SANS Technology Institute

11200 Rockville Pike, Ste. 200
North Bethesda, MD, 20851
(301) 241-7665 | info@sans.edu

July 1, 2021

James D. Fielder, Jr., Ph.D.
Secretary of Higher Education
Maryland Higher Education Commission
Nancy S. Grasmick Building, 10th Floor
6 North Liberty Street
Baltimore, MD 21201

Dear Dr. Fielder,

I am pleased to submit, on behalf of the SANS Technology Institute, the attached proposal for substantial modification to our existing Cyber Defense Operations post-baccalaureate certificate program.

I look forward to answering any questions you or your staff may have, or providing additional information as needed. I can be reached by cell phone at 440-321-3040.

Eric Patterson
Executive Director/Interim President
SANS Technology Institute

MHEC
ENGAGE • INFORM • SUPPORT

Office Use Only: PP#

Cover Sheet for In-State Institutions
New Program or Substantial Modification to Existing Program

Institution Submitting Proposal	SANS Technology Institute

Each action below requires a separate proposal and cover sheet.

○ New Academic Program	○ Substantial Change to a Degree Program
○ New Area of Concentration	○ Substantial Change to an Area of Concentration
○ New Degree Level Approval	● Substantial Change to a Certificate Program
○ New Stand-Alone Certificate	○ Cooperative Degree Program
○ Off Campus Program	○ Offer Program at Regional Higher Education Center

Payment Submitted:	○ Yes ○ No	Payment Type:	○ R*STARS # ○ Check #	Payment Amount:		Date Submitted:	

Department Proposing Program	Operations			
Degree Level and Degree Type	Post-baccalaureate certificate			
Title of Proposed Program	Cyber Defense Operations			
Total Number of Credits	12			
Suggested Codes	HEGIS: 5199.00		CIP: 11.1003	
Program Modality	● On-campus		○ Distance Education (*fully online*)	
Program Resources	● Using Existing Resources		○ Requiring New Resources	
Projected Implementation Date	● Fall	○ Spring	○ Summer	Year: 2021
Provide Link to Most Recent Academic Catalog	URL: https://www.sans.edu/media/Graduate-Course-Catalog.pdf			

Preferred Contact for this Proposal	Name:	Betsy Marchant
	Title:	Assistant Director
	Phone:	(804) 519-6863
	Email:	bmarchant@sans.edu
President/Chief Executive	Type Name:	Eric Patterson
	Signature:	Date: 07/01/2021
	Date of Approval/Endorsement by Governing Board:	06/30/2021

Revised 1/2021

Proposal for a Substantial Modification to an Existing Degree Program: Cyber Defense Operations Post-Baccalaureate Certificate

SANS Technology Institute
July 1, 2021

Table of Contents

Centrality to Institutional Mission and Planning Priorities

Program Description

The SANS Technology Institute proposes to substantially modify an existing post-baccalaureate certificate program titled Cyber Defense Operations (CDO). Established and approved by MHEC in 2015, the post-baccalaureate certificate program in CDO is designed to be a highly technical, 12 credit hour program with a cohesive set of learning outcomes focused on teaching the applied technologies used to design, build and defend the security of information assets and business systems of an organization. All work completed while pursuing the certificate program may be applied directly towards the fulfillment of the master's degree requirements should the student matriculate in the master's program. The proposed modifications to the CDO graduate certificate program will use existing institutional resources, and the changes will not require additional resources to implement.

Relation to Mission, Vision, and Strategic Goals of STI

The CDO program continues to directly align with the formal mission of the SANS Technology Institute:

> The SANS Technology Institute develops technically-skilled professionals and leaders who strengthen global information security through innovative and flexible approaches to learning. We prepare our students to master advanced practices through experiential and project-based learning which is delivered by faculty who are top scholar-practitioners in the industry, and our graduates implement and execute state-of-the-art cybersecurity.

The CDO certificate program advances this mission by focusing on educating "scientists/engineers in information security practices and techniques," providing technical education to individuals who need to understand core and advanced components used to protect and defend information assets and business systems. Graduates of the Cyber Defense Operations certificate program are proficient in the defensive technical skills required to become leaders in their respective teams

Summary of Key Changed Elements

This proposal of substantial modification is the result of a comprehensive program review of the CDO certificate in 2021, which assessed (1) the content, balance, coherence, and rigor of the CDO curriculum, (2) the alignment of student performance and outcomes with the program's learning objectives and with the STI mission, and (3) the alignment of the program's learning outcomes with employers' needs and expectations.

Largely, the proposed changes with regards to the concepts, content, or course level learning outcomes are minimal. However, swapping a core requirement with an elective and adding several new electives, we will meet the 33% changed threshold in which necessary to submit a formal change proposal.

Current graduation requirements

(with planned changes outlined in the comments field)

Required Course	Course Name	Credits	Proposed Changes
Core courses:			
ISE 6240	Continuous Monitoring & Security Operations	3	
ISE 5401	Intrusion Detection In-Depth	3	This course will be changed to an elective option. It is advanced and more specialized.
Choose 2 electives:			

ISE 6001	Implementing & Auditing the Critical Security Controls	3	This course will be removed from program as it is not a coherent fit in the curriculum. Several other more relevant courses will be added as elective options.
ISE 6215	Advanced Security Essentials	3	
ISE 6230	Securing Windows & PowerShell Automation	3	
ISE 6255	Defensible Security Architecture & Engineering	3	This course will be changed to a core requirement. It is broad and foundational course in cyber defense.

Proposed Graduation Requirements

Required Course	Course Name	Credits
Core courses:		
ISE 6240	Continuous Monitoring & Security Operations	3
ISE 6255	Defensible Security Architecture & Engineering	3
Choose 2 electives:		
ISE 4450	Security Operations and Analysis Fundamentals	3
ISE 6215	Advanced Security Essentials	3
ISE 5401	Intrusion Detection In-Depth	3
ISE 6230	Securing Windows & PowerShell Automation	3
ISE 6245	SIEM with Technical Analytics	3
ISE 6350	Automating Information Security with Python	3
ISE 6250	Purple Team Tactics & Kill Chain Defenses	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.

Critical and Compelling Regional or Statewide Need as Identified in the State Plan

Demand and Need for Program

Cybersecurity is a national priority and critical to the well-being of organizations. As technology becomes increasingly sophisticated, demand for an experienced and qualified workforce is essential. The CDO program is directly supportive of the development of professionals with the skills and capabilities to design, implement, and manage the protection of information assets that are central to the advancement and evolution of knowledge in the information age.

Cyberseek, a website created by the National Institute of Standards and Technology (NIST), indicates that there are 464,420 cybersecurity job openings nationally. CyberSeek states that the supply of cybersecurity workers nationally is “very low” relative to the demand. In Maryland alone, CyberSeek shows that there are 19,645 job openings and 2,883 of those openings that specifically request GIAC certifications which are obtained as a degree requirement of the CDO program. These data indicate a high demand not just for cybersecurity workers, but especially for those who have proven, by holding GIAC certifications, that they have the skills to do the job.

Cybersecurity jobs are already an important part of Maryland's economy, comprising the second highest concentration of professional and technical workers among all fifty states. With the increasing recognition of the vulnerability of critical public and private networks and the need to better protect those networks against constantly evolving threats, it is reasonable to expect that, in conjunction with the State Plan, Maryland will continue to attract additional information security workers and separating military veterans who wish to enter into this challenging field. This growth will call for educated technical leaders with diverse skillsets and the ability to implement, develop, integrate, orchestrate, and lead cybersecurity operations.

Relevance to Historically Black Institutions

This program proposal will have no impact on the uniqueness and institutional identity of mission of HBIs, as it does not represent a net change in the number or kind of offerings in graduate cybersecurity education within Maryland.

Alignment with Maryland State Plan for Postsecondary Education

Increase student success with less debt

This program will address the State Plan's goals to increase student success with less debt. Approximately 30% of our students fully fund their studies by way of employer tuition reimbursement, while another 40% utilize veteran education benefits.

Supporting veterans

Strategy 7 calls for special efforts to support veterans. Approximately 40% of our current study body is comprised of veterans, with nearly all of them using some combination of GI Bill benefits and employer tuition reimbursement to increase their knowledge and skills as they enter or further establish themselves in the civilian workforce.

