XXXX

安全管理平台招标要求

2005 年 **3** 月

目录

1 总则

1.1 关于本文件

一、 本文件为 XXXX 安全管理平台（SOC）项目的技术规范书。本规范书将作为谈判的基础，供应标方（以下称卖方）编制建议书及报价之用。

二、 规范书有关内容的澄清

1、 卖方对于规范书的疑问可以通过书面材料与买方联系。在规定的建议书提交最后期限以前，买方将以书面材料给予答复，有关买方答复材料的复印件也将递交所有得到技术规范书的卖方。

2、 在技术谈判的各个阶段，买方将以书面形式要求卖方对有关问题进行进一步的技术澄清，卖方应以书面资料给予正式应答；所有各阶段的技术澄清文件都将作为合同附件。

三、 买方在任何时候保留和拥有对本文件的解释权。买方有权在签订合同前，根据需要修改和补充本技术规范书，修改补充后的最终技术规范书将作为合同的附件。

1.2 卖方的建议书要求

一、 时间要求。卖方应根据本文件的要求在 14 天内提供建议书和报价，建议书和报价书应单独分册，其中：技术建议书要求提供 5 套，报价书 5 套，并提供建议书的电子文档。建议书要求采用中文书写。

二、 建议书的内容格式要求。

卖方所提供的建议书应按照以下内容格式进行编制：

1. 综述
2. 工程技术规范书
3. 技术规范书点对点应答
4. 网络安全管理平台建设方案建议

5. 设备配置和软件系统清单

6. 所提供设备和系统情况

7. 场地及环境准备要求

8. 工程进度安排

9. 分工界面，要求图示并加以说明

10. 测试及验收

11. 培训计划

12. 技术承诺

13. 技术服务、支持、保修

14. 所提供设备和系统(含软、硬件)技术文档

15. 网络设备的入网许可和网络安全产品的销售许可

16. 卖方公司资质证明、从业人员情况以及主要业绩说明

三、 技术规范书点对点应答要求

卖方的建议书中，要求对本规范书所提出各项要求进行逐条逐项答复、说明和解释，首先对实现或满足程度明确做出“满足”、“不满足”、“部分满足”等应答，然后做出具体、详细的说明。

四、 卖方在建议书中应说明对供货时间、安装、调测等进度的具体安排。

五、 卖方在建议书中应说明给买方提供的技术文件、技术支持、技术服务、人员培训等的范围和程度。

六、 卖方应在建议书中列出提供的书面技术资料的详细清单。

七、 卖方应列出其建议书中所提供设备和系统的推出时间、在全世界范围内的应用情况以及在各国公用数据网上的使用情况。

1.4 报价要求

2 工程描述

2.1 概述

随着网络和应用的飞速发展，网络安全逐渐成为影响网络进一步发展的关键问题。为了提升 XXXX 网络安全管理水平，提高网络安全性水平，增强网络竞争力，拟进行网络安全管理平台（SOC）的建设。

2.2 本工程目标

本工程的总目标为工程完成后，建成 XXXX 的全国网络安全管理平台。

2.3 本工程内容

本工程建设内容为：

一、 网络安全管理技术平台建设

二、 网络安全管理体系建设

2.4 本工程进度

本工程进度要求自合同签订 3 个月内完成网络安全管理平台工作。

3 资质与要求

3.1 厂商资质

1. 卖方应具备国家二级以上安全服务资质；
2. 卖方应具备 ISO9000 质量标准资质；
3. 卖方应具备涉密系统集成资质；
4. 卖方应具基于 CMMI 的质量保证体系

3.2 人员资质

1．卖方应有 5 个以上具备 CISSP 资质的人员；

2．卖方应有 5 个以上具备 CISP 资质的人员；

3．卖方应提供其他相关的人员认证资质；

3.3 产品资质

1．卖方提供的产品需符合国家相关安全标准；

4 技术支撑平台功能要求

安全管理中心技术支撑平台应具备监控、预警、响应、反击等功能。

4.1 监控

为了能实时监控信息网络的安全态势，安全管理平台（SOC）的安全监控功能必须具备以下四个方面：

1．资产管理功能；

2．安全事件管理功能；

3．安全黑名单功能；

4．业务安全监控功能

4.1.1 资产评估与管理

资产管理是信息安全管理的基础，要做到信息系统的安全管理，必须知晓系统中都有哪些资产，业务属性以及其安全状态等等。

为此资产管理应包括以下要求：

4.1.1.1 资产管理的内容

1． 资产的基本属性

- 资产名称、资产的 IP 地址、资产的 MAC 地址、资产的主机名；
- 资产的外部 ID、别名、相关描述；
- 资产拥有者的对应、资产的通告方式；
- 资产的创建信息、最近的更新信息；

