SANS Technology Institute

2025 Graduate Course Catalog

SANS Technology Institute
11200 Rockville Pike, Suite 200
North Bethesda, MD 20852
www.sans.edu | info@sans.edu

Table of Contents

Academic Calendar

SANS Technology Institute students choose from a variety of online and live course delivery options. Students begin their distance courses on the 1st and 15th of each month or live courses on various dates offered throughout the year. While the dates of terms are individualized for each student, the length of each term is standardized and varies only based on the specific course students are enrolled in. Though students enjoy this flexible enrollment model, student progress and enrollment reporting are based on a semi-annual semester cycle, 1/1 - 6/30, and 7/1 - 12/31.

Course lengths are detailed below in the Course Listings and Descriptions section, and full-time requirements are listed in the Student Handbook.

Our offices are closed on: New Year's Day, Martin Luther King Jr. Day, Memorial Day, Juneteenth Day, Independence Day, Labor Day, Thanksgiving and day after Thanksgiving, and Christmas Eve and Day.

Class instruction may be taken in a live classroom or online, as available. The following schedule is not an exhaustive list of live classroom opportunities, but rather larger events we anticipate being most popular with students.

2025 Select Live Learning Event Schedule

Event*	Start Date
Spring Semester Cycle	
SANS New Orleans	February, 2025
SANS Security East	March, 2025
SANS Orlando	April, 2025
SANS Security West	May, 2025
SANS Baltimore Spring	June, 2025
Fall Semester Cycle	
SANSFIRE	July, 2025
SANS Network Security	September, 2025

*Events are subject to change. The full schedule of upcoming events is available online at: https://www.sans.org/cyber-security-events

Programs of Study

The SANS Technology Institute offers the following programs of study at the graduate level:

- Master of Science in Information Security Engineering
- Post-baccalaureate certificate: Cloud Security
- Post-baccalaureate certificate: Cybersecurity Engineering (Core)
- Post-baccalaureate certificate: Cybersecurity Leadership
- Post-baccalaureate certificate: Cyber Defense Operations
- Post-baccalaureate certificate: Incident Response
- Post-baccalaureate certificate: Industrial Control Systems Security
- Post-baccalaureate certificate: Penetration Testing & Ethical Hacking
- Post-baccalaureate certificate: Purple Team Operations
- Post-baccalaureate certificate: Software Supply Chain Security

Master's Degree Program: Master of Science in Information Security Engineering

The program of study for the Master of Science in Information Security Engineering (MSISE) leads to proficiency in knowledge and skills that enable security practitioners to excel as technical leaders. The program is designed to ensure that each student achieves knowledge of the core, foundational domains of information security, plus allows them through elective choices to develop either concentrations in particular domains or add to the breadth of their expertise by exploring a mixed set of topics beyond the core areas. The MSISE program prepares students to weave deep technical expertise into the design of effective cybersecurity. It also provides them with the communications skills and knowledge to gain proactive support for security enhancements from (1) higher-level management, (2) other peer organizational leaders and staff who must cooperate in adopting the enhancements, and (3) technical team members who must build and deploy those enhancements.

Program Learning Outcomes

The program learning outcomes of the MSISE program are designed to ensure that students can:

1. **Formulate and implement comprehensive security policies and solutions.**
    - Demonstrate a thorough understanding of security foundations and practical applications of information technology.
    - Construct balanced security approaches aligning organizational needs with confidentiality, integrity, and availability.
    - Evaluate and design security architectures integrating intrusion detection, defensive infrastructures, and vulnerability analysis.

2. **Apply information security strategies and approaches.**
    - Demonstrate a solid foundation in information security strategies by assessing situations and prescribing appropriate security measures.
    - Analyze and design technical security controls, ensuring compliance with regulatory environments.
    - Apply standards-based approaches to minimize risk and enhance information security.

3. **Communicate and manage information security effectively.**
    - Communicate information security assessments, plans, and actions to both technical and non-technical stakeholders.
    - Manage security teams and build organizations with strong information security cores.
    - Conduct threat assessments, appraise vulnerabilities, and manage technical risks for enterprise information assets.

4. **Identify, investigate, and address emerging security technologies and issues.**
    - Identify and investigate emerging information security issues using security theories and evolving research.
    - Build and maintain awareness of emerging technologies, understanding their opportunities and threats.

- Formulate plans for adaptive detection of threats, leading intrusion detection, incident response, and forensic initiatives.

5. **Educate and align organizational policies with security needs.**
    - Ensure solutions align with policy, technology, and organizational education, training, and awareness programs.
    - Develop and implement comprehensive education and training programs to support security initiatives across the organization.

Curriculum

The M.S. in Information Security Engineering is a 36-credit hour program. Courses within a block can be shifted in order unless otherwise noted, but all must be completed before moving onto the next block.

Required Courses		**Credits**
Block 1		
ISE 5101	Security Essentials	3
ISE 5201	Hacking Techniques & Incident Response	3
ISE 5601	IT Security Leadership Competencies	3
Block 2		
ISE 6255	Defensible Security Architecture & Engineering	3
ISE 5433	Managing Human Risk	2
ISE 5401	Advanced Network Intrusion Detection & Analysis	3
ISE 5701	Situational Response Practicum	1
ISE 5002	Core Comprehensive Exam	0.5
Block 3		
ISE 5001	Security Leadership Essentials for Managers	3
ISE 6999	Elective Course*	3
ISE 6999	Elective Course*	3
Block 4		
ISE 5009	Research Methods**	0.5
ISE 6101	Security Project Practicum**	1
ISE 6999	Elective Course*	3
ISE 6300	NetWars Continuous Practicum	1
ISE 5901	Advanced Technical Research & Communication Practicum	3

**Students choose electives from an approved list of courses. Please see list of acceptable technical elective courses and their full descriptions in the course listings section later in this catalog.*

***ISE 5009 and ISE 6101 are required prerequisites for ISE 5901.*

Focus Areas

Master's candidates may elect to focus their elective courses in a particular area. If choosing a focus area, the student must select the following elective courses:

Focus Area	**Available Elective Courses**
Cloud Security	*Choose 3 from:* ISE 6442, ISE 6610, ISE 6612, ISE 6615, ISE 6630, ISE 6650, ISE 6655
Cyber Defense Operations	*Choose 3 from:* ISE 6215, ISE 6230, ISE 6240, ISE 6250, ISE 6270, ISE 6350
Incident Response	*Choose 3 from:* ISE 6420, ISE 6425, ISE 6440, ISE 6442, ISE 6445, ISE 6450, ISE 6455, ISE 6460, ISE 6608
Industrial Control Systems	ISE 6515, ISE 6520, ISE 6525
Penetration Testing	*Choose 3 from:* ISE 6315, ISE 6320, ISE 6325, ISE 6330, ISE 6350, ISE 6360, ISE 6370, ISE 6630
Cybersecurity Leadership	*Choose 3 from:* ISE 6001, ISE 6700, ISE 6715, or any other elective from the approved catalog

Full course descriptions can be found later in this catalog.

Post-Baccalaureate Certificate Programs

Cloud Security

The Post-baccalaureate Certificate in Cloud Security is a 12-credit-hour program with a cohesive set of learning outcomes focused on teaching cloud security applied concepts, skills, and technologies. Cloud Security certificate students will complete two required core courses and two elective courses, earning four industry recognized GIAC certifications.

Program Learning Outcomes

The program learning outcomes of the Cloud Security Graduate Certificate are designed to ensure that students can:

- Practice and demonstrate mastery of fundamental cloud security knowledge and skills.
- Understand, practice, and demonstrate mastery of important defensive techniques and identify indications of an attack to detect / respond to / mitigate incidents on cloud-based networks and applications.
- Understand, practice, and demonstrate mastery of cloud-based applications and be able to securely implement, integrate, and maintain those applications.

Cloud Security Curriculum

The post-baccalaureate certificate program in Cloud Security is a 12-credit-hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 6610	Cloud Security Essentials	3
ISE 6612	Public Cloud Security: AWS, Azure, and GCP	3
ISE 6999	Elective Course	3
ISE 6999	Elective Course	3

Students are required to take courses in the order listed. Exception requests must be submitted in writing and approved by the Dean of Student's Office.

Elective Course Options

Students will choose one of the following courses as their elective:
ISE 6270, ISE 6615, ISE 6630, ISE 6442, ISE 6650, ISE 6655

Full course descriptions can be found later in this catalog.

Cybersecurity Engineering Core

The Cybersecurity Engineering Core certificate program spans from an introductory 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.

Program Learning Outcomes

The program learning outcomes of the Cybersecurity Engineering (Core) Graduate Certificate are designed to ensure that students are able to:

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

Cybersecurity Engineering Core Curriculum

The post-baccalaureate certificate program in Cybersecurity Engineering Core is a 12-credit-hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 5101 **ISE 6215**	Survey course *(select one)*: Security Essentials Advanced Security Essentials	3
ISE 5201	Hacking Techniques and Incident Response	3
ISE 5401	Advanced Network Intrusion Detection and Analysis	3
ISE 6999	Elective Course *Students choose an elective from an approved list of courses.*	3
ISE 6200	Capstone: Core Comprehensive Exam	1

Students are required to take courses in the order listed. Exception requests must be submitted in writing and approved by the Dean of Student's Office.

Full course descriptions can be found later in this catalog.

Cybersecurity Leadership

The Post-baccalaureate Certificate in Cybersecurity Leadership is a 16-credit hour program with a cohesive set of learning outcomes focused on preparing experienced information security practitioners to become effective managers and leaders. Cybersecurity Leadership certificate students will complete four required core courses and two elective courses, earning five industry recognized GIAC certifications.

Program Learning Outcomes

The program learning outcomes of the Cybersecurity Leadership Graduate Certificate are designed to ensure that students can:

- Manage the information security function in an enterprise in a way that takes into account the relationship between and responsibilities shared by the communities of interest in an enterprise. These include the general business, information technology, and information security.
- Apply a standards-based approach to implement the principles and applications of risk management, including business impact analyses, cost-benefit analyses, and implementation methods that map to business needs/requirements.
- Integrate the elements of information security management-policy, strategic and continuity planning, implementation programs, and personnel-into an operation that can effectively manage the security needs of an enterprise.
- Articulate positions on the legal issues associated with the protection of information and privacy that meet generally accepted ethical standards and the security and business needs of the enterprise.
- Devise strategies and programs for incident detection and response, including business continuity planning and disaster recovery planning (BCP/DRP), that are cost effective and meet the business needs of the enterprise.

Cybersecurity Leadership Curriculum

The post-baccalaureate certificate program in Cybersecurity Leadership is a 16-credit hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 5001	Security Leadership Essentials for Managers	3
ISE 6700	Building and Leading Security Operations Centers	3
ISE 5601	Security Strategic Planning, Policy, and Leadership	3
ISE 5605*	Business Finance Essentials	1
ISE 6999	Elective Course	3
ISE 6999	Elective Course	3

*ISE 5605 is only available in the OnDemand modality.

