网络安全（信息通讯网络运行管理员）职业技能竞赛题库及答案（251-450 单选题）

251、关于恢复设备出厂设置，以下说法不正确的是？

A、可以通过 console 口恢复出厂设置

B、可以通过升级客户端加载同版本升级包恢复出厂设置

C、可以通过设备控制台恢复出厂设置

D、可以通过交叉线恢复出厂设置

正确答案：A

252、某客户希望将 AC 设备网桥模式部署在出口路由器和内网三层核心交换机之间，但发现设备上架前，出口路由器和三层核心交换机之间的接口都是 TRUNK 模式，请问以下说法正确的是？

A、AC 网桥模式不支持 TRUNK 模式，所以当前环境无法使用网桥模式部署

B、AC 网桥模式可以支持该环境，AC 网桥配置 TRUNK 相关配置，只能通过某个 VLANIP 管理设备

C、AC 网桥模式可以支持该环境，AC 网桥配置 TRUNK 相关配置，

使用配置的某个 VLANIP 可以管理设备

D、AC 网桥模式部署成功后，不需要配置 VLAN 协议剥离也可以审计经过 QinQ 封装的数据

正确答案：C

253、当需要控制的 URL 地址不在内置 URL 库时，需要自定义 URL。下面关于自定义 URL 方式，不正确的是？

A、www.sangfor.com.cn

B、*.qq.com

C、www.bai*.com

D、sina.com

正确答案：C

254、下列选项中关于访问网站识别，说法正确的是？

A、URL 过滤是在 DNS 解析阶段阻断用户请求的网站

B、识别网站是在 TCP 三次握手成功以后

C、请求包中带请求动作不带请求具体的 URL

D、请求具体的 URL 在 User-agent 字段中

正确答案：B

255、深信服行为审计技术选项中说法错误的是？

A、审计的前提是内网用户先完成用户认证

B、审计的前置条件是数据经过 AC 设备或者镜像数据给 AC 设备

C、应用审计动作会对客户端有感知

D、AC 开启直通后，上网审计功能依然有效

正确答案：C

256、关于 PC 访问网站的通信过程，下列选项中说法错误的是？

A、发起访问网站请求，第一步先进行 DNS 解析

B、发起访问网站请求，第二步进行 TCP 三次握手

C、三次握手成功后，客户端发 get 请求

D、三次握手不成功，可能是因为 AC 设备拦截了 GET 请求

正确答案：D

257、AC 基于目标流控，不能基于什么目标流控？

A、网络应用

B、网站类型

C、文件类型

D、数据包内容

正确答案：D

258、以下关于静态路由的需求背景说法正确的是？

A、动态路由无法解决设备之间的跨网段互访

B、AC 网桥模式部署，也必须配置指向内网网段的回指路由

C、AC 路由表里面没有直连路由

D、静态路由主要用于解决设备之间跨网段的互访

正确答案：D

259、以下那个端口不是AC13.0.47版本的准入用来通讯的端口？

A、82

B、667

C、85

D、61111

正确答案：C

260、AC 外置数据中心，不同步以下哪种日志？

A、访问网页的 URL 记录

B、管理员操作日志记录

C、收发邮件的内容记录

D、AC 设备的系统日志记录

正确答案：D

261、升级 13.0.47 以上版本的必要硬件条件是什么？

A、4G 以上内存

B、4 核以上 CPU

C、四个网口以上

D、磁盘大小不低于 1T

正确答案：A

262、关于 SSL 内容识别功能实现的说法正确的是？

A、HTTPS 流量经过设备并被设备代理时会导致策略路由无法生效

B、用户认证之前访问 HTTPS 网站时也可以重定向到认证页面，设备无需额外配置其他配置

C、设备做了 SSL 内容识别，且 PC 没有安装证书，可能会出现网站无法打开或资源显示不全

D、SSL 内容识别功能只能在路由模式下生效

正确答案：C

263、AC13.0.47 版本，用户不需要认证上不了线，如下原因说明中错误的是？

A、上网流量未双向经过设备

B、用户绑定了错误的 MAC