2. 资产的逻辑网络区域
   - 资产所属的企业逻辑网络区域；
3. 资产的类别
   - 资产的物理位置类别；
   - 资产的硬件平台类别；
   - 资产的操作系统类别；
   - 资产的应用系统类别；
   - 资产的业务系统类别；
   - 资产的商务作用类别；
   - 资产的数据作用类别；
   - 资产的重要级别类别；
   - 资产所遵循的法律和标准类别；
   - 资产的应用协议和端口类别；
4. 资产与资产的关联关系
   - 当物理资产具有多个逻辑资产属性时，逻辑资产的关联管理；
5. 资产的脆弱性管理
   - 支持按照常用漏洞库类别进行脆弱性管理；
   - 支持共享专家知识库的关联管理；
   - 能针对资产的新脆弱性进行自动更新；

4.1.1.2 资产管理的关联

1. 资产属性的组管理
   - 支持具有相同资产属性的组管理方式；
   - 支持自动同步在不同组下的资产属性管理；
   - 支持资产的组继承功能。

2. 资产属性的事件关联管理

- 支持所收集事件的源、目的、设备等其资产属性的自动匹配功能；
- 支持事件里的资产属性异常和更改的报警功能；
- 支持资产的类别和逻辑网络区域等属性能被单独调用和做策略。

4.1.2 安全事件管理

4.1.2.1 事件收集

安全管理中心的监控对象应不仅涵盖现有的网络设备、主机系统，而且还应涵盖已经部署的安全系统，包括加密机、防火墙系统、IDS 系统、防病毒系统等，因此需要对这些系统的日志和事件信息进行集中采集，它们根据可预先定义的配置，把各种类型的安全数据格式化成统一的格式。

为此安全管理中心（SOC）应满足以下几个方面：

一、 支持以下设备事件类型

1. 操作系统

- All Unix syslogs (Solaris, AIX, HP-UX etc.)
- All Linux syslogs
- Windows NT/2000/XP/2003
- Windows MACS

2. 路由器和交换机

- Cisco
- 华为
- Juniper
- Foundry

- Extreme
- 3Com

3. 防火墙

- 天融信TopSEC防火墙
- Check Point Firewall
- NOKIA
- 北电ASF
- Cisco Pix
- Cisco IOS Firewall
- Cyberguard Firewall Appliances
- Gauntlet Firewall
- 基于Iptables架构的防火墙
- Lucent Brick and LSMS
- McAfee Desktop Firewall
- Netgear
- NetScreen
- ISS IceCap Manager
- OpenBSD Packet Filter
- Secure Computing Sidewinder Firewall
- Sonicwall Firewall/VPN Appliances
- Symantec Enterprise Firewall

4. Honeypot

- HoneyD

5. 防病毒

- McAfee
- Symantec
- TrendMicro

6. 入侵检测 - 基于主机

- Enterasys Dragon Squire
- ISS RealSecure Server Sensor
- Nagios.org
- NFR HID
- SamHain labs HID
- Symantec Host IDS (fka ITA)
- Sana Primary Response

7. 入侵检测 - 基于网络

- 天融信
- 启明星辰
- 中联绿盟
- Cisco IDS
- Enterasys Dragon Sensor
- Intrusion SecureNet
- ISS RealSecure Network Sensor
- ISS NetworkICE

- NFR NID
- Snort
- Sourcefire Network Sensor
- Symantec ManHunt

8. 入侵防范

- Cisco CSA
- McAfee
- NetScreen IDP
- McAfee IntruShield
- TopLayer AttackMitigator IPS
- TrustCorps TruShield

9. 身份识别与访问控制管理

- Netegrity SiteMinder
- Oblix NetPoint
- Vormetric CoreGuard

10. 高速缓存

- Microsoft Internet Security & Acceleration Server (ISA) 2000

11. 内容分发

- NetApp NetCache Series

12. 数据安全&完整性

- Vormetric CoreGuard
- Tripwire Manager

- Tripwire for Server
- Tripwire Open Source

13. 企业系统集成

- HP OpenView
- Cisco CiscoWorks
- IBM Tivoli

14. 日志收集

- Aelita InTrust (fka Event Admin)
- Kiwi Enterprises
- Microsoft Audit Collection System (MACS)

