NetWitness Platform Training

Learn to Detect, Investigate, and Respond to Threats

community.rsa.com/community/training
# Table of Contents

About RSA ................................................................................................................................................. 3  
RSA NetWitness Platform Evolved SEIM ................................................................................................. 3  
RSA University ........................................................................................................................................... 3  
RSA NetWitness Role-based Learning Paths ............................................................................................. 4  
RSA Learning Modalities ......................................................................................................................... 5  
  Subscription Model ................................................................................................................................. 6  
RSA University On-Demand Subscriptions and Packages (NetWitness) .................................................. 7  
  Classroom Training ................................................................................................................................. 8  
RSA NetWitness Platform Foundations ..................................................................................................... 9  
RSA NetWitness Endpoint Foundations ................................................................................................... 10  
RSA NetWitness Platform Administration I ............................................................................................. 11  
RSA NetWitness Platform Administration II .......................................................................................... 12  
RSA NetWitness Platform Analysis ....................................................................................................... 13  
RSA NetWitness Platform Content Creation ........................................................................................... 14  
RSA NetWitness Platform Introduction to Hunting ................................................................................ 15  
RSA NetWitness Platform Reporting ...................................................................................................... 16  
  On Demand Learning ............................................................................................................................ 17  
  Introduction to the RSA NetWitness Platform .................................................................................... 18  
RSA NetWitness Platform 11.5: What’s New ......................................................................................... 19  
RSA NetWitness Ueba (User and Entity Behavior Analytics) Overview ................................................... 20  
RSA NetWitness Orchestrator Built on ThreatConnect - Fundamentals ................................................. 21  
RSA NetWitness Log Parser Tool ........................................................................................................... 22  
RSA NetWitness Platform ESA Fundamentals ....................................................................................... 23  
RSA NetWitness Platform ESA EPL Rules .............................................................................................. 24  
RSA NetWitness Lua Parsers for Logs ..................................................................................................... 25  
RSA NetWitness Endpoint YARA Rules ................................................................................................... 26  
  On Demand Labs .................................................................................................................................... 27  
  RSA NetWitness Orchestrator Built on ThreatConnect - Incident Response ................................. 28  
RSA NetWitness Log Parser Creation ..................................................................................................... 29  
RSA NetWitness Logs Event Source Configuration .............................................................................. 30  
  RSA Proven Professional Product Certification Program ................................................................... 31  
RSA Proven Professional Certification Program .................................................................................... 32  
  Industry / Information Security ............................................................................................................. 34  
  Training and Certification ....................................................................................................................... 34  
RSA Certified Information Systems Security Professional (CISSP) Certification Review ....................... 35  
EC Council Certified Network Defender (CND) ...................................................................................... 36  
EC Council Certified Threat Intelligence Analyst (CTIA) ........................................................................ 37  
EC Council: Certified Ethical Hacking (CEH) ......................................................................................... 38  
EC Council Certified Security Analyst (ECSA) ......................................................................................... 40  
EC Council Computer Hacking Forensic Investigator (CHFI) ............................................................... 41  
EC Council Certified Incident Handler (ECIH) ......................................................................................... 43  
EC Council Advanced Penetration Testing (APT) ................................................................................... 44  
EC Council Certified Chief Information Security Officer (CCISO) ......................................................... 45  
Additional Resources ............................................................................................................................... 46  
RSA NetWitness Platform and Information Security Matrix ................................................................... 47
About RSA
RSA is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

RSA helps more than 30,000 customers around the world take command of their security posture by partnering to build and implement business-driven security strategies. With RSA's award-winning cybersecurity solutions, organizations can effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. For more information, please visit www.RSA.com or email RSA_Global_Services_Sales@RSA.com.

RSA NetWitness Platform Evolved SEIM
Logs | Network | Endpoint | UEBA | O&A
Learn to Detect, Investigate, and Respond to Threats

The RSA NetWitness Platform applies the most advanced technology to enable security teams to work more efficiently and effectively. It uses behavioral analysis, data science techniques and threat intelligence to help analysts detect and resolve both known and unknown attacks BEFORE they disrupt your business. And it uses machine learning to automate and orchestrate the entire incident response lifecycle. Because the RSA NetWitness Platform does all of this—and more—on a single platform, it allows security teams to collapse disparate security tools and the data they generate into a single, powerful and blazingly fast user interface.

Organizations across industries face a Catch-22 with technology: The very technologies they need to compete—cloud applications, virtual infrastructure, mobile devices, etc.—provide attackers with more vulnerabilities to exploit and more ways to evade detection. Meanwhile, attackers have more resources than ever for surveilling organizations' infrastructure and launching their attacks, while security teams struggle with a talent shortage and an ever-expanding list of alerts.

The RSA NetWitness Platform was designed with these challenges in mind. It brings together evolved SIEM and threat defense solutions that deliver unsurpassed visibility, analytics and automated response capabilities to help security teams detect, prioritize and investigate threats across their organization’s entire infrastructure.

RSA University
RSA University (RSAU) offers technical training solutions that bolster performance of your security team and boost the security savvy of your organization's employee population. RSA University is your single source of learning for product enablement, certifications, and industry training that secures your world.

