编号：FGBGJ[2013]1965CPFA-02

2013 年国家信息安全专项
高级可持续威胁（APT）安全监测产品
测评方案

编制：_____

审核：_____

批准：_____

2014-1-1 发布　　2014-1-15 实施

公安部计算机病毒防治产品检验中心

目　　录

1. 测评依据

《国家发展改革委办公厅关于组织实施2013年国家信息安全专项有关事项的通知》（发改办高技[2013]1965号）

该项目所对应的国家/行业标准

GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法（第三级）

GB/T 25069－2010 信息安全技术 术语

GB/T 18336-2008 信息技术 安全技术 信息技术安全性评估准则（EAL3）

GA 243-2000 计算机病毒防治产品评级准则

公信安[2013]748号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）

2. 测试环境

高级可持续威胁（APT）安全监测产品是一种网络设备，通常以并联方式接入网络，能够实时监测网络环境中的高级可持续威胁（APT）事件和传统的网络病毒传播事件，能够精确定位威胁和病毒的来源。设备能够通过管理端口实现网络远程管理，并提供详细的监测日志信息。

2.1. 功能测试环境拓扑结构图

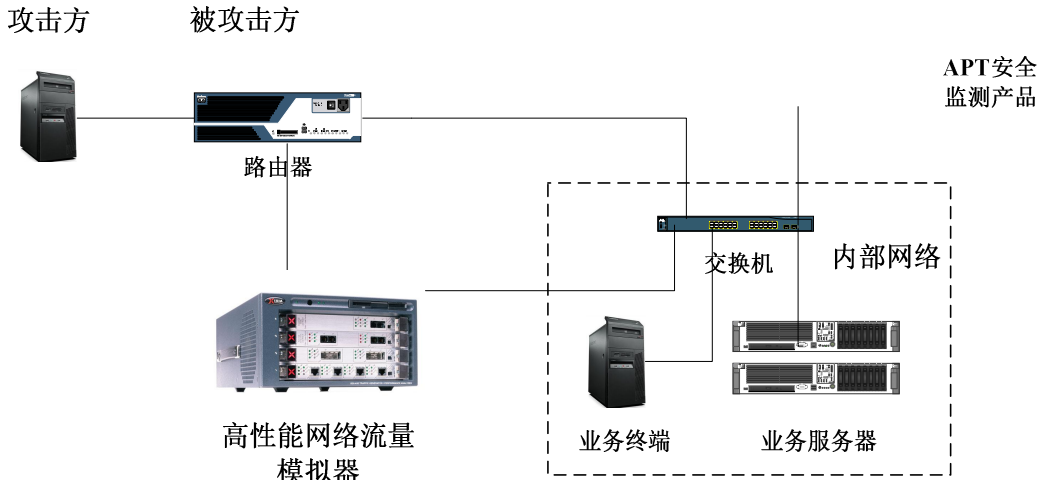

图 1　功能测试环境图

2.2. 性能测试环境拓扑结构图

图 2　性能测试环境图

2.3. 测试设备说明

根据上图所述的测试环境结构图，本节对所需的测试设备做一些说明。

表 1 测试设备说明

设备名称	说明	备注
路由器	用于搭建模拟网络环境，负责网络地址转换，传输速率10Gbps，支持 IPv4/IPv6 双栈、隧道	
交换机	用于搭建模拟网络环境，24 个 10 Gb SFP+ (10 Gb/1 Gb) 端口，转发率>960 Mbps,背板带宽>640Gbps	
网络分流器	支持 10Gbps	
业务服务器	用于模拟被攻击方内部业务系统，如 Web、FTP、DNS、MAIL 等基础服务。Intel Xeon E5-2650 x 2；内存：32G DDR3；硬盘：300G SAS x 8；网卡：四端口千兆网卡	
测试 PC 机	用于模拟攻击方和被攻击方	

	PC 机，Intel i5 处理器，4G 内存，500G 硬盘。	
高性能网络流量模拟器	全面支持 IPv4/IPv6，支持每秒 50 万 TCP 新建连接，并发 1500 万 TCP 连接；能够模拟多种病毒、多种攻击种类和类型、异常网络流量；病毒库内提供的供给种类>28000 种，攻击库内的供给种类>6000 种；支持批量自定义病毒库上传和产生；业务和协议数量能够支持仿真 200 种以上；内嵌真实环境流量场景，包括：典型的政府网络，金融机构网络、企业网络等。	

3. 测评前准备

3.1. 测评人员准备

3.1.1. 知识技能

在进行高级可持续威胁（APT）安全监测产品测评之前，测评人员必须学习并熟练掌握如下知识、软件及工具：

⑴ 计算机病毒、木马等恶意程序相关基础知识；

⑵ 软件漏洞相关基础知识；

⑶ 高级持续性威胁（APT）相关基础知识；

⑷ APT 安全监测产品、IDS、VDS 产品的基本概念、原理和用途；

⑸ Windows Server 2008、Windows 7 Professional 和 Redhat Linux 9.0 等操作系统；IIS 6.0 及操作系统相关服务；

⑹ 基于 IPv6 的 TCP/IP 协议的网络拓扑构建及分析；

⑺ DNS、HTTP、FTP、SMTP、POP/POP3、TELNET 等应用层协议和服务的原理及基本配置；

⑻ 流量仿真设备测试仪和威胁流量仿真设备测试仪的使用；

⑼ VMware、VirtualBox 等常用虚拟化软件的使用；

⑽ Metasploit、BackTrack 等工具的使用。

3.1.2. 测试环境准备

在检测开始之前，测评人员必须做好如下准备：

⑴ 根据 2.3 测试组件说明准备好检测所需要的硬件设备，并为之安装好相应的操作系统及软件；

⑵ 根据 2.1 、2.2 检测环境网络拓扑结构图构建好测试网络，并为之配好相应的 IP 地址等网络属性以及需要的服务；

⑶ 以送检产品分发和操作文档为依据，安装送检样品；

⑷ 确认送检产品是否能正常运行，准备工作完成，可以开始检测。

3.1.3. 标准准备

在检测时，测评人员尚需准备好如下标准，并通读标准，基本掌握标准内容，以便查询。

⑴ GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）

⑵ GB/T 25069－2010 信息安全技术 术语

⑶ GB/T 18336-2008 信息技术 安全技术 信息技术安全性评估准则（EAL3）

⑷ GA 243-2000 计算机病毒防治产品评级准则

⑸ 公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）

3.1.4. 测试用例的编写

在测试用例编写时，有如下原则与方法可以参考：

⑴ 测评人员需仔细研究标准含义，分析在实际情况中可能出现的每一种情况，然后采用等价类划分的方法做较全面的覆盖测试；

⑵ 对具有临界值的测试应尽可能采用边界值的方法进行测试；

⑶ 依据平时测评的经验，可以用错误推测法追加一些测试用例；

⑷ 建议根据业务流的规律，整理每条业务流所对应的标准功能点，依据业务流来进行检测。

3.2. 送检厂商准备

在测评开始之前，送检厂商必须做好如下准备：

⑴ 准备好全部技术文档及资料；

⑵ 准备好送检系统硬件设备及软件安装程序，并在送检之前确认系统版本是否正确，硬件工作是否正常；

⑶ 若必要，厂商需提供测试所需的实现产品功能的外围设备；

⑷ 为检测需要，厂商尚需提供本测评方案第 4 章中“文档要求”所规定的全部文档，并准备文档索引表，标明该部分“文档要求”对应所提供的具体文档名或哪本文档的第几页。

4. 测评方法及结果判定

4.1. 产品对应标准的内容（必测项）

本测评方案中要求项与依据标准的对应关系如表 4.1 所示。

表 4.1 产品测评标准对应表

本测评方案		对应标准		
要求项编号	要求项	要求项编号	要求项	标准名称
4.1.1.1.1	数据收集	6.1.1.1.1	数据收集	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.1.1.2	协议分析	6.1.1.1.2	协议分析	
4.1.1.1.3	行为监测	6.1.1.1.3	行为监测	
4.1.1.1.4	流量监测	6.1.1.1.4	流量监测	
4.1.1.1.5	异常流量处理	8.6	异常流量处理	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.1.2.1	防逃逸	6.2.1.1.1	防躲避能力	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.1.5	逃避检测防护	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.1.2.2	事件合并	6.2.1.1.2	事件合并	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.1.2.3	事件关联	6.3.1.1.1	事件关联	
4.1.1.3.1	威胁告警	6.1.1.3.1	安全告警	
4.1.1.3.2	告警方式	6.1.1.3.2	告警方式	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.3.5	告警方式	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.1.4.1	管理界面	6.1.1.4.1	图形界面	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.1.4.2	策略配置	6.1.1.4.4	策略配置	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）

		8.2.1	策略自定义	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.1.4.3	产品升级	6.1.1.4.5	产品升级	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.8	升级能力	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.1.5.1	事件记录	6.1.1.5.1	事件记录	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.3.6	事件记录	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.1.5.2	事件可视化	6.1.1.5.2	事件可视化	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.1.5.3	报告生成	6.1.1.5.3	报告生成	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.4.1	报表生成	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.1.5.4	报告查阅	6.1.1.5.4	报告查阅	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.1.5.5	报告输出	6.1.1.5.5	报告输出	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.4.2	报表导出	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）

4.1.1.5.6	报告定制	6.1.1.6.1	报告定制	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.2.1.1	用户鉴别	6.1.2.1.1	用户鉴别	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.10.2.1	基本鉴别	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.2.1.2	鉴别失败的处理	6.1.2.1.2	鉴别失败的处理	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.10.2.3	鉴别失败处理	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.2.1.3	超时设置	6.2.2.1.1	超时设置	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.2.1.4	会话锁定	6.2.2.1.2	会话锁定	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.2.1.5	多鉴别机制	6.3.2.1.1	多鉴别机制	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.10.2.1	基本鉴别	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.2.1.6	鉴别数据保护	6.3.2.1.2	鉴别数据保护	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.10.2.2	鉴别数据保护	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）