15. 管理控制台 - 特定厂商

- Enterasys Dragon Management Server
- Intrusion SecureNet Provider
- Intrusion CMDS
- ISS Site Protector
- Microsoft Operations Manager (MOM) 2000
- nCircle IP 360
- NetScreen Global Pro
- NFR CMS
- Sourcefire Management Console

16. 网络监控

- QoSient Argus

- TCP Dump

17. 安全策略管理

- Securify SecurVantage

18. 威胁响应技术

- Cisco Threat Response (CTR)

19. 双因素认证

- RSA SecurID / RSA ACE Server
- Secure Computing SafeWord PremierAccess

20. VPN

- 天融信
- Alcatel Secure VPN Gateway
- Check Point VPN-1
- Cisco VPN 3000 Concentrator Series
- Neoteris IVE Appliance (now NetScreen)
- Nortel Connectivity Switch

21. 漏洞管理

- eEye Retina Network Security Scanner
- Foundstone FoundScan
- Harris STAT scanner
- ISS Internet Scanner
- ISS System Scanner
- nCircle IP 360 Device Profiler

- Nmap
- Nessus
- OVAL
- QualysGuard
- Symantec ESM
- Visionael Security Audit

22. Web服务器

- Apache
- Microsoft IIS

23. 考虑网络设备管理信息的通用性，要求代理通过通用协议或应用服务收集设备信息，具体要求支持：

- SNMP v1、SNMP v2、SNMP v3
- SNMP Trap
- SysLog

24. 第三方还未支持的事件格式

- 在第三方厂商支持下，承诺5个工作日内支持

二、 统一化内容的基本要求

1. 事件的基本属性

- 事件时
- 事件名称和类型
- 事件信息内容
- 传输层和应用层协议类型

- 事件脆弱性的相关信息
- 流量信息
- 事件生成者信息
- 事件对应用户信息

2. 事件类型

- 安全重要性的类型
- 应对措施的类型
- 技术分析的类型

3. 威胁

- 资产威胁程度
- 影响严重性程度
- 发生可能性程度
- 可用性等级
- 分析处理的优先级别

4. 攻击者和目标者信息

- 主机信息
- 对应资产信息
- 对应用户信息

5. 设备信息

- 设备厂商信息
- 设备主机信息

4.1.2.2 事件整合

安全管理中心（SOC）通过对统一采集的事件进行过滤，冗余处理，以及根据预先定义的分类规则对事件进行归纳分类，并根据事件路由规则，把事件转发到各种事件处理服务器上或者直接转存到事件数据库中进行数据归档。

