CompTIA Cybersecurity Analyst (CySA+) 认证考试目标

考试编号：**CS0-001**

CompTIA

关于考试

CompTIA Cybersecurity Analyst (CySA+) 认证是一种厂商中立的认证。CompTIA CySA+ 考试是一种国际公认的中级安全技能和知识认证。不设先决条件，CompTIA CySA+ 认证的意图是通过 CompTIA Security+ 认证或同等经验，专注于 IT 安全分析的技术和实践技能。

CompTIA CySA+ 考试专为 IT 安全分析师、漏洞分析师或威胁情报分析师而设。本考试将证明及格考生具有配置和使用威胁检测工具，进行数据分析并解析结果，以识别组织漏洞、威胁和风险，从而保持组织内应用和系统安全所需的知识和技能。

我们建议 CompTIA CySA+ 认证考生具有以下条件：

- **3-4 年信息安全技能或相关经验**
- **Network+、Security+ 或同等知识**

CompTIA 授权材料使用政策

CompTIA Certifications, LLC 与未经授权的第三方培训网站毫无关联，亦不授权、背书或容忍任何人使用所提供的任何内容（也称为“信息垃圾”）。依照 CompTIA 考生协议，对于在准备任何 CompTIA 考试时使用此类材料的个人，我们将取消其证书，并将暂停其参加以后的考试。为了更明确地传达 CompTIA 有关使用未授权学习材料的考试政策，CompTIA 建议所有认证考生访问 **CompTIA 认证考试政策**。在开始任何 CompTIA 考试的学习过程之前，请查看所有 CompTIA 政策。考生将需要遵守 **CompTIA 考生协议**。如果考生对于某种学习材料是否被视为未授权（也称为信息垃圾）存有疑问，他/她应通过 examsecurity@comptia.org 联系 CompTIA 确认。

请注意

以项目符号列示的示例列表并不详尽。其它与各目标有关的技术、程序或任务示例，尽管没有列示或写入此目标文档，也可能列入考试范围。CompTIA 正持续审核我们考试的内容并更新考试问题，确保我们的考试是最新的，且问题的安全性得到保护。如有必要，我们将发布基于现有考试目标的更新版考试。但请记住，所有相关考试准备材料将仍有效。

考试细节

必考科目	CS0-001
问题数量	最多 85 个问题
问题类型	多选题和实机操作题
考试时长	165 分钟
推荐经验	Network+、Security+ 或同等知识。 最少 3-4 年信息安全技能或相关经验。不设先决条件，CySA+ 认证的意图是通过 CompTIA Security+ 认证或同等经验，专注于技术和实践技能。
及格分数	750 分（100-900 分制）

考试目标（领域）

下表列示了本次考试的考核领域及其范围。CompTIA CSA+ 考试则基于这些目标。

领域	考试占比
1.0 威胁管理	27%
2.0 漏洞管理	26%
3.0 网络事件响应	23%
4.0 安全架构和工具集	24%
总数	**100%**

1.0 威胁管理

1.1 设立前提，利用适当工具和程序应用环境侦查技术。

- **程序/常见任务**
  - 拓扑发现
  - 操作系统指纹识别
  - 服务发现
  - 包捕获
  - 日志审查
  - 路由/防火墙 ACL 审查
  - 电子邮件获取
  - 社交媒体分析
  - 社会工程
  - DNS 获取
  - 网络钓鱼
- **变量**
  - 无线与有线
  - 虚拟与物理
  - 内部与外部
  - 本地与云
- **工具**
  - NMAP
  - 主机扫描
  - 网络映射
  - NETSTAT
  - 封包分析器
  - IDS/IPS
  - HIDS/NIDS
  - 基于防火墙规则和日志
  - Syslog
  - 漏洞扫描器

1.2 设立前提，分析网络侦查结果。

- **时间点数据分析**
  - 封包分析
  - 协议分析
  - 流量分析
  - Netflow 分析
  - 无线分析
- **数据关联和分析**
  - 异常分析
  - 趋势分析
  - 可用性分析
  - 启发式分析
  - 行为分析
- **数据输出**
  - 防火墙日志
  - 包捕获
  - NMAP 扫描结果
  - 事件日志
  - Syslogs
  - IDS 报告
- **工具**
  - SIEM
  - 封包分析器
  - IDS
  - 资源监视工具
  - Netflow 分析器

1.3 给定一个基于网络的威胁，实施或建议适当的响应和对策。

- **网络分段**
  - 系统隔离
  - 跳线盒
- **诱捕蜜罐**
- **端点安全**
- **组策略**
- **ACL**
  - 隧道
- **强化**
  - 强制访问控制（MAC）
  - 补偿控件
  - 阻止未用端口/服务
  - 打补丁
- **网络访问控制（NAC）**
  - 基于时间
  - 基于规则
  - 基于角色
  - 基于位置