4.1.2.2.1	用户角色	6.1.2.2.1	用户角色	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.2.2.2	用户属性定义	6.2.2.2.1	用户属性定义	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
		8.10.1.1	属性定义	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.2.2.3	安全行为管理	6.2.2.2.2	安全行为管里	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.2.2.4	安全属性管理	6.3.2.2.1	安全属性管理	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.2.3.1	安全数据管理	6.1.2.3.1	安全数据管理	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.11.1	安全功能管理	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.2.3.2	数据存储告警	6.3.2.3.1	数据存储告警	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.3.6	事件记录	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.2.4.1	审计数据生成	6.2.2.3.1	审计数据生成	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.12.1	审计日志生成	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）

4.1.2.4.2	审计数据可用性	6.2.2.3.2	审计数据可用性	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.12.1	审计日志生成	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.2.4.3	审计查阅	6.2.2.3.3	审计查阅	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.12.3	审计日志管理	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.2.4.4	受限的审计查阅	6.2.2.3.4	受限的审计查阅	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		8.12.3	审计日志管理	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）
4.1.2.5.1	通信保密性	6.1.2.4.1	通信完整性	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
		13.2.28	远程保密传输	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.2.5.2	升级安全	6.1.2.4.3	升级安全	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.2.6.1	自我隐藏	6.1.2.5.1	自我隐藏	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）
4.1.2.6.2	自我检测	6.2.2.4.1	自我监测	GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法 （第三级）

		8.7	故障信息告警	公信安[2013]748 号 网络病毒监控系统（VDS）安全技术要求和测试评价方法（试行） （增强级）

4.1.1. 安全功能要求

4.1.1.1. 数据探测功能要求

4.1.1.1.1. 数据收集

测评依据：送检产品应具有实时获取被监控网络内的数据包和数据流的能力。获取的数据包和数据流应足以进行传统计算机病毒和高级持续性威胁（APT）检测和分析。

文档要求：

应提供文档说明产品的数据收集功能。

测评方法：

要求开发商以文档形式提交产品所能进行的网段内数据包获取的能力描述。检测员判断此产品是否提供了足够的证据，表明了产品能够获取威胁数据。

预期结果：

如果产品或产品文档没有提供足够的描述证据，则本项判为不合格。

4.1.1.1.2. 协议分析

测评依据：

送检产品至少应监视基于以下协议的事件：IP、ARP、TCP、UDP、RPC、HTTP、FTP、TFTP、IMAP、DNS、SMTP、POP3、NETBIOS、IRC、MSRDP、PcAnyWhere、TeamViewer以及国内常用的WebMail协议等。

文档要求：

应提供文档说明产品支持的协议。

测评方法：

检测员根据在 4.1.1.1.1 中已经获取的数据，检测产品是否能够按照要求的协议进行分析（攻击样本根据开发商提供的描述，在样本库中中随机抽取，）。

预期结果：

如果产品不能正确监视所要求协议，则本项判为不合格。

4.1.1.1.3. 行为监测

测评依据：送检产品至少应监视以下攻击行为：木马后门攻击、缓冲区溢出攻击、网络蠕虫攻击、挂马网页攻击、钓鱼邮件攻击、钓鱼网站攻击、恶意文档攻击等。

文档要求：

应提供文档说明产品的支持监测的攻击行为。

测评方法：

要求开发商以文档形式提交产品所有策略覆盖的入侵分类详细描述，分类按照要求类型进行。检测员判断此产品是否提供了足够的证据，以表明产品能够监视所要求的攻击行为。

预期结果：

如果产品或产品文档没有提供足够的描述证据，则本项判为不合格。

4.1.1.1.4. 流量监测

测评依据：

送检产品应监视整个网络或者某一特定协议、地址、端口的报文流量和字节流量。

文档要求：

应提供文档说明产品的流量监测功能。

测评方法：

检测员检测产品显示中或报告生成结果中是否具备标准所要求的流量监测能力。

预期结果：

如果产品不能正确监视所要求流量，则本项判为不合格。

4.1.1.1.5. 异常流量处理

测评依据：

送检产品应对碎片包、畸形报文等异常流量进行有效处理。

文档要求：

应提供文档说明产品的异常流量处理功能。

测评方法：

要求开发商以文档形式提交产品异常流量处理功能详细描述，检测员根据描述，使用网络流量模拟仪器模拟异常流量，查看检测产品是否具备异常流量处理功能。

预期结果：

如果产品不能正确处理异常流量，而造成误报、漏报或不能正常工作。则本项判为不合格。

4.1.1.2. 威胁分析功能要求

4.1.1.2.1. 防逃逸

测评依据：

送检产品应能发现躲避或欺骗检测的行为，如IP碎片重组，TCP流重组，协议端口重定位，URL字符串变形，shell代码变形，文件压缩，文件加密，文件加壳，文件内嵌，虚拟机或沙箱识别等。

文档要求：

应提供文档说明产品的防逃逸能力。

测评方法：

检测员检测产品是否能够按照要求对收集数据进行躲避或欺骗分析（使用网络流量模拟器、常用的文件变形、文件加密工具等进行模拟，并在威胁样本库中抽取具有反虚拟机或反沙箱属性的样本进行测试）。

预期结果：

如果产品不能分析出任何躲避或欺骗检测的行为，则本项判为不合格。

4.1.1.2.2. 事件合并

测评依据：

送检产品应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。

文档要求：

应提供文档说明产品的安全事件处理能力。

测评方法：

检测员检测产品是否能够提供视图，按照要求对相同安全事件数据进行合并告警（使用网络流量模拟仪器进行样本发送模拟）。

预期结果：

如果产品不能将事件进行合并，则本项判为不合格。

4.1.1.2.3. 事件关联

测评依据：

送检产品应具有把不同类型攻击事件关联起来，发现隐含的复合式高级持续性威胁攻击的能力。

文档要求：

应提供文档说明产品安全事件的关联分析能力。

测评方法：

要求开发商以文档形式提交产品事件关联功能描述，至少包括：关联算法，以及测试工具、测试环境和测试步骤等预测产品这方面的内容，检测人员根据文档模拟关联事件。

预期结果：

如果产品不能关联，或与厂商描述的不同，则本项判为不合格。

4.1.1.3. 威胁响应功能要求

4.1.1.3.1. 威胁告警

测评依据：

当系统检测到威胁事件时，应自动采取相应动作以发出威胁警告。

文档要求：

应提供文档说明产品的威胁告警功能。

测评方法：

检测员根据在 4.1.1.1.1 中已经获取的数据，检测产品是否能够按照要求对分析后的入侵行为或攻击事件产生相应的动作，至少包括威胁警告（威胁样本根据开发商提供的描述在威胁样本库中随机抽取，测试产品是否对入侵行为或攻击事件产生安全警告）。

预期结果：

如果产品不能对任何威胁事件产生安全警告，则本项判为不合格（安全警告必须有警示作用，日志记录不能代替）。

4.1.1.3.2. 告警方式

测评依据：

告警可以采取屏幕实时提示、E-mail告警、声音告警等几种方式。

文档要求：

应提供文档说明产品的威胁告警方式。

测评方法：

检测员根据在 4.1.1.3.1 中的方法，检测产品是否能够按照要求提供不同的安全警告方式。

预期结果：

如果产品不能提供任一标准要求的安全警告方式，则本项判为不合格。

4.1.1.4. 管理控制功能要求

4.1.1.4.1. 管理界面

测评依据：

送检产品应提供友好的用户界面用于管理、配置。管理配置界面应包含配置和管理产品所需的所有功能。

文档要求：

应提供文档说明产品管理界面的功能和使用方法。

测评方法：

检测员检测产品是否提供了简单易用的管理功能（例如中文界面、即时帮助、策略批操作、策略衍生操作、策略组、实时日志及时更新、日志排序，日志字段排序、荧屏过滤等），是否提供了所有配置管理功能。