因此事件整合需满足以下几个方面：

一、 事件信息的特征过滤

根据安全管理中心（SOC）总体策略的需求，往往只需获得事件其中某些特征信息即可，所以要求整合事件时可以过滤其特定特征字段，如：

1. 事件的基本属性

- 事件时
- 事件名称和类型
- 事件信息内容
- 传输层和应用层协议类型
- 事件脆弱性的相关信息
- 流量信息
- 事件生成者信息
- 事件对应用户信息

2. 事件类型

- 安全重要性的类型
- 应对措施的类型
- 技术分析的类型

3. 威胁

- 资产威胁程度

- 影响严重性程度
- 发生可能性程度
- 可用性等级
- 分析处理的优先级别

4. 攻击者和目标者信息

- 主机信息
- 对应资产信息
- 对应用户信息

5. 设备信息

- 设备厂商信息
- 设备主机信息

二、 事件信息的特征归并

1. 支持归并所有需要的特征字段；

2. 支持归并的方式：

- 支持某个时间段内进行事件归并，单位按秒计算；
- 支持当某个事件段内其事件数超过某个门限值时进行归并；

三、 事件的整合处理机制

1. 支持事件定量处理方式：

事件定量处理方式支持当系统达到一定的事件量或者某一个时间段结束时，通过阻断事件发送以实现降低其性能消耗和优化网络带宽的作用。

- 支持基于事件最早达到的时间方式进行处理；
- 支持基于事件的安全优先级别进行处理。

2. 支持事件时间处理方式：

- 支持事件处理的时间校验功能；
- 支持事件采用统一时间戳功能；

3. 支持事件缓存处理方式：

- 支持自定义事件整合缓存大小；
- 支持当超过设定的缓存空间大小时，将采取每隔自定义的时间段内进行一次报警；

4. 支持事件性能处理方式：

- 支持事件传输带宽速率的自定义；
- 支持事件的名字解析；
- 支持保留原始事件并上传；
- 支持自定义事件处理速率，如：自定义EPS性能指标；

5. 支持事件交替处理方式：

- 支持事件在缓存定量处理方式下，对待处理事件信息通过其自定义特殊处理方式进行；
- 支持事件交替处理的时间范围；
- 支持普通事件处理上述所有功能；

4.1.2.3 事件关联

一、 支持安全事件的横向关联分析，即可以根据同一时间里，发生的安全事件进行聚合。具体要求如下：

1. 根据攻击源进行信息聚合分析；
2. 根据攻击目标进行信息聚合分析；
3. 根据受攻击的设备类型进行信息聚合分析；

4. 根据受攻击的操作系统类型及版本信息进行聚合分析；
5. 根据安全事件类型进行聚合分析；
6. 根据用户的策略定制；
7. 根据特定时间要求和用户策略进行横向事后关联分析。

二、 支持安全事件的纵向关联分析，即可以根据安全事件发生的因果关系，进行逻辑上关联分析。具体要求如下：

1. 具备常见网络攻击行为分析数据库，包括 DDOS 攻击、网络信息嗅探、漏洞扫描、网络蠕虫、木马攻击等常见网络攻击行为的纵向逻辑分析；
2. 具备自定义网络攻击行为功能，可以通过可视化的流程图的定义某种网络攻击行为；
3. 给出事件关联相关度的定量分析；
4. 可根据网络安全的动态情况，自适应过滤相关度较低的事件；
5. 可根据用户过滤策略过滤事件；

三、 支持对安全事件信息导入，可以导入到常见的数据库：

1. MS SQL
2. Oracle
3. DB2

四、 支持对下列安全事件类型的分析

1. DDOS 攻击
2. 缓冲区溢出攻击
3. 网络蠕虫
4. 邮件病毒
5. 垃圾邮件
6. Spoofing
7. 非授权访问
8. 企图入侵行为
9. 木马
10. 非法扫描

11. 可疑 URL

12. 用户定义类型

五、 支持知识库的灵活管理

1. 支持第三方的脆弱性数据导入，至少包括CVE和CERT等；

2. 支持能对任何满足知识库的事件进行关联和报警；

3. 支持自定义的知识库的添加；

4. 支持知识库已添加内容的自动更新；

5. 支持指定知识库所关联的各种资源，如工单、事件、脆弱性等。

4.1.2.4 事件可视化

一．详尽的事件显示和查询功能

提供丰富的事件显示和查找的功能，以便管理员对非法入侵事件和行为有很好的追踪和分析处理。

- 支持提供多种查询处理的方式，可以根据事件的各个字段来设定的过滤条件，查询到相关的事件记录；
- 支持传统的网格、线形图、圆饼图、条状图、区域图和重叠区域图等多种方式来显示特定事件；
- 支持用于关联业务情况的自定义事件图，并能满足业务网络和逻辑网络的多级显示；
- 支持在选定事件的范围内，根据事件的源和目的的管理关系，把其事件其它相关属性进行图形化显示；
- 支持根据做关联性匹配的事件进行图形化显示。

二．支持安全态势的实时监视

- 支持按照资产类别、事件关联关系、事件图形化、事件顺从关系、地理事件图形、层次图表、时间、最后状态、系统特征、特点前几位等类型进行实时监视；
- 支持过滤事件的各个字段进行自定义实时监视

三．支持在线和离线的事件可视化

4.1.3 安全黑名单管理

一、 支持自定义事件的任意字段进行规则匹配并最终确认为安全黑名单；
二、 支持安全黑名单的授权修改，包括事件匹配字段、有效时间等；
三、 支持安全黑名单的过滤规则调用功能；

4.1.4 业务安全监控

一、 支持业务应用系统的事件特征监控；
二、 分析与制定安全域与业务安全控制策略；
三、 支持基于业务应用的流程异常监控，包括了业务应用的时间关系、用户信息、访问权限和访问设备等关联关系进行自定义的规则监控。

4.2 预警

安全预警是一种有效预防措施， SOC 平台需要提供构建安全预警体系的方案。

4.2.1 安全分析

一、 分析网络安全的趋势，分析的内容包括漏洞的分布范围、受影响的系统情况、可能的严重程度等，及时发布预警信息；
二、 根据安全事件的监控情况，给出中主要的攻击对象分布、地理位置分布、攻击类型分布等情况分析，及时发布预警信息；
三、 根据安全事件的关联分析，给出网络中异常行为和异常现象的情况分析，及时发布预警信息；
四、 提供人工预警信息发布接口。当新的安全漏洞出现时，系统管理员可以通过该接口发布预警信息

