COURSE SYLLABUS

Digital Forensics & Incident Response Certificate Program

Master the full federal incident investigation lifecycle, from response and containment through forensics and malware analysis, in one comprehensive credential. Aligned to NIST and CISA standards, it prepares you for incident responder, forensic examiner, and SOC roles and toward the GIAC GCIH and GCFE certifications.

> 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/digital-forensics-incident-response-certificate-program



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

Course Outline

This package includes these courses

- Federal Incident Response for Agency Practitioners Course (12 Hours)
- Digital Forensics and Incident Investigation for Federal Employees Course (12 Hours)
- Malware Analysis Fundamentals Course (12 Hours)

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.

Digital Forensics and Incident Investigation for Federal Employees Course

Conduct defensible digital forensics and incident investigations using the NIST SP 800-86 forensic process — Collection,

Examination, Analysis, and Reporting. Participants work through IOC investigation, chain of custody, and the federal legal and oversight framework, then bring it together in a full capstone investigation.

- The NIST SP 800-86 forensic process, tied back to the NIST SP 800-61 IR lifecycle.
- The legal and policy foundations for federal digital evidence, including when a matter goes to OIG, counsel, or law enforcement.
- Evidence collected and preserved in order of volatility — memory, disk, network, cloud — free of contamination.
- IOC investigation across host, network, and behavioral data to fix scope and build a timeline.
- Reconstruct timelines and correlate artifacts, with a clear sense of what forensic evidence can and cannot prove.
- Hold a defensible chain of custody and write findings for technical, executive, and legal readers.

Malware Analysis Fundamentals Course

Work through both static analysis (examining files without running them) and dynamic analysis (interpreting behavior from sandbox and monitoring reports), and build the judgment to know which technique fits each situation. Following NIST SP 800-83 Rev. 1, the course brings in the tools analysts rely on — disassemblers, sandboxes, YARA, network capture, and CISA's Malware Next-Gen — with a federal thread on sample sensitivity and data handling throughout.

- Static analysis technique: triage, string and metadata extraction, YARA, and basic disassembly
- Reading dynamic analysis output (sandboxing, monitoring, network simulation) and evasive behavior from example reports
- Capturing network IOCs and correlating them with threat intel and MITRE ATT&CK
- Using FLARE-VM, REMnux, and CISA Malware Next-Gen appropriately, as against public multi-scanners
- Writing a CISA-MAR-style report for technical and leadership readers
- Tracking one sample from triage through to the finished report