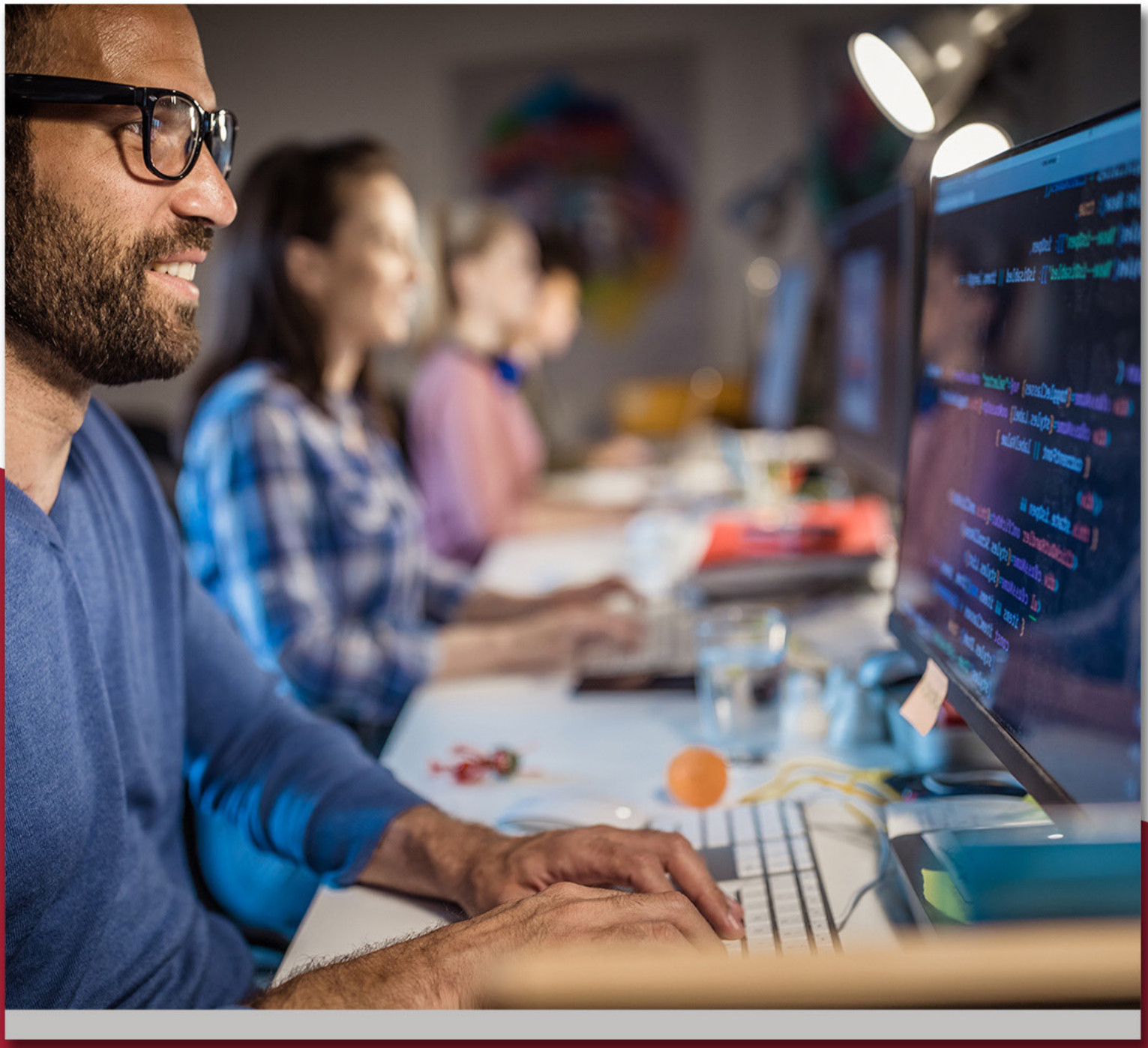


MIT | xPRO

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 U.S. as every year more companies and government agencies are seeking to hire cybersecurity engineers with the specialized technical skills needed to defend mission-critical computer systems, networks, cloud applications, and more 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 engineering specialist, you will be on the front line of 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 course leaders, insights from guest speakers, career coaching, mentorship, and the opportunity to create a capstone network development project for 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 with new skills or enhance your existing expertise, take the next step and register for the MIT xPRO Professional Certificate in Cybersecurity program.

