安全计算环境-安全设备-入侵检测（S3A3G3）作业指导书					
控制点	**安全要求**	**要求解读**	**测评方法**	**预期结果或主要证据**	**符合情况**
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换	为了安全起见，入侵检测只有经过授权的合法用户才能访问，一般来说，用户登录入侵检测的方式为通过浏览器以WEB方式登录。入侵检测为了便于用户管理，还提供了图形界面管理工具便于用户对设备进行管理和维护，需要对用户身份进行鉴别。 入侵检测不允许配置用户名相同的用户，同时要防止多人共用一个账户，实行分账户管理，每名管理员设置一个单独的账户，避免出现问题后不能及时进行追查。 同时为避免身份鉴别信息被冒用，应当保证口令复杂度和定期更改的要求。	1)以奇安信IDS为例，核查用户在登录时是否来用里身份鉴别措施。 通过浏览器以WEB方式登录 打开IE浏览器，在地址输入框中输入奇安信IDS的URL地址，如https://xx.x.x.x。回车后进入奇安信IDS的登录界面，，提示用户输入用户名和密码 输入用户名和密码后，点击”登录“按钮，即可登录到奇安信IDS。登录后，用户就可通过WEB界面对奇安信IDS进行配置管理 输入用户名，然后回车后，提示用户输入密码： 1）输入密码后，回车，即可登录到奇安信IDS。登录后，用户就可使用命令行方式对奇安信IDS进行配置管理。 2)应核查IDS管理员账户列表，测试用户身份标识是否具有唯一性，核查是否存在多人共用账户的情况，核查是否存在空口令用户。 3)应询问管理员对身份鉴别所采取的具体措施，确认口令长度是否8位以上，是否由数字、大小写字母和特殊字符中的两种以上组成，口令是否每季度至少更改一次	1)入侵检测使用口令鉴别机制对登录用户进行身份标识和鉴别 2)用户身份标识具有唯一性，不存在多人共用账户的情况，不存在空口令用户 3)口令长度8位以上，由数字、大小写字母和特殊字符中的两种以上组成，口令每季度至少更改一次	符合情况：通过用户名口令方式登录，口令长度8位以上，口令复杂度包含大写字母、小写字母、数字，口令有效期为90天； 部分符合情况：通过用户名口令方式登录，口令长度8位以上，复杂度为小写字母、数字、特殊字符，但未配置口令有效期； 不符合情况：通过用户名口令方式登录，口令长度为6位，复杂度为纯数字，未配置口令有效期，口令为弱口令。
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施	可以通过配置结束会话、限制管理员的最大登录失败次数、网络连接超时自动退出等多种措施实现登录失败处理功能。例如，设置管理员最大登录失败次数，一旦该管理员的登录失败次数超过设定数值，系统将对其进行登录锁定，从而防止非法用户通过暴力破解的方式登录到入侵检测	1)应在管理>系统设置里核查是否配置并启用了登录失败处理功能，核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能 2)应在管理>系统设置里，核查是否配置并启用了远程登录连接超时并自动退出功能	1)配置并启用了登录失败处理功能，配置并启用了限制非法登录达到一定次数后实现账户锁定功能。 进入管理界面。然后在管理>系统设置，进入在系统设置页面，选择“管理员账号”页签，进入管理员账号页面，点击收缩的下拉栏，可以查看到“最大登录失败次数”的配置。 2)配置并启用了远程登录连接超时并自动退出功能。进入管理界面。管理>系统设置，默认进入基础设置页面，可见WEB页面超时时间版块。在“管理员登录超时时间”后的时间设置文本框中，输入需要设置的Web页面超时时	符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，会话空闲30分钟自动退出； 部分符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，但未配置连接超时自动退出措施； 不符合情况：未配置登录失败处理功能和连接超时自动退出措施。
	c)当进行远程管理时，应采取必要措施、防止鉴别信息在网络传输过程中被窃听	为避免口令传输过程中别窃取，不应当使用明文传送的Telnet、HTTP服务，而应当采用SSH、HTTPS等加密协议等方式进行交互式管理	应询问系统管理员采用何种方式对入侵检测进行远程管理,核查通过WEB界面管理是否都通过SSL协议进行加密处理	通过WEB界面进行远程管理时，通过SSL协议进行加密处理。	符合情况：仅采用https协议进行管理，防止鉴别信息在网络传输过程中被窃听； 不符合情况：仅采用http协议进行管理，无法防止鉴别信息在网络传输过程中被窃听。

