云安全运营服务

职业技能等级标准

（2021年1.0版）

奇安信科技集团股份有限公司 制定

2021年3月　发布

目次

前　　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准起草单位：奇安信科技集团股份有限公司。

本标准主要起草人（按姓氏笔画排序）：于京、王隆杰、王巍、左英男、叶伟、史宝会、冯涛、刘浩、孙从从、孙善学、杜辉、杨东晓、杨洪雪、何红、但唐仁、邹德清、张锋、范维博、岳洋、周国烛、郑长亮、赵利民、赵波、段晓光、唐辉、崔岳阳、董雪、管小清。

起草人来自以下单位：奇安信科技集团股份有限公司、北京电子科技职业学院、北京信息职业技术学院、北京工业职业学院、深圳信息职业技术学院、深圳职业技术学院、华中科技大学、武汉大学国家网络安全学院。

1 范围

本标准规定了云安全运营服务职业技能等级对应的工作领域、工作任务及职业技能要求。

本标准适用于云安全运营服务职业技能培训、考核与评价，相关用人单位的人员聘用、培训与考核可参照使用。

2 规范性引用文件

下列文件对于本标准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标准。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 32400-2015 信息技术 云计算 概览与词汇

GB/T 25069-2010 信息安全技术 术语

3 术语和定义

国家、行业标准界定的以及下列术语和定义适用于本标准。

3.1

系统 system

具有确定目的的、分立的、可识别的物理实体、由集成的、交互的部件构成，其中每一个部件不能单独达到所要求的整体目的。

[GB/T 32400-2015，定义2.1.46]

3.2

安全服务 security service

根据安全策略，为用户提供的某种安全功能级相关的保障。

[GB/T 25069-2010，定义2.1.47]

3.3

信息安全 Information security

维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、

可靠性等性质。

[GB/T 25069-2010，定义2.1.52]

3.4

对象 object

系统中可供访问的实体。例如：数据、资源、进程等。

[GB/T 25069-2010，定义2.1.21]

3.5

入侵 intrusion

对某一网络或联网系统的未经授权的访问，即对某一信息系统的有意无意的未经授权的访问（包括针对信息的恶意活动）。

[GB/T 25069-2010，定义2.1.27]

3.6

计算机信息系统 computer information system

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规划对信息进行采集、加工、存储、检索等处理的人机系统。

[GB/T 25069-2010，定义2.1.13]

3.7

信息安全事件 information security incident

由单个或一系列以外或有害的信息安全事态所组成的，极有可能危害业务运行和威胁信息安全。

[GB/T 25069-2010，定义2.1.53]

3.8

信息安全事态 information security event

被识别的一种系统、服务或网络状态的发生，表明一次可能的信息安全策略违

规或某些防护措施失效，或者一种可能与安全相关但以前不为人知的一种情况。

[GB/T 25069-2010，定义2.1.54]

3.9

信息系统安全 IT security

与定义、获得和维护保密性、完整性、可用性、可核查性、真实性和可靠性有关的各个方面。

[GB/T 25069-2010，定义2.1.57]

3.10

备份文件 backup files

一种用于以后数据恢复的文件。

[GB/T 25069-2010，定义2.2.3.1]

3.11

应急预案 contingency plan

一种关于备份、应急响应和灾后恢复的计划。

[GB/T 25069-2010，定义2.2.3.4]

3.12

灾难恢复计划 disaster recovery plan

信息系统灾难恢复过程中所需要的任务、行动、数据和资源的文件，用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能。

[GB/T 25069-2010，定义2.2.3.5]

3.13

安全功能 security function

在系统中实施安全策略的部分。

[GB/T 25069-2010，定义2.2.1.3]

3.14

安全功能策略 security function policy

描述了特定安全行为的一组规则，由系统安全功能执行并可表达为对系统的一组安全功能需求。

[GB/T 25069-2010，定义2.2.1.4]