Students are required to take courses in the order listed. Exception requests must be submitted in writing and approved by the Dean of Student's Office.

Elective Course Options

Students can choose electives from two groups: leadership and technical. Students can either take two leadership electives or one elective from each group. Students cannot take more than one technical elective.

Leadership elective courses: ISE 5800, ISE 6001

Technical elective courses: ISE 5201, ISE 6255, ISE 6270, ISE 6445

Full course descriptions can be found later in this catalog.

Cyber Defense Operations

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.

Program Learning Outcomes

The program learning outcomes of the Cyber Defense Operations Graduate Certificate are designed to ensure that students can:

- Utilize a broad range of current tools and technologies in the design and implementation of security solutions deployed across organizations.
- 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.
- 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.
- 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.

Cyber Defense Operations Curriculum

The post-baccalaureate certificate program in Cyber Defense Operations is a 12-credit-hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 6240*	Continuous Monitoring and Security Operations	3
ISE 6255	Defensible Security Architecture & Engineering	3
ISE 6999	Elective Course	3
ISE 6999	Elective Course	3

*For students early in their career or new to working in a SOC environment, ISE 4450 is recommended as a prerequisite to ISE 6240.

Students are required to take courses in the order listed. Exception requests must be submitted in writing and approved by the Dean of Student's Office.

Elective Course Options

Students will choose two of the following courses as their electives:

ISE 4450, ISE 6215, ISE 5401, ISE 6230, ISE 6250, ISE 6270, ISE 6350, ISE 6655

Full course descriptions can be found later in this catalog.

Incident Response

The Graduate Certificate program in Incident Response 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 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.

Program Learning Outcomes

The program learning outcomes of the Incident Response Graduate Certificate are designed to ensure that students can:

- 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.
- Analyze the structure of common attack techniques to evaluate an attacker's footprint, target the ensuing investigation and incident response, and anticipate and mitigate future activity.
- Evaluate the effectiveness of available digital forensic tools and use them in a way that optimizes the efficiency and quality of digital forensic investigations.
- 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.

Incident Response Curriculum

The post-baccalaureate certificate program in Incident Response is a 12-credit-hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 6420*	Computer Forensic Investigations - Windows	3
ISE 6425	Advanced Computer Forensic Analysis & Incident Response	3
ISE 6440	Advanced Network Forensics & Analysis	3
ISE 6999	Elective Course	3

*For students early in their career or new to working in forensics, ISE 5201 is recommended as a pre-requisite to ISE 6420 as it introduces incident handling vocabulary.

Students are required to take courses in the order listed. Exception requests must be submitted in writing and approved by the Dean of Student's Office.

Elective Course Options

Students will choose one of the following courses as their electives:

ISE 5201, ISE 6270, ISE 6442, ISE 6445, ISE 6450, ISE 6455, ISE 6460, ISE 6608

Full course descriptions can be found later in this catalog.

Industrial Control Systems Security

The Industrials Control Systems Security Graduate Certificate program provides a broad and integrated mechanism for students to learn the essential security awareness, work-specific knowledge, and hands-on technical skills needed to secure automation and control system technology. These systems often form the backbone of infrastructures identified as critical to national security, economic security, public health, or safety. Traditional defenses found in business or corporate IT environments are not always effective when applied to the industrial or operation technology space. Legacy equipment, proprietary hardware and software, non-traditional protocols, and consideration for the health and safety of equipment, personnel, and communities all add to the challenges of securing these environments.

Program Learning Outcomes

The program learning outcomes of the Industrial Control Systems Security Graduate Certificate are designed to ensure that students can:

- Learn, integrate, practice, and demonstrate mastery of the essential knowledge, technical skills, and leadership abilities relevant to securing automation and control system technology.
- Utilize a broad range of current tools and technologies in the design and implementation of security solutions deployed across critical infrastructure organizations.
- Identify the information assets within an automation or control systems environment, classify them by value, and determine what management and technical controls can be used to monitor and audit them effectively and securely.
- Develop a program for analyzing the risk to the information assets in an automation or control systems environment and determine which technical and management controls can mitigate, remove, or transfer that risk.
- Articulate important attacker techniques, analyze the traffic that flows on automation or control system networks, and identify indications of an attack, engage in testing and auditing within their organization, and respond to incidents associated with these activities within their organization.

Industrial Control Systems Security Curriculum

The post-baccalaureate certificate program in Industrial Control Systems Security is a 12-credit-hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 6515	ICS/SCADA Security Essentials	3
ISE 6520	ICS Active Defense and Incident Response	3
ISE 6425 **ISE 6525** **ISE 6610**	*Specialization elective (select one):* Advanced Incident Response, Threat Hunting, and Digital Forensics Essentials for NERC Critical Infrastructure Protection Cloud Security Essentials	3
ISE 6999	Elective Course *Students choose an elective from an approved list of courses.*	3

Students are required to take courses in the order listed. Exception requests must be submitted in writing and approved by the Dean of Student's Office.

Elective Course Options

Students will choose any graduate technical elective for their additional elective.

Full course descriptions can be found later in this catalog.

Penetration Testing & Ethical Hacking

The Penetration Testing & Ethical Hacking Graduate Certificate curriculum advances the student's knowledge of the strategies and techniques utilized by hackers to gain access to networks and systems and builds on this base to allow students to further specialize their knowledge within different types of vulnerable networks and systems. Students must take a core penetration testing and incident handling course, two additional courses focused on penetration testing of networks and web applications, and then students may choose a further specialization from courses focused on mobile, wireless, or advance network penetration testing and incident handling. Students will demonstrate deep technical knowledge in identifying and analyzing risks while providing solutions to minimize the risk.

Program Learning Outcomes

The program learning outcomes of the Penetration Testing & Ethical Hacking Graduate Certificate are designed to ensure that students can:

- Conduct vulnerability scanning and exploitation of various systems and applications using a careful, documented methodology to provide explicit proof of the extent and nature of IT infrastructure risks, conducting these activities according to well-defined rules of engagement and a clear scope.
- Provide documentation of activities performed during testing, including all exploited vulnerabilities and how those vulnerabilities were combined into attacks to demonstrate business or institutional risk.
- Produce an estimated risk level for a given discovered flaw by using the amount of effort the team needed to expend in penetrating the information system as an indicator of the penetration resistance of the system.
- Provide actionable results with information about possible remediation measures for the successful attacks performed.

Penetration Testing & Ethical Hacking Curriculum

The post-baccalaureate certificate program in Penetration Testing & Ethical Hacking is a 12-credit-hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 5201	Hacking Techniques & Incident Response	3
ISE 6320	Enterprise Penetration Testing	3
ISE 6315 **ISE 6325** **ISE 6630**	Specialization Elective *(select one):* Web App Penetration Testing & Ethical Hacking Mobile Device Security & Ethical Hacking Cloud Penetration Testing	3
ISE 6999	Elective Course	3

Students are required to take courses in the order listed. Exception requests must be submitted in writing and approved by the Dean of Student's Office.

Elective Course Options

Students will choose one of the following courses as their elective:

ISE 6270, ISE 6315, ISE 6325, ISE 6330, ISE 6350, ISE 6360, ISE 6370, ISE 6630

Full course descriptions can be found later in this catalog.

Purple Team Operations

The Graduate Certificate in Purple Team Operations is a 12-credit-hour program with a cohesive set of learning outcomes focused on teaching blue and red applied concepts, skills, and technologies used in a merged fashion in the current best practice known as purple operations, or purple teams. This program is intended for experienced information security practitioners who are interested in rounding out their blue and red skills to effectively operate and lead at the intersection of those domains.

Program Learning Outcomes

The primary educational objectives of the program are to:

- Practice and demonstrate mastery of fundamental network security knowledge and skills.
- Understand, practice, and demonstrate mastery of important defensive techniques and identify indications of an attack to detect / respond to/ mitigate incidents on enterprise networks.
- Understand, practice, and demonstrate mastery of important attacker techniques and be able to utilize the full range of penetration techniques to breach a network, pivot within it, and disrupt, exploit, or exfiltrate data from it.
- Utilize a broad range of both blue team and red team tools, technologies, and mindsets in the integrated design and implementation of purple security activities and exercises in order to maximize the synergy of full spectrum security operations.

Purple Team Operations Curriculum

The post-baccalaureate certificate program in Purple Team Operations is a 12-credit-hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 5201	Hacking Techniques & Incident Response	3
ISE 6999	Students will select one Blue Team Elective	3
ISE 6999	Students will select one Red Team Elective	3
ISE 6250	Capstone: Purple Team Tactics & Kill Chain Defenses	3

Students are required to take courses in the order listed. Exception requests must be submitted in writing and approved by the Dean of Student's Office.

Elective Course Options

Students will choose one of the following courses as their Blue Team Elective:
ISE 5401, ISE 6215, ISE 6230, ISE 6240, ISE 6255, ISE 6270, ISE 6445

Students will choose one of the following courses as their Red Team Elective:
ISE 6315, ISE 6320, ISE 6325, ISE 6360, ISE 6370, ISE 6630

Full course descriptions can be found later in this catalog.

Software Supply Chain Security

The Graduate Certificate in Software Supply Chain Security is a 12-credit-hour program with a cohesive set of learning outcomes focused on teaching secure development applied concepts, skills, and technologies. This program is intended to support developers and leaders in the software supply chain to better support their teams and organizations in securely designing, writing, packaging, and deploying software.

Program Learning Outcomes

The primary educational objectives of the program are to:

- Understand the importance of a "***Security First***" or "***Shift Left***" mindset.
- Have a greater understanding of public cloud platforms and infrastructure.
- Recognize and mitigate common application and web application attacks.
- Holistically secure ***Software Development Lifecycles*** (SDLC), APIs, and microservices.
- Better implement and automate security, infrastructure, compliance, and auditing capabilities.

Software Supply Chain Security Curriculum

The post-baccalaureate certificate program in Software Supply Chain Security is a 12-credit-hour program, comprised of the following courses:

Required Courses		**Credits**
ISE 6650	Cloud Security and DevSecOps Automation	3
ISE 6612	Public Cloud Security: AWS, Azure, and GCP	3
ISE 6615	Defending Web Applications Security Essentials	3
ISE 6999	Elective course	3

Students are required to take courses in the order listed. Exception requests must be submitted in writing and approved by the Dean of Student's Office.

Elective Course Options

Students will choose one of the following courses as their elective:

ISE 5800, ISE 6315, ISE 6350, ISE 6610, ISE 6630, ISE 6715

Full course descriptions can be found later in this catalog.