1.4 解释用于保护企业环境的实践的用途。

- 渗透测试
  - 参与原则
    - 定时
    - 范围
    - 授权
    - 开发
    - 沟通
    - 报告
- **逆向工程**
  - 隔离/沙盒化
  - 硬件
    - 硬件来源真实性
    - 可信代工厂
    - OEM 文件
  - 软件/恶意软件
    - 指纹识别/散列
    - 分解
- **培训与练习**
  - 红队
  - 蓝队
  - 白队
- **风险评估**
  - 技术控制审查
  - 运行控制审查
  - 技术影响与可能性
    - 高
    - 中
    - 低

2.0 漏洞管理

2.1 设立前提，实施信息安全漏洞管理程序。

- **识别要求**
  - 监管环境
  - 企业政策
  - 数据分级
  - 资产库存
    - 关键
    - 非关键
- **确定扫描频率**
  - 风险偏好
  - 监管要求
  - 技术限制
  - 工作流程
- **根据规格配置进行扫描的工具**
  - 确定扫描标准
    - 灵敏度水平
    - 漏洞反馈
    - 范围
    - 证书式与非证书式
    - 数据类型
    - 基于服务器与基于代理
  - 工具更新/插件
    - SCAP
  - 权限与访问
- **执行扫描**
- **生成报告**
  - 自动与人工分配
- **修正**
  - 优先化
    - 关键性
    - 实施难度
  - 沟通/变更控制
  - 沙盒化/测试
  - 修正抑制因素
    - MOU
    - SLA
    - 组织管控
    - 业务流程中断
    - 降级功能
- **进行中的扫描与持续性扫描**

2.2 设立前提，分析漏洞扫描的输出结果。

- **分析漏洞扫描报告**
  - 审查并解析扫描结果
    - 识别误报
    - 识别例外
    - 响应行动优先化
- **验证结果并与其它数据点关联**
  - 与最佳实践或合规实践比较
  - 调解结果
  - R审查相关日志和/或其它数据源
  - 确定趋势

2.3 比较并对比组织内的以下目标中发现的共有漏洞。

- **服务器**
- **端点**
- **网络架构**
- **网络设施**
- **虚拟架构**
  - 虚拟主机
  - 虚拟网络
  - 管理界面
- **移动设备**
- **互连网络**
- **虚拟专用网络(VPN)**
- **工业控制系统(ICS)**
- **SCADA 设备**

3.0 网络事件响应

3.1 设立前提，区分威胁数据或行为，以确定事件影响。

- **威胁分级**
  - 已知威胁与未知威胁
  - 零日漏洞攻击
  - 高级持续性威胁
- **造成事件严重性和优先级的因素**
  - 影响范围
    - 停机时间
    - 恢复时间
    - 数据完整性
    - 经济性
    - 系统程序关键性
  - 数据类型
    - 个人可识别信息(PII)
    - 个人健康信息(PHI)
    - 支付卡信息
    - 知识产权
    - 公司机密
    - 会计数据
    - 合并与获取

3.2 设立前提，准备工具包并在调查期间使用适当的取证工具。

- **取证工具包**
  - 数据取证工作站
  - 写入阻止程序
  - 电缆
  - 驱动器适配器
  - 可擦除可移动介质
  - 照相机
  - 犯罪现场封锁胶带
  - 防篡改密封
  - 文件/表格
    - 监督链表格
    - 事件响应计划
    - 事件表格
    - 呼叫名单/升级名单
- **取证调查套件**
  - 映像实用程序
  - 分析实用程序
  - 监督链
  - 散列实用程序
  - OS 和程序分析
  - 移动设备取证
  - 密码破解器
  - 加密工具
  - 日志查看器

3.3 解释事件响应程序期间沟通的重要性。

- **利益相关者**
  - 人力资源部
  - 法务部
  - 市场部
  - 管理部
- **沟通程序的目的**
  - 沟通对象仅限于可信方
  - 按照监管/法规要求进行信息公开
  - 防止信息意外扩散
  - 安全的沟通方法
- **基于角色的职责**
  - 技术
  - 管理
  - 执法
  - 保留事件响应提供方

3.4 设立前提，分析常见症状，选择支持事件响应的最佳行动方案。

- **基于网络的常见症状**
  - 带宽消耗
  - 信标
  - 不规则点对点通信
  - 网络上的非法设备
  - 扫描
  - 不常见的流量高峰
- **基于主机的常见症状**
  - 处理器消耗
  - 内存消耗
  - 驱动器容量消耗
  - 未授权软件
  - 恶意程序
  - 未授权更改
  - 未授权权限
  - 数据外泄
- **基于应用的常见症状**
  - 异常活动
  - 引入新账号
  - 意外输出
  - 意外对外通信
  - 服务中断
  - 内存溢出