4.2.2 安全信息发布

提供网络安全管理信息模块的实现方案。

1.2.2.1 知识库

一、 实现网络安全信息的共享和利用，在 SOC 平台提供统一界面以安全 WEB 的形式发布最新的安全信息；

二、 知识库包含安全漏洞库，安全配置库，安全事件库，安全案例库等，形成一个安全共享知识库；

三、 支持知识库分级、分组的授权访问管理

1.2.2.2 安全通告

一、 重大安全漏洞公布时，可通过平台进行安全漏洞的及时发布；

二、 支持 Web，Mail，短信等方式进行通告；

三、 支持根据用户设备的不同级别和不同类型，分别通告与之相关的信息。

4.3 响应

4.3.1 安全报表

4.3.1.1 安全态势报表

- 支持可以按照特定时间段的报表自动计划输出功能，同时指定报表输出的文档格式和其报表使用的有效期；
- 支持区域图、饼图、条状图和线形图等图形报表和文本报表；
- 支持按照事件内容各字段的自定义条件报表输出；
- 支持特定事件字段条件的报表输出。

4.3.1.2 工单处理报表

- 支持可以按照特定时间段的报表自动计划输出功能，同时指定报表输出的文档格式和其报表使用的有效期；
- 支持区域图、饼图、条状图和线形图等图形报表和文本报表；

- 支持可以根据工单的名称、创建信息、追踪信息、事故信息、安全属性分类信息、响应信息、相关报表信息、攻击信息、相关脆弱性信息、工单历史记录信息等进行自定义报表输出。

4.3.1.3 资产情况报表

- 支持可以按照特定时间段的报表自动计划输出功能，同时指定报表输出的文档格式和其报表使用的有效期；
- 支持区域图、饼图、条状图和线形图等图形报表和文本报表；
- 支持可以根据资产的名称、别名、创建事件、拥有者、创建者、IP 地址、主机名、脆弱性等进行自定义报表输出。

4.3.1.4 通告信息报表

- 支持可以按照特定时间段的报表自动计划输出功能，同时指定报表输出的文档格式和其报表使用的有效期；
- 支持区域图、饼图、条状图和线形图等图形报表和文本报表；
- 支持根据通告信息的 ID 号、事件 ID 号、事件名称、安全级别、创建事件、通告等级、通告的确认状态和时间等进行自定义报表输出。

4.3.1.5 标准符合性报表

- 支持可以按照特定时间段的报表自动计划输出功能，同时指定报表输出的文档格式和其报表使用的有效期；
- 支持区域图、饼图、条状图和线形图等图形报表和文本报表；
- 支持根据国家法律、行业规定、安全技术标准（如 BS7799、ISO15408 等）进行自定义报表输出。

4.3.2 工单管理

一、 支持两种工单流程触发方式

- 在用户特定规则下其安全事件可以直接自动触发对应工单流程；
- 手工自定义触发对应的工单流程。

二、 初始触发工单系统时应包括以下基本信息

- 工单名称和可直接查询的工单号；
- 工单处理的类型、阶段进度、处理频率、操作影响的优先程度、安全级别、安全性影响程度、报告事故的基本时间信息（检测的时间、估计开始处理时间和估计恢复时间等）、这次工单对应的用户名称以及通知对象等信息；
- 这次工单的安全级别定义，如：攻击方式、攻击区域、敏感性级别、建议采取的应对方式等；

三、 跟踪处理工单系统时应包括以下信息

- 已经采取措施的详细说明；
- 计划将要采取措施的详细说明；
- 曾经建议应对措施的历史记录等；

四、 结束工单系统时应包括以下信息

- 确定攻击的方式；
- 确定攻击的协议；
- 确定攻击的操作系统；
- 确定攻击的程序；
- 确定攻击的时间；
- 攻击涉及的目标对象、服务、对业务的影响；
- 最终报告总结整个应对措施