C、IP 和 MAC 绑定关系错误

D、IP 被全局排除

正确答案：B

264、AC13.0.47，网桥模式部署，拒绝用户访问某网站，但是某网站还是可以正常打开，下面排查描述错误的是？

A、检查故障用户的 IP 是否开启了直通

B、检查故障用户的 IP 配置是否全局排除

C、检查用户流量是否经过设备

D、在URL分类库查询，该网站的分类是否是上网策略拒绝的类型，如果是则无需关注自定义应用

正确答案：D

265、认证策略设置为密码认证，终端要能重定向到认证页面，以下关于数据流的先后顺序说法正确是的？1、pc和公网服务器web服务器tcp三次握手2、pc访问AC设备的认证页面3、pc向公网服务器发送get/post请求4、pc和302重定向数据包里的地址建立三次握手5、AC设备向公网发rst中断连接，同时伪装成公网服务器向PC回复302重定向

A、1-2-3-4-5

B、1-3-5-4-2

C、1-3-5-2-4

D、1-2-4-3-5

正确答案：B

266、虚拟系统之间通过什么接口进行互访，下列说法正确的是哪项？

A、物理接口

B、VLAN 接口

C、子接口

D、虚拟接口

正确答案：D

267、客户在配置虚拟系统时发现虚拟系统无法支持根系统所有的功能，有些功能模块在虚拟系统下无法配置，关于虚拟系统不支持的功能模块下面说法错误的是哪项？

A、WEB 应用防护

B、漏洞攻击防护

C、应用控制策略

D、地域访问控制

正确答案：C

268、在客户现场进行病毒查杀的 POC 测试时，下面说法有误的是？

A、病毒样本不具有传染性，可以直接在现网环境下进行测试

B、在使用客户提供的病毒样本时，需要了解病毒文件的大小

C、在进行邮件病毒查杀前，需要明确邮件协议使用的端口

D、在进行文件病毒查杀前，需要明确文件传输使用的协议

正确答案：A

269、某客户发现大量源 IP 访问官网站点，导致业务访问缓慢，抓包发现该请求体表单中插入 sangfor 字段，如何针对该字段的请求体进行防护？

A、针对来源 IP 防 CC

B、Referer 防 CC

C、特定 URL 防 CC

D、自定义 CC 防护规则，针对表单数据进行匹配关键字进行检测

正确答案：D

270、AF 的业务安全中心，把事件根据风险进行分类，如果是检测到用户网站有黑链，而无其他风险记录，此类事件会被归到哪类？

A、已被入侵

B、曾被攻击

C、曾被收集信息

D、存在漏洞

正确答案：A

271、以下哪一项不会导致 AF 报错双机适配性不一致？

A、双机打包内容一致，但包的顺序不一致

B、双机开通的序列号不一致

C、双机心跳口 IP 配置不一致

D、虚拟路由组的监视口配置不一致

正确答案：C

272、以下哪个横块是通过机器学习，并建立访问基线对异常行为进行识别的?

A、SIEM 分析模块

B、UEBA 行为画像

C、威胁分析总览

D、访问关系

正确答案：B

273、在 SIP 平台安全告警中，解码小助手不支持（源内容）以

下那种解码方式？

A、URL

B、Base64

C、Unicode

D、utf-8

正确答案：D

274、在部署 STA 收集镜像流量的时候，需要很关注客户的网络情况,若没有做好镜像可能会影响检测效果,以下不包括哪一项检查？

A、镜像流量的封装协议是否支持

B、镜像流量的位置是否能采集到全面的流量

C、镜像流量中是否有 ipv6 协议

D、镜像流量中，是否以小包为主

正确答案：D

275、截止到 SIP3.0.66 版本，目前 SIP 平台可支持的推送告警有哪些？

A、短信通知

B、邮件通知

C、微信通知

D、以上都支持

正确答案：D

276、STA 不支持的 https 流量加密算法有哪些？

A、DES/3DES

B、AES

C、ECDH

D、ECDHE

正确答案：D

277、在 AC 配置用户信息同步到 SIP 的场景中，时常有转发端口没有添导致 SIP 上无法正常收到用户信息的情况，下列哪个端口是 SIP 接收用户信息的端口？

