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

Кваліфікаційна робота
на тему:

«Технологія виявлення та реагування на аномальну мережеву активність на прикладі FortiNDR»

Виконав: ДЕТЧЕНЯ Дмитро Юрійович, БСДМ-62
Керівник: ГАХОВ Сергій Олександрович, к.військ.н., доц.

Об'єкт дослідження – виявлення та реагування на аномальну мережеву активність

Предмет дослідження – технологія виявлення та реагування на аномальну мережеву активність на прикладі FortiNDR

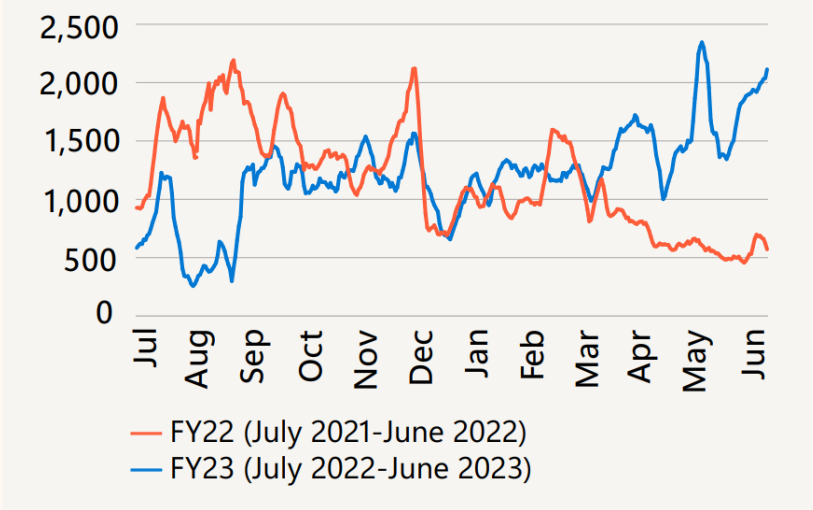
Мета роботи – розробити порядок застосування технології виявлення та реагування на аномальну мережеву активність та рекомендації щодо її реалізації

Наукові завдання:

- дослідити сутність проблеми виявлення та реагування на аномальну мережеву активність;
- проаналізувати підходи до виявлення та реагування на аномальну мережеву активність;
- проаналізувати існуючі рішення із виявлення та реагування на аномальну мережеву активність;
- проаналізувати методи та засоби виявлення та реагування на аномальну мережеву активність на базі FortiNDR;
- розкрити порядок реалізації технології виявлення та реагування на аномальну мережеву активність.

Дослідження проблеми виявлення та реагування на аномальну мережеву активність

У Звіті Microsoft Digital Defense Report 2023 констатується, що ландшафт кіберзагроз продовжує еволюціонувати в бік більш ефективних і руйнівних атак, які часто відбуваються у великих масштабах. Згідно з даними Microsoft, організації зіткнулися із загальним збільшенням кількості атак з використанням програм-вимагачів порівняно з попереднім роком, а кількість атак, керованих людьми, зросла майже втричі. 13% атак з використанням вірусів-здирників, які перейшли у фазу вимагання, включали в себе ту чи іншу форму викрадення даних.



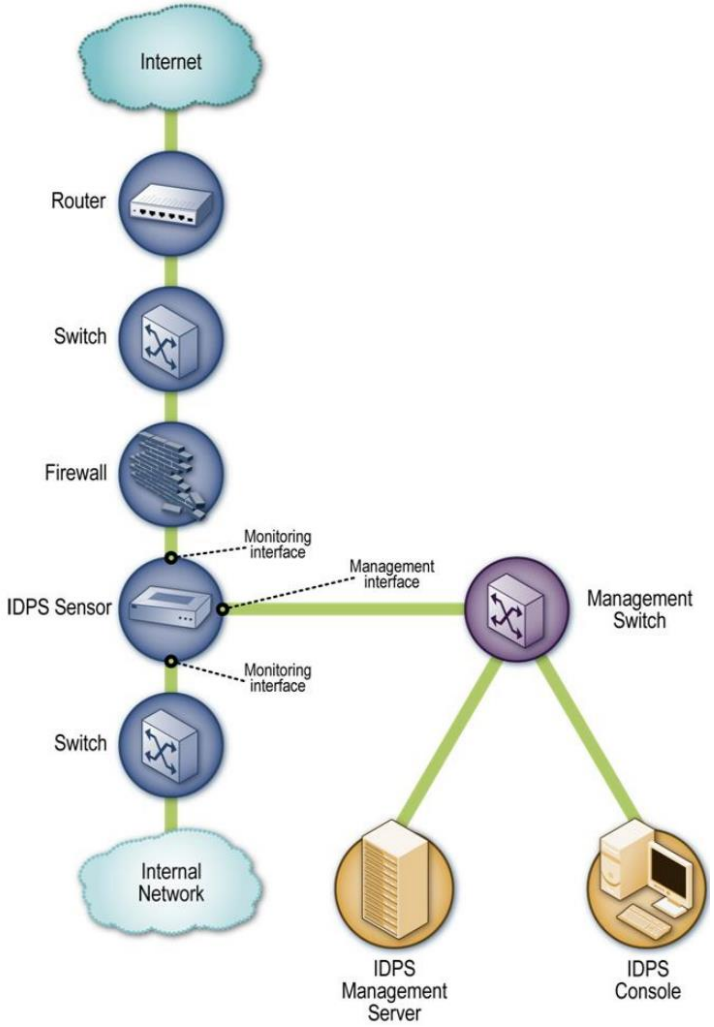
Source: Microsoft Global DDoS Mitigation Operations

