RSA EDUCATION SERVICES CATALOG

COURSE DESCRIPTION INDEX

ENABLE YOUR TEAM TODAY FOR TOMORROW'S IT SECURITY CHALLENGES

Value and Results from RSA Education Services

Do you have a plan to optimize your team's capabilities to address the challenges of managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments? Is your team ready to exploit the full potential of RSA solutions?

With Education comes expertise. RSA Education Services will improve the efficiency and effectiveness of your team as well as increase your organization's competitiveness. We can help you achieve maximum return on your investment in RSA products and solutions by:

– Enabling security strategies that lower your organizational risk
– Increasing productivity and decreasing operating costs
– Providing faster and more successful implementation of new security technologies
– Increasing employee satisfaction and confidence in RSA solutions
– Reducing your dependence on RSA Technical Support
– Developing more autonomy and control over your own systems

RSA Education Services provides practical and relevant courses that support security learning across an enterprise. Properly trained personnel are the lifeblood of any organization. As you implement new technologies, add new functionality to existing systems or orient new staff, education is a key element. Consistent and focused training helps maintain the security of your computing environment, improves the end user experience and increases productivity and job satisfaction among your staff.

FLEXIBLE DELIVERY OPTIONS

Instructor-Led Training (ILT)

Instructor-led classes offer comprehensive training in a fully-equipped RSA Learning Center. Public classes give you the opportunity to interact with your peers, further enhancing your learning experience by sharing real-world tips and best practices.

Video Instructor Led Training (Video ILT)

Video ILT courses combine the best of instructor-delivered lectures and presentations with the convenience and flexibility of an on-demand learning format. Video ILT is provided on CD/DVD to be used by the student directly on their own desktop or laptop computer.

Online Instructor-Led Training (Online ILT)

Online ILT provides real-time, interactive, virtual training where students participate online to access the instructor-led virtual classroom. Lecture, discussion, questions and answers, and lab exercises makes this a flexible training experience.

eLearning

Self-paced eLearning provides you with training that is generally one to three hours in length giving you the convenience of learning at your own pace.

RSA PRODUCT TRAINING

Our worldwide training services are targeted to serve professionals who are responsible for installing, supporting and administering the entire range of RSA solutions. Developed for security administration and network operations, the product courses offer a variety of teaching methods including traditional instructor-led and virtual instructor-led training, video-based learning, and elearning. Each of these options gives you the flexibility to select a learning mode that best fits your learning style, time constraints and budget.

SECURITY CONCEPTS AND PRINCIPLES

RSA Education Services offers a number of courses to support your organization's information security efforts. Our training offerings combine a mix of theory, technology, and scenario-based examples to keep the student on track, alert, and interested. Courses deliver the maximum amount of material in the shortest amount of time to keep your staff's downtime to a minimum.

Security Concepts and Principles for General Staff

No matter how much technology-based defense and offense you have in place, it's people who interact with sensitive information such as personally identifiable information, payment information, intellectual property, protected health information, confidential company plans, and financials. Employees can carry this sensitive information outside the office on laptops, mobile phones, USB drives, and paper in the course of doing their daily work. Security rests with all of your employees. Shifting the way employees think about and protect sensitive information can be a company's best protection.

Security Concepts and Principles for IT Staff

Employees who are on the front lines of deploying, managing, and securing information technology must be well-equipped to protect sensitive information. The Security Concepts and Principles for IT Staff courses are designed specifically for system architects to database administrators who deploy, maintain, and protect the enterprise infrastructure.

Security Concepts and Principles for Development Staff

By identifying and resolving vulnerabilities early in the software development lifecycle, your team can substantially reduce information risk cost-effectively. Secure coding has been greatly advanced by the adoption of formal software security assurance methodologies such as Microsoft SDL, OWASP's SAAM, and BSIMM. Central to the successful implementation of these methodologies is role-specific training for all development staff – whether they are architects, developers, QA testers, or managers.

Cloud Security Fundamentals

As organizations transition to cloud computing technology, IT Security professionals recognize the unique challenges faced by moving to a cloud environment.
This hands-on course provides an introduction to cloud security concepts, attributes, and steps associated with implementing a secure cloud environment.

CISSP Certification Boot Camp

The Certified Information Systems Security Professional (CISSP) certification is one of the most widley known and recognized standards of expertise in the industry.
This Certification Bootcamp involves intensive lectures, demonstrations, and review questions delivered by security professionals with years of experience as practitioners. Not only will participants become prepared to take the exam but real world examples are invaluable insight into security challenges and the approaches to solve them.

Security Concepts and Principles for General Staff eLearning courses:

– Information Security Awareness
– Information Privacy Awareness

Security Concepts and Principles for IT Staff eLearning courses:

– IT Security Fundamentals

Security Concepts and Principles for Development Staff eLearning courses:

– Application Security Fundamentals
– Application Security Fundamentals for Managers
– Secure Client/Server Development in C/C++
– Secure Web Development in Java
– Secure Web Development in .NET
– Secure Web Development in PHP

Information Security ILT courses:

– Secure Architecture and Design
– Cloud Security Fundamentals
– Certified Information Systems Security Professional (CISSP) Bootcamp

ONSITE TRAINING

To drive maximum return on investment from RSA software and solutions, your people need training. But, given all their day-to-day responsibilities, it can be costly and difficult to send them to off-site courses. The solution: bring the training to you, with onsite training from RSA Education Services. You can choose from RSA's comprehensive portfolio of courses that address the needs of your security administration and operations staff. Whatever course you choose, your RSA onsite training courses will be taught by RSA's experts: professionals with extensive experience helping enterprises deploy RSA solutions.

Substantial Cost Savings

RSA Onsite training rates can save an organization up to 40% when compared to individual student rates. Additional cost savings are realized by eliminating the need for student travel. What's more, since your students are not preparing for trips – or making their way back from airports after training – they are likely to be more productive and accessible in the days surrounding their training experience.

Convenient and Flexible Scheduling

With RSA Onsite training, you and your people aren't locked into a pre-existing schedule of public classes at a pre-existing location. RSA Education Services can work with you to schedule your training at the time and location that's most convenient for you. That means training doesn't have to conflict with your other business priorities – and it can be timed precisely to support your RSA implementation.

Mobile Classroom

With RSA Onsite training, you don't have to provide equipment or IT support, or worry about equipment or software problems interfering with class time. Just provide the space: we'll handle all the technology for you. For a reasonable fee, we'll ship equipment to your site to accommodate training for up to ten students. Our experienced professionals will set up and test all equipment in advance of class start time – so your people can hit the ground running, and get the greatest benefit from every minute of instruction.

Practical Benefits of Online Instructor-led Training

– No travel cost or travel time

– Live instructor with whom you can interact and ask questions

– Same content as the classroom version of the course

– Modest connectivity requirements let you participate from anywhere

– Hands-on labs reinforce concepts learned

– Publicly-scheduled classes for individual participants

– Private sessions for organizations that prefer virtual training for their dispersed teams

– Access to remote lab environment to practice outside of class hours (during duration of the class period)

ONLINE INSTRUCTOR-LED TRAINING

What is Online ILT?

Online ILT is real-time virtual training conducted remotely by RSA instructors. It's virtual training that mirrors the classroom experience with:

Live web casts. During scheduled web casts, students communicate with their RSA instructor and other students, ask questions, and experience RSA products through live demonstration.

Hands-on labs. Students access a remote lab environment that enables them to interact with RSA software and practice what they've learned.

Course materials. Course materials are shipped to participants in advance of the class. Just like in a classroom, students use these materials under the guidance of the instructor.

Instructor guidance. During class time, students have the benefit of the instructor's expertise to assist during the live web casts and Hands-on Labs. During lab time, the instructor can shadow students by virtually looking over the shoulder of each student to evaluate their progress and provide assistance.

Registration and Payment

Please complete your registration at www.rsa.com\training. Be sure you register with the e-mail address of the student attending class, as this is the *only* unique identifier we have for each student.

Complete details regarding payment by purchase order, credit card or check are provided on our web site.

RSA TRAINING CREDITS

Training is an invaluable means of facilitating growth in your organization and increasing the skills and knowledge of your employees. With RSA Training Credits (TCs) you can invest in RSA courses and use them whenever RSA training is necessary.

Training credits are simply RSA Education Services currency. They are deposited into a company's training account and are available for general consumption by your company's employees. Valid for one year from date of purchase, pre-paid TCs provide maximum flexibility to ensure your team's readiness.

With RSA TCs you can satisfy your training requirements as they evolve throughout the year. You reduce the paperwork and approvals associated with multiple enrollments by taking care of all your training needs with a single purchase.

RSA TRAINING CENTERS

Worldwide training center locations

Bedford, MA - US	Overland Park, KS - US	Reston, VA - US
Bracknell - UK	Berlin - DE	Düsseldorf - DE
Dreieich - DE	Hamburg - DE	München - DE
Espoo - FI	Bolzano - IT	Mexico - MX
Solna - SE	Singapore - SG	Dubai - UAE

Product training is also scheduled in other locations worldwide.
For the most current information, go to www.rsa.com/training.

RSA CERTIFIED SECURITY PROFESSIONAL CERTIFICATION

By becoming an RSA Certified Security Professional, you possess the credentials that demonstrate your knowledge and skills necessary to function as a practical expert in the rapidly growing information security industry. Job-based certifications are available for administrators for the product areas designated below. Our relationship with Pearson VUE, which operates 5,000 testing centers in 165 countries, provides convenient access to certification exams and ensures impartial testing.

The RSA Certified Administrator specialization is designed for professionals who administer and maintain enterprise security systems that use RSA SecurID® authentication or RSA® Archer™ security management.

Certification	Recommended RSA Courses
RSA Archer Certified Administrator	• Introduction to GRC • Getting Started with RSA Archer • RSA Archer Administration
RSA SecurID Certified Administrator	• RSA SecurID Administration • RSA SecurID Installation and Configuration

SUMMARY OF OFFERINGS BY DELIVERY MODE

	ILT	VILT	e-Learning	Online ILT
Access Management				
RSA Access Manager Administration, Installation and Configuration	✔			
Authentication				
RSA Adaptive Authentication (On Premise) Administration	✔			✔
RSA Adaptive Authentication Back Office Tools			✔	
Introduction to RSA Authentication Manager Express Administration			✔	
RSA Cryptographic & Digital Certificate Concepts		✔		
RSA Digital Certificate Management Solution Installation and Administration		✔		
RSA SecurID Administration	✔	✔		✔
RSA SecurID Installation and Configuration	✔	✔		✔
RSA SecurID Help Desk Basics				✔
Enterprise Governance, Risk and Compliance				
Getting Started with RSA Archer			✔	
Introduction to Governance, Risk and Compliance (GRC)			✔	
Navigating RSA Archer			✔	
RSA Archer Administration	✔	✔		✔
RSA Archer Advanced Administration	✔			✔
RSA Archer Audit Management Fundamentals			✔	
RSA Archer Business Continuity Management Fundamentals			✔	
RSA Archer Compliance Management Fundamentals			✔	
RSA Archer Enterprise Management Fundamentals			✔	
RSA Archer Incident Management Fundamentals			✔	
RSA Archer Policy Management Fundamentals			✔	
RSA Archer Risk Management Fundamentals			✔	
RSA Archer Threat Management Fundamentals			✔	
RSA Archer Vendor Management Fundamentals			✔	
What's New in RSA Archer 5.0			✔	

SUMMARY OF OFFERINGS BY DELIVERY MODE *(CONTINUED)*

	ILT	VILT	e-Learning	Online ILT
Data Loss Prevention				
RSA Data Loss Prevention Administration	✔	✔		✔
RSA Data Loss Prevention Policy and Classification	✔			
Data Protection				
RSA Data Protection Manager Administration			✔	
Network Monitoring				
RSA NetWitness Administration	✔			
RSA NetWitness Analyst I	✔			
RSA NetWitness Analyst II	✔			
RSA NetWitness Forensics	✔			
Security Event and Incident Management				
RSA enVision Administration	✔	✔		✔
RSA enVision Advanced Administration	✔			✔
Security Concepts and Principles				
Information Security Awareness			✔	
Information Privacy Awareness			✔	
IT Security Fundamentals			✔	
Application Security Fundamentals			✔	
Application Security Fundamentals for Managers			✔	
Secure Architecture and Design	✔			
Secure Client/Server Development in C/C++			✔	
Secure Web Development in Java			✔	
Secure Web Development in .NET			✔	
Secure Web Development in PHP			✔	
Cloud Security Fundamentals	✔	✔		
Certified Information Systems Security Professional (CISSP) Certification Boot Camp	✔			

RSA® Access Manager Administration, Installation and Configuration

Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course offers thoeretical and hands-on instruction in the administrative functions, operations, and installation and configuration tasks associated with the RSA Access Manager product. RSA Access Manager system architecture, server structure, integration of components into an enterprise infrastructure, user organization, and the importance of various configuration parameters are discussed. Hands-on labs allow the student to work step-by-step through the phases of RSA Access Manager implementation.

Extensive hands-on labs and the use of a realistic case study reinforce the tasks involved in creating a complete Web access management solution.

Audience

System, security, or help desk personnel who need to install, deploy and/or maintain RSA Access Manager.

Duration

4 days

Prerequisite Knowledge/Skills

Familiarity with Web and directory server or database technologies; A functional knowledge of OS and networking fundamentals.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Explain the basic architecture and integration of RSA Access Manager in an enterprise environment
- Describe the processes and methodology for performing a successful installation and implementation of the core servers, data adapter, Administrative Console and representative Agents
- Describe the management functions used for resource and end user administration
- Using a case study, perform typical administration functions to populate and configure users, administrators and groups in an RSA Access Manager database
- Explain the configuration parameters that can be used to tailor the RSA Access Manager components to accomplish specific tasks and functions
- Establish Entitlements and use RSA Access Manager Smart Rules™ to manage Web access and protect resources in a classroom Web environment
- Perform system troubleshooting and analysis through the use of audit logs and user reports
- Explore how runtime and administrative operations can be extended through the use of the API library

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
        781-515-7700 (International)

Fax: 781- 515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- **RSA Access Manager Overview**
    - High level description of RSA Access Manager and its contribution to access management

- **RSA Access Manager Architecture**
    - Description and functions of the Primary Servers; Web and Application Server Agents
    - Data Flow for the Runtime and Administrative operations
    - Description of how RSA Access Manager fits into a distributed security model

- **Installion and Configuration**
    - Description of RSA Access Manager system requirements and pre-installation readiness tasks
    - Installation procedure, options, and recommended practices
    - Installation of Access Manager Servers, LDAP Data Adapter, Administrative Console, and Web and Application Server Agents
    - Configuration of Web Server for Single Sign-On

- **Managing Resources**
    - Discussion of how resources (Web sites, Applications, etc.) are protected using RSA Access Manager – focusing on selectivity and granularity in various situations
    - Registration of Web Servers and definition of Applications
    - Discussion of Virtual Web Server Hosts
    - Configuration of Web Server for virtual hosts

- **Delegated Administration**
    - Discussion of the administrative structure that is possible in an RSA Access Manager installation
    - Use of Administrative Groups and ownership hierarchy of administrators, users, and objects
    - Examination of Administrative Roles and responsibilities

- **Managing the Organization**
    - Policy control for user authentication and passwords
    - Methodology of structuring users, groups, user attributes, and properties
    - Creation of user properties and addition of users to groups

- **Resource Protection and Authentication**
    - Discussion of Authentication Methods used to protect resources; Form-based vs. challenge/response authentication; Chaining and combining forms
    - Discussion of how resources are defined to allow granular protection
    - Use of RSA Access Manager Entitlements and Smart Rules to selectively manage access to resources
    - How to manage conflicts among Smart Rules and between Smart Rules and Entitlements
    - Configuration of Access Manager for external authentication and URL retention

- **Troubleshooting**
    - Examination of the log files and use of special configuration parameters to control log detail
    - Configuration of servers for centralized logging
    - Configuration of Network Management
    - Discussion of approaches to user and system troubleshooting

- **Development Tools**
    - Discussion of the various Runtime, Administrative, and Web Agent Extension API tools that are available
    - Examination and implementation of JAVA coding examples

- **Single Sign-On**
    - Discussion of the function and objectives of creating a single sign-on environment
    - Explanation of the differences and challenges of 'Intra-' vs. 'Inter-' site single sign-on
    - Configuration of Access Manager for SSO and ISSO

- **Distributed Authorization**
    - Discussion of achieving redundant functionality and failover
    - Explanation of the differences in Standard Mode vs. Distributed Mode failover
    - Test of centralized logging

Course Delivery Options

This course is currently available in the following formats:

ED CLRAIN110: *Public* Instructor led - includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED CLRAIN210: *On-site* Instructor led - held at the customer's location.

