ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

联 盟 标 准

CCIA XXXX—2019

网络安全态势感知系统技术要求

Technology requirements for network security situation awareness system

（征求意见稿）

2019-8-14

2019－XX－XX 发布　　2019－XX－XX 实施

中国网络安全产业联盟 发布

目　　次

前　言

本标准按照 GB/T1.1-2009 给出的规则起草。

本标准由中国网络安全产业联盟提出并归口。

本标准起草单位：公安部第三研究所，北京赛西科技发展有限责任公司等。

本标准主要起草人：

网络安全态势感知系统技术要求

1 范围

本标准规定了网络安全态势感知系统的安全功能要求和安全保障要求。

本标准适用于网络安全态势感知系统的设计、开发、建设、部署及检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 25069 信息安全技术 术语

GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

3 术语和定义

GB 17859-1999、GB/T 25069和GB/T 20986-2007界定的以及下列术语和定义适用于本文件。

3.1

网络安全态势感知系统 cyber security situation awareness system

通过采集网络环境要素（如资产、网络流量、运行状态、设备告警、脆弱性、安全事件和威胁情报等数据），利用数据挖掘等分析技术，对网络安全状况进行分析，对网络安全趋势进行预测，从而协助应急处置和安全决策的产品。

3.2

资产 asset

对网络信息系统有价值的信息或资源，是安全技术保护的对象，包括数据、软件、硬件、服务等。

3.3

网络流量 network traffic

连接网络的设备（包括各种网络设备、安全设备、服务器等）在网络上所产生的数据包的集合。

3.4

脆弱性 vulnerability

可能被威胁所利用的资产或若干资产的薄弱环节，包括漏洞、不安全地配置等。

3.5

风险 risk

威胁主体利用脆弱性的可能性以及对相关业务的影响。

3.6

设备告警数据 device alert data

安全设备或安全平台上根据对网络流量、日志、扫描探测返回信息等数据的分析结论或基于机器学习、引擎类设备、工具、组件关联分析生成的，描述异常网络情况、异常系统访问或系统脆弱性的信息。

3.7

网络安全事件 network security incident

由于人为以及软硬件本身缺陷或故障的原因，对信息系统构成潜在危害、甚至影响信息系统正常提供服务的情况。网络安全事件通常会对社会造成负面影响，且是经过确认需要做出一定处置措施的事实。

3.8

威胁情报 threat intelligence

一种基于证据的知识，包含了上下文、攻击机制、攻击指标、启示和可行建议。威胁情报描述了现存的、或者是即将出现针对资产的威胁或危险，并可以用于通知主体针对相关威胁或危险采取某种响应。

4 总体说明

4.1 产品描述

本标准将网络安全态势感知系统安全技术要求分为安全功能要求和安全保障要求两大类。

网络安全态势感知系统的安全功能框图如图1虚线部分所示，主要包括数据采集、数据处理、数据存储、数据分析、展示和告警、安全管理和自身安全功能，各类前端探针（如流量探针、服务器探针、监测平台等）的功能、利用产品结果进行决策和处置以及数据共享相关系统等的功能不在本标准的范围内。产品通过外部的流量探针、服务器探针、其他监测平台、第三方上报等采集得到资产数据、运行状态数据、设备告警数据、流量数据、脆弱性数据等，然后对采集到的数据进行处理、存储和分析之后，得到网络的安全状况并进行多维度的展示，从而为安全决策和应急处置等活动提供基础和依据。在实际某些情况下，态势感知的分析结果需要人工参与，此外，也需要通过接口等方式与第三方、上下级进行数据共享，这部分内容不在本标准阐述。

数据采集功能指明了系统应支持的采集方式、前端采集源管理和数据源类型等；数据处理功能提出了如何处理采集到的数据的要求；数据存储功能描述了应该存储什么类型的数据；数据分析功能要求系统具备数据分析能力，从而进行安全事件辨别、定级、关联分析等；展示和告警功能提出了安全态势展示、统计分析和安全告警等要求；安全管理功能提出对系统进行安全管理的要求，包括安全策略管理、安全事件管理、时间同步等要求；自身安全功能提出了与产品自身安全相关的要求，包括标识与鉴别、角色管理、远程管理、自身审计等要求。

