xPRO

PROFESSIONAL CERTIFICATE IN CYBERSECURITY

Delivered in collaboration with EMERITUS

Overview

Cyberattacks are becoming more frequent, complex, and targeted, collectively costing organizations billions of dollars every year. This is why cybersecurity is one of the fastest growing industries in the US, as every year more companies and government agencies are seeking to hire cybersecurity professionals with the specialized skills needed to defend mission-critical computer systems, networks, and cloud applications against cyberattacks.

Fighting cybercriminals is a strategic cat-and-mouse game of ever-changing defensive and offensive techniques. It's an exciting career that requires you to think quickly and strategically to ward off data breaches and network takeovers. As a cybersecurity professional, you will be on the front line protecting enterprise IT networks and other critical internet-based information systems against cyberattacks.

The MIT xPRO Professional Certificate in Cybersecurity is an immersive professional certificate that provides a comprehensive introduction to cybersecurity, focused on both the defensive and offensive aspects of the technology. It includes personalized feedback from program leaders, insights from guest speakers, career coaching, mentorship, and the opportunity to create a capstone project on a case study to include in a job portfolio.

MIT xPRO's online learning programs feature exclusive content from world-renowned experts to make learning accessible anytime, anywhere. If you want to accelerate your career or enhance your existing expertise, take the next step and register for the MIT xPRO Professional Certificate in Cybersecurity program.

PRICE
USD 7,450

DURATION
24 weeks
(excluding break weeks)
15–20 hours per week

USD 141,751

The average senior cybersecurity engineer's salary in the U.S.

(Source: salary.com, March 2021)

Program Highlights

Earn a certificate and 36 Continuing Education Units (CEUs) from MIT xPRO

Insights and case studies from renowned MIT faculty

A great foundation towards a degree or certification in cybersecurity

Capstone presentation project to share with potential employers

Services offered by Emeritus

Live weekly office hours with program leaders followed by a Q&A

Personalized feedback, support, career guidance, and network development

Program Experience

20+ hours
of prerecorded
MIT faculty videos

5+ hours
of live mentorship
and career support

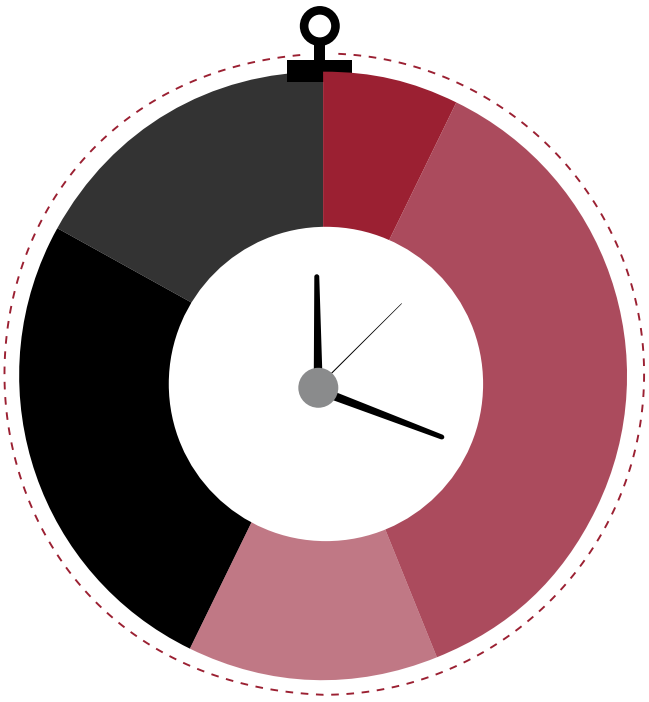
8 hours
of optional career
development activities

19 career
development video
lectures covering
30 career topics

Access to résumé
referrals to Emeritus
employer partners
for up to **6 months**
post–program

Sample Weekly Program Planner

Learners should expect to dedicate a minimum of **15-20 hours** per week to the program.



1-2 hours of recorded video lectures with faculty

10-20 hours of rigorous, graded assignments to apply and reinforce lecture material

2 hours of interaction with program learning facilitators

5-10 hours of self-study and practice exercises

1-5 hours of engaging group discussion with peers to exchange and generate ideas

*Services provided by Emeritus, a learning partner for this program.

Learning Journey

From navigating the enrollment process to identifying job opportunities, we partner with you to take the next step in your career.

LEARNING FACILITATOR

Your learning facilitator will leverage their industry experience and expertise to guide you by holding live sessions, providing assignment feedback, and answering questions.

LEARNING COMMUNITY

Your learning community will provide an interactive environment where you can learn with a group of like-minded individuals and build a global network of peers.

PROGRAM ADVISOR

Your program advisor will be your enrollment resource, answering any pre-program questions and easing your transition into the program.

