

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Тестване за проникване в облачна среда

Ръчно тестване на вашите облачни акаунти и работни натоварвания: неправилни конфигурации, идентичности с прекомерни права, изложени данни и пътищата за ескалация, които превръщат една грешка в компрометация на целия акаунт.

ПОДХОДЯЩО ЗА	Среди в AWS, Azure и GCP; прегледи преди одит; проверка на сигурността след миграция
ПОЛУЧАВАТЕ	Приоритизирани констатации за облака с корекции по IAM и конфигурацията
ОБХВАЩА	AWS, Azure и GCP

Отвъд скенера за състояние

Инструментите за оценка на облачното състояние отчитат неправилните конфигурации поотделно. Атакующите ги свързват: от публичен bucket изтича ключ, ключът поема роля, ролята достига до продукция. Ние изминаваме целия път ръчно — през идентичности, съхранение, изчислителни ресурси, мрежи и тайни.

Съчетаваме преглед на конфигурацията с удостоверяване и реална, ограничена по обхват експлоатация срещу акаунтите, които разрешите — безопасно и с доказателства.

Какво тестваме

- Идентичност и достъп (IAM, роли, политики)
- Съхранение и излагане на данни
- Изчислителни и контейнерни работни натоварвания
- Мрежова и периметрова конфигурация
- Управление на тайните и работа с ключове
- Пътища за ескалация на привилегии и странично движение

Как протича

- Обхват и достъп — Роли само за четене и целеви акаунти, договорени предварително.
- Преглед на конфигурацията — Преглед с удостоверяване на идентичности, данни и работни натоварвания.
- Експлоатация — Свързваме неправилните конфигурации в доказано въздействие, безопасно.
- Доклад и повторен тест — Приоритизирани корекции, съотнесени към вашия облак, след което проверени.

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

CIS Benchmarks (AWS, Azure, GCP) · MITRE ATT&CK; for Cloud · CSA Cloud Controls Matrix · NIST SP 800-115 · Принципите за тестване на OWASP · PTES · Насоките за сигурност на доставчиците (well-architected)

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