目录

目录 1
产品概述 2
服务范围 2
服务方式 2
服务参考标准 2
产品优势 2
专业团队 2
快速响应 2
流程规范 2
使用场景 2
有害程序事件 2
网络攻击事件 2
黑客入侵事件 3

产品概述

应急响应（Emergency Response Service，ERS）是当用户遭遇网络攻击、木马病毒、黑客入侵等安全事件时，金山云提供包括抑制止损、事件分析、系统恢复等的应急响应服务，帮助用户快速恢复业务，降低安全事件带来的损失。

服务范围

事件类别	详细描述
网络攻击事件	网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。包含后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件和其他网络攻击事件。
有害程序事件	有害程序事件是指蓄意制造、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。包含计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件
信息破坏事件	信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。包含信息篡改事件、信息伪造假冒的冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件

服务方式

金山云应急响应服务方式分为“远程服务”和“现场服务”。

- 远程服务：指通过电话、邮件等方式远程协助、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。
- 现场服务：当远程支持无法解决问题时，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。（目前金山云应急响应现场服务仅限北京区域）

服务参考标准

应急响应服务参考国家标准，从服务内容上和服务流程上保障服务规范性和服务质量：

《信息安全技术-信息安全事件管理指南》-GB/Z 20985-2007 《信息安全技术-信息安全事件分类分级指南》-GB/Z 20986-2007 《信息安全技术-信息系统应急响应规范》-GB/T 20988-2007 《信息安全技术-信息安全应急响应计划规范》-GB/T 24364-2009

产品优势

专业团队

专业的安全服务团队，拥有丰富的应急处置经验，保证应急响应过程高效可靠

快速响应

能够根据事件级别进行快速响应，帮助用户降低安全事件带来的损失

流程规范

遵从标准化的服务流程规范，确保用户隐私不会外泄

使用场景

有害程序事件

计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、网页内嵌恶意代码事件和其他有害程序事件。恶意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，影响系统的正常运行。

网络攻击事件

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、网络钓鱼事件和其他网络攻击事件。网络攻击事件造成业务系统中断，给业务运转造成严重经济损失

黑客入侵事件

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。