CAREER COACH

Your career coach will help you successfully navigate your job search by assisting with goal setting, providing feedback on your cover letter, résumé, and LinkedIn profile, and conducting mock interviews. They will be a source of up-to-the-minute information on hiring trends and help celebrate the next step in your career.

Program Frameworks

MITRE ATT&CK®

The MITRE ATT&CK knowledge base is explored deeper in the offensive and defensive aspects of this program. It contains adversary tactics and techniques that are utilized as the foundational development of specific threat models and methodologies.

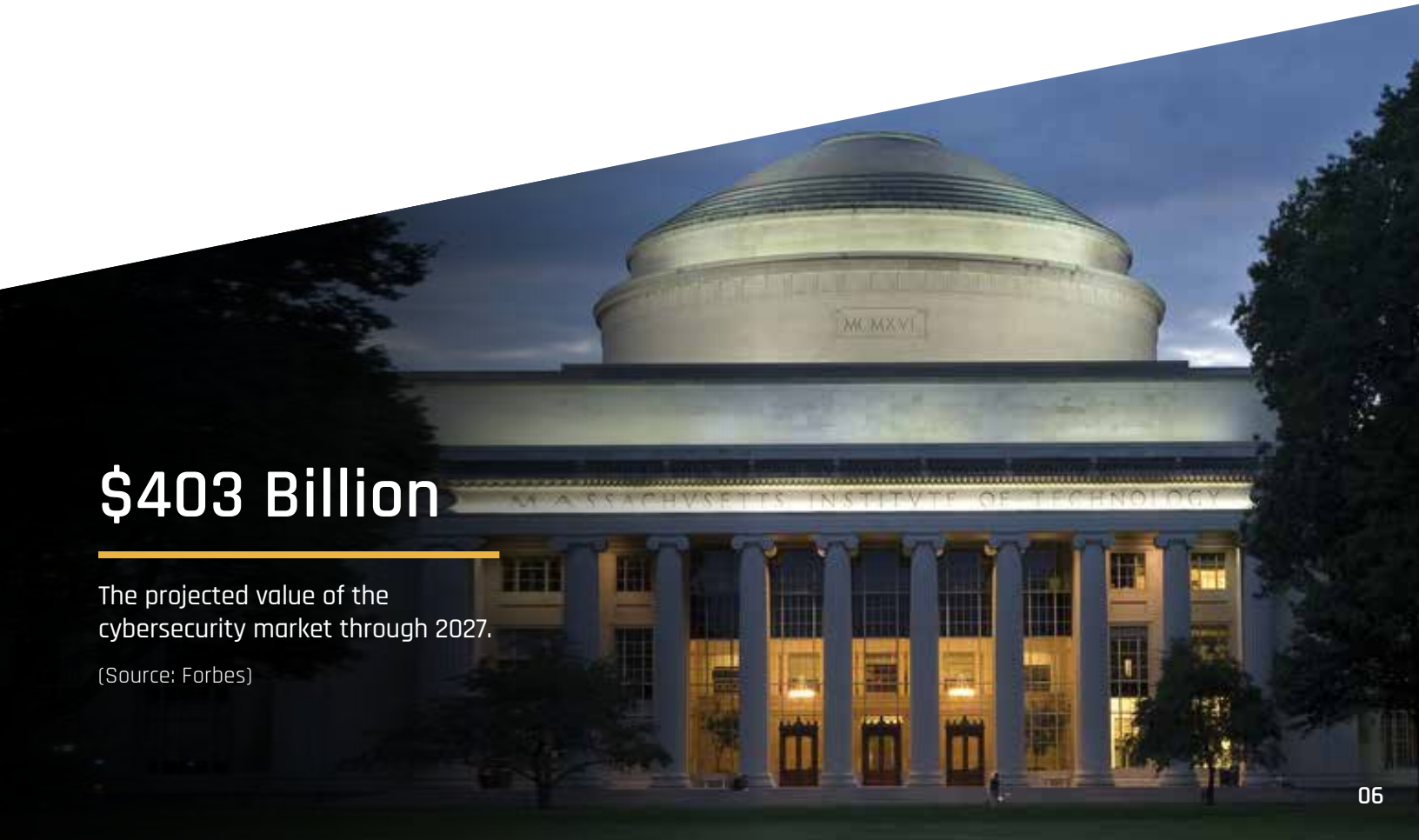
Cloud Security Alliance (CSA)

Cloud Controls Matrix (CCM)

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is discussed in the defensive cybersecurity section. This framework includes domains covering the aspects of cloud technology.

National Institute of Standards and Technology (NIST) Framework

The NIST CSF framework is threaded throughout the entire program as a commonly used framework. It is a widely used cybersecurity framework that encompasses guidelines for organizations to prepare themselves against cybersecurity attacks.



$403 Billion

The projected value of the cybersecurity market through 2027.

