Cybersecurity & CISSP®

Category and Courses Marketing Kit

Learn to protect your business. Or learn your way into a growing field.

MINDEDGE LEARNING

www.mindedge.com

Contents

I. Course Summary Descriptions

Cybersecurity & CISSP®

As more businesses migrate their data and services online, the need for cybersecurity training is greater than ever. MindEdge offers a range of introductory to advanced training for IT professionals. These courses cover topics from Cloud data security to cryptography, malware to risk management, and everything in between.

Certificate in Cybersecurity

Cybersecurity, also known as Information Security, is the protection of data and personally identifiable information from malicious attacks, theft, and destruction. Failures of cybersecurity policies, both in large corporations and governmental agencies, have earned significant visibility and negative publicity in recent months and years. As the amount of data being stored continues to increase, and as hackers become more sophisticated, the need for cybersecurity is greater than ever.

Learner Satisfaction: 97%
Estimated length: 40 hours
Access Time: 365 days
Credits: 4 CEUs

Real-World Cloud Cybersecurity Scenarios

This suite of five related courses covers various aspects of securing cloud services. Its structure is based on the Certified Cloud Security Professional (CCSP) certification administered jointly by the Cloud Security Alliance and (ISC)2. Each course is comprised of two modules. The first provides content related to the course subject matter. The second module engages the learner with real-world scenarios in which he or she must apply the content of the first module. This bundle is designed for adult learners who are interested in gaining an introduction to information technology security. Some understanding of basic IT concepts is helpful. Individual courses included in this bundle are listed below.

Learner Satisfaction: 97%
Estimated length: 25 hours
Access Time: 90 days
Credits: 2.5 CEUs

Real-World Cybersecurity Scenarios

What would you do in the face of an actual information security problem? These courses each include a module devoted to fictional scenarios, based on real-world challenges that cybersecurity professionals face. Each course is self-paced and contains interactive games, real-world examples, expert videos, quizzes, assessments, and focused instruction. Each of the courses in this bundle helps refine and enhance the skills that cybersecurity and IT professionals need. The concepts and principles covered focus attention on the needs of the expanding computer information security industry. This bundle is designed for adult learners who are interested in gaining an introduction to information technology security. Some understanding of basic IT concepts is helpful. Individual courses included in this bundle are listed below.

Learner Satisfaction: 98%
Estimated length: 30 hours
Access Time: 365 days
Credits: 3 CEUs

Access Control and Identity Management Scenarios

Access control is the restriction of access to a computer system. So how does a cybersecurity professional manage this access control? This course introduces the principles of access controls, beginning with the central modes of information security and continuing through various attacks and defenses. It provides an overview of Identity Management and the resources used on modern-day information systems, including Web and cloud-based ones. This course also features a number of fictional scenarios based on access control and identity management that professionals face in the real-world.

Learner Satisfaction: 96%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

A Manager's Guide to Cloud Computing and Cybersecurity

This course provides an overview of cloud computing and the business and security considerations of transitioning to a cloud environment or from one cloud service provider to another. The course is presented in two modules. In addition to providing information that aligns with industry standard content from the Cloud Security Alliance, this course also includes a module that presents different real-world scenarios to learners, asking them to apply what they have learned to situations they might encounter in the workplace.

Learner Satisfaction: 86%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Application, Data, and Host Security Scenarios

When you download an app, or access a database, you want to trust that the software engineer who developed the app had an eye toward security. This course covers the security of applications, data, and hosts in information systems. It provides a comprehensive examination of software development and change management. This course also features a number of fictional scenarios based on real-world application, data, and host security. Although not required, having some experience or working knowledge in IT concepts is helpful in taking this course.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Application Development for Cloud Computing

This course is intended to provide professionals who have some technical experience an overview of the application development process, how it applies to cloud computing, and the prevalent security concerns related to today's applications. It is not a software engineering course and does not require any programming knowledge. The content of this course covers much of the Application Security domain developed by the (ISC)2 and Cloud Security Alliance as part of the Cloud Computing Security Practitioner (CCSP) exam and certification. Further, the course also incorporates content that may be found on the CompTIA Cloud+ exam. As such, it should serve as useful preparation for anyone pursuing these certifications.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Asset Security

Companies must protect their assets. Just as locks go on the doors to protect physical assets, electronic and data assets must also be guarded. Asset security involves the full support of everyone in an organization, from corporate-level personnel down to front-line employees. Various security controls will be described that help protect privacy, along with data leakage prevention (DLP). Although it is not necessary, having some foundation in IT concepts is helpful in taking this course.

Learner Satisfaction: 95%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

CISSP® Exam Prep Course

The CISSP® Exam Prep Course prepares test-takers for the Certified Information Systems Security Professional exam, as administered by the International Information System Security Certification Consortium (ISC)2. The CISSP® certification is recognized worldwide and adheres to the strict standards of ISO/IEC 17024. As security breaches outpace the available pool of security experts, the need for information security professionals with proper certifications will continue to grow. Among other titles, obtaining the CISSP® certification prepares one for a position as a Security Analyst, Chief Information Security Officer, or as a Security Architect.

