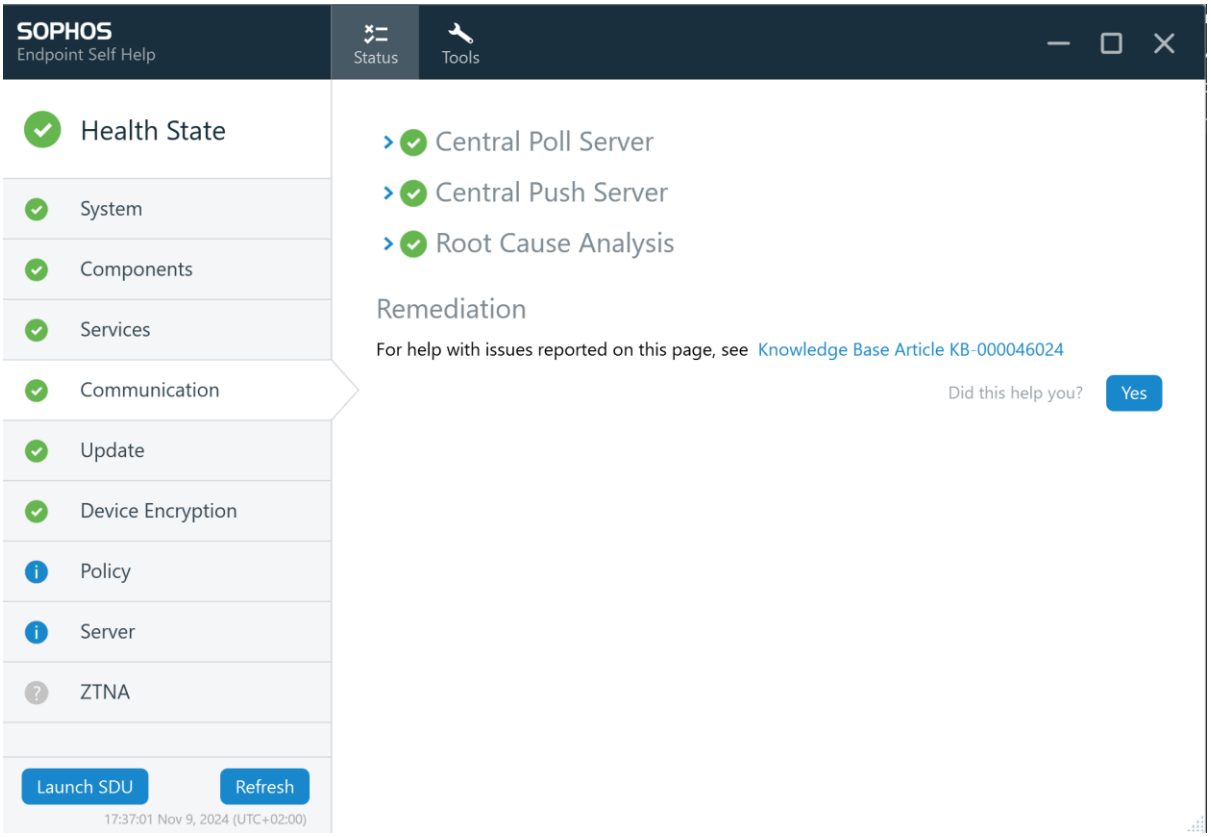


Рис. 2.1. Загальні функції Sophos Intercept X Endpoint

Synchronized Security забезпечує інтеграцію з іншими продуктами Sophos через Synchronized Security, що дозволяє обмінюватися даними між компонентами системи захисту, швидше виявляти загрози та координувати дії для мінімізації впливу на кінцеві точки.

Контроль додатків і веб-контроль дозволяє встановлювати обмеження на доступ до додатків та певних категорій веб-сайтів, знижуючи ризики від несанкціонованого доступу або небезпечних ресурсів.

Threat Intelligence – цей компонент використовує хмарний аналіз і дані про загрози для забезпечення актуального захисту, допомагаючи швидко реагувати на нові загрози [13].

Захист від активних загроз за допомогою комплексних підходів EDR і XDR. Важливо швидко припиняти атаки. Sophos XDR надає потужні інструменти та дані про загрози, які дозволяють виявляти, досліджувати та реагувати на їх підозрілу активність у всьому IT-середовищі користувача.

Фундамент потужного захисту. IT-команди, які мають обмежені ресурси, мають менше інцидентів для розслідування та вирішення, тоді як більше загрози нейтралізовуються заздалегідь. Sophos поєднує розширене виявлення та реагування у галузі захисту кінцевих точок, який блокує загрози до того, як вони почнуть діяти [13].

Вбудоване виявлення кінцевої точки та відповідь (EDR). Sophos XDR містить комплексні інструменти EDR, у тому числі потужний кастомізований пошук можливостей з доступом до даних кінцевої точки та сервера за 90 днів і безпечним віддаленим доступом до пристроїв.

Чим більше користувач бачить, тим швидше зможете діяти. Події як від Sophos, так і від інших продуктів приймаються, фільтруються, співвідносяться та пріоритезуються, розширюючи видимість усіх ключових поверхонь для атаки та дозволяє швидко виявляти та зупиняти активних противників [13].

Розширені рішення Sophos XDR. Технології Sophos бездоганно поєднуються в платформі XDR, щоб забезпечити найкращі можливі результати безпеки. Рідні інтеграції рішень включають Sophos Endpoint, Sophos Mobile, Sophos Firewall, Sophos NDR, Sophos ZTNA [13].

Електронна пошта та Sophos Cloud сумісні із наявними інструментами та технологіями.

Використовуючи телеметрію з широкого спектру інструментів безпеки, що не належать Sophos, і отримаючи більшу рентабельність інвестицій існуючі інвестиції користувача в технології, одночасно прискорюючи операції безпеки. Інтеграція включає ідентифікацію, мережу,

брандмауер, електронну пошту, хмару, продуктивність і безпеку кінцевої точки технології [13].

Ключовими моментами є [13]:

отримати видимість підозрілих активності по всіх ключових атаках поверхні;

уніфікована платформа XDR із широким асортимент інтегрованих Рішення Sophos;

наявні інструменти та інвестиції з широкими технологіями не від Sophos інтеграції;

можливість розслідувати та надавати відповідь швидко реагувати на загрози за допомогою пріоритетних виявлень штучного інтелекту і оптимізовані робочі процеси.

2.2 Архітектура рішення Sophos Intercept X Endpoint, призначення та основні функції компонентів

Архітектура Sophos Intercept X Endpoint багаторівнева і мульти-модульна, складається з різних допоміжних компонентів.

Антивірусний модуль

Використовує традиційні методи захисту, такі як сигнатурний аналіз, для ідентифікації вже відомих зразків шкідливого ПЗ.

Моудль поглибленого вивчення

Це нейронна мережа, яка аналізує файли до їх виконання, щоб визначити потенційно шкідливу поведінку навіть у невідомих або нових загрозах. Модель глибокого навчання працює без необхідності регулярного оновлення сигнатур.

Запобігання експлойтам

Цей модуль відстежує дії, характерні для експлойтів (наприклад, коду, який використовує вразливості програмного забезпечення). Він захищає від

атак, які експлуатують вразливості у популярному ПЗ, як-от Microsoft Office або веб-браузери.

Модуль виявлення і запобігання атак

Компонент, який спеціалізується на виявленні й запобіганні атак з вимогою викупу (ransomware). Він аналізує процеси, що можуть шифрувати файли, та блокує їх ще до того, як почнеться шифрування даних.

Модуль дослідження й реагування на інциденти

Це інструмент для виявлення, дослідження й реагування на інциденти безпеки. Він надає можливість адміністраторам системи аналізувати поведінку підозрілих процесів та своєчасно реагувати на загрози. Завдяки EDR адміністратори можуть створювати аналітичні звіти, досліджувати інциденти та проводити ретроспективний аналіз.

Веб-контроль та мережевий захист від загроз

Дозволяє адміністраторам встановлювати правила для контролю за використанням додатків, обмежувати доступ до певних веб-сайтів, а також захищати від мережевих атак, таких як сканування портів або розсилки шкідливого трафіку.

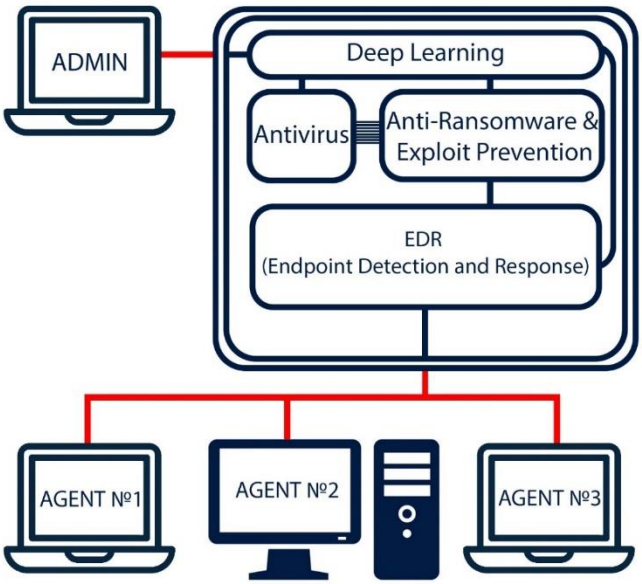


Рис. 2.2. Архітектура рішення Sophos Intercept x Endpoint

Розглянемо основні функції компонентів архітектури Sophos Intercept x Endpoint [14]:

захист від шкідливого програмного забезпечення. Виявлення, блокування та видалення шкідливих програм;

запобігання експлойтам. Захист від атак, спрямованих на вразливості в програмах;

захист від шифрувальних програм. Блокує спроби шифрування даних, не дозволяючи програмам зловмисників отримати доступ до файлів;

налітика та звітність. Адміністратори можуть аналізувати інциденти, отримувати звіти та рекомендації щодо дій;

контроль і політики безпеки. Дає можливість встановлювати обмеження на програми та веб-ресурси, що знижує ризики від соціальної інженерії.

Загалом рішення Sophos Intercept X Endpoint забезпечує комплексний захист завдяки багаторівневому підходу та використанню сучасних технологій, як-от глибоке навчання й EDR, дозволяючи протистояти сучасним загрозам.

2.3 Можливості рішення Sophos Intercept X Endpoint щодо розширеного виявлення загроз кінцевим точкам та реагування на них

Sophos Intercept X Endpoint надає розширені можливості для виявлення загроз на кінцевих точках і забезпечення оперативного реагування завдяки сучасним технологіям і інструментам для моніторингу, аналізу та нейтралізації інцидентів безпеки.

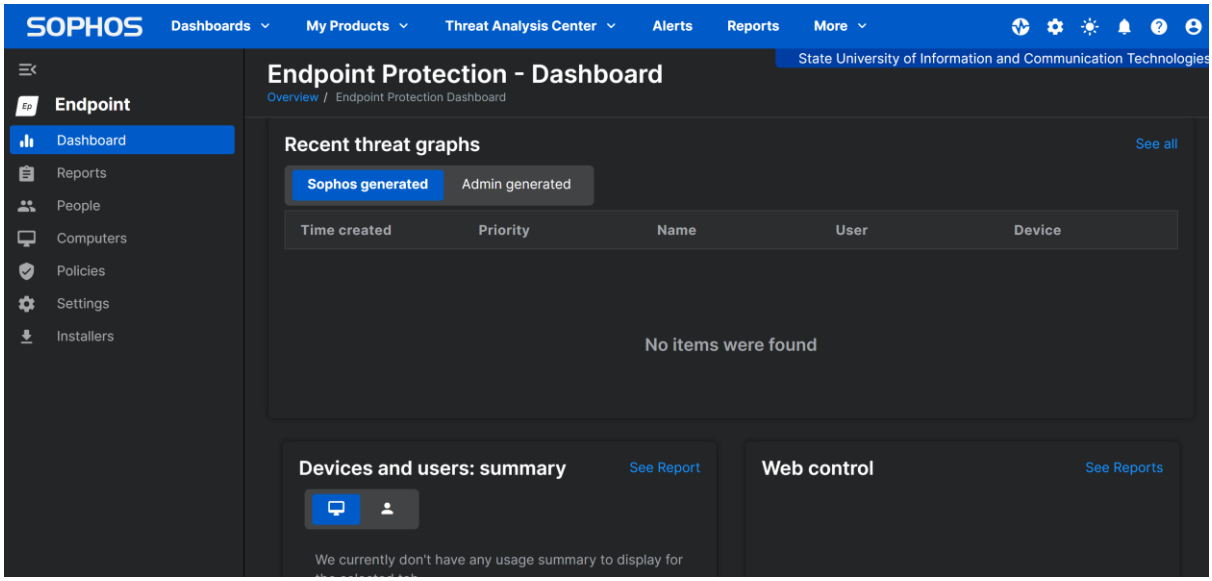


Рис. 2.3. Панель приладів

Система використовує Endpoint Detection and Response (EDR), який відстежує аномальну активність, застосовуючи поведінковий аналіз для раннього виявлення загроз. EDR також дозволяє адміністраторам досліджувати причини і наслідки інцидентів, аналізувати ланцюжок зараження і відстежувати всі дії зловмисного ПЗ, що сприяє кращому розумінню механізму атак [14].

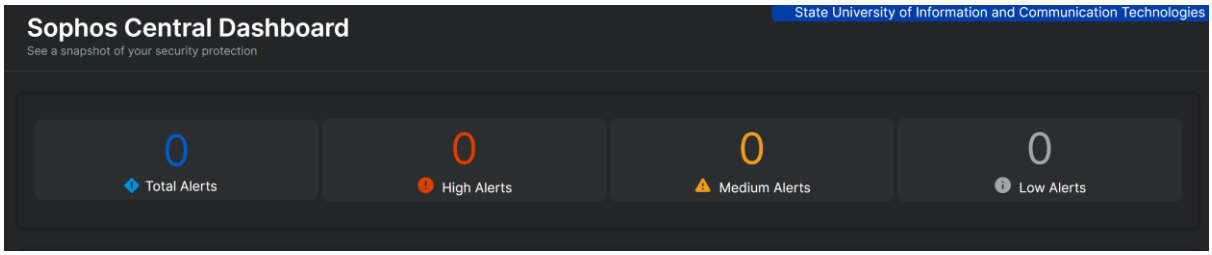


Рис. 2.4. Загальна статистика щодо поточного стану системи

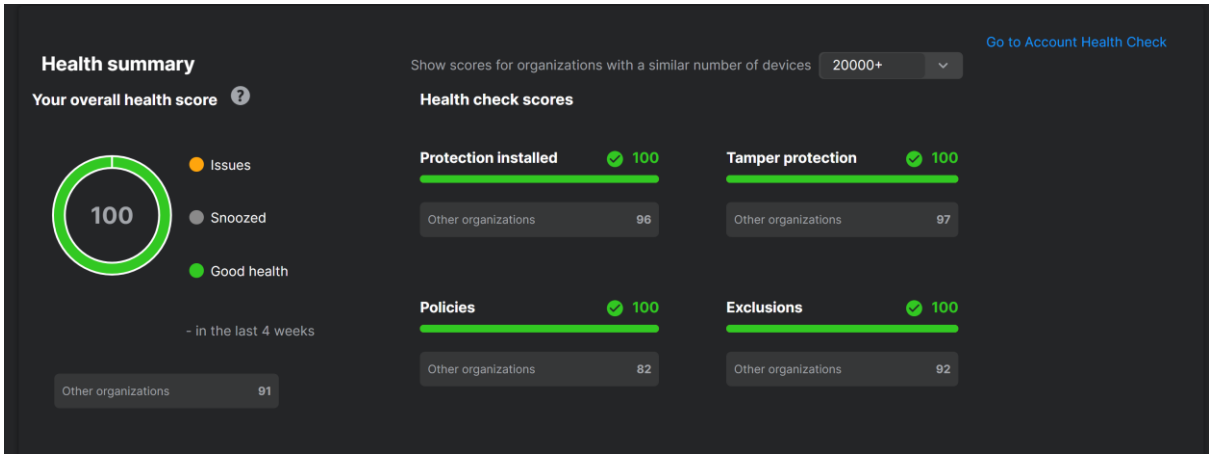


Рис. 2.5. Докладна статистика щодо поточного стану системи

Рішення включає глибокий аналіз файлів за допомогою модуля глибокого навчання, який прогнозує шкідливу активність ще до запуску файлів, виявляючи нові та невідомі загрози. Поведінковий аналіз забезпечує захист без необхідності у сигнатурах, блокуючи шкідливі дії, як-от несанкціоноване редагування пам'яті чи виконання небезпечного коду [14].