3.15

安全机制 security mechanism

实现安全功能，提供安全服务的一组有机组合的基本方法。

[GB/T 25069-2010，定义2.2.1.5]

3.16

安全控制 security controls

为保护某一系统及其信息的保密性、完整性和可用性以及可核查性、真实性、抗抵赖性、私有性和可靠性等，而对信息系统所选择并施加的管理、操作和技术等方面的控制（级防御或对抗）。

[GB/T 25069-2010，定义2.2.1.7]

3.17

安全审计 security audit

对信息系统的各种事件及行为实行检测、信息采集、分析，并针对特定事件及行为采取相应的动作。

[GB/T 25069-2010，定义2.2.1.8]

3.18

安全事态数据 security event data

反映与系统、服务或网络安全状态有关的数据。例如：在入侵检测系统中由传感器收集和管理的信息。

[GB/T 25069-2010，定义2.2.1.9]

3.19

端口 port

某一个连接的端点。对于物理连接，端口就是物理接口；对于逻辑连接，端口则是传输控制协议或用户数据报协议的逻辑信道端点，例如80端口是默认的超文本传送协议（http）信道的端点。

[GB/T 25069-2010，定义2.2.1.37]

3.20

流量分析 traffic analysis

通过观察通信流量而推断所关注的信息，例如通信流量的存在、不存在、数量、方向和频次等。

[GB/T 25069-2010，定义2.2.1.85]

3.21

入侵检测 intrusion detection

检测入侵的正式过程。该过程一般特征为采集如下知识：反常的使用模式，被利用的脆弱性及其类型、利用的方式，以及何时发生及如何发生。

[GB/T 25069-2010，定义2.2.1.100]

3.22

入侵检测系统 intrusion detection system

在信息系统和网络中，一种用于便是某些已经尝试、正在发生或已经发生的入侵行为，并可对其做出响应的技术系统。

[GB/T 25069-2010，定义2.2.1.101]

3.23

基线 baseline

经过一个正式评审并通过的规约或产品，作为后续开发的基础。对其变更只有通过正式的变更控制规程可进行。

[GB/T 25069-2010，定义2.2.4.3]

3.24

安全策略 security policy

用于治理组织及其系统内在安全上如何管理、保护和分发资产（包括敏感信息）的一组规则、指导和实践，特别是那些对系统安全及相关元素具有影响的资产。

[GB/T 25069-2010，定义2.3.2]

3.25

安全服务 security service

根据安全策略，为用户提供的某种安全功能及相关的保障。

[GB/T 25069-2010，定义2.1.47]

3.26

安全目的 security objective

依照安全标准以及相应的方法，验证某一安全可交付与标准的符合程度及其安全保障程度。

[GB/T 25069-2010，定义2.3.7]

3.27

网络安全策略 network security policy

由陈述、规则和惯例等组成的集合，说明使用其网络资源的组织途径，并指明如何保护网络基础设施和服务。

[GB/T 25069-2010，定义2.3.92]

3.28

组织安全策略 organizational security policies

组织为保障其运行而规定的若干安全规则、规程、实践和指南。

[GB/T 25069-2010，定义2.3.117]

3.29

响应（不测事件响应或入侵响应） response（incident response or intrusion response）

当攻击或入侵发生时，为了保护和恢复信息系统正常运行的条件以及存储在其中的信息而采取的行动。

[GB/T 25069-2010，定义2.3.98]

3.30

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式。

[GB/T 32400-2015，定义3.2.5]

3.31

云部署模型 cloud deployment model

根据对物理或虚拟资源的控制和共享方式组织云计算的方式。

[GB/T 32400-2015，定义3.2.7]

3.32

云服务 cloud service

通过云计算已定义的接口提供的一种或多种能力。

[GB/T 32400-2015，定义3.2.8]

3.33

云服务客户 cloud service customer

为使用云服务而处于一定业务关系中的参与方。

[GB/T 32400-2015，定义3.2.11]

