МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____ Михайло СТЕПАНОВ
«____»_____ 2023 р.

На правах рукопису
УДК 004.415.5:007:52

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Модуль моніторингу для розслідування інцидентів в кібербезпеці системами SIEM та XDR

Виконавець: Максим КОТЛЯР
Керівник: к.т.н. Наталія ГУЛАК
Консультант розділу «Охорона навколишнього середовища»: к.т.н., доцент Тетяна ДМИТРУХА
Нормоконтролер: к.т.н., доцент Наталія ГУЛАК

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Магістр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____ Михайло СТЕПАНОВ
«__» _____ 2023 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

здобувача вищої освіти Котляра Максима Олександровича

1. Тема: *Модуль моніторингу для розслідування інцидентів в кібербезпеці системами SIEM та XDR*

затверджена наказом ректора від «15» вересня 2023 № 1814/ст.

2. Термін виконання з 13.10.2023 р. по 04.01.2024 р.

3. Вихідні дані: система управління інформаційної безпеки, ризики інформаційної безпеки, методи оцінки вразливостей, загрози, системи виявлення та запобігання вторгненням IDS/IPS, VPN, системи SIEM та XDR

4. Зміст пояснювальної записки: оцінка вразливостей і впливу на інформаційні системи на основі стандарту ISO 27005, аналіз методів захисту від загроз та інцидентів засобами моніторингу інформаційних систем, розробка та тестування модуля моніторингу системами SIEM та XDR

5. КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

№ п/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1	Уточнення постановки задачі	16.10.2023	*Виконано*
2	Аналіз літературних джерел	20.10.2023	*Виконано*
3	Обґрунтування вибору рішення	24.11.2023	*Виконано*
4	Збір інформації	26.11.2023	*Виконано*
5	Оцінка вразливостей і впливу на ІС на основі стандарту ISO 27005	10.11.2023	*Виконано*
6	Аналіз методів захисту від загроз та інцидентів засобами моніторингу ІС	16.11.2023	*Виконано*
7	Розробка та тестування модуля моніторингу сумісно з системами SIEM та XDR	22.11.2023	*Виконано*
8	Апробація роботи на V Міжнародну науково-практичну конференцію Madrid, Spain	24.11.2023	*Виконано*
9	Перевірка на антиплагіат	12.12.2023	*Виконано*
10	Оформлення і друк пояснювальної записки	14.12.2023	*Виконано*
11	Оформлення презентації	15.12.2023	*Виконано*
12	Отримання рецензій від рецензента	22.12.2023	*Виконано*

6. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона навколишнього середовища	Дмитруха Т.І.		

7. Дата видачі завдання: «16» жовтня 2023 р.

Здобувач вищої освіти М. Котляр

(підпис, дата)

Керівник Н. Гулак

(підпис, дата)

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел і має 116 сторінок основного тексту, 42 рисунка, 3 таблиці. Список використаних джерел містить 24 найменування і займає 3 сторінки. Загальний обсяг роботи 135 сторінок.

Метою роботи є розробка та тестування модуля моніторингу та розслідування інцидентів системами SIEM та XDR.

В роботі розроблено алгоритм та модуль моніторингу для аналізу та оцінки ризиків інформаційної безпеки на основі ідентифікації активів та загроз, визначенні значень ключових оцінюючих компонентів та ступеню ризику. Розроблений модуль моніторингу відносяться до галузі інформаційної безпеки і може бути використані для підвищення рівня захищеності.

Можливі напрямки розвитку цієї роботи пов’язані із розширенням модулю моніторингу відповідно до вимог міжнародних стандартів, наприклад ISO 27005, для більш повного аналізу та оцінки ризиків.

Ключові слова: ризик, система аналізу і оцінки ризиків, інформаційна безпека, інформаційно-комунікаційна система, загроза, хост, ПК, моніторинг, SIEM, EDR, XDR, війна, угрупування, зловмисник, шкідливе програмне забезпечення.

Зміст

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЗІ	– захист інформації ;
ОС	– операйна система;
ПК	– персональний комп’ютер;
TCP	– Transmission Control Protocol – протокол управління передачею;
IP	– Internet Protocol – міжмережевий проткол;
ПЗ	– програмне забезпечення;
FTP	- File Transfer Protocol – протокол передачі файлів по мережі
UDP	– протокол передачі даних без встановлення з'єднання
ARP	– протокол перетворення IP-адреси на фізичну адресу
RIP	– протокол маршрутної інформації
TCP	– протокол управління передачею
DNS	– протокол встановлення відповідності мнемонічних імен та мережевих адрес
IGMP	– протокол передачі повідомлень про маршрутизацію
SMTP	– протокол забезпечення сервісу доставки повідомлень електронною поштою
SNMP	– протокол управління маршрутизаторами у мережах
EDR	– Endpoint detection and response, це технологія кібербезпеки, яка постійно контролює "кінцеву точку"
XDR	– Extended Detection & Response ефективніше рішення для проактивного виявлення інцидентів
SIEM	– Security information and event management

ВСТУП

Актуальність. Сьогодні неможливо уявити світ без Інтернету та інформаційних технологій. Вони міцно увійшли до нашого життя, значно спростивши його. З розвитком інформаційних технологій нам стають доступні нові інструменти, які роблять звичні процеси швидше, зручніше та дешевше. Проте захист даних у комп'ютерних мережах чи не найголовніша проблема у сфері інформаційних технологій. Відповідно до аналізу безпеки роботи мережі, її характеристики можна звести до трьох аспектів:

По-перше, приховані небезпеки мережі різноманітні. Безпека мережі не обов'язково викликана атаками хакерів або вірусними атаками. Проблеми можуть виникати через вплив об'єктивних умов, таких як природні фактори чи людський фактор[1].

По-друге, кібербезпека – це серйозно. Будучи середовищем зберігання великого обсягу інформації, комп'ютерна мережу несе у собі масу основної інформації у виробництві та житті людей. Виникнення загрози безпеці призведе до величезних втрат і навіть поставить під загрозу інформаційну безпеку країни[1].

Зрештою, по-третє, інформаційна безпека комп'ютерних мереж є змінною. З розвитком науки і техніки вдосконалюються й технології злому, а засоби та форми різних вірусів, що вторгаються у безпеку мережі, також зазнаватимуть змін. Як тільки технологія меревої безпеки стане відносно відсталою, вона сильно заважатиме безпеці мережі. Існують проблеми мережевої безпеки, спричинені лазівками в операційній системі[1].

Безпека мережі, викликана вірусними атаками, зовнішні вторгнення, з якими стикається безпека комп'ютерних мереж, здебільшого відносяться до вірусів. Вірус – це шкідлива програма, що атакує комп'ютерну безпеку. Як тільки вірус проникне в комп'ютер, він викличе крах усієї системи мережевої безпеки через свою здатність до супер відтворення, що створить серйозні ризики для безпеки. У

процесі популяризації мережевих та комп'ютерних технологій в IT-індустрії з'являється все більше фахівців практиків. Але технічні фахівці в галузі управління мережевою безпекою становлять лише невелику частину IT. Оскільки багато підрозділів не приділяють належної уваги мережевій безпеці, вони є відносно пасивними в обслуговуванні мережевої безпеки. Багатьом працівникам з обслуговування мережевої безпеки не вистачає професіоналізму, їм важко гарантувати безпеку мережі перед вірусними атаками. Висока швидкість передачі та великий обсяг інформації змушують багатьох зловмисників використовувати Інтернет для здирництва. Безпека мережі становить велику загрозу[2].

Використання систем управління інформаційною безпекою (SIEM) та розширених систем виявлення та реагування (XDR) є надзвичайно актуальними в умовах постійно зростаючих кіберзагроз. Обидві системи відіграють важливу роль у забезпеченні ефективного контролю над безпекою інформації в організаціях.

Зростання різноманітності та складності кіберзагроз вимагає ефективних інструментів для їх виявлення та реагування. SIEM та XDR разом надають комплексний погляд на безпеку, об'єднуючи дані з різних джерел. Обидві системи дозволяють здійснювати реакцію в реальному часі та приймати проактивні заходи для мінімізації ризиків, тому тема дипломної роботи є актуальною.

Метою роботи є розробка та тестування модуля моніторингу та розслідування інцидентів системами SIEM та XDR , який завдяки поєднанню декількох безпекових систем забезпечує повний захист всієї інфраструктури і надає розуміння безпековим командам про ландшафт загроз, які можуть вплинути на автоматизованих систем.

Для досягнення даної мети необхідно розв’язання таких задач:

- оцінка вразливостей і впливу на інформаційні системи на основі стандарту ISO 27005
- аналіз методів захисту від загроз та інцидентів засобами моніторингу інформаційних систем

- розробка та тестування модуля моніторингу системами SIEM та XDR

Об'єкт дослідження: процес захисту інформації системами SIEM та XDR.

Предмет дослідження: методи розслідування інцидентів в кібербезпеці системами SIEM та XDR

Методи дослідження. Аналітичні та статистичні методи аналізу розслідувань інцидентів та загроз кібербезпеки.

Галузь застосування. Даний модуль моніторингу інформації може використовуватися командами безпеки для інформаційних систем, або організаціями, які ведуть статистичний аналіз сучасних загроз ІБ.

Новизна. Наукова новизна полягає у сумісному використанні систем SIEM та XDR та інтегрування стороннього рішення VirusTotal для аналізу шкідливого програмного забезпечення, що дало можливість удосконалення виявлення зловтручань таких як шкідливі програми та спотворення інформації у модулі моніторингу ІБ.

Практична цінність. Запропонований модуль моніторингу може використовуватися в системах менеджменту інформаційної. Практична цінність розробленого модулю моніторингу полягає в функціональному рішенню виявлення інцидентів зловтручання, що буде корисним експертам в сфері інформаційної безпеки для моніторингу великого потоку даних, файлів, подій та фактичних змін в ОС за рахунок декількох безпекових систем, які формують один єдиний надійний модуль для моніторингу і захисту організацій.

Апробація. Основні положення роботи доповідалися та обговорювалися на такій конференції:

Котляр М.О. Аналіз загроз та інцидентів в сфері кібербезпеки під час повномасштабного вторгнення зі сторони росії /Н.К. Гулак, М.О. Котляр//V International Scientific and Practical Conference «Trends in science regarding the creation of new teaching methods», October 16-18, 2023, Madrid, Spain. - С. 182-184.

Розділ 1. ОЦІНКА ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ТА ЇХ КЛАСИФІКАЦІЯ НА ОСНОВІ СТАНДАРТУ 27005

1.1 Стандарт ISO/IEC 27005 (Ідентифікація та визначення цінності активів, Оцінки активів організації, Оцінка впливу)

Впровадження сучасних інформаційних технологій у корпоративних організаціях дозволяє вивести їхню роботу на якісно новий рівень, підвищити ефективність роботи фахівців та програмних служб та забезпечити лояльність персоналу. Однак одночасно з розробкою, впровадженням та удосконаленням інформаційної системи необхідно робити управлінські впливи, створені задля виявлення вразливих місць системи, загроз та ризиків. Правомірно поставити наступне питання: «Які ж загрози безпеці інформації можуть виникнути"? Насамперед це загрози, що створюють небезпеку конфіденційності інформації[1].

Набагато більший позов несуть загрози, що виходять з самої організації. Існує маса каналів витоку даних, в першу чергу це, звичайно ж, Інтернет та електронна пошта. Далі — портативні накопичувачі: «флешки», карти пам'яті, стільникові телефони і т. д. Потрібну інформацію можна роздрукувати на принтері. інформацію, що передається за даними каналам, то ризики у сфері ІБ можна звести до мінімуму. Але ці дії, що вимагають великих витрат людських та тимчасових ресурсів, з великою ймовірністю приречені на провал. Для забезпечення ІБ в організації повинні існувати корпоративні політики безпеки. А програмні та апаратні засоби лише покликані виконувати дані політики ІБ. У зв'язку з цим є необхідним визначення керівництвом основних напрямів розробки та впровадження системи управління інформаційною безпекою, в основі якої — створення ефективної системи управління інформаційною безпекою (СМІБ).[2] Цей підхід повинен підтримувати менеджмент ризиків для всієї організації.

Менеджмент ризиків інформаційної безпеки (ІБ) повинен бути невід'ємною частиною всіх видів діяльності, пов'язаних з менеджментом інформаційної безпеки, а також повинен застосовуватися для реалізації та підтримки функціонування СМІБ організації. Система менеджменту інформаційної безпеки (СМІБ) необхідна будь-якій організації, та її функціонування має бути спрямоване на збереження цілісності, конфіденційності та доступність її інформаційних активів.

Сучасні практики з управління СМІБ базуються на міжнародному стандарті ISO/IEC 27001. У цьому стандарті визначено основні цілі та засоби контролю, які дають змогу встановлювати, застосовувати, переглядати, контролювати та підтримувати ефективну систему менеджменту інформаційної безпеки. Стандарт встановлює вимоги до розроблення, впровадження, функціонування, моніторингу, аналізу, підтримці та вдосконаленню документованої системи менеджменту інформаційної безпеки у контексті існуючих ризиків організації. Менеджмент ризику інформаційної безпеки має бути безперервним процесом і пов'язаний з аналізом того, що може відбутися і якими можуть бути можливі наслідки, перш ніж виробити рішення про те, що і коли має бути зроблено для зниження ризику до прийнятного рівня. У в цьому контексті новий міжнародний стандарт ISO/IEC 27005:2011 «Інформаційні технології Методи забезпечення безпеки Управління ризиками інформаційної безпеки» може допомогти організаціям у підвищенні рівня управління ризиками інформаційної безпеки[2]. Новий стандарт описує процес управління ризиками інформаційної безпеки та відповідні дії та відповідає загальним принципам, перерахованим у стандарт ISO/IEC 27001:2005.

В стандарті ISO 27005 представлено загальний посібник з управління ризиками інформаційної безпеки. Він підтримує загальні концепції, викладені в ISO/IEC 27001, та призначений для «сприяння адекватному забезпечення інформаційної безпеки на основі ризик-орієнтованого підходу». Ризик інформаційної безпеки (Information security risk) визначено у стандарті як

потенційна загроза експлуатації вразливості активу або групи цінних властивостей, які можуть завдати шкоди організації. Стандарт застосовуємо до всіх видів організацій (у тому чисельності і організаціям, які діють у системі охорони здоров'я), які планують керувати ризиками інформаційної безпеки. Цей міжнародний стандарт забезпечує рекомендації щодо управління ризиками інформаційної безпеки в організації, що підтримує вимоги СМІБ (системи менеджменту інформаційної безпеки) згідно з ISO/IEC 27001[2]. Усі дії менеджменту ризиків інформаційної безпеки представлені як у Розділ 6 стандарту, так і згодом описаний у наступних розділах: встановлення стану у Розділі 7, оцінка ризику в Розділ 8, обробка ризику в Розділі 9, прийняття ризику у Розділі 10, перенесення ризику у Розділі 11, контроль та перегляд ризиків у Розділі 12. Порядок управління ризиками ISO 27005[15] представлений на рис. 1.

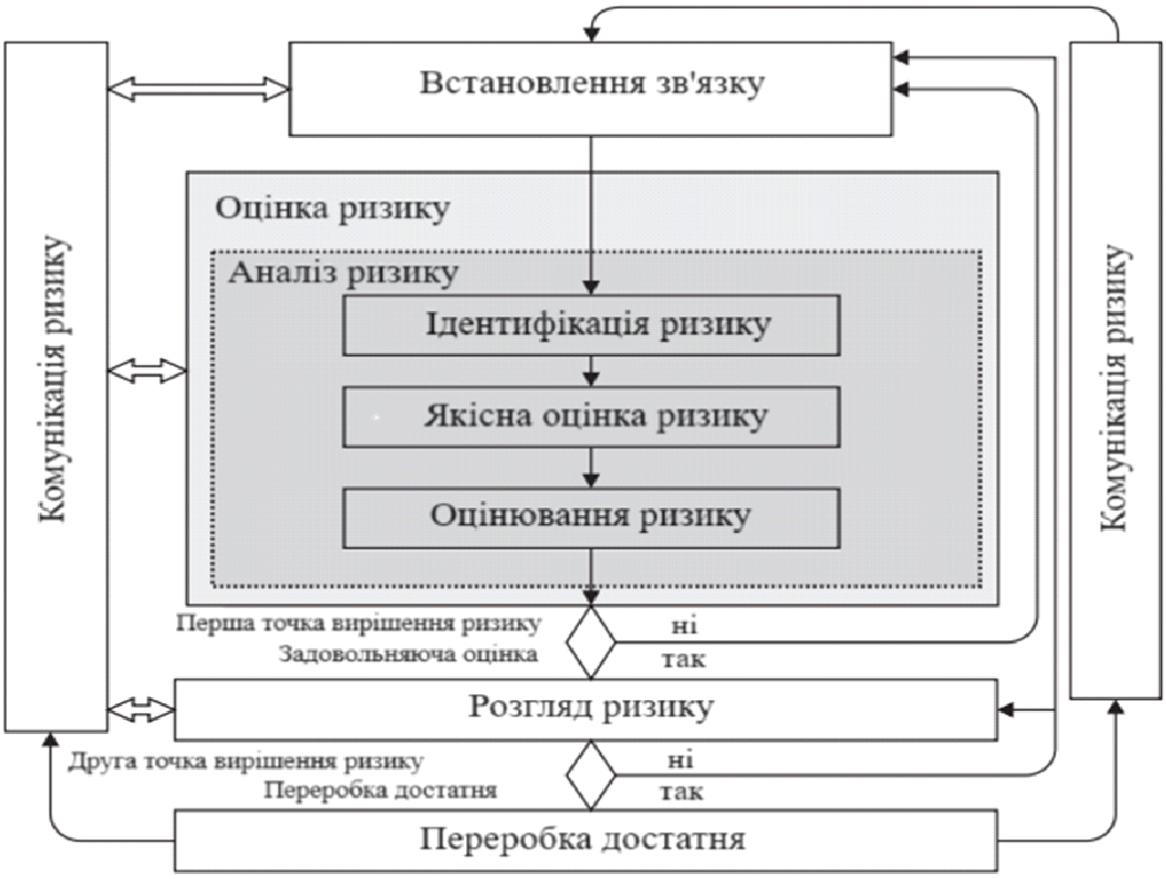


Рис. 1.1 Алгоритм управління ризиками ISO 27005

Рис. 1.1 ілюструє, що процеси менеджменту ризику зазвичай циклічні для оцінки ризику та дій з обробки ризиків. Циклічний підхід до проведення оцінки ризику може збільшити глибину та деталі оцінки кожного нового циклу. Такий підхід забезпечує хорошу рівновагу між зменшенням часу та зусиллям, гарантуючи, що високі ризики оцінені відповідно. Насамперед встановлюється контекст ризиків. Після цього проводиться оцінка ризику. Якщо надано достатньо інформації, щоб визначити ефективні дії, необхідні зміни ризиків до прийнятного рівня, тоді завдання вважається закінченим і проводиться обробка ризику. Якщо інформації буде недостатньо, то слідує інший цикл оцінки ризику з переглянутим контекстом (наприклад, критерії оцінки ризику). Ефективність обробки ризику залежить від результатів оцінки ризику Можливо, що обробка ризику не буде негайно призводити до прийнятного рівня залишкового ризику. У цій ситуації інший цикл оцінки ризику з зміненими контекстними параметрами (наприклад, оцінка ризику, прийняття ризику або критерії впливу) може у разі необхідності супроводжуватися подальшою обробкою ризику (рис. 1, друга точка вирішення ризику). Прийнятний рівень ризику повинен гарантувати, що залишкові ризики прийнято керівниками організації. У СМІБ встановлення контексту, оцінка ризику, розробка плану обробки ризику та прийняття ризику є частиною фази "планування".

Таблиця 1.1

Співвідношення СМІБ та процесу менеджменту ризиків інформаційної безпеки

Процес СМІБ	**Процес менеджменту ризиків ІБ**
Планування	Встановлення контексту
	Оцінка ризику
	Планування обробки ризику
	Прийняття ризику
Здійснення	Реалізація плану обробки ризику
Перевірка	Проведення безперервного моніторингу та перегляду ризиків

Продовження таблиці 1.1

1	2
Дія	Підтримка та удосконалення процесу менеджменту ризиків інформаційної безпеки

У фазі «здійснення» СМІБ дії та засоби контролю, потрібні для зниження ризику до прийнятного рівня, що реалізуються в відповідно до плану обробки ризику.

Можливості сучасних засобів забезпечення ІБ дуже широкі: захист інфраструктури організації, захист від атак, контроль поведінки абонентів, захист периметра мережі, моніторинг ІБ, захист від спаму, відображення вірусів, застосування політик, автентифікація пошти, контроль додатків та аудит мережної безпеки. У фазі «перевірка» ЗМІБ менеджери визначають потребу у перегляді обробки ризику у світлі інцидентів та змін обставин. У фазі «дія» здійснюються будь-які необхідні роботи, включаючи повторне ініціювання процесу управління ризиком ІБ. У табл. 1 підсумовуються види діяльності, пов'язаної з менеджментом ризику, значущі для чотирьох фаз процесу СМІБ[2]. Загалом діяльність з управління ризиками можна розглядати як основних 7 етапів, представлених на рис. 2. Для проведення повного аналізу інформаційних ризиків насамперед необхідно побудувати повну модель інформаційної системи з погляду ІБ. Це завдання мають виконувати висококваліфіковані фахівці, враховуючи складність алгоритму аналізу ризиків, що включає щонайменше близько ста параметрів, що дозволяє на виході дати максимально точну оцінку існуючих в інформаційній системі ризиків, засновану на глибокому аналізі особливостей інформаційної системи Далі проводиться аналіз загроз безпеці та вразливості.

Вихідні дані для оцінки загроз та вразливостей аудитор отримує від уповноважених представників організації у ході відповідних інтерв'ю. Для проведення інтерв'ю використовують спеціалізовані опитувальники. Питання

пов'язані з різними- ними категоріями ресурсів. Допускається коригування питань, виключення чи додавання нових. Задається частота виникнення кожної з виділених загроз, ступінь вразливості та цінність ресурсів. Все це використовується в надалі розрахунку ефективності застосування засобів захисту. Необхідно ідентифікувати всі види інформації, що становить цінність для організації. Ідентифікуються всі активи, задіяні у функціонуванні бізнес-процесів та що мають вплив на цінну для організації інформацію.

Дані активи включають:

- людські ресурси;
- інформаційні ресурси (як в електронному, так і паперовому вигляді);
- обладнання;
- програмне забезпечення;
- послуги, що надаються внутрішнім та зовнішнім замовникам.

Введені групи цінної інформації повинні бути розміщені користувачем на об'єктах зберігання інформації (серверах, робочих станціях і т.д.). Заключна фаза вказівки збитків по кожній групі цінної інформації, розміщеної на відповідних ресурсах, з усіх видів загроз. Одним із значних етапів є визначення та оцінка ризиків (risk assessment).

В рамках аналізу проводиться інвентаризація та категоризація ресурсів, що захищаються, з'ясовуються нормативні, технічні, договірні вимоги до ресурсів у сфері ІБ, та був з урахуванням цих вимог визначається вартість ресурсів.

У вартість входять усі потенційні витрати, пов'язані з можливими впливами на ресурси, що захищаються. Наступним етапом аналізу ризиків є складання переліку значних загроз та вразливостей для кожного ресурсу, а потім обчислюється ймовірність їх реалізації.

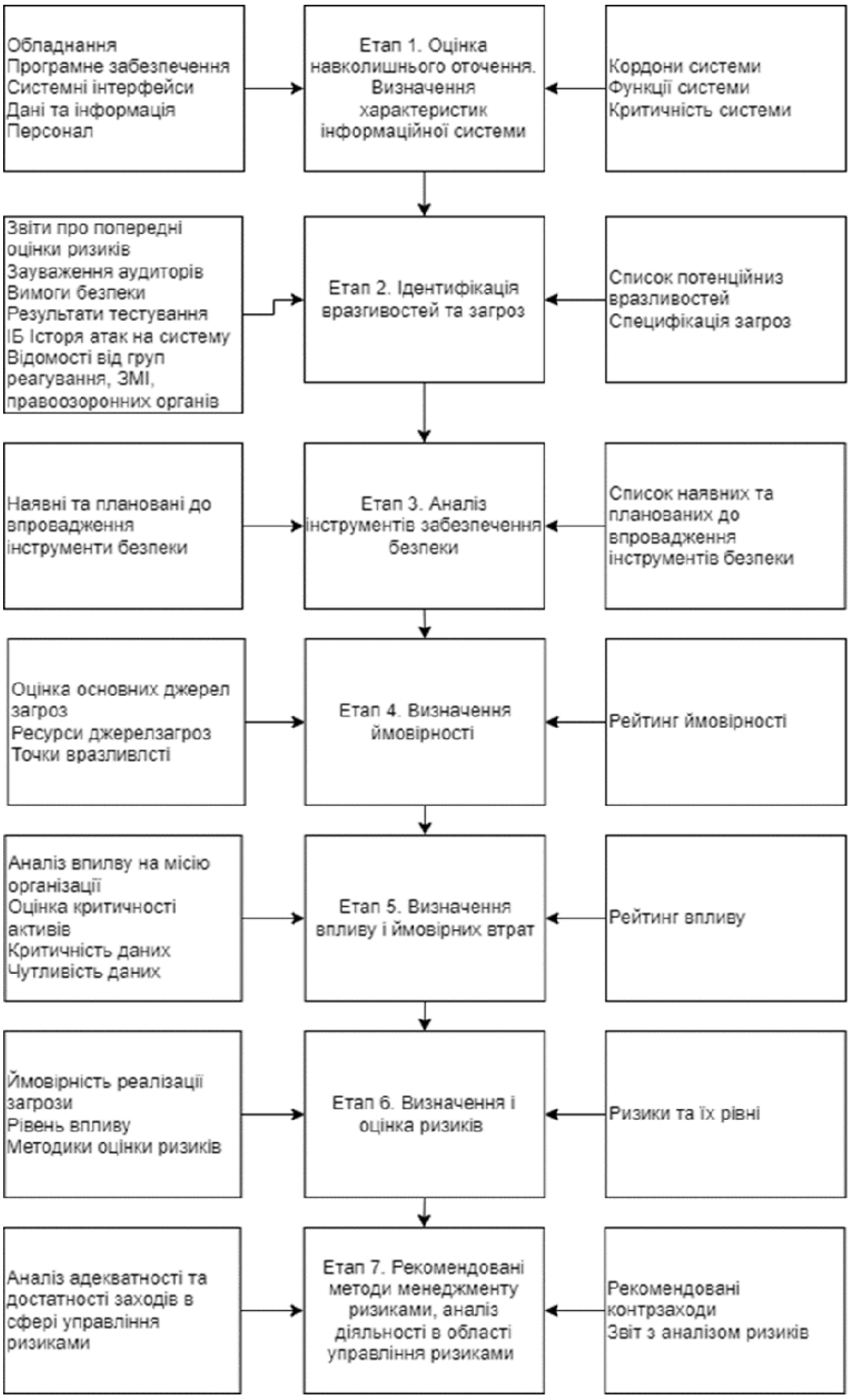


Рис. 1.2 Етапи та структура управлінських впливів у галузі управління ризиками

Стандарт допускає подвійне тлумачення поняття загрози ІБ: як умову реалізації вразливості ресурсу (у разі вразливості і загрози ідентифікуються окремо) і як загальна потенційна подія, здатна призвести до компрометації ресурсу (коли нали- чиї можливості реалізації вразливості і є загроза). Чи не забороняється поділ загроз ІБ на загрози цілісності, доступності та конфіденційності[4]. Оцінювання ризику проводиться шляхом його обчислення та зіставлення із заданою шкалою. Аналіз ризику може бути здійснений з різним ступенем деталізації залежно від критичності активів, поширеності відомих вразливостей та колишніх інцидентів, що стосувалися організації. Методологія вимірювання може бути якісною або кількісною або їх комбінацією в залежності від обставин. На практиці якісна оцінка часто використовується першою для отримання загальних відомостей про рівень ризику та виявлення основних значень ризиків. Пізніше може виникнути потреба в здійсненні більш специфічного або коли- чеського аналізу основних значень ризиків, оскільки зазвичай виконання якісного аналізу порівняно з кількісним є менш складним витратним. У стандарті докладно описуються деталі методології оцінки:

- Якісна оцінка використовує шкалу кваліфікації атрибутів для опису вели- чини можливих наслідків (наприклад, низький, середній та високий) та ймовірності виникнення цих наслідків. Перевага якісної оцінки полягає у простоті її розуміння всім відповідним персоналом, а недоліком є залежність від суб'єктивного вибору шкали. Такі шкали можуть бути адаптовані або скориговані таким чином, щоб задовольняти вимоги обставин, а для різних ризиків можуть використовуватись різні описи. Якісна оцінка може використовуватися:
  - як початкова діяльність з ретельної перевірки для ідентифікації ризиків, які потребують детальнішого аналізу;
  - там, де цей вид аналізу є відповідним для ухвалення рішення;
  - там, де числові дані чи ресурси є неадекватними для кількісної оцінки.

Кількісна оцінка використовує шкалу з числовими значеннями (а не описові шкали, які використовуються в якісній оцінки) наслідків та ймовірностей, що включає дані з різних джерел. Якість аналізу залежить від точності та повноти числових значень та від обґрунтованості використовуваних моделей. У більшості випадків кількісна оцінка використовує факти- ні дані за минулий період, забезпечуючи перевагу в тому, що вона може бути безпосередньо пов'язана з інформаційною метою безпеки та проблемами організації. Недоліки кількісного підходу можуть мати місце тоді, коли фактичні дані недоступні, тому створюється ілюзія цінності та точності оцінки ризику.

Допускається використання як кількісних, так і якісних методів оцінки ризиків, але, на жаль, у документі немає обґрунтування та рекомендацій щодо вибору математичного та методичного апаратів оцінки ризиків ІБ[5]. Додаток до стандарту містить єдиний приклад, який умовно можна віднести до якісного методом оцінки. Цей приклад використовує три- та п'ятибальні оціночні шкали:

1. Оцінюються рівні вартості ідентифікованого ресурсу за п'ятибальною шкалі: "незначний", "низький", "середній", "високий", "дуже високий".
2. Оцінюються рівні ймовірності загрози за трибальною шкалою: "низький", "середній", "високий".
3. Оцінюються рівні ймовірності вразливості: "низький", "середній", "високий".
4. За заданою таблицею розраховуються рівні ризику.
5. Проводиться ранжування інцидентів за рівнем ризику.

Після того, як ризик оцінений, має бути прийнято рішення щодо його обробки (risk treatment) точніше, вибору та реалізації заходів та засобів з мінімізації ризику. Крім оціненого рівня ризику, при прийнятті рішення можуть бути враховані витрати на впровадження та супровід механізмів безпеки, політика керівництва, простота реалізації, думка експертів та ін. Пропонується одна з чотирьох заходів обробки ризику:

1. Зменшення ризику. Ризик вважається неприйнятним, і для його зменшення вибираються та реалізуються відповідні заходи та засоби безпеки.

2. Передача ризику. Ризик вважається неприйнятним та на певних умовах (наприклад, у рамках страхування, постачання або аутсорсингу) переадресовується сторонньою організації.

3. Прийняття ризику. Ризик у конкретному випадку вважається усвідомлено допустимим організація має упокоритися з можливими наслідками. Зазвичай це означає, що вартість контрзаходів значно перевищує фінансові втрати у разі реалізації загрози чи організація неспроможна знайти відповідні заходи та засоби безпеки.

4. Відмова від ризику. Відмова від бізнес-процесів організації, які є причиною ризику. Наприклад, відмова від електронних платежів по Мережі.

Внаслідок обробки ризику залишається так званий залишковий ризик щодо якого приймається рішення про завершення етапу обробки ризику. Розділ «Безперервна діяльність з управління ризиками» торкається наступних двох фази менеджменту системи: контроль ризику та оптимізацію ризику. Для контролю ризику рекомендуються технічні заходи (моніторинг, аналіз системних журналів та виконання перевірок), аналіз зі сторони керівництва, незалежні внутрішні аудити ІБ. Фаза оптимізації ризику містить переоцінку ризику та відповідно перегляд політик, посібників з управління ризиками, коригування та оновлення механізмів безпеки. Процедури контролю ризиків та оптимізації, включаючи використання політик, заходів та засобів безпеки, ідентифікацію ресурсів, загроз та вразливостей, документування, гармонізовані з ISO 27001 та 27002[3]. У стандарті як додатки наведено приклади основних елементів оцінки вразливостей, загроз, ризиків, наведено варіант методики кількісної та якісної оцінки ризиків та ін. Результатом робіт з аналізу ризиків інформаційної безпеки, як правило, є: опис обстежених автоматизованих систем та сервісів, що застосовуються

адміністративних, організаційних заходів, програмно-технічних засобів забезпечення ІБ[6];

Картка ризиків інформаційної безпеки; план обробки ризиків, який включає комплекс впроваджуваних адміністративних, організаційних заходів та програмно-технічних коштів, спрямованих на зниження рівня ризиків інформаційної безпеки, оцінку вартості впровадження, а також графік заходів щодо впровадження заходів забезпечення чення ІБ (а в деяких випадках отримані дані можуть бути представлені у вигляді ескізного проекту реалізації системи інформаційної безпеки ІС організації). Зрештою рішення про впровадження в систему нових інструментів та механізмів інформаційної безпеки та вдосконалення наявних приймає керівництво організації, враховуючи пов'язані з цим витрати, їх прийнятність та кінцевий зиск для діяльності. Використання міжнародного стандарту ISO/IEC 27005:2011 дозволяє керівництву організувати цю діяльність на системній основі та захистити організацію від втрати будь-яких ресурсів, а найголовніше втрати ділової репутації.

