ICS 35.020
L 70

YD

中华人民共和国通信行业标准

网络安全监控系统技术要求

Technical requirements for network security monitor system

2011-12-20 发布　　2012-02-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：国防科学技术大学、国家计算机网络应急技术处理协调中心中国科学院计算技术研究所。

本标准主要起草人：韩伟红、贾　焰、舒　敏、云晓春、张建锋、刘江宁、黄善伟、李爱平、张永铮、杨树强、周　斌。

网络安全监控系统技术要求

1 范围

本标准规定了互联网安全监控系统的功能要求、性能要求以及接口规范。

本标准适用于计算机网络应急响应组织的互联网安全监控系统，也可供其他相关部门参考使用。

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，仅所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。

YD/T 1039.1-2005 900/1800MHz TDMA数字蜂窝移动通信网短消息中心设备技术要求 第一部分：点对点短消息业务部分

YD/T 1800-2008 信息安全运行管理系统总体架构

YD/T 1827-2008 网络安全事件描述和交换格式

YD/T 2251-2011 国家网络安全应急处理平台安全信息获取接口要求

YD/T 2388-2011 网络脆弱性指数评估方法

YD/T 2389-2011 网络威胁指数评估方法

IETF RFC 2821 简单邮件传输协议(Simple Mail Transfer Protocol)

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统 Information System

用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和。

3.2

安全对象 Security Object

网络安全工作保护的企业网络、设备、应用、数据。安全对象的价值不仅仅包括其采购价值，还包括其受侵害后导致的企业损失。

3.3

安全事件 Security Event

由计算机信息系统或者网络中的各种计算机设备，例如主机、网络设备、安全设备等发现并记录下的各种可疑活动。

3.4

安全事故 Security Incident

计算机信息系统或互联网的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改、泄漏造成系统不能正常运行或者数据机密性、完整性、可用性被破坏的现象。安全事故由一个或多个安全事件构成。

3.5

入侵检测　Intrusion Detection

通过对计算机系统中和互联网的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

3.6

告警　Alert

当攻击或入侵发生时，入侵检测系统向授权管理员发出的紧急通知。

3.7

响应　Response

当攻击或入侵发生时，针对信息系统及存储的数据采取的保护并恢复正常运行环境的行为。

3.8

信息安全运行管理系统　Security Operation Center（SOC）

实现信息安全管理体系(ISMS) 的技术支撑平台。它以信息系统风险管理为核心，为安全运营和管理提供支撑。

4　缩略语

下列缩略语适用于本文件。

IDMEF	Instruction Detection Message Exchange Format	入侵检测消息交换格式
IODEF	Incident Object Description and Exchange Format	事故对象描述与交换格式
ISMS	Information Security Management System	信息安全管理体系
SOC	Security Operation Center	信息安全运行管理系统

