SANS Technology Institute

Course Catalog

Version: 2018.2

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

Table of Contents

Academic Calendar

STI operates a continuous enrollment course schedule. Class instruction may be taken in a live classroom or via one of several distributed learning environments, as available. Given our open enrollment model we operate one academic term per year that begins on January 1 and ends on December 31. Applications are accepted throughout the year.

The Institute's offices are closed on: New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving and the Friday after Thanksgiving, and Christmas.

Graduation is held each year in conjunction with the SANS learning events.

2018 Learning Event Schedule

Event	Location	Start Date
1st Quarter		
SANS Security East 2018	New Orleans, LA	January 8, 2018
2nd Quarter		
SANS 2018	Orlando, FL	April 3, 2018
SANS Baltimore Spring	Baltimore, MD	April 21, 2018
SANS Security West 2018	San Diego, CA	May 11, 2018
3rd Quarter		
SANSFIRE	Washington, DC	July 14, 2018
SANS Baltimore Fall	Baltimore, MD	September 10, 2018
SANS Network Security 2018	Las Vegas, NV	September 23, 2018
4th Quarter		
Pen Test HackFest Summit	Bethesda, MD	November 12, 2018
SANS Cyber Defense Initiative 2018	Washington, DC	December 13, 2018

Students can find a full schedule of upcoming training events in-person and online at https://www.sans.org/security-training/by-location/north-america and https://www.sans.org/find-training/online.

Tuition and Fees

Master's Programs

Students enrolled in one of our master's programs pay tuition on a per credit basis. Students are only responsible for paying tuition on course(s) they are currently enrolled in. The below table reflects current tuition rates.

Program	Cost per Credit	No. of Credits	Capstone Fee	Total
MSISE	$1,250	36	$2,758	$47,758
MSISM	$1,250	35	$2,100	$47,100

Post-Baccalaureate Certificate Programs

Students enrolled in one of our post-baccalaureate certificate programs pay a flat tuition rate per course. Students are only responsible for paying tuition on the course(s) they are currently enrolled in. The below table reflects current tuition rates.

Program	Cost per Course	No. of Credits	Total
Cybersecurity Engineering Core	$5,000	12	$15,000
Penetration Testing & Ethical Hacking	$5,000	13	$20,000
Incident Response	$5,000	13	$20,000
Cyber Defense Operations	$5,000	12	$20,000

Cost of In-Person Requirements

Students are responsible for the costs of hotel, food, and travel to attend any of the residential institutes. The average hotel and food cost, if the hotel rooms are not shared, is $1,800 per residential institute ($200 per night for accommodations and $100 per day for food), though significant savings are available through room sharing. These amounts are to be paid directly to the hotel at which the residential institute is being conducted.

Fees

Application Fee*	$35 | $100
Late Course Change Fee	$150
GIAC Exam Retake Fee	$729

* Paid during the application process, Certificate application fee is $35. MS candidate application fee is $100.

Financial Aid / Scholarships

At the present time, SANS Technology Institute does not administer scholarships. STI is Title IV eligible, but does not participate in federal financial aid programs. STI recommends students check with their employers regarding tuition reimbursement or assistance programs for which they may be eligible.

STI is authorized by the Veterans Administration to accept VA Education Benefits.

Paying Tuition and Registering for Courses

STI students will utilize STI's course registration page provided in new student orientation materials to register for

each course. STI students are required to pay STI's established tuition at the time of registration for each course. Discounts or promotions offered by SANS Institute (an affiliate of STI) for individual course elements will not apply.

Refund and Change Fees

STI students who wish to cancel and receive a refund for a particular graduate course must submit a request by email to registrar@sans.edu. Requests must be received 45 days before the start of the course. Payments will be refunded by the method that they were submitted. Processing fees may apply.

Students who seek to change the venue, timing, or modality for a graduate course should submit a change request to registrar@sans.edu. Requests must be received 45 days before the start of the course. Processing fees may apply. No transfers will be given once online course materials have been accessed, or additional course materials have been mailed to the student.

Cancellation Fee*	$300 processing fee + shipping charges
Course Change Fee*	$150 processing fee + shipping charges

*Fees may apply per SANS policy for each modality

Cancellation of any approved registration for the GSE lab within 45 days prior to the start of the lab will be subject to forfeiture of the full lab fee.

STI participates in programs that allow US armed forces service members and veterans to utilize VA military education benefits. Students in this program may receive a refund for a course up to and including the day before the start of the course without incurring any 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.