Course Listings and Descriptions

Required Courses

These courses are required in at least one of the SANS.edu Graduate-level programs.

ACS 3275: Foundations: Computers, Technology, & Security
SANS SEC275 | GIAC GFACT | 3 Credit Hours | 90 Days

Restrictions | *This course is only required if conditionally admitted to the MSISE program.*

ACS 3275 is purpose-built to provide students with the fundamental technical knowledge and skills that serve as the baseline for all professionals in cybersecurity, reinforcing key concepts with interactive labs. Students establish a core understanding of technology component functions and apply that knowledge to security concepts such as reconstructing a crime from digital evidence or locating exploitable flaws in software and websites. The course ensures a solid mastery of computer, hardware, network, and cybersecurity fundamentals, including the study of operating systems, Windows security tools, Linux, programming with Python and C, advanced Google searches, reconnaissance, virtualization, and encryption. Students explore the inner workings of packets and protocols that allow the internet to function and learn the role of a computer's central processing unit (CPU), how it executes code, its relationship with memory, and the fundamentals of how attackers disrupt intended behavior.

ISE 4450: Security Operations and Analysis
SANS SEC450 | GIAC GSOC | 3 Credit Hours | 90 Days

Restrictions | *This course is only available in the Cyber Defense Operations Program.*

ISE 4450 is an accelerated on-ramp for new cyber defense team members and SOC managers. This course introduces students to the tools common to a defender's work environment, and packs in all the essential explanations of tools, processes, and data flow that every blue team member needs to know. Students will learn the stages of security operations: how data is collected, where it is collected, and how threats are identified within that data. The class dives deep into tactics for triage and investigation of events that are identified as malicious, as well as how to avoid common mistakes and perform continual high-quality analysis. Students will learn the inner workings of the most popular protocols, and how to identify weaponized files as well as attacks within the hosts and data on their network.

ISE 5001: Security Leadership Essentials for Managers
SANS LDR512 | GIAC GSLC | 3 Credit Hours | 90 Days

ISE 5001 covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls are covered in conjunction with key management topics that address the overall security lifecycle, including governance and technical controls focused on protecting, detecting, and responding to security issues.

ISE 5002: MSISE Program Midterm
Core Comprehensive Exam | 0.5 Credit Hour | 14 Days

The Core Comprehensive Exam determines if candidates have mastered the core technical skills required by top security consultants and individual practitioners. Through a series of exercises, students demonstrate their ability to integrate the knowledge, skills and techniques acquired in ISE 5101, ISE 5201, and ISE 5401 to address common challenges faced by technical leaders in the cybersecurity field.

ISE 5009: Research Methods
0.5 Credit Hours | 6 Months

This course will prepare you to conduct graduate-level research exploring a current applied cyber security problem. You will learn how to select an appropriate research question, design an experiment, and analyze the experiment's outcome to answer the research question. Students will develop a proposal for the research paper to be written in ISE 5901: Advanced Technical Research & Communication Practicum and learn how to complete the research paper requirements for the practicum.

ISE 5101: Security Essentials
SANS SEC401 | GIAC GSEC | 3 Credit Hours | 90 Days

ISE 5101 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, and exam are coordinated to introduce and develop the core technical, management, and enterprise-level capabilities that will be developed throughout the rest of the certificate program.

ISE 5201: Hacker Tools, Techniques, Exploits, & Incident Handling
SANS SEC504 | GIAC GCIH | 3 Credit Hours | 90 Days

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: Intrusion Detection In-Depth
SANS SEC503 | GIAC GCIA | 3 Credit Hours | 90 Days

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.

ISE 5433: Managing Human Risk
SANS LDR433 | SANS SSAP Exam | 1 Credit Hour | 45 Days

Restrictions | *This course is only available through SANS OnDemand.*

From phishing attacks and credential stuffing to lost devices or auto-complete in email, human risk has become the primary risk for most organizations. One of the most effective ways for an organization to manage its human risk is to build on their existing technical controls with a mature security awareness program. The program must go beyond just compliance and change organizational behaviors and ultimately, culture. In ISE 5433, you will learn the key concepts and skills to plan, maintain, and measure an effective security awareness program that makes an organization both more secure and compliant. Through a series of labs and exercises, you will develop your security awareness plan and complete the SANS Security Awareness Professional (SSAP) exam.

ISE 5601: IT Security Planning, Policy, & Leadership
SANS LDR514 | GIAC GSTRT | 3 Credit Hours | 90 Days

ISE 5601 covers the critical processes to be employed by technical leaders to develop the skills and techniques to select, train, equip, and develop a team into a single cohesive unit with defined roles that operate together in harmony toward team-objective accomplishment. Topics covered include: leadership development, coaching and training, employee involvement, conflict resolution, change management, vision development, motivation, communication skills, self-direction, brainstorming techniques, strategic planning and policy development, and the ten core leadership competencies.

ISE 5605: Business Finance Essentials
SANS SEC405 | None | 1 Credit Hour | 30 Days

Restrictions | *This course is only available in the Cybersecurity Leadership Program and must be taken in the OnDemand modality.*

ISE 5605 takes information security leaders on a journey to help them understand and successfully navigate their organization's financial status. Understanding and effectively communicating financial stewardship will contribute to their success, the success of the cybersecurity team that they lead, and, ultimately, the success of their organization.

ISE 5701: Situational Response Practicum
SANS SEC402, SEC405 | 1 Credit Hour | 45 Days

Restrictions | *SEC 402 and SEC 405 must be taken through SANS OnDemand.*

The purpose of this course is for students to learn and be assessed on their ability to come together as a team, assess a situation, develop a response, and prepare recommendations for decision to a C-Level audience within forty-five (45) days. You are put into a small group with other students and presented with an information security topic prompt. Your group then prepares a plan for researching and reporting on the assignment. Once the plan is prepared, the group executes the plan, adjusting as necessary, to develop a report of the research completed recommended actions.

ISE 5901: Advanced Technical Research & Communication Practicum
3 Credit Hours | 120 Days*
*Following approval of the student's initial proposal

Restrictions | *ISE 5009 and ISE 6101 are prerequisites for this course.*

ISE 5901 is an advanced graduate-level research and presentation course in which students will identify, investigate, and analyze a problem. Students will write a whitepaper interpreting the data collected and making recommendations for action. The whitepaper 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.

Students will then convert written material to an oral presentation in order to inform a technical audience about the topic. Delivered via a webinar, students use material from their paper to build and deliver a 30-minute presentation and to then field questions. Students demonstrate a variety of presentation skills. Exemplary presentations may be selected to present at a live SANS event for further professional development.

ISE 6101: Security Project Practicum
SANS SEC403 | 1 Credit Hour | 30 Days

The purpose of this course is for students to learn and be assessed on their ability to come together as a team, assess a situation, demonstrate leadership, develop a response, and prepare and present recommendations for a decision to a C-Level audience within 24-hours. This course builds on what you have learned in other courses and allows you to apply that knowledge. You are put into a small group with other students and presented with an information security topic prompt. Working as a group, you will analyze the situation, develop a technical response, and develop recommendations for an organizational response to the situation presented. Upon development of your recommended response, the group provides written and oral reports of recommendations for action to a mixed technical/non-technical audience of executives for decision.

ISE 6200: Capstone: Core Comprehensive Exam
Core Comprehensive Exam | 1 Credit Hour | 30 Days

The Core Comprehensive Exam determines if candidates have mastered the core technical skills required by top security consultants and individual practitioners. Through a series of exercises, students demonstrate their ability to integrate the knowledge, skills and techniques acquired in ISE 5101, ISE 5201, and ISE 5401 to address common challenges faced by technical leaders in the cybersecurity field.

ISE 6255: Defensible Security Architecture and Engineering
SANS SEC530 | GIAC GDSA | 3 Credit Hours | 90 Days

Effective security requires a balance between detection, prevention, and response capabilities. Defensible Security Architecture and Engineering is designed to help students establish and maintain a holistic and layered approach to security. Students will learn the fundamentals of up-to-date defensible security architecture and how to engineer it, with a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to significantly improve their organization's prevention

capabilities in the face of today's dynamic threat landscape. The course will also delve into the latest technologies and their capabilities, strengths, and weaknesses. Multiple hands-on labs conducted daily will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

ISE 6300: NetWars Continuous Practicum
1 Credit Hour | 60 Days

NetWars Continuous is an online training program that guides students through hands-on lessons to locate vulnerabilities, exploit diverse machines, and analyze systems. NetWars provides a forum to test and perfect cyber security skills in a manner that is legal and ethical. Students will face challenges derived from real-world environments and actual attacks that businesses, governments, and military organizations must deal with every day.

Technical Elective Course Options

The following are technical elective courses. Students in the MSISE program must choose 3 courses from this list. Graduate Certificate programs may require one or more elective options to be chosen from this list.

ISE 6001: Implementing & Auditing the Critical Security Controls
SANS SEC566 | GIAC GCCC | 3 Credit Hours | 90 Days

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. ISE 6001 will help you to ensure that your organization has an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches. As threats evolve, an organization's security should too. Standards based implementation takes a prioritized, risk-based approach to security and shows you how standardized controls are the best way to block known attacks and mitigate damage from successful attacks.

ISE 6215: Advanced Security Essentials
SANS SEC501 | GIAC GCED | 3 Credit Hours | 90 Days

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. 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 6240: Continuous Monitoring & Security Operations
SANS SEC511 | GIAC GMON | 3 Credit Hours | 90 Days

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.

ISE 6250: Purple Team Tactics & Kill Chain Defenses
SANS SEC599 | GIAC GDAT | 3 Credit Hours | 90 Days

ISE 6250 leverages the purple team concept by bringing together red and blue teams for maximum effect. Recognizing that a prevent-only strategy is not sufficient, the course focuses on current attack strategies and how they can be effectively mitigated and detected using a Kill Chain structure. Throughout the course, the purple team principle will be maintained, where attack techniques are first explained in-depth, after which effective security controls are introduced and implemented.

ISE 6270: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals
SANS SEC595 | GIAC GMLE | 3 Credit Hours | 90 Days

Restrictions | *You should have intermediate understanding of the Python language. ISE 6350 is a recommended prerequisite.*

ISE 6270 is squarely centered on solving information security problems. This course covers the necessary mathematics theory and fundamentals students absolutely must know to allow them to understand and apply the machine learning tools and techniques effectively. The course progressively introduces and applies various statistic, probabilistic, or mathematic tools (in their applied form), allowing students to leave with the ability to use those tools. The hands-on projects provide a broad base from which students can build their own machine learning solutions. This course teaches how AI tools like ChatGPT really work so that students can intelligently discuss their potential use by organizations and how to build effective solutions to solve real cybersecurity problems using machine learning and AI.