ED ACCMGRTRAIN CREDIT: Training credits for use with any RSA classes

RSA® Adaptive Authentication On-Premise Administration

Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course offers hands-on training on the installation, integration, configuration, and administration of RSA Adaptive Authentication On-Premise. The working principles behind RSA Adaptive Authentication On-Premise architecture, system components, and administrative tasks are discussed. Extensive hands-on labs reinforce the tasks involved in implementing an RSA Adaptive Authentication On-Premise system.

Audience

System, security, or help desk administrators who need to install, configure and/or maintain an RSA Adaptive Authentication On-Premise system.

Duration

3 days

Prerequisite Knowledge/Skills

Familiarity with user and system administration, networking fundamentals, and general information security concepts.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Explain the basic architecture and theory of operation of RSA Adaptive Authentication On-Premise
- Describe how RSA Adaptive Authentication On-Premise determines risk
- Describe the recommended workflows and deployment modes
- Perform the installation tasks involved in installing RSA Adaptive Authentication On-Premise
- Explain the steps required to integrate RSA Adaptive Authentication On-Premise with a web application
- Use the Back Office tools to configure, manage, and administer RSA Adaptive Authentication On-Premise
- Perform the day to day administrative tasks to keep the RSA Adaptive Authentication On-Premise functioning properly

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
             781-515-7700 (International)

Fax: 781- 515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- RSA Adaptive Authentication On-Premise Overview
  - Relevant terminology
  - Features and benefits of RSA Adaptive Authentication On-Premise
  - Risk-Based authentication
  - Device profiling
  - Behavioral profiling
  - What is multi-factor authentication?
  - How RSA Adaptive Authentication On-Premise provides for multi-factor?

- RSA Adaptive Authentication On-Premise Architecture
  - System components overview
  - Network Integration
  - RSA eFraudNetwork
  - RSA Risk Engine
  - Policy Editor
  - Back Office Applications
  - RSA Central
  - GeoIP Service
  - Scheduler
  - Adaptive Authentication utilities

- RSA Adaptive Authentication On-Premise Risk Score Calculation
  - How Adaptive Authentication determines risk
  - Risk score calculation stages

- RSA Adaptive Authentication On-Premise Workflows and Processes
  - Terminology used in workflows
  - RSA Adaptive Authentication On-Premise workflows

- RSA Adaptive Authentication On-Premise Installation
  - Deployment modes
  - Pre-installation overview
  - Installing RSA Adaptive Authentication On-Premise
  - Setting up maintenance and development utilities
  - Post-installation tasks

- RSA Adaptive Authentication Configuration
  - The configuration framework
  - Determining a deployment mode
  - Creating default configuration files
  - Customizing configuration files

- RSA Adaptive Authentication On-Premise Integration
  - Introduction to the Web services API and methods
  - Collecting device information
  - Message format and recommended data elements

- RSA Adaptive Authentication Back Office Tools
  - Overview of the Back Office tools
  - Access management
  - Policy Editor
  - Case Management
  - CSR (Customer Services Representative) Tool
  - Report Viewer

- Operations
  - Administration Console
  - GeoIP Update
  - Schedule tasks
  - Update the eFraudNetwork agent
  - Log files
  - RSA Central

Course Delivery Options

This course is currently available in the following formats:

ED AAOPADM110: *Public* instructor led - includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED AAOPADM210: *On-site* instructor led – held at the customer's location

ED AA CREDIT: Training credits for use with any RSA classes

RSA Adaptive Authentication Back Office Tools
Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview
This course offers training on the RSA Adaptive Authentication Back Office Tools. The working principles behind RSA Adaptive Authentication technology, architecture, and system components are discussed. Video demonstrations reinforce the tasks involved in using the RSA Adaptive Authentication Back Office Tools.

Audience
Team Leaders/Fraud Strategists responsible for fraud prevention planning. Customer Service Representatives who provide support for card holders requiring online transaction assistance, and Fraud Investigators/Analysts.

Duration
Approximately 2 hours
The modules and content presented depends on the student's job role. The job role is selected from a menu presented at the beginning of the training.

Prerequisite Knowledge/Skills
Familiarity with general information security concepts.

Course Objectives
Upon successful completion of this course, participants should be able to:
- Define RSA Adaptive Authentication for eCommerce
- Explain the basic system architecture and components of RSA Adaptive Authentication for eCommerce
- Provide an overview of the Adaptive Authentication for eCommerce Back Office Tools
- Use the Back Office Tools including:
  - Back Office Administration
  - Customer Service
  - Case Management
  - Policy Manager
  - Management Information Reports
- Generate Web Reports
- Describe Raw Data Reports

Register for Classes:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

Have Questions? Please contact us:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
        781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- RSA Adaptive Authentication for eCommerce Overview
  - History and evolution of Adaptive Authentication for eCommerce
  - Components and processes that make up 3DSecure
  - Transaction Monitoring
  - The RSA Risk Engine and eFraudNetwork
  - Describe low, high, and very high risk transaction workflows

- Back Office Tools Overview
  - Overview of the Back Office tools
  - Back Office Administration
  - Customer Service
  - Case Management
  - Policy Manager
  - Management Information Reports

- Back Office Administration
  - Describe the hierarchical structure of users
  - Roles and access
  - Manage groups
  - Manage CSRs

- Customer Service Application
  - Validate a cardholder's identity
  - Manage cardholders
  - View activity and transaction logs
  - Use the Personal Account Manager
  - Work with e-mail alerts

- Case Management Application
  - Describe a case
  - List case management best practices
  - Explain the importance of feedback and working cases
  - Describe repudiation files
  - View and update cases

- Policy Manager Application
  - View and update rule definitions
  - Add rules
  - Activate a new test rule
  - Edit and delete rules

- Reporting
  - Describe the different types of reports available
  - Generate web reports
  - Describe Raw Data Reports
  - Describe MIS reports

Course Delivery Options

This course is currently available in the following format:

ED AAECOM410: eLearning — Web-based asynchronous course available at your convenience via the Internet.

ED AA CREDIT: Training credits for use with any RSA classes

Introduction to RSA® Authentication Manager Express (AMX) Administration
Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient, and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview
This course offers training on the administration, installation, and configuration of RSA Authentication Manager Express, Authentication Agents, and other RSA AMX system components. The working principles behind RSA AMX technology, architecture, system components, and administrative tasks are discussed. Video demonstrations reinforce the tasks involved in administering an RSA AMX solution.

Audience
System, security, or help desk personnel who need to install, deploy, and/or maintain an RSA Authentication Manager Express system.

Duration
2 hours

Prerequisite Knowledge/Skills
Familiarity with user and system administration, networking fundamentals, and general information security concepts.

Course Objectives
Upon successful completion of this course, participants should be able to:
- Explain the basic architecture and theory of operation of the RSA Authentication Manager Express product
- Describe the configuration required for RSA Authentication Manager Express system operations
- Perform user administration functions to populate and manage users
- Understand the ongoing maintenance requirements
- Plan and perform pre-installation, installation, and configuration tasks for RSA Authentication Manager Express Appliance
- Create redundant/failover RSA Authentication Manager replica servers and understand the role and management of replica server instances
- Install and configure RSA Authentication Agent hosts for local workstation and web access protection
- Understand the setup and use of RSA Authentication Manager Express web tiers

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
       781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- RSA Authentication Manager Express Overview
  - Description of RSA Authentication Manager Express and its contribution to authentication
  - Advantages of RSA Authentication Manager Express
  - Licensing and configuration options

- Authentication
  - Multi-Factor Authentication
  - Risk-Based Authentication method
  - AMX risk engine
  - How risk engine scores are calculated
  - Assurance levels
  - Silent collection
  - On-demand Authentication

- RSA Authentication Manager Express Components
  - AMX administrative and user consoles
  - AMX components

- RSA Authentication Manager Express Setup
  - Appliance setup requirements
  - Primary appliance setup
  - Setting up a replica appliance

- Preparing RSA AMX for Administration
  - AMX security domains
  - AMX authentication policies
  - Adding security domains
  - Adding AMX users
  - AMX administrative roles

- Configuring RSA Authentication Manager Express
  - Installing an AMX authentication agent
  - Generating and deploying an integration script
  - Creating and delivering a node secret
  - Configuring On-Demand Authentication to use email or SMS for token delivery

- Monitoring System Activity
  - Types of activity monitors
  - Using an activity monitor to monitor system activity and troubleshooting
  - Registering a new device
  - Monitoring risky transactions
  - Enrolling a new user during silent collection

- RSA Web tier Deployments
  - Describe web tiers and their advantages
  - Typical web tier deployments
  - Load balancing in AMX
  - Web tier network considerations

Course Delivery Options

This course is currently available in the following formats:

ED AMXADM410: eLearning — Web based asynchronous course available at your convenience via the Internet.

ED SIDTRAIN CREDIT: Training credits for use with any RSA classes

RSA® Cryptographic and Digital Certificate Concepts Video-ILT

Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient, and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course provides an overview of the key concepts of cryptographic applications and digital certificates and how this technology enables e-commerce and enhances security. This course is a prerequisite to the RSA Digital Certificate Solutions course and is helpful for students in other RSA courses involving a base understanding of cryptographic principles.

This course is delivered in a self-paced video format with printable Student Guide files that can be used for further study.

Audience

IT professionals who need to understand the fundamentals of cryptographic functions and digital certificates so they can successfully implement PKI in their organizations.

Duration

Approximately 8 hours

Prerequisite Knowledge/Skills

None

Course Objectives

Upon successful completion of this course, participants should be able to:
- Understand cryptographic fundamentals and related applications
- Understand the role that cryptography plays in e-commerce and enterprise security
- Understand how a Public Key Infrastructure (PKI) is employed in RSA products
- Understand Digital Certificate standards and practices

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- Cryptographic Basics
  - Terminology
  - Cryptosystems (symmetric, message digest, hybrid systems)
  - Cryptographic Algorithms

- Public Key Infrastructure Standards
  - PKCS
  - PKIX
  - X.509

- Practical Applications of Cryptography and Digital Certificates

- Certification Authorities (CAs)
  - Trust relationships among CAs
  - Types of CAs
  - CA Structures

- Legal Issues Relating to Digital Certificates
  - Certificate practices statement
  - Digital signature legislation
  - Subscriber agreements

- PKI Implementation
  - Methodology for planning and implementing a PKI

Course Delivery Options

This course is currently available in the following formats:

ED PKIFND DVD: Video ILT — DVD video provides a recording of an instructor delivered course along with recorded labs, online quizzes, and additional content.

RSA® Digital Certificate Management Solution Installation and Administration Video-ILT
Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient, and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview
This course provides participants with the knowledge required to plan, install, configure, manage, and maintain the RSA Digital Certificate Solution product — which includes the Certificate Manager, Registration Manager, OneStep, Key Recovery Manager and RCM-API components.

Participants learn about the functions and capabilities of the RSA Digital Certificate Solution product suite, plan and deploy components according to a case study, and learn the various aspects of managing the Certificate Authority and maintaining certificates.

This course is delivered in a self-paced video format with lectures, demonstrations of various operations and includes printable Student Guide and Lab Exercise files that can be used for further study or hands-on work in the student's own environment.

Audience
Security Professionals who require an in-depth knowledge of installing and/or administering the RSA Digital Certificate Management Solution product.

Duration
Approx. 16 hours

Prerequisite Knowledge/Skills
RSA Cryptography and Digital Certificate Concepts course or equivalent PKI background; Familiarity with web browser applications; Networking and Operating System fundamentals – including Mail Server administration functions, DNS, TCP/IP, SSL and LDAP.

Course Objectives
Upon successful completion of this course, participants should be able to:
- Identify the components of a PKI (Public Key Infrastructure)
- Describe the RSA Digital Certificate Solution product suite and its applications, functions, administrator types, and roles
- Install and Configure Certificate Manager, Registration Manager and OneStep components
- Manage certificate and CA status
- Generate Certificate Revocation Lists (CRLs); configure certificate and CRL publishing
- Manage certificate profiles, renew certificates, and manage server certificates
- Identify solutions to common issues with RSA Digital Certificate Management Solution product
- Configure logging information
- Back up and restore the RSA Certificate Authority database
- Describe how to install RSA Key Recovery Manager and describe Key Recovery Operator tasks

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
         781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- Overview
  - Overview of the RSA Digital Certificate Solution product suite – its components and architecture
  - Overview of the RSA Digital Certificate Solution administration interface

- Planning and Installing RSA Certificate Manager
  - Planning your certificate needs and product deployment
  - Certificate Manager hardware and software requirements
  - Installing Certificate Manager

- Configuring RSA Certificate Manager
  - Creating the CA structure
  - Configuring High Availability

- Installing RSA Registration Manager and RSA OneStep
  - Registration Manager overview
  - Registration Manager hardware and software requirements
  - Installing Registration Manager
  - Installing OneStep
  - Enrolling for certificates using OneStep

- Vetting Certificates
  - Creating trust relationships
  - Obtaining a Vettor certificate
  - Editing certificate roles and vettor rights
  - Enrolling for end-user certificates
  - Vetting end-user certificate requests

- Managing Status
  - Changing certificate status
  - Changing CA status
  - Generating Certificate Revocation Lists (CRLs)
  - Generating Authority Revocation Lists (ARLs)
  - Configuring CRLs
  - Configuring a jurisdiction for external publishing
  - Configuring a CA for local publishing
  - Configuring CRL distribution points

- Maintaining Certificates
  - Viewing certificates
  - Creating reports based on search criteria
  - Modifying and creating certificate profiles
  - Configuring certificate expiry
  - Creating a certificate renewal policy
  - Renewing certificates
  - Reissuing an internal server certificate

- Troubleshooting
  - Identifying common issues, causes and solutions
  - Monitoring the system using log files, events and tracing
  - Backing up and restoring the Certificate Authority database

- Installing and Managing RSA Key Recovery Manager
  - Key Recovery Manager overview
  - Planning considerations for Key Recovery Manager
  - Installing Key Recovery Manager
  - Enabling a Jurisdiction for Key Recovery
  - Obtaining end-user single-use certificates
  - Renewing certificates
  - Obtaining a KRO certificate
  - Recovering encryption keys and certificates

Course Delivery Options

This course is currently available in the following formats:

ED CPKINS DVD: Video ILT — DVD video provides a recording of an instructor delivered course along with recorded labs, online quizzes, and additional content.