5　网络安全监控系统概述

5.1　网络安全监控系统体系结构

网络监控系统体系结构如图1所示，整个系统主要由数据采集模块、知识库、事件集成与分析模块、

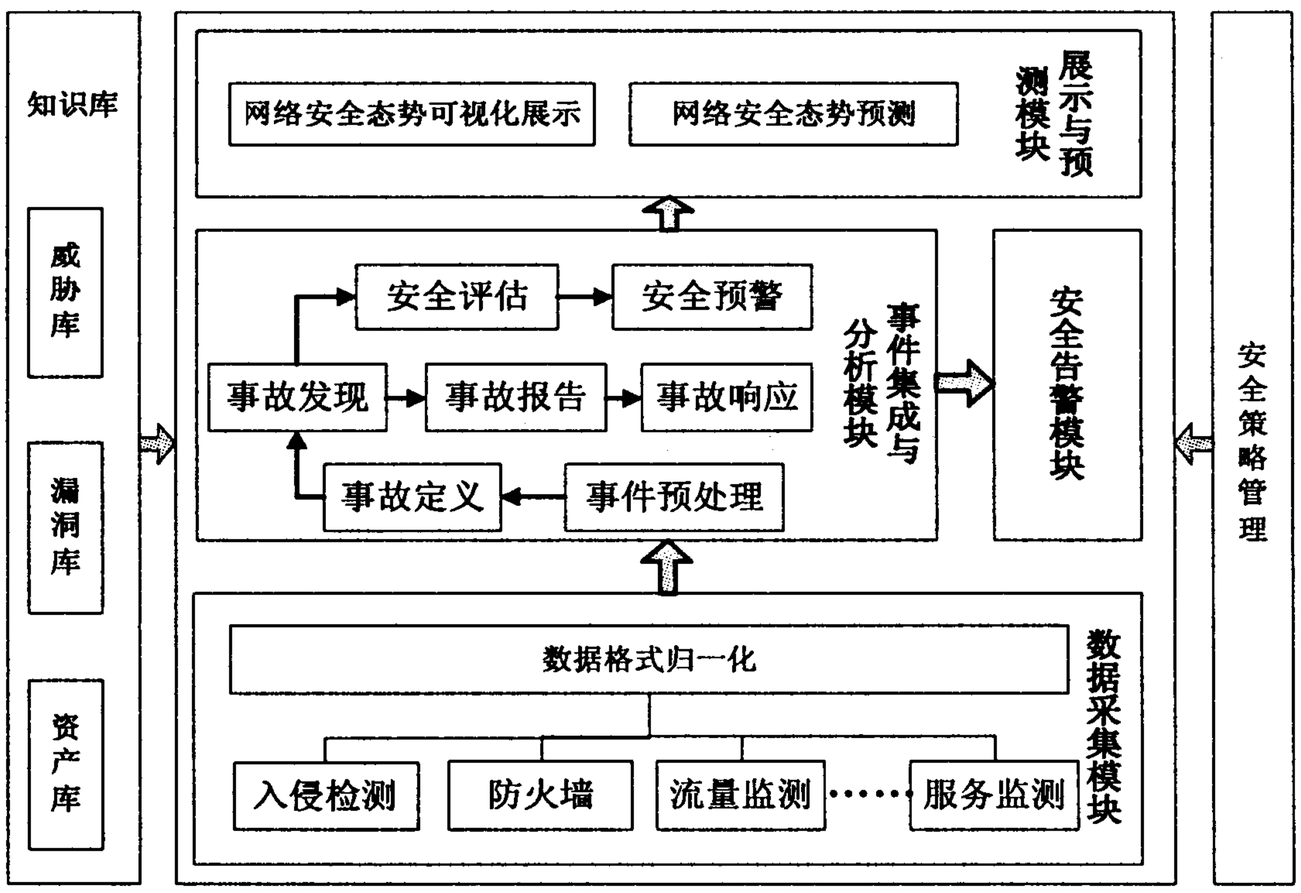

图1　网络安全监控系统功能架构

安全告警模块、展示与预测模块和安全策略管理模块5大模块组成，在本标准的第6章将对每个模块具体的实现提出相应的要求。

5.2 网络安全监控系统整体功能要求

针对大规模、国家级的网络监控系统，网络安全监控系统应具有如下的功能：

——应能够检测到网络上发生的基本攻击入侵行为，对当前网络面临的整体威胁做出评估，给出网络威胁态势和一个发展趋势；

——应对大规模、国家级的网络中的重点服务状态、核心节点状态进行实时监控，以便于及时采取措施；

——应对大规模网络存在的安全漏洞进行挖掘分析，对整体网络存在的脆弱性有一个整体的评估，给出一个网络潜在风险的大小；

——应对大规模网络的网络拓扑进行骨干网络一级的拓扑描述，体现出核心节点之间的关系；

——应能够对网络中的流量进行实时的检测，能够检测出流量的异常变化，根据变化特点给出其风险警报值；

——应提供丰富的展示界面，便于用户从多维度对网络安全态势进行详细的查看，满足用户对网络整体安全态势和局部安全态势的感知需求；

——应提供完善的管理机制，便于管理员对整个网络安全监控系统进行级联式的部署配置，满足大规模网络监控的需求；

——应对网络上发生的安全事件进行实时告警，通过语音、电子邮件等多种手段向管理员发出告警信息。

网络安全监控系统的数据流程见YD/T 1800-2008图2的信息安全运行管理系统数据处理流程。

5.3 网络安全监控系统整体性能要求

5.3.1 有效性要求

网络安全监控系统有效性主要包括以下几个方面：

——检测的精确度。网络安全监控系统对网络攻击检测的准确度是评测系统的主要指标，主要从漏报率、误报率两个方面对系统检测的准确度进行评估。网络安全监控系统应将漏报率和误报率控制在应用许可的范围之内，不能对用户的正常使用产品产生较大的影响。