预期结果：

只要产品提供以上简易管理实例中的任何一项功能，且产品功能不需要脱离产品界面，则本项判为合格。

4.1.1.4.2. 策略配置

测评依据：

送检产品应提供方便、快捷的系统策略配置方法和手段。

文档要求：

应提供文档说明产品的策略配置描述。

测评方法：

检测员检测产品是否提供了方便、快捷的策略配置管理功能（例如中文界面、即时帮助、策略批操作、策略衍生操作、策略组），是否提供了所有配置管理功能。

预期结果：

只要产品提供以上简易实例中的任何一项功能，则本项判为合格。

4.1.1.4.3. 产品升级

测评依据：

送检产品应具有及时更新、升级产品和事件库的能力。

文档要求：

应提供文档说明产品的升级能力。

测评方法：

检测员检测产品是否能够进行产品版本或特征库升级（自动或者手动都可以，但重新安装新版本产品不能记做升级功能），核查特征库是否有新增的内容或产品版本是否更新。

预期结果：

如果产品不提供此项功能，或者产品或特征库不能正常更新（包括不能更新和更新后产品不能正常运行），则本项判为不合格。

4.1.1.5. 事件记录和报告

4.1.1.5.1. 事件记录

测评依据：

送检产品应记录并保存检测到的威胁事件。

威胁事件信息应至少包含以下内容：事件发生时间、源地址、目的地址、危害等级、事件详细描述等。

文档要求：

应提供文档说明产品的事件记录能力。

测评方法：

检测员设置威胁监测策略，模拟威胁攻击事件产生记录。检测产品记录的信息内容是否至少包含：事件发生时间、源地址、目的地址、危害等级、事件详细描述。

预期结果：

如果产品漏记了以上任一项目，则本项判为不合格。

4.1.1.5.2. 事件可视化

测评依据：

用户应能通过管理界面实时清晰地查看威胁事件。

文档要求：

应提供文档说明产品的事件可视化。

测评方法：

检测员检测产品是否提供了简单易用的管理界面查看功能（例如实时日志及时更新、日志排序，日志字段排序、条件过滤等）。

预期结果：

只要产品提供以上例子中的任何一项功能，则本项判为合格。

4.1.1.5.3. 报告生成

测评依据：

送检产品应能生成详尽的检测结果报告。

文档要求：

应提供文档说明产品的报告生成能力。

测评方法：

检测产品是否提供了详尽的结果报告，比如：包括事件发生时间、源地址、目的地址、危害等级、事件详细描述。

预期结果：

如果产品报告不能生成这些项目或者报告内容同检测结果不符的，则本项判为不合格。

4.1.1.5.4. 报告查阅

测评依据：

送检产品应具有全面、灵活地浏览检测结果报告的功能。

文档要求：

应提供文档说明产品的报告查阅能力。

测评方法：

检测产品是否提供了全面、灵活的结果报告浏览功能，至少提供报告浏览功能，能够根据报告的不同属性进行结果变换浏览。

预期结果：

如果产品报告不提供报告浏览功能，则本项判为不合格。

4.1.1.5.5. 报告输出

测评依据：

检测结果报告应可输出成方便用户阅读的文本格式，如字处理文件、HTML 文件、文本文件等。

文档要求：

应提供文档说明产品的报告输出能力。

测评方法：

检测产品是否能够将报告输出为方便用户阅读的文本格式，例如： doc、pdf、xls、html、xml、txt 等等。

预期结果：

如果产品不能输出或者输出时信息内容与原始数据库数据不同，则本项判为不合格。

4.1.1.5.6. 报告定制

测评依据：

系统应支持授权管理员按照自己的要求修改和定制报告内容。

文档要求：

应提供文档说明产品的报告定制能力。

测评方法：

检测产品是否提供给用户参与定制(用户可以自定义报告的范围或者结构)报告的功能，比如：用户可以选择特定字段范围生成分类报告(时间，类型，风险）报告。

预期结果：

如果产品没有提供用户自定制报告功能，则本项判为不合格。

4.1.2. 产品安全要求

4.1.2.1. 身份鉴别

4.1.2.1.1. 用户鉴别

测评依据：

送检产品应在用户执行任何与安全功能相关的操作之前对用户进行鉴别。

文档要求：

应提供文档说明产品的用户鉴别功能。

测评方法：

检测产品在提供任何与安全功能相关的管理功能之前是否都对管理员进行身份鉴别。

预期结果：

如果产品在执行管理功能之前不要求管理员进行身份鉴别，则本项判为不合格。

4.1.2.1.2. 鉴别失败的处理

测评依据：

当用户鉴别尝试失败连续达到指定次数后，系统应锁定该帐号，并将有关信息生成审计事件。最多失败次数仅由授权管理员设定。

文档要求：

应提供文档说明产品的鉴别失败处理能力。

测评方法：

检验员模拟以管理员身份连续失败登录产品，直至超过最大失败次数（此次数可固定也可设置）。检验产品是否阻止管理员继续进行鉴别，锁定帐号或者使帐号失效一段时间。

预期结果：

如果产品没有提供这种功能，则本项判为不合格。

4.1.2.1.3. **超时设置**

测评依据：

应具有管理员登录超时重新鉴别功能。在设定的时间段内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够重新管理产品。最大超时时间仅由授权管理员设定。

文档要求：

应提供文档说明产品的超时设置功能。

测评方法：

检测员模拟登录超时，检查产品是否需要重新登录；检测员检测产品中是否只为授权管理员提供了最大超时时间限制权限。

预期结果：

如果产品不提供超时登录，或不能由且只由授权管理员设置最大超时时间，则本项判为不合格。

4.1.2.1.4. **会话锁定**

测评依据：

送检产品应允许用户锁定自己的交互会话，锁定后需要再次进行身份鉴别才能够重新管理产品。

文档要求：

应提供文档说明产品的会话锁定功能。

测评方法：

检测员检测产品是否提供了交互会话锁定功能。

预期结果：

如果产品不具备此项功能，或运行不正常，则本项判为不合格。

4.1.2.1.5. **多鉴别机制**

测评依据：

送检产品应提供多种鉴别方式，或者允许授权管理员执行自定义的鉴别措施，以实现多重身份鉴别措施。多鉴别机制应同时使用。

文档要求：

应提供文档说明产品的多鉴别机制。

测评方法：

要求开发商以文档形式提交产品提供的鉴别功能描述,至少包括：鉴别方式的种类、鉴别机制、或鉴别的实现，以及测试工具、测试环境和测试步骤等预测产品这方面的内容，检测人员根据文档应用多鉴别机制，测试鉴别时多种机制的执行情况。

预期结果：

如果产品不提供多鉴别机制,或实现的与厂商描述不同,则本项判为不合格。

4.1.2.1.6. 鉴别数据保护

测评依据：

应保护鉴别数据不被未授权查阅和修改。

文档要求：

应提供文档说明产品的鉴别数据保护能力。

测评方法：

要求开发商以文档形式提交产品鉴别数据保护的功能描述,至少包括：保护方法（比如使用加密手段，鉴别数据用户不可直接操作等）、保护的实现，以及测试工具、测试环境和测试步骤等预测产品这方面的内容，检测人员根据文档模拟非授权查阅或修改鉴别数据。

预期结果：

如果产品的鉴别数据能够被未授权查阅或修改，则本项判为不合格。

4.1.2.2. 用户管理

4.1.2.2.1. 用户角色

测评依据：

系统应设置多个角色，并应保证每一个用户标识是全局唯一的。

文档要求：

应提供文档说明产品的用户角色。

测评方法：

产品必须至少提供两类用户角色，其中至少有一类为管理员角色，并且保证此两类用户角色并不相同。检测员检测此两类用户角色是否不同，且是否有一类属于管理员角色；检测员尝试设置具有相同用户标识（即用户名，因为它与日志记录相关）的用户。

预期结果：

如果产品不提供两类以上（包括两类）用户角色的设置功能，或两类用户角色都相同，或没有一类属于管理员角色，或可以设置具有相同用户标识的用户（不论角色如何），则本项判为不合格。

4.1.2.2.2. 用户属性定义

测评依据：

送检产品应为每一个用户保存安全属性表，属性应包括：用户标识、鉴别数据（如密码）、授权信息或用户组信息、其它安全属性等。

文档要求：

应提供文档说明产品的用户属性定义。

测评方法：

检测员检测系统是否将所有以上字段作为安全属性保存（通过分析产品数据库中的内容或核实用户管理界面内容）。

预期结果：

如果产品不保存，或运行不正常，则本项判为不合格。

4.1.2.2.3. 安全行为管理

测评依据：

送检产品应仅限于已识别了的指定的授权角色对产品的功能具有禁止、修改的能力。

文档要求：

应提供文档说明产品的用户权限限制。

测评方法：

检测员检测系统是否提供了产品功能屏蔽功能，例如：可以通过界面设置将功能项分配给不同的授权角色。

预期结果：

如果产品不具备此项功能，或运行不正常，则本项判为不合格。

4.1.2.2.4. 安全属性管理

测评依据：

送检产品应仅限于已识别了的指定的授权角色对指定的安全属性进行查询、修改、删除、改变其默认值等操作。

文档要求：

应提供文档说明产品的用户权限限制。

测评方法：

检测员检测系统是否提供了产品功能屏蔽功能，例如：可以通过界面设置将功能项分配给不同的授权角色。

预期结果：

如果产品不具备此项功能，或运行不正常，则本项判为不合格。

4.1.2.3. 事件数据安全

4.1.2.3.1. 安全数据管理

测评依据：

送检产品应仅限于指定的授权角色访问事件数据，禁止其它用户对事件数据的操作。

文档要求：

应提供文档说明产品的事件数据访问限制。

测评方法：

产品必须至少提供用户角色分级（至少两级），保证此分级用户对事件数据的管理权利范围各不相同。

预期结果：

如果产品没有提供用户角色分级，或分级后管理权利范围全部相同的，则本项判为不合格。

4.1.2.3.2. 数据存储告警

测评依据：

系统应在发生事件数据存储器空间将耗尽等情况时，自动产生告警，并采取措施避免事件数据丢失。产生告警的剩余存储空间大小应由用户自主设定。

文档要求：

应提供文档说明产品的数据存储器空间耗尽处理能力。

测评方法：

开发商提供支持文档（文档包括：报警措施的实现描述；对空间耗尽的时间估计）。在审计记录存储到一定空间时(空间可以默认或自定义)，产品必须采取措施(例如：报警，回滚等)。

预期结果：

如果产品不提供这功能，则本项判为不合格。

4.1.2.4. 安全审计

4.1.2.4.1. 审计数据生成

测评依据：

应能为下述可审计事件产生审计记录：审计功能的启动和关闭，审计级别以内的所有可审计事件（如鉴别失败等重大事件）等。应在每个审计记录中至少记录如下信息：事件的日期和时间，事件类型，主体身份，事件的结果（成功或失败）等。

文档要求：

应提供文档说明产品的审计数据生成能力。

测评方法：

审计功能的开关记录（明确表明审计功能开关的记录）；任何对鉴别机制的使用（所有使用鉴别机制的状态记录，例如：用户和模块鉴别的成功或失败记录）；每条记录中都必须包括事件时间、事件类型、主体身份和事件结果。

预期结果：

如果不具备以上内容，或者记录内容与实际不符，则本项判为不合格。

4.1.2.4.2. 审计数据可用性

测评依据：

送检产品提供的审计数据的记录方式应便于用户理解。

文档要求：

应提供文档说明产品的审计数据可用性。

测评方法：

检测员检测系统是否提供了便于用户理解的审计数据记录方式，比如提供专用浏览记录工具，提供记录的属性描述。

预期结果：

如果产品不具备此项功能，或运行不正常，则本项判为不合格。

4.1.2.4.3. 审计查阅

测评依据：

送检产品应为授权管理员提供从审计记录中读取全部审计信息的功能。

文档要求：

应提供文档说明产品的审计查阅能力。

测评方法：

检测员检测产品是否能够为不同的用户角色设置不同的审计数据访问权限（至少有两种不同访问审计数据的用户角色）。

预期结果：

如果产品不提供至少两种不同的审计数据访问角色或者在访问审计数据时两种用户角色没有区别，则本项判为不合格。

4.1.2.4.4. 受限的审计查阅

测评依据：

除了具有明确的读访问权限的授权管理员之外，系统应禁止所有其它用户对审计记录的读访问。

文档要求：

应提供文档说明产品的审计查阅限制。

测评方法：

检测员模拟授权人员和非授权人员访问审计数据（主要是读取）。

预期结果：

如果非授权人员能够访问到审计数据，则本项判为不合格。

4.1.2.5. 通信安全

4.1.2.5.1. 通信保密性

测评依据：

送检产品应确保各组件之间传输的数据（如配置和控制信息、告警和事件数据等）不被泄漏或篡改。

文档要求：

应提供文档说明产品的通信保密性。

测评方法：

产品在各组件之间传输数据（如配置和控制信息、告警和事件数据等）时，数据能被正常传输；开发者文档中提供了保证各组件之间通信保密性所采取措施的详细描述，数据在传输过程中不丢失、不被篡改。（列举系统为保证通信完整性所采取的措施：探头、日志服务器、管理员主机、控制台等都要考虑。）

