OVERVIEW

Master's Degrees

Graduate Certificates

Regional Accreditation

Funding Options

2017

SANS
Technology
Institute

The best. Made better.

SANS Technology Institute

The best. Made better.

SANS graduate programs are the ultimate expression of our 25 years dedicated to the education and development of information security professionals.

The SANS Technology Institute transforms the world's best cybersecurity training and certifications into a comprehensive, rigorous, graduate education experience.

Our programs provide high-potential cybersecurity professionals with the combination of cutting-edge knowledge and leadership skills that takes careers to the highest levels.

The best. Made better.

SANS Technology Institute is an independent subsidiary of SANS, the largest and most trusted source for cybersecurity training in the world.

Higher Demands on Cyber Professionals

As cyber attacks increase in volume and complexity, and organizations scramble to keep pace, the career path for cybersecurity professionals is being transformed.

Leading an organization's security efforts now requires more than technical competence. In fact, cybersecurity professionals with advanced degrees now outnumber those with only a bachelor's degree, and information security professionals in management positions are 60% more likely to hold an advanced degree than only a bachelor's.

Higher Degree of Learning

The SANS Technology Institute offers practical, rewarding, and effective education programs that prepare cybersecurity professionals to meet these new demands for career advancement.

Master of Science Degrees

The Master's Programs of the SANS Technology Institute provide the foremost education for cyber professionals.

- Master of Science in Information Security Engineering (MSISE)
- Master of Science in Information Security Management (MSISM)

Graduate Certificates

Graduate Certificate Programs offer individuals the opportunity to earn a post-baccalaureate, graduate-level credential by completing a series of three to four related, technical courses.

- Cybersecurity Engineering (Core)
- Cyber Defense Operations
- Penetration Testing and Ethical Hacking
- Incident Response

Accreditation

The SANS Technology Institute is accredited by the Middle States Commission on Higher Education, 3624 Market Street, Philadelphia, PA 19104 (267-284-5000). The Middle States Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

Coursework to Meet Real World Demands

70%

Technical Expertise with Application Emphasis

- Rigorous technical excellence
- Hands-on skills emphasis
- Hyper-current content
- Real-world application

15%

Management and Communication

- Leadership and strategy
- Organizational effectiveness & managing people
- Mobilizing and implementing

15%

In-Practice Leading and Learning

- Team exercises and scenario response
- Group project development and management
- Presentation simulation

Flexible Course Options to Meet Your Schedule

Live Immersive Instruction

Attend class during SANS events held around the world throughout the year. Meet fellow students and instructors in person.

OnDemand

Online, self-paced instruction optimizes flexibility, allowing you to learn at your own pace from home or work.

vLive

Log in twice weekly for two months, meet with your class and instructor in an interactive, virtual classroom.

Working graduate students can choose any option with confidence. Each learning mode provides the same high level of quality and satisfaction.

World-Class Faculty with Exceptional Skills

The Elite SANS Instructors

Fewer than 75 faculty have qualified to teach for SANS, globally. A rigorous, multi-year selection process certifies fewer than 1 in 1,200.

Cutting-Edge Workplace Experience

Faculty average 15 years information security experience. They are real-world practitioners who specialize in what they teach, not IT generalists.

Extraordinary Teaching Skills

10+ years average teaching experience. Rare combination of technical expertise and student engagement skills.

Tuition Payment Options

We offer master's candidates a Tuition Payment Plan. In addition, tuition is often eligible for corporate tuition reimbursement.

Our graduate programs are approved for VA Education Benefits.

GI Bill.

SANS GIAC CERTIFICATIONS

Industry Recognized Certifications

Students earn GIAC certifications during most technical courses.

SANS
Technology
Institute

Master of Science in Information Security Engineering (MSISE)

The preeminent degree for technical leadership in cybersecurity.

Master of Science in Information Security Management (MSISM)

Focus on standards and systems for security management.

