IRS 文档

2020-02-20

百度智能云

目录

产品描述

产品介绍

应急响应是当发生黑客入侵、DDoS、数据窃取、木马病毒等事件时，提供包括抑制止损、事件分析、业务损失评估、系统加固、事件溯源的服务，降低安全事件对企业自身的影响与损失。

产品优势

丰富的应急处置经验

依托百度自身业务的多年安全实践经验，对事件进行精准的分析与还原，并协助企业对漏洞进行及时修复，防止类似威胁的再度发生

快速响应

能够根据事件级别进行快速响应和定位，降低因时间差造成的损失

事件分析与回溯

对事件发生的原因、方法及路径进行分析，并结合百度大数据威胁情报系统对事件进行回溯

专业的安全服务团队

安全服务团队成员都是由百度安全精心挑选的具备丰富应急处置经验的安全工程师，保证应急响应过程高效可靠

应用场景

事件确认

安全工程师与客户直接联系对接，通过与客户交流了解事件具体详情，并记录问题情况。根据客户描述现象与系统实际现象，对事件进行确认，定性；

事件抑制与分析

接到事件响应申请后， 安全工程师会根据情况进行远程或现场的响应。安全工程师会根据客户记录的安全事件描述，结合前期进行过的漏洞检测与分析结果、实时监控与审计结果等已有客户系统和网络状况，进行分析和判断。

事件处理

在对安全事件进行原因分析之后，安全工程师将进一步对安全事件进行处理，具体工作包括但不限于：

- 清理系统中存在木马、病毒、恶意程序；
- 清洗应用系统中存在的木马、webshell后门、挂马页面；
- 恢复被黑客篡改的系统配置，删除黑客创建的后门账号；
- 删除异常系统服务、清理异常进程；

事件分析报告

事件处理完毕后，根据具体情况编写事件应急响应报告，文档中阐述整个安全突发事件的现象、处理过程，处理结果、事件原因分析，并给出相应的安全建议。

产品定价

产品定价

目前物理服务器 IRS 只开放公测申请，如果您有购买意向，可以登录百度智能云官网选择应急响应IRS，然后点击立即申请，填写申请之后我们会有专门的人员为您提供报价，或者提交工单询问。

操作指南

开通应急响应服务

您可以登录百度智能云官网选择应急响应IRS，然后点击立即申请，完成应急响应服务在线申请表的填写，并在需求简述中，简单描写您的主要需求，我们会安排相关的人员跟进为您提供服务。

应急响应范围

应急响应范围包括网络或系统中的计算机或网络设备系统的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改、泄漏造成系统不能正常运行，或已经发现的有可能造成上述现象的安全隐患。

包括但不限于以下情况：

- 非授权访问，通过入侵的方式进入到未被授权访问的网络中，而导致数据信息泄漏；
- 信息泄密，数据在传输中因数据被截取、篡改、分析等而造成信息的泄漏；
- 拒绝服务，正常用户不能正常访问服务器提供的相关服务；
- 在系统日志中发现非法登录者；
- 发现网络大面积爆发计算机病毒感染；
- 发现有人在不断强行尝试登录系统；
- 系统中出现不明的新用户账号；
- 管理员收到来自其它站点系统管理员的警告信，指出系统可能被威胁；
- 文件的访问权限被修改；
- 因安全漏洞导致的系统问题；
- 其它入侵行为。

应急响应流程

事件响应的流程分为以下步骤：

第一步：事件确认

安全工程师与客户直接联系对接，通过与客户交流了解事件具体详情，并记录问题情况。根据客户描述现象与系统实际现象，对事件进行确认，定性；

第二步：事件抑制与分析

接到事件响应申请后， 安全工程师会根据情况进行远程或现场的响应。安全工程师会根据客户记录的安全事件描述，结合前期进行过的漏洞检测与分析结果、实时监控与审计结果等已有客户系统和网络状况，进行分析和判断。

第三步：事件处理

在对安全事件进行原因分析之后，安全工程师将进一步对安全事件进行处理，具体工作包括但不限于：

- 清理系统中存在木马、病毒、恶意程序；

- 清洗应用系统中存在的木马、webshell后门、挂马页面；
- 恢复被黑客篡改的系统配置，删除黑客创建的后门账号；
- 删除异常系统服务、清理异常进程；

第四步：事件分析报告

事件处理完毕后，根据具体情况编写《事件应急响应报告》，文档中阐述整个安全突发事件的现象、处理过程，处理结果、事件原因分析，并给出相应的安全建议，客户在获取报告后可以在对报告内容进行确认，也可以对服务过程提出反馈或投诉。

应急响应原则

实时原则

保证接受客户在事件应急响应提出的服务请求，并在接到客户的事件请求以后，在1小时内给予响应（电话或邮件）。

规范性原则

对每一次事件的发生都有严格的事件记录，并记录事件处理的全部过程。对于现场处理事件由客户签署认可建议。

保密性原则

对于所有事件的处理内容、时间、报告，严格遵从保密原则，不向任何的第三方透漏。

常见问题

一般性问题

应急响应时间？

答：我们会在您提出应急响应的1小时内响应并与您取得联系，具体排查与分析所需的时间，根据不同级别的事件及程度可能会有所差别。

是否一定能够定位到黑客？

答：我们会帮助您定位入侵事件发生的原因与弱点漏洞，但由于日志信息存在不完整或被黑客破坏的可能，我们会尽全力帮您清除后门病毒与定位黑客，但不能保证一定能定位到黑客。

如何收费？

答：正常情况下按次收费，我们会根据具体系统与服务器数量评估出费用，详细服务价格请您留下联系方式后，会有专人与您联系。