Programs of Study

STI offers the following programs of study:

- Master of Science in Information Security Engineering
- Master of Science in Information Security Management
- Post-baccalaureate certificate: Cybersecurity Engineering Core
- Post-baccalaureate certificate: Penetration Testing & Ethical Hacking
- Post-baccalaureate certificate: Incident Response
- Post-baccalaureate certificate: Cyber Defense Operations

Master of Science Degrees

Application Requirements and Process

All applicants must meet the following criteria:

- Have at least 12 months of professional work experience in information technology, security or audit.
- Be employed or have current access to an organizational environment that allows students to apply the concepts and hands-on technical skills learned during the master's degree 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) Letter of Recommendation
e) Essays and Writing Samples
    a. Goals and Outcomes Statement
    b. Leadership Essay
f) Video Presentation
g) Application Fee
h) Requirements for International Students
    a. Transcript Evaluation through World Evaluation Services (WES)
    b. Non-native English speakers must submit TOEFL Scores.

Application Submission

The completed Application for Admission and supporting credentials should be submitted online at apply.sans.edu.

Invitation to Matriculate

Once the Admissions Committee reviews and approves your application for admission, the Admissions Office will send you an Offer of Admission. Enrollment in the SANS Technology Institute will be contingent upon successful completion of the virtual New Student Orientation within 60 days of admission.

New Student Orientation

STI's New Student Orientation ensures that all new students are provided with the information necessary to navigate their STI 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. Our NSO is comprised of: an orientation module, a follow up survey, scheduling an appointment with your student advisor, and concludes with registering for your first course. Students wishing to attend an upcoming live event 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. For details on the start dates and preferred deadlines, please visit https://www.sans.edu/admissions/orientation.

Transfer Credit Policy

The SANS Technology Institute does not generally accept transfers of credit for coursework completed at other regionally accredited higher education institutions. Any decision to make an exception to this policy in a given individual instance would need to be approved by the Assistant Director in conjunction with the Admissions Committee OR Executive Program Director.

The SANS Technology Institute may grant credit to students accepted to its master's programs who are, or had been, participants in government or military educational and training programs that are taught by SANS Technology Institute faculty and based on the same course instruction and exam requirements that are included in the master's program. In cases where this prior work represents only part of the credits and requirements of a course, the incoming student will need to complete the remaining course requirements in order to receive full credit and a course grade.

The SANS Technology Institute does in certain circumstances waive requirements for course elements or courses within its program of studies as a reflection of a student's previous attainment of substantially similar intended learning outcomes. Waivers may be granted for up to, but not more than, one-quarter of the total number of credit hours or credit-hour equivalents required by the program, and are subject to various limits, requirements, and fees as described below (the "25% Limit").

Waivers will not be granted when the requirements of the waiver are met after a student matriculates, regardless of any alternative arrangements or costs available to take such course elements outside of the credit hour program and fee structure. In the event a waiver is granted for an entire course, no credit hours or grade will be awarded, nor will the course figure into the calculation of a student's cumulative grade point average. In the event a waiver is granted for part of a course's components, the grade(s) received on the remaining components completed by the matriculated student will be used to determine the course grade, and full-course credit hours will be awarded.

Waiver policy can also be reviewed online: https://www.sans.edu/admissions/transfer-of-credit

Waivers of Course Requirements

Applicants seeking waivers for graduate course requirements should indicate so on the Applicant Information Form during the application process.

SANS Institute Classes within SANS Technology Institute Courses

The SANS Technology Institute will grant a waiver to a student from the requirement within a SANS Technology Institute course to complete a specific SANS Institute class when the student has completed that class within the two years prior to matriculation. This is subject to the requirement that the student completes any remaining SANS Technology Institute course requirements associated with that course after matriculation, but prior to taking additional courses.

GIAC Certifications

The SANS Technology Institute will grant a waiver to a student from the requirements within a course to complete both a relevant SANS Institute class and GIAC exam if the student has taken and passed the relevant GIAC exam within the past three years. Waivers for GIAC certifications achieved without having taken the relevant SANS Institute class ("GIAC Challenges") will be subject to, and contribute to, the existing limit of two GIAC Challenges allowed.

GIAC Gold Papers

The SANS Technology Institute will grant a waiver to a student from the requirements within a research practicum course, in the event a student has successfully completed a GIAC Gold Paper within 5 years. This waiver is subject to

the Gold paper being reviewed within the Research Practicum requirements. If approved, a waiver would be granted for all course components of either RES 5500 or RES 5900.

PMP Certification

For students who hold a current PMP from the Project Management Institute, a waiver will be granted for the requirement to take ISE/ISM 5800 in its entirety (waiving both the component SANS MGT 525 course and the GIAC GCPM requirement).