——态势评估。网络安全监控系统能全面客观地反映出当前网络的安全状态，通过网络安全状态，使得管理者能够对当前所监控网络的安全状况有宏观的了解。

——态势预测。网络安全监控系统能够对未来的网络安全态势做出合理的预测，能够指导管理者提前掌握安全态势的发展趋势，做好防范。

——信息发布。网络安全监控系统能够根据不同的策略要求，实现信息的定向发布，对重大的网络安全事件能够及时有效地通知相关的人员进行处理。

5.3.2 效率要求

5.3.3 延迟时间要求

延迟时间是指从攻击发生到网络安全监控系统产生告警之间的时间，这个时间应该满足用户对系统使用的需求，延迟时间越小越好。

5.3.4 资源占用情况

资源占用情况应从网络安全监控系统的CPU占用率、内存占用率和带宽占用率3个方面综合考虑。在同等有效性下，资源占用率越低越好。

5.3.5 其它性能要求

网络安全监控系统应具有高的可靠性，保证能够防御一定程度的网络攻击，需要考虑各种失效状况：包括单点失效、通信失效等。

6 网络安全监控系统技术要求

6.1 数据采集技术要求

6.1.1 概述

数据采集系统是网络安全监控系统的基础，数据采集应遵循准确性、完备性、实时性、可兼容性等要求。

6.1.2 系统全面性

数据采集系统应从时间、空间、事件3个维度综合考虑数据采集的实施：

——从时间维度来说，数据采集不但应满足网络安全监控系统对实时性的要求，而且应采集到被监控网络每一个时刻的网络安全数据；

——从空间维度来说，针对大规模、国家级的网络，数据采集应采集到关键网络、关键节点、核心设施乃至整个网络的数据；

——从事件维度来说，数据采集应采集到包括流量数据、拓扑数据、服务状态数据、漏洞脆弱性数据以及各种网络攻击威胁数据。

6.1.3 兼容扩展性

数据采集系统的可扩展性应考虑以下几个方面的要求：

——数据采集系统应能够很好地集成现有的一些网络安全产品，能够在系统的部署中很方便的利用现有的主流安全产品和设备的数据；

——数据格式应该遵循统一的标准，数据采集系统需要采集多系统、多平台的数据，因此必须按照统一的格式进行规范化，这样才能更好地便于后续的事件集成与分析,网络安全数据格式应遵循 YD/T 1827-2008 中的要求；

——数据采集应该支持多种方式，包括 syslog、socket、SNMP 等采集方式；

——数据采集应支持分布式可扩展体系结构，能够很容易的集成不同位置的网络安全产品。

6.1.4 集中存储性

为了从宏观上实现对网络安全的监控，数据采集系统应该采用集中式的数据存储，各采集点收集到的数据应实时地发送到统一的数据服务器去存储。

6.2 网络安全事件集成与分析技术要求

6.2.1 数据预处理

数据采集部分由于采用的是分布式可扩展的数据集成技术，因此从各数据点传输过来的数据来自不同的网络节点和不同的安全设备，其收集的数据可能存在很大的重合性，必须对收集到的数据进行过滤去重，便于还原出数据的原来面貌。除此之外，需要对收到的数据按照不同的类型进行分类，这样便于后续数据做进一步的处理。

6.2.2 事故定义

事故定义应详细描述清楚如何由网络安全事件产生网络安全事故，为后面的安全事故发现和挖掘提供详细的专家知识，事故定义应由网络安全专家通过分析网络攻击行为特征和网络攻击原理综合给出。

6.2.3 网络安全事故发现技术

网络安全事故的发现应采取关联分析技术对不同地点、不同时间、不同层次的网络安全告警进行多维度的关联分析，从而挖掘出真实安全事故，识别真实的安全风险。网络安全事件关联分析技术应该具有从最大限度上降低系统误报率和漏报率的能力。网络安全事件通过关联分析产生网络安全事故至少应完成下述的关联分析：

——事件与资产的关联；

——事件与事件的关联；

——事件与漏洞脆弱性的关联。

6.2.4 事故报告

事故报告应能够存储网络安全事故的产生过程，通过事故报告能够反映出该网络安全事故是由哪些网络安全事件作用于哪些资产的哪些漏洞产生的。

6.2.5 事故响应

事故响应应根据产生的安全事故生成相对应的事故响应数据，根据不同的响应策略由网络安全告警模块将生成的事故响应数据定向发布给特定的网络安全管理人员。发布的信息应该包括：

——网络安全事件开始的时间；

——网络安全事件的类型、名称；

——网络安全事件源地址、目的地址、源端口、目的端口；

——网络安全事件的关联过程；

——网络安全事件的处理措施及防护建议。

6.2.6 威胁评估

威胁评估应对现有的安全事故进行评估，从而得到被监控网络的整体网络安全态势，应客观、全面地反映被监控网络的真实安全情况。具体要求见YD/T 2388-2011《网络脆弱性指数评估方法》和YD/T 2389-2011《网络威胁指数评估方法》。

6.2.7 安全预警

安全预警在网络安全监控系统历史数据的基础上，通过综合分析，对下一步的网络安全态势做出一个预期的判断，便于给管理者对未来所面临的安全状况做出一个预先的准备，尽可能减少网络攻击等行为给整体网络运行带来的危害。安全预警至少应从以下几个粒度进行：