RSA SecurID® Administration
Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course provides an overview of the administrative responsibilities associated with an RSA SecurID® system. The working principles behind RSA Authentication Manager software and RSA SecurID authenticators are discussed, including product architecture, time synchronization, using external Identity Sources and exploring all aspects of an administrative structure. Extensive hands-on labs reinforce the administrative tasks involved in managing a user population and token assignment.
The subject matter in this course prepares students with the classroom component recommended for the RSA SecurID Certified Administrator certification.

Audience

System, security, or help desk administrators who need to administer and support RSA SecurID products.

Duration

2 days

Prerequisite Knowledge/Skills

Familiarity with Microsoft® Windows® or UNIX system administration.

Course Objectives

Upon successful completion of this course, participants should be able to:
- Explain the basic architecture and theory of operation of the RSA SecurID product suite
- Describe the configuration required for RSA Authentication Manager system operations
- Perform user administration functions to populate and manage users
- Perform report functions and user troubleshooting
- Understand the ongoing maintenance requirements
- Understand the setup and use of software authenticators
- Understand the use of the RSA Credential Manager function

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
            781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- Product Overview
  - High level description of RSA Authentication Manager software and its contribution to authentication
  - Authentication as a foundation of security, trust and confidence in digital identities

- RSA SecurID Fundamentals
  - RSA Authentication Manager system components
  - RSA Authentication Manager/Agent system architecture
  - Concepts of strong user authentication
  - Token theory – time synchronization, authenticator types
  - Administrative access and task/scope delegation
  - Concepts of protecting access points, Agent functions and login
  - Description of Realm and Security Domain structures
  - Licensing Options

- RSA Authentication Manager Software Configuration
  - Setting system and Realm-level parameters
  - Access to administration consoles
  - Importing token records

- User Administration
  - Establishing Users and linking to external Identity Sources
  - Token operations
  - Establishing RSA Authentication Agent hosts
  - Setting RADIUS profiles

- System Administration
  - Setting up Security Domains and User Group structures
  - Administrative roles and delegation
  - Working with realms

- Auditing, Reports and Troubleshooting
  - RSA Authentication Manager report functions
  - Report customization
  - Troubleshooting procedures

- RSA SecurID Software Authenticators
  - Software/Hardware Token differences
  - Installation, deployment, and user packages
  - Software Token operation

- Credential Manager Function
  - Configuration of Credential Manager for user self-service functions
  - Description of authenticator management and provisioning using Credential Manager

Course Delivery Options

This course is currently available in the following formats:

ED SIDADM110: *Public* Instructor led - includes hands-on lab exercises that reinforce the concepts covered in lectures.
ED SIDADM210: *On-site* Instructor led – held at the customer's location.

ED SIDADMINDVD: Video ILT - DVD video provides a recording of an instructor delivered course along with recorded labs, online quizzes, and additional content.

ED SIDTRAIN CREDIT: Training credits for use with any RSA classes

RSA SecurID® Installation and Configuration

Course Description

Overview

This course offers hands-on training on the installation and configuration of RSA Authentication Manager software, Authentication Agents, and other RSA SecurID® system components.

This course assumes that the student has attended the RSA SecurID Administration course or has equivalent operations experience with RSA Authentication Manager – operations are not covered as part of this course. The subject matter in this course prepares students with the classroom component recommended for the RSA SecurID Certified Systems Engineer certification.

Audience

Technical personnel who install, service and support RSA SecurID installations.

Duration

2 days

Prerequisite Knowledge/Skills

Microsoft® Windows® or UNIX system administration; attendance in RSA SecurID Administration course, or equivalent v7.1 administration experience.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Plan and perform the pre-installation tasks to prepare for RSA Authentication Manager software installation in a Microsoft Windows environment
- Plan and perform pre-installation, installation, and configuration tasks for RSA Authentication Manager software and Appliance
- Describe the configuration required for RSA Authentication Manager system operations
- Connect to Identity Sources for external user repositories (Active Directory and LDAP)
- Create redundant/failover RSA Authentication Manager replica servers and understand the role and management of replica server instances
- Install and configure RSA Authentication Agent hosts for local workstation and web access protection
- Perform RSA Authentication Agent host configurations to accomplish system load balancing

---

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
           781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- Building a Security Solution
    - Enterprise assessment and analysis
    - Security planning – Scalability, redundancy, performance (host, remote, web, realm, server access, etc.)
    - Working with firewalls and Network Address Translation

- RSA Authentication Manager Software Installation
    - Pre-Installation considerations; Installation and configuration of software and Appliance solutions
    - RSA Authentication Agent software installation and system testing
    - Post-Installation tasks: system configuration parameters, Agent settings and options

- RSA SecurID Appliance
    - Similarities and Differences between the Appliance and Authentication Manager software
    - Explanation of Appliance models and installation/setup procedure

- RADIUS Interface
    - RADIUS functions and capabilities
    - Configuring RADIUS to integrate with RSA Authentication Manager software

- Managing RSA Authentication Manager Replica Servers
    - Strategies for dealing with primary server failures and replica promotion; Creating replica packages
    - Establishing preferred and failover servers in legacy Agent hosts

- Authentication Agent Configurations
    - Functions and features of representative Authentication Agent installations for Microsoft Windows and UNIX operating systems
    - Configuring Agent software for local, network and web access protection
    - Handling node secret and sdconf.rec files

- Maintenance and Disaster Recovery
    - System maintenance including backups and audit log archiving
    - Using the Command-line Utility package

- Credential Manager Configuration
    - Setting up the Credential Manager for provisioning

Course Delivery Options

This course is currently available in the following formats:

ED SIDINS110: *Public* Instructor led - includes hands-on lab exercises that reinforce the concepts covered in lectures.
ED SIDINS210: *On-site* Instructor led – held at the customer's location.

ED SIDINSTALLDVD: Video ILT - DVD video provides a recording of an instructor delivered course along with recorded labs, online quizzes, and additional content.

ED SIDTRAIN CREDIT: Training credits for use with any RSA classes

RSA SecurID® Help Desk Basics
Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course provides the fundamental information about an RSA SecurID® system deployment to assist Help Desk representatives respond to end users. An overview of RSA Authentication Manager and RSA SecurID authenticators is presented, as well as how functions and controls are accessed in the administrative interface. Instructor demonstrations of important operations relating to typical end user cases reinforce the steps that Help Desk representatives can take for troubleshooting and assisting their user population.

This course is useful for new representatives supporting RSA SecurID users as well as a refresher course for representatives who infrequently work with RSA SecurID support issues.

Audience

Help Desk representatives who need to assist and support RSA SecurID users

Duration

1 day

Prerequisite Knowledge/Skills

General familiarity with system administration functions

Course Objectives

Upon successful completion of this course, participants should be able to:

- Understand the high-level architecture and theory of operation of the RSA SecurID product suite
- Identify common authentication problem areas
- Perform common user assistance tasks
- Understand the use of the RSA Credential Manager and user Self-service capabilities

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- RSA SecurID System Overview
    - High level description of RSA SecurID and RSA Authentication Manager system components
    - Authentication process and data flow

- Authentication Problem Areas
    - Identifying and isolating user problems
    - Common user errors
    - Differentiating User vs Agent vs Server problems

- System Configurations
    - Organizational structures – users, groups, Security Domains and Identity Sources
    - Authentication options and policies

- Authenticator Operations
    - Hardware tokens
    - Software tokens
    - On-demand codes
    - Emergency and temporary codes

- Monitors and Reports
    - Using the Authentication Monitor
    - Generating reports to track and user activity

- User Troubleshooting
    - Troubleshooting procedures
    - Security considerations

- Credential Manager – Self-service Console
    - User self-service functions
    - Credential Manager provisioning flow
    - Troubleshooting user self-service problems

Course Delivery Options

This course is currently available in the following formats:

ED SIDHELPDESK110: Live Virtual Instructor led - includes instructor demonstrations to reinforce the concepts covered in lectures.

ED SIDTRAIN CREDIT: Training credits for use with any RSA classes

Getting Started with RSA® Archer™
Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course focuses on defining the typical RSA Archer business user needs and explaining how those needs can be met through the RSA Archer eGRC Suite. A brief overview of each of the RSA Archer Solutions is included in this training. The goal of this training is to help RSA Archer users understand how the RSA Archer Solutions fit together to address common business needs. The subject matter in this course is a recommended prerequisite for the RSA Archer Administration course.

Audience

RSA Archer administrations and business users who will begin using the RSA Archer product or higher-level managers who need to understand the purpose of RSA Archer in the business world.

Duration

Approximately 1 hour

Prerequisite Knowledge/Skills

Familiarity with user and system administration, networking fundamentals, and general information security concepts.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Articulate a typical user's business challenges

- Understand the user's desired outcomes

- Describe the key capabilities of the RSA Archer solutions

- Understand how RSA Archer solutions can meet business requirements

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

**HAVE QUESTIONS?
PLEASE CONTACT US:**

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
         781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- Understanding the Problem
  - Introduction of fictional company and its challenges
  - Exploration of those challenges in terms of negative business outcomes

- Defining the Goals
  - Defining the desired state of business
  - Exploration of the desired state in terms of positive business outcomes
  - Defining a set of required capabilities for the solution that will meet business needs

- How RSA Archer Can Help
  - RSA Archer eGRC Suite overview
  - Policy Management Solution overview
  - Enterprise Management Solution overview
  - Incident Management Solution overview
  - Risk Management Solution overview
  - Compliance Management Solution overview
  - Vendor Management Solution overview
  - Threat Management Solution overview
  - Business Continuity Management Solution overview
  - Audit Management Solution overview
  - Benefits of using RSA Archer

- Case Studies
  - Technology case study
  - Telecommunications case study
  - Retail case study

Course Delivery Options

This course is currently available in the following formats:

ED ARCGETSTART410: eLearning — Web-based asynchronous course available at your convenience via the Internet.

ED ARCTRAIN CREDIT: Training credits for use with any RSA classes

Introduction to GRC
Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview
This course provides an overview of the subjects of Governance, Risk, and Compliance (GRC), and explains the significance of GRC in today's business world. The subject matter in this course is a recommended prerequisite for the RSA Archer Administration course.

Audience
Administrators and business users of the RSA Archer eGRC Suite.

Duration
Approximately ½ hour

Prerequisite Knowledge/Skills
No prerequisite experience necessary

Course Objectives
Upon successful completion of this course, participants should be able to:

- Articulate what GRC means and its relevance within an organization

- Describe why GRC is an important business enabler

- Identify the business processes associated with GRC

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
           781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the
course objectives:

- Defining GRC
    - Definition of Governance, Risk, and Compliance
    - GRC in everyday life

- Background of GRC
    - Historical events that affected GRC
    - Risk and Compliance factors
    - Confusion related to GRC

- Importance of GRC
    - GRC in today's business world
    - Organizational areas affected by GRC
    - Stages of GRC adoption
    - Reactive vs. Proactive GRC

- GRC People and Processes
    - Who is concerned with GRC
    - Governance Processes
    - Risk Processes
    - Compliance Processes
    - GRC Linkage
    - Enterprise GRC Operationalized

Course Delivery Options

This course is currently available in the following formats:

ED INTROGRC410: eLearning — Web-based asynchronous course available at your convenience via the Internet.

ED ARCTRAIN CREDIT: Training credits for use with any RSA classes

Navigating RSA® Archer™

Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview
This course provides the basics a user needs to navigate the RSA Archer product. Participants will learn common navigation and data access techniques.

Audience
Archer administrators who will begin using the RSA Archer product.

Duration
1 hour

Prerequisite Knowledge/Skills
None

Course Objectives
Upon successful completion of this course, participants should be able to:
- Understand the general layout and structure of the RSA Archer eGRC interface
- Understand basic navigation of the interface
- Understand the layout and functions of the Navigation menu
- Perform searches and produce reports

Course Outline
The following topics are designed to support the course objectives:
- Login and basic user interface
- Top Frame functions
- Workspaces, iViews, and Quick Reference Links
- Application and Solution Navigation
- Navigation Menu functions
- Access privilege
- Searching and Reporting

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
        781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Delivery Options
This course is currently available in the following formats:

ED ARCHERNAV 410: eLearning — Web-based asynchronous course available at your convenience via the Internet.

ED ARCTRAIN CREDIT: Training credits for use with any RSA classes

RSA® Archer™ Administration
Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview
This course provides an overview to the concepts, processes, and procedures necessary to successfully design and administer the RSA Archer platform. Students will gain knowledge of the key RSA Archer platform components such as applications, security management, and communication tools through presentations and hands-on exercises. After taking this course, students will be able to plan, configure, and manage the RSA Archer environment. The subject matter in this course prepares students with the classroom component recommended for the RSA Archer Certified Administrator certifications.

Audience
Archer administrators who are responsible for building and managing the RSA Archer eGRC product.

Duration
4 days

Prerequisite Knowledge/Skills
Recommended viewing:
Introduction to GRC
Navigating Archer
Getting Started with RSA Archer

Course Objectives
Upon successful completion of this course, participants should be able to:
- Describe the components of the RSA Archer Enterprise Management Solution
- Configure the look and feel of the RSA Archer Platform interface
- Centralize and organize data
- Import data
- Alert users to data changes
- Optimize the user experience
- Manage user access
- Automate work streams
- Search and report on data
- Communicate information to key stakeholders
- Migrate changes between environments

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
　　　　781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the
course objectives:

- RSA Archer Overview
  - RSA Archer eGRC Suite
  - Enterprise Management Solution components
  - Introduction to the case study

- Configure the Appearance
  - Managing Themes
  - Managing the Appearance

- Centralize and Organize Data
  - Data structure
  - Application Builder overview
  - Inside Manage Applications
  - General Application Properties
  - Field Management
  - Page Layout
  - Navigation Menu

- Import Data
  - Using the Data Import Manager

- Alert Users to Data Changes
  - Creating Letterheads
  - Managing Subscription Notifications

- Optimize the User Experience
  - Data-Driven Events
  - Calculated Fields

- Manage User Access
  - Access Control Basics
  - User Accounts
  - Access Roles
  - Groups
  - Record Permissions
  - Private Fields

- Automate Work Streams
  - Configure a two-stage workflow

- Search and Report on Data
  - Quick Search
  - Advanced Search
  - Statistics Search and Chart Options
  - Reporting

- Communicate Information to Stakeholders
  - iViews
  - Dashboards
  - Workspaces
  - Additional Configuration Options

- Packaging for Production
  - Creating Packages
  - Installing Packages

- Vendor Management Case Study
  - Hands-on exercise in which participants are
    challenged to build a best-in-class vendor data
    application with minimal assistance

- Course Summary
  - Customer Support Options
  - Certification Exam Information

Course Delivery Options

This course is currently available in the following formats:

ED ARCADMIN110: *Public* Instructor-led — includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED ARCADMIN210: *On-site* Instructor-led — held at the customer's location; up to 10 students.

ED ARCADM DVD: Video ILT — DVD video provides a recording of an instructor delivered course along with recorded labs, online quizzes, and additional content.

ED ARCTRAIN CREDIT: Training credits for use with any RSA classes

RSA® Archer™ Advanced Administration
Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview
This course provides hands-on training on the administration, configuration and best-practice deployment of the RSA Archer Platform. Throughout the course, students will be presented with a diverse collection of real-world governance, risk, and compliance problems and be shown and guided through the recommended steps involved in solving these pain points by using the features available in the RSA Archer eGRC Suite.