Механізм запобігання експлойтам блокує атаки, які використовують вразливості програмного забезпечення, включаючи вразливості нульового дня. Це дозволяє зупиняти поширення загроз через поширені вектори атак, суттєво підвищуючи безпеку кінцевих точок.

Функція Anti-Ransomware захищає від атак-вимагачів за допомогою технології CryptoGuard, яка виявляє та блокує спроби шифрування файлів, запобігаючи втраті даних. У разі успішного блокування атаки система може автоматично відновити файли до їхнього початкового стану, що передував інциденту.

Sophos Intercept X Endpoint підтримує хмарний аналіз загроз та Threat Intelligence з інтеграцією через Synchronized Security, що дозволяє обмінюватися інформацією між компонентами системи [14].

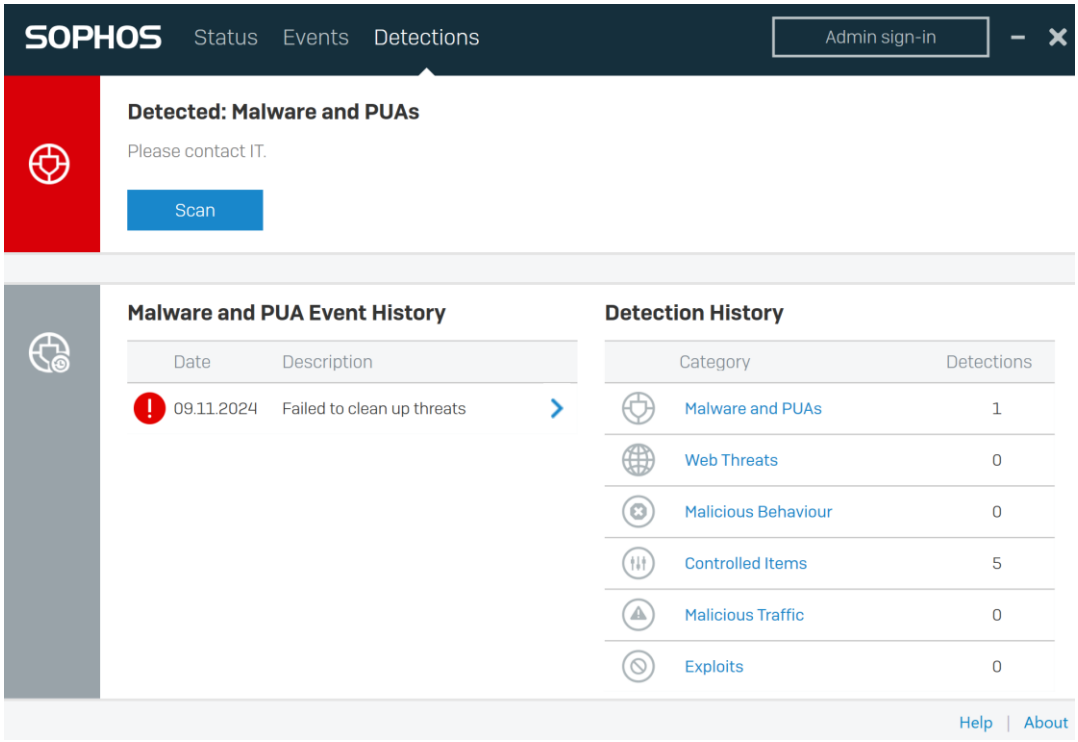


Рис. 2.6. Приклад, як Sophos виявляє загрози і попереджає про них

Це сприяє швидкому виявленню загроз як на рівні кінцевих точок, так і в інших елементах інфраструктури, таких як мережі. Хмарна аналітика загроз надає актуальні дані про нові загрози, що пришвидшує процес виявлення й аналізу небезпечної активності [14].

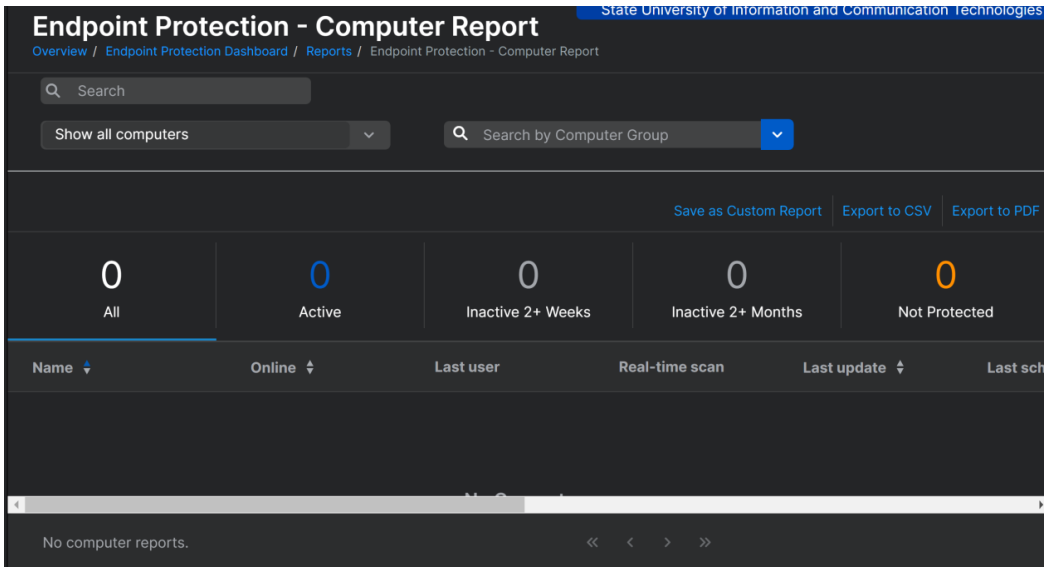


Рис. 2.7. Звітність щодо захисту кінцевих точок системи

Система також підтримує автоматизоване реагування на інциденти безпеки, при якому уражені пристрої можуть бути автоматично ізольовані, а шкідливі процеси – заблоковані для запобігання подальшого поширення загроз. Для команд безпеки надаються розширені можливості звітності та моніторингу з інструментами для створення звітів і дашбордів, що дозволяє відстежувати стан кінцевих точок у режимі реального часу [14].

Sophos Intercept X Endpoint поєднує можливості машинного навчання, поведінковий аналіз та розширені функції EDR, що гарантує високий рівень захисту кінцевих точок і сприяє ефективному реагуванню на сучасні кіберзагрози [14].

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ РОЗШИРЕНОГО ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИМ ТОЧКАМ ТА РЕАГУВАННЯ НА НИХ НА БАЗІ SOPHOS INTERCEPT X ENDPOINT

3.1 Розроблення варіанта технології системи розширеного виявлення загроз кінцевим точкам та реагування на них на базі Sophos Intercept x Endpoint

Sophos Intercept x Endpoint надає нам необмежений функціонал і можливість налаштування його для власного комфорту. Впровадження використання саме цих функцій і модулів є одним з найкращих варіантів технології системи розширеного виявлення загроз, які розраховані на кінцеві точки.

Інформаційна панель показує дані про сповіщення, події, користувачів, пристрої тощо.

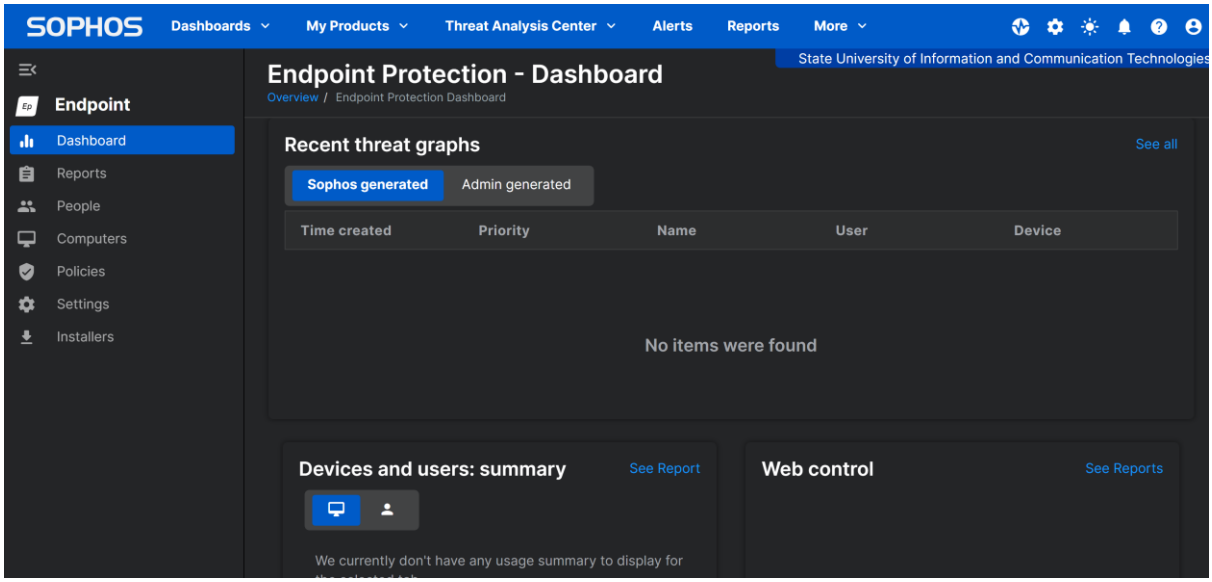


Рис. 3.1. Інформаційна панель

Надається можливість здійснити огляд інформаційної панелі центрального огляду, де в свою чергу відображається найважливіша інформація про сповіщення, пристрої та користувачів. Також можливо оглянути інформаційну панель перевірки стану облікового запису.

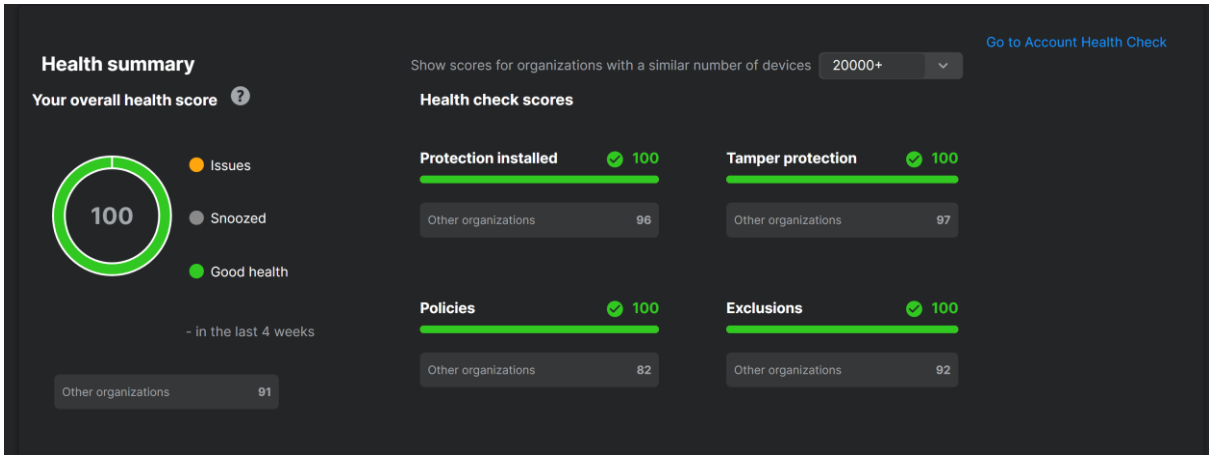


Рис. 3.2. Поточний стан пристроїв

Можливо побачити інформаційні панелі для окремих продуктів на сторінках цього продукту. Також можливо додати деякі з цих інформаційних панелей для певного продукту в меню «Інформаційні панелі».

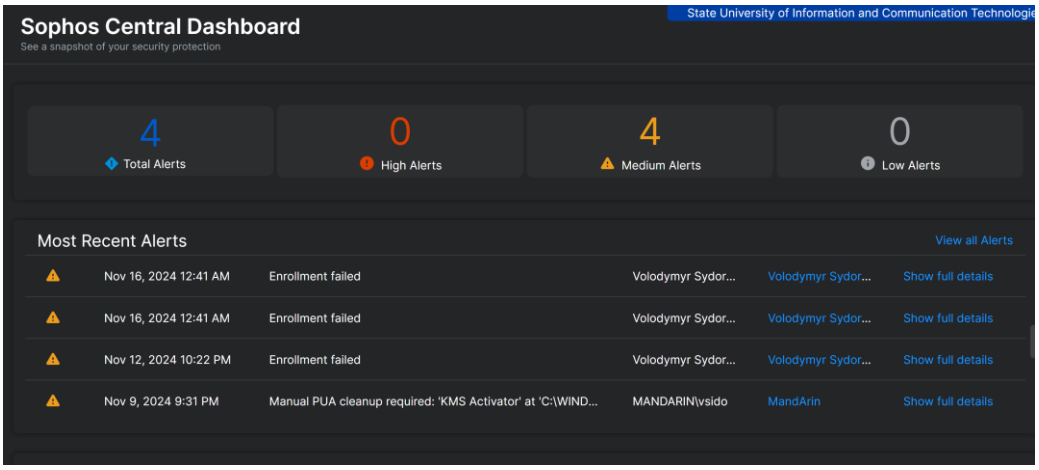


Рис. 3.3. Додаткова інформація на інформаційній панелі

Також хочеться виділити спеціальні інформаційні панелі, де надається можливість створювати власні інформаційні панелі, які відображатимуть потрібну інформацію. Ці інформаційні панелі призначені лише для осоистісного використання. Інші адміністратори їх не бачать.

