COURSE SYLLABUS

SOC Foundations for Federal Cyber Defense and Operations Course

Prepare to operate effectively inside a federal Security Operations Center, whether you are new to SOC work or an analyst who wants to firm up the federal standards and terminology behind the job. Unlike generic SOC training, every operational topic — log collection, continuous monitoring, detection engineering, and incident response — is grounded in the statutes, policy memoranda, and technical standards that actually govern federal cyber defense.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/soc-foundations-for-federal-cyber-defense-and-operations



support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1

Foundations of Federal Cybersecurity & the SOC Mission

Module 2

SOC Team Structure, Roles & Responsibilities

Module 3

Log Collection & Federal Logging Standards

Module 4

Continuous Monitoring & Detection Engineering

Module 5

Incident Response Workflow — NIST SP 800-61 Rev. 3

Module 6

Reporting, Coordination & Compliance

Module 7

SOC Metrics, Tools & Career Pathways