(Source: Forbes)

Who Is This Program For ?

Career Launchers: Early-career IT professionals, network engineers, and system administrators wanting to gain a comprehensive overview of cybersecurity and prepare themselves for continued career progression in this high-growth field.

Career Builders: IT project managers and engineers wanting to gain the ability to think critically about the threat landscape including vulnerabilities in cybersecurity, to better understand what kind of cybersecurity to specialize in, and upgrade their own resume for career advancement.

Career Switchers: Mid- or later-career professionals currently working outside of cybersecurity wanting to add critical cybersecurity knowledge and foundational lessons to their resume as they begin considering a career change to an in-demand field.

LAY THE FOUNDATION FOR FUTURE JOB TITLES LIKE:

- System Support Specialist
- Data Support Technician
- Technical Support Specialist
- Help Desk Technician

***Participants must be 18 or above to apply for this program.**

Program Schedule

Whether you are just starting your IT career or expanding into an adjacent field, this comprehensive program prepares you with the conceptual knowledge of both the offensive and defensive aspects of cybersecurity technology. Over the course of this program, you will:

- Apply cybersecurity concepts to real organizations and cyberattack scenarios
- Gather real-world insights from current cybersecurity professionals
- Explore the landscape of various network threats and vulnerabilities, and evaluate responses to each
- Create a digital journal of what you have learned, along with a capstone presentation to share with potential employers

Section 0

Orientation

The first week is an orientation module. You will gain access to the learning platform from the program start date. There is no teaching involved, and all content is pre-recorded.

Section 1

Introduction to Cybersecurity

Key Takeaways

- Explore the basic concepts of computer security systems and their operations
- Explore the threat landscape and break down the types of threats and vulnerabilities
- Identify the key components and sequences of incident response frameworks
- Explore the fundamentals and strategies to protect systems
- Learn how to identify and test vulnerabilities
- Gain knowledge of privacy laws, regulatory agencies and resources, and the types of protection they provide

Week 1: Introduction to Cybersecurity Risk Management

Week 2: Cybersecurity Foundation Concepts

Week 3: Federal Government Role: Law, Operations, and Standards

Week 4: Threats and Vulnerabilities

Week 5: Cybersecurity for Critical Urban Infrastructure

Week 6: Identity and Access Management (IAM) Concepts

Week 7: IAM Layers and Technology

Week 8: Preparing for a Job in Cybersecurity Risk Management

Section 2

Defensive Cybersecurity

Key Takeaways

- Explore the workings of secure communications between computer systems and organizations
- Learn how attacks are identified and how defensive cybersecurity responses are established
- Gain knowledge of the functions, strengths and weaknesses, and administration of Security Operations Center (SOC)
- Identify key components and sequences of incident response frameworks
- Learn how virtualization and the cloud are closely associated

Week 9: Introduction to Defensive Cybersecurity

Week 10: Cryptography

Week 11: Security Operations Center (SOC)

Week 12: Incident Response (IR)

Week 13: Secure Systems Administration

Week 14: Secure Network Administration

Week 15: Cloud Security

Week 16: Preparing for a Job in Cybersecurity Operations

Section 3

Offensive Cybersecurity

Key Takeaways

- Gain knowledge and understanding of how to identify and test vulnerabilities
- Observe simulated cyberattacks on web application security
- Learn to identify malicious activities cultivated by human actions
- Understand privacy policies and how they relate to data governance
- Learn to identify and mitigate risks associated with Operational Technology (OT) and Internet of Things (IoT) devices
- Explore artificial intelligence (AI) techniques and how they relate to the cyber environment

Week 17: Introduction to Offensive Cybersecurity

Week 18: Penetration Testing Part 1

Week 19: Penetration Testing Part 2

Week 20: Social Engineering

Week 21: Artificial Intelligence

Week 22: Policy and Privacy, Regulation, and Data Governance

Week 23: OT and IoT Risk

Week 24: Preparing for a Job in Offensive Cybersecurity Operations

Hands-On Learning

Learn from case studies and apply cybersecurity concepts to real organizations and scenarios.

Explore Cybersecurity Options

Examine different career paths within cybersecurity.

Capstone Project

Throughout the program, you will create a digital journal in which you will record what you have learned in each module. You will create a capstone project, a recorded presentation that demonstrates your cybersecurity knowledge. You will come away from this program with a professional-quality presentation that you can share on LinkedIn or with potential employers.

600,000

The number of unfilled cybersecurity positions in the US in 2022

(Source: Bloomberg)

Career Preparation and Guidance

This program offers a wide array of career support and guidance to help you develop your career path. These services are provided by Emeritus, our learning collaborator for this program, via the Emeritus Career Center (ECC). The primary goal is to help you build the skills needed to prepare for your career, however we do not guarantee job placement. Learn more about all of the services and support available to you, including:

A SUPPORT TEAM YOU CAN RELY ON

Your support team includes program leaders and career coaches who will help you reach your learning goals and guide you through your job search.