CISSP Certification

For students who hold a current CISSP from the ISC2 organization, a waiver will be granted within ISE/ISM 5101 for the SANS Institute class SEC 401 or MGT 512, respectively. Achievement of the associated GIAC GSEC or GSLC certifications, respectively, will still be required for the award of credit.

CISA Certification

For students who hold a current CISA from the ISACA, a waiver will be granted for the SANS AUD 507 and GIAC GSNA exam course components of ISM 6201. Students who have received a waiver but still must complete either or both an associated GIAC exam, will be charged for the additional experience in accordance with the tuition and fees in place at the time the student seeks to engage in these activities for credit.

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.

MSISE Program Learning Outcomes

By the end of this program, graduates will be able to:

- Formulate and implement policies and solutions that demonstrate a thorough understanding of security foundations and practical applications of information technology.
- Demonstrate a solid foundation in information security strategies and apply their knowledge by assessing an information security situation and prescribing an appropriate security approach.
- Construct an information security approach that balances organizational needs with those of confidentiality, integrity and availability. Solutions require a comprehensive approach that aligns with policy, technology, and organizational education, training and awareness programs.
- Effectively communicate information security assessments, plans and actions for technical and nontechnical audiences/stakeholders.
- Identify emerging information security issues, utilize knowledge of information security theory to investigate causes and solutions, and delineate strategies guided by evolving information security research and theory.
- Analyze and design technical information security controls and safeguards, including system specific policies,

network, and platform security countermeasures and access controls.
- Conduct threat assessments (offensive measures), appraise/prioritize vulnerabilities (defensive perspectives), and appraise technical risks for enterprise information assets/needs/requirements.
- Apply a standards-based approach to minimize risk through the implementation of the principles and applications of information security.
- Evaluate the appropriate security solutions required to design/build a security architecture - this includes the integration of intrusion detection, defensive infrastructures, penetration testing, and vulnerability analysis.
- Formulate plans for adaptive detection of threats, including leading/oversight of intrusion/malware detection, incident response, forensics, reverse engineering, and e-discovery initiatives and actions.

MSISE Graduation Requirements

The MSISE program requires completion of 36 credit hours with a 3.0 G.P.A, within 5 years. Students must complete the following requirements:

Required Course		Credits
ISE 5101	Security Essentials	3
ISE 5201	Hacking Techniques & Incident Response	3
ISE 5401	Advanced Network Intrusion Detection & Analysis	3
RES 5500	Graduate Research Practicum	2
ISE 5300	Building Security Awareness	1
ISE 5550	Research Presentation I	1
ISE 5700	Situational Response Practicum	1
ISE 5800	IT Security Project Management	3
ISE 6300	NetWars Continuous Practicum	1
ISE 5600	IT Security Leadership Competencies	1
ISE 6001	Standards-based Implementation of Security	3
RES 5900	Advanced Graduate Research Practicum	2
ISE 6100	Security Project Practicum	1
ISE 5900	Research Presentation II	1
ISE 6999	Elective Courses*	9
N/A	MSISE Capstone	1
Total		36

- Please see list of acceptable technical elective courses in the course listings section

Master of Science in Information Security Management

The Master of Science in Information Security Management (MSISM) Program is designed to accelerate the development of information security managers by providing practical experience that can be applied immediately on the job. Students learn from the industry experts how to see the world from an attacker's view, audit information systems, assess legal implications of an incident, and develop risk-based secure enterprise-level solutions that enable an organization's business processes to function in spite of the increasing threat presence. In addition to developing hands-on technical skills, the program emphasizes the development of communication and leadership skills that will improve the student's ability to implement information security solutions within their organization.

MSISM Program Learning Outcomes

By the end of this program, you will be able to:

- Formulate and implement policies and solutions that demonstrate a thorough understanding of security foundations and practical applications of information technology.
- Demonstrate a solid foundation in information security strategies and apply their knowledge by assessing an information security situation and prescribing an appropriate security approach.
- Construct an information security approach that balances organizational needs with those of confidentiality, integrity and availability. Solutions require a comprehensive approach that aligns with policy, technology, and organizational education, training and awareness programs.
- Effectively communicate information security assessments, plans and actions for technical and nontechnical audiences/stakeholders.
- Identify emerging information security issues, utilize knowledge of information security theory to investigate causes and solutions, and delineate strategies guided by evolving information security research and theory.
- Assess and balance the relationship and inter-responsibilities between all three communities of interest in Information Security: 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, Programs and Personnel - into a coordinated operation.
- Articulate positive and socially responsible positions on ethical and legal issues associated with the protection of information and privacy.
- Devise incident response strategies, including business continuity planning/disaster recovery planning (BCP/DRP) initiatives, while focusing on cost effectiveness from both a proactive and reactive perspective.