3.34

社区云 community cloud

云服务仅由一组特定的云服务客户使用和共享的一种云部署模型，这组云服务客户的需求相同，彼此相关，且由该客户成员对资源进行控制。

[GB/T 32400-2015，定义3.2.19]

3.35

混合云 hybrid cloud

至少包含两种不同的云部署模型的云部署模型。

[GB/T 32400-2015，定义3.2.23]

3.36

多租户 multi-tenancy

通过对物理或虚拟资源的分配实现多个租户以及他们的计算和数据彼此隔离和不可访问。

[GB/T 32400-2015，定义3.2.27]

3.37

私有云 private cloud

云服务仅被一个云服务客户使用，且资源被该云服务客户（3.29）控制的一类云部署模型。

[GB/T 32400-2015，定义3.2.32]

3.38

公有云 public cloud

云服务可被任意云服务客户使用，且资源被该云服务提供者控制的一类云部署模型。

[GB/T 32400-2015，定义3.2.33]

3.39

资源池化 resource pooling

将云服务提供者的物理或虚拟资源集成起来服务于一个或多个云服务客户。

[GB/T 32400-2015，定义3.2.34]

3.40

租户 tenant

对一组物理和虚拟资源进行共享访问的一个或多个云服务用户。

[GB/T 32400-2015，定义3.2.37]

3.41

安全域 security domain

在信息系统中，单一安全策略下运行的实体的汇集。例如，由单个或一组认证机构采用同一安全策略创建的各公钥证书的汇集。

[GB/T 25069-2010，定义2.2.1.17]

3.42

资产 asset

对组织具有价值的任何东西。

[GB/T 25069-2010，定义2.3.113]

3.43

组件 component

可包含在某一保护轮廓、安全目标或包中最小可选元素的集合。

[GB/T 25069-2010，定义2.3.116]

3.44

授权 authorization

赋予某一主体可实施某些动作的权力的过程。

[GB/T 25069-2010，定义2.1.33]

4 适用院校专业

中等职业学校：计算机应用、计算机网络技术、网络安防系统安装与维护、网络信息安全等相关专业。

高等职业学校：物联网应用技术、计算机应用技术、计算机网络技术、计算机信息管理、计算机系统与维护、信息安全与管理、云计算技术与应用等相关专业。

应用型本科学校：计算机科学与技术、网络工程、信息安全、物联网工程、智能科学与技术、信息与计算科学、信息管理与信息系统等相关专业。

5面向职业岗位（群）

【云安全运营服务】（初级）：基础运维工程师、云安全运维工程师、云安全运营工程师、网络安全运维工程师、（驻场）安全运营工程师。

【云安全运营服务】（中级）：云安全高级运营工程师、安全系统运营工程师、运营安全高级工程师、高级安全运营工程师、云安全技术运营工程师。

【云安全运营服务】（高级）：云安全运维专家、资深运维工程师、云安全解决方案工程师、云安全产品运营工程师。

6职业技能要求

6.1 职业技能等级划分

云安全运营服务职业技能等级分为三个等级：初级、中级、高级，三个级别依次递进，高级别涵盖低级别职业技能要求。

【云安全运营服务】（初级）：主要面向企事业单位、政府部门的私有云、社区云、混合云等云上业务系统，需要掌握以云上业务系统作为安全对象，使用云安全设备对云上业务系统进行安全环境基本配置和使用，掌握主机、云上主机的操作系统、应用系统的基本部署，以及满足安全基线的云上主机、云安全设备的基本操

作和维护作业，辅助云上业务系统的应急响应工作的执行。

【云安全运营服务】（中级）：主要面向企事业单位、政府部门的私有云、社区云、混合云等云上业务系统，掌握使用云安全设备对云上业务系统进行安全策略配置，对云上业务系统的告警信息进行响应和处置，掌握配置主机、云上主机的操作系统、应用系统的安全基线的技术和方法，以及云上业务系统和云安全设备的应急响应工作的执行。

