COURSE SYLLABUS

Digital Forensics & Incident Response Certificate Program (Self-Paced)

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 in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/certificates/digital-forensics-incident-response-certificate-program-self-paced

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

Course Outline

This package includes these courses

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

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, US-CERT, 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.

Digital Forensics and Incident Investigation for Federal Employees Course (Self-Paced)

Learn to conduct defensible digital forensics and incident investigations using the NIST SP 800-86 forensic process—Collection, Examination, Analysis, and Reporting. You'll master IOC investigation, chain of custody, and the federal legal and oversight framework, then put it all together in a full capstone investigation.

- Apply the NIST SP 800-86 forensic process and connect it to the NIST SP 800-61 IR lifecycle.
- Recognize the legal/policy foundations for federal digital evidence, and know when to refer to OIG/counsel/law enforcement.
- Collect and preserve evidence by order of volatility (memory, disk, network, cloud) without contaminating it.
- Investigate IOCs across host/network/behavioral data to establish scope and build a timeline.
- Reconstruct timelines and correlate artifacts, understanding the limits of what forensic evidence can prove.
- Maintain a defensible chain of custody and write findings for technical, executive, and legal audiences.

Malware Analysis Fundamentals (Intermediate) Course (Self-Paced)

Learn 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 works in the real 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: triage, string/metadata extraction, YARA, basic disassembly
- Interpret dynamic analysis (sandboxing, monitoring, network simulation) and evasive behavior from example reports
- Capture and correlate network IOCs with threat intel and MITRE ATT&CK
- Use FLARE-VM, REMnux, and CISA Malware Next-Gen appropriately (vs. public multi-scanners)
- Write a CISA-MAR-style report for technical and leadership audiences
- Follow a sample end-to-end through a worked example