MSISM Graduation Requirements

The MSISM program requires completion of 35 credit hours with a 3.0 G.P.A, within 5 years. Students must complete the following requirements:

Required Course		Credits
ISM 5101	Security Essentials	3
ISM 5201	Hacking Techniques & Incident Response	3
ISM 5601	Law of Data Security and Investigations	3
ISM 5300	Building Security Awareness	1
RES 5500	Graduate Research Practicum	2
ISM 5550	Research Presentation I	1
ISM 5700	Situational Response Practicum	1
ISM 5800	IT Security Project Management	3
ISM 5400	IT Security Strategic Planning, Policy, and Leadership	3
ISM 6300	Core NetWars Continuous Practicum	1
ISM 6001	Standards-based Implementation of Security	3
RES 5900	Advanced Graduate Research Practicum	2
ISM 6201	Auditing Networks, Perimeters and Systems	3
ISE 6999	Elective*	3
ISM 6100	Security Project Practicum	1

ISM 5900	Research Presentation II	1
N/A	MSISM Capstone	1
Total		35

* Please see list of acceptable technical elective courses in the course listings section

Post-baccalaureate Certificate Programs

Application Requirements and Process

All applicants must meet the following criteria:

- Have at least 12 months of professional work experience in information technology, security or audit.
- Be employed or have current access to an organizational environment that allows you to apply the concepts and hands-on technical skills learned in your program of study.
- Have earned a baccalaureate degree from a recognized college or university, or equivalent international education.

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

a) Personal Information Form
b) Current Resume
c) Official Transcripts
d) Outcomes Statement (Cybersecurity Engineering Core certificate program only)
   If you seek enroll in the Cybersecurity Engineering Core graduate certificate program, write a single-page, single-spaced, typed "Outcomes Statement" Essay describing how the certificate program will fit within your career development. We will evaluate your "Outcomes Statement" primarily to evaluate the quality of your writing, relative to the requirements in the Cybersecurity Engineering Core program for two 15-20 page research project/papers.
i) Non-Native English Speaking Applicants
   a. Transcript Evaluation through World Evaluation Services (WES)
   b. Non-native English speakers must submit TOEFL Scores.

Application Submission

The completed Application for Admission and supporting credentials should completed online at apply.sans.edu.

Invitation to Matriculate

Once the Admissions Committee reviews and approves your application for admission, the Admissions Office will send you an "Offer of Admission," requiring your review and return. This "Offer of Admission" letter will be contingent on successful completion of the virtual New Student Orientation within 60 days of admission.

New Student Orientation

STI's New Student Orientation ensures that all new students are provided with the information necessary to navigate their STI 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. Our NSO is comprised of: an orientation module, a follow up survey, scheduling an appointment with your student advisor, and concludes with registering for your first course. Students wishing to attend an upcoming live event 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. Orientation opens on the 1st of each month for certificate students. After admission, students must wait until the next available orientation date to begin classes. Students have 30 days to complete all NSO components once they begin the module.

Preferred Application Deadline: Please submit your application 30 days prior to your anticipated start month.

Course Waivers

Please refer to the Transfer Credit Policy.

Because students must earn a minimum of 75% of the credits directly from the SANS Technology Institute, graduate certificate students are only eligible to waive between three and four credits or one of the required courses. Graduate certificates cannot be awarded retroactively for coursework completed through the SANS Institute (and not through the graduate school).

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 certificate program are:

- Students will be able to utilize a broad range of current tools and technologies in the design and implementation of security solutions deployed across organizations.
- Students will be able to analyze network traffic to extract the observable characteristics of networks and network devices, thus providing a basis for defensive strategies.
- Students will be able to assemble tools and configure systems and networks to permit systems to foster resiliency and continuity of operations through attacks.
- Students will be able to 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 Graduation Requirements

The Cybersecurity Engineering Core post-baccalaureate certificate program targets completion of 12 credit hours with a 3.0 G.P.A, within 18 to 24 months. Students must complete the following requirements:

Required Courses		Credits
ISE 5101	Security Essentials	3
ISE 5201	Hacking Techniques and Incident Response	3
ISE 5401	Advanced Network Intrusion Detection and Analysis	3
RES 5500	Graduate Research	2
ISE 6300	Core NetWars Continuous	1
	Total	12

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 are able to:

- 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 Graduation Requirements

The Penetration Testing & Ethical Hacking post-baccalaureate certificate program targets completion of 13 credit hours with a 3.0 G.P.A, within 18 to 24 months. Students must complete the following requirements:

Required Courses		Credits
ISE 5201	Hacking Techniques & Incident Response	3
ISE 6315	Web Application Penetrating Testing & Ethical Hacking	3
ISE 6320	Network Penetration Testing & Ethical Hacking	3
ISE 6999	Elective Course	3
ISE 6300	Core NetWars Continuous Capstone	1
Total		13

Penetration Testing Elective Course Options

Students in the Penetration Testing & Ethical Hacking program must choose one course from the following list:

ISE 6325 Mobile Device Security and Ethical Hacking – *3 Credits*
ISE 6330 Wireless Ethical Hacking, Penetration Testing, and Defenses – *3 Credits*
ISE 6350 Python for Penetration Testers – *3 Credits*
ISE 6360 Advanced Penetration Testing, Exploits, and Ethical Hacking – *3 Credits*

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 in particular to examine and reverse engineer malicious code often supporting these attacks. The program introduces students to forensic analysis policy and procedures, forensic analysis tools, data recovery, and investigation techniques.

Program Learning Outcomes

The program learning outcomes of the Incident Response graduate certificate program are:

- The student will be able to 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.
- The student will be able to analyze the structure of common attack techniques in order to evaluate an attacker's footprint, target the ensuing investigation and incident response, and anticipate and mitigate future activity.
- The student will be able to evaluate the effectiveness of available digital forensic tools and use them in a way that optimizes the efficiency and quality of digital forensic investigations.
- The student will be able to 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 Graduation Requirements

The Incident Response post-baccalaureate certificate program targets completion of 13 credit hours with a 3.0 G.P.A, within 18 to 24 months. Students must complete the following requirements:

Required Courses		Credits
ISE 5201	Hacking Techniques & Incident Response	3
ISE 6425	Advanced Computer Forensic Analysis & Incident Response	3
ISE 6440	Advanced Network Forensics & Analysis	3
ISE 6460	Malware Analysis & Reverse Engineering	3
ISE 6400	DFIR NetWars Continuous Capstone	1
	Total	13

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

Graduates of the Cyber Defense Operations post-baccalaureate certificate program will be able to:

- 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 Graduation Requirements

The Cyber Defense Operations post-baccalaureate certificate program targets completion of 12 credit hours with a 3.0 G.P.A, within 18 to 24 months. Students must complete the following requirements:

Required Courses		Credits
ISE 5401	Advanced Network Intrusion Detection and Analysis	3
ISE 6240	Continuous Monitoring and Security Operations	3
ISE 6999	Elective Courses	6
	Total	12

Cyber Defense Operations Elective Course Options

Students in the Cyber Defense Operations program must choose one course from the following list:

ISE 6235 Securing Linux/Unix – *3 Credits*
ISE 6001: Implementing and Auditing Critical Security Controls – *3 Credits*
ISE 6215: Advanced Security Essentials – *3 Credits*
ISE 6230: Securing Windows with the Critical Security Controls – *3 Credits*
ISE 6235: Securing Linux/Unix – *3 Credits*

Course Listings and Descriptions

Information Security Engineering

ISE 5101 Security Essentials
SANS class: SEC 401 Security Essentials Boot-camp Style
3 Credit Hours

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 Hacking Techniques & Incident Response
SANS class: SEC 504 Hacker Techniques, Exploits & Incident Handling
3 Credit Hours

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 5300 Building Security Awareness
SANS class: MGT 433 Securing the Human: Building and Deploying an Effective Security Awareness Program
1 Credit Hour

Note: We recommend students take this course OnDemand.

One of the most effective ways to secure the human factor in an enterprise is an active awareness and education program that goes beyond compliance and leads to actual changes in behaviors. In ISE 5300, students learn the key concepts and skills to plan, implement, and maintain an effective security awareness programs that make organizations both more secure and compliant. In addition, metrics are introduced to measure the impact of the program and demonstrate value. Finally, through a series of labs and exercises, students develop their own project and execution plan, so they can immediately implement a customized awareness program for their organization.

ISE 5401 Advanced Network Intrusion Detection & Analysis
SANS class: SEC 503 Intrusion Detection In-Depth
3 Credit Hours

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.

RES 5500 Graduate Research Practicum
2 Credit Hours

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

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

ISE 5550 Research Presentation I
SANS class: MGT 305 Technical Communication and Presentation
1 Credit Hour

Note: MGT 305 is taken OnDemand, and requires in-person attendance for evaluation of presentation.

ISE 5550 gives students the ability to convert written material to a persuasive oral presentation such as might be appropriate in an enterprise environment. Students use research material written in a previous course in the curriculum to build and deliver a 30-minute presentation, typically given at a SANS training conference.