	d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现	采用双因子鉴别是防止欺骗的有效方法，双因子鉴别不仅要求访问者知道一些鉴别信息，还需要访问者拥有鉴别特征，例如采用令牌、智能卡等.目前主流入侵检测多采用“本地口令+证书认证”的方式进行认证。“本地口令+证书认证”认证时，用户既要通过入侵检测内部认证服务器的口令认证，也要通过证书认证才能够成功登录入侵检测	进入管理界面。 2）右侧显示用户列表信息，： 3)如果需要对用户进行两种或两种以上组合的鉴别技术，点击该用户条目右侧的“修改”图标，查看该用户的认证方式应该为“本地口令+证书认证”或者“外部口令+证书认证”。	以奇安信IDS为例，通过浏览器以WEB方式登录。 查看该用户的认证方式应该为“本地口令+证书认证”。	符合情况：通过用户名口令和谷歌验证码方式登录，验证码长度为6位，有效时间为30秒； 不符合情况：通过用户名口令方式登录，未采用两种或两种以上鉴别技术对用户进行身份鉴别。
访问控制	a)应对登录的用户分配账户和权限	为了确保入侵检测的安全，需要对登录的用户分配账户，并合理配置账户权限	进入管理界面。用户进入Web管理页面后，在导航栏区域点击管理>系统设置，进入系统设置页面，点击管理员账号，可进入管理员账号配置页面。 1)应针对每一个用户账户，核查用户账启和权限设置情况是否合理，如账户管理员和配置管理员不应具有审计员权限。 2)应核查是否已禁用或限制匿名、默认账户的访问	1、相关管理人员具有与职位相对应的账户和权限。 2、禁用或限制匿名、默认账户的访问权限。	符合情况：已对可登录用户分配账户和权限，相关管理员与职位相对应； 不符合情况：已启用匿名登录模式。
	b)应重命名或删除默认账户，修改默认账户的默认口令	对于入侵检测的默认账户，由于他们的某些权限与实际要求可能存在差异，从而造成安全隐患，因此这些默认账户应被禁用	进入管理界面。用户进入Web管理页面后，在导航栏区域点击管理>系统设置，进入系统设置页面，点击管理员账号，可进入管理员账号配置页面。点击进入，查看账号的状态为active或block。 1)应核查是否重命名或删除这些默认账户 2)应核查是否已修改默认账户的默认口令 3）根据实际情况决定是否应该关闭默认账户	入侵检测重命名或删除默认账户，修改默认账户的默认口令。	符合情况：已重命名系统默认账户a*为***，且口令修改为复杂口令； 部分符合情况：未重命名系统默认账户a**,已修改口令为复杂口令； 不符合情况：未重命名系统默认账户名，口令为设备出厂默认口令。
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在	入侵检测中如果存在多余的、过期的账户，可能会被攻击者利用其进行非法操作的风险，因此应及时清理路由器中的账户，删除或停用多余的账户	进入管理界面。用户进入Web管理页面后，在导航栏区域点击管理>系统设置，进入系统设置页面，点击管理员账号，可进入管理员账号配置页面。用户权限等级分为level0-level3四个等级，对应审计、配置、管理、系统四个级别，根据用户需求分配权限等级。 1) 应核查入侵检测用户账户列表，询问管理员各账户的具体用途，分析是否存在多余或过期账户，并核查管理员用户与账户之间是否一一对应。 2)如果因为种种原因导致某些多余的、过期的账户无法被删除，则应测试是否已经停用了这些多余的	入侵检测用户账户列表不存在多余或过期账户，不存在共享用户。	符合情况：设备中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况； 部分符合情况：管理员用户与账户之间一一对应，未发现共享账户的情况，但a*、s*为多余账户； 不符合情况：可登录账户仅有a*，所有管理员均通过a*登录。
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限	进入管理界面。用户进入Web管理页面后，在导航栏区域点击管理>系统设置，进入系统设置页面，点击管理员账号，可进入管理员账号配置页面。 1)应核查是否进行角色划分，审计、配置、管理、系统四个级别，每个管理员有其特定权限和职责。 2)应查看管理用户的权限是否已进行分离，是否为其工作任务所需的最小权限，如禁止对管理用户同时赋予配置管理员和审计管理员权限。	1)系统用户进行角色划分，系统中的账户分为系统管理员、安全管理员和审计管理员三类。其中，安全管理员可以制定安全策略，系统管理员可以配置安全策略，审计管理员可以查看日志。 2)管理用户的权限进行了分离，并为其工作任务所费的最小权限，如禁上对管理用户同时赋予配置管理员和审计管理员权限。	符合情况：已配置安全管理员s*、审计管理员a*、系统管理员s*，授予管理用户所需的最小权限； 部分符合情况：已配置安全管理员s*、系统管理员s*，但未配置审计管理员； 不符合情况：可登录账户仅有a*，未授予管理用户所需的权限分离，实现管理用户的权限分离。
