Cyber Defense Operations Graduate Certificate

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.

Cyber Defense Operations Graduate Certificate

The SANS Technology Institute's post-baccalaureate certificate program in Cyber Defense Operations is based upon existing course components from the graduate program leading to a Master of Science Degree in Information Security Engineering.

As an independent offering, the graduate certificate in Cyber Defense Operations is a highly technical, 12 credit hour program with a cohesive and progressive set of learning outcomes. These learning outcomes focus on the student's capability to uncover, analyze, and address the implications of information security vulnerabilities in systems/networks/applications in order to implement solutions and establish an effective defense. A hands-on focus is emphasized throughout the curriculum with multiple lab exercises present in each course.

Cyber Defense Certificate - 12 credit hours:	Graduate course incorporates	
ISE 5401 Advanced Intrusion Detection In-Depth	SEC 503	GCIA
ISE 6240 Continuous Monitoring & Security Operations	SEC 511	GMON
Select two (2) of the following:		
ISE 6001 Implementing and Auditing the Critical Controls	SEC 566	GCCC
ISE 6215 Advanced Security Essentials-Enterprise Defender	SEC 501	GCED
ISE 6230 Securing Windows with PowerShell and the Critical Security Controls	SEC 505	GCWN
ISE 6235 Securing Linux/Unix	SEC 506	GCUX

The graduate certificate in Cyber Defense Operations provides a path for professionals to specialize in a sub-area of the information security field, and this progression of courses in defensive techniques is made available just as they would be to a candidate for the master's degree in Information Security Engineering. Armed with a deep understanding of layered defense-in-depth techniques used by government and private sector organizations to protect their critical assets, the professional who earns the Cyber Defense Operations post-baccalaureate certificate will be empowered to identify and help remediate their organization's vulnerabilities.

Graduates of the Cyber Defense Operations 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. Identify the information assets of an enterprise, classify them by value, and determine what management and technical controls can be used to monitor and audit them effectively.
3. Develop a program for analyzing the risk to the information assets in an enterprise and determining which technical and management controls can mitigate, remove, or transfer that risk.
4. Articulate important attacker techniques, analyze the traffic that flows on networks, and identify indications of an attack, 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:

Standardized exams

1. Required:
    a. GIAC Certified Intrusion Analyst (GCIA) exam
    b. GIAC Certified Continuous Monitoring (GMON) exam
2. Elective Choice of:
    a. GIAC Certified Critical Controls (GCCC) exam
    b. GIAC Certified Enterprise Defender (GCED) exam
    c. GIAC Certified Windows Security Administrator (GCWN) exam
    d. GIAC Certified UNIX Security Administrator (GCUX) exam

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 5401: Advanced Network Intrusion Detection and Analysis
SANS class: SEC 503 Intrusion Detection In-Depth
Assessment: GIAC GCIA
3 Credit Hours | Tuition: $5,000

ISE 5401 arms students with the core knowledge, tools, and techniques to detect and analyze network intrusions, building in breadth and depth for advanced packet and traffic analysis. Hands-on exercises supplement the course book material, allowing students to transfer the knowledge in their heads to their keyboards 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.

SANS Technology Institute

Cyber Defense Operations Graduate Certificate

ISE 6240: Continuous Monitoring & Security Operations

SANS class: SEC 511 Continuous Monitoring and Security Operations
Assessment: GIAC GMON
3 Credit Hours | Tuition: $5,000

A new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses. ISE 6240 teaches this new proactive approach and strengthens student's skills to undertake that proactive approach. The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will help students best position their organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior.

Elective Courses – Choose two of the following:

ISE 6001: Implementing and Auditing Critical Security Controls

SANS class: SEC 566 Implementing and Auditing the Critical Security Controls - In-Depth
Assessment: GIAC GCCC
3 Credit Hours | Tuition: $5,000

Students are introduced to security standards and their implementation, with particular focus on the Consensus Guidelines that were developed through collaboration of U.S. Departments of Defense and Energy, the U.S. Computer Emergency Readiness Team, the FBI and other law enforcement agencies, and civilian penetration testers. The course teaches the theoretical and practical underpinnings for implementing or deploying a strategy for information assurance in an agency or organization to enable them to better understand these guidelines. Specifically the course has been designed with the philosophy of the offense teaching the defense. Using the information presented in the ISE 6001 course, this course helps students understand not only what to do to stop a threat, but why the threat exists and how to ensure that their organization is indeed in compliance with their standards.

ISE 6215: Advanced Security Essentials-Enterprise Defender

SANS class: SEC 501 Advanced Security Essentials - Enterprise Defender
Assessment: GIAC GCED
3 Credit Hours | Tuition: $5,000

Students will learn how to design and build a secure network that can both prevent attacks and recover after a compromise. They will also learn how to retrofit an existing network to achieve the level of protection that is required. While prevention is important to learn, students will also learn how to detect the indications that the attack is in progress and stop it before significant harm is caused. Packet analysis and intrusion detection are at the core of this study detection. In the third module, students will learn about the variety of tests that can be run against an organization and how to perform effective penetration testing. To round out the defensive posture, students will learn the practice of: identifying,

analyzing, and responding effectively to attacks, including the identification of malware and steps that can be taken to prevent data loss.

ISE 6230: Securing Windows with PowerShell and the Critical Controls

SANS class: SEC 505 Securing Windows with the Critical Security Controls
Assessment: GIAC GCWN
3 Credit Hours | Tuition: $5,000

ISE 6230 provides the deep technical information needed to prepare students to design security into systems and networks, including the specifics for hardening end-user devices. The course provides instruction in server and service hardening with laboratory exercises with Windows Server 2012 R2. Data protection is addressed both for data at rest, using whole disk encryption, and in transit, using IPSEC, TLS and other technologies.

ISE 6235: Securing Linux/Unix

SANS class: SEC 506 Securing Linux/Unix
Assessment: GIAC GCUX
3 Credit Hours | Tuition: $5,000

ISE 6235 provides the specific technical education to enable students to secure Linux and Unix clients and infrastructure. This course is particularly valuable for students who are involved with sysadmins and network administrators, given the popularity of *nix tools in that space. The course covers various vulnerabilities and defenses, and includes an introduction to forensic methods for *nix systems.

Enrollment design

The Cyber Defense Operations 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 all of their 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. 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 that may be chosen by a master's candidate during the normal course of studies, all credits earned while completing the Cyber Defense Operations certificate program may be applied directly in fulfillment of the master's degree requirements should the student matriculate later in the master's program.

SANS Technology Institute

Cyber Defense Operations Graduate Certificate

Admissions

Applicants to the Cyber Defense Operations 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 application form, a current resume, and delivery of official undergraduate transcripts.

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