Extensive hands-on labs reinforce the tasks involved in designing and automating GRC processes and extending the value of the RSA Archer eGRC Suite throughout the organization. After completing this class, students will be prepared to use the RSA Archer eGRC Suite to solve an extensive array of GRC problems and meet the business requirements of various enterprise stakeholders.

Audience
Governance, risk, and/or compliance professionals, business owners, or IT personnel who need to automate and streamline existing processes, integrate the RSA Archer platform with third-party systems, or deliver assessments across the enterprise.

Duration
4 days

Prerequisite Knowledge/Skills
Previous experience creating applications within the RSA Archer product or successful participation in the standard RSA Archer Administration course.

Course Objectives
Upon successful completion of this course, participants should be able to:
- Create a custom, multi-stage workflow process that automates a manual process
- Import existing information from a legacy system into RSA Archer applications and questionnaires
- Integrate the RSA Archer product with third-party systems and data sources to consolidate enterprise information
- Design best-practice assessment campaigns to measure compliance across the organization
- Construct complex search criteria to locate key information and identify data trends
- Visually showcase compliance with industry regulations through reports and dashboards
- Alert organization stakeholders through scheduled report distributions
- Export RSA Archer data into pre-formatted, professional-looking report templates

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
        781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline
The following modules are designed to support the course objectives:

- Streamlining GRC Processes — Day One
  - Replicating a multi-stage workflow to transfer a manual, paper-based process to an automated, online tool
  - Constructing a scalable access control framework for enabling end users to participate in GRC processes
  - Automating and manipulating data through calculations to support enhanced data analytics and reduce data entry time
  - Designing best-practice online forms to ensure user adoption of the system

- Integrating External Data — Day Two
  - Transferring leveled, document-centric policies into a data-centric format in the RSA Archer Platform
  - Using a data feed targeting flat file sources to quickly transfer legacy data to a centralized system
  - Creating a data feed to access an RSS source and retrieve the information into an RSA Archer application
  - Transferring data between RSA Archer applications to support data trending and
  - reduce manual effort

- Showcasing Enterprise Information – Day Three
  - Generating real-time reports across distant data relationships to provide greater insights into GRC processes
  - Designing a user-friendly dashboard and interface to clearly communicate the posture of various business units
  - Importing compliance questions into RSA Archer's global question library
  - Creating an assessment campaign to demonstrate compliance with internal and external regulations
  - Managing question scoring and findings generation to better understand the risk impact to the organization
  - Referencing existing assessment responses in future assessments

- Publishing Data Across the Enterprise – Day Four
  - Delivering snapshot reports on a set schedule to inform key stakeholders of the current status
  - Exporting RSA Archer data to email and Word templates to generate professional-looking, document-based reports for senior management
  - Discussing strategies for publishing RSA Archer data to external databases
  - Migrating applications and configurations from a development environment to a production environment
  - Troubleshooting common RSA Archer issues to ensure effective system operations

---

Course Delivery Options
This course is currently available in the following formats:

ED ARCADVADM110: *Public* instructor-led — includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED ARCADVADM210: *On-site* instructor-led — held at the customer's location; up to 10 students.

ED ARCTRAIN CREDIT: Training credits for use with any RSA classes

RSA® Archer™ Solution Fundamentals
Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

- RSA Archer Audit Management Fundamentals
- RSA Archer Business Continuity Management Fundamentals
- RSA Archer Compliance Management Fundamentals
- RSA Archer Enterprise Management Fundamentals
- RSA Archer Incident Management Fundamentals
- RSA Archer Policy Management Fundamentals
- RSA Archer Risk Management Fundamentals
- RSA Archer Threat Management Fundamentals
- RSA Archer Vendor Management Fundamentals

Overview
Each Solution course describes the functionality, configuration, and use of the RSA Archer Solution and its application components. Each course explains how applications can be set up to manage an organization's infrastructure and information. Interaction between individual applications and other RSA Archer Solutions is discussed. Participants are shown practical scenarios through the use of Solution demonstrations.

Audience
Business analysts and supporting staff members who will be using the RSA Archer product to document business structure and components.

Duration
Each individual course is approximately 1 hour or less in length.

Prerequisite Knowledge/Skills
Familiarity with RSA Archer eGRC framework and a general familiarity with organizational Enterprise Governance, Risk, and Compliance (eGRC) concepts.

Course Objectives
Common to all Solution courses are the following objectives:
- Understand the function of the given RSA Archer Solution
- Understand the Solution's "out-of-box" applications
- Understand the Solution components and design process
- Realize how the Solution can integrate with other eGRC components and Solutions

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following outlines describe the individual Solution courses:

RSA Archer Audit Management Fundamentals

- Audit Management Components and Integration
- Audit Management Application Descriptions
- Audit Management Solution Configuration and Design

RSA Archer Business Continuity Management Fundamentals

- Business Continuity Management Components and Integration
- Business Continuity Management Application Descriptions
- Business Continuity Management Solution Configuration and Design

RSA Archer Compliance Management Fundamentals

- Compliance Management Components and Integration
- Compliance Management Application Descriptions
- Compliance Management Solution Configuration and Design

RSA Archer Enterprise Management Fundamentals

- Enterprise Management Components
- Business Hierarchy and Enterprise Infrastructure Integration
- Enterprise Management Application Descriptions
- Enterprise Management Solution Configuration and Design

RSA Archer Incident Management Fundamentals

- Incident Management Components and Integration
- Incident Management Application Descriptions
- Incident Management Solution Configuration and Design

RSA Archer Policy Management Fundamentals

- Policy Management Components and Integration
- Policy Management Application Descriptions
- Policy Solution Configuration and Design
- Policy Gap Analysis, Design, and Planning
- Common Policy Migration Challenges

RSA Archer Risk Management Fundamentals

- Risk Management Components and Integration
- Risk Management Application Descriptions
- Risk Management Solution Configuration and Design

RSA Archer Threat Management Fundamentals

- Threat Management Components and Integration
- Threat Management Application Descriptions
- Threat Management Solution Configuration and Design

RSA Archer Vendor Management Fundamentals

- Vendor Management Components and Integration
- Vendor Management Application Descriptions
- Vendor Management Solution Configuration and Design

Course Delivery Options

These courses are currently available in the following formats:

eLearning — Web-based asynchronous course available at your convenience via the Internet. The currently available courses include:

ED ARCAUDMGTFUN410:	RSA Archer Audit Management Fundamentals
ED ARCBUSCONMGT410:	RSA Archer Business Continuity Management Fundamentals
ED ARCCOMMGTFUN410:	RSA Archer Compliance Management Fundamentals
ED ARCENTMGTFUN410:	RSA Archer Enterprise Management Fundamentals
ED ARCINCDNTMGT410:	RSA Archer Incident Management Fundamentals
ED ARCPLCYMGT410:	RSA Archer Policy Management Fundamentals
ED ARCRISKMTG410:	RSA Archer Risk Management Fundamentals
ED ARCTHRTMTG410:	RSA Archer Threat Management Fundamentals
ED ARCVENDMTG410:	RSA Archer Vendor Management Fundamentals

ED ARCTRAIN CREDIT: Training credits for use with any RSA classes

What's New in RSA® Archer™ 5.0
Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

The What's New in RSA Archer 5.0 online training course provides an in-depth review of the 5.0 release of the RSA Archer eGRC Suite. Featuring video demonstrations, descriptive diagrams, and expert commentary, this three-hour self-paced course allows existing RSA Archer professionals and consultants to learn best-practice approaches for building GRC processes in the 5.0 RSA Archer Platform.

This course takes students across the seven components of the RSA Archer eGRC Suite, exposing the student to the changes and new features across the system. Each section discusses the business value of the component, explains the new features, and showcases the best practice configurations through video demonstrations.

Audience

Customers and partners needing a detailed overview of the new features and changes to the RSA Archer eGRC Suite.

Duration

3 Hours

Prerequisite Knowledge/Skills

Familiarity with the 4.x version of the RSA Archer eGRC Suite.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Navigate the new RSA Archer 5.0 interface
- Identify the key new features of the release
- Recognize the differences between the 5.0 and 4.x versions of the RSA Archer eGRC Suite
- Configure the new options and manage the legacy features
- Understand the business value of the new features and enhancements

Course Outline

The following modules are designed to support the course objectives:

- User Experience
  – Navigating the Interface
  – Managing the Appearance

- Application Builder
  – Managing Fields
  – Designing Application Layouts
  – Building Calculations
  – Creating Data-Driven Events
  – Managing Packages

- Reports and Dashboards
  – Running an Advanced Search
  – Selecting a Search Display
  – Building a Cross-Application Search
  – Managing iViews
  – Building Dashboards and Workspaces

- Access Control
  o Reviewing Access Controls

- Workflow
  – Building a Workflow Stage
  – Completing a Workflow Assignment

- Notifications
  – Managing the General Notification Settings
  – Building a Subscription Notification
  – Sending a Scheduled Report
  – Using an On-Demand Template

- Integration
  – Building a Mail-Merge Template
  – Managing a Data Feed
  – Creating a Data Publication

Course Delivery Options

This course is currently available in the following formats:

ED ARC5WHTNEW410: eLearning — Web-based asynchronous course available at your convenience via the Internet.

ED ARCTRAIN CREDIT: Training credits for use with any RSA classes

RSA® Data Loss Prevention Administration

Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course provides comprehensive instruction in the administration and configuration of the RSA Data Loss Prevention (DLP) Suite.

Theory and product basics such as the RSA DLP Suite architecture, integration of RSA DLP components, and the importance of various configuration parameters are discussed.

Students participate in hands-on exercises that build on the basic concepts and allow practical experience in building an RSA DLP system.

Audience

System, security, or help desk personnel who need to install, deploy and/or maintain an RSA Data Loss Prevention system.

Duration

4 days

Prerequisite Knowledge/Skills

Familiarity with user and system administration, networking fundamentals, and general information security concepts. Familiarity with Web, Application and directory server (LDAP) and/or Relational Database (RDBMS) technologies as well as basic programming and scripting concepts is also beneficial.

Course Objectives

Upon successful completion of this course, participants should be able to:

- List the features and benefits of the RSA Data Loss Prevention Suite of products including DLP Network, DLP Datacenter, and DLP Endpoint
- Administer the RSA Data Loss Prevention Enterprise Manager
- Create and manage RSA Data Loss Prevention policies
- Create and manage RSA Data Loss Prevention content blades
- Deploy RSA Data Loss Prevention agents and grid scan groups
- Review what remediation actions are available and what the benefit of each is
- Generate RSA Data Loss Prevention incident and event reports
- Perform basic operational tasks including upgrading software, importing and exporting configuration files, reviewing
   high availability and load balancing, applying patches, and viewing alerts

---

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: (781) 515-6807

Fax: (781) 515-6810

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- Introduction to Data Loss Prevention
  - List the key features of the RSA DLP Suite
  - Identify the key components of the RSA DLP Suite
  - Describe the role of RSA DLP Enterprise Manager
  - Explain the differences between RSA DLP Network, Datacenter, and Endpoint
  - Define how policy violations are handled by RSA DLP Endpoint Enforce

- Enterprise Manager Administration
  - Login to the Enterprise Manager for the first time
  - List the key features of Enterprise Manager
  - Access and license the Enterprise Manager
  - List new dashboard features
  - Review the Enterprise Manager tabs
  - Enter LDAP configuration settings
  - Perform user and group administration
  - Configure an email server and notifications
  - Delete incidents and events
  - Display device status

- Network Appliance Configuration
  - Identify the main components of RSA DLP Network
  - Re-install an RSA DLP Network appliance
  - Login to an RSA DLP Network appliance
  - Perform an initial configuration of an appliance
  - Perform basic configuration for a RSA DLP Network Interceptor
  - Describe the Email Self Release feature
  - Evaluate sensor capacity needs
  - Diagram the ICAP server event flow
  - Perform a basic configuration of an ICAP server

- Introduction to Policies
  - Explain the function of the RSA DLP Content Classification and Analysis system
  - Describe the use and purpose of policies in the DLP Suite
  - Explain how content blades are used in policies to detect sensitive information
  - Create policies using a supplied template
  - Configure DLP Network policies in a virtual network environment

- DLP Datacenter
  - List key features and components of DLP Datacenter
  - Install the Enterprise Coordinator
  - Configure the Enterprise Coordinator
  - Describe the scan types available in DLP Datacenter
  - Install and configure a site coordinator
  - Create a grid scan group
  - View scan status and history

- Creating Content Blades
  - Compare fingerprinting and describing content
  - List the detection accuracy methods available
  - Discuss the importance of weight, score and count
  - Discuss the importance of accuracy and precision
  - Explain how a risk score determines severity
  - Manage and create content blades

- Working with Fingerprinted Content
  - Describe fingerprinting and hashes
  - Define fingerprinting terminology
  - Configure a file crawler
  - Configure a database crawler

- Agent and Repository Scans
  - Analyze agent scan status
  - Configure an agent scan group
  - Schedule an agent scan
  - Analyze agent scan history
  - Configure a repository database scan

- DLP Endpoint
  - Explain how DLP Endpoint Enforce works
  - List the components that comprise DLP Endpoint
  - Configure policy settings relevant to DLP Endpoint
  - Install DLP Endpoint Enforce agents
  - Create a DLP Endpoint Enforce group
  - Manually deploy a DLP Endpoint Enforce agent

- Workflow and Remediation
  - Describe incident and event workflow within RSA DLP
  - Compare DLP remediation actions
  - Describe how manual remediation functions
  - View policy, incident, and transmission details
  - View incident history and notifications

- Reports
  - Describe the main DLP reporting features
  - Navigate the Enterprise Manager dashboard
  - View and edit reports
  - Customize a report
  - Export report data
  - Create DLP Asset Heat Map reports

- Basic Operations
  - Export and import DLP configuration files
  - Review backup options for DLP
  - Discuss high availability options for DLP components
  - Describe how to configure Enterprise Manager failover
  - Review Patching and upgrade operations for DLP
  - List the benefits of integrating DLP and RMS
  - Select and associate an RMS template for use with DLP

Course Delivery Options

This course is currently available in the following formats:

ED DLPADM110: *Public* instructor-led — includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED DLPADM210: *On-site* instructor-led — held at the customer's location; up to 10 students.

ED DLPADM210: *Video ILT* – DVD video provides a recording of an instructor delivered course along with recorded labs, online quizzes, and additional content..

ED DLPTRAIN CREDIT: Training credits for use with any RSA classes

RSA® Data Loss Prevention Policy and Classification

Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course provides a comprehensive training program in policy and classification for data loss prevention. This training course centers around the RSA Data Loss Prevention Suite of products and on building the knowledge and skills to use the tools needed to detect sensitive content in the most accurate and efficient manner possible. This course also provides compliance officers and technical professionals with the knowledge and skills necessary to successfully safeguard enterprise content.

Audience

Technical professionals and security compliance officers who need to use the RSA Data Loss Prevention Suite of products to protect sensitive enterprise content.