RSAU offers product training in a variety of learning modalities to meet every need of our customers. This catalog will review the product training for NetWitness – including learning paths, course descriptions, pricing, subscription models, and certification. RSAU also delivers a variety of information security training and certification programs in the field of cybersecurity.
RSA NetWitness Role-based Learning Paths
RSA Learning Modalities
For your convenience, RSA University offers a variety of LIVE and ON-DEMAND delivery options

Live Classroom
- Scheduled, in-person classroom training; formerly known as instructor-led training (ILT)
- Ranges from one to several days
- Delivery Options: Private (On-Site) or Open Enrollment

Virtual Classroom
- Live training delivered by an instructor in a virtual classroom, either online or remote
- Ranges from one to several days
- Delivery Options: Private (On-Site) or Open Enrollment

On-Demand Learning
- Self-paced online training; formerly known as “eLearning”
- Ranges from minutes to hours of content
- Available at any time

On-Demand Lab
- Self-paced online training including On-Demand Learning and hands on lab activities
- Ranges from 1 to many hours of activity
- Available at any time

On-Demand Classroom
- Self-paced online training including a recorded classroom experience; content equivalent to the Live Classroom training
- Access to RSA University’s virtual lab environment includes the same hands on labs as in the Live Classroom training
- Available at any time

REGISTER FOR CLASSES:
For an up-to-date schedule of our Live Classroom and other training options, visit the RSA University pages on RSA Link-RSA’s community web site: community.rsa.com/community/training.

CONTACT US:
Click to contact us
Phone: 800-995-5095
Int'l: 781-515-7700
Fax: 781-515-6630
174 Middlesex Turnpike
Bedford, Massachusetts 01730
Subscription Model
RSA University On-Demand Subscriptions and Packages (NetWitness)

Start your learning journey with RSA University’s new On-Demand Subscriptions and Packages for RSA NetWitness. These offerings provide learners a flexible way to access the training they need when they need it. The subscriptions and packages allow self-paced enablement at a significant discount versus Live Classroom training.

Subscription and packaged are value-priced to allow a single student to select the On-Demand courses of interest during a one (1) year period. Courses designated in the catalog as “Coming Soon” as well as any new training which becomes available as an On-Demand delivery option are included in these On-Demand Subscription(s).

### 1-Year Individual Subscription and Packages Option Descriptions

<table>
<thead>
<tr>
<th><strong>RSA NetWitness Platform On-Demand (OD) Subscription</strong></th>
<th><strong>SKU/Pricing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes all OD Classroom, OD Labs and OD Learning for both Administrators and Analysts (see below for list of courses)</td>
<td>ED-NW-ODSUB-LVL1 $7,000 USD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>RSA NetWitness Administrator On-Demand (OD) Training Package</strong></th>
<th><strong>SKU/Pricing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes all OD Classroom, OD Labs and OD Learning for Administrators</td>
<td>ED-NW-ODPKG-ADMN $5,000 USD</td>
</tr>
<tr>
<td><strong>On-Demand Classroom:</strong> NW Platform Foundations, NW Endpoint Foundations, NW Platform Administration I, NW Platform Administration II, NW Content Creation, NW Platform Reporting</td>
<td></td>
</tr>
<tr>
<td><strong>On-Demand Learning:</strong> NW Platform ESA Fundamentals, NW Endpoint Insights Overview, NW Platform ESA EPL Rules, NW Platform Endpoint YARA Rules, NW Platform Lua Parser for Logs</td>
<td></td>
</tr>
<tr>
<td><strong>On-Demand Labs:</strong> NW Logs Event Source Configuration, NW Log Parser Creation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>RSA NetWitness Analyst On-Demand (OD) Training Package</strong></th>
<th><strong>SKU/Pricing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes all OD Classroom, OD Labs and OD Learning for Analysts</td>
<td>ED-NW-ODPKG-ANLY $5,000 USD</td>
</tr>
<tr>
<td><strong>On-Demand Classroom:</strong> NW Platform Foundations, NW Endpoint Foundations, NW Platform Analysis, NW Introduction to Hunting, NW Content Creation</td>
<td></td>
</tr>
<tr>
<td><strong>On-Demand Learning:</strong> NW Platform ESA Fundamentals, NW Endpoint Insights Overview, NW Platform ESA EPL Rules, NW Platform Lua Parser for Logs, NW Endpoint Yara Rules</td>
<td></td>
</tr>
<tr>
<td><strong>On-Demand Labs:</strong> NW Orchestrator (ThreatConnect 6.0) Incident Response, NW Log Parser Creation</td>
<td></td>
</tr>
</tbody>
</table>

*Consult your RSA Sales or Partner Rep for local (Geo-based) pricing; no other discounts apply. Value is not transferable. Training credits cannot be used for this special offer.