安全保障要求针对网络安全态势感知系统的整个周期过程提出具体的要求，包括开发、指导性文档、生命周期支持、测试和脆弱性评定。

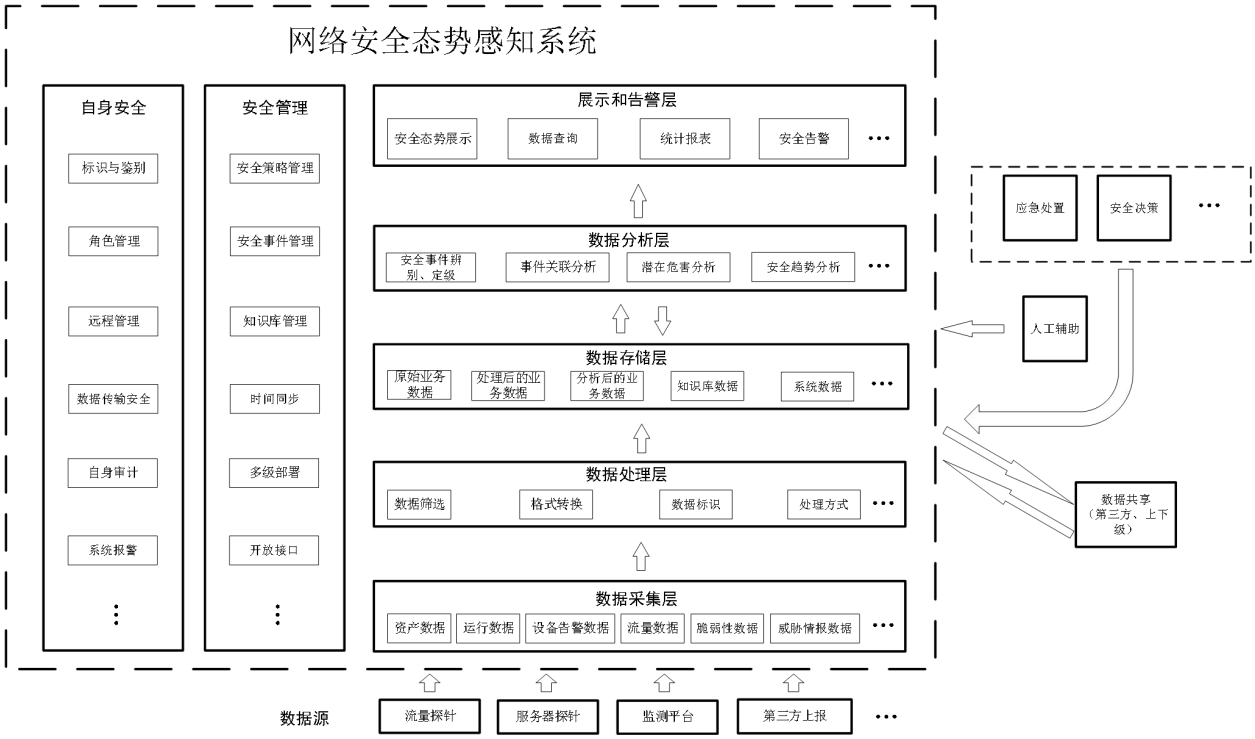

图 1 网络安全态势感知系统功能框图

4.2 安全等级划分

本标准按照网络安全态势感知系统安全功能的强度划分安全功能要求的级别，参照GB/T 18336.3-2015划分安全保障要求的级别。安全等级突出安全性，分为基本级和增强级，安全功能强弱和安全保障要求高低是等级划分的具体依据。

