

Security Training Programs

Overview

According to numerous sources, nothing in the information security arena brings a better return on investment (ROI) than security training and awareness. Emagined Security offers organizations a variety of on- and offsite training opportunities. These include an offering of a wide range of standard courses such as "Responding to Incidents and Forensics", "Windows 2008 Security", "Unix Security", Linux Security Hands-on, "Securing IIS Web Servers", "Securing Apache Web Servers," "Intrusion Detection and Prevention," Network Security, Information Security Basics, Cryptography, Mobile Computing Security, and Certification Examination Preparation Courses (the CISM and CISSP Prep Courses).

Benefits

Emagined Security's courses cover most critical knowledge and skill areas within information security. These courses are designed to enable attendees to gain and apply state-of-the-art, in-depth knowledge of critical concepts and issues in information security and assurance. Wherever possible, attendees are given the opportunity to gain hands-on experience with configuration tasks, analysis of critical information such as intrusion detection-related data, and scripting.

Emagined Security's instructors are well known, respected professionals within the security community who have depth of experience in the areas they cover. Instructors are regular presenters at major security conferences and are high-rated, experienced instructors who know how to motivate attendees to learn and help attendees learn at various levels that go well beyond rote knowledge. Our instructors provide many case studies and share a wide range real world experiences, thus making our training courses more meaningful, applicable and enjoyable. Several Emagined instructors have won teaching and speaking awards.

Emagined Security teaches courses that are available to the public, but we can also bring training to you. Our instructors can travel to your site, so you don't have to send the entire class to an offsite location, thus saving your organization time and money.

Another distinctive of Emagined Security's training is the number and quality of materials provided to attendees. Handouts list bullets that are understandable long after attendees have completed the training and provide a variety of extra resource materials and references. Most Emagined course materials also include a glossary for the benefit of attendees who possess less background knowledge than others.

Description of Courses

Emagined Security's courses focus general security awareness to specific technical security issues. We strive to make security training rewarding, educational and stimulating. Whether or not your audience has a security background, Emagined Security has a course that is right for you. We can tailor the content of each course to meet your specific requirements, or can even develop and teach a custom course geared specially towards your needs for you. Our standard course offerings include:

Responding to Incidents and Forensics (Two days)

The world of computing, and in particular the Internet, is subject to a wide range of security-related threats. No matter what type and how many controls and countermeasures are deployed, security-related incidents continually occur. Trends over the last few years in fact indicate that not only are more incidents occurring, but their impact and severity are greater. Incident response has thus become a mainstream activity, partly out of necessity, but also because an increasing number of organizations are realizing that an information security practice that does not achieve a reasonable balance between preventative controls and countermeasures and detective and reactive controls cannot be effective.

This two-day course provides thorough coverage of the major aspects of responding to incidents, starting with planning and going on to day-by-day activities in which those who respond to incidents must engage. The goal is to teach attendees the things they need to do in real-life operations. Developed by the founder of the Department of Energy's Computer Incident Advisory Capability (CIAC), the course includes a variety of case studies and scenarios in which attendees are presented with descriptions of real-life security breaches and must deal with each step-by-step, making the course as real and relevant as possible.

Topics covered include:

- An introduction to incident response
- Sizing the threat
- A methodology for incident response
- Tracing network attacks
- Legal considerations
- Forensics
- Setting and using traps and deceptive measures
- Responding to insider attacks
- Forming and managing an incident response team

The course is designed for a wide range of attendees. Much of the information concerns policies, procedures, and administrative/management considerations. Detailed technical information is

included at appropriate points in the course to help system and network administrators know exactly what to do, as well as to familiarize less technically proficient attendees about some of the technical side of incident response. Having at least some knowledge of and practical experience with Windows, Unix and Linux systems as well as networking is helpful in understanding the technical side of the course, but is not required.

Windows Server 2008 Security (Two days)

Windows Server 2008 (WS2008) is the latest version of Microsoft server operating systems. WS2008 incorporates many security-related improvements and represents the most secure version of an operating system that Microsoft has ever produced. This two-day course is designed to help attendees understand these improvements and to learn the specific configurations that are necessary to ensure reasonable levels of security. Topics include:

- An introduction to WS2008
- Security features and capabilities
- Vulnerabilities and vulnerability management
- WS2008 Active Directory
- Group Policy Objects
- Authentication
- File and share security
- Auditing
- Network security
- Using Windows Management Instrumentation (WMI)
- Conclusion

This course is extremely technical in nature and is thus most appropriate for network and system administrators and system programmers, although auditors and IT staff who have some experience with Windows operating systems will be able to understand most of the concepts in this course.