### BENEFITS

- One easy transaction
- Over 2x the value vs. buying individually
- Convenient, self-paced curriculum
- Content equivalent to Live Classroom, including the same hands-on labs
- Great way to get the training needed to get certified (self-paced training allows you to go back and take modules over as needed)
- Each Package and Subscription includes a Pearson Vue certification voucher, click here for more information on the RSA Certification Program

For further information regarding RSA NetWitness training courses and what is included as part of the subscription and package training offerings, please visit the RSA NetWitness Platform Training web site.

[Click here](#) to see a description of RSAU’s Learning Modalities.

[Click here](#) to browse RSA University’s Course Catalogs.

[Click here](#) to contact RSA University.
Classroom Training
RSA NetWitness Platform Foundations

At-A-Glance
This foundations course focuses on the core features and functions of the RSA NetWitness Platform for Administrators and Analysts.

Overview
This live classroom training provides a foundational overview of the core components of RSA NetWitness Platform. Students gain insight into the core concepts, uses, functions and features of RSA NetWitness Platform and also gain practical experience by performing a series of hands-on labs.

Audience
Anyone new to RSA NetWitness Platform

Delivery Type
- Classroom (delivered live) 3 days
- Virtual Classroom (live learning delivered remotely) 3 days
- On-Demand Classroom 3 days
  (self-paced recorded classroom experience; includes 20 hours of lab access over a 4-week period)

Prerequisite Knowledge/Skills
Students should be familiar with basic computer architecture, networking fundamentals and general information security concepts. Basic knowledge of the TCP/IP protocol stack is beneficial.

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

- Describe the RSA NetWitness Logs & Network architecture, components and functions
- Describe how metadata is created
- Differentiate between meta keys, meta values, and metadata
- Investigate data using simple and complex queries
- Customize the investigation display
- Filter data using rules
- Create new meta values using Application and Correlation rules and RSA Live content
- Create alerts using ESA and reporting rules to track potential threats
- Create and manage incidents

FIND OUT MORE
RSA NetWitness Endpoint Foundations

At-A-Glance
This classroom-based training introduces security analysts and executives to the major features of RSA NetWitness Endpoint, including Instant Indicators of Compromise and the Modules and Machines interfaces.

Overview
This classroom-based training provides a general introduction to RSA NetWitness Endpoint functionality. Students will participate in both lecture and hands-on experience using the RSA NetWitness Endpoint tool. The two days consist of about 50% lecture and 50% hands-on lab work in a virtual environment.

Audience
Anyone new to RSA NetWitness Endpoint interested in increasing their familiarity with the tool's analysis and admin functionality. Familiarity with other RSA NetWitness Platform tools is recommended.

Delivery Type
- Classroom (delivered live) 2 days
- Virtual Classroom (live learning delivered remotely) 2 days
- On-Demand Classroom 2 days
  (self-paced recorded classroom experience; includes 20 hours of lab access over a 4-week period)

Prerequisite Knowledge/Skills
- RSA NetWitness Platform Fundamentals
- Also recommended: basic knowledge of malware, networking fundamentals and general security concepts is recommended.

Learning Objectives
Upon successful completion of this training, participants should be able to:
- Define what NetWitness Endpoint is and what it does
- Identify architecture components
- Triage assessment of potentially malicious files and hosts by risk score
- Navigate the NetWitness Endpoint interface to investigate suspicious files and processes
- Customize the Endpoint interface
- Perform basic threat assessment in context of NetWitness meta

FIND OUT MORE
RSA NetWitness Platform Administration I

At-A-Glance

Are you an RSA NetWitness customer looking an overview of essential administrative tasks that are performed for the RSA NetWitness Platform – this course is for you.

Overview

This classroom-based course provides an overview of essential administrative tasks that are performed for RSA NetWitness Platform up and running. Students gain insight into configuring hosts and services and managing users within RSA NetWitness Platform and gain practical experience by performing a series of hands-on labs.

Audience

Anyone who is interested in the administration and operations of the RSA NetWitness Platform.

Delivery Type

- Classroom (delivered live) 2 days
- Virtual Classroom (live learning delivered remotely) 2 days
- On-Demand Classroom 2 days
  (self-paced recorded classroom experience; includes 20 hours of lab access over a 4-week period)

Prerequisite Knowledge/Skills

It is recommended that students complete the following courses prior to taking this training:

- RSA NetWitness Platform Foundations (ILT)

Learning Objectives

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

- Describe the RSA NetWitness Platform Architecture
- Configure RSA NetWitness hosts
- Configure RSA NetWitness system settings
- Describe the RSA NetWitness licensing model
- Configure Event Stream Analysis
- Configure the Archiver
- Configure RSA Live
- Configure the Context Hub
- Configure the Reporting Engine
- Manage NetWitness services on the command line
- Gather data for RSA Customer Support using a script
- Configure the NetWitness Endpoint Log Hybrid
- Generate and deploy the NetWitness Endpoint Agents
- Configure NetWitness Endpoint agents
- Describe the RSA NetWitness trust model
- Create and manage NetWitness users
- Describe/troubleshoot NetWitness users
- Configure external authentication using Active Directory
- Configure external authentication using SecurID
- Configure data privacy

FIND OUT MORE
At-A-Glance
Are you an RSA NetWitness customer looking for the knowledge and skills to monitor and maintain the platform – this course is for you.

