COURSE SYLLABUS

Cyber Defense & SOC Analyst Certificate Program

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



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

Course Outline

This package includes these courses

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

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.

- How FISMA, OMB policy, NIST guidance, and CISA directives combine to govern federal SOC operations.
- SOC organizational models and Tier 1–3 responsibilities set against the NICE Workforce Framework.
- The federal SOC's mandatory log sources and the current OMB M-26-14 requirements.
- Detection engineering and MITRE ATT&CK coverage mapping for alert triage and prioritization.
- The NIST SP 800-61 Rev. 3 incident response lifecycle and the CISA federal response playbooks.
- Federal incident reporting duties, and how SOC findings feed RMF and the ATO lifecycle.
- SOC performance metrics, the common toolset, and DoD 8140.03 career pathways.

Federal Incident Response for Agency Practitioners Course

This course gives federal incident response practitioners the operational grounding to detect, contain, and recover from cybersecurity incidents while satisfying FISMA, US-CERT, and OMB mandatory requirements. Participants build working skill across the full NIST SP 800-61 Rev. 3 incident response lifecycle — preparation, detection and analysis, containment, eradication and recovery, and post-incident review.

- Governance and the legal and policy basis for federal IR (FISMA, NIST SP 800-61 Rev. 3, OMB, CISA).
- Detecting and classifying incidents with NCISS and the federal incident categories.
- Determining which mandatory reporting obligations apply and meeting the deadlines.
- Containment, eradication, and recovery carried out without compromising evidence.
- Post-incident reviews that drive real program improvement.
- Tabletop exercise design and facilitation, including a MSEL.
- Working a simulated incident from detection through to the after-action report.

Threat Hunting and Detection Engineering Course

Take the threat hunting and detection engineering skills you already have and build them into a defensible program, using a methodology sourced entirely from NIST, CISA, and DoD publications. Participants work through a repeatable hunt process, bias-reducing analytic techniques, the full detection lifecycle, and the validation and metrics that prove risk is going down.

- A repeatable hunting capability founded on RA-10, CSF 2.0, and the Diamond Model.
- A plan/conduct/report hunt cycle keyed to CSF 2.0 Detect outcomes.
- Findings structured on the Diamond Model's four vertices, with pivots into related activity.
- Adversary behavior mapped to MITRE ATT&CK via CISA's six-step process and the Decider tool.
- ODNI structured analytic techniques applied against confirmation bias and anchoring.
- Program maturity benchmarked on the CSF 2.0 Implementation Tiers.
- The detection engineering lifecycle run from requirement to retirement, validated per NIST SP 800-115.
- Defensible performance measures built from SP 800-53 assessments and SP 800-55.