ISE 6315: Web App Penetration Testing and Ethical Hacking
SANS SEC542 | GIAC GWAPT | 3 Credit Hours | 90 Days

ISE 6315 is a highly technical information security course in offensive strategies where students learn the art of exploiting Web applications so they can find flaws in enterprise Web apps before they are otherwise discovered and exploited. Through detailed, hands-on exercises students learn the four-step process for Web application penetration testing. Students will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. They then utilize cross-site scripting attacks to dominate a target infrastructure in a unique hands-on laboratory environment. Finally, students explore various other Web app vulnerabilities in-depth with tried-and-true techniques for finding them using a structured testing regimen.

ISE 6320: Enterprise Penetration Testing
SANS SEC560 | GIAC GPEN | 3 Credit Hours | 90 Days

ISE 6320 prepares students to conduct successful penetration testing for a modern enterprise, including on-premise systems, Azure, and Azure AD. Students will learn how to plan, prepare, and execute a penetration test in a modern enterprise. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively. Using the latest penetration testing tools, students will undertake extensive hands-on lab exercises to learn the methodology of experienced attackers and practice their skills.

ISE 6325: Mobile Device Security & Ethical Hacking
SANS SEC575 | GIAC GMOB | 3 Credit Hours | 90 Days

ISE 6325 helps students resolve their organization's struggles with mobile device security by equipping then with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course teaches students to build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in their organization.

ISE 6330: Wireless Penetration Testing & Ethical Hacking
SANS SEC617 | GIAC GAWN | 3 Credit Hours | 90 Days

ISE 6330 takes an in-depth look at the security challenges of many different wireless technologies, exposing students to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, students will navigate through the techniques attackers use to exploit WiFi networks, Bluetooth devices, and a variety of other wireless technologies. Using assessment and analysis techniques, this course will show students how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

ISE 6350: Python for Penetration Testers
SANS SEC573 | GIAC GPYC | 3 Credit Hours | 90 Days

The ISE 6350 course teaches student in the pen testing specialization, and other students who want to use the Python programming language, how to enhance their overall effectiveness during information security engagements. Students will learn how to apply core programming concepts and techniques learned in other courses through the Python programming language. The course teaches skills and techniques that can enhance an information security professional in penetration tests, security operations, and special projects. Students will create simple Python-based tools to interact with network traffic, create custom executables, test and interact with databases and websites, and parse logs or sets of data.

ISE 6360: Advanced Penetration Testing, Exploit Writing, & Ethical Hacking
SANS SEC660 | GIAC GXPN | 3 Credit Hours | 90 Days

ISE 6360 builds upon ISE 6320 – Enterprise Penetration Testing. This advanced course introduces students to the most prominent and powerful attack vectors, allowing students to perform these attacks in a variety of hands-on scenarios. This course is an elective course in the Penetration Testing & Ethical Hacking certificate program, and an elective choice for the Master's program in Information Security Engineering.

ISE 6370: Red Team Operations and Adversary Emulation
SANS SEC565 | GIAC GRTP | 3 Credit Hours | 90 Days

ISE 6370 develops Red Team operators capable of planning and executing consistent and repeatable engagements that are focused on training and on measuring the effectiveness of the people, processes, and technology used to defend environments. Students will learn how to plan and execute end-to-end Red Teaming engagements that leverage adversary emulation, including the skills to organize a Red Team, consume threat intelligence to map against adversary tactics, techniques, and procedures (TTPs), emulate those TTPs, report and analyze the results of the Red Team engagement, and ultimately improve the overall security posture of the organization. As part of the course, students will perform an adversary emulation against a target organization modeled on an enterprise environment, including Active Directory, intelligence-rich emails, file servers, and endpoints running in Windows and Linux. Through this course, students will better understand and be able to show the value that Red Teaming and adversary emulations bring to an organization.

ISE 6420: Computer Forensic Investigations – Windows
SANS FOR500 | GIAC GCFE | 3 Credit Hours | 90 Days

ISE 6420 Computer Forensic Investigations – Windows focuses on the critical knowledge of the Windows Operating System that every digital forensic analyst needs to investigate computer incidents successfully. Students learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations or civil/criminal litigation. The course covers the methodology of in-depth computer forensic examinations, digital investigative analysis, and media exploitation so each student will have complete qualifications to work as a computer forensic investigator helping to solve and fight crime.

ISE 6425: Advanced Digital Forensics, Incident Response, & Threat Hunting
SANS FOR508 | GIAC GCFA | 3 Credit Hours | 90 Days

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 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 Forensic Analysis
SANS FOR572 | GIAC GNFA | 3 Credit Hours | 90 Days

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. Students will employ a wide range of open source and commercial tools, exploring real-world scenarios to help the student learn the underlying techniques and practices to best evaluate the most common types of network-based attacks.

ISE 6442: Enterprise Cloud Forensics and Incident Response
SANS FOR509 | GIAC GCFR | 3 Credit Hours | 90 Days

In ISE 6442: Enterprise Cloud Forensics and Incident Response, examiners will learn how each of the major cloud service providers (Microsoft Azure, Amazon AWS and Google Cloud Platform) are extending analyst's capabilities with new evidence sources not available in traditional on-premise investigations. Incident response and forensics are primarily about following breadcrumbs left behind by attackers. This class is primarily a log analysis class to help examiners come up to speed quickly with cloud based investigation techniques. Numerous hands-on labs throughout the course will allow examiners to access evidence generated based on the most common incidents and investigations. Examiners will learn where to pull data from and how to analyze it to find evil.

ISE 6445: Cyber Threat Intelligence
SANS FOR578 | GIAC GCTI | 3 Credit Hours | 90 Days

ISE 6445 will equip you, your security team, and your organization in the tactical, operational, and strategic level cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and to accurately and effectively counter those threats. This course focuses on structured analysis to establish a solid foundation for any security skillset and to amplify existing skills.

ISE 6450: Advanced Smartphone Forensics
SANS FOR585 | GIAC GASF | 3 Credit Hours | 90 Days

The focus of ISE 6450 is on teaching students how to perform forensic examinations on devices such as mobile phones and tablets. Students will add to their forensics skills with this course's focus on the advanced skills of mobile forensics, device file system analysis, mobile application behavior, event artifact analysis and the identification and analysis of mobile device malware. Students will learn how to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features a number of hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools.

ISE 6455: Mac and iOS Forensic Analysis and Incident Response
SANS FOR518 | GIAC GIME | 3 Credit Hours | 90 Days

ISE 6455 provides the techniques and skills necessary to take on any Mac or iOS case without hesitation. The intense hands-on forensic analysis and incident response skills taught in the course will enable students to broaden their capabilities and gain the confidence and knowledge to comfortably analyze any Mac or iOS device. In addition to traditional investigations, the course presents intrusion and incident response scenarios to help analysts learn ways to identify and hunt down attackers that have compromised Apple devices.

ISE 6460: Reverse-Engineering Malware
SANS FOR610 | GIAC GREM | 3 Credit Hours | 90 Days

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 6515: ICS/SCADA Security Essentials
SANS ICS410 | GIAC GICSP | 3 Credit Hours | 90 Days

ISE 6515 ICS/SCADA Security Essentials is an introductory study of the information technology and operational technology roles that have converged in today's industrial control system environments. This convergence has led to a greater need for a common understanding between the various groups who support or rely on these systems. Students in ISE 6515 will learn the language, the underlying theory, and the basic tools for industrial control system security in settings across a wide range of industry sectors and applications.

ISE 6520: ICS Active Defense and Incident Response
SANS ICS515 | GIAC GRID | 3 Credit Hours | 90 Days

ISE 6520 will empower students to understand their networked industrial control system environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. The course uses a hands-on approach and real-world malware to break down cyber-attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations.

ISE 6525: Essentials for NERC Critical Infrastructure Protection
SANS ICS456 | GIAC GCIP | 3 Credit Hours | 90 Days

ISE 6525 empowers students with knowledge of the "what" and the "how" of the version 5/6 standards. The course addresses the role of FERC, NERC and the Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

ISE 6610: Cloud Security Essentials
SANS SEC488 | GIAC GCLD | 3 Credit Hours | 90 Days

ISE 6610 will prepare you to advise and speak about a wide range of topics and help your organization successfully navigate both the security challenges and opportunities presented by cloud services. Like foreign languages, cloud environments have similarities and differences, and SEC488 covers all the major CSPs and thus all of the languages of cloud services.

ISE 6612: Public Cloud Security: AWS, Azure, and GCP
SANS SEC510 | GIAC GPCS | 3 Credit Hours | 90 Days

ISE 6612 provides cloud security practitioners, analysts, and researchers with an in-depth understanding of the inner workings of the most popular public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Students will learn industry-renowned standards and methodologies, such as the MITRE ATT&CK Cloud Matrix and CIS Cloud Benchmarks, then apply that knowledge in hands-on exercises to assess a modern web application that leverages the cloud native offerings of each provider. Through this process students will learn the philosophies that undergird each provider and how these have influenced their services.

ISE 6615: Defending Web Applications Security Essentials
SANS SEC522 | GIAC GWEB | 3 Credit Hours | 90 Days

ISE 6615 covers the OWASP Top 10 and provides students with a better understanding of web application vulnerabilities, enabling them to properly defend organizational web assets. Mitigation strategies from an infrastructure, architecture, and coding perspective are discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities is also covered so students can ensure their application is tested for the vulnerabilities discussed in class.

ISE 6630: Cloud Penetration Testing
SANS SEC588 | GIAC GCPN | 3 Credit Hours | 90 Days

ISE 6630 will equip you with the latest in cloud focused penetration testing techniques and teach you how to assess cloud environments. In this course we dive into topics like cloud based microservices, in-memory data stores, serverless functions, Kubernetes meshes, and containers, as well as identifying and testing in cloud-first and cloud-native applications. You will also learn specific tactics for penetration testing in Azure and AWS, particularly important given that Amazon Web Services and Microsoft account for more than half of the market. It's one thing to assess and

secure a datacenter, but it takes a specialized skillset to truly assess and report on the risk that an organization faces if their cloud services are left insecure.

ISE 6650: Cloud Security and DevOps Automation
SANS SEC540 | GIAC GCSA | 3 Credit Hours | 90 Days

ISE 6650 provides development, operations, and security professionals with a methodology to build and deliver secure infrastructure and software using DevOps and cloud services. Students will explore how the principles, practices, and tools of DevOps can improve the reliability, integrity, and security of on-premises and cloud-hosted applications. Starting with on-premises deployments, the first two days of the course examine the Secure DevOps methodology and its implementation using lessons from successful DevOps security programs. Students will gain hands-on experience using popular open-source tools to automate Configuration Management ("infrastructure as Code"), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance ("Compliance as Code"), and Continuous Monitoring. After laying the DevSecOps foundation, the final three days move DevOps workloads to the cloud, build secure cloud infrastructure, and deliver secure software.