Microsoft зазначає, що кількість DDoS-атак не лише продовжує зростати, але й, можливо, в майбутньому вони матимуть ще більший вплив. Минулого року глобальні операції Microsoft з протидії DDoS-атакам у середньому протистояли 1 700 DDoS-атакам на день (рисунок).

Необхідно відмітити, що зловмисники постійно вигадують і переосмислюють більш ефективні способи здійснення своїх атак. Їх ухильна поведінка та невидимі сліди, які вони залишають після себе, змінюються із високою швидкістю. Традиційні застарілі системи безпеки, призначені для захисту від зловмисників, не реагують на ці постійно мінливі моделі поведінки, що дає кіберзлочинцям свободу дій для шпигунства, розповсюдження та крадіжок. Тому, потрібен надійний спосіб виявлення прихованих зловмисників, які проникають всередину, і миттєвого реагування на них, щоб зупинити загрозу витоку даних.

Аналіз підходів до виявлення та реагування на аномальну мережеву активність

Існує багато типів технологій виявлення та попередження вторгнень, які відрізняються насамперед типами подій, які вони можуть розпізнавати, і методологіями, які вони використовують для виявлення можливих інцидентів.



IDPS на основі мережі, яка відстежує мережевий трафік для певних сегментів мережі або пристроїв і аналізує активність мережі та протоколів додатків, щоб виявити підозрілу активність.

IDPS на основі аналізу мережевої поведінки, яка досліджує мережевий трафік для виявлення загроз, що генерують незвичні потоки трафіку, таких як DDoS-атаки, сканування та певні форми шкідливого програмного забезпечення.

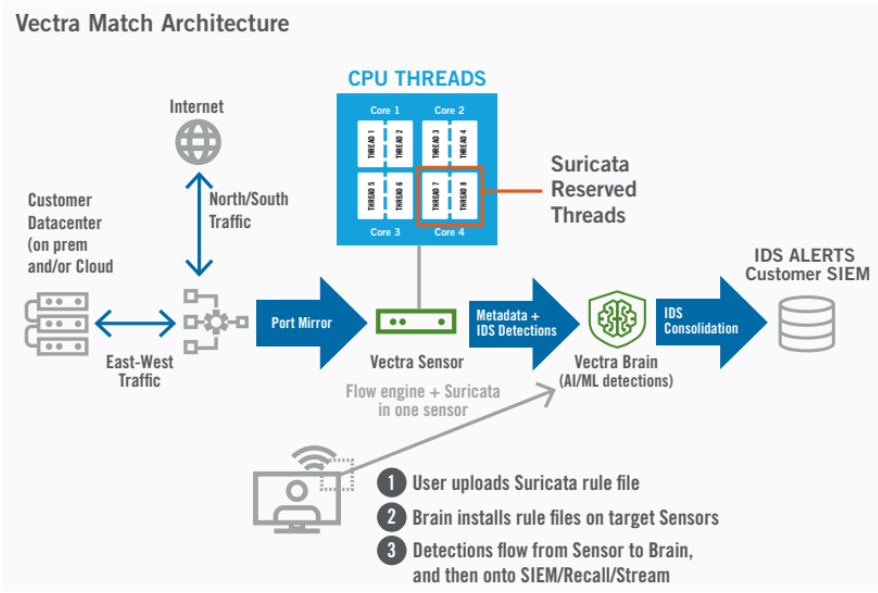
Як приклад, вбудований датчик розгортається таким чином, що мережевий трафік, який він контролює, повинен проходити через нього, подібно до трафіку, пов'язаного з брандмауером. Насправді, деякі вбудовані датчики є гібридними пристроями міжмережевого екрану/IDPS, тоді як інші є просто пристроями IDPS. Основна мотивація для розгортання вбудованих датчиків IDPS полягає в тому, щоб вони могли зупиняти атаки, блокуючи мережевий трафік.