Designed for Working Professionals

Tailor your class start dates and locations (live or online) to fit your schedule.

Flexible Duration

Complete your degree between 3 and 5 years.

GIAC Certifications

Earn 6-8 industry-recognized GIAC certifications even before you graduate.

Build Communication Skills

Improve your ability to present technical topics to non-technical audiences, be persuasive, and mobilize organizations to achieve security goals.

Admissions Checklist

- Application form
- Current résumé
- Two essays
- Video submission
- Letter of recommendation
- Official transcripts (undergraduate degree required)
- Application fee

Prepare to lead. The MSISE program is a rigorous, challenging, and rewarding experience that provides you with the rare combination of elite technical mastery and the leadership capability to mobilize people, organizations, and resources.

With a focus on ensuring your ability to apply knowledge and skills in real-world situations, the MSISE program prepares you to make an immediate and lasting impact on your team and your career.

Program Highlights:

SANS Technical Core

- Layered, defensive techniques
- Study of hacker techniques (offense informs defense)
- Intrusion detection & incident response

Deep, Advanced Elective Catalog

- Penetration testing
- Digital forensics
- Specialized defense practices

Integrated Learning: The best. Made better.

- Advanced labs & real-life simulations
- NetWars cyber range testing
- Project Management/PMP®

Research Relevant to Your Job

- Reviewed by industry experts
- Present at SANS conferences
- Security awareness programs

Focus: NetWars Cyber Range

Government agencies, military, law enforcement, and commercial entities continuously deploy this cyber range (and its cousin, SANS CyberCity) to train their teams and facilitate hands-on learning. Graduate students get months of continuous access to hone and practice their skills.

Sample Schedule

- **Year 1**: 4-5 courses, 11 credits
- **Year 2**: 6 courses, 13 credits
- **Year 3**: 5-6 courses, 12 credits
- **8-10 hours** per week investment

Who Should Enroll?

IT or Infosec professionals who seek to advance their careers to become technically proficient leaders and managers in their organizations.

This program will prepare professionals who will command the trust and confidence of their organizations because they will simultaneously have the requisite knowledge of underlying technologies and threat vectors, as well as the communication skills and organizational techniques to corral resources, effect change, and get things done.

Cybersecurity issues have arrived at the board and executive level – with a loud bang. Organizations can no longer manage cybersecurity as a technical support function. Effective decisions on strategic priorities and resource allocation for cybersecurity require new perspectives, new skills, and a new level of executive leadership.

The MSISM program provides students with the executive skills needed to define and deliver organization-wide strategies, programs, and policies. It teaches many of the technical underpinnings of information security, but focuses information security personnel on auditing information systems, managing the legal implications of an incident, evaluating emerging solutions, and implementing organization-wide standards.

Who Should Enroll?

IT or IS managers in larger organizations that emphasize organizational and policy considerations rather than technical, hands-on skills and knowledge.

MSISM students take required courses in policy development, audit, and legal considerations in place of some of the technical, applied-skills courses in the MSISE program. This is a difference in emphasis, but MSISM graduates will still understand the underlying technologies.

Core Courses

Course Number and Name		SANS Class	Assessment(s)	Credit Hours
ISE 5150	Enterprise Information Security	SEC401	GSEC Exam, Research Paper	4
ISE 5200	Hacking Techniques & Incident Response	SEC504	GCIH Exam, NetWars Continuous	4
ISE 5300	Building Security Awareness	MGT433	Writing Exercise	1
ISE 5400	Advanced Network Intrusion Detection & Analysis	SEC503	GCIA Exam, Research Paper	4
ISE 5550	Research Presentation I	MGT305	Oral Presentation	1
ISE 5600	IT Security Leadership Competencies	MGT514.4	Writing Exercise	1
ISE 5700	Group Incident Response Exercise	N/A	24-Hour Group Project, CIO Report	1
ISE 5800	IT Security Project Management	MGT525	GCPM Exam	3
ISE 5900	Research Presentation II	N/A	Oral Presentation	1
ISE 6000	Standards-based Implementation of Security	SEC566	GCCC Exam, Research Paper	4
ISE 6100	Security Implementation Team Project	N/A	Group Written Project Plan	2
ISE 6 _ _ _	3 Technical Electives (see next page)	SANS Class	GIAC Exam	9
MSISE Capstone	GIAC Security Expert (GSE) Certification		Exam, Two-day Hands-on Lab	1