3.5 总结事件恢复情况和事件后响应程序。

- **容错技术**
  - 分段
  - 隔离
  - 移除
  - 逆向工程
- **根除技术**
  - 杀毒
  - 重建/恢复映像
  - 安全处理
- **验证**
  - 打补丁
  - 权限
  - 扫描
  - 验证安全监视日志/通信
- **纠正措施**
  - 经验教训报告
  - 变更控制程序
  - 更新事件响应计划
- **事件总结报告**

4.0 安全架构和工具集

4.1 解释框架、常见政策、控件和程序之间的关系。

- **法规合规性**
- **框架**
  - NIST
  - ISO
  - COBIT
  - SABSA
  - TOGAF
  - ITIL
- **政策**
  - 密码政策
  - 正当用途政策
  - 数据所有权政策
  - 数据保留政策
  - 账户管理政策
  - 数据分级政策
- **控件**
  - 基于标准的控件选择
  - 组织定义的参数
  - 物理控件
  - 逻辑控件
  - 管理控件
- **程序**
  - 持续监视
  - 举证
  - 打补丁
  - 补偿控件开发
  - 控件测试程序
  - 例外管理
  - 修正计划
- **验证和质量控制**
  - 审计
  - 评价
  - 评估
  - 成熟度模型
  - 认证

4.2 设立前提，利用数据提出身份与访问管理相关安全问题的修正建议。

- **基于上下文验证的相关安全问题**
  - 时间
  - 地点
  - 频率
  - 行为
- **身份相关安全问题**
  - 人员
  - 端点
  - 服务器
  - 服务
  - 角色
  - 应用
- **身份库相关安全问题**
  - 目录服务
  - TACACS+
  - RADIUS
- **联合和单点登录相关安全问题**
  - 人工与自动身份供应/取消供应
  - 自助密码重置
- **漏洞利用**
  - 假冒
  - 中间人
  - 会话劫持
  - 跨网站脚本
  - 权限升级
  - Rootkit

4.3 设立前提，审查安全架构，并提出补偿控件的实施建议。

- **安全数据分析**
  - 数据聚合与关联
  - 趋势分析
  - 历史分析
- **人工审查**
  - 防火墙日志
  - Syslogs
  - 验证日志
  - 事件日志
- **纵深防御**
  - 人员
    - 培训
    - 双重控制
    - 职责分离
    - 第三方/顾问
    - 交叉培训
    - 强制休假
    - 继任计划
  - 程序
    - 持续改进
    - 定期审查
    - 程序退出
  - 技术
    - 自动报告
    - 安全设施
    - 安全套件
    - 外包
      - 安全即服务
    - 加密
  - 其它安全概念
    - 网络设计
    - 网络分段

4.4 设立前提，在参与软件开发生命周期(SDLC)时采用应用安全最佳实践。

- **软件开发期间的最佳实践**
  - 安全要求定义
  - 安全测试阶段
    - 静态代码分析
    - Web 应用漏洞扫描
    - 模糊测试
    - 使用拦截代理抓取应用
  - 人工同行审查
  - 用户验收测试
  - 应力测试应用
  - 安全回归测试
  - 输入验证
- **安全编码最佳实践**
  - OWASP
  - SANS
  - 互联网安全中心
    - 系统设计建议
    - 基准