【云安全运营服务】（高级）：主要面向企事业单位、政府部门的私有云、社区云、混合云等云上业务系统，需要掌握围绕云上业务系统的安全需求，参与云上业务系统安全运营的安全规划、安全建设和安全运营，对云上业务系统、云安全设备的安全缺陷制定针对性的修复解决方案。

6.2 职业技能等级要求描述

表 1 云安全运营服务职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1 资产管理	1.1 操作系统管理	1.1.1 能够按照标准操作手册，完成 Windows Server 操作系统的安装。
		1.1.2 能够按照标准操作手册，完成 Linux 操作系统的安装。
		1.1.3 熟练掌握 Windows Server 操作系统的基本命令与操作。
		1.1.4 熟练掌握 Linux 操作系统的基本命令与操作。
		1.1.5 熟练掌握虚拟化工具，完成虚拟化环境的镜像文件创建。
		1.1.6 熟练掌握虚拟磁盘格式转换工具，完成 VMDK、QCOW2、VHD、VDI 等磁盘格式之间的转换。
	1.2 应用系统管理	1.2.1 熟练掌握 Windows Server 操作系统中间件的部署方法，包括但不限于 Apache、Nginx、WebLogic。
		1.2.2 熟练掌握 Linux 操作系统中间件的部署方法，包括但不限于 Apache、Nginx、WebLogic。
		1.2.3 熟练掌握数据库系统的部署方法，包括但不限于 MySQL、SQL Server、Oracle、Redis、MongoDB。
		1.2.4 熟练掌握 SQL 命令，执行基本的增加、删除、修改、查询操作。
	1.3 网络管理	1.3.1 能够按照标准操作手册，配置交换机参数。
		1.3.2 能够按照标准操作手册，配置交换机引流向云安全设备。
		1.3.3 能够按照标准工作流程手册，做好工作记录。
	1.4 存储服务与管理	1.4.1 能够按照标准操作手册，对应用系统、数据进行全量备份操作。
		1.4.2 能够按照标准操作手册，对应用系统、数据进行增量备份操作。
		1.4.3 能够按照标准操作手册，对应用系统、数据进行差异备份操作。
		1.4.4 能够按照标准工作流程手册，做好工作记录。
2 日志管理	2.1 物理主机日志	2.1.1 能够掌握监控系统的安装，包括但不限于 nagios、cacti、zabbix、ganglia。
		2.1.2 能够按照标准操作手册，检查、收集监控

		系统运行状态。
		2.1.3 能够按照标准工作流程手册，提交监控系统偏差报告。
		2.1.4 能够按照标准工作流程手册，做好工作记录。
	2.2 网络日志	2.2.1 能够按照标准操作手册，检查、收集网络工作信息。
		2.2.2 能够按照标准工作流程手册，做好工作记录。
		2.2.3 能够按照标准工作流程手册，提交网络运行偏差报告。
	2.3 云主机日志	2.3.1 能够按照标准工作流程手册，检查、收集云主机威胁趋势信息。
		2.3.2 能够按照标准工作流程手册，检查、收集云主机安全事件信息。
		2.3.3 能够按照标准工作流程手册，检查、收集受攻击云租户信息。
		2.3.4 能够按照标准工作流程手册，检查、收集受攻击云主机信息。
		2.3.5 能够按照标准工作流程手册，检查、收集受攻击站点信息。
		2.3.6 能够按照标准工作流程手册，提交云主机安全告警报告。
		2.3.7 能够按照标准工作流程手册，做好工作记录。
	2.4 云安全设备日志	2.4.1 能够按照标准工作流程手册，检查、收集云安全设备服务健康状态。
		2.4.2 能够按照标准工作流程手册，检查、收集云安全设备物理资源分配率、物理资源使用率。
		2.4.3 能够按照标准工作流程手册，检查、收集云安全设备网络运行状态，网络流量、IP 资源池资源分配率。
		2.4.4 能够按照标准工作流程手册，检查、收集云安全设备性能运行状态，包括 CPU 使用率、内存使用率、磁盘使用率。
		2.4.5 能够按照标准工作流程手册，检查、收集云安全设备资源告警事件信息。
		2.4.6 能够按照标准工作流程手册，检查、收集云安全设备系统日志。
		2.4.7 能够按照标准工作流程手册，提交云安全设备运行偏差报告。
		2.4.8 能够按照标准工作流程手册，提交云安全设备告警报告。
		2.4.9 能够按照标准工作流程手册，做好工作记