Аналіз існуючих рішень із виявлення та реагування на аномальну мережеву активність

Фахівці з безпеки відмічають позитивний комплексний ефект поєднання інформації про виявлення та реагування мережі (NDR) із SIEM і EDR для формування тріади видимості SOC.
Сучасні рішення NDR використовують передову аналітику, машинне навчання і поведінковий аналіз для виявлення аномалій і невідомих загроз. Це має вирішальне значення, оскільки традиційні заходи безпеки можуть не впоратися з виявленням нових або постійно еволюціонуючих загроз.

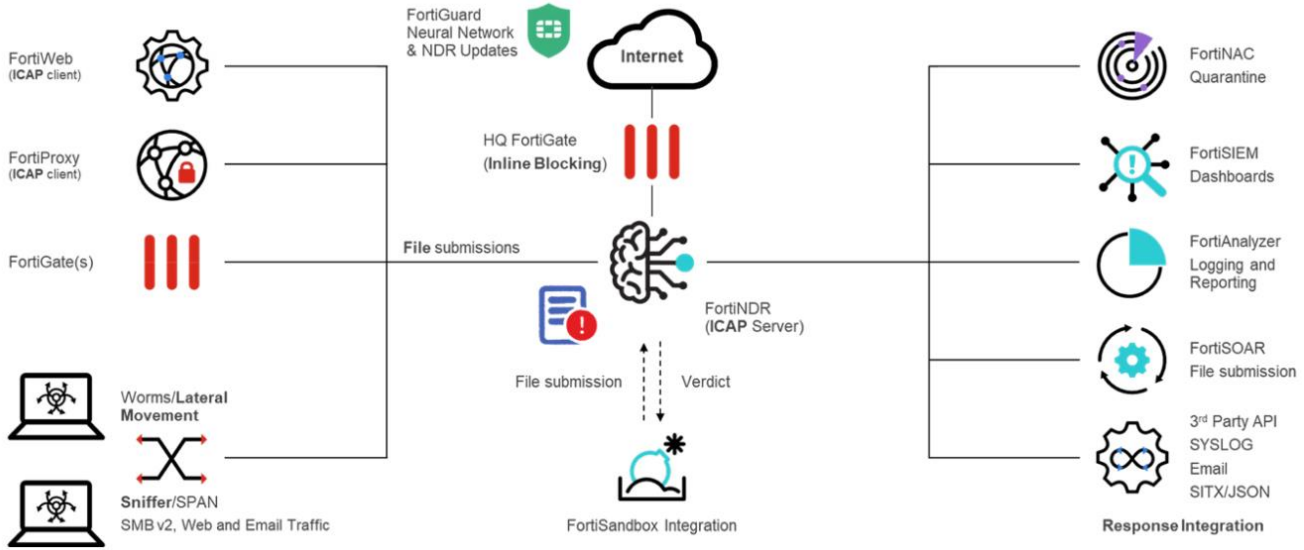
Reveal(x) 360 – це рішення для виявлення та відповіді на мережу (NDR) на основі SaaS який забезпечує уніфіковану безпеку в локальному та хмарному середовищах, широку видимість і ситуаційний інтелект без перешкод, а також миттєву цінність із низьким навантаженням на керування.

Основні можливості рішення Vectra NDR є поєднання з Suricata, що надає командам з протидії загрозам інформацію, необхідну для кращого виявлення загроз та точного відокремлення загроз від шуму.
Забезпечується краще виявлення та реагування на загрози. Отримання повної інформації про відомі та невідомі загрози у корпоративній мережі, поєднуючи контекст сигнатур Vectra Match і можливості Vectra NDR з аналітикою сигналів атак на основі штучного інтелекту Security AI.



Призначення та основні функції рішення FortiNDR

FortiNDR – це мережева технологія захисту від порушень на основі штучного інтелекту (ШІ), призначена для нечисленних команд Центрів управління безпекою (SOC) для виявлення, класифікації та реагування на загрози, в тому числі на ті, що добре замасковані. Контрольоване і неконтрольоване машинне навчання (ML) безперервно аналізує метадані, особливо дані зі сходу на захід в центрах обробки даних, для виявлення загроз, особливо тих, які можуть бути вже наявні в мережі. FortiNDR значно скорочує час на виявлення мережевих аномалій і шкідливого контенту у корпоративній мережі та їх усунення за допомогою Fortinet Security Fabric і інтеграції зі сторонніми розробниками.