	e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作，访问控制粒度要求主体为用户级或进程级，客体为文件、数据库表级	进入管理界面，然后在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1)应核查是否进行角色划分，确认访问控制策略仅由管理员进行管理。	用户的访问控制规则由管理进行管理；	符合情况：用户的访问控制规则由管理进行管理。 不符合情况：管理员无法配置访问规则。

	f)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作、访问控制粒度要求主体为用户级或进程级，客体为文件、数据库表统	进入管理界面，在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1)访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作、访问控制粒度要求主体为用户级或进程级，客体为文件	访问控制规则由管理进行管理,主体为用户账号，客体未功能模块，访问控制力度未功能模块；	符合情况：访问控制规则由管理进行管理,主体为用户账号，客体为功能模块，访问控制力度为功能模块； 不符合情况：所有访问的模块均一
	g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	敏感标记是强制访问控制的依据，主客体都有,它存在的形式无所谓，可能是整形的数字，也可能是字母，总之它表示主客体的安全级别。敏感标记由安全管理员进行设置，通过对重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作，实现强制访问控制	进入管理界面，进入管理界面，在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1）查看是否有安全标记重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	查看到具有安全标记重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	符合情况：查看到具有安全标记重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 不符合情况：未设置敏感标记。
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	为了对入侵检测的运行状况、网络流量、管理记录等进行检测和记录，需要启用系统日志功能。系统日志中的每个信息都被分配了一个严重级别，并伴随一些指示性问题或事件的描述信息。 入侵检测的系统日志信息通常输出至本地或日志服务器或日志审计设备,在缺省情况下，控制台端口上的日志功能处于	进入管理界面。用户进入Web管理页面后，在导航栏区域点击管理>全局配置，单击选择“网关服务器配置”页签，可进行配置和查看网关服务器配置信息。 同时也可通过SNMP协议被日志审计设备采集日志数据。	入侵检测设置正确的日志审计服务器或设备地址、端口、以及日志类别等信息。	符合情况：已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户； 不符合情况：无审计模块，无法对重要的用户行为和安全事件进行审计。
	b)审计记录应包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息	对于入侵检测来说，审计内容应包括时间、类型、用户、事件类型、事件是否成功等相关信息	进入管理界面。可视>日志显示，进入日志页面中可查看。 登录日志审计设备，进入日志源配置界面，查看所有日志收集源。确保日志源列表中包含了该入侵检测设备的IP。 在日志审计设备上，根据IP地址选择入侵检测后，便可对该入侵检测的日志进行核查，确认是否包括日期和时间、用户、事件类型、事件是否成功等相	审计记录包括事件的日期和时间、用户事件类型、事件是否成功及其他与审计相关的信息。	符合情况：审计记录包括事件的日期和时间、用户事件类型、事件是否成功及其他与审计相关的信息。 部分符合情况：仅有用户信息、登录时间。 不符合情况：无审计模块。
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	审计记录能修帮助管理人员及时发现系统运行状况和网络攻击行为，因此需要对审计记录实施技术上和管理上的保护，防止未授权修改、删除和破坏	以奇安信IDS为例，该设备日志存储时间决定于设备内存容量，所以需要日志审计设备对入侵检测的日志信息进行定期备份。 登录日志审计设备，进入日志源配置界面，查看所有日志收集源。确保日志源列表中包含了该入侵检测设备的IP。 在日志审计设备上，根据IP地址选择入侵检测后，便可对该入侵检测的日志进行核查，确认是否包括日期和时间、用户、事件类型、事件是否成功等相关的信息。	入侵检测日志信息定期转发至日志服务器，日志服务器上可查看到半年前的审计记录	符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，并留存半年以上，能够避免受到未预期的删除、修改或覆盖； 部分符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，但审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖； 不符合情况：未对审计记录记录进行保护，审计记录仅留存7天，无