1.2 Класифікація вразливостей та загроз

Під інформаційною безпекою (ІБ) розуміється стан захищеності інформаційних ресурсів (або ІС) та підтримуючої інфраструктури від випадкових чи навмисних впливів природного чи штучного характеру, пов'язаних із порушенням одного або кількох критеріїв ІБ (конфіденційність, доступність, актуальність/цілісність). Порушення ІБ зазвичай загрожують заподіянням шкоди власникам або користувачам інформаційних ресурсів. Особливого захисту потребують такі привабливі для зловмисників елементи мереж, як сервери та активне мережеве обладнання.[7] Перші – як концентратори великих обсягів інформації, другі – як елементи, у яких здійснюється перетворення даних (можливо через відкриту, незашифровану форму подання). При цьому в багатьох випадках отримати доступ до серверів та/або мережного обладнання організації зловмисників вдається, саме попередньо отримавши доступ до робочих станцій, які підключені до тому ж сегменту мережі, як і цільові компоненти інфраструктури. Розглянемо основні терміни та поняття, що стосуються ІБ, а також їх взаємозв'язки. Ризик – це ймовірність реалізації певної загрози ІБ (яка використовує деякі вразливості), а також величина можливої шкоди. Зазначимо, що поняття ризику є наслідком взаємного співвідношення логічного ланцюжка понять «актив» – «джерело загрози» – «вразливість» – «загроза» (дія) – «наслідки» (атака) – «збитки»:

- активи - ключові компоненти інфраструктури та значуща для власника інформація, що обробляється в інформаційній системі, що має певну цінність;
- джерело загрози інформаційній безпеці – суб'єкт доступу, матеріальний об'єкт чи фізичне явище, що є причиною виникнення загрози безпеці інформації;
- вразливість – це властиві об'єкту інформатизації властивості, що призводять до порушення безпеки інформації на конкретному об'єкті та обумовлені

особливостями процесу функціонування об'єкта інформатизації, властивостями архітектури автоматизованої системи, протоколами обміну та інтерфейсами, що застосовуються програмним забезпеченням. забезпеченням та апаратною платформою, а також умовами експлуатації;

- загроза (дія) – це можлива небезпека (потенційна чи реально існуюча) вчинення будь-якого діяння (дії чи бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), що завдає шкоди власнику, власнику або користувачеві, що виявляється в небезпеці спотворення, втрати та витоку інформації; • наслідки (атака) – це можливі наслідки реалізації загрози (можливі дії) при взаємодії джерела загрози через вразливості;
- збитки – витрати на відновлення системи у працездатний стан після можливого інциденту ІБ, а також на відновлення спотвореної, втраченої інформації або а нейтралізація наслідків витоку конфіденційної інформації.

1.2.1 Методи оцінки вразливостей

Вразливість необхідно оцінити[7]. Якщо класифікації універсальні, результати оцінки конкретної вразливості сильно залежить від IT-ландшафту, у якому вона виявлено.

Кожній вразливості надають ранг або оцінку серйозності на основі таких факторів, як:

- Які системи торкнулися.
- Які дані у небезпеці.
- Які бізнес-функції під загрозою.
- Наскільки легко реалізувати атаку і досягти компрометації ІС.
- Потенційні збитки внаслідок вразливості.

Виходячи з цього набору факторів, вразливість у тестовій версії ПЗ не така страшна, як така ж у продуктовій. Вразливість у старій версії ПЗ, для якої вже є патч, оцінюється як легша, ніж такий недолік у новітній програмі. При цьому в цілому вразливість віддаленого виконання коду в популярному MS Word

небезпечніша, ніж подібна дірка в якомусь рідкісному текстовому редакторі, оскільки вона торкається більше користувачів. Однак, якщо компанія використовує не Word, а саме це рідкісне рішення, то подібна помилка буде оцінена як критично небезпечна[8]. Повторимо, що залежить від контексту. Трапляються випадки, коли незрозуміло, як оцінювати вразливість. Зазвичай це з помилками конфігурації (наприклад, слабкий пароль на критичному сервісі). Такі кейси складно оцінити відповідно до загальноприйнятих стандартів. Проте він є і широко застосовується.

Стандарт CVSS

Common Vulnerability Scoring System без хибної скромності перекладається як загальна система оцінки вразливостей. Це галузевий стандарт, за яким оцінюють серйозність дірок у безпеці ІВ.

Коротка історія CVSS

На початку нульових Консультативна Рада з Інфраструктури США (NIAC) провела дослідження, завдяки яким у 2005 році з'явився перший стандарт із методами оцінки ПО-вразливостей. Закладені тоді принципові засади розрахунку метрики використовуються і сьогодні. Через те, що першу версію CVSS підтримувала ще молода експертна група CVSS-SIG, розробники почали скаржитися на численні недоліки стандарту.

У CVSS стали вносити правки і в 2007 році випустили другу версію зі зміненою формулою розрахунку. Пройшло сім років, перш ніж авторитетні Національний інститут стандартів та технологій (NIST) та Міжнародний союз електрозв'язку (ITU) випустили рекомендації щодо застосування цієї версії[9].

Третю версію CVSS NIAC опублікував у 2015 році. У розробці брали участь експерти Microsoft, IBM Internet Security Systems, Cisco, eBay, CERT/CC, Qualys, Symantec, DHS/MITRE. Її досі підтримує FIRST, хоча 2019 року вийшов апдейт: CVSS 3.1.

Метрики у CVSS CVSS дозволяє обчислити серйозність ризику за десятибальною шкалою. Чим більше число, тим вища небезпека і швидше потрібно на неї реагувати.

Ступені небезпеки за шкалою:

- низька - від 0,1 до 3,9 балів;
- середня - від 4 до 6,9;
- висока - від 7 до 8,9
- критична - від 9 до 10.

1.3 Вразливості

Властивості притаманні об'єкту інформатизації, невіддільні від нього та зумовлюються недоліками процесу функціонування, властивостями архітектури автоматизованих систем, особливостями протоколів обміну та інтерфейсів, що застосовуються програмним забезпеченням та апаратною платформою, умовами експлуатації та розташування[10]. Джерела загроз використовують вразливості для порушення безпеки інформації, отримання незаконної вигоди (завдання шкоди власнику, власнику, користувачу інформації). Крім того, можливі дії джерел загроз щодо активізації тих чи інших вразливостей, не пов'язані зі злим наміром. Найбільш поширеними причинами виникнення вразливостей є: • помилки при проектуванні, розробці та експлуатації програмно-апаратного забезпечення; • навмисні дії щодо внесення вразливостей у ході проектування, розробки та експлуатації програмно-апаратного забезпечення; • неправильні налаштування обладнання та ПЗ, неприпустима зміна режимів роботи пристроїв та програм; • несанкціоноване впровадження та використання неврахованих програм з подальшим необґрунтованим витрачанням ресурсів (наприклад, завантаження процесора, захоплення оперативної пам'яті, пам'яті на зовнішніх носіях); • впровадження шкідливих програм, що створюють вразливості у програмному та

програмно-апаратному забезпеченні; • несанкціоновані ненавмисні дії користувачів; • збої в роботі обладнання та ПЗ (викликані збоями в електроживленні, виходом з ладу апаратних елементів внаслідок старіння та зниження надійності, зовнішніми впливами електромагнітних полів технічних пристроїв та ін.). Кожній загрозі можуть бути зіставлені різні вразливості, усунення або суттєве послаблення, що впливає на ймовірність реалізації загроз ІХ. Загальна класифікація вразливостей. Вразливості ІБ можна поділити на об'єктивні, суб'єктивні та випадкові. Об'єктивні вразливості ґрунтуються на особливостях побудови та технічних характеристиках обладнання та ПЗ, що застосовуються на об'єкті, що захищається. Повне усунення цих вразливостей неможливе, але можуть істотно послаблюватися технічними і інженерно-технічними методами парірування загроз ІБ. Суб'єктивні вразливості залежать від дій суб'єктів (наприклад, розробників обладнання та ПЗ, системних адміністраторів та користувачів організації). Вразливості даного типу здебільшого усуваються організаційними та програмно-апаратними методами. Випадкові вразливості зумовлюються особливостями навколишнього об'єкту інформатизації середовища та непередбаченими обставинами. Багато з факторів, що забезпечують наявність таких вразливостей ІВ, загалом передбачувані, але повне їх усунення або неможливе, або утруднене та досяжне лише при проведенні цілого комплексу організаційних та інженерно-технічних заходів.

Уявімо у вигляді дерева рубрикатора.

- Вразливості.
  - Об'єктивні вразливості.
    - Супутні технічні засоби випромінювання.
      - ✦ Електромагнітні (побічні випромінювання елементів технічних засобів, кабельних ліній технічних засобів, випромінювання на частотах роботи генераторів, частотах самозбудження підсилювачів).

✦Електричні (наведення електромагнітних випромінювань на лінії та провідники, просочування сигналів у ланцюги електроживлення, в ланцюги заземлення, нерівномірність споживання струму електроживлення).

✦Звукові (акустичні, віброакустичні).

▪ Активізовані.

✦Апаратні закладки (встановлюються в лінії зв'язку, мережі електроживлення, приміщення, апаратне забезпечення та технічні засоби).

✦Програмні закладки (шкідливі програми, технологічні виходи із програм, нелегальні копії ПЗ).

✦Визначаються особливостями елементів.

✦Наявність елементів, робота яких пов'язана з електроакустичними перетвореннями (телефонні апарати, гучномовці та мікрофони, котушки індуктивності, дроселі, трансформатори та ін.).

✦Потенційні вразливості обладнання та ПЗ (наприклад, складність та недосконаліть коду ПЗ, що створюють передумови для успішних атак на відмова в обслуговуванні або "зрив" стека).

✦Наявність елементів, що піддаються впливу електромагнітного поля (магнітні носії, мікросхеми, нелінійні елементи, потенційно схильні до високочастотного нав'язування).

▪ Визначаються особливостями об'єкта, що захищається.

✦Розташування об'єкта (відсутність контрольованої зони, наявність прямої видимості об'єктів, віддалених та мобільних елементів об'єкта, що вібрують поверхонь, що відбивають).

✦Організація каналів обміну інформацією (використання радіоканалів, глобальних інформаційних мереж, орендованих

каналів, кабельних з'єднань, потенційно доступних зовні периметра, що охороняється).

- Суб'єктивні вразливості.
  - Помилки.
    - При розробці обладнання та ПЗ (наприклад, логічні та синтаксичні помилки при розробці алгоритмів та їх реалізації в ПЗ).
    - При підготовці та використанні ПЗ (при завантаженні та інсталяції ПЗ, подальшої експлуатації ПЗ, введення даних).
    - При керуванні складними системами (при використанні можливостей самонавчання систем, налаштування сервісів систем, організації управління потоками інформації).
    - При експлуатації технічних засобів (при включенні/вимкненні технічних засобів, використання технічних засобів охорони, використання засобів обміну інформацією).
  - Можливість порушень.
    - Вимог керівних документів.
    - Встановлені правила документування подій.
    - Режим охорони та захисту (доступу на об'єкт, доступу до технічних засобів).
    - Режим експлуатації технічних засобів (енергозабезпечення, життєзабезпечення).
    - Режим використання інформації (обробки та обміну інформацією, зберігання та знищення носіїв інформації, знищення виробничих відходів та шлюбу).
    - Режим конфіденційності (співробітниками в неробочий час, звільненими співробітниками).
- Випадкові вразливості.

▪ Потенційна можливість збоїв та відмов.

✦ Несправності обладнання та технічних засобів (обробних інформацію, що забезпечують працездатність засобів обробки інформації, що забезпечують охорону та контроль доступу).

✦ Старіння та розмагнічування носіїв інформації (дискет та знімних носіїв, жорстких дисків, елементів мікросхем, кабелів та сполучних ліній).

✦ Несправності ПЗ (ОС та СУБД, прикладних програм, сервісних програм, антивірусних програм тощо).

▪ Можливість порушення умов експлуатації.

✦ Порушення комунікацій (електро-, водо-, газо-, теплопостачання, каналізації, кондиціювання та вентиляції).

✦ Руйнування будівельних та огороджувальних конструкцій (зовнішніх огорож територій, стін та перекриттів будівель, корпусів технологічного обладнання).

1.3.1 Вразливість обладнання.

Апаратне забезпечення ІС піддається вразливості всіх трьох типів. У цілому нині вразливість устаткування пояснюється наступними чинниками, представленими нижче як дерева рубрикатора.

- Чинники, що зумовлюють вразливість устаткування.
  - Залежність від фізичного середовища експлуатації.
    - Схильність до обладнання вологості, пилу, забруднення.
    - Залежність від температури (плюс схильність до дії перепаду температур) і тиску.
    - Необхідність захисту від дії прямого сонячного проміння.
    - Схильність обладнання до вібраційних і ударних навантажень.

- Необхідність електроживлення (плюс схильність до флуктуацій електроживлення).

- Необхідність фізичного захисту від несанкціонованого доступу.
  - Необхідність розміщення інфраструктурного та клієнтського обладнання в приміщення з обмеженим доступом.
  - Необхідність наявності документації, що регламентує доступ до обладнання та відповідальність за несанкціонований доступ.
  - Залежність від правомірності та адекватності використання механізмів контролю фізичного доступу.
  - Беззахисність інфраструктурного та клієнтського обладнання щодо прямому фізичному впливу.

- Неминучі знос та старіння елементів обладнання.

- Необхідність обслуговування устаткування.
  - Необхідність наявності документації, що регламентує обслуговування обладнання та відповідальність за порушення вимог обслуговування.
  - Залежність від адекватності заходів щодо обслуговування обладнання (виконання вказівок регламентуючих документів).

- Неминуча ймовірність поломки елементів обладнання (сучасні технології проектування та виготовлення технічних засобів не дозволяють випускати обладнання з точно передбачуваним терміном роботи безвідмовної).

- Помилки та недоробки при проектуванні, виготовленні, доставці, підключенні, введення в експлуатацію, експлуатацію та обслуговування обладнання.

- Можливість впровадження апаратних закладок в обладнання.

1.3.2 Вразливість програмного забезпечення.

ПЗ також піддається вразливості всіх трьох типів. При цьому варто розрізняти системне та прикладне ПЗ. Системним ПЗ вважатимемо ОС, інфраструктурні системи управління базами даних (СУБД), драйвери пристроїв та протоколи мережевої взаємодії. У деяких випадках до системному ПЗ відносять мікропрограми, записані в пам'яті елементів обладнання (наприклад, прошивки материнських плат). Прикладне ПЗ - це програми, розраховані на безпосередню взаємодію з користувачем і призначені для виконання певних завдань користувача. Загальна характеристика вразливостей системного програмного забезпечення[11]. Вразливості системного ПЗ необхідно розглядати з прив'язкою до архітектури побудови обчислювальних систем. При цьому можливі вразливості:

• у мікропрограмах, прошивках ПЗП, ППЗП;

• у засобах ОС, призначених для управління локальними ресурсами (що забезпечують виконання функцій управління процесами, пам'яттю, пристроями введення/виведення, інтерфейсом з користувачем тощо), драйверах, утилітах;

• у засобах ОС, призначених для виконання допоміжних функцій – утилітах (архівування, дефрагментації та ін.), системних обробних програмах (компіляторах, компонувальників, відладчиків тощо), програмах надання користувачеві додаткових послуг (спеціальних варіантах інтерфейсу, калькуляторах, іграх тощо), бібліотеках процедур різного призначення (бібліотеках математичних функцій, функцій введення/виведення тощо);

• у засобах комунікаційної взаємодії (мережевих засобах) ОС. Вразливості в мікропрограмах і засобах ОС, призначених для управління локальними ресурсами та допоміжними функціями, можуть являти собою:

• функції та процедури, зміна параметрів яких певним чином дозволяє використовувати їх для несанкціонованого доступу без виявлення таких змін ОС;

• фрагменти коду програм (діри, люки), введені розробником, що дозволяють обходити процедури ідентифікації, аутентифікації, перевірки цілісності та ін; • відсутність необхідних засобів захисту (автентифікації, перевірки цілісності, перевірки форматів повідомлень, блокування несанкціоновано модифікованих функцій і т.п.);

• помилки в програмах (в оголошенні змінних, функцій і процедур, кодах програм), які за певних умов (наприклад, при виконанні логічних переходів) призводять до збоїв, у тому числі до збоїв функціонування засобів та систем захисту інформації

Стек протоколів TCP/IP[7]. Загальноприйнятим програмним мережевим стеком протоколів, які у сучасних мережах передачі, став TCP/IP. Цей стек спочатку був розроблено з ініціативи Міністерства оборони США наприкінці 1970-х років. і призначався для зв'язку експериментальної мережі ARPAnet із іншими сателітними мережами. Він представляє набір загальних протоколів для розрізнених обчислювальних середовищ.

Відповідність рівнів стека TCP/IP рівням моделі OSI досить умовна (рівні TCP/IP можна поставити у відповідність чотирьом верхнім рівням моделі OSI). Вразливості протоколів мережевої взаємодії пов'язані з особливостями їхньої програмної реалізації та обумовлені обмеженнями на розміри застосовуваного буфера, недоліками процедури аутентифікації, відсутністю перевірок правильності службової інформації та ін. Коротка характеристика вразливостей кількох протоколів верхніх рівнів OSI (На прикладі стека TCP/IP) наведена в табл. 2. У табл. 2 перераховані вразливості кількох протоколів стека TCP/IP, зумовлені факторами «на рівні ідеї» [12]. Необхідно відзначити, що у цих же протоколів є й інші вразливості, які обумовлені помилками та недоробками в їх реалізації, потенційною можливістю наявності в них «закладок», шкідливих програм тощо. протягом ПЗ, в якому реалізована підтримка цих протоколів, оновлюється, і відповідно кожна нова версія ПЗ може містити нові помилки або «закладки»

Для систематизації опису безлічі вразливостей програмних мережевих протоколів та ПЗ використовується єдина база даних (БД) вразливостей CVE (Common Vulnerabilities and Exposures), у розробці якої брали участь фахівці багатьох відомих компаній та організацій, таких як MITRE, ISS, Cisco, BindView, Axent, NFR, L-3, CyberSafe, CERT, Carnegie Mellon University, Інститут SANS тощо[13]. Ця БД постійно поповнюється і використовується при розробці численних програмних засобів аналізу захищеності та, насамперед, засобів моніторингу мереж.

Табл. 1.2

Таблиця вразливостей основних протоколів

Найменування протоколу	**Відповідність рівню OSI**	**Характеристика вразливості**	**Зміст порушення безпеки інформації**
FTP (File Transfer Protocol) – протокол передачі файлів по мережі	Прикладний, представлення, сеансовий	1. Аутентифікація на базі відкритого тексту (паролі пересилаються в незашифрованому вигляді). 2. Доступ за замовчуванням. 3. Наявність двох відкритих портів	Можливість перехоплення даних облікового запису (імен зареєстрованих користувачів, паролів). Отримання віддаленого доступу до хостів

Telnet – протокол керування віддаленим терміналом	Прикладний, представлення, сеансовий	Аутентифікація на базі відкритого тексту (паролі пересилаються у незашифрованому вигляді)	Можливість перехоплення даних облікового запису користувача. Отримання віддаленого доступу до хостів
RIP – протокол маршрутної інформації	Транспортний	Відсутність автентифікації керуючих повідомлень про зміну маршруту	Можливість перенаправлення трафіку через хост зловмисника
ARP – протокол перетворення IP-адреси на фізичну адресу	Мережевий	Аутентифікація на базі відкритого тексту (інформація пересилається у незашифрованому вигляді)	Можливість перехоплення трафіку зловмисником

Продовження таблиці 1.2

1	2	3	4
UDP – протокол передачі даних без встановлення з'єднання	Транспортний	Відсутність механізму запобігання перевантаженням буфера. Відсутність перевірки доставки пакетів адресату	Можливість реалізації UDP-шторму. Внаслідок обміну пакетами відбувається суттєве зниження продуктивності сервера. Ймовірність втрати інформації у процесі передачі

TCP – протокол управління передачею	Транспортний	Відсутність механізму перевірки коректності заповнення службових заголовків пакету	Істотне зниження швидкості обміну і навіть повний розрив довільних з'єднань за протоколом TCP
DNS – протокол встановлення відповідності мнемонічних імен та мережевих адрес	Прикладний, представлення, сеансовий	Відсутність засобів перевірки аутентифікації отриманих даних від джерела	Фальсифікація відповіді DNS-сервера

Продовження таблиці 1.2

1	2	3	4

IGMP – протокол передачі повідомлень про маршрутизацію	Мережевий	Відсутність автентифікації повідомлень про зміну параметрів маршруту	Можливість підробки маршруту. Приводить до зупинки операційних систем Win9x/WinNT
SMTP – протокол забезпечення сервісу доставки повідомлень електронною поштою	Прикладний, представлення, сеансовий	Відсутність підтримки автентифікації заголовків повідомлень	Можливість фальшування повідомлень електронної пошти, а також адреси відправника повідомлення
SNMP – протокол управління маршрутизаторами у мережах	Прикладний, представлення, сеансовий	Відсутність підтримки автентифікації заголовків повідомлень	Можливість досягнення максимальної пропускної можливості мережі

1.3.3 Загальна характеристика вразливостей прикладного програмного забезпечення.

Прикладні програми загального призначення - текстові та графічні редактори, медіапрограми (аудіо- та відеопрогравачі, програмні засоби прийому телевізійних програм тощо), системи управління базами даних, програмні платформи загального користування для розробки програмних продуктів (типу Delphi, Visual Basic»), засоби захисту інформації загального користування тощо[14].

Вразливості прикладного ПЗ можуть являти собою:

• функції та процедури, що стосуються різних прикладних програм і несумісні між собою (що не функціонують в одному операційному середовищі) через конфлікти, пов'язаних із розподілом ресурсів системи;

• функції та процедури, певна зміна параметрів яких дозволяє використовувати їх для проникнення в операційне середовище ІС та виклику штатних функцій ОС, виконання несанкціонованого доступу без виявлення таких змін ОС;

• фрагменти коду програм («дірки», «люки»), введені розробником, що дозволяють обходити процедури ідентифікації, автентифікації, перевірки цілісності та ін. передбачені ОС;

• відсутність необхідних засобів захисту (автентифікації, перевірки цілісності, перевірки форматів повідомлень, блокування несанкціоновано модифікованих функцій тощо);

• помилки в програмах (в оголошенні змінних, функцій та процедур, у кодах програм), які за певних умов (наприклад, при виконанні логічних переходів) призводять до збоїв, у тому числі до збоїв функціонування засобів та систем захисту інформації щодо можливості несанкціонованого доступу до інформації.

Класифікація вразливостей програмного забезпечення. У цілому нині вразливість ПО ІВ пояснюється такими чинниками, поданими нижче як дерева рубрикатора.

- Чинники, що зумовлюють вразливість ПЗ.
    - Помилки коду ПЗ.
        - Логічні.
        - Синтаксичні.
        - Помилки рівнів доступу.
            - ✦ Облікові записи, наділені певними повноваженнями, запроваджені розробниками в код, наприклад, для тестування ПЗ і потім забуті.
    - Закладені до коду вразливості.
        - "Закладки".
        - Мануфактурні входи (налагоджувальні входи).

- "Дірки" (коли помилка є, але ПЗ працює).
- "Банани" (коли через помилку ПЗ працювати перестає).
- Облікові записи, наділені певними повноваженнями, введені розробниками до коду для подальшого несанкціонованого доступу до систем користувачів цього програмного забезпечення.

- Недолік або відсутність необхідних засобів захисту (автентифікації, перевірки цілісності).
- Використання шкідливих програм.
- Наявність у коді ПЗ функцій, що потенційно дозволяють виконувати деструктивні дії.
- Відсутність чи недоліки перевірки коректності вхідних даних

1.4 Загрози

Загроза ІБ реалізується внаслідок утворення каналу реалізації загроз між джерелом загрози та носієм, що створює умови для порушення одного чи кількох критеріїв ІБ. Основними елементами каналу реалізації загроз ІХ є:

• джерело загроз ІБ – суб'єкт, матеріальний об'єкт чи фізичне явище, що утворюють загрози;

• середовище (шлях) поширення інформації чи впливів, у яких фізичне поле, сигнал, дані або програми можуть поширюватися і впливати на властивості, що захищаються (конфіденційність, актуальність, цілісність і доступність) інформації;

• носій – фізична особа або матеріальний об'єкт, у тому числі фізичне поле, в якому інформація знаходить своє відображення у вигляді символів, образів, сигналів, технічних рішень та процесів, кількісних характеристик фізичних величин.

Загальна класифікація загроз. Загрози ІБ класифікуються відповідно до таких ознак:

• за джерелом загроз ІБ;

• за способом реалізації загроз ІБ;

• за видом порушуваного якості ІБ (виду несанкціонованих дій, здійснюваних з информацией);

• за типом вразливості, що використовується;

• по об'єкту дії;

• за видом активів, схильних до загроз ІБ.

1.4.1 Класифікація джерела загроз.

Носіями загроз ІБ є джерела загроз, якими можуть бути як суб'єкти (особистість), і об'єктивні прояви[7]. Причому джерела загроз можуть бути як всередині організації, що захищається. внутрішні джерела, і поза нею – зовнішні джерела. Усі джерела загроз ІБ можна поділити на групи: антропогенні; технічні; стихійні (природні).

Антропогенні небезпеки. Джерелами загроз ІБ можуть виступати суб'єкти, дії (або бездіяльність) яких можуть бути кваліфіковані як навмисне чи випадкове заподіяння шкоди. Дії (чи бездіяльність) суб'єкта який завжди можна спрогнозувати і об'єктивно оцінити.

Як джерело загроз можна розглядати суб'єкта, який має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами, що захищається об'єкт. Суб'єкти (джерела), дії яких можуть призвести до порушення ІБ, поділяються на зовнішні і внутрішні.

Зовнішні джерела можуть бути випадковими або навмисними та мати різний рівень кваліфікації. До них відносяться:

• кримінальні структури;

• потенційні злочинці та зловмисники;

• недобросовісні партнери;

• конкуренти (конкуруючі організації

• представники наглядових організацій та аварійних служб;

• представники силових структур;

• представники провайдерів послуг зв'язку;

• у деяких випадках – звичайні користувачі ІС. Зовнішній порушник потенційно може здійснювати несанкціонований доступ:

• до каналів зв'язку, які виходять за межі службових приміщень;

• через автоматизовані робочі місця, підключені до мереж зв'язку загального користування;

• до інформації з використанням спеціальних програмних впливів за допомогою шкідливих програм, алгоритмічних чи програмних закладок;

• через елементи інформаційної інфраструктури, які у процесі свого життєвого циклу (модернізації, супроводу, ремонту, утилізації) опиняються поза контрольованої зони.

Необхідно відзначити, що вплив з боку зовнішніх порушників абсолютно необов'язково матимуть навмисний характер. Відповідно до технічних або організаційними особливостями будови ІВ дії (або бездіяльність) зовнішніх суб'єктів можуть призводити до порушень критеріїв ІБ у процесі нормальної експлуатації системи із використанням зовнішніх інтерфейсів доступу до неї. Крім того, перелічені вище зовнішні суб'єкти за певних умов можуть перейти до групи внутрішніх (наприклад, представники аварійних організацій та наглядових служб по службовій потреби можуть отримати можливість доступу до системи через її внутрішні інтерфейси).

Внутрішні суб'єкти (джерела) можуть являти собою як висококваліфікованих фахівців у галузі розробки та експлуатації ПЗ та технічних засобів (і бути знайомими зі специфікою розв'язуваних завдань, структурою, основними функціями та принципами роботи програмно-апаратних засобів захисту інформації), і малограмотними у сфері ІТ користувачами. До них відносяться:

• основний персонал;

• адміністративно-управлінський персонал;

• допоміжний персонал (бухгалтери, юристи, програмісти, системні адміністратори);

• технічний персонал (слюсарі, прибиральники, охорона).

Необхідно враховувати також, що особливу групу внутрішніх джерел становлять особи з порушеною психікою, а також спеціально впроваджені та завербовані агенти. Ця група розглядається у складі перелічених вище джерел загроз, але методи парирування загроз для цієї групи можуть мати свої відмінності.

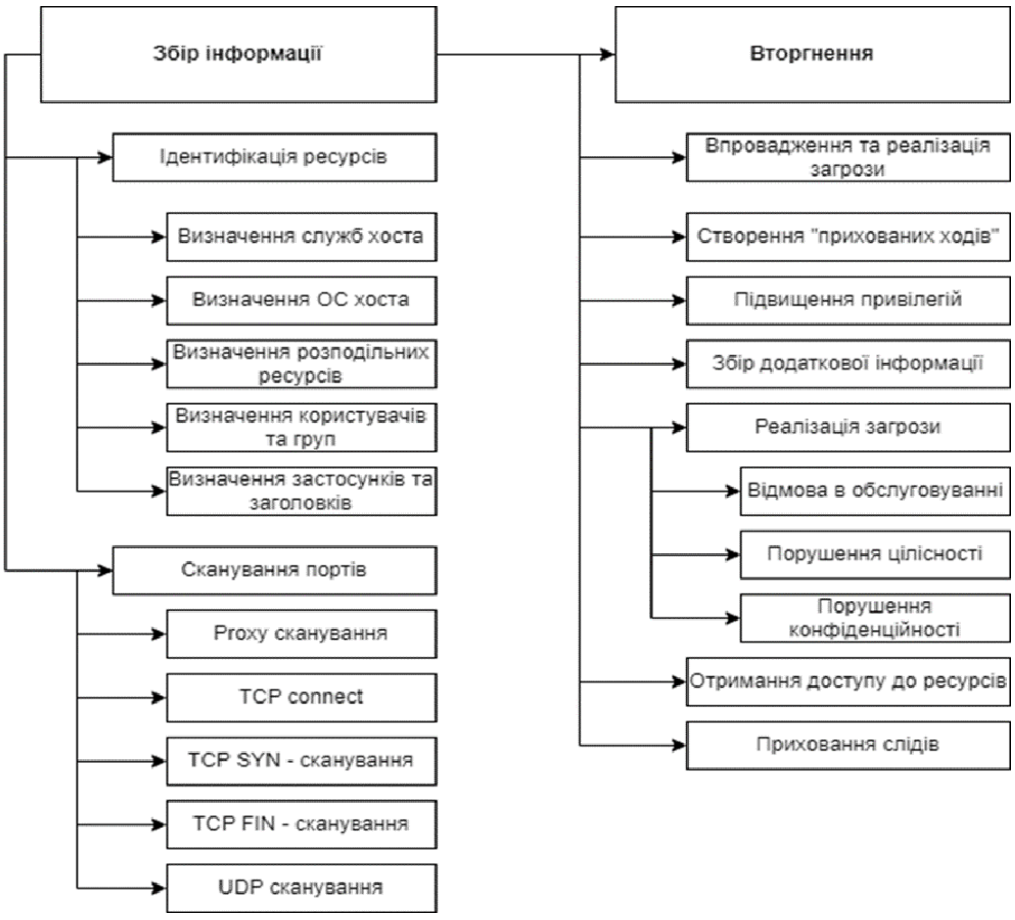


Рис 1.3 Класифікація загроз та вразливостей інформаційній безпеці в корпоративних системах

Класифікація на вигляд порушуваного властивості ІБ. За видом несанкціонованих дій, які здійснюються стосовно інформації, виділяються такі групи погроз:

• загрози, що призводять до порушення конфіденційності інформації (відпливу, копіювання або несанкціонованого поширення), при реалізації яких не здійснюється безпосереднього впливу на зміст інформації;

• загрози, що призводять до несанкціонованого (у тому числі випадкового) впливу на зміст інформації (порушення цілісності, актуальності);

• загрози, що призводять до несанкціонованого (у тому числі випадкового) впливу на програмно-апаратні елементи інформаційної системи, у результаті якого здійснюється блокування інформації (порушення доступності). Класифікація за видом вразливості включає:

• загрози, що реалізуються з використанням вразливості системного ПЗ;

• загрози, що реалізуються з використанням вразливості прикладного ПЗ;

• загрози, що виникають внаслідок використання вразливості в апаратних засобах;

• загрози, що реалізуються з використанням вразливостей протоколів мережевої взаємодії та каналів передачі даних;

• загрози, що реалізуються з використанням вразливостей, що зумовлюють наявність технічних каналів витоку інформації.

Класифікація об'єкта впливу містить загрози безпеці інформації:

• реалізовані через автоматизовані робочі місця користувачів; • реалізовані за допомогою впливу на сервери (у тому числі в кластери та хмарні сховища);

• зберігається та обробляється у виділених засобах обробки (принтерах, плоттерах, графопобудівниках, винесених моніторах, відеопроекторах, засобах звуковідтворення тощо);

• реалізовані у процесі взаємодії з каналами зв'язку. Класифікація за видом активів, схильних до загроз ІХ, включає:

• загрози безпеці даних і документів, що зберігаються на робочих станціях користувачів; • загрози безпеці даних і документів, що зберігаються на серверах (у в тому числі у кластерах та хмарних сховищах);
• загрози працездатності мережевих сервісів, обладнання та ПЗ робочих станцій та серверів, які можуть бути викликані успішними атаками на відмову в обслуговуванні або іншими причинами, що призводять до порушень якості доступності інформації.

1.5 Висновки до розділу

Описано загальну характеристику загроз, що реалізуються з використанням протоколів міжмережевої взаємодії. Основна мета створення класифікації загроз – найповніша, детальна класифікація, яка описує всі існуючі загрози ІБ, за якою кожна з загроз потрапляє тільки під одну класифікаційну ознаку і яка, таким чином, найбільш застосовна для аналізу ризиків реальних ІС.

ISO/IEC 27005 надає організаціям ефективний фреймворк для управління ризиками інформаційної безпеки, забезпечуючи їм засоби класифікації та оцінки загроз та вразливостей. Класифікація загроз дозволяє організаціям зосередитися на конкретних можливостях порушення безпеки інформації, визначаючи їхні основні характеристики та наслідки. Застосування ISO/IEC 27005 стає кроком до створення культури безпеки, забезпечуючи не лише реактивний підхід до управління ризиками, але й проактивний механізм адаптації до змін в загрозах та вразливостях. Цей стандарт стає надійним супутником для організацій, що прагнуть ефективно зберігати, обробляти та передавати інформацію в умовах постійної еволюції кіберзагроз.

Розділ 2. АНАЛІЗ ЗАГРОЗ ТА ІНЦИДЕНТІВ В СФЕРІ КІБЕРБЕЗПЕКИ

2.1 Аналіз загроз та інцидентів в кібербезпеці.