		录。
	2.5 报表管理	2.5.1 能够根据业务场景和安全目的，保存云安全设备生成报表。
		2.5.2 能够根据业务需要和安全目的，删除云安全设备报表。
		2.5.3 能够按照标准工作流程手册，提交报表报告。
		2.5.4 能够按照标准工作流程手册，做好工作记录。
3 安全管理	3.1 安全基线	3.1.1 能够按照指定的安全基线方案，检查物理主机与安全基线方案的偏差。
		3.1.2 能够按照指定的安全基线方案，检查云主机与安全基线方案的偏差。
		3.1.3 能够按照标准工作流程手册，提交安全基线偏差报告。
		3.1.4 能够按照标准工作流程手册，做好工作记录。
	3.2 云安全设备管理	3.2.1 能够按照标准工作流程手册，检查、收集云安全设备授权状态。
		3.2.2 能够按照标准工作流程手册，做好工作记录。
	3.3 应急响应	3.3.1 能够按照应急工作流程手册，汇报紧急安全事件。
		3.3.2 能够按照标准工作流程手册，做好工作记录。

表 2 云安全运营服务职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1 资产管理	1.1 操作系统管理	1.1.1 能够按照安全目的或指定的安全基线方案，制作、发布满足安全目的的镜像。
		1.1.2 能够按照标准操作手册，使用镜像部署虚拟机。
		1.1.3 能够按照安全目的和标准操作手册，划分资产安全域。
		1.1.4 能够按照安全目的和标准操作手册，对业务资产进行安全服务编排。
		1.1.5 能够按照标准工作流程手册，做好工作记录。
	1.2 应用系统管理	1.2.1 能够按照安全目的或指定的安全基线方案，优化虚拟机系统的服务配置。
		1.2.2 能够按照安全目的或指定的安全基线方案，优化虚拟机系统的端口配置。

		1.2.3 能够按照安全目的或指定的安全基线方案，优化虚拟机系统的文件系统配置。
		1.2.4 能够按照标准工作流程手册，做好工作记录。
	1.3 存储管理	1.3.1 能够按照标准操作手册，使用指定的备份方式备份镜像文件。
		1.3.2 能够按照标准操作手册，使用指定的还原机制还原镜像文件。
		1.3.3 能够按照标准工作流程手册，做好工作记录。
2 日志管理	2.1 物理主机日志	2.1.1 熟练掌握监控系统的配置方法。
		2.1.2 能够处置监控系统偏差报告中的各类告警信息。
		2.1.3 能够按照标准工作流程，做好处置记录。
		2.1.4 能够按照标准工作流程手册，做好工作记录。
	2.2 网络日志	2.2.1 能够处置网络运行偏差报告中的各类告警信息。
		2.2.2 能够按照标准工作流程，做好处置记录。
		2.2.3 能够按照标准工作流程手册，做好工作记录。
	2.3 云主机设备日志	2.3.1 能够处置云主机安全告警报告中的受攻击租户告警信息，包括但不限于受攻击租户、受攻击主机、受攻击站点等。
		2.3.2 能够按照标准工作流程手册，做好处置记录。
		2.3.3 能够按照标准工作流程手册，做好工作记录。
	2.4 云安全设备日志	2.4.1 能够处置云安全设备运行偏差报告中的告警信息。
		2.4.2 能够处置云安全设备运行资源告警报告中的物理资源告警信息。
		2.4.3 能够处置云安全设备运行资源告警报告中的网络资源告警信息。
		2.4.4 能够处置云安全设备运行资源告警报告中安全组件资源使用告警信息。
		2.4.5 能够按照标准工作流程手册，做好处置记录。
		2.4.6 能够按照标准工作流程手册，做好工作记录。
	2.5 报表管理	2.5.1 能够根据业务场景和安全目的，分析报表报告内容。
		2.5.2 能够根据业务场景和安全目的，配置报表模板。