Unix Security (Two days)

The Unix operating system is a dilemma. Its rich functionality, extensibility and portability have established this operating system in organizations throughout the world, yet more security incidents over the last two decades have involved Unix systems than any other type of operating system. This two-day course on Unix security presents the special problems and challenges that Unix presents for security, then systematically delves into technical and procedural measures that address these problems.

The major emphasis is upon the most widely used flavors of Unix, but course content is applicable to all Unix flavors. This course is designed for Unix system and network administrators, system integrators, IT auditors and managers, computer programmers, security administrators, and managers. Some knowledge of Unix functionality and commands is

necessary for understanding the content of this course, but high levels of technical proficiency are not necessary.

This course covers the following important topics:

- Introduction
- A high-level view of Unix security
- Major types of security-related vulnerabilities
- Physical security
- File protection
- System and network protection
- Account security
- Logging
- Special security features in different flavors of Unix
- The specifics---Securing Solaris, HP-UX, IRIX and RedHat
- Application Security
- Encryption
- Auditing a UNIX System
- Useful tools (ssh, sudo, tcpdump, Tripwire, Crack, Fix-Modes, etc.)
- Wrap-up

Linux Security Hands-on (Two days)

The Linux revolution is here, and with it have come dozens of flavors of Linux as well as a large number of vulnerabilities. This two-day hands-on course teaches attendees what to actually do to secure their Linux systems. Each module begins with a brief explanation of a set of related security-related issues, then shifts to having each attendee go through steps that produce the intended result with the instructor serving as troubleshooter. Attendees then test the controls they have put in place to ensure that they work. Topics include:

- Overview
- Vulnerabilities
- Physical security
- Password security
- Account and group security
- Securing services
- Host-based firewalls
- IP Tables and IP Chains
- Logging
- Updating and patching

This course teaches virtually everything someone needs to know to implement the desired level of Linux security. A basic knowledge of Linux and particularly of commands for major shells such as bash and the Bourne shell is required.

Securing IIS Web Servers (One day)

Securing Web servers is in and of itself a difficult challenge, and IIS Web servers are no exception to this principle. Although Microsoft has greatly tightened default settings on this server starting with IIS 6.0, over the years more successful attacks (including Web page defacements, denial of service attacks, and many other types) against IIS Web servers are reported on sites such as attrition.org than against any other type of Web server. Unless Web developers and Webmasters know specifically what threats exist and how to counter them, IIS Web servers can serve as easy prey for attackers.

This one-day course provides comprehensive coverage of IIS Web security, teaching Web developers and Webmasters what they need to know to secure IIS 6.0 and 7.0 Web servers. Highly technical in nature, the course starts with the basics of IIS Web deployment and functionality, then moves on to standard security options through advanced capabilities such as SSL/TLS encryption, and then covers advanced security issues, such as certificate issuance and handling.

Topics covered include:

- An introduction to IIS 6.0 and 7.0 (major features, directory structures, virtual servers, virtual directories, and so on)
- Types of security-related vulnerabilities
- Types of security features
- Achieving baseline security
- Going beyond baseline security
- Security administration
- IIS Web application security
- Wrap-up

Because of the technical nature of the course, only those who have at least some knowledge of and practical experience with Windows systems and Windows security should attend. Knowledge of Web server design and implementation is helpful, but is not a prerequisite. Bringing a laptop with IIS installed is potentially helpful to attendees, but is not required.

Apache Web Security (One day)

Apache is the world's most widely deployed Web server. Although with nearly every subsequent release it has become more secure out-of-the-box, numerous configuration changes must be made and new modules must be compiled in if Apache is to run securely. Additionally, Apache servers need to be continually analyzed and their log output inspected to determine whether or not they have been compromised. This course presents a very comprehensive coverage of Apache security, from the initial installation to day-to-day operational deployment. Topics include:

- Apache basics
- Vulnerabilities and exposures
- Installation
- Configuring Apache for security (includes access control, PHP, SSL and TLS)
- Operational security procedures
- Application security
- Conclusion

This course is designed specially for Web server administrators and Webmasters, and thus is very knowledge domain-specific and technical. Attendees without much knowledge and experience with Apache may still benefit from the course, however, if they understand basic Web services and protocols.