五、 支持查询和编辑这次工单所涉及的事件信息；

六、 支持工单变化状态的自动查询功能；

4.3.3 安全报警

一、 支持多种报警方式：邮件报警、短信报警、CALL 机报警、自定义程序报警；

二、 支持根据根据事件的各个字段建立报警策略。

4.3.4 事件处理系统

一、 支持根据事件策略规则执行 SOC 软件平台自身组件命令；

二、 支持根据事件策略规则和网管软件（如：HP 的 Open View 网管软件）进行互操支持根据事件策略规则自动触发工单处理系统；

三、 支持根据事件策略规则进行通告处理。

4.4 反击

4.4.1 事件归档审计

一、 支持所有安全事件的归档保存；

二、 支持所有归档事件的重新查询；

三、 支持所有归档事件的自定义报表输出；

四、 支持所有归档事件的深度关联分析。

4.4.2 攻击定位

一、 支持事件关联的攻击分析；

二、 支持确定攻击事件的详细信息查询；

三、 支持攻击源的事件图形化，包括攻击 IP、攻击相关协议、攻击技术方式；

四、 支持攻击源的物理位置、IP 地址、影响业务、对应资产的拥有者、对应的公司部门等查询。

5 技术平台架构

5.1 平台组件

5.1.1 事件收集引擎

安全管理平台的“事件收集引擎”负责收集和处理各类安全设备、网络设备、

服务器、工作站的日志以及报警信息。

5.1.1.1 事件收集分类

一、 支持通过 snmp trap、syslog、odbc 等方式接受事件日志，在这种形式下，在目的系统上无须安装组件；

二、 支持通过运行在特定设备或系统上的收集代理收集信息。

5.1.1.2 支持事件的类型

一、 安全设备：防火墙、入侵检测系统、防病毒系统、漏洞扫描系统、安全审计等；

二、 网络设备：路由器、交换机等；

三、 操作系统：Windows 操作系统(nt/2000/xp/2003)、linux、HP-UNIX 等；

四、 应用程序：Web、Iis ftp、Wu-ftp、Exchange、lotus、Sendmail 等；

五、 任何支持标准 SYSLOG、TOPSEC 等标准日志格式和 snmp trap、syslog、odbc 等。

六、 对特定系统的日志格式，支持开发事件收集引擎，开发时间标准为 5 个工作日；应用程序需要提供其日志相关的 API 接口，开发时间标准为 14 个工作日；

5.1.1.3 环境支持

一、 支持 Windows nt/2k/xp/2003 以上版本

二、 支持 Redhat 8.0 以上版本

三、 支持 Sun Solaris 8 以上版本

5.1.2 核心处理服务器

安全管理平台的核心处理服务器是主要对不同的事件收集引擎所收集的各类安全事件进行分布式的智能分析、过滤，并按照标准格式进行事件关联分析。

5.1.2.1 结构组成

一、 任务调度模块：负责周期性的执行用户设定的功能，支持每个月执行、每周执行、每天执行、一次性执行、立即执行等方式。

二、 报表统计：按照用户定制的要求，对原始日志数据进行统计分析，生成统计报表；

三、 安全检测：基于日志信息的入侵检测，采用模式匹配、神经网络、数据挖掘等多种成熟的入侵检测算法，实现对入侵行为的实时警告，对检测的危险事件进行分析并生成报表；

四、 数据库备份：可以将数据库中的日志数据进行备份。并且支持备份数据导入到历史数据库中；

五、 日志上传模块：将日志信息发送给上级的安全管理中心，可以定制发送几天内的数据，也可以定制上传的日志类型；

六、 日志审计：按照用户定义的规则，对全部日志进行筛选。支持审计管理器的日志查询功能；

七、 管理功能：包括过滤策略、安全级别映射策略、用户管理、权限管理、对象管理、响应策略等功能；

八、 版权保护：使用 hasp，对软件的 license 进行保护。防止软件的被非法用户盗版使用。维护正版用户的合法权益。

5.1.2.2 环境支持需求

一、 支持 Windows 2000/2003 server 以上版本

二、 支持 Redhat 8.0 以上版本

三、 支持 Sun Solaris 8 以上版本

四、 支持 HP-UX 11.0 以上版本

5.1.3 数据库

安全管理平台的数据库是储存所有安全事故和相关信息，同时提供安全分析师正确信息以及协助安全事故的处理。

5.1.3.1 主要功能：

一、 储存安全管理中心内收集到之各安全设备产生的安全事故，供进一步分析使用；

二、 储存安全管理中心内外分析与收集来的潜在弱点；

三、 储存安全管理中心内外收集来的安全事件与安全通报纪录；

四、 储存组织内应对安全事故的各项措施与纪录；

五、 数据库备份与回存功能。

5.1.3.2 环境支持需求:

