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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення та реагування на загрози в корпоративній мережі на базі Trend Micro Deep Discovery»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

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

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

_____ Олександр ІЛЛЮША
(підпис)

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

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

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

Київ 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NDR – Network Detection and Response

ZDI – Zero Day Initiative

APT – Advanced Persistent Threats

C&C – Command & Control Communication

ШІ – Штучний Інтелект

МН – Машинне Навчання

DDI – Deep Discovery Inspector

DDAn – Deep Discovery Analyzer

SIEM – Security information and event management

EDR – Endpoint Detection and Response

XDR – Extended Detection and Response

IDS/IPS – Intrusion Detection and Prevention Systems

NGFW – Next Generation Firewall

ВСТУП

Актуальність дослідження. Переважна більшість атак, які починаються з кінцевих точок, є лише першим кроком у спробі отримати доступ до мережі. Незважаючи на те, що все більше людей працюють з дому або поза офісом, вони все одно підключаються до мережі, яка є основним вектором атаки для хакерів.

Потрапивши в мережу, система безпеки, орієнтована на периметр, не бачить атаки і навіть не підозрює про її існування. Загроза може вільно переміщатися по мережі з невеликим шансом бути виявленою. У цьому випадку потрібні контрзаходи, щоб гарантувати, що зловмисна активність, яка рухається мережею з інфікованих машин, буде виявлена і належним чином оброблена.

Мережеве виявлення та реагування (NDR) - це клас рішення, який набуває все більшого визнання та значення серед фахівців з кібербезпеки та аналітичної спільноти. Мережеве виявлення та реагування дозволяє організаціям відстежувати мережевий трафік, що рухається по мережі на вході, виході та всередині (бокове переміщення), на предмет зловмисної активності та підозрілої поведінки. Після виявлення загрози на неї можна реагувати на мережевому рівні та за його межами. Заходи реагування можуть бути автоматизованими або ручними для полювання на загрозу або для посилення контролю. Тому тема кваліфікаційної роботи є актуальною.

Об'єкт дослідження – процес виявлення та реагування на загрози в корпоративній мережі.

Предмет дослідження – технологія виявлення та реагування на загрози в корпоративній мережі на базі рішень Trend Micro Deep Discovery.

Мета роботи – розробити варіант розгортання технології виявлення та реагування на загрози в корпоративній мережі на базі рішень Trend Micro Deep Discovery та рекомендації щодо застосування даної технології.

Наукові завдання:

- проаналізувати призначення та функції корпоративної мережі організації;
- провести аналіз проблеми виявлення та реагування на загрози в корпоративній мережі;
- проаналізувати основні загрози корпоративній мережі організації;
- проаналізувати методи та засоби виявлення та реагування на загрози в корпоративній мережі;
- розробити варіант розгортання системи виявлення та реагування на загрози в корпоративній мережі на базі рішень Trend Micro Deep Discovery та рекомендації щодо застосування даної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу виявлення та реагування на загрози в корпоративній мережі на базі рішень Trend Micro Deep Discovery.

Практичне значення одержаних результатів полягає в розробці технології розгортання системи виявлення та реагування на загрози в корпоративній мережі на базі рішень Trend Micro Deep Discovery та рекомендації щодо застосування даної технології в залежності від розмірів організації, що дозволить забезпечувати необхідний рівень кібербезпеки організації.

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

1 АНАЛІЗ НЕОБХІДНОСТІ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ В КОРПОРАТИВНІЙ МЕРЕЖІ

1.1 Архітектура, призначення та функції корпоративної мережі

Архітектура корпоративної мережі - це мережева архітектура, яка використовується для з'єднання комп'ютерів і пристроїв на підприємстві, наприклад, на підприємстві або в школі. Компоненти корпоративної мережі можна умовно поділити на три категорії: мережеве обладнання, мережеве програмне забезпечення та мережеві сервіси. Мережеве обладнання включає такі пристрої, як маршрутизатори, комутатори та фізичні сервери. Мережеве програмне забезпечення працює або на виділеному обладнанні, або на звичайних серверах. Мережеві сервіси - це програмні додатки, які працюють на серверах і забезпечують ряд функцій, таких як зберігання даних, безпека та зв'язок.

Існують три основні типи корпоративних мереж: локальні мережі (LAN), хмарні мережі та гібридні (локальна мережа у поєднанні з хмарними сервісами).

1. Локальні мережі - це приватні мережі, які зазвичай використовуються в межах однієї будівлі або офісу. Вони, як правило, швидкі та безпечні, але можуть бути дорогими у налаштуванні та обслуговуванні.

2. Хмарні мережі - це тип глобальної мережі, який використовує Інтернет для об'єднання локальних мереж. Хмарні мережі зазвичай є найдешевшим і найзручнішим варіантом корпоративної мережі, але вони можуть бути менш безпечними і надійними, ніж інші варіанти.

3. Гібридна хмарна мережа - це мережа, яка забезпечує передачу даних між локальними IT-ресурсами, приватними хмарами та публічними хмарами, іншими словами, гібридною хмарою. Гібридні хмарні обчислення підтримують переміщення робочих навантажень між цими середовищами і пов'язані між собою телекомунікаційними і хмарними сервісами та інфраструктурою, яка підтримує ці зв'язки.

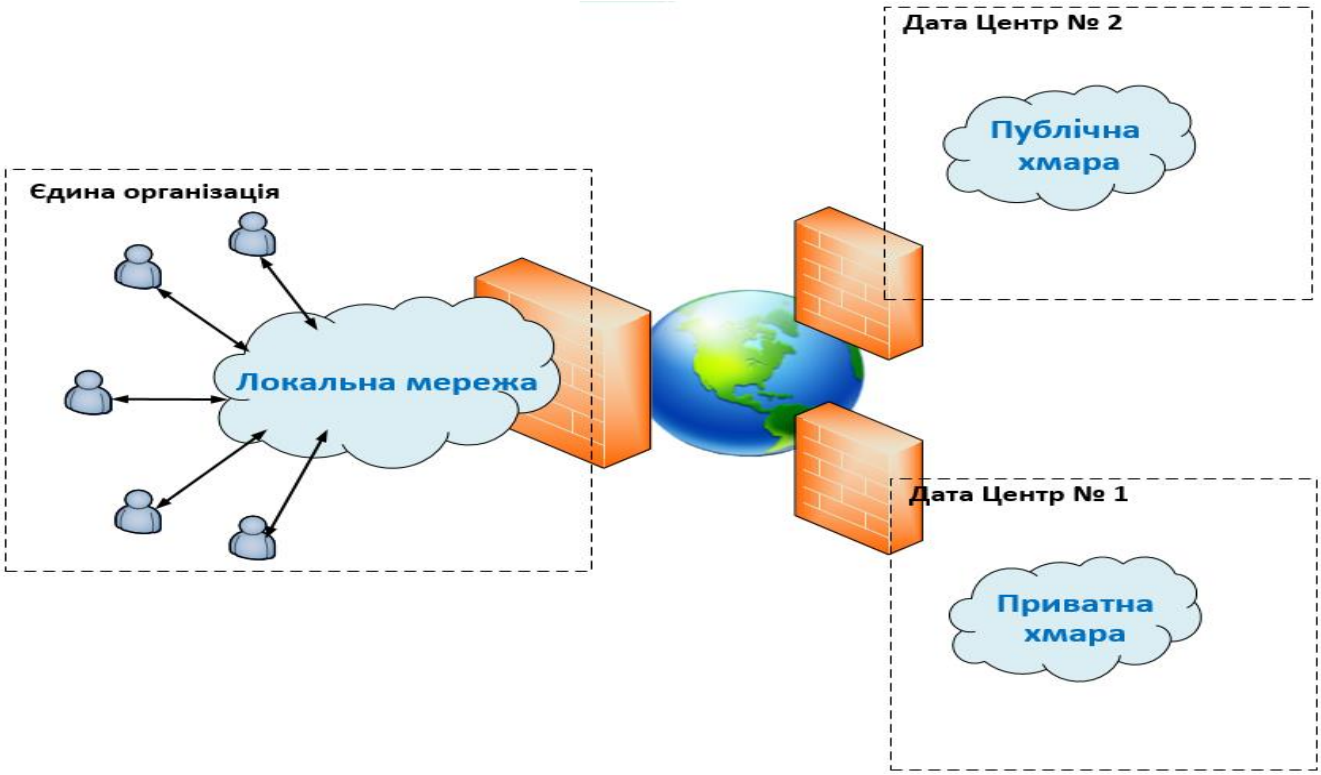


Рис 1.1 – Графічне відображення роботи локальної мережі у поєднанні з приватними хмарами

Корпоративна мережа є основою для полегшення комунікацій в організації та з'єднання комп'ютерів і пристроїв у всіх частинах корпоративної мережі. Зазвичай мережеве середовище підприємства налаштовується так, щоб полегшити доступ до даних та аналітики. Щоб забезпечити належне функціонування корпоративної мережі, важливо мати чітке уявлення про комунікаційні потреби організації та пристрої, які будуть підключені до мережі. Нижче наведено чотири основні концепції, якими слід керуватися при побудові корпоративної мережі:

1. Відмовостійкість: Відмовостійка мережа - це мережа, яка обмежує кількість пристроїв, на які впливають несправності, оскільки Інтернет іноді виходить з ладу.

2. Масштабованість: Здатність мережі розширюватися для розміщення додаткових користувачів або пристроїв без втрати продуктивності або надійності.

3. Якість обслуговування (QoS): Гарантія того, що критично важливі програми отримають необхідні ресурси, коли вони їм потрібні.

4. Безпека: Здатність захистити дані та пристрої від несанкціонованого доступу або крадіжки.

Корпоративна мережа забезпечує безпечне з'єднання між комп'ютерами та пристроями в організації. Це усуває ізольованість користувачів або команд і забезпечує безпечну та безперебійну передачу даних і зв'язок всередині та зовні з працівниками, діловими партнерами та клієнтами. Мережа - це процес з'єднання пристроїв разом, щоб вони могли взаємодіяти.

Управління мережею складається з п'яти функціональних областей: управління несправностями, управління конфігурацією, управління продуктивністю, управління безпекою та управління обліком.

1. Управління несправностями - це процес виявлення та виправлення будь-яких помилок в системі.

2. Управління конфігурацією - це процес моніторингу та підтримки пристроїв і мережевих конфігурацій.

3. Управління продуктивністю - це процес моніторингу та оптимізації продуктивності мережі.

4. Управління безпекою - це процес захисту мережі від будь-яких потенційних загроз.

5. Управління обліком - це процес відстеження та звітування про використання мережі.

Архітектура підприємства - це дисципліна, яка може допомогти організаціям проактивно реагувати на деструктивні сили. Архітектура передбачає визначення та аналіз виконання змін, спрямованих на досягнення бажаного бачення бізнесу та результатів. Це може допомогти організаціям приймати кращі рішення щодо того, як реагувати на підривні сили та досягати бажаних результатів.

Мета архітектури підприємства - забезпечити основу для обговорення та оцінки IT-активів та бізнес-процесів в організації. Це обговорення повинно бути

постійним, а зміни в бізнес-стратегії повинні відображатися в змінах в архітектурі підприємства. Для керівництва цими обговореннями слід використовувати керівні принципи, які гарантують, що вони ґрунтуються на загальній місії та цілях організації. Мережева безпека також є критично важливим компонентом будь-якої комп'ютерної мережі. Вона допомагає захистити мережу від несанкціонованого доступу і від різних атак.

1.2 Аналіз сучасних загроз корпоративній мережі

Налаштування кібербезпеки вимагає глибоких знань і ноу-хау, і вони не є взаємовиключними.

Купівля одного або декількох продуктів безпеки та можливість їх встановлення – це, безумовно, важлива частина створення надійного захисту. Але якщо організації не знають, від чого вони намагаються захиститися, то не можуть бути впевнені, що те, що у них є, забезпечить належний захист.

Вразливості можуть бути відомими, невідомими та нерозкритими, і дуже важливо знати, чи забезпечує обраний підхід до захисту покриття всіх цих типів вразливостей.

Відомі вразливості

Такий тип вразливостей відомий громадськості та засобам захисту. Ці вразливості або загрози додаються до баз даних репутації, усуваються фізичними та віртуальними виправленнями, для них написані файли шаблонів безпеки або створені сигнатури експлойтів для їх блокування. Незважаючи на те, що вразливості відомі, багато з них все одно проникають в систему - зазвичай через несвоєчасне виправлення в програмному забезпеченні. Нижче, на малюнку 1.5, представлений варіант використання відомої вразливості.

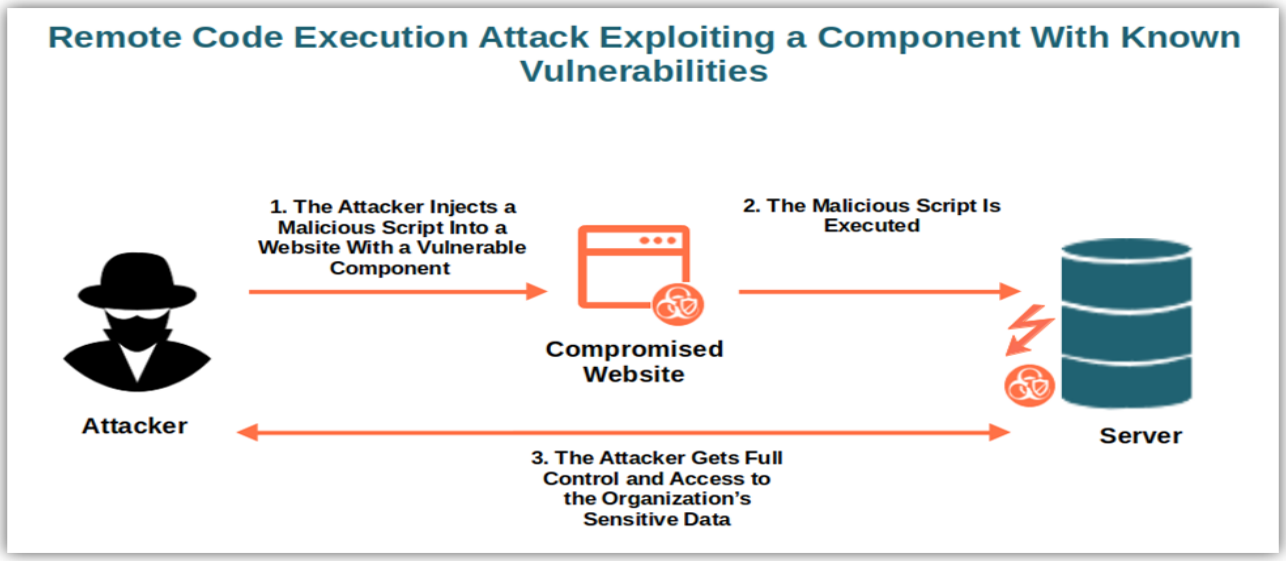


Рис.1.5 – Приклад віддаленого виконання коду за допомогою відомих вразливостей

Невідомі загрози

Невідомі загрози ніколи не зустрічалися раніше і, як правило, створюються спеціально для нападу на окрему особу або підприємство. Ці цілеспрямовані атаки і просунуті загрози налаштовані так, щоб обійти звичайні засоби захисту, і можуть залишатися прихованими, викрадаючи конфіденційні дані або шифруючи критично важливі дані до тих пір, поки не будуть виконані вимоги викупу. Невідомі загрози часто призначені для впливу на одну систему або невелику групу комп'ютерів. Ці цілеспрямовані атаки часто є багатовекторний вплив, зокрема, електронні листи, посилання, завантаження та внутрішні переміщення в корпоративній мережі.

Невиявлені вразливості «нульового дня»

Термін «нульовий день» став загальним для опису будь-якого типу загроз, які ще не були розкриті, але вже використовуються зловмисниками.

Існує три різних типи загроз "нульового дня", про які організаціям слід знати:

1) Вразливості нульового дня (рис. 1.2): Це вразливості, які ще не виявлені та не відомі більшості країн світу. Вже 13-й рік поспіль ZDI (Zero Day Initiative)-міжнародна ініціатива щодо вразливості програмного забезпечення - є світовим лідером у виявленні та розкритті вразливостей нульового дня. У 2020 році ZDI розкрила 60,5% повідомлених вразливостей, що більше, ніж всі інші постачальники

разом узяті. Життєвий цикл вразливості нульового дня продемонстрований на рисунку 1.6.

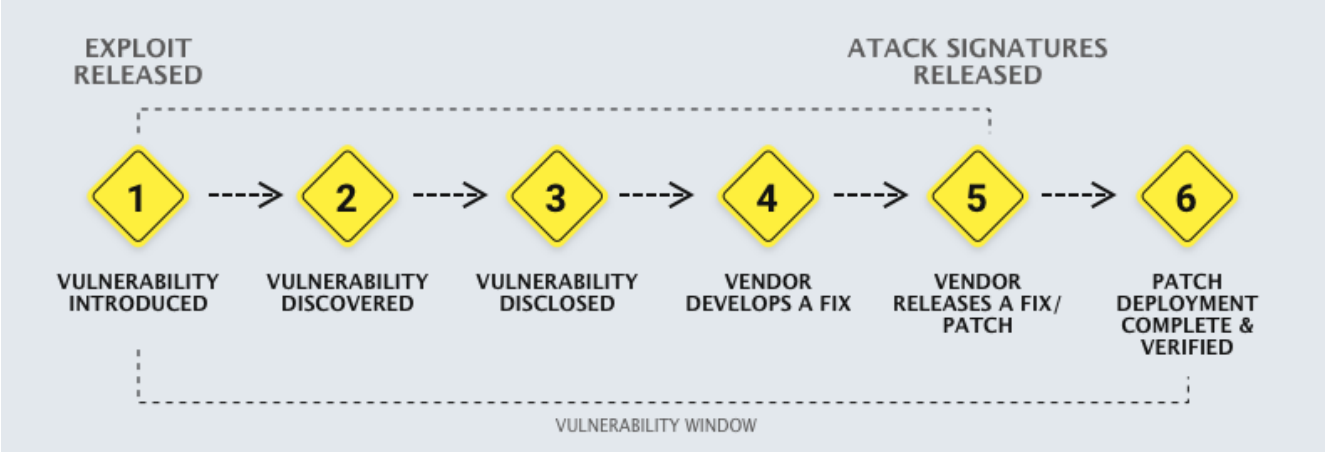


Рис. 1.6 – Життєвий цикл вразливості нульового дня

2) Експлойти нульового дня: Експлойт - це код, написаний спеціально для використання вразливості. Одна вразливість може мати сотні експлойтів, націлених на неї, кожен з яких використовує варіацію загальної техніки. Коли зловмисник створює абсолютно новий спосіб використання відомої вразливості, це називається експлойтом нульового дня. Для виявлення експлойтів "нульового дня" та цілеспрямованих атак більшість постачальників засобів захисту використовують комбінацію технологій, зокрема машинне навчання, евристику, виявлення аномалій та «пісочницю».

3) Шкідливе програмне забезпечення нульового дня: Переважна більшість шкідливих програм використовує відомі вразливості програмного забезпечення для отримання підвищених привілеїв доступу та зараження комп'ютера. Якщо шкідливе програмне забезпечення відоме постачальникам засобів захисту, його хеш-підпис можна виявити під час транспортування, що дозволяє їхнім рішенням відфільтрувати та заблокувати шкідливе програмне забезпечення. Але, змінивши лише один фрагмент коду, можна змінити всю сигнатуру, створивши нове, невідоме шкідливе програмне забезпечення, яке ніхто ніколи не бачив. Якщо це нове шкідливе програмне забезпечення нульового дня використовує вразливості нульового дня або експлойти нульового дня (або навіть і те, і інше), його майже неможливо виявити за допомогою звичайних засобів.

Нижче, на рисунку 1.7, зображено цикл атаки нульового дня.

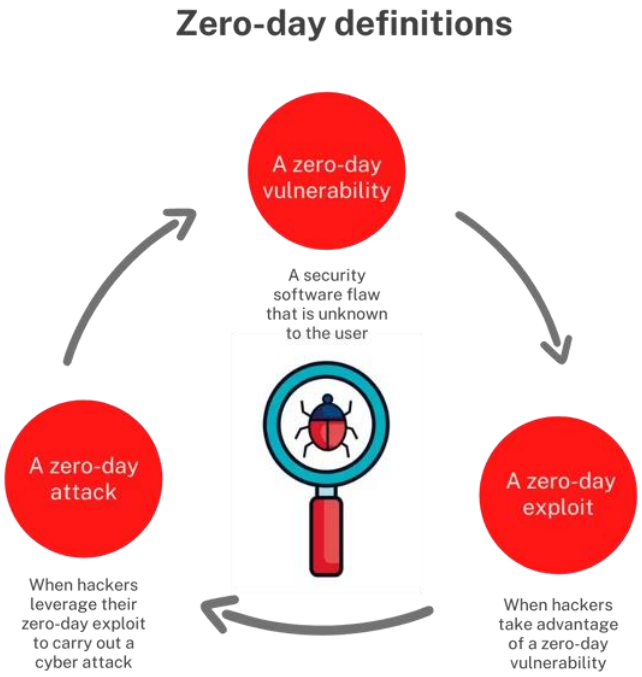


Рис. 1.7 – Цикл атаки нульового дня

1.3 Аналіз циклу сучасної кібератаки

Цільові атаки та сучасні постійні загрози (APT - Advanced Persistent Threats) - це високоорганізовані, цілеспрямовані зусилля, спеціально створені для проникнення в організації з метою отримання доступу до внутрішніх систем, даних та інших цінних активів.

Ланцюг ураження, спочатку придуманий військовими, - це концепція, яка визначає структуру атаки. Пізніше інженери корпорації Lockheed-Martin адаптували концепцію «ланцюга вбивств» (kill chain) для моделювання атак і вторгнень у комп'ютерні мережі. З часом «ланцюг вбивств» для кібербезпеки став відомий як життєвий цикл APT-атаки.

Цикл атаки APT розкриває етапи цілеспрямованої кібератаки від початкової розвідки до фінального витоку даних. Слід зауважити, що хоча кожна атака

пристосована до своєї цілі, вона, як правило, проходить безперервний процес з шести ключових етапів (рисунок 1.8).

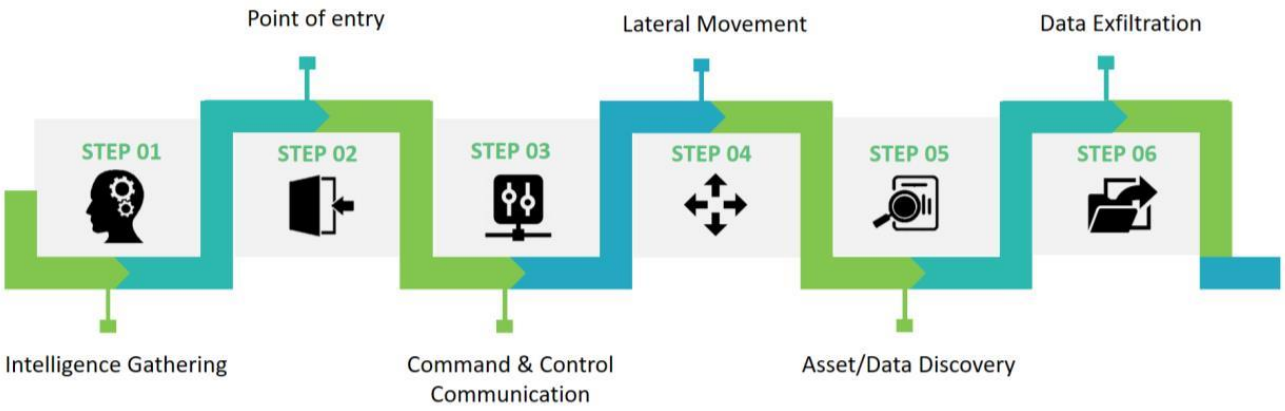


Рис. 1.8 – Цикл APT-атаки

Важливо зазначити, що різні етапи атаки не є особливо чіткими. Етапи цілеспрямованої атаки являють собою окремі кроки логічної, структурованої атаки. Однак, як показує практика, не всі кроки завжди вибудовуються у логічний ланцюг. Коли один з етапів завершено, це не обов'язково означає, що ніяких інших дій, пов'язаних з цим етапом, не буде. Цілком можливо, що кілька етапів атаки можуть відбуватися одночасно. Наприклад, C&C комунікація відбувається на всіх етапах цілеспрямованої атаки. Зловмиснику потрібно тримати під контролем всі дії, що відбуваються в мережі, тому цілком ймовірно, що C&C-трафік буде продовжувати відбуватися між зловмисником і будь-якими скомпрометованими системами.

Найкраще думати про кожен компонент як про різні аспекти однієї і тієї ж атаки, де різні частини мережі можуть стикатися з різними аспектами атаки в один і той же час.

Це може суттєво вплинути на те, як організація має реагувати на атаку. Не можна просто припустити, що оскільки атака була виявлена на "ранній" стадії, то "пізніші" стадії атаки ще не відбуваються. Належний план реагування на загрози

повинен враховувати це і повинен плануватися відповідним чином. Нижче наведено опис кожної фази циклу атаки.