预期结果：

如果产品文档描述不清，或者实际检测时获取明文信息（如：明文审计日志信息），则本项判为不合格。

4.1.2.5.2. 升级安全

测评依据：

系统应确保事件库和版本升级时的通信安全，应确保升级包是由开发商提供的。

文档要求：

应提供文档说明产品的升级安全能力。

测评方法：

要求开发商以文档形式提交升级安全的方法描述。检测员设置产品中对升级服务器识别的项目，尽量伪造服务器，模拟升级，判断此产品是否能够升级。

预期结果：

如果产品文档没有提供足够的证据证明，或产品能够在伪造的服务器上升级，则本项判为不合格。

4.1.2.6. 产品自身安全

4.1.2.6.1. 自我隐藏

测评依据：

送检产品应采取隐藏探测器 IP 地址等措施使自身在网络上不可见，以降低被攻击的可能性。

文档要求：

应提供文档说明产品的自身隐藏能力。

测评方法：

检测员检查产品监测口是否无 IP 地址，使用 RADCOM 串接监测口监听是否有数据包自监测口发出。

预期结果：

如果产品监测口必须设置 IP 地址，或有数据包自监测口发出，则本项判为不合格。

4.1.2.6.2. 自我检测

测评依据：

送检产品应在启动和正常工作时，周期性地、或者按照授权管理员的要求执行自检，以验证产品自身执行的正确性。

文档要求：

应提供文档说明产品的自检能力。

测评方法：

检测员尽可能小地破坏系统资源（比如，执行文件、库文件等）,检查产品是否提供了自检功能。

预期结果：

如果产品不具备此项功能，或运行不正常，则本项判为不合格。

4.2. 发改办高技[2013]1965 号的要求（必测项）

4.2.1. 动态检测

测评依据：

送检产品应具有虚拟机或沙箱执行等动态检测技术的威胁感知功能。

文档要求：

开发商应提供文档说明产品的规模化虚拟机或沙箱执行等动态检测技术的威胁感知功能和威胁分析机制。

测评方法：

检验员判断此产品是否提供了足够的证据（比如能够设置虚拟机或沙箱鉴定参数等）；根据开发商提供的虚拟机或沙箱执行等动态检测技术的威胁分析机制，检测产品是否能够按照要求对威胁样本进行检测（威胁样本根据开发商提供的描述在威胁样本库中随机抽取，测试产品是否分析出威胁事件），并提供包括详细检测过程和结果的记录或报告。

预期结果：

如果产品不能提供证据证明采用了虚拟机或沙箱执行等动态检测技术，或未通过虚拟机或沙箱执行等动态检测技术分析出任何威胁事件，或未能提供包括动态检测过程和结果的记录和报告，则本项判为不合格。

4.2.2. 规模化动态检测能力

测评依据：

送检产品应具备规模化动态检测能力。

文档要求：

开发商应提供文档说明产品具有规模化动态检测能力/机制。

测评方法：

检验员判断此产品是否提供了足够的证据证明具有规模化动态检测能力

（如：能够设置动态扩展虚拟机或沙箱的参数等）；根据开发商提供的规模化动态检测能力和机制，配置和管理多个虚拟机或沙箱一起工作。

预期结果：

如果产品不能提供证据证明具有规模化动态检测能力，或无法配置和管理多个虚拟机或沙箱实现规模化动态检测能力，则本项判为不合格。

4.2.3. 网络文件传输异常行为检测

测评依据：

送检产品应具备对各类设备网络文件传输异常行为检测能力。

文档要求：

开发商应提供文档说明产品具有对各类设备网络文件传输异常行为检测能力及分析机制。

测评方法：

检验员判断此产品是否提供了足够的证据（比如能够设置网络文件传输异常行为检测参数等）；根据开发商提供的网络文件传输异常行为分析机制，模拟网络文件传输异常行为（如：不可信源/目的地址的文件传输行为，包含关键敏感信息的文件传输行为、异常可执行程序的文件传输行为等），检测产品是否能够按照要求对网络文件传输异常行为进行检测。

预期结果：

如果产品不能提供证据证明具有网络文件传输异常行为检测能力，或未分析出任何网络文件传输异常行为，则本项判为不合格。

4.2.4. 漏洞利用行为检测

测评依据：

送检产品应具备对各类漏洞利用行为的检测能力。

文档要求：

开发商应提供文档说明产品具有对各类漏洞利用行为的检测能力及分析机制。

测评方法：

检验员判断此产品是否提供了足够的证据（比如能够设置漏洞利用行为检测参数等）；根据开发商提供的漏洞利用行为分析机制，模拟微软Office文档解析漏洞、Adobe Reader文档解析漏洞、Adobe FLASH组件解析漏洞、IE浏览器组件漏洞等多种利用行为，检测产品是否能够按照要求对漏洞利用行为进行检测（漏洞利用样本根据开发商提供的描述在威胁样本库中随机抽取，测试产品是否分析出漏洞利用事件）。

预期结果：

如果产品不能提供证据证明具有漏洞利用行为检测能力，或未分析出任何漏

洞利用行为，则本项判为不合格。

4.2.5. 未知木马检测

测评依据：

送检产品应具备对未知木马的检测能力。

文档要求：

开发商应提供文档说明产品具有对未知木马的检测能力及分析机制。

测评方法：

检验员判断此产品是否提供了足够的证据（比如能够设置未知木马检测参数等）；根据开发商提供的未知木马分析机制，模拟未知木马传播、活动行为，检测产品是否能够按照要求对未知木马进行检测（冻结被测产品的木马特征库，在威胁样本库中随机抽取送检日期后15日内的木马样本），测试产品是否分析出未知木马事件）。

预期结果：

如果产品不能提供证据证明具有未知木马检测能力，或未分析出任何未知木马事件，则本项判为不合格。

4.2.6. 隐蔽信道传输行为检测

测评依据：

送检产品应具备对隐蔽信道传输行为的检测能力。

文档要求：

开发商应提供文档说明产品具有对隐蔽信道传输行为的检测能力及分析机制。

测评方法：

检验员判断此产品是否提供了足够的证据（比如能够设置隐蔽信道传输行为检测参数等）；根据开发商提供的隐蔽信道传输行为分析机制，传输层协议字段隐藏、应用层协议行为伪装、长度式隐信道等多种隐蔽信道传输行为，检测产品是否能够按照要求对隐蔽信道传输行为进行检测。

预期结果：

如果产品不能提供证据证明具有隐蔽信道传输行为检测能力，或未分析出任何隐蔽信道传输行为，则本项判为不合格。

4.2.7. 组合性攻击检测能力

测评依据：

送检产品应具备对组合性攻击的检测能力。

文档要求：

开发商应提供文档说明产品具有对组合性攻击行为的检测能力及分析机制。

测评方法：

检验员判断此产品是否提供了足够的证据（比如能够设置组合性攻击行为检测参数等）；根据开发商提供的组合性攻击分析机制，模拟针对特定目标的网络文件传输异常行为、漏洞利用行为、未知木马、隐蔽信道传输等多种组合攻击行为，检测产品是否能够按照要求对组合性攻击行为进行检测。

预期结果：

如果产品不能提供证据证明具有组合性攻击行为的检测能力，或未能对多个攻击事件进行合并和关联，则本项判为不合格。

4.2.8. 持续性攻击检测能力

测评依据：

送检产品应具备对持续性攻击的检测能力。

文档要求：

开发商应提供文档说明产品具有对持续性攻击行为的检测能力及分析机制。

测评方法：

检验员判断此产品是否提供了足够的证据（比如能够设置持续性攻击行为检测参数等）；根据开发商提供的持续性攻击分析机制，模拟针对特定目标的持续性网络文件传输异常行为、漏洞利用行为、未知木马、隐蔽信道传输等多种攻击行为，检测产品是否能够按照要求对持续性攻击行为进行检测。

预期结果：

如果产品不能提供证据证明具有持续性攻击行为的检测能力，或未能在检测结果中标识攻击事件的持续性，则本项判为不合格。

4.3. 附加功能要求（选测项）

4.3.1. 异常网络行为分析

4.3.1.1. 异常电子邮件行为分析

测评依据：

送检产品应具备对远程/本地邮箱异常登录事件、异常远程/本地邮件操作事件（如：非授权远程收取、删除、发送等行为，邮件中包含敏感数据或未知加密格式的数据等）的检测分析能力。

文档要求：

开发商应提供文档说明产品具备对异常电子邮件行为的检测分析能力。

测评方法：

检验员判断开发商是否提供了足够的证据证明产品具备对异常电子邮件行为的检测能力；模拟电子邮件应用环境，并模拟异常电子邮件行为，检测产品是否能够按照要求对异常电子邮件行为进行检测。

预期结果：

如果开发商不能提供证据证明产品具有异常电子邮件行为的检测能力，或未

能在检测到异常电子邮件行为，则本项判为不合格。

4.3.1.2. 异常 Web 访问行为分析

测评依据：

送检产品应具备对远程/本地不可信地址的异常Web访问事件、远程/本地Web应用的异常登录事件、针对本地Web服务的异常请求内容、针对远程Web服务的异常请求内容（如：可疑文件下载、钓鱼网站访问、XSS、CSRF等）、针对远程Web服务的异常提交内容（如：带有敏感信息的数据提交、未知格式的加密数据提交）等的检测分析能力。