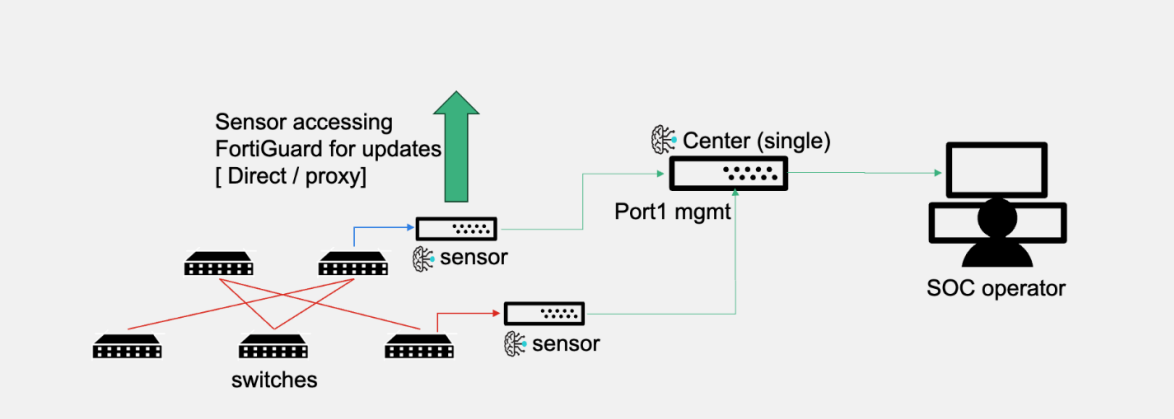


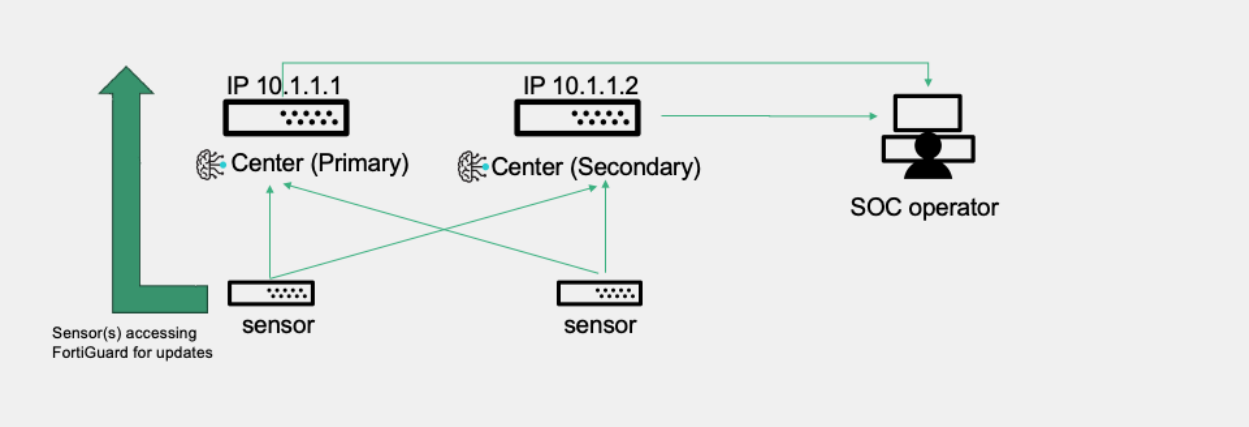
Застосовуючи низку загальних, а також специфічних AI та інших аналітичних інструментів, FortiNDR пропонує унікальне виявлення та спостереження на основі фреймворку MITRE ATT&CK. Це дозволяє розбити тактику, техніку і процедури (TTPs) зловмисника на прості для розуміння команди SOC, щоб вони могли діяти відповідно до них.

Призначення та основні функції компонентів FortiNDR

FortiNDR підтримує три режими роботи:

- *автономний*: підтримує всі функції та функції FortiNDR. FNR-1000F, VM16/32, FNR-3500F можуть працювати в автономному режимі;
- *централізований*: підтримує централізоване керування конфігураціями та даними, зібраними датчиками. Більшість, але не всі функції та функції доступні. Наразі FortiNDR 7.4 підтримує центральний режим лише в FNR-3500F;
- *режим сенсора*: підтримує налаштування датчика під час першого входу.

