安全攻防对抗服务

产品简介

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。

文档目录

产品简介
- 产品概述
- 服务内容
- 产品优势
- 应用场景

产品简介

产品概述

最近更新时间：2022-04-28 14:33:00

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，通过实战模拟 APT 攻击的手法，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。

产品功能

发现企业安全短板

以攻促防，通过安全攻防对抗服务，多维度、多视角检测可能造成企业信息化不安全的风险点。发现企业安全发展及建设的过程中存在的盲区，以便企业在攻防对抗后能够有针对性的进行补齐。

企业安全能力自检

对企业信息化安全建设中的基础设施安全、应用安全、办公网安全、安全管理等多方面的能力建设进行检查，检验这些能力在攻防实战中是否能够发挥其应有的效果。

实战防护能力检验

针对企业的安全防护能力进行检验。检验企业在遇到攻击时，是否能够快速发现并定位到攻击者，在攻击取得阶段性成果后，是否有明确的应急预案，是否能够有效进行应急处置。

服务内容

最近更新时间：2022-04-28 14:33:08

本文档将为您介绍安全攻防对抗服务的详细服务内容及交付内容。

服务阶段	服务内容	交付物
方案沟通	项目经理与客户确定本次攻防对抗演练的目标、范围、周期、约束条件、通报机制等。项目经理提供授权函模板，客户补齐授权测试的资产范围。	无
攻防对抗	由攻击队伍对企业相关资产进行攻击模拟，以方案中所确定的演练目标为目的，发现企业安全建设中的薄弱点，验证企业安全防护能力与安全响应机制。	《攻击成果报告》
对抗总结	对本次对抗的资源进行回收，梳理攻击链路，对本次攻防对抗的过程进行总结，提供企业安全的建设意见。	《攻防对抗总结报告》

产品优势

最近更新时间：2022-04-28 14:33:16

专业攻防队伍

腾讯安全团队拥有大量经验丰富的安全攻防专家，了解企业信息化资产面临的诸多安全隐患及当下流行的攻击及战法，使攻击更近实战。

自动化工具库

基于多年的攻防经验，沉淀归纳了攻击能力并自动化为测试工具。能够快速探测目标相关资产信息及可能存在的弱点，制定行之有效的战术，使攻击更高效。

规范与保密

攻击人员在攻防过程中遵守法律法规，不破坏系统或泄露敏感信息。在攻防对抗结束后，会清理攻击过程中遗留的木马，避免对业务带来安全隐患。

应用场景

最近更新时间：2022-04-28 14:33:20

防护能力自检

企业在信息化安全投入了大量的资源，需要通过模拟 APT 攻击的方式进行全方位的测试，检测自身安全防护能力整体水位。

安全攻防演练

企业在攻防演练前期，通过攻防模拟的方式确定企业安全能力是否存在短板、安全防护策略是否生效、是否存在安全盲区。

积累实战能力

通过模拟攻击与防护演练，积累实战经验，检验企业安全设备与人才队伍的作战能力，验证企业安全管理和服务部门之间的快速协同能力。

安全意识检测

检验公司员工的安全防护意识，在遇到非常规安全事件后能否有效的进行上报及处置，检验公司对攻击事件的发现能力。