CYBRARY

职业道路教学大纲：成为一名SOC分析师1

最后更新：2021年11月

职业道路描述

安全运营中心分析师（SOC分析师）是抵御当今组织所面临的网络威胁的前沿防线。SOC团队通过监控和响应已记录时间内的大量数据，确保组织的数字资产保持安全，不受未经授权的访问。在此角色中，您将通过监视数据来识别可疑活动来保护组织的基础设施，然后在漏洞发生之前降低风险。图书馆成为一个SOC分析师-一级职业道路将装备你进入该领域的技能与美国国家标准和技术协会的网络防御分析师NICE的工作角色。

职业道路上的期望和目标

我们发现在这个项目中最成功的学习者每天至少要花30分钟来学习。你的时间是非常宝贵的，所以如果有一个概念，你已经知道，不要犹豫，跳过那部分的课程。职业道路的目的是确保你拥有这个角色所需的知识/技能/能力。如果您已经有了它们，那么就没有必要重复这些工作。

职业路径可以包含课程、实验室和评估。同时使用这些材料可以为您提供教学和实践经验，这将提高您通过潜在认证考试的机会，并给您提供实际工作角色所需的经验。

我们也鼓励您与图书馆内部专业（CIP）松弛社区的导师和其他学习者接触。CIP社区成员将分享他们在旅途中获得的见解。此外，沟通困难的概念是一项可学习的技能，我们的社区为您提供了一个无风险的环境来测试该技能。

职业道路大纲

重要提示：这个教学大纲介绍了图书馆建议的通过职业道路的方法，但教学大纲项目不需要按照它们列出的顺序完成。你可以自由地按任何顺序完成项目。

成为一名SOC分析师-一级分析师	内容类型	难度	持续时间（小时）
欢迎来到SOC分析师一级职业道路	课程	初学者	0.03
Kali Linux基础知识	课程	初学者	2.1
命令行基础知识	课程	初学者	5.5
事件响应程序、取证和法医分析实验室	实验室	中间的	1.5
Linux攻击和响应实验室	实验室	中间的	1.5
如何使用BinWalk（BSWJ）	课程	中间的	0.1
恶意软件威胁	课程	中间的	4.5
主机数据完整性基线化	实验室	中间的	1
针对突发事件处理程序的攻击和持久性	课程	中间的	0.5
网络安全杀戮链	课程	初学者	1.75
爆炸后黑客攻击	课程	先进的	7.75
扫描、枚举和漏洞	课程	初学者	9
基于漏洞评估创建建议	实验室	中间的	1
奥瓦斯普	课程	中间的	12.1
嗅探	课程	初学者	14.25
深度潜水在数据包分析-使用有线鲨鱼和网络矿工实验室	实验室	先进的	1.5
将过滤器应用于TCP转储和钢丝鲨	实验室	中间的	1
使用有线鲨鱼来拦截网络流量	实验室	中间的	1
识别非安全的网络流量	实验室	初学者	0.75
解析网络流量中的文件	实验室	中间的	1
拆分介绍	课程	初学者	2.5

在Linux和Splunk实验室中的日志分析	实验室	先进的	1.5
日志事件报告	实验室	中间的	1
事件日志收集	实验室	中间的	1
日志相关性	实验室	中间的	0.75
日志相关性和分析，以确定潜在的IOC	实验室	中间的	1
通过日志识别Web攻击	课程	初学者	2.25
日志分析	实验室	中间的	1.5
集中监控	实验室	中间的	1
使用拆分创建SIEM报表	实验室	中间的	1
Python简介	课程	初学者	3
PowerShell脚本简介	课程	初学者	1.75
使用PowerShell来分析一个系统	实验室	中间的	1
CompTIA Security+ (SY0-601)	课程	初学者	8

总标题：34
总学习时间：95