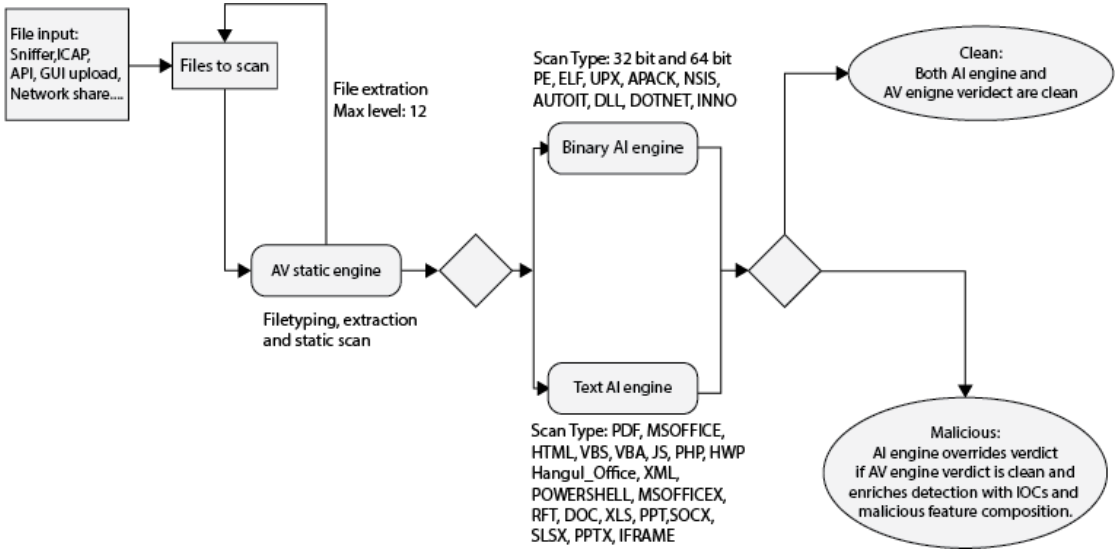




Порядок сканування файлів і шкідливого програмного забезпечення в рішенні FortiNDR

Розглянемо процеси сканування файлів і шкідливого програмного забезпечення, які відбуваються за допомогою AV та ANN рішення FortiEDR.

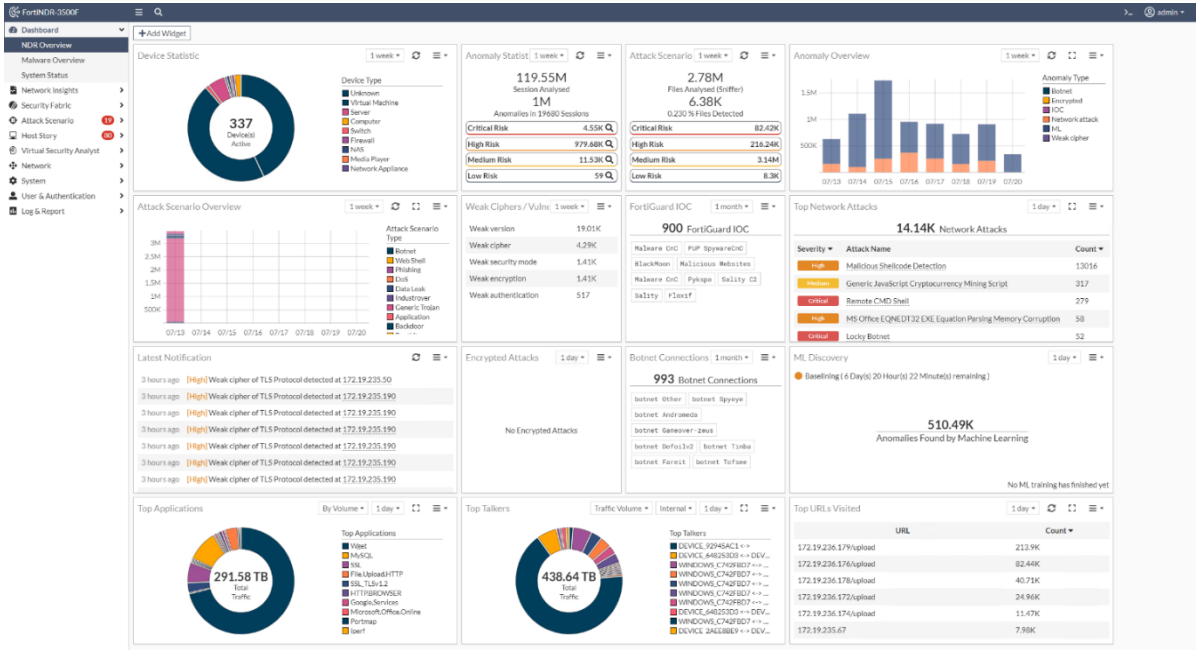
На першому етапі всі файли, які потрібно сканувати, проходять один і той самий потік. Спочатку файли скануються антивірусним статичним модулем. Механізм AV ідентифікує типи файлів і одночасно призначає вердикт. Якщо файли є архівними, наприклад ZIP або TAR, вони розпаковуються на цьому етапі (до 12 шарів). Потім витягнуті файли надсилаються назад для сканування статичним механізмом антивірусу (рисунок).



На другому етапі у разі, якщо тип файлу підтримується ANN (перераховані вище), файли надсилаються або в бінарний, або в текстовий ШІ-движок для сканування на Етапі 2. Файли пройдуть перевірку на Етапі 2 незалежно від результату на Етапі 1. ШІ скасовує вердикт лише в тому випадку, якщо на Етапі 1 файл визнано чистим, а на Етапі 2 – шкідливим. Перевірка ШІ на Етапі 2 збагачує інформацію про IoC і склад шкідливих елементів у детальному поданні зразка.