Duration

3 days

Prerequisite Knowledge/Skills

A functional knowledge of the RSA Data Loss Prevention Suite, Windows, and/or Linux system administration; familiarity with web, application and directory server (LDAP) and/or relational database (RDBMS) technologies; familiarity with basic programming and scripting concepts.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Identify the terms, patterns, and contextual evidence within content that identify it as sensitive
- Create queries and rules for detecting sensitive content with industry-leading levels of precision and recall
- Distinguish between high-sensitivity content and low sensitivity content, and create differential policies for both
- Apply these skills to all types of content, including personally identifiable information, payment card industry data, and corporate financials and intellectual property

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- Search and Categorization Overview
  - Review search methodologies
  - Define how to measure accuracy
  - Define precision and recall
  - Compare ranks and weights
  - Review search features related to words, phrases, patterns, and entities
  - Define how proximity is used
  - Build an effective rule set

- Regular Expression Basics
  - Define what regular expressions are and how they are used
  - List tools available to create and test regular expressions
  - Review detailed syntax for creating regular expressions
  - Analyze sample regular expressions
  - Create regular expressions to detect sensitive content

- Building Content Blades
  - Identify the types of content blades
  - Review detection rules
  - Compare describing and fingerprinting content
  - Build described content blades
  - Compare and analyze file and database fingerprinting in detail
  - Review fingerprinting frequently asked questions
  - Build fingerprinted content blades

- Content Blade Best Practices
  - Review described content blade best practices
  - Review fingerprinted content blade best practices

- Building Policies
  - Define what policies are and how they are used
  - Review common policy features
  - Explain the relationship between policies and content blades
  - Use policies to identify sensitive content
  - Review DLP Network policy features
  - Review DLP Endpoint policy features
  - Review DLP Datacenter policy features
  - Configure policy-level remediation
  - Create and tune policies to increase recall and precision
  - Navigate the policy template library

- Regulatory Compliance
  - Review existing regulatory compliance policies available in RSA DLP
  - Analyze FERC-related policies
  - Analyze HIPAA-related policies

- Incidents and Events
  - Define what incidents and events are
  - View incident lists
  - Customize searches for incidents and events
  - Review available incident actions
  - Analyze incident and event details

- Methodologies
  - Review best practices for building content blades
  - Research corporate policies
  - Gather test documents
  - Identify linguistic evidence
  - Build for recall
  - Tune for precision
  - Test for accuracy
  - Document detection rules

Course Delivery Options

This course is currently available in the following formats:

ED DLPPLCY210: *On-Site* Instructor-led — held at the customer's location; up to 10 students

ED DLPTRAIN CREDIT: Training credits for use with any RSA classes

RSA® Data Protection Manager Administration
Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview
This eLearning course provides an overview of Data Protection Manager including PKI concepts, architecture and workflows as well as administration concepts and tasks related to the DPM Server and Appliance.

Audience
Administrators of Data Protection Manager Server and Appliance.

Duration
Approximately 4 hours

Prerequisite Knowledge/Skills
- A working knowledge of Linux systems
- Basic knowledge of Key Management and/or Tokenization

Course Objectives
Upon successful completion of this course, participants should be able to:

- Describe the purpose of a Public Key Infrastructure
- Describe how algorithms and keys are used for encryption
- Describe how cryptosystems are used in PKI applications
- Describe how PKI concepts are used in Data Protection Manager
- Describe the basic functions of DPM
- Describe DPM architecture and storage options
- Describe encryption and tokenization workflows
- Identify the components in a DPM deployment
- List the phases in the DPM planning process
- Identify the criteria used to plan for an implementation
- Describe the deployment options
- Create and manage DPM users
- Identity the relationships between security objects
- Create and manage security objects using the DPM Server Administration console
- Manage the DPM appliance

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
         781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- PKI Overview
  - Public Key Infrastructure
  - Algorithms and keys
  - Symmetric and asymmetric cryptography
  - Cryptosystems
  - Digital signatures and certificates
  - Certificate structures in a Public Key Infrastructure
  - PKI concepts in Data Protection Manager

- Architecture and Workflow
  - Basic functions of DPM
  - Difference between encryption and tokenization
  - DPM architecture and storage options
  - Encryption and tokenization workflows

- Planning a DPM Deployment
  - Components in a DPM deployment
  - Phases in the DPM planning process
  - Criteria used to plan for an implementation
  - Deployment options

- Managing Users
  - DPM Administration Interfaces
  - Users, Groups and Roles
  - DPM Administrators
  - Creating users, groups and roles for DPM

- Managing Security Objects
  - Security object overview
  - Security object relationships and hierarchy
  - Configuring DPM for specific use cases
  - Managing the DPM Server and DPM Clients

- Managing the Appliance
  - Monitoring the appliance
  - Restarting and shutting down the appliance
  - Database diagnostics
  - Uploading certificates
  - Changing passwords
  - Adding and removing nodes from a cluster
  - Logs
  - Replication troubleshooting
  - Command line interface

Course Delivery Options

This course is currently available in the following formats:

ED DPMADM410: eLearning — Web-based asynchronous course available at your convenience via the Internet.

RSA NetWitness® Administration
Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview
This course focuses on administration of the RSA NetWitness product. The course provides an overview of RSA NetWitness, hands-on installation and configuration of components, including a Log Decoder, managing users, and creating filters and rules. Additionally, the course covers integration with other products, monitoring capabilities and troubleshooting of common issues.

Audience
RSA NetWitness Administrators

Duration
3 days

Prerequisite Knowledge/Skills
Familiarity with networking fundamentals and general information security concepts.

Familiarity with Linux.

Course Objectives
Upon successful completion of this course, participants should be able to:
- Describe RSA NetWitness component and data flows
- Install RSA NetWitness software
- Configure RSA NetWitness components
- Set up packet and log capture
- Set up LIVE feeds
- Manage users
- Create rules and filters
- Describe how to integrate NetWitness with other products
- Monitor RSA NetWitness
- Troubleshoot RSA NetWitness
-

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
          781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Outline

The following modules are designed to support the course objectives:

- RSA NetWitness Overview
  - RSA NetWitness architecture
  - RSA NetWitness components
  - Data flow between components

- Appliance Setup and Software Installation
  - RSA NetWitness appliance setup
  - RSA NetWitness software components

- Configuring RSA NetWitness
  - Managing Services
  - Configuring and M anaging Devices
  - Setting up data collection of packets and logs
  - Viewing packets and logs in Investigator

- RSA NetWitness Live
  - RSA NetWitness Live Overview
  - Configuring NetWitness Live subscriptions
  - Managing a Live feed

- Managing Users
  - User management interface
  - User groups and roles
  - Creating users and groups
  - Viewing groups and roles
  - Configuring external authentication
  - Editing user settings
  - Informer roles
  - Creating Informer Users

- Creating Rules and Filters
  - Rules, filters, feeds and parsers
  - Decoder filters and Informer rules
  - Best practices for creating filters and rules
  - Creating Decoder filters
  - Creating Informer rules and alerts
  - Creating a feed
  - Pushing a rule to the Decoder
  - Reprocessing a collection

- Integrating RSA NetWitness with Other Products
  - NetWitness SIEM link
  - Setting up Informer to communicate with SIEM products
  - Connecting to HP ArcSight †
  - The RSA enVision Connector

- Monitoring RSA NetWitness
  - Tools that can be used to monitor RSA NetWitness components
  - Configuring SNMP
  - Monitoring NetWitness components for performance and efficiency
  - Tips and best practices for tuning the Decoder, Concentrator, Broker and Informer
  - Methods for viewing and modifying logs

- Troubleshooting RSA NetWitness
  - Common problems
  - Investigating and resolving common problems
  - Troubleshooting tools

† Third-party products and brand names may be trademarks or registered trademarks of their respective owners.

Course Delivery Options

This course is currently available in the following formats:

ED NWADMIN110: *Public* instructor led - includes hands-on lab exercises that reinforce the concepts covered in lectures.
ED NWADMIN210: *On-site* instructor led – held at the customer's location

ED NWTRAIN CREDIT: Training credits for use with any RSA classes

RSA NetWitness® Analyst I
Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course focuses on providing a basic introduction to the technology of the RSA NetWitness NetGen system, focusing specifically on the features and functionality of the Investigator product. The course provides a basic level of understanding on how to create data sets and connect into an RSA NetWitness enterprise infrastructure.   Once connected to a data collection, the course provides an introduction to the navigational capabilities of the investigator and discusses performance considerations and best practices for effective navigation through large data sets. Additionally, the course covers the basics of viewing reports, charts and alerts in Informer and linking back to the Investigator for more in-depth analysis.

Audience

Aimed at junior analysts and those new to the RSA NetWitness system.

Duration

1 day

Prerequisite Knowledge/Skills

Knowledge of networking fundamentals and general information security concepts.

Course Outline

- Technology Overview

- Product Overview

- Investigator
    - Navigation (local vs. remote collection
    - Customization
    - Viewing Panes
    - Searching
    - Hints, Estimates, Accurate
    - Focused Drills
    - Content Reconstruction (session and file extraction)

Course Delivery Options

This course is currently available in the following formats:

ED NWANALYST110: *Public* instructor led - includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED NWANALYST210: *On-site* instructor led – held at the customer's location

ED NWTRAIN CREDIT: Training credits for use with any RSA classes

RSA NetWitness® Analyst II
Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course focuses on content development. The course teaches an advanced analyst how to develop application rules for detection, creating and leveraging threat feeds to model environments and identify known malicious systems. Informer is used to tie it all together to develop reports, charts, and alerts.

Audience

Aimed at security analysts.

Duration

2 days

Prerequisite Knowledge/Skills

RSA NetWitness Analyst I and familiarity with XML and rules structure.

Course Outline

- Technology Overview

- Product Overview

- Content Development within Investigator
    - Threat Feed Creation(Implementing a Threat Feed)
    - Modeling your Network (Update and Create Custom Meta)
    - Implementing a Model of your Network
    - Intellisence Syntax (Application Rule Creation)
- Informer
    - Create Content Using App Rules (Rules Writing, Reports, Alerts, Charts/Dashboards)
    - Content Development Best Practices
- External Integration
    - Linking into RSA NetWitness from other Tools (NW.vbs, SEIMlink

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
        781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Course Delivery Options

This course is currently available in the following formats:

ED NWANALYST2_110: *Public* instructor led - includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED NWANALYST2_210: *On-site* instructor led – held at the customer's location

ED NWTRAIN CREDIT: Training credits for use with any RSA classes

RSA NetWitness® Forensics

Course Description

Our approach to training is simple – provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course covers the threats facing computer networks today, understanding malicious code, learning investigative forensic techniques for Host and Network as well as developing detection indicators using a variety of freeware tools.

Audience

Aimed at experienced security analysts

Duration

2 days

Prerequisite Knowledge/Skills

Knowledge of security best practices and network packet structure and analysis.

Course Outline

- Day 1: Network and Host-Based Forensics Foundation
    - Threat Landscape and Trends
    - What is Network Forensics?
    - Incident Response Lifecycle, Remediation and SOC Workflow Best Practices
    - Investigator Primer
    - File Extraction
        - Extraction and Reassembly: Web, SMTP, FTP, Files
        - Beacon Trojan
        - Malware
        - Extortionware
        - Exploit Kits
        - SSN/Credit Card Exfiltration
    - Developing Basic Detection Patterns (Investigator)

- Day 2: What is Host-Based Forensics?
    - Understanding Binaries
    - Basic Detection Patterns for Malicious Binaries
        - Source Code Exfiltration
    - Malware Analysis/Leveraging and Understanding Available Tools
    - Understanding and Building Indicators/Leveraging Threat Feeds
        - Threat Feed - Waldec
        - Flex Parsing
    - Real World Practical Using Host-Based and Network-Based Methodologies

Course Delivery Options
This course is currently available in the following formats:

ED NWFORENSIC110: *Public* instructor led - includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED NWFORENSIC210: *On-site* instructor led – held at the customer's location

ED NWTRAIN CREDIT: Training credits for use with any RSA classes

RSA enVision® Administration

Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview

This course provides an overview of the RSA enVision product including functions and data flows. Students learn the essentials of data collection, event management, alerting, and reporting. The course provides practice creating views, queries, correlated alerts, and reports as well as watchlists and event traces.

Additionally, exercises explore how to create and deploy event-source support files for unknown devices using the Event Source Integrator (ESI) tool, thereby extending the compliance and security capabilities provided by enVision.

Audience

System, security, or help desk personnel who need to administer the RSA enVision product.

Duration

5 days

Prerequisite Knowledge/Skills

A functional knowledge of computer operations and networking fundamentals.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Explain the basic enVision data flows
- Describe how to collect data from event sources and configure enVision
- Create users
- View data in real time and from an historical perspective
- Create queries and various types of reports
- Create and manage dashboard reports
- Create alerts and correlated rules
- Describe how to set up an Enterprise Dashboard
- Create a watchlist
- Manage vulnerabilities and assets
- Describe how to back up data and obtain content updates
- Create and manage incidents
- Investigate incidents using Event Traces
- Describe the event-source-integration process
- Identify collection methods for different types of logs
- Extract events from an unknown event source
- Describe the EventSource Integrator (ESI) tool

Course Outline

The following modules are designed to support the course objectives:

- RSA enVision Overview
  - Description and functions of the RSA enVision product and its primary components
  - Description of the operational data flows
  - Discussion of services

- enVision Configuration and Data Collection
  - Brief description and tour of the user interface for management functions
  - Management of monitored devices and assets
  - Creation of users

- Monitoring Event Data
  - Use of the Event Viewer to view real-time data
  - Use of the Query function to define and refine data-retrieval parameters

- Reporting
  - Discussion of the use of RSA enVision to monitor and retrieve historical data for use in compliance and policy reporting
  - Report creation and scheduling
  - Report customization
  - Dashboard reports

- Alerting
  - Discussion of correlating certain events to trigger an alert
  - Creation of basic and correlated Alerts

- Enterprise Dashboard
  - Introduction of the Enterprise Dashboard function and how to manage the Dashboard layout

- Watchlists
  - Use of the Watchlist function to filter events for alerting and reporting purposes

- Vulnerability and Asset Management
  - Description of the Vulnerability and Asset Management functionality to leverage information about enterprise assets and known vulnerabilities in conjunction with IDS systems

- enVision Maintenance
  - Description of backup and restore methodologies and recommendations
  - Description of event-source updates

- Incident Handling
  - Introduction of the enVision Event Explorer feature to retrieve and analyze data
  - Use of Incident Management functionality to create, view, and refine incidents
  - Use of Event Traces for incident investigation

- Principles of Logging
  - Differentiate between events and log messages
  - Describe how log messages are organized
  - Describe how the syslog protocol is used in enVision
  - Identify the structure of support files

- Log Collection Methods and Formats
  - List enVision's alternative log-collection methods
  - Identify when to use a particular collection service
  - Outline the process to set up an alternative collection service
  - Extract log files

- Creating Support Files
  - Describe the EventSource Integrator (ESI)
  - Identify how headers and payloads are defined in ESI
  - Create support files for an unknown event source
  - Create and deploy the event source package
  - Test the event source integration

Course Delivery Options

This course is currently available in the following formats:

ED ENVADESI110: *Public* Instructor- led — includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED ENVADESI210: *On-site* Instructor-led — held at the customer's location; up to 10 students.

ED ENVSNADMINDVD: Video ILT — DVD video provides a recording of an instructor delivered course along with recorded labs, online quizzes, and additional content (includes enVision ESI).

ED ENVTRAIN CREDIT: Training credits for use with any RSA classes

RSA enVision® Advanced Administration
Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

Overview
This course provides in-depth coverage of specific enVision topics in the areas of data collection, reports, alerts, and Event Explorer. Students learn how to configure enVision to collect data from non-syslog collection methodologies. The course provides best practices for reports and alerts and practice using advanced reporting and alerting functions as well as creating advanced charts and tables in Event Explorer.

Audience
Customers and Partners who need to administer the RSA enVision product.

