

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Red Teaming

Целева симулация по множество вектори, която преследва конкретни задачи през хора, процеси и технологии и измерва доколко добре откривате и реагирате, а не само къде са дефектите.

ПОДХОДЯЩО ЗА	Зрели екипи по сигурността, валидиране на SOC и MDR, подготовка за DORA TLPT
ПОЛУЧАВАТЕ	Разказ за атаката, анализ на пропуските в откриването, съответствие с АТТ&СК;
ОБХВАЩА	Целева симулация на противник

Цели, а не контролни списъци

Тестът за проникване картографира покритието. Операцията на red team преследва конкретна цел — Domain Admin, най-ценните данни, измамна транзакция — по всеки реалистичен път и толкова тихо, колкото би го направил истински нападател.

Резултатът е трезва оценка на видимостта и реакцията на вашия blue team и точно къде да инвестирате, за да затворите пропуските, които имат значение.

Какво включва

- Външен първоначален достъп, включително фишинг
- Сценарии с предполагаем пробив
- Странично движение и ескалация на привилегии
- Целеви достъп до данни и експулзация
- Измерване на откриването и реакцията
- Сътрудничество с purple team, по избор

Как протича

- Цели и модел на заплахите — Договаряме задачите и профила на противника, който ще емулираме.
- Проучване и първоначален достъп — Реалистични входни точки: външни, социални или предполагаем пробив.
- Действия по целите — Незабелязано придвижване към целта, като проследяваме какво е засечено.
- Обсъждане на резултатите и purple team — Повтаряме атаката заедно със защитниците ви, за да подсилим откриването.

Какво получавате

- Разказ за атаката — Пълна хронология на операцията, стъпка по стъпка.
- Пропуски в откриването — Къде ни видяхте, къде не ни видяхте и защо.
- Съответствие с АТТ&СК; — Техниките, съотнесени към MITRE АТТ&СК; за приоритизиране.
- План за укрепване на защитата — Конкретни подобрения в откриването и реакцията.

Методологии и стандарти, на които се опираме

MITRE АТТ&СК; · TIBER-EU · DORA TLPT · Тестване, водено от заплахи, в стил CBEST · PTES · OSSTMM · NIST SP 800-115

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