5 安全功能要求

5.1 数据采集

5.1.1 采集方式

对于不同类型的数据，产品应能通过不同的方式进行采集，具体采集方式如下：

a) 被动接收；
b) 主动采集；
c) 文件导入；
d) 其他方式。

5.1.2 前端采集源管理

对于不同的前端采集源，产品应能进行不同方式的管理：

a) 对于通过主动方式采集数据的前端采集源，支持设置和下发采集规则、进行时钟校准、对采集设备的运行状态进行监测、对采集设备进行开启/关闭/重启等；
b) 对于通过被动方式采集数据的前端采集源，支持前端采集源进行识别和控制。

5.1.3 采集数据类型

产品应能采集不同类型的数据，具体数据类型如下：

a) 资产数据；
b) 网络流量数据；
c) 运行状态数据；
d) 设备告警数据；
e) 脆弱性数据；
f) 安全事件数据；
g) 威胁情报数据；
h) 其他数据。

5.2 数据处理

5.2.1 数据筛选

产品应能基于既定策略（如必填字段缺失、重要字段格式错误、重复数据等）对采集的数据进行筛选，确保数据的质量。

5.2.2 数据转换

产品应能对采集的同一类型、不同格式的原始数据转换为统一的数据格式，且转换时不能造成关键数据项丢失和损坏。

5.2.3 数据标识

产品应能对采集数据的重要字段进行标识。

5.2.4 处理方式

产品应对不同类型的数据采用实时处理、离线处理等处理方式。

5.3 数据存储

5.3.1 存储数据格式

产品应能存储结构化数据、半结构化数据和非结构化数据等不同格式的数据。

5.3.2 存储数据类型

产品应能将数据进行分类存储，具体存储数据类型如下：

a) 采集获取的原始业务数据、处理后的业务数据和分析后的业务数据；
b) 管理数据，如系统的安全策略数据、用户信息、运行日志及自身审计日志等；
c) 知识库数据，如资产库、安全事件库、漏洞库等；
d) 知识库数据，如威胁情报库等。

5.3.3 存储数据安全保护

产品应采取安全机制，保护存储的数据免遭未经授权的读取、删除或修改。

5.3.4 防止存储数据丢失

产品应提供以下措施防止存储数据的丢失：

a) 各类数据应存储于掉电非易失性存储介质中；
b) 当存储容量达到阈值时，发出报警信息；
c) 在存储空间耗尽前采取措施，避免数据受到未预期的删除、修改或覆盖等。

5.3.5 存储数据备份

产品应提供以下存储数据的备份功能：

a) 支持备份策略的自定义及数据的自动或手动备份；
b) 通过自动化方式将存储数据进行转存。

5.4 数据分析

5.4.1 安全事件辨别

产品应能对采集的数据进行分析，判断数据所属的安全事件类型。

5.4.2 安全事件定级

产品应能结合资产的重要程度、资产所处位置等为安全事件设定其级别，以表明事件的性质或揭示此类事件的发生给网络所带来危险程度。

5.4.3 事件关联分析

产品应提供事件关联分析功能，具体内容如下：

a) 从采集的不同类型的数据中关联分析出同一安全事件；
b) 从多个安全事件中关联分析出安全事件发生的因果关系；
c) 从多个安全事件中关联分析出事件的访问路径，得到安全事件相关的源主机与目标主机；
d) 其他关联分析功能。

5.4.4 异常行为分析

产品应维护一个网络内合法用户的正常行为集合，以此区分入侵者的行为以及合法用户的异常行为，具体内容如下：

a) 访问频次超限；
b) 访问流量超限；
c) 账户异常登录；
d) 非授权访问、外联；
e) 文件非授权外发、下载；
f) 文件异常修改；
g) 权限异常提升；
h) 日志异常变化；
i) 其他异常行为。