Develop new partnerships between colleges and businesses to support workforce development and improve workforce readiness

The CDO program makes substantial contributions to Maryland's goals by seeking to increase the number and quality of graduates who are desperately in demand in business and industry verticals across the state. Cybersecurity jobs are already an important part of Maryland's economy, comprising the second highest concentration of professional and technical workers among all fifty states. Yet, even with this standing, the demand for skilled and educated cybersecurity practitioners is outstripping the available supply. With more than 45,000 information security workers employed in Maryland, the state currently has almost 20,000 job openings in the field, with over 14,000 of those positions categorized as being in the "Protect & Defend" domain according to the NICE Cybersecurity Workforce Framework.

Quantifiable and Reliable Evidence and Documentation of Market Supply and Demand in the Region and State

The National Institute of Standards and Technology (NIST) supports a website called CyberSeek that contains data on cybersecurity jobs and lists the number of current job openings by state and metropolitan area. In this section we combine the CyberSeek data with employment projections from the Maryland Department of Labor Licensing and Regulation (DLLR) to estimate the demand for the BACS program in Maryland and in the region.

Cyberseek indicates that there are 464,420 cybersecurity job openings nationally. CyberSeek states that the supply of cybersecurity workers nationally is "very low" relative to the demand. In Maryland alone, CyberSeek shows that there are 19,645 job openings and 2,883 of those openings that specifically request GIAC certifications which are obtained as a degree requirement of the CDO program. These data indicate a high demand not just for cybersecurity workers, but especially for those who have proven, by holding GIAC certifications, that they have the skills to do the job.

Table 1: Current Positions and Projected Growth to 2028 in CyberSeek's "Top Cybersecurity Job Titles"

Job Title	**Maryland Positions in 2018**	**Growth to 2028**	**Growth in Percent**
Information Security Analysts	4,116	5,727	39.14%
Computer Systems Analysts	15,927	19,014	13.10%
Network Engineer/Architect	4,629	5,281	14.09%
Cyber Security Manager/Administrator	12,868	14,561	13.16%
Software Developer	9,311	11,773	26.44%

Source: http://www.dllr.state.md.us/lmi/iandoproj/maryland.shtml (accessed June 14, 2021).

Cybersecurity jobs are already an important part of Maryland's economy, comprising the second highest concentration of professional and technical workers among all fifty states. With the increasing recognition of the vulnerability of critical public and private networks and the need to better protect those networks against constantly evolving threats, it is reasonable to expect that, in conjunction with the State Plan, Maryland will continue to attract additional information security workers and separating military veterans who wish to enter into this challenging field. This growth will call for educated technical leaders with diverse skillsets and the ability to implement, develop, integrate, orchestrate, and lead cybersecurity operations.

Reasonableness of Program Duplication

This proposal for a “Substantial Modification” to the SANS Technology Institute’s CDO program does not alter the number or nature of existing programs related to information security engineering in Maryland, nor how our program relates to those programs. As this substantial modification mainly seeks to increase coherence of the program curriculum, and which incorporates only a marginal change of program learning outcomes, academic requirements, or course content, we do not feel that anything provided in this substantial modification impacts the prior determinations by MHEC regarding program duplication.

Relevance to High-demand Programs at Historically Black Institutions (HBIs)

No HBI offers a comparable credential.

Relevance to the identity of Historically Black Institutions (HBIs)

This program proposal will have no impact on the uniqueness and institutional identity of mission of HBIs, as it does not represent a net change in the number or kind of offerings in graduate cybersecurity education within Maryland.

Adequacy of Curriculum Design, Program Modality, and Related Learning Outcomes

Establishment of Program and Faculty

Established and approved by MHEC in 2015, the post-baccalaureate certificate program in CDO is designed to be a highly technical, 12 credit hour program with a cohesive set of learning outcomes focused on teaching the applied technologies used to design, build and defend the security of information assets and business systems of an organization. The CDO program is overseen by a faculty committee that includes the following individuals:

Dr. Johannes Ullrich
Johannes is Dean of Research at STI and also created and manages the SANS Internet Storm Center (ISC) and the GIAC research paper program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Johannes holds a PhD in physics from SUNY Albany. His daily podcast, listened to by more than 10,000 professionals, summarizes current security news in a concise format.

David Hoelzer
David is the Dean of Faculty at STI. He is the author of more than twenty days of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Consumer Financial Protection Bureau in a landmark case regarding information security governance within corporations in the financial sector and has previously served as an expert for the Federal Trade Commission for GLBA Privacy Rule litigation and other matters. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee, Long Range Planning Committee, GIAC Ethics Board, and as Dean of Faculty. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities. Outside of SANS, David is a research fellow in the Center for Cybermedia Research, a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC), an adjunct research associate of the UNLV Cybermedia Research Lab, a research fellow with the Internet Forensics Lab, and an adjunct lecturer in the UNLV School of Informatics. David has written and contributed to more than 15 peer reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT and an MS in Computer Science, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University.

Rob Lee
Rob Lee is the Chief Curriculum Director and Faculty Lead at the SANS Institute where he oversees the Digital Forensics, Incident Response, Cloud, Pen Testing, Audit, Application Security, and Cyber Defense curricula along with other operational functions in the company. With more than 24 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response, he provides consulting services in the Washington, D.C. area. Before starting his own business, Rob worked with government agencies in the law enforcement, defense and intelligence communities as a lead for vulnerability discovery and exploit development teams, a cyber forensics branch, and a computer forensic and security software development team.

Rob graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information operations. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team conducting computer crime investigations, incident response, and computer forensics. Prior to starting his own firm, he directly worked with a variety of government agencies, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber forensics branch, and lead for a digital forensic and security software development team. Rob was also a director for MANDIANT, a company focused on investigating advanced adversaries, such as the APT, for five years prior to starting his own business. Rob co-authored the book Know Your Enemy, 2nd Edition. Rob earned his MBA from Georgetown University in Washington DC. Rob is also a co-author of the MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat.

Educational Objectives and Intended Student Learning Outcomes

During the program review process, STI faculty affirmed the appropriateness of the following, pre-approved, Cyber Defense Operations program learning outcomes:

1. Students will be able to utilize a broad range of current tools and technologies to design, build and maintain security solutions deployed across organizations.

2. The student will be able to identify the information assets of an enterprise, classify them by value, and determine what management and technical controls can be used to monitor and audit them effectively.

3. The student will be able to develop a program for analyzing the risk to the information assets in an enterprise and determining which technical and management controls can mitigate, remove, or transfer that risk.

4. Students will know how to systematically remediate any known security issues and design an infrastructure that minimizes the exposure from future attacks.

Program Outline

Required Course	Course Name	Credits
Core courses:		
ISE 6240	Continuous Monitoring & Security Operations	3
ISE 6255	Defensible Security Architecture & Engineering	3
Choose 2 electives:		
ISE 4450	Security Operations and Analysis Fundamentals	3
ISE 6215	Advanced Security Essentials	3
ISE 5401	Intrusion Detection In-Depth	3
ISE 6230	Securing Windows & PowerShell Automation	3
ISE 6245	SIEM with Technical Analytics	3
ISE 6350	Automating Information Security with Python	3
ISE 6250	Purple Team Tactics & Kill Chain Defenses	3

Course Requirements and Descriptions

ISE 6240: Continuous Monitoring & Security Operations
SANS SEC 511 | GIAC GMON | 3 Credit Hours | 90 Days

ISE 6240 teaches a 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.

Upon completing this course, students will be able to:

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and Security Operations Centers (SOC)
- Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key CIS Controls

ISE 6255: Defensible Security Architecture and Engineering
SANS SEC 530 | 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.

Upon completing this course, students will be able to:

- Analyze a security architecture for deficiencies
- Implement technologies for enhanced prevention, detection, and response capabilities
- Comprehend deficiencies in security solutions and understand how to tune and operate them
- Apply the principles learned in the course to design a defensible security architecture
- Determine appropriate security monitoring needs for organizations of all sizes
- Maximize existing investment in security architecture by reconfiguring existing assets
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Configure appropriate logging and monitoring to support a Security Operations Center and continuous monitoring program

ISE 4450: Security Operations and Analysis Fundamentals
SANS SEC 450 | GIAC GSOC | 3 Credit Hours | 90 Days

ISE 4450 provides students with the technical knowledge and key concepts essential for security operation center (SOC) analysts and new cyber defense team members. 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.