ISE 6655: Cloud Security Attacker Techniques, Monitoring and Threat Detection
SANS SEC541 | GIAC GCTD | 3 Credit Hours | 90 Days

ISE 6655 focuses on cloud threat detection, covering various attack techniques used against cloud infrastructure and teaching the observation, detection, and analysis of cloud telemetry. With 20 hands-on labs and CTF, this course equips security analysts, detection engineers, and threat hunters with practical skills and knowledge to safeguard their organization's cloud infrastructure against potential threats.

ISE 6700: Building and Leading Security Operations Centers
SANS LDR551 | GIAC GSOM | 3 Credit Hours | 90 Days

Managing a security operations center (SOC) requires a unique combination of technical knowledge, management skills, and leadership ability. Whether you are looking to build a new SOC or take your current team to the next level, this course provides the right balance of these elements to super-charge your people, tools, and processes. You will learn how to build a high-performing SOC tailored to your organization and the threats it faces. You will be given the tools needed to manage an effective defense, measure progress towards your goals, and build out more advanced processes like threat hunting, active defense, and continuous SOC assessment. Each section includes hands-on labs, introductions to some of the industry's best free and open-source tools, and an interactive game in which you will apply your new SOC management skills in real-world scenarios.

ISE 5800: IT Security Project Management
SANS LDR525 | GIAC GCPM | 3 Credit Hours | 90 Days

Restrictions | *This course is only available as an elective within Cybersecurity Leadership Certificate.*

In ISE 5800 you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. The course utilizes project case studies that highlight information technology services as deliverables. ISE 5800 follows the basic project

management structure from the PMBOK® Guide 5th edition and provides specific techniques for success with information assurance initiatives. All aspects of IT project management are covered - from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes.

ISE 6608: Enterprise-Class Incident Response & Threat Hunting
SANS FOR608 | GIAC GEIR | 3 Credit Hours | 90 Days

ISE 6608 focuses on identifying and responding to incidents too large to focus on individual machines. The concepts are similar: gathering, analyzing, and making decisions based on information from hundreds of machines. This requires the ability to automate and the ability to quickly focus on the right information for analysis. By using example tools built to operate at enterprise-class scale, students will learn the techniques to collect focused data for incident response and threat hunting. Students will then dig into analysis methodologies, learning multiple approaches to understand attacker movement and activity across hosts of varying functions and operating systems by using timeline, graphing, structured, and unstructured analysis techniques.

Credit Hours

A credit hour is the unit of measurement representing the amount of work typically required by an average student over a specified period in achieving intended learning outcomes. The SANS Technology Institute's Credit Hour Policy calculates credit hours based on reasonable approximations of instruction and student preparation work, in alignment with the credit hour as defined by the Maryland Higher Education Commission.

For standard courses, credit hours are calculated based on the total number of contact hours, including course content, assignments, and labs, in addition to the expected student preparation work, as outlined in the course syllabus.

For practicum courses, credit hours are reasonably approximated at 1 credit per 45 instructional hours.

Admissions Requirements and Application Process

All applicants must meet the following criteria:

- Have at least 12 months of professional work experience in information technology, or security.
- Be employed or have current access to an organizational environment that allows students to apply the concepts and hands-on technical skills learned during their program.
- Have earned a baccalaureate degree from a recognized college or university, or the international equivalent, with a minimum cumulative grade point average of 2.8.

All applicants must submit the following (detailed application guidelines can be found online):

a) Application Form
b) Current Resume
c) Official Transcripts
d) Application Fee
e) Aptitude Assessment
f) Requirements for International Students
    - Transcript Evaluation through one of our partners
    - Non-native English speakers must submit English proficiency scores from one of our approved assessment exams.

Applicants to the Master's degree program must also submit:

i. Letter of Recommendation
ii. Goals and Outcomes Statement
iii. Video Presentation

Application Submission

The completed application for admission and supporting credentials should be submitted online at https://application.sans.edu/apply/.

Invitation to Matriculate

Once the Admissions Committee reviews and approves an application for admission, the Admissions Office will send an Offer of Admission. Enrollment in the SANS Technology Institute will be contingent upon successful completion of the virtual New Student Orientation within 30 days of admission and beginning the first course within 3 months of admission.

Conditional Admission

Students are conditionally admitted to SANS Technology Institute for various reasons. Our goal is to support the success of our students in the Master's program. Conditional admission stipulates that students complete ACS 3275 (SEC 275 + GFACT) as their first course and pass the associated exam (GFACT) with a score of 80 or higher. Upon successful completion of this requirement, students will proceed into the Master's program and receive a 100% discount on ISE 5701: Situational Response Practicum, a course of equal value to ACS 3275. Students who do not complete the GFACT exam with a score of 80 or higher will not receive full admission to the Master's program and will be referred to Admissions to explore other program options.

New Student Orientation

Our New Student Orientation (NSO) ensures that all new students are provided with the information necessary to navigate their college experience successfully. It is important that students refrain from registering for their first course before completing NSO to prevent delays and complications in registration processing. During NSO, a student will: complete an orientation module and follow-up survey, schedule an appointment with their student advisor, and register for their first course. Students wishing to attend an upcoming live event as part of their first course are encouraged to communicate that at the time of admission.

We recommend students set aside 30 minutes to complete the orientation module and survey and an additional 30 minutes for the academic advising appointment.

Registration

Students must register for courses using personalized instructions provided by their student advisor. These instructions are unique to each student and are not publicly available. Registrations paid for through SANS.org are not transferrable to SANS.edu. This policy is strictly enforced.

To meet course start deadlines, students must register (with tuition paid in full) at least 7 calendar days before their chosen start date. For students residing outside of the United States, it is

recommended to register at least 14 days in advance. These deadlines ensure adequate processing time for tuition payments and book shipments. Late registrations will not be accepted. Students who submit registrations within the 7-day window will have their start date deferred to the next available course start date. For registration questions and/or instructions, please contact your assigned student advisor.

Course Start Dates by Modality

Courses in the OnDemand or other distance-learning modalities start on the 1st and 15th of each month unless otherwise noted. The schedule of live courses offered in the In-Person or Live-Online modalities is available at www.sans.org/cyber-security-courses. The start date for live courses is the first day of the class at the scheduled SANS training event.

Add/Drop Policy

To support student success and ensure a smooth start to the course term, enrollments must be finalized at least one week before the first day of class.

- Add/Drop Deadline: Students must add or drop a course at least 7 calendar days prior to the start date listed in their SANS.edu course syllabus.
    - Students may drop a course only if they have not accessed the online course or received the shipment of course materials.
- After this deadline, changes to enrollment, including withdrawals, modality changes, schedule adjustments, or section transfers, are not be permitted.

Tuition refunds or credits will not be issued for courses dropped on or after the first day of the course. See the "Cancellation and Change Fees" section below for associated fees.

We encourage students to carefully review their course schedules, commitments, and materials before the deadline to ensure the best fit for their academic goals. For exceptional cases (e.g., medical or family emergencies), students may submit a formal appeal with supporting documentation to the Dean of Students Office at deanofstudents@sans.edu.

Tuition and Fees

Students pay tuition on a per course basis and are required to pay tuition at the time of registration for each course. Students are expected to pass each course before starting another. Therefore, students may only register and pay for one course at a time, except when approved to overlap terms with another class. See Maximum Enrolled Credit Limits in the Student Handbook.

In the Master's degree program, the cost of tuition is based off a per credit hour rate based on SANS Technology Institute's Credit Hour Policy, while in the Graduate Certificate programs, tuition is a flat rate per course. Tuition includes the cost of the course, textbooks, and certification tests that serve as mid-term or final exams for graduate courses. The cost of travel and lodging is in addition to the cost of tuition, for students who choose to attend in-person courses. Additional fees may also apply (e.g., application fees, exam retake fees). Total tuition will be reduced by the full amount associated with any SANS course or GIAC certification that the student has already completed, up to the total amount approved during the admissions process.

Discounts or promotions offered by SANS Institute, including the SANS Work Study Program, do not apply to graduate course tuition.

The following tables reflect the tuition rates by program.

Master's Degree

Program	Cost per Credit+	Total Credits
M.S. in Information Security Engineering	$1,500	36

Post-Baccalaureate Certificate Programs

Program	Cost per Credit	Cost of Capstone	Total Credits	Total Cost
Cybersecurity Engineering (Core)	$1,900	$1,900	13	$24,700
Penetration Testing & Ethical Hacking	$1,900	n/a	12	$22,800
Incident Response	$1,900	n/a	12	$22,800
Cyber Defense Operations	$1,900	n/a	12	$22,800
Industrial Control Systems Security	$1,900	n/a	12	$22,800
Purple Team Operations	$1,900	n/a	12	$22,800
Cybersecurity Leadership	$1,900*	n/a	16	$29,275
Cloud Security	$1,900	n/a	12	$22,800
Software Supply Chain Security	$1,900	n/a	12	$22,800

**Cybersecurity Leadership program includes ISE 5605 (1 credit) with a course tuition of $750.*

Single Courses, Non-Degree Seeking Students

Students enrolled in a single course as a non-degree seeking student pay a flat tuition rate per course of $6,500, with the exception of ACS 3275 ($1,500). For any student, there is a lifetime cap of two courses as a non-degree seeking student. If a non-degree seeking student does not pass a course on the first exam attempt, they are allowed to retake the exam one time. The cost of retake exam is an additional fee set by GIAC. If unsuccessful after two exam attempts, the student would not be allowed to pursue a second single course and be required to wait 1 year before applying to a SANS.edu program.

Fees

The following fees may apply:

Application Fee*	Varies by program
GIAC Exam Retake Fee	Set by GIAC

* Paid during the application process. Application fee amount is available on the Graduate Admission webpage: https://www.sans.edu/admissions/graduate/

Cost of Live Learning Events

Travel and Lodging

Students are responsible for the costs of hotel, food, and travel should they attend a live SANS event as part of their coursework. Any arrangements and associated lodging costs are to be paid directly to the hotel at which the learning event is being conducted.

Live Class Add-ons

Students attending live SANS events have the option to add supplemental items, such as a 2-day In-person Summit pass, to their registration. As these items are not program requirements, they are not included in graduate course tuition and will incur an additional cost to the student. If interested, students should ask their advisor how to add these items to their registration.

Student using GI Bill® benefits will find that these add-ons are not covered by VA Education Benefits.

Cancellation and Change Fees

SANS.edu students who wish to cancel and receive a refund for a course must submit a request by email to their student advisor. Requests must be received 45 days before the start of the course. Payments will be refunded by the method that they were submitted and a processing fee of $300 will be deducted. Requests received within 45 days of the start of the course may not receive a refund, but credit towards enrollment in a future course.