Аналіз загроз та інцидентів в кібербезпеці - це важливий процес, спрямований на виявлення, оцінку та управління потенційними загрозами кібербезпеці, а також відслідковування і вирішення фактичних інцидентів[16]. Цей процес включає в себе декілька ключових кроків:

- Збір інформації:
- Збір і аналіз даних про потенційні загрози: це може включати в себе сторонні джерела інформації, такі як оголошення від служб кібербезпеки, відкриті джерела, статистику та інші джерела.
- Моніторинг інфраструктури та мережі для виявлення незвичних або підозрілих активностей.
- Оцінка загроз:
- Визначення природи та серйозності потенційних загроз.
- Визначення вразливостей та можливих шляхів вторгнення для кожної конкретної загрози.
- Управління ризиками:
- Розробка та впровадження стратегій та заходів для зменшення ризиків, пов'язаних з ідентифікованими загрозами.
- Застосування технологічних і організаційних заходів для забезпечення кібербезпеки.
- Виявлення та реагування на інциденти:
- Моніторинг мережі для виявлення потенційних інцидентів.
- Розробка планів реагування на інциденти та їх реалізація у випадку інциденту.

- Збір та аналіз інформації про інцидент:
- Збір доказів та аналіз подій, що сталися під час інциденту.
- Визначення масштабу і серйозності інциденту.
- Відновлення та уникнення подібних інцидентів:
- Відновлення систем та мережі після інциденту.
- Розробка заходів для запобігання подібним інцидентам у майбутньому.
- Звітність та аналіз:
- Створення звітів про виявлені загрози та інциденти для внутрішнього та зовнішнього використання.
- Аналіз ефективності заходів та політик кібербезпеки.

Важливо регулярно вдосконалювати та оновлювати плани і стратегії кібербезпеки, оскільки загрози постійно змінюються і розвиваються. Також важливо мати механізми співпраці зі сторонніми організаціями, які можуть надавати додаткову підтримку і інформацію щодо загроз.

Сьогодні ні для кого не секрет, що поширення мережі Інтернет стало причиною незворотних і глобальних за своїми масштабами процесів стрімкої інформатизації всіх напрямків діяльності сучасної світової спільноти, призвело до справді революційних перетворень у житті людства. У зв'язку з цим очевидним є той факт, що питання забезпечення інформаційної безпеки в мережі Інтернет повинні мати комплексний характер і, перш за все, ґрунтуватися на глибокому аналізі можливих негативних наслідків використання мережі[16].

На жаль, у науковій літературі проблема класифікації загроз інформаційної безпеки в мережі Інтернет розглядається досить вузько: в основному з позиції порушень основних властивостей інформації - конфіденційності, доступності та цілісності. При такому підході вся увага зміщена на технічну компоненту Інтернету як особливу технологію обміну даними (інформацією). Водночас не можна забувати і про соціально-правову складову мережі Інтернет як особливий

простір, призначений для здійснення масової інформації та комунікації. І у цьому перше місце виходить зміст інформації, розміщеної у мережі. Позначена точка зору дозволяє нам як критерій для класифікації загроз інформаційної безпеки в мережі Інтернет виділити характер впливу на властивості інформації, що розміщується в мережі. На підставі цього критерію загрози інформаційної безпеки в мережі Інтернет доцільно розділити на дві великі групи: 1) загрози порушення конфіденційності, доступності та цілісності інформації; 2) загрози порушення вимог до змістовної частини інформації. До загроз порушення конфіденційності інформації ми відносимо розкрадання (копіювання) та витік інформації; до загроз доступності – блокування інформації; до загроз цілісності - модифікацію (спотворення) або заперечення справжності інформації. Реалізація перелічених загроз відбувається у вигляді:

– по-перше, створення та використання шкідливого програмного забезпечення, тобто. програм, які негативно впливають на роботу комп'ютера. До них відносяться віруси та програми-шпигуни (комп'ютерні віруси, мережеві черв'яки, троянські програми), небажане рекламне програмне забезпечення та різні форми шкідливих кодів;

- по-друге, розсилки спаму - небажаних електронних листів, що містять рекламні матеріали та/або шкідливі програми (у вигляді вкладень, що самозапускаються). Причин, з яких до спаму слід ставитися як до окремої категорії сучасних інтернет-загроз, кілька – це збільшення навантаження на поштові сервери, і ризик втрати важливої інформації, і ризик стати жертвою шахраїв, і марнування часу і оплаченого інтернет-трафіку. До загроз порушення вимог до змістовної частини інформації, розміщеної в мережі Інтернет, ми відносимо доступ до неналежного контенту та доступ до незаконного контенту. Під неналежним контентом слід розуміти розміщену в мережі інформацію, що не відповідає загальноприйнятим нормам моралі та моральності.

Як можливість заподіяння шкоди об'єкту інформаційних відносин загрози можуть поділятися на об'єктивні та суб'єктивні. Об'єктивні загрози викликані можливими впливами на інформаційні системи різних процесів, які залежать від волевиявлення людини (наприклад, стихійних природних явищ). Суб'єктивні загрози пов'язані з діяльністю людини. До них можна віднести:

- навмисні загрози, пов'язані з корисливими, ідейними чи іншими устремліннями людей;

– ненавмисні (випадкові) загрози, спричинені помилками у програмному забезпеченні чи діях персоналу.

В рамках цього виду загроз негативний відтінок набуває термін «соціальний інжиніринг» як вид маніпулювання людьми з метою проникнення в захищені інформаційні системи підприємств та/або окремих користувачів.

Кібербезпека стала однією з найбільш актуальних тем в сучасному світі, оскільки комп'ютеризація нашого життя зробила наші дані та інфраструктуру більш доступними для атак і зловмисних дій. Загрози кібербезпеки виходять далеко за межі звичайного вірусу або шкідливого ПЗ. Вони стали більш різноманітними та руйнівними, і для їх виявлення та запобігання використовуються різні інструменти та методи. Один з найефективніших підходів до розуміння та боротьби з кіберзагрозами - використання MITRE ATT&CK і CVE.

2.2 База даних атак MITRE ATT&CK

MITRE ATT&CK — це доступна в усьому світі база знань про тактики та прийоми зловмисника, заснована на реальних спостереженнях. База знань ATT&CK [3] використовується як основа для розробки конкретних моделей загроз і методологій у приватному секторі, в уряді та в спільноті продуктів і послуг

кібербезпеки. Створюючи ATT&CK, MITRE виконує свою місію з вирішення проблем для безпечнішого світу — об'єднуючи спільноти для розробки більш ефективної кібербезпеки. ATT&CK відкритий і доступний будь-якій особі чи організації для безкоштовного використання[18].

MITRE розробила ATT&CK у 2013 році для документування Тактик, Технік та Процедур (ТТП), які зловмисники використовували для цілеспрямованих кібератак на корпоративні інфраструктури під керуванням Windows. Фреймворк було створено з метою документування дій зловмисників для використання у дослідницькому проекті MITRE під назвою FMX. Метою FMX було дослідження можливості використання аналітики та телеметрії операційних систем для виявлення зловмисників після отримання ними доступу до корпоративних мереж. Команда нападу імітувала дії атакуючих усередині спеціальної лабораторії, а команда захисту розробляла аналітику для виявлення їхніх дій. ATT&CK використовувався як основа для тестування ефективності сенсорів та аналітики в рамках FMX, а також виступав спільною мовою для спільної роботи команд нападу та захисту.

- Тактика відповідає питанням *«чому?»* виконується техніка чи підтехніка ATT&CK. Це тактична мета зловмисника, причина вчинення дії. Наприклад, атакуючому може бути необхідно закріпитися в системі.
- Техніка відповідає питанням *«як?»* зловмисник досягає тактичної мети, виконуючи певну дію. Наприклад, атакуючий може створити або модифікувати системний процес, щоб закріпитися в системі.
- Підтехніка — це конкретніший, низькорівневий опис дії зловмисника. Наприклад, атакуючий може модифікувати системний сервіс ОС Windows, щоб закріпитися в системі.
- Процедура – це конкретна реалізація техніки чи підтехніки. Наприклад, атакуючий модифікує системний сервіс через реєстр Windows за допомогою утиліти Reg.exe, змінюючи значення ключа ImagePath на шлях до

шкідливого файлу. Процедури класифікуються в ATT&CK як варіанти реалізації техніки, виявлені в реальних комп'ютерних атаках. Вони перелічені на сторінках з описом технік у розділі «Procedure Examples».

ATT&CK також надає інформацію про «групи» загроз, які пов’язані з діяльністю вторгнення, а також програмне забезпечення, яке використовується цими групами. ATT&CK використовує термін «програмне забезпечення» для визначення зловмисного програмного забезпечення, спеціальних або комерційних інструментів, програмного забезпечення з відкритим вихідним кодом і утиліт ОС, які використовують зловмисники[18].

Сьогодні ATT&CK представляє структуру даних «кампанії», яка визначається як угрупування дій вторгнення, що виконуються протягом певного періоду зі спільними цілями. На даний момент ATT&CK включає 22 кампанії.

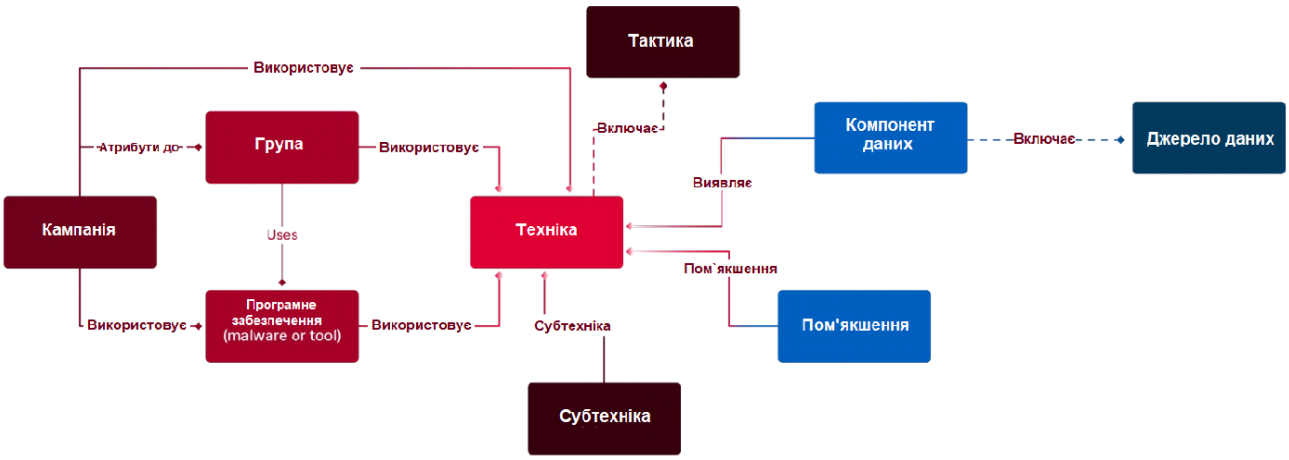


Рис 2.1. Життєвий цикл атак по MITRE

На рисунку 2.1. представлені зв’язки між об’єктами в MITRE ATT&CK Framework. Протягом життєвого циклу своїх атак групи кіберзагроз використовують «Методики» ATT&CK для досягнення своїх цілей, які в структурі класифікуються як «Тактики». MITRE ATT&CK визначає певне шкідливе

програмне забезпечення або інструменти для виконання методів зловмисників як «Програмне забезпечення». Як повна база знань, структура MITRE ATT&CK надає цінну інформацію про кожну техніку та способи пом’якшення за допомогою «Пом’якшення» та «Джерела даних».

2.3 Список відомих вразливостей CVE

CVE (Common Vulnerabilities and Exposures) – це список відомих вразливостей та дефектів безпеки. Розглянемо, що він являє собою і які дефекти безпеки з нього були затребувані у хакерів у 2021 році. До 1999, коли CVE [4] був запущений, було складно передавати інформацію про вразливість між різними базами, сканерами та іншими інструментами. Кожен виробник рішень щодо пошуку дефектів безпеки мав свою базу зі своїм способом іменування та набором параметрів вразливості. Для вирішення цієї проблеми компанією MITRE було створено CVE[19].

MITRE Corporation – американська некомерційна організація, що спеціалізується у галузі системної інженерії. Організація підтримує проекти у різних галузях, таких як космічна безпека, інформатика у охороні здоров'я, кібербезпека та інших. Ще одним відомим проектом MITRE є ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) – список відомих технік, прийомів та тактик, якими зловмисники користуються для атак на інформаційні системи, представлений у вигляді таблиць.

CVE це "словник" відомих загроз, кожен запис якого складається з наступних розділів: CVE ID, Reference, Description. CVE ID починається з префікса CVE-і записується із зазначенням року, в якому було повідомлено про вразливість та номер, присвоєний CNA (CVE Numbering Authorities).

CNA – це розробники програмного забезпечення, Bug Bounty програми та інші організації, що займаються пошуком вразливостей, уповноважені додавати нові записи до CVE. Основним CNA є MITRE, проте зараз статус CNA має 226 організацій з 34 країн світу[19].

Для того, щоб вразливість включили в CVE вона повинна відповідати критеріям:

- Вразливість має бути виправлена;
- Розробник, у продукті якого знайдено вразливість, повинен визнати, що вона має негативний наслідок безпеки;
- Вразливість стосується лише однієї кодової бази. Якщо вразливість пов'язана з помилками в open-source бібліотеках, протоколах чи стандартах, то CVE призначається кожному за порушеного продукту. Винятком є випадки, коли неможливо залишатися захищеним, використовуючи вразливий загальний код.

2.4 Аналіз втручань в ІС України на базі CrowdStrike

Російсько-українська війна, яка почалася в 2022 році, передбачала безпрецедентне використання кіберпотенціалів, які зберігалися протягом тривалої військової кампанії. CrowdStrike[6] Intelligence спостерігала за спектром активності Russia-Nexus, пов’язаної з цим конфліктом, включаючи масштабну діяльність зі збору розвідувальних даних, інформаційні операції з метою вплинути на суспільні настрої та розгортання деструктивних атак проти урядових і комерційних мереж[21]. Ці операції, проведені на тлі широкомасштабного патріотичного хактивізму, пов’язаного з цілями Росії, часто були спрямовані проти західних організацій, які супротивники російського державного зв’язку наразі не бажають переслідувати. Незважаючи на те, що Кремль інтегрував кіберпотенціал у свої військові кампанії задовго до 2022 року — як правило,

включаючи розподілені атаки на відмову в обслуговуванні (DDoS), — його діяльність у 2022 році демонструє ступінь, до якого Росія використовуватиме широкий спектр інструментів для досягнення своїх цілей, з різними ступенями успіху. На рис 2.2. показано загальний огляд того, як змінювалися рівні оперативної активності зв'язку Russia-Nexus протягом 2022 року, класифіковані за категоріями intelligence collection (збору розвідданих), information operations (інформаційні операції) та руйнівних мотивів.

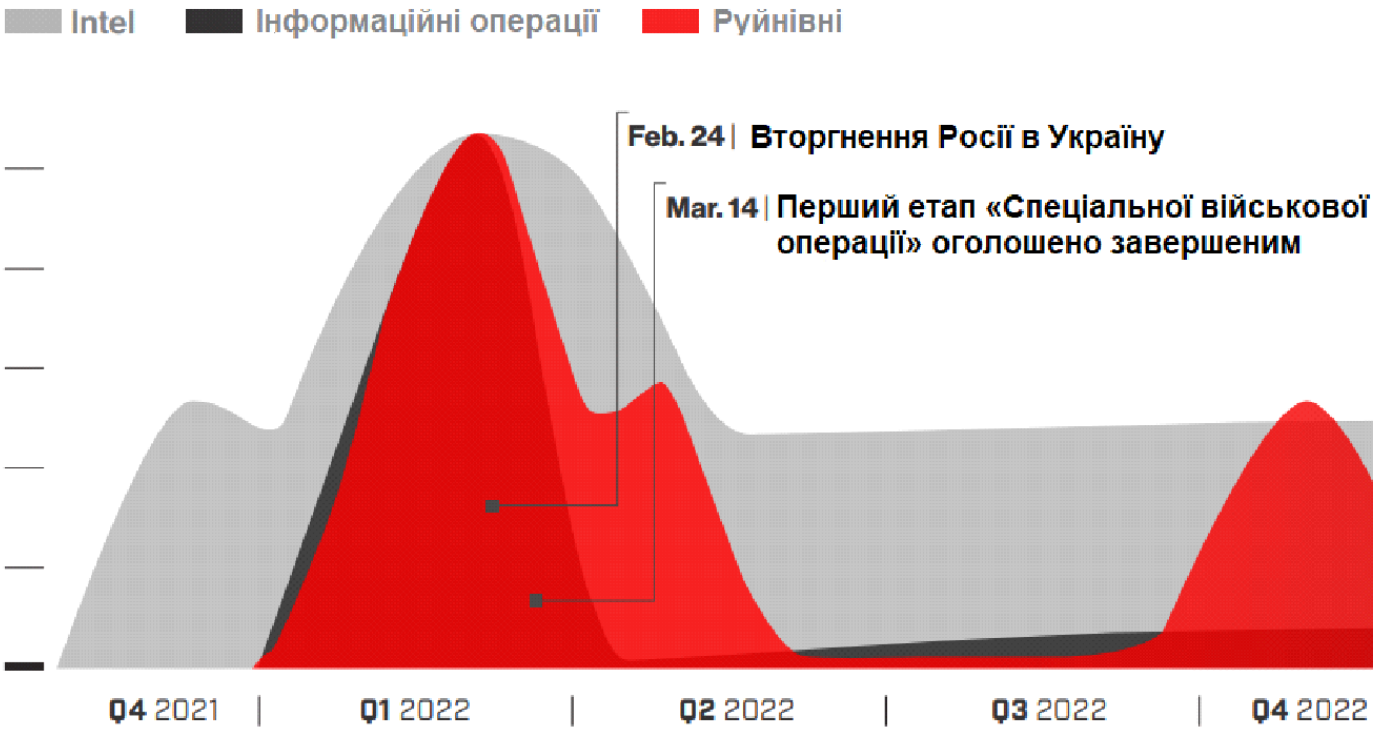


Рис 2.2. Графік атак Росії під час війни з Україною за 2022 рік

CrowdStrike Intelligence протягом 2022 року виявила цільові дії на українські організації в операціях, пов'язаних із різними супротивниками, пов'язаними з Росією, приєднаними до Росії чи ймовірно вихідцями з Росії. Відповідно до військової спрямованості Росії, Головне розвідувальне управління (ГРУ), здається, несе відповідальність за багато операцій проти України, хоча Федеральна служба безпеки (ФСБ) також підтримувала військові дії шляхом збору розвідданих. Такі вороги, як FANCY BEAR, EMBER BEAR, VOODOO BEAR, PRIMITIVE BEAR і GOSSAMER BEAR, а також кластери RepeatingUmbra та LostPotential, були

особливо активними проти України у 2022 році[21]. Інші кампанії без атрибуції також були націлені на організації та окремих осіб в Україні, ймовірно, для збору розвідданих. цілей. Вони зазвичай використовували методи фішингу облікових даних, щоб отримати доступ до облікових записів електронної пошти своїх цілей. 14 січня 2022 року, до вторгнення Росії в Україну, безперервний потік розвідданих, що проводився проти українських об'єктів, був доповнений серією руйнівних операцій EMBER BEAR, які включали пошкодження веб-сайтів і розгортання зловмисного програмного забезпечення WhisperGate. Ця кампанія, швидше за все, мала на меті погіршити дієздатність українського уряду, а також психологічно вплинути на українських громадян, вказавши, що українська влада не зможе захистити їх від наступної військової кампанії. Психологічні операції загострилися протягом лютого 2022 року з численними DDoS-атаками на українські державні портали та фінансові установи, які, ймовірно, мали на меті чинити тиск на українських громадян, порушуючи їхню здатність виконувати рутинні дії, такі як доступ до банківських послуг. Західні урядові джерела пізніше приписали деякі з цих атак ГРУ[21].

Багато деструктивних російських операцій проти українських мереж з початку вторгнення проводилися таємно з метою позбавити громадян України доступу до певного ресурсу — наприклад, енергопостачання чи урядової бази даних — без залучення громадськості. На відміну від цього, деструктивні операції EMBER BEAR у період із січня по лютий 2022 року проводилися відкрито, псували урядові веб-сайти, щоб оголосити про знищення даних і витік публічної інформації під приводом хактивізму, щоб ввести в оману авторство. Цей новий підхід до руйнівних операцій вказує на те, що EMBER BEAR, ймовірно, працюватиме в обмежених ситуаціях, коли психологічний вплив є особливо важливим.

23 лютого 2022 року зловмисники Russia-nexus почали численні атаки на українську мережеву інфраструктуру, використовуючи незрівнянну кількість

унікальних сімейств зловмисного програмного забезпечення, а також продовжували псувати веб-сайти. Протягом 48 годин нові сімейства зловмисних програм DriveSlayer, PartyTicket, IsaacWiper і AcidRain були розгорнуті проти цільових мереж, що збіглося з початком військового вторгнення Росії вранці 24 лютого 2022 року. Використання AcidRain — розгорнуто менше ніж через годину після Оголошення російського президента Володимира Путіна про «спеціальну військову операцію» — було особливо помітним, оскільки, як виявилося, було спеціально розроблено для переривання сегментів супутникової мережі Viasat, що забезпечує підключення до України.

Хоча справжні наслідки цієї ранньої дії проти українських урядових і військових комунікацій залишаються неясними, вони відчувалися за її межами. Принаймні три інтернет-провайдери по всій Європі також постраждали від цього збою, що призвело до перебоїв у роботі тисяч клієнтів і перебоїв у мережі вітряних турбін у деяких частинах Німеччини. Після початкового сплеску активності в перший тиждень війни, наступальні кібероперації Russia-Nexus продовжувалися в дуже високому темпі, хоча й із помітним зменшенням можливостей і різноманітності інструментів. Наприклад, wiper (витирач) DoubleZero був вперше розгорнутий у середині березня 2022 року, але не демонстрував складності, порівнянної з іншими деструктивними шкідливими програмами, розгорнутими в Україні. Ця зміна в якості свідчить про те, що в цей час операції стали більш тактичними та пристосованими, що, ймовірно, відображає брак планування поза межами очікувань Кремля щодо короткого періоду військового конфлікту. Діяльність, приписувана VOODOO BEAR, була винятком із цього скорочення операційної активності. Це включало розгортання CaddyWiper, яке почалося 14 березня 2022 року та тривало протягом року, а також атаки на український енергетичний сектор із використанням нового варіанту CrashOverride та ряду скриптів, призначених для видалення систем Linux і Solaris. Ці операції, швидше за все, були складнішими — хоча, ймовірно, з невеликим

масштабним ефектом — і тому вимагали більш тривалого періоду підготовки та виконання, що ілюструє складність ефективного використання кібероперацій порівняно з добре встановленою кінетичною військовою доктриною. Російська кіберактивність у другій половині 2022 року значною мірою характеризувалася зміщенням акценту на операції зі збору розвідданих, що, ймовірно, вказує на зростання вимог російської армії та Кремля до ситуаційної обізнаності, оскільки їхнє просування в Україну зупинилося та повернулося назад. Визначені кампанії включали значні зусилля FANCY BEAR, PRIMITIVE BEAR і кластерів активності RepeatingUmbra і LostPotential для проведення операцій з фішингу облікових даних проти українських цілей. Операції з фішингу облікових даних GOSSAMER BEAR також зберігали високі операційні темпи з лютого 2022 року, включаючи напади на державні дослідницькі лабораторії, військових постачальників, логістичні компанії та неурядові організації із серпня 2022 року. Це цілеспрямоване націлювання, ймовірно, вказує на амбіції противника щодо збору розвідданих, пов'язаних із західною військовою підтримкою України, хоча націлювання на неурядові організації також може означати підготовку інформаційних операцій проти організацій, які можуть бути залучені до загрозливих розслідувань російських військових злочинів[21].

Незважаючи на більший наголос на зборі розвідданих, у жовтні та листопаді 2022 року було розгорнуто сімейство зловмисних програм Prestige і RansomBoggs, які ймовірно зв'язані з Росією, замасковані під програми-вимагачі. Історично VOODOO BEAR широко маскували свої наміри видалення за допомогою псевдозагроз програм-вимагачів, однак їхні останні розгортання wipers (витирачів) не використовували цей обман, ймовірно, через обмежену користь від приховування атрибуції проти українських цілей. Нещодавнє повернення Росії до використання підроблених програм-вимагачів свідчить про її намір розширити свою таргетацію, щоб включити сектори та регіони, у яких деструктивні операції вважаються політично ризикованими. Наразі загальний вплив кібероперацій Росії

в контексті вторгнення в Україну 2022 року незрозумілий. Хоча російські кіберпотенціали, безсумнівно, сприяли військовій кампанії Росії, вони також продемонстрували обмеження, властиві воєнному часу. Це особливо вірно у випадку руйнівних атак, які часто вимагають ретельного планування, але часто є менш ефективними та довготривалими порівняно зі своїми кінетичними аналогами. Крім наслідків значної допомоги, яку Україна отримала від міжнародного співтовариства, оперативна ефективність Росії також, ймовірно, була знижена через покращення оборонних можливостей України після вторгнення Росії в Крим у 2014 році. Ці фактори потенційно вплинули на курс російської військової стратегії в цьому конфлікті , що розходиться з очікуваннями суспільства щодо того, як кібероперації можуть підтримувати сучасну війну. Атаки на ключові сектори, такі як енергетика, телекомунікації, транспорт і медіа, не були такими масовими, як передбачалося, що, ймовірно, свідчить про те, що Кремль очікував швидкої та рішучої перемоги над Україною та планував використати ці функціонуючі ресурси, щоб зберегти Україну під новим режимом. Ранні побоювання щодо значного супутнього збитку міжнародним мережам також не були повністю усвідомлені. Виявлені атаки здебільшого були локалізовані в українських мережах і уникали використання неконтрольованих механізмів розповсюдження, які могли б поширюватися на небажані сектори та регіони. Незважаючи на це, наразі незачеплені сектори можуть зазнати майбутніх цілей у міру того, як війна прогресуватиме та потенційно змінить курс.

2.5 Аналіз втручань в ІС України на базі Picus Security

Picus Labs проаналізувала понад 500 000 зразків зловмисного програмного забезпечення в період із січня 2022 року по грудень 2022 року, щоб визначити тактики, прийоми та процедури (TTP), які вони демонстрували[22]. Кожен спостережуваний TTP був класифікований за допомогою MITRE ATT&CK®

Framework. Загалом Picus Labs [7] спостерігали понад 4,3 мільйона методів ATT&CK і використовували ці дані, щоб визначити найбільш поширені. Звіт 2023 висвітлює десять найпоширеніших виявлених методів ATT&CK і містить інформацію, яка допоможе командам безпеки відповідно визначити пріоритети своїх захисних дій[22].

Підкреслення горизонтального руху супротивників. Найважливішим висновком цьогорічного звіту є те, що зловмисники все частіше використовують зловмисне програмне забезпечення для виконання бічного руху. Латеральний рух це тактика, яку зловмисники використовують для переходу від однієї скомпрометованої системи в мережі до іншої, допомагаючи їм досягати своїх цілей. T1021 Remote Services і T1018 Remote System Discovery — це нові методи в десятці найкращих цього року Red Report, які в основному використовуються для бокового руху. Третій новачок у списку, T1047 Windows Management Instrumentation, зловживаний зловмисниками для виконання файлів і команд у віддалених системах. На додаток до вищезазначених методів, зловмисники також використовують T1059 Command and Scripting Interpreter і T1003 OS Credential Dumping, перший і другий найпоширеніші ідентифіковані методи, щоб виконувати команди на віддалених системах і отримувати облікові дані облікових записів. Вони також сприяють латеральному руху. Зростання поширеності методів, які застосовуються для здійснення бокового руху, підкреслює важливість покращення запобігання та виявлення загроз як на охоронному периметрі, так і всередині мереж[22].

Методологія. У період із січня 2022 року по грудень 2022 року Picus Labs проаналізувала 556 107 унікальних файлів, із яких 507 912 (91%) були класифіковані як шкідливі. Джерела цих файлів включають, але не обмежуються:

- комерційні та відкриті служби розвідки про загрози
- постачальники безпеки та дослідники
- пісочниці шкідливих програм

- бази шкідливих програм

З цих файлів було вилучено 5 388 946 дій, у середньому 11 шкідливих дій на зловмисне програмне забезпечення. Потім ці дії були зіставлені з методами MITRE ATT&CK, виявивши в середньому 9 прийомів на зловмисне програмне забезпечення. Щоб скласти десятку найкращих Red Report 2023, дослідники Picus Labs підрахували відсоток зловмисного програмного забезпечення в наборі даних, які використовували кожну техніку ATT&CK. Наприклад, метод T1059 Command and Scripting Interpreter був продемонстрований у 159 196 (31%) із 507 912 проаналізованих шкідливих файлів.

Ключові висновки

- *Основні ідеї Red Report 2023 для команд безпеки: Бічний рух наростає: зловмисники використовують нові, а також випробувані методи*

Зловмисники все частіше використовують методи бічного переміщення, тактику переходу від однієї скомпрометованої системи в мережі до іншої. Крім інтерпретатора команд і сценаріїв і дампу облікових даних ОС, які широко поширені, нові методи, такі як Remote Services, Remote System Discovery і WMI, також все частіше використовуються для виявлення віддалених систем, виконання команд на віддалених системах і отримання облікових даних.

- *Програми-вимагачі залишаються поширеними: Шифрування даних є головною загрозою*

Data Encrypted for Impact другий рік поспіль зберігає свою позицію третьої найбільш часто використовуваної техніки зловмисниками. Ця техніка, яку демонструє майже чверть усіх проаналізованих шкідливих програм, шифрує файли та підкреслює постійну загрозу програм-вимагачів для організацій.

- *Зловживання віддаленим дослідженням і доступом: Зловмисники використовують вбудовані інструменти Windows, Linux і macOS*

Нові методи, Remote System Discovery і Remote Services передбачають зловживання вбудованими інструментами та протоколами операційних систем, як-

от net, ping, RDP, SSH і WinRM, із зловмисною метою. Це дозволяє зловмисникам збирати інформацію про цілі, включаючи системи Windows, Linux і macOS у скомпрометованій мережі, і переміщатися по всій мережі, не будучи виявленими засобами безпеки. Ця тенденція вказує на те, що зловмисники все частіше використовують законні інструменти та служби віддаленого виявлення та доступу.

Ідентифікація та облікові дані є новим периметром: традиційної безпеки периметра вже недостатньо

OS Credential Dumping (Дамп облікових даних ОС) T1003 тепер є другою за поширеністю спостережуваною технікою. Ця техніка дозволяє зловмисникам отримувати дані для входу в обліковий запис та облікові дані зі зламаних машин. Будь-яка отримана інформація може бути використана для переміщення в мережі, підвищення привілеїв і доступу до інформації з обмеженим доступом. Зростання дампінгу облікових даних підкреслює той факт, що традиційної безпеки периметра вже недостатньо для захисту від кібератак. Натомість організаціям необхідно посилити кіберстійкість, підготувавшись до захисту від (перед) скомпрометованих і (пост) скомпрометованих атак.

Розкриття темної сторони легітимних інструментів: зловмисники використовують законне програмне забезпечення для кібератак

Зловмисники віддають перевагу використанню легітимних інструментів над інструментами, розробленими на замовлення. Це підкреслюється найпоширенішою технікою, T1059 Command and Scripting Interpreter, яка передбачає зловживання законними інтерпретаторами, такими як PowerShell, AppleScript і оболонки Unix, для виконання довільних команд. Інші приклади законних інструментів, якими зазвичай зловживають зловмисники, включають утиліти для дампінгу облікових даних ОС, виявлення системної інформації, віддалених служб, WMI, запланованих завдань/завдань і віддаленого виявлення системи.

Шкідливе програмне забезпечення продовжує розвиватися швидко: зростання багатогранних тактик кібератак

Згідно з аналізом, у середньому зловмисне програмне забезпечення використовує 11 різних TTP (тактики, техніки та процедури). Одна третина зловмисного програмного забезпечення (32%) використовує понад 20 TTP, а одна десята шкідливого програмного забезпечення використовує понад 30 TTP. Ці висновки свідчать про те, що розробники зловмисного програмного забезпечення, які стоять за цими атаками, дуже досвідчені. Ймовірно, вони вклали значні ресурси в дослідження та розробку широкого спектру методів уникнення виявлення та компрометації систем.

Найпоширеніші методи ATT&CK, визначені у 2022 році, перераховані за відсотком зразків зловмисного програмного забезпечення, у яких виявлено таку поведінку:

- Command and Scripting Interpreter (Інтерпретатор команд і скриптів)
- OS Credential Dumping (Демпінг облікових даних)
- Data Encrypted for Impact (Дані зашифровані для впливу)
- Process Injection (Ін'єкція коду в процес)
- System Information Discovery (Виявлення системної інформації)
- Remote Services (Віддалені служби)
- Windows Management Instrumentation (Інструмент керування Windows)
- Scheduled Task/Job (Заплановане завдання)
- Virtualization/Sandbox Evasion (Ухилення від віртуалізації/пісочниці)
- Remote System Discovery (Віддалене виявлення системи)

Рекомендації для команд безпеки:

- *Регулярно перевіряйте та оптимізуйте засоби безпеки.* Ландшафт загроз постійно змінюється, оскільки зловмисники постійно розробляють нові методи атак і ухилення. Регулярне тестування та налаштування елементів керування безпекою мають важливе значення, щоб гарантувати, що засоби

безпеки здатні виявляти та запобігати найновішим методам обхідних атак. Оптимізувавши засоби контролю безпеки, організації можуть покращити загальний стан кіберзахисту та зменшити ризик успішних кібератак.