一、 支持 Oracle 9i 以上版本

二、 支持 DB2

5.1.4 控制台

安全管理平台的 GUI（图形用户接口）控制台提供一个图形化的界面，使得所有安全管理平台的操作与配置都可以在一个平台上实现，并通过安全管理平台的内部安全隧道进行数据传输。

5.1.4.1 主要功能：

一、 支持安全事件的实时动态监控操作；

二、 支持安全事件的深入分析与处理；

三、 支持各种报表的定制与发送；

5.1.4.2 环境支持需求:

一、 支持 Windows 2000 以上版本

二、 支持 Redhat 8.0 以上版本

5.1.5 Web 入口

安全管理中心的 WEB 入口是一台 WEB 服务器。

5.1.5.1 主要功能：

一、 支持通过 SSL 安全加密隧道进行基于 WEB 方式的访问

二、 支持通过 WEB 方式远程查询与监视相关的事件和安全态势

三、 支持输出和查询用户自己的相关报表

四、 支持工单的查询与跟踪

五、 支持安全通告、知识库的查询

5.1.5.2 环境支持需求:

一、 支持 Windows 2000 以上版本

二、 支持 Redhat 8.0 以上版本

6 平台建设服务要求

6.1 安全风险评估

风险评估是 SOC 建设的基础。

6.1.1 资产风险评估

1. 提供风险评估的参考标准
2. 提供详细的资产风险评估计划
   - 人员组织和责任划分；
   - 时间进度安排；
   - 阶段性文档提交；
   - 验收标准；
   - 质量保证和风险规避措施等；
3. 提供风险评估工具的列表和法律符合性要求

6.1.2 安全域评估与划分

1. 安全拓扑评估
2. 安全域划分
3. 资产域初始化

6.1.3 业务系统评估

1. 关键业务系统人工评估
2. 业务流程梳理与评估

6.1.4 安全管理评估

1. 安全管理调查

2． 安全管理策略分析

6.2 平台系统初始化

SOC 平台系统初始化是 SOC 建设的关键。

6.2.1 资产初始化

1．根据资产调查，将结果录入 SOC 系统

2．根据安全评估结果，对资产属性进行初始化

3．根据安全域划分，确定资产的域初始化

6.2.2 用户权限初始化

1．根据实际情况设立用户组和用户角色

2．根据角色设置用户帐户

3．对每个用户组和用户角色进行权限初始化

6.2.3 监控面板定制化

1．根据实际需求定制监控面板

2．定制过滤条件，优化监控界面

6.2.4 响应流程初始化

1．根据实际情况制定安全响应流程

2．系统平台中对响应流程进行初始化配置

3．实现响应流程的自动化处理

6.2.5 安全报表初始化

1．根据实际需求定制安全报表格式

2．定制报表产生时间

3．不同级别人员报表初始化

6.2.6 规则库初始化

1．制定各种安全技术规则

2．制定安全管理策略规则

3．制定业务安全管理规则

6.2.7 知识库初始化

1．提供安全漏洞知识库

2．提供系统安全知识库

3．提供网络安全知识库

4．提供安全案例知识库

6.3 安全管理体系建设

6.3.1 组织架构

对于 XXXX 的安全管理中心，应建设一套完整的管理机构。

6.3.1.1 组织架构组成

一、 协助成立安全管理中心管理小组对整个安全管理中心的全面管理工作

二、 协助成立日常管理小组针对安全管理中心的内部事务型工作的处理

三、 协助成立协调小组协调组织内部各种资源的协调

四、 协助成立运维小组对全网的信息资产进行监视、对安全事件进行分析、产生必要的警告和报警，以维护网络的正常运行。

五、 协助成立专家组对安全管理中心的安全事件进行分析和处理

六、 协助成立审计监督小组对所有人员行为进行审计和监督等

七、 协助成立运行与保障小组保证安全管理中心自身的安全运行。

6.3.1.2 组织成员管理

安全管理中心（SOC）的组织成员根据自身业务的安全需求情况，要求协助进行如下工作：

一、 背景调查: 包含了学历，资历,专业技能，专业证照，语言等项目；
二、 忠诚查核: 包含其过往经历的道德评价，公安机关的良好纪录证明等；
三、 员工保密合约的签定 ；
四、 职位鉴定，任用，升迁与绩效评估；
五、 教育训练计划；
六、 人员轮调计划；
七、 人员委外合约。