Overview
This Instructor-Led course provides students with the knowledge and skills related to the administration and operation of the RSA NetWitness Platform. Topics covered include NetWitness Platform Services, Health and Wellness, Event Source Monitoring, backup and recovery, and administration tools for monitoring and troubleshooting the NetWitness platform.

Students will gain practical experience by performing a series of hands-on labs.

Audience
Anyone who is interested in the administration and operations of the RSA NetWitness Platform.

Delivery Type
- Classroom (delivered live) 3 days
- Virtual Classroom (live learning delivered remotely) 3 days
- On-Demand Classroom (self-paced recorded classroom experience; includes 20 hours of lab access over a 4-week period)

Prerequisite Knowledge/Skills
It is recommended that students complete the following courses prior to taking this training:
- RSA NetWitness Platform Foundations (ILT)
- RSA NetWitness Platform Administration I (ILT)

Learning Objectives
Upon successful completion of this training, participants should be able to:
- Describe the difference between Core services and Platform services
- Create custom Health and Wellness policies
- Take investigative steps to locate the cause of and remediate an alarm
- Modify, export and import event source attributes
- Monitor and debug event sources
- Perform Backup and Restore procedures

FIND OUT MORE
RSA NetWitness Platform Analysis

At-A-Glance
This instructor-led classroom-based course provides experience using the features and functions of RSA NetWitness Logs & Network to perform forensic analysis on network-based security breaches.

Overview
This instructor-led classroom-based course provides hands-on experience using the RSA NetWitness Platform to investigate and remediate security incidents on your network. The course consists of about 50% hands-on lab work, following a practical methodology from the incident queue through investigation, event reconstruction, damage assessment, and documentation using real-world use cases.

Audience
Level 1 and Level 2 analysts relatively new to RSA NetWitness Platform, who wish to increase their familiarity with the tool’s features and functions within the context of incident response and analysis.

Delivery Type
- Classroom (delivered live) 2 days
- Virtual Classroom (live learning delivered remotely) 2 days
- On-Demand Classroom 2 days
  (self-paced recorded classroom experience; includes 20 hours of lab access over a 4-week period)

Prerequisite Knowledge/Skills
Students should have familiarity with the basic processes of cybersecurity analysis, including some knowledge of network architecture, the TCP/IP stack, networking protocols, and integrating log and packet traffic to perform analysis on network-based security events.

Students should have completed the following courses (or have equivalent knowledge) prior to taking this training:

- RSA NetWitness Platform Foundations

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

- Describe SOC roles and models
- Describe the Investigative Methodology
- Identify types of incidents
- Describe the Incident Response process
- Use analysis tools and techniques to investigate an incident
- Document the incident
- Use the incident response process and tools to investigate an incident using packets
- Use the incident response process and tools to investigate an incident using logs
- Use the incident response process and tools to investigate an incident using packets and endpoint
- Use the incident response process and tools to investigate an incident using logs, packets and endpoint

FIND OUT MORE
RSA NetWitness Platform Content Creation

At-A-Glance
This Live Instructor-Led course provides recommended methodologies for creating content to assist you in discovering, analyzing and resolving threats in RSA NetWitness Platform.

Overview
This Instructor-Led course provides recommended methodologies for creating content to assist you in discovering, analyzing and resolving threats in RSA NetWitness Platform. Students will benefit from both lecture and hands-on lab exercises using their own virtual environment to practice the techniques learned in class.

Audience
Customer, PS, CS, SE, Partners

Delivery Type
- Classroom (delivered live) 2 days
- Virtual Classroom (live learning delivered remotely) 2 days
- On-Demand Classroom 2 days
  (self-paced recorded classroom experience; includes 20 hours of lab access over a 4-week period)

Prerequisite Knowledge/Skills
Student should have completed or have comparable knowledge to what is provided in the following course:
- RSA NetWitness Foundations

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Describe content types and identify how and when to use each content type
- Create content including application rules, feeds, custom meta, ESA rules and simple parsers
- Optimize content for performance and functionality
- Identify how to use Live content to address specific needs
- Describe Hunting Pack content
- Use external content types, such as STIX feeds
- Describe a recommended methodology for creating content
- Create a taxonomy for rules and reports
- Describe how to find and use malicious data in content creation
- Create reports to verify efficacy of content
- Use techniques and methodologies to automate threat detection
- Monitor the performance or alerts and parsers
- Validate results and refine your approach accordingly

FIND OUT MORE
RSA NetWitness Platform Introduction to Hunting

At-A-Glance
Interested in hunting? Don't know where to start? This course is a great place to begin as we will give you a recommended approach for identifying threats using the RSA NetWitness Platform.

Overview
This classroom-based course provides an overview of threat hunting and covers hunting tools, content and methodologies that can be used to proactively find suspicious behavior. Students will apply the techniques acquired in this course to identify anomalies and find threats in the environment using Packets, Logs and Endpoint.

