SANS Technology Institute

The SANS Technology Institute makes shorter groups of courses available to students who are unable to commit to a full master's degree program. These certificate programs will augment your skills, provide specialized training, enable you to earn employer-recognized GIAC certifications, and impart a specialized credential from the SANS Technology Institute that will help advance your career. Participants enrolled in these graduate certificate programs likely qualify for tuition reimbursement if their employer offers that benefit.

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 from a survey of fundamental information security tools and techniques to a more advanced study of the inter-relationships between 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.

Cybersecurity Engineering (Core) Certificate- 12 credit hours:	**Graduate course incorporates**	
ISE 5100 Engineering Enterprise Information Security	SEC 401	GSEC, Paper
ISE 5200 Hacking Techniques & Incident Response	SEC 504	GCIH, NetWars
ISE 5400 Advanced Network Intrusion Detection & Analysis	SEC 503	GCIA, Paper

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. Two written research papers covering general security essentials and intrusion analysis.
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 5100 Enterprise Information Security

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

ISE 5100 is the introductory, 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 paper 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 5200 Hacking Techniques & Incident Response

SANS class: SEC504 Hacker Techniques, Exploits & Incident Handling
Assessment: GIAC GCIH, NetWars Continuous
4 Credit Hours | Tuition: $5,000

By adopting the viewpoint of a hacker, ISE 5200 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, exam, and NetWars simulation are coordinated to develop and test a student's ability to utilize the core capabilities required for incident handling.

ISE 5400 Advanced Network Intrusion Detection & Analysis

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

ISE 5400 arms you with the core knowledge, tools, and techniques to prepare you to defend your networks. Course topics span fundamentals of traffic analysis, application protocols, open source

intrusion detection tools such as Snort and Bro, and network traffic forensics and monitoring. Hands-on exercises include the freely available Packetrix VMWare distribution, developed by SANS faculty member Mike Poor, allowing students to perform packet and traffic analysis using multiple practical techniques. All exercises have two different approaches - a basic one that assists you by giving hints for answering the questions and a second which provides no hints, thus providing a more challenging experience.

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 each course within five months of their course start date, for credit and a grade. 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 application form, 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 for the two 15-20 page applied research papers/projects required in the program.

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