- *Використовуйте поведінкове виявлення.* Зловмисники все частіше використовують легітимні інструменти та служби для зловмисних цілей і ухиляються від виявлення. Команди безпеки повинні використовувати поведінкові методи виявлення, зосереджені на виявленні зловмисної активності на основі того, як вона відхиляється від нормальної поведінки, а не намагатися ідентифікувати та блокувати відомі статичні індикатори компрометації (IOC). Це дозволить командам виявляти атаки, які не можуть бути виявлені традиційними засобами безпеки.
- *Розкриття шляхів атак.* Зловмисники використовують різноманітні методи, щоб пересуватися мережами та отримати облікові дані. Команди безпеки повинні виявити шляхи атак, щоб зрозуміти, як зловмисники пересуваються мережею та які методи вони використовують. Це дозволить командам визначити першопричину порушень і зосередитися на найбільш критичних прогалинах у безпеці, щоб визначити пріоритети для пом’якшення. Завдяки цьому організації можуть краще зрозуміти конкретні етапи атаки, визначити системи та дані, які знаходяться під загрозою, і запровадити відповідні засоби контролю безпеки для виявлення та реагування на атаки.
- *Операціоналізація MITRE ATT&CK.* Зловмисники використовують різноманітний набір тактик, методів і процедур (TTP) для здійснення кібератак. Операціоналізація MITRE ATT&CK може допомогти організаціям ідентифікувати, виявляти та запобігати кібератакам, надаючи повне розуміння TTP, які використовують зловмисники. Це також дозволяє організаціям визначати пріоритети своїх захисних зусиль, виявляти та запобігати атакам, а також покращувати співпрацю.

2.6. Засоби захисту мережі

Засоби захисту мережі – це інструменти, механізми та технології, додані до мережі для забезпечення безпеки даних, голосової та відео-інформації, які зберігаються та передаються по мережі. Ці засоби продовжують безперервно вдосконалюватись, але основні знання на цю тему легко доступні[23]. Щоб не дозволити зловмисникам проникнути до мережі, необхідно їм перешкоджати. Для цього використовуються міжмережеві екрани, проксі-сервери та шлюзи. Було б необачно вважати, що цих пристроїв достатньо, щоби повністю виключити проникнення зловмисників у мережі. Раніше чи пізніше вони знаходять якусь лазівку. Широко відомий хакер Кевін Мітник запевняє, що коли його наймають компанії для перевірки системи безпеки своїх мереж, він у 100% випадків проникає до мережі. Спосіб зламати мережу завжди знаходиться. Щоб надійно забезпечити безпеку, потрібно безперервно вчитися, удосконалювати захист та випереджати хакерів хоча б на крок. На випадок вторгнення в мережу дуже важливо мати план і команду реагування на інциденти.

Засоби захисту мережі[8]:

- Міжмережевий екран
- IDS/IPS
- VPN
- Антивірусне програмне забезпечення
- Журнали, моніторинг та SIEM
- EDR/XDR системи

2.6.1 Міжмережевий екран

Міжмережевий екран - це система мережної безпеки, яка контролює вхідний та вихідний мережевий трафік на основі заданих правил безпеки. Міжмережевий екран встановлює бар'єр між довіреною мережею та недовіреною мережею, такою як інтернет. Призначення міжмережевого екрану - фільтрувати хороший від

поганого, або довірений від недовіреного трафіку. Термін походить від концепції фізичних стін, які є бар'єрами для уповільнення поширення вогню до прибуття пожежників. За аналогією, міжмережеві екрани призначені для керування мережевим трафіком - зазвичай з метою уповільнити поширення мережевих загроз[23].

Міжмережеві екрани зазвичай встановлюються на межі між довіреною та недовіреною мережею, щоб створити “точку заповільнення”, через яку проходить весь трафік. Вони аналізують дані, що надсилаються комп'ютерною мережею, і приймають рішення на основі набору правил. Дані, що надсилаються по комп'ютерній мережі, збираються в пакет, який містить IP-адреси відправника та одержувача, номери портів та іншу інформацію. Перш ніж пакет досягне свого пункту призначення, він відправляється на міжмережевий екран для перевірки. Якщо міжмережевий екран визначає, що пакет дозволено, він відправляє їх у пункт призначення; інакше міжмережевий екран відкидає пакет.

Налаштування ММЕ визначають, який трафік дозволено пропускати, при цьому враховується тип трафіку та потреби бізнесу. Відповідно до найкращих практик ММЕ за умовчанням блокує весь трафік. Потім у налаштуваннях надається дозвіл пропускати лише певний трафік до відомих служб. Для ефективної роботи ММЕ необхідно його правильно налаштувати, тому адміністратор, який виконує налаштування, має бути дуже кваліфікованим[23].

Міжмережеві екрани працюють на різних рівнях моделі OSI. Зазвичай це рівні з другого до п'ятого. Якщо ММЕ працює на прикладному рівні (L7), його часто називають проксі-сервером або шлюзом. Винятком є захисний екран для веб-додатків (WAF), для якого термін «екран» застосовується і на сьомому рівні. Міжмережевий екран аналізує інформацію, що знаходиться на рівні моделі OSI, на якому він працює.

Приклад роботи ММЕ на різних рівнях:

- L2 (канальний рівень) - MME може блокувати або пропустити трафік на основі MAC-адреси відправника;
- L3 (мережевий рівень) - MME пропускає через себе або блокує трафік, аналізуючи IP-адресу всередині пакета;
- L4 (транспортний рівень) - MME блокує або пропускає через себе трафік на основі номера TCP-порту в датаграмі.
- L5 (сеансовий рівень) - MME блокує або пропускає через себе трафік на основі інформації протоколу передачі в реальному часі (RTP).
- L7 (прикладний рівень/рівень програм) — MME блокує або пропускає через себе трафік, аналізуючи програму або службу програм.

Міжмережевий екран конфігурують за допомогою списку правил (політик). MME переглядає цей список, щоб визначити, що робити з вхідним трафіком. Список переглядається послідовно, зверху донизу. Спочатку MME порівнює кадр або пакет із першим правилом списку. Якщо вхідний тип трафіку відповідає всім критеріям правила фільтрації, виконується вказана дія: пропустити або заблокувати. Якщо кадр або пакет не відповідає першому правилу, міжмережевий екран порівнює його з другим правилом тощо. Якщо трафік не відповідає жодному із заданих правил, MME слідуватиме останньому правилу: заблокувати трафік.

2.6.2 Проксі

Проксі-сервер із функціями MME працює на сьомому рівні моделі OSI. Коли проксі отримує трафік, він обробляє кадр або пакет, піднімаючись рівнями. Наприклад, кадр видаляється на другому рівні, заголовки пакета - на третьому, і так далі до сьомого рівня, де інформація подається у вигляді даних. Протокол TLS припиняє діяти після четвертого рівня, і з цього моменту дані проксі-сервері передаються відкритим текстом. Тоді проксі аналізує дані, що передаються, чого на більш низьких рівнях не дозволяло зробити шифрування. Таким чином, проксі може аналізувати набагато більше даних, ніж стандартний MME. Звичайно, для

проксі-сервера з функціями MME потрібно більше часу або обчислювальної потужності, але він забезпечує більш надійний контроль трафіку користувача.

2.6.3 IDS/IPS (Системи виявлення та запобігання вторгненням)

Ще одним завданням безпеки є виявлення вторгнень у мережу за допомогою систем виявлення вторгнень (IDS). Цей пристрій (або програмний продукт) поводиться пасивно. Воно відстежує мережевий трафік і якщо виявить, що він є підозрілим, то реєструє цей факт у журналі подій. IDS може бути як мережним, так і кінцевим пристроєм. Залежно від місця встановлення IDS поділяються на мережеві (network-based IDS, NIDS) і хостові (host-based IDS, HIDS). NIDS зазвичай підключається до TAP-порту або SPAN-порту комутатора. Трафік без перешкод передається до місця призначення, а його копія надсилається на SPAN-порт NIDS для аналізу. Хостовий IDS може встановлюватися на ноутбуці, планшеті, сервері тощо. Більшість HIDS аналізують не трафік у режимі реального часу, а журнали трафіку постфактум. Якоїсь миті виробники вирішили вивести ці пристрої на новий рівень. Якщо IDS можуть виявити атаку, логічно було б відразу видаляти підозрілі кадри або пакети, не обмежуючись повідомленням про них. В результаті з'явилися системи запобігання вторгненням (IPS). IPS також поділяються на мережеві (NIPS) та хостові (HIPS). Це чудова ідея, але й є зворотний бік медалі. IPS спочатку потрібно пояснити, який трафік вважати поганим. Цього можна досягти за допомогою файлів сигнатур чи навчання.

2.6.4 Віртуальна приватна мережа (VPN)

Наступне питання, яке необхідно вирішити, — як захистити під час передачі дані, голосову інформацію чи відео від сторонніх очей. Це стосується як корпоративної чи домашньої мережі, так і інтернету чи мережі постачальника послуг.

Для вирішення цієї проблеми застосовується шифрування, яке перетворює дані в форму, що не читається без ключа. Для захисту даних, що передаються, є кілька варіантів шифрування. Ось вони:

- криптографічний протокол SSL/TLS;
- протокол віддаленого доступу SSH (Secure SHell);
- стек протоколів IPsec (Internet Protocol Security).

SSL/TLS

SSL/TLS використовується з 1995 р. для захисту з'єднань між браузером та веб-сервером. Протокол SSL (Secure Socket Layer) розробила компанія Netscape Communications. Потім з'явилися версії 2.0 і 3.0, але після того, як Internet Engineering Task Force (IETF) стандартизував SSL, протокол перейменували в TLS (Transport Level Security). Це сталося, коли корпорація America Online (AOL) придбала Netscape. На даний момент найновіша версія протоколу - TLS 1.3 (RFC 8446). TLS використовується не тільки для підключення до Інтернету. На нього також можуть спиратися з'єднання VPN. SSL/TLS – це протокол транспортного рівня, який використовує для браузер-з'єднань TCP-порт 443.

SSH

SSH – найпоширеніший метод для віддаленого входу до системи. Цей протокол шифрує всю інформацію, що передається по мережі. За допомогою SSH мережеві адміністратори віддалено керують мережевими пристроями: маршрутизаторами та комутаторами. В першу чергу SSH створили для заміни Telnet, який є небезпечним, оскільки він не шифрує дані, хоча може застосовуватися для VPN-з'єднань. Специфікація транспортного протоколу SSH міститься у документі IETF RFC 4253. За замовчуванням SSH працює на TCP-порту 22.

IPsec

IPsec – це набір протоколів мережного рівня, що забезпечує шифрування та перевірку цілісності для будь-якого типу з'єднання. Розроблено кілька документів IETF RFC, у яких містяться специфікації протоколів, що входять до IPsec. RFC 6071 показано, як ці документи співвідносяться один з одним. В IPsec входять два протоколи безпеки: AH (Authentication Header) та ESP (Encapsulating Security

Payload). AH перевіряє справжність джерела та цілісність даних. Для реалізації IPSec не обов'язково підтримувати AH, який додає IP-пакет спеціальний заголовок з контрольною сумою. Протокол ESP повинні обов'язково підтримувати всі реалізації IPsec, оскільки він забезпечує як справжність джерела, так і цілісність та конфіденційність даних. ESP шифрує корисну інформацію IP-пакету.

2.6.5 Антивірусне програмне забезпечення

Антивірусне програмне забезпечення - це спеціальне програмне забезпечення, яке призначене для виявлення, блокування та видалення шкідливого програмного забезпечення, такого як віруси, троянці, шпигунське ПЗ і інші загрози для комп'ютерної безпеки. Воно працює шляхом сканування файлів і програм на наявність вразливостей та загроз, а також спостереження за активністю в реальному часі. Антивірусне ПЗ допомагає захищати комп'ютери та інші пристрої від інфікування та може допомогти зберегти конфіденційність і цілісність даних.

Основні функції антивірусного програмного забезпечення:

- Виявлення загроз: Антивірусне ПЗ аналізує файли і програми, щоб виявити можливі загрози для безпеки. Воно використовує бази даних відомих вірусів і шкідливого ПЗ, а також евристичні методи для виявлення незвіданих загроз.
- Блокування атак: Якщо антивірус виявляє загрозу, він може намагатися заблокувати або ізолювати її, щоб запобігти поширенню шкідливого програмного забезпечення.
- Вилучення шкідливого ПЗ: Антивірус може спробувати вилучити виявлені загрози з комп'ютера або пристрою. Це може включати видалення файлів, ключів реєстру та інших складових шкідливого програмного забезпечення.
- Оновлення баз даних: Антивірусне ПЗ потребує постійного оновлення своїх баз даних відомих загроз, оскільки нові віруси та шкідливе ПЗ постійно з'являються. Оновлення дозволяють антивірусу розпізнавати нові загрози.

- Сповіщення користувача: Якщо антивірус виявить загрозу або здійснить дії для її блокування, він може сповістити користувача про це через сповіщення або попередження.

2.6.6 Журнали подій, моніторинг та системи SIEM

Можливо, найбільш важливими заходами забезпечення безпеки бізнесу є виявлення подій та коригування недоліків. Відправною точкою для цього є реєстрація подій. Фактично всі мережеві системи чи системи, підключені до мережі, мають генерувати логи (журнали подій). Що саме реєструвати залежить від бізнес-цілей. Реєструвати можна спроби входу в систему, потоки трафіку, пакети, дії або навіть кожне натискання клавіші користувачем. При виборі подій для логу враховується рівень ризиків, критичність ресурсів та вразливість систем компанії.

Системи та пристрої, які повинні генерувати логи

Мережеві пристрої та системи:

- маршрутизатори та комутатори;
- IDS та IPS;
- міжмережеві екрани.

Підключені до мережі пристрої та системи:

- сервери;
- ноутбуки;
- камери;
- ПК та мобільні телефони;
- бази даних;
- усі пристрої Інтернету речей (IoT).

У результаті записується безліч подій. Щоб розібратися у всіх цих даних, необхідно надсилати логи, які є даними контролю безпеки, наприклад, на syslog-сервер в центральній локації. Коли дані надходять на syslog-сервер, їх аналізує SIEM (Security Information Event Manager). SIEM – це інструмент, який корелює та

аналізує події всіх систем, виявляючи індекси компрометації (IoC). Наявність IoC не завжди є доказом того, що підозрілі події мали місце, тому аналіз мають завершити спеціалісти. Які дії слід робити далі, визначають фахівці SOC та команд з реагування на інциденти.

2.6.7. EDR/XDR системи

EDR та XDR – це ефективні інструменти для захисту корпоративних інформаційних ресурсів від постійно зростаючих кіберзагроз. Обираючи між ними, компанії повинні враховувати свої потреби, масштаб і складність інфраструктури для максимальної ефективності виявлення та реагування на загрози. EDR – це технологія, спрямована на захист кінцевих точок в мережі. Вона виявляє та реагує на аномальну активність, шкідливі програми та інші загрози, що можуть впливати на комп'ютери та сервери в корпоративному середовищі. EDR використовує аналіз поведінки, сигнатури та інші методи для ефективного виявлення та блокування загроз. XDR піднімає концепцію EDR на новий рівень, розширюючи область виявлення на всю мережу та інші важливі компоненти інфраструктури. XDR об'єднує дані від різних джерел, таких як ендпойнти, файерволи, електронні пошти та інші, для комплексного аналізу. Це забезпечує більший контекст та здатність виявлення складних загроз.

Основні функції EDR та XDR:

- Виявлення загроз:
- EDR: Виявлення загроз на рівні кінцевих точок, аналізуючи поведінку процесів та дій користувачів.
- XDR: Комплексне виявлення загроз на різних рівнях інфраструктури, координуючи дані з різних джерел.
- Реагування на інциденти:
- EDR: Локалізація та ізоляція загроз на конкретній кінцевій точці.
- XDR: Реагування на інциденти на рівні всієї мережі, забезпечуючи швидкий відгук та запобігаючи розповсюдженню загроз.

- Переваги використання EDR та XDR:
- EDR: Фокус на деталях та подробицях подій на конкретній кінцевій точці.
- XDR: Широкий контекст та аналіз великої кількості данних з різних джерел.
- Інтеграція:
- EDR: Інтеграція з іншими системами безпеки на рівні кінцевих точок.
- XDR: Інтеграція з різними елементами мережі та безпековими рішеннями для спільного аналізу.

2.7 Висновки до розділу

Було розглянуто актуальні загрози та інциденти в кібербезпеці. В тому числі їх вплив на системи. Також проведений аналіз загроз за аспектами: збору інформації, оцінки загроз, управління ризиками, виявлення та реагування на інциденти, збору та аналізу інформації про інцидент, звітності та аналізу.

Згадано про MITRE ATT&CK - світову базу знань про тактики та прийоми зловмисників, заснована на реальних спостереженнях, і про CVE (Common Vulnerabilities and Exposures) - список відомих вразливостей та дефектів безпеки, створений компанією MITRE і взятий за стандарт.

Особлива увага приділена кібератакам зі сторони Росії, починаючи з 24 лютого 2022 року. Зазначені відомі угруповання кіберзлочинців, які мають безпосереднє відношення до Росії, програмні продукти та тактики використані з диструкційними цілями на мережу всього українського сегменту.

Найважливішим висновком цьогорічних тенденцій є те, що зловмисники все частіше використовують зловмисне програмне забезпечення для виконання латерального руху. Латеральний рух — це тактика, яку зловмисники використовують для переходу від однієї скомпрометованої системи в мережі до

іншої, допомагаючи їм досягати своїх цілей. На основі звіту від Picus Labs створений список найпоширеніших методів ATT&CK із зазначеними техніками, визначені у 2022 році.

Подальший аналіз, моніторинг та безпеку від шкідливого програмного забезпечення та стороннього впливу на АС та корпоративні мережі визначають антивірусні програми, хмарні платформи для інтеграції безпеки з існуючою інфраструктурою, SIEM системи, системи IDS/IPS, системи EDR/XDR. Все зазначене буде розглядатися в наступному розділі.

Розділ 3. СТВОРЕННЯ МОДУЛЮ МОНІТОРИНГУ СИСТЕМАМИ SIEM ТА XDR

3.1 Алгоритм роботи модулю моніторингу

Алгоритм роботи модуля зображено на рис 3.1 та також в додатку А

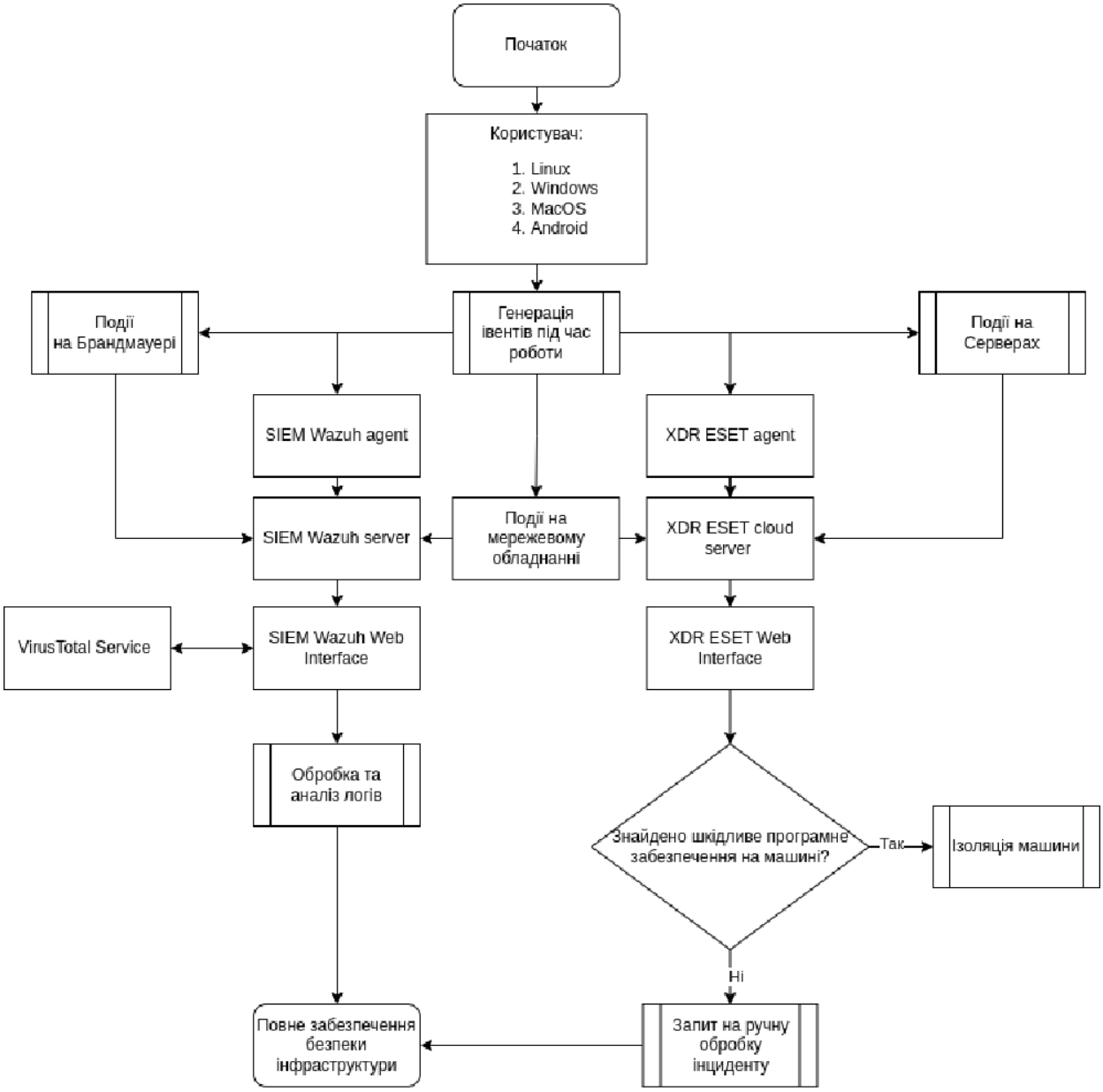


Рис. 3.1. Алгоритм роботи модуля моніторингу

Візуальне представлення модулю для моніторингу та захисту інфраструктури системами SIEM та XDR зображено на рис 3.2

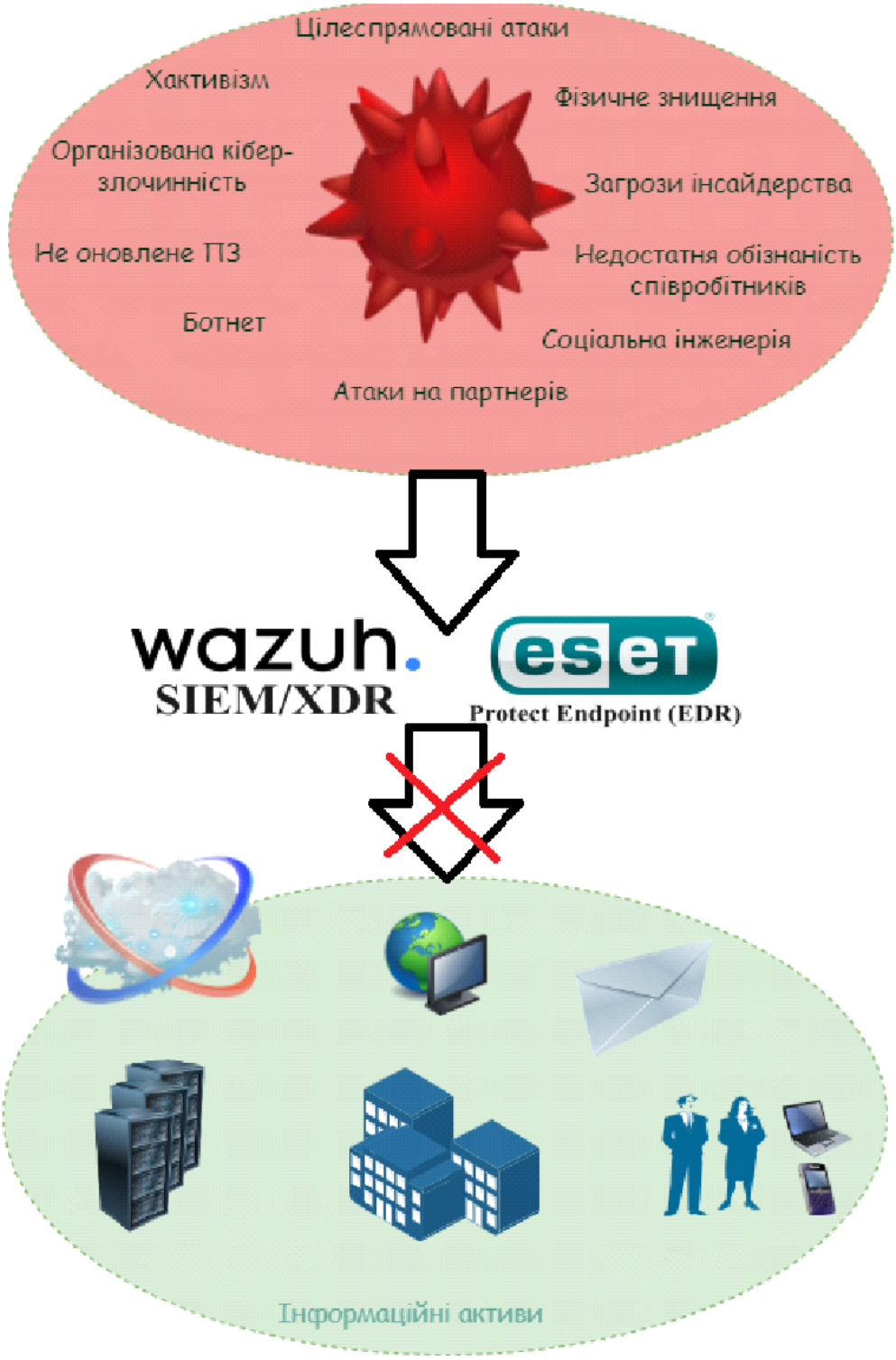


Рис 3.2 Модуль для моніторингу та захисту інфраструктури системами SIEM та XDR

3.2 Створення модулю моніторингу

Для створення даного модулю моніторингу було використано дві системи для забезпечення безпеки:

- SIEM/XDR Wazuh
- EDR ESET

3.2.1 SIEM/XDR Wazuh

Wazuh — це безкоштовна платформа безпеки з відкритим кодом, яка об’єднує можливості XDR і SIEM. Він захищає робочі навантаження в локальних, віртуалізованих, контейнерних і хмарних середовищах.

Wazuh допомагає організаціям і окремим особам захистити свої дані від загроз безпеки. Він широко використовується тисячами організацій по всьому світу, від малих до великих підприємств.

Функціонал Wazuh:

- *Аналітика безпекових рішень*
- *Виявлення вторгнень*
- *Аналіз даних журналів*
- *Моніторинг цілісності файлів*
- *Виявлення вразливостей*
- *Оцінка конфігурації*
- *Реагування на інцидент*
- *Відповідність нормативним вимогам*
- *Хмарна безпека*
- *Безпека контейнерів*

В якості системи SIEM/XDR була вибрана Wazuh, оскільки Wazuh пропонує кілька переваг як платформа XDR з відкритим кодом. Він налаштовується та може бути змінений відповідно до конкретних потреб, надаючи більшу гнучкість і контроль над вашим середовищем. Він має велику спільноту користувачів і

розробників, які надають підтримку та експертизу. Крім того, він інтегрується з широким спектром рішень безпеки, що дозволяє створити комплексну екосистему безпеки.

Wazuh розширює свої можливості виявлення загроз, інтегруючи рішення сторонніх розробників і об'єднуючи телеметрію з різних джерел для консолідації даних журналу в реальному часі. Він отримує телеметрію через системний журнал або API від сторонніх додатків, пристроїв і робочих навантажень, як-от хмарних провайдерів і постачальників SaaS.

Тобто у Wazuh немає жорсткої прив'язки до своєї інфраструктури. Правила та патерни виявлення шкідливого програмного забезпечення чи підозрілого мережевого трафіку можуть повністю змінюватись залежно від рішень користувача та редагуватися ним.

Основними модулями моніторингу в системі Wazuh являються рис. 3.2:

Security Events (Події безпеки): перегляд сповіщень безпеки, визначаючи проблеми та загрози у вашому середовищі. передбачає перевірку та отримання цінної інформації з файлів журналів, створених різними системами, програмами чи пристроями. Ці журнали містять записи подій, які надають корисну інформацію для усунення несправностей, аналізу та моніторингу безпеки та оптимізації продуктивності. Аналіз даних журналу є важливою практикою, яка сприяє безпечній, ефективній і надійній IT-екосистемі. Wazuh збирає, аналізує та зберігає журнали з кінцевих точок, мережевих пристроїв і програм. Агент Wazuh, який працює на контрольованій кінцевій точці, збирає та пересилає журнали системи та програм на сервер Wazuh для аналізу. Крім того, ви можете надсилати повідомлення журналу на сервер Wazuh через системний журнал або інтеграцію стороннього API

Integrity monitoring (Контроль цілісності): передбачає моніторинг цілісності файлів і каталогів для виявлення та попередження про події додавання, модифікації або видалення файлів. FIM забезпечує важливий рівень захисту

конфіденційних файлів і даних шляхом регулярного сканування та перевірки цілісності цих активів. Він визначає зміни файлів, які можуть свідчити про кібератаку, і генерує сповіщення для подальшого дослідження та виправлення, якщо це необхідно. Модуль моніторингу цілісності файлів Wazuh з відкритим кодом відстежує дії, що виконуються в контрольованих каталогах або файлах, щоб отримати розширену інформацію про створення, зміну та видалення файлів. Коли файл змінюється, Wazuh порівнює його контрольну суму з попередньо обчисленою базовою лінією та запускає сповіщення, якщо виявляє невідповідність. Модуль з відкритим вихідним кодом виконує моніторинг у реальному часі та планове сканування залежно від рівня чутливості файлів, що контролюються.

System auditing (Системний аудит): аудит поведінки користувачів, моніторинг виконання команд і сповіщення про доступ до критичних файлів. Функція who-data дозволяє модулю FIM отримувати інформацію про те, хто вносив зміни у контрольований файл. Ця інформація містить користувача, який вніс зміни до відстежуваних файлів, і назву програми або використовуваний процес. Функція моніторингу who-data використовує підсистему Linux Audit для отримання інформації про те, хто вносить зміни в контрольований каталог. Ці зміни створюють події аудиту. Модуль FIM обробляє події аудиту та повідомляє про них на сервер Wazuh. Ця функція розширює атрибут реального часу, замінюючи його. Це означає, що whodata здійснює моніторинг у реальному часі з додаванням інформації who-data.

Vulnerabilities (Вразливості): Модуль Wazuh Vulnerability Detector допомагає користувачам виявляти вразливості в операційній системі та програмах, встановлених на контрольованих кінцевих точках Щоб виявити вразливості, агенти Wazuh збирають список встановлених програм із контрольованих кінцевих точок і періодично надсилають його на сервер Wazuh. Цей список зберігається в локальних базах даних SQLite на сервері Wazuh. Крім того, сервер Wazuh створює

глобальну базу даних вразливостей із загальнодоступних репозиторіїв CVE. Він використовує цю базу даних для перехресної кореляції цієї інформації з даними інвентаризації програми агента, Детектор вразливостей генерує сповіщення під час базового сканування для кожної виявленої вразливості. Детектор вразливостей також генерує сповіщення, коли виявляє нові вразливості або коли користувачі усувають виявлені вразливості.