Audience
All (customers, partners, internals)

Delivery Type
- Classroom (delivered live) 2 days
- Virtual Classroom (live learning delivered remotely) 2 days
- On-Demand Classroom (self-paced classroom experience) 2 days
  (self-paced recorded classroom experience; includes 20 hours of lab access over a 4-week period)

Prerequisite Knowledge/Skills
- Introduction to the RSA NetWitness Platform
- RSA NetWitness Platform Foundations
- RSA NetWitness Platform Analysis

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Describe threat hunting and Incident Response roles
- Describe the Hunting Guide
- Describe the Hunting Methodology
- Describe the Hunting Pack meta
- Describe RSA NetWitness Platform hunting tools
- Identify protocol/service anomalies
- Identify indicators of malicious traffic
- Use hunting techniques, methodology and tools to detect threats
- Respond to incidents
- Report findings

FIND OUT MORE
RSA NetWitness Platform Reporting

At-A-Glance
Looking to create reports or alerts in RSA NetWitness? This instructor-led course covers the configuration and use of the RSA NetWitness Platform Reporting Engine.

Overview
This course will outline and demonstrate the use of the RSA NetWitness Platform Reporting Engine to create a simple or complex report and configure its execution properties by scheduling a report. Students will learn about and practice configuring the Reporting Engine’s data sources as well as create reports, alerts and charts.

Audience
- Customers
- Internal (CS, PS, SE, Partner)

Delivery Type
On-Demand Classroom 2 days
(self-paced recorded classroom experience; includes 20 hours of lab access over a 4-week period)

Prerequisite Knowledge/Skills
Students are encouraged to have taken the following courses:
- RSA NetWitness Platform Foundations or equivalent knowledge
- Concept and knowledge of basic SQL or SQL-like syntax (SELECT, WHERE) & operators are helpful, but not required.

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Understand the Reporting Engine, its components and workflow
- Configure the Reporting Engine, data sources, notifications and options
- Use the Reporting Engine to create reports, alerts and charts

FIND OUT MORE
On Demand Learning
Introduction to the RSA NetWitness Platform

At-A-Glance
High-level introduction to NetWitness Platform concepts plus walkthroughs of simple incident response workflows.

Overview
This On-Demand Learning consists of two sections: the role and fundamental concepts of RSA NetWitness Platform, including the threat visibility gained from Network, Logs, and Endpoint perspectives. This section also includes basic architecture and data flow for these tools. The second section shows the toolset in action. Demonstration videos walk through incident response use cases employing the central features used in SIEM and SOC environments.

Audience
All novice NW users and admins

Delivery Type
On-Demand Learning

Duration
90 minutes

Prerequisite Knowledge/Skills
None

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

- For RSA NetWitness Network and Logs functionality, describe:
  - Infrastructure
  - Data flow
  - Meta
- For RSA NetWitness Endpoint, describe:
  - Instant Indicators of Compromise
  - Behavior tracking
  - Module and machine definitions
- Perform a simple incident response workflow including pivots between the Respond and Investigate functionality

FIND OUT MORE
RSA NetWitness Platform 11.5: What’s New

At-A-Glance
Want to know what’s new in RSA NetWitness 11.5? This On-Demand Learning focuses on reviewing the new features of the RSA NetWitness Platform 11.5 product release to get you started.

Overview
This FREE on-demand learning provides an overview of the new features and enhancements available in RSA NetWitness Platform version 11.5.

Audience
Anyone interested in RSA NetWitness Platform

Delivery Type
On-Demand Learning

Duration
20 minutes

Prerequisite Knowledge/Skills
Knowledge of the following is suggested for attending this course:

- Previous RSA NetWitness Platform versions

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

- List the new features of NetWitness Platform 11.5
- Explain the major features and functions of NetWitness Platform 11.5 that are of interest to the Administrator and Analyst including UEBA, Endpoint and the new Meta-Only Decoder

FIND OUT MORE
RSA NetWitness UEBA (User and Entity Behavior Analytics)

Overview

At-A-Glance

Want to know about RSA UEBA - this self-paced, on-demand course is a perfect introduction to get you started!

Overview

This self-paced, on-demand course is a perfect introduction to RSA NetWitness UEBA (user and entity behavior analytics). It provides a high-level overview of the UEBA solution. There are three instructional videos. The first video includes instruction on what UEBA is and how it works, as well as demonstrations on how to navigate the UEBA user interface. The second video provides an overview of the RSA UEBA architecture as it relates to the system workflow. The third video focuses on the setup and administration of RSA UEBA.

Audience

Anyone interested in an overview of the RSA NetWitness UEBA solution

Delivery Type

On-Demand Learning

Duration

45 minutes

Prerequisite Knowledge/Skills

Students should have the following skills or taken the following training prior to attending this course:

- RSA NetWitness Platform Foundations
- RSA NetWitness Platform Administration I

Or, equivalent experience using the NetWitness Logs and Network product in a production environment

Learning Objectives

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

- Define UEBA and what it does
- Describe use cases for UEBA
- Describe the RSA UEBA workflow
- Navigate the UEBA screens in RSA NetWitness
- Provide an overview of the RSA UEBA architecture as it relates to the system workflow
- Examine a simplified system workflow
- Describe the pre-work required before setting up the UEBA solution
- List the data required to establish an initial baseline for RSA UEBA
- Discuss the three main schemas that are used for adapting log meta used in the UEBA solution
- Examine the timeline for the training process for the UEBA deployment
- Describe the five main steps in the setup process of UEBA

FIND OUT MORE
RSA NetWitness Orchestrator Built on ThreatConnect - Fundamentals

At-A-Glance
This On-Demand course describes the use of RSA NetWitness Orchestrator (built on ThreatConnect) for bridging NetWitness and third-party SOC tools and alerts, and standardizing incident response with playbooks.

