# ВСТУП

*Актуальність дослідження.* В наш час все більше компаній та підприємств інформатизуються та реалізують в своєму робочому процесі нові цифрові технології. Це все призводить до того, що інформації стає все більше, так само як і загроз безпеки цієї інформації.

Слова кібератаки та кібербезпека все частіше можна зустріти в заголовках новин, або на афішах бізнес форумів чи в списках тем для обговорення на міжнародних самітах. Якщо на початку 21 століття захисту потребували лише великі корпорації та державно-військовий сектор то наразі це питання стоїть перед всіма людьми, що мають доступ до глобальної мережі.

Сучасні кібератаки постійно вдосконалюються та використовують більш складні методи, а їх реалізація спричиняє великі репутаційні та фінансові збитки або може загострювати політичні конфлікти чи навіть призвести до смерті людей. Під час кібератак використовують складні техніки та методи, особливо досвідченими та впливовими зловмисними угрупуваннями. Існує проблема розслідування кіберінцидентів, особливо тих, які пов’язані з складними атаками. Неповноцінне розслідування може призвести до повторення атаки або її неповної ліквідації. Це дозволяє зловмисникам залишатися прихованими та подовжити контроль над скомпрометованими інфраструктурами.

Організації в силу недооцінювання ризиків або через брак фізичних чи людських ресурсів не приділяють потрібної уваги до розслідувань. Зазвичай розслідування мають лише поверхневий характер і не мають на меті повністю дослідити зловмисну активність та її наслідки.

*Об’єкт дослідження* – процес проведення розслідування кіберінцидентів в сучасних інформаційно-телекомунікаційних системах.

*Предмет дослідження* – технологічний комплекс компанії ESET для розширеного виявлення та реагування на кіберінциденти.

*Мета роботи* – розробити технологію та методику розслідування кіберінцидентів та рекомендації щодо використання рішень компанії ESET для проведення розслідування.

*Наукові завдання:*

визначити принципи проведення розслідування кіберінцидентів в ІТС та проаналізувати основні проблеми під час розслідування та варіанти їх вирішення.

проаналізувати та дослідити рішення компанії ESET, їх архітектуру та функціонал;

проаналізувати процес розслідування інциденту за допомогою рішення ESET PROTECT&Inspect на прикладі симульованої атаки в тестовому середовищі;

проаналізувати автоматизацію процесу реагування та розслідування за допомогою інструментів компанії ESET;

розробити рекомендації для спеціалістів з інформаційної безпеки по проведенню розслідування на базі рішень компанії ESET.

*Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, побудова тестової платформи та симуляції кібератаки.

*Практичне значення одержаних результатів становлять собою* рекомендації для удосконалення методів та технологій проведення розслідувань кіберінцидентів на базі технологічного комплексу компанії ESET.

*Апробація результатів дипломної роботи*. Основні наукові та технічні аспекти теми магістерської роботи були представлені та обговорені на :

## 1.1. Огляд функцій та структури сучасних інформаційно-телекомунікаційних систем.

Перш за все потрібно зрозуміти, що таке інформаційно-телекомунікаційна система. У законі №81/94 Верховної Ради України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 є наступне визначення для інформаційно-телекомунікаційної системи:

Інформаційно-телекомунікаційна система (ІТС) — це сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле[1].

Спрощено ІТС можна описати на прикладі звичайної домашньої мережі де персональні пристрої, наприклад смартфон та ноутбук, є частиною інформаційної системи, а мережа маршрутизатора яка з’єднує ці пристрої між собою та з мережею інтернет, є частиною телекомунікаційної системи.

Інформаційно-телекомунікаційну систему можна розглядати з двох сторін:

- З точки зору функціоналу системи;
- З точки зору її структури;

З функціональної точки зору інформаційно-телекомунікаційна система - це сукупність технологічних систем та технологій для зберігання, обробки та передачі інформації. Функціонал ІТС визначається потребами організації в тих чи інших процесах обробки інформації. Ці потреби в свою чергу формують список технологій та технологічних систем які буде використовувати організація для забезпечення функціонування ІТС. Розгляд ІТС з функціонального боку має свої переваги, так як вся увага фокусується на тому, які технологічні комплекси будуть використовувати користувачі під час роботи. Такий підхід допомагає організаціям швидко підібрати програмне та апаратне забезпечення для повноцінного забезпечення бізнес-процесів,

власноруч або за допомогою експертів (найчастіше за допомогою системних інтеграторів).

Зі структурної точки інформаційно-телекомунікаційну систему можна розглядати як певну сукупність людей, процесів, моделей, технологій та інформації (даних) які формують комплексну структуру, основною метою якої є виконання певних функцій та завдань. Структурне визначення спирається на те, що ІТС є соціально-технічними системами, тобто системи, що складаються з людей, правил поведінки та технічних концепцій з якими працюють ці люди. Такий підхід допомагає побудувати норми поведінки працівників в рамках ІТС, що особливо важливо під час організації політик безпеки організації.

Будь-яка інформаційно-телекомунікаційна система під час своєї роботи отримує, зберігає та передає інформацію. Ці процеси потребують контролю, аналізу їх результату та проблем які можуть виникнути під час роботи.

Комп'ютери (в загальному розумінні кінцеві пристрої) є основними елементами ІТС в питаннях обробки і передачі інформації, однак вони є не єдиними компонентами. Кінцевий пристрій – це лише невелика частина складної і розгалуженої ІТС. Сучасні інфраструктури містять велику кількість інформаційних технологій які допомагають користувачам зручно і безпечно працювати в рамках ІТС.

Інформаційні технології широко визначають як сукупність програмно-апаратного забезпечення, що використовується в інфраструктурі. Ця сукупність включає спеціалізоване комунікаційне обладнання, обладнання для зберігання даних, програмне забезпечення для обробки даних та керування системами ІТС, кінцеві пристрої та інші системи. Інформаційні технології займають основне місце в структурі ІТС.

Ще один важливий компонент при роботі сучасних ІТС це комплексна система захисту інформації (КСЗІ). Комплексна система захисту інформації (КСЗІ) — це сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС. До складу КСЗІ входять заходи та засоби, які

реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін [2].

Захист інформації яка використовується та зберігається в сучасних ІТС дуже важливий, так як втрата цієї інформації або її модифікація можуть нанести великі репутаційні та матеріальні збитки компанії. Усі функції ІТС, а також її структура повинні бути захищені по всім стандартам політики безпеки організації, а сама політика безпеки повинна містити інформацію стосовно цих функцій та процесів.

## 1.2. Сутність сучасних кібератак та принципи реагування на кіберінциденти

Згідно Закону України "Про основні засади забезпечення кібербезпеки України":

**Кібератака** – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання

комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту.

**Інцидент кібербезпеки** (далі - **кіберінцидент**) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють ймовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів [3].

Мотиви у зловмисників для проведення кібератак можуть бути різними, це і матеріальні мотиви, так і ідеологічні або політичні. Зловмисники звісно можуть працювати поодинці, але зазвичай вони об'єднуються в угрупування.

Найбільш підготовлені і досвідчені угруповання називають APT (advanced persistent threat) - угрупування. APT-угрупування зазвичай підпорядковується державним спецслужбам або отримають фінансування від держави. Але є приклади угрупувань в яких не доведений зв'язок з державними органами і які є незалежними. Мета APT-угрупувань полягає в тому, щоб порушити безпеку урядів,

Рис. 1.1 Хронологія кібератак в Україні на початку 2022 року

високопоставлених осіб або стратегічних компаній, а також уникнути виявлення з метою отримання дуже конфіденційних даних. Наприклад, угруповання пов'язані з ГРУ росії проводили низку атак на державні ресурси України до початка та після повномасштабного вторгнення росії в Україну (рис. 1.1.) [4].

Ці групи володіють високим рівнем досвіду та значними ресурсами, серед яких методики, інструменти та експлойти для вразливостей нульового дня (вразливості, відомі зловмисникам, але які ще не оприлюднені та не виправлені).

Сучасні кіберзлочинці та APT-угрупування використовують все більш вишукані та складні методи атак. Дуже складно уявити в сучасних реаліях реалізацію таких атак як хробак Морріса або навіть атак на кшталт Not Petya. Більшість сучасних кібератак є багаторівневим, а первинні дії зловмисники все частіше маскується під нормально поведінку користувачів. Під час атак злочинці можуть використовувати велику кількість різних технік, кожна з яких може розглядатися як окремий

кіберінцидент. Спеціалісти із урядової команди CERT-UA визначили наступні категорії та типи інцидентів (рис. 1.2-6) [5]:

| Код xx | Категорія інциденту | Код xx | Тип інциденту | Тип інциденту англійською | Опис типу інциденту |
|---|---|---|---|---|---|
| 01. | Шкідливий (образливий) вміст (Abusive content) | 01. | Спам | Spam | Надсилання небажаних повідомлень або великої кількості повідомлень (флуд) |
| 02. | Шкідливий програмний код (Malicious Code) | 01. | Зараження шкідливим програмним забезпеченням (далі – ШПЗ) | Malware infection | У системі виявлено ШПЗ. |
| | | 02 | Розповсюдження ШПЗ | Malware distribution | Розповсюдження ШПЗ, наприклад шляхом розсилки повідомлень електронної пошти, що містятять вкладення з шпз або посилання на його завантаження. |
| | | 03 | Командно-контрольний центр (C2) | Command & Control (C2) | Система, яка використовується як точка керування та управління ботнетом та/або служить точкою для збору інформації, викраденої ботнетами. |
| | | 04 | Шкідливе підключення | Malicious connection | Спроби з'єднання від/ до IP/URL - адреси, пов'язаної з відомим ШПЗ, наприклад C2C або ресурсом розповсюдження компонентів, пов'язаних із активністю певної бот-мережі. |

Рис.1.2. Категоризації інцидентів від команди CERT-UA

| | | | | | |
|---|---|---|---|---|---|
| 03. | Збір інформації зловмисником (Information Gathering) | 01. | Сканування | Scanning | Збір інформації про системи або мережі. |
| | | 02 | Снiфінг | Sniffing | Несанкціоноване перехоплення (логічне або фізичне) та аналіз мережевого трафіку. Несанкціонований моніторинг та зчитування мережевого трафіку. |
| | | 03 | Фішинг | Phishing | Спроба збору інформації про користувача чи систему за допомогою методів соціальної інженерії (масова розсилка електронною поштою спрямована на збір даних, може містити посилання на фішингові сайти) |
| 04. | Спроби втручання (Intrusion Attempts) | 01 | Спроба експлуатації вразливості | Vulnerability exploitation attempt | Спроба вторгнення з використанням вразливості у системі, компоненті чи мережі |
| | | 02 | Спроби авторизації/ входу в систему | Login attempts | Спроба входу до служб або механізмів автентифікації / доступу. Невдала спроба підбору автентифікаційних даних чи використання раніше скомпрометованих вже не актуальних даних. |

Рис.1.3. Категоризації інцидентів від команди CERT-UA

| | | | | | |
|---|---|---|---|---|---|
| 05. | Втручання (Intrusion) | 01 | Компрометація облікового запису | Account compromise | Фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора |
| | | 02 | Компрометація системи | System compromise | Фактичне вторгнення в систему чи її компоненту, сервісу, застосунку через використання вразливості в компоненті або мережі. Несанкціонований доступ до системи або компоненту в обхід системи контролю доступу. |

Рис.1.4. Категоризації інцидентів від команди CERT-UA

| | | | | | |
|---|---|---|---|---|---|
| 06. | Порушення доступності (Availability) | 01 | Атака на відмову в обслуговуванні | DoS/DDoS | Вплив на нормальне функціонування системи чи сервісу що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів. |
| | | 02 | Саботаж / шкідливі дії | Sabotage | Дії (навмисні або ненавмисні), спрямовані на пошкодження системи, переривання процесів, зміну або видалення інформації тощо. |
| | | 03 | Збій | Outage, no malice | Збій в роботі системи чи її компоненту без зловмисного втручання. |
| 07. | Порушення властивостей інформації (Information Content Security) | 01 | Несанкціонований доступ до інформації | Unauthorised access to information | Несанкціонований доступ до інформації. Несанкціонований обмін конкретним набором інформації. |
| | | 02 | Несанкціонована модифікація | Unauthorised modification of info | Несанкціонована зміна або видалення певного набору інформації. |
| 08. | Шахрайство (Fraud) | 01 | Шахрайський сайт | Fraudulent site | Створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів. Використання ресурсів установи для цілей, відмінних від передбачуваних. |

Рис.1.5. Категоризації інцидентів від команди CERT-UA

| | | | | | |
|---|---|---|---|---|---|
| 09. | Відома вразливість (Vulnerable) | 01 | Вразливість | Vulnerability | Наявність в системі чи її компонентах відомих вразливостей, відкритих для експлуатації |
| | | 02 | Некоректна конфігурація | Misconfiguration | Недоліки в налаштуваннях, що можуть бути використані зловмисником (налаштування за замовчуванням тощо) |
| 10. | Інше (Other) | 01 | Невизначений інцидент | Undetermined incident | Недостатньо даних для обробки інциденту |

Рис.1.6. Категоризації інцидентів від команди CERT-UA

Зазначені кіберінциденти можуть бути як індикатором кібератаки так і подією не пов'язаною з атакою. Однак, будь-який кіберінцидент потребує реагування.

На кіберінциденти зазвичай реагують спеціалісти **SOC (Security Operations Center)**, який ще також називають **центром управління кібербезпекою**. Спеціалістів які працюють з кіберінцидентам називають **офіцерами безпеки**. Офіцери безпеки працюють з системою виявлення вразливостей і реагування на кіберінциденти та кібератаки, яка є основним інструментом для виявлення, реагування та розслідування кіберінцидентів та кібератак. **Система виявлення вразливостей і реагування на кіберінциденти та кібератаки** – це сукупність програмних та програмно-апаратних засобів, які забезпечують проведення цілодобового моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об’єктах кіберзахисту і можуть мати негативний вплив на їх стале функціонування [6].

Розглянемо механізм реагування на кіберінциденти. Під час моніторингу офіцери безпеки можуть побачити аномальну або підозрілу активність (яка могла бути заблокована або дозволена продуктами захисту). Офіцер безпеки аналізує це виявлення і вирішує чи було  це спрацювання хибним чи ні. Якщо спрацювання хибне, офіцер безпеки може зробити для нього виключення на майбутнє, а у випадку якщо спрацювання не хибне то офіцер безпеки може створити на його основі інциденти і далі займатися розслідуванням та діями по блокуванню активності зловмисників. Важливо зазначати, що більшість сучасних систем захисту інформації є автоматизованими, тому адміністратори таких систем повині моніторити як необроблені продуктом виявлення так і оброблені, щоб не пропустити первинні дії зловмисників.

## Аналіз проблеми розслідування кіберінцидентів

Розслідування кіберінцидентів - це важливий процес під час забезпечення комплексного захисту інформації. Розслідування завжди є частиною реагування на кіберінцидент, але може бути проведене як після ліквідації основної стадії атаки так і паралельно діям по блокуванню активності зловмисника. Важливо зазначити, що кожне розслідування є унікальним і підхід до нього визначається початковими умовами в яких знаходяться офіцери безпеки (інформацією яка відома про атаку, наявні ресурси та технології, тощо).

Для детального розуміння етапів розслідування, змоделюємо приклад атаки та подальшого її розслідування. Адміністратор безпеки компанії під час щоденного аудиту безпеки, побачив аномальну активність з комп'ютера бухгалтера. Аномальна активність полагала в тому, що на комп'ютері під користувачем запускалася команда nslookup, після якої користувач бухгалтера мав велику кількість спроб підключення до домен контролера по RDP за невелику кількість часу, наприклад, 120 спроб підключення за 2 хвилини. Зрозуміло, що в даному випадку можна припустити, що обліковий запис бухгалтера був скомпрометований і його використовував зловмисник для атаки повного перебору на контролер домену, задля отримання доступу до нього по RDP. Усю ці інформацію адміністратор безпеки передав офіцерам безпеки для подальшого розслідування.

В даному випадку, офіцери безпеки можуть провести розслідування наступним чином:

1. Ізолювати ПК бухгалтера від мережі для ліквідації подальших дій зловмисника та відключити обліковий запис бухгалтера у випадку якщо використовується домена автентифікація.

2. Зібрати системні журнали з скомпрометованого ПК за допомогою спеціальних інструментів, а також журнали з продуктів захисту, якщо такі присутні на даному ПК.

3. Проаналізувати спрацювання в системах моніторингу та в системах захисту, якщо такі присутні і проаналізувати журнали які були зібрані з скомпрометованого ПК.

4. Підготувати звіт на основі знайденої інформації та запланувати дії по відновленню та посиленню захисту.

Зрозуміло, що це лише приблизний і основний план дій який може бути використаний при розслідуванні. В цей план можна додати ще багато чого, наприклад, впровадження додаткових технологічних комплексів для розслідування та захисту або залучення додаткових спеціалістів до розслідування, але подібні дії є ситуаційними і в даному випадку офіцери могли обійтися і без них.

Як можна побачити, результатом розслідування зазвичай є певний звіт який може містити наступне:

- Дані по скомпрометованим під час атаки системам, ресурсам, обліковим записам користувачів, тощо;
- Ресурси, методи, техніки та інструменти які були використані зловмисниками під час атаки;
- Набір вразливостей які були використані зловмисниками для реалізації атаки;
- Набір дій які були виконані офіцерами безпеки під час розслідування;
- Хронологію подій атаки;
- Набір рекомендацій для покращення стану безпеки організації;

У випадку масштабних атак або атак нульового дня, подібні звіти будуть виглядати як повна хронологія подій до атаки, під час неї і після. Цю інформацію офіцери безпеки використовують для подальшого реагування на кіберінцидент, наприклад, для модернізації інфраструктури для запобігання подібних атак в

майбутньому та для ліквідації наслідків та “залишків” атак або для формування рекомендацій для інших спеціалістів, щоб вони отримали досвід з реагування на подібні атаки [7].

Сучасні кібератаки можуть нанести дуже великої репутаційної або матеріальної шкоди компанії але, на жаль, компанії не завжди коректно реагують на індикатори компрометації і починають реагувати на атаки і розслідувати їх пізніше ніж треба. Загалом проблеми при розслідуваннях можна розділити на три категорії, а саме проблеми пов'язані з людським фактором, технологічні проблеми та непередбачувані проблеми.

Проблеми з людським фактором – це проблеми пов'язані з компетенцією експертів з інформаційної безпеки та комунікацією спеціалістів на підприємстві. До таких проблем можна віднести:

- Складну ієрархію на підприємстві, яка накладає дуже багато обмежень в свободі дій під час розслідування
- Недостатня кількість експертів з кібербезпеки для розслідування або їх недостатня компетенція.
- Некоректну оцінку ризиків компанією і подальше ігнорування кібератаки.
- Високий рівень бюрократії, особливо у державних підприємствах, який уповільнює розслідування.

Вирішувати такі проблеми можна по різному, наприклад, залучаючи спеціалістів сторонніх компаній або залучення державного органу контролю який би покращив процес комунікації під час розслідування.

Технологічні проблеми – це проблеми з технологічним забезпеченням компанії або з втратою, не доступністю чи нестачею інформаційних даних для розслідування. До таких проблем можна віднести:

- Відсутність технологічних комплексів для реагування та розслідування кіберінцидентів які б збирали дані про атаку.

- Відсутність журналів подій внаслідок їх видалення зловмисниками або внаслідок недостатнього рівня логування.
- Несвоєчасне виявлення атак через недосконаліть продуктів моніторингу та захисту.

Зазвичай вирішенням подібних проблем є впровадження нових технологічних комплексів для розслідування та відновлення інформаційних журналів для розслідування. В випадку, якщо атака була помічена несвоєчасно, офіцери безпеки можуть розслідувати залишки атаки, для розуміння дій які могли зробити зловмисники.

Непередбачувані проблеми – це ситуації які не піддаються прогнозуванню але можуть трапитись під час розслідування та вплинути на його проведення. Такі ситуації можуть бути різного роду походження, наприклад, повне відключення електроенергії або вихід з ладу апаратного забезпечення компанії. Вирішення подібних ситуацій може бути прописане в політиках безпеки організації але зазвичай вирішення є ситуативним.

**Висновок до Розділу 1:**

Сучасні ІТС є структурно складними системами які потребують багаторівневого захисту та впровадження продуманої КСЗІ. При розроблені КСЗІ треба розуміти принципи та методики які використовують сучасні зловмисники та APT-угрупування, а також розуміти з якими кіберінцидентами може зіштовхнутися система захисту та спеціалісти які її обслуговують.

Аналіз проблем розслідування кіберінцидентів показав, що хоч в даному напрямку існує багато проблем, які пов’язані як з людським фактором так і з технологічним, однак ці проблеми мають вирішення при правильному підході. Можна зробити висновок, що розслідування кіберінцидентів потребують спеціального підходу як зі сторони підбору людей які будуть з ними працювати, так і зі сторони

технологічних комплексів які будуть використовуватися під час роботи з кіберінцидентами.

# 2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РЕАГУВАННЯ ТА РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ НА БАЗІ РІШЕНЬ ESET

## 2.1. Функціонал та архітектура централізованої системи керування та управління кіберінцидентам на базі рішення ESET PROTECT & Inspect

**ESET PROTECT&Inspect** — це рішення, яка дозволяє централізовано та дистанційно керувати продуктами ESET на робочих станціях, серверах і мобільних пристроях у мережевому середовищі та захищати кінцеві пристрої. ESET PROTECT&Inspect використовує архітектуру клієнт-сервер, де клієнти (віддалені кінцеві точки) запитують і отримують відповіді від центрального сервера. Сервер чекає запити від клієнтів і потім відповідає на них. В ідеалі сервер надає клієнту стандартизований прозорий інтерфейс, щоб клієнту не потрібно було знати подробиці системи (тобто апаратного та програмного забезпечення), що надає послуги. Клієнти зазвичай розташовані на робочих станціях або ПК, тоді як сервери розташовані в інших місцях мережі, зазвичай на більш потужних машинах. Ця модель обчислень особливо ефективна, коли клієнт і сервер регулярно виконують різні завдання. Оскільки клієнтський і серверний комп'ютери вважаються окремими пристроями, клієнт-серверна модель суттєво відрізняється від старої моделі, де централізований мейнфрейм обробляв усі пов'язані з ним завдання.

Визначаючи клієнт-серверні системи як масштабовані, деякі аналітики стверджують, що одноранговий зв'язок є більш гнучким і універсальним для керування непередбачуваними навантаженнями. Експерти говорять про такі речі, як резервування та зони доступності та відновлення після збоїв як спосіб підтримувати роботу бізнес-систем в режимі онлайн, незважаючи на зміни вимог або інші проблеми.

### 2.1.1. Архітектура ESET PROTECT

ESET PROTECT дозволяє з єдиного центру керувати продуктами ESET на робочих станціях, серверах і мобільних пристроях, які працюють у мережі.

Щоб зрозуміти принципи роботи системи ESET PROTECT, важливо ознайомитися з функціональними можливостями її окремих компонентів і тим, як вони взаємодіють один з одним [8].