1. Збір розвідувальних даних (Intelligence Gathering)

На цьому етапі атаки кіберзлочинці мають виявляють свої цілі і проводять дослідження для виявлення цільових осіб в організації, а потім готують індивідуальну атаку, найімовірніше, використовуючи загальнодоступні джерела, такі як LinkedIn, Facebook чи інші соціальні мережі. Завдяки великій кількості особистої інформації, що надається на цих сайтах, зловмисники озброюються глибокими знаннями про людей в організації. Наприклад, про їхню роль, хобі, членство в професійних асоціаціях та імена тих, хто входить до їхнього особистого кола спілкування.

Маючи цю інформацію на руках, зловмисники готують індивідуальну атаку, щоб проникнути в організацію.

2. Точка входу (Point of Entry)

Початкова компрометація, як правило, відбувається через шкідливе програмне забезпечення нульового дня, що доставляється за допомогою соціальної інженерії (електронною поштою/месенджером або шляхом завантаження). Створюється бєкдор завдяки якому в мережу можна проникнути. Крім того, може бути використана експлуатація веб-сайту або прямий злом мережі.

Після того, як кіберзлочинці зібрали розвідувальну інформацію про свою ціль, вони починають працювати над розробкою точки входу в організацію.

3. Командно-контрольна комунікація (C&C – Command & Control Communication)

Командно-контрольний зв'язок використовується зловмисником для інструктажу та управління скомпрометованими комп'ютерами та шкідливим програмним забезпеченням, яке використовується на всіх наступних етапах атаки (бічне переміщення, виявлення даних та ексфільтрація).

Після успішного встановлення шкідливого програмного забезпечення на скомпрометовану машину, воно може зв'язатися з серверами управління кіберзлочинця для отримання подальших інструкцій або завантажити додаткові

шкідливі програми та інструменти зловмисника, такі як клавіатурні шпигуни, троянські програми-бекдори, програми-вимагачі та інструменти для злому паролів. Це дозволяє зловмиснику переміщатися в мережі і викрадати дані.

4. Бічне переміщення (Lateral Movement)

Потрапивши в мережу, зловмисник компрометує додаткові комп'ютери, щоб отримати облікові дані та підвищити рівень привілеїв. Зловмисник також отримує стратегічну інформацію про IT-середовище - операційні системи, рішення для забезпечення безпеки та структуру мережі, щоб підтримувати постійний контроль над організацією-мішенню.

Бічне переміщення (переміщення зловмисника всередині мережі) використовує легальні інструменти системного адміністрування, щоб допомогти приховати свою діяльність, і має на меті три цілі: підвищення доступних привілеїв в цільовій мережі, проведення розвідки в цільовій мережі і бічне переміщення до інших комп'ютерів в самій мережі. Для підвищення рівня доступу зловмисника в мережі часто використовується декілька інструментів, зокрема, перенаправлення портів, інструменти сканування та інструменти віддаленого виконання процесів.

5. Виявлення активів/даних (Asset/Data Discovery)

Під час сучасної атаки кіберзлочинці переслідують цінні активи. Це може бути що завгодно: фінансові дані, комерційна таємниця або вихідний код, і що найцікавіше, зловмисники знають, які саме дані їх цікавлять, ще до того, як обирають організацію-мішень.

Мета зловмисника - якнайшвидше виявити дані, що його цікавлять, і зробити це непомітно. На цьому етапі атаки зловмисник може використовувати кілька різних методів. Наприклад, зловмисник може зробити наступне:

1) Перевірити конфігурацію поштового клієнта зараженого хоста, щоб знайти поштовий сервер.

2) Знайти файлові сервери, перевіривши хост на наявність відображених мережевих дисків.

3) Отримати історію браузера, щоб визначити внутрішні веб-служби, такі як CMS або CRM-сервери.

4) Просканувати локальну мережу на наявність папок, до яких мають спільний доступ інші кінцеві точки, щоб виявити варті уваги сервери та сервіси, які містять дані, що цікавлять зловмисника.

5) Використати сканування портів для виявлення відкритих портів.

6. Витік даних (Data Exfiltration)

Витік даних - це несанкціонована передача даних у зовнішні місця. На цьому етапі цілеспрямованої атаки конфіденційна інформація збирається, а потім передається на внутрішній проміжний сервер, де вона розбивається на частини, стискається і часто шифрується для передачі на зовнішні сервери під контролем зловмисника.

З яскравою демонстрацією APT-атаки можна ознайомитись з підсумків розслідування компанії Trend Micro останніх дій APT36, також відомої як Earth Karkaddan, політично вмотивованої групи сучасних постійних загроз (APT). Компанією Trend Micro розглянуто використання нею *CapraRAT* - шкідливого програмного забезпечення для Android, що має явну схожість у дизайні з улюбленим шкідливим програмним забезпеченням для Windows, *Crimson RAT*. Це розслідування було проведено компанією Trend Micro 24 січня 2022 року.

APT36, також відома як Earth Karkaddan, політично вмотивована сучасна група постійних загроз (APT), історично націлена на військові та дипломатичні ресурси Індії. Ця група APT (також відома як Operation C-Major, PROJECTTM, Mythic Leopard та Transparent Tribe) використовує соціальну інженерію та фішингові приманки як точку входу, після чого розгортає шкідливе програмне забезпечення *Crimson RAT* для викрадення інформації у своїх жертв.

Наприкінці 2021 року було помічено, що група використовує *CapraRAT*, *Android RAT*, який має явну схожість у дизайні з улюбленим шкідливим програмним забезпеченням для Windows, *Crimson RAT*.

Це дослідження ґрунтується на даних Trend Micro Smart Protection Network (SPN), зібраних з січня 2020 року по вересень 2021 року.

Метод проникнення в корпоративну мережу групи Earth Karkaddan включають використання фішингових електронних листів і USB-черв'яка, який потім скидає і запускає троянську програму для віддаленого доступу – RAT. (рис. 1.9). Шкідливі електронні листи містять різноманітні приманки для обману жертв, щоб змусити їх завантажити шкідливе програмне забезпечення, включаючи підроблені урядові документи, "медові пастки" з профілями привабливих жінок, а останнім часом - інформацію на тему коронавірусу.

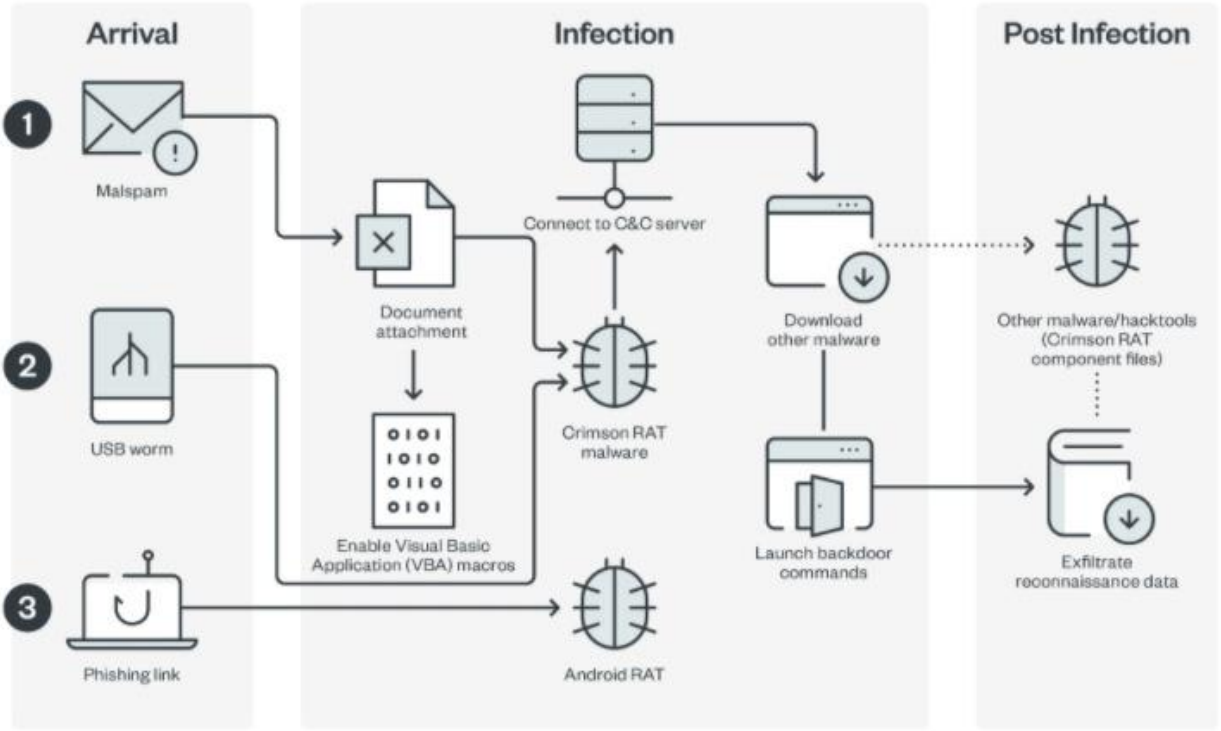


Рис. 1.9 – Відображення атаки групи Earth Karkaddan з використання *Crimson RAT*

Коли жертва завантажує шкідливий макрос, він розшифровує вбудований виконуваний файл, прихований у текстовому полі, який потім зберігається за жорстко заданим шляхом, перш ніж він буде запущений на комп'ютері. Нижче наведено шкідливий макрос, який розшифровує виконуваний файл, прихований у текстовому полі (рис. 1.10).

```
If InStr(Application.OperatingSystem, "6.02") > 0 Or InStr(Application.OperatingSystem, "6.03") > 0 Then
    arlothra = Split(UserForm1.TextBox2.Text, "i")
Else
    arlothra = Split(UserForm1.TextBox1.Text, "i")
End If



Dim btsothra() As Byte

Dim linothra As Double

linothra = 0

For Each vl In arlothra
    ReDim Preserve btsothra(linothra)

    btsothra(linothra) = CByte(vl)

    linothra = linothra + 1
Next




Open path_othra_file & "xe" For Binary Access Write As #3
     Put #3, , btsothra
Close #3



 Shell path_othra_file & "xe", vbNormalNoFocus
```

Рис. 1.10 – Приклад шкідливого макросу

Після запуску виконуваний файл розпакує файл з ім'ям *mdkhm.zip*, а потім запускає виконуваний файл *Crimson RAT* з назвою *dlrarhsiva.exe* (рис. 1.11).

Time	PID	Process Path	Operation	Info
15:42:07:507	1852	C:\Windows\System...	new process	"C:_virus\hbraeiwas - Copy.exe"
15:42:07:832	1208	C:_virus\hbraeiwas ...	create file	C:\ProgramData\Hdlharas\dlrarhsiva
15:42:07:835	1208	C:_virus\hbraeiwas ...	modify file	C:\ProgramData\Hdlharas\dlrarhsiva
15:42:07:847	1208	C:_virus\hbraeiwas ...	rename file	C:\ProgramData\Hdlharas\mdkhm.zip
15:42:07:847	1208	C:_virus\hbraeiwas ...	modify file	C:\ProgramData\Hdlharas\mdkhm.zip
15:42:07:897	1208	C:_virus\hbraeiwas ...	create file	C:\ProgramData\Hdlharas\dlrarhsiva.exe
15:42:07:975	1208	C:_virus\hbraeiwas ...	modify file	C:\ProgramData\Hdlharas\dlrarhsiva.exe

Рис. 1.11 - Запуск виконуваного файлу *Crimson RAT*

Відомо, що учасники Earth Karkaddan використовували шкідливе програмне забезпечення *Crimson RAT* у своїх кампаніях для зв'язку зі своїм командно-контрольним сервером (C&C) для завантаження інших шкідливих програм або витоку даних.

1.4 Аналіз необхідності своєчасного виявлення та якісного реагування на загрози в корпоративній мережі

Коли організації зазнають кібератаки, важлива кожна секунда. Чим більше часу зловмисник проводить у корпоративній мережі організації, тим більша ймовірність того, що він завдасть серйозної шкоди, що призведе до простою систем, втрати даних і стрімкого зростання витрат на відновлення.

Ефективна стратегія виявлення загроз і реагування на них дозволяє організаціям захистити себе від кібератак шляхом постійного моніторингу своїх мереж і додатків на предмет підозрілої активності та вжиття швидких заходів для пом'якшення будь-яких потенційних загроз. Однак розробка такої стратегії вимагає певних зусиль. Щоб випередити зловмисників, організації повинні впроваджувати сучасні технології, розробляти чіткі комунікаційні плани та інвестувати в постійне навчання співробітників в напрямку кібербезпеки.

Метою виявлення та реагування на загрози є виявлення потенційних загроз та їх нейтралізація якомога раніше, в ідеалі - до того, як буде завдано шкоди. Процес починається зі збору даних з різних джерел, таких як мережевий трафік, системні журнали та пристрої безпеки, такі як аналізатори мережевого трафіку (NDR – Network Detection and Response), брандмауери, системи виявлення вторгнень (IDS) та EDR.

Потім ці дані аналізуються для виявлення будь-яких аномалій або підозрілої поведінки, які можуть вказувати на потенційну кіберзагрозу. Це вимагає використання передових алгоритмів розвідки загроз і машинного навчання, які можуть виявляти закономірності і аномалії у великих масивах даних, допомагаючи виявляти загрози, які можуть бути пропущені традиційними заходами безпеки. З людського боку, це також вимагає кваліфікованого персоналу, культури безпеки, а також чітко визначених процесів і процедур, які регулярно тестуються і оновлюються, щоб бути на крок попереду нових загроз.

Після виявлення загрози починається етап реагування. Це передбачає вжиття відповідних заходів для стримування загрози та зменшення будь-якої шкоди, яку

вже було завдано. Це може включати ізоляцію уражених систем чи пристроїв, блокування шкідливого трафіку та видалення виявленого шкідливого коду чи програмного забезпечення. Загалом, ефективний процес виявлення та реагування на загрози може мінімізувати вплив кібератак і захистити конфіденційні дані та критичні системи від шкоди.

Нижче, на рисунку 1.12, наведено приклад циклу виявлення та реагування на загрози

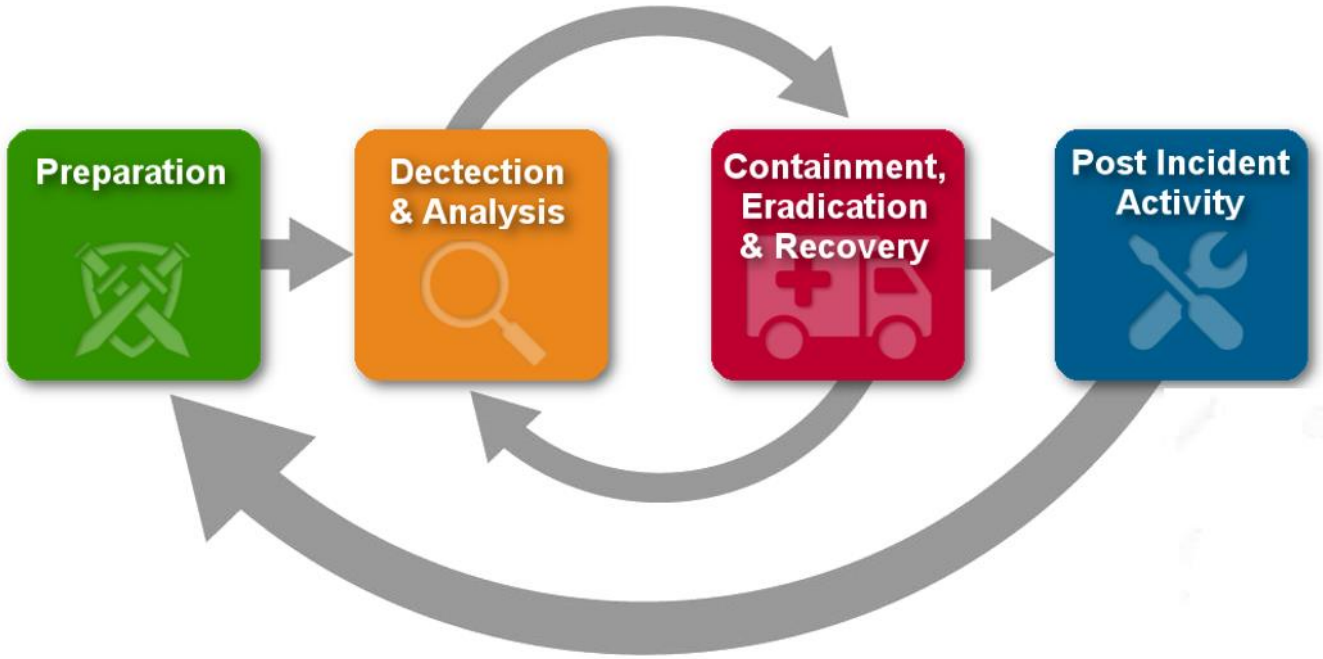


Рис. 1.12 – Цикл виявлення та реагування на загрози

Найкращі практики виявлення загроз

Окрім основних кроків, описаних вище, організації можуть використовувати різні методи для підвищення рівня виявлення загроз та посилення захисту від кіберзлочинів, такі як:

1. Розширена розвідка загроз

Розширена розвідка загроз передбачає використання автоматизованих інструментів для моніторингу та аналізу даних про загрози з різних джерел, включаючи мережеві журнали, стрічки подій безпеки та звіти про аналіз шкідливого програмного забезпечення. Застосовуючи до цих даних розширену аналітику та алгоритми машинного навчання, ці інструменти можуть виявляти закономірності та аномалії, щоб швидко позначити потенційну загрозу. Це дозволяє організаціям швидко реагувати на будь-яку підозрілу активність.

2. Регулярна оцінка вразливостей

Захист корпоративної мережі є настільки сильний, наскільки сильним є його найслабше місце. Регулярно скануючи свої системи, мережі та додатки на наявність відомих вразливостей, організації можуть виявити слабкі місця у свої мережах та системах до того, як ними скористаються зловмисники. Також слід провести ретельний пошук прогалин у власному кіберзахисті за допомогою внутрішніх командних заходів, основною частиною яких стане випробування на так званому кіберполігоні (або ж простіше – виконання тесту на проникнення). Після цього буде можливо виявити і заповнити прогалини в безпеці за допомогою таких дій, як застосування патчів, оптимізація стеку засобів захисту або впровадження додаткових засобів контролю безпеки.

3. Вивчення поведінки зловмисника

Легше виявити зловмисників, які проникли у корпоративну мережу, якщо знати, як виглядає нормальна мережева та системна активність. Щоб розробити базовий профіль поведінки, команди безпеки організацій мають вивчити такі дані, як потік трафіку, доступ до даних і використання додатків, і визначити для себе шаблони загроз, які є поширеними і очікуваними в конкретній мережі чи системі. Це дозволить організаціям швидко виявити будь-яку незвичну активність, яка може свідчити про потенційну загрозу.

4. Використання штучного інтелекту та машинного навчання

Штучний інтелект (ШІ) і машинне навчання (МН) можуть посилити стратегію виявлення загроз, дозволяючи організаціям автоматизувати аналіз величезних обсягів даних. Зокрема, однією з переваг ШІ та МН є їхня здатність

виявляти раніше невідомі загрози. Традиційні інструменти безпеки часто обмежуються виявленням відомих загроз на основі заздалегідь визначених правил або сигнатур. На відміну від них, ШІ та МН можуть навчатися на історичних даних і виявляти нові загрози на основі моделей їхньої поведінки, навіть якщо вони ніколи раніше не зустрічалися. Крім того, штучний інтелект і машинний інтелект можуть допомогти відфільтрувати конкретну загрозу від великого потоку трафіку, зменшуючи кількість хибних спрацьовувань і позначаючи найбільш релевантні оповіщення для подальшого розслідування командою безпеки.

Найкращі практики реагування на загрози

Коли справа доходить до захисту організацій від кібератак, виявлення - це лише перший крок. Команди кібербезпеки повинні також вжити швидких і рішучих заходів для ізоляції загроз, зменшення шкоди та усунення будь-яких основних вразливостей, виявлених в результаті атаки. Досягти цього можна найлегше, якщо дотримуватись трьохетапного підходу до кібербезпеки, що включає людей, технології та процедури. Плануючи заздалегідь та інвестуючи в правильні інструменти та практики, можна забезпечити організації необхідним обладнанням для швидкого та ефективного реагування на загрози.

1. Розробка та тестування планів реагування на інциденти

План реагування на інциденти окреслює кроки, які організація зробить у разі кібератаки. Щоб розробити подібний план, слід почати з визначення обсягу та цілей, виявлення потенційних загроз і розподілу ролей та обов'язків між учасниками. Після того, як ці керівні принципи будуть розроблені, потрібно протестувати їх, проводячи регулярні тренування та вправи, щоб переконатися, що план є ефективним та актуальним. Підвищити реалістичність цих вправ можливо, розгорнувши їх у контрольованому середовищі, наприклад, на кіберполігоні, який імітує унікальний технологічний стек захисту організації.

2. Встановлення чітких протоколів комунікації

Коли організація зазнає кібератаки, час має вирішальне значення. Заздалегідь розробивши чіткі протоколи комунікації, - це спростить реагування та забезпечить

якнайшвидше усунення загроз. Цей протокол повинен передбачати шляхи ескалації та канали зв'язку для ключових зацікавлених сторін, включаючи зовнішні сторони, такі як клієнти, партнери та регуляторні органи. Заздалегідь спланувавши, як комунікувати в разі нагальної загрози, - це збільшить шанси протистояти загрозі до того, як вона завдасть значної шкоди.

3. Ізоляція та локалізація загрози

Після виявлення загрози першим кроком має бути її ізоляція, щоб запобігти її поширенню та полегшити усунення наслідків. План реагування на інцидент повинен включати кроки для швидкого виявлення уражених систем, відключення їх від Інтернету та введення карантину на уражених кінцевих точках/системах. Полегшити процес локалізації інциденту можна завдяки впровадженню превентивних заходів, таких як сегментація мережі для обмеження впливу атаки та забезпечення наявності та актуальності резервних копій, щоб можливо було швидко відновити системи у разі втрати даних.

4. Усунення основної причини атаки

Усунення передбачає вжиття заходів для усунення першопричини кібератаки та запобігання її повторенню. Після того, як інцидент локалізовано, потрібно ретельно розслідувати атаку та визначити, як вона сталася. Отримавши інформацію, необхідно вжити відповідних коригувальних заходів, які можуть включати такі кроки, як виправлення вразливостей, оновлення політик безпеки або проведення додаткового навчання для співробітників.

5. Навчання працівників процедурам реагування

Навчання працівників процедурам реагування на загрози має вирішальне значення для забезпечення розуміння ними своїх обов'язків у разі кібератаки. Це допоможе забезпечити скоординоване та ефективне реагування, зменшивши ризик подальшої шкоди для організації. Окрім надання чітких і стислих інструкцій щодо реагування на потенційні загрози, слід проводити регулярні тренінги, в тому числі навчання на кіберполігоні, які дозволять співробітникам попрактикуватися в реалістичних сценаріях. Важливо також проводити постійні освітні та інформаційні програми, щоб тримати команду кібербезпеки в курсі останніх загроз.

1.5 Аналіз технологій виявлення та реагування на загрози в корпоративній мережі

Ефективне виявлення загроз і реагування на них є дедалі складнішим і постійно еволюціонуючим викликом для команд безпеки. Раніше для захисту від кібератак було достатньо превентивних технологій, включаючи антивірусне та антивірусне програмне забезпечення в парі з брандмауером. Сьогодні організаціям потрібна стратегія більш глибокого захисту, яка включає ці технології, а також більш досконалі інструменти, такі як SIEM, NDR, EDR/XDR, IPS/IDS, NGFW, WAF та ін.

Управління інформацією та подіями безпеки (SIEM)

Рішення SIEM є ключовим інструментом в арсеналі будь-якого фахівця з кібербезпеки. Вони збирають та агрегують дані журналів, що генеруються в IT-середовищі, можуть виявляти відхилення від норми та допомагають командам безпеки вжити відповідних заходів для зменшення загрози. Рішення SIEM, як правило, здатні аналізувати сповіщення про загрози в режимі, близькому до реального часу, що робить їх життєво важливим компонентом у процесі виявлення загроз. Найкращі рішення SIEM на ринку поєднують в собі управління журналами безпеки, аналітику поведінки користувачів та організацій (UEBA), а також можливості автоматизації/оркестрування.

Виявлення та реагування на кінцевих точках (EDR)/ Розширене виявлення та реагування (XDR)

Інструменти EDR забезпечують моніторинг і збір даних про кінцеві точки в режимі реального часу, що дозволяє командам безпеки виявляти, розслідувати і запобігати потенційним загрозам. Вони здатні виявляти та аналізувати підозрілі дії на кінцевих пристроях, таких як ноутбуки, робочі станції та мобільні пристрої.

XDR, з іншого боку, розширює ці можливості шляхом інтеграції декількох продуктів безпеки в єдину платформу виявлення інцидентів безпеки та реагування на них. Native XDR поєднує в собі можливості EDR, особливо в поєднанні з аналізом мережевого трафіку того ж постачальника та іншими інструментами

безпеки, щоб забезпечити цілісне уявлення про стан безпеки організації. Така комплексна видимість значно полегшує виявлення та усунення загроз у мережі організації.

