专家服务

应急响应

产品文档

腾讯云

文档目录

应急响应
服务概述

最近更新时间：2019-08-01 17:11:44

基本概念

安全事件应急响应

随着信息技术的发展，安全威胁的数量、形式、种类越来越多，其破坏性也越来越大。当系统遭受网络攻击、病毒传播、黑客入侵等安全事件时，会导致信息业务中断、系统宕机、网络瘫痪、数据丢失、网页篡改等后果，对组织和业务运行产生直接或间接的负面影响。
安全事件应急响应是指安全技术人员在遇到突发事件后采取的措施和行动，是对已经发生的安全事件进行监控、分析、协调、处理、保护资产安全属性的活动。

腾讯云安全专家应急响应服务

腾讯作为中国最大的互联网公司之一，每天在与黑产、黑客等各类外部攻击者进行持续对抗，通过分析各种流行的安全问题和事件，已经形成了独具特点的、成熟的处理思路和丰富的技术手段。
腾讯云安全专家应急响应服务（简称“ SOS 服务”）主要为您提供专业的入侵原因分析、黑客溯源取证、业务损失评估以及系统恢复加固的安全应急响应服务，通过采取紧急措施和行动，协助用户以最快速度恢复系统的可用性、保密性和完整性，进而阻止和减小安全事件带来的负面影响，并调查安全事件发生的原因，避免同类安全事件再次发生，在需要司法机关介入时，为司法机关提供法律认可的数字证据等。

客户收益

快速止损，原因分析

腾讯安全专家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客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，帮助客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

在安全专家与客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。

服务优势

优势点	优势说明
安全研究能力	腾讯云拥有技术实力一流和攻防经验丰富的专家团队，同时联合腾讯 7 大安全实验室攻防专家进行前瞻安全漏洞技术研究，洞察最新安全威胁。
安全对抗能力	腾讯身为全球最大的即时通讯软件平台，长期对抗黑色产业，积累了丰富的安全防护经验，具备先进的安全防护技术，能实时为您保驾护航。
安全实践能力	信息安全建设需要长期进行。腾讯云可提供具备长期履行承诺能力的、保障用户测试服务可长期落地执行的、系统化的解决方案。
规范与保密	腾讯云具备标准规范的流程和良好的风险控制策略，可确保客户私密信息不会外泄。
专业服务团队	全服务团队主要由 CISP、CISSP、CCSK、ISO27001 主任审核员、CCIE 等安全专家，联合腾讯 7 大安全实验室以及业内领先的安全攻防能力人员组成。
成熟的知识库	腾讯具有行业公认的信息系统全生命周期安全服务的知识库和方法论，同时具备先进的工具，以保障测试维度全面、完善、专业。
大数据风险联动	基于腾讯云海量用户的常见入侵、威胁等数据进行安全分析，将积累的防御对抗经验运用于客户安全建设，达到实践与理论相结合的目的。
精准防护策略	腾讯自身在行业已积累丰富的安全对抗经验，可协助用户输出可全面高效的精准防护策略，快速解决用户痛点问题。

服务内容

最近更新时间：2019-08-01 17:23:08

服务范围

事件类别	详细描述
病毒传播	病毒传播事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序是指插入到信息系统中的一段程序，有害程序危害系统中数据、应用程序或操作系统的保密性、可用性和完整性，或影响信息系统的正常运行。
网络攻击	网络攻击事件是指通过网络或其他技术手段，利用信息系统的缺陷对信息系统实施攻击，并造成信息系统异常的信息安全事件，包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。网络攻击造成客户信息业务系统中断，给客户业务运转造成严重经济损失。
黑客入侵	黑客入侵事件是指黑客入侵信息系统造成的信息被篡改、窃取、泄漏、假冒、丢失、破坏等信息安全事件，包括信息篡改事件、信息窃取事件、信息泄漏事件、信息假冒事件、信息丢失事件和其它信息破坏事件。
安全事件	除计算机病毒入侵造成客户信息业务系统数据外泄、篡改、删除破坏严重安全威胁。网页挂马降低公众信誉度，影响客户行业公众形象，挂马使网站成为木马传播的帮凶；网络攻击造成客户信息业务系统中断，给客户业务运转造成严重经济业损失。