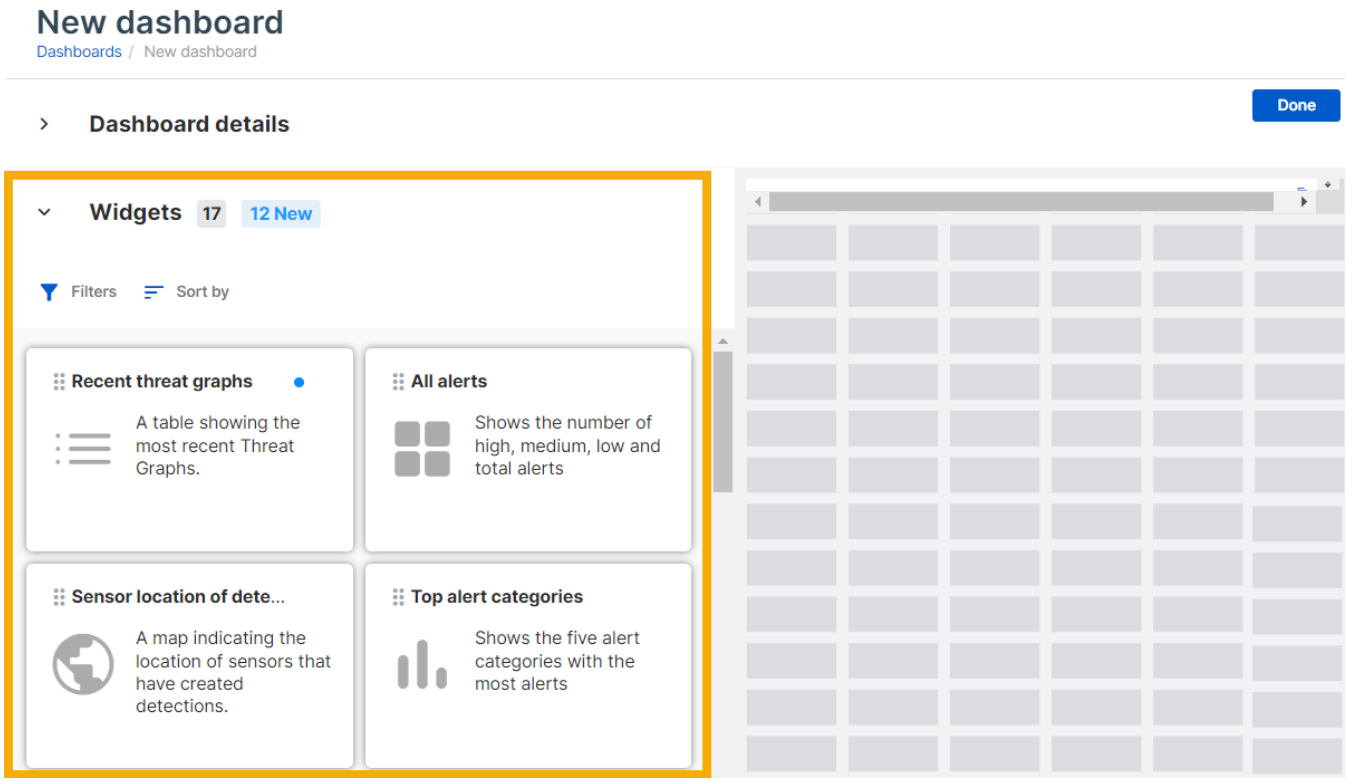


Рис. 3.4. Можливість кастомізації інформаційної панелі

Вкладка «Звіти» містить список звітів, які можна створити про функції безпеки в Sophos Central.

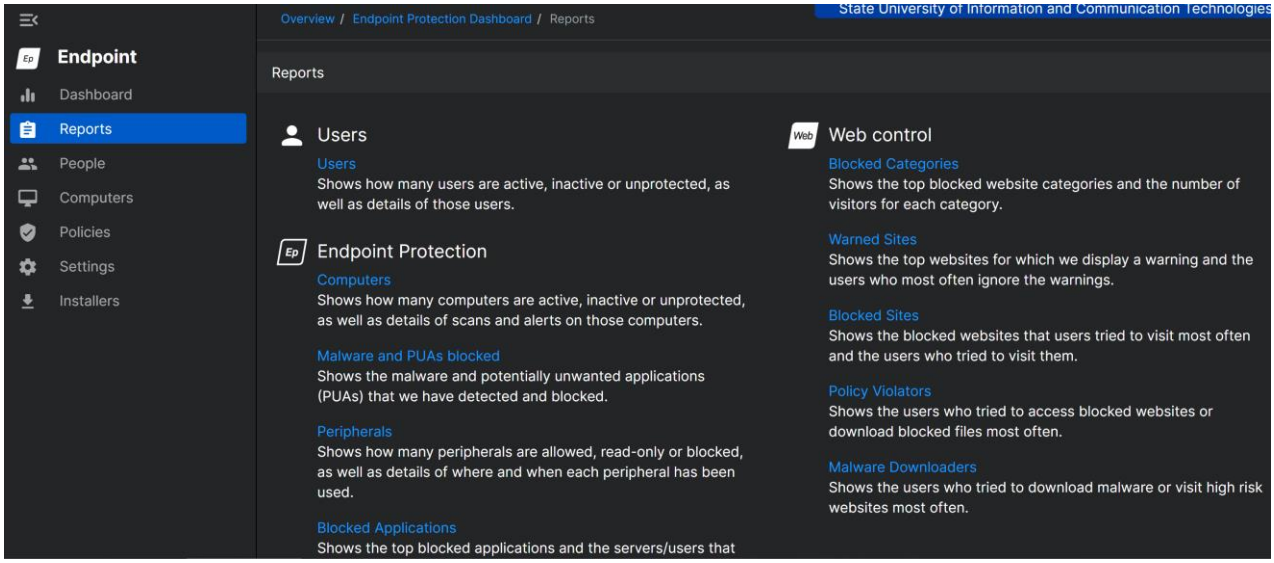


Рис. 3.5. Звіти

Можливо переглядати журнали звітів. Також надається можливість форматування, редагування звітів і перегляд власника цих звітів.

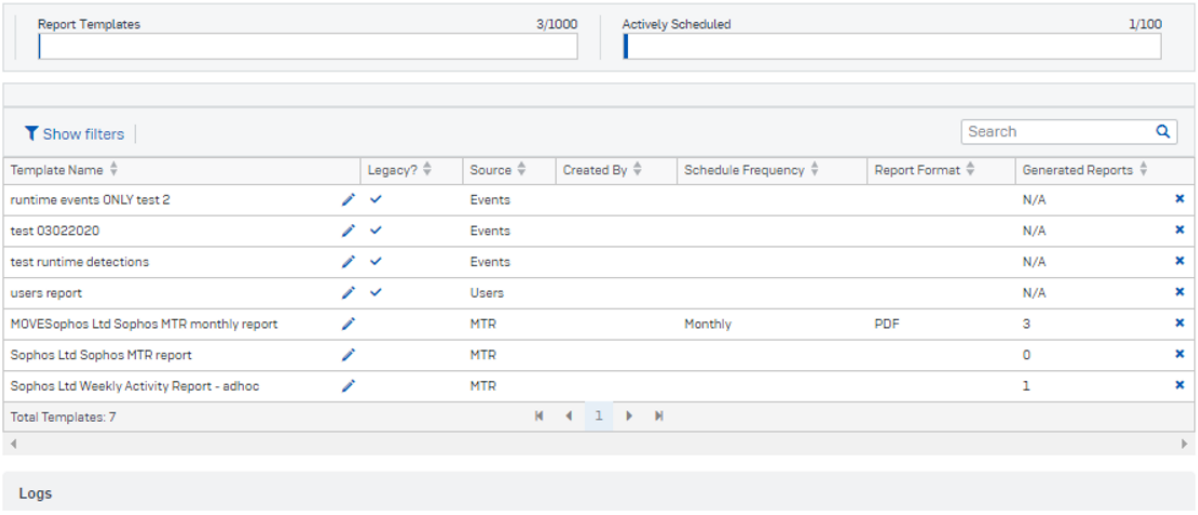


Рис. 3.6. Журнал звітів

Нижче наведені приклади звітності, які можна переглянути, та яку саме інформацію вони надають користувачеві.

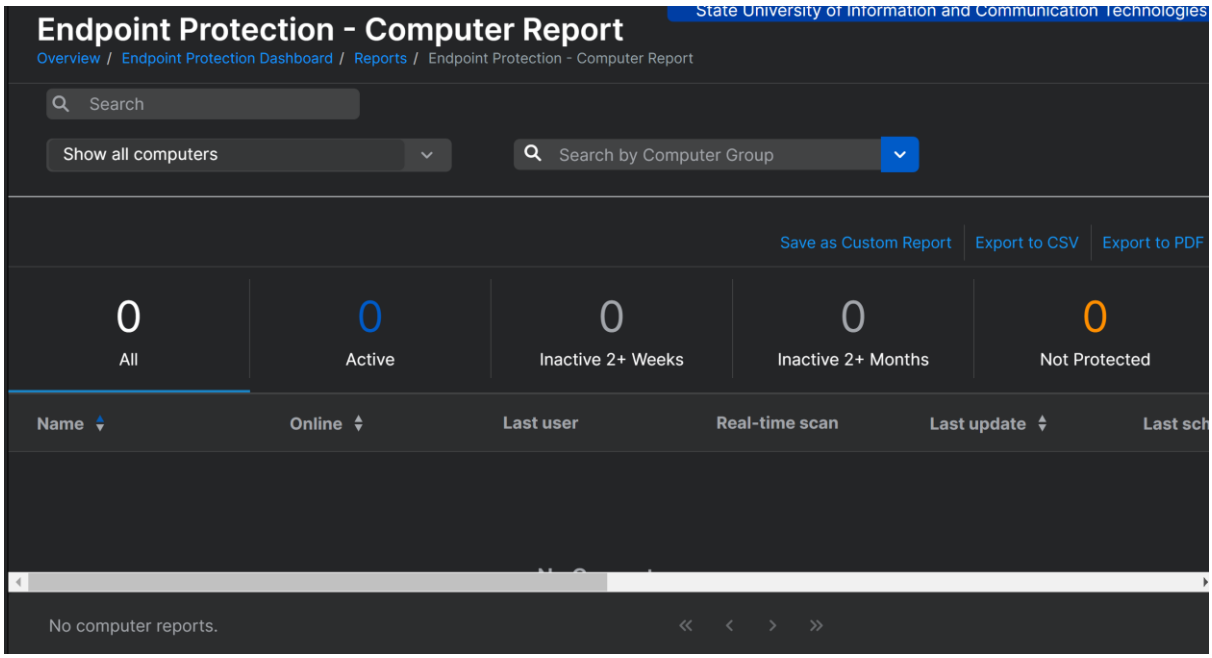


Рис. 3.7. Приклад різних звітів (Звіт про поточний стан комп’ютера)

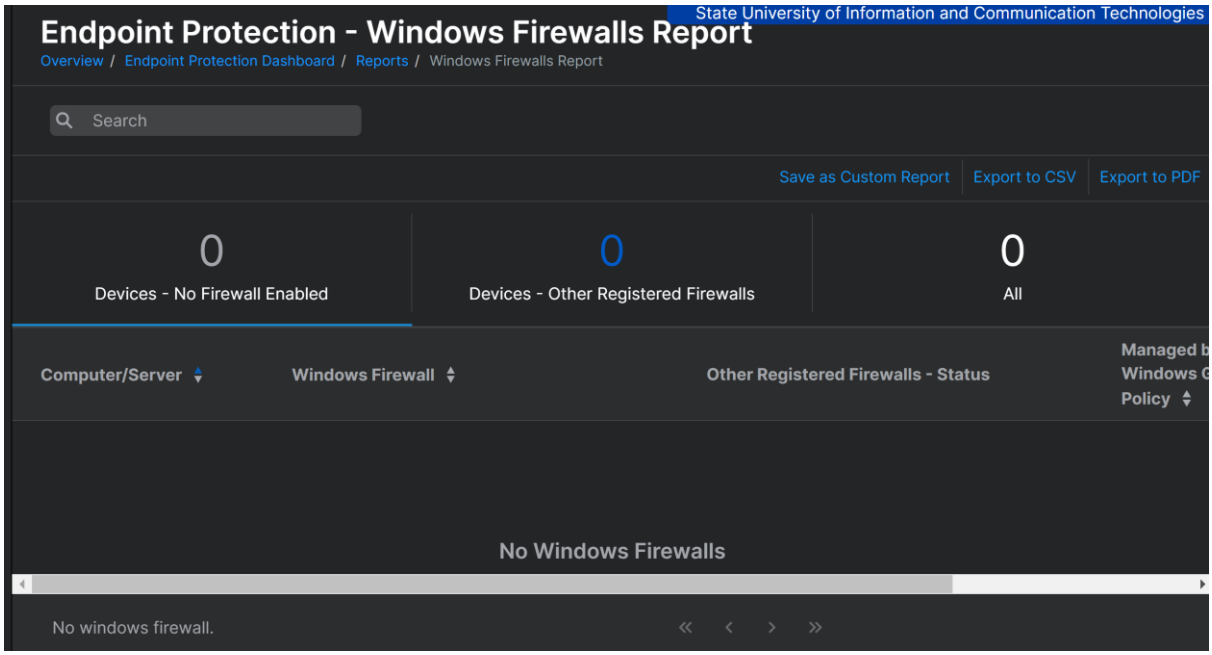


Рис. 3.8. Приклад різних звітів (Звіт про поточний стан Фаєрволу Windows)

Хочеться приділити увагу безпеці електронної пошти. В цілому, якщо актуальність підключених доменів до Sophos Gateway і Sophos Mailflow присутня – то, можна побачити одну панель для кожного типу підключення.

Панель безпеки електронної пошти використовує інтерактивні звіти. Коли користувач змінює період часу, усі області інформаційної панелі електронної пошти негайно оновлюються.

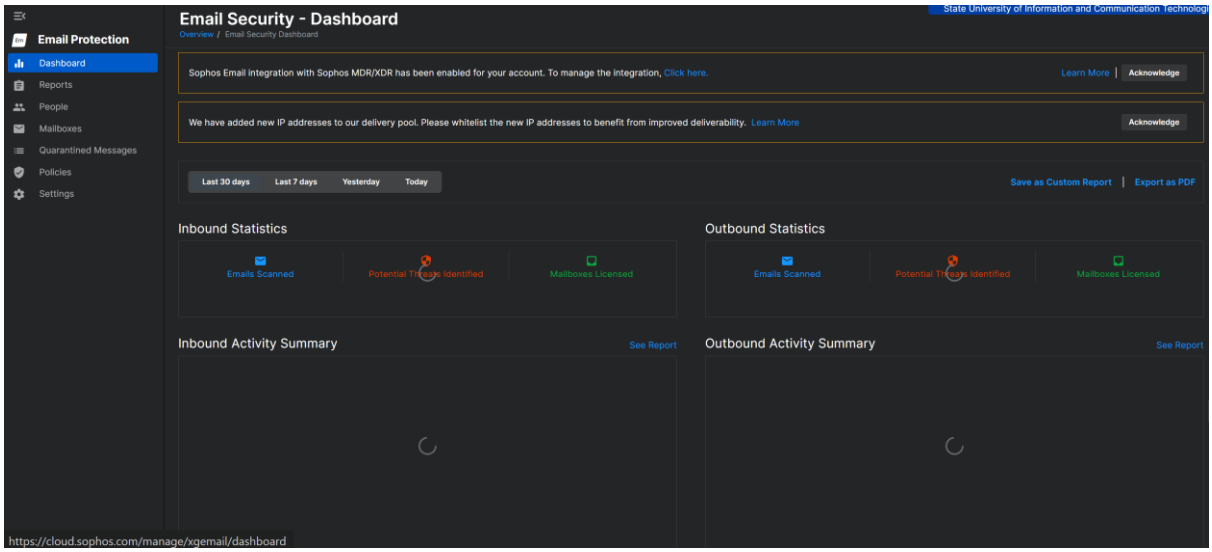


Рис. 3.9. Панель безпеки електронної пошти

Рішення надає комплексний захист і підхід до захисту електронної пошти. Маючи багаторівневі модулі, здатні комплексно реагувати на внутрішні і зовнішні загрози.

Sophos Mailflow захищає електронні листи Microsoft 365. Він безпосередньо інтегрується з Microsoft 365 із службами Microsoft Exchange Connector для сканування електронних листів. Sophos Mailflow використовує Microsoft API для створення правил потоку пошти у середовищі користувача Microsoft 365. Ці правила потоку електронної пошти направляють електронні листи до Sophos і назад до Microsoft 365. Налаштування Sophos Mailflow виконується з Sophos Central [14].

Sophos Gateway – це визнаний метод захисту електронної пошти. Він розроблений для захисту локальних середовищ електронної пошти, а також працює з усіма хмарними службами електронної пошти, наприклад Google Workspace.

