

## ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

## Тестване за проникване, водено от заплахи

Контролирана операция на red team срещу вашата продукционна среда, водена от разузнавателна информация за заплахите и структурирана според изискванията на DORA за тестване, водено от заплахи, и рамката TIBER-EU — тества хора, процеси и технологии срещу противниците, които действително ви атакуват. Дали даден ангажимент се квалифицира като TLPT и какви изисквания към тестерите се прилагат, се решава от вашия компетентен орган по TLPT; потвърждаваме това с вас при определянето на обхвата.

|              |                                                                                   |
|--------------|-----------------------------------------------------------------------------------|
| ПОДХОДЯЩО ЗА | Банки, платежни дружества и финансови субекти по DORA; зрели екипи по сигурността |
| ПОЛУЧАВАТЕ   | Доклад в стил TIBER, хронология на откриването, констатации, подходящи за борда   |
| ОБХВАЩА      | Red team по DORA / TIBER-EU                                                       |

### Първо разузнаване, после атака

Тестването, водено от заплахи, започва с разузнавателна информация за това кой би ви атакувал и как, след което емулира точно тези противници срещу продукционната ви среда — като измерва предотвратяването, откриването и реакцията така, както регулаторът иска да ги види.

Структурираме ангажиментите около фазите на TIBER-EU и изискванията на DORA за TLPT, с вниманието, което тестването в продукцията изисква. Формалната акредитация по TIBER се различава в отделните юрисдикции — ще потвърдим изискванията на вашия регулатор заедно с вас.

### Какво включва

- Целенасочена разузнавателна информация за заплахите
- Емуляция на сценарии и на конкретни противници
- Контролирано тестване в продукционна среда
- Измерване на предотвратяването, откриването и реакцията
- Повторение и обсъждане на резултатите с purple team
- Докладване, съобразено с регулатора

### Как протича

- Подготовка — Договарят се обхватът, мерките за контрол на риска и white team.
- Разузнавателна информация — Изграждаме реалистични, целенасочени сценарии за атака.
- Red team — Емулираме противника срещу продукционната среда, безопасно.
- Приключване — Повторение, обсъждане на резултатите и доклад, готов за регулатора.

### Какво получавате

- Резюме за ръководството — Бизнес рискът, представен ясно за ръководството и управителния съвет.
- Технически доклад — Всяка констатация със степен на критичност, доказателства и възпроизвеждане.
- Приоритизирани корекции — Конкретни стъпки за отстраняване, подредени по реален риск и готови за изпълнение от разработчиците.
- Писмо за повторен тест — Проверяваме вашите корекции и потвърждаваме писмено закриването им.

### Методологии и стандарти, на които се опираме

Рамката TIBER-EU · DORA (тестване за проникване, водено от заплахи) · CBEST · MITRE ATT&CK; · NIST SP 800-115 · Рамки в стил iCAST / CORIE

Старши тестери. Доказателства за всяка констатация. Включен повторен тест. Минимум пет дни тестване. Обхват и примерни доклади — [pxlsec.com/bg/services/threat-led-penetration-testing](https://pxlsec.com/bg/services/threat-led-penetration-testing).