Learner Satisfaction: 97%
Estimated length: 40 hours
Access Time: 180 days
Credits: 4 CEUs

CISSP® Practice Exams and Exam Strategies

This course is designed to give learners an assessment of their readiness to take ISC2's CISSP® Exam. It contains two 120-question practice exams, which cover The International Information System Security Certification Consortium's eight domains.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Cloud Data Security

This course is comprised of two modules. The first addresses many of the important concepts of cloud-based data and the security responsibilities of both cloud consumers and cloud service providers. The second module offers a series of scenarios that relate to cloud data security to ensure you have mastered the material.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Cloud Infrastructure and Platform Security

This course is comprised of two modules. The first addresses many of the challenges for both cloud consumers and cloud service providers in securing the infrastructure and platforms used in cloud computing. The second module offers a series of real-world scenarios designed to give learners a sense for how the concepts might be applied in their everyday work. This course is designed for IT professionals and other adult learners who have some knowledge of internet-related technology.

Learner Satisfaction: 93%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Cloud Operations Security

This course begins by covering security issues with regard to operating cloud services. While it covers many aspects relevant to a cloud service provider, it should be particularly valuable to helping cloud consumers understand how security responsibilities may be divided between consumer and provider. The second module engages the learner with real-world scenarios that represent the challenges to securing cloud operations. This course is designed for IT professionals and other adult learners who have some knowledge of internet-related technology.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Communication and Network Security

This course covers topics related to communications and network security. It begins with a lesson in the different types of networks and different transmission technologies. It also covers the two main models that govern how networks work: the OSI model and the TCP/IP model, as well as their related layers. The course includes a detailed discussion of the many protocols that allow networks and network devices to communicate with one another and includes a discussion of firewalls and wireless networks. This course is designed for IT professionals and other adult learners who are interested in gaining an introduction to information technology security.

Learner Satisfaction: 97%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Compliance and Operational Security Scenarios

This course contains a discussion of the role of security governance and risk management in information security. It looks at the policies and standards that are needed to operate an effective information security function and to oversee good information security practices. This course also features a number of fictional scenarios based on compliance and operational security to allow you to practice the concepts learned in the material. This course requires some basic understanding of IT concepts.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

CompTIA Security+® Exam Prep Course

The CompTIA Security+ Exam Prep Course prepares test-takers for the Security+ exam, as administered by CompTIA. The CompTIA certification is recognized worldwide and adheres to the strict standards of ISO/IEC 17024 and is approved by the US Department of Defense to meet directive 8140/8570.01-M requirements. The course contains a variety of content presentation methods to help teach the concepts and vocabulary, and ultimately, learners are given ample opportunity to assess their skills with a multiple choice practice exam.

Estimated length: 30 hours
Access Time: 180 days
Credits: 3 CEUs

Cryptography Scenarios

This course contains an introduction to the key concepts of cryptography and security engineering. It examines the role of encryption in information security and considers common encryption methods. This course also features a number of fictional scenarios based on cryptography to help you apply the concepts to situations you may see in the real world. This course requires some basic understanding of IT concepts.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Cybersecurity for Healthcare Professionals

In this course, managers are introduced to essential information security principles and concepts. These concepts are critically important in the healthcare sector as a data breach can have far-reaching consequences for individuals and organizations. Beyond financial losses and the embarrassment of having personal information exposed online, a security breach in healthcare can result in a patient becoming seriously injured or killed.

This course is designed to help managers navigate crucial cybersecurity concepts as applied to HITECH and HIPAA-covered entities. Learners will explore the reasons why breaches occur, the motivation of attackers, and how to protect Personal Health Information (PHI) while it is in use, in storage, and in transit across a network.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Fundamentals of Application Security

The assignments in this course introduce many of the concepts of application development and the security issues that relate to them. The course covers various software development models and considerations and introduces learners to basic security concepts such a cryptography and the common vulnerabilities and exposures list. In this material, we will also introduce the basic concepts of cybersecurity, including cryptography, and illustrate how the many vulnerabilities found in applications today can trace their origin to some point in the development process. While this is not a "coding" course, it provides examples of coding techniques and explores and contrasts the many different models of software development. Ultimately, this content should prove valuable to managers, developers, and security professionals who are looking for a comprehensive understanding of how the many components of the application creation process come together under an umbrella of security.

Learner Satisfaction: 100%
Estimated length: 3 hours
Access Time: 90 days
Credits: 0.3 CEUs

Identity and Access Management

This course introduces students to the principles of access controls, beginning with the central modes of information security and continuing through various attacks and defenses. The course presents different kinds of authentication techniques, how they work, and how they are distinguished from each other. This course requires some basic understanding of IT concepts.