CAREER PREPARATION SERVICES THAT GET YOU NOTICED

- Write noteworthy resumes and cover letters
- Create effective LinkedIn profiles
- Navigate your job search
- Prepare for interviews
- Craft your elevator pitch
- Negotiate your salary

Emeritus Career Center

Comprehensive career services. One convenient location.

The Emeritus Career Center is your one-stop shop for streamlined access to career-related services. As a participant in the program, you will gain lifetime access to the ECC and its related benefits, including:

COACHING
Schedule appointments with a career coach, and share details about new jobs and job search outcomes with them.

EVENT ACCESS
Learn about upcoming career events, register to attend, and view previously recorded webinars.

DOCUMENT STORAGE
Store your resume and other application materials in one convenient location.

RESOURCE LIBRARY
Access our growing Resource Library anytime to find job search resources, resume checklists, and other helpful information.

CAREER PROFILE
Create a profile for networking and to provide valuable information to our employer relations team and potential employers.

UNLOCK ADDITIONAL BENEFITS: SHARE YOUR RESUME

Upload your resume to the ECC for approval and take advantage of:

- A resume review and feedback from your career coach.
- Access to the job board, with postings from our employer partners and others seeking talent.
- An easy application process and the ability to track your application steps.
- Inclusion in resume books that our employer relations team will refer to employers.

Emeritus Hiring Partners

Professional Certificate in Cybersecurity is designed to equip you with the in-demand skills that employers seek. The program support team includes dedicated career coaches to guide you through your job search. However, a job placement is not guaranteed.

Over the course of the program, you will gain access to customized recruiting plans developed in collaboration with our hiring partners, connect with hiring managers, obtain personal and industry feedback, and participate in virtual events. Our Employer Partners include:

Our Graduates Work At

Baxter International Inc.	Google (via Vaco)	International Republican Institute
Microsoft	Pyramid Consulting Inc.	Solutions Granted

Faculty

Keri Pearlson

Executive Director of Cybersecurity at MIT Sloan (CAMS): The Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity at the MIT Sloan School of Management

Dr. Pearlson is the executive director of Cybersecurity at MIT Sloan: The Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)3. Pearlson has held positions in academia and industry, including Babson College, The University of Texas at Austin, Gartner's Research Board, CSC, and AT&T. She founded KP Partners, a CIO advisory services organization, and the IT Leaders' Forum, a community of next-generation IT executives. She is the founding director of the Analytics Leadership Consortium at the International Institute of Analytics. She began her career at Hughes Aircraft Company as a systems analyst.

Dr. Pearlson's research spans MIS, business strategy, and organizational design. Her current research studies how organizations build a culture of cybersecurity and how organizations build trust to share mitigations for cyber breaches. Dr. Pearlson holds a doctorate in business administration in MIS from Harvard Business School along with an M.S. in industrial engineering and a B.S. in mathematics from Stanford University. She is the founding president of the Austin Society for Information Management and was named "2014 National SIM Leader of the Year."

Nickolai Zeldovich

Professor of Electrical Engineering and Computer Science, and a member of the Computer Science and Artificial Intelligence Laboratory at MIT

Dr. Zeldovich is a professor of electrical engineering and computer science at MIT and a member of the Computer Science and Artificial Intelligence Laboratory. He received his Ph.D. from Stanford University in 2008. His research interests are in building practical secure systems. Recent projects by Prof. Zeldovich and his students and colleagues include the CryptDB encrypted database, the STACK tool for finding undefined behavior bugs in C programs, the FSCQ formally verified file system, the Algorand cryptocurrency, and the Vuvuzela private messaging system.

Dr. Zeldovich has been involved with several startup companies, including MokaFive (desktop virtualization), PreVeil (end-to-end encryption), and Algorand (cryptocurrency). His work has been recognized with "best paper" awards at the ACM SOSP conference, a Sloan fellowship (2010), an NSF CAREER award (2011), the MIT EECS Spira teaching award (2013), the MIT Edgerton faculty achievement award (2014), the ACM SIGOPS Mark Weiser award (2017), and an MIT EECS Faculty Research Innovation Fellowship (2018).

Danny Weitzner

3Com Founders Principal Research Scientist, Founding Director, MIT Internet Policy Research Initiative, MIT Computer Science and Artificial Intelligence Lab

Prof. Weitzner is founding director of the MIT Internet Policy Research Initiative and principal research scientist at CSAIL. In addition, he teaches internet public policy in MIT's Electrical Engineering and Computer Science Department. His research pioneered the development of accountable systems to enable computational treatment of legal rules.