Upon completing this course, students will be able to:

- Describe how SIEM, threat intelligence platforms, incident management systems, and automation should connect and work together to provide a painless workflow for analysts
- Analyze common alert types including HTTP(S), DNS, and email-based attacks
- Identify of post-exploitation attacker activity
- Build mental models for understanding alerts and attack patterns that can help to effectively prioritize alerts
- Perform high-quality, bias-free alert analysis and investigation
- Identify the most high-risk alerts, and quick ways to verify them
- Collect logs throughout the environment and the importance of parsing, enrichment, and correlation capability of the SIEM
- Create and tune threat detection analytics to eliminate false positives

ISE 6215: Advanced Security Essentials
SANS SEC 501 | 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.

Upon completing this course, students will be able to:

- Identify network security threats against infrastructure and build defensible networks that minimize the impact of attacks
- Access tools that can be used to analyze a network to prevent attacks and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises systems and how to respond to attacks
- Perform penetration testing against an organization to determine vulnerabilities and points of compromise
- Apply the six-step incident handling process
- Use various tools to identify and remediate malware across your organization
- Create a data classification program and deploy data-loss-prevention solutions at both a host and network level
- Analyze network configurations for routers and build a defensible network architecture
- Perform detailed analysis of traffic using various sniffers and protocol analyzers
- Identify and track attacks and anomalies in network packets
- Use various tools to perform vulnerability scanning, penetration testing, and network discovery
- Analyze both Windows and Unix systems during an incident to identify signs of a compromise
- Find, identify, and clean up various types of malware, such as Ransomware

ISE 5401: Intrusion Detection In-Depth
SANS SEC 503 | 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.

Upon completing this course, students will be able to:

1. Analyze traffic traversing your site to avoid becoming another "Hacked!" headline
2. Identify potentially malicious activities for which no IDS has published signatures
3. Place, customize, and tune your IDS/IPS for maximum detection
4. Detect, analyze, and network forensic investigation with a variety of open-source tools
5. Understand TCP/IP and common application protocols to gain insight about your network traffic, enabling you to distinguish normal from abnormal traffic
6. Understand the benefits of using signature-based, flow, and hybrid traffic analysis frameworks to augment detection

- Configure and run open-source Snort and write Snort signatures
- Configure and run open-source Bro to provide a hybrid traffic analysis framework
- Understand TCP/IP component layers to identify normal and abnormal traffic
- Use open-source traffic analysis tools to identify signs of an intrusion
- Comprehend the need to employ network forensics to investigate traffic to identify a possible intrusion
- Use Wireshark to carve out suspicious file attachments
- Write tcpdump filters to selectively examine a particular traffic trait
- Craft packets with Scapy
- Use the open-source network flow tool SiLK to find network behavior anomalies
- Use your knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire

ISE 6230: Securing Windows & PowerShell Automation
SANS SEC 505 | GIAC GCWN | 3 Credit Hours | 90 Days

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.

Upon completing this course, students will be able to:

- Write PowerShell scripts for Windows and Active Directory security automation
- Safely run PowerShell scripts on thousands of hosts over the network
- Defend against PowerShell malware such as ransomware
- Harden Windows Server and Windows 10 against skilled attackers

ISE 6245: SIEM with Tactical Analytics
SANS SEC 555 | GIAC GCDA | 3 Credit Hours | 90 Days

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.

Upon completing this course, students will be able to:

- Deploy the SANS SOF-ELK VM in production environments
- Demonstrate ways most SIEMs commonly lag current open source solutions (e.g. SOF-ELK)
- Bring students up to speed on SIEM use, architecture, and best practices
- Know what type of data sources to collect logs from
- Deploy a scalable logs solution with multiple ways to retrieve logs
- Operationalize ordinary logs into tactical data
- Develop methods to handle billions of logs from many disparate data sources
- Understand best practice methods for collecting logs
- Dig into log manipulation techniques challenging many SIEM solutions
- Build out graphs and tables that can be used to detect adversary activities and abnormalities
- Combine data into active dashboards that make analyst review more tactical
- Utilize adversary techniques against them by using frequency analysis in large data sets
- Develop baselines of network activity based on users and devices
- Develop baselines of Windows systems with the ability to detect changes from the baseline
- Apply multiple forms of analysis such as long tail analysis to find abnormalities
- Correlate and combine multiple data sources to achieve more complete understanding
- Provide context to standard alerts to help understand and prioritize them
- Use log data to establish security control effectiveness
- Implement log alerts that create virtual tripwires for early breach detection
- Understand how to handle container monitoring and log collection
- Baseline and find unauthorized changes in cloud environments
- Integrate and write custom scripts against a SIEM

ISE 6350: Python for Penetration Testers
SANS SEC 573 | 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.

Upon completing this course, students will be able to:

- Leverage Python to perform routine tasks quickly and efficiently
- Automate log analysis and packet analysis with file operations, regular expressions, and analysis modules to find evil
- Develop forensics tools to carve binary data and extract new artifacts
- Read data from databases and the Windows Registry
- Interact with websites to collect intelligence
- Develop UDP and TCP client and server applications
- Automate system processes and process their output

ISE 6250: Purple Team Tactics & Kill Chain Defenses
SANS SEC 599 | 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.

Upon completing this course, students will be able to:

- Leverage MITRE ATT&CK as a "common language" in the organization
- Build a Cuckoo sandbox solution to analyze payloads
- Develop effective group policies to improve script execution (including PowerShell, Windows Script Host, VBA, HTA, etc.)
- Understand key bypass strategies for script controls (Unmanaged Powershell, AMSI bypasses, etc.)
- Stop 0-day exploits using ExploitGuard and application whitelisting
- Understand key bypass strategies in application whitelisting (focus on AppLocker)
- Detect and prevent malware persistence
- Leverage the Elastic stack as a central log analysis solution
- Detect and prevent lateral movement through Sysmon, Windows event monitoring, and group policies
- Block and detect command and control through network traffic analysis
- Leverage threat intelligence to improve security posture

General Education Requirements

General education requirements are not applicable to the SANS Technology Institute CDO program. Students are required to have completed a bachelor's degree before admittance.

Specialized Accreditation/Certification Requirements

No specialized accreditations or certifications are required for this program or its students.

Contract with Another Institution or Non-collegiate Organization

The modifications made to the CDO program precipitating this Program Proposal neither include nor impact any changes to any relationship the SANS Technology Institute has with another institution or non-collegiate organization. Courses are authored and taught by members of the faculty of the SANS Technology Institute. Commensurate with the approval of the SANS Technology Institute as a degree-granting institution in the State of Maryland in 2005, and as reviewed and accredited by the Middle States Commission on Higher Education, the SANS Technology Institute will continue to engage the support services of its parent, the Escal Institute for Advanced Technologies (d/b/a/ SANS Institute) and its sister subsidiary, GIAC. The agreements are not designed specifically for the CDO program, but as supporting structures for STI, these agreements support the delivery and management of this program. The MOUs have enabled all STI degree programs since STI was established and were most recently reviewed and approved during the Middle States accreditation team visit.

Prospective and Current Student Communications

CDO program requirements and student services are found on our website at www.sans.edu. All marketing materials will be updated with the new version of the curriculum.

Once enrolled, new students attend orientation before registering for their first course. During orientation (outlined at https://www.sans.edu/students/orientation), students learn about modalities, faculty/student interaction, learning management systems, costs and payment policies, and academic support services available. As a final stage of orientation, students meet with their advisor to discuss course and degree requirements and any questions that the students have a result of completing orientation.

Adequacy of Articulation

STI's CDO program does allow for the transfer or waiver of one prior SANS course and/or GIAC examinations. STI does not accept for transfer coursework from other academic programs. Thus, no articulation agreements currently exist and none are anticipated.