服务内容

服务内容	详细说明
入侵分析	全面排查主机是否被黑客入侵，及时对进行中的攻击进行处理和安全加固，阻止黑客进一步攻击，限制黑客横向移动范围。 全面查找和清理病毒、蠕虫、木马等恶意程序。 全面查找和清理 Web 站点中的 WebShell、暗链、挂马页面等。 全面对入侵导致的异常进行处理，帮助客户快速恢复业务。 为客户提供安全应急服务报告。
业务止损	快速修复系统异常，对安全漏洞进行安全加固，协助客户尽快恢复业务的正常服务。
黑客溯源	基于腾讯黑产对抗经验，结合腾讯威胁情报系统和安全云追查入侵源头和证据，定位黑客身份信息。

服务方式

腾讯云应急响应服务包括单次服务和年度服务两种形式，客户可以根据需求选择服务地点。

单次服务/年度服务

根据服务周期，腾讯云应急响应服务可以分为单次服务和年度服务。

- 单次服务：指为客户提供的一次性应急响应服务。一般由发生安全事件的客户临时申请应急响应支持人员参与应急事件处理，支持人员在分析完客户提供的所有信息后，向客户提交应急响应报告。
- 年度服务：服务期限以年为单位，服务年度内为客户提供有限次数的应急响应支持工作，每次服务均会提供详细的应急响应报告。

现场服务/远程服务

根据服务地点，腾讯云应急响应服务可以分为现场服务和远程服务。

- 现场服务：指接到客户紧急服务请求后，支持人员在最短时间内赶赴客户现场，协助客户分析事件发生的可能原因，解决各类安全事件。
- 远程服务：指通过电话、QQ 等方式远程协助、远程接入等非现场的服务，协助客户分析事件发生的可能原因，解决各类安全事件。

服务流程

1. 客户在腾讯云应急响应官方网址 腾讯云应急响应服务 中单击立即申请按钮，填写相关信息并提交申请。
2. 在线申请完成后，腾讯云安全专家和销售团队会与客户进行需求沟通，提供服务信息和报价信息。
3. 在确认客户安全需求后，双方签订合同，客户完成付款。
4. 腾讯云会与客户协商实施方式是由腾讯云实施或腾讯云推荐第三方实施（第三方实施过程腾讯云监督审计），实施完成后输出报告，最后由客户进行服务验收确认。

服务报告

腾讯云安全服务专家人员在应急响应工作完成后 3～5 个工作日内，会为客户提供一份应急响应报告。在报告中，安全服务专家人员将对整个安全事件进行详尽的分析，并给出最终的分析结果，还将根据分析结果提出解决方案和相关的安全建议，为事件的后期处理提供参考。最终将输出如下报告：

《XX 客户应急响应服务处理报告及安全优化建议》

服务提示

应急响应是一项要求强时效性服务，当错过某个时间点或者某个关键步骤都有可能影响到后期分析所得的结果。鉴于此，腾讯云安全服务专家建议客户在发生安全事件后不要惊慌失措，应采取如下措施以达到更好的服务效果：

1. 尽可能保留现场（如果因为特殊原因无法保留现场，也需要尽可能收集相关信息，为后续分析提供相关证据）。
2. 对于应急响应服务中可能出现的各种不确定因素，可在云服务专家的指导下开展证据搜集工作，常见支持工作如下：

工具记录

应急响应过程中，支持人员可能需要帮助客户去收集分析数据，此时必然会用到一些专门的工具。腾讯云安全服务专家在选择信息收集工具时要对使用的工具进行严格的测试，确保工具不会对使用目标产生任何的影响，更加不会扰乱安全事件相关的痕迹。

操作记录

应急响应过程中，客户可对服务过程中所进行的每项操作都进行详细的记录，包括执行了什么命令、复制了什么文件等，以便出现意外后进行追查。

方法依据

最近更新时间：2019-08-01 17:26:36

“工欲善其事，必先利其器”，腾讯云安全服务专家在多年的安全应急响应服务及安全对抗工作中，积累了丰富的安全应急响应经验，其中落地下来的理论方法包含成熟方法论和工具集合，通过经验理论指导操作步骤、工具快速定位分析原因，保障安全响应工作的快速、及时、有效进行。

