安全应急响应服务白皮书

1.1. 服务内容

1.1.1. 服务定义

了解客户业务安全事件具体详情，进行事件定性；及时排查隔离清理系统木马、病毒、恶意程序、暗链、篡改页面等，抑制攻击事态发展；通过各类设备流量与日志排查，尽可能达到攻击溯源效果；提供专业全面的应急响应报告和加固建议。

1.1.2. 服务范围说明

主要针对面向外网的 web 系统、主机服务器等

面向内网的需架设 vpn 通道进入本地内网排查

1.1.3. 服务内容说明

服务进度	服务内容	方式
应急前	确认受攻击目标情况 提供受攻击目标排查权限	客户提供
响应中	受攻击目标排查 威胁文件修改或隔离删除 问题加固建议	人工排查
响应后	输出应急响应报告	邮箱或其他联系方式

1.1.4. 服务流程

项目启动

同业主确认受攻击目标情况

受攻击目标情况：网页篡改、服务器进程异常、后门等

受攻击目标排查权限：root 或普通管理员权限

附件一 Xxx 系统应急调研表

项目中

同业主及时反馈响应情况

受攻击目标排查：事件描述、分析诊断、解决方法

威胁文件修改或隔离删除：威胁解决

问题加固建议：合理安全配置、漏洞修补、加设安全设备等

业务应急

可选随机时间段，7*24 业务应急

报告输出

在应急响应结束后，项目服务人员根据应急响应结果编写《应急响应报告》，报告内容包括事件描述、分析诊断、应急解决等内容。

1.1.5. 服务实施方

本服务由卓见云实施并提供技术支持和质量管理。

1.1.6. 服务形式

经客户授权采用远程互联网方式提供服务

说明：针对部分内网情况，可通过本地 vpn 通道方式进行。

1.1.7. 服务输出

- 《应急响应报告》

1.2. 风险控制

类别	风险控制项	风险管理办法
人员组织安全	组织要求	由卓见云交付服务团队提供服务。
	人员要求	所有服务人员均经过卓见云交付团队能力评估。
保密要求	保密协议	根据业主目标协定是否需签署保密协议。
过程安全	操作安全	应急前双方协定授权排查账号权限大小以及时间。 应急中及时沟通事件问题、解决方法。

1.3. 职责与分工

项目方	职责分工
业主	提供详细的受攻击目标情况与排查权限。 指派一名负责人对接服务工作。 应急中及时沟通事件问题、解决方法。
实施方	完成对目标的相关服务工作。 编写服务报告。

1.4. 结束标志

本服务以服务报告通过验收作为结束标志。