业务安全舆情监测使用指南

知道创宇业务安全舆情监测服务为客户提供及时有效的漏洞响应报告，实时监测和验证与客户网络资产相关的安全事件，安全漏洞，及时通报客户并且提供相应的处理方案，让企业在千变万化的网络安全威胁中，总是快人一步。

安全隐患，不可不知

漏洞信息爆炸：国家信息安全漏洞共享平台 2017 年收录 15403 个漏洞，同比增长 49.5%，漏洞类型变得越来越多也越加复杂。

安全事件监测弱：2018 年 Facebook 8700 万用户数据泄露，华住 5 亿客户数据泄露，万豪旗下酒店集团 5 亿客户信息被盗。

安全意识薄弱：应用组件漏洞的不规律爆发，业务安全的监测能力差，以及员工安全意识薄弱，导致敏感代码或者密码泄露。

威胁情报，不得不读

漏洞响应速递

服务内容：提供最新漏洞相关信息以及相关升级服务。在漏洞概况、影响版本、复现结果、影响范围以及防护措施等漏洞内容基础上，增

加漏洞细节、漏洞验证程序、修复方案等内容，提供正式规范的漏洞详细文档。

服务时效：最新漏洞响应并编写漏洞详细报告

交付方式：电子邮件实时推送漏洞详细报告

业务安全舆情监测

服务内容：定期对网站内容进行巡查，对发现的包括但不限于账号密码泄露，数据库泄露，业务系统敏感信息泄露，博彩，色情，恶意广告等内容进行预警通报，并提出整改建议。巡查范围包括但不限于百度、Google 和 Bing 等搜索引擎，Facebook、Twitter 等社交媒体，Pastbin 等第三方匿名数据分享平台，Github 等代码管理仓库等。

服务时效：即时给出安全事件处理建议方案

交付方式：电子邮件、微信推送漏洞详细报告

业务安全威胁情报

服务内容：404 安全专家基于创宇盾安全大数据分析平台，持续为客户挖掘对客户有价值威胁情报，并协助处理，包括但不限于网站异常

日志针对性分析、网站新业务安全巡查、网站攻击态势异常分析和网站业务逻辑异常分析等。

服务时效：定期季度报告，不定期漏洞报告

交付方式：电子邮件、微信推送漏洞详细报告

具体的服务开通方式，请联系您的安全顾问。