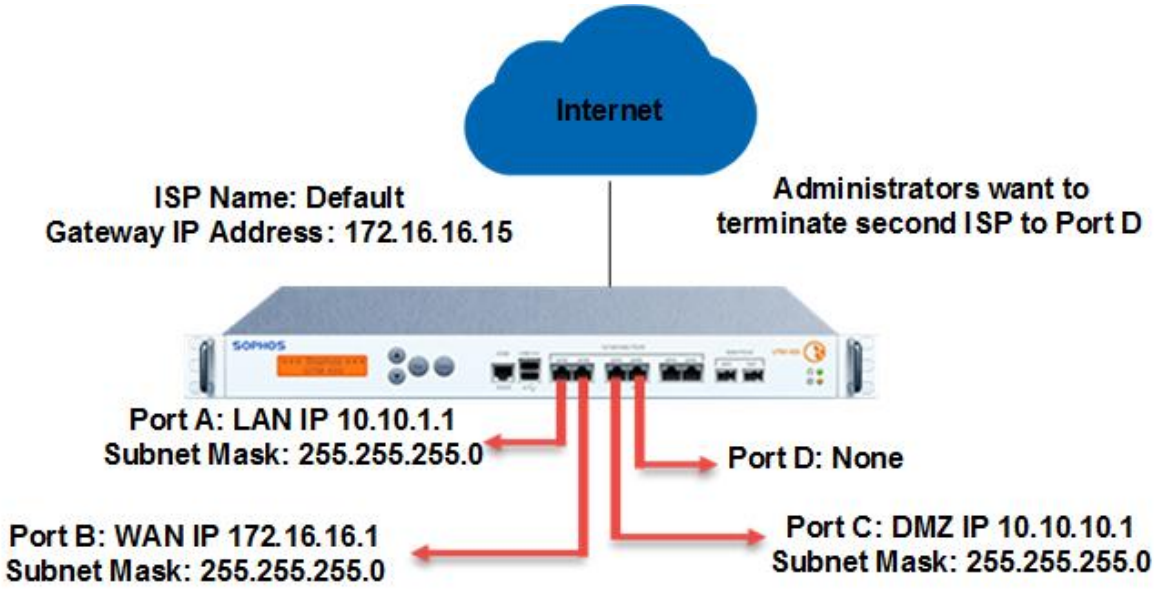


Рис. 3.10. Схема роботи Sophos Gateway [14]

Якщо формувати просте уявлення про підхід до захисту елеткронної пошти то основні модулі захищають від спаму та інших небажаних повідомлень, контролюють дані запобігаючи видаленню даних із організації користувача. Надає можливість безпечних повідомлення, контролюючи шифрування електронних листів та інші функції безпеки.

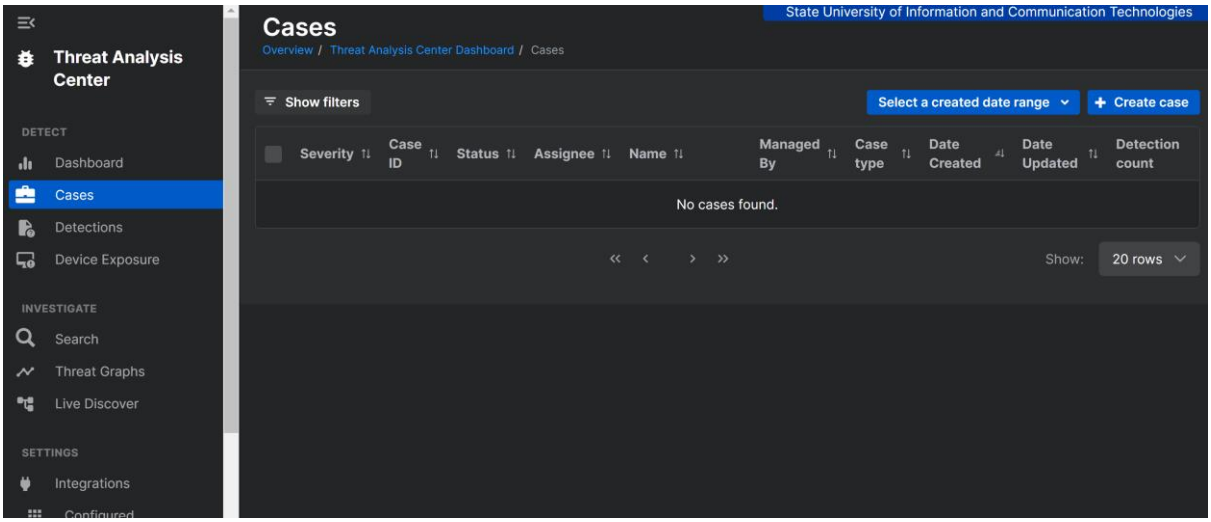


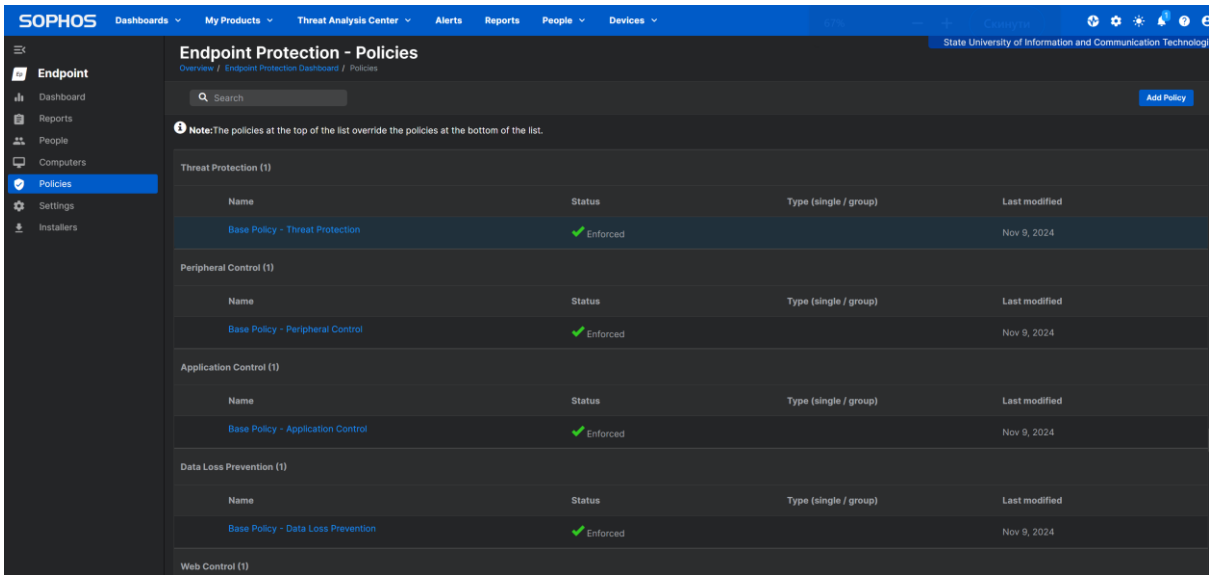
Рис. 3.11. Панель статистики

Стрічка статистики має розширений і зрозумілий інтерфейс, де можна переглянути відомості про виявлені загрози та просканові електронні листи за вибраний період часу.

Веб-контроль показує статистику захисту вашого веб-контролю. Цифри наведено для заблокованих загроз, заблокованих порушень політики та попереджень політики. Існує також цифра для «попереджень щодо політики», тобто кількості користувачів, які обійшли попередження та відвідали веб-сайт [14].

Інформаційні панелі використовують невеликі елементи інтерфейсу користувача, які називаються віджетами, щоб відображати інформацію про сповіщення, користувачів, пристрої, політики, стан безпеки тощо. Користувач може створювати власні інформаційні панелі за допомогою наданих Sophos віджетів [14].

Політика – це набір параметрів (наприклад, налаштувань для захисту від шкідливих програм), які Sophos Central застосовує до захищених користувачів, пристроїв, серверів або мереж [14].



3.12. Політики Sophos

Існує політика для кожного продукту або функції, яка є частиною продукту. Наприклад, існує політика для функції контролю програми. Призначена користувачу роль адміністратора впливає на можливості користувача.

Sophos XDR (Extended Detection and Response) дозволяє досліджувати виявлені загрози (графіки загроз) і шукати нові загрози або слабкі місця безпеки. Це також дозволяє контролювати пристрої та виправляти проблеми віддалено. Sophos XDR Sensor пропонує альтернативний спосіб отримати функції XDR. Користувач не отримує захист від загроз, але отримуєте деякі функції виявлення, дослідження та реагування [14].

Sophos XDR Sensor не підтримує Sophos Security Heartbeat, функцію, яка дозволяє пристроям регулярно повідомляти про свій стан безпеки брандмауеру Sophos.

3.2 Технологія застосування рішення Sophos Intercept X Endpoint

Sophos Intercept X Endpoint є одним із провідних рішень для захисту кінцевих точок, яке поєднує багаторівневу безпеку, штучний інтелект, глибоке навчання та сучасні технології Extended Detection and Response (XDR). Управління цією програмою відбувається через централізовану платформу Sophos Central, що забезпечує гнучкість, ефективність і прозорість для адміністраторів.

Розглянемо всі ключові аспекти технології управління Sophos Intercept X Endpoint, включаючи архітектуру, функціональні можливості, процеси впровадження та переваги.

Архітектура Sophos Intercept X Endpoint

Архітектура програми передбачає два основні компоненти:

Агент Sophos Intercept X Endpoint – встановлюється на кінцеві точки (персональні комп’ютери, ноутбуки, сервери).

Його функції:

постійний моніторинг системи;

виявлення підозрілої активності;

захист від загроз у реальному часі;

автоматичне реагування на інциденти.

Sophos Central – хмарна платформа управління:

єдиний центр адміністрування всіх пристроїв;

налаштування політик безпеки;

моніторинг стану системи;

звітування та аналітика.

Ця архітектура дозволяє ефективно захищати кінцеві точки без необхідності складного локального адміністрування.

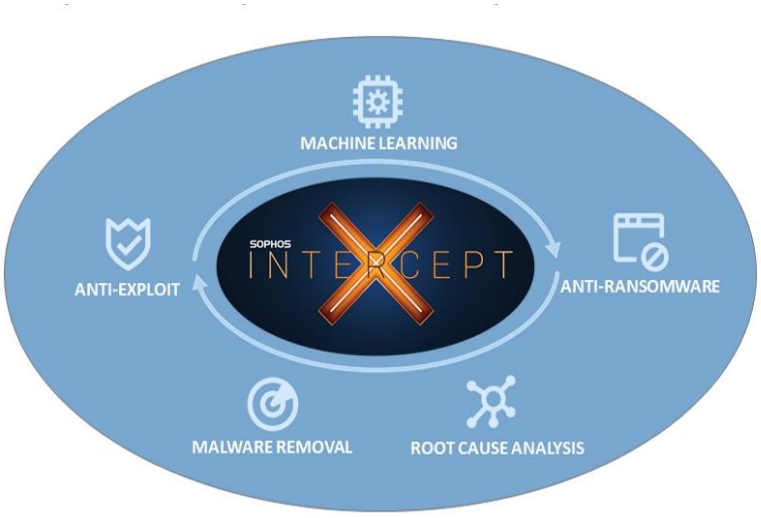


Рис. 3.13 Спрощений вигляд архітектури даного рішення [14]

Sophos Intercept X Endpoint інтегрує найсучасніші технології кібербезпеки:

Deep Learning

Це технологія штучного інтелекту, яка аналізує величезні обсяги даних для виявлення:

відомих загроз (на основі сигнатур);

невідомих або нульових загроз (Zero-Day);

складних атак, включаючи безфайлові.

CryptoGuard

Захищає від програм-вимагачів (ransomware), блокуючи процеси шифрування даних у реальному часі. Навіть якщо шифрування вже почалося, CryptoGuard здатний відновити змінені файли.

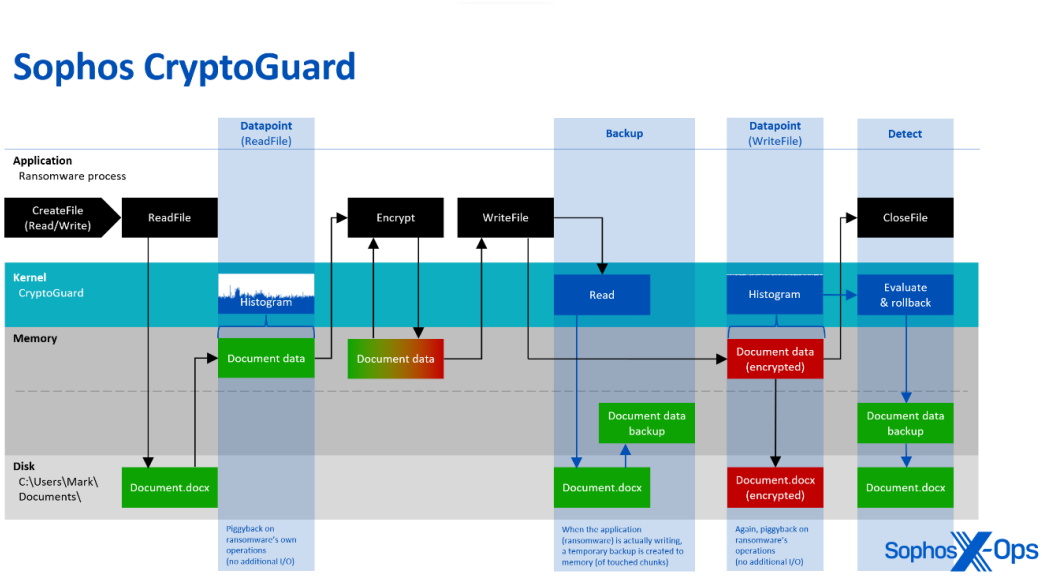


Рис. 3.14. Sophos Crypto Guard [14]

Антиексплойт-захист

Запобігає використанню вразливостей у програмному забезпеченні. Це особливо важливо для захисту програм, які не були вчасно оновлені.

Extended Detection and Response (XDR)

XDR об'єднує дані з різних джерел (кінцеві точки, сервери, мережі) для створення повної картини атак. Це дозволяє:

виявляти загрози, які раніше залишалися непоміченими;

відслідковувати джерела атак;

надавати детальну інформацію для усунення загрози.

Захист від безфайлових атак

Sophos Intercept X Endpoint аналізує поведінку додатків і процесів, виявляючи підозрілі дії навіть без присутності файлів-загроз.

Процеси управління

Додавання пристроїв:

ручна інсталяція. Завантаження агента через Sophos Central та його встановлення на пристрій;

інтеграція з Active Directory. Автоматичне додавання пристроїв до системи через синхронізацію з AD;

масове розгортання. Інсталяція агента через сценарії або інструменти управління конфігурацією (SCCM);

Управління політиками:

Sophos Central дозволяє створювати та застосовувати політики безпеки для різних груп пристроїв. Основні функції:

контроль доступу до зовнішніх пристроїв (USB, принтери);

налаштування веб-фільтрації для обмеження доступу до небезпечних сайтів;

захист програмного забезпечення через контроль дозволених додатків (Application Control).