成熟方法论

Windows 应急响应

常规分析

安全事件发生以后，常常有蛛丝马迹遗留在下列信息当中可供追溯，支持人员在处理安全事件时通常会收集这些信息来帮助应急响应的分析工作。

检查类别	检查原因
网络（非法链接）	是否仍然存在数据外传、非法外联等行为。
进程（服务、端口）	是否仍然存在伪造的木马进程。
自启动项目	处理完成后是仍会还会开机自启。
文件	是否仍然存在残留后门或恶意文件。
日志	日志中是否记录了黑客的攻击路径和利用方式。
驱动	底层是否存在可被利用的漏洞驱动版本。
软件版本	部分软件版本存在明显安全漏洞或者配置问题。

恶意代码

对于黑客入侵、病毒传播等类型的安全事件来说，支持人员必须要做的一项工作就是要检测事件目标是否已经被植入了恶意代码。
典型的恶意代码可能具有文件感染、数据加密、线程注入、SPI、端口复用、隐秘外联等功能，往往需要依赖于安全服务专家人为采用第三方检测工具进行深入逆向分析。

Unix/Linux 应急响应

常规分析

同 Windows 类似，主要从网络连接、进程状态、自启动项目、文件、日志、软件版本及配置等进行综合分析，收集此类信息后结合安全服务专家经验进行关联分析判断。

恶意代码

由于 Unix 类恶意代码的种类较少，检测目标也以 Rootkit、木马文件为主，其它恶意代码基本在常规检测中通过分析即可得出结果。

Web 入侵分析

当安全事件发生在 Web 应用上面的时候，支持人员会用到 Web 应用检测相关的技术，其中最主要的是 Web 应用访问日志分析、 Web 配置分析及软件版本分析工作，通过分析可以发现下列类型的安全事件：

- 应用层安全漏洞（SQL 注入、命令执行、信息泄露等）。
- 配置缺陷。
- 远程扫描等。

高效工具集

以下列出部分为常见的应急响应支持工具，但并不能包括真实环境下的全部应急响应工具。

信息收集工具

工具名称	工具说明
Process Explorer	微软内置工具集：SysinternalsSuite，进程分析工具。
Process Monitor	微软内置工具集：SysinternalsSuite，文件和注册表操作监视工具。
Autoruns	微软内置工具集：SysinternalsSuite，启动项检查工具。
Regmon	微软内置工具集：SysinternalsSuite，注册表监视工具。
Tcpview	微软内置工具集：SysinternalsSuite，网络连接查看工具。
Linux 常规工具	Linux 自带工具集合，例如 netstat/ps/ls/nc/iftop。
入侵分析脚本	腾讯云安全服务专家内部快速分析自动化脚本。

恶意代码检测

工具名称	工具说明
IDA Pro 商业版	专业逆向工具 下载地址 。

工具名称	工具说明
OllyDbg	开源免费工具 下载地址。
Chrootkit	Linux 常用后门检查工具 下载地址。
Rootkit hunter	Linux 常用后门检查工具 下载地址 。
Icesword	不明程序检测工具。
### Web 日志分析	
工具名称	官方地址
LogParser	日志分析工具 官方网址。
AWstats	日志文件分析工具 官方网址。
日志分析脚本/工具	腾讯云安全应急响应服务专家自用工具集。

实施原则

最近更新时间：2019-08-01 17:28:24

腾讯云安全专家在提供应急响应服务过程中，将遵循以下原则。

保密性原则

保密性原则是安全服务中最重要的原则。腾讯云安全专家应急响应服务的保密范围，包括实施过程的保密性和输出成果的保密性，对服务过程中获知的任何客户系统信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息进行任何侵害客户的行为；对服务报告的提交不得扩散给未经授权的第三方单位或个人。

标准性原则

腾讯云安全专家应急响应服务将在国家法律、法规允许的范围内进行，并按照 PDR2 等模型实施并提供整体修复建议。

规范性原则

腾讯云安全专家应急响应服务实施必须由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

风险规避原则

腾讯云安全应急响应服务工作应尽可能控制事件影响范围，避免其它系统和网络的二次事件扩散风险，尽可能无损地恢复客户业务。

购买指南

最近更新时间：2019-07-19 11:50:29

- 您可以按 使用流程 提交服务申请，或直接 联系我们 进行购买咨询。
- 工作时间：工作日早9：00 - 晚6：00。