Intrusion Detection and Prevention (Two days)

Intrusion detection has grown from something that at one time was considered a "black art" to a mainstream activity in organizations throughout the world. Intrusion prevention is relatively new and with this newness come many uncertainties. Intrusion detection and intrusion prevention involve considerably more than deploying intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). The particular manner in which IDSs and IPSs are deployed greatly affects their usefulness, but few people genuinely understand the "in's and out's" of intrusion detection and intrusion prevention sufficiently to use each optimally. Additionally, successful use of intrusion detection and intrusion prevention requires establishing an infrastructure that includes appropriate policy provisions, management oversight, incident response procedures, and many other considerations.

This two-day course "puts it all together" by providing attendees with in-depth information about the most critical aspects of intrusion detection and intrusion prevention. This course also teaches attendees what they need to know to set up an intrusion detection program and make sound technical and managerial decisions concerning deployment of the various elements of these programs.

Topics covered include:

- Introduction
- Approaches to Intrusion Detection and Intrusion Prevention
- How IDSs and IPSs Work
- Intrusion Detection and Prevention Systems Architecture
- Case Studies: Real-Life IDSs
- Limitations in IDSs and IPSs
- Event Correlation
- The Administrative/Procedural/Legal Side of Intrusion Detection and Intrusion Prevention
- The Future of Intrusion Detection and Intrusion Prevention

- Wrap-Up

This course is designed for a wide range of attendees, including system and network administrators, IT staff, information security staff, and auditors. It contains a mixture of technical and non-technical information. Some knowledge of networking, Unix, Linux and Windows operating systems is helpful in understanding some of the technical content of this course, but is not required.

Network Security (Two days)

Today's computer networks have capabilities far beyond those envisioned by experts years ago. With the increased networking capabilities have come new, difficult challenges for achieving control and security. This two-day course provides a comprehensive view of networking--its mechanisms and protocols--but with a security slant. It begins with a broad overview of networking, then proceeds to cover security-related threats and control mechanisms. The course also delves into specific network-related issues that users and organizations typically face and how to address them. Topics include:

- Networking basics
- Major types of network security exposures
- Major control measure solutions (including strengths and weaknesses of each)
- Securing network services
- Securing Web servers
- Firewalls
- Network monitoring
- Encryption
- Secure email
- Wrap-up

The course is designed for a wide range of attendees. Much of the information concerns policies, procedures, and administrative/management considerations. Technical information is included at appropriate points in the course with the intention of helping system and network administrators know exactly what to do as well as to familiarize less technically proficient attendees about some of the technical side of incident response. Having at least some knowledge of and practical experience with Windows, Unix and Linux systems as well as networking is helpful in understanding the technical side of the course, but is not required.

Information Security Fundamentals (Two days)

Computer security (more commonly known in professional circles as "information security" and in government circles as "information assurance") has grown substantially in importance over the years. System administrators, users, and managers are often forced to make changes because of security considerations without genuinely understanding why. This two- day course presents the

"why's and wherefore's" of information security/information assurance with the goal of helping you understand why things are done the way they are in this arena. Topics include:

- An introduction to information security
- The basics: Risk assessment and risk management
- Asset valuation and classification
- Vulnerabilities and exposures
- Types of control measures and countermeasures
- Weighing costs versus benefits
- Creating and maintaining an information security program
- Evaluating a security program's progress
- Dealing with compliance and regulation considerations
- Wrap-up

This course includes a wide range of both high-level and technical information in addressing these issues. There are no prerequisites for attending this course.

Cryptography (One day)

Cryptography is an extremely interesting and potentially very useful area to information security professionals, yet few people genuinely understand the "why's and wherefore's" of cryptography. This one day course is designed to give IT and audit professionals a clear understanding of cryptography, how it works, how it can be used, and what the advantages and disadvantages of each cryptographical system or application are. Topics covered include:

- Major cryptographic methods
- When it is and is not appropriate to use each cryptographic method
- What makes cryptographic systems resistant to attack
- Major methods of key exchange and the strengths and weaknesses associated with each
- Practical applications based on cryptographic methods
- Wrap-up

This course has no prerequisites, but some knowledge of mathematics is useful in understanding concepts that will be covered.