4.5 比较并对比各种网络安全工具和技术的一般用途和原因。

（**该目标的意图并非测试特定厂商的特征集。）

- **预防**
  - IPS
    - Sourcefire
    - Snort
    - Bro
  - HIPS
  - 防火墙
    - Cisco
    - Palo Alto
    - Check Point
  - 防病毒
  - 防恶意软件
  - EMET
  - Web 代理
  - Web 应用防火墙（WAF）
    - ModSecurity
    - NAXSI
    - Imperva
- **集合**
  - SIEM
    - ArcSight
    - QRadar
    - Splunk
    - AlienVault
    - OSSIM
    - Kiwi Syslog
  - 网络扫描
    - NMAP
  - 漏洞扫描
    - Qualys
    - Nessus
    - OpenVAS
    - Nexpose
    - Nikto
    - Microsoft Baseline Security Analyzer
  - 包捕获
    - Wireshark
    - tcpdump
    - Network General
    - Aircrack-ng
  - 命令行/IP 实用程序
    - netstat
    - ping
    - tracert/traceroute
    - ipconfig/ifconfig
    - nslookup/dig
    - Sysinternals
    - OpenSSL
  - IDS/HIDS
    - Bro
- **分析**
  - 漏洞扫描
    - Qualys
    - Nessus
    - OpenVAS
    - Nexpose
    - Nikto
    - Microsoft Baseline Security Analyzer
  - 监视工具
    - MRTG
    - Nagios
    - SolarWinds
    - Cacti
    - NetFlow Analyzer
  - 拦截代理
    - Burp Suite
    - Zap
    - Vega
- **漏洞利用**
  - 拦截代理
    - Burp Suite
    - Zap
    - Vega
  - 漏洞利用框架
    - Metasploit
    - Nexpose
  - 模糊测试工具
    - Untidy
    - Peach Fuzzer
    - Microsoft SDL File/Regex Fuzzer
- **取证**
  - 取证套件
    - EnCase
    - FTK
    - Helix
    - Sysinternals
    - Cellebrite
  - 散列
    - MD5sum
    - SHAsum
  - 密码破解
    - John the Ripper
    - Cain & Abel
  - 映像
    - DD

CySA+ Cybersecurity Analyst 缩略词列表

以下是出现在 CompTIA Cybersecurity Analyst 考试中的缩略语列表。我们鼓励考生查看整个列表并了解如何运用所有列出的缩略词，这是全面备考计划的一部分。

缩略词	完整拼写
ACL	访问控制列表
ARP	地址解析协议
BYOD	自带设备
CIS	互联网安全中心
CoBiT	信息与相关技术控制目标
CCTV	闭路电视
CRM	客户关系管理
DDOS	分布式拒绝服务
DNS	域名服务
EMET	增强减灾体验工具包
FISMA	联邦信息安全管理法案
FTK	取证工具包
FTP	文件传输协议
HBSS	主机型安全系统
HIDS	主机型入侵检测系统
HIDS	主机型入侵防护系统
HR	人力资源
ICS	工业控制系统
IDS	入侵检测系统
IMAP4	互联网消息存取协议
IOC	攻陷指标
IPS	入侵防御系统
ISO	国际标准化组织
ITIL	信息技术基础设施库
LDAP	轻量级目录访问协议
MAC	强制访问控制
MD5	信息摘要 5
MOA	协议备忘录
MOU	谅解备忘录
MRTG	多路由器流量图形化程序
NAC	网络访问控制
NAXSI	Nginx 防止 XSS & SQL 注入
NIC	网络接口卡
NIDS	网络型入侵检测系统
NIST	国家标准和技术研究所
OEM	原始设备制造商
OSSIM	开源安全信息管理
OWASP	开放 Web 应用安全计划
PAM	可插拔认证模块

缩略词	完整拼写
PCA	主成分分析
PCI	支付卡行业
PHI	受保护健康信息
PII	个人可识别信息
RACI	负责、有责任、被咨询、知情
RADIUS	远程身份验证拨入用户服务
SABSA	舍伍德可执行业务安全体系
SANS	系统管理、联网和安全研究所
SCADA	数据采集与监视控制
SCAP	安全内容自动化协议
SDLC	软件开发生命周期
SEO	搜索引擎优化
SHA	安全散列算法
SIEM	安全事件管理器
SLA	服务级别协议
SOC	安全运营中心
SPF	发送方政策框架
SSH	安全外壳
SSL	安全套接字层
TACACS	终端访问控制器访问控制系统+
TFTP	普通文件传输协议
TLS	传输层安全
TOGAF	开放组织架构框架
USB	通用串行总线
VAS	漏洞评估系统
VDI	虚拟桌面基础设施
VLAN	虚拟局域网
VPN	虚拟专用网
WAF	Web 应用防火墙

为 CySA+ 认证培训推荐的教室设备

**CompTIA 包含该硬软件示例列表，用于协助考生准备 CySA+ 考试。此列表也对提供培训、创建实验室组件的培训公司非常有用。每个主题下的大纲列表只是一个示例清单，并不是很详尽。

IT 硬件
- 路由器
- 交换机
- 防火墙
- 工作站/笔记本电脑
- IDS/IPS
- 服务器
- 写入阻止程序
- Pelican 箱子
- 无线访问点
- 驱动器适配器
- VoIP 电话
- 手机

工具
- 螺丝起子
- PC 服务工具包

耗材
- CAT5/6 电缆
- 备用驱动器/闪存

软件
- 虚拟化平台
- Kali Linux/BackTrack
- 虚拟化攻击目标
  - Web 服务器
  - 数据库服务器
  - 时间服务器
  - DNS 服务器
  - PC 工作站

CompTIA.