Prof. Weitzner was U.S. deputy chief technology officer for internet policy in the White House, where he led initiatives on privacy, cybersecurity, copyright, and digital trade policies promoting the free flow of information. He was responsible for the Obama administration's Consumer Privacy Bill of Rights and the OECD Internet Policymaking Principles. He has a law degree from Buffalo Law School, and a B.A. in philosophy from Swarthmore College. His writings have appeared in Science, the Yale Law Review, Communications of the ACM, Washington Post, Wired Magazine, and Social Research.

Stuart Madnick

John Norris Maguire Professor of Information Technologies, Emeritus, Sloan School of Management, Professor of Engineering Systems, School of Engineering and Founding Director, research consortium Cybersecurity at MIT Sloan (CAMS)

Dr. Madnick is the John Norris Maguire Professor of Information Technologies, Emeritus at the MIT Sloan School of Management and the founding director of Cybersecurity at MIT Sloan: the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. His involvement in cybersecurity research goes back to 1979, when he co-authored the book Computer Security. Currently, he heads the Cybersecurity at MIT Sloan Initiative.

Dr. Madnick holds a Ph.D. in computer science from MIT and has been an MIT faculty member since 1972. He served as head of MIT's Information Technologies Group in the Sloan School of Management for more than 20 years. He is the author or co-author of more than 300 books, articles, and reports. Besides cybersecurity, his research interests include big data, semantic connectivity, database technology, software project management, and the strategic use of information technology.

Larry Susskind

Ford Professor of Urban and Environmental Planning, MIT
Vice Chair and Co-founder, Program on Negotiation at Harvard Law School

Prof. Susskind's research interests focus on the theory and practice of negotiation and dispute resolution, the practice of public engagement in local decision-making, cybersecurity for critical urban infrastructure, entrepreneurial negotiation, global environmental treaty-making, the resolution of science-intensive policy disputes, renewable energy policy, water equity in older American cities, climate change adaptation, socially responsible real estate development, and the land claims of Indigenous peoples.

Prof. Susskind is director of the MIT Science Impact Collaborative. He is the founder of the Consensus Building Institute, a Cambridge-based not-for-profit organization that provides mediation services in complex resource management disputes around the world. He is also one of the co-founders of the interuniversity Program on Negotiation at Harvard Law School where he now directs the MIT-Harvard Public Disputes Program, serves as vice chair for instruction, and leads PON's Master Classes in Negotiation. He is the recipient of ACSP's prestigious Educator of the Year Award and recipient of MIT's Award for Digital Instruction.

Una-May O'Reilly

Principal Research Scientist and Leader of ALFA Group at MIT-CSAIL

Dr. O'Reilly's research group, AnyScale Learning for All, develops new, data-driven analyses of online coding courses, deep learning techniques for program representations, adversarial attacks on machine learning models, model training for adversarial robustness, and cyber hunting tools and cyber arms race models.

One of the main areas Dr. O'Reilly is investigating is cybersecurity and how to stop destructive and escalating arms races. She hopes to understand the nature of adversarial intelligence by computationally replicating it—that is, by developing "artificial adversarial intelligence." This helps reveal the dynamics of conflicting behavior and how adaptation drives it, so that these types of arms races can be stopped. Dr. O'Reilly holds a Ph.D. from Carleton University in Ottawa, Canada.

Barbara Johnson

Senior Security Consultant, Security Certification Educator, Lecturer at MIT Sloan School of Management, Education: BSISE, MBA, $(ISC)^2$ Certifications: CISSP and ISSMP, ISACA Certifications: CISA, CISM, CRISC, CDPSE, Business Continuity Certifications: CBCP and MBCI

Securing information systems is Barbara's purpose and educating security professionals is her passion.

Barbara Johnson is a Senior Security, Audit and Compliance Management Consultant with over 20 years of experience. She designs and manages information security programs for the government, automotive, entertainment, financial, and travel sectors. Her security, privacy, risk, and audit frameworks include ISO 27001, ISACA COBIT, NIST, HIPAA, and PCI. She brings global best practices into her client's enterprise security governance, policies, standards, architecture, and operations, including cryptography, incident response, and business continuity, and disaster recovery. However, she tailors a security strategy to a client's industry and risk appetite.

Barbara enhances educational delivery as a security, audit, and compliance practitioner. Barbara is a lecturer at MIT Sloan School of Management and a courseware developer for the MIT xPro Cyber Program. For $(ISC)^2$ CISSP and ISSMP: she develops courseware, teaches as a senior and lead instructor, speaks at Security Congress, and was Chair of $(ISC)^2$ Common Body of Knowledge. Furthermore, she imparts ISACA global best practices through its CISA, CISM, and CRISC certification classes. As a security educator, she has readied thousands of security professionals for certification exams.