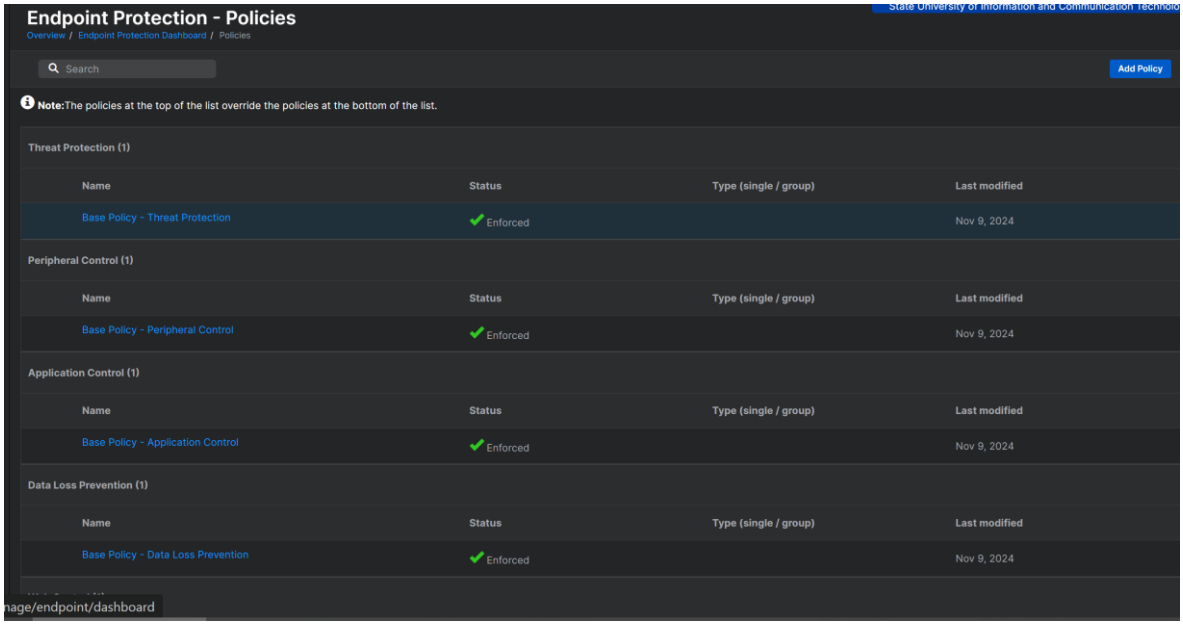


Рис. 3.15. Налаштування політик в даному рішенні

Моніторинг стану

Sophos Central забезпечує:

огляд у реальному часі стану пристроїв;

повідомлення про інциденти безпеки;

детальні звіти про типи та кількість загроз.

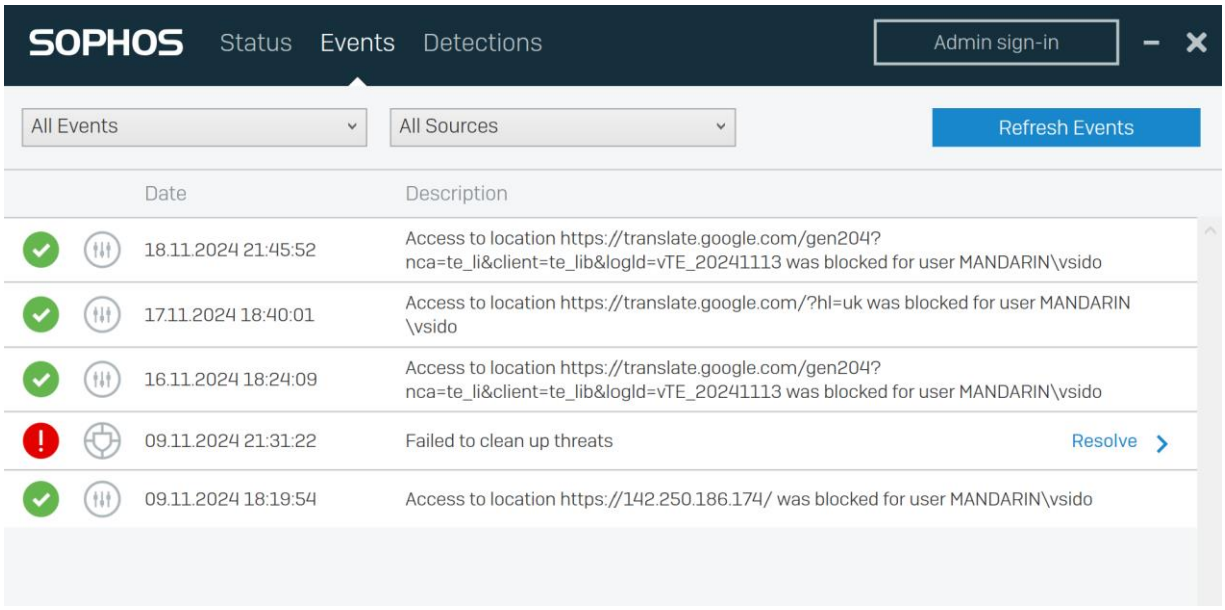


Рис. 3.16. Моніторинг стану за допомогою подій в Sophos

Реагування на загрози

Sophos Intercept x Endpoint пропонує два підходи:

автоматичне реагування. Система самостійно блокує загрози, видаляє шкідливі файли або ізолює заражений пристрій;

ручне втручання. Адміністратор може аналізувати загрозу, виконувати ізоляцію, запускати глибокий сканер або відновлювати систему.

Оновлення

Sophos Intercept X Endpoint автоматично отримує оновлення баз загроз і програмного забезпечення через Sophos Central, забезпечуючи захист від нових видів атак.

Переваги Sophos Central для управління

Хмарна платформа

Адміністратори можуть керувати кінцевими точками з будь-якого місця через веб-інтерфейс.

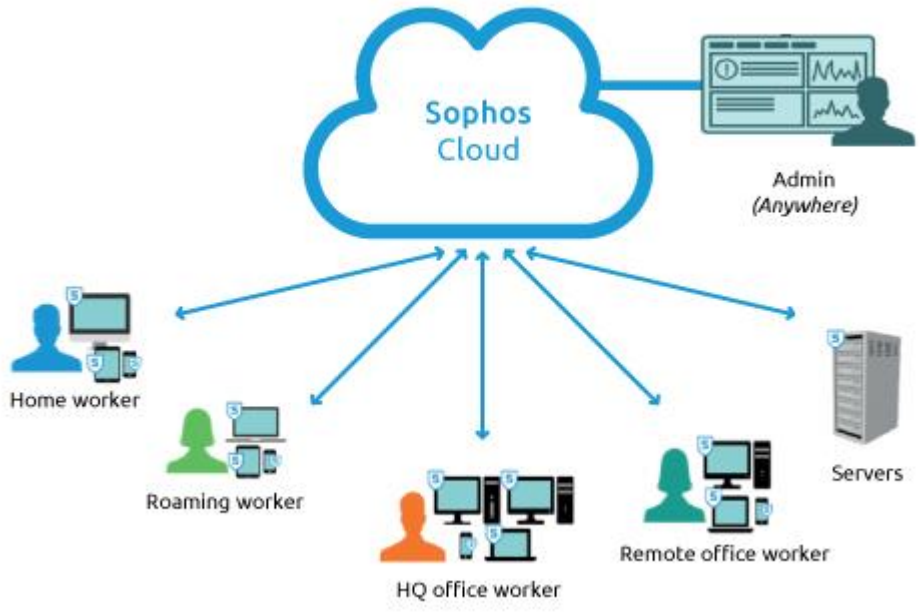


Рис. 3.17. Приклад хмарної технології [14]

Інтеграція з іншими продуктами Sophos

Sophos Central дозволяє об'єднувати Endpoint Protection, Email Security, Firewall та інші продукти в єдину екосистему.

Інтуїтивно зрозумілий інтерфейс

Дашборд надає повну інформацію про стан пристроїв, інциденти та політики.

Автоматизація завдань

Можливість автоматизувати реагування на певні типи загроз, що мінімізує людський фактор.

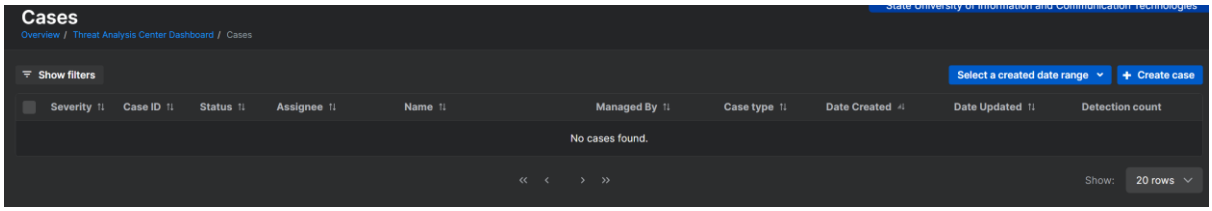


Рис. 3.18. Можливість автоматизації завдань

Розширені функції XDR

Sophos Intercept X Endpoint із XDR дає змогу глибоко аналізувати загрози:

кореляція даних. Інтеграція даних із кінцевих точок, серверів і мереж для виявлення складних атак;

деталізація інцидентів. Кожен інцидент має хронологію подій, що дозволяє зрозуміти, як загроза проникла в систему;

інтеграція з іншими системами безпеки. Дані можуть бути використані для подальшого аналізу через сторонні інструменти.

Переваги Sophos Intercept X Endpoint:

комплексний захист. Виявлення та блокування як простих, так і складних загроз (Zero-Day, ransomware, безфайлових атак);

простота управління. Централізоване адміністрування через Sophos Central;

швидке реагування. Автоматизація процесів забезпечує миттєве блокування загроз;

масштабованість. Підходить як для малого бізнесу, так і для великих корпорацій;

інтеграція з XDR. Дозволяє отримати детальну картину інцидентів і забезпечує кращий контроль.

Реалізація в організації

Підготовчий етап. Проведення аудиту існуючої IT-інфраструктури для виявлення слабких місць і планування розгортання.

Тестування. Запуск пілотного проекту для перевірки ефективності Sophos Intercept X Endpoint у певній частині інфраструктури.

Повномасштабне впровадження. Масова інсталяція агента, налаштування політик безпеки та інтеграція з іншими системами.

Навчання персоналу. Тренінги для IT-адміністраторів та співробітників щодо використання платформи та дотримання правил кібербезпеки.

З вище сказаного можна резюмувати, що Sophos Intercept X Endpoint це – рішення, яке забезпечує надійний захист кінцевих точок завдяки сучасним технологіям, зручному управлінню та інтеграції з іншими компонентами кіберзахисту. Воно ідеально підходить для компаній, які прагнуть захистити свої дані від сучасних кіберзагроз.

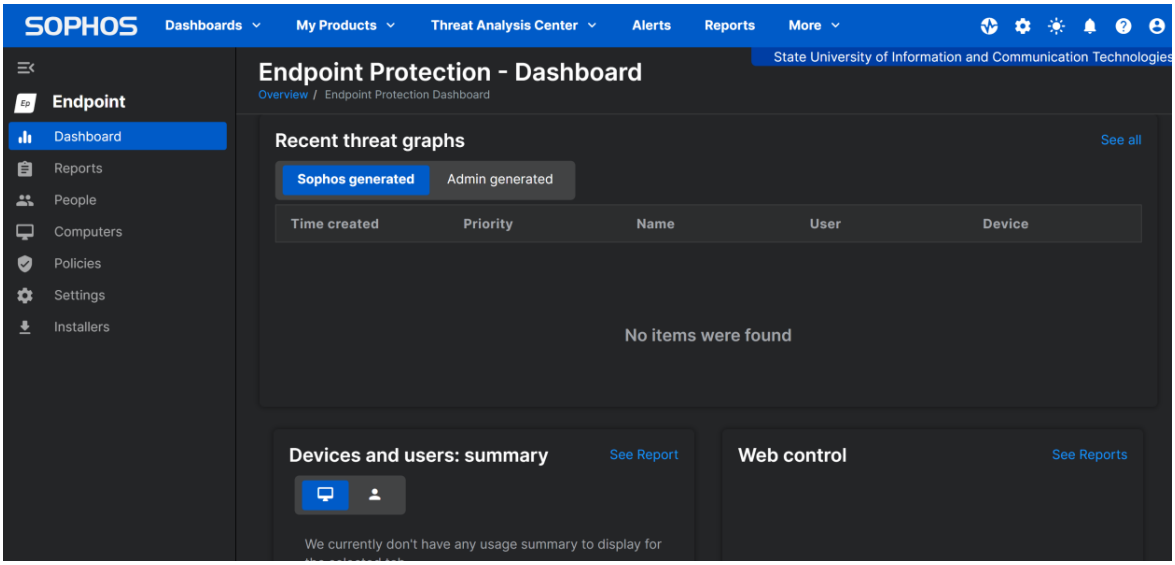


Рис. 3.19. Sophos Central

Для роботи рішення на кінцевих точках встановлюється спеціальний агент Sophos Intercept X, який відповідає за моніторинг активності, виявлення загроз та реагування на них. Sophos Central надає зручний веб-інтерфейс, через який адміністратори можуть відслідковувати стан пристроїв, отримувати звіти про загрози, встановлювати політики безпеки та автоматизувати оновлення.

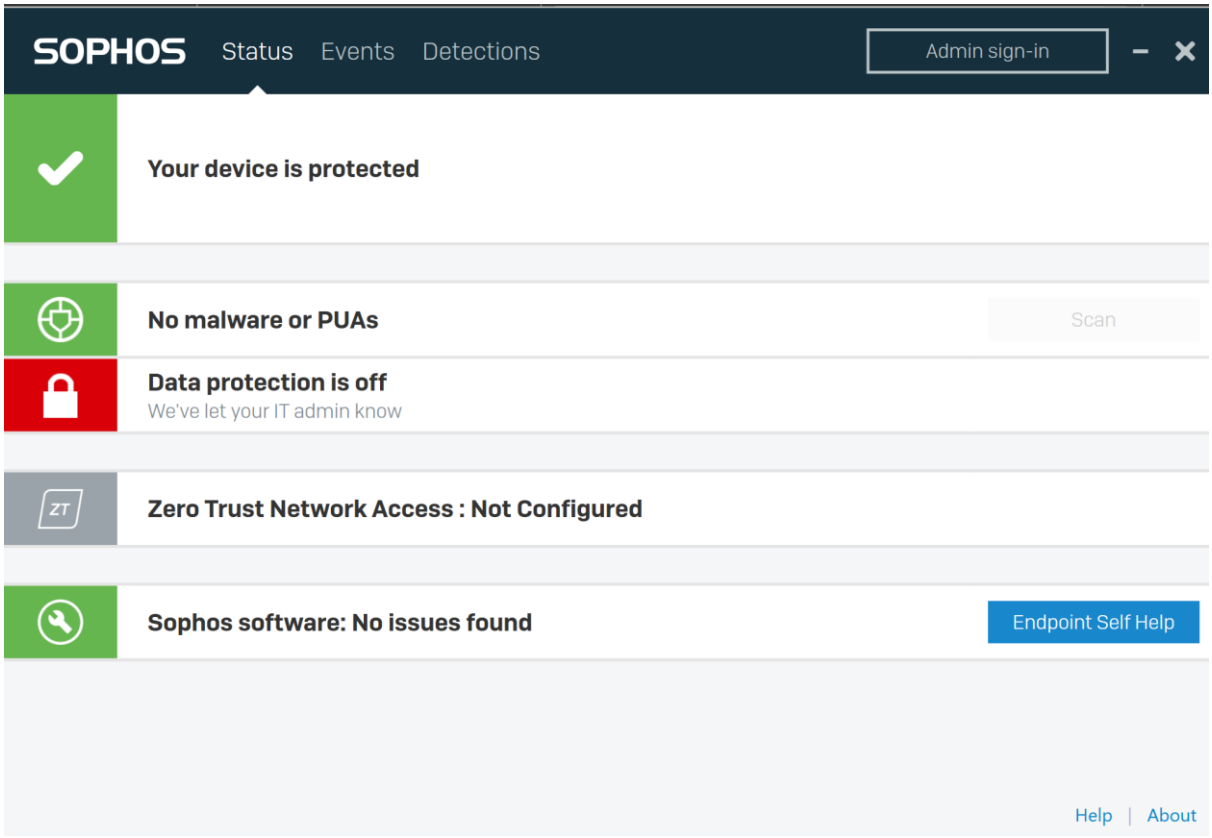


Рис. 3.20. Sophos Intercept X

Система пропонує розширені можливості моніторингу та реагування, включаючи автоматичне блокування підозрілих процесів, ізоляцію інфікованих пристроїв та відновлення пошкоджених файлів.