		2.5.3 能够根据业务需要和安全目的，按需生成一次性报表。
		2.5.4 能够按照标准工作流程手册，定期编制云安全运维情况报告。
		2.5.5 能够按照标准工作流程手册，做好工作记录。
3 安全管理	3.1 安全基线	3.1.1 能够按照指定的安全基线方案，配置物理主机管理策略，包括但不限于安装终端杀毒软件、仅开放必要的服务端口、组策略等。
		3.1.2 能够按照指定的安全基线方案，配置云主机管理策略，包括但不限于安装终端杀毒软件、仅开放必要的服务端口、组策略等。
		3.1.3 能够按照标准工作流程手册，做好工作记录。
	3.2 云安全设备管理	3.2.1 能够按照安全目的和标准操作手册，配置云安全设备授权。
		3.2.2 能够按照标准操作手册，完成云安全设备类型的添加、删除、修改工作。
		3.2.3 能够掌握云安全设备运行状态控制，包括设备的启动、停止等操作。
		3.2.4 能够根据业务场景和安全目的，设置云安全设备的安全策略，包括但不限于主机安全、防火墙、Web 应用防火墙、防篡改系统、数据库审计、漏洞扫描、堡垒机、日志审计、威胁感知、态势感知、云网安全分析、安全审计等云安全设备。
		3.2.5 能够按照标准工作流程手册，做好云安全设备的配置变更记录。
		3.2.6 能够按照标准工作流程手册，做好工作记录。
	3.3 应急处置	3.3.1 能在具备资质的工作人员指导下，辅助应急响应方案的执行。
		3.3.2 能够按照标准工作流程手册，做好工作记录。

表 3 云安全运营服务职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1 资产管理	1.1 操作系统管理	1.1.1 能够按照安全目的，编制 Windows 操作系统缺陷修复方案。
		1.1.2 能够按照安全目的，编制 Linux 操作系统缺陷修复方案。
		1.1.3 能够按照安全目的，编制镜像文件缺陷修复方案。

	1.2 应用系统管理	1.2.1 能够按照安全目的，编制应用软件漏洞缺陷修复方案。
		1.2.2 能按照安全目的，编制中间件缺陷修复方案。
		1.2.3 能按照安全目的，编制数据库缺陷修复方案。
	1.3 网络管理	1.3.1 能按照安全目的，编制路由缺陷修复方案。
		1.3.2 能按照安全目的，编制交换缺陷修复方案。
		1.3.3 能按照安全目的，编制虚拟局域网缺陷修复方案。
	1.4 存储管理	1.4.1 能够按照安全目的，编制数据备份方案。
		1.4.2 能够按照安全目的，编制数据容灾方案。
		1.4.3 能够按照安全目的，编制扩容方案。
2 日志管理	2.1 物理主机日志	2.1.1 能够根据业务场景和安全目的，审计物理主机日志内容。
		2.1.2 能根据审计结果，解决安全管理问题和缺陷。
		2.1.3 能按照标准工作流程手册，编写物理主机日志审计报告。
		2.1.4 能按照标准工作流程手册，做好工作记录。
	2.2 网络日志	2.2.1 能够根据业务场景和安全目的，审计网络设备日志内容。
		2.2.2 能根据审计结果，解决安全管理问题和缺陷。
		2.2.3 能按照标准工作流程手册，编写网络设备日志审计报告。
		2.2.4 能够按照标准工作流程手册，做好工作记录。
	2.3 云安全设备日志	2.3.1 能够根据业务场景和安全目的，审计云安全设备日志内容，包括但不限于主机安全、防火墙、Web 应用防火墙、防篡改系统、数据库审计、漏洞扫描、堡垒机、日志审计、威胁感知、态势感知、云网安全分析、安全审计等云安全设备。
		2.3.2 能根据审计结果，解决安全管理问题和缺陷。
		2.3.3 能按照标准工作流程手册，编写云安全设备日志审计报告。
		2.3.4 能够按照标准工作流程手册，做好工作记录。
	2.4 报表管理	2.4.1 能够根据业务场景和安全目的，分析云安