Одним з обов'язкових компонентів є **сервер ESET PROTECT**. Це програма, яка обробляє всі дані, отримані від клієнтів, які підключаються до нього. Сервер ESET PROTECT обробляє всі дані, отримані з клієнтських комп'ютерів, і управляє клієнтами із розгорнутим рішенням ESET Management Agent. Роль сервера полягає в тому, щоб виступати центральним пунктом управління та моніторингу. Усе середовище налаштовується з одного сервера. Немає необхідності підключатися до іншого сервера, щоб налаштувати певну частину мережі. Сервер ESET PROTECT можна встановити як на сервери Windows, так і на Linux, а також він поставляється як віртуальний пристрій.

Серверу необхідний сервер баз даних для обробки та зберігання даних. Уся інформація зберігається в базі даних, зокрема це налаштування сервера, політики, групи, завдання, журнали, сертифікати тощо. Сервер баз даних можна встановити на тому ж комп'ютері або розмістити на окремій спеціальній машині. Якщо за певних обставин сервер ESET PROTECT аварійно завершить роботу, можна встановити новий екземпляр сервера і підключити його до вихідної бази даних та відновити попередній стан сервера. Підтримуються сервери баз даних MS SQL та MySQL. За замовчуванням сервер інсталюється разом із MS SQL Server Express.

Ще одним обов'язковим компонентом є **веб-консоль ESET PROTECT**. Веб-консоль є інтерфейсом для сервера ESET PROTECT. Вона працює на веб-сервері Apache Tomcat. До веб-інтерфейсу веб-консолі можна отримати доступ за допомогою

будь-якого браузера та з будь-якого пристрою мережі. Якщо зробити веб-сервер доступним через Інтернет, ESET PROTECT можна використовувати будь-де та з будь-якого пристрою з підключенням до Інтернету.

Третім обов'язковим компонентом є **ESET Management Agent**. Це проста, високомодульна та полегшена служба, яка охоплює всі з'єднання між сервером ESET PROTECT та будь-яким продуктом ESET або операційною системою. Агент автономний, тому гарантує швидке та ефективне реагування на інциденти безпеки, що відбуваються на клієнтському комп'ютері. ESET Management Agent є важливою частиною ESET PROTECT.

Агент це проста полегшена служба, яка охоплює всі з'єднання між сервером та будь-яким продуктом ESET або операційною системою. Продукт безпеки ESET не взаємодіє безпосередньо із сервером ESET PROTECT, а використовує Агент для передачі будь-якої інформації на сервер. Комп'ютер або операційна система з встановленим належним чином та підключеним Агентом називається «керованими».

ESET Management Agent також відповідає за застосування будь-яких налаштувань та виконання дій на основі тригерів, визначених на сервері. При цьому, не потрібно чекати з'єднання з сервером, а потім отримувати команди для обробки конкретних ситуацій, таких як виявлення вірусів, відсутність оновлення операційної системи тощо, він зберігає команди локально і може миттєво реагувати. Тобто ESET Management Agent є автономним. Серед переваг ESET Management Agent можна виділити такі:

- Просте налаштування - можливе розгортання агента як стандартної корпоративної програми.
- Оперативне управління безпекою. Оскільки Агент може бути налаштований на зберігання декількох сценаріїв безпеки, час реакції на загрози значно скорочується.
- Управління безпекою в режимі офлайн. Агент може реагувати на подію, навіть якщо він не підключений до сервера ESET PROTECT у цей момент.

Крім основних компонентів ESET PROTECT також має низку додаткових компонентів які можуть додати додаткових функцій серверу або полегшити роботу деяких функцій. Одним з таких додаткових компонентів є **ESET Bridge**. Це HTTP проксі-сервер який може виконувати наступні функції:

- Завантаження та кешування: Оновлення модулів ESET, пакети інсталяції й оновлення, просунуті ESET PROTECT (наприклад, інсталятор MSI ESET Endpoint Security), оновлення продуктів ESET для захисту (оновлення компонентів і продуктів), результати ESET LiveGuar
- Переспрямування обміну даними з агентами ESET Management на сервер ESET PROTECT.

**RD Sensor** – це додатковий компонент, який допомагає ідентифікувати комп’ютери в локальній мережі. За замовчуванням це пасивний датчик, який виявляє мережеві пристрої. Отримана інформація передається на сервер ESET PROTECT. Сервер оцінює, чи знайдені датчиком пристрої невідомі чи вже є керованими. На інформаційній панелі веб-консолі присутні Звіти RDS.

**Mobile Device Connector** – це компонент, що забезпечує підключення мобільних пристроїв Android та iOS до сервера ESET PROTECT для управління ними та для адміністрування ESET Endpoint Security для Android (рис. 2.1.).

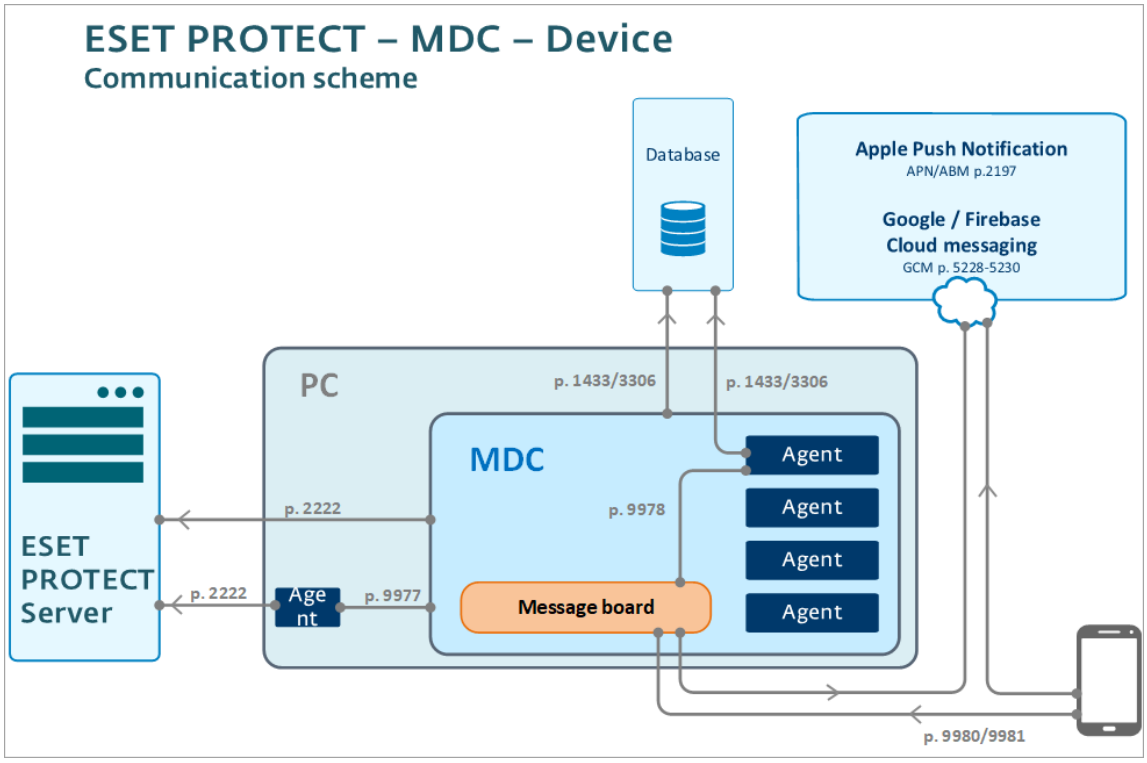



Рис. 2.1. Схема архітектури Mobile Device Connector

Він тимчасово зберігає дані від клієнтів та дані про них у власній базі даних. Mobile Device Connector служить хостом для віртуальних агентів мобільних пристроїв. Це означає, що агенти не встановлюються безпосередньо на мобільних пристроях.

Як показано на схемі (рис. 2.2.), ESET PROTECT складається з безлічі компонентів, і вся система досить складна.

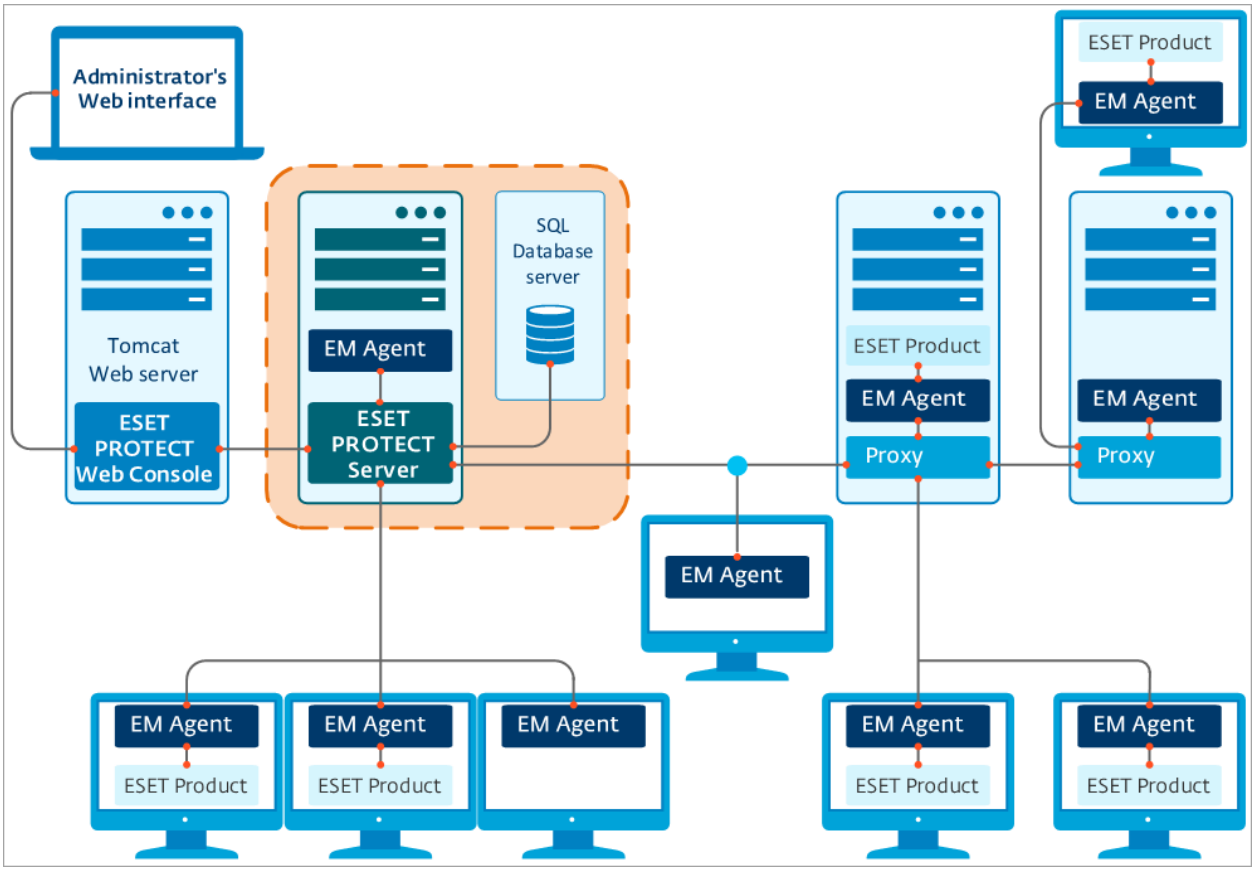



Рис 2.2. Схема архітектури рішення ESET PROTECT

### 2.1.2. Функціонал та інструменти адміністрування в ESET PROTECT

ESET PROTECT має велику кількість вбудованих інструментів які допомагають адміністраторам керувати кінцевими точками та отримувати інформацію про них у зручному вигляді. Основною при роботі з цими інструментами є веб-консоль ESET PROTECT, саме через яку виконується керування всіма клієнтами. Для зручності, функції і інформації в веб-консолі розподілена по вкладкам-категоріям, які націлені на полегшення роботи з ESET PROTECT. Основними вкладками є Панель інструментів, Комп'ютери, Виявлені об'єкти, Звіти, Завдання, Політики та Сповіщення. Розглянемо більш детально кожну з них.

**Панель Інструментів** – це інформаційна вкладка на які можна побачити дуже багато корисної інформації (Рис. 2.3.). Інформація на цій вкладці представлена у вигляді текстових та графічних звітів які розбиті по категоріям. Адміністратори консолі керування можуть використовувати як вбудовані панелі та звіти так і створювати власні на основі як вбудованих так і власних звітів [9].

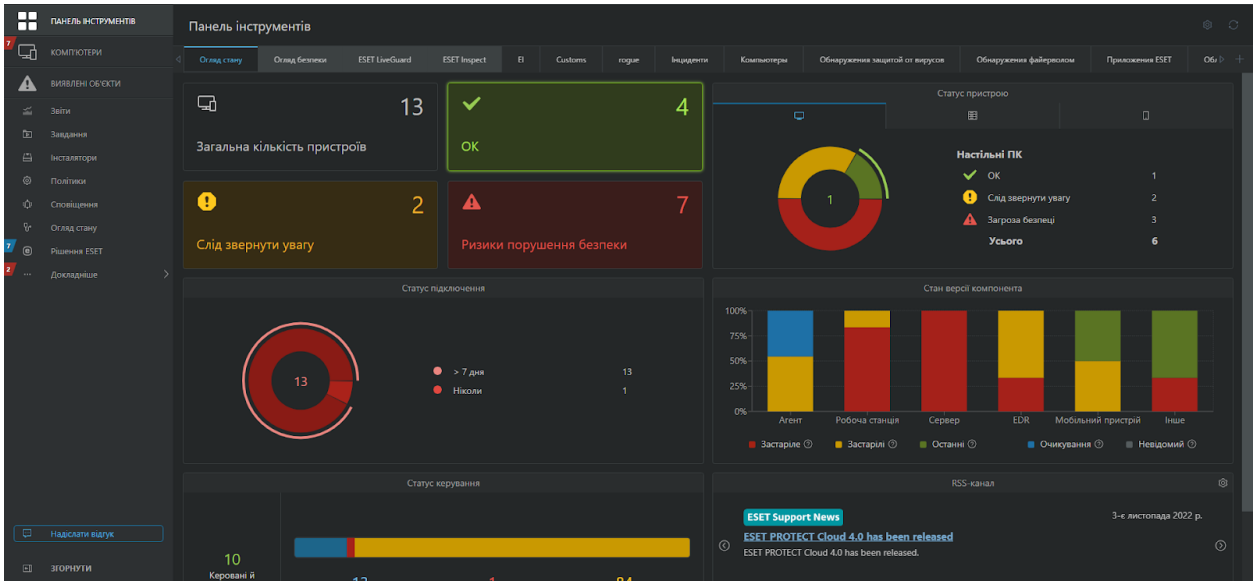



Рис. 2.3. Панель інструментів ESET PROTECT

Вкладка **Комп'ютери** відображає основну інформацію про комп'ютери які підключені до консолі керування та про ті Комп'ютери які відомі консолі але ще не мають агента керування. Дана вкладка дозволяє фільтрувати комп'ютери за певними

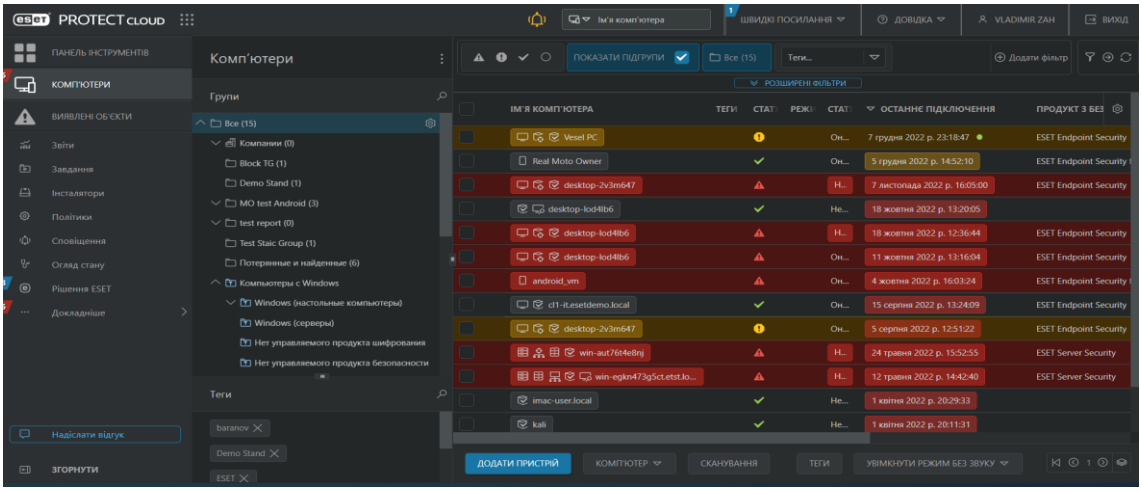



Рис. 2.4. Панель управління Комп'ютерами ESET PROTECT

умовами керувати ними та за потреби відкривати більш детальну інформацію про комп’ютер (рис. 2.4.).

Вкладка **Виявлені Об'єкти** відображає основну інформацію про виявлення які здійснили моделі продукту захисту або рішення і сет інспектор (рис. 2.5.). Тут адміністратор консолі керування може аналізувати виявлені об’єкти, помічати їх як оброблені або необроблені, та за потреби зробити виключення. Виключення дозволяють виключити об’єкт зі сканування та виявлення за наступними параметрами ім’я загрози, точна хеш сума файлу який був виявлений, або шлях до файлу та ім'я загрози загрози яка була виявлена.

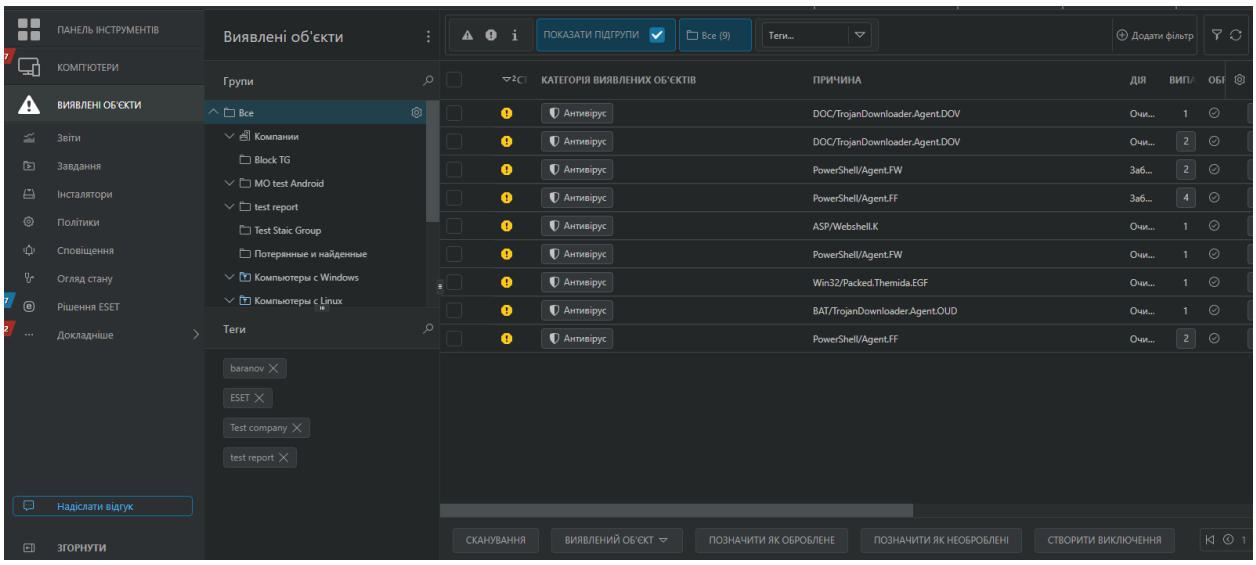



Рис. 2.5. Огляд Виявлених об’єктів

Вкладка **Звіти** відповідає за створення та використання звітів які допомагають адміністратором консолі керування отримувати актуальну інформацію про продукти

захисту, інфраструктуру компанії, виявлення об’єкти, тощо. Адміністратори консолі можуть використовувати як вбудовані звіти (які представлені у декількох категоріях) так і створювати нові категорії і звіти за потреби. Звіти можуть бути завантажені у форматах CSV та PDF або відправлені електронною поштою адміністратору. Формування та надсилання звітів можна запланувати (рис. 2.6.).

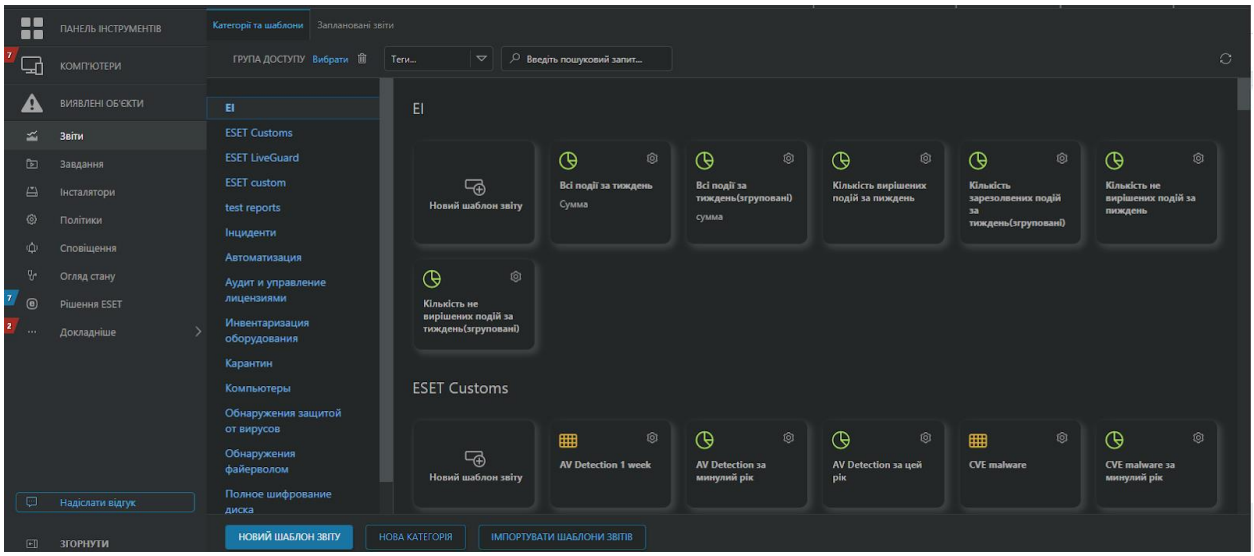


Рис. 2.6. Вкладка Звіти в ESET PROTECT

В вкладці **Завдання** адміністратори консолі можуть створювати клієнтські та серверні задачі які є основним інструментом керування кінцевими точками та продуктами захисту які на них встановлені. За допомогою задач адміністратор може, наприклад, встановити нову версію продукту захисту, запустити сканування на кінцевій точці, запустити командний рядок з визначеними параметрами, та багато іншого. За запуск завдань відповідають так звані тригери. Тригери можуть бути одноразові, регулярними або специфічними.

