网络安全审计服务资质认证证书申报 企业的安全系统日志

产品名称	网络安全审计服务资质认证证书申报 企业的安全系统日志
公司名称	广东昊霖企业管理有限公司
价格	.00/个
规格参数	可售卖地:全国 服务优势:全程一对一咨询辅导办理 办理周期:1-3个工作日
公司地址	深圳市宝安区松岗街道芙蓉路9号
联系电话	17707584459 17707584459

产品详情

系统日志的内容

系统日志主要根据网络安全级别及强度要求，选择记录部分或全部的系统操作。如审计功能的启动和关闭，使用身份验证机制，将客体引入主体的地址空间，删除客体、管理员、安全员、审计员和一般操作人员的操作，以及其他专门定义的可审计事件。对于单个事件行为，通常系统日志主要包括：事件发生的日期及时间、引发事件的用户IP地址、事件源及目的地位置、事件类型等。

【广东昊霖企业管理有限公司】

网络安全审计服务资质认证证书申报 企业的安全系统日志

安全审计的记录机制

对于各种网络系统应采用不同的记录日志机制。日志的记录方式有3种：由操作系统完成，也可以由应用系统或其他专用记录系统完成。大部分情况都采用系统调用Syslog方式记录日志，少部分采用SNMP记录。其中，Syslog记录机制主要由守护程序、规则集及系统调用3部分组成。

日志分析

日志分析的主要目的是在大量的记录日志信息中找到与系统安全相关的数据，并分析系统运行情况。主要任务包括：

（1）潜在威胁分析。日志分析系统可以根据安全策略规则监控审计事件，检测并发现潜在的入侵行为。其规则可以是已定义的敏感事件子集的组合。

（2）异常行为检测。在确定用户正常操作行为基础上，当日志中的异常行为事件违反或超出正常访问行为的限定时，分析系统可指出将要发生的威胁。

（3）简单攻击探测。日志分析系统可对重大威胁事件的特征进行明确的描述，当这些攻击现象再次出现时，可以及时提出告警。

（4）复杂攻击探测。更的日志分析系统，还应可检测到多步入侵序列，当攻击序列出现时，可及时预测其发生的步骤及行为，以便于做好预防。

审计事件查阅与存储

审计系统可以成为追踪入侵、恢复系统的直接证据，所以，其自身的安全性更为重要。审计系统的安全主要包括审计事件查阅安全和存储安全。审计事件的查阅应该受到严格的限制，避免日志被篡改。可通过以下措施保护查阅安全：

（1）审计查阅。审计系统只为专门授权用户提供查阅日志和分析结果的功能。

（2）有限审计查阅。审计系统只能提供对内容的读权限，拒绝读以外权限的访问。

（3）可选审计查阅。在有限审计查阅的基础上，限制查阅权限及范围。

审计事件的存储安全具体要求为：

（1）保护审计记录的存储。存储系统要求对日志事件具有保护功能，以防止未授权的修改和删除，并具有检测修改及删除操作的功能。

（2）保证审计数据的可用性。保证审计存储系统正常安全使用，并在遭受意外时，可防止或检测审计记录的修改，在存储介质出现故障时，能确保记录另存储且不被破坏。

（3）防止审计数据丢失。在审计踪迹超过预定值或存满时，应采取相应的措施防止数据丢失，如忽略可审计事件、只允许记录有特殊权限的事件、覆盖以前记录、停止工作或另存为备份等。