Learner Satisfaction: 98%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Introduction to Cybersecurity

Globally, incidents of data breaches, identity thefts, and cybercrimes are on the rise, along with the explosive growth of online personal data and the expansion of computer networks. This course teaches the fundamental concepts of information security one will encounter in the cybersecurity field. This course will set the groundwork with basic vocabulary and then introduces concepts such as access controls, risk management, cyber attacks, and digital forensics. This course requires a basic understanding of IT concepts.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Introduction to IT Governance, Risk, and Compliance

As organizations become increasingly globalized and as legal environments quickly evolve, the importance of governance, risk management, and compliance continues to gain in importance. Regulatory compliance forces organizations to better manage their data as noncompliance can lead to penalties, fines, and worse. With the proper governance and risk management structures in place, an organization can better manage data and risk to improve business outcomes while adhering to regulations. This course is designed for IT professionals and other adult learners who are interested in furthering their knowledge of governance, risk management, and compliance as these relate to information technology.

Learner Satisfaction: 100%
Estimated length: 7 hours
Access Time: 90 days
Credits: 0.7 CEUs

Introduction to Malware

Malicious software, better known as malware, has become a central element in not just cybersecurity but daily life. It has played a role in everything from our politics to our economy, to our personal lives. However, it remains a poorly understood and reported subject. This course provides a clear and comprehensive introduction to malware and how to defend against it. Instruction is divided into two modules. The first provides an overview of the history and mechanisms of malware. The second module offers a series of real-world scenarios in which the learner must apply several of the concepts covered in the first module.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Network Security Scenarios

This course examines communications and network security. It covers the different types of networks and different transmission technologies and the two main models that govern how networks work, the OSI model and the TCP/IP model, and their related layers. This course also features a number of fictional scenarios that will help you apply what you've learned to situations you may encounter in the real world. This course requires a basic understanding of IT concepts.

Learner Satisfaction: 93%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Security and Risk Management

This course covers the role of governance and risk management in information security. It looks at the policies and standards that are needed to operate an effective information security function and to oversee good information security practices. The course also includes a look at how modern organizations manage information security risks and how to conduct a risk analysis. It concludes by examining the process for providing information security training and education. This course requires some basic understanding of IT concepts.

Learner Satisfaction: 97%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Security Assessment and Testing

This course covers security assessment and testing, focusing on potential disruptions that can affect organizations and how they can be addressed with assessments and plans. Students will have the opportunity to practice how to assess the impact of disasters that may arise as well as to develop their own versions of these plans. This course requires a basic understanding of IT concepts.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Security Engineering

This course contains an introduction to the key concepts of cryptography and security engineering. It examines the role of encryption in information security and considers common encryption methods. In addition, the course discusses ciphers, their substitutes, and how they work. Public key infrastructure and management is also covered. This course requires a basic understanding of IT concepts.

Learner Satisfaction: 98%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Security Operations

This course contains a detailed overview of security operations: administrative controls, trusted recovery and change and incident management. This course establishes a foundation in auditing, monitoring and detection in information security. This course requires a basic understanding of IT concepts.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Software Development Security

This course covers software development security while focusing on the systems development life cycle, operating systems, and their environments. Additional topics include the role of various databases in security and how to recognize and guard against attacks on software. Students will have the opportunity to apply application security controls. This course requires a basic understanding of IT concepts.

Learner Satisfaction: 94%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

Threats and Vulnerabilities Scenarios

This course examines the process of identifying and mitigating threats and vulnerabilities in information systems. It covers common categories of threats and vulnerabilities and the resources used to detect them. This course also features a number of fictional scenarios based on threats and vulnerabilities. This course is designed for IT professionals and other adult learners who are interested in information technology security, with an eye towards handling real-world scenarios.

Learner Satisfaction: 100%
Estimated length: 5 hours
Access Time: 90 days
Credits: 0.5 CEUs

II. Testimonials

The following testimonials are provided by learners that have completed courses in the Cybersecurity & CISSP suite.

Asset Security

"That course was cutting edge for my new role in Data Management."

CISSP® Exam Prep Course

"Great course. I really like the length of each page...there was just enough content to read in one sitting. The quizzes were very good also."

CISSP® Practice Exams and Exam Strategies

"Both have allowed me to enrich the memory of all my computer skills, and especially information security."

Introduction to Cybersecurity

"Fantastic course, easy to understand."

Introduction to Malware

"Good information regarding malware type of viruses in the digital era. Keep it up."

Network Security Scenarios

"The module is beneficial and the scenario offered help to develop the reflexes of network security."

Security and Risk Management

"I am new in the area of information security and risk management. Going through the course has increased my interest in the subject area, and I plan to learn more and implement at my work place. I have enjoyed the course, and I would highly recommend it."

Security Engineering

"This module is rich in all aspects of communication security and equipment security."