Degree Total: 36 Credit Hours

Electives

Course Number and Name		SANS Class	Assessment	Credit Hours
ISE 6215	Advanced Security Essentials	SEC501	GCED Exam	3
ISE 6230	Securing Windows with the Critical Security Controls	SEC505	GCWN Exam	3
ISE 6235	Securing Linux/Unix	SEC506	GCUX Exam	3
ISE 6240	Continuous Monitoring & Security Operations	SEC511	GMON Exam	3
ISE 6315	Web App Penetration Testing & Ethical Hacking	SEC542	GWAPT Exam	3
ISE 6320	Network Penetration Testing & Ethical Hacking	SEC560	GPEN Exam	3
ISE 6325	Mobile Device Security	SEC575	GMOB Exam	3
ISE 6330	Wireless Penetration Testing	SEC617	GAWN Exam	3
ISE 6350	Python for Penetration Testers	SEC573	GPYC Exam	3
ISE 6360	Advanced Penetration Testing	SEC660	GXPN Exam	3
ISE 6420	Computer Forensic Investigations - Windows	FOR408	GCFE Exam	3
ISE 6425	Advanced Computer Forensic Analysis & Incident Response	FOR508	GCFA Exam	3
ISE 6440	Advanced Network Forensics & Analysis	FOR572	GNFA Exam	3
ISE 6450	Advanced Smartphone Forensics	FOR585	GASF Exam	3
ISE 6460	Malware Analysis & Reverse Engineering	FOR610	GREM Exam	3
ISE 6515	ICS/SCADA Security Essentials	ICS410	GICSP Exam	3
ISE 6520	ICS Active Defense & Incident Response	ICS515	GRID Exam	3
ISE 6615	Defending Web Applications Security Essentials	DEV522	GWEB Exam	3
ISE 6715	Auditing Networks, Perimeters & Systems	AUD507	GSNA Exam	3
ISE 6720	Law of Data Security & Investigations	LEG523	GLEG Exam	3

SANS Technology Institute

Graduate Certificates In Cybersecurity

Strengthen essential technical knowledge and skills.

Who Should Enroll?

Professionals seeking to benefit from only technical subsets of the master's programs, in different engineering practice areas.

Certificate Timeline

Individual courses take 3 to 5 months to complete. The entire program should be completed over the course of approximately 18 to 24 months.

Tuition Options

Regional accreditation enables many students to use corporate tuition reimbursement.

Certificate programs are eligible for VA Education Benefits.

Admissions

- Shorter process (application form, résumé, official transcripts)
- Undergraduate degree required
- Application fee

Cybersecurity professionals operate amidst rapid, constant change. New threats emerge daily. Knowledge currency is essential and an ongoing task. The SANS Technology Institute's Graduate Certificate Program provides a shorter, technically focused set of courses that sharpen your skills and keep your knowledge current. Certificate program credit is directly applicable to the Master's Program.

Students can choose from 4 options and will earn 3 to 4 GIAC certifications while earning a graduate-level credential.

Cybersecurity Engineering (Core)

Spans from an introductory survey of fundamental information security tools and techniques to more advanced study of the inter-relationships between offensive (attack/penetration testing) and defensive (intrusion detection and incident response) information security best practices.

Cyber Defense Operations

Focuses on developing the student's capability to defend and secure information assets and business systems at an organization.

Penetration Testing and Ethical Hacking

Focuses on developing the student's capability to discover, analyze, and understand the implications of information security vulnerabilities in systems/networks/applications in order to identify solutions before others exploit these flaws.