A、UDP1773

B、UDP1775

C、UDP443

D、UDP7443

正确答案：B

278、下列哪个SIP大屏中有安全域视角的数据展示？

A、综合态势大屏

B、网络攻击大屏

C、全球网络攻击态势

D、分支安全态势

正确答案：A

279、下列有关EDR基线检查功能说法正确的是？

A、可以检查windows系统是否符合基线要求，不符合项可以进行自动修复

B、可以检查Linux系统是否符合基线要求，不符合项可以进行自动修复

C、可以检查windows系统是否符合基线要求，对根据修复指导文档对不符合项进行修复加固

D、可以检查客户业务系统软件是否符合基线要求

正确答案：C

280、下列哪种 USB 设备不支持被外设管控功能进行管控？

A、U 盘

B、USB 移动硬盘

C、USB 鼠标键盘

D、USB 便携设备（手机、相机等）

正确答案：C

281、下列关于「威胁检测」功能说法错误的是？

A、支持终端病毒快速查杀、全盘查杀、强力专杀，以及导出查杀记录

B、支持基于 windows、linux 系统的终端漏洞扫描

C、支持配置添加终端文件的后缀例外扫描

D、支持 windows、linux 系统的终端基线检查

正确答案：C

282、下列哪个端口是终端 Agent 升级过程中使用的通信端口？

A、TCP443

B、TCP4430

C、TCP8083

D、TCP54120

正确答案：B

283、下列关于终端分组说法正确的是？

A、终端分组管理不支持通过手动添加分组的方式进行分组

B、终端自动分组管理不支持以 IP 地址段的方式进行自动分组

C、终端分组管理不支持 LDAP 同步的方式进行分组

D、未配置 LDAP 同步的情况下，新安装的终端默认会添加到未分组终端组里面

正确答案：D

284、linuxagent 部署对系统环境有一定要求，下列不是安装 agent 所必须的工具的是？

A、iptables

B、df

C、awk

D、ipset

正确答案：D

285、以下关于 agent 安装说法错误的是？

A、linux 环境可以指定目录安装

B、Windows 环境可以指定目录安装

C、Linux 终端 ping 不通 mgr 会导致安装失败

D、Windows 终端 ping 不通 mgr 会导致安装失败

正确答案：D

286、针对零信任 aTrust 接入场景描述，下列说法错误的是？

A、远程办公接入场景是零信任 aTrust 的基础功能场景

B、远程办公接入场景，可实现隐藏内网业务服务器对外暴露的端口，收缩暴露面

C、远程办公接入场景下，同时也是需要客户将内网业务服务器的相关业务端口映射到公网

D、远程办公接入场景下，只需要暴露零信任 aTrust 的相关端口即可

正确答案：C

287、在发布 http 和 https 资源进行访问时，零信任采用何种代理？

A、使用客户端进入隧道，代理网关直接代理访问

B、反向代理技术

C、正向代理技术

D、同时使用正向代理和反向代理

正确答案：B

288、atrust 与微软 AD 域对接实现用户认证，以下相关说法正确的是？

A、atrust 设备端不需要进行任何配置，只需在 AD 域进行配置，即可进行对接认证

B、同步用户信息包含用户组织结构、用户名、用户密码等信息

C、必须要将 AD 域用户同步到 atrust 设备才能用于用户认证

D、对接 AD 服务器后如果需要精细化的授权，必须要把用户或者用户组导入到本地，才能进行精细化授权

正确答案：D

289、零信任 aTrust 替换 SSLVPN 场景下列说法正确的是？

A、支持将 SSLVPN 设备的所有配置导入到零信任 aTrust 设备

B、只允许将 SSLVPN 的用户、用户组导入零信任 aTrust 设备

C、允许将 SSLVPN 的用户、用户组、角色、应用和应用组之间的关联关系导入至零信任 aTrust 设备

D、SSLVPN 设备导入零信任 aTrust 设备，不受版本的限制

正确答案：C

290、某用户在使用零信任的时候，使用本地账号密码作为认证，为了增加安全性，需要用户进行二次认证，在授信终端上可以免二次认证，授信终端可以自助绑定。同时在首次登录的终端上需要进行增强认证，二次认证和增强认证方式都是短信验证码，那么一个新入职的员工首次登录的场景会是以下那种情况？