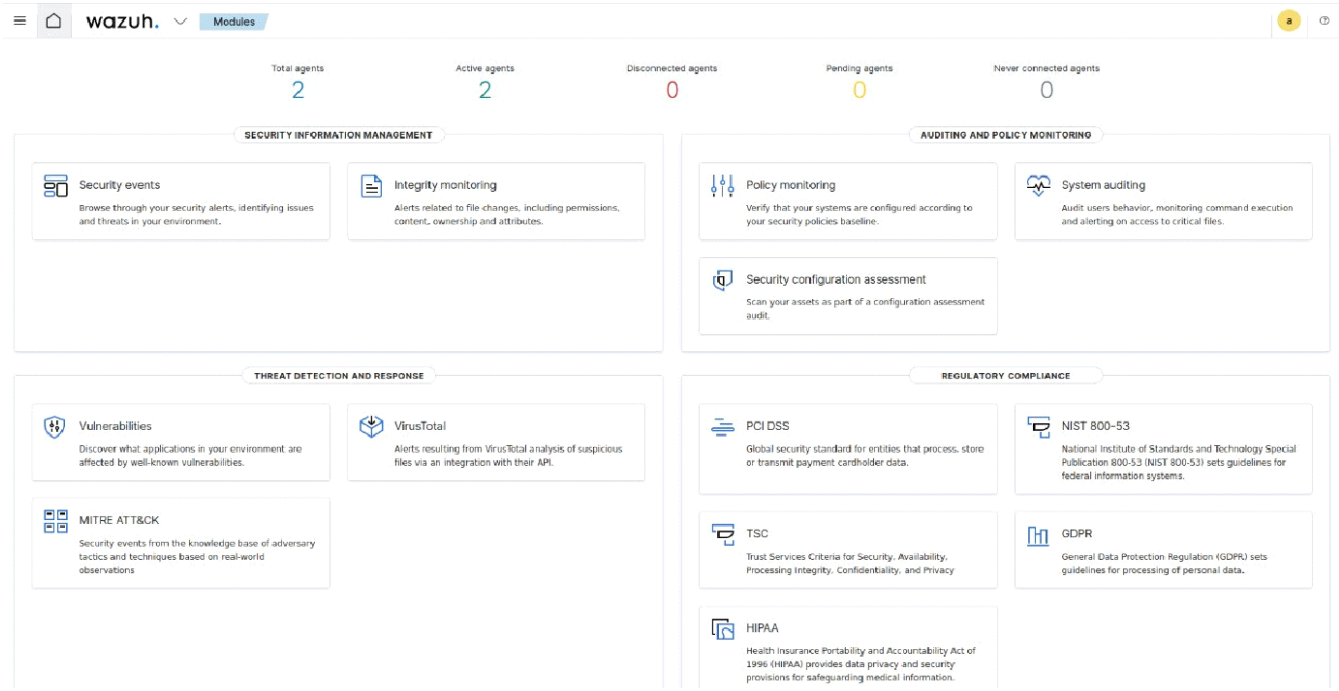


Рис. 3.3 Менеджмент інформацією безпеки

3.2.1.1 Security Events (Події безпеки)

На рис. 3.4 та рис 3.5. зображено дві панелі модуля Security events:

- Dashboard: дашборди які базуються на подіях інформаційної безпеки
    - Events: логи з кінцевих пристроїв з рівнем ризику за яким визначаються подальші автоматизовані дії стосовно цього івенту:
        - виконання кастомного скрипта
        - видалення файлу
        - відправка сповіщення про небезпеку на пошту

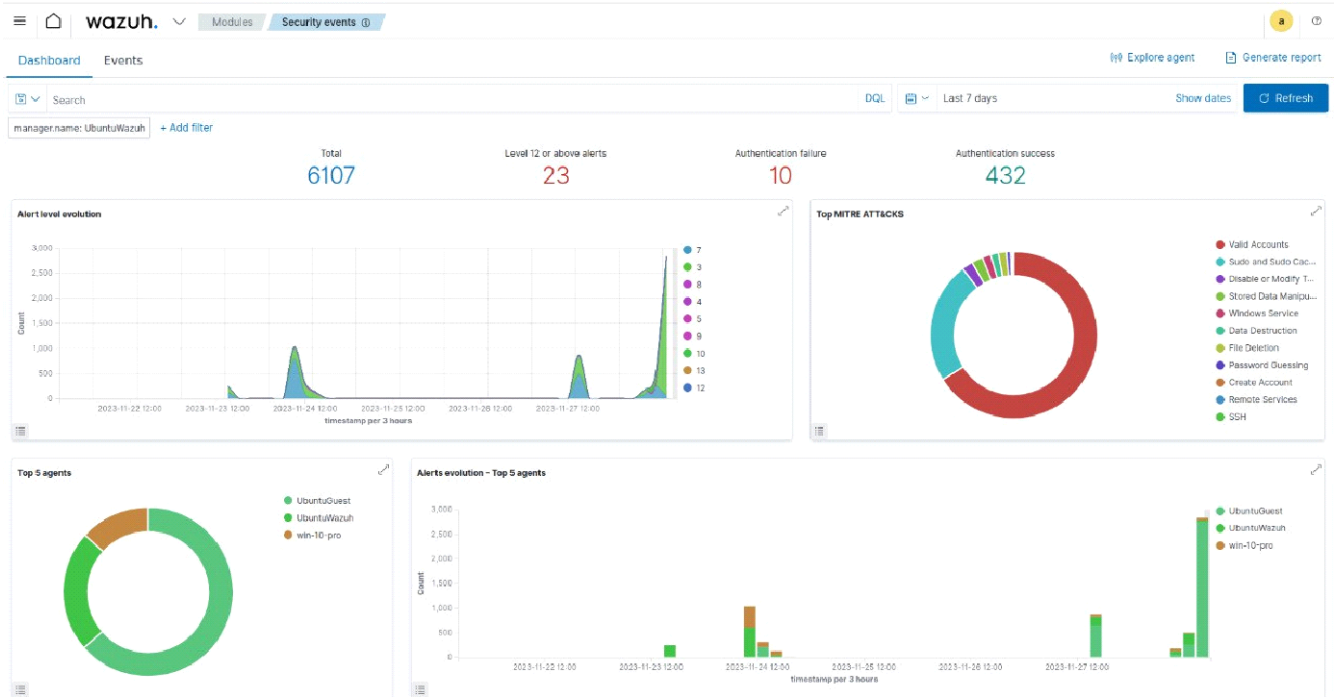


Рис 3.4 Панель “Dashboards” Security events

Time	agent.name	rule.description	rule.level	rule.id
Nov 28, 2023 @ 22:49:33.323	Win10Pro	VirusTotal: Alert - No records in VirusTotal database	3	87103
Nov 28, 2023 @ 22:49:32.459	Win10Pro	VirusTotal: Alert - No records in VirusTotal database	3	87103
Nov 28, 2023 @ 22:49:30.763	Win10Pro	VirusTotal: Alert - No records in VirusTotal database	3	87103
Nov 28, 2023 @ 22:49:29.514	Win10Pro	VirusTotal: Alert - No records in VirusTotal database	3	87103
Nov 28, 2023 @ 22:49:27.854	Win10Pro	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:49:27.807	Win10Pro	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:49:27.792	Win10Pro	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:49:27.792	Win10Pro	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:49:27.792	Win10Pro	Registry Key Integrity Checksum Changed	5	594
Nov 28, 2023 @ 22:49:27.763	Win10Pro	Registry Key Integrity Checksum Changed	5	594
Nov 28, 2023 @ 22:49:04.085	Maks-Ubuntu	Host-based anomaly detection event (rootcheck).	7	510
Nov 28, 2023 @ 22:49:04.074	Maks-Ubuntu	Host-based anomaly detection event (rootcheck).	7	510
Nov 28, 2023 @ 22:48:21.172	Win10Pro	Windows logon success.	3	60106
Nov 28, 2023 @ 22:48:21.170	Win10Pro	Sysmon - Suspicious Process - svchost.exe	12	61618
Nov 28, 2023 @ 22:46:10.328	Maks-Ubuntu	Host-based anomaly detection event (rootcheck).	7	510
Nov 28, 2023 @ 22:46:10.317	Maks-Ubuntu	Host-based anomaly detection event (rootcheck).	7	510
Nov 28, 2023 @ 22:44:44.786	Win10Pro	VirusTotal: Alert - No records in VirusTotal database	3	87103
Nov 28, 2023 @ 22:44:43.901	Win10Pro	VirusTotal: Alert - No records in VirusTotal database	3	87103
Nov 28, 2023 @ 22:44:43.022	Win10Pro	VirusTotal: Alert - No records in VirusTotal database	3	87103

Рис 3.5 Панель “Events” Security events

3.2.1.2 Security Events (Події безпеки) Integrity Monitoring

На рис. 3.6, рис. 3.7 та рис. 3.8 зображено три панелі модуля Integrity monitoring:

- Inventory: у розділі «Інвентаризація» відображається список усіх файлів, які проіндексував модуль FIM. Кожен файл містить інформацію про введення, зокрема назву файлу, дату останньої зміни, користувача, ідентифікатор користувача, групу та розмір файлу.

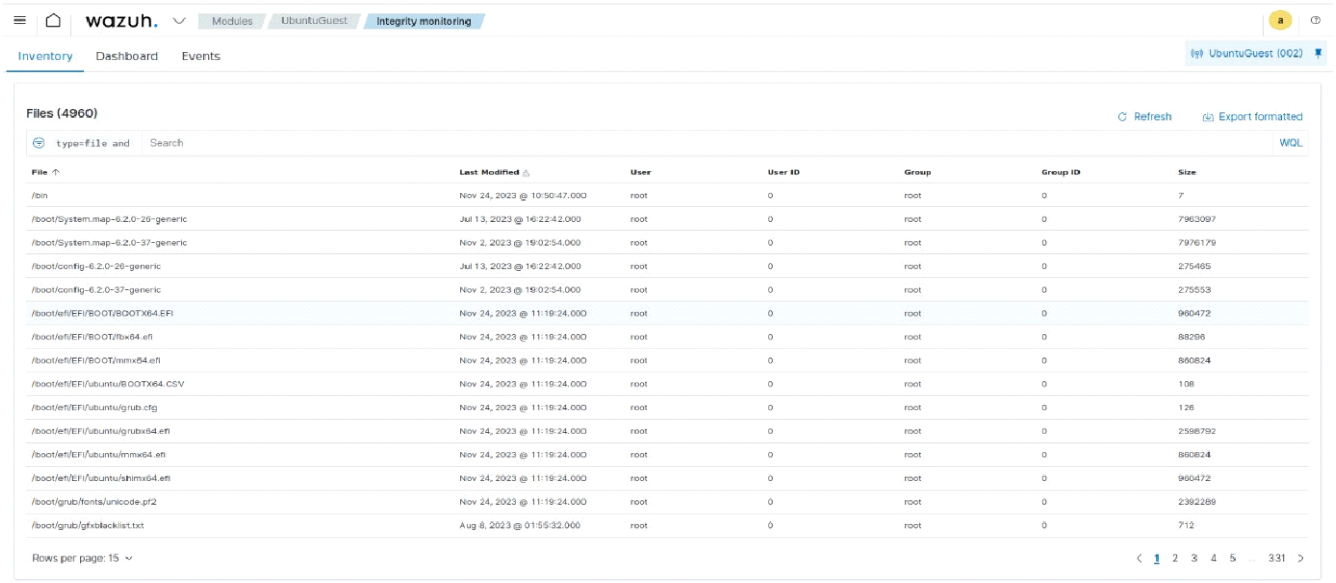


Рис 3.6 Панель “Inventory” Integrity monitoring

- Dashboard: розділ «Інформаційна панель» містить огляд подій, ініційованих модулем FIM для всіх контрольованих кінцевих точок. Ви також можете оптимізувати його, щоб відображати події для вибраної контрольованої кінцевої точки.

- Events: у розділі «Події» показано сповіщення, ініційовані модулем FIM. Він відображає такі деталі, як ім’я агента, шлях до відстежуваного файлу, тип події FIM, опис попередження та рівень правила для кожного попередження.

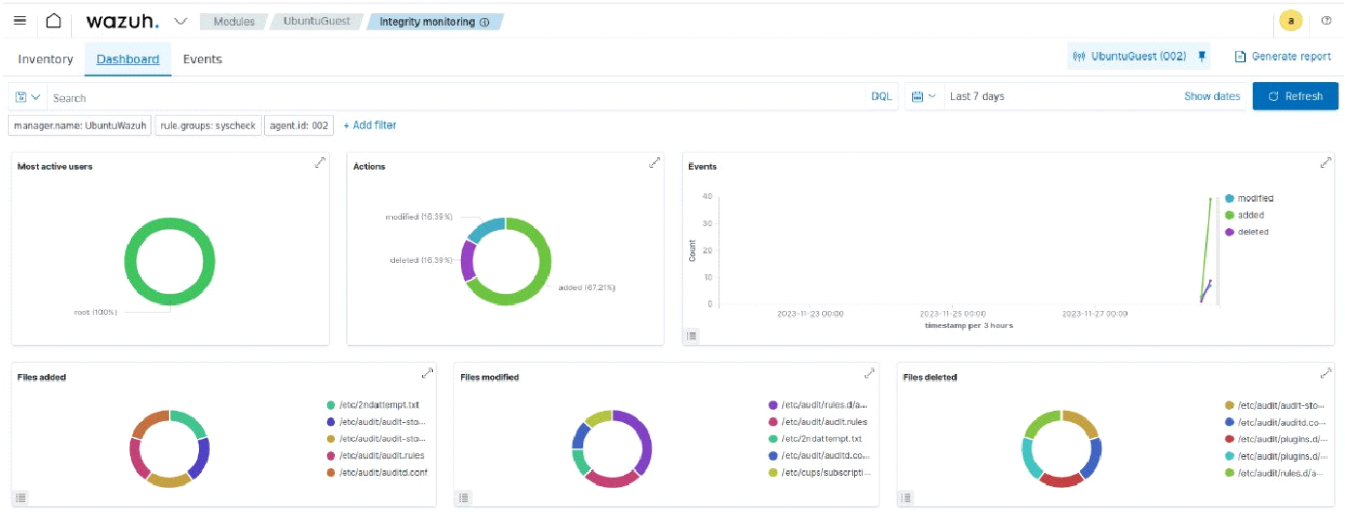


Рис 3.7 Панель “Dashboards” Integrity monitoring

Time	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Nov 28, 2023 @ 22:49:27.854	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:49:27.807	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:49:27.792	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime	modified	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:49:27.792	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:49:27.792	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Key Integrity Checksum Changed	5	594
Nov 28, 2023 @ 22:49:27.763	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime	modified	Registry Key Integrity Checksum Changed	5	594
Nov 28, 2023 @ 22:44:39.226	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:44:39.210	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:44:39.194	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime	modified	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:44:39.194	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Key Integrity Checksum Changed	5	594
Nov 28, 2023 @ 22:44:39.194	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:44:39.151	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime	modified	Registry Key Integrity Checksum Changed	5	594
Nov 28, 2023 @ 22:39:51.063	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750
Nov 28, 2023 @ 22:39:51.019	Win10Pro	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750

Рис 3.8 Панель “Events” Integrity monitoring

3.2.1.3 System auditing (Системний аудит)

На рис. 3.9 та рис. 3.10 зображено дві панелі модуля Integrity monitoring:

- Dashboard: розділ «Інформаційна панель» містить огляд подій, ініційованих модулем FIM для всіх контрольованих кінцевих точок. Підсистема

аудиту Linux для отримання інформації про те, хто вносить зміни в контрольований каталог. Після чого система створює діаграми та графіки з візуалізацією подій.

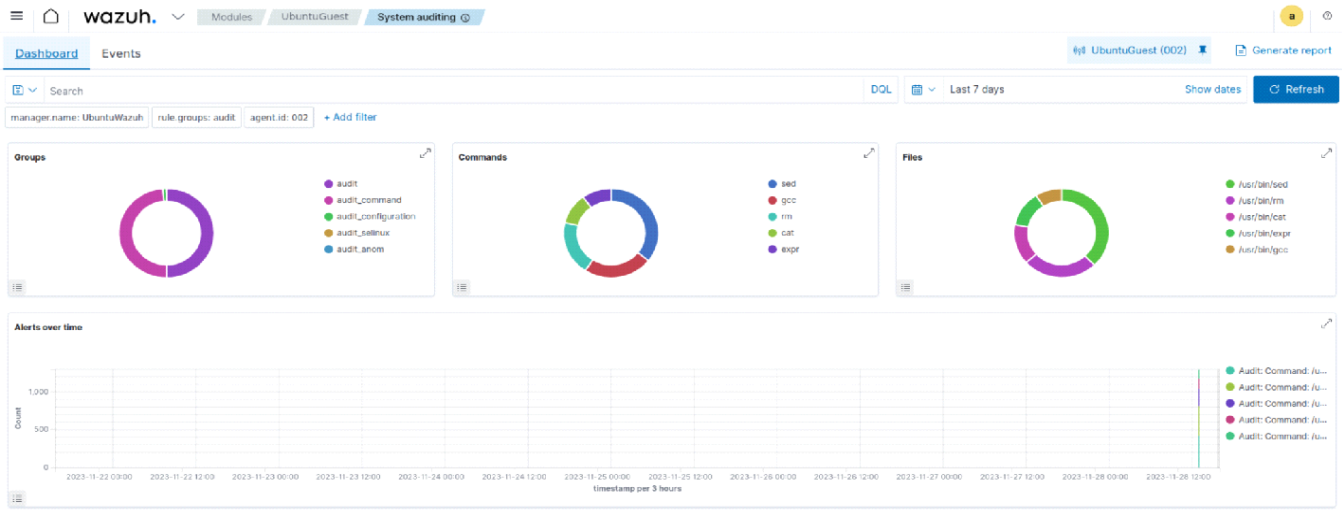


Рис 3.9 Панель “Dashboard” System auditing

- Events: у розділі «Події» показано сповіщення, ініційовані модулем FIM. Підсистема аудиту Linux для отримання інформації про те, хто вносить зміни в контрольований каталог. Ці зміни створюють події аудиту.

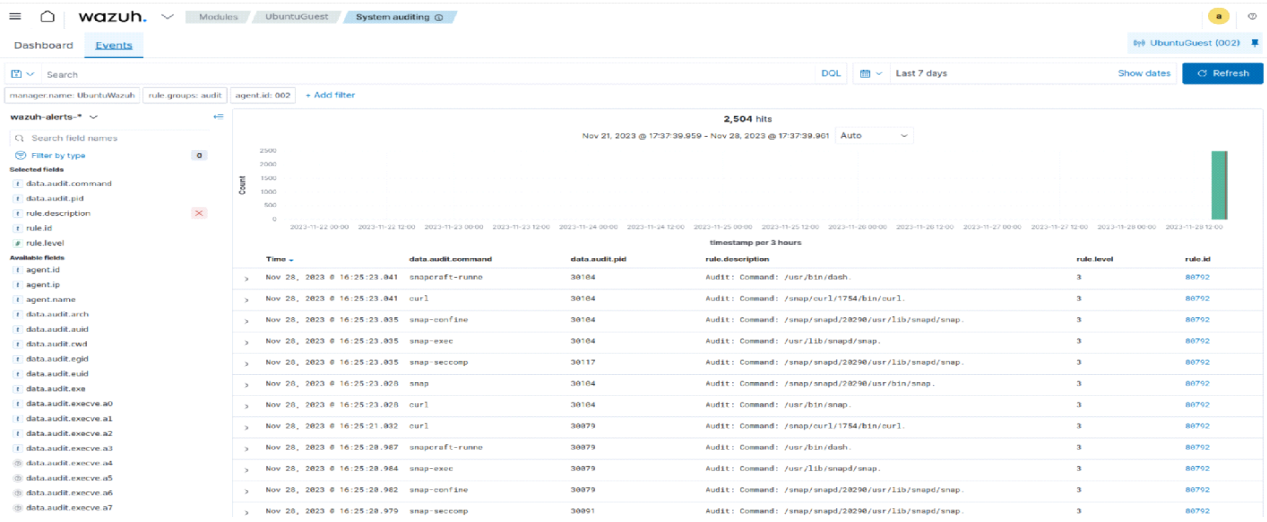


Рис 3.10 Панель “Events” System auditing

3.2.1.4 Vulnerabilities (Вразливості)

На рис. 3.11 та рис. 3.12 зображено дві панелі модуля Integrity monitoring:

- Dashboard: розділ «Інформаційна панель» містить огляд вразливостей, для вибраної контрольованої кінцевої точки.

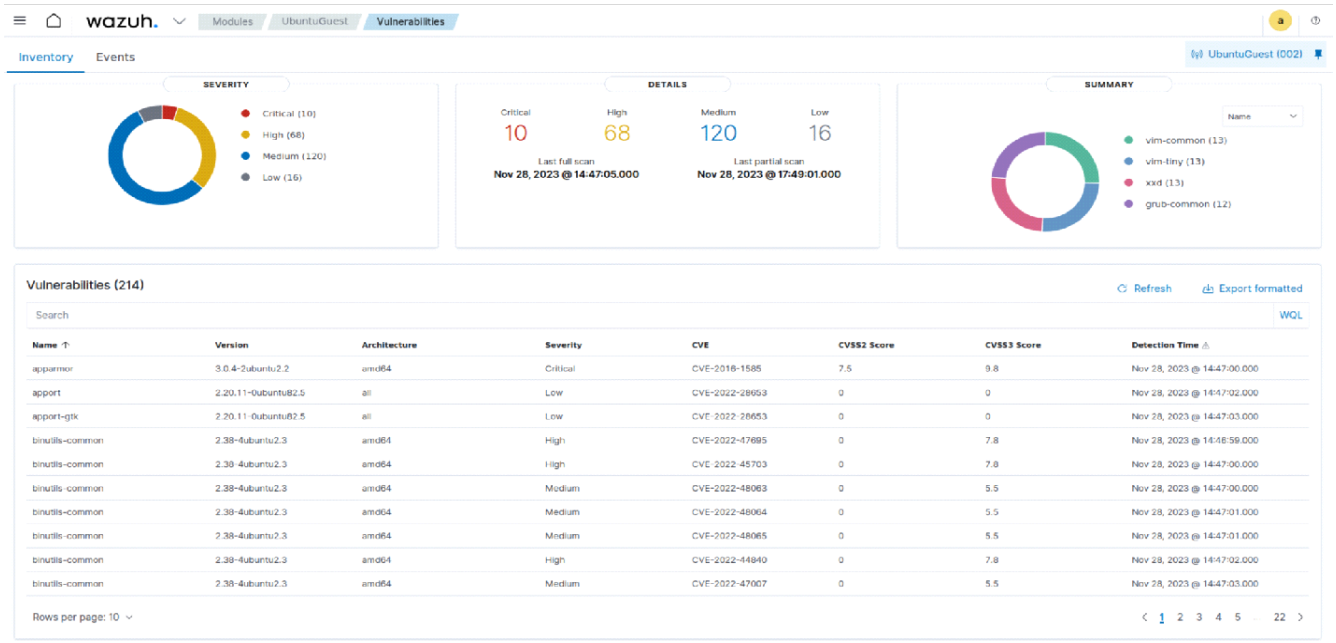


Рис 3.11 Панель “Dashboard” Vulnerablilities

- Events: у розділі «Події» показано сповіщення, які були ініційовані виявленням вразливостей на кінцевій машині:

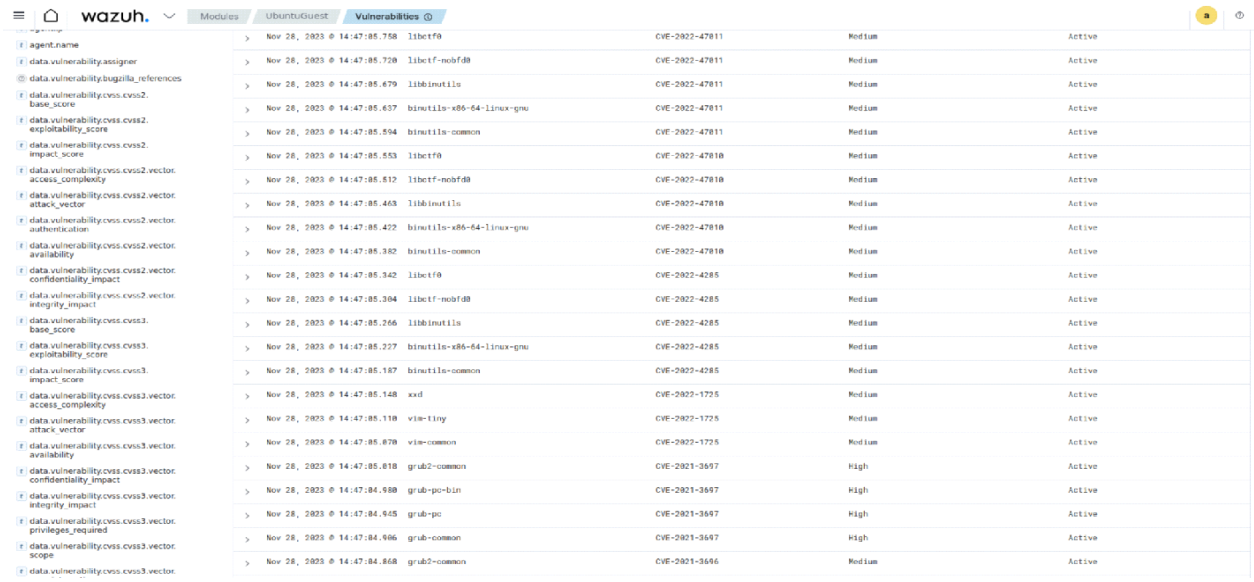


Рис 3.12 Панель “Events” Vulnerablilities

3.2.2 Інтерація сервісу VirusTotal в SIEM систему Wazuh

Алогритм аналізу файлу за допомогою інтегрованого сервісу VirusTotal зображено на рис. 3.13

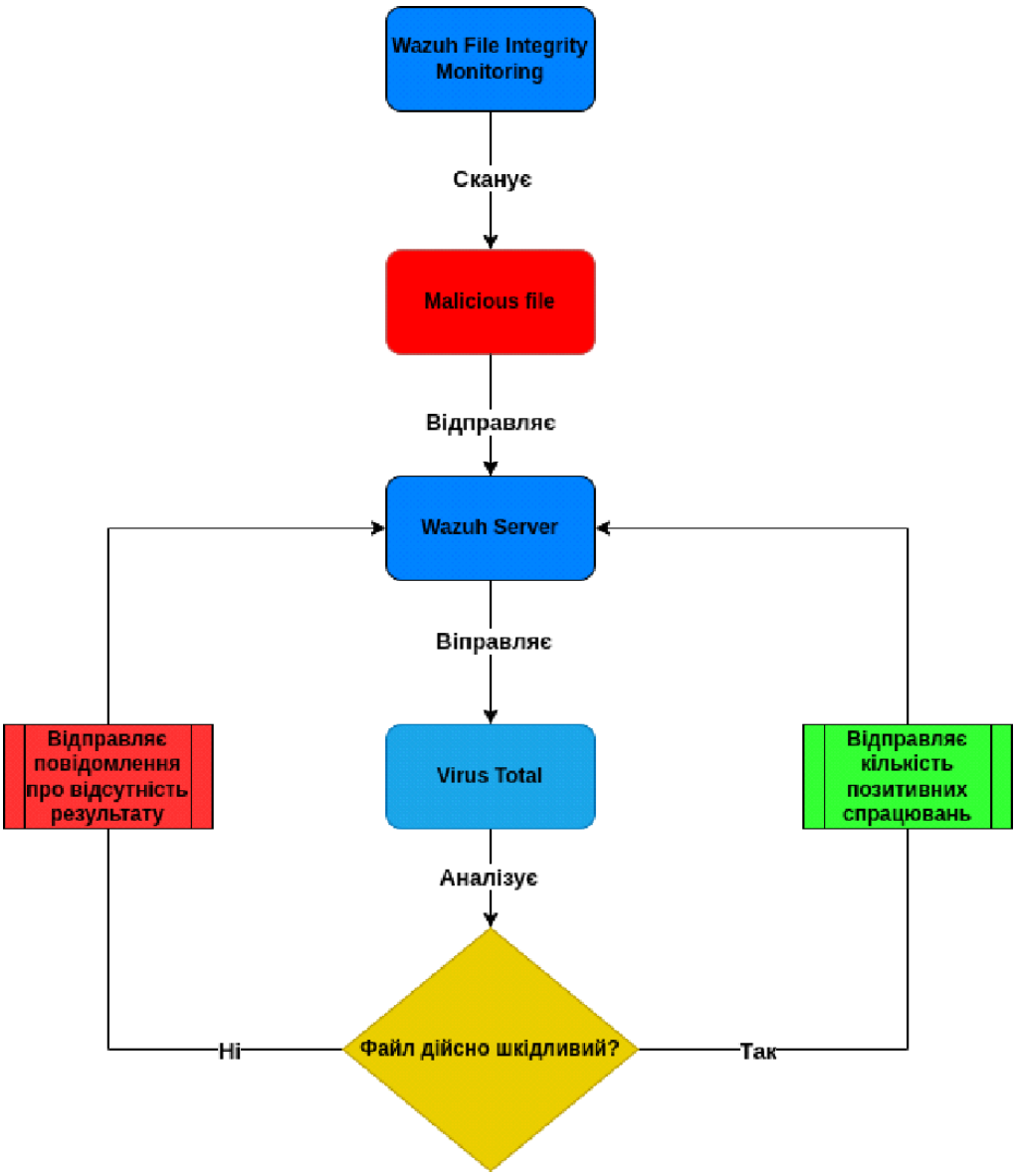


Рис 3.13 Алгоритм сканування за допомогою інтеграції VirusoTotal

В якості новизни було інтегровано сервіс VirusTotal до системи Wazuh. Wazuh виявляє шкідливі файли за допомогою інтеграції з VirusTotal, потужною платформою, що об’єднує кілька антивірусних продуктів і систему онлайн-сканування. Поєднання цього інструменту з модулем контролю цілісності файлів забезпечує ефективний спосіб перевірки контрольованих файлів на наявність шкідливого вмісту.

VirusTotal — це онлайн-служба, яка аналізує файли та URL-адреси для виявлення вірусів, хробаків, троянів та іншого шкідливого вмісту за допомогою антивірусних механізмів і сканерів веб-сайтів.

VirusTotal — це безкоштовний сервіс із численними корисними функціями. Ми виділяємо наступне, що стосується нашої мети:

VirusTotal зберігає всі проведені аналізи, дозволяючи користувачам шукати хеші файлів. Надсилаючи хеш механізму VirusTotal, ви можете дізнатися, чи VirusTotal уже просканував цей конкретний файл, і ви можете проаналізувати його звіт.

VirusTotal також надає API, який дозволяє отримати доступ до інформації, згенерованої VirusTotal, без використання HTML-інтерфейсу веб-сайту. Цей API регулюється його умовами обслуговування, які ми коротко обговорюємо в наступному розділі.

Ця інтеграція використовує API VirusTotal для виявлення шкідливого вмісту у файлах і каталогах, які відстежуються за допомогою функції моніторингу цілісності файлів Wazuh. Ця інтеграція працює, як описано нижче.

Wazuh FIM шукає будь-які додавання, зміни або видалення файлів у контрольованих папках. Цей модуль зберігає хеш цих файлів і запускає сповіщення, коли виявляє будь-які зміни.

Якщо ввімкнено, Wazuh запускає інтеграцію VirusTotal, коли виникає сповіщення FIM. З цього сповіщення інтеграція витягує хеш-поле файлу.

Потім інтеграція робить запит HTTP POST до бази даних VirusTotal за допомогою VirusTotal API. Цей виклик надсилає хеш видобутого файлу для порівняння з інформацією в базі даних VirusTotal.

Інтеграція отримує відповідь JSON, яка є результатом запиту. Відповідь викликає одне з таких сповіщень Wazuh:

- Помилка: перевірте облікові дані.

- Помилка: досягнуто обмеження кількості запитів загальнодоступного API.
- Сповіщення: немає записів у базі даних VirusTotal.
- Сповіщення: позитивних результатів не знайдено.
- Попередження: X систем виявили цей файл. X — кількість антивірусних рішень.

Wazuh реєструє викликане сповіщення у файлі /var/ossec/logs/integration.log і зберігає його у файлі /var/ossec/logs/alerts.log разом із усіма іншими сповіщеннями.

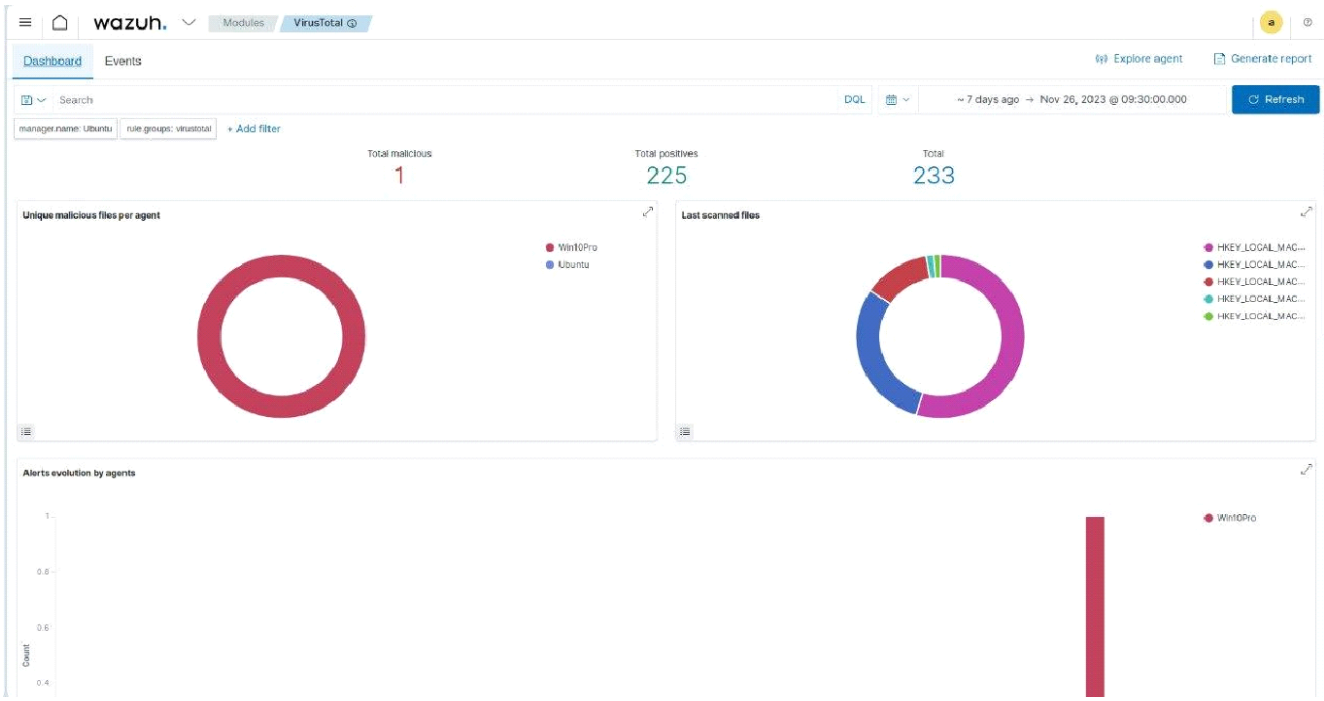


Рис 3.14 Панель “Dashboard” VirusTotal

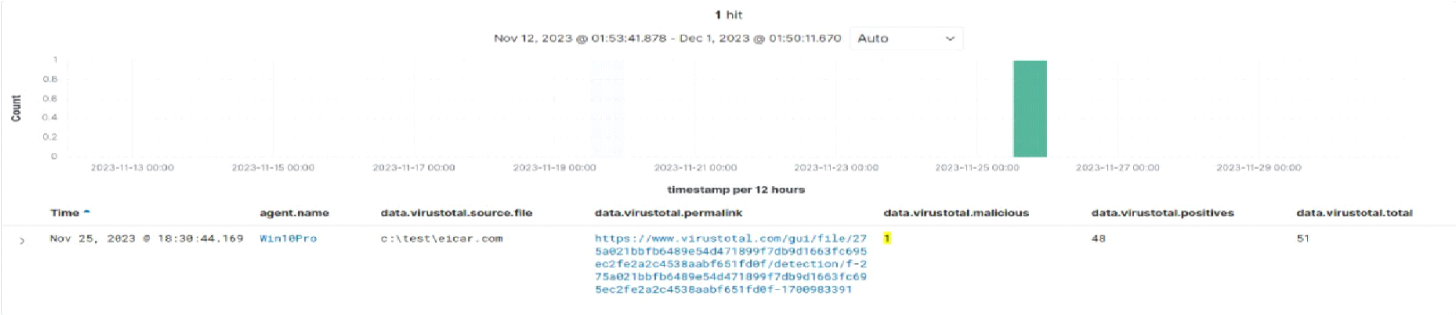


Рис 3.15 Панель “Events” VirusTotal

Рис 3.16 Рузультат спрацювання на виявлення шкідливого файлу

В якості зловмисного файлу для перевірки спрацювань виявлення шкідливих файлів був вибраний тестовий псевдо шкідливий файл Eicar.com (стандартний файл, який використовується для перевірки, чи працює антивірус). Як видно зі скріншота, файл був детектований SIEM системою. Wazuh File Integration Monitoring виявив наявність файлу в директорії, яка підлягає перевірці в режимі реального часу і відправив запит на перевірку хешу файлу на VirusTotal. Оскільки хеш файлу вже був проаналізований і в результаті зберігався в базі даних сервісу, то нам повернувся результат у вигляді кількості позитивних спрацювань антивірусних рішень. В даному випадку 48 з 51 антивірусних рішень визначили файл як зловмисний.

