安全攻防对抗服务

常见问题

产品文档

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

常见问题

最近更新时间：2022-04-28 14:33:46

什么是安全攻防对抗服务?

安全攻防对抗服务（Cybersecurity Attack-Defense Confrontation, CADC）基于腾讯安全专家能力及多年的攻防对抗经验构建。面向对安全能力有较高要求的企业用户，在用户授权后，通过模拟 APT 攻击的方式，对企业信息化资产以及可能产生危害的安全风险进行测试。通过多维度、多视角的安全攻防对抗，动态检测企业安全防护的整体水位。

做了渗透测试，还需要做安全攻防对抗吗?

渗透测试的检测维度较为单一，仅能检测所测试应用自身及承载服务器、组件的安全性。企业安全除应用安全外，可能还存在其他诸多隐患，这些是渗透测试无法覆盖的。而安全攻防对抗能够对这些风险面进行测试，检验企业整体安全防护能力。

安全攻防对抗与渗透测试的区别?

攻防演习与传统渗透测试存在明显的区别，主要区别在以下方面：

- **目的：**传统渗透测试是对业务系统自身开展安全检查与渗透性测试，核心目的是找到业务系统自身存在的可利用漏洞。攻防演习是在渗透测试的基础上，以获取目标系统的最高控制权为目标，目的是检验客户人机结合、协同处置等方面的综合防护能力。
- **人员配比：**渗透测试在实施中主要由渗透工程师完成，配备的人员比较单一。而在攻防演习过程中，一般以演习预期目标为导向，要求与渗透测试相比更为复杂，一般由不同技术背景人员来组成攻击小组。
- **侧重点：**渗透测试检验侧重点主要是渗透目标的安全性，是否存在可利用的安全漏洞。而在攻防演习过程中，检验的侧重点则是参演目标的安全性、参演单位的安全防护能力、参演单位的应急响应能力，更注重对参演单位整个网络安全体系的有效性检验。

安全攻防对抗可以对非腾讯云资产进行检测么?

安全攻防对抗服务可以对公有云、私有云、混合云、IDC 等多场景下的资产进行检测，但您需保证对所测试的资产具有合法权利、保证有权委托腾讯云对相关资产进行安全测试，且在测试正式开始前，您需出具授权函，允许腾讯云服务团队对您的所属资产进行攻防对抗测试。

安全攻防对抗的购买有什么限制么?

因安全攻防对抗服务测试的对象和范围较复杂，为保障安全攻防服务效果，本服务对攻击团队人员数量及演练周期时长限制了最小购买数量。攻击团队人员数量的最小购买数为3（人），演练周期时长的最小购买数量为5（天）。