Порядок застосування технології виявлення та реагування на аномальну мережеву активність на базі FortiNDR

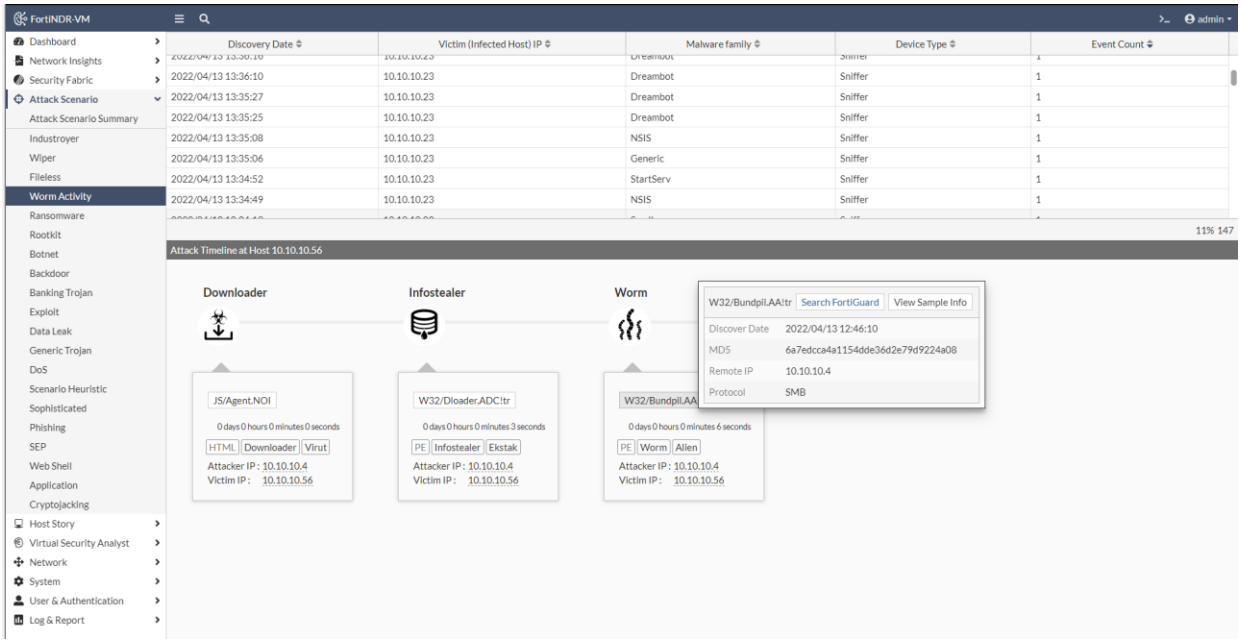
Рішення FortiNDR дозволяють командам безпеки переходити від виявлення до розслідування та пошуку загроз кількома натисканнями миші. Забезпечуючи інтеграцію з Fortinet Security Fabric і численними інструментами сторонніх розробників, такими як EDR, SOAR, SIEM і XDR, рішення FortiNDR забезпечують автоматизацію дослідження, сортування та виправлення.



Інформаційна панель відображає загальні аномалії, виявлені FortiNDR, а також стан системи. Інформаційна панель містить три перегляди: огляд NDR, огляд шкідливого програмного забезпечення та стан системи. Користувачі можуть додавати власні інформаційні панелі та відповідні віджети, адаптовані для їхніх операцій. Існують такі віджети FortiNDR, як Botnet, Attack Scenarios і Sessions Analyzed, щоб задовольнити різні потреби (рисунок). Завдяки можливостям виявлення на основі штучного інтелекту та експертного аналізу групи безпеки можуть завчасно виявляти атаки та реагувати на них.

Порядок застосування технології виявлення та реагування на аномальну мережеву активність на базі FortiNDR

Під час атаки інфекції часто поширюються швидко, і аналітикам SOC може бути дуже важко відстежити джерело (нульовий пацієнт). Застосовується компонент FortiNDR Virtual Analyst. Це механізм AI на основі сценаріїв, який може швидко визначити джерело атаки. Це економить час під час розслідування порушень, зазвичай скорочуючи його з днів до секунд. FortiNDR допомагає аналітикам своєчасно впоратися з джерелом проблеми.



Сценарій атаки (рисунок) відображає IP-адреси жертви з часом виявлення. Натисніть IP-адресу, щоб відобразити часову шкалу подій, а також графічну інтерпретацію атаки.

На рисунку наведено приклад зараження хробаками. FortiNDR Virtual Analyst показує віддалену IP-адресу, з якої виникла атака, часову шкалу та інші шкідливі файли, виявлені на зараженому хості, а активність хробака показує, що він намагається поширитися.