Adequacy of Faculty Resources

The STI faculty is comprised of and appointed from the 100+ individuals who have achieved the status of being "SANS Certified Instructors," an industry-recognized demarcation of technical achievement practiced in the field, superior teaching effectiveness and student engagement as exemplified in the classroom and online, and successful completion of a competitive development process that employs both student and peer-faculty feedback to prove that the instructors possess these qualities. Among the faculty are people who are called upon to investigate attacks on the U.S. government and our largest commercial enterprises, who are entrusted to teach practitioners of cybersecurity at the highest and most sensitive (classified) levels, and who through their professional practice and research advance our understanding of cyber threats and potential remediation, and then transmit that knowledge forward to our students and the larger community. Even beyond their superlative technical abilities, our faculty have skills as teachers that truly set them apart and allow them to impart sometimes dense technical lessons with enthusiasm, applicable real-world examples, and charismatic engagement. While a handful of faculty members serve in full-time teaching and research roles, most are scholar-practitioners who teach less than full-time for the school so that they can engage in the practice of cybersecurity, keep their skills advanced and current, and feed their experiences and learnings back into the courses and class discussions.

STI's current faculty leadership includes the following individuals:

Dr. Johannes Ullrich
Johannes is Dean of Research at STI and also created and manages the SANS Internet Storm Center (ISC) and the GIAC research paper program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Johannes holds a PhD in physics from SUNY Albany. His daily podcast, listened to by more than 10,000 professionals, summarizes current security news in a concise format.

David Hoelzer
David is the Dean of Faculty at STI. He is the author of more than twenty days of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Consumer Financial Protection Bureau in a landmark case regarding information security governance within corporations in the financial sector and has previously served as an expert for the Federal Trade Commission for GLBA Privacy Rule litigation and other matters. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee, Long Range Planning Committee, GIAC Ethics Board, and as Dean of Faculty. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities. Outside of SANS, David is a research fellow in the Center for Cybermedia Research, a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC), an adjunct research associate of the UNLV Cybermedia Research Lab, a research fellow with the Internet Forensics Lab, and an adjunct lecturer in the UNLV School of Informatics. David has written and contributed to more than 15 peer reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also

serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT and an MS in Computer Science, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University.

Rob Lee
Rob Lee is the Chief Curriculum Director and Faculty Lead at the SANS Institute where he oversees the Digital Forensics, Incident Response, Cloud, Pen Testing, Audit, Application Security, and Cyber Defense curricula along with other operational functions in the company. With more than 24 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response, he provides consulting services in the Washington, D.C. area. Before starting his own business, Rob worked with government agencies in the law enforcement, defense and intelligence communities as a lead for vulnerability discovery and exploit development teams, a cyber forensics branch, and a computer forensic and security software development team.

Rob graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information operations. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team conducting computer crime investigations, incident response, and computer forensics. Prior to starting his own firm, he directly worked with a variety of government agencies, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber forensics branch, and lead for a digital forensic and security software development team. Rob was also a director for MANDIANT, a company focused on investigating advanced adversaries, such as the APT, for five years prior to starting his own business. Rob co-authored the book Know Your Enemy, 2nd Edition. Rob earned his MBA from Georgetown University in Washington DC. Rob is also a co-author of the MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat

The full listing of STI faculty can be reviewed on our website at https://www.sans.edu/academics/faculty.

Faculty Recruitment and Development

One of the most serious responsibilities of the administration after student learning is the continued development and recruitment of qualified faculty. Especially since the institute is committed to using only Scholar/Practitioners of a Master Teacher caliber, continuous development and recruitment is critical to the sustainability of the college. To this end, the SANS Technology Institute and the affiliated SANS Institute partner for faculty development. The high-level roadmap for faculty development is illustrated in Figure 1.

To maintain the staffing levels required, the affiliated SANS Institute actively recruits individuals within the various communities of practice who demonstrate a high degree of mastery within a particular subject area as evidenced by achieving a high score on the ANSI accredited certification exam. Individuals who are willing to participate are then given additional coaching and training by a college faculty member and have the potential to eventually qualify as a Faculty member.

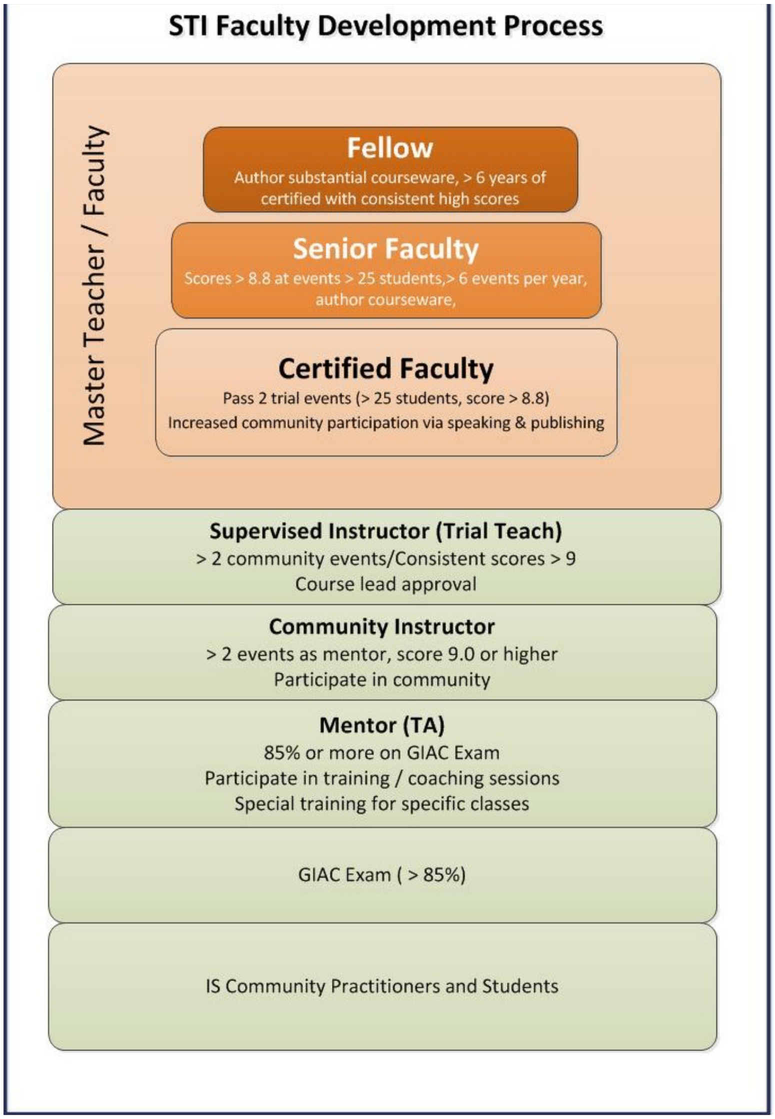
STI Faculty Development Process
Master Teacher / Faculty
Fellow
Author substantial courseware, > 6 years of certified with consistent high scores
Senior Faculty
Scores > 8.8 at events > 25 students,> 6 events per year, author courseware,
Certified Faculty
Pass 2 trial events (> 25 students, score > 8.8)
Increased community participation via speaking & publishing
Supervised Instructor (Trial Teach)
> 2 community events/Consistent scores > 9
Course lead approval
Community Instructor
> 2 events as mentor, score 9.0 or higher
Participate in community
Mentor (TA)
85% or more on GIAC Exam
Participate in training / coaching sessions
Special training for specific classes
GIAC Exam (> 85%)
IS Community Practitioners and Students

Figure 1 - Faculty Development Process

Mentor / TA

Individuals who demonstrate continued interest and ability are given the opportunity for coaching by a faculty member. Should he demonstrate willingness and an aptitude toward teaching, he will be given the opportunity to act as a "Mentor" for a particular course. The role of a mentor is to conduct a weekly recitation of material that students have prepared independently. His responsibility is to act as subject matter expert for this small group, providing an experience akin to a traditional Teaching Assistant role during a recitation.

Each Mentor is evaluated after each recitation by the students present. These evaluations are tabulated by an assessment analyst and forwarded to the staff of the affiliated SANS Institute for review and progress monitoring.

Community Instructor / TA

The success of a Mentor is measured by the outcome of student evaluations. Should a Mentor successfully complete two separate Mentoring experiences, he may qualify for an opportunity to participate at a smaller "Community" event hosted by the SANS Institute affiliate.

Prior to being invited to instruct at a Community event the candidate must first successfully pass a Murder Board. This is a live teaching simulation where the candidate must present a section of the course material to one or more of the college faculty. At least one of the faculty will have the role of challenging the potential instructor with difficult questions, unusual classroom control problems and other simulations to gauge both the subject matter mastery and the ability of the candidate to effectively control a classroom.