Системи виявлення та запобігання вторгнень (IDS/IPS)

Системи виявлення та запобігання вторгненням є критично важливими компонентами надійної стратегії виявлення та реагування на загрози. Вони відстежують мережевий трафік на предмет підозрілих дій і порушень політики. Системи виявлення вторгнень (IDS) аналізують мережевий трафік, щоб виявити потенційні загрози та попередити команди безпеки, тоді як системи запобігання вторгненням (IPS) йдуть далі, надсилаючи сигнал брандмауерам/проксі-серверам для автоматичного блокування або пом'якшення виявлених загроз.

Брандмауери нового покоління (NGFW) та Брандмауери веб-додатків (WAF)

NGFW - це вдосконалені версії традиційних брандмауерів, оснащені розширеними функціями, такими як глибока перевірка пакетів, системи запобігання вторгненням, зіставлення антивірусних хешів і можливість інтегрувати зовнішню розвідку загроз. Вони забезпечують покращену видимість і контроль над мережевим трафіком, допомагаючи організаціям краще виявляти загрози та реагувати на них.

Брандмауери для веб-додатків (WAF) захищають веб-додатки шляхом моніторингу та фільтрації HTTP-трафіку між веб-додатком та Інтернетом. Вони допомагають виявляти і запобігати веб-атакам, таким як міжсайтовий скриптинг (XSS), SQL-ін'єкції та іншим загрозам, переліченим у списку OWASP Top 10.

Мережеве виявлення та реагування (NDR)

Рішення для мережевого виявлення та реагування (NDR) використовують комбінацію передових аналітичних методів, таких як машинне навчання, для виявлення підозрілої мережевої активності. Це дозволяє командам реагувати на аномальний або зловмисний трафік і загрози, які не помічають інші інструменти безпеки. Рішення NDR безперервно відстежують і аналізують необроблений мережевий трафік підприємства для створення базової лінії нормальної поведінки мережі. При виявленні підозрілих шаблонів мережевого трафіку, які відхиляються

від цієї базової лінії, інструменти NDR попереджають команди безпеки про потенційну присутність загроз в їхньому середовищі.

Мережі розширюються в хмару і безперервно зростають як в розмірі, так і в складності. Це призвело до безпрецедентного обсягу даних, що проходять через розподілену мережу, і створило ідеальне середовище для зловмисників, в якому вони можуть ховатися. Рішення NDR вирішують цю проблему шляхом збору телеметрії з мережевих пристроїв і застосування аналітичних методів, таких як машинне навчання, для виявлення загроз, які інші інструменти пропускають.

Рішення та інструменти NDR можуть:

1. Виявляти аномальний мережевий трафік, який традиційні інструменти пропускають, застосовуючи методи виявлення, що не базуються на сигнатурах, такі як поведінкова аналітика та машинне навчання.

2. Моделювати базову лінію нормальної поведінки мережі та попереджати команди безпеки про будь-який підозрілий трафік, що виходить за межі цього нормального діапазону.

3. Відстежувати всі потоки трафіку - як вхідні, так і вихідні, а також переміщення всередині мережі, щоб команди мали розширену видимість, необхідну для виявлення та усунення інцидентів безпеки, незалежно від того, звідки походить загроза.

4. Аналізувати необроблену мережеву телеметрію в реальному часі або майже в реальному часі та надавати своєчасні сповіщення, щоб команди могли покращити час реагування на інциденти.

5. Пов'язувати зловмисну поведінку з конкретною IP-адресою та проводити криміналістичний аналіз, щоб визначити, як загрози переміщувалися в середовищі. Це дозволяє командам безпеки бачити, які ще пристрої можуть бути заражені, що призводить до швидшого реагування на інциденти та стримування загроз, а також кращого захисту від несприятливих наслідків для бізнесу.

6. Забезпечити можливості реагування, які можуть покращити ручне реагування на інциденти та полювання на загрози або оптимізувати операції та заощадити час команд за рахунок автоматизації.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ДЛЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ В КОРПОРАТИВНІЙ МЕРЕЖІ

2.1 Архітектура рішень Trend Micro Deep Discovery

Моніторинг бокового руху через такі протоколи, як SMB, RDP, SNMP, IRC, є критично важливим. Якщо в організаціях немає такого інструменту для моніторингу цих протоколів, вже існуючу атаку на організацію можна не помітити. В середньому, загроза залишається невиявленою протягом декількох місяців через стратегію безпеки, орієнтовану на периметр. Як тільки загроза потрапляє в мережу, цей трафік не відстежується через припущення, що інструменти периметру заблокували всі атаки.

Технологія Deep Discovery розроблена таким чином, щоб відстежувати не тільки вхідний і вихідний трафік, а й трафік, що рухається по корпоративній мережі, контролюючи понад 100 протоколів та всі порти. Така широка видимість допоможе запобігти вільному переміщенню невиявленого шкідливого програмного забезпечення по мережі. Deep Discovery передає свої висновки щодо виявлення іншим продуктам безпеки, що дає змогу в режимі реального часу вживати заходів для усунення загрози.

Trend Micro Deep Discovery захищає від цілеспрямованих атак, сучасних загроз і програм-вимагачів, надаючи вам можливість виявляти, аналізувати та реагувати на сучасні приховані атаки в режимі реального часу.

Deep Discovery поєднує в собі спеціалізовані засоби виявлення та реагування на загрози – Trend Micro Deep Discovery Inspector, індивідуальну пісочницю – Trend Micro Deep Discovery Analyzer та глобальну аналітику загроз із інтелектуальної мережі Trend Micro Smart Protection Network для виявлення шкідливих програм «нульового дня», зловмисних повідомлень і дій зловмисників. Розгорнуте окремо або як інтегроване рішення, Deep Discovery має можливість працювати разом із продуктами Trend Micro та сторонніх виробників для захисту мереж, забезпечуючи розширений захист від загроз для всієї корпоративної мережі організації.

Можливості технології Deep Discovery

1. Перевірка мережевого контенту: Deep Discovery Inspector може працювати в автономному режимі (підключений до дзеркального порту комутатора) або в режимі on-line для моніторингу всього трафіку в фізичних і віртуальних сегментах мережі, всіх мережевих портів і більш ніж 100 мережевих протоколів для виявлення цілеспрямованих атак, сучасних загроз і програм-вимагачів. Використання агностичного підходу до мережевого трафіку дозволяє Deep Discovery виявляти цілеспрямовані атаки, сучасні загрози і програми-вимагачі у вхідному і вихідному мережевому трафіку, а також латеральне переміщення, злом і інші дії зловмисників на всіх етапах життєвого циклу атаки.

2. Розширені методи виявлення: Виявлення з використанням репутації файлів, веб-сайтів, IP-адрес, мобільних додатків, евристичного аналізу, розширеного сканування загроз, спеціального аналізу в «пісочниці» і корельованої розвідки загроз для виявлення програм-вимагачів, експлойтів «нульового дня», складних шкідливих програм і поведінки зловмисників.

3. Налаштовуваний аналіз в пісочниці: В ізольованій системі використовуються віртуальні образи, налаштовані так, щоб точно відповідати конфігурації системи, драйверам, встановленим програмам і мовним версіям організації. Такий підхід підвищує рівень виявлення сучасних загроз і програм-вимагачів, які намагаються обійти стандартні віртуальні образи.

4. Гнучкі можливості розгортання: Deep Discovery Analyzer можна розгортати як автономну пісочницю або паралельно з більш масштабним розгортанням Deep Discovery Inspector, щоб додати додаткову пропускну здатність пісочниці. Його можна масштабувати для підтримки до 60 пісочниць в одному пристрої. Кілька пристроїв можна об’єднати в кластер для забезпечення високої доступності або налаштувати на гаряче або холодне резервне копіювання. Deep Discovery Inspector доступний як у вигляді апаратного пристрою, так і у вигляді віртуального пристрою, щоб допомогти задовольнити ваші цілі та потреби в розгортанні.

5. Розширене виявлення: Такі методи, як статичний аналіз, евристичний аналіз, аналіз поведінки, веб-репутація та репутація файлів, забезпечують швидке виявлення загроз. Deep Discovery також виявляє багатоступеневі шкідливі файли, вихідні з'єднання та повторні з'єднання з підозрілими файлами.

6. Розвідка загроз: Deep Discovery співвідносить і передає розширені дані про загрози, використовуючи стандартизовані формати і засоби передачі даних, такі як STIX/TAXII і YARA. Це дозволяє організаціям випереджати невідомі загрози, які можуть проникнути в мережу.

7. Аналітика загроз: Забезпечує кращу видимість атаки, допомагаючи вам визначити пріоритетність загроз і показати, як саме загроза проникла в мережу, куди вона потрапила, і хто ще постраждав від атаки. Натисніть кнопку відтворення і подивіться весь процес атаки крок за кроком.

Deep Discovery створено для роботи як із продуктами Trend Micro (рис. 2.1), так і з продуктами сторонніх виробників. Завдяки вбудованій інтеграції та технології API Deep Discovery допомагає автоматизувати реагування на загрози безпеки, обмін індикаторами компрометації (IOC), а також запобігання сучасним загрозам і цілеспрямованим атакам.

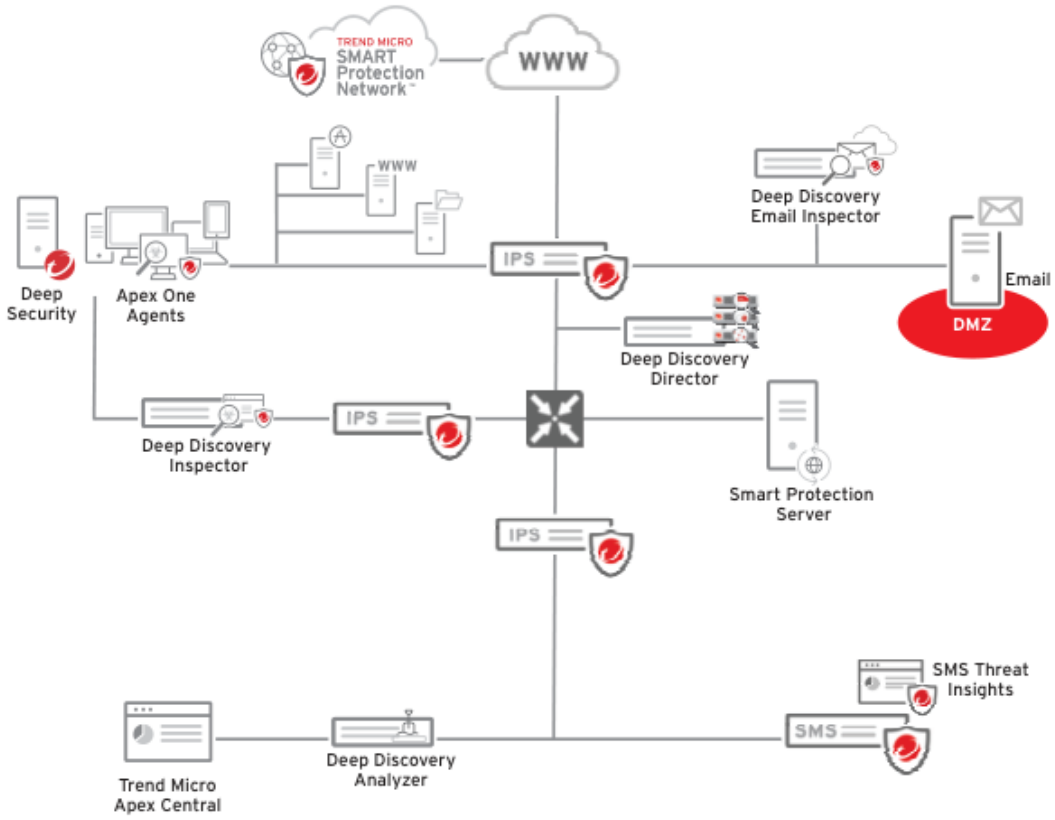


Рис. 2.1 – Архітектура рішень Deep Discovery у поєднанні з іншими рішеннями безпеки компанії Trend Micro

2.2 Призначення, функції та архітектура рішення Trend Micro Deep Discovery Inspector

Deep Discovery Inspector (DDI) - це рішення для моніторингу мережі, призначене для швидкого виявлення сучасних шкідливих програм, які зазвичай обходять традиційні засоби захисту і викрадають конфіденційні дані. Розроблений для виявлення та реагування на цілеспрямовані атаки та загрози у будь-якій точці корпоративної мережі. Deep Discovery Inspector виявляє шкідливий вміст, командні та керуючі комунікації (C&C) та поведінку, які можуть вказувати на сучасне шкідливе програмне забезпечення або активність зловмисників на кожному етапі послідовності атак. Це рішення виявляє та ідентифікує ухильні загрози в режимі

реального часу, а також надає глибокий аналіз і дієві аналітичні дані, необхідні для запобігання, виявлення та стримування атак на ресурси організації. Консоль рішення виглядає наступним чином (рисунок 2.2).

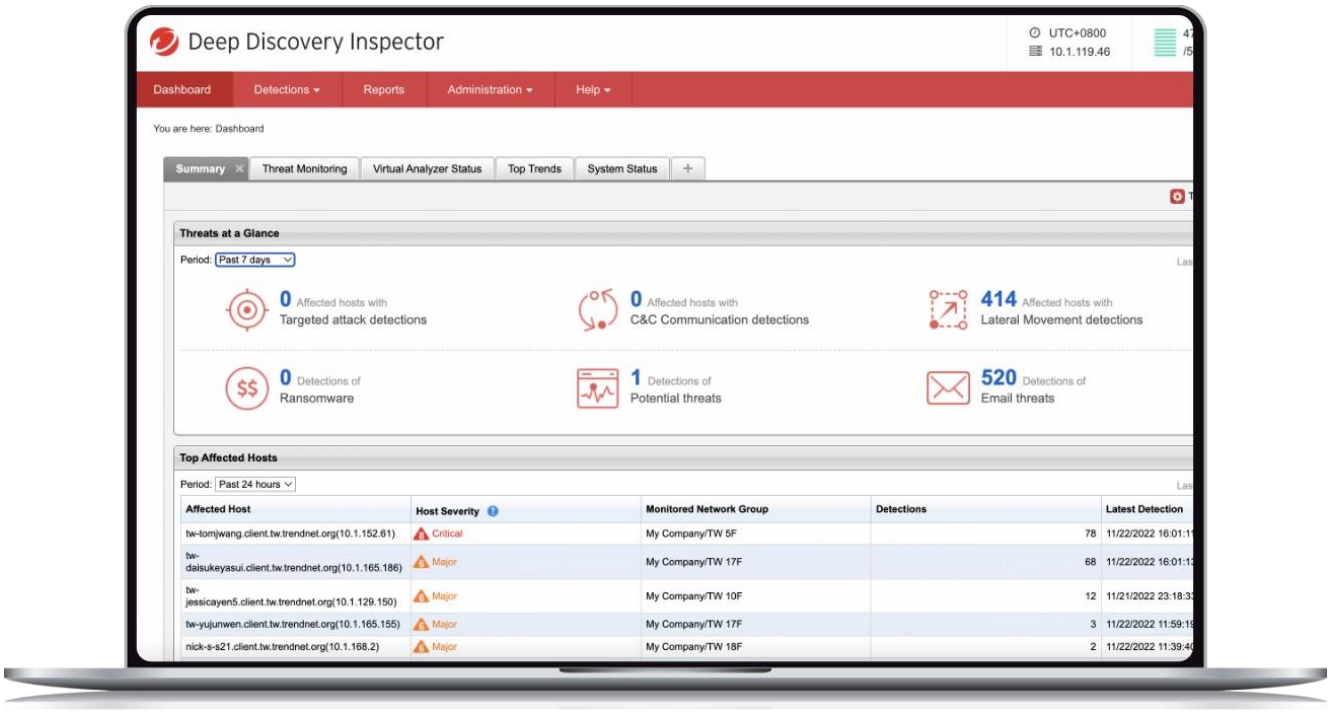


Рис. 2.2 – Веб-консоль DDI

Deep Discovery Inspector доступний у вигляді фізичного (рис. 2.3) або віртуального мережевого пристрою і може працювати в режимі автономного моніторингу (підключений до дзеркального порту комутатора) з мінімальним перериванням роботи мережі або без нього, відстежуючи мережевий трафік і виявляючи відомі та потенційні загрози безпеці. При розгортанні фізичного Deep Discovery Inspector додатково є можливість розгортання обладнання в режимі онлайн. При розгортанні в лінію Deep Discovery Inspector діє як прозорий міст і може перевіряти розшифрований TLS-трафік.

Рис. 2.3 – DDI у вигляді апаратного рішення

Ключові особливості та функціональність DDI

1. Перевіряє весь мережевий трафік

Deep Discovery Inspector відстежує весь трафік у фізичних і віртуальних сегментах мережі, всі мережеві порти і понад 100 мережевих протоколів, щоб виявити цілеспрямовані атаки, сучасні загрози і програми-вимагачі. Завдяки агностичному підходу до мережевого трафіку DDI здатний виявляти цілеспрямовані атаки, сучасні загрози і програми-вимагачі у вхідному і вихідному мережевому трафіку, а також бічні переміщення, злом та інші дії зловмисників на всіх етапах життєвого циклу атаки.

2. Наявність розширених методів виявлення

Для виявлення програм-вимагачів, експлойтів "нульового дня", сучасних шкідливих програм і поведінки зловмисників використовуються методи

розширеного виявлення, які використовують репутацію файлів, веб-сайтів, IP-адрес, мобільних додатків, евристичний аналіз, розширене сканування загроз, спеціальний аналіз в ізольованому середовищі та корельовану розвідку загроз.

3. Кастомний аналіз в ізольованій середовищі

На відміну від інших рішень для ізольованих систем, які використовують стандартні шаблони ОС і програм, Deep Discovery Inspector використовує віртуальні образи, які точно відповідають конфігураціям системи, драйверам, встановленим програмам і мовним версіям організації. Такий підхід підвищує рівень виявлення сучасних загроз і програм-вимагачів, які намагаються обійти стандартні віртуальні образи.

4. Кероване виявлення та реагування

Завдяки послузі Trend Micro Managed Detection and Response експерти Trend Micro з питань безпеки допоможуть відстежувати загрози, виявлені за допомогою DDI, і визначати їх пріоритетність. Ця керована служба працює в режимі 24/7 і може бути розширена, щоб охопити кінцеві точки, електронну пошту та хмарні робочі навантаження для кращого розуміння спрямованих атак.

5. Перетворення невідомих загрози на відомі

Deep Discovery Inspector використовує стандартизований обмін розширеними даними про загрози, щоб випереджати їх (STIX/TAXII і YARA). DDI автоматизує обмін інформацією про загрози між рішеннями Trend Micro та сторонніх розробників, що дає змогу одночасно зміцнити кілька ланок ланцюга захисту.

6. Мережева аналітика

Фахівці з безпеки отримують дані про загрози з численних джерел. Мережева аналітика допомагає визначити пріоритетність загроз і дає змогу простежити за атакою. Озираючись на місячні історичні дані, ви зможете побачити, що було першою точкою входу, хто ще в організації зазнав впливу, і з ким спілкується загроза (наприклад, C&C).

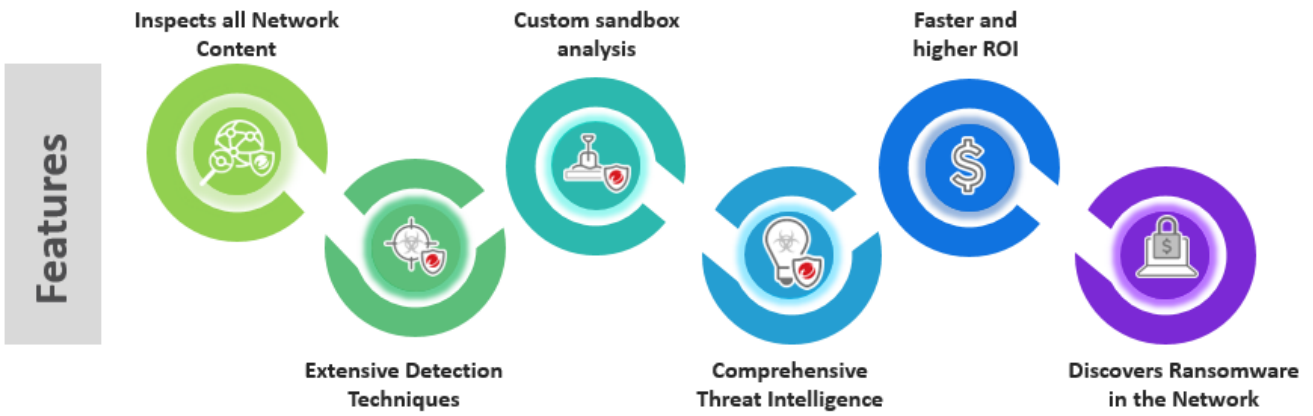


Рис. 2.4 – Ключові можливості DDI

Фізично DDI створений на базі серверів Dell. Кількість інтерфейсів такого серверу залежить від форм-фактора DDI та базового обладнання. Нижче наведені найбільш популярні на ринку специфікації апаратного варіанту DDI.

	Model 500/1000	Model 4000/9000
Hardware Model	510/1200	4200
Sandboxes Supported	2(500), 4(1000)	20 (Linux)
Form Factor	IU Rack-Mount, 48.26cm (19")	2U Rack-Mount, 48.26cm (19")
Weight	19.9kg (43.87 lb)	28.6kg (63.05 lb)
Dimensions (WxDxH)	43.4 (17.09") x 64.2 (25.28") x 4.28 (1.69") cm	482.0mm (18.98 inches) x 715.5mm (28.17 inches) x 86.8mm (3.42 inches)
Management Ports	10/100/1000 Base-T RJ45 Port x 1	10/100/1000 BASE –T RJ45 Port x 1 iDrac Enterprise RD45 x 1
Data Ports	10/100/1000 Base- T RJ45 x 3	10Gb SFP+ with SX transceiver x 4 10/100/1000 Base-T RJ45 x 5
AC Input Voltage	100 to 240 VAC	100 to 240 VAC
AC Input Current	7.4A to 3.7A	10A to 5 A
Hard Drives	2 x 1 TB 3.5" SATA	4 x 1 TB 3.5-inch SAS
RAID Configuration	RAID 1	RAID 1+0
Power Supply	550 W Redundant	750W (4200)/1100W (9200), 100-240 VAC 50/60 HZ
Power Consumption	604 W	847W (Max)
Heat	2133 BTU/hr (Max)	2891 BTU/hr (Max)
Frequency	50/60 Hz	50/60 Hz
Operating Temp	10-35	10°C to 35°C at 10% to 80% relative humidity (RH)
Hardware Warranty	3 Years	3 Years

Рис. 2.5 – Специфікації DDI моделей 500/100 та 4000/9000

У всіх випадках перша мережева карта (eth0) використовується для управління, що включає зв'язок з адміністратором через HTTP / SSH і взаємодію з іншими продуктами (такими як рішення для захисту кінцевих точок, пошти, веб-

шлюз та ін.) та службами (такими як WRS - Web Reputation Services, ActiveUpdate чи Retro Scan).

Починаючи з версії 6.0, DDI підтримує розгортання в лінію для виконання перевірки TLS. Інтегроване розгортання підтримується тільки на апаратних версіях Deep Discovery Inspector і вимагає встановлення додаткової мережевої карти. Однак через дефіцит мережевих карт клієнтам необхідно придбати додаткову карту, щоб розгорнути DDI в потоковому режимі і підтримувати перевірку TLS.

Інтерфейс мережі передачі даних

Порти даних в Deep Discovery Inspector використовуються для прийому вхідного мережевого трафіку. У типовому сценарії розгортання вони підключаються до портів моніторингу корпоративних комутаторів. Щоб переконатися, що Deep Discovery Inspector перехоплює трафік в обох напрямках, налаштуйте дзеркальний порт і переконайтеся, що трафік в обох напрямках відображається на цей порт.

Мережевий інтерфейс керування (NIC)

Порт управління Deep Discovery Inspector використовується для зв'язку між адміністраторами через HTTP / SSH і взаємодії з іншими продуктами (такими як Deep Discovery Analyzer, Apex Central та іншими) і службами (такими як WRS, ActiveUpdate та іншими).

Вбудовані порти

Коли Deep Discovery Inspector розгорнуто як вбудований в лінію трафіку пристрій і налаштовано на дешифрування TLS-трафіку, такі події, як збій системи, відключення електроенергії або інші непередбачувані обставини можуть мати вплинути на доступність мережі. DDI може автоматично вмикати обхід трафіку або вмикати його вручну. При автоматичному обході трафіку Deep Discovery Inspector виконує самоперевірку працездатності. Якщо виявлено проблему, DDI автоматично переходить в режим обходу трафіку, щоб запобігти потенційному впливу на мережу. Коли це відбувається, в консолі керування з'являється глобальне сповіщення, і,

якщо налаштовано, Deep Discovery Inspector може надіслати сповіщення електронною поштою або SNMP-пастку.

Механізми виявлення загроз

Deep Discovery Inspector поєднує в собі спеціалізовані механізми виявлення для перевірки мережевого трафіку та виявлення критично важливих загроз. Нижче наведено основні механізми DDI, які використовуються для виявлення загроз:

1. Механізм і шаблон перевірки мережевого вмісту (NCIE – Network Content Inspection Engine and Pattern)

Механізм перевірки мережевого вмісту - це програмний модуль Deep Discovery, який сканує вміст, що проходить через мережевий рівень. Наприклад, він виявляє підозрілий мережевий трафік і трафік додатків, визначених адміністратором (IM, P2P і потокове передавання даних).