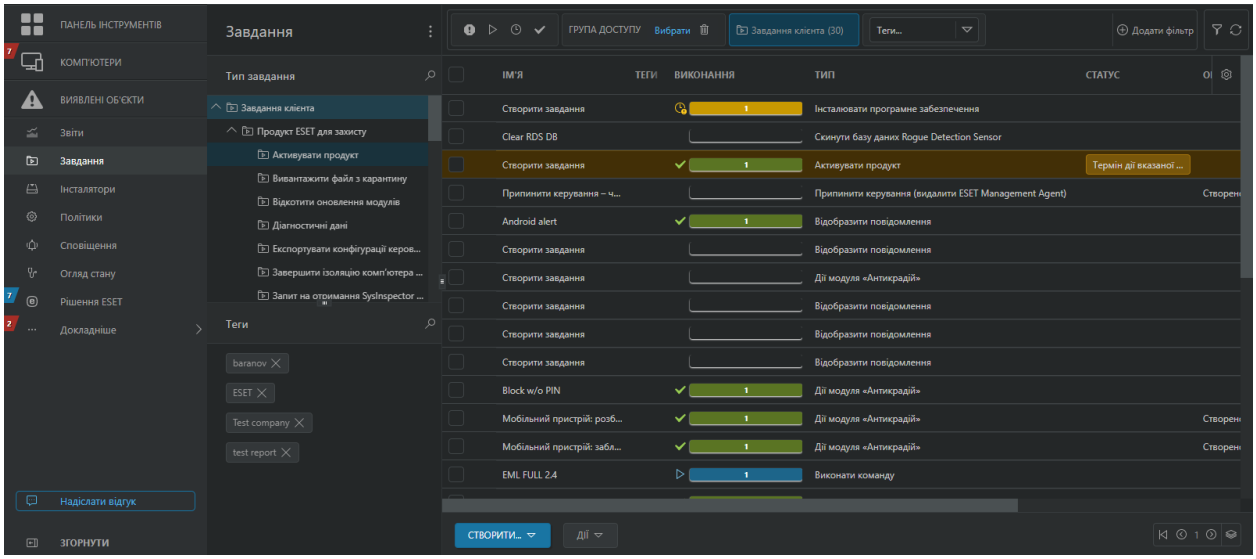



Рис. 2.7. Приклад списку завдань в ESET PROTECT

Вкладка **Політики** відповідає за політики налаштувань продуктів компанії ESET. Адміністратор може застосувати певні конфігурації за допомогою політик що дозволяє не налаштовувати продукти на кожній кінцеві точці окремо (рис. 2.8.). Політики можуть бути застосовані на статичні динамічні групи або на окремі комп'ютер. Кожен комп'ютер може мати довільну кількість політик.

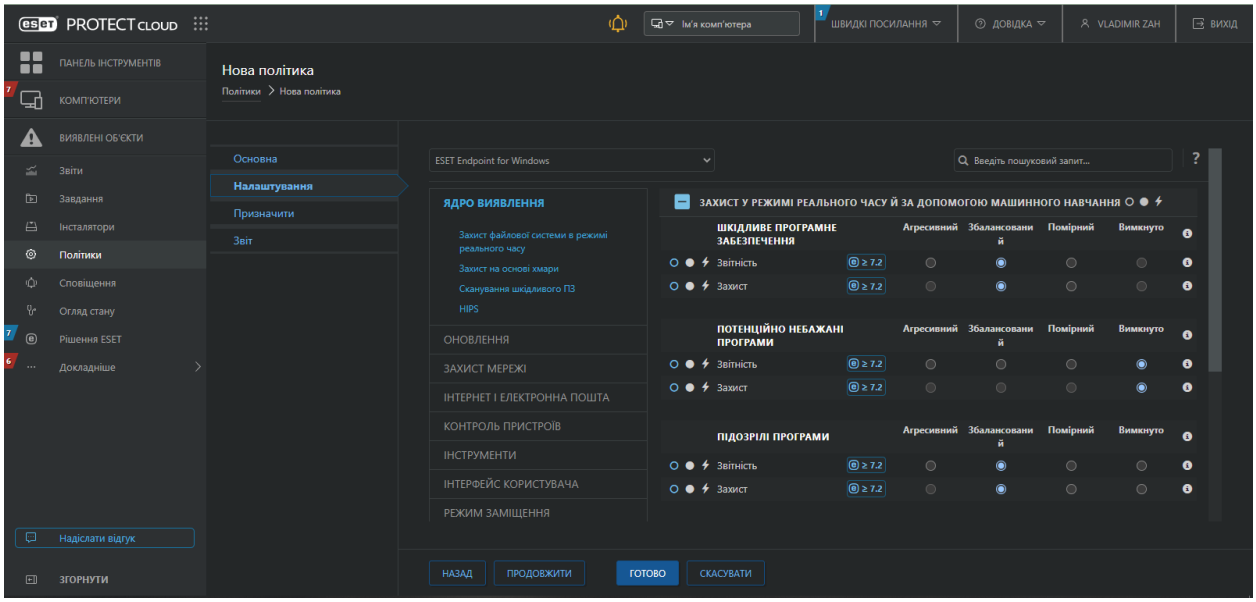



Рис. 2.8. Приклад налаштування політики для ESET Endpoint Security

У вкладці **Сповіщення** адміністратор Адміністратор консолі може створити або використати вже створені сповіщення. За наявності відповідних параметрів сповіщення попереджає, коли щось, що потребує уваги адміністратора. ESET PROTECT пропонує широкий спектр попередньо визначених шаблонів сповіщень, які можна увімкнути або вимкнути, та розповсюджувати на обрані адреси електронної пошти. Сповіщення можна використовувати по факту членства в певних динамічних групах або виконувати за специфічними показаннями, наприклад, активні загрози, застаріла операційна система, застарілий продукт безпеки, низька ємність накопичувачів, та іншими подіями (рис. 2.9.).

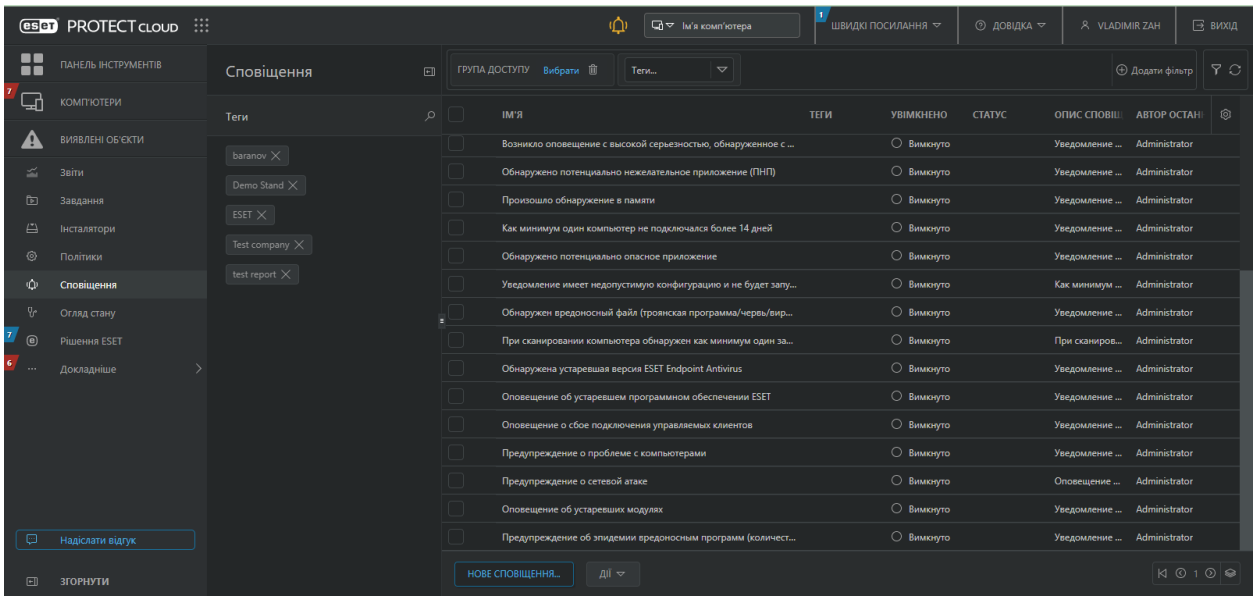


Рис. 2.9. Вбудовані сповіщення ESET PROTECT

## 2.2.. Архітектура та функціонал рішення ESET Inspect

Сучасні системи захисту кінцевих точок не можуть гарантувати стовідсоткової безпеки. Зловмисники можуть використовувати невідоме ШПЗ, загрози нульового

дня, тощо. Для якісного моніторингу фахівцям з безпеки потрібні спеціалізовані інструменти з моніторингу та реагування. Одним з таких інструментів є системи розширеного виявлення та реагування (XDR – Extended detection and response).

Основною задачею XDR є моніторинг діяльності в мережі компанії та реагування на аномальну та шкідливу діяльність на кінцевих точках. За допомогою XDR команда SOC може відслідити спроби атак на кінцевих точках інфраструктура. На відміну від SIEM систем, XDR дає можливість не тільки моніторити та виявляти аномальну та зловмисну активність, а також блокувати та досліджувати її. В порівнянні з SIEM системами, XDR є більш зручними в управління та має набагато менший рівень помилкових спрацювання, що підвищує ефективність рішення і стан захищеності інфраструктур [10].

XDR допомагає виявляти складні загрози та цілеспрямовані атаки, атаки з невідомими інструментами та шкідливим програмним забезпеченням, без файлові атаки, компрометацію облікових записів та інші типи атак. Функціонал XDR залежить від постачальника і може включати різні технологічні розробки, що працюють в автоматичному, напівавтоматичному або ручному режимі і мати інструменти які дозволяють розширити функції офіцерів безпеки.

В основі кожного XDR рішення основним компонентом є дані які допомагають створити глобальне розуміння того що відбувається на кінцевих пристроях компанії та створити хронологію подій які були під час кібератаки. Можна виділити 2 функції з даними в системах

По-перше це збір даних які проводить система. Системи збирають дані в режимі реального часу не заважаючи бізнес-процесами на кінцевих точках. Ці дані включають в себе більшість інформації з кінцевої точки, такої як інформація про системні процеси, моменти передачі даних, мережеві з’єднання та інше. Обробка цих даних допомагає системі виявити аномально та шкідливу поведінку яка може бути індикатором кібератак.

Друга функція це зберігання даних та їх обробка рішенням. Оскільки система зазвичай збирають дуже велику кількість даних з кінцевих пристроїв то рішення класу потребують дуже багато ресурсів для обробки та зберігання цих даних. Чим більше ресурсів є організації для зберігання та обробки даних тим довше організація може зберігати дані з кінцевих пристроїв

Важливо зазначити що навіть автоматичні системи потребують людського контролю. Дані які агрегуються системою повинні аналізуватися та оброблятися в режимі реального часу як за допомогою автоматичних технологій так і за допомогою експертизи, яка зазвичай проводиться фахівцями з інформаційної безпеки. Система також може використовувати технології машинного навчання для того щоб виявляти не тільки аномальну поведінку, ай типову поведінку організації що дозволяє створювати виключення та фільтрувати дані. Аномальна та шкідлива поведінка потребує реакції. Система може виконувати різні дії по блокуванню та ліквідації загроз. Це можуть бути такі дії як блокування виконуваних файлів, блокування мережевих з'єднань кінцевої точки або блокування файлів по їх хеш суммы.

XDR системи як інструмент безпеки дуже сильно розширюють можливості SOC команди оскільки вони здатні виявляти ти реагувати на аномально та шкідливу діяльність, а також збирають дані з різних рівнів кінцевої точки, що дуже допомагає при розслідуванні кіберінцидентів. XDR в значній мірі засновані на правилах, але машинне навчання або методи штучного інтелекту поступово знайшли свій шлях у ці системи, щоб полегшити пошук нових закономірностей і кореляцій. XDR розширює антивірусні можливості, оскільки XDR ініціює сповіщення, коли виявить аномальну поведінку. Тому XDR може виявити невідомі загрози та запобігти їх до того, як вони стануть шкідливими через поведінку, а не лише через підписи.

ESET Inspect (далі EI) – це XDR система для забезпечення найвищого рівня безпеки інфраструктури та розслідування кіберінцидентів. ESET Inspect дозволяє виявляти, досліджувати кіберінциденти та реагувати на них. ESET Inspect збирає дані в режимі реального часу на кінцевих пристроях. Потім ці дані зіставляються з набором

правил для автоматичного виявлення підозрілих дій. Агреговані дані обробляються, а інформація розставляється за пріоритетами та корелюється у зручну форму для подальшого пошуку. Оброблені дані дозволяють офіцерам безпеки ефективніше шукати аномальні та підозрілі дії, а також забезпечують точне реагування на інциденти, управління та звітування [11].

EI базується на 3 компонентах:

**ESET Inspect Server** – це сервер який обробляє і зберігає дані з кінцевих пристроїв та відображає їх у веб консолі.

**ESET Inspect Web Console** – це Web інтерфейс який допомагає адміністратором більш зручніше керувати рішенням.

**ESET Inspect Connector** – це агент який збирає дані на кінцевих пристроях та виконує дії прописані в правилах, наприклад, блокування програмного забезпечення на основі цифрового підпису компанії. ESET Inspect Connector який збирає дані Про всі операції в операційній системі в режимі реального часу на кінцевих пристроях З встановленим продуктом захисту ESET. Потім ці дані, які ще іменують Raw Events (Data), обробляються сервером Inspect за допомогою вбудованих та власноруч створених правил.

Для коректної роботи EI в організації потрібний розгорнутий сервер ESET PROTECT. Сервер EI потребує прямого підключення до сервера захисту ESET, для автентифікації користувачів (рівень доступу користувача в EI визначається в ESET PROTECT), обміну структурою комп'ютерів/груп, а також для посиленої безпеки (рис. 2.10.)

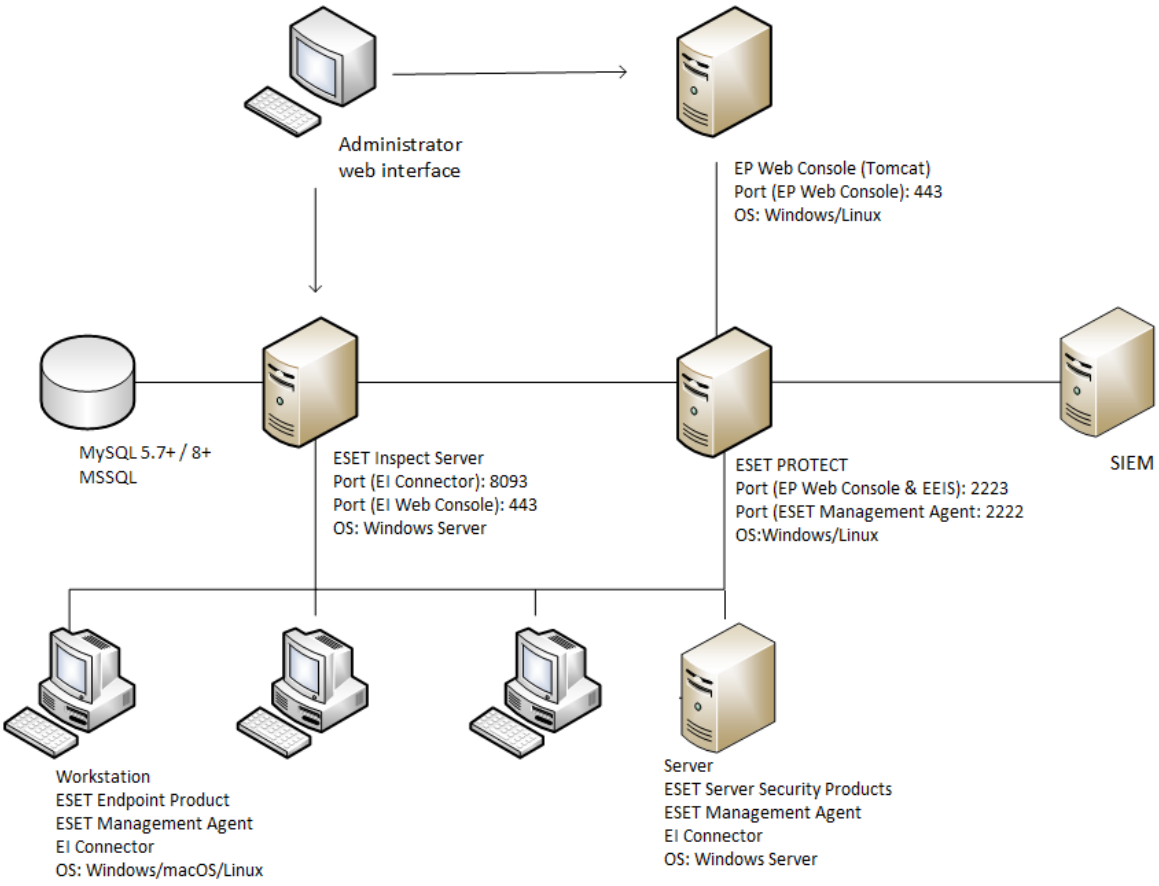



Рис. 2.10. Схема архітектури рішення ESET Inspect

Рівень довіри за допомогою сертифікатів і зашифрованого зв'язку є частиною екосистеми, де агентам необхідно довіряти серверу, якому вони повідомляють інформацію, щоб запобігти будь-якому чутливому витоку даних. Сертифікати надаються ESET PROTECT. ESET PROTECT також використовується для розгортання та оновлення агента EI, розповсюдження ліцензій, сповіщень та інтеграції функції виявлення з базою даних ESET PROTECT (виявлення які генерує EI потрапляють до вкладки Виявлення в ESET PROTECT), що дозволяє подальше створення звітів. Кожне виявлення EI включає пряме посилання, яке переміщується безпосередньо до конкретного об'єкта в консолі EI.

**Панель Інструментів (Dashboard)** забезпечує огляд стану мережі з урахуванням роботи EI. Вона показує хронологію виявлень (на основі їх критичності), які показують, чи знаходиться мережа під потенційною або існуючою атакою, і які виявлення були знайдені.

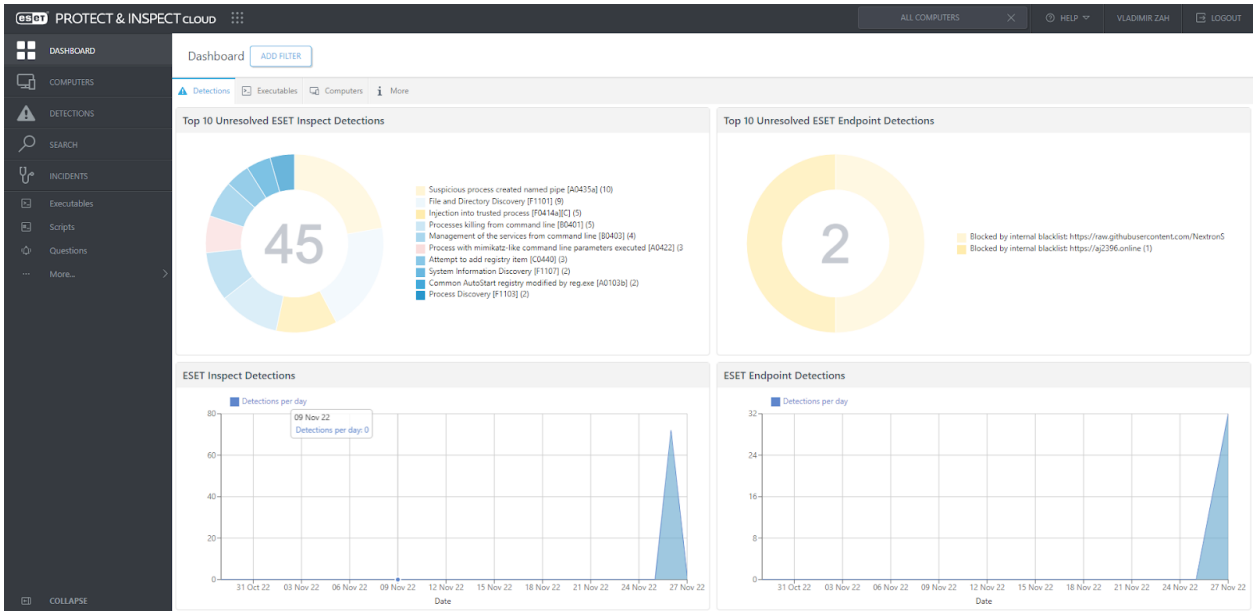



Рис. 2.11. Вкладка Detections

Друга вкладка Executables показує перегляд виконуваних файлів, які відображають підозрілу поведінку, згруповану за кількістю виявлень (всього і унікальних), які вони запустили (рис. 2.12.).

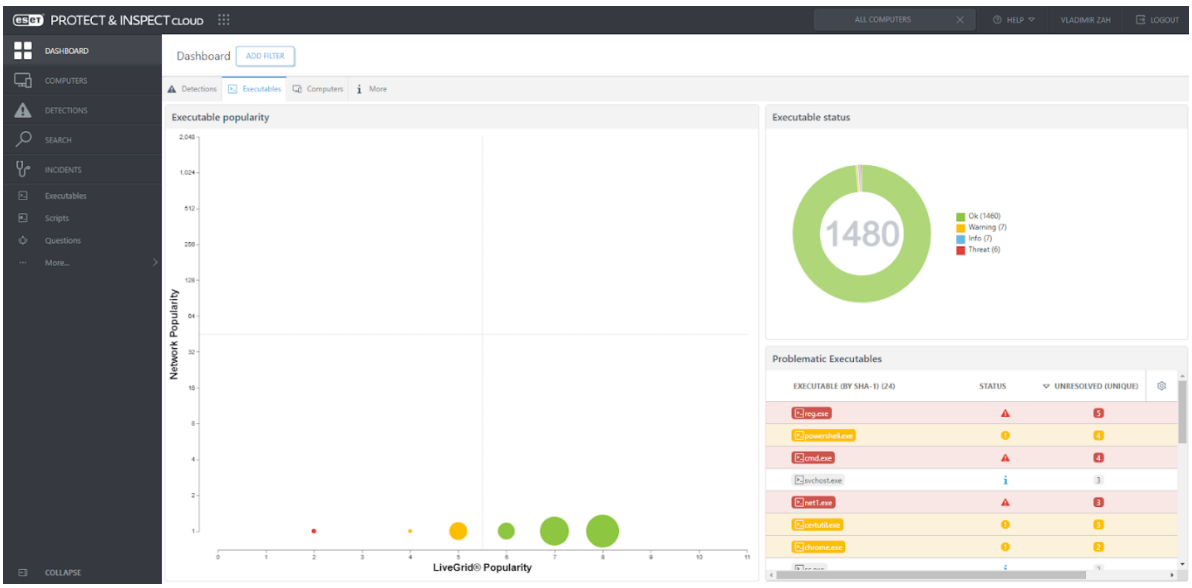



Рис. 2.12. Вкладка Executables

Панель показує список всіх виявлених виконуваних файлів у мережі, групуючи їх за популярністю у мережі та у ESET LiveGrid, допомагаючи відфільтрувати безпечні та відомі виконувані файли з тих, які можуть бути унікальними, і не є популярними взагалі, що може свідчити про цілеспрямовану атаку.

Вкладка Computers панелі інструментів концентрується виключено на кінцевих точках підключених до ESET Inspect і допомагає виявити потенційно ризиковані комп'ютери, або комп'ютери, які вказують на будь-який вид підозрілої поведінки, що вартий подальшого розслідування.