Students who seek to change the venue, timing, or modality for a course should submit a change request by email to their student advisor. Requests must be received 45 days before the start of the course. Processing fees may apply.

No cancellations or changes will be made once:

- Online course materials have been accessed
- Print course materials have been mailed to the student
- The student has arrived at a live event

Cancellation Fee	$300 processing fee
Course Change Fee	$150 processing fee

Students using VA Education Benefits may cancel a course up to 7 days prior to the start of a course without incurring any cancellation or change fees. For cancellations within 7 days of a course

starting, students will be responsible for paying cancellation or change fees. Refunds of military education benefits will be resolved via the VA's Debt Management Center. As part of any such refund, any overpayment received by the student (e.g., Chapter 30 tuition payments or Chapter 33 book or housing stipend) will be the responsibility of the affected student.

Financial Aid/Title IV Eligibility

The SANS Technology Institute is approved by the US Department of Education as an eligible Title IV institution. While we do not participate in Title IV funded student loan programs, eligibility status permits us to, from the date of eligibility forward, offer the following opportunities to our students:

- Provide a 1098-T to students who are funding part of their program cost in order for them to file for possible tax credit.
- Students may be eligible to utilize 529 educational funds where there is a state requirement for Title IV eligibility.
- Students may be eligible to utilize corporate or employer tuition reimbursement programs where Title IV eligibility is required.

SANS.edu Tuition Payment Program (TPP)

The SANS Technology Institute Tuition Payment Program (TPP) is a monthly payment program designed to allow graduate students without alternative funding options to make monthly installments towards courses taken as part of an academic program. The TPP is not a student loan and does not incur interest.

TPP Basics

Participant Eligibility

To be eligible for the SANS Technology Institute Tuition Payment Program (TPP), participants must meet these criteria:

- Be enrolled into a graduate-level academic program at SANS Technology Institute
- Be a U.S. citizen
- Meet financial eligibility requirements
- Agree to utilize a U.S. bank with automated, monthly EFT payment withdrawals
- Agree to respond to communications from the Bursar's Office by phone and email

Application

- Participants can apply before or during their academic program at SANS.edu through our application portal.
- Applicants are required to provide financial information including: monthly income, monthly expenses, proof of income, Experian credit report, and other financial documents requested by the TPP Committee.
- If accepted into the Tuition Payment Program, applicants will need to provide bank details to set up automated monthly EFT withdrawals.
- Applications that are not complete within 30 days will be automatically closed.

- Due to the sensitive nature of application materials, SANS Technology Institute will securely store and transmit applicant information. Once a participant's TPP account balance has been paid in full, application materials will be removed from our systems.

Monthly Payments

- On the 1st day of each month, all current TPP users, including recently admitted students, will be scheduled for a payment to be withdrawn on the 15th. Any requested changes to a TPP participant's bank account needs to be communicated to the Bursars Office prior to the 1st of the month.
- As is customary for intra-bank transfers, the transactions will be initiated a few days prior to the 15th of the month, so participants shall ensure adequate funds are available in their account by the 10th of the month to avoid insufficient funds.
- Monthly payment amounts will be directly withdrawn on the 15th of the month. If the 15th of the month falls on a weekend or bank holiday, the payment may be delayed a few days.
- Once the monthly payments have cleared, an email receipt will be sent to participants.
- Payments that are rejected due to insufficient funds are subject to the Late Payment policy below.
- Monthly payments will not be paused between courses, or while a student is on a Leave of Absence and a balance remains on their TPP Account.

TPP Policies

TPP Account Balance

- Approved applicants will be permitted to register for courses up to the maximum tuition amount needed to complete their academic program. This amount is subject to change based upon waived courses, tuition increases, or retaking failed courses. Retake exams are paid directly to GIAC and cannot be added to a TPP account balance.
- Approved TPP participants will be provided with a code to be used at the time of course registration. By using this code, the tuition associated with that course will be added to their TPP account balance. Participants shall not share their TPP code with any other students.
- Participants are financially responsible for paying the total tuition amount for all courses in which a participant has registered using their TPP code and started the course, regardless of their participation or course grade.
- Participants who wish to use alternative funds such as employer tuition assistance or VA Education Benefits to pay for a course may do so on a limited basis. However, multiple payment methods cannot be combined in a single course registration. By using an alternative funding method, the associated tuition will be removed from the TPP account balance.
- Monthly payments are applied towards a participant's TPP account balance, and not towards a specific course registration. As a result, students will not receive a "Paid" invoice for individual courses when utilizing the TPP; these invoices show as "Comped".
- A detailed TPP account ledger can be requested by emailing bursar@sans.edu.
- Participants can only have one active TPP account at a time. If a participant begins another program and would like to use TPP, there are two options:
    1. Make a one-time payment to pay the remaining balance in full, or
    2. Continue with the monthly auto-draft payments until the balance is fully paid.

    Once the balance is cleared, students can contact the Bursar's office to proceed with using TPP for a second program. If you choose to continue with the auto-draft

payments, you may still move forward with a new program, but will need to provide an alternative payment method, as TPP cannot be used until the balance from a prior program has been paid in full.

Late Payments

- Monthly payments that are rejected due to insufficient funds will be considered "Late" and incur a $25 fee. The SANS.edu Bursar will notify participants by email and provide instructions to call in a credit card payment. Participants are expected to submit their late payment and fee within 5 days of being notified.
- If late payments are not resolved within 10 days of the original payment date, the participant will be dismissed from the Tuition Payment Program and be subject to the policies for Closing a TPP Account below.
- If late payments are not resolved within 30 days of the original payment date, the participant may be dismissed from their academic program, with a hold on their official academic records.
- Participants are permitted a total of 2 late payments over the duration of their participation in the TPP. Upon a third late payment, participants will be dismissed from the TPP and be subject to the policies for Closing a TPP Account below.

Additional Payments

- Participants can submit additional lump sum payments to reduce monthly payments on the back end of the payment terms. Additional payments will not substitute for regular monthly payments.
- Additional payments can be submitted in two ways:
    - Calling in a credit card payment
    - Increasing the amount of the next month's payment
- Students wishing to submit an additional payment should email bursar@sans.edu for further instructions.

Closing a TPP Account

- Participants can withdraw from the TPP at any time without penalty.
- Participants who withdraw, or are dismissed, from the TPP are responsible for paying off their remaining TPP account balance before registering for any additional courses through SANS.edu. Participants are not responsible for the tuition of any course that was not registered for and started.
- Participants who withdraw, or are dismissed, from the TPP and have a credit on their TPP account will be issued a refund via check.
- Participants who are dismissed from their academic program will continue to make monthly payments until their TPP account balance is paid off.
- Participants who do not resolve late payments as directed may be dismissed from SANS Technology Institute with a hold on their academic records.
- Tuition balances not paid by the due date may be sent to collections and incur additional fees of up to 35% of the balance due. In addition, participants will be responsible for all fees and costs incurred by SANS in collecting the debt owed, including collection costs, attorneys' fees, and judicial expenses.
- If participants file for bankruptcy while participating in the TPP, they are still required to pay off any remaining TPP account balance.

- SANS Technology Institute reserves the right to dismiss TPP participants at any time if we have reason to believe a participant committed fraud in connection with the TPP application.

Miscellaneous

- SANS Technology Institute reserves the right to modify the policies and procedures associated with the Tuition Payment Program. The current TPP policies will be published in the Course Catalog and can be accessed on our website. By remaining in the Tuition Payment Program, participants are agreeing to abide by these policies.

Veterans Benefits

The SANS Technology Institute is authorized by the Department of Veterans Affairs to accept VA Education Benefits. Students using VA Education Benefits are responsible for any tuition not paid to SANS.edu directly by the VA by the end of their course term. Please refer to the Veterans Benefits section towards the end of this catalog for more detailed information.

Credit Transfers and Waivers

Credit Transfers

Graduate Programs Transfer Credit

The SANS Technology Institute does not accept any transfer credits from other colleges/universities in place of SANS.edu curriculum for our Graduate Certificate programs or Master's degree program.

Waivers of Course Requirements

"Waiver credit" refers to credit earned from previously completed SANS courses, GIAC exams, PMP or CISSP.

Waivers may be granted for up to, but not more than, one-quarter of the total number of credit hours required by a program (the "25% limit"), and are subject to the requirements as described below:

- All waivers are granted *only* prior to a student's matriculation.
- Students may *not* take courses outside SANS.edu for credit in their program after they matriculate.
- Course waivers receive no credit hours or grades awarded. Waivers are not figured into the calculation of a student's cumulative grade point average (GPA).
- All certifications must be active and current to eligible for credit. See the GIAC renewal policies.
- Waiver exceptions for government and military employees: Learn about exceptions to the waiver limit, which only applies to the Master's degree, in the website section on Participants in Government or Military Education and Training Programs - https://www.sans.edu/admissions/transfer-of-credit/?msc=main-nav

GIAC Exam Challenges

Graduate students may elect to place out of a course by challenging the associated final GIAC exam without first taking the associated SANS class. In this case, the student will register and pay tuition for the exam attempt but will not receive course materials.

Master's degree students are limited to two GIAC exam challenges, while Graduate Certificate students are limited to a single GIAC exam challenge. Waivers granted for GIAC exam challenges will count against the waiver limit of one-quarter of the program's credit hours.

GIAC Gold Papers

The SANS Technology Institute will grant a waiver to a student from the requirements within a research practicum course (ISE 5501 or ISE 5901), in the event a student has successfully completed a GIAC Gold Paper within 5 years of being admitted to the program. This waiver is subject to the Gold Paper being reviewed within the Technical Research and Communication requirements.

CISSP Certification

Students who hold a current CISSP from the ISC² organization may choose to receive a waiver for ISE 5101 or ISE 5001 for the SANS class (SEC401 and LDR512, respectively). Achievement of the associated GIAC certification (GSEC or GSLC) will still be required for the award of credit. Students interested in pursuing this waiver will need to confirm their intention with their student advisor during New Student Orientation and pay tuition for the GIAC exam. Note that students who elect to take the GIAC exam only will *not* receive course materials for the SANS SEC401 or LDR512 class.

Technology and Software Requirements

To fulfill the requirements of the SANS Technology Institute curriculum, you are expected to have, or have access to:

- A personal computer capable of connecting to the internet,
- An email account,
- A word-processor software program such as *Microsoft* Word, *iWork* Pages, or *Open Office* Writer,
- A web-browser (Internet Explorer, Firefox, Chrome, etc.), and
- A webcam is required to take GIAC exam remotely through ProctorU.

In addition, most of your classes will require special software to be loaded on your computer. Approximately a week before class, you will receive notice of that class's software requirements. This will tell you where to get any software needed for the class and labs, as well as any configuration settings that need to be applied.

