GREYCORTEX MENDEL

All-Seeing Network Security

GREYCORTEX MENDEL – використовує передові технології штучного інтелекту, машинне навчання, аналіз великих об'ємів даних, а також сигнатурний аналіз та аналіз на основі правил для пошуку загроз, виявлення уразливостей та надання повної інформації про стан мережі спеціалістам з інформаційної безпеки.

Складні атаки є досить поширеними та важко виявляються

8 атак
проникає в мережу компанії за рік

40%
кіберзагроз залишаються невиявленими

49 днів
потрібно для виявлення загрози за допомогою стандартних засобів безпеки

Існуючі інструменти безпеки є уразливими до:

Невідомих загроз

Вчасно не виявлені невідомі загрози, такі як шкідливе програмне забезпечення, троянські програми та шифрувальники, призводять до:

- Втрати конфіденційних даних
- Атак на організації
- Завдання шкоди бізнесу
- Втрати репутації

Недостатньої видимості

Недостатня видимість мережі ускладнює виявлення підозрілих пристроїв та дій зловмисників, а також призводить до:

- Критичних затримок
- Появи прихованих пристроїв
- Втрати часу
- Втрати коштів

Недбалості співробітників

Співробітники та посередники навмисно чи випадково порушують політики безпеки. У свою чергу, це призводить до:

- Витоку конфіденційних даних
- Атак на організацію
- Проблем із дотриманням нормативних актів
- Порушення відповідності GDPR

Ризики для бізнесу РЕАЛЬНІ

Аналіз мережевого трафіку запобігає порушенням

Аналіз мережевого трафіку (NTA) поєднує в собі **штучний інтелект, комп'ютерне навчання** та інші інструменти для виявлення підозрілих або аномальних мережевих подій. **GREYCORTEX MENDEL використовує NTA** для моніторингу периметру мережі, а також трафіку всередині мережі для повного охоплення.

GREYCORTEX MENDEL виявляє загрози у всій мережі, включаючи пристрої BYOD / IoT, і навіть складні невідомі атаки, **які залишаються невидимими для інших рішень.**

65%
втрачають довіру клієнтів

Потужне виявлення з винятковою швидкістю

Розширені невідомі загрози, включаючи шкідливе програмне забезпечення, троянські програми, шифрувальники, RAT та «0-денні» загрози виявляються протягом 1 хв. - 6 годин замість 49 днів.

23%
втрачають бізнес-можливості

Повний огляд мережі

- Навіть у мережах SCADA
- Кожен хост
- Кожен пристрій
- Кожна підмережа
- Кожен сервіс
- Кожен додаток
- Кожен BOYD/ IoT

5%
зіштовхуються з падінням вартості акцій

Джерело: Ponemon Institute
Дослідження: 2011 - 2017

Ефективне реагування

- Блокування з'єднання у брандмауері безпосередньо з MENDEL
- Розбір інцидентів командою аналітиків
- Легке управління інцидентами
- Проведення аналізу та розслідування причин

MENDEL включає

Машинне навчання покращує виявлення

Передовий штучний інтелект і машинне навчання, що використовуються в MENDEL, виявляють загрози більш ефективно, порівняно з іншими рішеннями.

- Розрізняє комунікацію людини та бота
- Виявляє аномальну поведінку
- Знаходить приховані загрози

Перешкоджання атакам під час їх перебігу

MENDEL забезпечує зворотній зв'язок з інфраструктурою, щоб перешкоджати атакам у разі виявлення.

- Інтегрується з існуючим брандмауером
- Простий інтерфейс дозволяє виконати загальне чи конкретне блокування
- Коли оперативність надважлива, конфігурація та блокування відбуваються за секунди

Повна видимість мережі, включаючи BYOD/IoT

MENDEL розрізняє вхідний та вихідний трафік, а також комунікації між пристроями всередині мережі.

- Відмінно працює з BYOD / IOT
- Візуалізує окремі пристрої та додатки, а не лише комунікації на окремому рівні.
- Швидко фільтрує кожне з'єднання

Врахування контексту для швидшого вирішення

Ефективне виявлення атак - це лише частина пазлу мережевої безпеки. MENDEL надає додаткові контекстні дані для швидшого вирішення подій.

- Інтегровані GEOIP та «чорні» списки
- Розшифровує трафік SSL / TLS за допомогою імпортованого приватного ключа
- Інтеграція MENDEL із Active Directory для ідентифікації користувачів у мережі

Кореляція точності виявлення загроз

Атаки можуть відбуватися покроково, а деякі їх етапи можуть бути безпечними. MENDEL збирає всі події разом, щоб показати справжню природу атаки.

- Загрози не можуть приховатися у великих об'ємах даних
- Ідентифікує події в багатьох офісах з одного місця
- Вирішення проблеми займає до двох хвилин

Ефективний як самостійне рішення або як додаткове джерело даних

Різні інфраструктури безпеки потребують різних конфігурацій. MENDEL доповнює ваші існуючі інструменти для заповнення прогалин у безпеці.

- Результати рівня SIEM вдвічі дешевше та в десятеро швидше для малих та середніх підприємств
- Експорт даних в системи SIEM для великих команд IT-безпеки
- Управління інцидентами дозволяє застосовувати більш гнучке вирішення

MENDEL захищає

Малий та середній бізнес, а також великі корпорації

Державні установи

SCADA/ICS

Об’єкти інфраструктури

Варіанти розгортання

Локально (на віртуальному або фізичному сервері)

Як сервіс (SaaS)

В оперативному центрі безпеки (SOC)

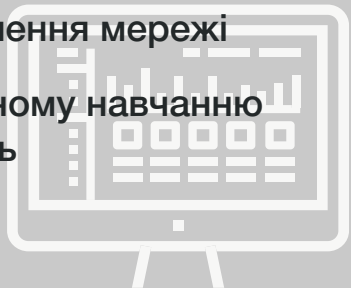
Аудит мережі

Впровадження MENDEL

30 хвилин на інсталяцію

Автоматичне вивчення мережі

Сприяння машинному навчанню
~ 5 хвилин на день



Спробуйте MENDEL

Безкоштовна тестова ліцензія на 30 днів.
Допоможе виявити проблеми у мережі – від атак до проблем продуктивності.

Проблеми існують навіть у «чистих» мережах:

20% мережевих пристроїв становлять загрозу для решти мережі через віруси / шкідливі програми / трояни / RAT

«0-денні» атаки

Шкідливі програми для мобільних пристроїв

Уразливості IoT пристроїв

Неефективна матриця мережі

Програми без застосованих виправлень

Аномалії / проблеми продуктивності

Несанкціонований доступ до даних

Підготовка до ексфільтрації даних

Проблеми відповідності регулятивним нормам (наприклад, GDPR)

GREYCORTEX

З питань партнерства та придбання в Україні, будь ласка, звертайтесь за телефоном +38044 545 77 26 або електронною адресою sales@eset.ua