A、用户账号密码登录，成功登录，手动绑定授信终端，然后收到一次短信验证码

B、用户账号密码登录，收到两次短信验证码，登录成功，手动绑定授信终端

C、用户账号密码登录，收到一次短信验证码，登录成功，手动绑定授信终端

D、用户账号密码登录，收到一次短信验证码，登录成功，再收到一次短信验证码，手动绑定授信终端

正确答案：B

291、关于 aTrust 联动 VDI 场景，以下说法错误的是？

A、零信任 aTrust 联动 VDI 后，不需要将 VDI 的相关的端口映射，也能通过 aTrust 实现远程运维。

B、目前 VDI 仅专有桌面以及非加域场景的虚拟应用支持 aTrust 单点登录，还原桌面与加域场景的虚拟应用均不支持。

C、需要保证 VDC 本地有与 aTrust 认证用户相同的账号或者组织结构，才可正常联动登录并获取 VDI 资源信息

D、只要 aTrust 版本大于 2.1.17，就能支持与 VDI 对接，对 VDI 版本没有要求。

正确答案：D

292、客户反馈将 LDAP 用户/组织架构导入 aTrust 失败，如下哪个原因说明是错误的？

A、配置的 LDAP 管理员账号权限不足

B、LDAP 服务器是 openldap，用户属性的过滤条件配置为（objectCategory=person）

C、LDAP 服务器不支持分页处理

D、aTrust 当前仅支持将 AD 域的组织架构导入设备，其他类型 LDAP 服务器不支持将组织架构导入设备

正确答案：D

293、所有用户打不开用户登录页面，如下原因错误的是？

A、设备没配置客户端接入地址

B、用户关联的资源包含用户接入地址

C、441 端口没有一对一映射

D、开启了 spa 功能，没有安装专属客户端或没有使用安全码接入

正确答案：C

294、发布隧道应用，用户接入 atrust 后访问内网应用失败了，如下哪个原因说明是错误的？

A、代理网关 441 端口未映射

B、资源地址或协议配置错误

C、启用了虚拟 IP，内网没有写回包路由指向 aTrust 代理网关/综合网关

D、控制中心到内网服务器之间有安全设备拦截导致控制中心无法访问内网应用

正确答案：D

295、客户需要通过堡垒机访问内网的门户网站，以下访问流程正确的是？

A、客户端->OSM->门户网站

B、客户端->应用发布服务器->门户网站

C、客户端->OSM->应用发布服务器->门户网站

D、客户端->应用发布服务器->OSM->门户网站

正确答案：C

296、等级保护制度是中国网络安全保障的特色和基石，等级保护建设的流程是？

A、定级、备案、监督检查、建设整改、等级测评

B、定级、备案、建设整改、等级测评、监督检查

C、建设整改、等级测评、监督检查、定级、备案

D、等级测评、定级、备案、建设整改、监督检查

正确答案：B

297、测评环节中，我司需要协助测评机构进行测评，以下哪份材料可以帮助我们高效完成测评？

A、《深信服等保技术差距分析表（含高风险项）

B、《等保建设规划方案》&《等保建设实施方案》

C、《深信服安全产品等保三级场景配置指导手册集》

D、《深信服安全产品等保佐证说明》

正确答案：D

298、安全整改环节中，我司在设备上架过程中做等保的合规配置，以下那份材料可以帮助高效完成安全整改？

A、《深信服等保技术差距分析表（含高风险项）

B、《等保建设规划方案》&《等保建设实施方案》

C、《深信服安全产品等保三级场景配置指导手册集》

D、《深信服安全产品等保佐证说明》

正确答案：C

299、小明准备给客户的环境做合规自检，帮助客户检查服务器的合规情况，但客户对数据有保密性的要求，不愿意把设备名密码直接给我们，且只允许数据存在本地，以下哪种检测方式适合该客户的环境？

A、纪元平台（aCheck）+云平台在线检测

B、纪元平台（aCheck）+云平台离线检测

C、部署软件云镜检测

D、以上检测方式均不合适

正确答案：C

300、HTTPS 前期的 SSL 握手阶段加密方法以及 SSL 握手协商成功后使用的加密方法分别是什么？

A、均是非对称加密

B、均是对称加密

C、对称加密，非对称加密

D、非对称加密，对称加密

正确答案：D

301、PC 访问 baidu.com，会先进行 DNS 解析，若没有本地没有

DNS 缓存，会请求 LDNS 做 DNS 查询，若 LDNS 本地无缓存，LDNS 会向外部的 DNS 服务器做 DNS 查询。请问这个过程中，PC-LDNS 使用的是什么方式的 DNS 查询，LDNS-外部 DNS 服务器使用的是什么方式的 DNS 查询？