Rajiv Shridhar

Information Security Officer and Director of Research Computing, MIT Sloan School of Management

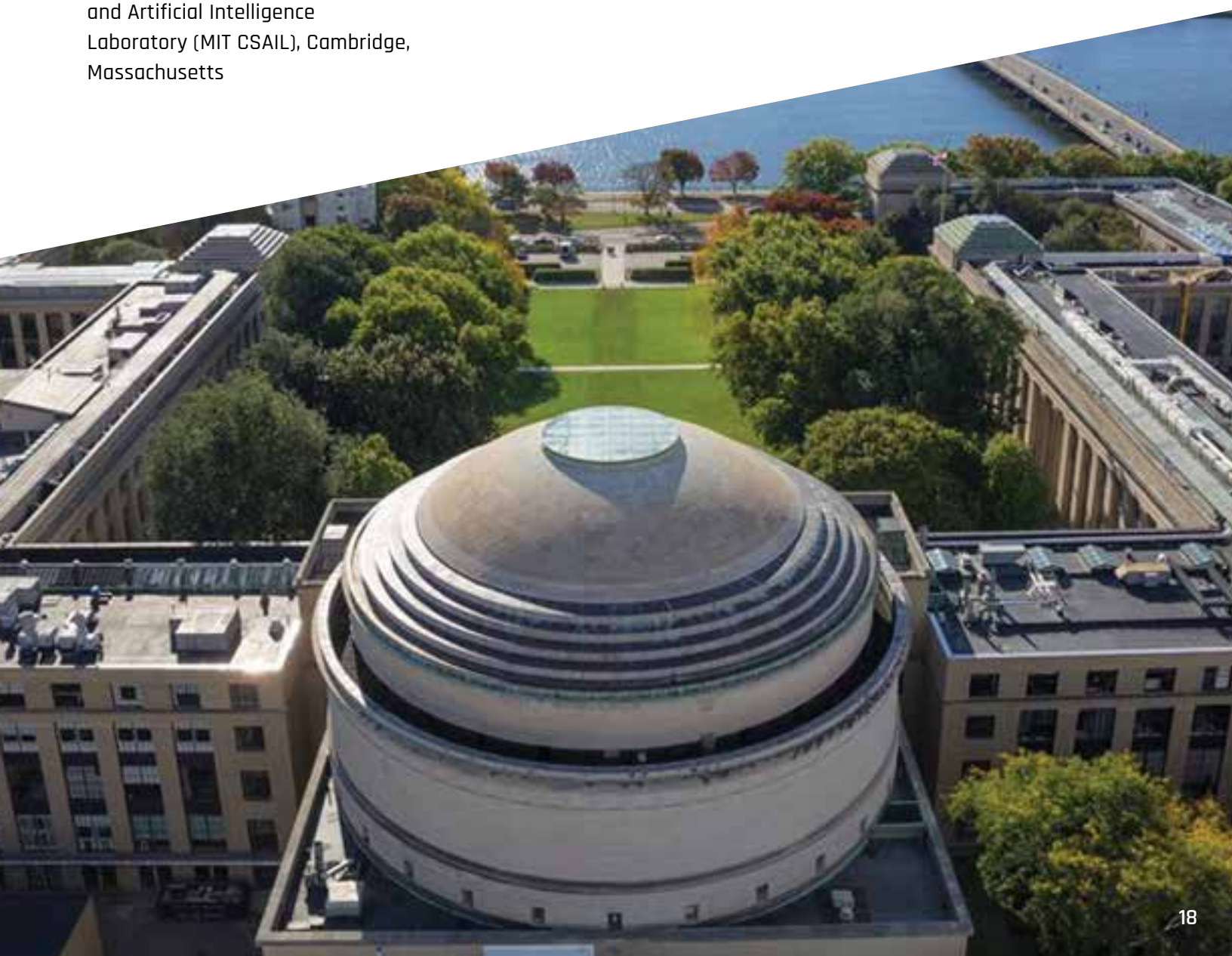
Rajiv Shridhar is the Information Security Officer and Director of Research Computing at MIT Sloan School of Management. He leads the team that enables the research of MIT Sloan faculty, students and collaborators by providing specialized computing infrastructure, datasets, software tools, support and technology consulting. As Information Security Officer, he is responsible for the development and oversight of risk and security frameworks in alignment with the information security needs of MIT Sloan.

Rajiv is a senior lecturer at Northeastern University, where he teaches graduate level programs in computer engineering, cyber physical systems and telecommunication networks. In his teaching, he seeks to maximize student learning outcomes by reinforcing and extending in-class learning with experiential education via extensive hands-on projects, labs, and assignments. Rajiv received an M.S. in Computer Systems Engineering from Northeastern University.

