应急响应服务

产品简介

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【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或95716。

文档目录

产品简介
产品概述

最近更新时间：2022-11-29 14:31:42

应急响应服务（Cybersecurity Incident Response Service，CIRS）基于腾讯安全专家能力及多年的攻防对抗经验构建。对发生的安全事件进行响应处理，采取标准化可控的应急处理方案，发现云上资产的安全问题，还原黑客的攻击路径，对用户在受到黑客攻击后所造成的影响进行止损。

产品功能

攻击路径还原

应急响应服务团队可以通过对服务器日志、攻击者痕迹、安全设备日志及流量的分析，还原得到攻击者的路径，了解到服务器沦陷的真实原因。

蠕虫及后门清理

基于对事故场景的探测和发现，应急响应服务团队将对用户服务器中可能隐藏的蠕虫病毒、后门程序、Rootkit 等恶意软件提供清理方案。

攻击者画像

通过对木马文件、安全日志及攻击痕迹等信息进行分析，应急响应服务团队结合 OSINT 以及其他平台对攻击者信息进行关联，对黑客的虚拟身份进行模拟画像，在数据量充足的情况下可以定位攻击者的真实身份。

安全漏洞复检

对于应急响应服务团队发现的失陷问题，提供相应的安全加固建议，在用户对资产完成加固后提供漏洞复检相关工作，以确认漏洞完全修复，避免再次出现相同的问题。

用户收益

快速止损，原因分析

应急响应服务团队凭借在互联网前线应急响应领域丰富的经验和深入的事件分析处理能力，能够更加快速地帮助用户定位到事件原因并避免同类问题再犯，将信息丢失、被破坏的程度降到最低，快速止损，帮助用户迅速有效地从安全事件中恢复过来，避免业务系统经济损失的持续增加和负面影响的不断扩散。

完善技能，优化体系

在应急响应服务团队与用户相关人员的交互过程中，协助提升用户的安全技能，同时发现安全运维体系中的不足并提出优化建议，建立安全事件响应机制以抵制信息安全威胁，提高企业信息业务系统发展的安全竞争力。

产品优势

最近更新时间：2022-01-26 10:41:22

全面的应急预案

基于长期对抗黑色产业所积累的安全防护经验，有效沉淀了各类安全事件的应急处置预案，使得安全服务团队在面临各类被入侵的事件场景时，能够成熟面对并有效的解决问题。

自动化应急工具

基于长期运营的数据库，以入侵痕迹探测、威胁感知、关联性分析等视角，成功转化为应急响应工具并用于实战，具备快速定位问题、自动化处理安全事件的能力，提高应急处置速度。

规范与保密

腾讯云安全服务团队具备规范的流程和完备的风险控制策略，有效处理安全事件应急工作的同时，规避了可能导致数据泄漏的风险点，确保用户私密信息不会外泄。

应用场景

最近更新时间：2025-05-20 17:55:32

企业被入侵

通过应急响应服务帮助用户阻断攻击进程，同时对受控制机器进行隔离，还原攻击路径并清理被植入的后门，协助加固入侵过程中被利用的漏洞。降低因生产网沦陷而对企业经济造成的损失。

网站被篡改

通过应急响应服务帮助用户恢复网站内容，发现并阻断攻击者控制网站的方法，协助加固网站或服务器安全漏洞，降低因网站被篡改而对企业名誉造成的影响。

挖矿病毒

通过应急响应服务帮助用户清除挖矿病毒，发现挖矿病毒得以传播的具体路径，协助加固服务器安全漏洞，降低因监管通告而对企业造成的影响。