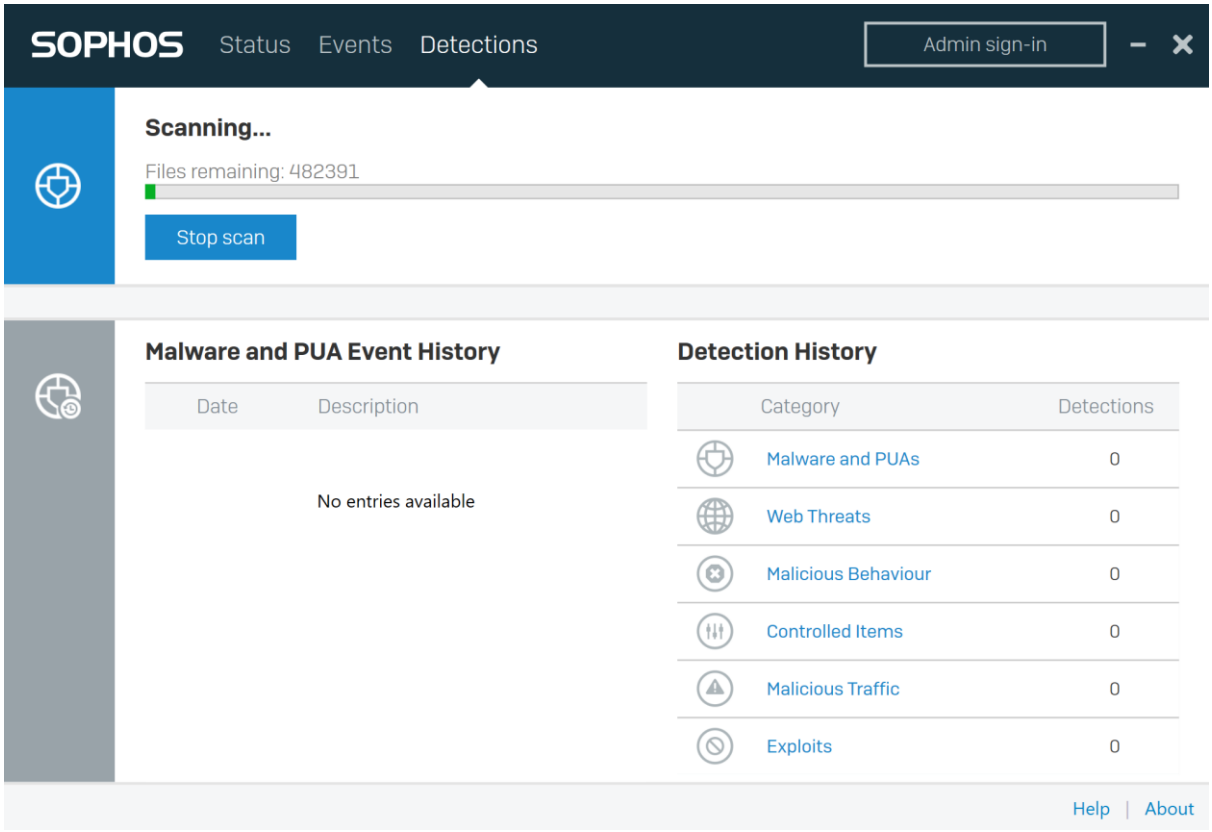


Рис. 3.21. Перевірка/діагностика системи на наявність загроз

Також є можливість глибокого аналізу інцидентів через функції Extended Detection and Response (XDR), що дозволяє корелювати дані з різних джерел для побудови єдиної картини атаки. Sophos Intercept X Endpoint забезпечує високий рівень безпеки завдяки технологіям штучного інтелекту, які виявляють як відомі, так і нові загрози, а також захищають від складних атак, включаючи програми-вимагачі та безфайлові атаки.

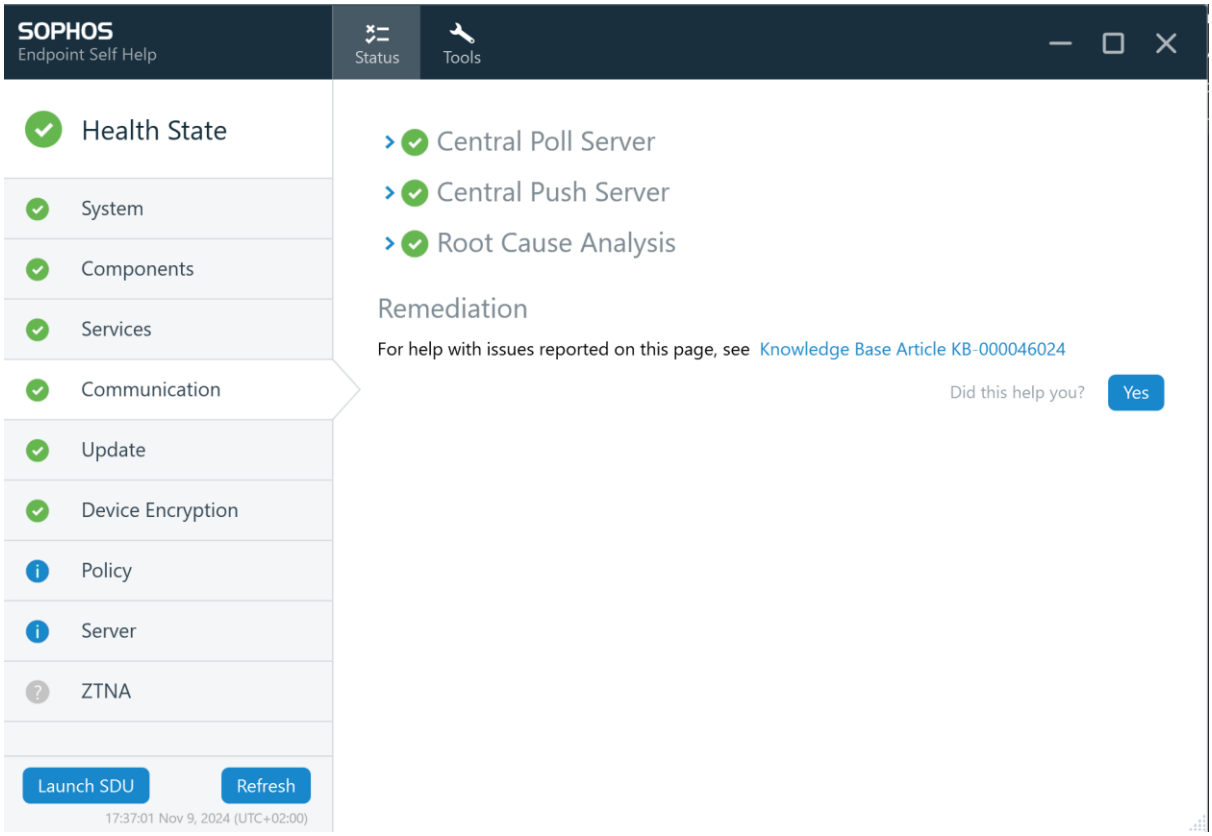


Рис. 3.22. Поточний статус системи

Серед ключових функцій рішення варто відзначити контроль USB-пристроїв, обмеження доступу до певних програм, автоматизацію оновлень та детальні звіти для аналізу інцидентів.

Sophos Intercept X Endpoint також інтегрується з іншими продуктами Sophos, що дозволяє створити комплексну екосистему кіберзахисту.

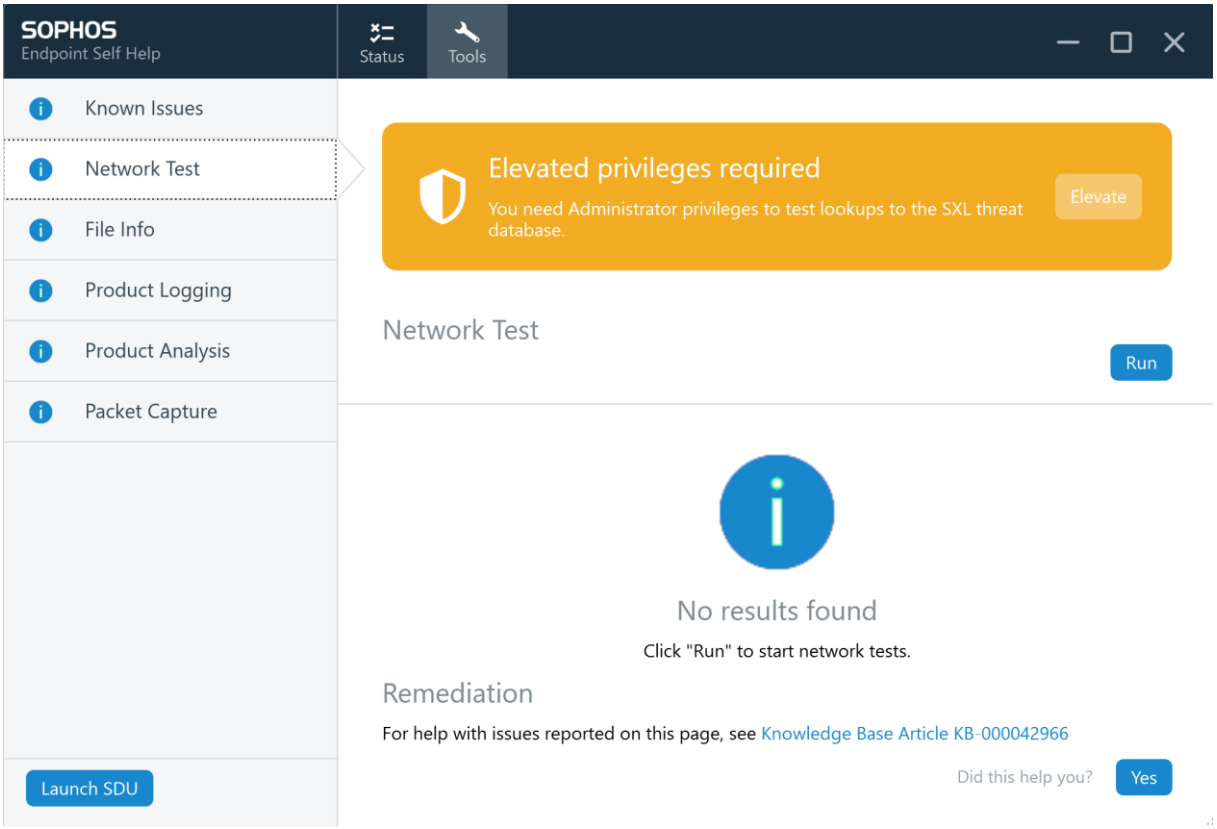


Рис. 3.23. Інструменти Sophos Intercept X Endpoint

Ця система ефективно працює навіть у великих інфраструктурах і підходить для організацій будь-якого масштабу.

Даний вендор є потужним рішенням для захисту кінцевих точок, яке об'єднує сучасні технології виявлення, аналізу та нейтралізації кіберзагроз. Управління цим продуктом здійснюється через хмарну платформу Sophos Central, яка дозволяє централізовано контролювати всі підключені пристрої.

3.3 Рекомендації щодо розширеного виявлення загроз кінцевим точкам та реагування на них

У підсумку хотілось би сформулювати конкретні рекомендації щодо технології розширеного виявлення загроз кінцевим точкам та реагування на них.

Необхідно визначення потреб організації, а саме обсяг і тип даних, які треба захистити, потенційні загрози, які потрібно контролювати, а також рівень чутливості до різних типів атак.

Інтеграція із існуючою інфраструктурою, перевірка сумісності з операційними системами, мережею та програмним забезпеченням організації. Це забезпечить легке розгортання та подальше керування системою.

Розгортання Sophos Intercept X Endpoint і встановлення агентів на кінцеві точки (робочі станції, сервери, мобільні пристрої) для забезпечення моніторингу в реальному часі.

Налаштування політик безпеки для виявлення різних типів загроз, таких як шкідливе ПЗ, фішингові атаки та підозрілі дії користувачів.

Налаштування розширеного моніторингу та виявлення загроз і налаштування базових правил EDR для визначення аномалій та підозрілих активностей на основі поведінкових патернів.

Інтеграція із штучним інтелектом та машинним навчанням: використання вбудованих алгоритмів Sophos для автоматичного виявлення невідомих загроз та запобігання поширенню атаки в мережі.

Автоматизація реагування та запобігання, що є автоматичним блокуванням загроз, налаштуванням автоматичних реакцій, таких як ізоляція кінцевої точки, видалення загрози та припинення шкідливої активності.

Сигналізація та повідомлення про загрози. Автоматичне надсилання сповіщень для адміністраторів безпеки або інших відповідальних осіб.

Присутність аналітики та звітності забезпечить розробку панелі моніторингу, централізований огляд активностей і загроз, що дозволяє стежити за загальним станом безпеки мережі.

Звітування про події визначить налаштування регулярних звітів про спроби атак, зупинені загрози та загальний стан безпеки.

Навчання співробітників щодо безпечного використання систем та реагування на сповіщення про потенційні загрози.

Покращення алгоритмів виявлення загроз через регулярні оновлення та вдосконалення політик безпеки, що базуються на нових загрозах.

Оцінка ефективності та корекція забезпечить моніторинг продуктивності та аналіз ефективності рішення EDR для оцінки його здатності швидко та ефективно реагувати на загрози. Корекція налаштувань відповідно до змін в інфраструктурі або нових типів загроз.

Ці кроки допоможуть побудувати надійну систему розширеного виявлення загроз, яка автоматично реагує на атаки, захищаючи кінцеві точки організації від сучасних кібератак.

ВИСНОВКИ

В роботі проведено дослідження проблеми розширеного виявлення загроз кінцевим точкам, визначено її мету та завдання.

Проведено аналіз існуючих технологій захисту кінцевих точок. Технологія розширеного виявлення загроз кінцевим точкам та реагування на них (EDR) забезпечує інтегрований підхід до протидії складним кіберзагрозам. Вона дозволяє поєднати виявлення загроз, аналіз інцидентів та реагування на них у єдиній платформі для максимального захисту кінцевих точок.

Досліджено функціональні можливості Sophos Intercept X Endpoint, який використовує штучний інтелект для виявлення загроз, таких як експлойти та програми-вимагачі.

Рішення надає інструменти для аналізу загроз у реальному часі, запобігання атакам, відновлення систем після інцидентів та автоматизації процесу реагування.

На основі проведених досліджень було запропоновано порядок впровадження Sophos Intercept X Endpoint у корпоративне середовище. Деталізовано практичні рекомендації для фахівців з кібербезпеки щодо інтеграції цього рішення в корпоративну інфраструктуру.

За допомогою Sophos Intercept X Endpoint реалізується технологія розширеного виявлення загроз кінцевим точкам та реагування на них, яка забезпечує інтегровану систему захисту в таких аспектах:

аналіз загроз у режимі реального часу – система використовує штучний інтелект для виявлення атак, таких як експлойти, програми-здирники та інші сучасні кіберзагрози;

запобігання експлойтам – Sophos Intercept X Endpoint дозволяє виявляти та блокувати вразливості програмного забезпечення до їх експлуатації;

відновлення після атак – рішення включає функції автоматизованого відновлення систем після атак, мінімізуючи вплив інцидентів на бізнес-процеси;

автоматизація реагування на загрози – забезпечується швидке виявлення та усунення інцидентів з мінімальним залученням фахівців з кібербезпеки.

Функції безпеки Sophos Intercept X Endpoint можна гнучко налаштовувати відповідно до потреб організації.

Таким чином, правильна реалізація технології розширеного виявлення загроз кінцевим точкам та реагування на них сприяє підвищенню загального рівня безпеки організації та забезпечує захист її інформаційних ресурсів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Сидоренко В.Д. Технологія розширеного виявлення загроз кінцевим точкам та реагування на них. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний університет інформаційно-комунікаційних технологій. 25 жовтня 2024. Тези доповідей. С. 241-244. URL: https://duikt.edu.ua/uploads/p_2661_48963150.pdf (дата звернення: 19.11.2024).

2. Sophos 2024 Threat Report. URL: https://assets.sophos.com/X24WTUEQ/at/wwf5phjtj9bjvmpqqsbfxc/sophos-2024-threat-report.pdf (дата звернення: 19.11.2024).