Скрипт налаштувань Wazuh Manager представлений в додатку Б.

3.2.3 EDR ESET

Рішення ESET для захисту кінцевих точок використовують багаторівневий підхід із використанням кількох технологій, працюючи разом із можливістю постійно балансувати продуктивність, виявлення та помилкові спрацьовування.

Продукти ESET Endpoint Protection підтримують усе ОС — Windows (включаючи Windows на ARM), macOS, Linux і Android. Всіма продукти захисту кінцевих

точок можна повністю керувати з однієї панелі; управління мобільними пристроями для iOS і Android також повністю вбудований.

Усі рішення ESET для захисту кінцевих точок керуються з єдиної консолі ESET PROTECT, яка може бути на базі хмари або локально, гарантуючи повний огляд вашої мережі.

Функції EDR ESET:

- *Управління з єдиної консолі*
- Усіма продуктами ESET для захисту робочих станцій, у тому числі мобільних пристроїв, можна управляти з єдиної хмарної або локальної консолі ESET PROTECT.
- *Блокування цілеспрямованих атак*
- Рішення ESET використовують інформацію про глобальне поширення загроз для визначення пріоритетів та ефективного блокування нових загроз, попереджаючи їх подальше розповсюдження у світі. Крім цього, можливість оновлення на основі хмарних технологій дозволяє швидко реагувати на виявлені об’єкти без необхідності чекати запланованого оновлення.
- *Захист від мережевих атак*
- Покращує виявлення відомих вразливостей на мережевому рівні.
- *Машинне навчання*
- Починаючи ще з 1997 року, усі продукти ESET для захисту робочих станцій використовують машинне навчання на додаток до усіх інших рівнів захисту. Зокрема, машинне навчання використовується у формі консолідованої вихідної та нейронної мереж. Для розширеного аналізу мережі існує спеціальний режим поглибленого машинного навчання, який працює навіть без підключення до Інтернету.
- *Захист від програм-вимагачів*
- Додатковий рівень захисту користувачів від програм-вимагачів. Технологія контролює та оцінює всі виконані програми на основі їхньої поведінки

та репутації, а також завдяки технології Intel® для виявлення загроз забезпечує покращене виявлення програм-вимагачів.

- *Сканер UEFI*
- ESET — перший постачальник рішень для Інтернет-безпеки, який доповнив власні продукти захистом інтерфейсу Unified Extensible Firmware Interface (UEFI). Сканер забезпечує захист середовища попереднього завантаження та перевіряє цілісність вбудованого програмного забезпечення. У разі виявлення будь-яких змін, сканер повідомляє про це користувачу.
- *Захист від експлойтів*
- Технологія, як правило, перевіряє додатки (браузери, програми для роботи з документами, поштові клієнти, Flash, Java та інші) і замість спрямування на конкретні ідентифікатори CVE фокусується на методах використання вразливостей. У разі виявлення загроза може бути відразу заблокована на робочій станції.
- *Запобігання атакам без використання файлів*
- Для захисту від атак без використання файлів рішення ESET для захисту робочих станцій виявляють додатки, які можуть несанкціоновано використовуватись зловмисниками. Тоді як спеціальні сканери постійно перевіряють пам’ять на наявність підозрілих об’єктів.
- *Захист веб-браузера*
- Цей спеціальний рівень захисту зосереджується на захисті браузера, який є основним інструментом для доступу до важливих даних усередині периметра Інтранет-мережі та у хмарі. Захищений браузер забезпечує розширений захист пам’яті для процесу браузера в поєднанні із захистом клавіатури, а також дозволяє адміністраторам додавати URL-адреси, які будуть захищені.
- *Захист від ботнетів*

- Забезпечує захист від загроз виду ботнет, запобігаючи тим самим розсилці спаму та здійснення мережевих атак з інфікованого комп'ютера. Блокує шкідливі зв’язки та повідомляє про це користувачу.
- *Захист від атак методом підбору паролів*

Виявляє та блокує автоматизовані атаки, які використовують методи підбору пароля для отримання доступу до вашої мережі.

- *Внутрішня пісочниця*
- Допомагає визначити реальну поведінку шкідливого програмного забезпечення, яку було замасковано.
- *Система запобігання вторгненням (HIPS)*
- Здійснює моніторинг активності системи та використовує заздалегідь визначений набір правил для розпізнавання і припинення підозрілої поведінки в системах.
- *Розширений сканер пам'яті*
- Унікальна технологія ESET відстежує поведінку шкідливого процесу та сканує його, як тільки він проявляє активність у пам’яті. Шкідливе програмне забезпечення без використання файлів не потребує постійних компонентів у файловій системі, які можна виявити стандартним методами. Тільки сканування пам'яті може успішно виявити та зупинити такі шкідливі атаки.

Керування кінцевими точками відбувається за допомогою фізично встановленого сервера ESET Protect, або у вигляді хмарного рішення ESET Protect Cloud. І так званих “агентів” ESET Endpoint Secuity”, які встановлюються на кінцеві точки для моніторингу і реагування на події в операційних системах. Особливістю агентів являється можливість обмеження для їх видалення за допомогою застосування паролю, накладеним адміністратором EDR системи. Тобто видалити агент з ПК у звичайного користувача операційної системи не вийде. В дипломній роботі в цілях ознайомлення було обрано ESET Protect Cloud.

3.2.3.1 Розбір інструментарію наданим головним меню Eset Protect Cloud

Розбір інструментарію наданим головним меню Eset Protect Cloud зображеного на рис 3.17

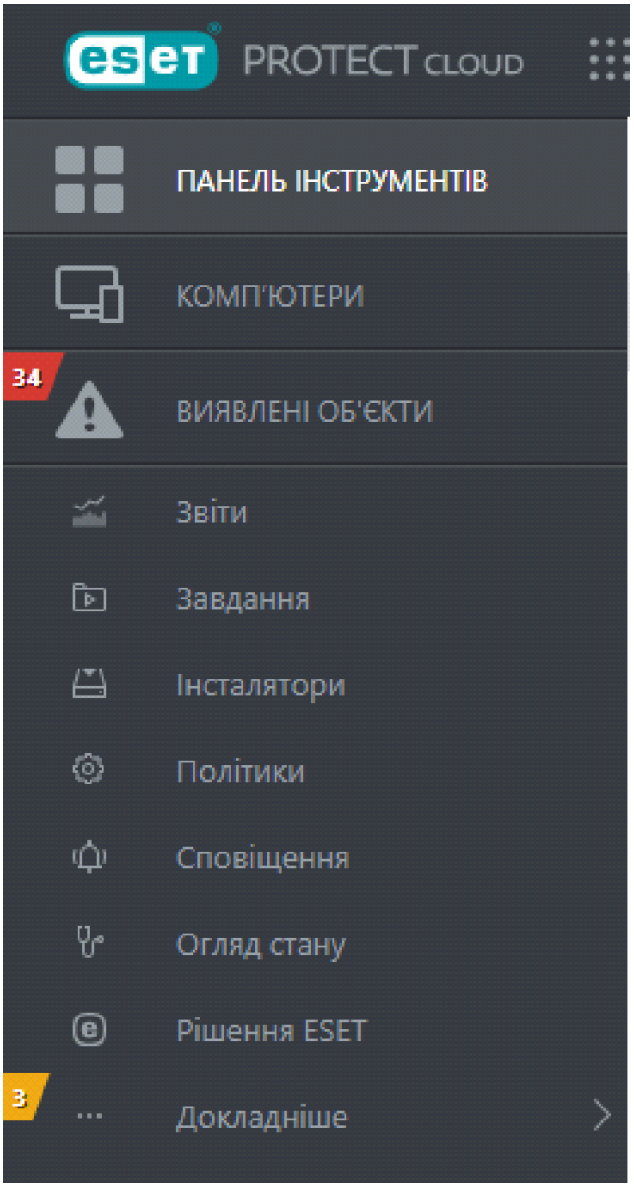


Рис 3.17 Панель інструментів

- *Панель інструментів***.** Сторінка, яка за замовчуванням відображається після першого входу у веб-консоль ESET PROTECT Cloud. Тут відображаються попередньо налаштовані звіти про мережу у вигляді графіків та діаграм.

- *Комп'ютери.* Тут за групами відображаються всі клієнтські пристрої, додані до ESET PROTECT Cloud. Кожен пристрій відноситься до окремої статичної групи.
- *Виявлені об'єкти.* У розділі можна переглянути об'єкти, виявлені на керованих пристроях.
- *Звіти.* За допомогою звітів ви отримуєте доступ до бази даних і можливість відфільтрувати її дані в зручний спосіб. Вікно звітів містить дві таблиці.
- *Завдання.* Завдання можна використовувати для керування ESET PROTECT Cloud, клієнтськими комп'ютерами та інстальованими на них продуктами ESET. Завдання допомагають автоматизувати виконання поширених процесів
- *Інсталятори.* У цьому розділі показано, як створити інсталяційні пакети для розгортання агента ESET Management на клієнтських комп'ютерах. Пакети інсталяції зберігаються у ESET PROTECT Cloud веб-консолі, і ви можете за потреби повторно завантажувати їх.
- *Політики.* Політики використовуються для застосування певних конфігурацій до продуктів ESET, які виконуються на клієнтських комп'ютерах. Це дозволяє не налаштовувати продукт ESET на кожному клієнтському комп'ютері окремо. Політики можуть бути спрямовані на окремі комп'ютери або на декілька груп (статичних і динамічних).
- *Сповіщення.* Сповіщення мають важливе значення для відстеження загального стану вашої мережі. Коли відбувається нова подія (згідно з конфігурацією сповіщень), ви отримуєте сповіщення на електронну пошту, що дає змогу вжити відповідні заходи.
- *Огляд стану.* ESET PROTECT Cloud періодично проводить діагностичні перевірки. У розділі Огляд стану можна переглянути статистику використання та загальний статус ESET PROTECT Cloud.

- *Рішення ESET.* Цей розділ дає змогу виконати спрощене розгортання таких продуктів: ESET LiveGuard AdvancedESET; Full Disk Encryption

3.2.3.2 Панель інструментів

На рис. 3.18, рис. 3.19, рис. 3.20 та рис. 3.21 зображено основні панелі візуалізацій подій в мережі:

- *Огляд стану.* На ній відображається загальна інформація про вашу мережу:
- *Статус пристроїв* – відображає кількість керованих пристроїв на відповідних вкладках на основі інстальованого типу продукту для захисту. Якщо в певній групі не розгорнуто жоден продукт для захисту, на вкладці відобразиться запит на розгортання відповідного пакета інсталяції.
- *Статус підключення* – відображає список останніх підключень керованих пристроїв.
- *Статус підключення* – відображає список останніх підключень керованих пристроїв.
- *Статус керування* – відображає кількість *керованих та захищених* (клієнтські пристрої з встановленим агентом ESET та продуктом для захисту), *керованих* (клієнтські пристрої з агентом), *некерованих* (клієнтські пристрої у вашій мережі без інстальованого агента, про які відомо ESET PROTECT Cloud) та *неавторизованих* (виявлені Rogue Detection Sensor клієнтські пристроїв, про які невідомо ESET PROTECT Cloud) пристроїв.

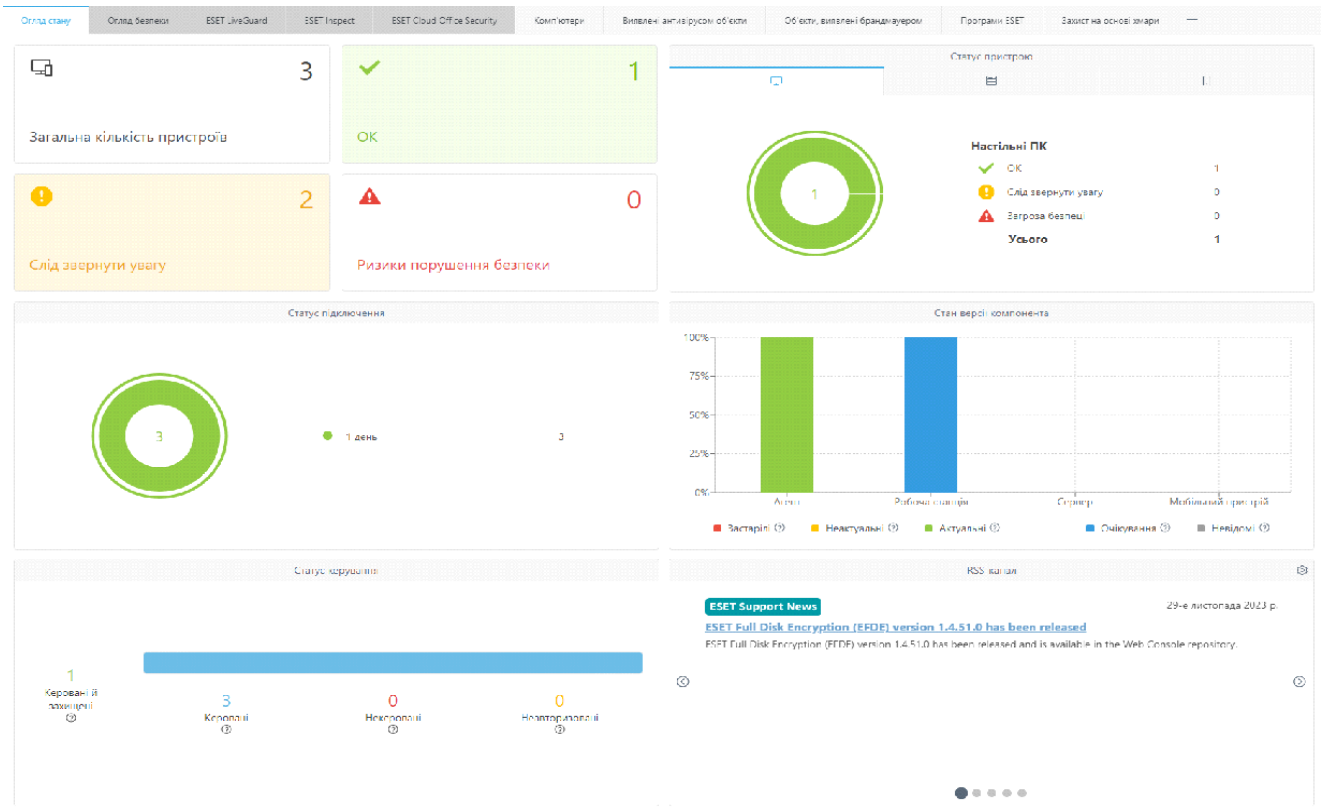


Рис 3.18 Огляд стану

- Огляд безпеки. На цій панелі інструментів відображаються основні відомості про необроблені виявлені об’єкти за останні сім днів, зокрема рівень їхньої серйозності, метод виявлення, статус обробки, а також 10 комп’ютерів/користувачів із найбільшою кількістю виявлених об’єктів.

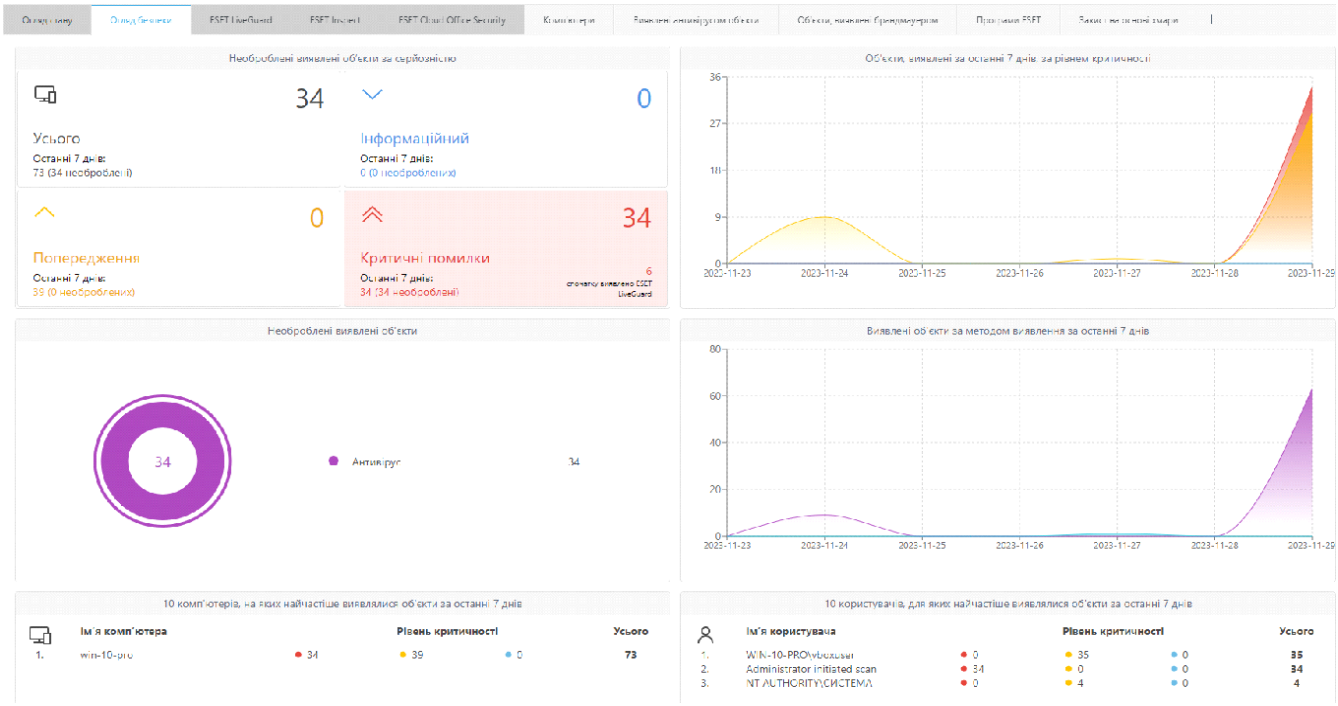


Рис 3.19. Огляд Безпеки

- *Комп'ютери.* На цій панелі інструментів відображаються основні відомості про клієнтські машини, зокрема статус захисту, операційні системи та статус оновлення.

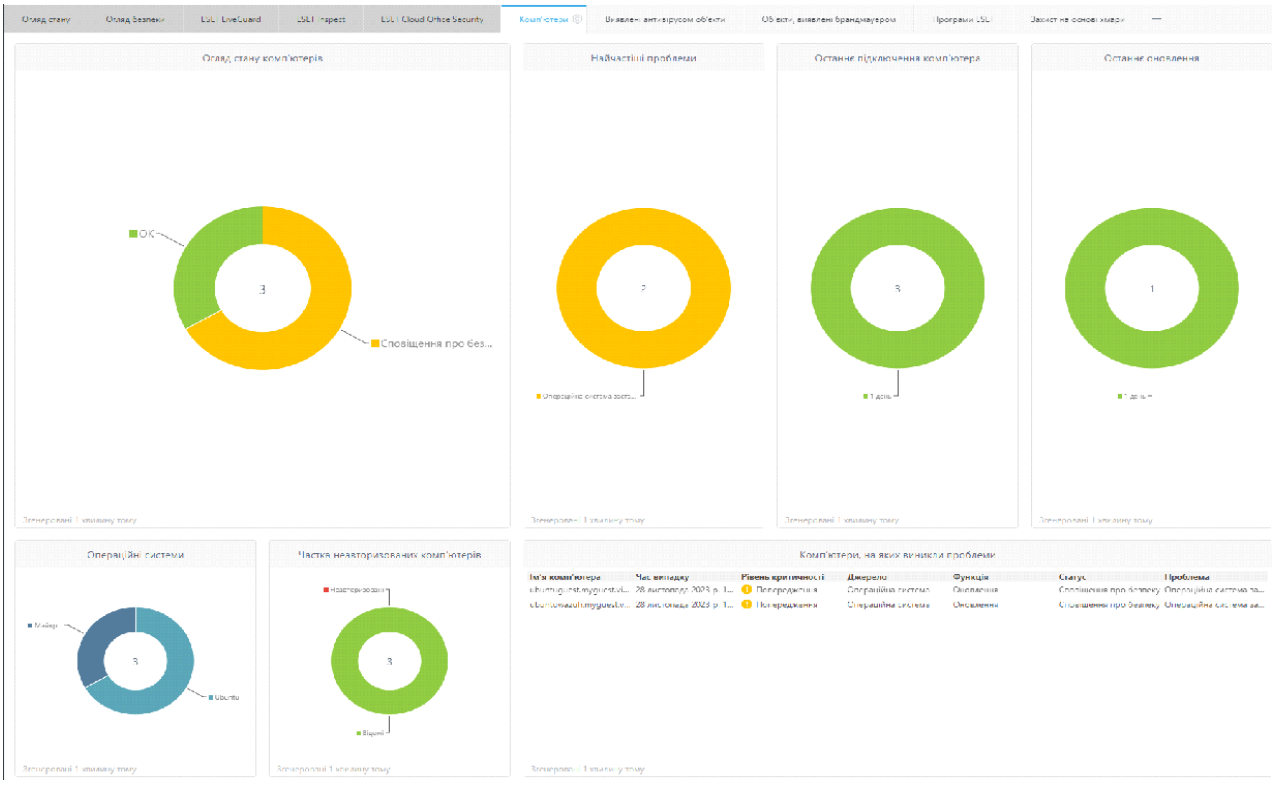


Рис 3.20 Комп'ютери

- Виявлені антивірусом об’єкти. Тут можна переглянути звіти від антивірусного модуля продуктів безпеки клієнта: активні виявлені об’єкти, виявлені об’єкти за останні 7/30 днів тощо.

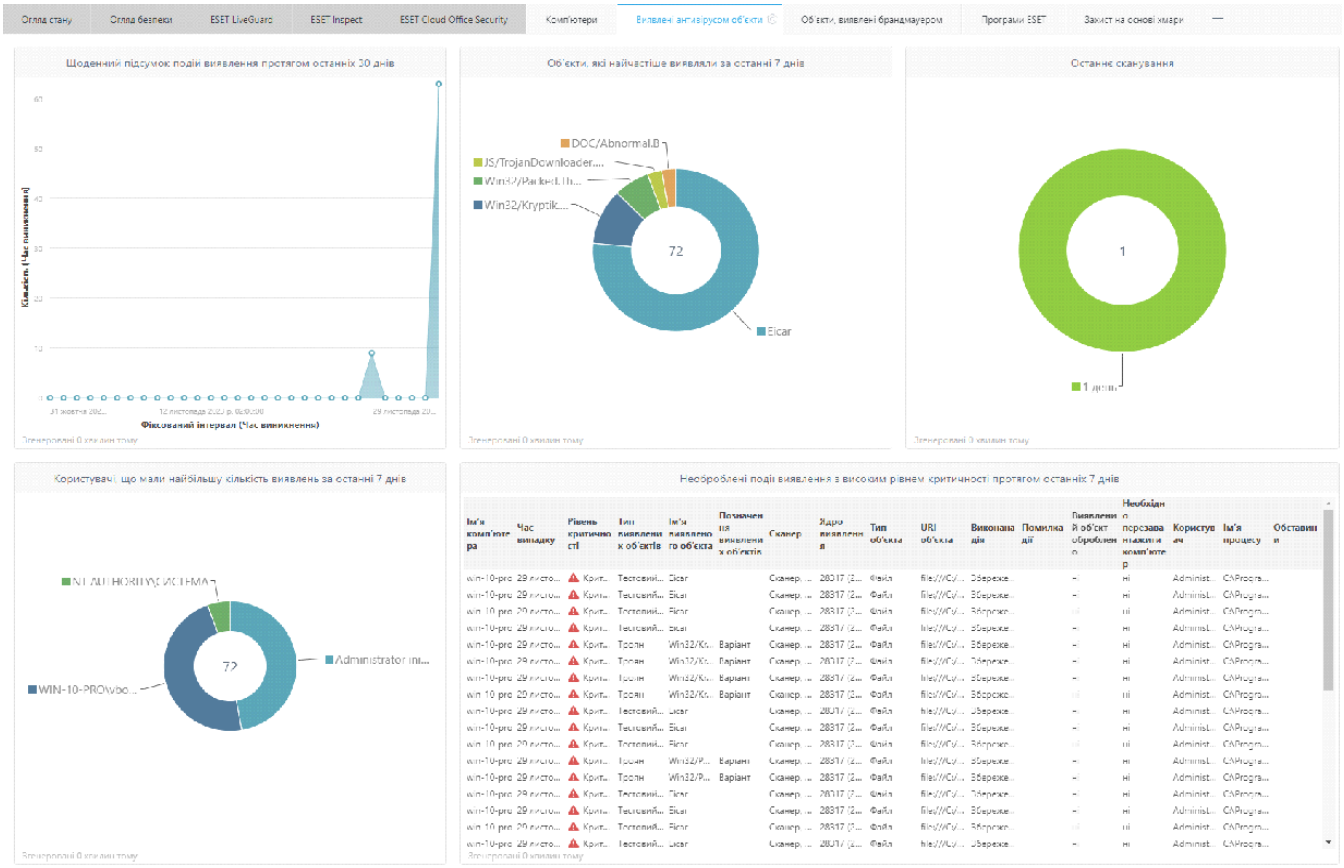


Рис 3.21 Виявлені антивірусом об’єкти

3.2.3.3 Комп’ютери

Тут за групами відображаються всі клієнтські пристрої, додані до цього ESET PROTECT Cloud. Кожен пристрій відноситься до окремої статичної групи.

“Некеровані” комп’ютери (клієнти в мережі, на яких не встановлено агента ESET Management), зазвичай відображаються в групі “Утрачені й знайдені”. Статус клієнта, що відображається у веб-консолі ESET PROTECT Cloud, не залежить від налаштувань продуктів ESET для захисту на клієнтському комп’ютері. Ось чому навіть якщо певний статус не відображається в клієнті, відомості про нього все одно передаються на веб-консоль ESET PROTECT Cloud.

Параметри меню комп’ютер:

- Ім’я комп’ютера
- IP-адреса
- Теги
- Статус
- Помилка
- Попередження
- ОК
- Останнє підключення
- Сповіщення - кількість сповіщень
- Виявлені об’єкти - кількість виявлених об’єктів
- Назва ОС
- Користувач

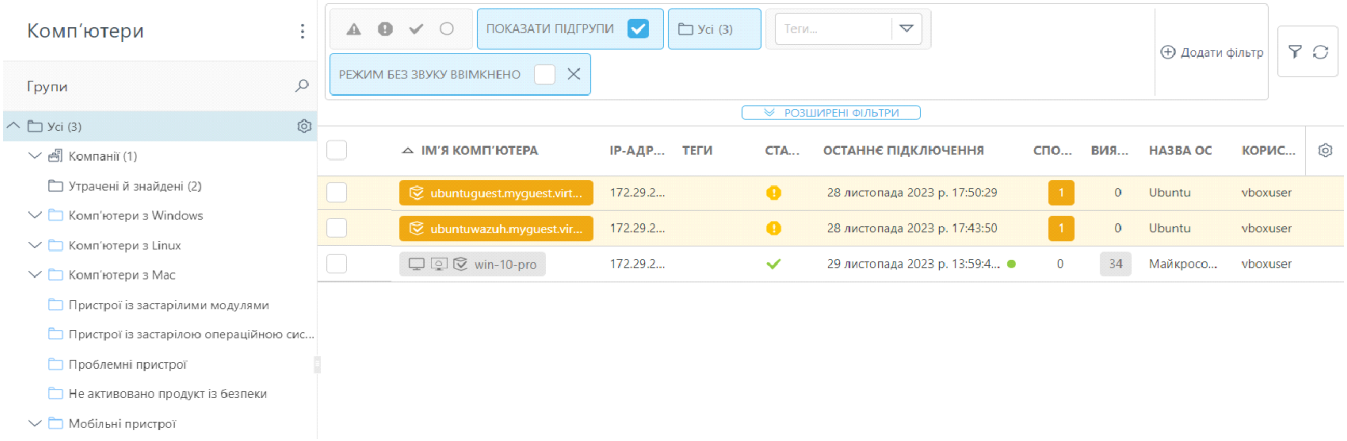


Рис 3.22 Панель «Комп’ютери» ESET Protect Cloud

В даному випадку бачимо, що в тестовій інфраструктурі присутні три комп’ютера:

- Ubuntu 2x: у кожного по одному сповіщенню
- Майкрософт Windows 10 Pro: 34 виявлених об’єкти

3.2.3.4 Виявлені об’єкти

У розділі Виявлені об’єкти можна переглянути об’єкти, виявлені на керованих пристроях.

Існує два типи виявлених об’єктів відповідно до статусу:

- *Активні виявлені об’єкти* – виявлені об’єкти, які ще не очищено. Щоб очистити виявлений об’єкт, виконайте *детальне сканування* з увімкненим очищенням для папки, що містить виявлені об’єкти. Щоб очистити виявлений об’єкт і більше його не виявляти, завдання сканування має завершитись успішно. Якщо користувач не усунить активний виявлений об’єкт протягом 24 годин із моменту виявлення, об’єкт утратить статус *активного*, але залишиться неусуненим;
- *Усунені об’єкти* – це виявлені об’єкти, які користувач позначив як усунені, але ще не виконував їх *детальне сканування*. Пристрої з виявленими об’єктами, які позначено як усунені, усе ще відображатимуться у відфільтрованому списку результатів до виконання сканування.

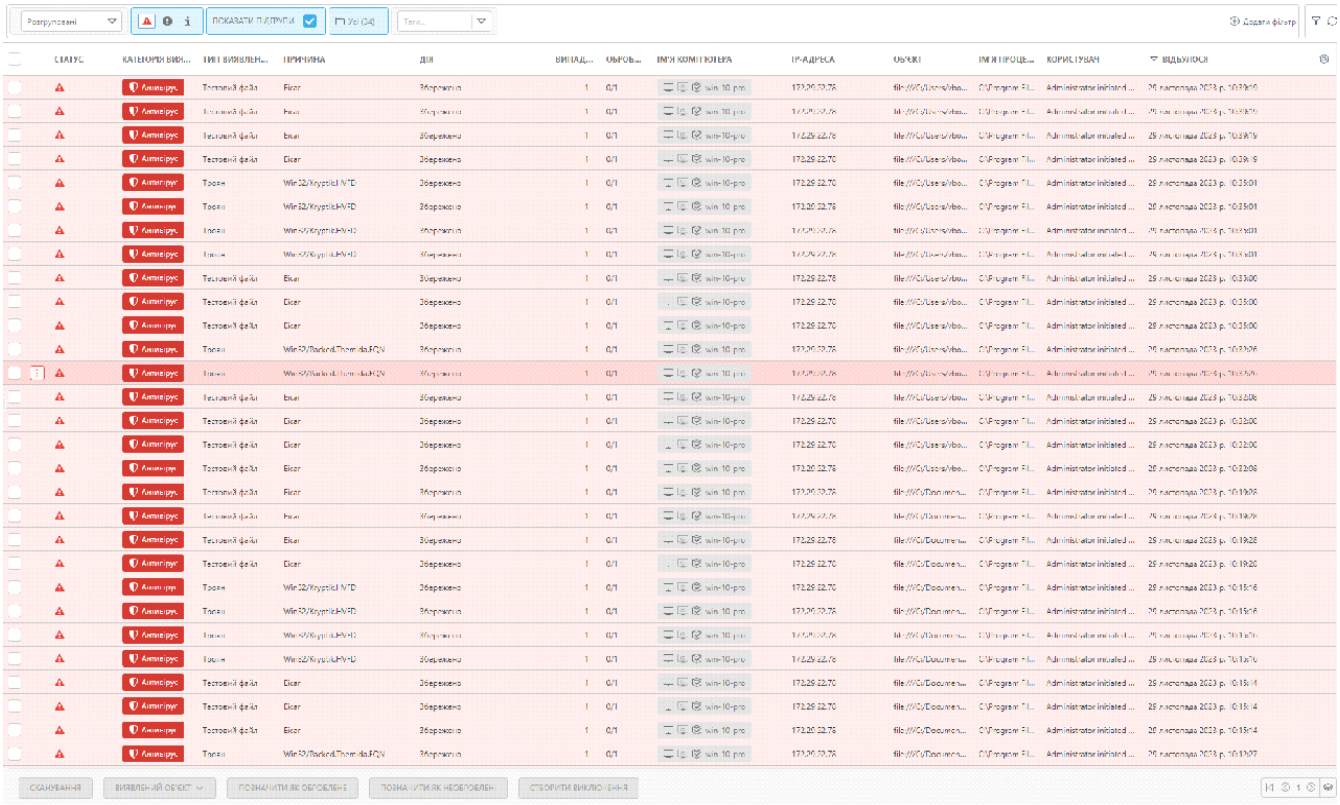


Рис 3.23 Панель «Виявлені об’єкти» ESET Protect Cloud

Для тестування функціоналу EDR ESET було використано зразки зловмисного програмного забезпечення завантажених із відкритих джерел. Можна побачити, що саме ці 34 виявлені об’єкти із статусом “Помилка” і відображалися

на панелі минулого підрозділу “Комп’ютери” в операційній системі Майкрософт Windows 10 Pro.

3.2.3.5 Сповіщення

Сповіщення мають важливе значення для відстеження загального стану вашої мережі. Коли відбувається нова подія (згідно з конфігурацією сповіщень), ви отримуєте сповіщення на електронну пошту, що дає змогу вжити відповідні заходи.

