Network Detection and Response

XDR без NDR – це просто EDR

Усуньте загрози, перш ніж вони завдадуть удару

Виявляйте те, що неможливо виявити, та зупиняйте приховані атаки. Trellix Network Detection and Response (NDR) допомагає вашій команді зосередитися на актуальних загрозах, швидко і розумно відбивати вторгнення, а також посилити слабкі місця вашої кібербезпеки.

Автоматично адаптуйтеся до нових загроз

Виявляйте поширені загрози в мережі та центрах обробки даних з можливістю автоматичної адаптації, щоб ви могли розпізнати загрози, що постійно розвиваються, і своєчасно реагувати на них.

Захист від мережі до хмари

Захистіть свою хмару, IoT, інструменти для спільної роботи, кінцеві точки та інфраструктуру. Автоматизуйте свої дії, щоб адаптуватися до середовища безпеки.

Підлаштовуйте рішення під потреби вашої організації

Інтегруйтеся з будь-яким постачальником та підвищуйте операційну ефективність, відображаючи лише важливі для вас оповіщення.

ПРОДУКТИ TRELLIX ДЛЯ МЕРЕЖЕВОЇ БЕЗПЕКИ

Trellix Network Security

- Автоматично виявляйте підозрілу поведінку в мережі та запобігайте атакам, які вислизають від традиційних сигнатурних систем безпеки.
- Виявляйте та блокуйте складні загрози та переміщення по периметру організації в режимі реального часу.
- Прискорюйте усунення виявлених загроз за допомогою вичерпних доказів та оперативних даних.

Trellix Network Forensics

- Виявляйте та усувайте широкий спектр загроз швидше.
- Визначайте масштаб та вплив загроз, а також відновлюйте захищений стан вашої мережі.
- Візуалізуйте події до, під час та після атаки, щоб унеможливити повторне зараження мережі.

Trellix Intrusion Prevention System

- Перевіряйте весь мережевий трафік на наявність нових та невідомих загроз.
- Оптимізуйте операції з безпеки з кореляцією подій з усіх джерел у режимі реального часу.
- Відстежуйте свою мережу на предмет шкідливої активності та блокуйте вторгнення у момент їх виявлення.

Виявляйте можливі атаки та запобігайте загрозам, непомітним для інших продуктів

МОЖЛИВІСТЬ	ФУНКЦІОНАЛ
Виявлення загроз без сигнатур	Виявляє багатопотокові, багатоетапні, поліморфні, Zero-Day-атаки, а також програми-вимагачі та інші просунуті загрози
Виявлення в режимі реального часу та заднім числом	Відстежує відомі та невідомі загрози в режимі реального часу та в минулому
Багатовекторна кореляція	Автоматизує перевірку та блокує атаки на електронну пошту, кінцеві точки та інші вектори безпеки
Виявлення руху по периметру організації	Виявляє раніше невідомий підозрілий мережевий трафік усередині мережі
Запобігання DoS та DDoS	Запобігає потраплянню шкідливого трафіку у вашу мережу, не заважаючи проходженню легального трафіку
Розшифровка вхідного/вихідного SSL	Виявляє шкідливі програми та інші сучасні загрози у вхідному та вихідному зашифрованому трафіку
Сумісність з багатьма ОС, форматами файлів та додатками	Підтримує гетерогенні середовища кінцевих точок для широкого спектра додатків
Надійний гіпервізор	Приховує сліди віртуалізації, щоб обійти техніки ухилення від аналізу

Проактивно реагуйте та швидко локалізуйте інциденти

МОЖЛИВІСТЬ	ФУНКЦІОНАЛ
Блокування в режимі реального часу	Миттєво зупиняє атаки
Удосконалена система запобігання вторгненням	Виконує глибоку перевірку мережевого трафіку (DPI) для виявлення та захисту від ботнетів та інших складних загроз
Інтегровані робочі процеси безпеки	Швидкий перехід від виявлення до розслідування та реагування
Відмовостійкість	Забезпечує надійний безперебійний захист мережі
Сигнатурне виявлення вторгнень без хибних спрацьовувань	Автоматизує та прискорює обробку сповіщень для усунення надлишкової ручної роботи
Виявлення та класифікація потенційно небезпечного ПЗ	Класифікує шкідливі програми на критичні та некритичні для визначення пріоритетів ресурсів реагування
Ефективний контекстний інтелект	Прискорює усунення просунутих загроз, надаючи докладну інформацію про атаку та зловмисника

Визначайте масштаб наслідків інциденту і покращуйте якість реагування

МОЖЛИВІСТЬ	ФУНКЦІОНАЛ
Широкий контекст	Перевіряє мережеві пакети, з'єднання та сеанси до, під час та після атаки
Ретроспективний пошук загроз	Інтегрує аналітику загроз для історичного аналізу IOC та сповіщення про виявлені IOC, наявні у вашій мережі днями або тижнями раніше
Зменшення збитків від атак	Прискорює процес розслідування завдяки єдиному робочому простору з миттєвим переходом зі сповіщень до даних про сеанси одним клацанням миші