ISE 5600 IT Security Leadership Competencies
SANS class: MGT 514 IT Security Strategic Planning, Policy, and Leadership, days 3,4, and 5
1 Credit Hour

Note: We recommend students take this course OnDemand.

ISE 5600 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 5700 Situational Response Practicum
1 Credit Hour

Note: This course requires in-person attendance.

In ISE 5700, a small group of students is given an information security scenario that is partly based on current events, and requires a broad knowledge of information security concepts. Their task is to evaluate the scenario and to recommend a course of action. This experience is a timed 24-hour event and culminates in a group written report and presentation at the end of the 24-hour preparation time.

ISE 5800 IT Security Project Management
SANS class: MGT 525 IT Project Management, Effective Communication, and PMP® Exam Prep
3 Credit Hours

Note: This course requires in-person attendance. SANS MGT 525 is only offered at live training events. It is not available online.

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 also 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.

RES 5900 Advanced Graduate Research Practicum
2 Credit Hours

RES 5900 is a graduate-level research course in which students will identify, investigate and analyze a problem. Students will write a research paper interpreting the data collected and making recommendations for action. The research paper will reflect original work towards a new practice, solution, tool, policy, or paradigm offering the potential for real impact in the field of information security.

ISE 5900 Research Presentation II
1 Credit Hour

ISE 5900 gives a chance to further develop their skills at converting written material into a persuasive oral presentation such as might be appropriate in an enterprise environment. Students use research material written from previous courses in the curriculum to build and deliver a 30-minute presentation, either at a SANS training conference, or in an online environment.

ISE 6001 Standards-based Implementation of Security
SANS class: SEC 566 Implementing and Auditing the Twenty Critical Security Controls
3 Credit Hours

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 6100 Security Project Practicum
1 Credit Hours

In ISE 6100, a small group of students is given an information security project that requires a broad knowledge of information security concepts. Their task is to evaluate the project assignment and to recommend a course of action. This experience is a timed 30-day event. Students receive the project assignment from faculty, and must respond with a project plan to address the assignment within 5 days. The group then uses their plan to address the assignment, and deliver a written report at the end of the 30-day period.

ISE 6300 NetWars Continuous Practicum
1 Credit Hour

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.

ISE 6400 DFIR NetWars Continuous Practicum
(Incident Response Certificate only)
1 Credit Hour

DFIR NetWars Continuous is an incident simulator packed with a vast amount of forensic, malware analysis, threat hunting, and incident response challenges designed to help you gain proficiency without the risk associated when working real-life incidents.

Technical Elective Course Options

The following are technical elective courses. Students in the MSISE program must choose 3 courses from this list.

Students in the MSISM program must choose 1 course from this list.

ISE 6215 Advanced Security Essentials
SANS class: SEC 501 Advanced Security Essentials - Enterprise Defender
3 Credit Hours

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 6230: Securing Windows and Resisting Malware
SANS class: SEC 505 Securing Windows and Resisting Malware
3 Credit Hours

ISE 6230 shows students how to secure servers, workstations and portable devices running Microsoft Windows. Windows is the most frequent target of hackers and advanced malware. While other courses focus on detection or remediation of a compromise after the fact, the aim of this course is to substantially reduce these compromises in the first place. For scalability and automation, this course includes many hands-on labs with Group Policy and PowerShell scripting. No prior scripting experience is required. Learning at least the basics of PowerShell is an essential skill for anyone who manages Windows servers or clients in an enterprise.

ISE 6235: Securing Linux/Unix
SANS class: SEC 506 Securing Linux/Unix
3 Credit Hours

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

ISE 6240: Continuous Monitoring & Security Operations
SANS class: SEC 511 Continuous Monitoring & Security Operations
3 Credit Hours

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 6245: SIEM with Tactical Analytics
SANS class: SEC 555
3 Credit Hours

This course is designed to demystify the Security Information and Event Management (SIEM) architecture and process, by navigating the student through the steps of tailoring and deploying a SIEM to full Security Operations Center (SOC) integration.

ISE 6315: Web App Penetration Testing and Ethical Hacking
SANS class: SEC 542 Web App Penetration Testing and Ethical Hacking
3 Credit Hours

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: Network Penetration Testing and Ethical Hacking
SANS class: SEC 560 Network Penetration Testing and Ethical Hacking
3 Credit Hours

ISE 6320 prepares students to conduct successful penetration testing and ethical hacking projects. 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. Students will participate in an intensive, hands-on Capture the Flag exercise, conducting a penetration test against a sample target organization.

