Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps v1.0 (300-215)

考试简介： Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps v1.0 (CBRFIR 300-215) 时长 90 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取证分析和事件响应的基础知识、技术与流程。“使用思科 CyberOps 技术进行取证分析和事件响应”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 分析根本原因分析报告所需的内容
- 1.2 描述对基础设施网络设备进行取证分析的过程
- 1.3 解释反取证策略、技术和程序
- 1.4 识别编码和混淆技术（例如 64 进制和十六进制编码）
- 1.5 阐释用于恶意软件识别、分类与记录的 YARA 规则（基础）有何用途和特征
- 1.6 解释以下各项的作用：
  - 1.6.a DFIR 调查中的十六进制编辑器（HxD、Hiew 和 Hexfiend）
  - 1.6.b 用于基本恶意软件分析的反汇编程序和调试工具（例如 Ghidra、Radare 和 Evans Debugger）
  - 1.6.c 反混淆工具（例如 XORBruteForces、异或工具和脱壳工具）
- 1.7 阐释从虚拟环境（主要是云供应商）收集证据的相关问题

20% 2.0 取证分析

- 2.1 识别 MITRE 攻击框架中已确定的无文件恶意软件分析方法
- 2.2 确定所需文件以及文件在主机上的位置
- 2.3 评估输出，识别主机上的 IOC
  - 2.3.a 流程分析
  - 2.3.b 日志分析
- 2.4 根据现有代码片段确定代码类型
- 2.5 构建 Python、PowerShell 和 Bash 脚本，解析和搜索日志或多个数据源（例如 Cisco Umbrella、Sourcefire IPS、AMP for Endpoints、AMP for Network 和 PX Grid）
- 2.6 识别脚本库和工具（例如Volatility、Systernals、SIFT 工具和 TCPdump）的目的、用途与功能

30%	3.0	**事件响应技术**
	3.1	解释警报日志（例如 IDS/IPS 和 syslog）
	3.2	根据事件类型（基于主机和基于网络的活动）确定待关联数据
	3.3	确定攻击媒介或受攻击面，并推荐给定场景的缓解策略
	3.4	根据事后分析推荐应采取的措施
	3.5	针对来自防火墙、入侵防御系统 (IPS)、数据分析工具（例如 Cisco Umbrella Investigate、Cisco Stealthwatch 和 Cisco SecureX）及其他系统的已评估警报，推荐缓解技术，应对网络事件
	3.6	为零日漏洞推荐响应措施（漏洞管理）
	3.7	根据情报干扰因素推荐响应措施
	3.8	为给定场景的检测和漏洞预防推荐思科安全解决方案
	3.9	解读威胁情报数据，确定 IOC 和 IOA（内外部来源）
	3.10	评估威胁情报干扰因素，确定威胁源起方概况
	3.11	阐释与威胁情报相关的思科安全解决方案的功能（例如 Cisco Umbrella、Sourcefire IPS、AMP for Endpoints 和 AMP for Network）
15%	4.0	**取证流程**
	4.1	解释反取证技术（例如调试、定位和混淆）
	4.2	分析现代网页应用和服务器（Apache 和 NGINX）的日志
	4.3	使用网络监控工具（例如 Wireshark 的 NetFlow 和显示过滤）分析与恶意活动相关的网络流量
	4.4	根据给定场景中文件的主要特征，推荐文件评估流程后续步骤
	4.5	使用二进制文件分析和其他命令行工具（例如 Linux、Python 和 Bash）解读二进制文件
15%	5.0	**事件响应流程**
	5.1	阐述事件响应的目标
	5.2	评估事件响应脚本中的必备要素
	5.3	评估 ThreatGrid 报告中的相关内容
	5.4	在给定场景中，推荐端点文件评估流程和特殊扫描流程的后续步骤
	5.5	分析不同格式的现有威胁情报（例如 STIX 和 TAXII）