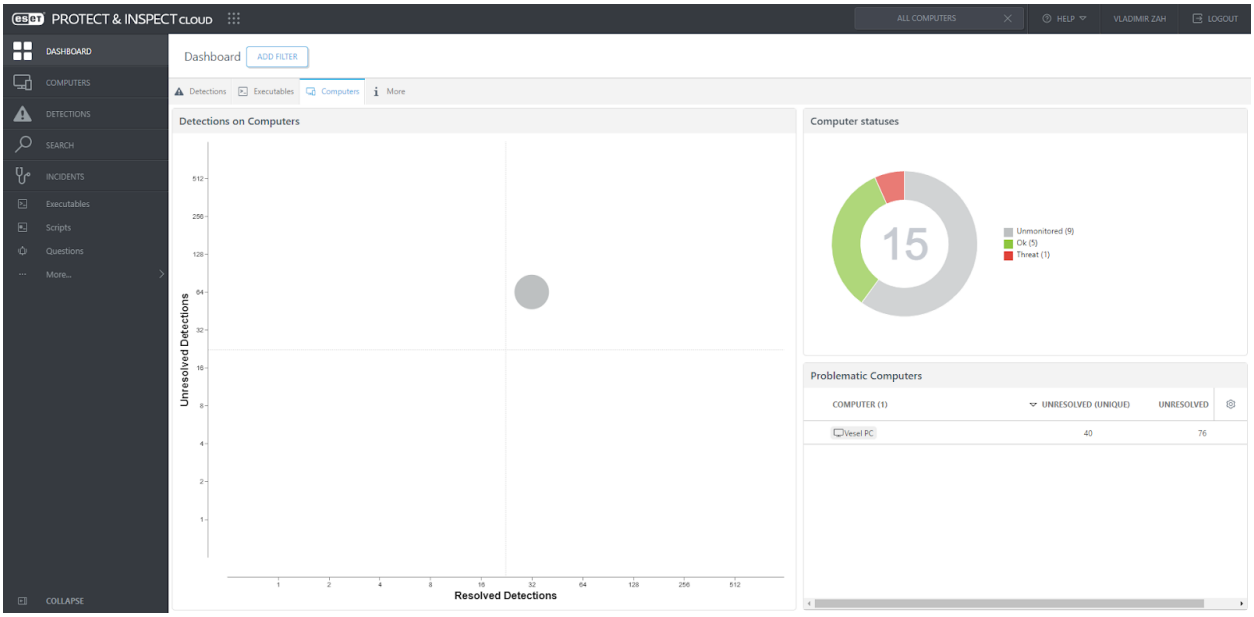



Рис. 2.13. Вкладка Computers

Вкладка More інші статистичні дані про різні ситуації, пріоритети, статус вирішених/невирішених спрацювань, стан з'єднань, стан подій, статус версії агента, а також стан комп'ютера.

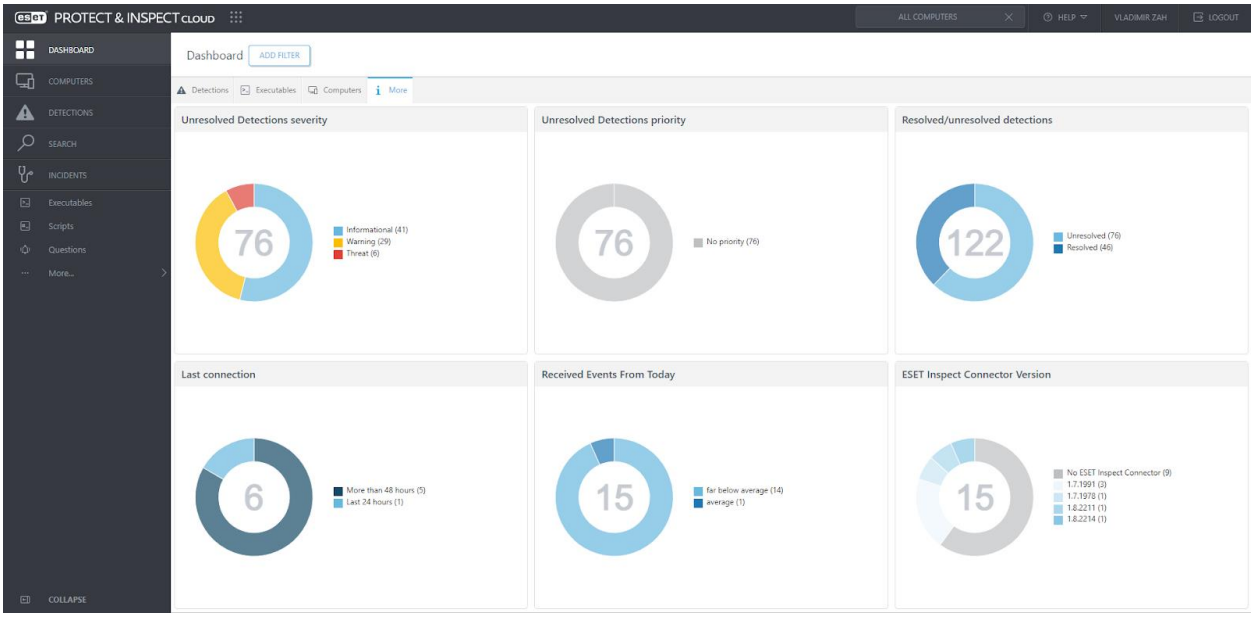



Рис. 2.14. Вкладка More

Загальний стан EI можна перевірити за допомогою вкладки Server Status (доступна у випадку локального розгортання), яка вказує, чи коректно працює EI і чи всі системні служби працюють належним чином, без надмірного використання системних ресурсів.

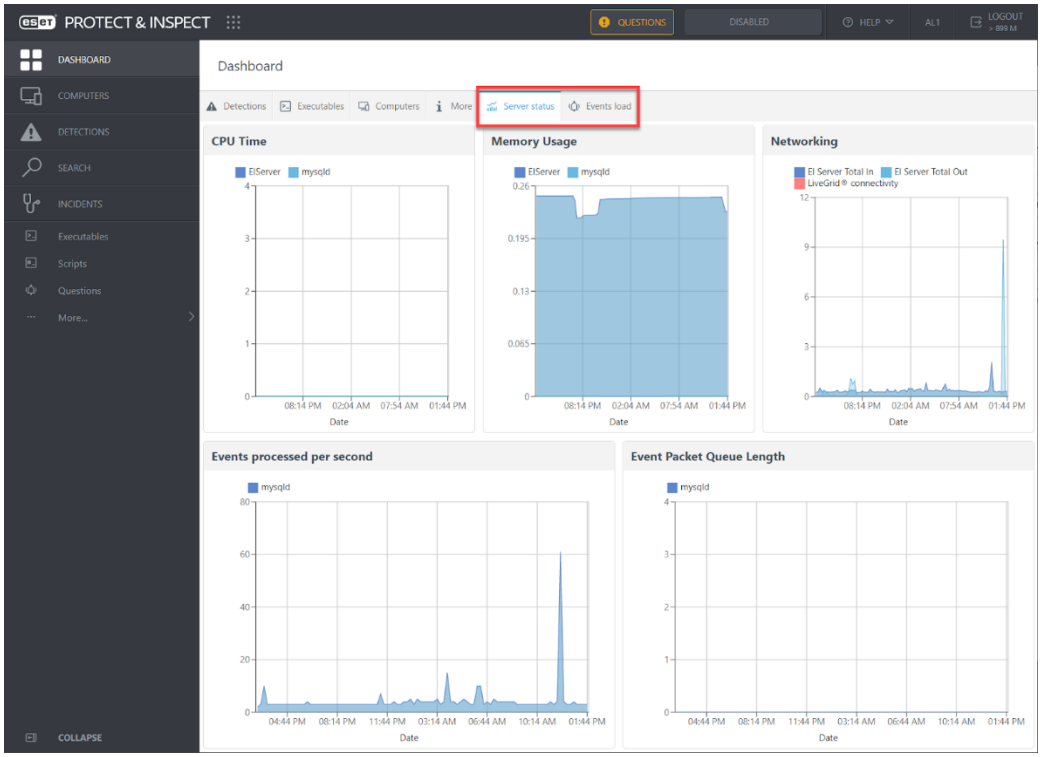



Рис. 2.15. Вкладка Server Status

Вкладка Events Load (доступна у випадку локального розгортання) призначена для того, щоб спеціалісти з безпеки могли бачити потік даних, що обробляються, спроби невдалого очищення і відображення які виконувані файли породжують найбільше подій. Згодом, якщо певний тип подій генерує занадто багато шуму і вважається не зовсім необхідним для моніторингу в цьому конкретному середовищі (варіюється в залежності від організації), його можна легко відфільтрувати в майбутньому, створивши фільтр подій.

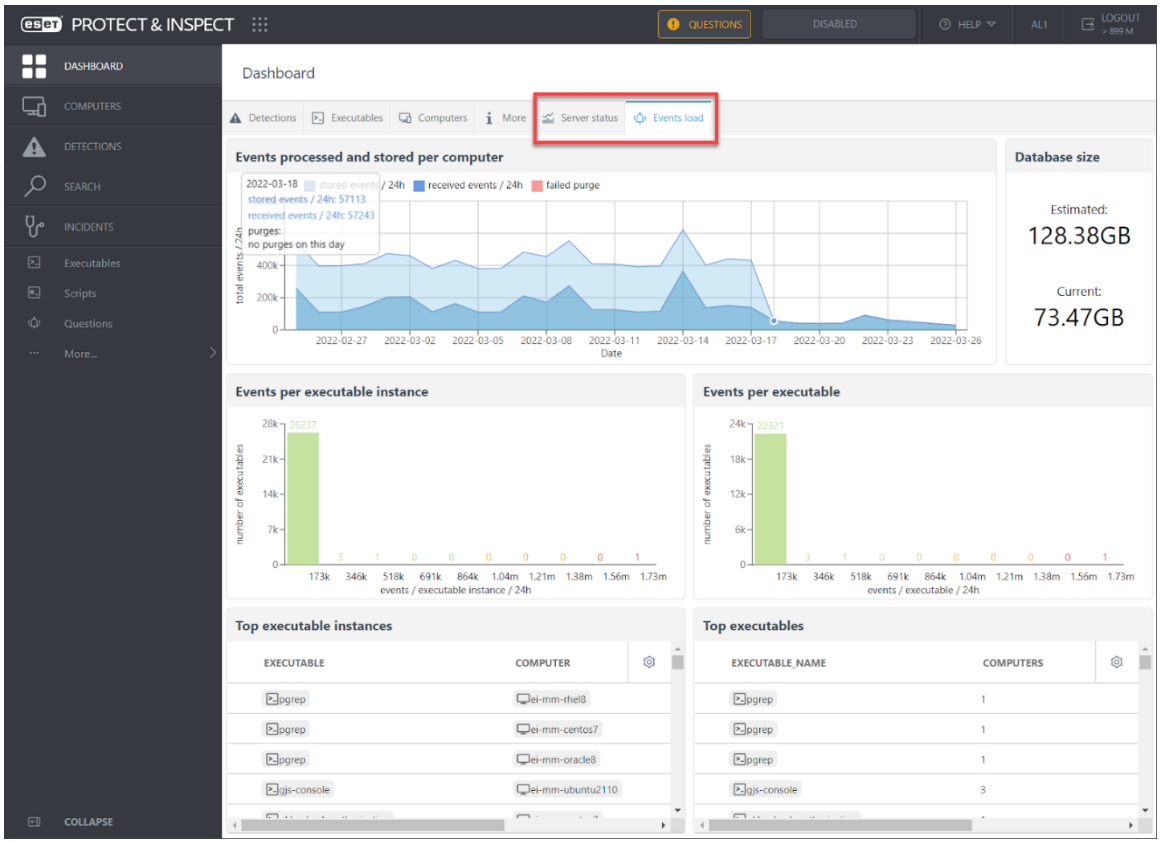



Рис. 2.16. Вкладка Events Load

Розділ Комп'ютери показує структуру компанії. Дані в цьому розділі синхронізовані з ESET PROTECT. Тут стан відображається не з точки зору функціональних проблем, а з точки критичності невирішених детекцій, які на даний момент присутні на машині. Інші стовпчики, що показують подробиці про кількості виявлень по критичності та кількість унікальних виявлень, дозволяє спеціалістам з безпеки зосередити увагу на комп'ютерах з найвищою швидкістю генерації подій,

ступенем тяжкості, частотою виявлення, що може свідчити про те, велику кількість спрацювань які потребують оптимізації або про наявну зловмисну діяльність. На комп'ютерах можна легко виконувати дії, такі як ініціювання перезавантаження/вимикання комп'ютера, ізоляцію від мережі, запит на передачу даних компонентом ESET Inspect Connector (Send Wake-Up Call), запускати сканування і за необхідністю перегляд інформації про конкретний ПК в консолі ESET PROTECT. Також EI дозволяє відкриття віддаленого терміналу PowerShell на будь-який комп'ютер з ОС Windows для швидкого реагування (рис. 2.17.). Деякі з цих дій додатково буде розглянуто у Розділі 3.2. даної роботи. В детальній інформації про ПК адміністратор може переглядати активні та оброблені виявлення, їх критичність, виявлені та виконані виконувані файли і скрипти, а також переглядати всі операції на ПК які зафіксував ESET Inspect Connector (RAW Data) протягом періоду за який вони зберігаються в БД EI.

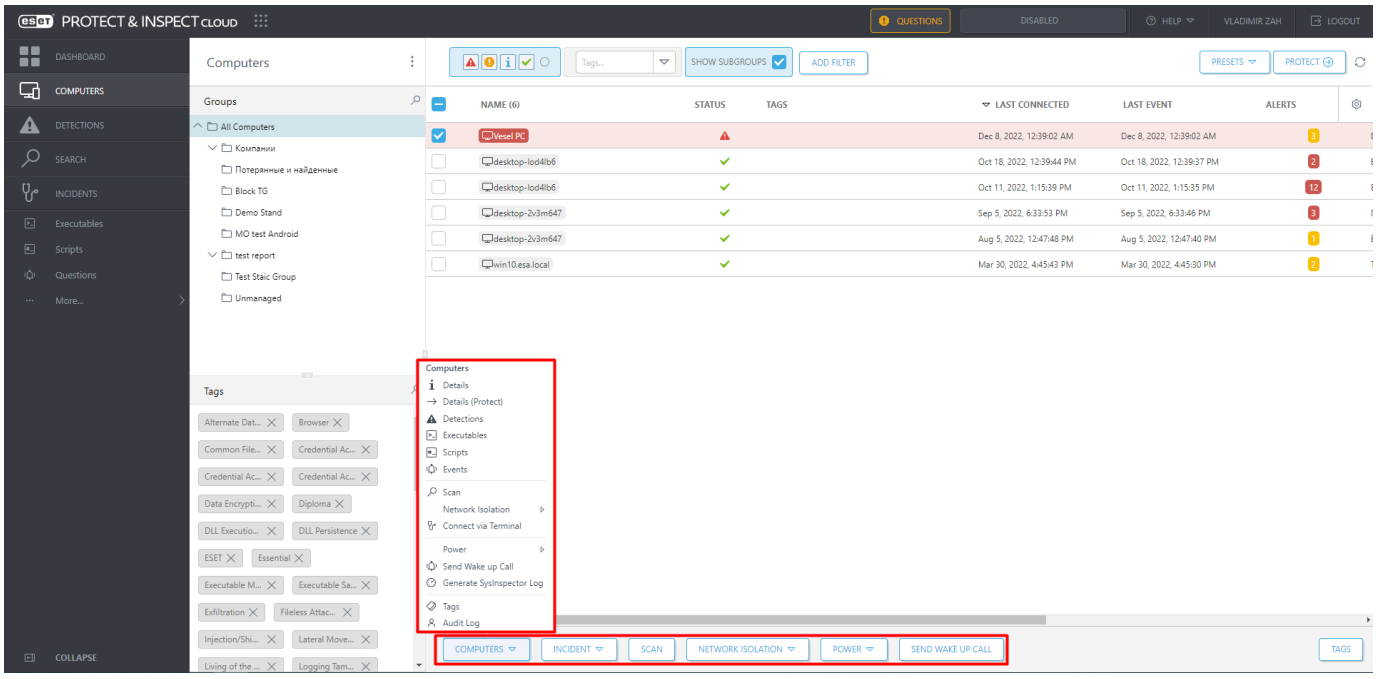



Рис. 2.17. Розділ Computers та дії які можна виконати на кінцевій точці

ESET Inspect включає в себе механізм виявлення на основі правил. Правила використовується для виявлення шкідливої. аномальної та діагностичної поведінки і фільтрують всю знайдену інформацію за визначеними в них параметрами. Правила в ESET Inspect використовують в своїй структурі мову XML і мають доволі простий в використані синтаксис, що дозволяє адміністраторам створювати власні правила для виявлення потрібних їм моментів мережі. Спрацювання які створюються при обробці правил відображаються у розділі Detections (рис. 2.18.). Кожне виявлення в даному розділі має чітким визначенням того, де воно відбулося(комп'ютер), який виконуваний файл його створив, і навіть який саме процес його запустив цей виконуваний файл. Виявлення супроводжуються інформацією про ступінь критичності і можливістю призначити пріоритет кожному з виявлень (їх можна використовувати для фільтрування). Також можна виявлення з ESET Inspect відображаються в ESET PROTECT з можливістю детального їх аналізу в EI.

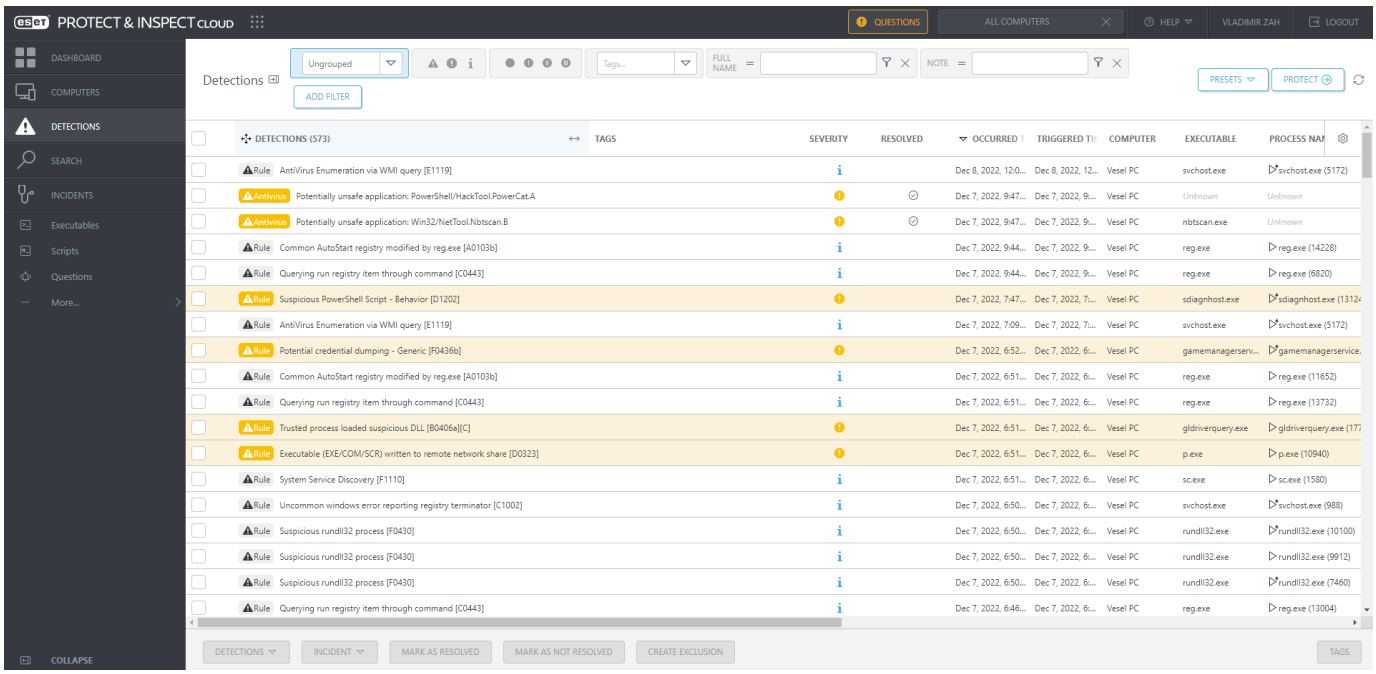



Рис. 2.18. Розділ Detections

Коли детекція отримує статус оброблено в EI або ESET PROTECT, вона також вирішується в іншій системі. Фільтрація спрацювань дозволяє спеціалістам з безпеки

зручно і швидко обробляти спрацювання, відфільтровуючи їх за потребами. Крім того, можна зберігати набори фільтрів, що буде розглянуто більш детально в розділі 3.3. даної роботи. Адміністратор може дослідити розширені деталі кожного виявлення, де буде показано подробиці щодо виконуваного файлу, процесу, користувача та комп'ютера із-за яких було спрацювання і пояснення можливих причин, з запропонованим наступними кроками розслідування та реагування. Інструкція для реагування додається шляхом посилання на техніки MITER ATT&CK(TM), де це можливо. Цей фреймворк описує різні прийоми атаки і методи їх розслідування. Правила виявлення EI які надаються розробниками ESET посилаються на різні методи ATT&CK і адміністратор при розслідування може легко перейти на веб-портал MITRE і отримати додаткову інформацію стосовно спрацювання. З детальної інформації про виявлення адміністратор може перейти до деталей виконуваного, процесу, правила і продовжити подальше розслідування.

EI має високо функціональний пошук, де офіцери безпеки можуть шукати IOC в реальному часі, використовуючи простий запит з певними змінними або додатково писати набагато складніший запит на XML для максимально детального пошуку (рис. 2.19.). Функція пошуку автоматично завершують для відповідних категорій записів.

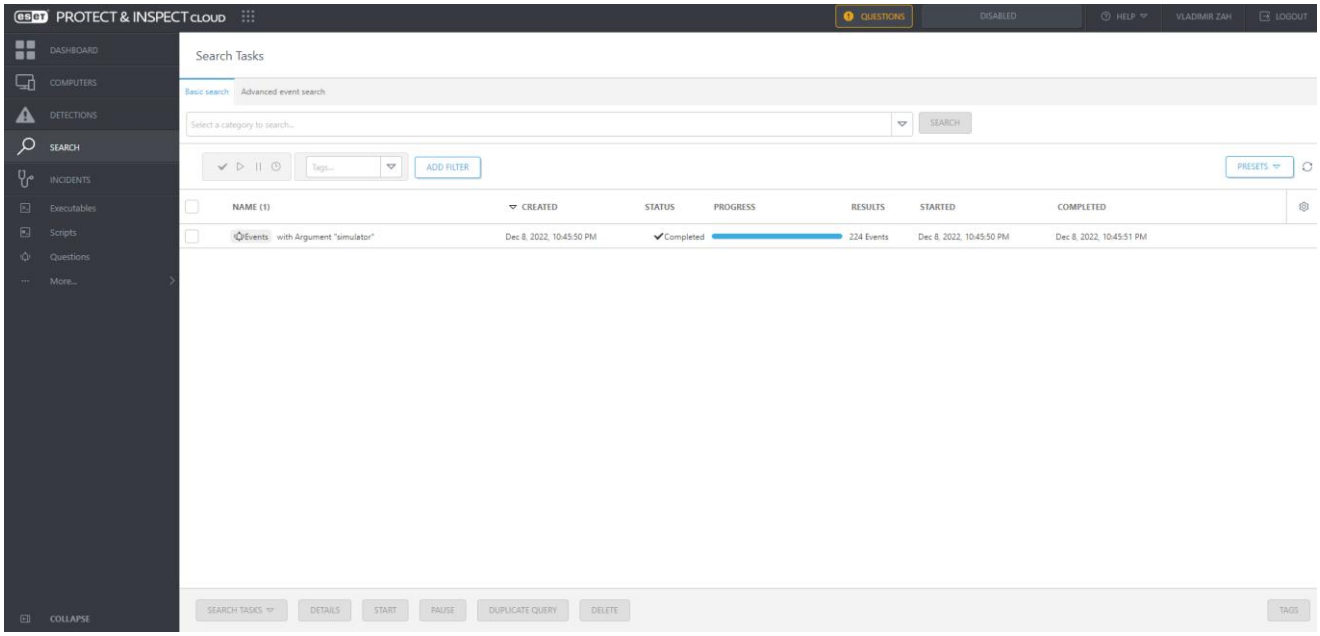



Рис. 2.19. Розділ Search

Пошук в EI можливий по виявленням, комп'ютерам, виконуваним файлам, процесів і навіть по окремим діям і подіям. Пошук є дуже потужним інструментом з точки зору швидкого пошуку  потрібної інформації, наприклад, наданої стороннім аудитором, і дозволяє офіцерам безпеки знаходити конкретні файли або їх активність в мережі. Під час виконання пошуку можна побачити шкалу прогресії. Яка відображає на скільки процентів просканові файли в базі даних, а також можна побачити скільки на даний момент пошук знайшов записів які відповідають його критеріям. Важливо зазначати, у розділі пошуку зберігається історія запитів які створював адміністратор, що дозволяє повернутися до результатів в майбутньому або запустити вже конфігурований пошук заново.

