**深信服安全服务**

1.1服务内容说明

|  |  |
| --- | --- |
| 服务名称 | 服务内容 |
| **安全运营服务MSS-10** | **一、服务概述：**  安全运营服务以保障网络安全“持续有效”为目标，围绕资产、漏洞、威胁、事件四个要素，通过云端安全运营中心和安全专家团队有效协同的“人机共智”模式7\*24H持续性开展网络安全保障工作，与用户一同构建持续 (7\*24小时) 、主动、闭环的安全运营体系。  **二、服务期限：**  仅限于在本合同签订生效之日起一年内启用，自服务正式上线/启用之日起算服务期限。  **三、具体服务内容：**  **1.现状评估及处置加固**  1.1资产识别与梳理资产发现与识别：借助安全工具对用户资产进行全面发现和深度识别，并在后续服务过程中触发资产变更等相关服务流程，确保深信服安全运营中心中资产信息的准确性和全面性；资产信息梳理与管理：结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理，并将信息录入到安全运营平台中进行管理。  1.2安全现状评估：包含脆弱性、病毒类事件、攻击行为、失陷类事件等安全现状的评估  1.3问题处置：建立安全事件的进度监控机制，现场T1上门提供首次处置服务。  **2.持续有效运营**  2.1漏洞管理漏洞分析与管理：通过漏洞扫描工具识别系统安全漏洞，结合多种信息对识别的漏洞进行优先级排序，最后提出切实可行的漏洞修复指导；弱口令分析与管理：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等；针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测，并将检测发现的问题通过工单系统跟踪修复状态。  2.2威胁管理威胁分析与通告：实时监测网络安全状态，对攻击事件自动化生成工单,及时进行分析与预警。攻击事件包含境外黑客攻击事件、高级黑客攻击事件、持续攻击事件。实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。 病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发DOS型、C&C访问型、文件感染型、木马型；流行威胁通告与排查：结合威胁情报，安全专家排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固；主动分析与响应：每月主动分析病毒类、攻击类、漏洞利用类、失陷类的安全事件，并提供相应解决方案；策略管理：安全专家每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果；持续攻击对抗：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗。  2.3事件管理事件分析与处置：实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件；针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进 行根除，帮助客户快速恢复业务，消除或减轻影响；应急响应：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务，同时还原攻击路径，分析入侵事件原因，指导用户进行安全加固、提供整改建议、防止再次入侵。 |
| **安全风险评估服务** | **一、服务概述：**  服务工程师通过自研工具对组织信息资产面临的威胁、存在的脆弱性、现有防护措施及综合作用而带来风险的发生可能性进行评估，最终提供完整的风险评估报告及修复建议。  **二、具体服务内容：**  a.资产识别使用深信服的自研工具 (RAP、TSS 等) 对包括：业务系统、服务器、安全设备、网络设备等进行自动化扫描发现、识别、评估，可覆盖所有的资产，根据业务对资产的实际依赖程度区分重要资产，脆弱性识别、威胁 识别、风险分析等后期工作将针对重要资产进行识别；  b.脆弱性评估弱点存在于物理环境、硬件、软件、业务系统等各个方面，这些都可能被各种安全威胁利用来侵害用户的资产，让资产的价值受损。主要工作如下：漏洞扫描：使用 TSS 工具的漏洞扫描功能，快速从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全漏洞，并给出关于安全隐患的详细信息；基线配置核查：使用 TSS 工具的基线配置核查功能识别信息系统的安全配置情况；  c.威胁评估分 析用户信息系统存在的威胁种类，确定威胁分类的标准；综合威胁来源、种类和其他因素后得出威胁列表；针对每项需要保护的信息资产，尽可能 全面的发现资产所面临的威胁；  d.防护能力评估识别已有的安全控制措施，分析安全措施的有效性，确定威胁利用弱点的实际可能性，指出当前安全 措施的不足；  e.风险分析综合考虑资产本身的价值、威胁发生几率、脆弱性 的破坏力、现有防护能力等因素分析资产可能存在的安全风险，结合风险对业务战略的影响程度区别明确风险处置计划；  f.风险评估报告根据资产识别、脆弱性评估、威胁评估、防护能力评估的输出结果进行风险分析之后，通过 RAP 工具输出风险评估报告，风险评估报告中为用户提供符合业务需求的安全整改建议。 |

1.2采购清单

|  |  |  |
| --- | --- | --- |
| 项目 | 名称 | 数量 |
| 1 | 安全运营服务MSS-10 | |
| 1.1 | 安全运营服务 MSS-10资产 | 1年 |
| 2 | 安全风险评估服务 | |
| 2.1 | 资产数量：150台 | |
| 2.2 | 服务次数：1次 | |
| 2.3 | 安全服务工程师T1-A | 2天 |