Trial Instructor / Supervised Instruction / TA

Community Instructors who, based on student evaluations, successfully teach at two separate Community engagements with the partner SANS Institute may qualify for an opportunity as a Trial Instructor. Qualification is contingent on approval from the Research Faculty responsible for the relevant course experience. Given that individuals at this strata are essentially candidates for Adjunct Faculty, a senior faculty member of the college will become engaged.

Trial Instructors are invited to work directly with a qualified senior member of the college faculty. Under the direction of the faculty member one hour segments of course material are selected for preparation and delivery by the trial instructor. Based on student evaluations and instructor observations, the trial instructor may be invited to present additional course hours.

Trial Instructors should expect to receive direct constructive feedback from the supervising faculty member. Trial Instructors are strongly encouraged to follow the recommendations of the supervising faculty member.

During the balance of the course experience, the Trial Instructor acts as a Teaching Assistant for the supervising faculty member. Trial Instructors are encouraged to pay close attention to how the faculty member delivers the course material, how the classroom is managed, how contact hours are managed and how student success and understanding is ensured.

Certified Instructor

Following two successful engagements as a Trial Instructor and based upon student evaluations and supervising faculty recommendation, a Trial Instructor may be promoted to Certified Instructor. At this point, the individual is qualified as an Adjunct Faculty member to teach courses within the college under the direction of the Professor of Practice, the Program Directors and the Research Faculty overseeing the particular courses being taught.

Certified Instructors, as Adjunct Faculty, are also expected to display the aspects of a Scholar/Practitioner as discussed on page **Error! Bookmark not defined.**. As a Certified Instructor/Adjunct Faculty it is also expected that the individual will maintain the high caliber of instructor required of a Master Teacher and, as such, will be subject to the same periodic assessment by the Program Directors and Professor of Practice.

Principal Instructor

This section previously wasn't included, not sure what needs to be said here.

Senior Instructor

Individuals who qualify as members of the faculty at the SANS Technology Institute are clearly outstanding. However, some faculty engage more deeply with the college and affiliated entities.

Faculty members who consistently achieve the highest evaluated ratings and who additionally have more than 240 course contact hours each year may qualify as Senior Instructors. Senior Instructors typically have additionally demonstrated significant leadership within the community of practice, perhaps through the development of course material used within the college or an affiliated entity.

Faculty Fellow

Those Senior Instructors who distinguish themselves through significant contributions to the community of practice and who have maintained a Senior Instructor designation for more than six years may be recommended to receive the designation of “Faculty Fellow.”

While a Faculty Fellow does not receive any additional privileges within the college, it is expected that those receiving the Faculty Fellow distinction maintain a leadership position not only within his respective community of practice, but also among the faculty. These individuals should take a real interest in newly promoted faculty and strive to make them feel welcome in the faculty ranks. Faculty Fellows are also expected to be willing to come to the table when a mentor is needed for a fellow faculty member or potential faculty member who is struggling to meet or maintain his qualifications.

This designation is determined by the Academic and Student Affairs committee at one of its periodic meetings. Recommendations for Faculty Fellow are made by committee members. All discussions, recommendations, votes, etc. that pertain to Faculty Fellow recommendations are confidential.

Faculty Development Opportunities

Prospective faculty members who are progressing through the faculty development process, nearing certification as certified faculty members, have the opportunity to participate in a six-hour faculty development workshop. This workshop is overseen by a faculty fellow or curriculum lead. During the first three hours of the workshop, particular attention is given to the development of teaching skills, classroom management skills, keys for successful class preparation, and more through an interactive discussion with the instructor.

After the first three-hour discussion, prospective faculty members are given specific teaching assignments to prepare and are also assigned observation tasks to be completed over the next 18-24 hours. The second three-hour segment is dedicated to providing specific feedback to each participant on his or her own teaching style.

Faculty members may elect to attend the current iteration of this faculty development workshop at any point. Current faculty members may be asked to have limited participation in the presentation aspect in the second three hours depending upon enrollment constraints.

Faculty who participate in our distance learning modalities undergo specific training to help modify their style to this format. We engage a team of individuals to assist in online-specific methods to enable virtual student-faculty interactions, including employing an assistant in the room who participates in the class on behalf of distance students by flagging the instructor’s attention when questions are asked or issues are raised by virtual students.

Adequacy of Library Resources

The challenges of information security are constantly evolving, and excellence in performance demands continuous monitoring of changes in threats, technology, and practices. SANS conducts an extensive research program that helps STI students and alumni maintain their edge in security. The SANS Resource Center is a compilation of thousands of original research papers, security policies, and security notes, along with a wealth of unique network security data. Supplemented by an online research library subscription and other SANS information services, our current and future students have continuous access to the following list of primary resources:

- The SANS Information Security Reading Room, which contains more than 2,000 original research studies, not available from any other source, in 76 knowledge domains relevant to the study of information security. They are downloaded more than a million times each year.
- Free and unlimited access to EBSCO's "Computers and Applied Sciences (Complete)" database. EBCSO is the leading provider of online research databases, e-journals, magazine subscriptions, e-books, and discovery services of all kinds. This full-text database covers computing, technology and engineering disciplines, and contains 650 active full-text journals and magazines, 520 active full-text peer- reviewed journals, 320 active full-text peer-reviewed journals with no embargo, and 410 active full-text and indexed journals.
- The SANS Security Policy Collection, which contains model security policies developed by major corporations and government agencies. The collection contains about 35 policies and grows as new security issues arise and policy templates are needed.
- The SANS Technology Institute's Cyber Research page, which provides access to exemplary graduate-level research papers, group projects, and presentations that cover a wide variety of topics of practical and academic relevance that have real- world impact and often provide cutting-edge advancements to the field of cybersecurity knowledge.
- The SANS Top-20 V7, a consensus list of vulnerabilities that require immediate remediation. The list is the result of a process that brought together dozens of leading security experts.
- The SANS Newsletter Collection, which helps keep students up to date with the high- level perspective of the latest security news.
- The Security Glossary, which is among the largest glossaries of security terms available on the Internet. It was developed jointly by SANS and the National Security Agency and provides authoritative definitions of many of the specialized terms students will encounter.
- The SANS Collection of Frequently Asked Questions about Intrusion Detection, available at contains 118 authoritative discussions of the primary topics that arise when planning and implementing intrusion detection technologies. The collection is available at http://www.sans.org/security-resources/idfaq/.
- The SANS Internet Storm Center Handler Diaries and Archives, which contain contemporaneous analyses of new attacks that are discovered on the Internet. The archives constitute an extraordinary research asset because of the depth of the analysis and the currency of the topics covered. They also provide SANS students with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects that analyze attack patterns and how fast worms and other attacks spread through the Internet.
- SANS Web Briefings held several times a month that feature SANS faculty and other security experts providing up-to-date web briefings for SANS alumni on new threats seen at the Internet Storm Center, ew techologies that are emerging, and analysis of security trends.

Adequacy of Physical Facilities, Infrastructure and Instructional Equipment

As a Proposal for Substantial Modification, there is no change in the physical facilities, infrastructure an instructional equipment required by the program. This program will continue to be offered in combinations of online modalities and in residential institutes. More than 400 residential institutes are available to STI students each year with a cumulative capacity of more than 40,000 students. Each year the residential program expands by 10 to 20 institutes. Thus, the proposed program will easily be accommodated in the existing in-person training programs.

Similarly, the STI programs draw on SANS's online technology that currently serves more than 18,000 students each year and is not capacity-constrained.