A、迭代查询，递归查询

B、递归查询，迭代查询

C、递归查询，递归查询

D、迭代查询，迭代查询

正确答案：B

302、关于堆叠、VRRP、MLAG，以下说法错误的是？

A、堆叠是指多台支持堆叠特性的单机设备组合在一起，从逻辑上合为一台整体设备

B、MLAG 是一种链路聚合的技术，实现链路高可用。较于堆叠，MLAG 不支持跨设备链路聚合，堆叠可实现多台设备做链路聚合

C、VRRP 虚拟路由协议通过几台设备组成一台虚拟的路由设备，把虚拟路由设备的 IP 地址作为用户的默认网关实现通信。

D、堆叠较于 VRRP 和 MLAG，简化了网络的管理和日常运维。

正确答案：B

303、防止计算机中信息被窃采取的手段不包括？

A、用户识别

B、权限控制

C、数据加密

D、病毒控制

正确答案：D

304、关于 SQL 注入攻击。下列说法错误的是？

A、查询以输出他人数据，导致数据泄密

B、查询以提升服务器的防 DDOS 能力

C、插入修改现有数据

D、删除现有数据

正确答案：B

305、关于 HTTP 协议说法正确的是？

A、发布 HTTP 网站不能使用 443 端口发布

B、响应状态码 502 一般为客户端浏览器解析异常

C、HTTP1.0 协议限制了服务器只能被动响应客户端请求

D、HTTP 协议是应用层协议

正确答案：C

306、以下关于 AD 域成员和 AD 域控通信会使用到的协议/服务错误的是?

A、Kerberos

B、LDAP

C、STP

D、SMB

正确答案：C

307、下列有关认证模式的说明，正确的一项是？

A、分支 AC 接入认证中心 AC 后，依然可以在分支 AC 上自行配置 Portal 认证策略

B、用户每次上线时，都会把用户信息上传到认证中心 AC

C、分支 AC 如果没有配置[认证托管/LDAP 服务端口]或认证中心没有开启 LDAP 服务，分支会通过增量的方式在本地新增用户组/用户

D、用于认证中心 AC 重定向的 80 端口可以自行修改

正确答案：C

308、关于短信认证，下列选项说法正确的是？

A、短信认证属于令牌认证

B、短信认证必须结合密码认证使用

C、短信认证用于人员较为固定的场景

D、短信认证的好处是用户不需要记忆密码

正确答案：D

309、关于用户绑定功能选项中说法错误的是?

A、免认证和不需要认证是同一种认证方式

B、免认证是已通过认证用户，下次登录不需要再次认证（用户无感知上线）

C、限制登录是用户只能在某个限定的 IP/MAC 范围内进行认证；

D、免认证与不需要认证，对于用户第二次及以后的登录，实现效果是相同的

正确答案：A

310、下列选项中，关于关于 B/s 和 b/s 的关系（B/s 表示 Byte/s，b/s 表示 bit/s），正确的是？

A、1MB/s=10Mb/s

B、1MB/s=8Mb/s

C、1Mb/s=1000KB/s

D、1Mb/s=10MB/S

正确答案：B

311、流量管理为了更好的呈现效果，选项中说法错误的是?