Рекомендації щодо застосування технології виявлення та реагування на аномальну мережеву активність

Network Detection and Response (NDR) є комплексним рішенням кібербезпеки, призначеним для моніторингу та аналізу мережевого трафіку для виявлення потенційних загроз і реагування на них. Він надає організаціям покращену видимість їхньої мережевої інфраструктури, дозволяючи їм ефективно виявляти та пом'якшувати інциденти безпеки. NDR використовує передові методи, такі як машинне навчання, аналіз поведінки та виявлення аномалій, щоб виявити зловмисну діяльність, зокрема спроби несанкціонованого доступу, викрадання даних, зараження зловмисним програмним забезпеченням та інші мережеві атаки.

Під час розгортання рішень NDR організаціям слід розглянути кілька найкращих практик, щоб максимізувати ефективність їхнього впровадження.

Щоб підвищити виявлення та реагування на аномальну мережеву активність за допомогою рішень NDR, потрібно дотримуватися кількох найкращих практик. Ось кілька важливих рекомендацій для ефективного впровадження NDR рішень:

- ✓ Рекомендація 1. Необхідно визначити чіткі цілі.
- ✓ Рекомендація 2. Необхідно оцінити ступінь видимості мережі.
- ✓ Рекомендація 3: Необхідно налаштувати спеціальні правила виявлення.
- ✓ Рекомендація 4: Необхідно запровадити базовий моніторинг.
- ✓ Рекомендація 5: Необхідно здійснити інтеграцію з існуючою інфраструктурою безпеки.
- ✓ Рекомендація 6: Необхідно здійснювати безперервний моніторинг.
- ✓ Рекомендація 7: Необхідно здійснити автоматизацію та оркестровку.
- ✓ Рекомендація 8: Постійно проводьте навчання персоналу та розвиток навичок.
- ✓ Рекомендація 9: Постійно проводьте регулярну оцінку та оптимізацію.
- ✓ Рекомендація 10: Необхідно підтримувати ПЗ в актуальному стані.

ВИСНОВКИ

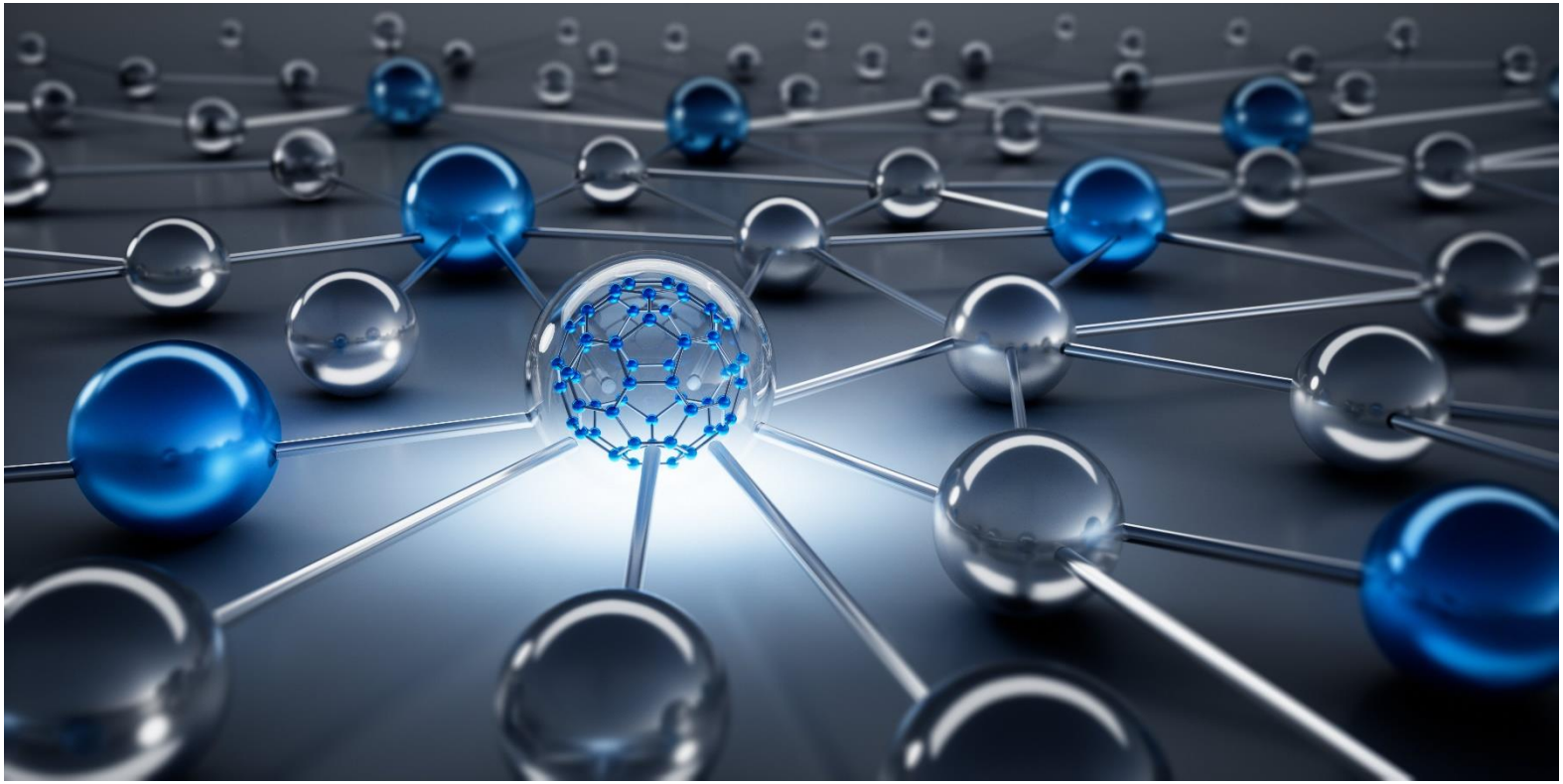
В роботі проведено дослідження проблеми виявлення та реагування на аномальну мережеву активність. Сьогодні інформаційні ресурси організацій зазнають постійних кібератак на корпоративні мережі та через них. Реалізація технології виявлення та реагування на аномальну мережеву активність є важливою складовою частиною загального процесу забезпечення кібербезпеки інформаційних ресурсів організації. Завдяки реалізації даної технології організації можуть ефективно виявляти кібератаки та інші загрози безпеці корпоративним мережам та реагувати на них.