Розділ Incidents відповідає за систему управління інцидентами, яка допомагає адміністраторам групувати кілька об'єктів, таких як виявлення і комп'ютери, в логічні цілісності, де потенційно зловмисні події можна побачити на хронологічній шкалі, включаючи також дії користувача EI для поліпшення співпраці команди і прозорості розслідування (рис. 2.20.).

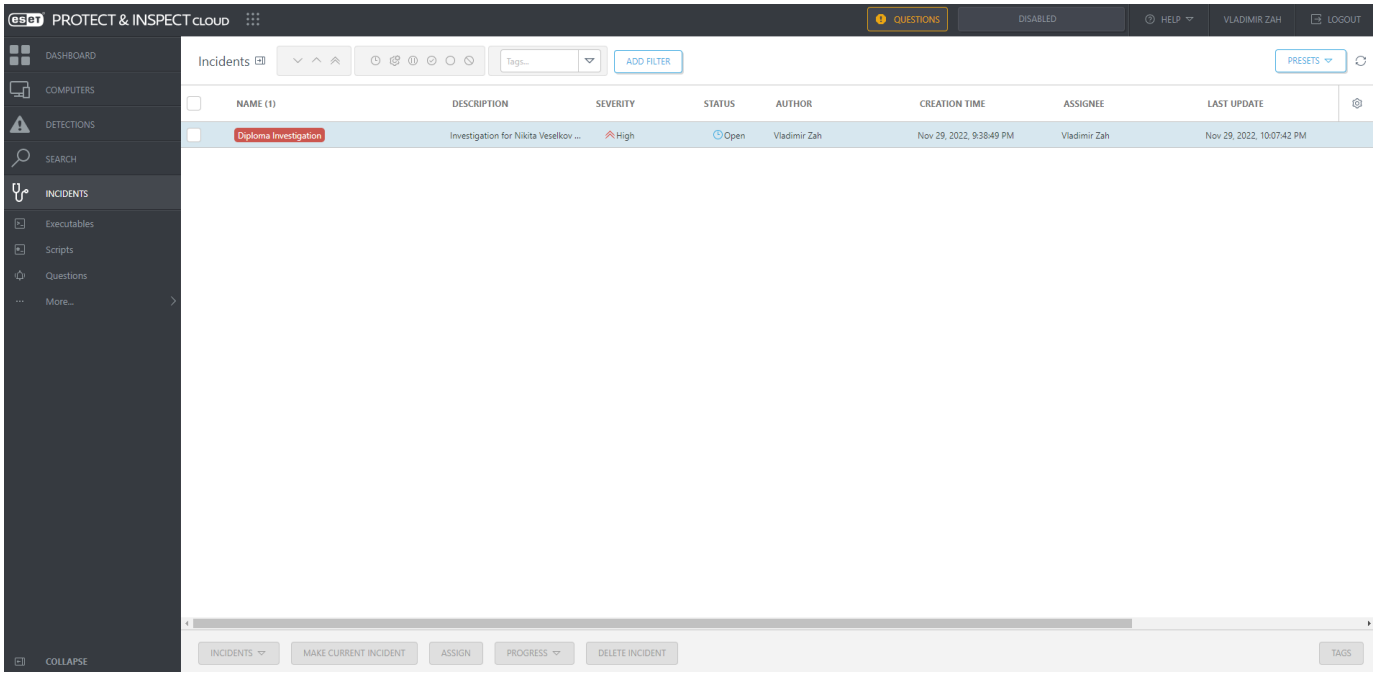



Рис. 2.20. Розділ Incidents

Для створення інциденту користувач вручну вибирає спрацювання на основі якого(яких) буде створено інциденті і які представляють інтерес для подальшого дослідження. При додаванні спрацювання у адміністратора є вибір, створити новий інцидент на основі даного спрацювання або додати його в вже існуючий інцидент. Згодом система автоматично пропонує пов'язані об'єкти та події для збагачення контексту інцидентів. Система управління інцидентом включає в себе кілька інструментів, таких як можливість коментувати інцидент, редагувати його атрибути, присвоювати його різним користувачам і змінювати його статус, для відображення поточного прогресу. При перегляді інциденту адміністратор може переключатися між вкладками загальною хронологією інциденту, виявленням, комп'ютерами, виконуваними файлами та процесами, які входять до його складу.

## 2.2. Технології комплексного захисту кінцевих точок на базі рішень ESET

Еволюція загроз, спрямованих на бізнес, стала причиною появи нового покоління технологій безпеки кінцевих точок. Нині загрози поширюються усіма можливими каналами зв'язку, що спокунає технологічних вендорів та компанії використовувати засоби захисту на всіх можливих рівнях передачі даних.

Сучасні продукти захисту кінцевих точок вже давно отримали приставку “комплексний” до назви продукт захисту. Це каже про те , що сучасні продукти захисту кінцевої точки вже давно вийшли за рамки антивірусу та базового брандмауеру. На разі, такі продукти мають дуже багато технологічних розробок, наприклад, захист електронної пошти (перевірка трафіку POP3(S), IMAP(S), тощо), персональний брандмауер, антивірусний захист та інші. Список технологій унікальний для кожного вендора, особливо це стосується назв тих чи інших технологій але запити ринку формують так званий “базовий набір” технологій які

повинні бути в продукті захисту кінцевої точки. Для розуміння сучасних технологій захисту та їх тенденцій, розглянемо технологічний набір в продуктах ESET Endpoint Security й ESET Server Security (ESS) [12].

**ESET Endpoint Security (EES)** – це комплексний продукт безпеки, який дозволяє реалізувати усесторонній захист кінцевої точки. Задовільний стан захищеності досягається за допомогою поєднання різних технологій які зібрані в модулі продукту. Кожен з модулів має детальні налаштування, що допомагає адміністраторам налаштувати ідеальний баланс між захищеністю та впливом продукту захисту на бізнес процеси організації. Використання ESET Endpoint Security з ESET PROTECT у корпоративному середовищі дозволяє легко керувати будь-якою кількістю робочих станцій клієнта, застосовувати політики та правила, контролювати виявлення та віддалено налаштовувати клієнтів з будь -якого мережевого комп'ютера.

**ESET Server Security (ESS)** - це комплексний продукт безпеки, який дозволяє реалізувати усесторонній захист Windows та Unix серверів. Продукт ESS використовує ті ж технологічні розробки, що й продукт для захисту кінцевої точки EES, за винятком кількох додаткових функцій які допомагають продукту краще адаптуватися до серверних середовищ.

Розглянемо основні технології та модулі представлені в ESET Endpoint Security:

**Ядро виявлення** - це модуль який захищає систему від зловмисних атак, контролюючі обмін та використання даних, електронних повідомлень та роботу з файлами в Інтернеті. Якщо буде виявлено об'єкт, класифікований як зловмисне програмне забезпечення, Ядро виявлення почнеться процес реагування. Під час реагування Ядро виявлення може видалити файл, заблокувати його і потім очистити або перемістити загрозу в карантин.

Додатковим захистом до усіх цих модулів є репутаційний сервіс ESET LiveGrid. Він збирає дані від користувачів ESET з усього світу й передає до дослідницької лабораторії ESET. Отримуючи підозрілі зразки та метадані від ESET LiveGrid,

дослідники ESET можуть миттєво реагувати на загрози і своєчасно оновлювати системи ESET.

Система репутації ESET LiveGrid, допомагає покращити загальну ефективність рішень захисту ESET. Користувачі можуть перевіряти репутацію запущених процесів і файлів безпосередньо з інтерфейсу EES. Крім того, додаткову інформацію про нові загрози можна отримати за допомогою технології ESET LiveGrid. Коли в системі користувача перевіряється виконуваний файл або архів, його хештег спочатку порівнюється з базою даних об'єктів, згрупованих у білий і чорний списки. Якщо файл знайдено в білому списку, він вважається безпечним і буде без перешкод виконуватися під час наступних перевірок. Якщо ж він у чорному списку, система вживає заходів відповідно до типу загрози. Якщо збігів не знайдено, файл проходить ретельну перевірку. Відповідно до її результатів файл зараховується до загрозливих або безпечних об'єктів. Такий підхід значно покращує ефективність перевірки. Система репутації дає змогу ефективно виявляти зловмисний код іще до того, як його сигнатури будуть додані до антивірусної базі даних на комп'ютері користувача (остання оновлюється кілька разів на день) [13].

**Захист від експлойтів** – це модуль, що служить для захисту програм, які зловмисники зазвичай використовуються для зараження системи. Технологія стежить за поведінкою процесів і виявляє підозрілі дії, що можуть свідчити про наявність експлойту.

**Захист від експлойтів Java** — відстежує програми, створені мовою Java, на предмет шкідливої поведінки, схожу на поведінку експлойтів.

*Удосконалений сканер пам'яті* – цг технологія, що працює разом із засобом захисту від експлойтів. Вона посилює захист від зловмисного ПЗ, призначеного для обхода захисних продуктів за допомогою обфускації та/або шифрування. У випадках, коли звичайна емуляція чи евристика можуть не виявити загрозу, удосконалений сканер пам'яті може визначити підозрілу поведінку та просканувати загрози, коли вони проявляються в системній пам'яті.

**Система запобігання вторгненням** (HIPS) – це модуль який захищає систему від зловмисного ПЗ та небажаної діяльності, яка намагається негативно вплинути на кінцеву точку. HIPS використовує вдосконалений поведінковий аналіз у поєднанні з можливостями виявлення мережевої фільтрації для моніторингу запущених процесів, файлів і ключів реєстру. HIPS є окремою системою захисту файлової системи в режимі реального часу і не є брандмауером; він відстежує лише процеси, що виконуються в операційній системі.

**Контроль пристроїв** – цей модуль дозволяє блокувати зовнішнішні пристрої і налаштовувати дозволи для пристроїв, використання яких дозволено в організації.

**Персональний брандмауер** - це модуль який контролює весь вхідний та вихідний мережевий трафік кінцевої точки. Адміністратор безпеки може створювати спеціальні правила для блокування або дозволу з'єднань, зазначаючи при цьому як параметри вихідні або вхідні адреси та порти, а також служби та програми які створюють мережеві з'єднання. Персональний брандмауер EES може працювати в декількох режимах:

*Автоматичний режим* – брандмауер дозволяє весь вихідний трафік та блокує весь вхідний трафік із мереж які не визначені як довіренні.

*Інтерактивний режим* – в цьому режимі брандмауер питає в користувача яку дію використовувати для трафіку який не визначений в правилах. Після чого продукт захисту створює правило для з'єднання на основі рішення користувача.

*Режим на основі правил* – в цьому режимі брандмауер блокує всі вхідні і вихідні з'єднання, а дозволяє лише ті для яких створенні відповідні правила. Даний режим потребує тонких налаштувань але є найбільш ефективним з точки зору безпеки.

*Режим навчання* – в цьому режимі брандмауер автоматично створює дозволяючи правила для всього трафіку на кінцевій точці, після чого створені правила може використовувати адміністратор безпеки для створення політики брандмауера і застосування режиму на основі правил.

Також персональний брандмауєр може виявляти поведінкові зміни в програмному забезпеченні. Сповіщення відображається, якщо модифікована програма, для якої існує правило брандмауера, намагається встановити підключення.

**Захист від мережевих атак** - це модуль який містить в собі IDS та технології для виявлення вторгнень в систему, технологію захисту від атак повним перебором та захист від ботнетів.

*Система виявлення вторгнень (IDS)* – аналізує вміст мережевого трафіку та захищає від мережевих атак. Будь-який трафік, який система визначить як шкідливий, буде заблоковано.

*Захист від атак методом повного перебору* – блокує атаки підбору пароля для служб RDP і SMB. Атака методом повного перебору — це метод виявлення цільового пароля шляхом систематичної перевірки всіх можливих комбінацій літер, цифр і символів.

*Технологія виявлення вторгнень* – це розширення брандмауера, яке дає змогу ефективніше виявляти експлойти для відомих вразливих місць на рівні мережі. Воно застосовує алгоритми виявлення поширених експлойтів у широко використовуваних протоколах, таких як SMB, RPC й RDP, і створює додатковий рівень захисту від шкідливого програмного забезпечення, мережевих атак і застосування вразливостей, для яких іще недоступне або не встановлено виправлення.

*Захист від ботнет-вірусів* – виявляє шкідливе програмне забезпечення, аналізуючи використовувані ним протоколи мережевої взаємодії.

**Захист доступу до Інтернету** – цей модуль перевіряє обмін даних користувачів при роботі з протоколами HTTP(S) і також додатково, йде перевірка програм JavaScript які можуть бути використані браузером або веб-порталом. Також, в даному модулі реалізована перевірка обміну даних по протоколу SSL/TLS.

**Захист поштового клієнту** - це модуль який допомагає інтегруватися з наявним поштовим клієнтом, наприклад, MS Outlook та перевіряти поштовий трафік на наявність шкідливих вкладень або СПАМ-листів.

Важливо зазначити, що кожен з цих модулів та технологій, мають велику кількість параметрів для тонкого налаштування, що дозволяє адаптувати продукти захисту кінцевих точок та серверів до різних інфраструктур та їх потреб. Налаштовувати ці параметри можна як віддалено за допомогою ESET PROTECT так і локально через інтерфейс продукту.

### 2.3. Функціонал та архітектура додаткових рівнів захисту інфраструктури на базі рішень ESET

Ринок безпеки, як ми знаємо, переживає бурхливий розвиток. Ландшафт загроз розвивається, з дедалі більш цілеспрямованими і наполегливими атаками, які звичайні контрзаходи не можуть запобігти. Зростання атак спонукало до попиту на удосконалені засоби безпеки, які покращують видимість і надають додаткові дані, щоб дозволити виявлення, відповідь на події і судовий аналіз. Щоб запобігти шкідливому програмуванню, компанії готові додати інші шари захисту поверх рівня EPP (Endpoint Protection Platform) до або одночасно з витонченими рішеннями XDR. Це робиться відповідно до Gartner ASA (архітектура адаптивної безпеки) і його еволюції у вигляді CARTA (безперервна адаптивна оцінка ризику і довіри), де існують чотири первинні квадранти:

- прогнозування
- запобігання
- виявлення і реагування, які є ключовими аспектами в сучасних реаліях.

Вирішення проблеми ринку визначається як мережева пісочниця для виявлення зловмисних програм. Gartner зазначає: «Мережева пісочниця не повинна використовуватися для виявлення зловмисних програм, з якими можна займатися більш економічно ефективними методами. Вона повинна бути використана для виявлення невідомого, можливо, складного шкідливого програмного забезпечення —

шкідливого програмного забезпечення, яке, ймовірно, не виявляється традиційними методами. Мережева пісочниця є однією з перших технологій, які організації можуть розгорнути для виявлення складних шкідливих програм набагато раніше, ніж очікування коли їх традиційні рішень будуть спроможні їх виявляти». Розгортання мережевої пісочниці є наступним кроком для підвищення безпеки на більшості платформ захисту кінцевих точок.

**ESET LiveGuard Advanced** — протидіючий хмарний захист від цільових атак і нових, Never Before-Seen типів загроз, особливо загроз класу програм вимагачів. Для максимізації виявлення в рішені використовуються чотири окремих шари виявлення. Зразки спочатку проходять статичний аналіз і розпакування за станом, і відповідність базі даних з відомими загрозами. Другий шар виконує статичний та динамічний аналіз, використовуючи алгоритми машинного навчання та методи, які включають глибинне навчання. Зразки потім обробляються у витончених пісочницях, які стежать за будь-якими ознаками зловмисної поведінки. Зрештою, всі дані з пісочниць піддаються поглибленому поведінковому аналізу, щоб виявити відомі зловмисні патерни і дії (рис. 2.21.) [14].

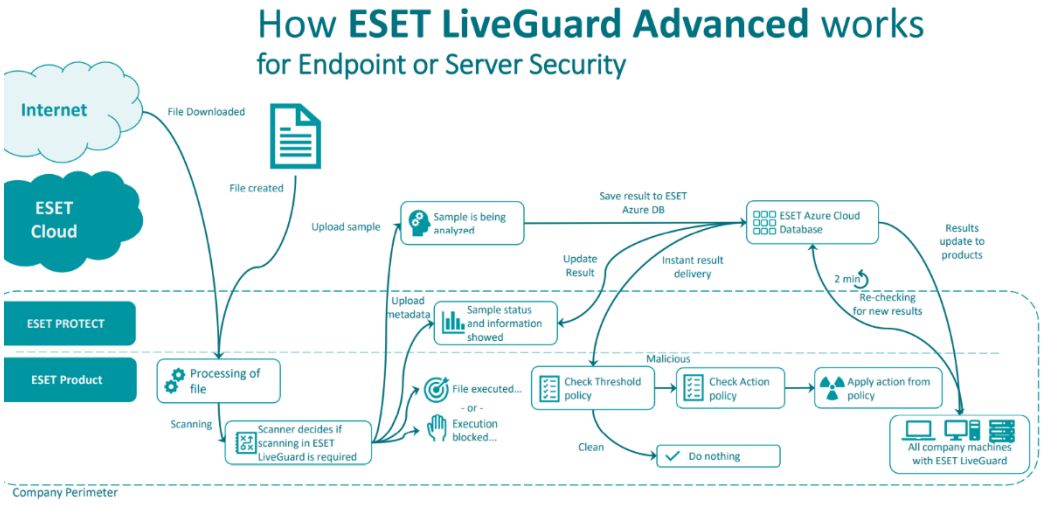



Рис. 2.21. Принцип роботи ESET LiveGuard Advanced

Людина є найслабшим елементом в безпеці будь-якої організації, так як у людини неможливо “налаштувати” функції безпеки і людський фактор дуже часто стає причиною компрометації інфраструктур. Одна з найбільших небезпек пов'язаних

з працівниками — це погана парольна гігієна. За статистикою, працівники не лише використовують один і той самий пароль для більшості ресурсів, а й іноді вільно діляться своїми паролями з друзями, сім'єю і колегами. Навіть коли організації створюють парольні політики для своїх працівників, то працівники все одно нехтують правилами безпеки і записують свої нові “складні” паролі в текстові файли та на наліпки на робочому місці. Для вирішення цієї проблеми все більше організацій починають використовувати багатофакторну автентифікацію.

Багатофакторна автентифікація (MFA), також відома як двофакторна автентифікація (2FA), є методом автентифікації яка потребує двох (або більше) незалежних наборів інформації для перевірки даних користувача. MFA є набагато сильнішим методом, ніж традиційний метод (статичний пароль або PIN-автентифікація). MFA доповнює традиційний метод і зменшує вірогідність підбору паролю та компрометації облікових записів.

У сучасних реаліях кібербезпеки, щодня відбувається велика кількість вдалих спроб компрометації облікових записів. Найпоширенішим методом який використовують зловмисники для компрометації є підбір та злам слабких паролів які використовуються в організації, а також використання ботів та фішингу для викрадення облікових даних користувачів. Одним з методів протидії зловмисників є побудова комплексної парольної політики і повноцінне розмежування доступу в організації. Але цей крок зазвичай негативно впливає на бізнес процеси в компанії, так як комфортом користувачів жертвують в користь безпеки, що ускладнює комунікацію і роботу працівників. Використання MFA в свою чергу дуже сильно підвищує стан безпеки інфраструктури і має мінімальний вплив на роботу

користувачів. Додавання MFA кардинально не впливає на роботу працівників, так як процес додаткового підтвердження займає мало часу (рис. 2.22.) [15].

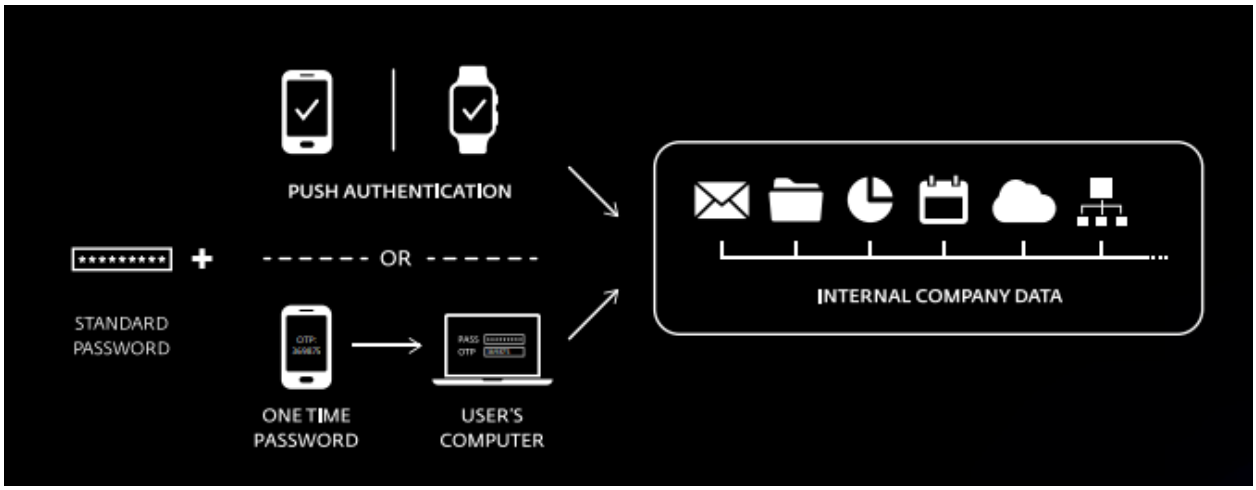



Рис. 2.22. Принцип дії MFA

ESET Secure Authentication (ESA) є простим у використанні та ефективним багатофакторним рішенням автентифікації на базі мобільних телефонів, яке захищає організації від слабких паролів і несанкціонованого доступу до даних які зберігаються локально, або в хмарі. ESA забезпечує MFA для компаній різних розмірів і працює на таких поширених системах як VPN, Remote Desktop Protocol, Office 365, Outlook Web Access, вхід до операційної системи та інших.