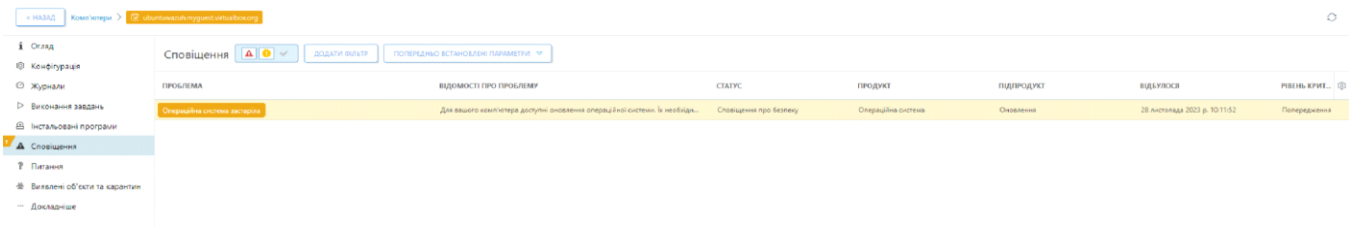


Рис 3.24 Панель «Сповіщення» ESET Protect Cloud

В якості прикладу була взята одна з операційних систем Ubuntu. Можна побачити, що саме це сповіщення із статусом “Попередження” і відображалися на панелі минулого підрозділу “Комп’ютери” в операційній системі Ubuntu. Текст сповіщення: “Для вашого комп’ютера доступні оновлення операційної системи. Їх необхідно інсталювати, щоб забезпечити захист системи.”. Тобто це значить, що EDR ESET, як було зазначено раніше відслідковує оновлення операційних систем та програмних забезпечень.

3.2.3.6. Налаштування автоматизації для реагування на інциденти

Однією з основних переваг систем EDR являється можливість керування кінцевими точками. Серед усього спектру можливостей керування кінцевими точками можна виділити “завдання” ізоляції ПК в залежності від налаштованих політик ПК, або критичності статусу спрацювання на інцидент.

Завдання «Ізолювати комп’ютер від мережі» ізолює вибрані комп’ютери від мережі. Всі підключення, окрім тих, які необхідні для правильної роботи продуктів ESET, будуть заблоковані. Дозволені підключення включають наступне:

- комп'ютер отримує IP-адресу

- зв’язок ekrn.exe, ESET Management Agent, ESET Inspect Connector
- можливість входу в домен

Розширенням базового функціоналу “завдання” є створення “тригеру” залежного від нього. Тобто ініціатором початку виконання завдання являється саме “тригер”.

В переліку вбудованих шаблонних завдань в ESET PROTECT присутнє завдання “Ізолювати комп’ютер від мережі”. Для того шоб створити користувацьке (кастомне) завдання треба в панелі завдання натиснути кнопку “Створити…”, далі “Завдання клієнта”.

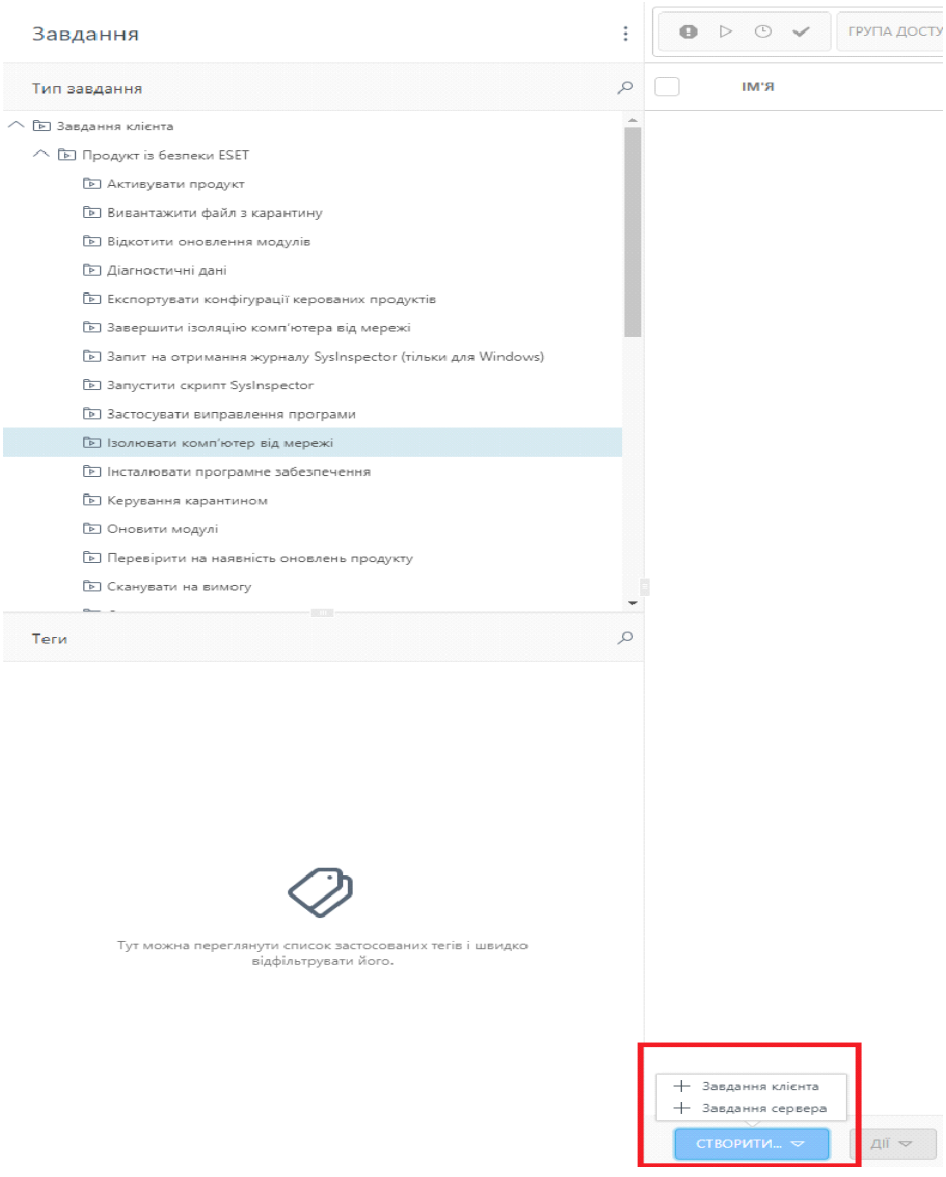


Рис 3.25 Створення завдання для ізоляції ПК

В панелі “Нове завдання клієнта” зазначити параметри завдання:

- Ім’я
- Теги
- Опис
- Категорія завдання
- Завдання

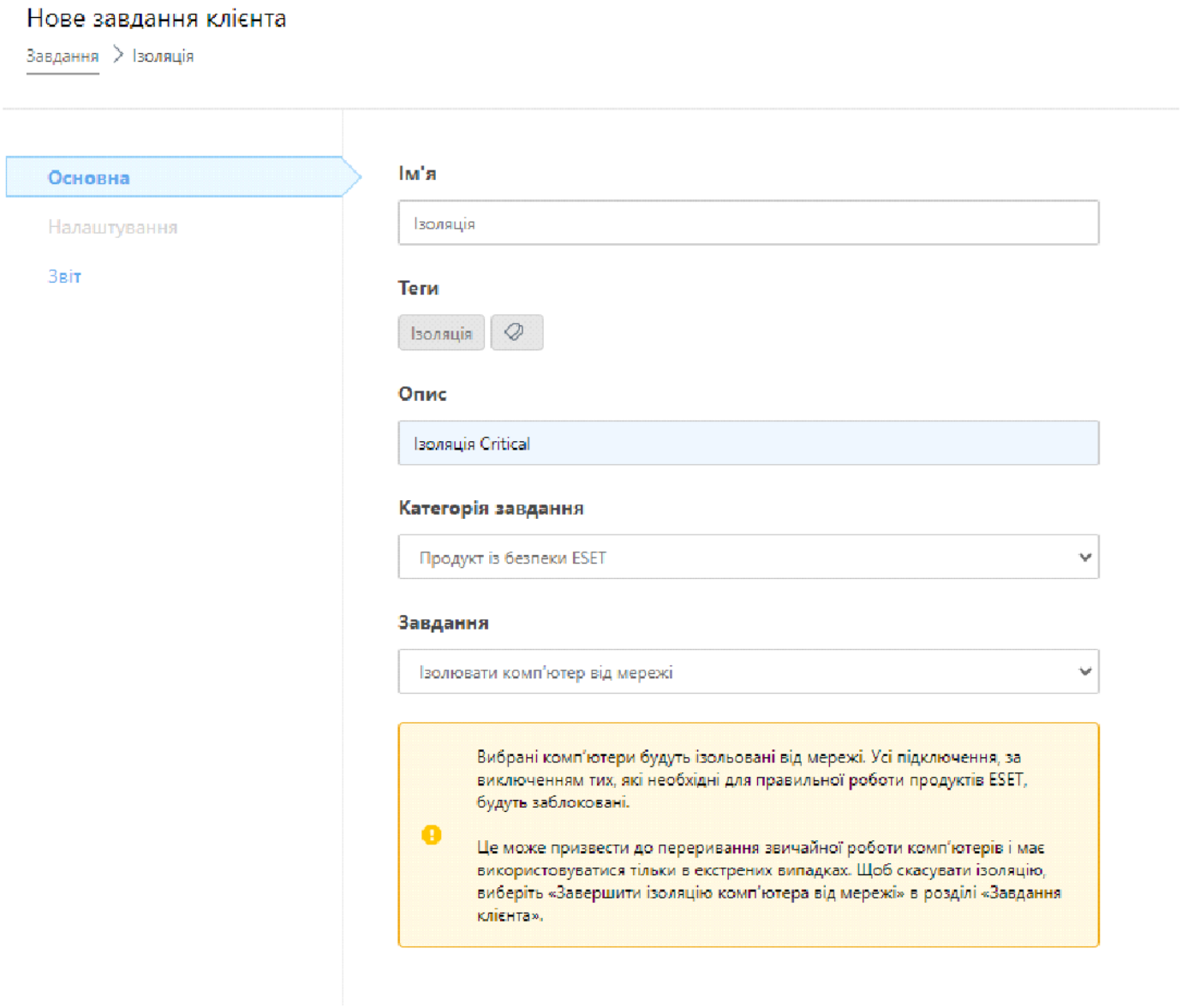


Рис 3.26 Приклад заповнення форм для створення завдання

В полі “Категорія завдання” обрати “Продукт із безпеки ESET”, а в полі “Завдання” обрати “Ізолювати комп’ютер від мережі”. Після чого натиснути

кнопку “Готово”. Далі на екрані буде запропоновано додати тригер до завдання. Треба натиснути кнопку “Створити тригер”.

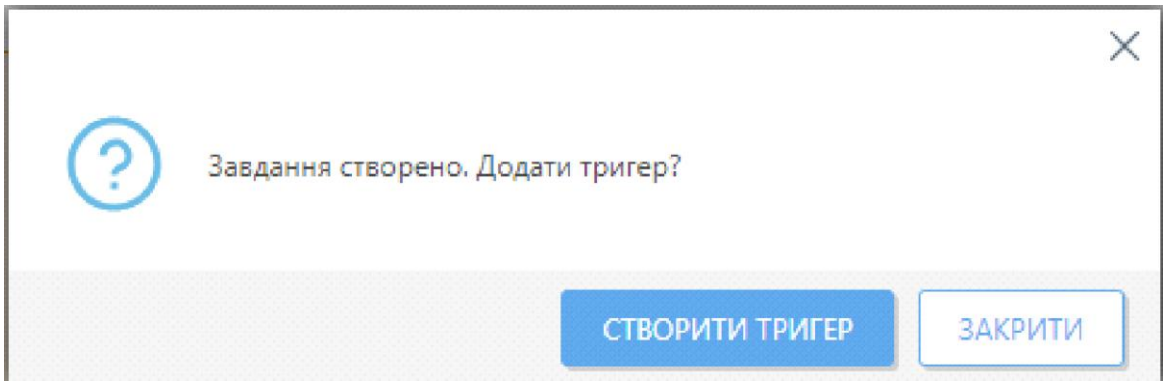


Рис 3.27 Створення трігеру на основі завдання

В панелі “Додати новий тригер” зазначити:

- Опис тригера
- Об’єкт
- Тип тригера
- Тип журналу
- Логічний оператор для фільтрів
- Фільтр

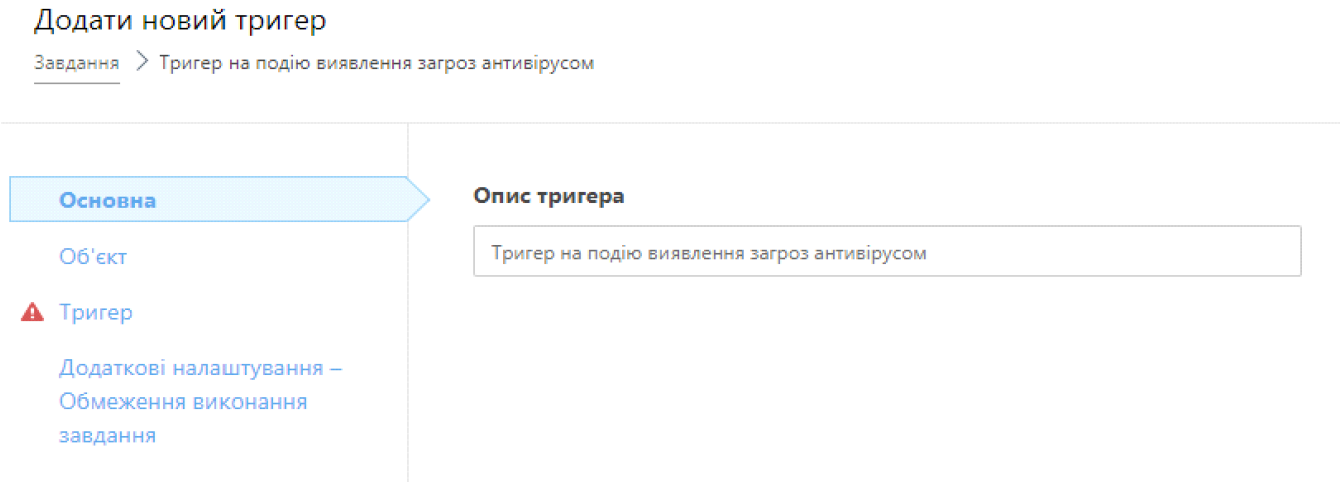


Рис 3.28 Приклад заповнення форм для створення тригеру

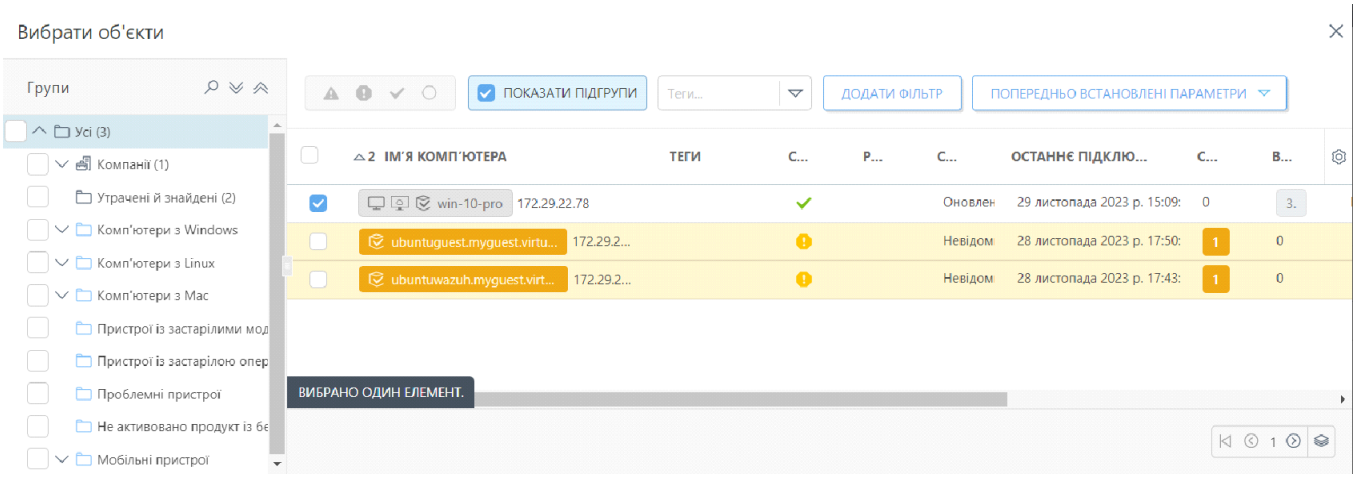


Рис 3.29 Вибір ПК на який буде поширюватися тригер

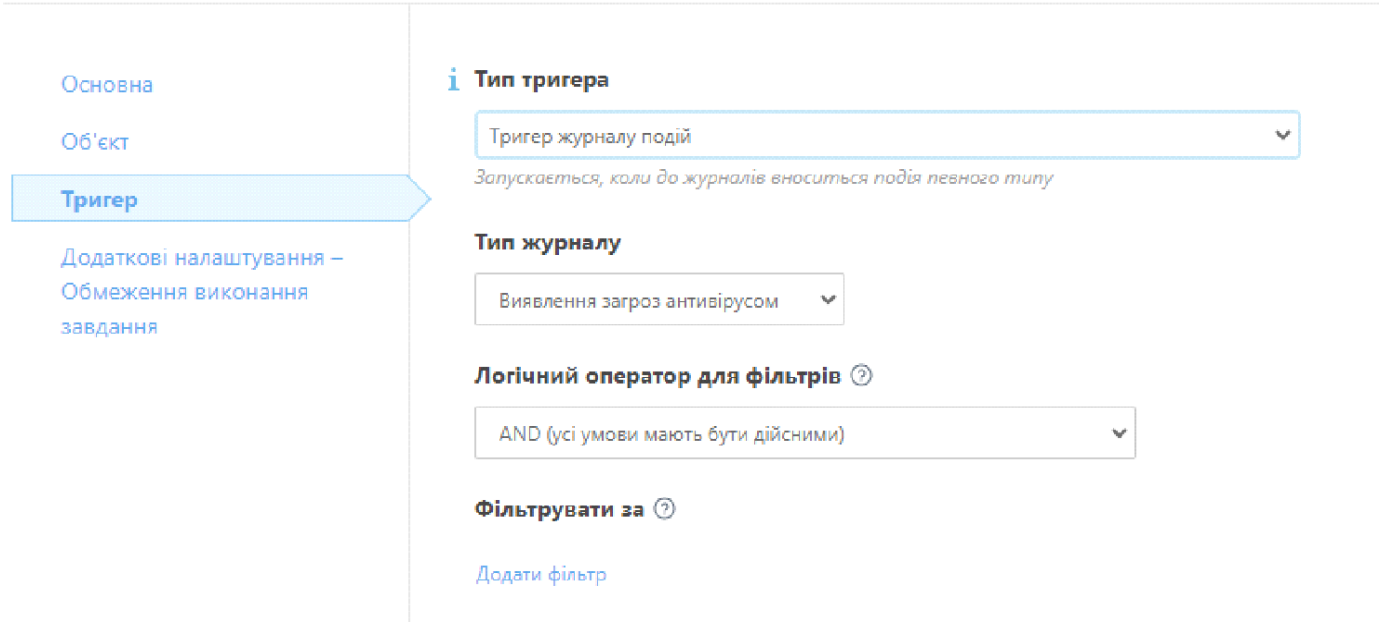


Рис 3.30 Приклад заповнення форм для створення тригеру

На моменті вибору об’єкту можна вибрати окрему групу і тоді тригер буде застосований для всіх ПК, які знаходяться в визначеній групі. В даному випадку був окремо обраний ПК із операційною системою Майкрософт Windows 10 Pro. Після створення завдання з’явиться в панелі завдань.

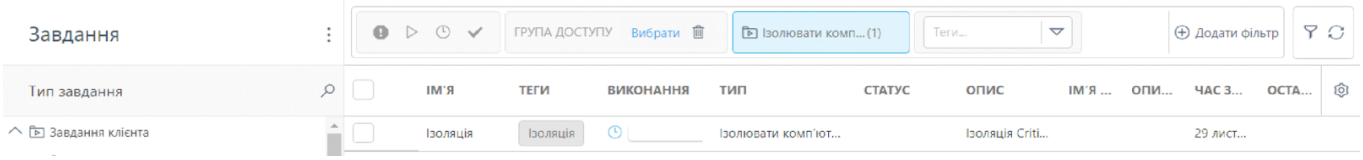


Рис 3.31 Приклад створеного завдання на ізоляцію

Для демонстрації працездатності даного функціоналу було встановлено і запущено віртуальну машину Windows 10 Pro. На машині був встановлений агент ESET Endpoint Security.

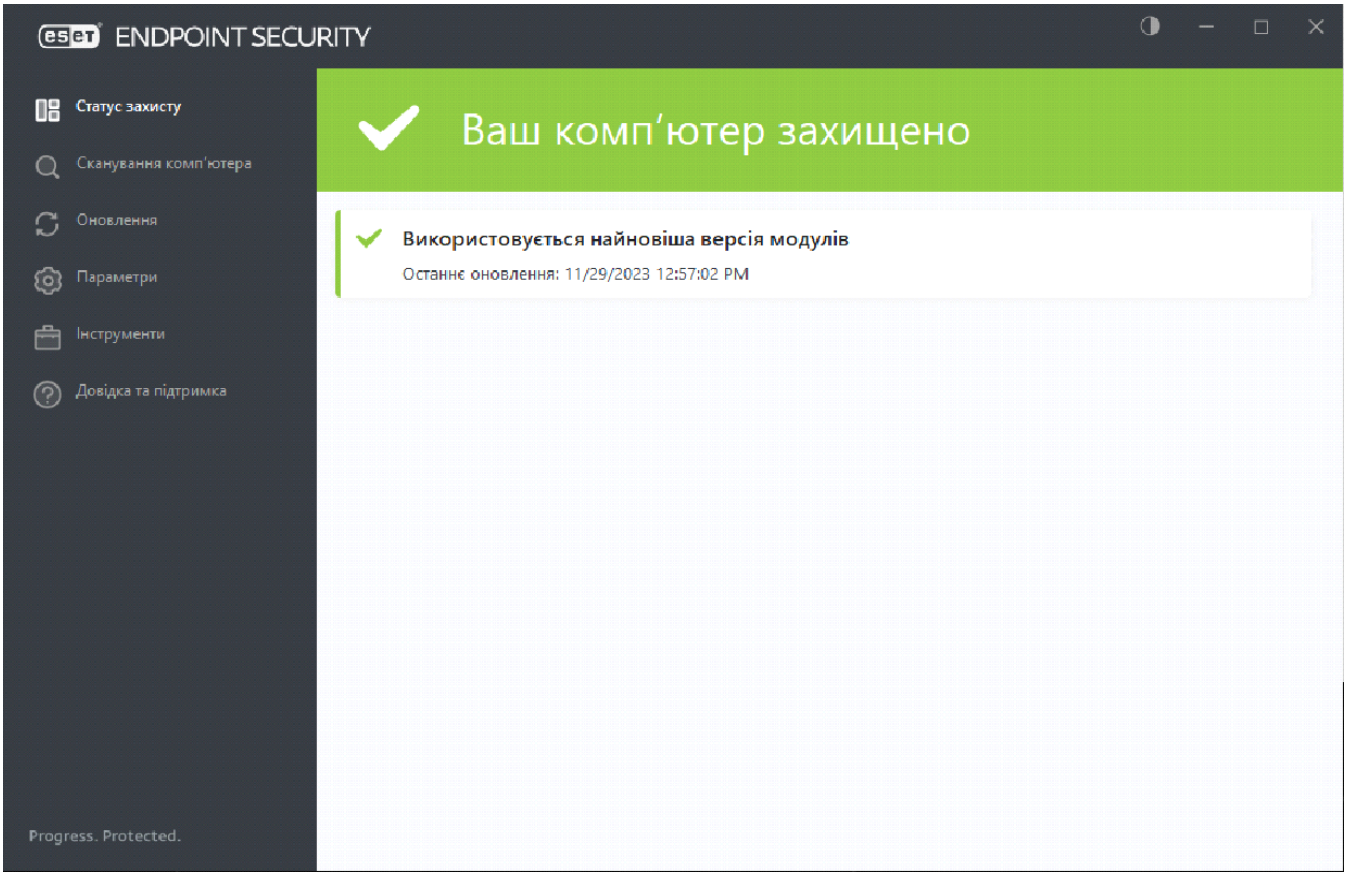


Рис. 3.32. Встановлений агент ESET Endpoint Security на ПК

Можна побачити, що можливість виходу в інтернет у машини з самого початку є. В якості підтвердження була проведена перевірка з'єднання за допомогою команди ping в командному рядку за ip адресою dns серверу компанії Google.

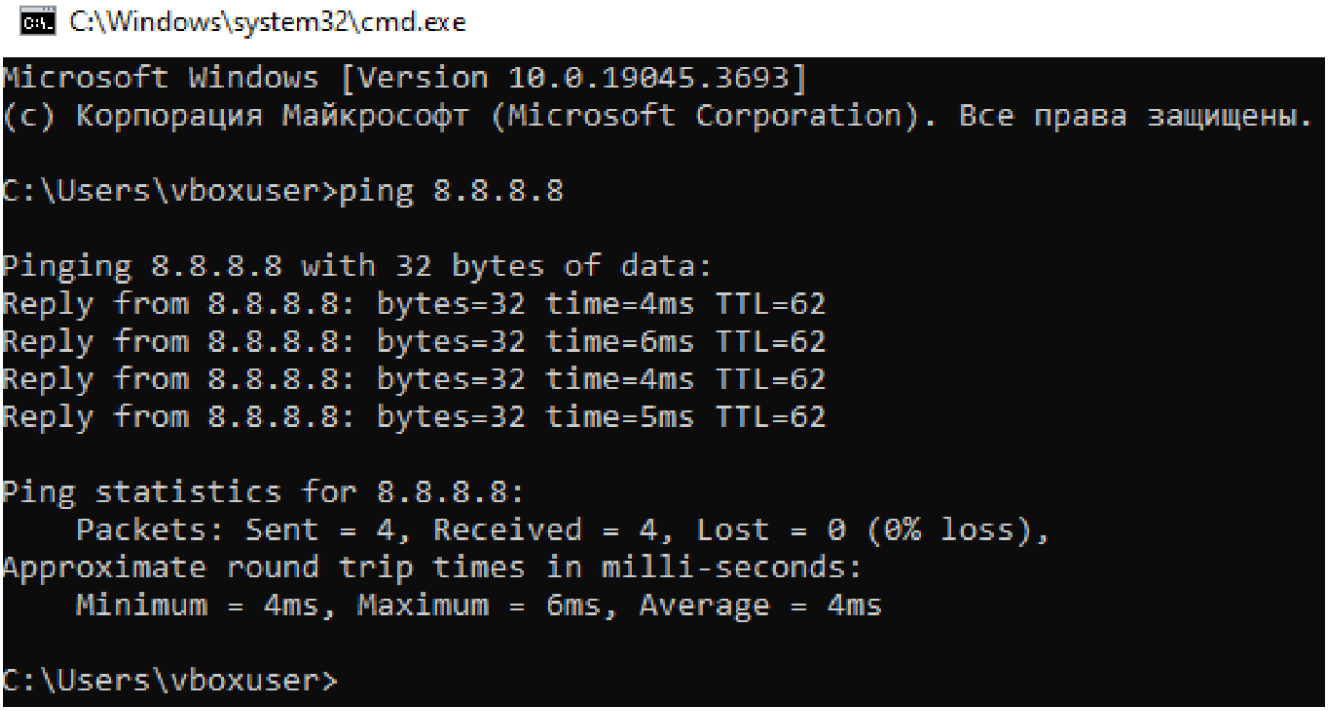


Рис. 3.33. Демонстрація наявності зв’язку із мережею Інтернет

Далі було завантажено архів із назвою eicar_com та типом файлу .zip з офіційного сайту eicar[.]com

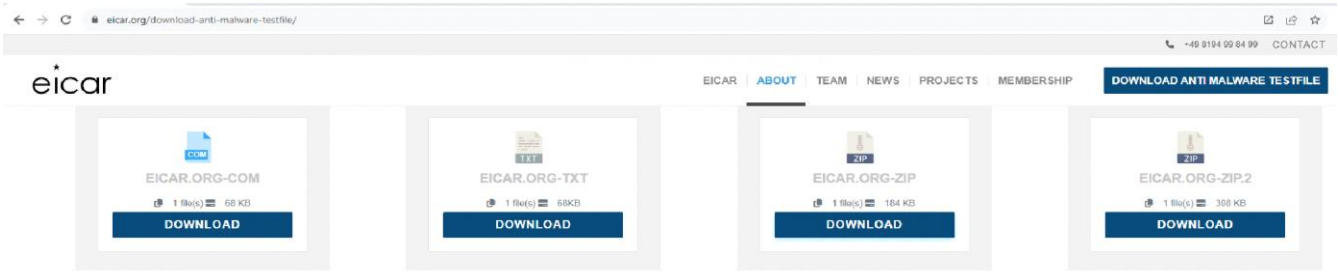


Рис. 3.34. Псевдо зловмисні файли з офіційного сайту eicar.org

В якості зловмисного файлу для перевірки спрацювань виявлення шкідливих файлів знову, як і в розділі 3.2.1.5, був вибраний тестовий псевдо шкідливий файл Eicar.com (стандартний файл, який використовується для перевірки, чи працює антивірус).

Після завантаження файлу ESET Endpoint Security показав сповіщення про спрацюванню алгоритму виявлення вірусу та переніс файл до “Картантину”, після чого видалив файл на ПК. Як тільки виникло позитивне спрацювання через шкідливий файл, почало виконуватись раніше створене завдання для ізоляції

кінцевої точки. Статус захисту, що відображається в ESET Endpoint Security тепер “Доступ до мережі заблоковано” рис 3.35.

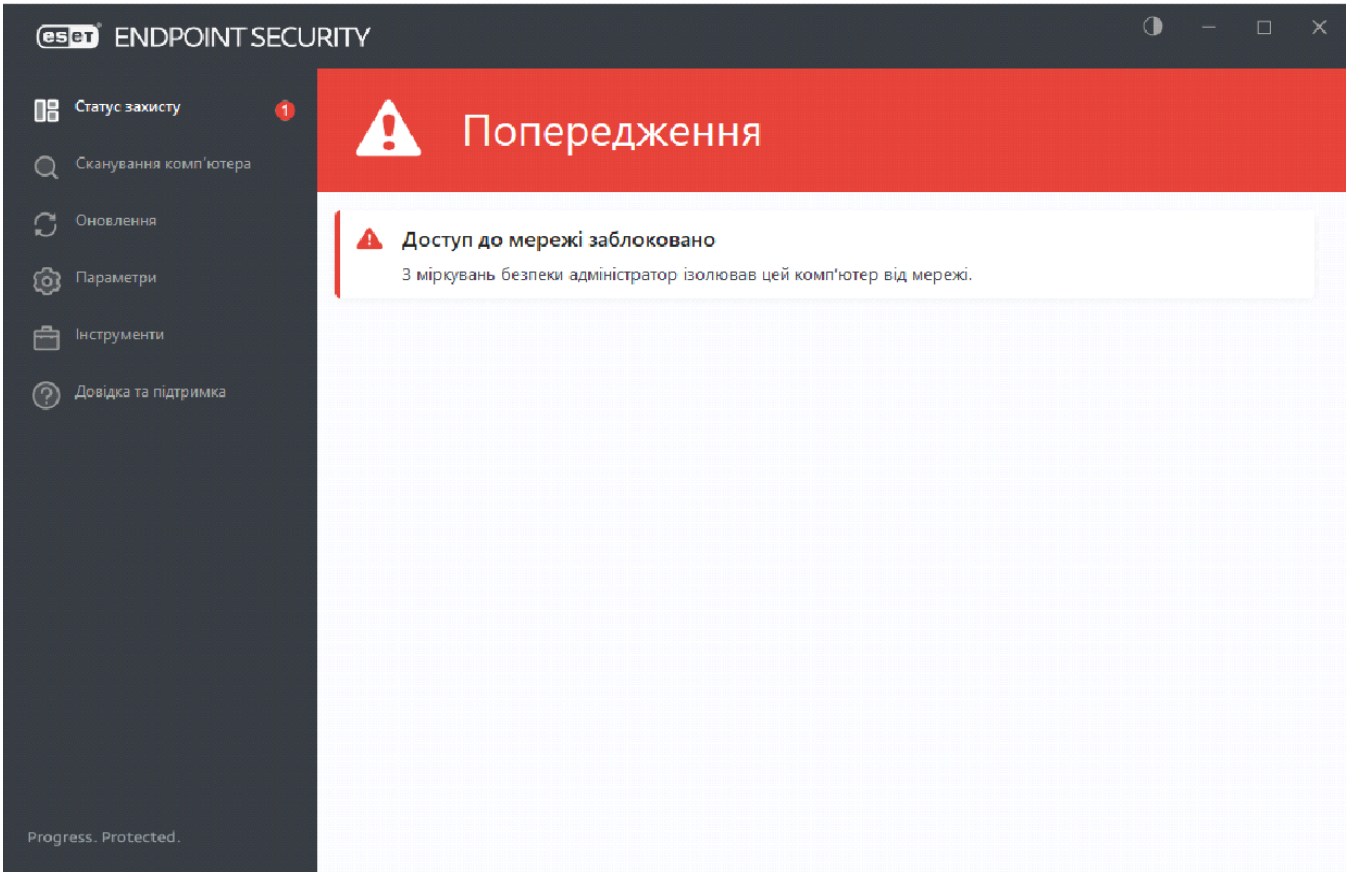


Рис 3.36. Статус захисту агента ESET Endpoint Security

Повторна спроба перевірки з'єднання з мережею Інтернет є невдалою

```
C:\Users\vboxuser>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
General failure.
General failure.
General failure.
General failure.
```

Рис. 3.37. Демонстрація відсутності зв’язку із мережею Інтернет

В панелі “Виявлені об’єкти” відображаються події видалення псевдо шкідливих файлів

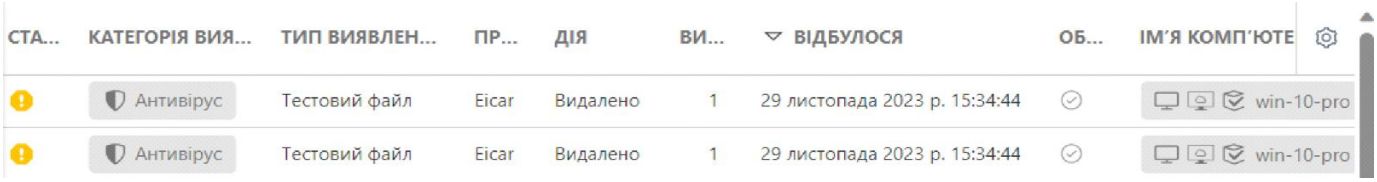


Рис 3.38. Виявлені об'єкти в ESET Protect Cloud

В сповіщеннях ПК відображається подія обмеження доступу до мережі

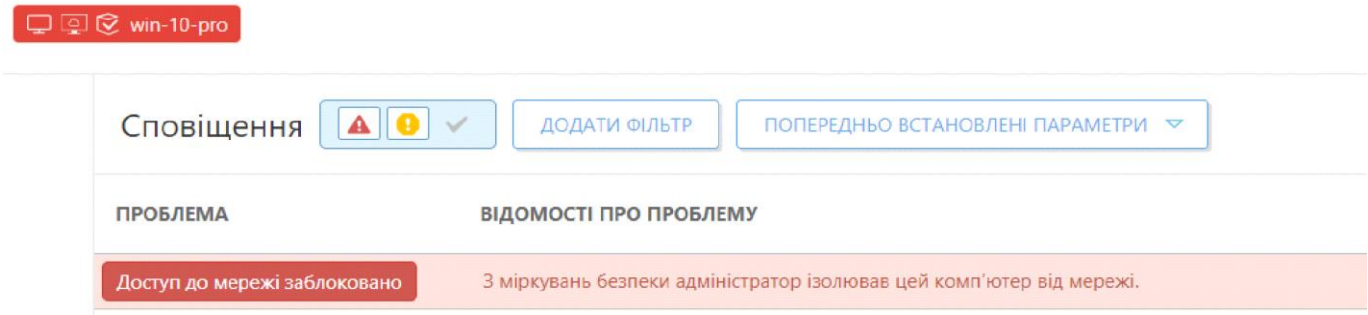


Рис 3.39. Обмеження доступу до мережі ПК win-10-pro ESET Protect Cloud

Для виведення ПК з ізоляції треба в панелі "Комп'ютери" натиснути на необхідну машину правою кнопкою миші, перейти в "Ізоляція мережі", далі "Завершити ізоляцію мережі".

