COURSE SYLLABUS

Cyber Defense & SOC Analyst Certificate Program (Self-Paced)

Build the complete federal security operations skill set, starting with how a federal SOC actually works, moving into responding when something is found, and finishing with proactively hunting threats before an alert ever fires. Aligned to NIST and CSF 2.0 standards, it prepares you for Federal SOC Analyst, Detection Engineer, and threat hunter roles and toward the CompTIA CySA+, GIAC GCIH, and GMON credentials.

> 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/certificates/cyber-defense-and-soc-analyst-certificate-program-self-paced



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

Course Outline

This package includes these courses

- SOC Foundations for Federal Cyber Defense and Operations Course (Self-Paced) (12 Hours)
- Federal Incident Response for Agency Practitioners Course (Self-Paced) (12 Hours)
- Threat Hunting and Detection Engineering Course (Self-Paced) (12 Hours)

SOC Foundations for Federal Cyber Defense and Operations Course (Self-Paced)

This course prepares you to operate effectively inside a federal Security Operations Center, whether you're new to SOC work or an analyst who wants to solidify 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.

- How FISMA, OMB policy, NIST guidance, and CISA directives fit together to govern federal SOC operations
- SOC organizational models and Tier 1–3 responsibilities, mapped to the NICE Workforce Framework
- The log sources a federal SOC must collect, and current requirements under OMB M-26-14
- Detection engineering and MITRE ATT&CK coverage mapping, applied to alert triage and prioritization
- The incident response lifecycle under NIST SP 800-61 Rev. 3 and the CISA federal response playbooks
- Federal incident reporting obligations, and how SOC findings connect to RMF and the ATO lifecycle
- SOC performance metrics, the common toolset, and career pathways mapped to DoD 8140.03

Federal Incident Response for Agency Practitioners Course (Self-Paced)

This course equips federal incident response practitioners with the operational knowledge to detect, contain, and recover from cybersecurity incidents while meeting FISMA, CISA, and OMB mandatory requirements. Participants develop practical skills across the full NIST SP 800-61 Rev. 3 incident response lifecycle, from preparation, detection and analysis, containment, eradication and recovery, and post-incident review.

- Governance and legal/policy basis for federal IR (FISMA, NIST SP 800-61 Rev. 3, OMB, CISA).
- Detect and classify incidents using NCISS and federal incident categories.
- Identify which mandatory reporting obligations apply and meet the deadlines.
- Contain, eradicate, and recover while preserving evidence.
- Run post-incident reviews that drive program improvement.
- Design and facilitate tabletop exercises (including a MSEL).
- Walk a simulated incident from detection to after-action report.

Threat Hunting and Detection Engineering Course (Self-Paced)

Take your existing threat hunting and detection engineering skills and build them into a defensible program, using a methodology sourced entirely from NIST, CISA, and DoD publications. You will learn a repeatable hunt process, bias-reducing analytic techniques, the full detection lifecycle, and the validation and metrics that prove risk is going down.

- Stand up a repeatable hunting capability grounded in RA-10, CSF 2.0, and the Diamond Model
- Run a plan/conduct/report hunt process tied to CSF 2.0 Detect outcomes
- Structure findings across the Diamond Model's four vertices and pivot across related activity
- Map adversary behavior to MITRE ATT&CK using CISA's six-step process and the Decider tool
- Apply ODNI structured analytic techniques to counter confirmation bias and anchoring
- Benchmark program maturity against the CSF 2.0 Implementation Tiers
- Run the detection engineering lifecycle end-to-end, with validation per NIST SP 800-115
- Produce defensible performance measures using SP 800-53 assessments and SP 800-55