6.3.1.3 组织成员培训

为了安全管理中心的正常运作，要求完成对组织成员的如下培训：

一、 安全运维工程师技能培训
二、 安全分析师技能培训
三、 网络管理员技能培训
四、 数据库管理员技能培训
五、 系统管理员技能培训
六、 高级安全管理培训

6.3.2 安全运维流程

安全管理中心（SOC）需要建立一整套的运营维护各项流程：

一、 安全事件监控操作流程
二、 安全事件通报流程

三、 安全通告发布流程

四、 安全事件应急处理流程

五、 灾难恢复计划

六、 风险评估计划

七、 内部审计计划与流程

八、 配置变更管理流程

6.3.3 安全管理制度

安全管理中心（SOC）需要建立一整套的安全管理制度：

一、 管理中心物理安全制度

二、 管理中心日常管理制度

三、 管理中心人员值班制度

四、 管理中心人员参观制度

五、 管理中心访问控制制度

六、 管理中心知识库管理制度

七、 管理中心安全事件分级原则

八、 管理中心病毒防护制度

九、 管理中心数据备份制度

一〇、 管理中心安全检查制度

一一、 管理中心报表管理制度

6.4 平台支持服务

卖方应对安全管理平台提供一年的各类支持服务：

一、 一年的软件 license 升级支持

二、 一年的规则库定期升级支持

三、 一年的知识库定期升级支持

四、 一年的 5×8 电话咨询服务

五、 一年的 7×24 应急响应服务

6.5 经验要求

6.5.1 SOC 建设经验

1．卖方应提供 SOC 建设经验和案例

2．卖方提供的 SOC 建设服务应具备可操作性

3．卖方应提供可展示的安全管理平台

6.5.2 SOC 运营经验

1．卖方应具备实际的安全管理中心运营经验

2．卖方自身的安全管理中心至少应具备远程异地备份的结构

3．卖方提供的 SOC 运营流程应具备实际可操作性

4．卖方提供的 SOC 安全管理制度应具备实际可操作性

7 平台部署

7.1 分级部署

一、 系统要支持多级管理和多级部署。

二、 多级平台的信息交换内容可以灵活选择。

三、 系统的分级管理能够灵活的配合行政管理的组织架构。

四、 二级系统能够单独制定策略，同时一级中心能够对二级中心进行统一的策略分配。

五、 一级中心能够对二级中心的管理内容和权限进行控制。

7.2 可靠部署

7.2.1 性能设计

一、 事件收集引擎不得影响主机的性能，CPU 占用低于 2%

二、 系统事件处理能力大于 5000 条事件/秒

三、 支持多种大型数据库（Oracle、DB2）

四、 计算安全管理平台网络流量，保证足够的带宽

五、 计算安全管理平台的数据量，保证足够的数据库空间

7.2.2 冗余设计

一、 主机系统支持双机热备，当系统故障时能够立即备份系统的在线工作，切换时间小于 1 秒。

二、 支持数据库的双机热备，数据库故障时能够自动切换；

三、 建立良好的数据备份与恢复机制，保障数据的及时备份与冗余；

四、 在分级部署的中，二级系统无备份措施的情况下，当二级系统故障时，二级系统所监控的范围，可以自动由一级系统暂时监控。当二级系统恢复时，可以进行监控权恢复。

7.3 安全部署

7.3.1 平台自身防护

一、 平台系统的管理员可以分成不同的权限，符合权限分割原则，同时提供超级管理员。

二、 分级平台之间的管理权限有良好的配合性。

三、 多级系统之间的信息交换应提供良好的安全性。

四、 所有平台组件之间的通信为 SSL 加密通信

五、 支持带内管理和带外管理

7.3.2 平台安全保护

一、 应考虑平台的物理安全措施，给出安全隔离和访问控制措施

二、 应考虑平台的逻辑安全措施，给出安全隔离、访问控制、入侵检测、防病毒等安全产品的部署方案

三、 所有平台相关设备应进行安全加固与优化配置

8 平台标准

一、 通过平台制度与策略等建设，帮助实现等级保护等政府关于信息安全方面的指导性文件（27 号文件和 66 号文件）。

二、 该系统的建设要能够将使用者的安全管理标准化并与国际接轨，如 BS7799 等，同时要保证与使用者的现状相符。

三、 系统在为使用者建立策略等内容时，符合 GB18336 标准，能够进行审计、审查和安全性分析。