文档要求：

开发商应提供文档说明产品具备对异常Web访问行为的检测分析能力。

测评方法：

检验员判断开发商是否提供了足够的证据证明产品具备对异常 Web 访问行为的检测能力；模拟 Web 应用环境，并模拟异常 Web 访问行为，检测产品是否能够按照要求对异常 Web 访问行为进行检测。

预期结果：

如果产品不能提供证据证明具有异常 Web 访问行为的检测分析能力，或未能在检测到异常 Web 访问行为，则本项判为不合格。

4.3.1.3. 异常远程控制行为分析

测评依据：

送检产品应具备对远程/本地不可信地址的异常远程控制行为（包括：MSRDP、PcAnyWhere、VNC、TeamViewer以及常见远程控制类木马等）的检测分析能力。

文档要求：

开发商应提供文档说明产品具备对异常远程控制行为的检测分析能力。

测评方法：

检验员判断开发商是否提供了足够的证据证明产品具备对异常远程控制行为的检测能力；并模拟异常远程控制行为，检测产品是否能够按照要求对异常远程控制行为进行检测。

预期结果：

如果产品不能提供证据证明具有异常远程控制行为的检测分析能力，或未能在检测到异常远程控制行为，则本项判为不合格。

4.3.2. 异常文件分析

测评依据：

送检产品应具备对异常文件（如：恶意程序、异常文档文件、异常图片文件）的检测分析能力。

文档要求：

开发商应提供文档说明产品具备对异常文件的检测分析能力。

测评方法：

检验员判断开发商是否提供了足够的证据证明产品具备对异常文件行为的检测能力；从威协样本库中抽取异常文件样本，通过网络流量模拟器发送，检测产品是否能够按照要求对异常文件进行检测。

预期结果：

如果产品不能提供证据证明具有异常文件的检测能力，或未能在检测到异常文件行为，则本项判为不合格。

4.3.3. 异常事件分析报告

4.3.3.1. 异常电子邮件行为分析报告

测评依据：

送检产品应为用户提供可视化的异常电子邮件行为分析报告查看功能，报告中应至少包括：事件时间、电子邮件地址（收/发件人）、邮件服务器域名及IP地址、邮件服务器程序类型、邮件主题、邮件内容、邮件附件信息等。

文档要求：

开发商应提供文档说明产品具备为用户提供可视化的异常电子邮件行为分析报告查看功能。

测评方法：

检验员判断开发商是否提供了足够的证据证明产品具备异常电子邮件行为分析报告查看功能；模拟电子邮件应用环境，从威协样本库中抽取样本，模拟异常电子邮件行为，检查产品是否能够检测到异常电子邮件事件并提供分析报告，分析报告应包含：事件时间、电子邮件地址（收/发件人）、邮件服务器域名及 IP 地址、邮件服务器程序类型、邮件主题、邮件内容、邮件附件信息等。

预期结果：

如果产品未提供异常电子邮件行为分析报告功能，或漏报以上任一项目，则本项判为不合格。

4.3.3.2. 异常 Web 访问行为分析报告

测评依据：

送检产品应为用户提供可视化的异常Web访问行为分析报告查看功能，报告中至少包括：事件时间、URL、域名及对应的IP地址、访问请求参数、访问请求/回复内容等。

文档要求：

开发商应提供文档说明产品具备为用户提供可视化的异常 Web 访问行为分析报告查看功能。

测评方法：

检验员判断开发商是否提供了足够的证据证明产品具备异常 Web 访问行为分析报告查看功能；模拟 Web 应用环境，从威协样本库中抽取样本，模拟异常 Web 访问行为，检查产品是否能够检测到异常 Web 访问并提供分析报告，分析报告应至少包含：事件时间、URL、域名及对应的 IP 地址、访问请求参数、访问请求/回复内容等。

预期结果：

如果产品未提供异常 Web 访问行为分析报告功能，或漏报以上任一项目，则本项判为不合格。

4.3.3.3. 异常远程控制行为分析报告

测评依据：

送检产品应为用户提供可视化的异常远程控制行为分析报告查看功能，报告中至少包括：事件时间、远程控制工具类型、主控端IP地址及端口、被控端IP地址及端口、持续时间等。

文档要求：

开发商应提供文档说明产品具备为用户提供可视化的异常远程控制行为分析报告查看功能。

测评方法：

检验员判断开发商是否提供了足够的证据证明产品具备异常远程控制行为分析报告查看功能；模拟异常远程控制行为，检查产品是否能够检测到异常远程控制行为并提供分析报告，分析报告应至少包含：事件时间、远程控制工具类型、主控端 IP 地址及端口、被控端 IP 地址及端口、持续时间等。

预期结果：

如果产品未提供异常远程控制行为分析报告功能，或漏报以上任一项目，则本项判为不合格。

4.3.3.4. 异常文件分析报告

测评依据：

送检产品应为用户提供可视化的异常文件分析报告查看功能，报告中应至少包括：文件基本属性分析（文件名、文件大小、文件 HASH 校验值、文件类型、文件时间戳）、进程操作行为分析、文件操作行为分析、配置操作行为分析、网络操作行为分析，并详细记录行为发生时间、行为主体、行为客体、执行参数、执行返回值等信息。

文档要求：

开发商应提供文档说明产品的恶意程序鉴定报告及报告中的各数据项含义。

测评方法：

检测员检测产品是否提供了简单易用的管理界面查看此功能，并查看报告内容是否包含文件基本属性分析结果、进程操作行为分析结果、文件操作行为分析结果、配置操作行为分析结果、网络操作行为分析结果，并详细记录了行为发生时间、行为主体、行为客体、执行参数、执行返回值等信息。

预期结果：

如果产品未提供恶意程序鉴定报告功能，或漏报以上任一项目，则本项判为不合格。

4.3.4. 异常文件提取

测评依据：

送检产品应允许用户对检测到的威胁事件中的异常文件进行提取，并保证文件的完整性。

文档要求：

开发商应提供文档说明产品具备允许用户提取威胁事件中的异常文件的能力。

测评方法：

检验员判断开发商是否提供了足够的证据证明产品具备提取威胁事件中的异常文件的能力；模拟产品应用环境，从威胁样本库中发送威胁样本文件，检测产品是否能够还原威胁样本文件，并允许用户提取相关文件；检查还原后的文件与原始文件是否一致。

预期结果：

如果开发商不能提供证据证明产品具有提取威胁事件中的异常文件的能力，或未能提取到威胁事件中的异常文件，或提取的文件与原始样本文件不一致，则本项判为不合格。

4.3.5. 用户分析接口

测评依据：

送检产品应允许用户提交样本，支持样本类型包括：URL、文档文件、可执行文件等，对提交样本进行分析检测。

文档要求：

开发商应提供文档说明产品具备允许用户提交样本能力。

测评方法：

使用送检产品提供得提交样本接口进行威胁样本提交，样本类型包括：URL、文档文件、可执行文件等。

预期结果：

如果开发商不能提供证据证明产品具有提取威胁事件中的异常文件的能力，或产品无相关接口，或产品无法对URL、文档文件、可执行文件中任意一种威胁

样本进行分析，则本项判为不合格。

4.4. EAL3 级测评（必测项）

4.4.1. TOE 描述

本次被测产品为 XXX 公司的“XXX VX.X”，以下简称“XXX 高级持续性威胁（APT）监测产品”。XXX VX.X 是一款 XXX，由专用硬件平台及运行于该平台上的软件组成。主要功能包括：XXXX、XXXX 等。XXX VX.X 提供了 x 个 CONSOLE 口，x 个百/千兆电口，可通过 xx 方式对产品进行管理。

本次评估对象（TOE）仅限于在《XXX VX.X 安全目标》中所定义的 TOE 安全功能（TSF），以及构成 TOE 安全功能的接口。其中所有在 TOE 安全功能范围之外的 XXX、XXX、XXX 以及运行 XXX VX.X 的所有硬件均不属于本次评估范围。

TOE 软硬件配置信息如下表所示：

项目	描述
产品名称	
产品版本	
产品（系统）形态	软件（ ） 硬件（ ） 固件（ ）
生产集成厂商	
软件运行环境	
硬件配置信息	

4.4.2. 测评证据

序号	证据
1.	XXX VX.X 安全目标
2.	XXX VX.X 功能规范
3.	XXX VX.X 高层设计
4.	XXX VX.X 对应性分析
5.	XXX VX.X 配置管理
6.	XXX VX.X 交付和运行

序号	证据
7.	XXX VX.X 开发安全
8.	XXX VX.X 管理员指南
9.	XXX VX.X 用户指南
10.	XXX VX.X 测试文档
11.	XXX VX.X 脆弱性分析
12.	用于测试的 TOE

4.4.3. 测评活动

GB/T 18336 EAL3 测评活动包括：

1) 安全目标评估；
2) 开发活动评估；
3) 交付和运行评估；
4) 配置管理评估；
5) 指导性文档评估；
6) 生命周期支持评估；
7) 测试评估；
8) 脆弱性评估。

4.4.4. 测评判据

评估内容	预期结果
ASE 评估	满足 EAL3 相关要求
ADV_FSP.1	满足 EAL3 相关要求
ADV_HLD.2	满足 EAL3 相关要求
ADV_RCR.1	满足 EAL3 相关要求
ADO_DEL.1	满足 EAL3 相关要求
ADO_IGS.1	满足 EAL3 相关要求
ACM_CAP.3	满足 EAL3 相关要求
ACM_SCP.1	满足 EAL3 相关要求
AGD_ADM.1	满足 EAL3 相关要求
AGD_USR.1	满足 EAL3 相关要求
ALC_DVS.1	满足 EAL3 相关要求

ATE_COV.2	满足 EAL3 相关要求
ATE_DPT.1	满足 EAL3 相关要求
ATE_FUN.1	满足 EAL3 相关要求
ATE_IND.2	满足 EAL3 相关要求
AVA_MSU.1	满足 EAL3 相关要求
AVA_SOF.1	满足 EAL3 相关要求
AVA_VLA.1	满足 EAL3 相关要求