Suggested Laptop Requirements

A properly configured system is required to fully participate in your courses at SANS Technology Institute (SANS.edu). Although SANS.edu does not have standardized laptop requirements applicable to all courses, below is a suggestion of requirements based on one of our more requirement-demanding courses. ***Please note that these requirements are subject to change.*** You may want to browse the laptop requirements for some of the classes you intend to take. Make sure your computer can run VMWare. As a test, download the free VMWare Player (or a trial version of VMWare Workstation) and install a Windows 10 and an Ubuntu virtual machine. Make sure they both run sufficiently well and can communicate with each other.

A modern, well configured, laptop is critical for your success in any SANS class. Exercises make up a crucial part of your learning experience. You need full administrative access to your laptop and you need to be able to configure all system settings, including BIOS. It may be necessary to disable some security features like VPNs or anti-malware products.

Laptop Requirements

- CPU: a recent 64-bit Intel/AMD (x86-64 Bit) processor. For example, Intel i5/i7 4th generation or later.
- **CRITICAL NOTE: Apple systems using the M1/M2 processor line cannot perform the necessary virtualization functionality and, therefore, cannot in any way be used for most classes. The same is true for other ARM architecture-based systems.**
- It is critical that your CPU and operating system support 64-bit so that our 64-bit guest virtual machine will run on your laptop. VMware provides a free tool for Windows that will detect whether or not your host supports 64-bit guest virtual machines. For further troubleshooting, this article also provides good instructions for Windows users to determine more about the CPU and OS capabilities. For Macs, please use this support page from Apple to determine 64-bit capability.
- BIOS settings must be set to enable virtualization technology, such as "Intel-VT". **Be absolutely certain you can access your BIOS if it is password protected**, in case changes are necessary. Test it!

- A minimum of 16GBytes of RAM is required. Many classes recommend 32GBytes.
- USB 3.0 Type-A port is required. At least one open and working USB 3.0 Type-A port is required. (A Type-C to Type-A adapter may be necessary for newer laptops.) (Note: Some endpoint protection software prevents the use of USB devices - test your system with a USB drive before class to ensure you can load the course data.)
- 1TB of SSD hard drive space. Classes may require up to 350 Gigabytes of Free Space.
- Local Administrator Access is required. This is absolutely required. Don't let your IT team tell you otherwise. If your company will not permit this access for the duration of the course, then you should make arrangements to bring a different laptop.
- **Wireless 802.11 Capability is required.**

Operating System

- Host Operating System: Latest version of Windows 10 or macOS 10.15.x
- Please note: It is necessary to fully update your host operating system prior to the class to ensure you have the right drivers and patches installed to utilize the latest USB 3.0 devices.

Veterans Benefits

Introduction

This section provides explanations for how veterans benefits will work relative to the programs at the SANS Technology Institute (SANS.edu). In addition to the information provided here, we recommend that students review the Student Handbook, which contains additional academic and student conduct policies.

Background Information

Our programs are delivered in non-standard academic terms and are designed to maximize the flexibility by which a student can engage in the required coursework. Rather than taking courses on-campus during fixed semesters, our programs are delivered through a series of courses taken via a mix of modalities (primarily at a student's option), with asynchronous start dates. All students enrolled in a degree program will need to satisfy the same requirements, but the timing of individual student progression may differ according to individual schedules and the availability of courses.

PROGRAM CHARACTERISTIC	STANDARD COLLEGE	SANS TECHNOLOGY INSTITUTE
ENROLLMENT PERIOD	Typical semesters	Asynchronous start dates
STANDARD TERMS	15-19 weeks	Varying course-term lengths depending upon course
COURSE MODALITY	Either on-campus, in-person classroom instruction or 100% online	Mix of in-person and at-a-distance modalities, at the student's option

The flexible structure of our programs – course start dates, the mix of in-classroom and at-a-distance options, the varying terms for courses, their associated credit hours, and calculated pace of progress – impacts how payment benefits are calculated by the VA. As a result, there may be significant fluctuations in the payments students receive throughout the course of their program. This is not to suggest that total available benefits are enhanced or diminished, but simply that our structure may cause a variability in payments at different times as students enroll in courses, experience gaps between courses, and engage in different instructional modalities. The resulting payments will be different and less consistent than they would be if students were to attend a traditional, brick-and-mortar college with fixed semester terms and standard credit hour assignments per course.

Additionally, an individual taking a single course as a non-degree seeking student may *not* use their VA educational benefits to fund that course. GI Bill® benefits will only cover courses that are taken as part of a degree-granting program.

Because the rules and processes associated with VA educational benefits are complex, a full description is beyond the scope of this guide. However, we will generally distinguish between Post-9/11 GI Bill® and other sections in this guide, and will seek to point out where and how payment amounts that students receive are determined by the courses they might be taking at the time.

Approved Live Learning Events for 2025

At this time, the SANS Technology Institute is approved and eligible to receive veterans benefits only in the State of Maryland. Because of this, Student Veterans may apply their benefits only to courses where the instruction element is delivered live at an approved location in Maryland, or delivered at-a-distance. Resident course offerings in Maryland vary each year. Here are the approved training sites for 2025:

Baltimore:

Hyatt Regency Baltimore
300 Light Street
Baltimore, MD 21201

Hilton Baltimore Inner Harbor
401 W Pratt Street
Baltimore, MD 21201

Kimpton Hotel Monaco Baltimore Inner Harbor
2 North Charles St
Baltimore, MD 21201

The Royal Sonesta Harbor Court Baltimore
550 Light Street
Baltimore, MD 21202

Columbia:

Sheraton Columbia Town Center
10207 Wincopin Circle
Columbia, MD 21044 US

Rockville:

Hilton Washington DC/Rockville
1750 Rockville Pike
Rockville, MD 20852

Bethesda:

Hyatt Regency Bethesda
One Bethesda Metro Center
7400 Wisconsin Ave
Bethesda, MD 20814

Chapter 33 Post-9/11 GI Bill®

For Chapter 33 benefits, tuition and fees are sent directly to the school to pay for courses that have been certified. It also provides a monthly housing allowance and book stipend which are described below. Students with questions regarding specific amounts for housing allowances are encouraged to reach out to the VA directly at the GI Bill® help line (888-442-4551) or online at https://gibill.custhelp.va.gov/

Costs Covered

- The VA pays the school tuition and fees directly, based on the student's eligibility percentage.
    - Example, Student A has 100% eligibility for Chapter 33 benefits, and Student B has 80% eligibility.
    - Student A would have 100% of tuition and fees covered, whereas Student B would have 80% of tuition and fees covered.
- Students needing to purchase exam retakes from GIAC **may** have the cost of the exam reimbursed by the VA.

Rate of Pursuit

As detailed earlier in the catalog, each course is itself the enrollment term as far as how we certify enrollment to the VA. This means that when we certify enrollment terms to the VA, those terms are simply each course. Additionally, we certify terms (courses) to the VA one week before the course begins, which is the deadline for any schedule changes.

- Graduate students using GI Bill® will be considered full-time in each term (course) if they pursue courses that have a 1 credit per 1 month ratio. For example, a 3-credit course taken over the 3-month period is considered full-time (3/3), while a 3-credit course taken over 4-months is less than full-time (3/4).
    - *Monthly Housing Allowance (MHA) payment for courses taken at less than full-time will be determined by the VA.*
    - Students are encouraged to work with their assigned student advisors and refer to the information in the Sentinels' Resource Center in Canvas to review courses that are less than full-time rate of pursuit.
- The VA will calculate a prorated MHA amount based upon a student's benefit level, the rate of pursuit, and the number of days in a month the student was enrolled in a course.
- Students may complete coursework earlier than the targeted timeframe and we will adjust the certification to reflect the actual time taken to complete the course. These adjustments may impact MHA payments, as it relates to enrollment periods changing.

Housing Allowance

The VA will calculate a prorated Monthly Housing Allowance amount based upon a student's benefit level, the rate of pursuit, and the number of days in a month the student was enrolled in a course.

The MHA is paid directly to the student on the 1st of the month, based upon enrollment time in the previous month. MHA will be paid for periods when:

a. The student is enrolled in at least one course,
b. The student is earning credits at a rate of pursuit greater than half-time (as described in the previous section), and
c. The student is not on active duty.

The calculation of MHA is impacted by the following considerations:

- Students who take a course in-person (in Maryland) will be paid per the calculation determined by the BAH for an "E-5 with Dependents" using the ZIP code of *the live event attended*.
- Students who take a distance education course will be paid a housing stipend at the online rate, set as roughly one-half the national average.
- More information about the MHA can be found at https://www.benefits.va.gov/GIBILL/resources/benefits_resources/rates/ch33/ch33rates080118.asp#HOUSING

Please note that students should not expect MHA for exam retake attempts.

Books and Fees Stipend

The book stipend is a lump sum paid directly to the student for each enrollment certification processed, up to an annual cap. A yearly books and supplies stipend of up to $1,000.00 paid proportionately based on enrollment. The annual cap re-sets the 1st of August each year.

Vocational Rehabilitation & Employment

Costs Covered

Similar to the Post 9/11 GI Bill®, Vocational Rehabilitation and Employment (VR&E) benefits pay the school directly for 100% of tuition and fees. It also provides monthly housing allowance based on the student's rate of pursuit.

Students will work closely with their assigned student advisors, as well as their Ch 31 counselors, as they progress through their program and maintain Ch 31 approvals.

Students needing to purchase exam retakes through GIAC should work with their assigned student advisor to ensure VA counselor approval. Please note that students should not expect subsistence allowance for exam retake attempts.

Other GI Bill® Chapters, including Chapter 30 Montgomery Bill

Costs covered

Veterans using other GI Bill® Chapters (30, 35, 1606) receive monthly stipend payments directly from the VA, based on their enrollment term training time (full-time, ¾ time, etc.), and then they are responsible for paying tuition and fees to the College.

Eligible students who are certified for these VA benefits do not have to remit the full tuition payment at the time of registration. However, students using benefits under these chapters will be required to pay their tuition to SANS Technology Institute by the end of their course terms.

The VA determines the amount the VA will pay students for their enrollment term, based upon calculating a veteran's training time, and **students should be advised that after their VA payments, they may still owe tuition**, the amount of which depends on their enrollment terms.

Please note:

- At the Graduate level, the College determines full-time training time, which is any course with the 1 credit: 1 month ratio.
- Students are encouraged to work with their assigned student advisors and refer to the information in Canvas to review courses that are less than full-time training time.
- Students may complete coursework earlier than the targeted timeframe, and we will adjust the certification as the course term to reflect actual time taken to complete the course.
    - **These adjustments will impact VA payments, as it relates to a reduction in enrollment term length, which will result in owing tuition out of pocket**.
- Students are encouraged to review payment rates based on training time here.

