XEdge для кібербезпеки

Безперервна валідація політик від реального шляху приватної мережі UE — від RF та забезпечення додатків до кіберперевірки.

Що таке XEdge?

XEdge — це платформа на основі сенсорів для забезпечення безперервного підключення в приватних і мобільних мережах. Виділені датчики XEdge спостерігають за мережею з точки зору користувацького обладнання та надсилають заплановані вимірювання до контролера XEdge для видимості, сповіщень, історії та інтеграції. XEdge забезпечує постійний рівень вимірювання в точках, де пристрої фактично підключаються та використовують сервіси. Він доповнює спеціалізовані RF, протокольні та безпекові інструменти, показуючи, чи надає мережа очікуваний сервіс з боку пристрою.

Моніторинг радіочастот	Моніторинг додатків	Кібермоніторинг
Вимірювання сили сигналу та якості, стану реєстрації, контекст часу та місця розташування.	Повторювані активні тести, такі як ping, HTTP і пропускна здатність, з результатами, збереженими в XEdge Controller.	Валідація доступності вибраного сервісу, ідентифікації, політики сегментації та дрейфу конфігурації на стороні UE.

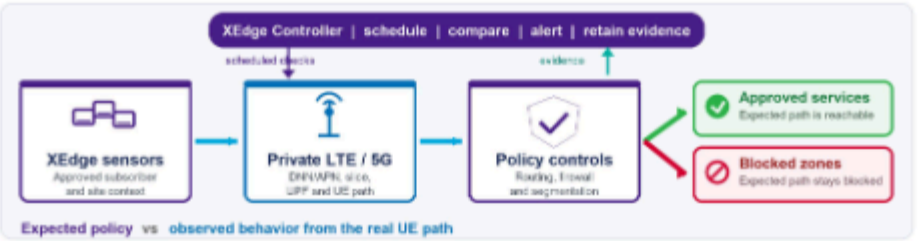
Чому кібермоніторинг має значення

Приватні мережі передають трафік між датчиками, операційними пристроями, корпоративними додатками та IT- або OT-сервісами. Цей трафік формується ідентичністю абонента, DNN/APN, зрізами, розміщенням UPF, локальним розривом, маршрутизацією, правилами міжмережевого екрану та політикою застосування. Мережу можна правильно спроєктувати на момент запуску, але вона все одно дрейфує після зміни конфігурації або додатку. XEdge Cyber повторює перевірки, затверджені клієнтом, через той самий шлях UE, що використовується для операційних пристроїв. Він порівнює очікувану політику з спостереженою поведінкою та фіксує докази, які команди безпеки та операцій можуть переглядати після змін, інцидентів та оновлень політик.

Побудуй правильно. Потім безперервно моніторити.

Контекст безперервного моніторингу: Рамкова рамка управління ризиками NIST, крок моніторингу

Положення вимірювання XEdge



XEdge порівнює очікувану політику з спостережуваною поведінкою на тому ж шляху UE, що використовується для операційних пристроїв.

Як XEdge Cyber перевіряє політику

Контрольований цикл валідації від визначення політики до доказів

Кожен профіль валідації визначає затверджений контекст джерела, цілі, сервіси, очікувані результати та операційні обмеження перед будь-яким тестуванням. XEdge виконує заплановані, низькочастотні перевірки та записує як результат, так і контекст тесту.

Обсяг валідації

Можливості	Цінність для клієнта
Матриця політик	Визначає затверджений профіль джерела, DNN/APN або зріз, сайт, ціль, протокол, порт і очікуваний результат дозволу або відхилення перед початком тестування.
Названа перевірка порту TCP	Виконує низькошвидкісні перевірки зв'язку щодо іменованих, авторизованих цілей і портів для виявлення несподіваного впливу або блокування.
Перевірка DNS та HTTPS	Перевіряє роздільну здатність, ідентифікацію сертифіката, час підключення та відповідь затвердженої служби, а не лише перевіряє, чи відкритий порт.
Виявлення змін і дрейфу	Повторює затверджені перевірки після змін у мережі, міжмережевому екрані, ядрах або додатку та підкреслює підтверджені відхилення від прийнятої базової лінії.
Звіт про докази	Фіксує датчик і профіль, часову позначку, ціль, очікуваний і спостережуваний результат, використаний інтерфейс, час, причину помилки та виключення тестів.

Як інтерпретуються результати

Політика матчів	Дрейф політики	Невідомо	Помилка тесту
Спостережувана поведінка відповідає затвердженому правилу.	Підтверджена поведінка суперечить затвердженому правилу.	Кінцеву точку чи керування не можна з упевненістю ізолювати окремо.	Перевірка пройшла неправильно і потребує перегляду.

Бізнес-цінність

Видимість кібербезпеки
Перевіряйте вибрані маршрути та сервіси з боку пристрою та поверхневого дрейфу політики за допомогою доказів.

Операційна ефективність
Замініть повторні ручні перевірки на заплановану валідацію до та після контрольованих змін.

Забезпечення політики
Пов'язати результати з точним контекстом абонента, сайтом і шляхом, включеним у затверджену політику тестування.

Обсяг і обмеження

Покриття	Результати застосовуються лише до профілів абонентів, цілей, сервісів, сайтів і шляхів, включених до затвердженої політики валідації.
Застосування	XEdge перевіряє поведінку за шляхом UE. Міжмережеві екрани, системи контролю доступу, маршрутизація та мобільне ядро залишаються відповідальними за виконання політики.
Інструменти безпеки	XEdge доповнює управління вразливостями, тестування на проникнення, SIEM та спеціалізовані інструменти безпеки. Вона їх не замінює.
Негативні результати	Невдалий з'єднання не автоматично підтверджує блокування міжмережевого екрану. Коли контроль не можна ізолювати, результат повідомляється як невідомий.
Управління тестами	Для кожного профілю валідації потрібні авторизація клієнта, іменовані цілі, списки дозволів, обмеження тарифів і затверджені процедури контролю змін.

XEdge надає незалежні докази того, що вибрана політика працює з шляху пристрою. Він не стверджує, захист мережевих зон або сервісів, які не були протестовані.