Таблиця 3.1

Порівняльний аналіз сучасних EDR систем

Характеристика	ESET EDR	Cisco Secure Endpoint
Виявлення Загроз та Реагування	Використовує аналіз поведінки, сигнатури та інші методи для виявлення загроз. Надає можливість реагувати та ізолювати загрози.	Використовує технології машинного навчання та аналізу поведінки для виявлення складних загроз. Забезпечує автоматизовану реакцію та ізоляцію систем.
Інтеграція з Іншими Системами	Інтегрується з іншими продуктами безпеки та системами для обміну інформацією та покращення взаємодії.	Забезпечує інтеграцію з іншими продуктами Cisco та сторонніми системами через API для об'єднаного управління безпекою.

Продовженяня таблиці 3.1

1	2	3
Керування Загрозами	Надає інструменти для управління загрозами, включаючи відслідковування подій та аналіз інцидентів.	Забезпечує велику кількість функцій для аналізу, категоризації та управління загрозами. Використовує Threat Response для спільного реагування.
Адаптивний Захист	Використовує адаптивний захист для виявлення нових та розширених загроз.	Застосовує адаптивні алгоритми для виявлення та захисту від змінюючихся загроз у реальному часі.
Інтегрована Аналітика	Використовує аналітичні засоби для розуміння контексту подій та виявлення аномалій.	Забезпечує інтегровані аналітичні засоби для вивчення структури атак та виявлення ускладнених загроз.
Інтерфейс Користувача	Надає інтуїтивний та зручний інтерфейс для користувачів.	Має користувацький інтерфейс, який спрощує адміністрування та моніторинг системи.
Підтримка та Сервіси	Забезпечує технічну підтримку та оновлення програмного забезпечення.	Надає технічну підтримку, навчання та послуги консультування для користувачів.
Вартість та Ліцензування	Вартість може варіюватися в залежності від обсягу та функціоналу. Ліцензії на кінцеві точки та підписка на сервіс.	Вартість залежить від обраного пакету та обсягу користувачів. Можливості ліцензування включають підписку та варіанти пакетів.

Обидві системи, ESET EDR та Cisco Secure Endpoint, представляють сучасні інструменти для захисту інформаційної безпеки на корпоративному рівні. Вони мають ряд спільних та унікальних характеристик, які варто врахувати при виборі між ними. Ось кілька ключових висновків:

- Виявлення та Реагування на Загрози:
- Обидві системи використовують сучасні методи для виявлення та реагування на загрози, такі як аналіз поведінки, машинне навчання та автоматизована реакція.
- Інтеграція та Сумісність:
- Обидві системи підтримують інтеграцію з іншими продуктами безпеки та сторонніми системами, забезпечуючи об'єднану систему управління безпекою.
- Аналітика та Адаптивний Захист:
- ESET EDR та Cisco Secure Endpoint використовують аналітичні засоби для аналізу загроз та забезпечують адаптивний захист для виявлення нових та розширених загроз.
- Інтерфейс Користувача та Підтримка:
- Обидві системи ставлять у фокус інтуїтивний користувацький інтерфейс та надають технічну підтримку для користувачів.
- Вартість та Ліцензування:
- Вартість та ліцензування обох систем можуть варіюватися в залежності від обраного пакету та обсягу користувачів.

Обрання між ESET EDR та Cisco Secure Endpoint:

- Якщо важливий інтуїтивний інтерфейс та ефективний захист:
- ESET EDR може бути відмінним вибором з простим інтерфейсом та надійними функціями захисту.
- Якщо необхідна інтегровану екосистему та потужні аналітичні можливості:
- Cisco Secure Endpoint забезпечує інтеграцію з іншими продуктами Cisco та розширені функції аналітики.

Важливо здійснити оцінку потреб організації та привилегій вибір системи, яка найкращим чином відповідає вашим вимогам до безпеки та ресурсам.

3.3 Висновки до розділу

Поєднуючи запропоновані рішення у вигляді систем для моніторингу, а саме SIEM/XDR Wazuh та виявлення, реагування і керування EDR від ESET можна повністю забезпечити екосистему, або інфраструктуру трьома основними принципами інформаційної безпеки: конфіденційністю, цілісністю та доступністю. Оскільки використовуючи Wazuh в якості SIEM/XDR системи аналізом покривається весь вектор мережевих та апаратних подій, за допомогою збирання даних журналів подій із низки джерел, та визначення нетипових дії за допомогою аналізу в реальному часі й уживання відповідних заходів. Використовуючи ESET Protect в якості EDR системи в свою чергу, можна запровадити повний контроль та реагування на інциденти кібербезпеки над кінцевими точками за допомогою політик безпеки та автоматизації процесів менеджменту. Додатковими засобами захисту можуть бути інтегровані системи безпеки, які надають більше аналітичних та поведінкових даних стосовно будь-якого інциденту. Даний модуль для моніторингу, розслідування інцидентів в кібербезпеці системами SIEM та XDR буде корисним всім сучасним командам захисту в кіберпросторі та безпековим аналітикам.

Розділ 4. СТВОРЕННЯ МОДУЛЮ МОНІТОРИНГУ СИСТЕМАМИ SIEM ТА XDR

4.1 Аналіз загроз екологічної безпеки

Охорона навколишнього середовища є однією з найбільш актуальних та важливих проблем сучасності. Зростання населення, індустріалізація та технологічний розвиток призводять до значного впливу на природу, що ставить під загрозу екологічну безпеку.

Проаналізовано актуальні загрози екологічній безпеці Автономної Республіки Крим, Донецької та Київської областей. Досліджено функції безпеки вказаних регіонів для основних об‟єктів захисту – осіб, господарських об‟єктів і довкілля. На основі дослідження тенденцій виникнення надзвичайних ситуацій в регіонах України здійснено короткострокове прогнозування їхнього розвитку. Розглянуто методологію оцінки природно-техногенних загроз для порівняльного аналізу стану екологічної безпеки регіонів держави.

Сучасний стан екологічної безпеки України характеризується надмірним використанням життєзабезпечувальних природних ресурсів, значним техногенним забрудненням основних екологічних систем і виснаженням їх відновлювальних можливостей, зниженням родючості сільськогосподарських угідь, критичним скороченням площі лісів, надзвичайною зарегульованістю річкової мережі, а також масштабами наслідків Чорнобильської катастрофи. В цілому це призвело до формування масштабних деструктивних процесів у навколишньому середовищі, які за просторово-часовими характеристиками становлять реальну загрозу національній безпеці держави. Аналіз актуальних тенденцій розвитку стихійних лих та техногенних катастроф свідчить про високу ймовірність виникнення НС природного та техногенного характеру зі значними ризиками для населення і держави у випадку їх реалізації. Подолання негативних тенденцій зростання втрат

і витрат внаслідок НС різного походження можливе на основі комплексного аналізу ризиків та управління ними у рамках загальнодержавної системи регулювання безпеки населення і територій. Основою цієї системи має стати аналіз можливих природно-техногенних загроз регіональній безпеці держави. Регіональна безпека характеризує такий стан захищеності регіону, коли він спроможний протистояти дестабілізуючим впливам зовнішніх і внутрішніх загроз, а його функціонування не створює загроз самому регіону та елементам навколишнього середовища. Розглянемо методичний підхід до комплексного аналізу актуальних природно-техногенних загроз регіональній безпеці держави.

У роботі було проведено кластерний аналіз регіонів України за показниками головних загроз екологічній безпеці держави. Результати аналізу показали, що Донецька, Київська області та Автономна Республіка Крим входять до 3 різних кластерів за компонентами основних загроз екологічній безпеці. На підставі оновлених даних Міністерства надзвичайних ситуацій України здійснено аналіз актуальних загроз екологічній безпеці вказаних регіонів держави.

Аналіз ризиків на регіональному рівні тісно пов'язаний з аналізом загроз, які, у свою чергу, визначають рівень безпеки регіонів. Теоретичну основу оцінки рівнів безпеки регіонів може становити теорія надійності, відповідно до якої надзвичайні ситуації слід розглядати як «відмови» елементів систем, що призводять до порушення їхньої стійкості. Припустимо, що безпека регіону визначається величиною ризику, який не перевищує прийнятний рівень. Нехай SΣ(t) – функція безпеки, а сукупність характеристик аварій і катастроф, які мають рівні ймовірності їхнього виникнення, визначається за допомогою функцій ризику HΣ(t). При цьому

$$S_{\sum}(t) = \prod_i^n S_i(t) \tag{4.1}$$

$$H_{\sum}(t) = \sum_i^n H_i(t) \tag{4.2}$$

де Si, Hi – функції безпеки та ризику і-ї загрози, n – кількість загроз. Нехай розглядається пуасонівський потік «відмов». У такому разі можна записати

$$S_{\sum}(t) = exp\left(-\sum_i^n \lambda_i(\tau)\rho_{ij}(\tau)d\tau\right) \quad (4.3)$$

$$H_{\sum}(t) = \left(-\sum_i^n \lambda_i(\tau)\rho_{ij}(\tau)d\tau\right) \quad (4.4)$$

де λ_i – інтенсивність надзвичайних ситуацій і-го виду, ρ_{ij} – ймовірність j-ї компоненти системи для і-го виду надзвичайної ситуації. Розрахунок ймовірностей ρ_{ij}передбачає наявність технічних, екологічних, економічних і соціальних критеріїв безпеки. В даний час ці критерії відсутні. За таких умов у першому наближенні можна припустити:

$$\rho_{ij} = \frac{n_{ij}}{n_i} \quad (4.4)$$

Розглянемо основні загрози екологічної безпеки та проведемо аналіз їх впливу на навколишнє середовище.

1. Забруднення повітря

Однією з основних загроз є забруднення повітря викидами в атмосферу від промислових підприємств, транспортних засобів та інших джерел. Домішки та токсичні речовини, що потрапляють в повітря, можуть мати серйозний вплив на здоров'я людей та екосистему.

2. Забруднення води

Викиди промислових відходів та неконтрольоване скидання стічних вод призводять до забруднення водних ресурсів. Це впливає на рибний фонд, водні рослини та може призвести до виникнення "мертвих зон" у водоймах.

3. Знищення біорізноманіття

Втрата природного середовища та знищення екосистем призводять до зменшення біорізноманіття. Вимирання видів та порушення екологічного балансу стають серйозною загрозою для стійкості природних систем.

4. Зміна клімату

Викиди парникових газів, таких як вуглекислий газ та метан, сприяють глобальній зміні клімату. Збільшення температур, погіршення погодних умов та підвищення рівня морів є наслідками цього явища, що може призвести до серйозних наслідків для життя на Землі.

5. Відходи та переробка відходів

Недоцільна утилізація та великі обсяги відходів стають проблемою, що вимагає негайного вирішення. Переробка відходів та впровадження більш ефективних систем утилізації можуть сприяти зменшенню негативного впливу на навколишнє середовище.

6. Ландшафтне використання та забудова

Інтенсивна забудова та зміни в ландшафтному використанні можуть призводити до втрати природних екосистем та природних резервів. Забудова може створювати бар'єри для руху тварин та впливати на місцевий клімат, що має подальші наслідки для екосистем.

7. Вплив хімічних речовин

Хімічні речовини, такі як пестициди та хімічні добрива, використовуються в сільському господарстві та інших галузях, що може викликати забруднення грунтів та водних джерел. Це має негативний вплив на рослинництво, тваринництво та здоров'я людей.

8. Енергетична безпека та відновлювані джерела енергії

Залежність від нестійких джерел енергії, таких як вугілля та нафта, не лише призводить до викидів парникових газів, але і ставить під загрозу енергетичну безпеку. Перехід до відновлюваних джерел енергії може сприяти зменшенню екологічного впливу та забезпеченню сталого розвитку.

9. Глобальна перерозподіл природних ресурсів

Нерівномірний доступ до природних ресурсів та їх несправедлива перерозподіл може викликати конфлікти між країнами та внутрішніми соціальними проблемами. Раціональне управління та спільне використання ресурсів може допомогти зберегти природні багатства та забезпечити стале використання ресурсів.

10. Роль освіти та наукових досліджень

Важливою частиною розв'язання проблем екологічної безпеки є підвищення рівня освіти та наукових досліджень в галузі екології. Розвиток нових технологій, методів управління та освітніх програм може сприяти створенню сталого та екологічно безпечного суспільства.

Для території України найхарактернішими є такі загрози:

1. Аварії на промислових, цивільних та військових об‘єктах, пов‘язаних із втратою надійності та стійкості конструкцій.

2. Аварії (катастрофи) на транспорті.

3. Пожежі, вибухи на промислових об‘єктах.

4. Пожежі в природних екосистемах.

5. Аварії з викидом (загрозою викиду) небезпечних хімічних речовин на об'єктах економіки (крім транспортних).

6. Метеорологічні надзвичайні ситуації.

7. Геологічні надзвичайні ситуації.

8. Отруєння людей.

9. Інфекційна захворюваність людей

4.2 Висновки до розділу

Аналіз загроз екологічної безпеки свідчить про те, що важливо вжити термінових заходів для збереження природи та забезпечення сталого розвитку.

Взаємодія суспільства, влади та підприємств у реалізації стратегій збереження навколишнього середовища може сприяти створенню екологічно безпечного майбутнього. Спільні зусилля на рівні глобального співтовариства є ключем до вирішення проблем, які ставлять під загрозу наше природне спадщину та екологічну безпеку.

ВИСНОВКИ

Після виконання завдань роботи було отримано наступне:

Проведено оцінку вразливостей та визначено результати впливу шкідливими факторами на інформаційні системи на основі стандарту ISO/IEC 27005, що дало можливість оцінити результат впливу через визначення контексту ідентифікації активів загроз та вразивостей.

Проаналізовано засоби та методи захисту загроз та інцидентів на основі моніторингу інформаційних систем, що дало можливість розробки та реалізації модуля моніторингу.

Розроблено та протестовано модуль моніторингу для сумісного використання систем SIEM та XDR, що дозволяє збирати, аналізувати та реагувати на події в інформаційній системі в реальному часі, що являється ключовим етапом у впровадженні превентивних заходів. Цей модуль дозволяє збирати, аналізувати та реагувати на події, що відбуваються в інформаційній системі в реальному часі.

Загальний підхід, спрямований на визначення ризиків, впровадження ефективних методів захисту та використання продуктивних систем моніторингу, допомагає організаціям побудувати стійку та високопродуктивну інформаційну безпеку. Це забезпечує вчасну реакцію на загрози, захист важливих активів та збереження надійності інформаційних систем в умовах постійного еволюційного середовища кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мазов Н. А., Ревнивых А. В., Федотов А. М. Классификация рисков информационной безопасности // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2011. Т. 9, вып. 2. С. 80–89.

2. Ревнивых А. В., Федотов А. М. Обзор политик информационной безопасности // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2012. Т. 10, вып.

3. С. 66–79. 3. Галатенко В. А. Основы информационной безопасности. М., 2004. 264 с.

4. Raúl Rojas, Ulf Hashagen. The First Computers: History and Architectures. MIT Press, 2002.

5. Камер Д. Сети TCP/IP. = Internetworking with TCP/IP. М.: Вильямс, 2003. Т. 1: Принципы, протоколы и структура.

6. Паркер Т., Сиян К. TCP/IP. Для профессионалов. 3-е изд. СПб.: Питер, 2004.

7. Вихорев С. В. Классификация угроз информационной безопасности. URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml.

8. Скрипник Д. А. Общие вопросы технической защиты информации. М.: ИНТУИТ.РУ Интернет-университет информационных технологий, 2004.

9. Цирлов В. Л. Основы информационной безопасности автоматизированных систем: Краткий курс. М.: Феникс, 2008.

10. Киреенко А. Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения // Молодой ученый. 2012. № 3.

11. Радько Н. М., Скобелев И. О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: Радио Софт, 2010.

12. Технические средства и методы защиты информации: Учебник для вузов / Под ред. А. П. Зайцева, А. А. Шелупанова. М.: Машиностроение, 2009.

13. Марков А.С., Цирлов В.Л. Управление рисками нормативный вакуум// Открытые системы. 2007. № 7.

14. Леденко С.А., Марков А.С. и др. О внедрении ГОСТ ИСО/МЭК 17799 и 27001// InformationSecurity. 2006. № 3/4.

15. ISO/IEC 27005:2011. Information technology Security techniques Information security risk management. Доступно на эл.ресурсе http://www.iso.org/iso/catalogue_detail?csnumber=56742.

16. ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ И ТЕНДЕНЦИИ ИХ РАЗВИТИЯ [Электронный ресурс] / Абдулкадыров Умалт Умарович – Электрон. дан. – Режим доступу: World Wide Web. – URL: https://cyberleninka.ru/article/n/tehnologii-informatsionnoy-bezopasnosti-kompyuternyh-setey-i-tendentsii-ih-razvitiya/viewer

17. Понятие и классификация угроз информационной безопасности в сети Интернет [Электронный ресурс] / Е.О. Напханенко – Электрон. дан. – Режим доступу: World Wide Web. – URL: https://cyberleninka.ru/article/n/ponyatie-i-klassifikatsiya-ugroz-informatsionnoy-bezopasnosti-v-seti-internet/viewer

18. MITRE ATT&CK [Электронный ресурс] – Режим доступу: World Wide Web. – URL:

https://attack.mitre.org/

19. CVE [Электронный ресурс] – Режим доступу: World Wide Web. – URL: https://cve.mitre.org/

20. Технологии и решения сетевой безопасности [Электронный ресурс] / Цыбенко О.С. – Электрон. дан. – Режим доступу: World Wide Web. – URL: https://cyberleninka.ru/article/n/tehnologii-i-resheniya-setevoy-bezopasnosti/viewer

21. CrowdStrike Global Threat Report [Электронный ресурс] - Режим доступу: World Wide Web. – URL: https://iitd.com.ua/wp-content/uploads/2023/03/crowdstrike2023globalthreatreport.pdf

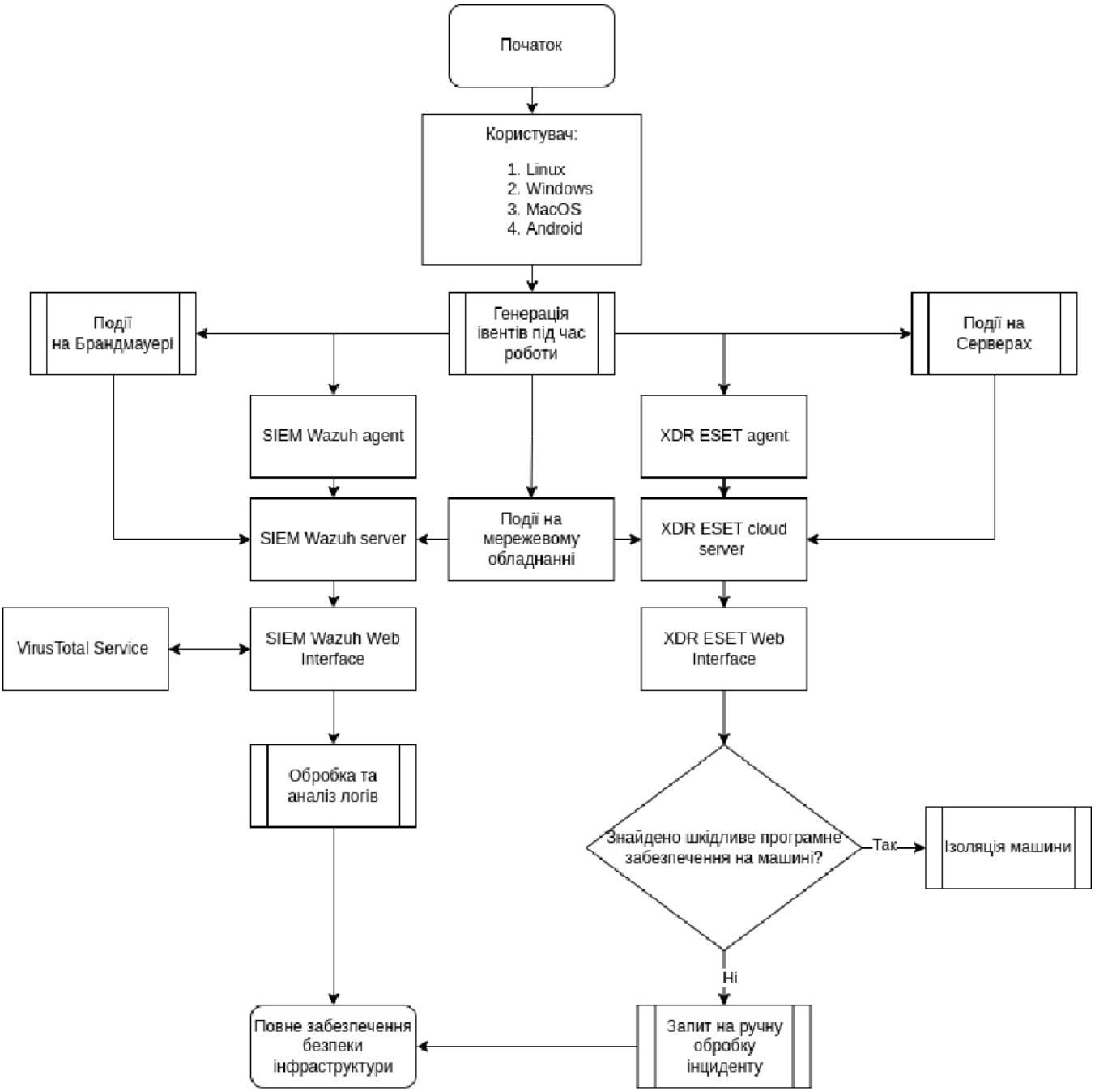
22. Picus The Red Report 2023 [Электронный ресурс] - Режим доступу: World Wide Web. – URL: https://iitd.com.ua/wp-content/uploads/2023/02/redreport2023-picus.pdf

23. Угрозы и атаки сетевой безопасности [Электронный ресурс] / Вартанян Артур Артурович – Режим доступу: World Wide Web. – URL: https://cyberleninka.ru/article/n/ugrozy-i-ataki-setevoy-bezopasnosti/viewer

24. Апробація роботи на V Міжнародну науково-практичну конференцію «Trends in science regarding the creation of new teaching methods». Іспанія, Мадрид, 16-18 жовтня 2023.

Додаток А

Алгоритм роботи модуля моніторингу



Додаток Б

Скрипт налаштувань Wazuh Manager

```
<!--
  Wazuh - Manager - Default configuration for ubuntu 22.04
-->
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>

  <!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->
  <logging>
    <log_format>plain</log_format>
  </logging>

  <remote>
    <connection>secure</connection>
    <port>1514</port>
    <protocol>tcp</protocol>
    <queue_size>131072</queue_size>
  </remote>

  <!-- Policy monitoring -->
```

```
  <rootcheck>
    <disabled>no</disabled>
    <check_files>yes</check_files>
    <check_trojans>yes</check_trojans>
    <check_dev>yes</check_dev>
    <check_sys>yes</check_sys>
    <check_pids>yes</check_pids>
    <check_ports>yes</check_ports>
    <check_if>yes</check_if>

    <!-- Frequency that rootcheck is executed - every 12 hours -->
    <frequency>43200</frequency>

    <rootkit_files>etc/rootcheck/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>etc/rootcheck/rootkit_trojans.txt</rootkit_trojans>

    <skip_nfs>yes</skip_nfs>
  </rootcheck>

  <command>
    <name>yara_linux</name>
    <executable>yara.sh</executable>
    <extra_args>-yara_path /usr/local/bin -yara_rules
/tmp/yara/rules/yara_rules.yar</extra_args>
    <timeout_allowed>no</timeout_allowed>
  </command>

  <active-response>
    <command>yara_linux</command>
    <location>local</location>
    <rules_id>100300,100301</rules_id>
  </active-response>

  <wodle name="cis-cat">
    <disabled>yes</disabled>
    <timeout>1800</timeout>
    <interval>1d</interval>
    <scan-on-start>yes</scan-on-start>

    <java_path>wodles/java</java_path>
    <ciscat_path>wodles/ciscat</ciscat_path>
  </wodle>
```

```
<!-- Osquery integration -->
<wodle name="osquery">
  <disabled>yes</disabled>
  <run_daemon>yes</run_daemon>
  <log_path>/var/log/osquery/osqueryd.results.log</log_path>
  <config_path>/etc/osquery/osquery.conf</config_path>
  <add_labels>yes</add_labels>
</wodle>

<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <ports all="no">yes</ports>
  <processes>yes</processes>

  <!-- Database synchronization settings -->
  <synchronization>
    <max_eps>10</max_eps>
  </synchronization>
</wodle>

<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<vulnerability-detector>
  <enabled>no</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
```

```
<provider name="canonical">
  <enabled>no</enabled>
  <os>trusty</os>
  <os>xenial</os>
  <os>bionic</os>
  <os>focal</os>
  <os>jammy</os>
  <update_interval>1h</update_interval>
</provider>

<!-- Debian OS vulnerabilities -->
<provider name="debian">
  <enabled>no</enabled>
  <os>buster</os>
  <os>bullseye</os>
  <os>bookworm</os>
  <update_interval>1h</update_interval>
</provider>

<!-- RedHat OS vulnerabilities -->
<provider name="redhat">
  <enabled>no</enabled>
  <os>5</os>
  <os>6</os>
  <os>7</os>
  <os>8</os>
  <os>9</os>
  <update_interval>1h</update_interval>
</provider>

<!-- Amazon Linux OS vulnerabilities -->
<provider name="alas">
  <enabled>no</enabled>
  <os>amazon-linux</os>
  <os>amazon-linux-2</os>
  <os>amazon-linux-2022</os>
  <update_interval>1h</update_interval>
</provider>

<!-- SUSE OS vulnerabilities -->
<provider name="suse">
  <enabled>no</enabled>
```

```
    <os>11-server</os>
    <os>11-desktop</os>
    <os>12-server</os>
    <os>12-desktop</os>
    <os>15-server</os>
    <os>15-desktop</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Arch OS vulnerabilities -->
  <provider name="arch">
    <enabled>no</enabled>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Alma Linux OS vulnerabilities -->
  <provider name="almalinux">
    <enabled>no</enabled>
    <os>8</os>
    <os>9</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Windows OS vulnerabilities -->
  <provider name="msu">
    <enabled>yes</enabled>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Aggregate vulnerabilities -->
  <provider name="nvd">
    <enabled>yes</enabled>
    <update_interval>1h</update_interval>
  </provider>

</vulnerability-detector>

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
```

```
<frequency>43200</frequency>

<scan_on_start>yes</scan_on_start>

<!-- Generate alert when new file detected -->
<alert_new_files>yes</alert_new_files>

<!-- Don't ignore files that change more than 'frequency' times -->
<auto_ignore frequency="10" timeframe="3600">no</auto_ignore>

<!-- Directories to check  (perform all possible verifications) -->
<directories>/etc,/usr/bin,/usr/sbin</directories>
<directories>/bin,/sbin,/boot</directories>

<!-- Files/directories to ignore -->
<ignore>/etc/mtab</ignore>
<ignore>/etc/hosts.deny</ignore>
<ignore>/etc/mail/statistics</ignore>
<ignore>/etc/random-seed</ignore>
<ignore>/etc/random.seed</ignore>
<ignore>/etc/adjtime</ignore>
<ignore>/etc/httpd/logs</ignore>
<ignore>/etc/utmpx</ignore>
<ignore>/etc/wtmpx</ignore>
<ignore>/etc/cups/certs</ignore>
<ignore>/etc/dumpdates</ignore>
<ignore>/etc/svc/volatile</ignore>

<!-- File types to ignore -->
<ignore type="sregex">.log$|.swp$</ignore>

<!-- Check the file, but never compute the diff -->
<nodiff>/etc/ssl/private.key</nodiff>

<skip_nfs>yes</skip_nfs>
<skip_dev>yes</skip_dev>
<skip_proc>yes</skip_proc>
<skip_sys>yes</skip_sys>

<!-- Nice value for Syscheck process -->
<process_priority>10</process_priority>
```

```
  <!-- Maximum output throughput -->
  <max_eps>50</max_eps>

  <!-- Database synchronization settings -->
  <synchronization>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <max_eps>10</max_eps>
  </synchronization>
</syscheck>

<!-- Active response -->
<global>
  <white_list>127.0.0.1</white_list>
  <white_list>^localhost.localdomain$</white_list>
  <white_list>127.0.0.53</white_list>
</global>

<command>
  <name>disable-account</name>
  <executable>disable-account</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>restart-wazuh</name>
  <executable>restart-wazuh</executable>
</command>

<command>
  <name>firewall-drop</name>
  <executable>firewall-drop</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>host-deny</name>
  <executable>host-deny</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
```

```
  <name>route-null</name>
  <executable>route-null</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>win_route-null</name>
  <executable>route-null.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>netsh</name>
  <executable>netsh.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<!--
<active-response>
  active-response options here
</active-response>
-->

<!-- Log analysis -->
<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
</localfile>

<localfile>
  <log_format>full_command</log_format>
  <command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\
\+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 == \3 ==
\4 \5/' | sort -k 4 -g | sed 's/ == \(.*\) ==/:\1/' | sed 1,2d</command>
  <alias>netstat listening ports</alias>
  <frequency>360</frequency>
</localfile>

<localfile>
  <log_format>full_command</log_format>
  <command>last -n 20</command>
```

```
    <frequency>360</frequency>
  </localfile>

  <ruleset>
    <!-- Default ruleset -->
    <decoder_dir>ruleset/decoders</decoder_dir>
    <rule_dir>ruleset/rules</rule_dir>
    <rule_exclude>0215-policy_rules.xml</rule_exclude>
    <list>etc/lists/audit-keys</list>
    <list>etc/lists/amazon/aws-eventnames</list>
    <list>etc/lists/security-eventchannel</list>

    <!-- User-defined ruleset -->
    <decoder_dir>etc/decoders</decoder_dir>
    <rule_dir>etc/rules</rule_dir>
  </ruleset>

  <rule_test>
    <enabled>yes</enabled>
    <threads>1</threads>
    <max_sessions>64</max_sessions>
    <session_timeout>15m</session_timeout>
  </rule_test>

  <!-- Configuration for wazuh-authd -->
  <auth>
    <disabled>no</disabled>
    <port>1515</port>
    <use_source_ip>no</use_source_ip>
    <purge>yes</purge>
    <use_password>no</use_password>

<ciphers>HIGH:!ADH:!EXP:!MD5:!RC4:!3DES:!CAMELLIA:@STRENGTH</cipher
s>
    <!-- <ssl_agent_ca></ssl_agent_ca> -->
    <ssl_verify_host>no</ssl_verify_host>
    <ssl_manager_cert>etc/sslmanager.cert</ssl_manager_cert>
    <ssl_manager_key>etc/sslmanager.key</ssl_manager_key>
    <ssl_auto_negotiate>no</ssl_auto_negotiate>
  </auth>

  <cluster>
```

```
    <name>wazuh</name>
    <node_name>node01</node_name>
    <node_type>master</node_type>
    <key></key>
    <port>1516</port>
    <bind_addr>0.0.0.0</bind_addr>
    <nodes>
        <node>NODE_IP</node>
    </nodes>
    <hidden>no</hidden>
    <disabled>yes</disabled>
  </cluster>

</ossec_config>

<ossec_config>
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/auth.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/syslog</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/kern.log</location>
  </localfile>

  <integration>
```

```
  <name>virustotal</name>

<api_key>2ca40b2bc9f45c2faf4e30276559362899a4578f9c5bedf221657001a51f6431</
api_key>
  <group>syscheck</group>
  <alert_format>json</alert_format>
  </integration>

</ossec_config>
```