Overview
This on-demand course provides foundational concepts of the RSA NetWitness Orchestrator (ThreatConnect version). Students will gain insights into the major features of the product via video demonstrations, explanations, and screenshots.

Audience
Anyone interested in an overview of the RSA NetWitness Orchestrator solution.

Delivery Type
On-Demand Learning

Duration
180 minutes

Prerequisite Knowledge/Skills
None

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

- Describe the role, functionality, and analytic approach of RSA NetWitness Orchestrator built on ThreatConnect
- Perform basic administrative tasks such as adding a new user and updating a cloud-based Playbook
- Customizing your environment by enabling two-factor authentication, selecting which Indicators and groups are visible, and creating a custom space
- Browse threat intelligence
- Interpret and discern between scores for Threat Rating, Confidence, and ThreatAssess
- Create a basic Workflow, Indicator, and Playbook
- Interpret and assess the run results of a Playbook
- Contribute to your organization's pool of knowledge by creating posts and associating your findings with indicators and groups

FIND OUT MORE
At-A-Glance
This course provides a demonstration of the steps used to create a log parser.

Overview
In this course you will learn how to create and deploy a log parser for a specific device by viewing demonstrations using the Log Parser Tool (LPT).

Audience
Customer, PS, CS, ES, Partners

Delivery Type
On-Demand Learning

Duration
30 minutes

Prerequisite Knowledge/Skills
Knowledge of the following is required for attending this course:

- Introduction to the RSA NetWitness Platform
- RSA NetWitness Platform Foundations

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

- Describe the Log Parser Tool (LPT)
- Identify the steps for creating a log parser using the LPT
- Identify the steps for deploying the log parser in RSA NetWitness
RSA NetWitness Platform ESA Fundamentals

At-A-Glance
Are you an RSA SecurID Access customer looking for guidance on troubleshooting? This OnDemand learning will provide you with the right information to get started.

Overview
This On-Demand learning course presents an overview of Event Stream Analysis including a description of correlation approaches and ESA’s role in correlation, ESA components and features, when to use ESA and how configuration settings affect ESA rules. It focuses on the basics of ESA including architecture, creating basic rules, deploying rules, creating enrichments and notifications and forwarding alerts to the RESPOND module.

Audience
Anyone who is interested in Event Stream Analysis (ESA) with relation to the RSA NetWitness Platform.

Delivery Type
On-Demand Learning

Duration
60 minutes

Prerequisite Knowledge/Skills
Prior to attending this class, students are encouraged to have a working knowledge of the RSA NetWitness Platform.

It is recommended that students complete the following eLearning courses prior to taking this training:

- RSA NetWitness Platform Foundations (ILT)
- RSA NetWitness Platform Administration I (ILT)

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

- Describe a correlation approach
- Describe ESA’s role in correlation
- Describe the features and components of ESA
- Identify when and how to use an ESA rule
- Describe the features of the basic rule builder
- Create a basic rule
- Create enrichments
- Describe how configuration settings affect ESA rules
- Explain the best practices for writing ESA rules

FIND OUT MORE
RSA NetWitness Platform ESA EPL Rules

At-A-Glance
This on-demand learning presents a recommended approach to learning EPL syntax and for writing EPL rules to detect threats.

Overview
This on-demand learning identifies a best practice strategy for creating EPL rules as well as for learning the EPL rule syntax. It uses examples and use cases to illustrate EPL rule concepts, such as streams, constructs, data windows and time constraints.

Audience
Anyone interested in using RSA NetWitness Logs & Network Event Stream Analysis to create EPL rules to help identify suspicious activity

Delivery Type

On-Demand Learning

Duration

1.5 hours

Prerequisite Knowledge/Skills
Students should have completed the following courses (or have equivalent knowledge) prior to taking this training:

• RSA NetWitness Introduction
• RSA NetWitness Logs & Network Introduction to ESA or RSA NetWitness Platform Foundations

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

• Describe the Esper engine and EPL
• Describe EPL Rule Types
• Describe data windows
• Describe how time is calculated
• Describe a recommended process for designing and writing EPL rules
• Describe EPL syntax
• Create EPL rules for specific use cases
• List the best practices for ESA rules

FIND OUT MORE
RSA NetWitness Lua Parsers for Logs

At-A-Glance
This On-Demand Learning course will provide students with an overview of creating custom log parsers for RSA NetWitness using Lua.

Overview
This On-Demand Learning course will provide students with an overview of creating custom log parsers for RSA NetWitness using Lua. Students will cover topics such as when to use a custom parser, the components of a Lua parser, how to create the Lua parser for logs and basic troubleshooting.