5.4.5 潜在危害分析

产品应能通过数据挖掘等技术对采集的不同类型数据进行潜在危害分析，如通过将已发现的异常行为与原始日志的进行关联，用于探测未知安全威胁。

5.4.6 安全趋势分析

产品应能基于不同时间发生的安全事件，分析网络的安全趋势。

5.5 展示和告警

5.5.1 整体态势展示

产品应能对网络内的整体安全态势进行评估和展示，具体内容如下：

a) 对网络的总体安全状况用分值或等级等方式进行评估和展示；
b) 对不同业务单元、不同设备等进行分块安全评估和展示；
c) 对不同时间段的网络安全状况进行评估和展示；
d) 支持对不同的管理员展示不同维度、不同视图的网络安全状况的能力；
e) 采用多种视图展示安全态势的细节，如雷达图、地理信息图、关联关系图、威胁路径图、态势图等。

5.5.2 专题态势展示

5.5.2.1 资产态势

产品应能对网络内的资产态势进行评估和展示，具体内容如下：

a) 实时获取当前资产的类型和数量；
b) 识别资产的IP地址、所处位置等并进行统计，特别是暴露在互联网的资产；
c) 识别资产的类型、型号、版本号、开放的端口、运行状态等；
d) 标识并展示资产的重要程度；
e) 对资产的安全状况进行分析，包括资产的分值/等级、资产存在的脆弱性类型/数量等。

5.5.2.2 流量态势

产品应能对网络内的流量态势进行评估和展示，具体内容如下：

a) 对所有流量数据进行统计分析，呈现流量分布、流量排名、流量趋势等；
b) 对互联网的流量数据进行统计分析，呈现流量分布、流量排名、流量趋势等；
c) 对特定用户的流量数据进行统计分析，呈现流量分布、流量排名、流量趋势等。

5.5.2.3 运行态势

产品应能对网络内的运行态势进行评估和展示，具体内容如下：

a) 实时呈现网络的拓扑结构，包括资产间连接情况、资产属性等；
b) 展示被监测资产的运行状态，包括但不限于在线情况、CPU及使用情况、内存及使用情况、网络使用情况等。

5.5.2.4 脆弱性态势

产品应能对网络内的脆弱性态势进行评估和展示，具体内容如下：

a) 监测操作系统、Web应用和第三方组件等存在的常见漏洞；
b) 展示存在高危漏洞的资产、漏洞资产分布、漏洞类型分布、漏洞级别分布等；
c) 提供漏洞修复的建议；
d) 识别并指出系统安全配置的脆弱性。

5.5.2.5 攻击态势

产品应能对网络内的攻击态势进行评估和展示，具体内容如下：

a) 实时获取并展示当前网络的攻击情况，包括攻击时间、攻击源IP、目标IP、攻击类型、攻击方式、攻击路线等；
b) 根据采集的数据确定攻击类型分布和攻击时间段分布情况；
c) 评估攻击对资产造成的影响或损害程度；
d) 评估攻击者当前所处的攻击阶段；
e) 展示攻击路径。

5.5.2.6 异常行为态势

产品应能对网络内的攻击态势异常行为进行评估，具体内容如下：

a) 对网络中的实体行为进行分析评估，包括主机操作系统、网络设备、安全设备、数据库、中间件等IT基础设施的行为分析；
b) 对网络内的用户行为进行评估，包括用户行为倾向、访问URL分布、访问情况等；
c) 对网络的异常行为进行评估，实时展现发生异常行为的资产、资产类型分布等行为；
d) 对网络内的业务访问用户行为进行分析，包括访问协议、访问对象、访问情况等；
e) 对用户及实体的异常行为进行告警，包括实体帐号盗用、特权账号异常、数据窃取等。

5.5.2.7 安全事件态势

产品应能对网络内的安全事件态势进行评估和展示，具体内容如下：

a) 根据时间、类型、等级等进行安全事件的展示；
b) 基于安全事件数量、类型、等级、目标IP地址、目标端口、源IP地址、源端口、资产分布等进行安全事件排名。

5.5.3 数据查询

产品应能够根据资产、安全事件、漏洞等相关属性进行数据查询。

5.5.4 统计报表

产品应能够根据数据分析、态势评估的结果生成统计报表，并以通用格式输出。

5.5.5 分析报告

产品应能根据数据分析结果生成分析报告，并能够以通用格式输出，分析报告应包含以下内容：

a) 网络总体安全状况；
b) 网络中重要资产或高风险等级资产的安全状况；
c) 根据分析结果提供修补建议；
d) 根据数据挖掘分析得到的知识，提供预测性信息。

5.5.6 安全告警

产品应能针对以下安全事件，进行告警：

a) 触发安全告警策略的事件，如高危险级别的事件等；
b) 关联分析结果表明网络中某一资产存在风险；
c) 异常行为分析结果表明网络中存在入侵者的行为或合法用户的异常行为；