- Проведено аналіз підходів до виявлення та реагування на аномальну мережеву активність. Мережеві системи виявлення та реагування відстежують мережевий трафік для певних сегментів мережі або пристроїв і аналізують мережеві, транспортні та прикладні протоколи для виявлення підозрілої активності. Компоненти мережевих систем виявлення та реагування схожі на інші типи технологій IDPS, за винятком датчиків. Мережевий датчик IDPS відстежує та аналізує мережеву активність в одному або декількох сегментах мережі. Датчики доступні у двох форматах: датчики на основі пристроїв, які складаються зі спеціалізованого апаратного та програмного забезпечення, оптимізованого для використання датчиків IDPS, та датчики лише на основі програмного забезпечення, які можуть бути встановлені на хости, що відповідають певним специфікаціям.
- Проведено аналіз існуючих рішень із виявлення та реагування на аномальну мережеву активність. Сучасні рішення NDR використовують передову аналітику, машинне навчання і поведінковий аналіз для виявлення аномалій і невідомих загроз. Це має вирішальне значення, оскільки традиційні заходи безпеки можуть не впоратися з виявленням нових або постійно еволюціонуючих загроз.

ВИСНОВКИ

- Проведено аналіз методів та засобів виявлення та реагування на аномальну мережеву активність на базі FortiNDR. FortiNDR – це мережева технологія захисту від порушень на основі штучного інтелекту, призначена для нечисленних команд Центрів управління безпекою для виявлення, класифікації та реагування на загрози, в тому числі на ті, що добре замасковані. Контрольоване і неконтрольоване машинне навчання безперервно аналізує метадані, особливо дані зі сходу на захід в центрах обробки даних, для виявлення загроз, особливо тих, які можуть бути вже наявні в мережі. FortiNDR значно скорочує час на виявлення мережевих аномалій і шкідливого контенту у корпоративній мережі та їх усунення за допомогою Fortinet Security Fabric і інтеграції зі сторонніми розробниками.
- На основі досліджень проведених в роботі запропоновано порядок застосування технології виявлення та реагування на аномальну мережеву активність на прикладі рішення FortiNDR. Рішення FortiNDR як частина платформи Fortinet SecOps надає команді безпеки можливість виявляти, визначати пріоритети, досліджувати, шукати та реагувати на атаки у корпоративній мережі. Завдяки можливостям виявлення на основі штучного інтелекту та експертного аналізу групи безпеки можуть завчасно виявляти атаки та реагувати на них.
- Розроблено рекомендації фахівцям з кібербезпеки щодо застосування технології виявлення та реагування на аномальну мережеву активність. Дотримуючись цих рекомендацій, організації можуть покращити рівень безпеки та можливості виявлення загроз і реагування на них, а також ефективно використовувати свої інвестиції в NDR для захисту своїх критично важливих активів і конфіденційних даних.

Отже, технологія NDR – це важливе рішення для кібербезпеки, яке забезпечує розширене виявлення загроз, можливості реагування на інциденти, підтримку відповідності нормативним вимогам і повну видимість мережі. Її впровадження може значно підвищити рівень безпеки організації та забезпечити проактивний захист від складних кіберзагроз, гарантуючи захист критично важливих активів і конфіденційних даних.



Дякую за увагу!
Доповідь закінчено