ESET Secure Authentication пропонує два режими інтеграції. Це інтеграція Active Directory для організацій які використовують домени Windows або автономного режиму, який підходить для організацій без домену. Інтеграція та налаштування рішення не займає багато часу та ресурсів із за нескладної архітектури. Сервер ESA займається обробкою інформації та відповідає за налаштування інтеграції в робочі сервіси компанії. Сервер має API та SDK, які допомагають інтегрувати ESA з іншими рішеннями безпеки, а також з сервісами і платформами які використовуються в компанії. Веб-консоль ESA допомагає адміністраторам зручно керувати роботою та налаштуваннями сервера. Додаток на смартфони, допомагає в зручному форматі надавати користувачам OTP для роботи. Для роботи ESA немає потреби в спеціальних токенах або пристроях для співробітників. Додаток ESA

працює на всіх смартфонах iOS і Android, і може інтегруватися з біометрикою пристроїв (Touch ID, face ID, Android fingerprint) для підвищеної безпеки і кращого користувацького досвіду [16].

Можливість отримувати та збирати останню інформацію про нові загрози в кіберпросторі має вирішальне значення для захисту корпоративних активів даних. Ця інформація допомагає компанія зробити оцінку ризиків проведення та наслідків подібних атак. Більше інформації про ці ризики безпеки дозволяє активно запобігати потенційним пошкодженням, здійснити необхідні заходи щодо його пом'якшення, модернізувати та налаштовувати власну КСЗІ для протистояння сучасним загрозам.

ESET Intelligence Threat Intelligence (ETI) надає інформацію, засновану на доказах, та поради, щодо існуючих або виникаючих загрозах. Послуги ETI попереджають компанії про зловмисне програмне забезпечення або діяльність, яка може їм загрожувати. Інформація надається компаніям у вигляді ESET Intelligence Data Feeds and Reports. Завдяки технології ESET LiveGrid, компанія ESET має більш ніж 110 мільйонів кінцевих точок, які діють як сенсори та збирають інформацію про зловмисну активність. Після автоматичної та ручної обробки цієї інформації дослідниками ESET, компанії можуть отримати інформацію щодо поточних загроз, APT-угрупувань, зловмисних програм та їх властивостей, серверів, що використовуються для їх поширення, і навіть URL-адреси і домени, які поширюються їх. Звіти надають інформацію про ті загрози, які найбільш критичні і актуальні на даний момент. Дослідники безпеки ESET працюють в багатьох напрямках і, отже, можуть поділитися актуальну ситуацією щодо того, що відбувається в кіберпросторі. Організації, які використовують рішення отримують як електронні звіти, які зручні для аналізу та обговорення, так і індикатори компрометації (IoC), які можна використовувати в наявних системах захисту [17].

# 3. Розроблення технологій та методів розслідування кіберінцидентів на базі рішення ESET PROTECT & Inspect

## 3.1. Технологія розслідування сучасних атак за допомогою рішення ESET Inspect

Як вже було зазначено в даній роботі, розслідування кіберіндицентів це комплексний процес. який має певні правила і методики, однак, кожне розслідування є унікальним. В даному розділі, розглянуто технології розслідування кіберінцидентів та розподілення доступу під час них на базі рішення ESET PROTECT&Inspect і також методи які використовую я та мої колеги, технічні спеціалісти представники компанії ESET в Україні. Для розслідування була використана хмарна версія рішення ESET PROTECT&Inspect, а також тестова кінцева точка на базі операційної системи Windows 10 з встановленим комплексним продуктом захисту ESET Endpoint Security.

Для будь-якого розслідування потрібні ввідні дані. Для генерації таких даних було використано інструмент APT Simulator, який імітує таку активність зловмисників як збір даних про систему та мережу, спроба підвищення привілеїв, обхід систем захисту та інших методик. Було завантажено останню версію інструменту з порталу GitHub, після чого скрипт інструменту був запущений через командний рядок з правами адміністратора (Рис. 3.1).

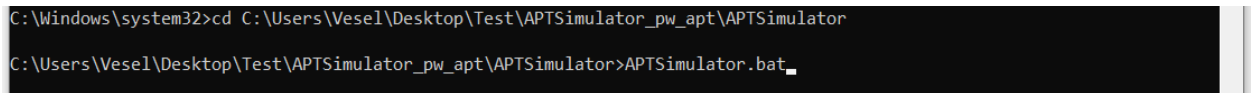



Рис 3.1. Запуск AptSimulator з командного рядка

Після запуску скрипту, було відображено повідомлення з попередженням стосовно використання даної утиліти. Після підтвердження було відображено список дій які може імітувати дана утиліта (рис.3.2).

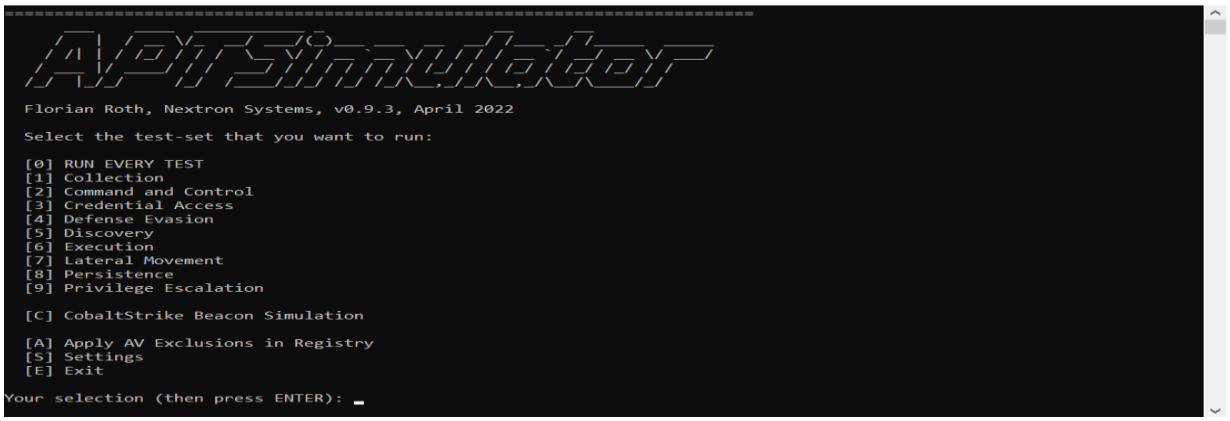



Рис 3.2. Список методів імітацій в AptSimulator

Для розслідування було запущено перший пункт RUN EVERY TEST, хоча під час розслідування ми розглянемо лише деякі спрацювання по даній утиліти. Після завершення симуляції можна побачити повідомлення про успішне завершення і інформацію про дії які були заблоковані продуктом захисту і інформацію як дозволити їх виконання.

Приблизний час початку симуляції 12:55. Так як ми розуміємо, що була симульована атака, для наглядного прикладу, імітуємо поведінку офіцера безпеки, який в нормальних умовах не знає про атаку і просто аналізує спрацювання в ESET Inspect. Перш за все, можна побачити в консолі керування 67 спрацювань, які ми згрупували по правилам, що в результаті дало спрацювання по 33 правилам. Гарною практикою є першочергове розслідування критичних спрацювань, які в консолі позначаються червоним кольором. Відфільтрувавши лише критичні спрацювання, можна побачити спрацювання по наступним правилам User/group management from command line [B1003], Silent execution of PsExec [B0903], Remote execution using

PsExec [B0901], Process with mimikatz-like command line parameters executed [A0422] (рис. 3.4.).

Рис 3.4. Критичні спрацювання в веб-консолі ESET Inspect

Розглянемо їх в хронологічному порядку, спочатку правило [B1003]. Для початка розслідування, треба перейти в детальну інформацію про спрацювання. (рис.3.5.).

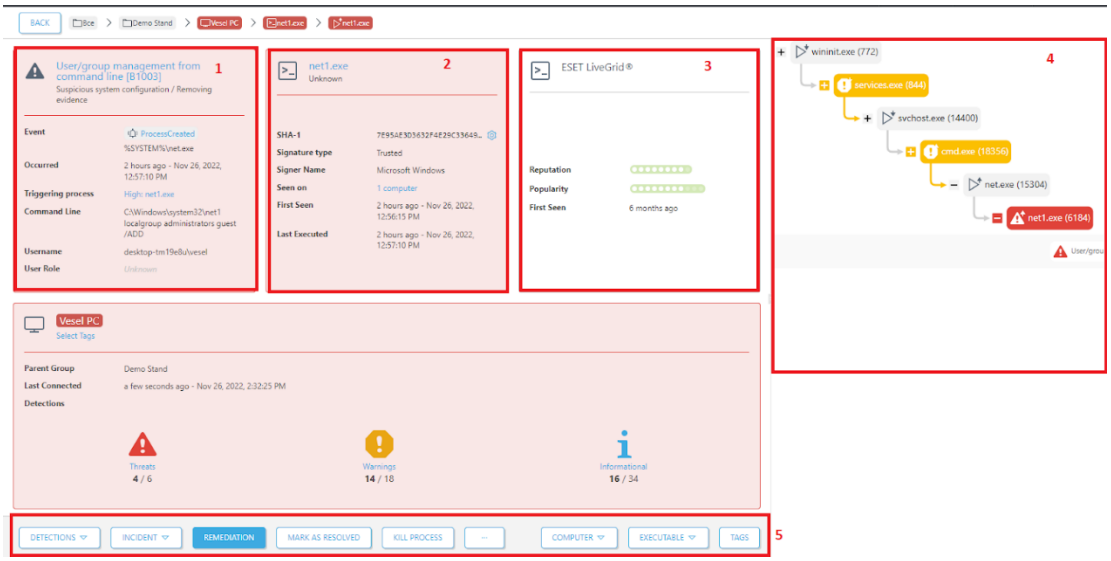



Рис 3.5. Детальна інформація про спрацювання

Відповідно до умовних позначень на рисунку 1 – Основна інформація про спрацювання, яка містить назву правила по якому відбулося спрацювання, подія спрацювання, час спрацювання, а також процес по якому було спрацювання та параметри з якими він був запущений і користувач який його запустив. 2 – це більш детальна інформація про процес по якому було спрацювання, а саме його хеш сума, компанія підписант і валідність підпису і інформація про цей файл в мережі компанії.

3 – це інформація з репутаційного сервісу ESET LiveGrid про репутацію процесу з пункту 2. 4 – це дерево процесів пов'язаних з спрацюванням. Воно дозволяє відслідити батьківські процеси і дії які далі виконував цей процес. 5 – це панель інструментів роботи зі спрацюванням, де адміністратор може. наприклад, позначити спрацювання як оброблене, завершити процес на кінцевій точці, створити інцидент та інше. Також, якщо спуститися вниз у інформації про спрацювання можна побачити більш детальну інформацію про спрацювання, де будуть рекомендації від розробників ESET стосовно розслідування та реагування на дане спрацювання, а також посилання на методики MITRE ATT&CK які з ним пов'язані (Рис. 3.6.).

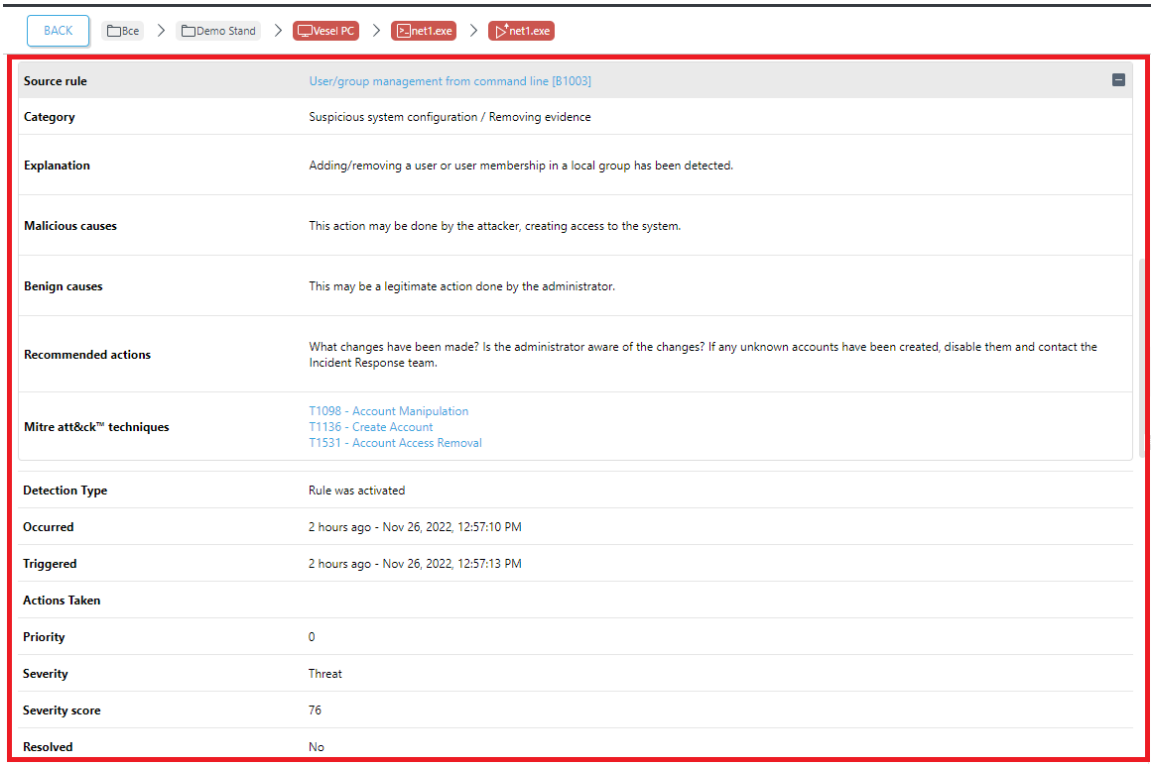



Рис. 3.6. Інформація MITRE ATT&CK про спрацювання

Дане спрацювання є підозрілим, так як можна побачити створення облікового запису гостя в системі за допомогою запуску служби net з параметрами *C:\Windows\system32\net1 localgroup administrators guest /ADD*, що є типовою методикою зловмисників. Для подальшого розслідування створимо інцидент на базі цього спрацювання (рис. 3.7.), який потім будемо доповнювати іншими спрацюваннями які будуть пов'язані з даною атакою.

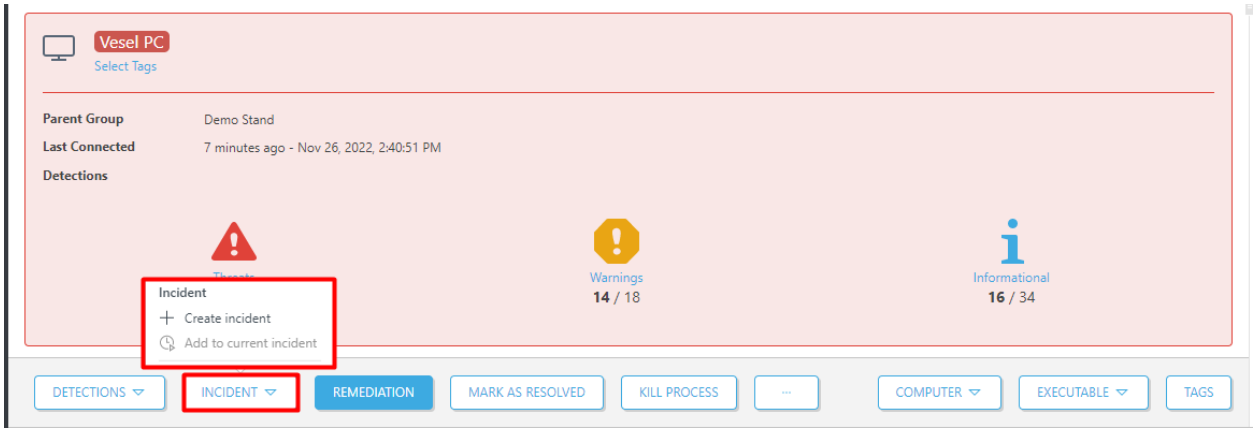



Рис. 3.7. Створення інциденту з контекстного меню спрацювання

Під час створення інциденту можна налаштувати ім'я інциденту, його опис, критичність, прив'язати його до певного користувача і додати теги для зручності. Після створення інциденту, адміністратор може побачити загальний таймлайн того, що відбувалося з інцидентом (додавання нових спрацювань, коментарів, зміна налаштувань, тощо), а також переглядати окремо спрацювання, комп’ютери, виконувані файли та процеси які були додані до інциденту (рис. 3.8.).

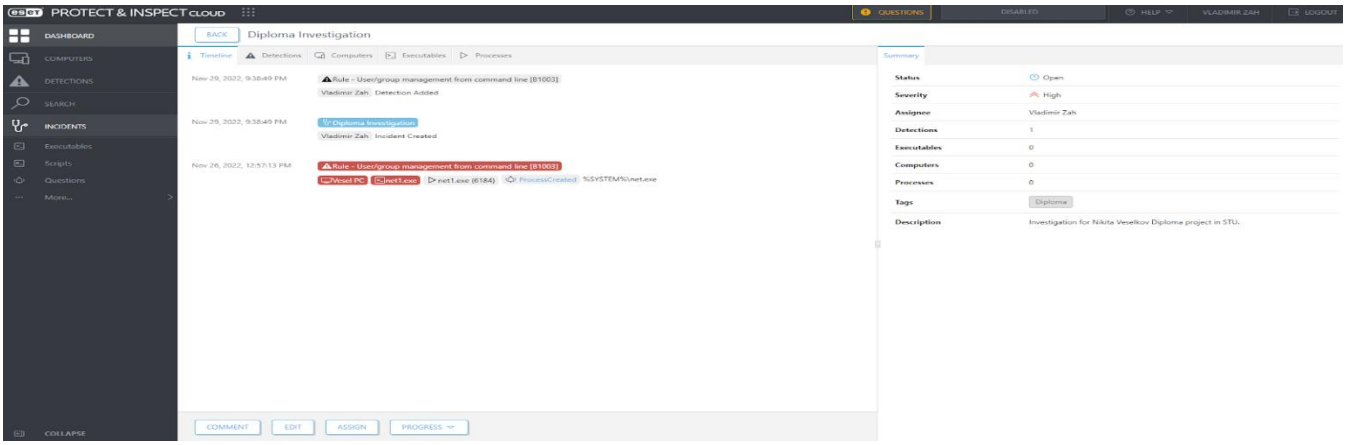



Рис. 3.8. Огляд створеного інциденту

Наступним кроком розслідування буде дослідження кінцевої точки зі спрацюванням [B1003]. Це дозволить зрозуміти, чим була спровокована дана і чи мала вона певне продовження після знайденого спрацювання. Додаймо кінцеву точку до інциденту і переглянемо спрацювання які були до та після підозрілої активності. При перегляді можна побачити підозрілі спрацювання які можна пов'язати з інцидентом (рис. 3.9.).

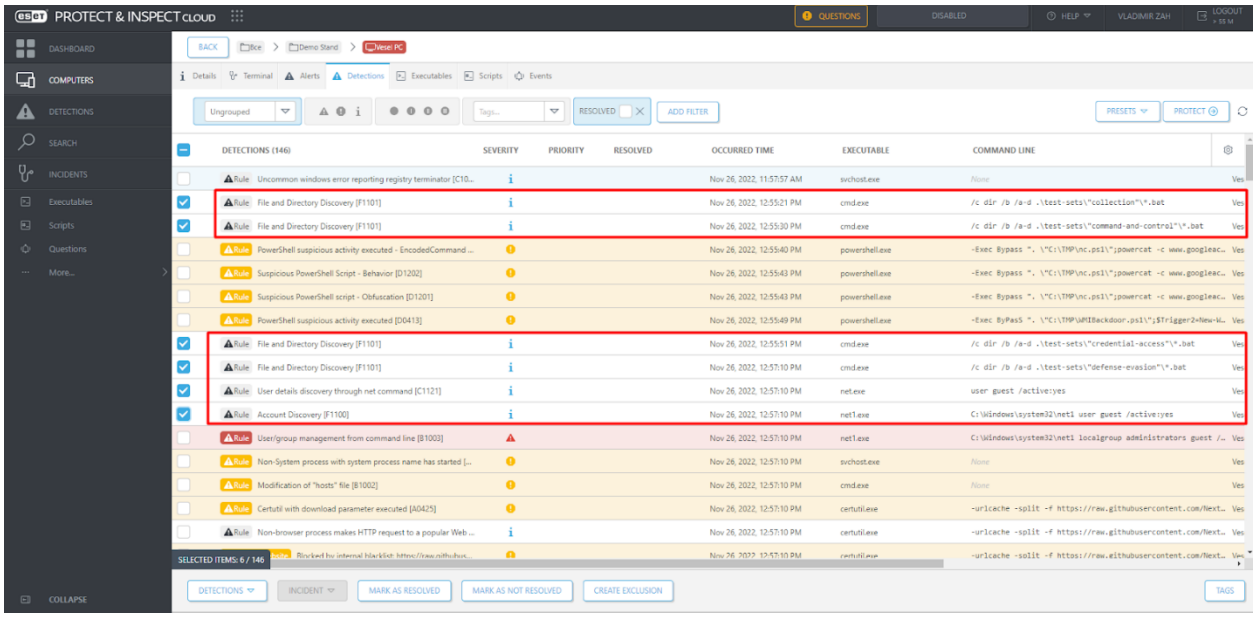



Рис. 3.9. Підозрілі спрацювання на кінцевій точці Vesel-PC

В цих спрацюваннях задектованго запуск підозрілих скриптів powershell та .bat, а також була запущена перевірка наявності дозволу на створення гостьового запису в системі. При детальному перегляді спрацювань, можна побачити спільні для всіх батьківський процес cmd.exe (18356), який був запущений процесом svchost.exe (14400) (рис. 3.10.).

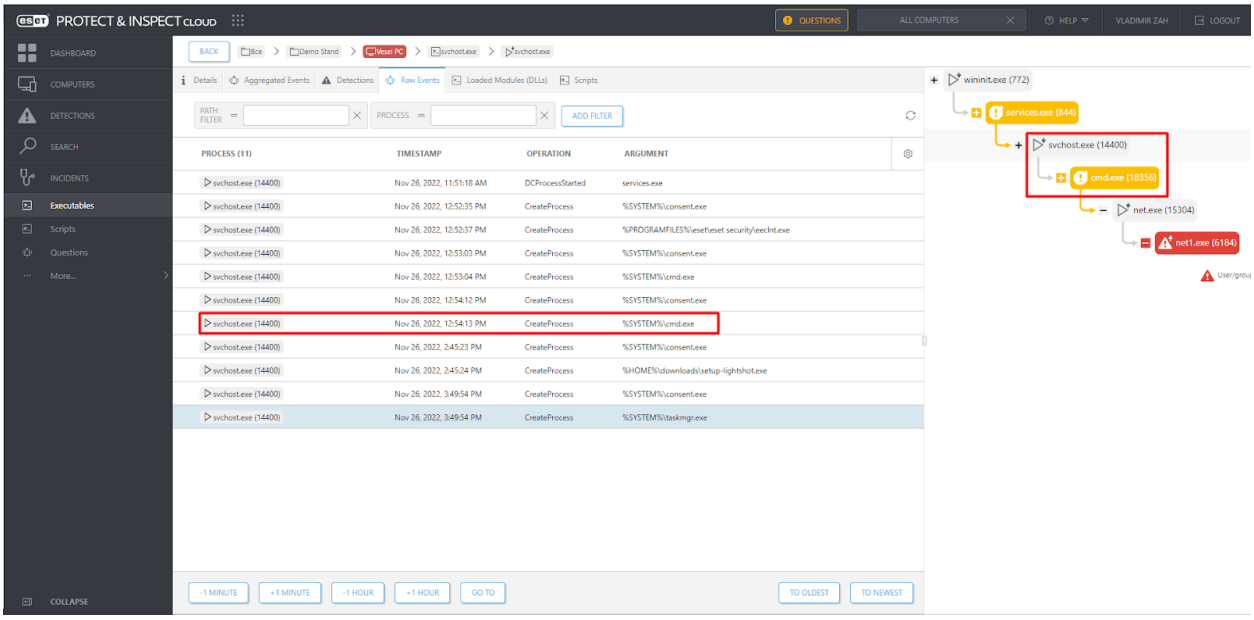



Рис. 3.10. Запуск cmd.exe (18356) від svchost.exe (14400)

Обидва процеси було додано до інциденту. З інформації про процес cmd.exe (18356) можна отримати багато цікавої інформації для розслідування. По-перше, при огляді агрегованих подій можна побачити події даного процесу пов’язані з модифікацією файлів та реєстру, а також мережі підключення які були зініційовано процесом (рис. 3.11.).