Duration
5 days

Prerequisite Knowledge/Skills
The RSA enVision Administration course and three-to-six months' experience using enVision.

Course Objectives
Upon successful completion of this course, participants should be able to:
- Describe the enVision collection process, including troubleshooting techniques
- Describe various collection methodologies
- Configure enVision to collect data from non-syslog event sources
- Describe how to troubleshoot collection issues
- Describe best practices for reports and alerts
- Identify how to set up a security policy for reporting
- Create reports that support the security policy
- Identify how to plan a strategy for alerting
- Create alerts using multithreading, cache variables, thresholds, and severity levels
- Extract data in Event Explorer using charts and tables
- Identify best practices for charts and tables
- Describe Event Trace data stores
- Create charts using SQL in Event Explorer

Course Outline
The following modules are designed to support the course objectives:

- Configuring Data Collection
  - enVision Collection process
  - Tips and techniques for troubleshooting the Collection process
  - LEA Collection Service configuration and troubleshooting
  - SDEE Collection Service configuration and troubleshooting
  - File Reader Collection Service configuration and troubleshooting
  - Windows Collection Service configuration and troubleshooting
  - Agentless Windows Collection configuration and troubleshooting
  - ODBC Collection Service configuration and troubleshooting
  - SNMP Collection Service configuration and troubleshooting
  - VMware Collector

- Advanced Reporting
  - Security-management reporting strategy
  - Best practices for reports
  - Report performance enhancements
  - Troubleshooting reports

- Advanced Alerting
  - Alert strategy planning
  - Best practices for alerts
  - Rule-creation process
  - Advanced alerting techniques
  - Debugging correlation rules

- Extracting Data Using Event Explorer
  - Exploring taxonomy in Event Explorer
  - Best practices for charts and tables
  - Event trace storage
  - Advanced charting using SQL
  - Data extraction using drill down and data points
  - Extracting data using advanced tables
  - Chart dashboard

Course Delivery Options
This course is currently available in the following formats:

ED ENVADVADM110: *Public* Instructor-led — includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED ENVADVADM210: *On-site* Instructor-led — held at customer's location; up to 10 students.

ED ENVTRAIN CREDIT: Training credits for use with any RSA classes

Information Security Awareness
Course Description

Interface & Interactivity:

- *Easy-to-Navigate Interface*
- *Interactive Learning*
- *Integrated Assessment Quizzes*
- *Auto-Scrolling Transcript*

Engaging Topics:

- *Mitigating Social Engineering Attacks*
- *Email Precautions*
- *Reporting and Responding to Threats (Interactive Scenarios)*
- *Configurable Link to your Internal Security Policy*

DELIVERY:

This SCORM 1.2-compliant course can be integrated into a client's Learning Management System or it can be delivered as an on-demand service through our education portal.

CUSTOMIZATION:

This course can be customized to meet the specific requirements of each client. Clients can customize the course by modifying or removing standard content and/or by adding custom content.

SECURITY IS EVERY EMPLOYEE'S RESPONSIBILITY

Is there anyone in your organization who is not in a position—every day—to behave in a way that either exposes or protects the valuable information that is in their hands? No matter how much technology-based defense and offense you have in place, it's *people* who interact with sensitive information such as personally identifiable information, payment information, intellectual property, protected health information, confidential company plans, and financials.

Employees can carry this sensitive information outside the office on laptops, mobile phones, USB drives, and paper — just in the course of doing their work every day. Security rests with all of your employees. A misstep by any one of them could create an opportunity for a motivated attacker.

A shift in the way employees think about and protect sensitive information can be a company's best protection. The Information Security Awareness eLearning course for general staff is designed to reduce your organization's information risk by increasing security awareness among all your business staff.

Overview

This highly interactive scenario-based course equips employees to recognize the value of different types of information; to understand the scope, nature, and origin of the diverse risks to such information; and to behave proactively to protect this information in their everyday work. Topics include computer crime, social engineering, physical security, technology threats, and information security self-defense.

Audience

This course is appropriate for all employees who have access to an organization's computers, systems, and information.

Duration

Approximately 80 minutes out-of-the-box.

Prerequisite Knowledge/Skills

This introductory course is appropriate for all staff regardless of role. There are no course prerequisites.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Understand computer crimes and criminals
- Understand the insider threat and industrial espionage
- Describe actions that increase identity theft and steps to minimize it
- Understand social engineering; how to spot it and mitigate attacks
- Understand physical security, risks of hardware theft, and travel security
- Understand the threats of computer malware and wireless security
- Identify sensitive data
- Understand email and password precautions

Course Outline

Module 1: Computer Crime

- Introduction to Computer Crime
  - Examples of computer criminals and opponents
  - Examples of recent computer crime
- Identity Theft
  - How attackers use personally identifiable information
  - Actions that increase the potential for identity theft
  - Techniques to minimize the risk of identity theft
- Insider Theft
  - Controls for the insider threat
  - The importance of encrypting sensitive data
  - Impacts of sharing passwords
- Industrial Espionage
  - How individuals and organization use information systems attacks for competitive advantage
  - How the insider threat relates to industrial espionage
  - Controls that help minimize the risk of information system compromises related to industrial espionage

Module 2: Social Engineering

- Introduction to Social Engineering
  - What social engineering is and how it works
  - Examples of real world social engineering attacks
- Tips for Spotting Social Engineering Attacks
  - Techniques that help distinguish between routine inquiries and social engineering attacks
- Best Practices to Mitigate Social Engineering Attacks
  - Best practices that minimize the effectiveness of social engineering attacks

Module 3: Physical Security

- Introduction to Physical Security
  - How attackers bypass physical security features
  - Actions that increase the potential of a successful physical security breach
- Accepted practices for minimizing the risk of a physical security breach
  - Hardware theft
  - Types of data that may be exposed in hardware theft
  - Types of devices at risk for loss or theft
  - Impacts to the business from loss of devices
  - Techniques for minimizing the risk of data exposure due to device loss
  - Why not storing data on mobile devices is safer than the use of encryption or remote wipe technologies

- Travel Security
  - Risks associated with transporting sensitive data
  - The importance of maintaining personal security while traveling
  - Types of conversations never to have in public
  - Techniques and strategies for keeping data secure while traveling
  - Best practices for accessing public computers and sharing information via USB and Bluetooth

Module 4: Technology Threats

- Computer Malware
  - Types of malware that typically infect computers
  - Impacts of malware
  - Strategies to avoid malware
  - Why is antivirus necessary but not sufficient
  - Tools that can complement antivirus
- Wireless Security Risks
  - Risks of wireless technology
  - Using VPNs, SSL, or some other encrypted protocols
  - Best practices for using wireless security

Module 5: Information Security Self Defense.

- Identifying Sensitive Data
  - Distinguishing sensitive data from non-sensitive data
  - Defining Personally Identifiable Information (PII)
  - Different types of sensitive information
  - Examples of sensitive data
- Email Precautions
  - The impact of sending sensitive information over an insecure medium
  - Potential dangers of email attachments
  - Why HTML email can potentially be dangerous
  - Strategies for using email securely
- Password Precautions
  - Risks of weak passwords
  - Distinguishing between strong and weak passwords
  - Creating a strong password that is memorable
  - Why passwords must expire
- Report/Respond Threat
  - When and how to respond to information security threats
  - Customer-specific notes about how and where to report threats

---

Technical Specifications:

All courses are SCORM 1.2-compliant. Courses can be integrated into a client's Learning Management System or delivered as an on-demand service.

Minimum Requirements:

Computer:
- Screen Resolution: 1280x720
- Standard Operating System:
  - Mac OSX 10.x or above
  - Windows XP or above

Web Browser:
- Microsoft internet Explorer 6.0 SP3 or above
- Mozilla Firefox 3.0 or above
- Mac: Safari 4.0 or above

Flash Player:
- Adobe Flash Player v10.0 or above (preferred)
[Courses will work with v8 and 9 but **not** v7.]

Audio:
- Highly recommended
[If sound is unavailable, user can follow on-screen transcript.]

Information Privacy Awareness
Course Description

Interface & Interactivity:

- *Easy-to-Navigate Interface*
- *Interactive Learning*
- *Integrated Assessment Quizzes*
- *Auto-Scrolling Transcript*

Engaging Topics:

- *Securing Personal Information*
- *Transmitting Data Securely*
- *Managing Data Over Time*
- *Service Providers*

Overview
This introductory course is designed for general staff in roles such as human resources, legal, marketing, finance, sales, operations and customer service. This course equips employees to recognize the importance of understanding what constitutes private data and how to behave in a proactive manner to protect this information in their everyday work.

Audience
This course is appropriate for all employees who have access to an organization's computers, systems, and information.

Duration
Approximately 15 minutes out-of-the-box.

Prerequisite Knowledge/Skills
This introductory course is appropriate for all staff regardless of role. There are no course prerequisites.

Course Objectives
Upon successful completion of this course, participants should be able to:

- Identify personal information that must be protected
- Electronically transmit and store personal information securely
- Securely handle physical records
- Maintain the security of personal information over time
- Manage third-party access to personal information

DELIVERY:

This SCORM 1.2-compliant course can be integrated into a client's Learning Management System or it can be delivered as an on-demand service through our education portal.

CUSTOMIZATION:

This course can be customized to meet the specific requirements of each client. Clients can customize the course by modifying or removing standard content and/or by adding custom content.

Course Outline

Module 1: Information Privacy Awareness

- Identifying Personal Information
    - Meeting regulatory requirements
    - Ensuring good business practices
    - Preventing identify theft
    - Accurately identifying personal information
    - Masking personal information

- Electronic Transmission and Storage of Personal Data
    - Encrypting personal data
    - Secure FTP
    - Password protecting files
    - Restricting access

- Physical Data Handling
    - Handling printed documents
    - Securing cabinets, drawers, and doors
    - Properly disposing of paper
    - Securing your workstation

- Managing Data Privacy Over Time
    - Review system access periodically
    - Handling transfers, terminations or role changes
    - Securely disposing of documents
    - IT asset management

- Managing Service Providers
    - Verify security procedures being used
    - Help desk security assessments
    - Validate all personal information requests

- Other Types of Sensitive Data
    - Customer information
    - Project details
    - Intellectual property
    - Financial data

Technical Specifications:

All courses are SCORM 1.2-compliant. Courses can be integrated into a client's Learning Management System or delivered as an on-demand service.

Minimum Requirements:

Computer:
- Screen Resolution: 1280x720
- Standard Operating System:
    - Mac OSX 10.x or above
    - Windows XP or above

Web Browser:
- Microsoft internet Explorer 6.0 SP3 or above
- Mozilla Firefox 3.0 or above
- Mac: Safari 4.0 or above

Flash Player:
- Adobe Flash Player v10.0 or above (preferred)
[Courses will work with v8 and 9 but **not** v7.]

Audio:
- Highly recommended
[If sound is unavailable, user can follow on-screen transcript.]

IT Security Fundamentals
Course Description

Interface & Interactivity:

- *Easy-to-Navigate Interface*
- *Interactive Learning*
- *Integrated Assessment Quizzes*
- *Auto-Scrolling Transcript*

Engaging Topics:

- *Access Control Considerations for Operating Systems, Networks, and Applications*
- *User Access Management*
- *Operational Procedures*
- *Monitoring and Auditing*

DELIVERY:

This SCORM 1.2-compliant course can be integrated into a client's Learning Management System or it can be delivered as an on-demand service through our education portal.

CUSTOMIZATION:

This course can be customized to meet the specific requirements of each client. Clients can customize the course by modifying or removing standard content and/or by adding custom content.

ARMING YOUR ADMINISTRATIVE STAFF WITH ESSENTIAL SECURITY CONCEPTS

Employees who are on the front lines of deploying, managing and securing information technology must be well equipped to protect sensitive information. The IT Security Fundamentals training course was designed specifically to arm employees — from system architects to database administrators — essential information to securely deploy, maintain, and protect the enterprise infrastructure.

Overview

This course is designed to give members of an IT staff a baseline understanding of secure IT Administration by providing them with basic security concepts.

Audience

This course is appropriate for IT operations staff, help desk, and administrators.

Duration

Approximately 120 minutes out-of-the-box.

Prerequisite Knowledge/Skills

This course is appropriate for all administrative staff regardless of role.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Understand access control issues involving operating systems, user management, and authentication
- Understand network access control issues including control restrictions, node authentication, connections, routing, and VPNs
- Understand the importance of application access controls including information access, sensitive system isolation, and separation of duties
- Understand user access management issues and controls including procedures for access rights, privilege management, and role-based access control
- Understand the importance of monitoring systems to ensure conformity with policies, detect unauthorized activities, and determine the effectiveness of security measures
- Recognize the value of operational procedures and responsibilities
- Know how to effectively use audits and auditing tools

Course Outline

Module 1: Application Security: An Introduction

Module 2: Systems Access Control
- Control of access to computer services and data on the basis of business requirements
- Access control policy

Module 3: Operating Systems Access Control
- Automatic terminal identification
- Terminal logon procedures
- User IDs
- Password management
- Event alarming and escalation
- Terminal time out
- Limited connection time
- Biometrics
- RSA SecurID® Tokens
- Single use password devices
- Multi-factor authorization
- Single sign-on/reduced sign-on

Module 4: Network Access Control
- Control of connections to network services to ensure that connected users or computer services do not compromise the security of any other networked services
- Limited services
- Enforced path
- Control restrictions by IP address
- User authentication
- Node authentication
- Remote diagnostic port protection
- Network segregation
- Network connection control
- Network routing control
- Security in network services
- User certificates
- VPN

Module 5: Application Access Control
- Logical access controls to protect application systems and data from unauthorized access
- Information access restriction
- Separation of duties
- Monitoring — user privilege violations
- Unique IDs for tasks
- Information access restriction
- Sensitive system isolation
- Access control to program source libraries

Module 6: User Access Management
- Formal procedures to control allocation of access rights to IT systems and services
- Authorization/Approvers (data owners, Information Stewards/Custodians)
- User registration
- Privilege management
- User password management
- Review of user access rights
- Procedures to remove inactive IDs and IDs that are no longer needed
- Maker/checker process
- RBAC

Module 7: Monitoring Systems Access and Use
- Monitoring systems to ensure conformity with access policy and standards
- Monitoring systems to detect unauthorized activities
- Monitoring systems to determine the effectiveness of adopted security measures
- Event logging
- Clock synchronization
- Centralized log storage and protection
- Log file entries standards

Module 8: Operational Procedures and Responsibilities
- Established responsibilities and procedures for the management and operation of all computers and networks
- Documented operating procedures
- Operational change control procedures and requirements
- Incident management procedures
- Segregation of duties
- Separation of development and operational facilities
- External facilities management

Module 9: Audit Controls and Tools
- Controls to safeguard operational systems and audit tools during system audits
- Minimization of interference to and from the system audit process
- Protection of the integrity and preventing the misuse of audit tools
- Other protection requirements for system audit tools
- Secure storage of audit reports
- Access to audit reports
- Audit occurrence policies, for example, those that must occur annually, triggers for audits, and so forth

---

Technical Specifications:

All courses are SCORM 1.2-compliant. Courses can be integrated into a client's Learning Management System or delivered as an on-demand service.

Minimum Requirements:

Computer:
- Screen Resolution: 1280x720
- Standard Operating System:
  – Mac OSX 10.x or above
  – Windows XP or above

Web Browser:
- Microsoft internet Explorer 6.0 SP3 or above
- Mozilla Firefox 3.0 or above
- Mac: Safari 4.0 or above

Flash Player:
- Adobe Flash Player v10.0 or above (preferred)
[Courses will work with v8 and 9 but **not** v7.]