A、设备刚上架不了解流量类型，可以在流量管理状态查看（已启用流控模块）

B、流量管理状态可以查看当前每个通道的带宽使用情况

C、流量可视只能查看限制通道，不支持查看保障通道

D、流量可视支持查看动态流控趋势

正确答案：C

312、客户采购了某安全杀毒软件，希望实现未运行杀毒软件的终端不能上网，下列选项中说法错误的是？

A、客户可以通过深信服 AC 的终端准入规则策略实现

B、准入规则定义需检查持续运行的进程名

C、准入客户端支持在 Windows 和 macOS 系统安装

D、如果客户端没有运行杀软，可以实现禁止上网并提醒终端客户

正确答案：C

313、下列关于 RADIUS 协议描述不准确的是？

A、当 AC/SG 使用外部 RADIUS 认证时，AC/SG 充当 RADIUS 客户端角色

B、使用外部认证时，AC/SG 和 RADIUS 服务器进行交互，认证协议支持 PAP、CHAP 和 EAP-MD5

C、使用 PAP 过程中，AC/SG 会传递用户名和密码等相关信息给 RADIUS 服务器

D、使用 CHAP 过程中，AC/SG 会传递用户名和密码等相关信息给 RADIUS 服务器

正确答案：D

314、全局排除了某个域名，但是时而不生效，以下原因不可能的是？

A、DNS 流量不经过设备

B、用户未认证上线

C、AC 设置的 DNS 服务器和终端 PC 不一致

D、访问该域名流量不经过设备

正确答案：B

315、OA 认证的流程正确的？①、用户访问外网被重定向到认证页面②、点击图标放通流量并重定向到授权页面③、终端和 OA 服务器通信完成后重定向到回调域名并返回 code 参数给 AC 设备④、扫二维码或点击授权按钮授权登录⑤、AC 通过 tocken 参数获取 OA 服务器的用户信息并完成认证⑥、AC 通过 code 参数从 OA 服务器获取 tocken 参数

A、①->②->④->③->⑥->⑤

B、①->②->③->④->⑥->⑤

C、①->②->③->④->⑤->⑥

D、①->②->④->③->⑤->⑥

正确答案：A

316、关于脚本单点登录说法错误的是？

A、脚本单点登录成功，需要 AC 和域服务器能正常通讯

B、脚本单点登录成功，需要 PC 正常加入域

C、脚本单点登录成功，需要 PC 和 AC 能正常通讯

D、脚本单点登录成功，需要保证秘钥填写正确

正确答案：A

317、AC12.0.44 的 admin 启用别名登录后，下面说法正确的是？

A、启用别名后，也能够使用 admin 登录控制台

B、交叉线恢复密码后，别名并不会恢复

C、交叉线恢复默认配置后，别名设置会恢复

D、只有 admin 用户才可以设置别名

正确答案：A

318、下面关于新架构带外管理口的说法有错误的是？

A、禁用带外管理时，管理口不能作为业务口使用

B、启用带外管理时，业务网段和管理网段有冲突也不会影响设备的管理

C、启用带外管理时，设备的规则库更新优先通过管理口更新的

D、禁用带外管理时，需要单独添加默认路由

正确答案：A

319、关于新架构双机的特点说法错误的是？

A、新架构双机支持路由主主模式，可以建立不同的虚拟组和虚拟 IP 来实现流量的负载

B、新架构双机可以不配置数据同步接口，直接使用心跳接口

C、新架构双机在接口配置中无法填写-HA 的地址

D、新架构双机路由主备镜像模式需要配置虚拟 IP 地址，进行路由转发

正确答案：D

320、AF 开启恶意域名重定向的注意事项说法错误的是？

A、内网用户上网的流量是双向经过 AF 设备

B、内网为 DNS 服务器代理环境

C、非内网为 DNS 服务器代理环境不能开启恶意域名重定向

D、僵尸网络防护功能默认不启用恶意域名重定向，需要手动开启

正确答案：C

321、关于 AF 老架构双机原理，下列说法错误的是？

A、主备部署时，优先级大的为主，在相同优先级时，会比较心跳口 IP 地址，IP 大的为主

B、主备部署时，主设备是通过虚拟 IP 与对方通信

C、主备部署时，主设备是通过虚拟 MAC 与对方通信

D、如果想某接口的 IP 不同步到备控设备，可在接口配置的 IP/掩码后面加“-HA”

正确答案：B

322、AF 开启了应用控制策略记录日志，但是查询不到动作为允许的应用控制策略日志，下列原因错误的是？

A、应用控制策略未开启日志记录选项

B、应用控制策略未匹配上，所以未记录到日志

C、设备磁盘大小为 32G

D、AF 产品不支持记录动作为允许的应用控制策略

正确答案：D

323、以下关于态势感知的级联功能说法不正确的是？

A、级联默认使用 7443 端口，可以自定义使用端口

B、首次接入，下级会上报近 1 个月的安全事件相关信息（下级平台可配置），接入之后，会 5min/次增量上报；

C、上下级如果存在资产冲突的情况，针对安全事件，在[处置中心/威胁视角/安全事件]页面，可以根据资产导航来区分是上级还是下级，针对安全告警，可以在[重保中心]页面，根据数据来源区分是上级还是下级