Audience
Customer, PS, CS, ES, Partners

Delivery Type
On-Demand Learning

Duration
60 minutes

Prerequisite Knowledge/Skills
Knowledge of the following is required for attending this course:

- General programming concepts including local and global variables, conditional logic (if, then, else) and program loops (while, do) is highly suggested but not required
- Use of a source code editor (such as Notepad++)
- Basic understanding of the grep command in Linux
- RSA NetWitness for Logs and Network Introduction – eLearning
- RSA NetWitness Platform Foundations
- RSA NetWitness Logs Parser Overview eLearning
- RSA NetWitness for Logs and Network Lua Parsers – eLearning

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

- Identify when the use of Lua is necessary for parsing and creating custom content
- Understand and explain the use of RSA NetWitness meta callbacks
- Understand and explain the use of nw.getPayload(), tostring() and nw.LogInfo() functions
- Understand and explain the use of basic Lua string pattern-matching
- Create a custom log (device) parser for a supported event source using a Lua parser
- Test a Lua log parser for use in RSA NetWitness for Logs
- Deploy a Lua log parser for use in RSA NetWitness for Logs
- Perform basic troubleshooting of a Lua log parser
RSA NetWitness Endpoint YARA Rules

At-A-Glance

Overview
This on-demand learning provides an introduction to writing rules for RSA NetWitness Endpoint using YARA. Students will gain familiarity with the YARA tool's syntax and functionality to write rules that optimize flexibility and minimize false positives.

Audience
Anyone interested in YARA tool's syntax and functionality

Delivery Type
🔥 On-Demand Learning (self-paced eLearning)

Duration
45 minutes

Prerequisite Knowledge/Skills
Students should have familiarity with:
- Programming fundamentals
- Knowledge of C Programming and Perl regular expressions desirable
- Skills provided in the RSA NetWitness Endpoint Foundations course

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

- Describe what YARA is
- Describe why YARA rules are used in RSA NetWitness Endpoint
- Write basic YARA rules
- Explain the available strings and conditions used in YARA rules
- Enable custom YARA content on the RSA NetWitness Endpoint
- Download YARA rules from other web sites
- Research YARA rules from popular web sites

FIND OUT MORE
On Demand Labs
(Self-Paced eLearning with Lab)

Accessing the Lab Environment

Lab exercises are performed in the RSA University virtual lab environment. The downloadable Lab Guide provides detailed instructions on access the environment. For more information please view the document Access RSA University Virtual Labs – available on the RSA University site: RSA University Content.
RSA NetWitness Orchestrator Built on ThreatConnect - Incident Response

At-A-Glance
This On-Demand Lab will teach you the skills for bridging RSA NetWitness and third-party tools and alerts, and standardizing incident response with playbooks.

Overview
This On-Demand hands-on course outlines and demonstrates the use of RSA NetWitness Orchestrator Built on ThreatConnect for bridging RSA NetWitness and third-party tools and alerts, and standardizing incident response with playbooks. Fundamental concepts such as incident definitions also covered.

Audience
All security analysts and SOAR engineers employing Orchestrator Built on ThreatConnect and NetWitness platform.

Delivery Type
On-Demand Lab

Duration
4 hours
Note: RSA University’s on-demand lab environment is provided for 10 hours of overall practice time over a 14-day period.

Prerequisite Knowledge/Skills
Students should have completed the following courses (or have equivalent knowledge) prior to taking this training:
- Familiarity with NW 11.x and the Respond Module (alerts and incidents)
- RSA NetWitness Orchestrator Built on ThreatConnect Fundamentals On-Demand Course
- Familiarity with the incident response process

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Describe core RSA NWOTC functionality
- Implement NetWitness integration
- Prepare RSA NWOTC playbook data handling
- Create and utilize custom playbooks for incident response
- Utilize 3rd party integrations for collection and enrichment
At-A-Glance
This On-Demand lab will provide students with the information and a virtual environment to practice creating and deploying log parsers within RSA NetWitness.

Overview
This On-Demand lab will provide students with the information and a virtual environment to practice creating and deploying log parsers within RSA NetWitness. Students will be introduced to reviewing the metadata framework, creating log parsers using the NetWitness Log Parser Tool (LPT), and deploying log parsers within RSA NetWitness Logs.

Audience
SE, PS, CS, Customer, Partner

Delivery Type
On-Demand Lab

Duration
Approximately 4 hours of On-Demand Learning and 4-hour lab
Includes 10 hours of lab access over a 14-day period

Prerequisite Knowledge/Skills
RSA NetWitness Platform Foundations
RSA NetWitness Platform Administration I

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

- Describe the RSA NetWitness Logs & Network log data flow
- Describe the role of parsers in RSA NetWitness Logs & Network
- Describe the process used to create and deploy log parsers
- Create a Log Parser using the Event Source Integrator (ESI) Tool
- Deploy a Log Parser for use in RSA NetWitness Logs & Network
- Modify service configuration files to add custom meta keys
- Modify Security Analytics to receive file-based logs from devices not currently supported

FIND OUT MORE
RSA NetWitness Logs Event Source Configuration

At-A-Glance
This self-paced, on-demand lab provides an overview of how RSA NetWitness log collection is configured and performed for a variety of event source types such as Windows, File Reader, ODBC, Check Point Firewall, VMware, SDEE, SNMP and Netflow.