Adequacy of Financial Resources with Documentation

Tables

Table 1: Program Resources

Resource Categories	2021	2022	2023	2024	2025
1. Reallocated Funds	0	0	0	0	0
2. Tuition/Fee Revenue (c + g)	550,000	715,000	825,000	880,000	935,000
a. Number of F/T Students	50	65	75	80	85
b. Annual Tuition/Fee Rate	11,000	11,000	11,000	11,000	11,000
c. Total F/T Revenue (a x b)	550,000	715,000	825,000	880,000	935,000
d. Number of P/T Students	0	0	0	0	0
e. Credit Hour Rate	0	0	0	0	0
f. Annual Credit Hour Rate	0	0	0	0	0
g. Total P/T Revenue (d x e x f)	0	0	0	0	0
3. Grants, Contracts & Other External Sources	0	0	0	0	0
4. Other Sources	0				
TOTAL (Add 1-4)	550,000	715,000	825,000	880,000	935,000

Table 2: Expenditures

Expenditure Categories	2021	2022	2023	2024	2025
1. Faculty (b + c below)	0	0	0	0	0
a. Number of FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
2. Admin. Staff (b + c below)	23,100	30,800	38,500	38,500	46,200
a. # FTE	.3	.4	.5	.5	.6
b. Total Salary	16,500	22,000	27,500	27,500	33,000
c. Total Benefits	6,600	8,800	11,000	11,000	13,200
3. Support Staff (b + c below)	0	0	0	0	0

a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
4. Technical Support and Equipment	0	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses	220,000	286,000	330,000	352,000	374,000
TOTAL (Add 1-7)	243,100	316,800	368,500	368,500	420,200

Financial Data Narrative

Table 1: RESOURCES

Re-allocated Funds
N/A

Tuition and Fee Revenue
The tuition projection builds upon current student enrollment headcount and admissions trends for this program. The projection also incorporates current retention data and average times to graduation.

Grants and Contracts
N/A

Other Sources
N/A

Total Year
N/A

Table 2: EXPENDITURES

Faculty
CDO students may receive instruction live in-classroom or online, depending on the course and their own choices. When they attend live in-classroom, they join a class already being taught by STI faculty to other students, to include non-STI students, and therefore CDO students typically represent no more than a 5% - 10% increase in the total students in any given classroom. When they choose to take the course online, no additional faculty are required and, similar to live classes, CDO students represent only a small fraction of those students being taught by the existing group of subject-matter experts and teaching assistants and at any given time. Therefore, we do not anticipate any increase in the number of faculty required to teach STI students, either live or online. The cost associated with the faculty and subject-matter experts/teaching assistants who teach these students is embedded into the payments associated with the Memorandum of Understanding between STI and SANS and is represented in line 5.

Administrative and Support Staff
The STI graduate programs currently operate at a ratio of students to administrative staff ratio of 150:1. Average salary and benefit information is reflective of our current cost experience and market expectations.

Equipment, Library, New and/or Renovated Space
The CDO program will not require any additional equipment, library facilities, or any new and/or renovated space. We have ample capacity in our existing facilities, residential institutes, online platform capacity, and offices.

Other Expenses
A core design element of the SANS Technology Institute are the Memoranda of Understanding signed with our parent, the SANS Institute, and a related entity, GIAC Corporation, that allow STI to select and pay for many costs on a variable, per-student basis. The financial projections assume the same mix of payments that STI incurs today per student, as reviewed by the Middle States evaluation team during our re-accreditation study.

Adequacy of Provisions for Evaluation of Program

Continuous, closed-loop evaluation has been the hallmark of STI programs since the school was established. STI employs a three-level evaluation program completely embedded in the curriculum. The 2018 Middle States Evaluation Team commended this evaluation methodology: "SANS Technology Institute should be commended for the fact that its curriculum automatically embraces learning outcomes and program outcomes."

1. **Every day, in every STI class, every student is expected to complete an evaluation of the teaching effectiveness, the currency and value of the course material, and the quality of the labs, exercises, and other aspects of their learning experience.** Their forms are processed by an evaluation team and results are delivered by 6:30 the following morning to STI's president and senior staff. The course faculty often reviews the forms the evening of the day they are completed. The evaluation team follows up on all strong concerns and, in several cases when a faculty member was clearly struggling, has replaced the teacher by noon the next day based on the evaluations. In addition, the evaluation team compiles and feeds course content suggestions or concerns to the course author for consideration or inclusion in the annual (or sometimes more frequent) course updates. Data on labs or other technology go to the appropriate teams for continuous or major product improvement. This evaluation system is also used in vLive and Simulcast distributed learning modalities. For On-Demand, the evaluation cycle is based on module completion rather than days, but the system functions identically and in fact responses are easier to process because entries are already in digital form when submitted.

2. **Evaluation of course-level student outcomes uses reliable measures of mastery** not subject to variability associated with individual faculty members' understanding of the course outcomes. Each course has an associated examination that is recognized as a widely accepted and valued way to validate mastery of the course outcomes. For example, all CDO students are required to complete a course in which they learn incident handling techniques, common attack techniques, and the most effective methods of stopping intruders using those attack techniques. The exam and certification associated with this course is called the Global Cybersecurity Incident Handler (GCIH) test and certification. The value of this exam is demonstrated by the fact that each year employers pay for more than 11,000 of their employees and job candidates to take this course and sit for the GCIH exam (pass rate of approximately 70%). The acceptance of the exam is validated by the U.S. Department of Defense (DoD) directive that names GCIH certification as proof that a DoD employee or contractor is capable of taking on the highest of three levels of technical cybersecurity roles in DoD. The GIAC certifications used for evaluating student mastery of course objectives are updated using a large-scale job-task analysis that interviews practitioners at least every three years. This process, along with the psychometric assessments that shaped question assessment, is subjected to regular review by the American National Standards Institute. GIAC exams increasingly include hands-on test questions where students can demonstrate they can use what they learned.

3. **To evaluate program outcomes,** STI tracks all graduates and asks them (and when possible, their employers) annually for feedback on how well the program worked for them and how it might be improved. Additionally, STI has implemented its formal Learning Outcomes Assessment Plan, as endorsed by the MSCHE evaluation team. Under this plan, each program undergoes a formal review by an evaluation team comprised of subject matter experts every four years. This review process will ensure alignment of (1) course outcomes to program learning objectives, of (2) program learning objectives to any capstone requirements, and of (3) both program learning objectives and capstone requirements to a survey of industry requirements. This request for substantial change is based upon the CDO program review in 2021.

Consistency with the State’s Minority Student Achievement Goals

STI is committed to maintaining an environment of appropriate conduct among all persons and respect for individual values. The Institute is committed to enforcing non-discrimination and anti-harassment in order to create an environment free from discrimination, harassment, retaliation and/or sexual assault. Discrimination or harassment based on race, gender and/or gender identity or expression, color, creed, religion, age, national origin, ethnicity, disability, veteran or military status, sex, sexual orientation, pregnancy, genetic information, marital status, citizenship status, or on any other legally prohibited basis is unlawful and undermines the character and purpose of STI. Such discrimination or harassment will not be tolerated.

Relationship to Low Productivity Programs Identified by the Commission

This program is not related to an identified low productivity program.

Adequacy of Distance Education Programs

The combination of live classroom and three distance learning modalities used in the CDO program was commended for its “creative and forward looking teaching methodology” in the April 2018 Team Report to the Middle States Commission on Higher Education. That report also noted that all modalities resulted in equivalent scores, with the distance learning modalities earning slightly higher scores in several tougher courses where students needed more time to absorb (and review) the material.

The three distance learning modalities available to students to complete the SANS technical course component are OnDemand, vLive, and Simulcast. Students who use the OnDemand platform are given access to a learning management system with modules pre-loaded into the system and are also provided with printed course books containing written lectures and labs. Each module is a recording from an in-person course session. The learning management system allows students to revisit lectures and also complete quizzes to verify understanding. A recommended viewing schedule is included in course syllabi. Each STI course has a responsible faculty member, who in most cases is the same person recorded for the OnDemand course system. A teaching assistant referred to as a virtual mentor is available for all OnDemand courses to help answer student questions or assist with lab issues.

The vLive learning modality is conducted online with established course meeting times led by an instructor – typically twice per week for up to eight weeks – through a learning management system that allows for direct interaction with the instructor and other course participants. Each course session is recorded for students to review previously covered material, or to view if they miss a session.

The Simulcast delivery modality allows students to participate in a course being offered through the in-person modality, but from their location of choice, enabled through a digital learning management system. Students meet during the same time the in-person course meets. They can participate in classroom lectures by seeing and hearing the instructor, in addition to asking questions and participating in classroom discussion.

If a student chooses a distance learning modality, that experience is comprised of the very same coherent, cohesive, and academically rigorous curriculum used for the course when taken via our traditional residential institute-based, in-person instructional format. The faculty member assigned to the STI course reviews student performance on exams and papers and assigns a grade at the end of the course.

