SANS Technology Institute

Graduate Certificate Program
Incident Response Graduate

The SANS Technology Institute's post-baccalaureate certificate program in Incident Response is based entirely upon courses already available as an elective path through its graduate program leading to a Master of Science Degree in Information Security Engineering.

As an independent offering, the graduate certificate in Incident Response is a highly technical, 13 credit hour program with a cohesive and progressive set of learning outcomes. A hands-on focus is emphasized throughout, including the requirement to unlock the upper levels of the NetWars Continuous internet-accessible cyber range as the capstone experience. These learning outcomes are focused on developing the student's capability to properly manage both a computer and network-based forensics investigation as well as the appropriate incident responses.

Course Number and Name	SANS Class and GIAC Exam	Credit Hours
ISE 5201 Hacking Techniques & Incident Response	SEC 504, GCIH	3
ISE 6425 Advanced Computer Forensic Analysis & Incident Response	FOR 508, GCFA	3
ISE 6440 Advanced Network Forensics & Analysis	FOR 572, GNFA	3
ISE 6460 Malware Analysis & Reverse Engineering	FOR 610, GREM	3
ISE 6400 DFIR NetWars Continuous Capstone	DFIR NetWars	1
	Total	**13**

The graduate certificate in Incident Response provides a path for professionals to specialize in a sub-area of the information security field, and this progression of courses in incident response is made available just as they would be to a candidate for the master's degree in Information Security Engineering. It is designed to provide students with knowledge of attack vectors and techniques, the capabilities to seek out, identify and counter these attacks at both the host and network levels, and the ability in particular to examine and reverse engineer malicious code often supporting these attacks. The program introduces students to forensic analysis policy and procedures, forensic analysis tools, data recovery, and investigation techniques.

Graduates of the Incident Response post-baccalaureate certificate program will be able to:

1. Explain the role of digital forensics and incident response in the field of information security, and recognize the benefits of applying these practices to both hosts and networks when investigating a cyber incident.
2. Analyze the structure of common attack techniques in order to evaluate an attacker's footprint, target the ensuing investigation and incident response, and anticipate and mitigate future activity.
3. Evaluate the effectiveness of available digital forensic tools and use them in a way that optimizes the efficiency and quality of digital forensic investigations.
4. Utilize multiple malware analysis approaches and tools to understand how malware programs interact with digital environments and how they were coded, in order to reverse the effects of the program on networks and systems.

The following assessment methods will be utilized to determine if students meet the program learning outcomes:

1. Standardized exams
    - **a.** GIAC Certified Incident Handler (GCIH) exam,
    - **b.** GIAC Certified Forensics Analyst (GCFA) exam,
    - **c.** GIAC Network Forensic Analyst (GNFA) exam,
    - **d.** GIAC Reverse Engineering Malware (GREM) exam;
2. Simulation Experience – DFIR NetWars Continuous

Course Descriptions

Individual course descriptions are provided below. For additional, detailed technical goals for each course, please link through to individual SANS class descriptions on the sans.org website.

Required Courses

ISE 5201: Hacking Techniques & Incident Response

SANS class: SEC 504 Hacker Techniques, Exploits & Incident Handling
Assessment: GIAC GCIH
3 Credit Hours | Tuition: $5,000

By adopting the viewpoint of a hacker, ISE 5201 provides an in-depth focus into the critical activity of incident handling. Students are taught how to manage intrusions by first looking at the techniques used by attackers to exploit a system. Students learn responses to those techniques, which can be adopted within the framework of the incident handling process to handle attacks in an organized way. The faculty instruction, lab exercises, and exam are coordinated to develop and test a student's ability to utilize the core capabilities required for incident handling.

ISE 6425: Advanced Computer Forensic Analysis and Incident Response

SANS class: FOR 508 Advanced Computer Forensics and Analysis
Assessment: GIAC GCFA
3 Credit Hours | Tuition: $5,000

ISE 6425 teaches the necessary capabilities for forensic analysts and incident responders to identify and counter a wide range of threats within enterprise networks, including economic espionage, hacktivism, and financial crime syndicates. The course shows students how to work as digital forensic analysts and incident response team members to identify, contain, and remediate sophisticated threats-including nation-state sponsored Advanced Persistent Threats and financial crime syndicates. Students work in a hands-on lab developed from a real-world targeted attack on an enterprise network in order to learn how to identify what data might be stolen and by whom, how to contain a threat, and how to manage and counter an attack.

ISE 6440: Advanced Network Forensics and Analysis

SANS class: FOR 572 Advanced Network Forensics and Analysis
Assessment: GIAC GNFA
3 Credit Hours | Tuition: $5,000

ISE 6440 focuses on the most critical skills needed to mount efficient and effective post-incident response investigations. Moving beyond the host-focused experiences in ISE 6420 and ISE 6425, ISE 6440 covers the tools, technology, and processes required to integrate network evidence sources into investigations, covering high-level NetFlow analysis, low-level pcap exploration, and ancillary network log examination. Hands-on exercises cover a wide range of open source and commercial tools, and real-world scenarios help the student learn the underlying techniques and practices to best evaluate the most common types of network-based attacks.

ISE 6460: Malware Analysis and Reverse-Engineering

SANS class: FOR 610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Assessment: GIAC GREM
3 Credit Hours | Tuition: $5,000

ISE 6460 teaches students how to examine and reverse-engineer malicious programs - spyware, bots, Trojans, etc. - that target or run on Microsoft Windows, within browser environments such as JavaScript or Flash files, or within malicious document files (including Word and PDF). The course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools. The malware analysis process taught in this class helps students understand how incident responders assess the severity and repercussions of a situation that involves malicious software and plan recovery steps. Students also experience how forensics investigators learn to understand key characteristics of malware discovered during the examination, including how to establish indicators of compromise (IOCs) for scoping and containing the incident.

ISE 6400: DFIR NetWars Continuous Capstone

SANS component: DFIR NetWars Continuous
1 Credit Hour | Tuition: *No additional tuition charged*

Enrollment Design

The Incident Response graduate certificate program is designed to be completed in 18-24 months, allowing each student adequate time between courses to practice and implement their skills. For each course, enrolled students must complete the class and associated exam within three months of their course start date. Grades for each course are assigned according to a student's performance on the assessments, with letter grades for GIAC exams established versus a pre-determined numerical curve. All courses taken for credit must be taught by faculty of the SANS Technology Institute, but otherwise may be taken either live at a SANS event or online from home or work. Credit is earned only when a student enrolls first in a given certificate program and then registers for the appropriate graduate courses.

Certain waivers may be available for previous SANS Institute class or GIAC certifications, please inquire at info@sans.edu for more information.

Because the certificate program is based on the courses that may be chosen by a master's candidate during the normal course of studies, all credits earned while completing the Incident Response certificate program may be applied directly in fulfillment of the master's degree requirements should the student later matriculate in the master's program.

Admissions

Applicants to the Incident Response post-baccalaureate certificate program must hold a bachelor's degree from a regionally accredited US institution (or international equivalent), and have at least 12 months of professional work experience in information technology, information security, or audit. The admissions process requires the submission of our online application, a current résumé, and delivery of official undergraduate transcripts.

For additional information on the admissions process, please inquire at info@sans.edu.