SANS Technology Institute

Cybersecurity Engineering Core Graduate Certificate

As a distinct experience, the **Cybersecurity Engineering Core** post-baccalaureate certificate program is built from the three technical courses at the core of the program leading to a Master of Science in Information Security Engineering. Topics span fundamental information security tools and techniques to the advanced study of offensive (attack/penetration testing) and defensive (intrusion detection and incident response) information security best practices. Courses in the program familiarize the student with essential tools and techniques used in cybersecurity engineering, teach the student various cyber attack techniques which may be employed in penetration testing and incident response, and reinforce a practitioner's ability to detect attacks through packet analysis and intrusion detection. Student capabilities are reinforced through multiple hands-on labs and network simulations.

Course Number and Name	SANS Class and GIAC Exam	Credit Hours
ISE 5101 Enterprise Information Security	SEC 401, GSEC	3
ISE 5201 Hacking Techniques & Incident Response	SEC 504. GCIH	3
ISE 5401 Advanced Network Intrusion Detection & Analysis	SEC 503, GCIA	3
RES 5500 Graduate Research Practicum	Research Paper	2
ISE 6300 Core NetWars Continuous Capstone	Core NetWars	1
	Total	**12**

The ideal candidate for the Cybersecurity Engineering Core certificate program is an information technology professional with a year or more of experience working with network infrastructures, or an information security professional who is or seeks to be involved in detecting and responding to malicious traffic in order to build defensible networks.

Graduates of the Cybersecurity Engineering Core post-baccalaureate certificate program will be able to:

1. Utilize a broad range of current tools and technologies in the design and implementation of security solutions deployed across organizations.
2. Analyze network traffic to extract the observable characteristics of networks and network devices, thus providing a basis for defensive strategies.
3. Assemble tools and configure systems and networks to permit systems to foster resiliency and continuity of operations through attacks.
4. Understand important attacker techniques, engage in penetration testing within their organization, and respond to incidents associated with these activities within their organization.

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

1. Standardized exams
    - **a.** GIAC Security Essentials (GSEC) exam,
    - **b.** GIAC Certified Incident Handler (GCIH) exam, and
    - **c.** GIAC Certified Intrusion Analyst (GCIA) exam
2. Written research paper
3. Simulation Experience – 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.

ISE 5101 Security Essentials

SANS class: SEC 401 Security Essentials Boot-camp Style
Assessment: GIAC GSEC
3 Credit Hours | Tuition: $5,000

ISE 5101 is the technically-oriented survey course in the information security engineering master's program. It establishes the foundations for designing, building, maintaining and assessing security functions at the end-user, network and enterprise levels of an organization. The faculty instruction, readings, lab exercises, exam, and required student monograph are coordinated to introduce and develop the core technical, management, and enterprise-level capabilities that will be developed throughout the information security engineering master's program.

ISE 5201 Hacking Techniques & Incident Response

SANS class: SEC504 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 5401 Advanced Network Intrusion Detection & Analysis

SANS class: SEC 503 Intrusion Detection In-Depth
Assessment: GIAC GCIA
3 Credit Hours | Tuition: $5,000

ISE 5401 arms you with the core knowledge, tools, and techniques to prepare you to defend your networks. Hands-on exercises supplement the course book material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. All exercises in the course can be approached in two ways. A basic approach, which assists you by giving hints for answering the questions; or, an advanced approach, which provides no hints so that it is a more challenging experience.

RES 5500 Graduate Research Practicum

2 Credit Hours | Tuition: $0.00

RES 5500 is a graduate-level research course in which students will identify, investigate and analyze a problem. Students will write a research paper interpreting the data collected and making

recommendations for action. The research paper will reflect original work towards a new practice, solution, tool, policy, or paradigm offering the potential for real impact in the field of information security.
Prerequisites: ISE 5101, ISE 5201, ISE 5401

ISE 6300 Core NetWars Continuous Capstone
1 Credit Hour | Tuition: $0.00

Enrollment design

The Cybersecurity Engineering Core 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. Enrolled students must complete ISE 5200 within four months of their course start date, and all other courses 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, averaged with the grades for the research papers and performance on the NetWars simulation. 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, at an on-site hosted at your organization, 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 experiences, please inquire at admissions@sans.edu for more information.

Because the certificate program is based on the courses within the master's program, all credits earned while completing the Cybersecurity Engineering Core certificate program may be applied directly in fulfillment of the master's degree requirements should the student matriculate later in that program.

Admissions

Applicants to the Cybersecurity Engineering Core 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 resume, and delivery of official undergraduate transcripts. Applicants to the Cybersecurity Engineering Core certificate program must also submit a one-page, single-spaced writing sample for evaluation by our admissions staff, given the graduate-level English writing skills required in the program.

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