Performing CyberOps Using Cisco Security Technologies v1.0 (350-201)

考试简介： Performing CyberOps Using Cisco Security Technologies v1.0 (CBRCOR 350-201) 时长 120 分钟，是思科 CyberOps 资深人才认证的一项考试。该考试旨在考查候选者是否掌握了核心网络安全运营知识，包括网络安全基础知识、技术、流程和自动化。“使用思科安全技术执行 CyberOps”课程可帮助候选者备考这门科目。

以下考试指南列举了考试中通常会涉及的主题，但某些考试中也可能包含其他相关主题。为了准确清楚地列明考试内容，以下考试指南随时可能更改，恕不另行通知。

20%	1.0	**基础知识**
	1.1	阐释脚本内容
	1.2	根据脚本场景确定所需工具
	1.3	将脚本应用于常见场景（例如未经授权的权限提升、DoS 和 DDoS、网站篡改）
	1.4	推断各类合规标准所在行业（例如 PCI、FISMA、FedRAMP、SOC、SOX、PCI、GDPR、数据隐私和 ISO 27101）
	1.5	阐释网络风险保险的概念和局限
	1.6	分析风险分析的要素（组合资产、漏洞和威胁）
	1.7	应用事件响应工作流
	1.8	通过常见事件响应指标来阐释特征和待改进领域
	1.9	解释云环境类型（例如 IaaS 平台）
	1.10	比较云平台的安全运营注意事项（例如 IaaS、PaaS）
30%	2.0	**技术**
	2.1	推荐数据分析技术，满足特定需求或回答特定问题
	2.2	阐释强化机器映像在部署中的用途
	2.3	解释资产安全态势评估流程
	2.4	评估环境的安全控制，诊断差距，并提出改进建议
	2.5	确定行业标准资源和系统强化建议
	2.6	确定给定场景的补丁建议
	2.7	指出给定场景中建议禁用的服务
	2.8	将分段应用于网络
	2.9	通过网络控制强化网络
	2.10	确定 SecDevOps 建议
	2.11	阐述使用威胁情报平台 (TIP) 自动化情报的相关用途和概念
	2.12	通过工具应用威胁情报
	2.13	根据通用标准，应用数据丢失、资料泄漏、传输中数据、使用中数据和静态数据的概念
	2.14	阐释数据丢失预防技术的不同检测与实施机制

2.14.a 基于主机
2.14.b 基于网络
2.14.c 基于应用
2.14.d 基于云

2.15 推荐不同规则、过滤器和政策的调优或调适设备与软件
2.16 阐释安全数据管理概念
2.17 阐释安全数据分析工具的用途和概念
2.18 推荐工作流，处理问题描述到升级、自动化和解决问题等步骤
2.19 应用仪表板数据，与技术人员、负责人或高管沟通
2.20 分析异常用户和实体行为 (UEBA)
2.21 根据用户行为警报确定后续措施
2.22 描述网络分析工具及其缺陷（例如数据包捕获工具、流量分析工具、网络日志分析工具）
2.23 评估数据包捕获文件中的人工因素和数据流
2.24 解决现有检测规则的问题
2.25 根据攻击确定战术、技术和程序 (TTP)

30% 3.0 流程

3.1 按优先顺序排列威胁模型要素
3.2 确定常见案例类型的调查步骤
3.3 在恶意软件分析流程中应用概念和步骤顺序:
3.3.a 提取并识别样本（例如使用数据包捕获文件或数据包分析工具），进行分析
3.3.b 开展逆向工程
3.3.c 通过沙盒环境进行动态恶意软件分析
3.3.d 确定对其他静态恶意软件分析的需求
3.3.e 进行静态恶意软件分析
3.3.f 总结并分享结果
3.4 基于流量模式分析，解释攻击时的事件顺序
3.5 确定调查不同平台类型（例如台式机、笔记本电脑、物联网、移动设备）潜在端点入侵时的步骤
3.6 确定给定场景中的已知漏洞指示 (IOC) 和攻击指示 (IOA)
3.7 确定沙盒环境中的 IOC（包括生成复杂指示）
3.8 确定给定场景中调查不同程序载体（例如云、端点、服务器、数据库、应用）潜在数据丢失时的步骤
3.9 推荐通用缓解步骤，解决漏洞问题
3.10 基于行业评分系统（例如 CVSS）和其他技术，推荐漏洞分类和风险分析的后续步骤

20% 4.0 自动化

4.1 比较编排与自动化的概念、平台和机制
4.2 解读基础脚本（例如 Python）
4.3 修改现有脚本，自动化安全运营任务
4.4 识别常见数据格式（例如 JSON、HTML、CSV、XML）
4.5 确定自动化与编排机会
4.6 确定使用 API 时的限制条件（例如速率限制、超时设定与有效负荷）

4.7 解释与 REST API 相关的常见 HTTP 响应代码
4.8 评估 HTTP 响应的各个部分（响应代码、头文件、正文）
4.9 解释 API 认证机制：基础知识、自定义标记和 API 密钥
4.10 使用 Bash 命令（文件管理、目录导航和环境变量）
4.11 描述 CI/CD 管道的组件
4.12 应用 DevOps 实践的原则
4.13 阐释基础架构即代码原则