Incident Response

Focuses on developing the student's capability to manage both a computer and network-based forensic investigation as well as the appropriate incident responses.

Course Lists

Cybersecurity Engineering (Core) Certificate – 12 Credit Hours

Course Number and Name		SANS Class	Assessment(s)	Credit Hours
ISE 5150	Enterprise Information Security	SEC401	GSEC Exam, Research Paper	4
ISE 5200	Hacking Techniques & Incident Response	SEC504	GCIH Exam, NetWars Continuous	4
ISE 5400	Advanced Network Intrusion Detection & Analysis	SEC503	GCIA Exam, Research Paper	4

Cyber Defense Operations – 12 Credit Hours

Course Number and Name		SANS Class	Assessment	Credit Hours
ISE 5101	Security Essentials	SEC401	GSEC Exam	3
ISE 6001	Implementing & Auditing Critical Security Controls	SEC566	GCCC Exam	3
ISE 6215	Advanced Security Essentials	SEC501	GCED Exam	3
Select one of the following:				
ISE 5401	Advanced Network Intrusion Detection & Analysis	SEC503	GCIA Exam	3
ISE 6230	Securing Windows with the Critical Security Controls	SEC505	GCWN Exam	3
ISE 6235	Securing Linux/Unix	SEC506	GCUX Exam	3
ISE 6240	Continuous Monitoring & Security Operations	SEC 511	GMON Exam	3
ISE 6715	Auditing Networks, Perimeters & Systems	AUD 507	GSNA Exam	3

Course Lists (continued)

Penetration Testing & Ethical Hacking Certificate – 13 Credit Hours

Course Number and Name	SANS Class	Assessment(s)	Credit Hours
ISE 5200 Hacking Techniques & Incident Response	SEC504	GCIH Exam, NetWars Continuous	4
ISE 6315 Web Application Penetration Testing & Ethical Hacking	SEC542	GWAPT Exam	3
ISE 6320 Network Penetration Testing & Ethical Hacking	SEC560	GPEN Exam	3
Select one of the following:			
ISE 6325 Mobile Device Security	SEC575	GMOB Exam	3
ISE 6330 Wireless Networks Penetration Testing	SEC617	GAWN Exam	3
ISE 6350 Python for Penetration Testers	SEC573	GPYC Exam	3
ISE 6360 Advanced Penetration Testing	SEC660	GXPN Exam	3

Incident Response Certificate – 13 Credit Hours

Course Number and Name	SANS Class	Assessment(s)	Credit Hours
ISE 5200 Hacking Techniques & Incident Response	SEC504	GCIH Exam, NetWars Continuous	4
ISE 6425 Advanced Computer Forensic Analysis & Incident Response	FOR508	GCFA Exam	3
ISE 6440 Advanced Network Forensics & Analysis	FOR572	GNFA Exam	3
ISE 6460 Malware Analysis & Reverse Engineering	FOR610	GREM Exam	3

"The SANS faculty make this program unique. They're at the top of their industry and not a single one is too busy to engage with students at all levels."

– Ron Hamann, MSISE Candidate
Consultant, Slalom Consulting

"I was challenged by both the coursework and faculty. Earning a graduate degree from SANS had a direct and positive influence on my career."

– Russ McRee, MSISE
Director, Security Response & Investigations, Microsoft

"I chose the SANS Technology Institute over other programs primarily because of the ability to tailor the program to my career goals."

– Sally Vandeven, MSISE
Security Tester, Black Hills Information Security

SANS.EDU

SANS
Technology
Institute

The best. Made better.

The SANS Technology Institute develops leaders to strengthen enterprise and global information security. We educate managers and engineers in information security practices and techniques, attract top scholar-practitioners as faculty, and engage both students and faculty in real-world applied research.

SANS Technology Institute
Telephone: 301-241-7665
Email: info@sans.edu