ISE 6325: Mobile Device Security
SANS class: SEC 575 Mobile Device Security and Ethical Hacking
3 Credit Hours

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
SANS class: SEC 617 Wireless Ethical Hacking, Penetration Testing, and Defenses
3 Credit Hours

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 class: SEC 573 Python for Penetration Testers
3 Credit Hours

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 Network Penetration Testing
SANS class: SEC 660 Advanced Penetration Testing, Exploits, and Ethical Hacking
3 Credit Hours

ISE 6360 builds upon ISE 6320 – Network Penetration Testing and Ethical Hacking. 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 6420: Computer Forensic Investigations - Windows
SANS class: FOR 500 Computer Forensic Investigations - Windows In-Depth
3 Credit Hours

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 and Incident Response
SANS class: FOR 508 Advanced Digital Forensics and Incident Response
3 Credit Hours

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

ISE 6440: Advanced Network Forensic Analysis
SANS class: FOR 572 Advanced Network Forensics and Analysis
3 Credit Hours

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 6445 Cyber Threat Intelligence
SANS class: FOR 578 Cyber Threat Intelligence
3 Credit Hours

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 in order to establish a solid foundation for any security skillset and to amplify existing skills.

ISE 6450: Advanced Smartphone Forensics
SANS class: FOR 585 Advanced Smartphone Forensics
3 Credit Hours

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 6460: Malware Analysis and Reverse Engineering
SANS class: FOR 610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
3 Credit Hours

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 class: SANS ICS 410 ICS/SCADA Security Essentials
3 Credit Hours

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 Class: SANS ICS 515 ICS Active Defense and Incident Response
3 Credit Hours

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 class: ICS 456 Essentials for NERC Critical Infrastructure Protection
3 Credit Hours

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 6615: Defending Web Applications Security Essentials
SANS class: DEV 522 Defending Web Applications Security Essentials
3 Credit Hours

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 6715 Auditing Networks, Perimeters and Systems
(available as an elective to MSISE students only)
SANS class: AUD 507 Auditing Networks, Perimeters, and Systems
3 Credit Hours

ISE 6715 is organized specifically to provide a risk driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high level audit issues and general audit best practice, students have the opportunity to dive deep into the technical how to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatably verify these controls and techniques for continuous monitoring and automatic compliance validation are given from real world examples.

ISE 6720 Legal Issues in Data Security and Investigations
(available as an elective to MSISE students only)
SANS class: LEG 523 Legal Issues in Information Technology and Security
3 Credit Hours

ISE 6720 introduces students to the new laws on privacy, e-discovery, and data security so students can bridge the gap between the legal department and the IT department. It also provides students with skills in the analysis and use of contracts, policies, and records management procedures.

MSISE Capstone
1 Credit Hour

Note: The GSE lab is offered twice a year.

The GSE exam Capstone experience has two parts. The first is a multiple-choice exam, which may be taken at a proctored location just like any other GIAC exam. Passing this exam qualifies students to sit for the GSE hands-on lab. The first day of the two-day GSE lab consists of an incident response scenario that requires the candidate to analyze data and report their results in a written report. The second consists of a rigorous battery of hands-on exercises drawn from a variety of information security domains listed.

Information Security Management

ISM 5101 Security Essentials
SANS class: MGT 512 Security Leadership Essentials
3 Credit Hours

ISM 5101 is the introductory, survey course in the information security management master's program. It establishes the foundations for developing, assessing and managing security functions at the end-user, network and enterprise levels of an organization. The faculty instruction, readings, exam, and required student writing assignment are coordinated to introduce and develop the core technical, management, and enterprise-level capabilities that will be developed throughout the master's program.

ISM 5201 Hacking Techniques & Incident Response
SANS class: SEC 504 Hacker Techniques, Exploits & Incident Handling
3 Credit Hours

By adopting the viewpoint of a hacker, ISM 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.

ISM 5300 Building Security Awareness
SANS class: MGT 433 Securing the Human: Building and Deploying an Effective Security Awareness Program
1 Credit Hour

Note: We recommend students take this course OnDemand.

One of the most effective ways to secure the human factor in an enterprise is an active awareness and education program that goes beyond compliance and leads to actual changes in behaviors. In ISM 5300, students learn the key concepts and skills to plan, implement, and maintain an effective security awareness programs that make organizations both more secure and compliant. In addition, metrics are introduced to measure the impact of the program and demonstrate value. Finally, through a series of labs and exercises, students develop their own project and execution plan, so they can immediately implement a customized awareness program for their organization.