Mobile Computing Security (One day)

The user computing environment has changed considerably over the last decade because of the increased mobility of users. Mobility poses many security-related challenges (anonymous connections, always on connections, cleartext network traffic, wireless networks, and so on), many or most of which are typically not adequately addressed, even though proven solutions are widely available. Topics covered in this course include:

- Introduction

- Vulnerabilities
- Policies and procedures
- Securing wireless networks
- Securing handheld devices
- Evaluating and auditing security in mobile environments
- Security products
- Wrap-up

Included in the course is an intensive class exercise in which attendees evaluate a real-life mobile computing policy and propose ways to improve it.

This course is appropriate for IT security and audit staff and system and network administrators. Contains a mixture of technical and non-technical content. A fundamental knowledge of networking and particularly network security would be helpful, but is not necessary.

CISM Certification Examination Preparation Course (Three days)

Organizations are increasingly relying on complex information systems and applications to conduct their business and must thus ensure information security managers have the expertise to adequately manage the continuously growing number of associated security threats and risks. Additionally, organizations are facing a plethora of regulatory and compliance requirements, many of which are information security related, that if not adequately met can result in deleterious consequences. These challenges have elevated the importance of the role of the information security manager to new heights.

Unfortunately, however, many individuals who hold information security management positions do not have the breadth and depth of knowledge nor do they have the ability to perform tasks necessary to adequately safeguard their organizations' information assets and resources and to achieve regulatory compliance at an acceptable cost. CISM certification training is designed to help information security managers possess gain the requisite knowledge as well as understand how to perform essential tasks to achieve desired outcomes. Attendees will also be taught how to plan, implement and maintain a security program that will adequately safeguard their organizations' information assets and resources at an acceptable cost.

This three-day course covers the following five core areas of information security management in detail:

1. Information security governance. What information security governance is; why it is so important; its relationship to overall corporate governance; how to create a security framework and action plans; and how to determine whether objectives are being met; the elements and purpose of an information security policy, what standards, procedures and guidelines are and why they are important, and how policy, standards, procedures and guidelines are interrelated; what a security architecture is and why it is potentially so useful.

2. Risk management. What risk management is and why it is so important; what risk assessment

is and how it works; strategies for dealing with risk; what a business impact analysis is and how it can be used in risk management; and how to determine the effectiveness of risk management.

3. Information security program management. What an information security program is, what its components are, and how to set such a program up; what controls and countermeasures are and how they can be used; types of controls and countermeasures and their effectiveness; and important additional considerations such as resource management.

4. Information security program maintenance. How to maintain and continuously monitor an information security program once it has been created; the many functions associated with program maintenance and how they should work; resource management considerations; security training and awareness; developing and using metrics and testing; compliance considerations.

5. Incident management. What incident management is and how it differs from incident response; what an incident response plan is and why it is critical; elements of and procedures involved in incident response; business continuity and disaster recovery planning, testing and execution; measuring the effectiveness of incident management.

This course helps attendees learn essential terms and concepts necessary to pass the CISM exam. It also teaches attendees how to apply concepts to real-life information security situations and scenarios--more CISM exam questions that tap ability to apply concepts are present on a typical examination than any other type of question. Much of the training also involves answering practice questions that are extremely similar to actual CISM examination questions. Finally, attendees are taught how to carefully read each question to understand what type of knowledge each question is trying to tap and how to readily weed out incorrect answers.

CISSP Certification Preparation Course (Three days)

Of all the information security-related certifications available, no certification is held by more information security professionals than the Certified Information Systems Security Professional (CISSP) certification. This course thoroughly covers the 10 Core Body of Knowledge (CBK) areas represented within the examination:

- Access Control Systems and Methodology
- Applications and Systems Development
- Business Continuity Planning
- Cryptography
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical Security
- Security Architecture and Models
- Security Management Practices
- Telecommunications, Network & Internet Security

This course helps attendees master fundamental terms and constructs required to pass the CISSP examination. Because the CISSP exam also includes many questions that require application of constructs, the course also includes numerous real-life case studies and situations. Attendees are also taught how to anticipate the types of items that are most likely to appear in the exam and strategies for answering these items. Practice questions that parallel real-life CISSP test questions are also presented throughout the course.

A major advantage of this course over competing CISSP examination preparation courses is that this course is taught over a three-day period. Using the time-tested 80-20 principle, attendees are taught what is most important to learn to pass the test instead of being bombarded with so many details that the course content becomes overwhelming (as too often occurs in a five-day course). Attendees thus walk out of the course with a knowledge structure that is most conducive to truly understanding course constructs, leaving them with a framework that will not only better help them to determine what knowledge or knowledge's each question is trying to tap, but also how to use sound reasoning to decide up a good answer to each.