D、上级和下级平台之间存在 NAT 时不能使用级联功能

正确答案：D

324、在安全运营建设的项目中，一般都会涉及到剧本的编写，下面关于剧本说法不对的是？

A、剧本承载的是结合组织与人员、技术和工具、机制与流程的数字化安全过程，是安全自动化和数字化的核心元素

B、日常事务型的剧本用于辅助处理如漏洞管理、威胁情报管理等日常运营事务的剧本。这类剧本融入到安全运营人员的日常事务和

企业流程当中，或是能大大简化流程，或是能减少人工操作，以大幅减少运营人员的日常琐事

C、应急预案型剧本通常是冷剧本，需要手动执行，用于推动一个或多个工作流的执行。帮助团队应对突发的紧急情况

D、一个好的剧本，使用频率和通用性不用纳入考量当中

正确答案：D

325、小王在进行 SOAR 编写的时候，需要配置联动 EDR 对主机进行病毒查杀，请问小王应该使用什么节点实现？

A、过滤节点

B、决策节点

C、动作节点

D、审核节点

正确答案：C

326、轻量版的安全运营解决方案中，客户使用的是 SIP 作为平台，关于 SIP 分析思路正确的是？

A、首先关注重保中心的事件，优先考虑攻击成功，失陷的，可以通过筛选条件进行筛选

B、可信度：安全事件>安全告警>安全日志

C、在重保中心筛选完成后，可以通过日志检索进行分析。首先筛选出安全检测日志，可以看到多种攻击类型.