PRICE

USD 6,950

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 from MIT xPRO to recognize your skills and success

Insights and case studies from renowned MIT faculty

Market-ready cybersecurity skills in a high-growth market

Capstone presentation project to share with potential employers

Develop a strong foundation for industry certifications such as CompTIASecurity and CISSP

Services offered by Emeritus

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

Personalized feedback, support, career guidance, and network development

Program Frameworks

National Institute of Standards and Technology (NIST) Framework

The NIST framework is a widely used cybersecurity framework that encompasses guidelines for organizations to prepare themselves against cybersecurity attacks.

Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

The CSA Cloud Controls Matrix framework includes domains covering the aspects of cloud technology.

MITRE ATT&CK®

The MITRE ATT&CK® knowledge base contains adversary tactics and techniques which are utilized as the foundational development of specific threat models and methodologies.

15%

The projected annual growth rate for the cybersecurity market through 2026.

(Source: Modor Intelligence, 2020)

Who Is This Program For ?

Career Launchers: Early-career IT professionals, network engineers, and systems administrators wanting to specialize in cybersecurity as a way to move up in a high-growth field with high-demand job opportunities.

Career Builders: IT project managers and engineers who want to improve their organization's preparedness and response against cyberattacks and grow their career as leaders in cybersecurity strategies.

Career Switchers: Mid- or later-career IT professionals looking to switch to cybersecurity as a specialty to refresh their career and take advantage of the demand for cybersecurity talent in marketing, sales, human resources, operations, or any other field.

PREPARE FOR THESE POTENTIAL JOB TITLES

- Cybersecurity Engineer
- Cybersecurity Specialist
- Information Security Engineer

Program Schedule

Whether you are just starting your IT career or expanding into a new specialty, this comprehensive program will prepare you with the skills needed to excel in both the offensive and defensive aspects of cybersecurity technology. Through the course of this program, you will:

- Apply cybersecurity concepts to real organizations and cyberattack scenarios
- Utilize 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 the content is pre-recorded.

Section 1

Introduction to Cybersecurity

Key Takeaways

- Explore the basic concepts of a computer security system 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 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 working 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 SOCs
- Identify key components and sequences of incident response frameworks
- Learn how virtualization and the cloud are closely associated

Week 9: Introduction to Defense and Network Administration

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
- See 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 as 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.

Industry-Valued Certifications

Gain a strong foundation for industry certifications such as CompTIASecurity and CISSP.

Capstone Project

Throughout the course, you will work to create a digital journal in which you will record what you have learned in each course module. You will use the journal to create a capstone project, a recorded presentation that demonstrates your cybersecurity skills which qualify you for opportunities as a cybersecurity engineering specialist. You will come away from this course with a professional-quality presentation that you can share on LinkedIn or with potential employers.

338K+

There were 338,576 unique job postings in the U.S. requiring cybersecurity as a skill between March 2020 and March 2021.

(Source: EMSI Data, 2021)

Career Preparation and Guidance

Stepping into a career in cybersecurity engineering requires a variety of skills, both hard and soft. This course guides you in navigating a career path into tech, including crafting your elevator pitch and communication tips. These services are provided by Emeritus, our learning collaborator for this program. The program support team includes course leaders who help you reach your learning goals and career coaches to guide you through your job search. The primary goal is to give you the skills needed to be prepared for a job in this field, however, job placement is not guaranteed.

Emeritus provides the following career preparation services:

- Crafting your elevator pitch
- Navigating your job search
- LinkedIn profile guidance
- Interview tips and preparation
- Resume/cover letters
- Negotiating salary

Career exercises focused on launching a career in cybersecurity include:

- Job search and interviewing for cybersecurity positions
- Communicating cybersecurity concepts through presentation skills
- Building your personal brand and promoting your skills

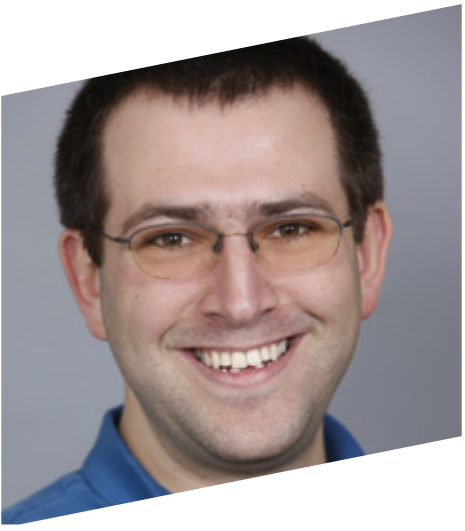
Faculty

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 firm 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.