2. Удосконалений механізм сканування загроз (ATSE - Advanced Threat Scan Engine)

- Удосконалений механізм сканування загроз виявляє віруси та інше шкідливе програмне забезпечення в мережевому трафіку.
- Знаходить відомі та потенційні шкідливі програми
- Виявляє загрози нульового дня за допомогою евристичного сканування
- Виявляє підозрілі вбудовані об'єкти (скрипти/код) у файлах документів
- Сумісний з VSAPI (Virus Scan API – механізм сканування файлів від Trend Micro, основний компонент більшості продуктів Trend Micro для захисту. Це сучасний технологічний модуль, який відповідає за обробку файлових об'єктів і класифікацію їх як шкідливих, підозрілих або нешкідливих файлів)

3. Механізм кореляції мережевого контенту (NCCE - Network Content Correlation Engine)

- Механізм кореляції мережевого вмісту аналізує всі факти про вміст пакетів для виявлення відомих і потенційних загроз
- NCCE співвідносить підказки від інших модулів і надає узагальнені результати

- Використовує правила виявлення Deep Discovery Inspector для зіставлення правил

4. Віртуальний аналізатор

Віртуальний аналізатор виявляє підозрілу поведінку у файлах, дозволяючи коду в файлі виконуватися в ізольованому віртуальному середовищі (пісочниці), щоб визначити, що робить код (наприклад, видаляє файли або змінює параметри реєстру). Технологія пісочниці Virtual Analyzer доступна в багатьох продуктах Trend Micro для мережевого захисту. Віртуальний аналізатор може бути вбудований у сам продукт, як у Deep Discovery Inspector, або як зовнішній автономний апаратний пристрій – Deep Discovery Analyzer.

5. Механізм фільтрації URL-адрес (TMUFE – Trend Micro URL Filtering Engine)

DDI використовує TMUFE для аналізу URL-адрес. Цей механізм перевіряє локальний кеш у пам'яті на наявність інформації про рейтинг URL. Якщо репутація URL-адреси не зберігається в кеші, за замовчуванням через протокол HTTP здійснюється зв'язок із хмарною службою веб-репутації Trend Micro, яка запитує репутацію URL-адреси.

6. Предиктивний механізм машинного навчання

Механізм предиктивного машинного навчання співвідносить інформацію про загрози та виконує глибокий аналіз файлів, щоб виявити нові невідомі ризики для безпеки за допомогою цифрового ДНК-відбитку, API-маппингу та інших характеристик файлів. Цей механізм використовує моделювання шкідливих програм для порівняння зразків з відомими моделями шкідливих програм, щоб визначити ймовірні типи шкідливих програм, які містить зразок файлу, і присвоїти їм оцінки ймовірності.

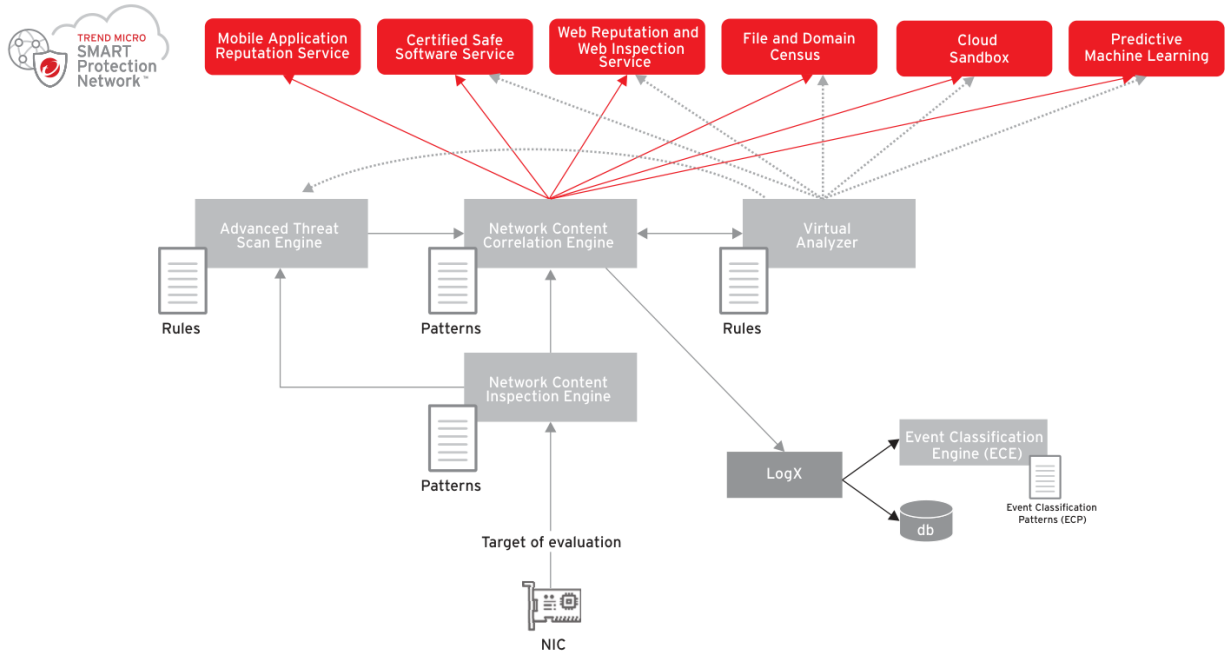


Рис. 2.6 – Демонстрація роботи механізмів виявлення загроз та комунікації цих механізмів із зовнішніми сервісами Trend Micro

Механізми виявлення загроз Deep Discovery повинні мати можливість підключатися до різних хмарних хмарними службами Trend Micro, щоб забезпечити можливості виявлення, описані нижче.

1. Сертифікована служба безпечного програмного забезпечення (CSSS – Certified Safe Software Service)

Служба сертифікованого безпечного програмного забезпечення (CSSS), також відома як GRID, визначає, чи був портативний виконуваний файл вже перевірений як безпечний.

2. Служба веб-репутації

Відстежує надійність веб-доменів. Служба веб-репутації виставляє оцінки репутації на основі таких факторів, як вік веб-сайту, історичні зміни місцезнаходження та ознаки підозрілої діяльності, виявлені за допомогою аналізу поведінки шкідливого програмного забезпечення.

3. File and Domain Census

- Community File Reputation (CENSUS): Визначає поширеність виявлених файлів. Поширеність - це статистичне поняття, що означає кількість разів, коли файл був виявлений датчиками Trend Micro за певний проміжок часу.
- Domain Census: Визначає поширеність виявлених доменів та IP-адрес. Поширеність - це статистичне поняття, що означає кількість випадків виявлення домену або IP-адреси датчиками Trend Micro за певний проміжок часу.

4. Служба веб-інспекції

Додаткова служба служби перевірки репутації веб-сайтів, яка надає користувачам результати перевірки на детальних рівнях і повні назви загроз.

Назва загрози та ступінь небезпеки можна використовувати як критерії фільтрації для проактивних дій і подальшого інтенсивного сканування.

5. Інтелектуальна мережа захисту (Smart Protection Network)

Deep Discovery Inspector взаємодіє з технологією Trend Micro Smart Protection Network. Smart Protection Network - це хмарно-клієнтська інфраструктура захисту вмісту, призначена для захисту клієнтів від ризиків безпеки та веб-загроз.

Механізм фільтрації URL-адрес (TMUFE) взаємодіє зі службою оцінки репутації в мережі Smart Protection Network. Ця служба виставляє оцінку репутації й блокує або дозволяє користувачам доступ до веб-сайту.

2.3 Призначення, функції та архітектура рішення Trend Micro Deep Discovery Analyzer

Deep Discovery Analyzer - це спеціальний сервер аналізу в режимі пісочниці, який посилює захист від спрямованих атак продуктів Trend Micro та сторонніх розробників. Deep Discovery Analyzer підтримує готову інтеграцію з продуктами Trend Micro (рис. 2.7) для захисту електронної пошти та Інтернету, а також може використовуватися для розширення або централізації аналізу в ізольованому середовищі інших продуктів.

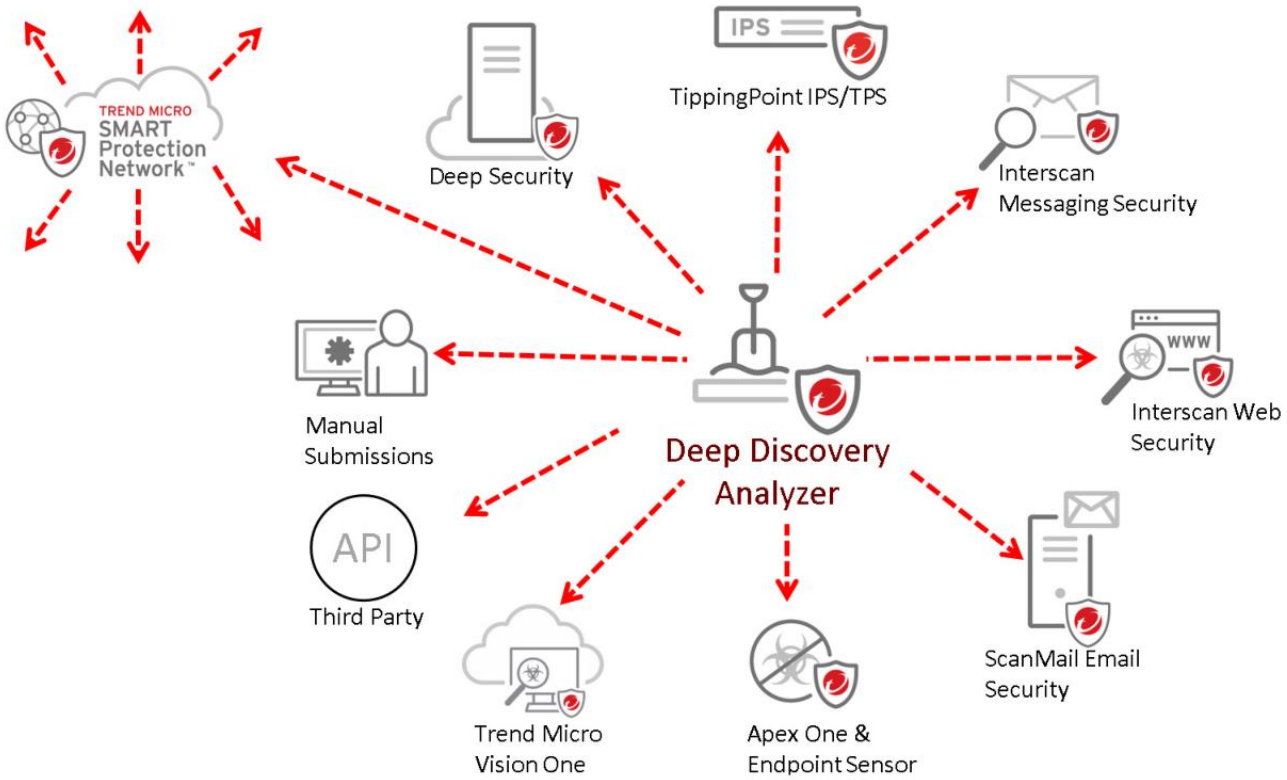


Рис. 2.7 – Інтеграція DDAn з іншими рішеннями Trend Micro

Налаштовуване середовище пісочниці, яке можна створити в Deep Discovery Analyzer, відповідає конфігурації цільового програмного забезпечення для настільних комп'ютерів, що підвищує точність виявлень і зменшує кількість хибних спрацьовувань. Deep Discovery Analyzer також надає API веб-служб для інтеграції з будь-яким продуктом сторонніх розробників та функцію ручного відправлення даних для дослідження загроз. Поєднання Deep Discovery Analyzer з іншими методами виявлення загроз оптимізує рівень виявлення та здатність якісно реагувати, дозволяючи використовувати правильну техніку в потрібний час для боротьби із загрозами.

Впровадження пісочниці DDAn є одним з ключових аспектів багаторівневого захисту. Завдяки такому підходу Deep Discovery Analyzer може значно покращити виявлення та реагування. Нижче наведено опис задач, які вирішуються завдяки DDAn:

1. Швидкий автоматизований обмін даними: Окремі продукти для захисту – від кінцевих точок до електронної пошти та мережевої безпеки – стають

потужнішими завдяки інтеграції на основі інтерфейсу прикладного програмування API. Потенційні загрози, виявлені цими інструментами, автоматично надсилаються до пісочниці Deep Discovery Analyzer. Якщо виявлення визнано зловмисним, воно автоматично поширюється на всі інші підключені рішення для захисту, що дає змогу швидше та якісніше реагувати на загрози.

2. Зменшення кількості хибних спрацювань: Коли безпечні файли або URL-адреси помилково сприймаються як загрози, а потім блокуються, це може призвести до значного зниження продуктивності користувачів. Помилкові спрацьовування можна звести до мінімуму, перенаправляючи будь-яку потенційну загрозу до Deep Discovery Analyzer для отримання остаточної відповіді. Це покращує захист і зберігає продуктивність роботи корпоративної мережі.

Покращення видимості: Дані про загрози корелюються, що полегшує зв'язок між мережею, кінцевими точками, серверами та продуктами мережевої безпеки. Це забезпечує кращу видимість загроз у міру їх виявлення.

Збільшення цінності: Deep Discovery Analyzer підтримує як продукти Trend Micro, так і сторонніх продукти для захисту як від Trend Micro, так і від інших виробників.

Ключові можливості та функціонал Deep Discovery Analyzer

1. Увімкнення пісочниці як централізованої служби

Deep Discovery Analyzer забезпечує оптимізовану продуктивність за допомогою масштабованого рішення, здатного об’єднуватись із рішеннями для захисту електронної пошти, мережі, кінцевих точок та ін.

2. Налаштовувана пісочниця

Deep Discovery Analyzer виконує моделювання та аналіз в ізольованому середовищі, яке відповідає конфігураціям настільного програмного забезпечення, яке зловмисник очікує побачити в корпоративній мережі організації, та забезпечує оптимальне виявлення з низьким рівнем помилкових спрацьовувань.

4. Широкий діапазон аналізу файлів

Deep Discovery Analyzer аналізує широкий спектр виконуваних файлів Windows, Microsoft Office, PDF, веб-вмісту та стиснутих типів файлів, використовуючи кілька механізмів виявлення та імітацію пісочниці.

5. Правила YARA

Deep Discovery Analyzer використовує правила YARA для виявлення шкідливих програм. Правила YARA - це шаблони виявлення шкідливого програмного забезпечення, які можна повністю налаштувати для виявлення цілеспрямованих атак і загроз безпеці, характерних для конкретної корпоративної мережі.

6. Виявлення експлойтів у документах

Використовуючи спеціалізовані засоби виявлення та ізольоване середовище, Deep Discovery Analyzer виявляє шкідливе програмне забезпечення та експлойти, які часто передаються в звичайних офісних документах та інших форматах файлів.

7. Автоматичний аналіз URL-адрес

Deep Discovery Analyzer виконує сканування сторінок і аналіз URL-адрес, які автоматично надсилаються інтегрованими продуктами.

8. Детальні звіти

Deep Discovery Analyzer надає повні результати аналізу, включно з детальними вибірковими діями шкідливого програмного забезпечення та C&C комунікаціями за допомогою центральних інформаційних панелей і звітів.

9. Кластерне розгортання

Кілька автономних пристроїв Deep Discovery Analyzer можна розгорнути й налаштувати в кластер, який забезпечить відмовостійкість, підвищену продуктивність або їх поєднання.

10. Надсилання зразків

Deep Discovery Analyzer дозволяє надсилати зразки одним із таких способів:

- Інтегровані продукти захисту через API веб-служб
- Ручне відправлення на консолі управління
- Відправлення електронною поштою з дозволених доменів відправників і SMTP-серверів

- Сканування мережевих ресурсів
- Інструмент надсилання зразків вручну

11. Інтеграція з індивідуальним захистом

Deep Discovery Analyzer автоматично обмінюється новими даними про виявлення у вигляді IOC з іншими рішеннями Trend Micro та продуктами для захисту від сторонніх розробників.

Deep Discovery Analyzer виконує статичний і динамічний аналіз для виявлення помітних характеристик об'єкта. Характерні ознаки зловмисного об’єкта, який було виявлено та направлено до пісочниці, в DDAn класифікуються наступним чином:

- Антизахист і самозбереження
- Автозапуск або інша конфігурація системи
- Обман та соціальна інженерія
- Видалення, завантаження, обмін або реплікація файлів
- Захоплення, перенаправлення або крадіжка даних
- Неправильно сформоване, дефектне або з відомими ознаками шкідливе програмне забезпечення
- Зміна процесів, сервісів або об'єктів пам'яті
- Руткіт, маскування
- Підозріла мережева активність або активність обміну повідомленнями

Архітектура Deep Discovery Analyzer (рис. 2.8)

1. Dispatcher: Приймає вхідні зразки (EXE, PDF, XLS, DOC, ...)

2. Coordinator: Контролює життєвий цикл виконання зразків

- Запускає зразки або пов'язані з ними програми для зразків
- Вставляє хуки у зразки/програми
- Збирає інформацію щодо поведінки зразка

3. Decision Engine/rules: Виділення шкідливих зразків за зібраною поведінкою

4. API hooks:

- Хуки, що впроваджуються в процес зразка під час запуску
- Широке перехоплення DLL для перехоплення викликів Win32 API для доступу до файлів, реєстру, процесів, системних об'єктів, потоків, мережі.

5. Kernel hooks: Збір даних про поведінку на рівні ядра.

- Монітор файлової системи (tmfilex.sys) - драйвер файлового фільтру, який відстежує будь-який доступ до файлів
- Монітор реєстру (tmregx.sys) - драйвер фільтрації реєстру, який відстежує будь-які зміни, внесені до реєстру Windows
- Монітор процесів (ProcObsrv.sys) - драйвер процесів та модулів, який відстежує процеси, що запускаються або завершуються
- Сканер руткітів (RootkitBuster.exe) - драйвер, який відстежує зміни системних привілеїв
- WinPCAP (npf.sys) - драйвер перехоплення пакетів, який дозволяє перехоплювати мережеві пакети, що надсилаються та отримуються

6. Процеси-приманки:

- Підроблені антивіруси: Копіює файли-приманки фальшивих антивірусів до певних каталогів
- Підроблений провідник: Підроблений процес провідника Windows, який використовується для запуску шкідливих DLL
- Підроблений сервер: Частина засобу мережевої емуляції, що забезпечує підтримку емуляції серверів FTP, IRC та SMTP
- Підроблений веб-сервер: Частина засобу мережевої емуляції, що забезпечує підтримку емуляції HTTP і HTTPS. Це дозволяє працювати багатьом троянам, завантажувачам і хробакам, які потребують підключення до веб-серверів.

Якщо з'єднання із запитуваним сервером недоступне, запит перенаправляється на фальшивий сервер або фальшивий веб-сервер. Ці фальшиві сервери надають фальшиві відповіді на запити в надії змусити шкідливе програмне

забезпечення продовжити виконання, щоб викликати більш активну поведінку. FakeServer надасть просту відповідь на запит, коли отримає його.

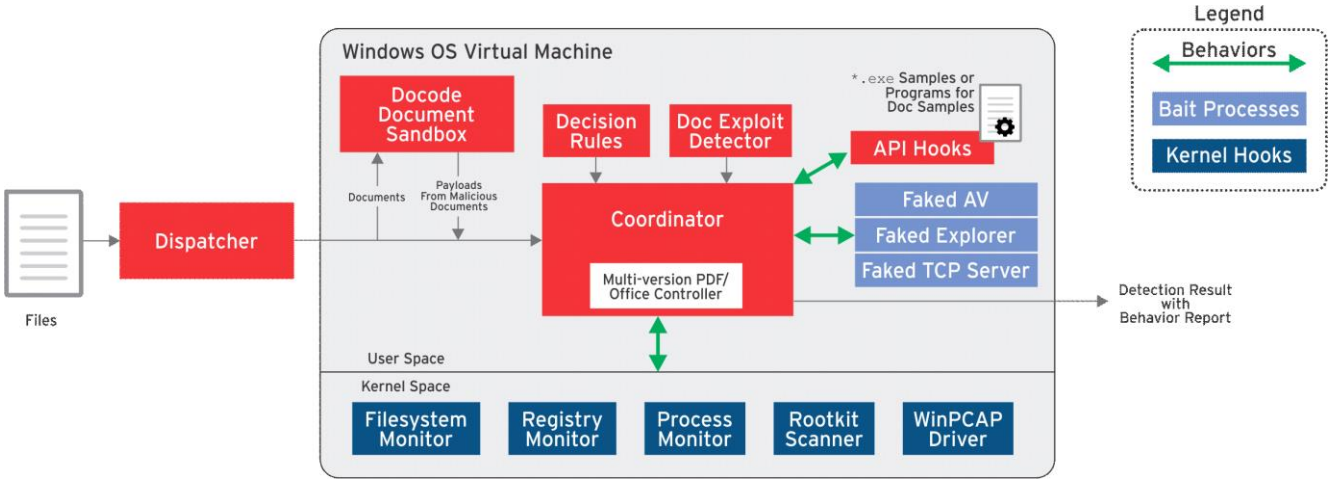


Рис. 2.8 – Архітектура пісочниці на базі DDAn

2.4 Вимоги до розгортання рішень Trend Micro Deep Discovery

Розміщуючи Deep Discovery Inspector в корпоративній мережі, слід звернути увагу, що він повинен мати можливість приймати весь трафік, який може бути спричинений шкідливим програмним забезпеченням.

Крім того, DDI повинен бачити оригінальні IP-адреси кінцевих точок, тому між кінцевими точками і Deep Discovery Inspector не повинно існувати трансляції мережевих адрес (NAT) або проксі-сервісів.

Для управління ризиками Deep Discovery Inspector слід розміщувати в мережі, де знаходяться найбільш критичні та важливі активи. Також можна відстежувати бічні переміщення, залежно від трафіку та продуктивності.

Deep Discovery Inspector може відстежувати мережевий трафік за допомогою наступних методів:

1. Моніторинг декількох портів (рис. 2.9)

Deep Discovery Inspector може здійснювати моніторинг різних сегментів мережі, використовуючи різні порти даних. Порти даних Deep Discovery Inspector підключаються до дзеркальних портів доступу або розподілу комутаторів.

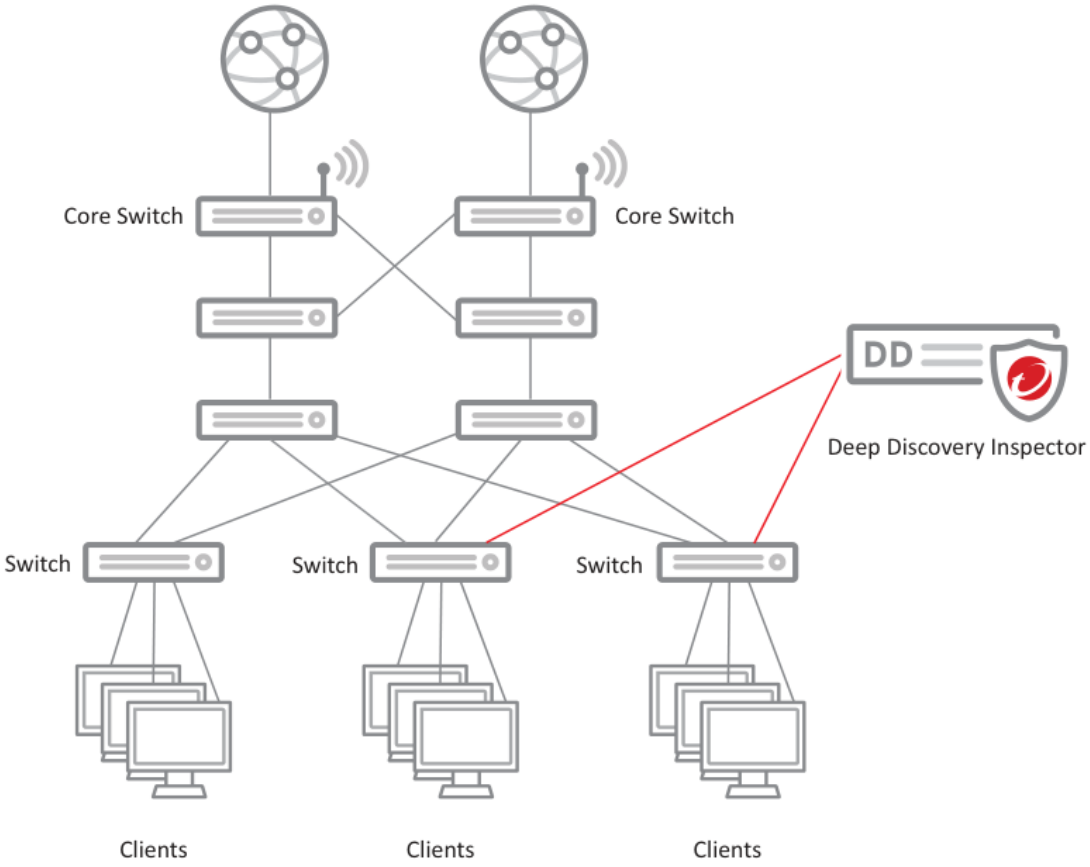


Рис. 2.9 – Відзеркалення трафіку з основних комутаторів корпоративної мережі

2. Моніторинг портів на основі VLAN

Дзеркалення портів на основі VLAN дозволяє користувачам відстежувати трафік на всіх портах, що належать до певної VLAN. У цьому сценарії Deep Discovery Inspector підключається до комутатора і трафік дзеркалюється з певного порту, який належить конкретним VLAN або ж трафік дзеркалюється з магістрального каналу.