3. Gridinsoft. Endpoint Detection and Response. URL: https://gridinsoft.ua/edr (дата звернення: 19.11.2024).

4. Radix. MTTD (Mean Time to Detect) Uncovered: A DevOps Imperative. URL: https://radixweb.com/blog/what-is-mean-time-to-detect (дата звернення: 19.11.2024).

5. NIST Cybersecurity Framework (CSF). URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 19.11.2024).

6. MITRE ATT&CK Framework. URL: https://attack.mitre.org/ (дата звернення: 19.11.2024).

7. ISO/IEC 27001. ISO/IEC 27001.Management System Information Security. Dr. Amar Massoud. Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques. URL: https://certification.com.ua/iso27001?gad_source=1&gclid=Cj0KCQiAi_G5BhDXARIsAN5SX7r-hustjm1MQKQKJ9pBQ0gnpVtt97tqyFMu9X0YlNVOQ-fU_7XnnywaAhzdEALw_wcB (дата звернення: 19.11.2024).

8. ISO/IEC 27002. Information security, cybersecurity and privacy protection — Information security controls. URL: https://www.iso.org/es/contents/data/standard/07/56/75652.html (дата звернення:

19.11.2024).

9. Andrew Davies, Mitchell Schneider. Magic Quadrant for Security Information and Event Management. 8 May 2024 - ID G00780705. URL: https://www.gartner.com/doc/reprints?id=1-2FFCXFP9&ct=231025&st=sb (дата звернення: 19.11.2024).

10. CrowdStrike Falcon. URL: https://www.crowdstrike.com/en-us/?srsltid=AfmBOor_-hlyvELtl-zLqt_Y00lJ-xAilQ0o3QeSNtzU45uUQxGw5cMA (дата звернення: 19.11.2024).

11. SentinelOne. URL: https://www.sentinelone.com/ (дата звернення: 19.11.2024).

12. Microsoft Defender for Endpoint. URL: https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint (дата звернення: 19.11.2024).

13. Sophos. URL: https://www.sophos.com/en-us (дата звернення: 19.11.2024).

14. Sophos Firewall. URL: https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/GettingStarted/index.html (дата звернення: 19.11.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Кваліфікаційна робота

на тему:

«ТЕХНОЛОГІЯ РОЗШИРЕНОГО ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИМ ТОЧКАМ ТА РЕАГУВАННЯ НА НИХ НА БАЗІ SOPHOS INTERCEPT X ENDPOINT»

Виконав: СИДОРЕНКО Володимир Дмитрович, БСДМ – 62

Керівник: ГАХОВ Сергій Олександрович, к.військ.н., доцент

Об’єкт дослідження – розширене виявлення загроз кінцевим точкам.

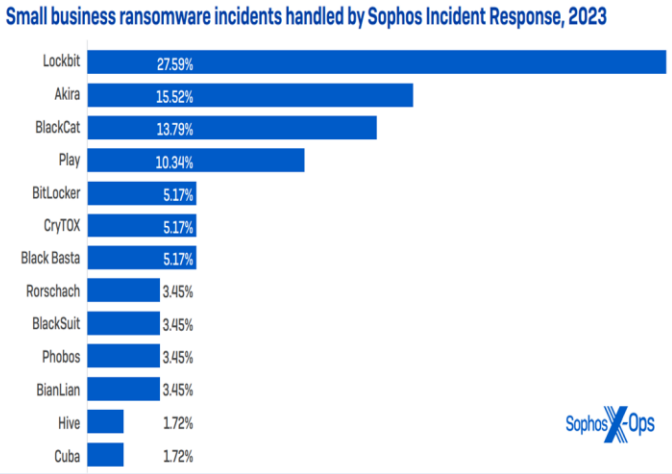
Предмет дослідження – технології розширеного виявлення загроз кінцевим точкам та реагування на них на базі Sophos Intercept X Endpoint.

Мета роботи – розробити рекомендації щодо розширеного виявлення загроз кінцевим точкам та реагування на них.

Наукові завдання:

- Дослідити проблеми технології розширеного виявлення загроз кінцевим точкам;
- Проаналізувати існуючі рішення щодо технологій розширеного виявлення загроз кінцевим точкам та реагування на них;
- Проаналізувати методи та засоби розширеного виявлення загроз кінцевим точкам та реагування на них на базі Sophos Intercept X Endpoint;
- Дослідити архітектуру рішення Sophos Intercept X Endpoint, призначення та основні функції компонентів;
- Розробити варіант технології системи розширеного виявлення загроз кінцевим точкам та реагування на них на базі Sophos Intercept X Endpoint;
- Розробити загальні рекомендації щодо розширеного виявлення загроз кінцевим точкам та реагування на них.

ДОСЛІДЖЕННЯ ПРОБЛЕМИ ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИМ ТОЧКАМ

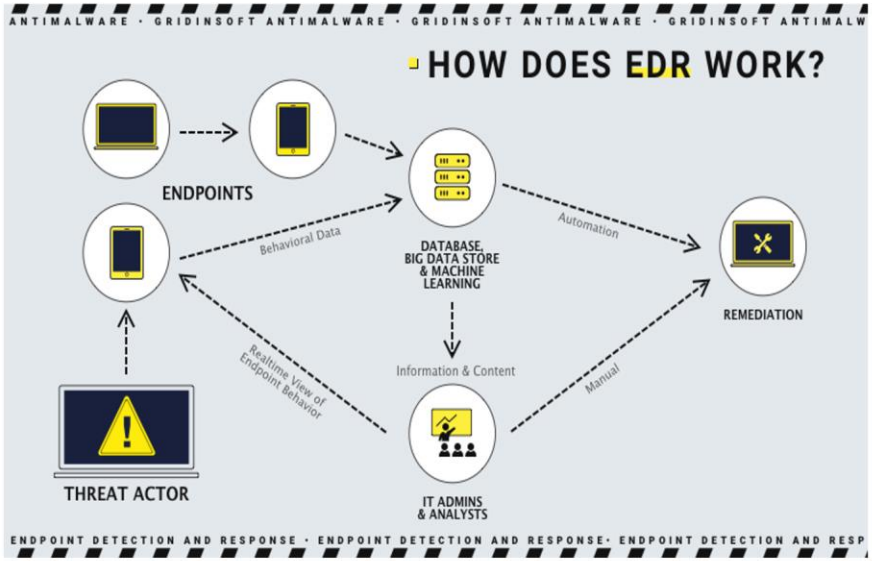


Згідно зі звітом Sophos 2024 Threat Report, організації стикаються з дедалі більшою складністю управління системами виявлення загроз на кінцевих точках. Дослідження акцентує увагу на важливості використання інтегрованих рішень, які поєднують штучний інтелект із традиційними методами виявлення загроз, для ефективної протидії все більш складним атакам. Крім того, зростання кількості атак із використанням програм-вимагачів спонукає компанії приділяти пріоритетну увагу захисту кінцевих точок, оскільки ці загрози стають не лише більш поширеними, але й виходять за межі своїх звичних цілей.

Програми-вимагачі продовжують залишатися однією з основних загроз для малого бізнесу. Хоча вони складають відносно невелику частку серед усіх виявлених зловмисних програм, їхній вплив залишається найзначнішим. Такі атаки зачіпають підприємства будь-якого розміру та галузі, проте найчастіше вони спрямовані саме на малі та середні компанії.

У 2021 році робоча група з програм-вимагачів Інституту безпеки та технологій виявила, що 70% атак програм-вимагачів були спрямовані на малий бізнес. Хоча загальна кількість атак програм-вимагачів змінюється щороку, цей відсоток підтверджується нашими власними показниками. Програмне забезпечення-вимагач LockBit було найпоширенішою загрозою в справах безпеки малого бізнесу, які взяло на себе Sophos Incident Response у 2023 році. LockBit – це програмне забезпечення-вимагач як послуга, надане кількома дочірніми компаніями, яке було найбільш поширеним програмним забезпеченням-вимагачем у 2022 році

АНАЛІЗ ПІДХОДІВ ДО ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИХ ТОЧОК



Системи EDR надають потужні інструменти для проведення аналізу після інцидентів. Зібрані логи та події з кінцевих точок дозволяють дослідити, як саме загроза потрапила в систему, які дії виконувала, і як можна було уникнути її в майбутньому. Ця інформація сприяє вдосконаленню політик безпеки та захисних механізмів.

EDR дає командам із безпеки змогу отримувати уніфіковану видимість і керування наявними кінцевими точками, а також виявляти некеровані кінцеві точки, підключені до мережі, які можуть бути джерелом типових вразливостей та недоліків (CVE). Вони також можуть використовувати EDR для зменшення можливостей для атак, позначаючи вразливості та неправильні конфігурації.

Завдяки EDR, фахівці з кібербезпеки можуть здійснювати моніторинг активностей на кінцевих точках у режимі реального часу. Це дозволяє виявляти підозрілу поведінку, а також будь-які відхилення від нормального стану системи. Після виявлення загрози система може автоматично або вручну блокувати або ізолювати підозрілу кінцеву точку, знижуючи ризик поширення загрози по всій мережі.

У підсумку, EDR забезпечує проактивний підхід до кібербезпеки, дозволяючи організаціям не лише реагувати на інциденти, але й запобігати їхньому виникненню, підвищуючи загальний рівень захищеності мережі та кінцевих точок.

NIST CYBERSECURITY FRAMEWORK (CSF)

Вимоги NIST CSF містить у собі управління активами (ID.AM). Організація повинна мати повний облік кінцевих точок, включаючи комп'ютери, сервери, мобільні пристрої та інші активи. EDR повинен допомагати в ідентифікації всіх кінцевих точок і контролювати некеровані або невідомі пристрої. Управління ризиками (ID.RA). Необхідно оцінювати ризики, пов'язані з кінцевими точками, враховуючи потенційні загрози. EDR сприяє оцінці ризиків, допомагаючи ідентифікувати уразливі кінцеві точки та оцінювати вплив потенційних атак.

Вимоги NIST CSF – планування реагування на інциденти (RS.RP). EDR повинен підтримувати процеси швидкого реагування на інциденти, дозволяючи ізолювати скомпрометовані кінцеві точки або зупинити підозрілі процеси. Аналіз (RS.AN). Після виявлення загрози EDR повинен забезпечити аналіз інциденту, включаючи його джерело, вектори атаки та вплив. Реагування на інциденти (RS.CO). EDR повинен надавати засоби для координації реагування, автоматизації заходів щодо нейтралізації загроз та мінімізації їхнього впливу. Навчання після інциденту (RS.IM). EDR повинен надавати можливості для аналізу інциденту після його завершення, щоб визначити, які техніки були використані і як їх уникнути в майбутньому.

МАГІЧНИЙ КВАДРАНТ GARTNER

Figure 1: Magic Quadrant for Endpoint Protection Platforms

Магічний квадрант Gartner за 2024 рік пропонує цінну інформацію для організацій, які обирають рішення для захисту кінцевих точок. У цьому звіті виділено чотири провідні компанії: Microsoft, CrowdStrike та SentinelOne, які демонструють високі можливості та чудові результати у сфері захисту кінцевих точок.

Ці рішення є провідними (еталонними) у своїй сфері. Ці компанії є лідерами в галузі завдяки своїм інноваційним підходам до виявлення загроз і реагування на інциденти, а також постійному розвитку своїх технологій.

Організації повинні ретельно аналізувати свої потреби у сфері захисту кінцевих точок та враховувати рекомендації Магічного квадранта Gartner при виборі постачальника рішень EDR (Endpoint Detection and Response). Окрім цього, важливо забезпечувати регулярне оновлення та підтримку EDR-рішень, оскільки це є ключовим для своєчасного виявлення загроз, захисту даних та мінімізації ризиків кібератак, які можуть вплинути на бізнес-процеси.

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ЩОДО ТЕХНОЛОГІЙ РОЗШИРЕНОГО ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИМ ТОЧКАМ

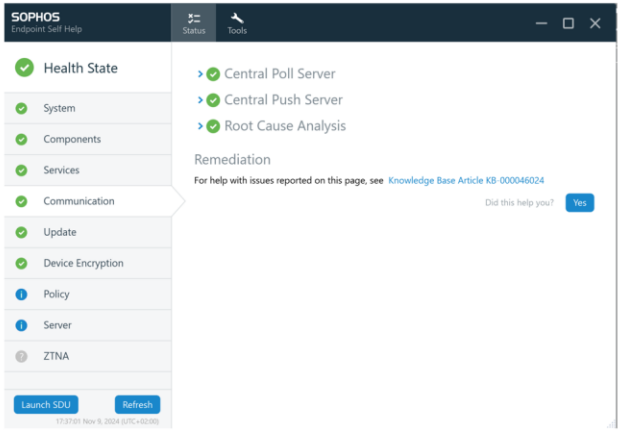
Microsoft Defender for Endpoint

Microsoft Defender for Endpoint (колишній Microsoft Defender ATP) інтегрується з екосистемою Microsoft і є потужним EDR-рішенням. Він забезпечує активне виявлення та захист від складних загроз на кінцевих точках за допомогою розширених аналітичних інструментів, таких як поведінковий аналіз та штучний інтелект. Перевагою є глибока інтеграція з іншими продуктами Microsoft, що дозволяє легко керувати безпекою в корпоративних середовищах з великою кількістю кінцевих точок. Переваги Microsoft Defender for Endpoint: комплексний захист: MDE охоплює всі аспекти безпеки кінцевих точок, включаючи виявлення, реагування, аналіз та усунення наслідків; інтеграція з Microsoft 365: Легко інтегрується з існуючими сервісами Microsoft, забезпечуючи узгодженість і зручність у використанні; хмарні можливості: Завдяки хмарній архітектурі система може швидко адаптуватися до нових загроз і забезпечувати високий рівень продуктивності без втрати швидкодії; зручний для великих компаній: Ідеальний для підприємств із великими IT-інфраструктурами завдяки можливості централізованого управління та широкому спектру аналітичних інструментів.

CrowdStrike Falcon

Платформа CrowdStrike Falcon поєднує превентивний захист, автоматичне виявлення загроз і можливості розслідування інцидентів в реальному часі. Серед переваг – висока швидкість розгортання, мінімальний вплив на продуктивність кінцевих точок і постійне оновлення даних загроз завдяки хмарній інфраструктурі. поглиблений аналіз загроз. Falcon надає детальну інформацію про атаки, включаючи контекст подій: механізми здійснення атак, використані вразливості та скомпрометовані системи. Це допомагає командам безпеки ефективніше усувати наслідки інцидентів. Швидка реакція на інциденти. Платформа дозволяє не лише виявляти, але й миттєво реагувати на загрози. Інструменти для ізоляції кінцевих точок, видалення шкідливих файлів та відновлення систем допомагають мінімізувати вплив атак на бізнес-процеси Завдяки системі Threat Graph платформа щодня аналізує трильйони подій. Інструмент збирає дані про поведінку кінцевих точок у глобальній мережі CrowdStrike, що дозволяє виявляти та попереджати загрози в реальному часі.