1. **Curriculum and instruction**

   a) ***A distance education program shall be established and overseen by qualified faculty.***

   When implemented for distance education, the courses are converted from the live in- class courses in consultation with and under the direction of the faculty

   b) ***A program’s curriculum shall be coherent, cohesive, and comparable in academic rigor to programs offered in traditional instructional formats.***

   If a student chooses a distance learning modality, that experience is comprised of the very same coherent, cohesive, and academically rigorous curriculum used for the course when taken via our traditional residential institute-based, in-person instructional format. The faculty member who oversees the STI course reviews student performance on exams and papers and assigns a grade at the end of the course. Moreover, the outcomes achieved by students employing STI’s distance learning modalities are demonstrably equivalent to those achieved by students who attend live in-person courses.

   The working group for the 2014 Substantive Change Request, whereby STI was approved by Middle States to deliver more than 50 percent of our credit via distance modalities, reported:

> “A 2013 study of all certification exam results provided evidence that the exam scores achieved on these standardized certification exams were not statistically different when comparing delivery modalities – such as whether the course instruction was taken via our traditional, live instructional format or via either our OnDemand or vLive instructional modalities....A similar analysis was conducted using calendar year 2014 exam outcomes. Results from the analysis were consistent with trends noticed in the 2013 study of all certification exams. On average, students who enrolled in a distance education course in 2014 performed slightly better on exams than students who enrolled in in-person courses.”

To update these assessments, the working group once again compared the GIAC scores of students who had taken their classes live versus those who took their classes through STI’s OnDemand modalities, and once again found the measured learning outcomes to be the same among both groups (Table A4.1).

Table A2.1 Comparison of GIAC Exam Score Performance via Live and OnDemand Modalities, 2014-2017

Modality	Overall Score	Master’s Program	Certificate Program
Live Class	84.6	86.6	82.4
OnDemand Class	83.7	87.2	82.0

c) ***A program shall result in learning outcomes appropriate to the rigor and breadth of the program.***

The learning outcomes of the courses included in the Applied Cybersecurity Program have been validated by the faculty as appropriately rigorous and broad and are integrated into each course and measured quantitatively through ANSI-standardized certification exams for the three advanced courses and through integrated testing in each of the other courses.

d) ***A program shall provide for appropriate real-time or delayed interaction between faculty and students.***

A teaching assistant referred to as a virtual mentor is available for all OnDemand courses to help answer student questions or assist with lab issues.

The vLive learning modality is conducted online with established course meeting times led by an instructor – typically twice per week for up to eight weeks – through a learning management system that allows for direct interaction with the instructor and other course participants. Each course session is recorded for students to review previously covered material, or to view if they miss a session.

The Simulcast delivery modality allows students to participate in a course being offered through the in-person modality, but from their location of choice, enabled through a digital learning management system. Students meet during the same time that the in- person course meets. They can participate in classroom lectures by seeing and hearing the instructor, in addition to asking questions and participating in classroom discussion.

e) ***Faculty members in appropriate disciplines in collaboration with other institutional personnel shall participate in the design of courses offered through a distance education program.***

STI faculty members design all distance learning programs.

2. Role and mission

a) ***A distance education program shall be consistent with the institution’s mission.***

The distance education program at STI is identical in content and impact to the live training program and has been designed, with strong faculty leadership and deep embedded course and program assessment, to focus precisely on meeting STI's mission to develop leaders to strengthen enterprise and global information security.

b) ***Review and approval processes shall ensure the appropriateness of the technology being used to meet a program's objectives.***

The appropriateness of the technology STI uses for distance education has evolved over more than 11 years to be optimized for meeting the active learning needs of full-time working professionals, and it been assessed and approved by STI faculty. But that is not the end of the development process. The distance learning technology is continuously evaluated through evaluations completed by every one of the more than 3,000 cybersecurity professionals using it each day. If a course is not helping students master the key learning objectives, we hear about it quickly and fix the problems.

3. Faculty support

a) ***An institution shall provide for training for faculty who teach with the use of technology in a distance education format, including training in the learning management system and the pedagogy of distance education.***

Faculty who participate in our OnDemand, vLive, and Simulcast distance learning modalities undergo specific training to help modify their style to this format. We engage a team of individuals to assist in online-specific methods to enable virtual student-faculty interactions, including (when a class is Simulcast to students) employing an assistant in the room who participates in the class on behalf of distance students by flagging the instructor's attention when questions are asked or issues are raised by virtual students.

b) ***Principles of best practice for teaching in a distance education format shall be developed and maintained by the faculty****.*

Members of the STI faculty have developed guidelines for best practice when teaching in our distance education formats. The guidelines are reproduced below.

> ***Instructor Guidelines for SANS Simulcast Classes***
>
> *What to Expect*
> During a SANS Simulcast you will be teaching live students in the same room AND students at remote locations. To accomplish this, your on-site moderator will log into GoToTraining and our system will capture everything that is projected in the classroom. You will also wear a wireless microphone to transmit your voice to remote students. The moderator will also set up a webcam and broadcast video from the classroom. We highly encourage the use of video, but if you do not want video to run in your class, please contact the Simulcast staff.
>
> All-day classes will be broken into two sessions: morning and afternoon. When you break for lunch please remind all students to log out of GoToTraining and to log into the afternoon session when they return. You will also need to do the same thing, so please return from your lunch break a few minutes early. The key to teaching a successful vLive! Simulcast is to always **remember that you are teaching remote students; keep them engaged** by promptly responding to their questions and periodically addressing them directly.
>
> *Advance Planning*
> 1. The vLive! and Onsite teams will schedule a planning call with the customer point of contacts two weeks before the course; please plan on attending this call.

2. The AV kit that contains all necessary equipment for the Simulcast will be shipped to the Simulcast location prior to class.
3. The vLive! support team will be setting up the audio equipment and test the setup with you. This test is critical to the success of the Simulcast session and must be completed prior to starting class.
4. If it is possible, plan to do the audio testing the day before class starts. If this is not possible please make sure you arrive 2 hours early on the first day of class to complete the audio setup.
5. The vLive! team will introduce you to the virtual moderator who will be working the classroom. This moderator is a SANS employee who is there to assist with the running of the Elluminate platform, running labs, and assisting with student questions. Many instructors prefer that the moderator relays questions from the virtual students by raising his or her hand and reading the question.

Audio Tips

6. Do not wear your cell phone on your belt next to the transmitter or lay it next to the receiver by the laptop. Your cell phone and student cell phones can create interference. You may need to disable Bluetooth functionality on your phone if it is causing buzzing.
7. Leave your wireless microphone on at all times, but turn off your GoToTraining audio during breaks. To do this, simply ask your on-site moderator to mute you on the Simulcast laptop.
8. ALWAYS repeat comments and questions from students at your location; remote students can hear you, but all other sound will be muffled or inaudible.

Starting Class

9. When it is time to start class, your moderator will start the recording and give you a signal that everything is ready on the remote side.
10. After the moderator has turned the class over to you, introduce yourself and briefly explain to students how the Simulcast class will work.
11. It is important to make the remote and on-site students aware of each other. Identify and welcome each remote site by name. A roster with the remote sites and student counts will be provided to you.
12. Please encourage remote students to participate by typing their questions and comments into the Chat window.
13. Directing questions about class material to the virtual students can also help to keep them engaged throughout the class.
14. The moderator will relay any questions from the online students to you.
15. Discuss any other housekeeping items as needed (timing of breaks, confirming that VMWare is correctly set up, etc.).

Teaching Tips

16.ALWAYS repeat comments and questions from students at your location; remote students can hear you, but all other sound will be muffled or inaudible.
17. If you need to discuss issues that students should not see, please use the “Organizers Only” or “private message” chat option as your means of communication.
18. Address remote students often to ensure they feel like they are part of the class; remote students become passive listeners if they are not actively engaged.
19. All scripts, videos, demos, etc. that you wish to show to students must be shared with GoToTraining’s application sharing feature.
20. Remote students’ systems (and your host’s network) can be slowed down if you send very large files. If a file is necessary for class try to send it before class or during a break. If it is not course-related (e.g., music while on break), consider not sending it.

21. Use the GoToTraining timer when breaking from lecture so remote students know when class will be resuming; tell the moderator how many minutes you would like and they will set up the timer for you.
22.When breaking for lunch, please explain to students that they will need to log out of the morning session and log into the afternoon session upon their return.
23. Allow plenty of time to log into GoToTraining when arriving in the morning or returning from lunch. Depending on the location, you may have to extend the lunch break.
24. Conduct a quick audio check after each break and lunch to confirm that your microphone is on and that your remote students can hear you.