3. Дзеркалювання портів VMware

Використовується цей метод тоді, коли необхідно дзеркалювати трафік з мережі VMware. У цьому випадку трафік проходить через віртуальний розподілений комутатор та переходить до DDI.

4. В лінію (Inline)

При розгортанні в лінію Deep Discovery Inspector діє як прозорий міст і може перевіряти розшифрований TLS-трафік (рис. 2.10). DDI не може блокувати

трафік. Коли Deep Discovery Inspector розгорнуто в лінію, трафік лише перевіряється або не перевіряється.

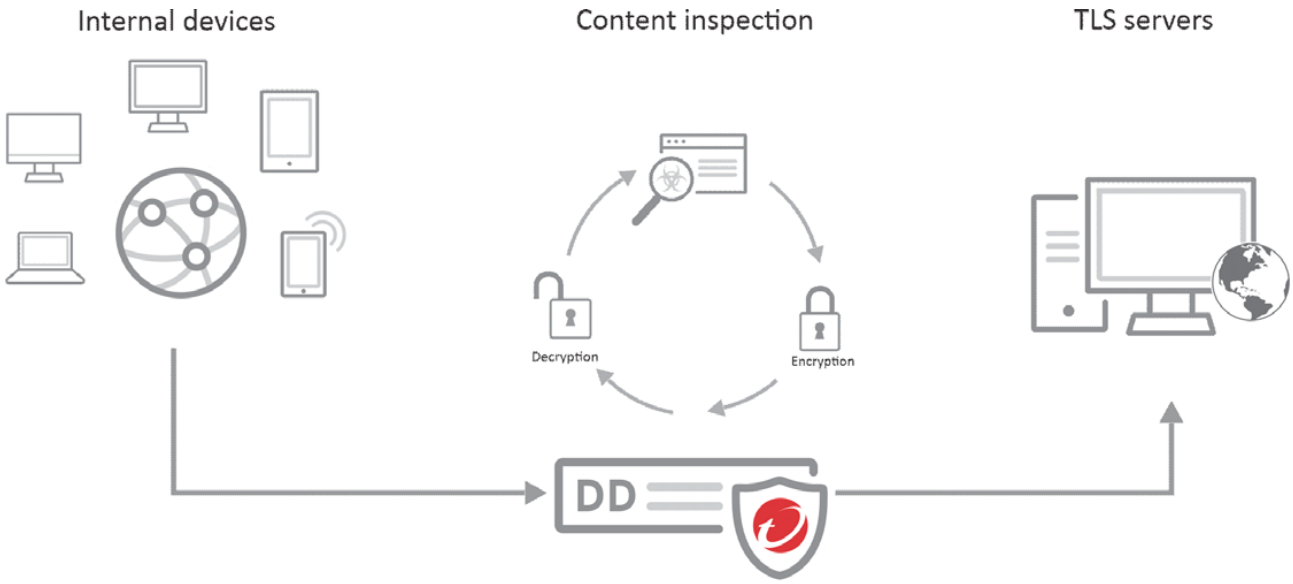


Рис. 2.10 – Розгортання DDI режимі Inline

Додаткові вимоги щодо розгортання DDI в корпоративній мережі

1. DDI повинен приймати весь трафік, який може бути спричинений шкідливим програмним забезпеченням

У більшості випадків сучасні шкідливі програми (ботнети тощо) намагаються встановити з'єднання з інтернет-сервером, а це означає, що Deep Discovery Inspector повинен бачити весь вихідний мережевий трафік. Однак, якщо адміністратори безпеки зосередяться тільки на вихідному трафіку, шкідливе програмне забезпечення, яке поширюється всередині великої корпоративної мережі, буде пропущено, оскільки для цього DDI повинен перехоплювати внутрішній трафік через інтерфейси даних. Якщо в організації працюють внутрішні DNS, SMTP, проксі-сервери або інші сервери, слід налаштувати відзеркалення трафіку до Deep Discovery Inspector таким чином, щоб бачити трафік між цими серверами і кінцевими точками.

2. DDI повинен бачити оригінальні IP-адреси кінцевих точок

Якщо між кінцевими точками і Deep Discovery Inspector є NAT або кінцеві точки використовують проксі-сервер, розташований між кінцевими точками і Deep Discovery Inspector, DDI не зможе побачити справжню IP-адресу кінцевої

точки. Це може призвести до того, що інспектор повідомить неправильну IP-адресу кінцевої точки серверам усунення загрози. У разі з'єднань через проксі-сервери можна ввімкнути перезапис IP-адреси, щоб визначити початкове джерело запиту.

3. Швидкості портів мережевих пристроїв повинні збігатися

Швидкість порту призначення повинна збігатися зі швидкістю порту-джерела, щоб забезпечити однакове дзеркалювання портів. Якщо порт призначення не може обробляти більшу швидкість порту-джерела, то порт призначення може втратити частину даних.

Також, під час розгортання Deep Discovery Inspector, адміністратори повинні враховувати різні мережеві підключення, які DDI встановлює через інтерфейс керування (рис. 2.11).

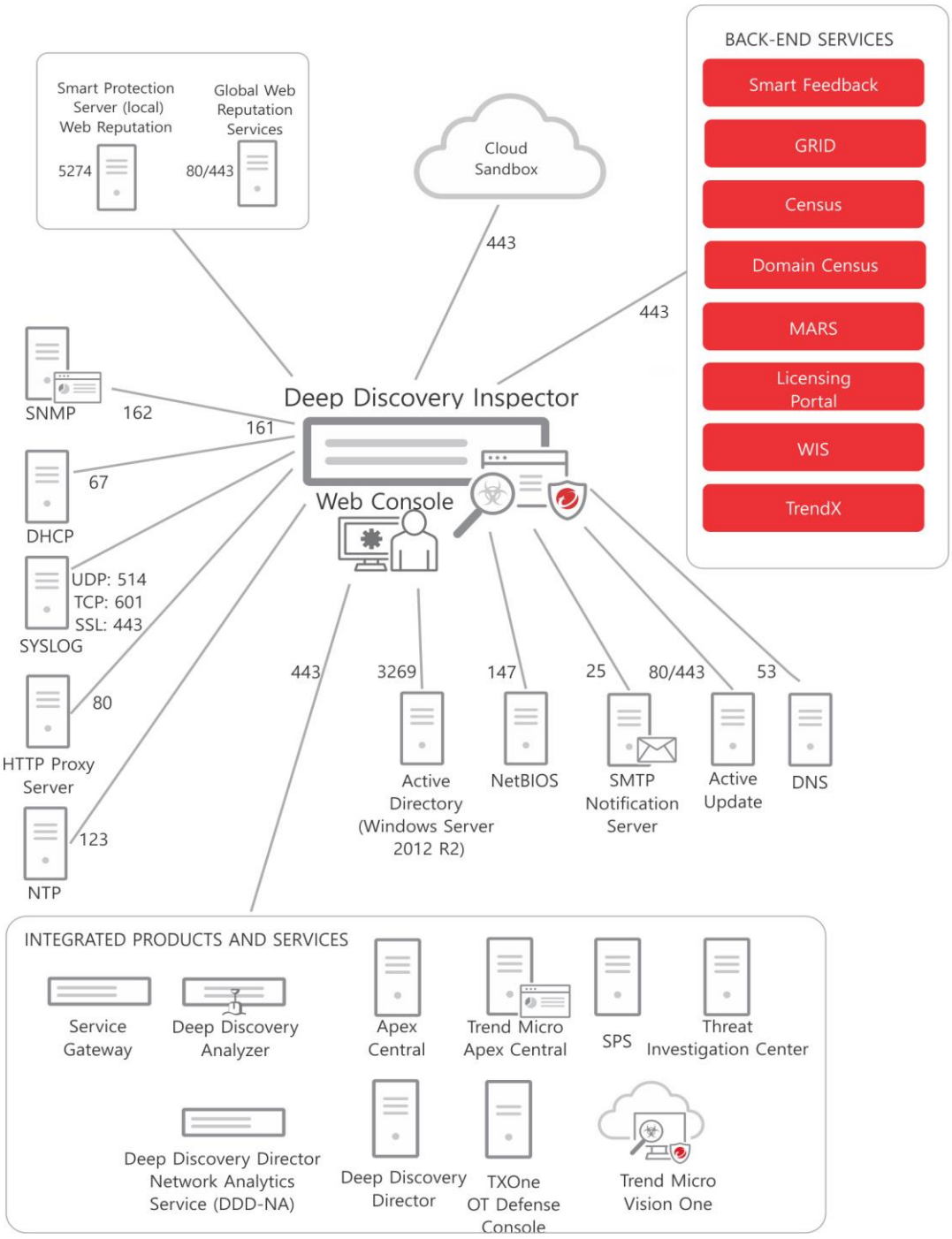


Рис. 2.11 – Необхідні порти, які повинні бути відкриті для комунікації DDI з внутрішніми та зовнішніми сервісами

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ В КОРПОРАТИВНІЙ МЕРЕЖІ НА БАЗІ РІШЕНЬ TREND MICRO DEEP DISCOVERY

3.1 Розроблення варіанта розгортання системи виявлення та реагування на загрози в корпоративній мережі на базі рішень Trend Micro Deep Discovery

Варіанта розгортання рішення Trend Micro Deep Discovery Inspector

Після завершення впровадження DDI в корпоративну мережу та налаштування початкових мережевих параметрів необхідно застосувати певні рекомендовані конфігурації, які допоможуть правильно почати роботу з Deep Discovery Inspector та налаштувати пристрій для подальших можливостей своєчасного виявлення та якісного реагування.

Ці налаштування включають наступне:

- Налаштування параметрів часу та географічного розташування
- Оновлення компонентів Deep Discovery Inspector
- Визначення груп мереж для виявлення загроз, за якими буде вестись спостереження
- Реєстрація доменів і служб

Налаштування місцезнаходження для географічної мапи загроз

Віджет Географічна карта загроз - це графічне зображення уражених хостів на віртуальній карті світу. Всі уражені комп'ютери в різних країнах протягом вибраного періоду часу відображаються в наступних категоріях:

- Джерела шкідливого програмного забезпечення
- Джерела мережевих експлойтів
- Вихідні коди до документів, що експлуатуються
- Джерела шкідливої електронної пошти
- Шкідливі програми зворотного виклику (C&C)

Щоб географічний віджет для певної корпоративної мережі, необхідно виконати такі дії, як перехід до вкладки *Dashboard* > *Threat Monitoring* (рис. 3.1). Далі необхідно налаштувати цей віджет, обравши з переліку країн необхідну країну, в якій фізично розташоване рішення DDI (рис. 3.2)

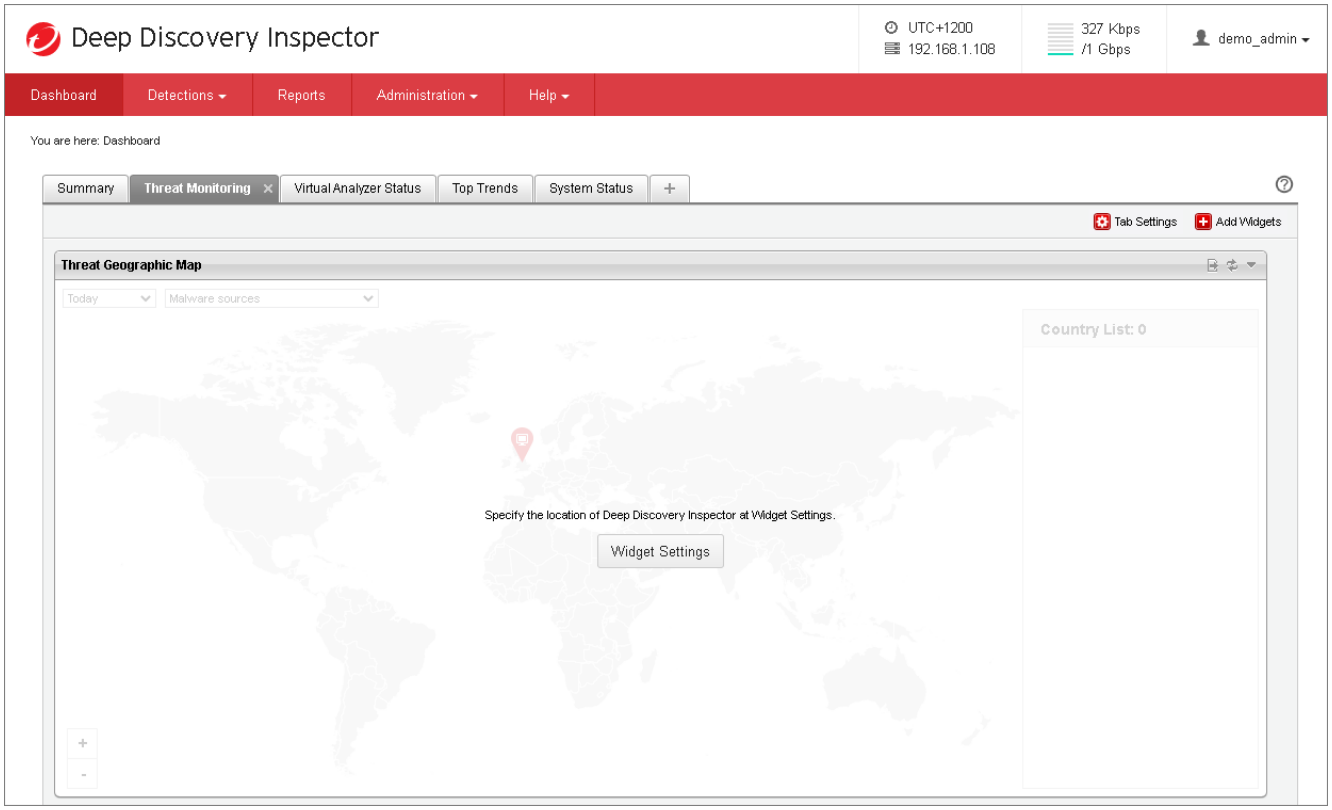


Рис. 3.1 – Налаштування географічного віджету

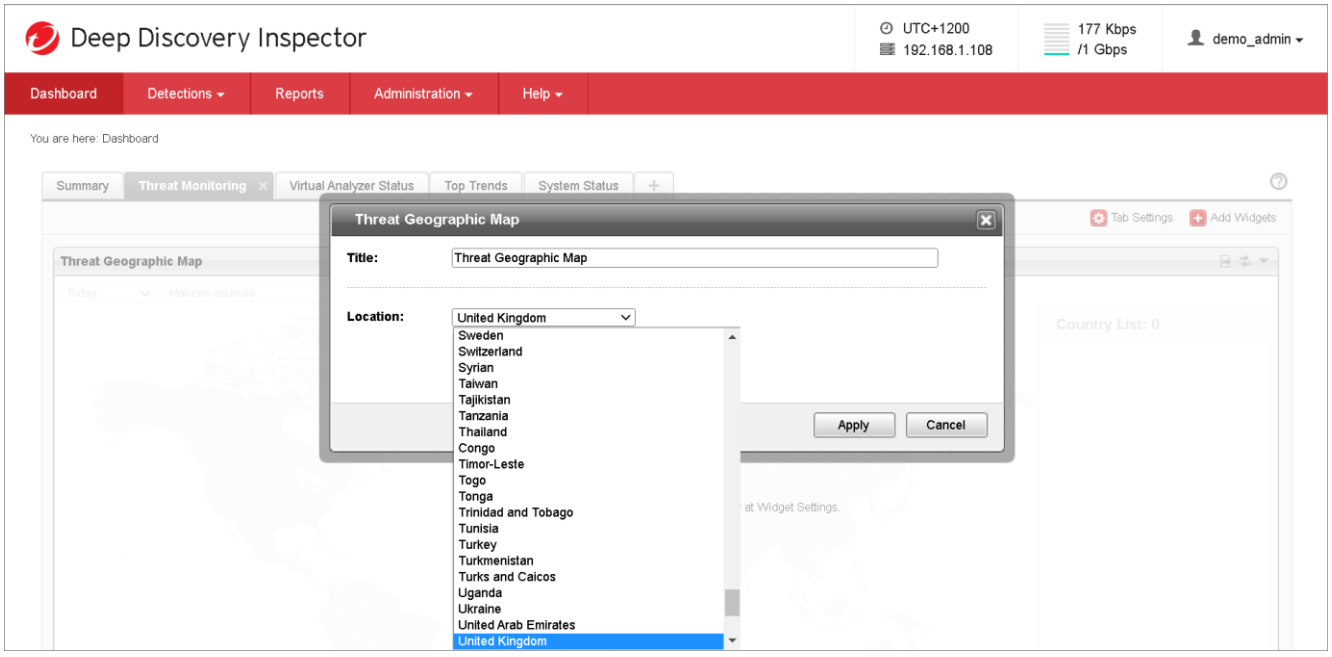


Рис. 3.2 – Вибір необхідної країни

Визначення контрольованих мереж для виявлення загроз

Щоб DDI міг визначати, звідки походять атаки - зсередини або ззовні корпоративної мережі, необхідно налаштувати мережі, за якими буде вестись спостереження, створивши мережеві групи. Правила виявлення Deep Discovery Inspector і рівні серйозності можуть відрізнятися в залежності від того, чи знаходиться хост, який викликає подію, в мережі, що моніториться, чи ні. Тому слід додати всі діапазони IP-адрес корпоративної мережі, які будуть контролюватися Deep Discovery Inspector.

Щоб додати мережеву групу в Deep Discovery Inspector, потрібно перейти до розділу *Administration*, далі обрати розділ *Network Groups and Assets* і натиснути *Network Groups* (рис. 3.3).

Слід також звернути увагу, що якщо внутрішній хост має публічну IP-адресу (наприклад, цей хост знаходиться в DMZ або це ж і є мережа DMZ), то його необхідно також додати в контрольовані мережі.

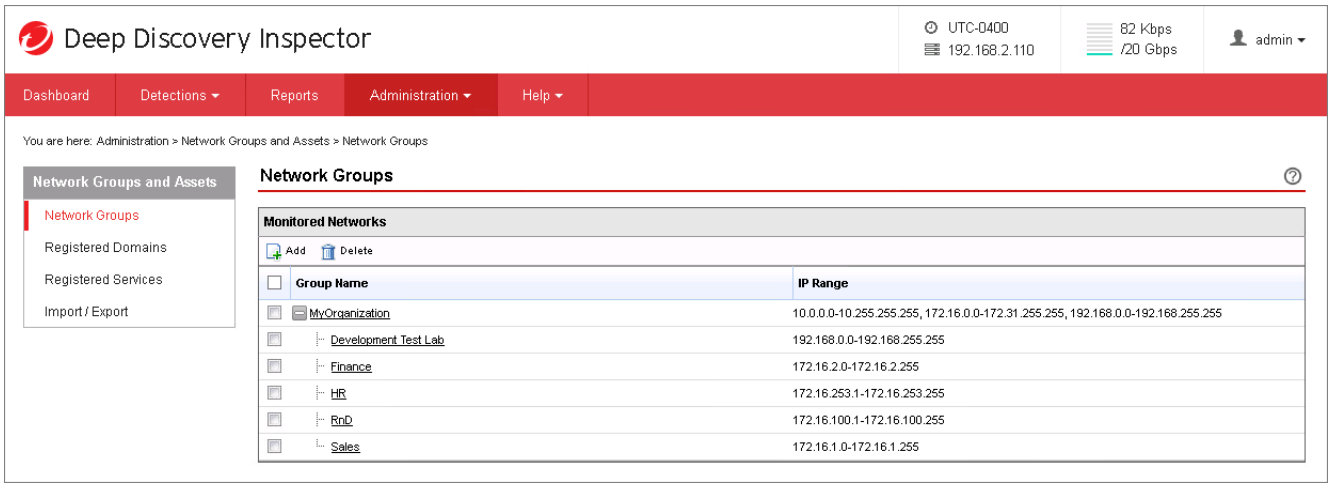


Рис. 3.3 – Налаштування мережевих груп

Реєстрація довірених доменів і служб

У налаштуваннях Registered Domain and Registered Services и Deep Discovery Inspector вказано, які домени та служби (наприклад, DNS, FTP, SMTP тощо) є довіреними (рис. 3.4 та рис. 3.5). Це допомагає організаціям виявляти будь-які несанкціоновані служби або ненадійні домени. Визначення довірених доменів і служб в корпоративній мережі не тільки забезпечує виявлення несанкціонованих

доменів, додатків або служб, але й дозволяє уникнути непотрібних виявлень довірених доменів і служб, які відволікають увагу від важливих спрацювань, що потребують більшої уваги.

Щоб додати зареєстрований домен, потрібно перейти до розділу *Administration*, далі обрати розділ *Network Groups and Assets* і натиснути *Registered Domains* (рис. 3.4).

Кнопка *Analyze* використовується для автоматичного виявлення доменів. Якщо будуть знайдені якісь домени, вони відобразяться у списку, де можна буде обрати ті, які потрібно додати як зареєстрований домен.

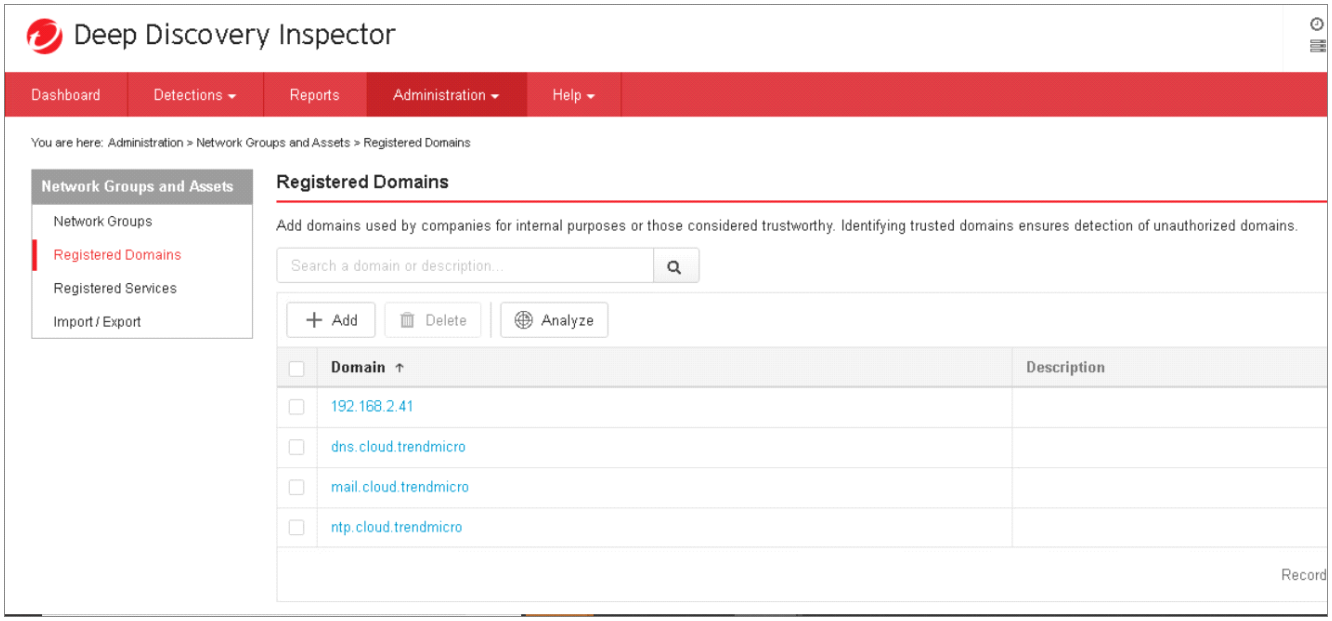


Рис. 3.4 – Додавання зареєстрованих доменів

Зареєстровані служби можна визначити у веб-консолі, перейшовши до розділу *Administration*, далі обравши розділ *Network Groups and Assets* і натиснувши *Registered Services* (рис. 3.5). Зареєстровані служби можна ввести вручну або автоматично виявити, натиснувши кнопку *Analyze*.