评估活动需满足上表要求，评估最终裁定结果为通过。

4.4.5. 测评内容

4.4.5.1. 安全目标评估

4.4.5.1.1. ST 引言的评估(ASE_INT.1)

a) 评估方法
   1) 检查 ST 引言中是否包含 ST 标识信息，该标识应可用于控制和标识 ST 的版本变化，以及与其对应的 TOE 的标识和描述性信息；
   2) 检查 ST 引言中是否包含对 ST 概括性描述；
   3) 检查 ST 引言中是否包含与 GB/T 18336 的一致性声明，该声明是否陈述了 TOE 与 GB/T 18336 的一致性，如有与 GB/T 18336 不一致的情况也须声明。
b) 预期结果
   1) ST 引言中包含了 ST 标识信息，该标识应可用于控制和标识 ST 的版本变化，以及与其对应的 TOE 的标识和描述性信息；
   2) ST 引言中包含了对 ST 概括性描述；
   3) ST 引言中包含了与 GB/T 18336 的一致性声明，该声明陈述了 TOE 与 GB/T 18336 的一致性，其中与 GB/T 18336 不一致的情况也已声明。

4.4.5.1.2. TOE 描述的评估(ASE_DES.1)

a) 评估方法
   1) 检查 TOE 描述部分是否概括陈述 TOE 的类型，并从物理和逻辑两方面概述 TOE 的范围和边界；
b) 预期结果
   1) TOE 描述部分概括陈述了 TOE 的类型，并从物理和逻辑两方面概述了 TOE 的范围和边界。

4.4.5.1.3. 安全环境的评估(ASE_ENV.1)

a) 评估方法
   1) 检查 TOE 安全环境部分是否以 TOE 的预期使用环境为基础分析 TOE 所要保护的资产，标识并解释 TOE 或其环境所保护的资产可能面临的任何已知或假定的威胁；
   2) 检查 TOE 安全环境部分是否列出以认为 TOE 是安全的为前提而做出

的所有假设；

3） 检查 TOE 安全环境部分是否列出所有 TOE 及其环境必须遵守的组织安全策略，这些策略是否是由控制 TOE 使用环境的组织制定的。

b） 预期结果

1） TOE 描述部分概括陈述了 TOE 的类型，并从物理和逻辑两方面概述了 TOE 的范围和边界；

2） TOE 安全环境部分列出了以认为TOE是安全的为前提而做出的所有假设；

3） TOE 安全环境部分列出了所有 TOE 及其环境必须遵守的组织安全策略，这些策略是由控制 TOE 使用环境的组织制定的。

4.4.5.1.4. 安全目的的评估(ASE_OBJ.1)

a） 评估方法

1） 检查 ST 的安全目的一节是否包括 TOE 安全目的和环境安全目的的两部分，并证明了安全目的与假设、威胁、组织安全策略之间的对应关系。

b） 预期结果

1） ST 的安全目的一节包括了 TOE 安全目的和环境安全目的的两部分，并证明安全目的与假设、威胁、组织安全策略之间的对应关系。

4.4.5.1.5. IT 安全要求的评估(ASE_REQ.1)

a） 评估方法

1） 检查文档是否描述了安全功能要求和安全保证要求，并对其内容进行了正确的个性化描述，以及组件之间的依赖关系是正确的。

b） 预期结果

1） 文档描述了安全功能要求和安全保证要求，并对其内容进行了正确的个性化描述，以及组件之间的依赖关系是正确的。

4.4.5.1.6. 明确陈述的 IT 安全要求的评估(ASE_SRE.1)

a） 评估方法

1） 检查文档是否存在自定义的安全组件，并判断其正确性。

b） 预期结果

1） 文档存在自定义的安全组件，并且是正确的。

4.4.5.1.7. TOE 概要规范的评估(ASE_TSS.1)

a） 评估方法

1） 检查文档是否文档描述了 TOE 的安全功能和保证措施，并证明其与安全要求之间的对应关系；

2） 检查对于所有用到了概率和置换机制实现的安全功能，是否在 ST 中声明了其应达到的最低强度级别。

b） 预期结果

1） 文档描述了 TOE 的安全功能和保证措施，并证明了其与安全要求之

间的对应关系；

2) 对于所有用到了概率和置换机制实现的安全功能，在 ST 中都声明了其应达到的最低强度级别。

4.4.5.1.8. PP 声明的评估(ASE_PPC.1)

a) 评估方法

1) 检查 ST 是否包含了与 PP 的符合性声明，未遵循 PP 的 ST 此项可不考虑。

b) 预期结果

1) ST 包含了与 PP 的符合性声明。

4.4.5.2. 开发活动评估

4.4.5.2.1. 非形式化功能规范评估(ADV_FSP.1)

a) 评估方法

1) 检查开发者是否提供了一个功能规范；
2) 检查功能规范是否使用了非形式化风格来描述产品安全功能及其外部接口；
3) 检查功能规范是否是内在一致的；
4) 检查功能规范是否描述了所有外部接口的用途与使用方法，是否提供了效果、例外情况和错误消息的细节；
5) 检查功能规范是否完备地表示了产品安全功能。

b) 预期结果

1) 开发者提供了一个功能规范；
2) 功能规范使用了非形式化风格来描述产品安全功能及其外部接口；
3) 功能规范是内在一致的；
4) 功能规范描述了所有外部接口的用途与使用方法，提供了效果、例外情况和错误消息的细节；
5) 功能规范完备地表示了产品安全功能。

4.4.5.2.2. 安全加强的高层设计评估(ADV_HLD.2)

a) 评估方法

1) 检查开发者是否提供了产品安全功能的高层设计；
2) 检查高层设计的表示是否是非形式化的；
3) 检查高层设计是否是内在一致的；
4) 检查高层设计是否按子系统描述安全功能的结构；
5) 检查高层设计是否描述了每个安全功能子系统所提供的安全功能性；
6) 检查高层设计是否标识了安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
7) 检查高层设计是否标识了安全功能子系统的所有接口；
8) 检查高层设计是否标识了安全功能子系统的哪些接口是外部可见的；

9) 检查安全加强的高层设计是否描述了产品的功能子系统所有接口的用途与使用方法，是否提供了效果、例外情况和错误消息的细节；
10) 检查安全加强的高层设计是否把产品分成安全策略实施和其他子系统来描述。

b) 预期结果
1) 开发者提供了产品安全功能的高层设计；
2) 高层设计的表示是非形式化的；
3) 高层设计是内在一致的；
4) 高层设计按子系统描述了安全功能的结构；
5) 高层设计描述了每个安全功能子系统所提供的安全功能性；
6) 高层设计标识了安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
7) 高层设计标识了安全功能子系统的所有接口；
8) 高层设计标识了安全功能子系统的哪些接口是外部可见的。
9) 安全加强的高层设计描述了产品的功能子系统所有接口的用途与使用方法，提供了效果、例外情况和错误消息的细节；
10) 安全加强的高层设计把产品分成安全策略实施和其他子系统来描述。

4.4.5.2.3. 非形式化对应性证实评估（ADV_RCR.1）

a) 评估方法
1) 检查开发者是否提供了产品安全功能表示的所有相邻对之间的对应性分析；
2) 检查分析是否阐明了产品安全功能所表示的每个相邻对；
3) 检查开发者是否在较具体的安全功能表示中正确且完备地细化了较为抽象的安全功能表示的所有相关安全功能。

b) 预期结果
1) 开发者提供了产品安全功能表示的所有相邻对之间的对应性分析；
2) 分析阐明了产品安全功能所表示的每个相邻对；
3) 开发者已在较具体的安全功能表示中正确且完备地细化了较为抽象的安全功能表示的所有相关安全功能。

4.4.5.3. 交付和运行评估

4.4.5.3.1. 交付程序评估（ADO_DEL.1）

a) 评估方法
1) 检查开发者是否使用一定的交付程序交付产品，并将交付过程文档化；
2) 检查交付文档是否描述了在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

b) 预期结果
1) 开发者使用了一定的交付程序交付产品，并将交付过程文档化；
2) 交付文档描述了在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

4.4.5.3.2.安装、生成和启动程序评估（ADO_IGS.1）

a) 评估方法
   1) 检查开发者是否提供了文档说明产品的安装、生成和启动的过程；
   2) 检查安装、生成和启动文档是否描述了产品安全地安装、生成和启动必需的所有步骤；
   3) 检查安装、生成和启动程序是否最终产生了一个安全的配置。
b) 预期结果
   1) 开发者提供了文档说明产品的安装、生成和启动的过程；
   2) 安装、生成和启动文档描述了产品安全地安装、生成和启动必需的所有步骤；
   3) 安装、生成和启动程序最终产生了一个安全的配置。

4.4.5.4. 配置管理评估

4.4.5.4.1. 授权控制评估（ACM_CAP.3）

a) 测试方法
   1) 检查开发者是否为产品的不同版本提供了唯一的标识；
   2) 检查开发者是否使用了配置管理系统并提供了配置管理文档；
   3) 检查配置管理文档是否包括一个配置清单；
   4) 检查配置清单中是否唯一标识了组成产品的所有配置项并对配置项进行描述；
   5) 检查配置清单中是否描述了对配置项给出唯一标识的方法，并提供了所有的配置项得到有效维护的证据；
   6) 检查配置管理文档是否包括一个配置管理计划；
   7) 检查配置管理计划中是否描述了如何使用配置管理系统；
   8) 检查实施的配置管理是否与配置管理计划相一致；
   9) 检查开发者是否提供了所有的配置项得到有效地维护的证据，是否保证只有经过授权才能修改配置项。
b) 预期结果
   1) 开发者为产品的不同版本提供了唯一的标识；
   2) 开发者使用了配置管理系统并提供了配置管理文档；
   3) 配置管理文档包括了一个配置清单；
   4) 配置清单中唯一标识了组成产品的所有配置项并对配置项进行描述；
   5) 配置清单中描述了对配置项给出唯一标识的方法，并提供了所有的配置项得到有效维护的证据；
   6) 开发者使用了配置管理系统并提供了配置管理文档；
   7) 配置管理文档包括了一个配置清单；
   8) 配置清单中唯一标识了组成产品的所有配置项并对配置项进行描述；
   9) 配置清单中描述了对配置项给出唯一标识的方法，并提供了所有的配置项得到有效维护的证据。