D、以上都正确

正确答案：D

327、在SIP【系统维护】-【系统检测】中检测到硬盘异常，下列情况中最可能造成该问题的是？

A、SIP是1U设备

B、SIP是测试设备，部分磁盘插槽没有插磁盘

C、SIP组了集群

D、SIP版本为非标准版本

正确答案：B

328、关于sip分析中心残余攻击的说明正确的是？

A、残余攻击是指部署在防御体系之后的探针检测到的攻击

B、残余攻击是指sip检测到了威胁情报但edr查杀不出的场景

C、残余攻击是指SIP不支持检出的攻击

D、残余攻击是指由于sta镜像流量不全导致漏掉攻击数据

正确答案：A

329、下列有关 EDR 单个管理端支持接入最大终端数量是？

A、5000 点

B、8000 点

C、10000 点

D、20000 点

正确答案：C

330、下列关于 EDR 级联部署中，下级管理端通过（）方式建立连接将数据上报给到上级管理平台？

A、SSH

B、HTTPS

C、SFTP

D、HTTP

正确答案：A

331、下列关于 LDAP 同步功能说法正确的是？

A、当安装 Agent 终端以域帐号登录域、并触发 LDAP 同步后，域用户信息才会同步至本地用户并根据 OU 自动分组

B、用户信息同步支持同步域账号中的用户名、电话、邮箱等属性，但不支持映射到本地账号属性

C、EDR 仅支持定时自动 LDAP 同步，无法通过手动触发的方式进行同步

D、LDAP 同步的域用户到 EDR 后，可以在系统管理中的账号管理进行查看

正确答案：A

332、下列关于 EDR 支持的终端补丁包下载方式说法错误的是？

A、终端可以通过 EDR 平台上下载系统补丁包

B、终端第一优先从 EDR 管理平台上下载系统补丁包，且不支持调整该优先顺序

C、EDR 可以设置终端从自身互联网出口链接到微软官方补丁站点进行下载

D、EDR 可以设置终端从客户内网 WSUS 补丁更新服务器进行下载

正确答案：B

333、关于 EDR 的端网联动功能说话正确的是？

A、EDR 会根据内置的僵尸网络规则库定位访问恶意域名的进程

B、联动取证到进程之后必须到发起联动的设备处置对应文件

C、EDR 会采集全网终端访问域名和进程情况，上报给发起联动的设备分析异常进程

D、端指的是 EDR 终端安全产品，网指的是网络侧的 A

F、SIP 安全产品

正确答案：D

334、客户反馈 EDR 安装之后电脑特别卡慢。以下处理思路正确的是？

A、关闭实时监控测试是否正确，如果关闭正常，建议客户后续该电脑不要开启实时监控

B、测试重命名实时监控驱动是否正常，如果修改正常，可以告知客户已经解决

C、禁用所有微隔离策略确认是否微隔离拦截数据导致电脑卡慢

D、确认进程占用情况，是否 edr 杀毒导致电脑卡

正确答案：D

335、关于 aTrust 的认证策略，下列说法错误的是？

A、用户首次认证，可以配置多种认证方式

B、增强认证中的“账号弱密码登录”针对的账号是外部用户账号

C、移动端和 PC 端支持的增强认证和二次认证类型一样

D、配置了豁免规则，在满足条件的情况下，可以实现免二次认证。

正确答案：C

336、关于配置 WEB 模式资源时，以下哪项是正确的？

A、后端服务器地址可以是 IP 或者是域名

B、前端服务器地址只能是域名

C、发布的 web 资源一定要上传授信证书

D、客户没有授信证书时，可以用设备自带证书，进行应用发布

正确答案：C

337、关于 VPN 配置转换工具的用法，下列说法正确的是？

A、skip 命令，能实现将重名的用户、资源、将跳过不导入，但重名的角色会覆盖。

B、add 命令，能实现能实现将重名的用户、资源、角色将跳过不导入。

C、-n 参数，能否实现将资源归属到指定的区域，默认会归属到 Default 区域中。

D、--hide 参数能实现把外部用户导入到指定的用户目录中

正确答案：C

338、客户黄工正在对接 oauth2 认证，其中 aTrust 地址为 https：//sdpc.company.com；OAuth2.0 认证服务器地址为 https：//sso.company.com。oauth2.0 票据认证服务器简化流程正确的是？

1、浏览器输入客户端接入地址 https：//sdpc.company.com

2、访问 https：//sso.company.com/oauth2/token 获取认证 ticket 票据信息

3、控制中心重定向至 OAuth2.0 认证服务器登录地址：https：//sso.company.com/oauth2/authorize 访问认证门户页面

4、用户认证：https：//sso.company.com/oauth2/get_user_info 获取用户信息

5、用户退出登录：https：//sso.company.com/oauth2/user_logout 用户注销

A、1-2-3-4-5

B、1-3-2-4-5

C、1-4-3-2-5

D、1-3-4-2-5

正确答案：B

339、关于本地集群和分布式集群，下列说法错误的是？

A、设备组建集群后，接入地址为 SDPC 的集群 IP，需要把客户端接入地址改成集群 IP 的地址，若做了端口映射，则需修改成 SDPC 的集群 IP 映射后的地址

B、SDPC 和 Proxy 各自组建集本地群后，SDPC 会自动同步配置，Proxy 不会同步配置

C、控制中心、代理网关和综合网关，都可配合智能 DNS 方案组建分布式集群组建，实现跨数据中心的高冗余和高可靠性

D、即使版本一致，性能配置一致，网络通信正常，硬件设备和软件设备也不能组建本地集群

正确答案：C

340、用户 AD 域认证的过程是怎样的？①用户选择 AD 域认证输入账号密码，SDPC 将认证的数据转发到 AD 域服务器；②用户向 SDPC 请求认证页面，SDPC 向用户返回输入账号密码的页面；③认证通过下发用户策略和用户资源到客户，登入完成；④AD 域进行账号密码的校验，并将结果返回到 SDPC；

A、①②③④

B、②①④③

C、①②④③

D、①④②③

正确答案：B

341、关于 atrust 对接桌面云 VDI 方案说法错误的是？

A、aTrust2.2.4-2.2.10 版本支持对接 VDI5.5.2 版本工作台模式

B、VMP 需要开放 5500-5699、8888 端口

C、aTrust 对接的客户端仅支持 WIN7、WIN10 和 MAC 终端

D、VDI 的还原桌面模式支持单点登录虚拟机功能

正确答案：D