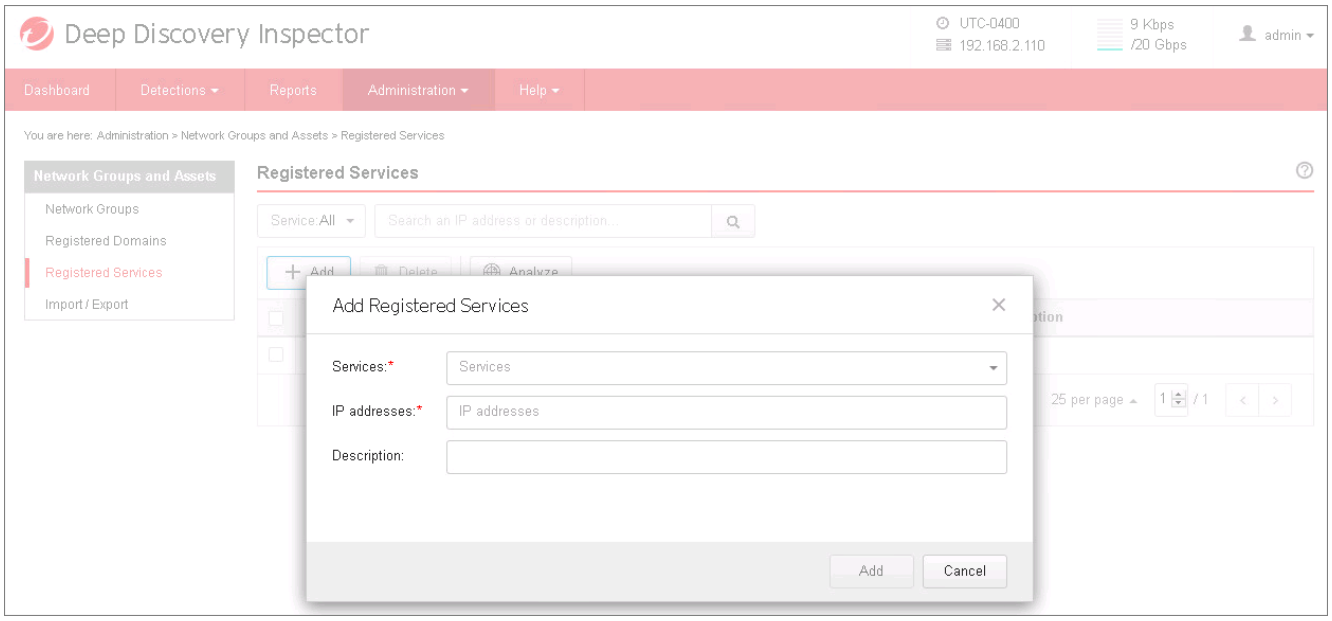


Рис. 3.5 – Додавання зареєстрованих сервісів

Налаштування правил виявлення

Здебільшого правила виявлення в Deep Discovery Inspector, які вже налаштовані та увімкнені за замовчуванням, є гарним початком для початку моніторингу корпоративної мережі на наявність загроз. Проте є також можливість керувати цими правилами, редагувати їх да додавати нові.

Щоб налаштувати правила виявлення, потрібно до розділу *Administration*, далі обрати розділ *Monitoring / Scanning* і натиснути *Detection Rules* (рис. 3.6). В цьому розділі є можливість увімкнути або вимкнути правила виявлення для Deep Discovery Inspector.

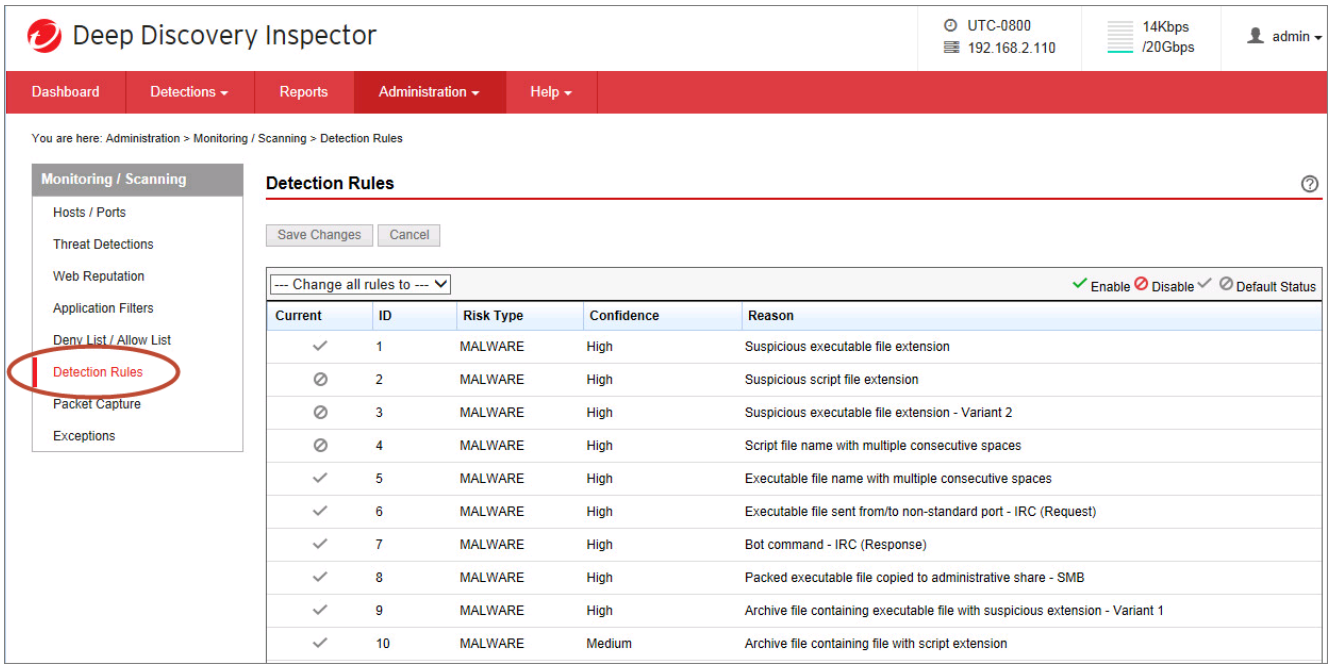


Рис. 3.6 – Налаштування правил виявлення

Налаштування DDI для надсилання підозрілих об'єктів на DDAN

В корпоративних мережах, в яких розгорнуто Deep Discovery Inspector, для аналізу віртуальної пісочниці може використовуватись рішення Deep Discovery Analyzer. Deep Discovery Inspector можна налаштувати таким чином, щоб він надсилав виявлені підозрілі зразки на цю пісочницю Deep Discovery Analyzer.

Для цього потрібно виконати декілька простих кроків, а саме:

1. У веб-консолі DDI необхідно перейти до розділу *Administration* > *Virtual Analyzer* і настинути *Setup*.

2. Встановити для *Virtual Analyzer* параметр *External* і налаштувати параметри наступним чином:

- Адреса сервера: Потрібно ввести IP-адресу пісочниці Deep Discovery Analyzer, налаштованої в корпоративній мережі (рис. 3.7).

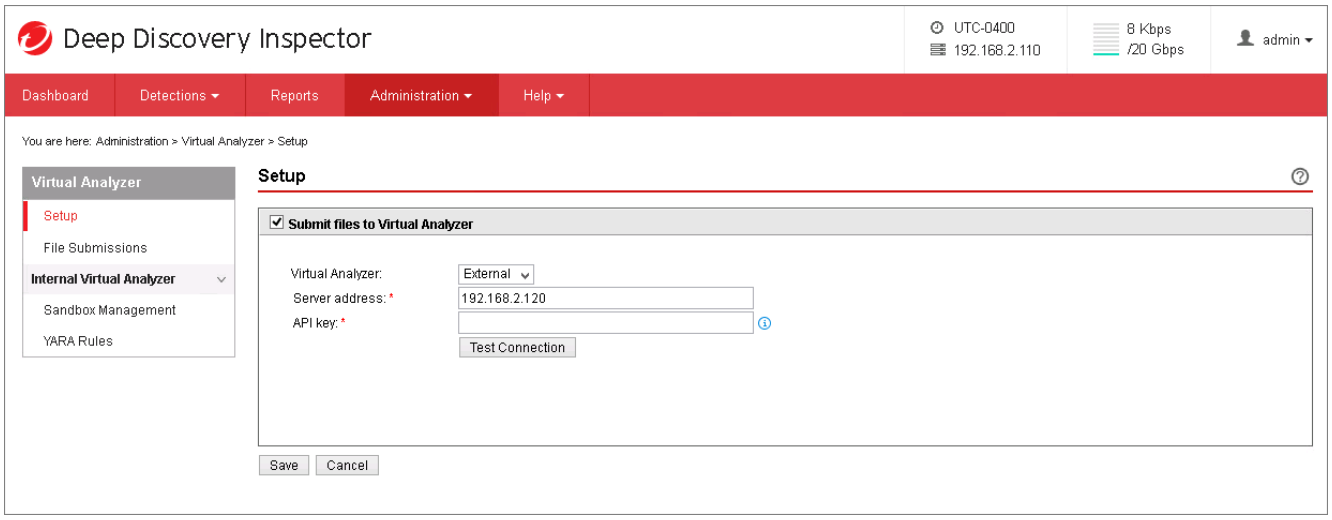


Рис. 3.7 – Додавання параметрів DDAn в консолі DDI

- Ключ API: Далі необхідно взяти ключ, який буде використовуватись для синхронізації DDAn з DDI. Отримати цей ключ можна, використовуючи веб-консоль Deep Discovery Analyzer. В консолі необхідно перейти до розділу *Help* > *About* та скопіювати ключ API (рис. 3.8).

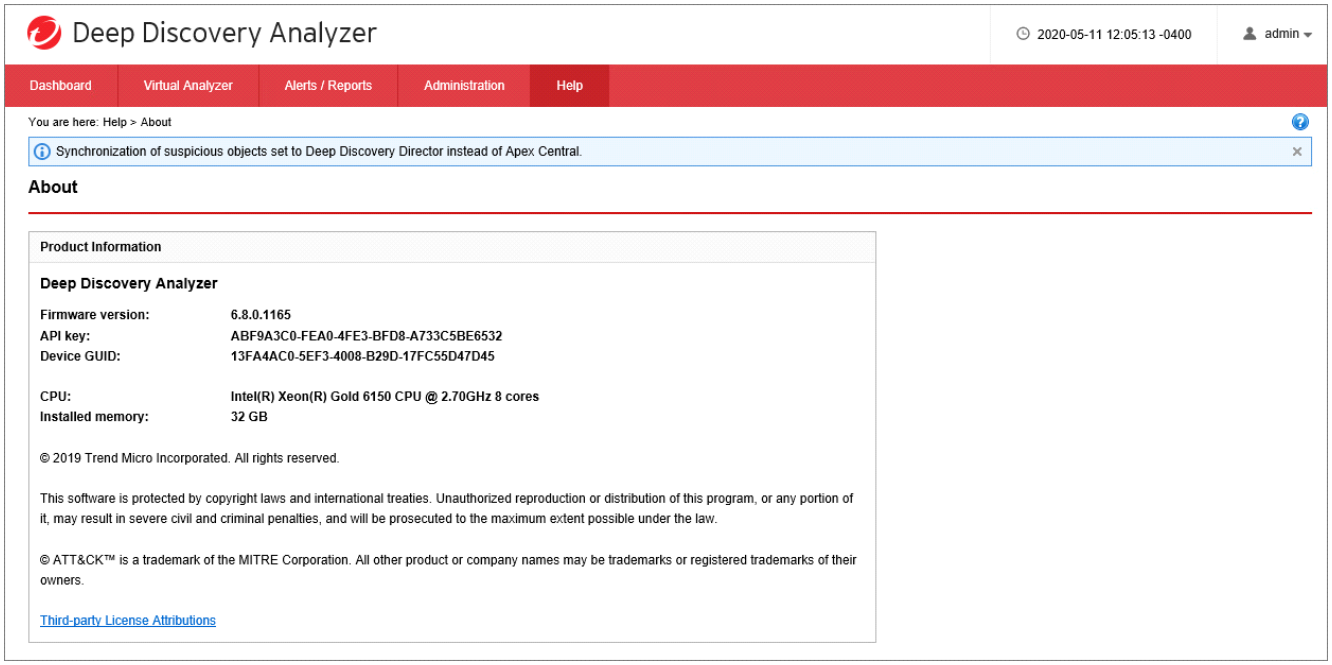


Рис. 3.8 – Отримання ключа API

- Копіюємо та вставляємо ключ API в консолі DDI (рис. 3.9). Натискаємо *Test Connection* для перевірки з'єднання з Deep Discovery Analyzer.

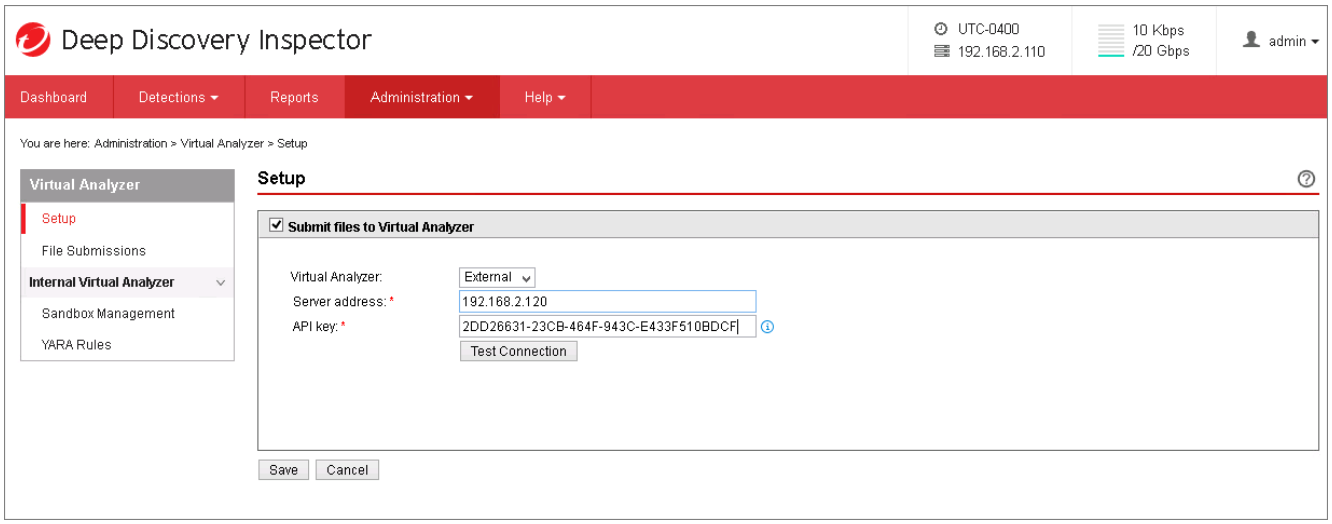


Рис. 3.9 – Завершення налаштування синхронізації DDI з DDAn

На цьому синхронізація завершена.

Варіанта розгортання рішення Trend Micro Deep Discovery Analyzer

Адміністратори можуть створити власну пісочницю для Deep Discovery Analyzer за допомогою інструменту *Virtual Analyzer Image Preparation Tool*, якщо організації потрібне певне середовище поза корпоративною мережею для аналізу підозрілих файлів і поведінки файлів.

Створення пісочниці Windows

Нижче наведено короткий опис кроків, необхідних для створення власної пісочниці та її імпорту до DDAn:

1. Підготовка та встановлення необхідних компонентів та програмного забезпечення на образ віртуальної машини користувацької пісочниці.

2. Імпорт образу віртуальної машини спеціальної пісочниці до Deep Discovery Analyzer.

Вимоги до пісочниці Windows

Перш ніж експортувати образ пісочниці до OVA-файлу, портібно інсталювати на ньому такі компоненти та програми:

1. .NET Framework 3.5 (або новішої версії)

2. Microsoft Office 2003, 2007, 2010 або 2016: Якщо інстальовано Microsoft Office 2010, усі макроси мають бути ввімкнені.

3. (Додавтково) Adobe Flash Player. Він буде автоматично встановлений, якщо його не встановлено.

4. (Додатково) Adobe Acrobat Reader 8, 9 або 11. В цьому випадку потрібно дотриматись певних вимог:

- Trend Micro рекомендує інсталювати версію Acrobat Reader, яка широко використовується в організації.
- Вимкнення автоматичних оновлень для уникнення проблем із моделюванням загроз.
- Інсталювання необхідних мовних пакетів Adobe Reader, щоб можна було обробляти зразки файлів, створені іншими мовами.
- Якщо Acrobat Reader не встановлено, Adobe Reader 8, 9 і 11 буде автоматично інстальовано під час імпорту пісочниці до Deep Discovery Analyzer. Всі три версії використовуються під час моделювання, що вимагає додаткових ресурсів на кожній пісочниці.

Перевірка конфігурації пісочниці

Після створення образу пісочниці його потрібно обробити за допомогою інструменту *Virtual Analyzer Image Preparation Tool*, щоб перевірити і підготувати його до використання у Deep Discovery Analyzer. Інструмент перевіряє, чи виконано всі вищезазначені вимоги до конфігурації, а також вимикає служби, які необхідно вимкнути для належної функціональності пісочниці. Цей інструмент можна отримати безпосередньо в центрі завантажень Trend Micro або за посиланням у веб-консолі Deep Discovery Analyzer. DDAn підтримує імпорт образів пісочниці розміром до 30 ГБ.

Використання інструменту Virtual Analyzer Image Preparation Tool

Після імпортування образу віртуальної машини до пісочниці DDAn, виконуються такі функції:

1. Створюється група пісочниці

Виконуються наступні дії:

- Перевірка, чи було створено OVA-файл за допомогою VirtualBox
- Визначення обсягу вільного дискового простору і попередньо виділення необхідного простору для користувацької пісочниці
- Збереження інформації про групу пісочниці

2. Налаштування шлюзу NAT для віртуальної машини

3. Додаткове налаштування образу віртуальної машини для пісочниці:

- Налаштовуються IP-адреса та назва комп'ютера
- Вмикається автозапуск
- Перевіряється наявність наступного програмного забезпечення: Microsoft Office, Internet Explorer, .NET Framework, Adobe Acrobat Reader/Flash Player (автоматично встановлюється, якщо його немає)
- Встановлюється наступне програмне забезпечення: WinPCAP, Середовище виконання Java (JRE), Adobe Acrobat Reader/Flash Player (якщо не встановлено), Visual C Redistributable
- Deep Discovery Analyzer автоматично вимкне наступне: Брандмауер, Windows Update, Заставка, Windows EDP, служба Центру безпеки, Office Update, Adobe Update та Блокувальник спливаючих вікон (в Windows 7 вимкнуться наступні функції: Захисник Windows, UAC та захищений режим Internet Explorer)
- Deep Discovery Analyzer автоматично налаштує наступне: Захист Microsoft Office (Word, Power Point та Excel) на низький рівень, Безпека Internet Explorer на низький рівень, Конфіденційність Internet Explorer - Приймати всі файли cookie

4. Перезавантаження віртуальної машини.

5. Також є можливість клонувати створену для пісочниці віртуальну машину.

3.2 Розроблення рекомендацій щодо застосування технології виявлення та реагування на загрози в корпоративній мережі на базі рішень Trend Micro Deep Discovery

Рекомендації щодо виявлення та реагування на базі рішення Trend Micro Deep Discovery Inspector

Deep Discovery Inspector досить простий у використанні та адмініструванні. Завдяки широкому набору інструментів DDI дозволяє максимально якісно та швидко виявляти потенційні загрози корпоративній мережі та реагувати на них. Нижче наведений список основних можливостей DDI для виявлення та реагування на загрози в корпоративній мережі.

Використання меню Dashboard для перегляду виявлених загроз

Адміністратори можуть використовувати веб-консоль Deep Discovery Inspector для перегляду інформаційну панель (рис. 3.10), щоб побачити всі загрози, які були виявлені Deep Discovery Inspector.

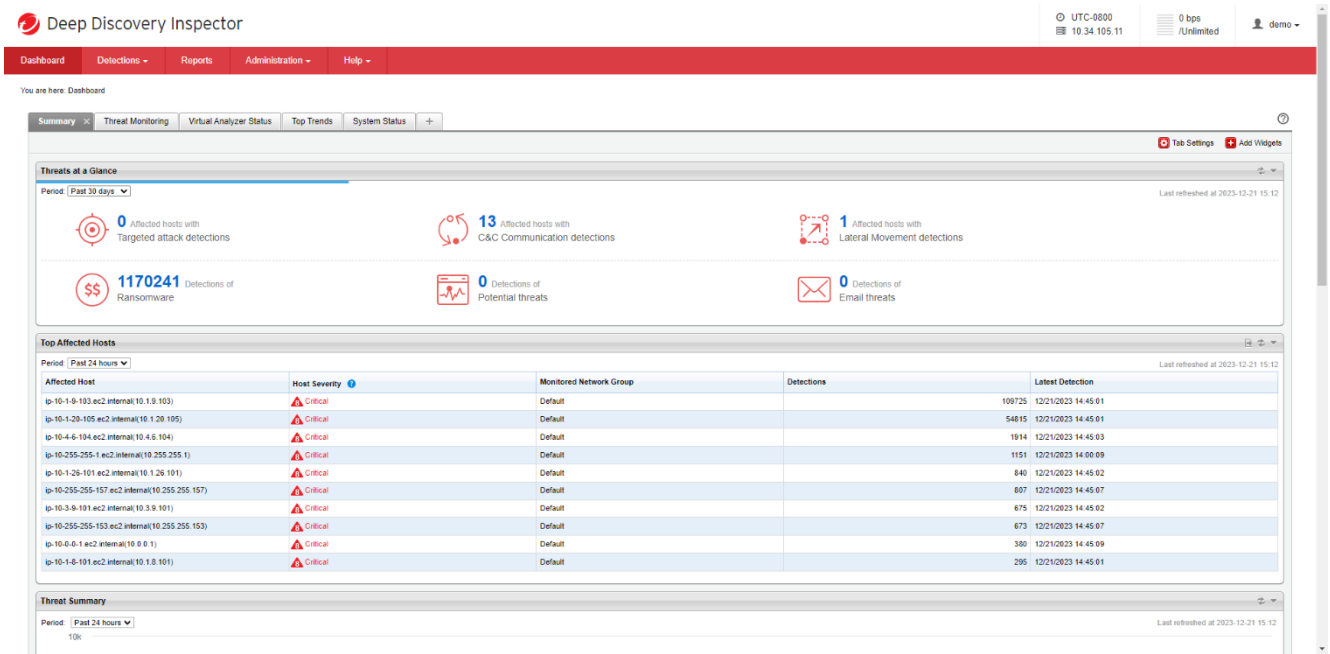


Рис. 3.10 – Панель *Dashboard* веб-консолі DDI

Віджет *Threats at a Glance* на панелі *Dashboard* (рис. 3.11) веб-консолі показує дієву інформацію, яку адміністратори можуть використовувати для отримання доступу до активності атак і загроз у своїх мережах.

Показники, які можна отримати (і надалі проаналізувати), включають:

- Виявлення цільових атак (Відомі загрози)
- Виявлення C&C комунікацій
- Виявлення бічного руху
- Програми-вимагачі
- Потенційні загрози
- Загрози електронної пошти

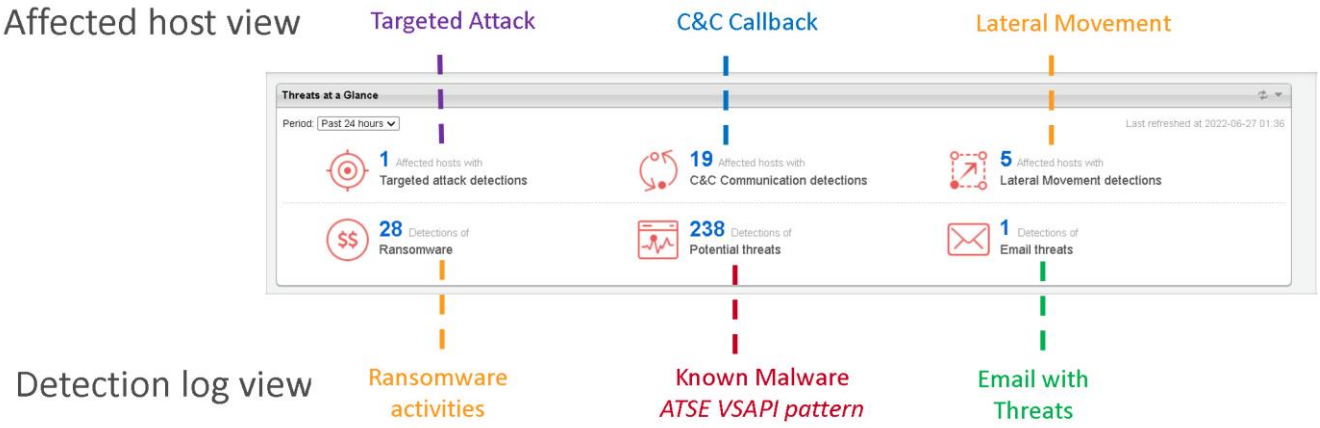


Рис. 3.11 – Віджет *Threats at a Glance*

Використання меню Detections для аналізу виявлених загроз

Меню *Detections* (рис. 3.12) - це місце, де офіцери безпеки будуть проводити більшу частину свого часу у веб-консолі Deep Discovery Inspector, вивчаючи і занурюючись вглиб виявлення загроз, зроблених Deep Discovery Inspector.