	d)应对审计进程进行保护，防止未经授权的中断	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容	应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护	非审计员的其他账户来不能中断审计进程，验证审计进程是否得到保护	符合情况：审计进程权限配置合理，仅授权用户可终止审计进程； 不符合情况：审计进程权限配置不合理，部分普通用户可关闭审计进
	a)应遵循最小安装的原则仅安装需要的组件和应用程序	遵循最小安装原则，仅安装需要的组件和应用程序，能够极大的降低遭受攻击的可能性。及时更新系统补丁，避免遭受由于系统漏洞带来的风险	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现
	b)应关闭不需要的系统服务、默认共享和高危端口	关闭不需要的系统服务、默认共享和高危端口，可以有效降低系统遭受攻击的	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现

入侵防范	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制	为了保证安全，避免未授权的访问，需要对远程管理入侵检测的登录地址进行限制，可以是某一特定的IP地址，也可以来自某一子网、地址范围或地址组	登录设备进行核查。进入管理界面,后在左侧导航树中选择系统管理》配置,查看登录地址限制列表；	设备本地设置访问控制列表限制终端接入范围。	符合情况：已限制终端接入地址范围，仅允许通过10.*.*.*/32地址进行管理； 部分符合：已限制终端接入地址范围，但限制登录地址范围为10.*.*.*/16，可登录地址范围过大； 不符合情况，未限制终端接入方式或网络地址范围，任意地址均可登
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求	本条款要求应用系统应对数据的有效性进行验证，主要验证那些通过人机接口(如程序的界面)输入或通过通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出错(如SQL 注入攻击等）,人而影响系统的正常使用甚至危害系统的安	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞	核查漏扫修补报告，管理员定期进行漏洞扫描。发现漏洞在经过充分测试评估后及时修补漏洞	1)应进行漏洞扫描，核查是否不存在高风险漏洞 2)应访谈系统管理员，核查是否在经过充分测试评估后及时修补漏洞	管理员定期进行漏洞扫描，发现漏洞，在经过充分测试评估后及时修补漏洞	符合情况：定期对安全设备进行漏洞扫描，发现漏洞及时修复，并形成报告。 部分符合情况：定期进行漏洞扫描，但未进行漏洞修复。 不符合情况：未定期进行扫描，且无法及时对漏洞进行修复。
	f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警	要维护系统安全，必须进行主动监视，一般是在网络边界、 核心等重要节点处部署IDS. IPS等系统，以检查息是否发生了入侵和攻击	此项不适合，该项要求一般在安全设备上实现	此项不适合，该项要求一般在安全设备上实现	符合情况：能够对所有的入侵时间进行拦截并记录。 部分符合：设备授权已过期，仅能对已知的攻击行为进行拦截。 不符合情况：设备未接入，无法实现入侵防御行为。
恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断	无论是Windows主机还是Linux主机，都面临木马、蠕虫等病毒的破坏。因此一般的主机为防范病毒，均会安装反病毒软件，或者采用可信验证机制对系统程序、应用程序等进行可信执行验证	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现。
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	设备应作为通信设备或边界设备对待	查看设备是否具有可信根芯片	查看设备是否具有可信根芯片	符合情况：安装了可信根芯片，对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 不符合情况：未安装可信根芯片，无法对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计