——应支持短期预测（分钟级）；

——应支持中期预测（小时级）；

——应支持长期预测（周级）。

6.3 网络态势展示技术要求

6.3.1 事件维度

网络态势展示应从事件维度对各种不同的网络事件态势进行展示，需要根据用户的需求展示出具体某一种网络安全事件的态势情况，事件维度宜覆盖以下几类事件。

——分布式拒绝服务攻击事件；

——木马事件；

——病毒事件；

——僵尸网络事件；

——网页挂马事件；

——恶意域名事件；

——网页篡改事件。

6.3.2 时间维度

网络态势展示应从不同时间刻度对网络安全态势进行展示，具体应支持以下几个时间维度：

——应支持实时级、小时级、天级的网络安全态势展示；

——应支持现有数据同往年同期的数据比较展示；

——应支持现有数据同上几个月的数据比较展示；

——应支持分钟级、小时级、周级的网络安全态势预测展示。

6.3.3 空间维度

对于一个大规模的、国家级的网络安全监控系统，应按照网络的层次结构对不同规模的网络态势进行展示，应支持国家级、省级及市县级的网络安全态势展示。

6.4 安全告警技术要求

安全告警就是要对网络安全事件分析产生的重大安全警报进行实时的告警，应支持以下的几种告警方式：

——通过铃声、指示灯产生报警信号；

——通过电子邮件的方式产生报警信号；

——通过手机短消息的方式产生报警信号。

6.5 知识库的管理

6.5.1 知识库构建要求

网络安全监控系统的知识库是进行网络威胁、网络漏洞等识别的基础，应具备完整性、可靠性等特点。知识库应支持基于专家的修改和自动地在线更新功能。应提供接口对现有的一些知识库进行转换。

6.5.2 漏洞库

漏洞库存放标准的漏洞信息，包括漏洞的名称、威胁级别、建议的处置方式等。

漏洞库应支持实时的更新，包括人工更新和网络更新。

漏洞库应支持对现有漏洞库的转换集成。

6.5.3 威胁库

威胁库存放标准的威胁信息，包括威胁的名称、危害性的大小、建议的处置方式等。

7 网络安全监控系统接口要求

7.1 内部接口

7.1.1 数据采集接口

网络安全监控系统应根据YD/T 1827-2008的要求，通过规定的事件描述和交换格式来集成分布式的网络安全检测工具。数据采集为了满足分布式异构集成技术的要求，应符合一定的接口要求，具体的事件描述格式见表1。

表1　网络安全事件格式

数据项名称	名　称	数据类型	是否必须	说　明
Timestamp	时间戳	TIMESTAMP	是	用来标示事件发生的时间
Sensor	探测器	TEXT	是	用来标示是哪个探测器探测的事件
Dev_type	设备类型	TEXT	是	用来标示是哪个设备类型
event_type	事件描述	TEXT	是	用来对检测到事件进行详细的描述
event_type	事件描述	TEXT	是	用来对检测到事件进行详细的描述
Src_ip	源地址	INTEGER	否	检测到威胁发生的源地址
Dst_ip	目的地址	INTEGER	否	检测到威胁发生的目的地址
Src_port	源端口	INTEGER	否	检测到威胁发生的源端口
Dst_port	目的端口	INTEGER	否	检测到威胁发生的目的端口
Priority	优先级	INTEGER	否	该事件的优先级
Reliability	可靠性	INTEGER	否	该事件的可靠性
Risk	危险级别	INTEGER	否	该事件的危险级别
Data	原始信息	TEXT	否	检测到威胁的原始数据包
设备类型参见 YD/T 2251-2011 附录 A.3 设备类型编码方式				

7.1.2　网络告警接口

网络安全告警的数据接口应支持具体使用者提供的告警接口进行实现。电子邮件接口应符合IETF RFC 2821,用于网络安全告警的电子邮件通知。短信息告警应符合YD/T 1039.1-2005。

7.2　外部接口

为了实现大规模、层次式的网络安全监控，各个网络安全监控系统应支持标准的IODEF接口，通过标准接口实现上下级网络安全监控系统之间的数据交换。实现外部接口的要求见YD/T 2251-2011中的9.2节。

中华人民共和国
通信行业标准
网络安全监控系统技术要求
YD/T 2387-2011
*
人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061
宝隆元（北京）印刷技术有限公司印刷
*
开本：880×1230 1/16 2012年1月第1版
印张：1.25 2012年1月北京第1次印刷
字数：28千字
ISBN 978-7-115-2448/12-26
定价：15元