Меню *Detections* включає наступні підрозділи:

- *Affected Hosts:* Надає уявлення про всі хости, які були задіяні в одній або декількох фазах цільової атаки
- *C&C Callback Addresses:* Показує хости зі спробами C&C-відповідей на відомі C&C-адреси

- *Suspicious Objects:* Надає інформацію щодо виявлених та проаналізованих підозрілих об'єктів, виявленими DDI та проаналізованими за допомогою DDAn
- *RetroScan:* Історичні журнали веб-доступу для спроб зворотних викликів на C&C-сервери та інших пов'язаних з ними дій
- *All Detections:* Перегляд хостів з виявленнями з усіх журналів подій, включаючи глобальну розвідку, користувацьких списків та інших джерел

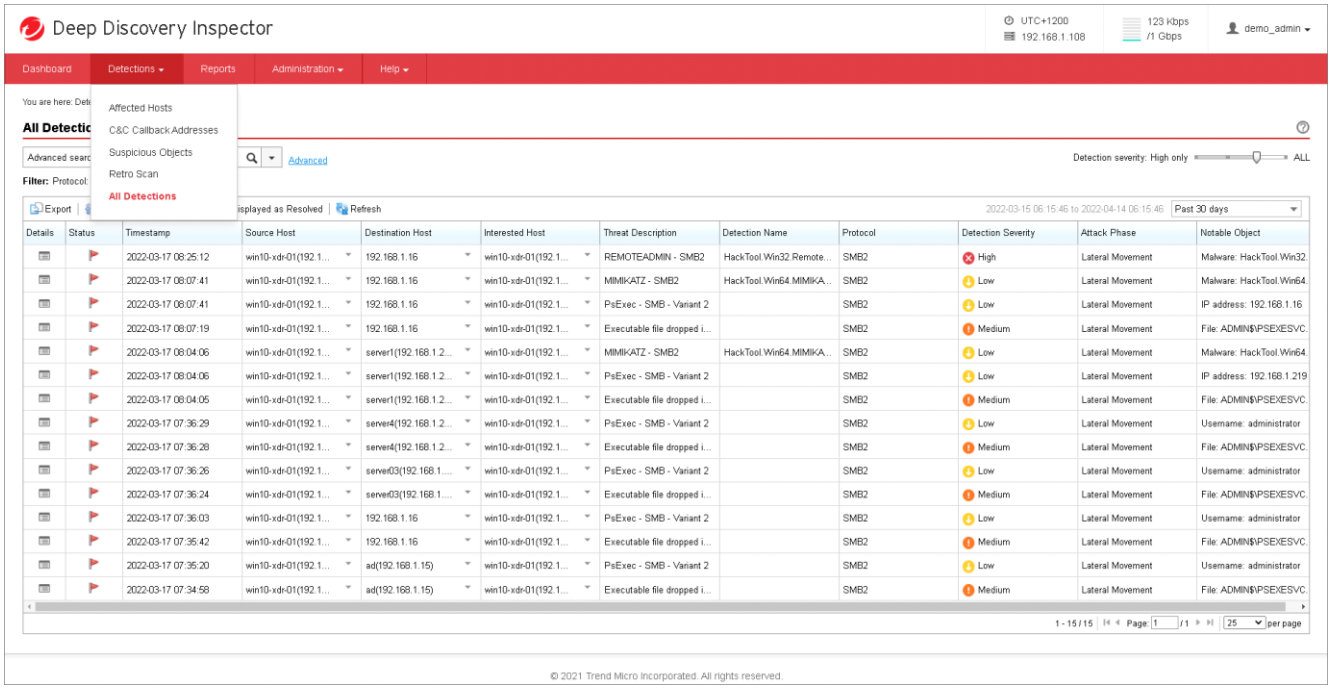


Рис. 3.12 – Меню *Detections*

Вкладка *Affected Hosts* (рис. 3.13) в меню *Detections* веб-консолі дозволяє точно визначити джерело загроз та атак в корпоративній мережі. Це дає змогу ретельніше вивчити інформацію щодо кінцевих точок, які беруть участь в атаці або використовуються для її проведення.

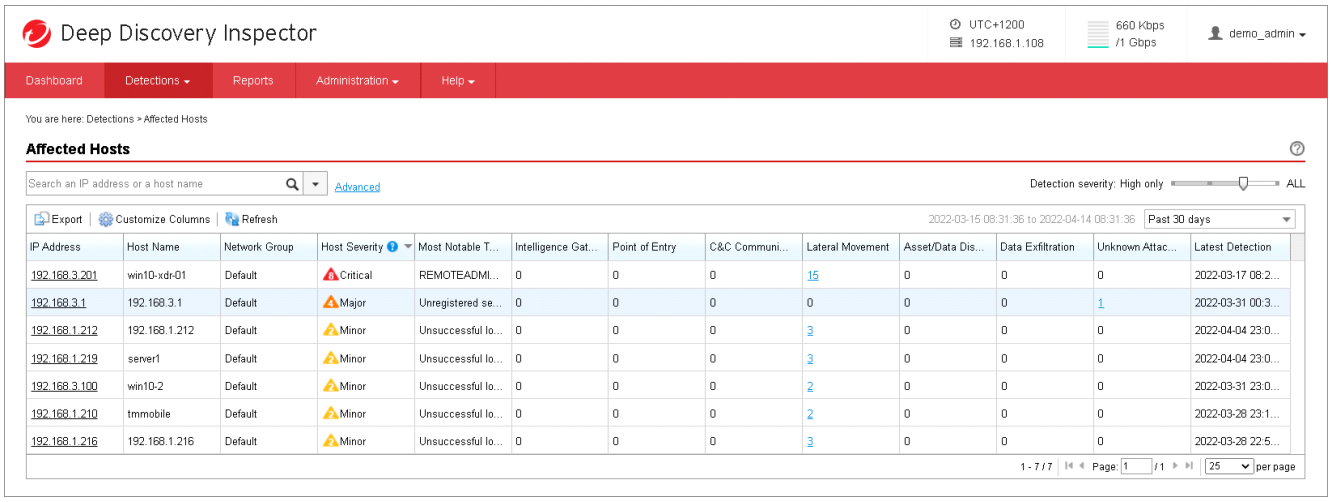


Рис. 3.12 – Відображення інформації на вкладці *Affected Hosts*

Використовуючи цю вкладку додатково можна позначити виявлення як Вирішене, коли воно буде розслідувано (наприклад, офіцером безпеки), натиснувши кнопку *Mark Displayed as Resolved*.

Перегляд деталей виявлення

Перегляд всіх відомостей про виявлення загроз, зібраних Deep Discovery Inspector, доступний завдяки піктограмі *Details*. Ця інформація включає наступні ключові розділи:

- Інформація про виявлення (*Detection Information*)
- Комплексна інформація про з'єднання (*Connection Summary*)
- Інформація про протокол (*Protocol Information*)
- Інформація про виявлений файл/об'єкт (*File Information*)
- Додаткова інформація (*Additional Information*)

На наступному рисунку (3.13) показано сторінку *Detection Details* із загрозою *POISONIVY - HTTP (Response)*, яку виявив Deep Discovery Inspector.

Deep Discovery Inspector

Detection Details

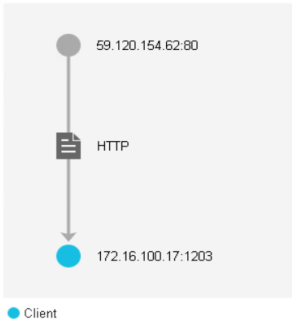
Connection Details

View in Threat Connect | Download

Detection Information

Detection severity:	High
Timestamp:	2022-06-13 16:31:53 -04:00
Detection rule ID:	0
Threat description:	POISONIVY - HTTP (Response)
Notable object:	Malware: BKDR_POISON.BLW
Attack phase:	Point of Entry
Event class:	Malware
Detection type:	Malicious Content
Detection name:	BKDR_POISON.BLW
Virtual Analyzer risk level:	High
	(Refer to File Analysis Result)
Threat:	BKDR_POISON.BLW

Connection Summary



Source

IP address and port:	59.120.154.62:80
Host name:	59-120-154-62.hinet-ip.hinet.net
MAC address:	00:50:56:e3:19:d5 (VMware, Inc.)
Network zone:	No network zone

Destination

IP address and port:	172.16.100.17:1203
Host name:	172.16.100.17
MAC address:	00:50:56:3c:f6:41 (VMware, Inc.)
Network group:	MyOrganization/RnD
Network zone:	Trusted
Operating system:	Windows

Protocol Information

Protocol:	HTTP
User agent:	Mozilla/4.0 (Windows XP 5.1) Java/1.7.0_06
URL:	http://ok.aa24.net/meeting/hi.exe

File Information

File Name	File Size (Bytes)	File SHA-1	File SHA-256
hi.exe	16,896	2F695367E5A694681C33F3840C11815230306C03	09D10AE0F763E91982E1C276AAD0B26A575840AD98...

Additional Information

Detected by:	Advanced Threat Scan Engine
Mitigation:	To be mitigated

File Analysis Result

View Virtual Analyzer Report | Download

File Information

Virtual Analyzer risk level:	High
Threat:	BKDR_POISON.BLW
File name:	hi.exe
File size:	16,896 bytes
File type:	Windows 32-bit EXE file
File SHA-1:	2F695367E5A694681C33F3840C11815230306C03
File SHA-256:	09D10AE0F763E91982E1C276AAD0B26A575840AD986B8F53553A4EA0A948200F
File MD5:	4A55BF1448262BF71707EEF7FC168F7D
Tactics:	TA0002 - Execution, TA0004 - Privilege Escalation, TA0005 - Defense Evasion
Techniques:	T1134 - Access Token Manipulation, T1204 - User Execution

Notable Characteristics

- Anti-security, self-preservation (1)
- Autostart or other system reconfiguration (1)
- Deception, social engineering (1)
- File drop, download, sharing, or replication (5)
- Hijack, redirection, or data theft (1)
- Malformed, defective, or with known malware traits (1)
- Process, service, or memory object change (1)

Рис. 3.13 – Відображення відомостей про виявлену загрозу *POISONIVY - HTTP (Response)*

Інформація про виявлення (*Detection Information*)

Інформація, що надається у розділі *Detection Information* (рис. 3.14), включає наступне:

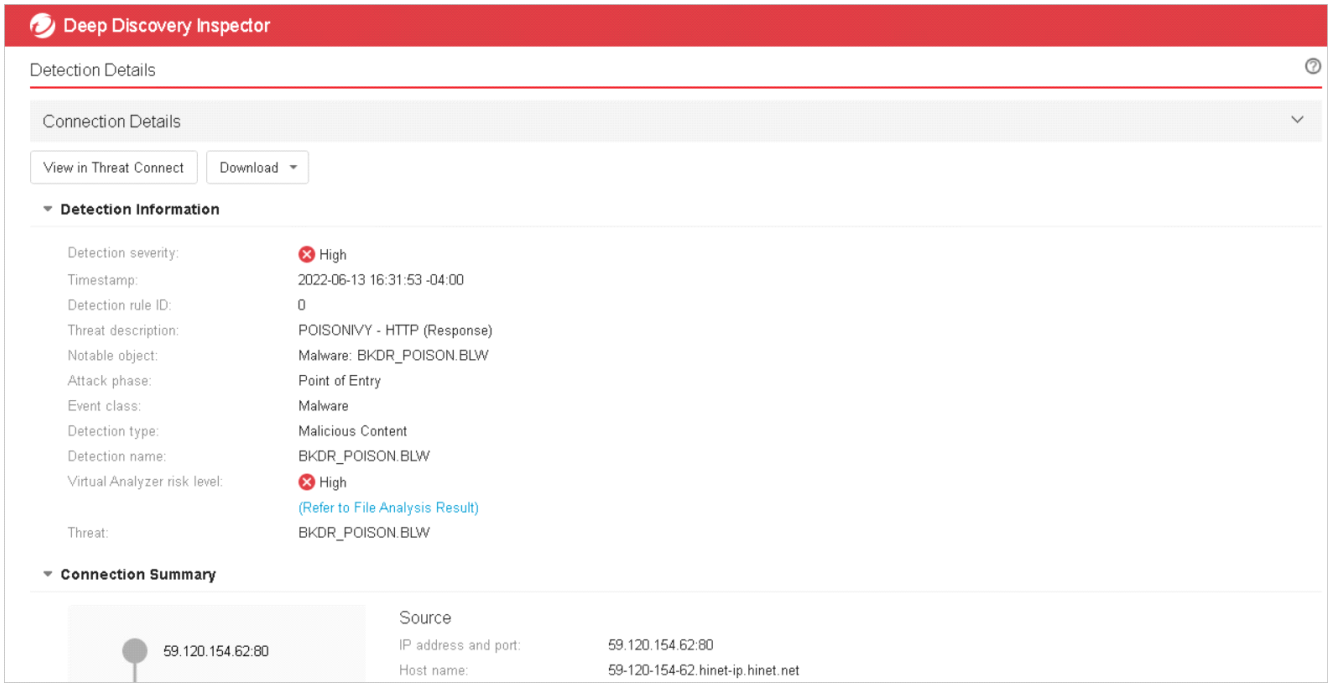


Рис. 3.14 – Інформація про виявлення на вкладці *Detection Information*

- інформація про тип, клас, назву виявленої загрози
- ID правила, яке виявило цю загрозу з посиланням (рис. 3.15) на розширену інформацію щодо цього правила, причини виникнення цієї загрози в корпоративній мережі та рекомендації по локалізації та знищенню цієї загрози

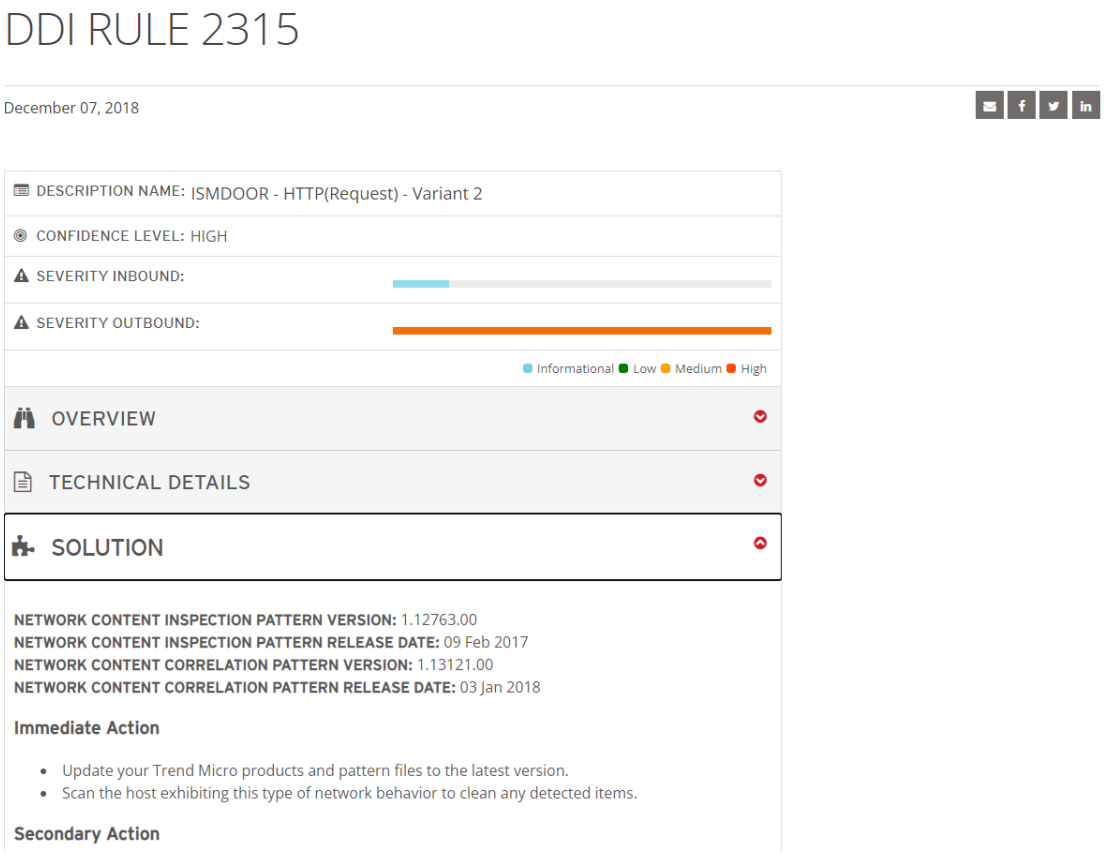


Рис. 3.15 - Розширена інформація щодо правила виявлення

- інформація про техніки та тактики, які використовувались зловмисником, згідно бази знань MITRE ATT&CK, а також посилання на ці техніки та тактики на портал MITRE ATT&CK для більш детального вивчення (рис. 3.16)

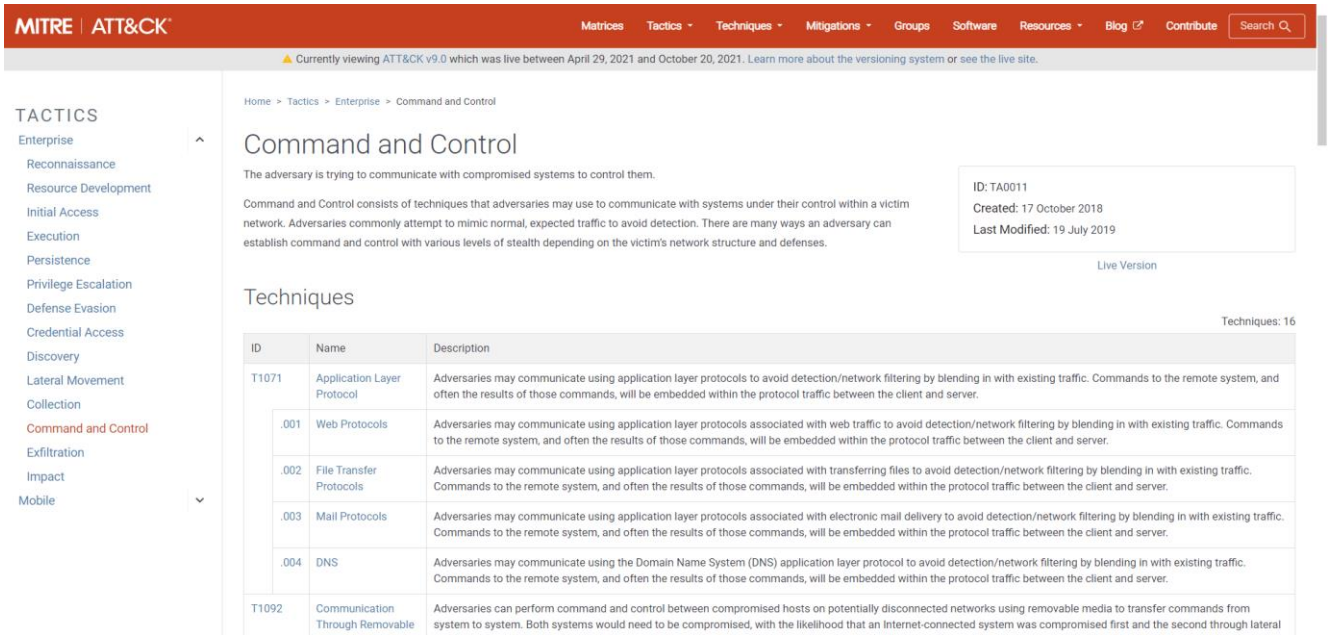


Рис. 3.15 – Приклад тактики TA0011(C&C) на порталі MITRE ATT&CK

Додаткова інформація в розділі *Detection Information* може з'являтися в залежності від різних типів інцидентів.

Використання розділу Connection Summary

Інформація, що міститься в цьому розділі (рис. 3.16), включає в себе:

- Графічне відображення, яке включає напрямок події та іншу інформацію. Клієнт на діаграмі – це хост, який ініціював з'єднання.
- Інформація про хост, яка може включати наступне: ім'я хоста; IP-адреса та порт; користувач, який останній раз входив в систему; MAC-адреса; мережева група; мережева зона; операційна система

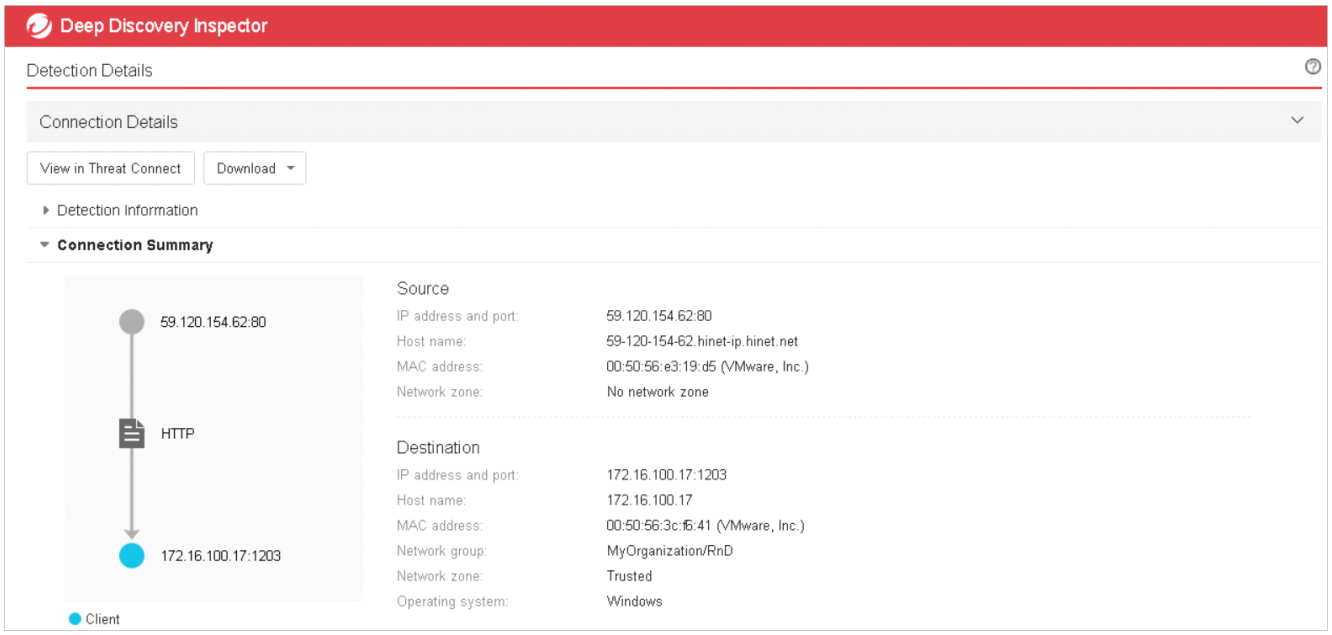


Рис. 3.16 – Відображення деталей мережевих підключень, пов’язаних з виявленою загрозою

Використання розділу Protocol Information

Розділ протоколу містить таку інформацію, як команда бота, URL-адреса бота, доменне ім'я, HTTP-референт, протокол, запитуваний домен, одержувачі тощо (рис. 3.17).

Рис. 3.17 – Відображення деталей протоколу, який використовувався загрозою

Використання розділу File Information

Інформація, що надається в цьому розділі, може включати наступне: ім'я файлу, хєш файлу, розмір файлу (рис. 3.18).

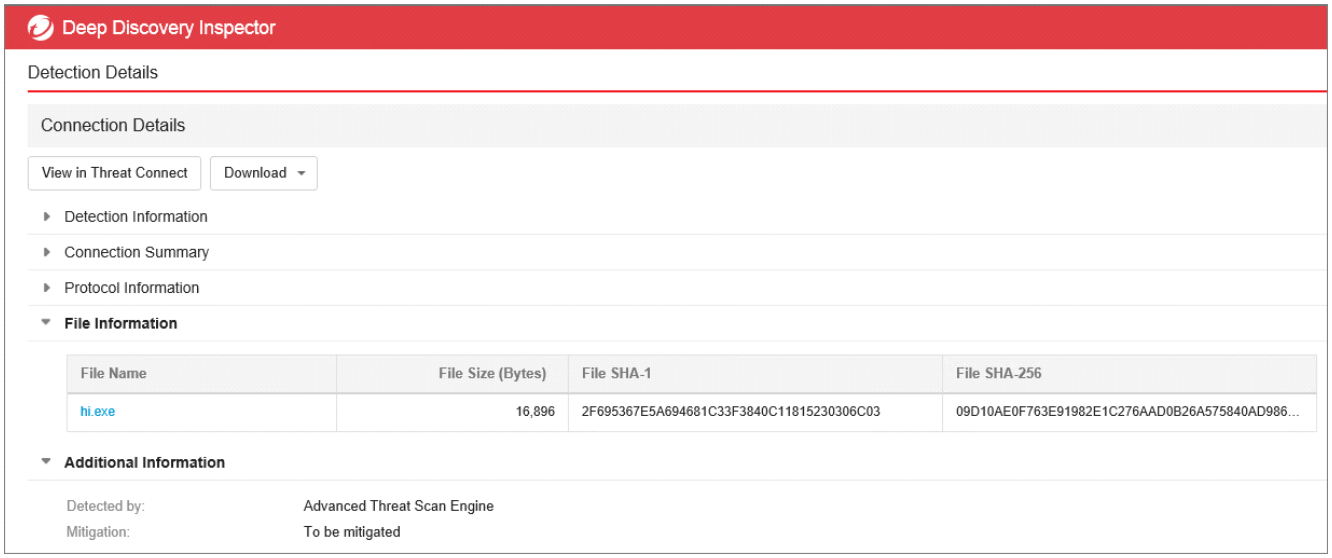


Рис. 3.19 - Відображення деталей виявленого файлу

Перегляд додаткової інформації за допомогою вкладки Threat Connect

На сторінці *Detection Details* можна додатково вибрати вкладку *View in Threat Connect*, розташовану вгорі сторінки, щоб використовувати інформацію з Trend Micro Threat Connect. Threat Connect співвідносить підозрілі об'єкти, виявлені в корпоративній мережі, з даними про загрози з мережі Trend Micro Smart Protection Network. Надаючи доступ до аналітичних баз даних Trend Micro за запитом, Threat Connect дає змогу виявляти й досліджувати потенційні загрози в корпоративній мережі організацій. Крім того, автоматична кореляція дозволяє миттєво створювати

звіти з детальним аналізом загроз і рекомендаціями щодо їх усунення. Ці звіти забезпечують ситуативну обізнаність, необхідну для впровадження більш цілеспрямованих заходів реагування та виправлення ситуації, а також для покращення загального стану безпеки вашої організації. Наприклад, після вибору вкладки *View in Threat Connect*, з'являється наступна сторінка з даними про загрози, отриманими з Trend Micro Global Intelligence Network (рис. 3.20).