Audio:
- Highly recommended
[If sound is unavailable, user can follow on-screen transcript.]

RSA® Cloud Security Fundamentals
Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
          781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

Overview

This course provides an overview of the concepts, processes, and best practices needed to successfully secure information within Cloud infrastructures. Students will learn the basic Cloud types and delivery models and develop an understanding of the risk and compliance responsibilities and challenges for each Cloud type and service delivery model. The student will also learn how to apply RSA's trust-based security model to real-world security problems. The course concludes with a module on guidance for building private Clouds and a lab exercise where the student will implement a private cloud using a 3rd party provider's interface.

Some materials in this course have been developed in conjunction with the Cloud Security Alliance.

Audience

This course is meant for RSA/EMC customers who have virtualized a portion of their environment and wish to acquire Cloud services either externally via a public Cloud or to implement Cloud technologies internally (private Cloud). This course will be valuable for those who work in security or virtualization administration, compliance, architecture, and audit roles within their organization.

Duration

4 days

Prerequisite Knowledge/Skills

- Basic familiarity with IT concepts, including storage, computation and networking
- Working knowledge of TCP/IP networking technologies (equivalent to CompTIA Network+ certification)
- Working knowledge of Information Security concepts (equivalent to CompTIA's Security+ certification)
- Conversant with virtualization concepts
- Comfortable using a command-line interface

Course Objectives

Upon successful completion of this course, participants should be able to:
- Identify security aspects of each cloud model
- Develop a risk-management strategy for moving to the Cloud
- Implement a public cloud instance using a public cloud service provider
- Apply RSA's trust-based security model to different layers in the infrastructure stack
- Distinguish between cloud providers and 3rd party managed service providers

Course Outline

The following modules are designed to support the course objectives:

- Introduction to Cloud Computing
  – Cloud Overview
  – Cloud Service Models
  – Cloud Deployment Models

- Managing Cloud Security and Risk
  – Impact of Cloud Tiers on Security and Risk
  – Standards Organization
  – RSA's Cloud Trust model
  – Things to Look for in a Cloud Provider

- Infrastructure Layer Trust
  – Infrastructure Trust Layer Definition
  – Disaster Recovery
  – Virtualization
  – Segmentation and Isolation
  – Log Management
  – Secure Communications
  – Multi-Tenancy

- Application Layer Trust
  – Application Layer Trust: definition
  – Web Application Security Fundamentals
  – Application Security Phases and Lifecycle
  – SDLC
  – PaaS Security Concerns

- Information Layer Trust
  – Information Layer Trust: Definition
  – Data Retention / Destruction
  – Data Leakage
  – Data Privacy
  – Data Encryption and Key Management
  – Data Geolocation
  – E-Discovery
  – Data Portability
  – Data Classification

- Management
  – Management Layer Trust: Definition
  – Identity and Access Management
  – Contract SLAs
  – Roles and Responsibilities
  – Provider Viability
  – Compliance Monitoring
  – Business Continuance
  – Provider Supply Chain
  – Third-party Risk Assessment
  – Software Licensing Risk

- Securing Private Clouds
  – Enterprise IT Evolution
  – Private Cloud Security Primer

- Final Lab Exercise
  – Hands-on exercise in which participants are challenged to build a best-in-class vendor data application with minimal assistance

Course Delivery Options

This course is currently available in the following formats:

ED CLDSECFN110: *Public* Instructor-led — includes hands-on lab exercises that reinforce the concepts covered in lectures.

ED CLDSECFN210: *On-site* Instructor-led — held at the customer's location; up to 10 students.

ED CLDSECFNDVD: *Video ILT* — DVD video provides a recording of an instructor delivered course along with recorded labs, online quizzes, and additional content (includes enVision ESI).

Certified Information Systems Security Professional (CISSP®) Certification Bootcamp

Course Description

Our approach to training is simple — provide training that is relevant, timely, convenient and cost-effective. Our goal is to ensure that you maximize the value of your security investment by understanding RSA technology and solutions at the right level while respecting your budget and your time.

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site, http://www.rsa.com/training

HAVE QUESTIONS?
PLEASE CONTACT US:

Worldwide Training

Email: trainingregistration@rsa.com

Phone: 800-995-5095
        781-515-7700 (International)

Fax: 781-515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

GET PREPPED FOR THE CISSP EXAM BY RSA'S SECURITY EXPERTS

RSA, The Security Division of EMC, has developed an extensive curriculum to prepare candidates to become security practitioners and successfully pass ISC2's CISSP certification exam.

This Certification Bootcamp involves intensive lectures, demonstrations, and review questions delivered by a security professional with years of experience as a practitioner. Not only will participants become prepared to take the exam but the anecdotes and real world examples from this course are invaluable insight into real world security challenges and approaches to solve them.

The modules of this course follow the 10 Domains of the ISC2 Common Body of Knowledge. Each module presents the concepts and vocabulary from a technical and management aspect, bridging the gap that is often present in organizations today, a holistic approach to the technical, physical and administrative controls that make up a security program.

Each module is also followed by review questions, detailed explanations and exam tips related to the material and how it may be presented on the exam.

RSA's CISSP Bootcamp has been updated to reflect the 2012 Domain Name and content changes. Participants will come away empowered for the exam and beyond.

2012 Common Body of Knowledge Domains:

- Access Control
- Telecommunications and Network Security
- Information Security Governance & Risk Management
- Software Development Security
- Cryptography
- Security Architecture and Design
- Security Operations
- Business Continuity and Disaster Recovery
- Legal, Regulations, Investigations and Compliance
- Physical (Environmental) Security

Added Bonus Module: Security Insights from Senior Executives

RSA has a 30-year legacy of working with clients worldwide to deliver security solutions. In this module, we explore the security issues that senior executives from global organizations face as they enable their businesses and implement their security programs. This content is unique to RSA's CISSP Curriculum and not available elsewhere.

ED CISSP110
Public Instructor-Led 5-day course

About RSA Education Services

RSA Education Services provides training worldwide on RSA products and many additional advanced security topics. It is our mission to enable the current and next generation of security professionals to address the latest threats to information and infrastructure security. RSA's CISSP Bootcamp has been developed and reviewed by security practitioners, thought leaders, and contributing authors to the most widely recognized CISSP materials available. When you seek security knowledge, come to the source.

RSA Education Services is not affiliated with ISC2 or its subsidiaries. Participation in this course does not guarantee the successful completion of the ISC2 CISSP Exam. RSA Education Services has developed the course content from direct experience in the areas of the Common Body of Knowledge and has used the ISC2 CISSP Candidate Information Bulletin as a reference as to technical depth and topics on the exam. Course costs do not include exam fees or facilitate exam registration. Exam schedules are available on ISC2.org.

Application Security Fundamentals
Course Description

SOFTWARE DEVELOPMENT TEAMS PLAY A CRITICAL ROLE IN PROTECTING SENSITIVE INFORMATION

By identifying and resolving vulnerabilities early in the software development lifecycle, your team can substantially reduce information risk cost-effectively.

Only recently have companies begun to meaningfully integrate security into the software development lifecycle. Secure coding has been greatly advanced by the adoption of formal software security assurance methodologies such as Microsoft SDL, OWASP's SAAM, and BSIMM. Central to the successful implementation of these methodologies is role-specific training for all development staff — whether they are architects, developers, QA testers, or managers.

Overview

The Application Security Fundamentals eLearning course is designed for all staff who participate in application development projects — developers, architects, testers, and project managers. This introduction to application security equips students with a common vocabulary, an understanding of common attacks against software, and a set of tools and techniques for building more secure applications. Topics include the OWASP Top Ten, key security principles, setting information security goals and controls, validating and sanitizing input and output, and managing risk and security in the software development life cycle.

Audience

This course is appropriate for all staff who participate in application development projects — developers, architects, testers, business analysts, project managers, quality assurance professionals, system administrators, and database administrators.

Duration

Approximately 120 minutes out-of-the-box.

Prerequisite Knowledge/Skills

This introductory course requires basic knowledge of the software development lifecycle.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Understand computer crimes and criminals, information security drivers, and security misconceptions and myths
- Understand injection flaws, cross-site scripting, unvalidated redirects and forwards, and insecure direct object references
- Describe the importance of security goals and controls
- Understand essential strategic, design, and implementation principles
- Describe the importance of input validation and output sanitation
- Understand how to holistically manage risk and incorporate security throughout the software development lifecycle

DELIVERY:

This SCORM 1.2-compliant course can be integrated into a client's Learning Management System or it can be delivered as an on-demand service through our education portal.

CUSTOMIZATION:

This course can be customized to meet the specific requirements of each client. Clients can customize the course by modifying or removing standard content and/or by adding custom content.

Course Outline

Module 1: Application Security: An Introduction

- Computer Crime
  - Reasons why people attack systems
  - Common attack modes
- Computer Crime Incidents
  - Frequency and financial impact of computer crime
- The Hacker's Mindset
  - The hacker's mindset and the impact of faulty assumptions
- Information Security Drivers
  - The business imperatives of information security
  - The technology drivers behind information security
  - The impact of regulations on information security
- Information Security Misconceptions and Myths
  - Common misconceptions about information security
  - The reality behind common information security myths

Module 2: OWASP Top 10 Security Risks

- OWASP Top 10 Security Issues
  - The OWASP security risks and available resources
- Injection Flaws
  - Common types of injection flaws and the impact to an application from an injection flaw
- Cross-Site Scripting
  - Mechanics of a cross-site scripting attack and common mechanisms for defending against cross-site scripting
- Unvalidated Redirects and Forwards
  - How attackers exploit an unvalidated redirect or forward; the controls needed to protect from malicious redirection
- Broken Authentication and Session Management
  - How web applications typically maintain user state
  - Common flaws in authentication and session management mechanisms
- Insecure Direct Object Reference
  - Types of objects often left vulnerable to insecure direct reference and how to mitigate it
- Security Misconfiguration
  - The impact of security misconfiguration and the control developers have over security configuration
- Failure to Restrict URL Access
  - The impact of failure to restrict URL access and potential defense mechanisms to properly restrict URL access
- Cross-Site Request Forgery
  - The mechanics of a cross-site request forgery flaw and how to remediate cross-site request forgery issues
- Insufficient Transport Layer Protection
  - Risk to applications that do not provide transport layer security and mechanisms to provide it
- Cryptographic Storage
  - The need to protect data at rest; the characteristics of strong cryptography

Module 3: Information Security Goals and Controls

- Introduction to Security Goals and Controls
  - The three security goals: confidentiality, integrity, and availability
  - The three security controls: authentication, authorization, and auditing
- Security Goals
  - The impact of confidentiality on system design and development
  - Threats to data integrity
  - Issues of system availability
- Security Controls
  - Different types of authentication factors
  - How users and data are categorized for the purposes of authorization
  - Auditing best practices

Module 4: Security Principles

- Strategic Principles
  - How complexity and security are often at odds; the importance of layered security
- Design Principles
  - The principle of least privilege; the security benefits of segmentation
- Implementation Principles
  - The importance of proper error handling and the security benefits of input validation and output sanitization

Module 5: Handling Input and Output Securely

- Input Validation
  - The importance of effective input validation in applications and the different roles responsible
  - How to implement effective input validation principles in applications to handle common threats
  - Real-world examples of input validation
- Output Sanitization
  - The necessity of effective application output sanitization
  - How to implement output sanitization measures to handle common output error messages in applications
  - Real-world examples of output sanitization

Module 6: Managing Security and Risk in the Software Development Lifecycle (SDLC)

- Risk Management
  - Four ways to manage security risk
  - Potential security risks involved in applications
  - The importance of documentation in maintaining security
- SDLC
  - The importance of incorporating security throughout the entire SDLC
  - Ways to incorporate security into each development phase

Technical Specifications:

All courses are SCORM 1.2-compliant. Courses can be integrated into a client's Learning Management System or delivered as an on-demand service.

Minimum Requirements:

Computer:
- Screen Resolution: 1280x720
- Standard Operating System:
  – Mac OSX 10.x or above
  – Windows XP or above

Web Browser:
- Microsoft internet Explorer 6.0 SP3 or above
- Mozilla Firefox 3.0 or above
- Mac: Safari 4.0 or above

Flash Player:
- Adobe Flash Player v10.0 or above (preferred)
[Courses will work with v8 and 9 but **not** v7.]

Audio:
- Highly recommended
[If sound is unavailable, user can follow on-screen transcript.]

Application Security Fundamentals for Managers

Course Description

Interface & Interactivity:

- *Easy-to-Navigate Interface*
- *Interactive Learning*
- *Integrated Assessment Quizzes*
- *Auto-Scrolling Transcript*

Engaging Topics:

- *Application Security*
- *Information Security Goals*
- *Security Principles*
- *Managing Security and Risk*

Overview

The Application Security Fundamentals course for managers is designed to introduce managers to the basics of application security. The course introduces the essential goals and controls needed to create secure software and properly manage risk in the software development lifecycle.

Audience

This course is appropriate for managers of the software development lifecycle.

Duration

Approximately 120 minutes out-of-the-box.

Prerequisite Knowledge/Skills

Students should have an understanding of information security basics before taking this course. This foundational course requires basic knowledge of the software development lifecycle.

Course Objectives

Upon successful completion of this course, participants should be able to:

- List the reasons people attack systems
- Challenge misconceptions about information security
- Identify auditing best practices
- List the four strategic, design, and implementation principles of security
- Incorporate security into each software development phase
- Communicate risk to stakeholders

DELIVERY:

This SCORM 1.2-compliant course can be integrated into a client's Learning Management System or it can be delivered as an on-demand service through our education portal.

CUSTOMIZATION:

This course can be customized to meet the specific requirements of each client. Clients can customize the course by modifying or removing standard content and/or by adding custom content.

Course Outline

Module 1: Application Security: An Introduction

- Describe the reasons people attack systems
- Identify the business imperatives of information security
- Challenge misconceptions about information security

Module 2: Information Security Goals and Controls

- Explain the impact of confidentiality on system design and development
- Describe the different types of authentication factors
- Identify auditing best practices

Module 3: Security Principles

- Identify the four strategic principles of security
- Identify the four design principles of security
- Identify the four implementation principles of security

Module 4: Managing Security and Risk in the SDLC

- Describe the importance of incorporating security throughout the entire SDLC
- Illustrate various ways to incorporate security into each development phase
- Communicate risk to application stakeholders

-

Technical Specifications:

All courses are SCORM 1.2-compliant. Courses can be integrated into a client's Learning Management System or delivered as an on-demand service.

Minimum Requirements:

Computer:
- Screen Resolution: 1280x720
- Standard Operating System:
  - Mac OSX 10.x or above
  - Windows XP or above

Web Browser:
- Microsoft internet Explorer 6.0 SP3 or above
- Mozilla Firefox 9.0 or above
- Mac: Safari 4.0 or above

Flash Player:
- Adobe Flash Player v10.0 or above (preferred)
[Courses will work with v8 and 9 but **not** v7.]

Audio:
- Highly recommended
[If sound is unavailable, user can follow on-screen transcript.]

Secure Architecture and Design
Course Description

Interface & Interactivity:

- *Easy-to-Navigate Interface*
- *Interactive Learning*
- *Integrated Assessment Quizzes*
- *Auto-Scrolling Transcript*

Engaging Topics:

- *Network Security*
- *Host Security*
- *Managing Risk*
- *Real-world Architecture Review*
- *Security Leadership*

DELIVERY:

Instructor-led.