d) 潜在危害分析结果表明网络中存在潜在危害；
e) 对于高频发生的相同告警事件进行合并告警，避免出现告警风暴；
f) 告警事件内容至少包括：日期时间、安全事件类型、级别、告警发生次数等。

5.6 安全管理

5.6.1 安全策略管理

产品应为授权管理员提供以下安全策略管理的功能：
a) 采集策略、安全事件告警策略、监控策略等安全策略的集中管理；
b) 对安全策略的自定义设置。

5.6.2 安全事件管理

产品应为授权管理员提供以下安全事件管理的功能：
a）安全事件必须包含发生时间、IP地址、区域、事件类型、数量和危害等级等信息；
b）根据安全事件的起因、表现、结果等对事件进行分类；
c）根据安全事件发生后的危害程度、影响范围等因素对事件进行分级。

5.6.3 知识库管理

产品应为授权管理员提供以下知识库管理的功能：
a) 知识库的增加、删除、修改和导入，对知识库进行动态维护；
b) 对知识库的类型和字段等进行自定义。

5.6.4 时间同步

如产品由多个组件组成，应提供时间同步功能，保证产品组件间时间的一致性。

5.6.5 多级部署

产品应支持分布式多级方式部署。

5.6.6 开放接口

产品应至少提供一个标准的、开放的接口，能按照该接口的规范为第三方产品或系统编写相应的程序模块，以便共享信息或规范化联动。

5.7 自身安全

5.7.1 标识与鉴别

5.7.1.1 用户标识

产品应为用户提供唯一的身份标识，同时将用户的身份标识与该用户的所有可审计事件相关联。

5.7.1.2 用户鉴别

产品应提供用户鉴别的功能，包括：
a) 在用户请求访问产品时，进行身份鉴别；
b) 若采用口令鉴别机制，需对口令进行鉴别信息复杂度校验；
c) 采用两种或两种以上的组合鉴别方式；

d) 鉴别数据不能被未授权查阅和修改。

5.7.1.3 超时锁定

产品应具有访问超时锁定的功能，在设定的时间段内用户没有任何操作的情况下终止会话，需要再次进行身份鉴别才能重新操作。

5.7.1.4 鉴别失败处理

当用户连续鉴别失败达到设定次数后，系统应采取措施阻止用户的进一步请求。

5.7.2 角色管理

产品应提能针对不同角色设定不同的访问权限，并按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，形成相互制约关系。