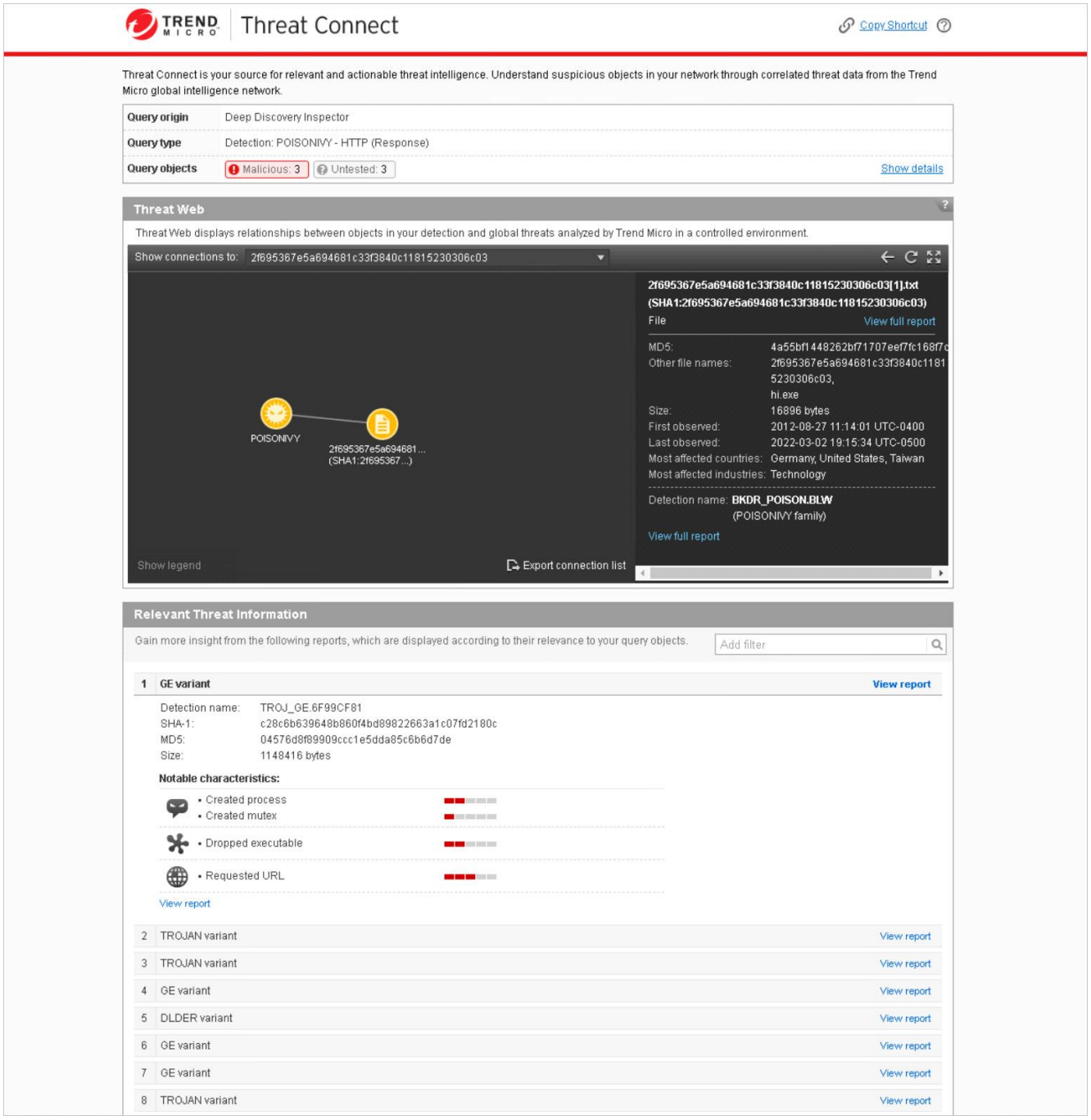


Рис. 3.20 – Відображення додаткової інформації по виявленій загрозі за допомогою Trend Micro Threat Connect

Перегляд інформації щодо командно-контрольних з'єднань (Command and Control Callbacks)

Використовуючи меню *C&C Callback Addresses* можна переглянути список командно-контрольних серверів зловмисників, до яких або від яких було звернення в корпоративну мережу (рис. 3.21)

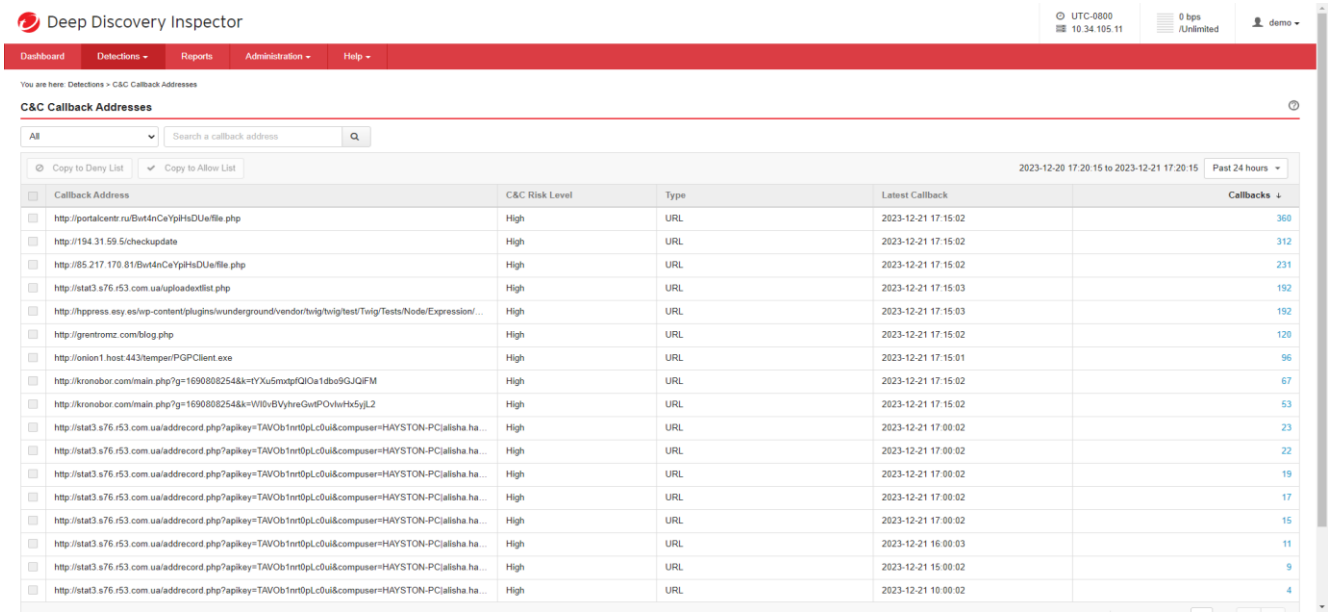


Рис. 3.21 – Відображення списку командно-контрольних серверів в меню *C&C Callback Addresses*

Також слід зауважити на можливість переглядати інформацію щодо звернення до командно-контрольних серверів зловмисників відносно конкретних кінцевих точок. Для цього потрібно використати необхідний фільтр, зображений на рисунку 3.22

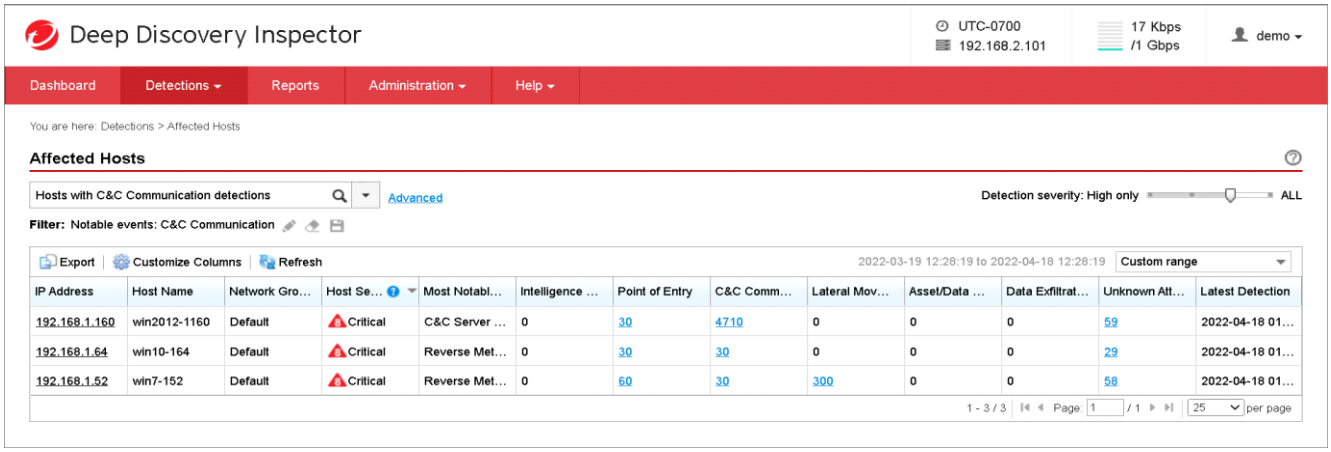


Рис. 3.22 – Використання фільтру C&C на вкладці *Affected Hosts*

Натиснувши на піктограму *Details* для певного хоста, можна переглянути всі C&C виклики, виявлені Deep Discovery Inspector для цього хоста (рис. 3.23).

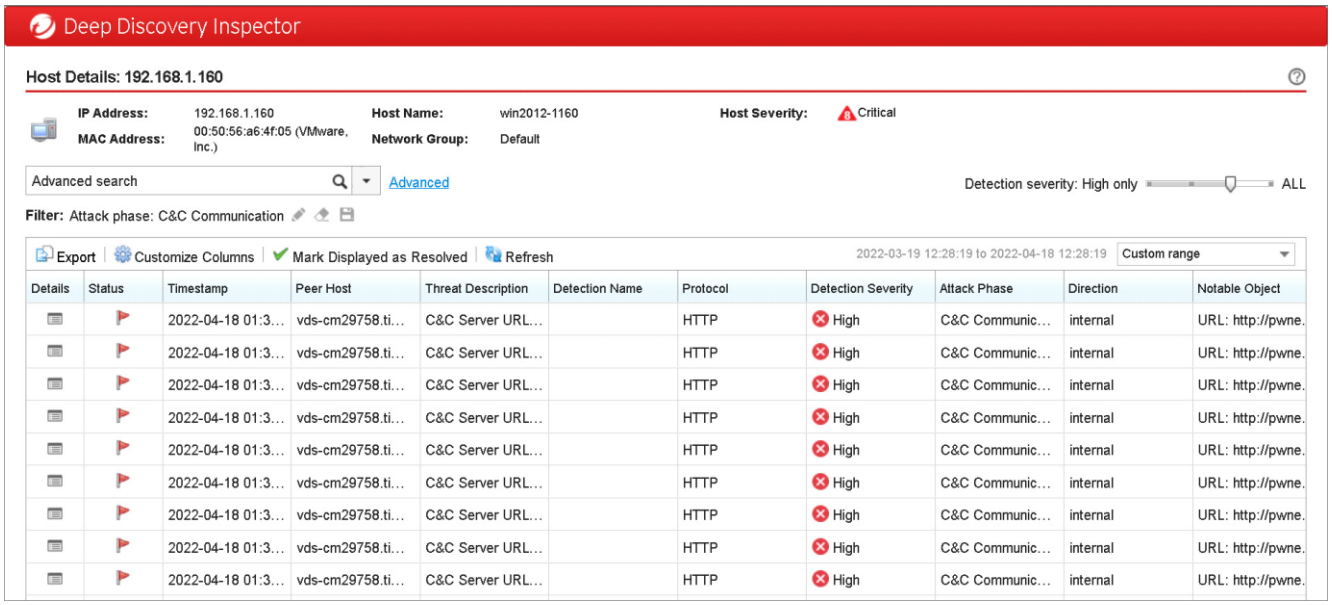


Рис. 3.23 – Відображення інформації щодо C&C викликів відносно певного хоста

Рекомендації щодо використання розширених можливостей виявлення та реагування за допомогою рішення Trend Micro Deep Discovery Analyzer

Перегляд деталей результатів аналізу

Деталі результатів аналізу для оброблених зразків можна переглянути в розділі *Virtual Analyzer* > *Submissions*, натиснувши на запис зразка у вкладці *Completed* (рис. 3.24).

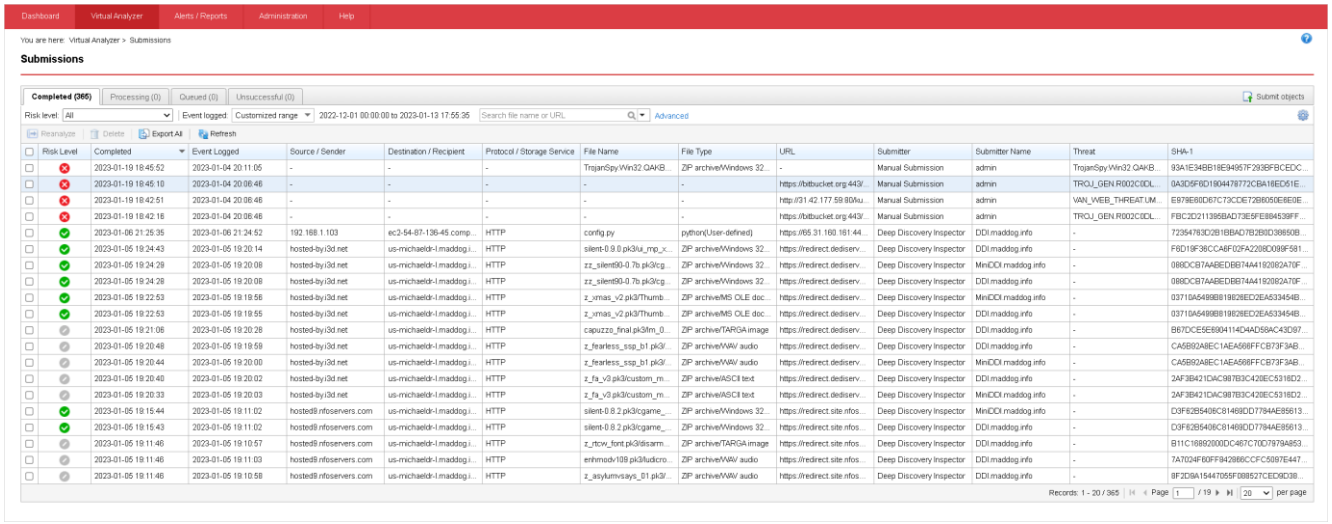


Рис. 3.24 – Список оброблених зразків на вкладці *Submissions*

Обравши будь-який зразок, ви можете переглянути всю аналітичну інформацію, згенеровану аналізатором Deep Discovery Analyzer для цього зразка (рис. 3.25).

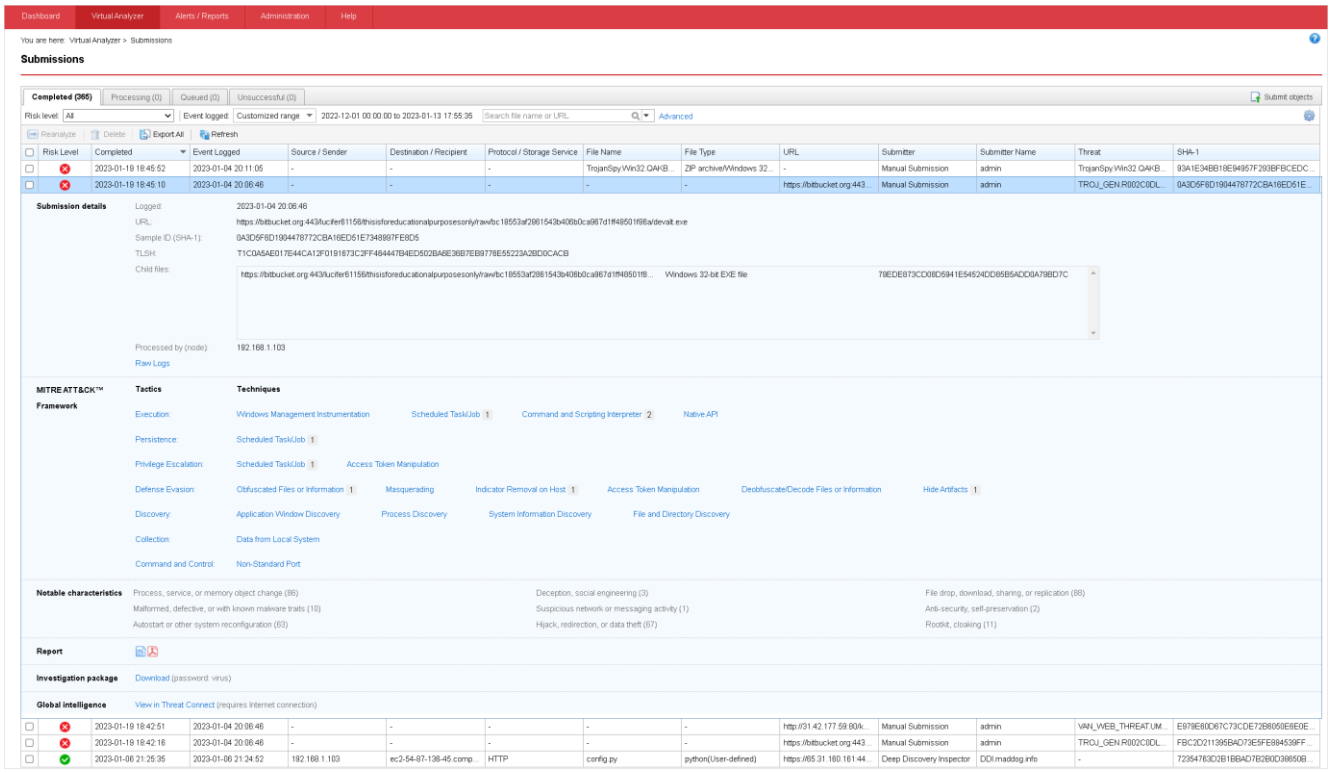


Рис. 3.25 – Перегляд детального аналізу обраного об’єкта

Натиснувши на об'єкт, можна переглянути наступні деталі для аналізованого зразка:

- Деталі аналізу (*Submission details*), що показують URL-адресу пов'язану з об’єктом, значення SHA-1, список дочірніх файлів (якщо такі є), які було виконано.
- Група посилань на всі тактики і методи MITRE ATT&CK Framework, які були використані.
- Примітні характеристики (*Notable Characteristics*), які містять короткий опис характеристик шкідливого програмного забезпечення або підозрілих дій об'єкта, які спостерігав Deep Discovery Analyzer, і які були використані для класифікації шкідливого програмного забезпечення як шкідливого.

- Область *Report*, де можна переглянути HTML-версію звіту або, за бажанням, завантажити PDF-версію звіту.
- Пакет розслідування (*Investigation Package*), який може бути корисним дослідникам загроз для перевірки та інтерпретації даних про загрози, згенерованих із зразків, які проаналізував DDAn. Пакет створюється у вигляді zip-файлу та зашифровується за допомогою пароля *virus*.

ВИСНОВКИ

В роботі проведено дослідження проблеми виявлення та реагування на загрози в корпоративній мережі, досліджено архітектуру та функції корпоративної мережі організації.

Під час аналізу проблеми виявлення та реагування на загрози в корпоративній мережі встановлено актуальність даної проблеми. Визначено актуальні загрози корпоративній мережі та їх використання зловмисниками в рамках циклу сучасної кібератаки (APT). Переміщення зловмисників в середині мережі може залишатись непоміченим без використання належних рішень для виявлення подібних дій. Кожна хвилина має вирішальне значення і не своєчасне виявлення та реагування на загрози, які вже проникли в корпоративний мережевий трафік може призвести до катастрофічних наслідків.

Проведено аналіз сучасних методів та засобів для виявлення та реагування на загрози в корпоративній мережі. Важливим фактором при виборі цих рішень є багатофункціональність цих рішень, якісне відображення становища корпоративної мережі відносно наявних загроз всередині, їх адаптивність під різні варіації корпоративної мережі, можливість інтеграції цих рішень з іншими рішеннями безпеки.

В ході роботи проаналізовано призначення та можливості рішень Trend Micro Deep Discovery Inspector та Deep Discovery Analyzer. Визначено основні функції, необхідні фахівцям з кібербезпеки для своєчасного виявлення загроз та якісного реагування на них. Deep Discovery Inspector виявляє атаки в будь-якій точці корпоративної мережі за допомогою спеціалізованих механізмів виявлення та правил кореляції. Технології, які надає DDI, такі як статичний аналіз, евристичний аналіз, аналіз поведінки, веб-репутації та репутації файлів, забезпечують швидке виявлення загроз, а також багаторівневих шкідливих файлів, вихідних з'єднань та повторні з'єднання з підозрілими файлами. В свою чергу, Deep Discovery Analyzer, який виступає в якості пісочниці, використовує віртуальні образи, налаштовані так, щоб точно відповідати конфігурації системи, драйверам, встановленим програмам

та мовним версіям організації. Такий підхід підвищує рівень виявлення сучасних загроз і програм-вимагачів, які намагаються обійти стандартні віртуальні образи.

В практичній частині роботи розроблено порядок розгортання рішень Deep Discovery Inspector та Deep Discovery Analyzer для виявлення та реагування на загрози в корпоративній мережі. Даний порядок розгортання цих рішень є актуальним на сьогодні та може використовується компаніями будь-якого рівня.

Також в ході роботи надано рекомендації щодо найкращого підходу по застосуванню рішень Trend Micro Deep Discovery Inspector та Deep Discovery Analyzer для своєчасного виявлення та якісного реагування на загрози в корпоративній мережі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Enterprise Networking Architecture [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-an-enterprise-network.html
2. How to design an enterprise core network [Електронний ресурс] – Режим доступу: https://www.arelion.com/knowledge-hub/how-to-guides/how-to-design-an-enterprise-network
3. Incident Response Tools [Електронний ресурс] – Режим доступу: https://www.squadcast.com/incident-response-tools
4. Incident Response Process [Електронний ресурс] – Режим доступу: https://www.bluevoyant.com/knowledge-center/what-is-incident-response-process-frameworks-and-tools
5. Incident Response Playbook for Beginners [Електронний ресурс] – Режим доступу: https://www.trendmicro.com/vinfo/us/security/news/managed-detection-and-response/cyberattacks-from-the-frontlines-incident-response-playbook-for-beginners
6. Incident Response Services & Playbooks Guide [Електронний ресурс] – Режим доступу: https://www.trendmicro.com/en_us/ciso/22/i/incident-response-services.html
7. Advanced Persistent Threat [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Advanced_persistent_threat
8. APT Attack Sequence [Електронний ресурс] – Режим доступу: https://docs.trendmicro.com/all/ent/ddi/v5.5/en-us/ddi_5.5_olh/APT-Attack-Sequence.html
9. Top 21 Emerging Cyber Threats - https://www.aura.com/learn/emerging-cyber-threats
10. Zero-Day Vulnerability [Електронний ресурс] – Режим доступу: https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability
11. Threat Encyclopedia [Електронний ресурс] – Режим доступу: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/

12. Deep Discovery Inspector Overview [Електронний ресурс] – Режим доступу: https://www.trenddefense.com/datasheets/ds_deep_discovery_inspector.pdf

13. Deep Discovery Analyzer Overview [Електронний ресурс] – Режим доступу: https://www.trenddefense.com/datasheets/DS06_DD_Analyzer_171013US.pdf

14. Deep Discovery Inspector Installation and Deployment Guide [Електронний ресурс] – Режим доступу: https://docs.trendmicro.com/o-help/ent/ddi/v6.5/en-us/docs/ddi_6.5_idg.pdf

15. Deep Discovery Inspector Administrator's Guide [Електронний ресурс] – Режим доступу: https://docs.trendmicro.com/o-help/ent/ddi/v6.5/en-us/docs/ddi_6.5_ag.pdf

16. Deep Discovery Analyzer Installation and Deployment Guide [Електронний ресурс] – Режим доступу: https://docs.trendmicro.com/o-help/ent/ddan/v7.5/en-us/ddan_7.5_idg.pdf

17. Deep Discovery Analyzer Administrator's Guide [Електронний ресурс] – Режим доступу: https://docs.trendmicro.com/o-help/ent/ddan/v7.5/en-us/ddan_7.5_ag.pdf