Howard Shrobe is a Principal Research Scientist at the Massachusetts Institute of Technology (MIT) Computer Science and Artificial Intelligence Laboratory (MIT CSAIL), Cambridge, MA. He is a former Associate Director of CSAIL and former Director of CSAIL's Cybersecurity@ CSAIL initiative. His research interests include AI, cybersecurity (particularly of control systems), and new computer architectures for inherently secure computing. Howard has a Ph.D. from MIT.

Howard Shrobe

Principal Research Scientist at the Massachusetts Institute of Technology (MIT) Computer Science and Artificial Intelligence Laboratory (MIT CSAIL), Cambridge, Massachusetts



Guest Speakers

Guest speakers comment on their career paths, advice for entry level learners, various cybersecurity issues, and themes that arise in their professional roles.

Caren Shiozaki

EVP-CIO for TMST, Inc., Santa Fe, New Mexico,
Vice Chair for SIM and Founder of the SIM Cybersecurity SIG

Caren Shiozaki is EVP-CIO for TMST, Inc., a mortgage organization in Santa Fe, New Mexico. She is also a Senior Fellow with the DivIHN Center of Excellence for digital security and risk. Previously she was CIO for a Dallas-based media organization. She has worked internationally for Bank of America and American Express. Caren is Chair Emeritus for SIM's National Board and co-founder of the national Digital Risk SIG. She is board chair for the Santa Fe Alliance for Science and the Santa Fe Animal Shelter. She holds professional certifications in corporate governance and data privacy and is a certified e-discovery specialist. She holds a degree in genetics from UC Berkeley.

Erica Wilson

CISO for Cass Information Systems

Erica Wilson has over 20 years of IT experience, 18 of which are in the field of cybersecurity. Erica currently serves as the CISO for Cass Information Systems. She has responsibility for all aspects of the company's cybersecurity program, including security strategy, policies and procedures, technologies, and training. In addition, Erica leads all aspects of technology risk management, including compliance with internal and regulatory controls as well as the Business Continuity Program. Erica also has a passion for STEM education. Throughout her professional career, she has consistently identified ways to influence and encourage others in the community to explore opportunities to work in the field of information technology and cybersecurity. In this program.

Ion Santotomas

Lead Security Analyst at Schneider Electric

Ion is a diligent senior cybersecurity professional with a strong technical background in systems engineering and infrastructure management. Ion is passionate about both offensive and defensive aspects of cybersecurity and actively participates in events, conferences, and online challenges to sharpen his technical skills and knowledge about the latest trends and attack vectors in order to become a better defender.

Daniel Gorecki

Group Information Security Manager and CISO at Ascot Group

Daniel Gorecki is a Group Information Security Manager and CISO at Ascot Group. In this role he manages a global team for information risk management and cyber resiliency for the global organization. Prior to joining Ascot Group, he was the CISO at Aramark and held the CISO and CIO roles at Intercept Pharmaceuticals. Dan maintains the certification for Certified Information Systems Security Professional (CISSP), Certified Data Privacy Solutions Engineer (CDPSE), has completed SIM's Regional Leadership Forum for IT Executives, and holds a B.E. in Computer Engineering from Stony Brook University.

Josh Schwartz

Senior Director of Technical Security for The Paranoids, the Information Security Team at Yahoo

Josh Schwartz is the Senior Director of Technical Security for The Paranoids, the information security team at Yahoo, where he oversees an organization focused on offensive security assessments, red team methodology, and building products that support security culture and behavioral change initiatives.

Matthew Lange

Assistant Director of the Adversarial Security Testing team at Northwestern Mutual

Matt Lange is currently the Assistant Director of the Adversarial Security Testing team at Northwestern Mutual where he leads a team of offensive security professionals accountable for penetration testing, red teaming, and purple teaming. He began his career in cybersecurity as an incident responder and forensic analyst. He quickly transitioned to penetration testing and red teaming where he helped build those programs from scratch. Matt graduated from the University of Wisconsin where he double majored in Mandarin Chinese and East Asian Politics, as well as Milwaukee Area Technical College where he received a degree in Information Systems Security and is an active member of its IT Security advisory board.

Keri Chisolm

Cybersecurity Advisor for FedEx Services

Keri Chisolm has been working in Information Security for over 20 years. She began her security career as a staff member at the Center for Computer Security Research with the Computer Science and Engineering Department at Mississippi State University. As the security program at Mississippi State University grew, she also worked with the National Forensics Training Center and the Critical Infrastructure Protection Center. In addition to these roles, she also served as the systems administrator for the department where she supported numerous educational, production, and research systems. Later she joined the Information Security Team at FedEx where she worked for 3 years in Identity and Access Management with a particular focus on federated identities. In her current role with FedEx, she has joined the Cloud Security team with a focus on securing large IaaS and PaaS cloud offerings. Keri has earned her CISSP and CCSK certifications as well as multiple platform specific certifications. In her free time, she enjoys traveling, studying history, spending time with family, and attending sporting events.