- Students using these benefits chapters are strongly encouraged to work with the College's Veterans Office (veterans@sans.edu) prior to enrolling to determine out of pocket tuition costs.

Yellow Ribbon Program

Because our typical costs do not exceed the established thresholds under the Post-9/11 GI Bill®, the SANS Technology Institute does not participate in the Yellow Ribbon Program.

Registering and Paying for Courses

Once students have completed orientation and their initial advising appointment, they are able to register for their first course and request to be certified with the VA. Here is an outline of the process:

1) After the initial advising meeting, a student advisor will email registration instructions which will prompt the students to indicate "using GI Bill®" as payment method. This provides SANS.edu with consent to be "certified" with the VA for the course.
2) The College will certify enrollment to the VA, regardless of benefits chapter, to trigger the tuition payment process.
3) Students using Chapter 33 at less than 100% eligibility, or students using other Chapters, have up until the end of the course to pay tuition. Failure to have tuition paid by the end of the course term may result in academic dismissal.

Tuition & Fees

Students are responsible for any costs not covered by the VA. Situations in which a student using GI Bill® benefits can expect to owe out-of-pocket tuition include, but are not limited to:

- Student is less than 100% eligible for benefits
- Student's certifications exceed the annual private school tuition cap
- Student withdraws from a course that was certified to the VA
- Students using Chapter 1606 benefits
- Student stops meeting attendance requirements in a course that was certified to the VA
- Student's benefit expires during enrollment term (the "delimiting date" on the Certificate of Eligibility)

Tuition balances not paid by the due date may be sent to collections and incur additional fees up to 35% of the balance due.

Please note:

- Students using GI Bill® benefits will not be penalized while the College awaits payment from the Department of Veteran Affairs.
- Students do not need to use VA benefits for every course throughout the program but can instead elect to use it for only certain courses. Therefore, students need to indicate on each course registration form (as indicated in Step 1 above) if they would like to utilize their benefits.

- Many schools offer a Priority Enrollment status for students using GI Bill®. Because all students have equal registration access, SANS.edu does not have a Priority Enrollment policy in place for students using GI Bill®.

VA Requirements of Students using VA Education Benefits

- Students who seek to use GI Bill® or VR&E must first apply for benefits online and submit official documentation to SANS Technology Institute (i.e. Certificate of Eligibility or VR&E Authorization Form) at the time of admission.
- The VA will only pay for courses listed in the catalog that are required for a degree and for programs that have been approved for study by the VA.
- If students take courses in addition to those listed for their approved program, they will not be entitled to receive VA benefits for them.
- Students who do not complete a course that has been certified by the VA will generate a tuition debt with the College as well as to the VA for any associated MHA.
- Students who fail their exam attempt need not worry about generating any VA debt due to their exam failure.
- Verify enrollment
    - Students using Ch 30 benefits must verify their enrollment to receive payments from the VA; review guidance here.
    - Students using Ch 33 benefits must verify their enrollment to receive MHA payments from the VA; review guidance here.
- Report address changes
    - Students using VR&E who move may be reassigned to a new VR&E counselor. Students must inform this change to veterans@sans.edu.
    - Students using other GI Bill® chapters must keep their mailing address updated to ensure timely delivery of benefits related information.

Course Attendance Requirements

- Students using GI Bill® must adhere to the course benchmarks outlined in the syllabus to demonstrate course attendance for GI Bill®, regardless of the modality in which the course is taken.
- If a student using GI Bill® stops attending and does not complete a course, we are required to inform the VA of their last date of participation. The VA defines this situation as having unofficially withdrawn from the course and schools must report enrollment changes.
- This enrollment change will result in the student ultimately bearing responsibility for any tuition and MHA issued. The VA will seek a tuition from the school, and the student will then owe the school that tuition debt, due within 60 days of debt notification.
- If a student using GI Bill® requests and is awarded an incomplete grade, their VA certification for the course term will not be amended and therefore, no additional benefits will be received. Students who owe a tuition balance are not eligible for an incomplete grade.
- Students are expected to maintain satisfactory academic progress as outlined in the *Student Handbook*.

VA Requirements of SANS Technology Institute

Monitor Course and Program Progress

SANS.edu will monitor students' course attendance to ensure that they are progressing appropriately. We track course attendance by checking how successfully students have met course milestone due dates. Additionally, students are required to follow the Satisfactory Academic Progress policy as mandated by SANS.edu to remain in good standing with the institution.

Certify Enrollments (VA Form 22-1999)

We will submit VA form 22-1999 (Enrollment Certification) ~7 days prior to the first day of class, regardless of modality.

Please note refunds are not given after classes begin for in-person/Live Online courses, nor after 7 days prior to the start of OnDemand courses.

Report Enrollment Information

SANS.edu is required to report any changes in student enrollment status to the VA. Enrollment changes could include withdrawals (official or unofficial), change course date, change delivery modality, etc. These changes could affect a student's rate of pursuit which could impact their stipend and/or benefits payments. We also report academic progress (including dismissal) and certify graduation/program completion.

Review of School Records by VA and Maryland State Approving Agent

By law, SANS.edu is required to maintain and make available student records (such as enrollment periods, grade information, student application, etc.) to authorized representatives of the government. We will retain a student's records for a minimum of 3 years following the termination of their enrollment.

What students can expect from the VA

Benefit Letters

The VA will mail an award (benefit) letter to the student showing we certified them and indicating the amounts they will receive during the course enrollment period/term. Students are advised to stay informed as to their remaining benefits, as they are responsible for any tuition the VA does not pay.

Payments

- Chapter 30 and Chapter 35: The VA will deposit money directly into the bank account students have provided to them.
- Chapter 33, Chapter 31: The VA will send funds for tuition and fees directly to SANS Technology Institute and deposit funds for the book stipend and MHA to the student.

VA Resources and Contact Information

While we will make every effort to help students navigate their benefits, it is ultimately the student's responsibility to understand their benefits. We cannot advise students on eligibility of benefits, as we do not represent the Department of Veterans Affairs. The following resources are available to help students find the information they need:

- GI Bill® Official Web Site: http://www.benefits.va.gov/gibill/
- Online benefits application portal: https://www.vets.gov/
- GI Bill® Education Forms hard copies: http://www.benefits.va.gov/gibill/handouts_forms.asp
- GI Bill® FAQ: https://gibill.custhelp.com/app/answers/list
- Payment Rates and Comparison Tool: http://www.benefits.va.gov/gibill/comparison_tool.asp
- Post-9/11 GI Bill® Summary: http://www.benefits.va.gov/gibill/post911_gibill.asp
- Harry W. Colmery Veterans Educational Assistance Act (Forever GI Bill®): https://www.benefits.va.gov/GIBILL/FGIBSummaries.asp
- Education Benefits Phone Number: 1-888-GIBILL-1 (1-888-442-4551)

GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA). More information about education benefits offered by VA is available at the official U.S. government Web site at www.benefits.va.gov/gibill.

California State Tuition Recovery Fund Disclosures

As a registered out-of-state accredited institution, and as required by California state law, the SANS Technology Institute is providing residents of California, with the following disclosures:

The State of California established the Student Tuition Recovery Fund (STRF) to relieve or mitigate economic loss suffered by a student in an educational program at a qualifying institution, who is or was a California resident while enrolled, or was enrolled in a residency program, if the student enrolled in the institution, prepaid tuition, and suffered an economic loss. Unless relieved of the obligation to do so, you must pay the state-imposed assessment for the STRF, or it must be paid on your behalf, if you are a student in an educational program, who is a California resident, or are enrolled in a residency program, and prepay all or part of your tuition.

You are not eligible for protection from the STRF and you are not required to pay the STRF assessment, if you are not a California resident, or are not enrolled in a residency program.

It is important that you keep copies of your enrollment agreement, financial aid documents, receipts, or any other information that documents the amount paid to the school. Questions regarding the STRF may be directed to the Bureau for Private Postsecondary Education, 1747 North Market Blvd., Suite 225, Sacramento, California, 95834, (916) 574-8900 or (888) 370-7589. To be eligible for STRF, you must be a California resident or are enrolled in a residency program, prepaid tuition, paid or deemed to have paid the STRF assessment, and suffered an economic loss as a result of any of the following: 1. The institution, a location of the institution, or an educational program offered by the institution was closed or discontinued, and you did not choose to participate in a teach-out plan approved by the Bureau or did not complete a chosen teach-out plan approved by the Bureau. 2. You were enrolled at an institution or a location of the institution within the 120 day period before the closure of the institution or location of the institution, or were enrolled in an educational program within the 120 day period before the program was discontinued. 3. You were enrolled at an institution or a location of the institution more than 120 days before the closure of the institution or location of the institution, in an educational program offered by the institution as to which the Bureau determined there was a significant decline in the quality or value of the program more than 120 days before closure. 4. The institution has been ordered to pay a refund by the Bureau but has failed to do so. 5. The institution has failed to pay or reimburse loan proceeds under a federal student loan program as required by law, or has failed to pay or reimburse proceeds received by the institution in excess of tuition and other costs. 6. You have been awarded restitution, a refund, or other monetary award by an arbitrator or court, based on a violation of this chapter by an institution or representative of an institution, but have been unable to collect the award from the institution. 7. You sought legal counsel that resulted in the cancellation of one or more of your student loans and have an invoice for services rendered and evidence of the cancellation of the student loan or loans. To qualify for STRF reimbursement, the application must be received within four (4) years from the date of the action or event that made the student eligible for recovery from STRF. A student whose loan is revived by a loan holder or debt collector after a period of noncollection may, at any time, file a written application for recovery from STRF for the debt that would have otherwise been eligible for recovery. If it has been more than four (4) years since the action or event that made the student eligible, the student must have filed a written application for recovery within the original four (4) year period, unless the period has been extended by another act of law. However, no claim can be paid to any student without a social security number or a taxpayer identification number.

Maryland Guaranty Student Tuition Fund

A student may be entitled to make a claim against the Maryland Guaranty Student Tuition Fund for For-profit Institutions of Higher Education ("Student Tuition Fund") in the case of certain events, including a school closure. The Student Tuition Fund is administered by the Maryland Higher Education Commission. Information about the Student Tuition Fund and instructions for filing a claim may found in Regulations 13B.02.06.01 through .13 of the Code of Maryland Regulations or by contacting the Maryland Higher Education Commission.

Course Catalog Archive

The current version of this Course Catalog can be accessed via the SANS Technology Institute's Student Consumer Information web page:

https://www.sans.edu/about/student-consumer-information/

Archived versions of SANS Technology Institute's Course Catalogs and other academic documents can be accessed using the following website:

https://web.archive.org/

To access a previous version of this document, enter the URL of the current version of the document shown on the Student Consumer Information page into the search bar. From there, you can search by date to find the document version that you require.