		全运维情况报告。
		2.4.2 能够根据云安全运维情况报告与安全目的的差异，编写云安全运维能力偏差报告。
		2.4.3 能够根据业务场景和安全目的，配置报表生成策略。
3 安全管理	3.1 安全基线	3.1.1 能够业务场景和安全目的，规划和设计安全基线方案。
		3.1.2 能够根据租户业务系统安全目的，制定安全运维服务计划，并持续改进。
		3.1.3 能够根据租户业务系统安全目的，制定服务编排方案，并持续改进。
		3.1.4 能够根据业务场景和安全目的，规划和设计安全能力方案。
	3.2 云安全设备管理	3.2.1 能够根据云安全设备的故障现象（非功能故障），设计、实施针对性的解决方案，包括但不限于主机安全、防火墙、Web 应用防火墙、防篡改系统、数据库审计、漏洞扫描、堡垒机、日志审计、威胁感知、态势感知、云网安全分析、安全审计等云安全设备。
		3.2.2 能够根据业务场景和安全目的，配置安全组件的 HA、集群模式，包括但不限于防火墙、WEB 应用防火墙等安全组件。
		3.2.3 能根据安全组件的告警、网络流量、日志等信息，对发生的安全事件进行关联分析和安全策略处置。
		3.2.4 能够根据租户业务系统安全目的，制定云安全设备整体解决方案。
		3.2.5 能够按照标准工作流程手册，做好工作记录。
	3.3 应急处置	3.3.1 能够按照指定的应急处理方案，对云安全设备采取紧急制动措施。
		3.3.2 能够按照指定的应急响应方案，对物理主机、云主机实施应急响应预案规定的动作。
		3.3.3 能按照标准工作流程手册，做好工作记录。

参考文献

[1] GB/T 1.1-2009 标准化工作导则

[2] 中等职业学校专业目录（含2019增补专业）

[3] 普通高等学校高等职业教育（专科）专业目录及专业简介

[4] 中等职业学校专业教学标准（试行）

[5] 高等职业学校专业教学标准（2018年）

[6] 普通高等学校本科专业类教学质量国家标准（2018年发布）

[7] 国家职业技能标准编制技术规程（2018年版）

[8] 中华人民共和国职业分类大典（2015年版）

[9] GB/T 25069-2010 信息安全技术 术语

[10] GB/T 31167-2014 信息安全技术 云计算服务安全指南

[11] GB/T 31168-2014 信息安全技术 云计算服务安全能力要求

[12] GB/T 32399-2015 信息技术 云计算 参考架构

[13] GB/T 32400-2015 信息技术 云计算 概览与词汇

[14] GB/T 34080.1-2017 基于云计算的电子政务公共平台安全规范 第1部分：总体要求

[15] GB/T 34080.2-2017 基于云计算的电子政务公共平台安全规范 第2部分：信息资源安全

[16] GB/T 34942-2017 信息安全技术 云计算服务安全能力评估方法

[17] GB/T 35279-2017 信息安全技术 云计算安全参考架构

[18] GB/T 36626-2018 信息安全技术 信息系统安全运维管理指南

[19] GB/T 36326-2018 信息技术 云计算 云服务运营通用要求

[20] GB/T 38249-2019 信息安全技术 政府网站云计算服务安全指南