4.4.5.4.2. 配置管理覆盖评估（ACM_SCP.1）

a) 测试方法
   1) 检查配置管理范围中是否包括了产品实现表示、设计文档、测试文档、指导性文档、配置管理文档；
   2) 检查上述文档的修改是否在一个正确授权的可控方式下进行；
   3) 检查配置管理文档是否能跟踪上述内容并描述了配置管理系统是如何跟踪这些配置项的。

b) 预期结果
   1) 配置管理范围中包括了产品实现表示、设计文档、测试文档、指导性文档、配置管理文档；
   2) 文档的修改是在一个正确授权的可控方式下进行的；
   3) 配置管理文档能跟踪上述内容，并且描述了配置管理系统是如何跟踪这些配置项的。

4.4.5.5. 指导性文档评估

4.4.5.5.1. 管理员指南评估（AGD_ADM.1）

a) 评估方法
   1) 检查开发者是否提供了管理员指南；
   2) 检查管理员指南是否与为评估而提供的其他所有文档保持一致；
   3) 检查管理员指南是否说明了管理员可使用的管理功能和接口；
   4) 检查管理员指南是否说明了怎样安全地管理产品；
   5) 检查管理员指南是否说明了在安全处理环境中应被控制的功能和权限；
   6) 检查管理员指南是否说明了所有对与产品的安全操作有关的用户行为的假设；
   7) 检查管理员指南是否说明了所有受管理员控制的安全参数，如果可能，应指明安全值；
   8) 检查管理员指南是否说明了每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；
   9) 检查管理员指南是否说明了所有与管理员有关的 IT 环境安全要求。

b) 预期结果
   1) 开发者提供了管理员指南；
   2) 管理员指南与为评估而提供的其他所有文档保持一致；
   3) 管理员指南说明了管理员可使用的管理功能和接口；
   4) 管理员指南说明了怎样安全地管理产品；
   5) 管理员指南说明了在安全处理环境中应被控制的功能和权限；
   6) 管理员指南说明了所有对与产品的安全操作有关的用户行为的假设；
   7) 管理员指南说明了所有受管理员控制的安全参数，如果可能，应指明安全值；
   8) 管理员指南说明了每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；
   9) 管理员指南说明了所有与管理员有关的 IT 环境安全要求。

4.4.5.5.2. 用户指南评估（AGD_USR.1）

a) 评估方法
   1) 检查开发者是否提供了用户指南；
   2) 检查用户指南是否与为评估而提供的其他所有文档保持一致；
   3) 检查用户指南是否说明了产品的非管理员用户可使用的安全功能和接口；
   4) 检查用户指南是否说明了产品提供给用户的安全功能和接口的使用方法；
   5) 检查用户指南是否说明了用户可获取但应受安全处理环境所控制的所有功能和权限；
   6) 检查用户指南是否说明了产品安全操作中用户所应承担的职责；
   7) 检查用户指南是否说明了与用户有关的 IT 环境的所有安全要求。
b) 预期结果
   1) 开发者提供了用户指南；
   2) 用户指南与为评估而提供的其他所有文档保持一致；
   3) 用户指南说明了产品的非管理员用户可使用的安全功能和接口；
   4) 用户指南说明了产品提供给用户的安全功能和接口的使用方法；
   5) 用户指南说明了用户可获取但应受安全处理环境所控制的所有功能和权限；
   6) 用户指南说明了产品安全操作中用户所应承担的职责；
   7) 用户指南说明了与用户有关的 IT 环境的所有安全要求。

4.4.5.6. 生命周期支持评估

4.4.5.6.1. 安全措施标识评估（ALC_DVS.1）

a) 评估方法
   1) 检查开发者是否提供了开发安全文档；
   2) 检查开发安全文档是否描述了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；
   3) 检查开发安全文档是否提供了在产品的开发和维护过程中执行安全措施的证据。
b) 预期结果
   1) 开发者提供了开发安全文档；
   2) 开发安全文档描述了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；
   3) 开发安全文档提供了在产品的开发和维护过程中执行安全措施的证据。

4.4.5.7. 测试评估

4.4.5.7.1. 覆盖分析评估（ATE_COV.2）

a) 评估方法
   1) 检查开发者是否提供了测试覆盖的分析结果；
   2) 检查测试覆盖的分析结果是否表明了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之间的对应性是完备的。
b) 预期结果
   1) 开发者提供了测试覆盖的分析结果；
   2) 测试覆盖的分析结果表明了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之间的对应性是完备的。

4.4.5.7.2. 测试：高层设计（ATE_DPT.1）

a) 评估方法
   1) 检查开发者是否提供了测试深度的分析；
   2) 检查深度分析是否证实了测试文档中所标识的测试足以证实该产品的功能是依照其高层设计运行的。
b) 预期结果
   1) 开发者提供了测试深度的分析；
   2) 深度分析中证实了测试文档中所标识的测试足以证实该产品的功能是依照其高层设计运行的。

4.4.5.7.3. 功能测试（ATE_FUN.1）

a) 评估方法
   1) 检查开发者是否测试了安全功能，将结果文档化并提供了测试文档；
   2) 检查测试文档中是否包括了测试计划，标识了要测试的安全功能，并描述了测试的目标；
   3) 检查测试文档中是否包括了测试过程，应标识要执行的测试，并描述每个安全功能的测试概况，这些概况应包括对于其他测试结果的顺序依赖性；
   4) 检查测试文档中是否包括了预期的测试，结果应表明测试成功后的预期输出；
   5) 检查测试文档中是否包括了实际测试结果，应表明每个被测试的安全功能能按照规定进行运作。
b) 预期结果
   1) 开发者测试了安全功能，将结果文档化并提供了测试文档；
   2) 测试文档中包括了测试计划，标识了要测试的安全功能，并描述了测试的目标；
   3) 测试文档中包括了测试过程，标识了要执行的测试，并描述每个安全功能的测试概况，这些概况应包括对于其他测试结果的顺序依赖性；
   4) 测试文档中包括了预期的测试，结果表明测试成功后的预期输出；
   5) 测试文档中包括了实际测试结果，表明每个被测试的安全功能能按照规定进行运作。

4.4.5.7.4. 独立测试——抽样（ATE_IND.2）

a) 评估方法
   1) 检查开发者是否提供了一组相当的资源，用于安全功能的抽样测试。
b) 预期结果
   1) 开发者提供了一组相当的资源，用于安全功能的抽样测试。

4.4.5.8. 脆弱性评估

4.4.5.8.1. 指南审查（AVA_MSU.1）

a) 评估方法
   1) 检查开发者是否提供了指导性文档；
   2) 检查指导性文档是否标识了所有可能的产品运行模式（包括失败或操作失误后的运行）、它们的后果以及对于保持安全运行的意义；
   3) 检查指导性文档是否是完备的、清晰的、一致的、合理的；
   4) 检查指导性文档是否列出了关于预期使用环境的所有假设；
   5) 检查指导性文档是否列出了对外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求。
b) 预期结果
   1) 开发者提供了指导性文档；
   2) 指导性文档标识了所有可能的产品运行模式（包括失败或操作失误后的运行）、它们的后果以及对于保持安全运行的意义；
   3) 指导性文档是完备的、清晰的、一致的、合理的；
   4) 指导性文档列出了关于预期使用环境的所有假设；
   5) 指导性文档列出了对外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求。

4.4.5.8.2. TOE 安全功能强度评估（AVA_SOF.1）

a) 评估方法
   1) 检查开发者是否对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明了安全机制达到或超过定义的最低强度级别或特定功能强度度量。
b) 预期结果
   1) 开发者对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明了安全机制达到或超过定义的最低强度级别或特定功能强度度量。

4.4.5.8.3. 开发者脆弱性分析（AVA_VLA.1）

a) 评估方法
   1) 检查开发者是否执行了脆弱性分析，并提供了脆弱性分析文档；
   2) 检查开发者是否从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档；
   3) 对被确定的脆弱性，检查开发者是否明确记录采取的措施；

4） 对每一条脆弱性，检查其是否有证据显示在使用产品的环境中，该脆弱性不能被利用。

b） 预期结果

1） 开发者执行了脆弱性分析，并提供了脆弱性分析文档；

2） 开发者从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档；

3） 对被确定的脆弱性，开发者明确记录了采取的措施；

4） 对每一条脆弱性，有证据显示在使用产品的环境中，该脆弱性不能被利用。

4.4.5.9. 独立性测试

a） 评估目的：

TOE 安全功能执行的正确性。

b） 预期结果：

1. 开发者应提供一个与开发者的安全功能测试中使用的资源相当的合集；

2. 评估者参考开发者提供的测试文档形成抽样子集；如下表：

序号	安全功能	测试用例	备注
1			
2			

根据实际产品的安全功能进行增加。

4.4.5.10.穿透性测试

a） 评估目的：

b） 根据脆弱性分析文档进行渗透性测试。

开发者应提供脆弱性分析文档，描述产品可以存在的每一个脆弱性；

c） 评估方法及步骤

针对可能实施的脆弱性和渗透性测试方法，对其实现手段进行简单介绍。其中网络脆弱性测试主要针对对象是提供服务的宿主主机，Web 应用脆弱性测试主要针对对象是现有的 Web 应用服务。