5.7.3 远程管理

若产品提供远程管理功能，应采取以下措施保证远程管理安全：

a) 对远程管理信息进行保密传输；

b) 对远程登录主机的地址进行限制。

5.7.4 数据传输安全

若产品组件间通过网络进行通讯，产品应对组件间相互传输的数据进行保护，保证数据在传送过程中的保密性和完整性。

5.7.5 自身审计

5.7.5.1 审计日志生成

产品应能对以下事件生成审计日志：

a) 管理员的登录事件，包括成功和失败；

b) 因鉴别尝试不成功的次数达到设定值，导致的会话连接终止；

c) 对安全策略的相关操作；

d) 对安全事件的相关操作；

e) 对知识库的相关操作；

f) 对存储的数据的删除和备份操作；

g) 对前端采集源的相关操作；

h) 对通过主动方式采集数据的前端采集源的策略下发、时钟校准、状态变更等操作；

i) 对安全角色进行增加，删除和属性修改的操作；

j) 管理员的其他操作。

应在每一条审计日志中记录事件发生的日期、时间、用户标识、事件描述和结果。若产品提供远程管理功能，还应记录远程登录主机的地址。

5.7.5.2 审计日志管理

产品应提供以下审计日志管理功能：

a) 只允许授权管理员访问审计日志；

b) 按条件对审计日志进行查询；

c) 对审计日志进行分析。

5.7.6 系统报警

5.7.6.1 报警事件类型

产品应能对以下系统事件进行报警：

a) 存储空间达到设定值；
b) 用户鉴别失败的次数达到设定值；
c) 授权管理员自定义的其他系统事件。

5.7.6.2 报警消息

产品的报警消息内容应满足以下要求：

a) 为管理员可理解；
b) 至少包括事件发生的日期、时间、事件主体和事件描述。

5.7.6.3 报警方式

产品的报警方式应包含以下方式中的一种或多种：

a) 弹出报警窗口；
b) 发送报警邮件；
c) 发送 Snmp trap 消息；
d) 发送声光电信号；
e) 发送 SMS 短消息。

6 安全保障要求

6.1 开发

6.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a) 与产品设计文档中对安全功能实施抽象描述的级别一致；
b) 描述与安全功能要求一致的产品安全功能的安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 证实产品安全功能能够防止被破坏；
e) 证实产品安全功能能够防止安全特性被旁路。

6.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a) 完全描述产品的安全功能；
d) 描述所有安全功能接口的目的与使用方法；
e) 标识和描述每个安全功能接口相关的所有参数；
f) 描述安全功能接口相关的安全功能实施行为；
g) 描述由安全功能实施行为处理而引起的直接错误消息；
h) 证实安全功能要求到安全功能接口的追溯；

i） 描述安全功能实施过程中，与安全功能接口相关的所有行为；
j） 描述可能由安全功能接口的调用而引起的所有直接错误消息。

6.1.3 实现表示

开发者应提供全部安全功能的实现表示，实现表示应满足以下要求：
a） 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；
b） 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
c） 以开发人员使用的形式提供。

6.1.4 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：
a） 根据子系统描述产品结构；
b） 标识和描述产品安全功能的所有子系统；
c） 描述安全功能所有子系统间的相互作用；
d） 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
e） 根据模块描述安全功能；
f） 提供安全功能子系统到模块间的映射关系；
g） 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；
h） 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
i） 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

6.2 指导性文档

6.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：
a） 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b） 描述如何以安全的方式使用产品提供的可用接口；
c） 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d） 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e） 标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f） 充分实现安全目的所必须执行的安全策略。

6.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：
a） 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b） 描述安全安装产品及其运行环境必需的所有步骤。

6.3 生命周期支持

6.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；
b) 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识配置项；
c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
d) 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变；
e) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致；
f) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

6.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a) 产品、安全保障要求的评估证据和产品的组成部分；
b) 实现表示、安全缺陷报告及其解决状态。

6.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

6.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

6.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

6.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

6.4 测试

6.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；
b) 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

6.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；
b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

6.4.3 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b) 预期的测试结果，表明测试成功后的预期输出；

c) 实际测试结果和预期的一致性。

6.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

6.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗以下攻击行为：

a) 具有基本攻击潜力的攻击者的攻击；

b) 具有增强攻击潜力的攻击者的攻击。

7 等级划分要求

7.1 划分概述

依据网络安全态势感知系统的研发、生产现状及实际应用情况，对安全功能要求和安全保障要求划分基本级和增强级。

7.2 安全功能要求等级划分

网络安全态势感知系统的安全功能要求等级划分如表 1 所示。

表 1 信息技术 网络安全态势感知系统安全功能要求等级划分

安全功能要求		基本级	增强级
数据采集	采集方式	5.1.1 a)、c)	5.1.1
	前端采集源管理	5.1.2 b)	5.1.2
	采集数据类型	5.1.3 a)、b)、d)、e)、f)	5.1.3
数据处理	数据筛选	5.2.1	5.4.1
	数据转换	5.2.2	5.2.2
	数据标识	——	5.2.3
	处理方式	——	5.2.4
数据存储	存储数据格式	5.3.1	5.3.1
	存储数据类型	5.3.2 a)~c)	5.3.2
	存储数据安全保护	5.3.3	5.3.3
	防止存储数据丢失	5.3.4 a)、b)	5.3.4
	存储数据备份	5.3.5 a)	5.3.5
数据分析	安全事件辨别	5.4.1	5.4.1
	安全事件定级	5.4.2	5.4.2