ISM 5400 IT Security Planning, Policy & Leadership
SANS class: MGT 514 IT Security Strategic Planning, Policy, and Leadership
3 Credit Hours

ISM 5400 covers the entire strategic planning process: how to plan the plan, horizon analysis, visioning, environmental scans (SWOT, PEST, Porter's etc.), historical analysis, mission, vision, and value statements. The course also reviews the planning process core, candidate initiatives, the prioritization process, resource and IT change management in planning, how to build a roadmap, setting up assessments, and revising the plan.

RES 5500 Graduate Research Practicum
2 Credit Hours

RES 5500 is a graduate-level research course in which students will identify, investigate and analyze a problem. Students will write a research paper interpreting the data collected and making recommendations for action. The research paper will reflect original work towards a new practice, solution, tool, policy, or paradigm offering the potential for real impact in the field of information security.

ISM 5550 Research Presentation I
SANS class: MGT 305 Technical Communication and Presentation
1 Credit Hour

Note: MGT 305 is taken OnDemand, and requires in-person attendance for evaluation of presentation.

ISM 5550 gives students the ability to convert written material to a persuasive oral presentation such as might be appropriate in an enterprise environment. Students use research material written in a previous course in the curriculum to build and deliver a 30-minute presentation, typically given at a SANS training conference.

ISM 5601 Legal Issues in Data Security and Investigations
SANS class: LEG 523 Legal Issues in Information Technology and Security
3 Credit Hours

ISM 5601 introduces students to the new laws on privacy, e-discovery, and data security so students can bridge the gap between the legal department and the IT department. It also provides students with skills in the analysis and use of contracts, policies, and records management procedures.

ISM 5700 Situational Response Practicum
1 Credit Hour

Note: This course requires in-person attendance.

In ISM 5700, a small group of students is given an information security scenario that is partly based on current events, and requires a broad knowledge of information security concepts. Their task is to evaluate the scenario and to recommend a course of action. This experience is a timed 24-hour event and culminates in a group written report and presentation at the end of the 24-hour preparation time.

ISM 5800 IT Security Project Management
SANS class: MGT 525 IT Project Management, Effective Communication, and PMP® Exam Prep
3 Credit Hours

Note: This course requires in-person attendance. SANS MGT 525 is only offered at live training events. It is not available online.

In ISM 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. ISM 5800 follows the basic project management structure from the PMBOK® Guide 5th edition and also 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.

RES 5900 Advanced Graduate Research Practicum
2 Credit Hours

RES 5500 is a graduate-level research course in which students will identify, investigate and analyze a problem. Students will write a research paper interpreting the data collected and making recommendations for action. The research paper will reflect original work towards a new practice, solution, tool, policy, or paradigm offering the potential for real impact in the field of information security.

ISM 5900 Research Presentation II
1 Credit Hour

ISM 5900 gives a chance to further develop their skills at converting written material into a persuasive oral presentation such as might be appropriate in an enterprise environment. Students use research material written from previous courses in the curriculum to build and deliver a 30-minute presentation, either at a SANS training conference, or in an online environment.

ISM 6001 Standards-based Implementation of Security
SANS class: SEC 566 Implementing and Auditing the Twenty Critical Security Controls
3 Credit Hours

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. ISM 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.

ISM 6100 Security Project Practicum
1 Credit Hour

In ISM 6100, a small group of students is given an information security project that requires a broad knowledge of information security concepts. Their task is to evaluate the project assignment and to recommend a course of action. This experience is a timed 30-day event. Students receive the project assignment from faculty, and must respond with a project plan to address the assignment within 5 days. The group then uses their plan to address the assignment, and deliver a written report at the end of the 30-day period.

ISM 6201 Auditing Networks, Perimeters and Systems
SANS class: AUD 507 Auditing Networks, Perimeters, and Systems
3 Credit Hours

ISM 6201 is organized specifically to provide a risk driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high level audit issues and general audit best practice, students have the opportunity to dive deep into the technical how to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for continuous monitoring and automatic compliance validation are given from real world examples.

ISE 6300 NetWars Continuous Practicum
1 Credit Hour

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.

MSISM Capstone
Assessment: GSM
1 Credit Hour

Note: The GSM lab is offered once or twice a year, dependent on need.

The GSM exam Capstone experience is a two-day hands-on lab exercise where students demonstrate their ability to formulate and implement policies and solutions that demonstrate a thorough understanding of security foundations and practical applications of information technology. Students work through scenarios which require them to: construct information security approaches that balance organizational needs, apply standards-based approaches to information security risk management, and devise incident response strategies.

Technology and Software Requirements

In order to fulfill the requirements of the STI course 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.)

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' 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.