CUSTOMIZATION:

This course can be customized to meet the specific requirements of each client. Clients can customize the course by modifying or removing standard content and/or by adding custom content.

Overview

This course is designed to give an architect or senior developer a comprehensive understanding of the risks of building today's information systems, using the students' own architectures as examples, so results are directly applicable after the class. The class includes a live review of these actual architectures to demonstrate how to conduct a full-fledged architecture review.

Audience

This course is appropriate for experienced developers and architects that need to understand how to architect and design secure systems. No background in information security is necessary.

Duration

1 days

Prerequisite Knowledge/Skills

Course attendees are strongly recommended to have an understanding of security fundamentals before taking this course. RSA's 1-day course titled *Application Security Fundamentals* is the ideal prerequisite.

Course Objectives

Upon successful completion of this course, participants should be able to:

- List network security tools and recommendations for securing the network
- Discuss host security concepts covering common malware including worms, viruses, spyware, Trojan horses, and root kits
- Identify the SANS Top 25 list of critical software vulnerabilities
- Design an architecture diagram
- Discuss how to manage security as risk and communicate this risk throughout the organization
- Determine the level of risk inherent in their own applications
- Conduct a security architecture review using their own architecture
- Discuss security leadership and the role architects play in the overall environment and defenses

Course Outline

Day 1: Duration 8 hours

- Security Fundamentals Review: Quick review of topics that will be discussed in depth later on in the course to ensure consistent foundational knowledge and address any minor gaps students may have

- Network Security: Overview of network security concepts, including demonstrations of common network security tools and recommendations for securing the network

- Host Security: Overview of host security concepts, covering common malware including worms, viruses, spyware, Trojan horses, and root kits, and offering recommendations for securing hosts

- Application Security: Introduces the SANS Top 25 list of critical software vulnerabilities and covers several key issues

- Case Study: Draw your Architecture: Students draw a diagram of an architecture that they are familiar with and these examples are used extensively throughout the course

- Identifying & Managing Risk: A discussion of how to manage security as risk and communicate this risk throughout the organization

- Feasibility/Risk Rating: Students learn how to determine the level of risk inherent in their own applications

- Lab: Real-world Architecture Review: Students learn how to conduct a security architecture review using their own architecture

- Security Leadership: Discussion of security leadership and the role architects play in the overall environment and defenses

Secure Client/Server Development in C/C++
Course Description

Interface & Interactivity:

- *Easy-to-Navigate Interface*
- *Interactive Learning*
- *Integrated Assessment Quizzes*
- *Auto-Scrolling Transcript*

Engaging Topics:

- *Secure C/C++ Coding*
- *Memory corruption Bugs*
- *Design Bugs*
- *Privacy and Secrets*
- *Secure Coding*

COURSE OVERVIEW

This advanced course is designed for software developers creating applications in the C/C++ family of languages. This highly interactive scenario-based course equips developers to recognize the common causes of software bugs to mitigate security issues. Along with summarizing the mechanics of memory corruption bugs and understanding the difference between good and bad exception handling with design bugs, learners will be able to express the implications of privacy issues and understand various approaches to code review.

AUDIENCE

This course is appropriate for all developers creating applications in C/C++.

DURATION

Approximately 150 minutes out-of-the-box.

PREREQUISITE KNOWLEDGE/SKILLS

This advanced course requires knowledge of the C/C++ language and familiarity with creating applications in C/C++.

COURSE OBJECTIVES

Upon successful completion of this course, participants should be able to:

- List the key attributes of secure C/C++ coding
- Identify vulnerabilities in the Software Development Lifecycle (SDLC)
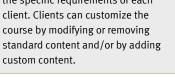- Detect and diagnose memory corruption bugs
- Appropriately handle exceptions and privileges in C/C++
- Identify how privacy relates to software development
- Review methods for protecting privacy and secrets
- Compare and contract techniques used to secure code

DELIVERY:

This SCORM 1.2-compliant course can be integrated into a client's Learning Management System or it can be delivered as an on-demand service through our education portal.

CUSTOMIZATION:

This course can be customized to meet the specific requirements of each client. Clients can customize the course by modifying or removing standard content and/or by adding custom content.

COURSE OUTLINE

Module 1: Introduction to Secure C/C++ Coding

- Introduce the key attributes of C and C++
- Create a foundation for working with the C/C++ family of languages
- Introduce the vulnerabilities that exist in the Software Development Life Cycle (SDLC)
- Review common causes of software bugs

Module 2: Memory Corruption Bugs

- Develop efficient applications free of errors
- Review C/C++ memory layouts
- Identify the various types of memory corruption bugs
- Compare examples of each bug type
- Detect and diagnose bugs in applications

Module 3: Design Bugs

- Introduce design bugs, exceptions, and privileges
- Review and compare proper and improper exception handling
- Correctly handle exceptions
- List the implications of privilege within C and C++

Module 4: Privacy and Secrets

- Identify how to keep data private
- Review privacy issues
- List the negative implications from improper data handling
- Review effective methods and tactics for protecting privacy and secrets
- Compare cryptography, passwords and random numbers

Module 5: Securing Code

- Analyze, review and verify code securing techniques
- Protect data through formal methods
- Compare and contrast static and dynamic testing techniques
- Discuss various approaches to accurate code review

Technical Specifications:

All courses are SCORM 1.2-compliant. Courses can be integrated into a client's Learning Management System or delivered as an on-demand service.

Minimum Requirements:

Computer:
- Screen Resolution: 1280x720
- Standard Operating System:
  – Mac OSX 10.x or above
  – Windows XP or above

Web Browser:
- Microsoft internet Explorer 6.0 SP3 or above
- Mozilla Firefox 9.0 or above
- Mac: Safari 4.0 or above

Flash Player:
- Adobe Flash Player v10.0 or above (preferred)
[Courses will work with v8 and 9 but **not** v7.]

Audio:
- Highly recommended
[If sound is unavailable, user can follow on-screen transcript.]

Secure Web Development in Java™
Course Description

Interface & Interactivity:

- *Easy-to-Navigate Interface*
- *Interactive Learning*
- *Integrated Assessment Quizzes*
- *Auto-Scrolling Transcript*

Engaging Topics:

- *Application Vulnerabilities*
- *Logging Framework*
- *Input Validation*
- *Data access Threats*
- *Data Breaches*

Overview
This course offers training on the administration, installation, and configuration of RSA Authentication Manager Express, Authentication Agents, and other RSA AMX system components. The working principles behind RSA AMX technology, architecture, system components, and administrative tasks are discussed. Video demonstrations reinforce the tasks involved in administering an RSA AMX solution.

Audience
System, security, or help desk personnel who need to install, deploy, and/or maintain an RSA Authentication Manager Express system.

Duration
2 hours

Prerequisite Knowledge/Skills
Familiarity with user and system administration, networking fundamentals, and general information security concepts.

Course Objectives
Upon successful completion of this course, participants should be able to:
- Explain the basic architecture and theory of operation of the RSA Authentication Manager Express product
- Describe the configuration required for RSA Authentication Manager Express system operations
- Perform user administration functions to populate and manage users
- Understand the ongoing maintenance requirements
- Plan and perform pre-installation, installation, and configuration tasks for RSA Authentication Manager Express Appliance
- Create redundant/failover RSA Authentication Manager replica servers and understand the role and management of replica server instances
- Install and configure RSA Authentication Agent hosts for local workstation and web access protection
- Understand the setup and use of RSA Authentication Manager Express web tiers

DELIVERY:

This SCORM 1.2-compliant course can be integrated into a client's Learning Management System or it can be delivered as an on-demand service through our education portal.

CUSTOMIZATION:

This course can be customized to meet the specific requirements of each client. Clients can customize the course by modifying or removing standard content and/or by adding custom content.

Course Outline

Module 1: Security for Web Applications

- Identify why web applications are vulnerable to security defects
- List common Web application vulnerabilities
- Mitigate threats associated with data tampering, cross-site scripting, request forgery, and HTTP response splitting

Module 2: Input Validation and Output Sanitization

- Discuss why it is important to validate input
- List input sources and validation techniques
- Perform proper input validation techniques

Module 3: Logging and Exception Handling

- Discuss logging basics
- Compare and contrast log4j and JDK logging frameworks
- Discuss exception handling in Java
- Properly handle exceptions in Java code

Module 4: Data Access Security Basics

- Discuss data access threats
- Examine defenses to ward off data access threats

Module 5: Privacy and Secrets

- Discuss how recent data breaches impact development efforts
- List potential impacts of failing to create a clean production environment
- Securely handle outbound password storage
- Choose the correct type of random number generator
- Discuss the benefits of using prebuilt cryptographic protocols and tools

---

Technical Specifications:

All courses are SCORM 1.2-compliant. Courses can be integrated into a client's Learning Management System or delivered as an on-demand service.

Minimum Requirements:

Computer:
- Screen Resolution: 1280x720
- Standard Operating System:
  - Mac OSX 10.x or above
  - Windows XP or above

Web Browser:
- Microsoft internet Explorer 6.0 SP3 or above
- Mozilla Firefox 9.0 or above
- Mac: Safari 4.0 or above

Flash Player:
- Adobe Flash Player v10.0 or above (preferred)
[Courses will work with v8 and 9 but **not** v7.]

Audio:
- Highly recommended
[If sound is unavailable, user can follow on-screen transcript.]

RSA

EMC²

Secure Web Development in .NET™

Course Description

Overview

The Secure Web Development in .NET course is designed to teach learners the importance of security for web applications written in the .NET framework, illustrating authentication and authorization methods, identifying how to properly handle exceptions and understanding basic session management. Learners will also be introduced to many common application testing approaches.

Audience

This course is appropriate for all developers and architects creating Web applications in .NET.

Duration

Approximately 120 minutes out-of-the-box.

Prerequisite Knowledge/Skills

This intermediate course requires knowledge of the .NET framework and familiarity with creating applications in .NET.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Identify the importance of authentication in .NET applications
- Create code to authenticate end users using ASP .NET applications
- Apply different authentication mechanisms to write secure code and authenticate end users
- Define the process of authorization in .NET applications
- Explain the need for authorization verification and compliance in .NET applications
- Discuss the methods and forms of authorization used in .NET applications
- Identify the issues related to logging in .NET applications
- Perform logging in .NET applications
- List the general considerations for secure exception handling in .NET
- Use the Microsoft Enterprise Library's Exception Handling application

Course Outline

Module 1: Authentication in .NET Applications

- Identify the importance of authentication in .NET applications
- Create code to authenticate end users using ASP .NET applications
- List the issues to be considered when performing authentication between applications
- Apply different authentication mechanisms to write secure code and authenticate end users

Module 2: Authorization in .NET Applications

- Define the process of authorization in .NET applications
- Identify common pitfalls related to authorization in .NET applications
- Use the Microsoft Authorization Manager to configure role-based authorization in .NET applications
- Explain the need for authorization verification and compliance in .NET applications
- Discuss the methods and forms of authorization used in .NET applications

Module 3: Auditing and Logging

- Explain the need for logging in .NET applications
- Identify the issues related to logging in .NET applications
- Perform logging in .NET applications using log4net
- Perform logging in .NET applications using the Microsoft Enterprise Library

Module 4: Exception Handling in .NET Applications

- List the general considerations for secure exception handling in .NET
- Use the try, catch, and block code to handle exceptions
- Identify the mechanism for handling missed exceptions
- Use the Microsoft Enterprise Library's Exception Handling application

---

Technical Specifications:

All courses are SCORM 1.2-compliant. Courses can be integrated into a client's Learning Management System or delivered as an on-demand service.

Minimum Requirements:

Computer:
- Screen Resolution: 1280x720
- Standard Operating System:
  – Mac OSX 10.x or above
  – Windows XP or above

Web Browser:
- Microsoft internet Explorer 6.0 SP3 or above
- Mozilla Firefox 9.0 or above
- Mac: Safari 4.0 or above

Flash Player:
- Adobe Flash Player v10.0 or above (preferred)
[Courses will work with v8 and 9 but **not** v7.]

Audio:
- Highly recommended
[If sound is unavailable, user can follow on-screen transcript.]

Secure Web Development in PHP

Course Description

Interface & Interactivity:

- *Easy-to-Navigate Interface*
- *Interactive Learning*
- *Integrated Assessment Quizzes*
- *Auto-Scrolling Transcript*

Engaging Topics:

- *Application Security*
- *Data Security*
- *Authentication*
- *Authorization*
- *Logging*

Overview

The Secure Web Development in PHP course is designed to teach learners the importance of security for web applications written in the PHP language, illustrating why web applications are vulnerable, identifying what vulnerabilities look like and understanding how to mitigate these threats. Learners will also be able to understand how to securely interact with supporting systems in order to holistically address security concerns.

Audience

This course is appropriate for all developers and architects creating Web applications in PHP.

Duration

Approximately 120 minutes out-of-the-box.

Prerequisite Knowledge/Skills

This intermediate course requires knowledge of the PHP language and familiarity with creating applications in PHP.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Discuss the importance of application security
- Demonstrate the importance of adhering to application security principles
- Perform proper input/output security techniques
- Execute proper data security measures for an application
- Implement a multifaceted approach to secure data access
- Choose the correct session management best practices for various attack vectors
- Apply secure coding principles to mitigate against attacks
- Discuss the importance of exception catching, error reporting, and logging

DELIVERY:

This SCORM 1.2-compliant course can be integrated into a client's Learning Management System or it can be delivered as an on-demand service through our education portal.

CUSTOMIZATION:

This course can be customized to meet the specific requirements of each client. Clients can customize the course by modifying or removing standard content and/or by adding custom content.

Course Outline

Module 1: Application Security: An Introduction

- Discuss the importance of application security
- Demonstrate the importance of adhering to application security principles
- Provide examples of solutions which conform to each application security principle

Module 2: Handling Input and Output Securely

- Identify the risks associated with improper input/output handling
- List the best practices for input/output security
- Perform proper input/output security techniques

Module 3: Data Security

- Discuss the importance of securing data and common attacks that target data
- List data security best practices
- Execute proper data security measures

Module 4: Authentication and Authorization

- Discuss the common vulnerabilities that exist related to authentication and authorization
- Demonstrate the importance of and articulate various methods of authentication and authorization
- Implement a multifaceted approach to secure data access using authentication and authorization

Module 5: Session Management

- Discuss examples of common session management attacks
- Compare session management best practices for various attack vectors
- Illustrate how to construct a secure session management environment

Module 6: Secure System Access

- Defend against exploits present in common system components such as files, includes, and commands
- Discuss the importance of securing all system components to add an additional layer of protection
- Apply secure coding principles to mitigate against attacks

Module 7: Logging and Exception Handling

- Discuss the importance of exception catching, error reporting, and logging
- Identify the best exception handling and logging methods available for an application
- Implement safeguards for applications

Technical Specifications:

All courses are SCORM 1.2-compliant. Courses can be integrated into a client's Learning Management System or delivered as an on-demand service.

Minimum Requirements:

Computer:
- Screen Resolution: 1280x720
- Standard Operating System:
  - Mac OSX 10.x or above
  - Windows XP or above

Web Browser:
- Microsoft internet Explorer 6.0 SP3 or above
- Mozilla Firefox 9.0 or above
- Mac: Safari 4.0 or above

Flash Player:
- Adobe Flash Player v10.0 or above (preferred)
[Courses will work with v8 and 9 but **not** v7.]

Audio:
- Highly recommended
[If sound is unavailable, user can follow on-screen transcript.]