Participant Testimonials

"The content presented by the professors was the best part of the program for me. It's all relevant to what we are currently facing, and it can be applied to any organization."

Euclides Garcia

Global IT Director, Infrastructure and Security, Del Monte Fresh Produce

"The availability and accessibility of the program were the best parts. I loved being able to do the course at any time during the week rather than set times. The material was very informative and helped strengthen my skills in the field."

Allison Hamm

SOC Analyst, Solutions Granted Inc.

"The topics on cryptography and penetration testing were the best parts of the program for me. These are the areas that I lacked confidence in, and this program has given me the baseline knowledge to advance to the next stage in my career."

Mark Hughes

Integration Manager, QTS Global

"The vast number of case studies gave me a more in-depth view into cybersecurity and its risks."

Berndt Pilgram

Principal Lead of IT Systems and Data Science, Infineon Technologies

"The program roadmap was the best part of the program for me because the lessons were structured in a way that made learning each week's lessons interconnected to each other in an intuitive way."

Richard Napalan

FC Associate, Amazon

Financing Options

We want to make sure that the Professional Certificate in Cybersecurity is an affordable option for all. This is why we offer you many different ways to pay for the program.

Loan Partners (For US Residents)

Climb Credit	Immediate repayment, interest-only repayment, and deferred payment options are available.

- Visit the Climb Credit application portal
- Fill in your basic details and proceed to the loan section of the application
- Select 'Emeritus/MIT xPRO' under the Campus dropdown, 'Professional Certificate in Cybersecurity' from the Program dropdown, and enter your program start date
- Choose your preferred repayment option and enter financial information
- Agree to the disclosure and submit your application
- Our program advisors will contact you for a confirmation on your loan application
- After confirmation, we will certify your loan. You will receive a welcome email with login instructions from notifications@instructure.com within 3 business days

Sallie Mae	Fixed repayment, interest-only repayment, and deferred payment options are available.

- Visit the Sallie Mae application portal
- Fill in your basic details and proceed to the loan application page.
- At the time of loan application, please select '**Student and Career Training School**' when prompted
- Choose from fixed repayment, interest-only repayment, and deferred payment options and submit your application
- Our program advisors will contact you for a confirmation on your loan application*
- After confirmation, we will certify your loan. You will receive a welcome email with login instructions from notifications@instructure.com within 3 business days

Ascent Funding	Immediate repayment, interest-only repayment, and deferred payment options are available.

- Visit the Ascent Funding application portal
- Enter your email address and select the 'Professional Certificate in Cybersecurity' option from the dropdown list
- Choose from immediate repayment, interest-only repayment, and deferred payment options and submit your application
- Our program advisors will contact you with a confirmation on your loan application*
- After confirmation, we will certify your loan and you will sign the final disclosures.
- You will then receive a welcome email with login instructions from notifications@instructure.com within 3 business days

Financing options also available exclusively for UK residents

Flexible Payment Options (For All Countries)

- Choose to make your payment in two, three, or six installments for higher flexibility.
- Complete your application for the Professional Certificate in Cybersecurity and enroll for the program.

You can opt for any one of the financing options to cover up to the full cost of the program tuition. If you are considering financing your program through one of our partners, the enrollment process can only be completed with the assistance of your program advisor or by calling +1 315 756 6926.

*Due to processing time, the loan application should be submitted no later than four business days prior to the enrollment deadline.

Certificate

Get recognized! Upon successful completion of this program, MIT xPRO grants a certificate of completion to participants and 36 Continuing Education Units (CEUs). This program is graded as a pass or fail; participants must receive 75% to pass and obtain the certificate of completion.

After successful completion of the program, your verified digital certificate will be emailed to you, at no additional cost, with the name you used when registering for the program. All certificate images are for illustrative purposes only and may be subject to change at the discretion of MIT.

About MIT xPRO

MIT xPRO's online learning programs leverage vetted content from world-renowned experts to make learning accessible anytime, anywhere. Designed using cutting-edge research in the neuroscience of learning, MIT xPRO programs are application focused, helping professionals build their skills on the job. To explore the full catalog of MIT xPRO programs, visit: xpro.mit.edu.

About Emeritus

MIT xPRO is collaborating with online education provider Emeritus to deliver this online program through a dynamic, interactive, digital learning platform. This program leverages MIT xPRO's thought leadership in engineering and management practice developed over years of research, teaching, and practice.

Easily schedule a call with a program advisor from Emeritus to learn more about this MIT xPRO program.

SCHEDULE A CALL

You can apply for the program here

APPLY

CONNECT WITH A PROGRAM ADVISOR

Email: mit@emeritus.org

Phone: US: +1 315 756 6926
UK: +44 192 824 1403
SG: +65 3129 4023

MIT xPRO

Delivered in collaboration with

EMERITUS