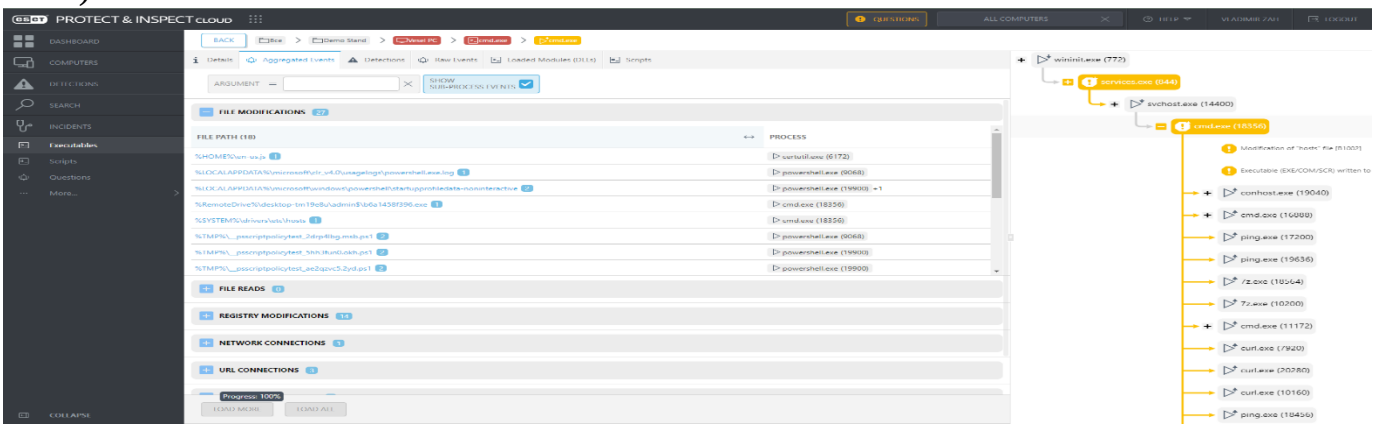



Рис. 3.11. Огляд файлів які були модифіковані

Також, за допомогою дерева процесі можна знайти процеси powershell.exe які були запущені через команду строку та переглянути вміст скриптів які запущені на кінцевій точці (рис. 3.12.).

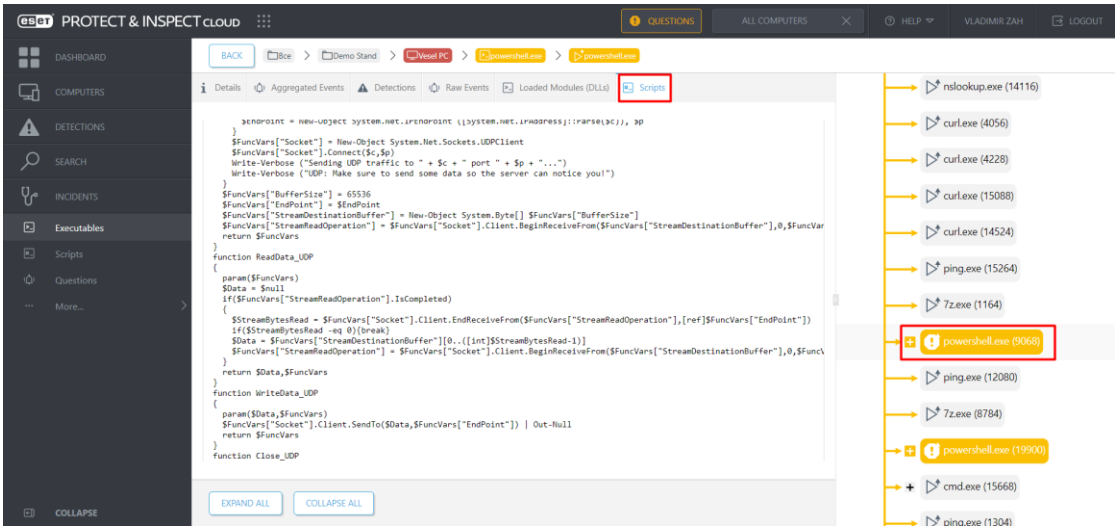



Рис. 3.12. Вміст одного з скриптів запущених під час симуляції

З інформації про процес cmd.exe (18356) можна перейти до повної хронології процесів на ПК Vesel-PC де можна побачити початок симуляції та події які виконувалися після запуску утиліти (рис. 3.13.).

| PROCESS (76095) | TIMESTAMP | OPERATION | ARGUMENT |
|---|---|---|---|
| ping.exe (19636) | Nov 26, 2022, 12:55:25 PM | ProcessCreated | %SYSTEM%\cmd.exe |
| chrome.exe (12404) | Nov 26, 2022, 12:55:27 PM | CreateProcess | %PROGRAMFILES%\google\chrome\application\chrome.exe |
| chrome.exe (10900) | Nov 26, 2022, 12:55:27 PM | ProcessCreated | %PROGRAMFILES%\google\chrome\application\chrome.exe |
| chrome.exe (12404) | Nov 26, 2022, 12:55:27 PM | CreateProcess | %PROGRAMFILES%\google\chrome\application\chrome.exe |
| chrome.exe (9556) | Nov 26, 2022, 12:55:27 PM | ProcessCreated | %PROGRAMFILES%\google\chrome\application\chrome.exe |
| wmiapsrv.exe (19948) | Nov 26, 2022, 12:55:27 PM | ProcessTerminate | %SYSTEM%\wbem\wmiapsrv.exe |
| ping.exe (19636) | Nov 26, 2022, 12:55:29 PM | ProcessTerminate | %SYSTEM%\ping.exe |
| cmd.exe (18356) | Nov 26, 2022, 12:55:29 PM | CreateProcess | %DESKTOP%\test\aptsimulator_pw_apt\aptsimulator\helpers\7z.exe |
| 7z.exe (18564) | Nov 26, 2022, 12:55:29 PM | ProcessCreated | %SYSTEM%\cmd.exe |
| 7z.exe (18564) | Nov 26, 2022, 12:55:29 PM | ProcessTerminate | %DESKTOP%\test\aptsimulator_pw_apt\aptsimulator\helpers\7z.exe |
| cmd.exe (18356) | Nov 26, 2022, 12:55:29 PM | CreateProcess | %DESKTOP%\test\aptsimulator_pw_apt\aptsimulator\helpers\7z.exe |

Рис. 3.13. Події на початку симуляції

На даному етапі, можна вважати інцидент повністю наповненим (у випадку, якщо не розглядати інші методики які були використані під час запуску AptSimulator). Загальна хронологія події можна побачити у створеному інциденті (рис. 3.14.).

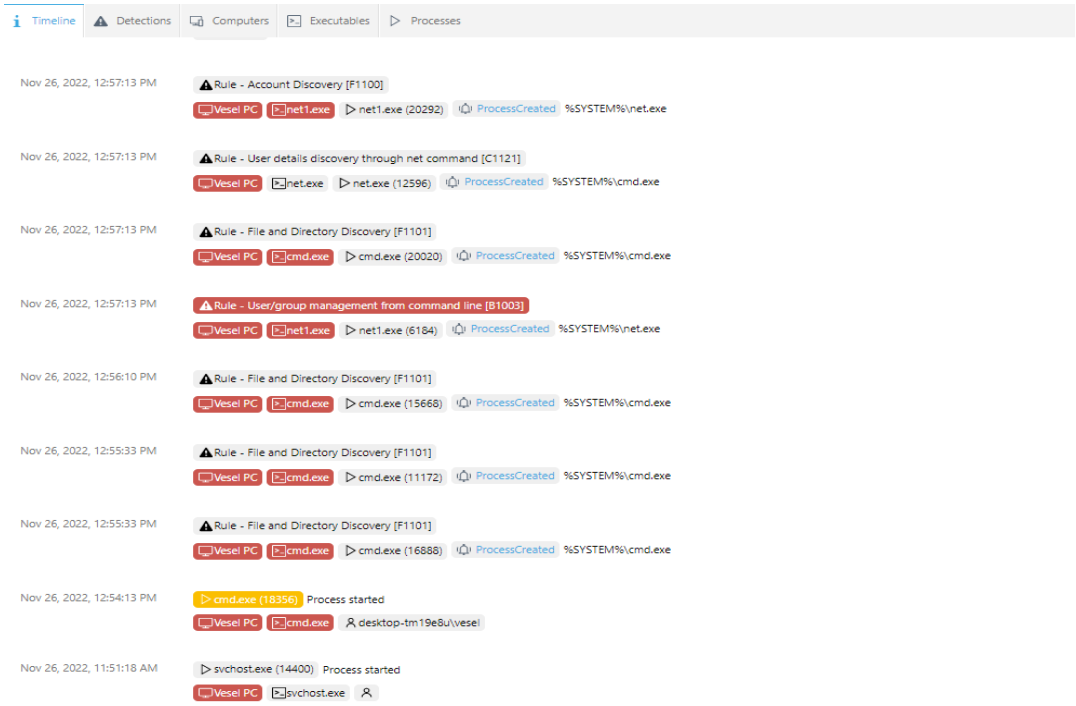



Рис. 3.14. Повна хронологія подій в інциденті

Загальний звіт про даний інцидент може мати наступний вигляд:

26.11.2022 на ПК Vesel-PC було зафіксовано підозрілу активність, яка полягала в додаванні користувачем адміністратора desktop-tm19e8u\vesel до локальних користувачів гостьовий запис. Під час розслідування, було виявлено, що процес cmd.exe(183560) який виконував ці дії, до цього запускав скрипти для збору даних про систему, а також перевіряв в локальних налаштуваннях параметри дозволу створення гостьових записів, а також список користувачів які наявні в системі. Ця поведінка класифікована як зловмисна. Під час аналізу подій пов'язаних з cmd.exe(183560), було виявлено створення тимчасових папок в ОС, завантаження скрипту з адреси https://raw.githubusercontent.com/nextronsystems/aptsimulator/master/download/cactus.js 2 і його запуск. Аналіз інших подій командного рядка показав, що активність була проведена за допомогою інструменту AptSimulator.

### 3.2. Технологія автоматизації збору додаткових даних для розслідування з кінцевих точок

Для розуміння функціоналу та можливостей ESET PROTECT в автоматизації реагування на атаки та збору додаткових даних для їх розслідування, розглянемо одну із практик яка була створена мною та моїми колегами Володимиром Захаренко та Заруцьким Романом, командою SOC українського представництва компанії ESET.

Для виявлення та реагування на складні та доволі критичні спрацювання, які можуть бути пов'язані з проведенням комплексної атаки на організацію або підготовку до такої атаки, ми створено динамічну групу (далі динамічна група Threats), яка буде фільтрувати кінцеві точки за наявністю в карантині певних спрацювань. Це такі спрацювання як Pterodo Win32/KillDisk, Win32/GenCBL, Win32/KillMBR, Win32/RiskWare.RemoteAdmin, WinGo/Filecoder, CobaltStrike, Industroyer, Filecoder.NKH, WannaCryptor, Filecoder.AES, Win32/Agent.AE, DOC/TrojanDownloader.agent, Win32/HyperBro, Win32/LuckyMouse, Win32/Korplug, Win64/Spy.Tmanger, Win32/Industroyer, Win32/Agent.AE, PowerShell/HackTool.Agent, Linux/Agent.PC, Linux/KillFiles, Win32/Exaramel, Win32/Agent, Linux/Agent, Linux/Exaramel, Win32/PSW.Agent, Win32/RiskWare.Mimikatz. При виявлені будь-якої з цих загроз на кінцевій точці автоматично буде запущено завдання на ізоляцію цієї машини від мережі, збір додаткових даних для розслідування, повне сканування кінцевої точки, відображення інформаційного повідомлення для користувача, а також адміністратор отримає сповіщення та звіт електронною поштою для інформування

про зараження або атаку. Ці задачі будуть відпрацьовувати по факту виявлення на комп'ютері загроз, зазначених в динамічній групі Threats (рис. 3.15-16.).

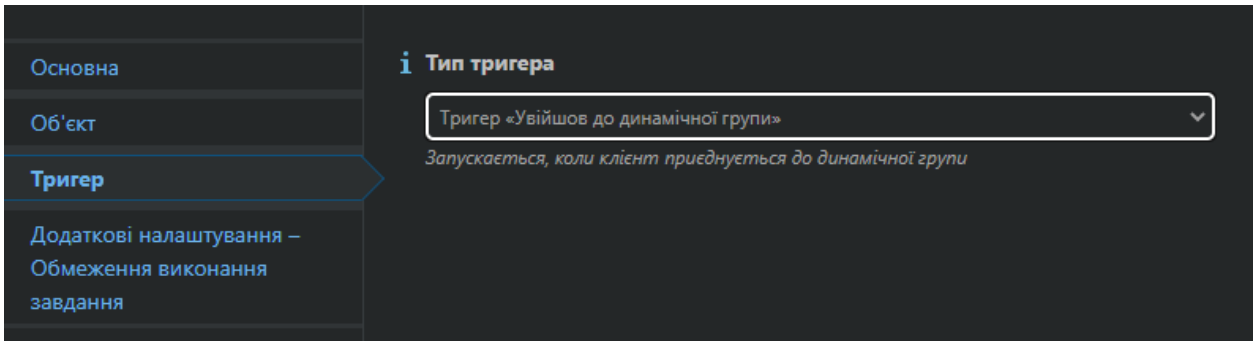



Рис. 3.15. Налаштування тригеру відпарювання задач

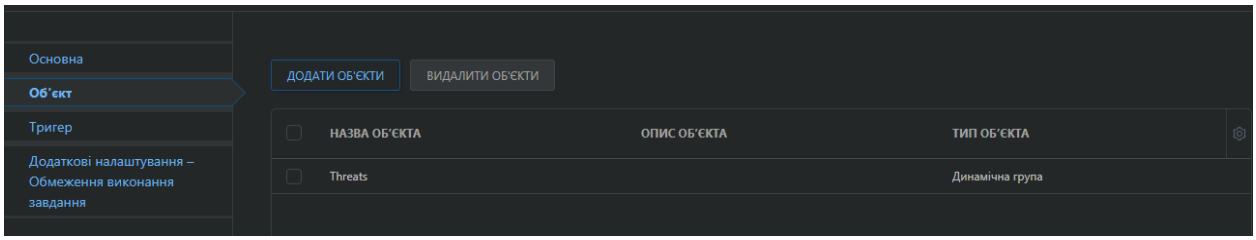



Рис. 3.16. Налаштування тригеру відпарювання задач

Розглянемо кожну з цих дій окремо.

Завдання на ізоляцію кінцевої точки, блокує всі підключення, за виключенням тих, які необхідні для правильної роботи продуктів ESET. Це дозволяє зменшити ризик того, що зловмисна активність буде розповсюджуватися на інші кінцеві точки в мережі, а зловмисники отримають до неї доступ. Однак, до цієї задачі треба підходити дуже обережно, так як, якщо кінцева точка не має прямого доступу до сервера, а наприклад, підключається до нього через VPN, то після виконання задачі можна втратити контроль над кінцевою точкою.

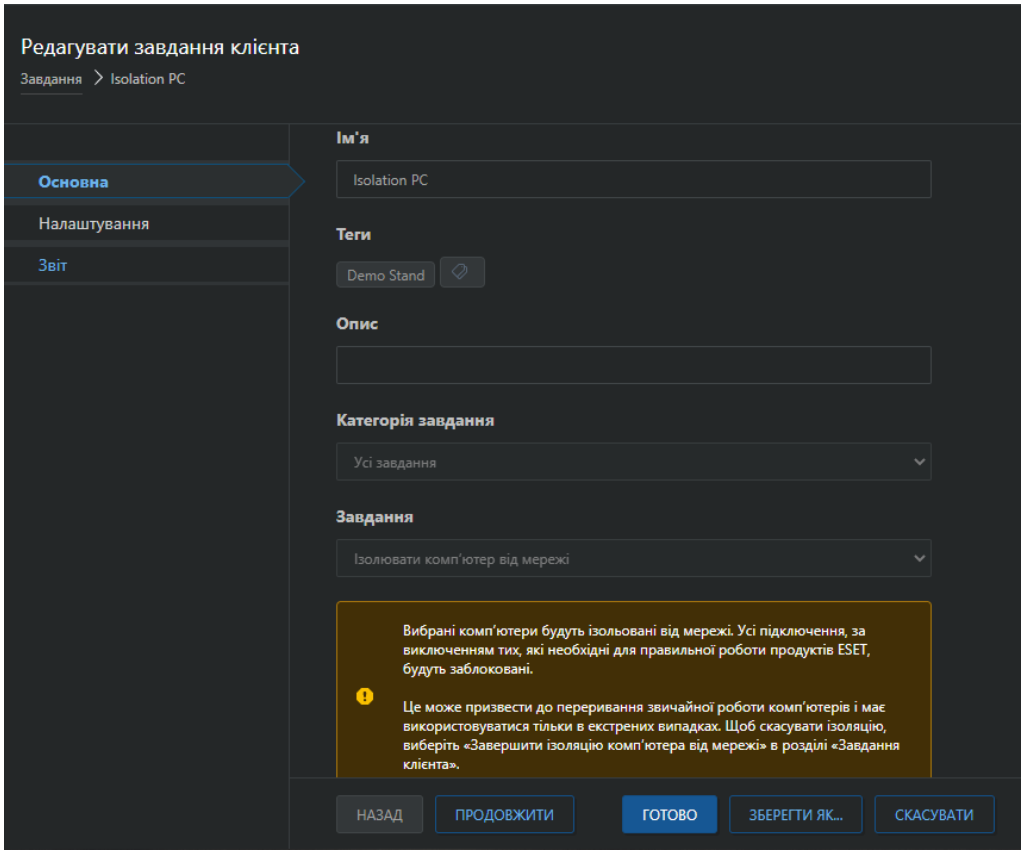
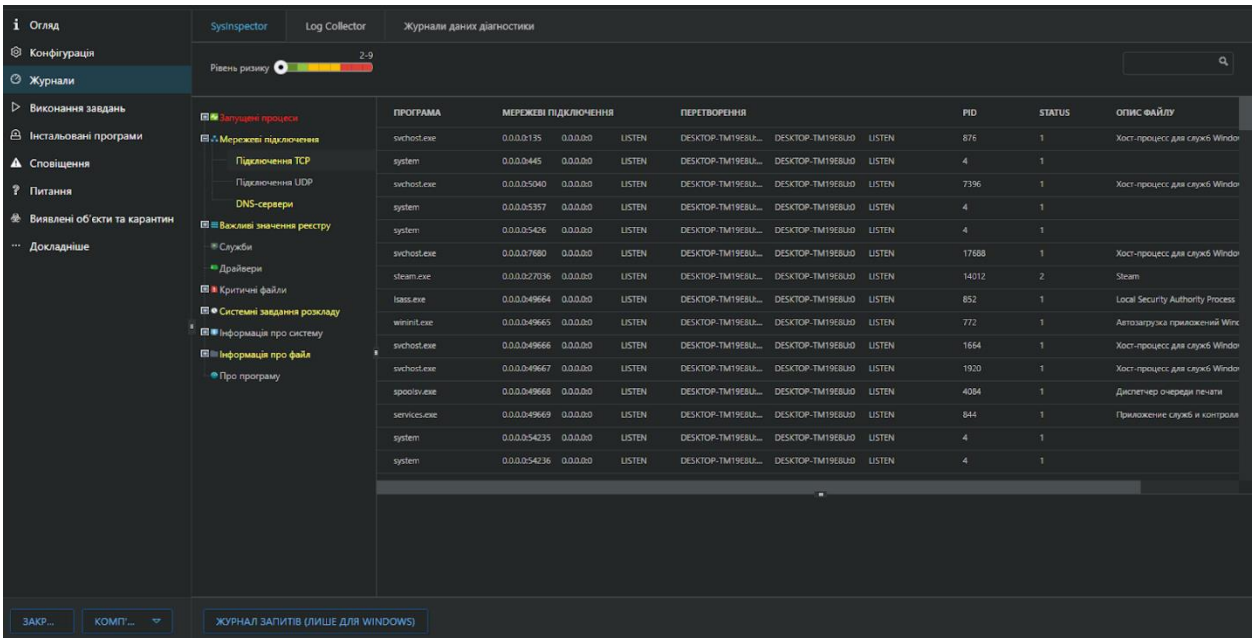



Рис. 3.17. Налаштування завдання по ізоляції ПК від мережі

За необхідністю, ізоляцію кінцевої точки можна швидко зупинити вручну або за допомогою задачі на зупинку ізоляції.

Для аналізу атак, спеціалістам з безпеки потрібні дані з кінцевої точки. Це як журнали продуктів захисту, так і операційної системи. Розглянемо інструменти за допомогою яких можливий збір подібних даних. Перший інструмент це ESET Log Collector. Ця утиліта допомагає зібрати журнали та конфігурацію продуктів ESET з кінцевої точки, що дозволяє дослідити журнали виявлень продуктів, а також отримати системну інформацію до якої вони мають доступ. Наступний інструмент це ESET SysInspector який збирає системні логи операційної системи та допомагає виявити критичні та підозрілі моменти. ESET SysInspector присвоює кожному запису певний рівень ризику, позначений відповідним кольором, що допомагає зручніше аналізувати зібрані дані. Журнали SysInspector можна збирати і за допомогою ELC, а можна

самостійною задачею в ESET PROTECT. Журнали зібрані цією задачею, можна відразу переглянути в консолі керування (рис. 3.18.).