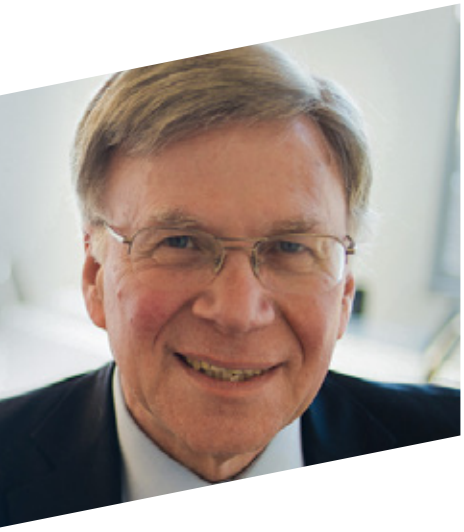
Dr. Zeldovich has been involved with several startup companies, including MokaFive (desktop virtualization), PreVeil (end-to-end encryption), and Algorand (cryptocurrency). His work has been recognized with "best paper" awards at the ACM SOSP conference, a Sloan fellowship (2010), an NSF CAREER award (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.

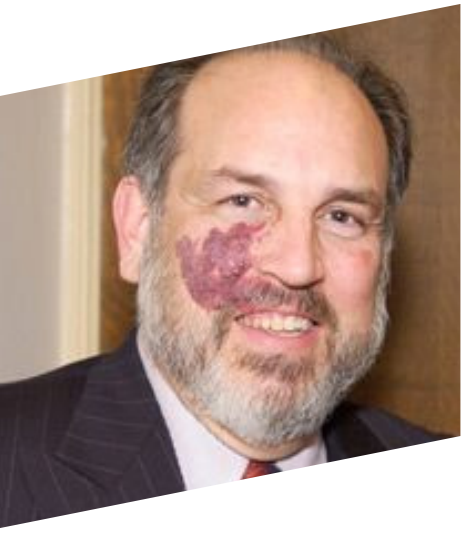


Stuart Madnick

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 founder of the Consensus Building Institute, a Cambridge-based not-for-profit company that provides mediation services in complex resource management disputes around the world. He also was 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-SAIL

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 will help reveal the dynamics of conflicting behavior and how adaptation drives it, so that we can put a stop to these types of arms races. 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 and standards, architecture, and operations, inclusive of 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 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, data sets, 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 courses 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 MS 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 PhD from MIT.

Howard Shrobe

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

Guest Speakers

Caren Shiozaki

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

Caren Shiozaki is EVP-CIO for TMST, Inc, a mortgage company 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 company. 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 certification in corporate governance, 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 & 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 information technology and cybersecurity.

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, to be a better defender.

Daniel Gorecki

Group Information Security Manager & CISO at Ascot Group

Daniel Gorecki is a Group Information Security Manager & 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

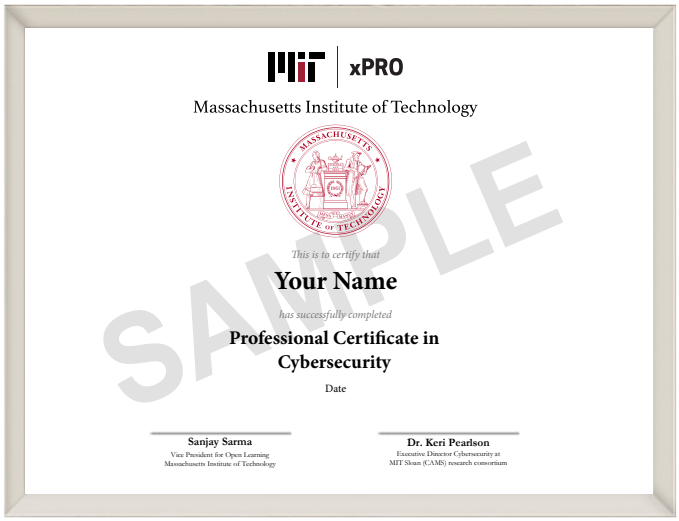
Senior Director of Technical Security for The Paranoid, the Information Security Team at Yahoo

Josh Schwartz is a 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.

Certificate

Get recognized! Upon successful completion of this program, MIT xPRO grants a certificate of completion to participants. 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 courses and programs, visit: xpro.mit.edu.

About Emeritus

MIT xPRO is collaborating with online education provider Emeritus to deliver this online course through a dynamic, interactive, digital learning platform. This course 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: +1-617-855-1045

MIT xPRO

Delivered in collaboration with

EMERITUS