Suggested Best Practices
Jason Fossen:

- Each day I used a second laptop to log onto vLive as an attendee so that I could see how fast my application sharing window was updating its screen. It was also useful for checking the sound, video, and file-sharing features. I granted my other account moderator status so that, in case my primary laptop had an issue, I could switch over to the secondary and continue teaching.
- New vLive instructors (or new laptops for prior instructors) should go through the setup and test process before flying on-site; there won't be enough time to fix any problems like these the morning of.
- Return early after lunch to log back into GoToTraining
- Make sure your Internet connection is wired and not shared by the students.
- Make sure to have the vLive emergency contact info on hand.
- The instructor should have the slides to teach the course on his/her laptop in case the slides in the vLive system are missing, wrong, or have any problems.

Jason Lam:

- Make sure that the OnSite students are aware of the virtual students.
- Be available for remote students before or after class in the Elluminate Office session.
- Depending on the class size and your teaching style you might need longer than usual to prepare for class (questions, demos, labs).
- Have the moderator type names of products, vendors, URLs, etc. in the chat for the virtual students.

c) ***An institution shall provide faculty support services specifically related to teaching through a distance education format.***

SANS Simulcasts are supported by the Onsite and vLive teams. The Onsite team takes the lead with most sales issues, while the vLive team provides most of the support during class. While you are teaching you will have one or more vLive moderators in the vLive virtual classroom to provide assistance with labs and logistics.

4. An institution shall ensure that appropriate learning resources are available to students including appropriate and adequate library services and resources.

The challenges of information security are constantly evolving, and excellence in performance demands continuous monitoring of changes in threats, technology, and practices. SANS conducts an extensive research program that helps STI students and alumni maintain their edge in security. The SANS Resource Center is a compilation of thousands of original research papers, security policies, and security notes, along with a wealth of unique network security data. The list below outlines some of the primary resources available.

- The SANS Information Security Reading Room contains more than 2,000 original research studies, not available from any other source, in 76 knowledge domains relevant to the study of information security. They are downloaded more than a million times each year. The Reading Room is available at http://www.sans.org/reading_room/.
- The SANS Security Policy Collection contains model security policies developed by major corporations and government agencies. The collection contains about 35 policies and grows as new security issues arise and policy templates are needed.
- The SANS Top-20 V7 is a consensus list of vulnerabilities that require immediate remediation. It is the result of a process that brought together dozens of leading security experts.
- The SANS Newsletter Collection helps keep students up to date with the high-level perspective of the latest security news.
- The Security Glossary is among the largest glossaries of security terms available on the Internet. It was developed jointly by SANS and the National Security Agency and provides authoritative definitions of many of the specialized terms students will encounter.
- The SANS Collection of Frequently Asked Questions about Intrusion Detection contains 118 authoritative discussions of the primary topics that arise when planning and implementing intrusion detection technologies. The collection is available at http://www.sans.org/security-resources/idfaq/.
- The SANS Internet Storm Center Archives contain contemporaneous analyses of new attacks that are discovered on the Internet. The archives constitute an extraordinary research asset because of the depth of the analysis and the currency of the topics covered. They also provide SANS students with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects that analyze attack patterns and how fast worms spread through the Internet.
- SANS Web Briefings held several times a month feature SANS faculty and other security experts providing up-to-date web briefings for SANS alumni on new threats seen at the Internet Storm Center, new technologies that are emerging, and analysis of security trends.

5. Students and Student Services

a) A distance education program shall provide students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial aid resources, and costs and payment policies.

- Curriculum information is posted, in detail, at the SANS.EDU website at https://www.sans.edu/academics/
- Course and degree requirements are posted online in the STI Course Catalog at https://www.sans.edu/downloads/STI-Course-Catalog-2018.pdf
- The nature of faculty/student interaction are described on our website at https://www.sans.edu/academics/course-delivery/more
- Assumptions about technology competence and skills are posted at our Admissions website at https://www.sans.edu/admissions/masters-programs
- Technical equipment requirements are posted with individual courses at the SANS course website.
- Learning management systems information is posted in detail at https://www.sans.org/ondemand/faq
- The availability of academic support services and financial aid resources is posted at https://www.sans.edu/students/services, and on page 33 of the Student Handbook at page 33, https://www.sans.edu/downloads/sti-student-handbook.pdf

- Costs and payment policies are posted at https://www.sans.edu/admissions/tuition

b) ***Enrolled students shall have reasonable and adequate access to the range of student services to support their distance education activities.***

With STI students taking approximately half of their credits through distance learning, the overall satisfaction with student services may be considered a reliable surrogate for effectiveness of distance learning student services. Evidence from student surveys indicates that measures of overall student satisfaction are high (above 90%).

Quantified measures of specific sub-processes with student management were also high, with about 90% of respondents saying they were "Somewhat Satisfied" and "Very Satisfied" for each of the operational elements (Table A.4.2).

Table A.2.2. Student Satisfaction with Student Management as Reported in the 2016 Student Experience Survey

	Very Dissatisfied	Somewhat Dissatisfied	Somewhat Satisfied	Very Satisfied
Registration/Billing	<1%	10%	21%	68%
Academic Advising	2%	8%	25%	65%
GI Bill Certification	2%	6%	17%	75%

c) Accepted students shall have the background, knowledge, and technical skills needed to undertake a distance education program.

Our CDO students are working professionals with at least one year of experience in information technology or information security. Thus, they have the needed background, knowledge, and technical skills to use the distance learning modalities.

a) ***Advertising, recruiting, and admissions materials shall clearly and accurately represent the program, and the services available***

STI has a solid record of meeting Middle States' high standards for transparency and accuracy in all its marketing and admissions materials and will continue to do so. Advertising, recruiting, and admissions materials for CDO students were available in the Resource Room during our 2017 MSCHE and MHEC evaluation team visit.

5. Commitment to support

Every teacher is evaluated every day by every student, and those evaluations specifically measure the teachers' effectiveness in distance education. Those evaluations affect teachers' compensation as well as their long-term career prospects with STI.

a) ***Policies for faculty evaluation shall include appropriate consideration of teaching and scholarly activities related to distance education programs.***

Every teacher is evaluated every day by every student, and those evaluations specifically measure the teachers' effectiveness in distance education. Those evaluations affect teachers' compensation as well as their long-term career prospects with STI.

b) ***An institution shall demonstrate a commitment to ongoing support, both financial and technical, and to continuation of a program for a period sufficient to enable students to complete a degree or certificate.***

STI has adequate faculty, infrastructure, and financial resources, as demonstrated in Sections H, J, and K, to maintain the CDO program.

6. Evaluation and assessment

a) ***An institution shall evaluate a distance education program's educational effectiveness, including assessments of student learning outcomes, student retention, student and faculty satisfaction, and cost-effectiveness.***

STI employs a three-level evaluation program completely embedded in the curriculum. The 2018 Middle States Evaluation Team commended this evaluation methodology: "SANS Technology Institute should be commended for the fact that its curriculum automatically embraces learning outcomes and program outcomes." The assessment system and processes are detailed in the evaluation section of this document. This same system will be used in the distance learning component of the CDO program.

b) ***An institution shall demonstrate an evidence-based approach to best online teaching practices.***

STI online teaching practices are currently in use by more than 3,000 students, and at least 50,000 students have used it during the past eight years. Each of those students evaluates the effectiveness of the learning modality in every course, and we continually improve the practices to ensure those ratings continue to match or exceed live classroom training scores.

c) ***An institution shall provide for assessment and documentation of student achievement of learning outcomes in a distance education program.***

Ultimate student achievement in the CDO program will be measured by grades on the internationally standardized GIAC exams for each area of security. We compare these scores in distance and in-person learning modalities. As shown in Table A.4.3, the GIAC test scores in distance learning are essentially identical to scores of students who used live, in-person residential training programs:

Table A.2.3. Comparison of GIAC Exam Score Performance via Live and OnDemand Modalities, 2014–2017

Modality	Overall Score	Master's Program	Certificate Program
Live Class	84.6	86.6	82.4
OnDemand Class	83.7	87.2	82.0

We will continue to monitor GIAC scores in the CDO program, by delivery modality.