

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Оценка на уязвимостите

Широко, повторяемо покритие на цялата ви среда, съчетано с експертна проверка, която отстранява погрешно отчетените уязвимости. Ефикасната отправна точка преди по-задълбочено тестване.

ПОДХОДЯЩО ЗА	Големи среди, повтарящи се базови оценки, подготовка преди тест за проникване
ПОЛУЧАВАТЕ	Проверен регистър на уязвимостите, подреден по риск
ОБХВАЩА	Широко, проверено покритие

Покритие, на което можете да се доверите

Непровереният резултат от скенер е непосилен за обработка и пълен с шум. Ние извършваме сканиране с удостоверяване върху цялата атакувана повърхност, след което експерт проверява резултатите и премахва дубликатите, така че до екипа ви стига само това, което е реално, подредено по риск и приложимо.

Подходяща е като повтаряща се базова оценка, преди тест за проникване или за да държите голяма среда под постоянно наблюдение.

Какво обхваща

- Външна атакувана повърхност
- Вътрешна мрежа и хостове
- Уеб приложения, за широчина на покритието
- Конфигурация и състояние на облачната среда
- Пропуски в обновяването и конфигурацията
- Проверени резултати без дубликати

Как протича

- Откриване на активи — Установяваме какво в действителност имате изложено и къде.
- Сканиране с удостоверяване — Задълбочено сканиране с идентификационни данни за точно покритие.
- Експертна проверка — Човек премахва погрешно отчетените уязвимости и потвърждава реалния риск.
- Приоритизиран доклад — Подреден регистър с възможност за проследяване на това, което да поправите първо.

Какво получавате

- Регистър, подреден по риск — Всеки проблем, приоритизиран според реален, потвърден риск.
- Премахнат шум — Погрешно отчетените уязвимости са филтрирани, а дублиращите се констатации — обединени.
- Насоки за отстраняване — Ясни, практични стъпки за затварянето на всеки пропуск.
- Повторни сканирания — Проследявайте напредъка във времето с планирани повторни оценки.

Методологии и стандарти, на които се опираме

NIST SP 800-115 · CIS Benchmarks · CVSS · CWE · OWASP Top 10 · Сканиране в стила на PCI DSS ASV

Старши тестери. Доказателства за всяка констатация. Включен повторен тест. Минимум пет дни тестване. Обхват и примерни доклади — pxlsec.com/bg/services/vulnerability-assessment.