安全功能要求			基本级	增强级
	事件关联分析		5.4.3 a)、b)	5.4.3
	异常行为分析		5.4.4 a)、b)、c)、d)	5.4.4
	潜在危害分析		——	5.4.5
	安全趋势分析		——	5.4.6
展示和告警	整体安全态势展示		5.5.1 a)、d)	5.5.1
	专题态势展示	资产态势	5.5.2.1 a)、b)、c)	5.5.2.1
		流量态势	5.5.2.2 a)	5.5.2.2
		运行态势	——	5.5.2.3
		脆弱性态势	5.5.2.4 a)、b)	5.5.2.4
		攻击态势	5.5.2.5 a)、b)、c)	5.5.2.5
		异常行为态势	5.5.2.6 a)、b)、c)、d)	5.5.2.6
		安全事件态势	5.5.2.7 a)	5.5.2.7
	数据查询		5.5.3	5.5.3
	统计报表		5.5.4	5.5.4
	分析报告		5.5.5 a)、b)、c)	5.5.5
	安全告警		5.5.6 a)、b)、c)、f)	5.5.6
安全管理	安全策略管理		5.6.1	5.6.1
	安全事件管理		5.6.2	5.6.2
	知识库管理		5.6.3	5.6.3
	时间同步		5.6.4	5.6.4
	多级部署		——	5.6.5
	开放接口		5.6.6	5.6.6
自身安全	标识与鉴别	用户标识	5.7.1.1	5.7.1.1
		用户鉴别	5.7.1.2 a)、b)、d)	5.7.1.2
		超时锁定	5.7.1.3	5.7.1.3
		鉴别失败处理	5.7.1.4	5.7.1.4
	角色管理		5.7.2	5.7.2
	远程管理		5.7.3 a)	5.7.3
	数据传输安全		5.7.4	5.7.4
	自身审计	审计日志生成	5.7.5.1	5.7.5.1
		审计日志管理	5.7.5.2	5.7.5.2
	系统报警	报警事件类型	5.7.6.1	5.7.6.1
		报警消息	5.7.6.2	5.7.6.2

安全功能要求			基本级	增强级
		报警方式	5.7.6.3	5.7.6.3
注：基本级应至少具备 5.5.2.1~5.5.2.7 中的 3 项；增强级应至少具备 5.5.2.1~5.5.2.7 项中的 6 项；且每个级别下，需满足对应级别下的子项要求。				

7.3 安全保障要求等级划分

网络安全态势感知系统的安全保障技术要求等级划分如表 2 所示。

表 2 信息技术 网络安全态势感知系统安全保障技术要求等级划分

安全保障要求		基本级	增强级
开发	安全架构	6.1.1	6.1.1
	功能规范	6.1.2 a）～f）	6.1.2
	实现表示	——	6.1.3
	产品设计	6.1.4 a）～d）	6.1.4
指导性文档	操作用户指南	6.2.1	6.2.1
	准备程序	6.2.2	6.2.2
生命周期支持	配置管理能力	6.3.1 a）～c）	6.3.1
	配置管理范围	6.3.2 a）	6.3.2
	交付程序	6.3.3	6.3.3
	开发安全	——	6.3.4
	生命周期定义	——	6.3.5
	工具和技术	——	6.3.6
测试	覆盖	6.4.1 a）	6.4.1
	深度	——	6.4.2
	功能测试	6.4.3	6.4.3
	独立测试	6.4.4	6.4.4
脆弱性评定		6.5 a）	6.5 b）