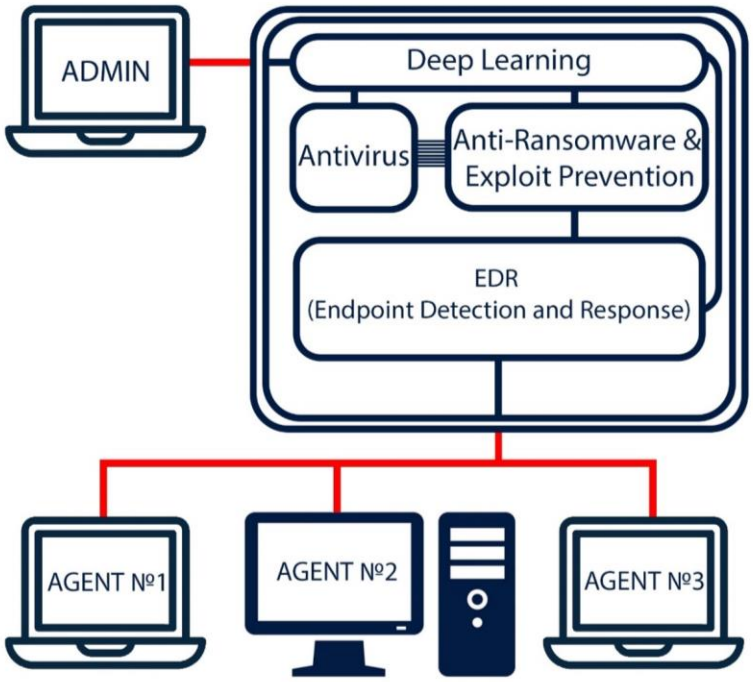
АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РОЗШИРЕНОГО ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИМ ТОЧКАМ ТА РЕАГУВАННЯ НА НИХ НА БАЗІ SOPHOS INTERCEPT X ENDPOINT



В цілому Intercept X Endpoint має багаторівневий захист завдяки поєднанню методів сигнатурного, поведінкового та евристичного аналізу; розширені функції EDR для ефективного розслідування інцидентів безпеки; синхронізація з іншими рішеннями Sophos для швидшого реагування на загрози; захист від сучасних видів атак на основі експлойтів, атак типу "нульового дня" та шифрувальників.

Розширені рішення Sophos XDR. Технології Sophos бездоганно поєднуються в платформі XDR, щоб забезпечити найкращі можливі результати безпеки. Рідні інтеграції рішень включають Sophos Endpoint, Sophos Mobile, Sophos Firewall, Sophos NDR, Sophos ZTNA. Використовуючи телеметрію з широкого спектру інструментів безпеки, що не належать Sophos, і отримаючи більшу рентабельність інвестицій існуючі інвестиції користувача в технології, одночасно прискорюючи операції безпеки. Інтеграція включає ідентифікацію, мережу, брандмауер, електронну пошту, хмару, продуктивність і безпеку кінцевої точки технології.

АРХІТЕКТУРА РІШЕННЯ SOPHOS INTERCEPT X ENDPOINT, ПРИЗНАЧЕННЯ ТА ОСНОВНІ ФУНКЦІЇ КОМПОНЕНТІВ



Моудль поглибленого вивчення
Це нейронна мережа, яка аналізує файли до їх виконання, щоб визначити потенційно шкідливу поведінку навіть у невідомих або нових загрозах.

Запобігання експлойтам
Цей модуль відстежує дії, характерні для експлойтів (наприклад, коду, який використовує вразливості програмного забезпечення). Він захищає від атак, які експлуатують вразливості у популярному ПЗ, як-от Microsoft Office або веб-браузери.

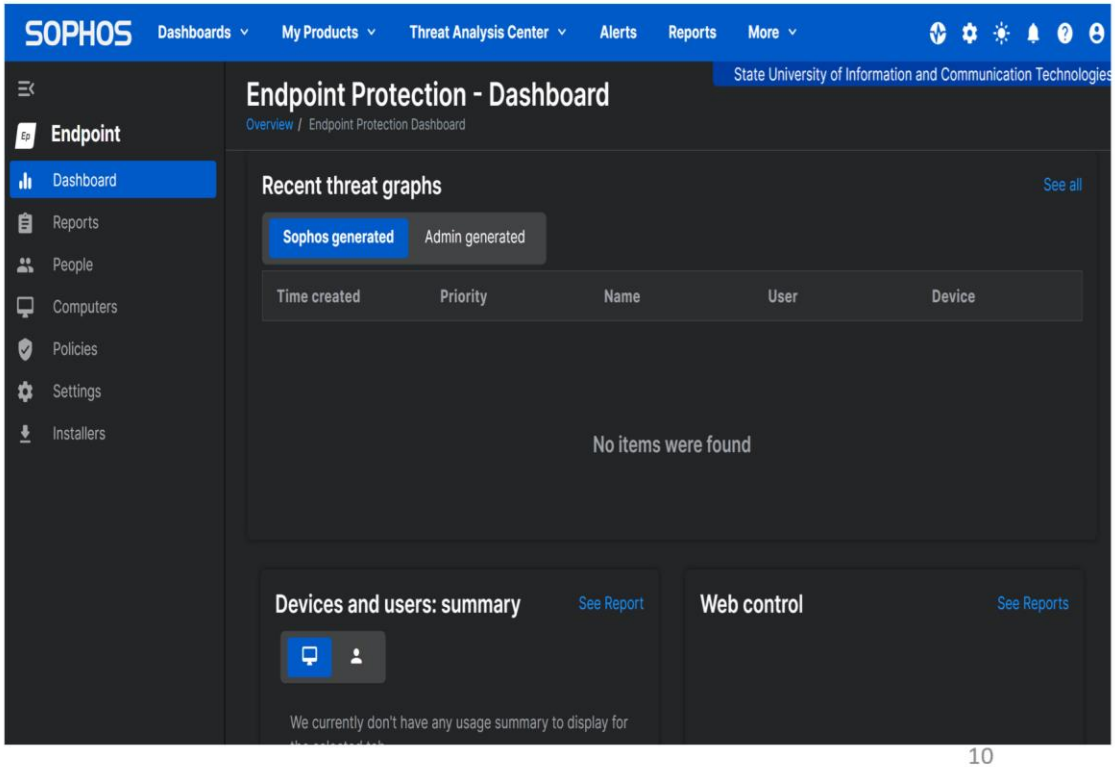
Модуль виявлення і запобігання атак
Компонент, який спеціалізується на виявленні й запобіганні атак з вимогою викупу (ransomware).

Модуль дослідження й реагування на інциденти
Це інструмент для виявлення, дослідження й реагування на інциденти безпеки.

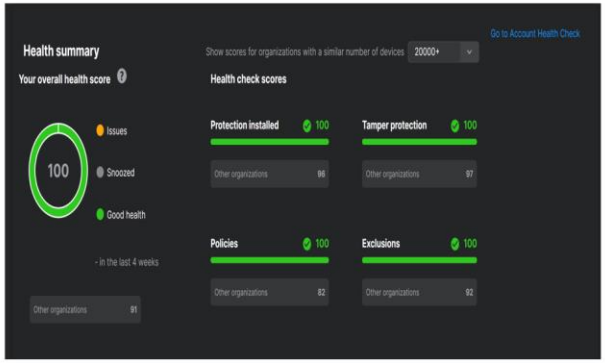
Веб-контроль та мережевий захист від загроз
Дозволяє адміністраторам встановлювати правила для контролю за використанням додатків, обмежувати доступ до певних веб-сайтів, а також захищати від мережевих атак, таких як сканування портів або розсилки шкідливого трафіку.

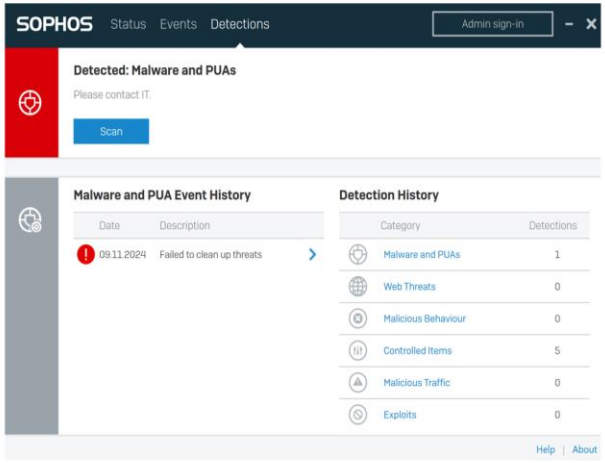
Розглянемо основні функції компонентів архітектури Sophos Intercept x Endpoint: Виявлення, блокування та видалення шкідливих програм; запобігання експлойтам. Захист від атак, спрямованих на вразливості в програмах; захист від шифрувальних програм. Блокує спроби шифрування даних, не дозволяючи програмам зловмисників отримати доступ до файлів; налітика та звітність. Адміністратори можуть аналізувати інциденти, отримувати звіти та рекомендації щодо дій; контроль і політики безпеки. Дає можливість встановлювати обмеження на програми та веб-ресурси, що знижує ризики від соціальної інженерії.

Загалом рішення Sophos Intercept X Endpoint забезпечує комплексний захист завдяки багаторівневому підходу та використанню сучасних технологій, як-от глибоке навчання й EDR, дозволяючи протистояти сучасним загрозам.



МОЖЛИВОСТІ РІШЕННЯ SOPHOS INTERCEPT X ENDPOINT ЩОДО РОЗШИРЕНОГО ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИМ ТОЧКАМ ТА РЕАГУВАННЯ НА НИХ



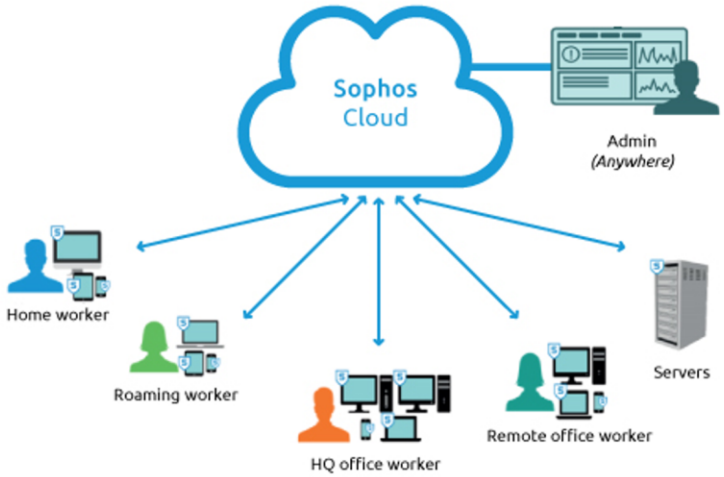


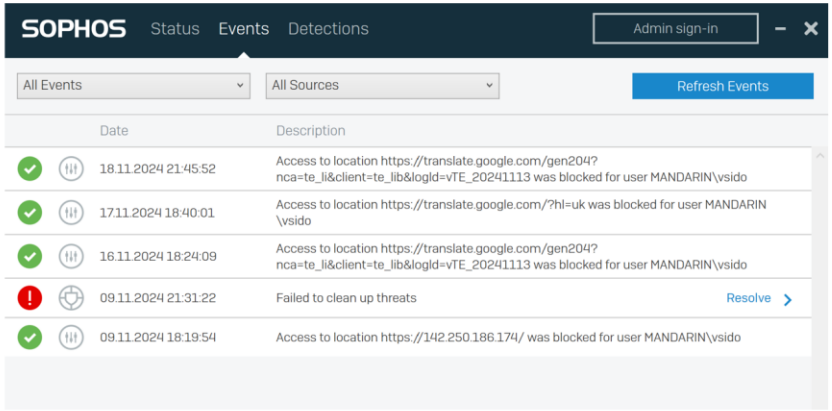
Sophos Intercept X Endpoint надає розширені можливості для виявлення загроз на кінцевих точках і забезпечення оперативного реагування завдяки сучасним технологіям і інструментам для моніторингу, аналізу та нейтралізації інцидентів безпеки. Система використовує Endpoint Detection and Response (EDR), який відстежує аномальну активність, застосовуючи поведінковий аналіз для раннього виявлення загроз.

EDR також дозволяє адміністраторам досліджувати причини і наслідки інцидентів, аналізувати ланцюжок зараження і відстежувати всі дії зловмисного ПЗ, що сприяє кращому розумінню механізму атак. Рішення включає глибокий аналіз файлів за допомогою модуля глибокого навчання, який прогнозує шкідливу активність ще до запуску файлів, виявляючи нові та невідомі загрози. Поведінковий аналіз забезпечує захист без необхідності у сигнатурах, блокуючи шкідливі дії, як-от несанкціоноване редагування пам'яті чи виконання небезпечного коду.

Механізм запобігання експлойтам блокує атаки, які використовують вразливості програмного забезпечення, включаючи вразливості нульового дня. Це дозволяє зупиняти поширення загроз через поширені вектори атак, суттєво підвищуючи безпеку кінцевих точок.

РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ СИСТЕМИ РОЗШИРЕНОГО ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИМ ТОЧКАМ ТА РЕАГУВАННЯ НА НИХ НА БАЗІ SOPHOS INTERCEPT X ENDPOINT





Sophos Intercept X Endpoint є одним із провідних рішень для захисту кінцевих точок, яке поєднує багаторівневу безпеку, штучний інтелект, глибоке навчання та сучасні технології Extended Detection and Response (XDR). Управління цією програмою відбувається через централізовану платформу Sophos Central, що забезпечує гнучкість, ефективність і прозорість для адміністраторів.

Sophos Intercept X Endpoint це – рішення, яке забезпечує надійний захист кінцевих точок завдяки сучасним технологіям, зручному управлінню та інтеграції з іншими компонентами кіберзахисту. Воно ідеально підходить для компаній, які прагнуть захистити свої дані від сучасних кіберзагроз.

РЕКОМЕНДАЦІЇ ЩОДО РОЗШИРЕНОГО ВИЯВЛЕННЯ ЗАГРОЗ КІНЦЕВИМ ТОЧКАМ ТА РЕАГУВАННЯ НА НИХ

- *Необхідно визначення потреб організації, а саме обсяг і тип даних, які треба захистити.*
- *Інтеграція із існуючою інфраструктурою, перевірка сумісності з операційними системами, мережею та програмним забезпеченням організації. Розгортання Sophos Intercept X Endpoint і встановлення агентів на кінцеві точки.*
- *Налаштування політик безпеки для виявлення різних типів загроз, таких як шкідливе ПЗ, фішингові атаки та підозрілі дії користувачів.*
- *Налаштування розширеного моніторингу та виявлення загроз і налаштування базових правил EDR.*
- *Інтеграція із штучним інтелектом та машинним навчанням.*
- *Автоматизація реагування та запобігання, що є автоматичним блокуванням загроз.*
- *Сигналізація та повідомлення про загрози. Автоматичне надсилання сповіщень для адміністраторів безпеки або інших відповідальних осіб.*
- *Присутність аналітики та звітності забезпечить розробку панелі моніторингу, централізований огляд активностей і загроз.*
- *Звітування про події визначить налаштування регулярних звітів про спроби атак, зупинені загрози та загальний стан безпеки.*
- *Навчання співробітників щодо безпечного використання систем та реагування на сповіщення про потенційні загрози.*
- *Покращення алгоритмів виявлення загроз через регулярні оновлення та вдосконалення політик безпеки, що базуються на нових загрозах.*
- *Оцінка ефективності та корекція забезпечить моніторинг продуктивності та аналіз ефективності рішення EDR.*

ВИСНОВКИ

• В роботі проведено дослідження проблеми розширеного виявлення загроз кінцевим точкам, визначено її мету та завдання.

• Проведено аналіз існуючих технологій захисту кінцевих точок. Технологія розширеного виявлення загроз кінцевим точкам та реагування на них (EDR) забезпечує інтегрований підхід до протидії складним кіберзагрозам.

• Також досліджено функціональні можливості Sophos Intercept X Endpoint, який використовує штучний інтелект для виявлення загроз, таких як експлойти та програми-вимагачі.

• На основі проведених досліджень було запропоновано порядок впровадження Sophos Intercept X Endpoint у корпоративне середовище. Деталізовано практичні рекомендації для фахівців з кібербезпеки щодо інтеграції цього рішення в корпоративну інфраструктуру.

• Функції безпеки Sophos Intercept X Endpoint можна гнучко налаштовувати відповідно до потреб організації.

• Сформовані загальні рекомендації щодо технології розширеного виявлення загроз кінцевим точкам та реагування на них.

ДЯКУЮ ЗА УВАГУ!
ДОПОВІДЬ ЗАКІНЧЕНО