1） 网络脆弱性测试

探测工具：脆弱性扫描工具、审计网络用的安全分析工具等。

渗透工具集：包括针对各种操作系统和数据库的溢出渗透工具、口令破解工具等。

2） Web 应用脆弱性测试

探测工具：Web 应用安全扫描器（如明鉴 Web 应用弱点扫描器），针对 Web 应用渗透性测试主要分为：注入检测、跨站脚本攻击检测、Web 认

证攻击检测、会话管理攻击、信息泄露检测（源代码、目录信息）等。

渗透验证：可通过扫描工具或手工调用浏览器验证 Web 应用漏洞，如利用 SQL 注入点获取后台数据库相关信息。

d) 预期结果

如果产品未提供文档，或产品存在脆弱性（如漏洞、未申明端口等），则本项判为不符合。

4.5. 自主知识产权评估

测评依据：

对厂家产品代码同业界已有产品代码进行比较，检测厂家产品的自主知识情况。

文档要求：

提供对产品源代码的自主知识产权申明，加盖单位公章。

测评方法：

1. 要求厂家以源代码的形式提供产品代码，并提供证明产品代码已经通过代码格式审查工具的检查，格式符合代码相似度检查的要求；

2. 要求厂家在独立干净的机器上进行源代码的编译和生成，并能够对应到已经部署的软硬件设备上的实际执行代码；

3. 使用工具对产品的源代码（关键核心模块）进行对比分析测试，得到相似程度；

4. 相似分析结果。

预期结果：

被测产品关键核心模块源代码与基准数据的相似分析结果符合自主原创测评指南的要求。

4.6. 性能测试（必测项）

4.6.1. 并发检测

测评依据：

发改办高技[2013]1965 号文中要求，送检产品应支持 1000 个以上的并发检测能力。

文档要求：

提供文档说明产品的并发检测能力。

测评方法：

1. 检验员判断此产品是否提供了足够的证据证明其具有 1000 个以上的并发检测能力；

2. 测试仪表通过网络分流器连接被测产品，选择 1000 个以上不同的 APT 威胁样本，配置相应的接口地址，进行并发测试。

预期结果：

如果产品或产品文档没有提供足够的描述证据，或测试过程中未能检测到1000 个以上的并发威胁事件，则本项判为不合格。

4.6.2. 漏报率

测评依据：

发改办高技[2013]1965 号文中要求，送检产品基于国内外主流特征库检测的漏报率应低于 5%。

文档要求：

提供文档说明产品基于国内外主流特征库检测的漏报率。

测评方法：

1. 检验员判断此产品是否提供了足够的证据证明其基于国内外主流特征库检测的漏报率低于 5%；

2. 高性能网络流量模拟器通过网络分流器连接被测产品，基于国内外主流特征库（包括国家计算机病毒应急处理中心恶意代码样本库、CVE、OSVDB、CNVD、BackTrack、Metasploit 等）选择 5000 个以上不同的 APT 威胁样本，配置相应的接口地址，进行测试。

预期结果：

如果产品或产品文档没有提供足够的描述证据，或测试过程中对测试样本漏报率高于 5%，则本项判为不合格。

4.6.3. 误报率

测评依据：

发改办高技[2013]1965 号文中要求，送检产品误报率低于 10%。

文档要求：

提供文档说明产品的误报率。

测评方法：

1. 检验员判断此产品是否提供了足够的证据证明其误报率低于 10%；

2. 高性能网络流量模拟器通过网络分流器连接被测产品，模拟典型的金融机构网络应用流量，并发送数量不少于 5000 个的正常可执行文件和文档文件，配置相应的接口地址，进行测试。

预期结果：

如果产品或产品文档没有提供足够的描述证据，或测试过程中对测试样本误报率高于 10%，则本项判为不合格。

4.7. IPv6 协议一致性与环境适应性测试（必测项）

4.7.1. IPv6 协议一致性要求

4.7.1.1. IPv6 协议一致性测试

测评依据：

产品能够符合“RFC2460, Internet Protocol, Version 6 (IPv6) Specification”和“RFC 2464, Transmission of IPv6 Packets over Ethernet

Networks”的要求。

文档要求：

提供文档说明产品的 IPv6 核心协议一致性。

测评方法：

1. 送检产品至少应提供 1 个管理接口，并必须支持 ICMPv6；

2. 测试仪表通过网络分流器连接被测产品，选择相应模板，配置相应的接口地址，进行测试；

3. 根据 RFC2460 对 Header Format(2)、Hop-by-Hop Options Header(10)、Extension Header Order(4) 、 Hop-by-Hop and Destination Options Header(32)、Option(9)、Routing Header(16)、Fragment Headers(17)、No Next Header(4)、Packet Size(1)、Flow Labels(3)、Traffic Classes(2)、Upper-Layer Checksum(2) 、 Frame Format and Address Mapping(4) 、 Hop-by-Hop and Destination Options Header-2(17)的 14 大项（123 小项）规定，对产品 IPv6 协议正确实现情况进行检测。

预期结果：

如果产品不满足 RFC2460 和 RFC2464 要求，或 RFC2460 测试模版符合率（符合项目数/123*100%）小于 50%，则本项判为不合格。

4.7.1.2. IPv6 邻居发现协议一致性测试

测评依据：

产品能够符合“RFC4861”的要求。

文档要求：

提供文档说明产品的 IPv6 邻居发现协议一致性。

测评方法：

1. 送检产品应至少提供 1 个管理接口；

2. 测试仪表通过网络分流器连接被测产品，选择相应模板，配置相应的接口地址，进行测试；

3. 根据 RFC4861 的规定，对产品 IPv6 协议正确实现情况进行检测。

预期结果：

如果产品不满足 RFC4861 要求，或 RFC4861 测试模版符合率（符合项目数/XX*100%）小于 50%，则本项判为不合格。

4.7.1.3. IPv6 无状态地址自动配置一致性测试

测评依据：

产品能够符合“RFC4862, IPv6 Stateless Address Autoconfiguration”的要求。

文档要求：

提供文档说明产品的 IPv6 无状态地址自动配置一致性。

测评方法：

1. 送检产品应提供2个接口，并在接口上能够发送NA、RA协议，参与IPv6地址自动配置；

2. 测试仪表通过网络分流器连接被测产品，选择相应模板，配置相应的接口地址，进行测试；

3. 根据 RFC4862 对 Protocol Specification, Node Configuration Variables, Creation of Link-Local Addresses (3)、Duplicate Address Detection (5)、Message Validation(2)、Sending Neighbor Solicitation Messages(4)、Receiving Neighbor Solicitation Messages, Receiving Neighbor Advertisement Messages (3)、Creation of Global Addresses, When Duplicate Address Detection Fails(2)、Router Advertisement Processing (10)、Address Lifetime Expiry (2)、Configuration Consistency (1)的 9 大项（32 小项）规定，对产品 IPv6 协议正确实现情况进行检测。

预期结果：

如果产品不满足 RFC4862 要求，或 RFC4862 测试模版符合率（符合项目数/32*100%）小于 50%，则本项判为不合格。

4.7.1.4. IPv6 PMTU 发现协议一致性测试

测评依据：

产品能够符合“RFC1981, Path MTU Discovery for IP version 6”的要求。

文档要求：

提供文档说明产品的 IPv6 PMTU 发现协议一致性。

测评方法：

1. 送检产品应至少提供 1 个管理接口，并能够支持连接不同 MTU 网络的能力；

2. 测试仪表通过网络分流器连接被测产品，选择相应模板，配置相应的接口地址，进行测试；

3. 根据 RFC1981 对 Protocol Tests (2)、Protocol Requirements Tests(4)、Storing PMTU Information Tests(2)、Purging Stale PMTU Information Tests(1)的 4 大项（9 小项）规定，对产品 IPv6 协议正确实现情况进行检测。

预期结果：

如果产品不满足 RFC4862 要求，或 RFC4862 测试模版符合率（符合项目数/32*100%）小于 50%，则本项判为不合格。

4.7.1.5. ICMPv6 协议一致性测试

测评依据：

产品能够符合“RFC4443,Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”的要求。

文档要求：

提供文档说明产品的 ICMPv6 协议一致性。

测评方法：

1. 送检产品接口应至少提供 1 个管理接口，并必须能够支持 ICMPv6；
2. 测试仪表通过网络分流器连接被测产品，选择相应模板，配置相应的接口地址，进行测试；
3. 根据 RFC4443 对 Message Source Address Determination(3)、Message Checksum Calculation (2)、Message Processing Rules (13)、Destination Unreachable Message (12)、Packet Too Big Message (2)、Time Exceeded Message (4)、Parameter Problem Message (5)、Echo Request Message (2)、Echo Reply Message (1)的 9 大项（44 小项）规定，对产品 IPv6 协议正确实现情况进行检测。

预期结果：

如果产品不满足 RFC4443 要求，或 RFC4443 测试模版符合率（符合项目数/44*100%）小于 50%，则本项判为不合格。

4.7.2. IPv6 环境适应性要求

4.7.2.1. 纯 IPv6 环境适应性安全功能测试

测评依据：

产品能够适用于纯 IPv6 环境的威胁检测。

文档要求：

提供文档说明产品安全功能的纯 IPv6 环境适应性。

测评方法：

1. 通过部署测试主机和路由交换设备，模拟纯 IPv6 环境；
2. 将送检产品并联入模拟的纯 IPv6 环境，测试产品的网络信息分析能力。

预期结果：

如果产品不支持纯 IPv6 环境，或不能够正确执行网络信息分析功能，则本项判为不合格。

4.7.2.2. IPv4/6 双栈环境适应性安全功能测试

测评依据：

产品能够适用于 IPv4/6 双栈环境的攻击检测。

文档要求：

提供文档说明产品安全功能的 IPv4/6 双栈环境适应性。

测评方法：

1. 通过部署测试主机和路由交换设备，模拟 IPv4/6 双栈环境；

2. 将送检产品并联入模拟的 IPv4/6 双栈环境，测试产品的网络信息分析能力。

预期结果：

如果产品不支持 IPv4/6 双栈环境，或不能够正确执行网络信息分析功能，则本项判为不合格。

4.7.2.3. IPv6 环境下管理功能适应性

测评依据：

产品能够适用于 IPv6 环境下的远程管理。

文档要求：

提供文档说明产品管理能力的 IPv6 环境适应性。

测评方法：

1. 通过部署测试主机和路由交换设备，模拟 IPv6 环境；

2. 测试产品的远程管理能力。

预期结果：

如果产品不支持 IPv6 环境，或不能够正确进行管理，则本项判为不合格。