Рис, 3.18. Перегляд журналу ESET SysInspector в веб-консолі ESET PROTECT

Останній інструмент це ESET System Vulnerability Checker (ESVC). Це внутрішня утиліта компанії ESET для пошуку вразливостей та зловмисної активності на кінцевій точці. Вона збирає системні журнали та журнали продуктів безпеки, після чого спеціальний додаток обробляє їх та видає таку інформацію як наявні вразливості операційної системи, спроби підбору паролю, локальні та віддалені підключення до кінцевої точки, список установленого ПЗ та інші параметри. Всі ці утиліти можливо запустити віддалено через завдання в ESET PROTECT. В адміністраторів є можливість запустити окремо кожну з цих утиліт або запустити комплексну утиліту ESET Log Master яку розробив Володимир Захаренко з команди ESET UA. Ця утиліта наразі існує в двох варіантах, у вигляді .exe файлу для локального запуску на кінцевій точці і у вигляді скрипту, який можна запустити як локально так і віддалено з консолі керування. Результатом виконання утиліти є зашифрований архів 7Zip який містить зібрані журнали та текстовий документ з ключем дешифрування. З точки зору принципів безпечної передачі даних ми рекомендуємо передавати архів і пароль до

нього різними каналами зв'язку. Важливо зауважити, що у випадку виконання скрипту, є можливість вказати мережеву шару, на яку буде збережено файли після збору (рис. 3.20.).

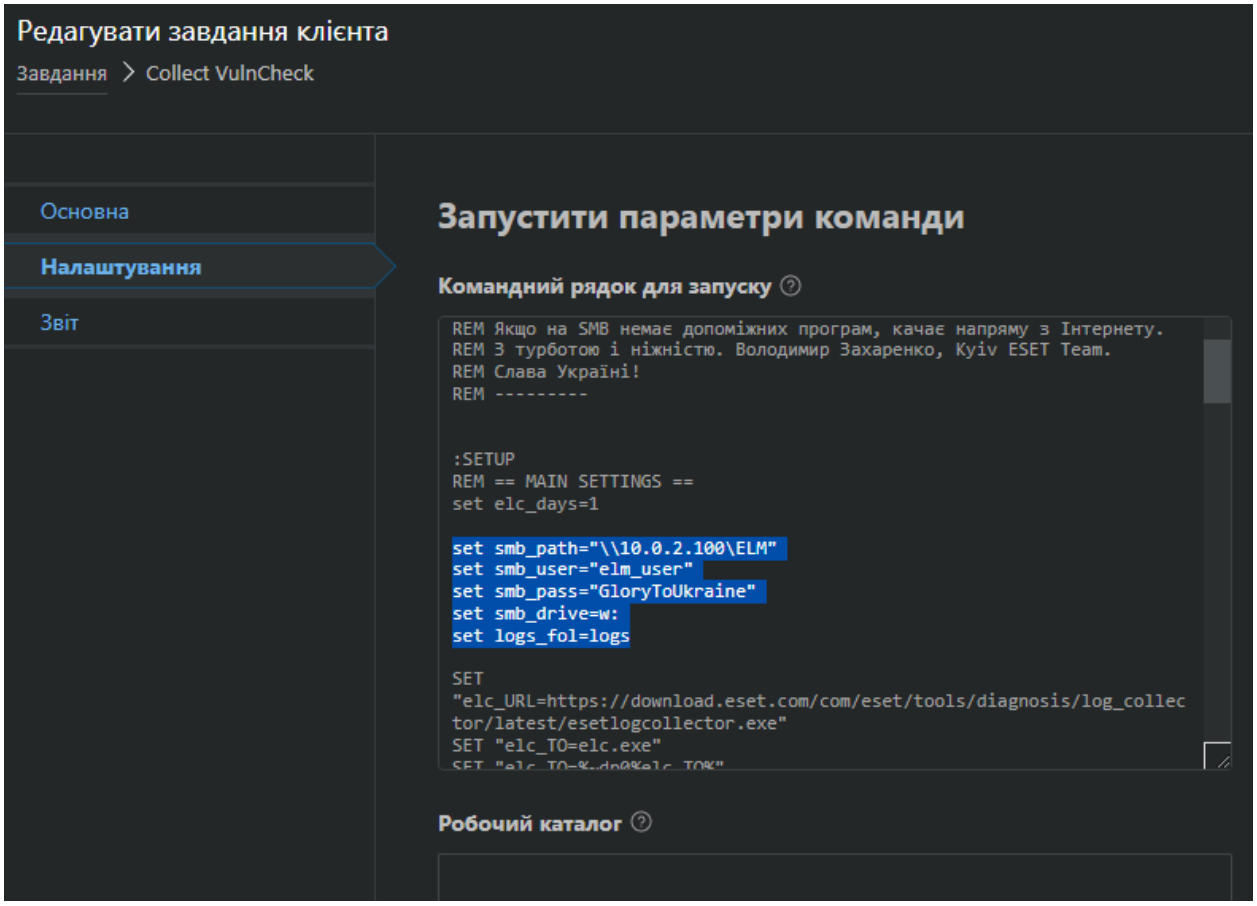



Рис. 3.20. Приклад задачі по запуску ESET Log Master

Задача на повне (детальне) сканування ПК потрібна для того, щоб проскандувати всю файлову систему після виявлення підозрілої активності. На практиці, дуже багато адміністраторів зневажають скануванням і зазвичай спираються тільки на захист файлової системи в реальному часу, хоча деякі загрози можуть не проявляти активність і бути незадетиктованими. Детальне сканування буде сканувати всі файли в системі і очищати будь-які знайдені умови (рис. 3.21.). Більш детальні параметри сканування можна налаштувати в політиці продукту захисту кінцевої точки.

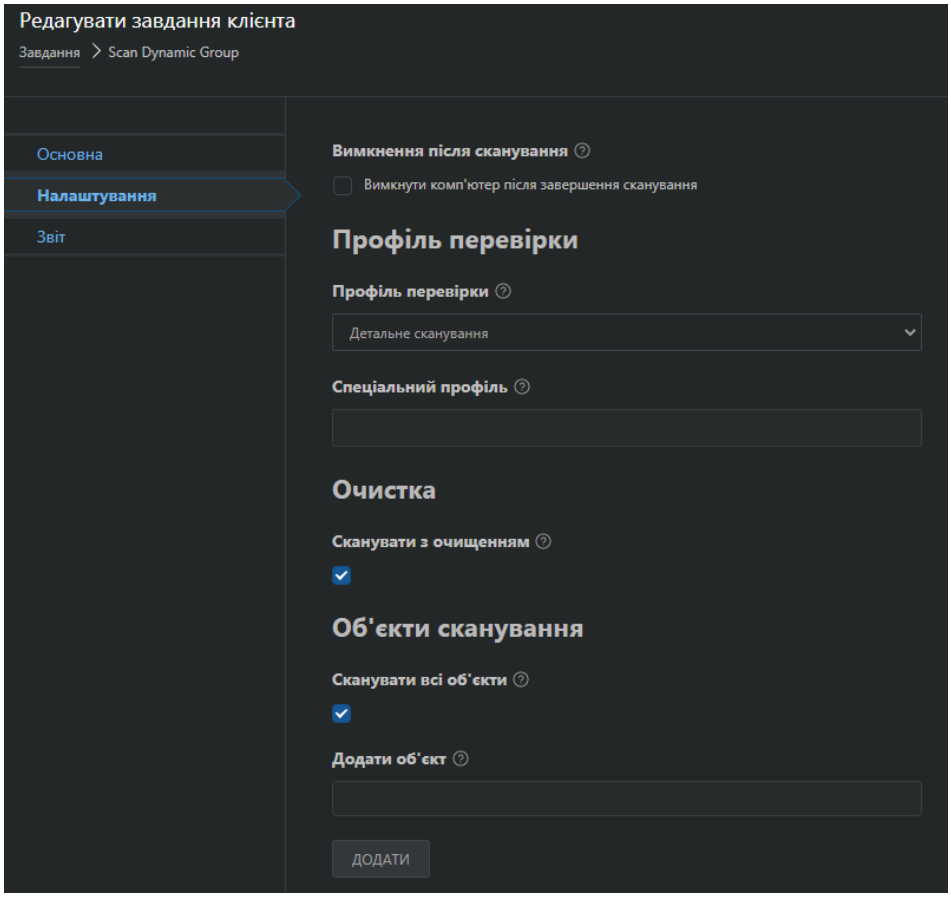



Рис. 3.21. Налаштування завдання сканування

Задача на відправлення повідомлення користувача потрібна для того, щоб працівник який працює за робочою станцією розумів чому в нього пропали мережеві з'єднання та зміг би сконтактувати з технічною підтримкою організації. Текст повідомлення може бути різний в залежності від потреб і побажань організації, наприклад мати наступний вигляд:

*“Шановний(а) користувач! На вашому комп'ютері була зафіксована зловмисна діяльність. На момент розслідування, ви будете ізольовані від мережі. Просимо сконтактувати з технічними спеціалістами за номером 111-222-333. Дякуємо за розуміння!”*

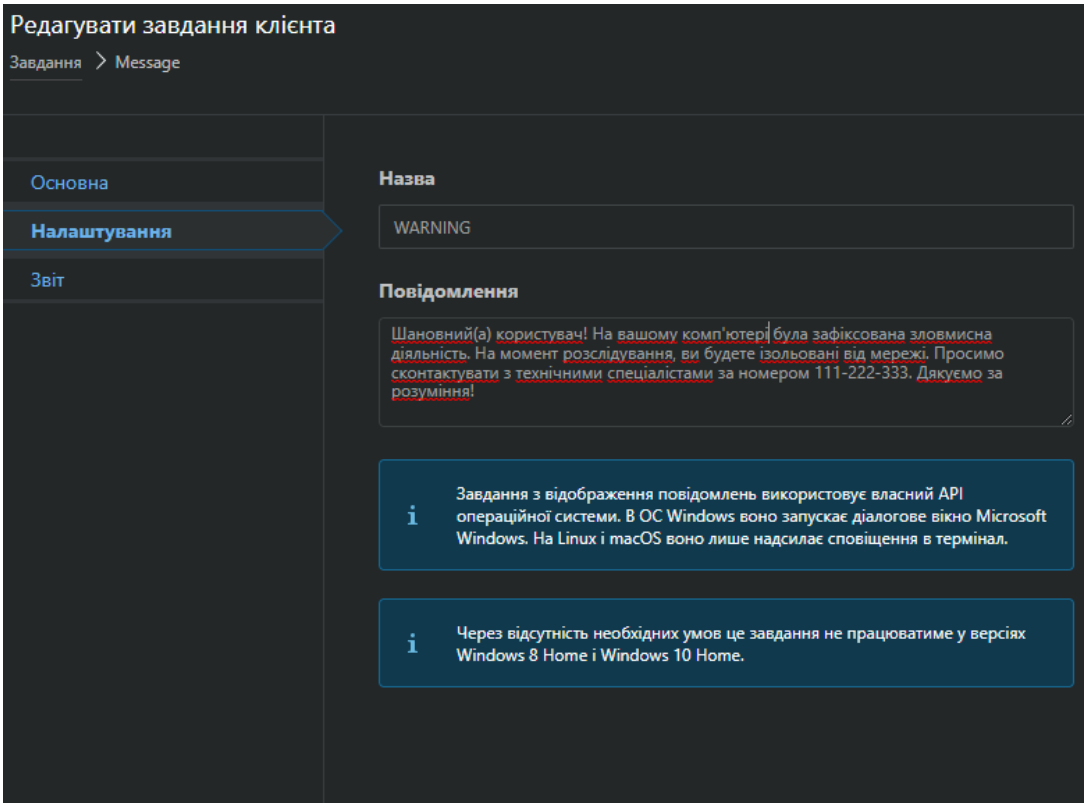



Рис. 3.22. Налаштування повідомлення для користувача

Адміністратори можуть отримувати різні звіти для аналізу атак і інцидентів. В даному випадку, можна використати два звіти. Це звіт про об’єкти в карантині та звіт про результати детального сканування, який ми запускали в попередньому пункті. Для відправки таких звітів треба запланувати їх відправлення, вибравши звіти які потрібні, тригер “Список учасників динамічної групи змінено” та вказати на яку адресу буде доставлено звіти (рис. 3.23-25.).

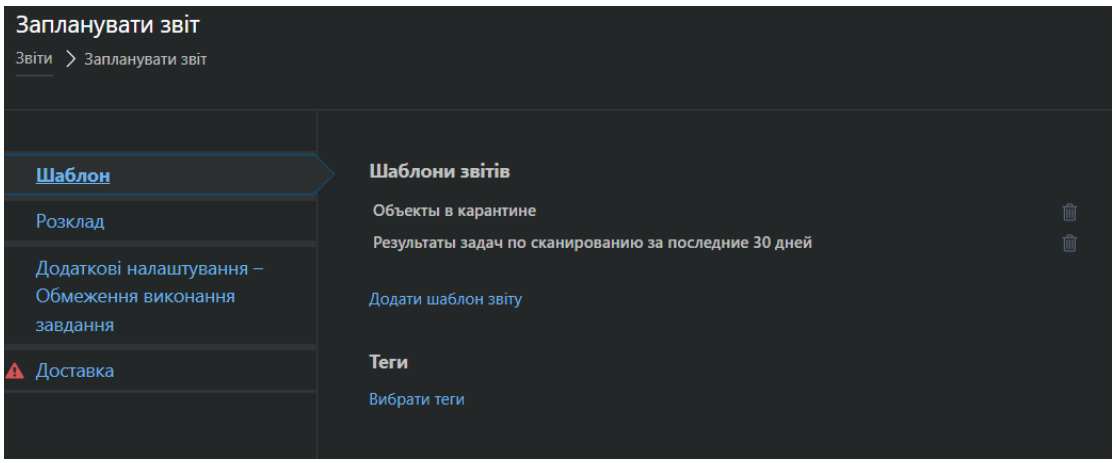



Рис. 3.23. Вибір звітів для відправки

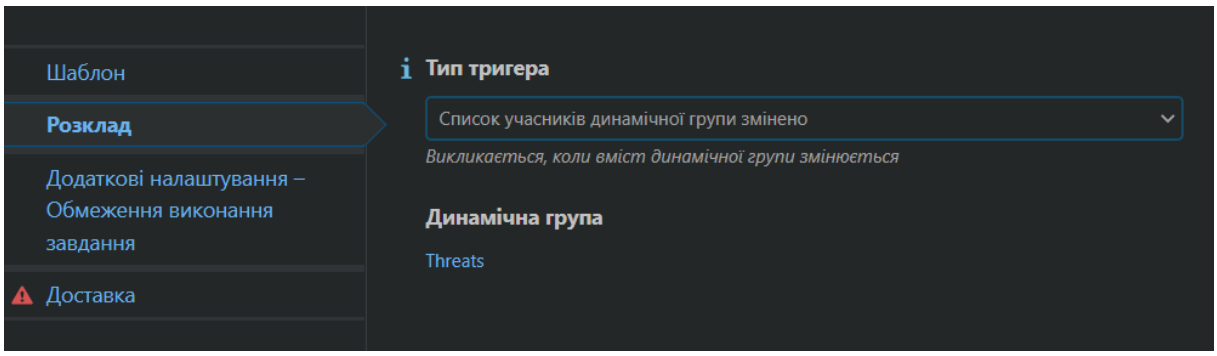



Рис. 3.24. Налаштування тригеру для відправки

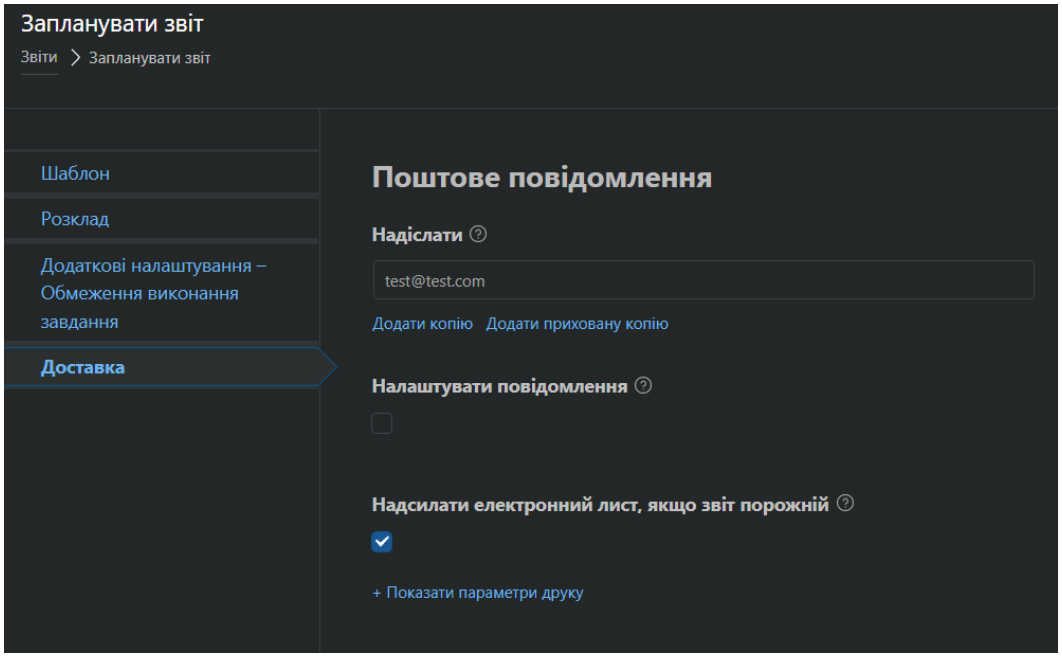



Рис. 3.25. Вибір адрес отримувачів

## 3.3. Розроблення рекомендацій щодо застосування рішень ESET для розслідування кіберінцидентів

На основі даної магістерської роботи та на основі власного досвіду роботи з кіберінцидентами, як сертифікованого технічного спеціаліста компанії ESET, я можу надати наступні рекомендації при розслідувані кіберінцидентів на базі рішень ESET:

1. Адміністратори безпеки повинні по максимуму використовувати можливості автоматизації рішення ESET PROTECT&Inspect для автоматизації процесів реагування та розслідування. Для автоматизації можна використовувати як рекомендації з Розділу 3.2. даної роботи, так і власний досвід, наприклад, для створення користувацьких правил в ESET Inspect;

2. Потрібно проводити постійний аудит спрацювань ESET Inspect для виявлення зловмисної або несанкціонованої активності користувачів з метою запобігати діям, які можуть призвести до зниження рівня захисту, спричинити витік даних чи зупинення критично важливих процесів або будь-яку іншу шкоду;

3. Потрібно проводити постійний аудит виконуваних файлів та виконаних сценаріїв в ESET Inspect з метою виявлення та блокування несанкціонованих спрацювань та розслідування їх запуску;

4. Інструмент створення інцидентів допомагає зручно зібрати разом всі пов’язанні події під час розслідування кіберінцидентів в ESET Inspect;

5. Під час розслідування дуже важливо використовувати механізм пошуку в ESET Inspect для детального пошуку спрацювань, процесів, подій, тощо по певним індикатором які були знайдені під час розслідування;

6. Для отримання більш детальної інформації про процеси треба переглядати детальну інформацію про нього, особливо агреговані події по категоріям, Raw Events та інформацію про скрипти які були запущені процесом;

7. Створення регулярних знімків стану ОС для можливості проведення порівняльного аналізу у разі необхідності за допомогою інструменту SysInspector та аналіз журналів, отриманих з проблемних об’єктів захисту для визначення причин та усунення недоліків на рівні всієї інфраструктури;

8. Розслідування інцидентів повинні проводитися класифікованими спеціалістами, які розуміють принципи роботи ОС, мережевих зв’язків, методів зловмисників, роботи шкідливого ПЗ, тощо;

9. При необхідності виявлення специфічних спрацювань, рекомендую, створити для цього спеціальне правило в ESET Inspect з вказуванням потрібних для розслідування параметрів. Такий метод є більш ефективнішим ніж пошук даних спрацювань за допомогою відповідного інструменту [18];

10. Під час аудиту спрацювань, рекомендую опрацьовувати їх по рівню критичності, спочатку опрацьовуючи критичні спрацювання (червоні), потім спрацювання попередження (жовті), а потім вже інформаційні спрацювання (білі);

11. Для отримання першочергової інформації під час розслідування можна використовувати дерево процесів, для визначення дій зловмисників, до зафіксованого спрацювання і після;

12. Використання описаних технік реагування в вбудованих правилах від ESET, а також методики Mitre att&ck може допомогти офіцерам безпеки з визначенням наступних кроків розслідування та реакції на спрацювання;

13. При аналізі спрацювань, дуже важливо звертати увагу на параметри запуску процесів, так як вони зазвичай містять дуже важливу інформацію для розуміння наслідків які процес міг залишити в системі.

# ВИСНОВКИ

У магістерській роботі проведено аналіз технологій проведення розслідування кіберінцидентів в ІТС на базі рішень ESET, а також проблеми які можуть виникати під час розслідування. Продемонстровано та обґрунтовано методи розслідування кіберінцидентів.

Розроблено технологію реагування та подальшого розслідування кіберінцидентів на базі рішення ESET PROTECT&Inspect.

У результаті магістерській роботі вирішено такі наукові завдання:

1. Визначені принципи проведення розслідування кіберінцидентів в ІТС та проаналізовані основні проблеми під час розслідування та запропоновані варіанти їх вирішення.

2. Проаналізовано та досліджено рішення компанії ESET, їх архітектуру та функціонал.

3. Продемонстрований процес розслідування інциденту за допомогою рішення ESET PROTECT&Inspect на прикладі симульованої атаки в тестовому середовищі.

4. Розглянуто автоматизацію процесу реагування та розслідування за допомогою інструментів компанії ESET, що дозволяє побудувати складну систему для зниження часу реакції офіцерів безпеки та автоматизації процесу розслідування.

5. Розроблені рекомендації для спеціалістів з інформаційної безпеки по проведенню розслідування на базі рішень компанії ESET.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Закон України : від 05.07.1994 р. № 81/94–ВР "Про захист інформації в інформаційно–телекомунікаційних системах" [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

2. Achkoski J. CYBER TERRORISM AND CYBER CRIME – THREATS FOR CYBER SECURITY / J. Achkoski, M. Dojchinovski. // Military Academy “General Mihailo Apostolski ”, 2020. – 8 с.

3. Закон України : від 17.08.2022 р. " Про основні засади забезпечення кібербезпеки України" [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

4. ESET APT Activity Report T2 2022 [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.welivesecurity.com/2022/11/14/eset-apt-activity-report-t2-2022/.

5. ПЕРЕЛІК категорій кіберінцидентів [Електронний ресурс] – Режим доступу до ресурсу: https://cert.gov.ua/recommendation/16904.

6. Постанова Кабінету Міністрів України "Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки" [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text.

7. Sood A. K. Targeted Cyberattacks: A Superset of Advanced Persistent Threats. / A. K. Sood., 2013.

8. Загальний опис ESET Protect [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/protect_admin/10.0/uk-UA/.

9. Панель інструментів | ESET Protect [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/protect_admin/90/uk-UA/?dashboard.html.

10. Intelligence-driven computer network defenses informed by analysis of adversary campaigns and intrusion kill chains. / E. M. Hutchins, M. J. Cloppert., 2011.

11. ESET Inspect [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/ei/1.8/en-US/

12. ESET Endpoint Security [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/ees/10/uk-UA/.

13. Глосарій ESET [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/glossary/uk-UA.

14. ESET LiveGuard Advanced [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/elga/uk-UA/.

15. Multi-Factor Authentication - PCI Security Standards Council [Електронний ресурс] – Режим доступу до ресурсу: https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf.

16. Огляд ESET Secure Authentication [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/esa/30/uk-UA/.

17. ESET Threat Intelligence [Електронний ресурс] – Режим доступу до ресурсу: https://help.eset.com/eti/en-US/.

18. Garbis J. Zero Trust Security / J. Garbis, J. Chapman. – Boston, MA, USA: apress, 2021. – 427 с.