Overview
This self-paced, on-demand lab provides an overview of how RSA NetWitness log collection is configured and performed for a variety of event source types such as Windows, File Reader, ODBC, Check Point Firewall, VMware, SDEE, SNMP and Netflow. It also provides steps to practice configuring syslog, Windows, ODBC and FileReader event sources.

Audience
Internal, CS, PS, SE, Partner, Customer

Delivery Type
On-Demand Lab

Duration
Approximately 3 hours of On-Demand Learning and 4-hour lab
Includes 10 hours of lab access over a 14-day period

Prerequisite Knowledge/Skills
- RSA NetWitness Logs and Packets Foundations training course or equivalent experience
- Familiarity with networking fundamentals
- Familiarity with Linux
- Familiarity with MS Windows

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Describe the RSA NetWitness Logs & Network log data flow
- Describe how log data is created and processed by RSA NetWitness
- Configure log collection for RSA supported event source types.
  Lab exercises will be provided for the most common event source types which include:
  - Syslog
  - Windows
  - File Reader
  - ODBC
- Validate data capture
- Set up event source monitoring
- Troubleshoot Event Sources

FIND OUT MORE
RSA Proven Professional Product Certification Program
RSA Proven Professional Certification Program

Overview
RSAs Proven Professional Certification Program establishes a scalable framework that reflects conceptual and practical role-based knowledge of RSA products. This certification program establishes a standard of excellence within a governance model that validates the competency of the user. The certification framework is as follows.

RSAs Proven Professional Certification Program is based on real-world experience with our industry-leading security solutions. Each RSA product certification has its own unique path to excellence and is based on role-specific practical and conceptual knowledge. Each certification level is more in-depth and requires greater expertise and product knowledge.

Associate Certification
RSA’s Proven Professional Associate Certification is the baseline certification for all follow-on certifications. This certification establishes a fundamental understanding and knowledge of an RSA product. This is the first step moving to more advanced, role-based concepts and tasks.

Specialist Certification
Each Specialist Certification is role-based and focuses on practical understanding of a product and industry best practices. This certification requires recertification every two years due to product maturity, market evolution, and industry changes.

Expert Certification
The Expert Certification is also role-based, focusing on product and industry evolution considering advanced-level practical and conceptual knowledge of RSA’s products. This certification also requires recertification every two years.

Master Certification
The Master Certification is the highest-level certification level available from RSA. This certification requires subject matter expertise across multiple RSA products. This certification requires recertification every two years.
RSA NetWitness

NetWitness certifications begin with the Associate exam which is the prerequisite to the role-based Specialist exams. Advancing beyond the Associate level, the Specialist exams are specific to the Analyst or Administrator roles. Customers, partners, and employees can take certifications for one or for both roles.

The NetWitness Associate exam is based on the RSA NetWitness Platform Foundations course, RSA NetWitness Administration I course, and the RSA NetWitness Endpoint Foundations course.

The NetWitness Specialist exam: Administrator is based on the RSA NetWitness Administration I and Administration II courses, RSA NetWitness Content Creation courses, and other on-demand training.


At this time, no Expert or Master level exams are being offered for NetWitness.
Industry / Information Security Training and Certification
RSA Certified Information Systems Security Professional (CISSP) Certification Review

At-A-Glance
Our mission is to enable the next generation of security professionals to address the latest threats to information and infrastructure security. RSA’s CISSP Certification review uses the latest CISSP review materials and is delivered by security practitioners to prepare you to succeed in passing this internationally recognized industry certification.

Overview
RSA delivers an effective program to prepare candidates to become security practitioners and validate their skills by passing the ISC2 CISSP certification exam.

The Certification review course involves intensive lectures, and question reviews delivered by an experienced security professional practitioner with years of experience. Not only will participants become prepared to pass the exam, but the anecdotes and real-world examples for the course are invaluable insight into real world security challenges and approaches on how to solve them.

The modules of the course follow the 8 domains of the ISC2 Common Body of Knowledge. Each module presents 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 successful security program.

Each module is also followed by review using proven test engines as practice and detailed explanations and tips related to the material and how to manage the new adaptive format of the CISSP exam with success. RSA’s CISSP certification review has been updated to reflect the 2018 Domain names and content changes. Participants will come away empowered for success on the exam and with additional knowledge to add to their security practitioner skill set.

Audience
Security professionals who are pursuing CISSP certification and want to advance within their computer security career.

Delivery Type and Duration

- Classroom (delivered live or virtual) 5 days
- Virtual Classroom (live learning delivered remotely) 5 days

2020 Common Body of Knowledge Domains

- Domain 1: Security and Risk Management
- Domain 2: Asset Security
- Domain 3: Security Architecture and Engineering
- Domain 4: Communication and Network Security
- Domain 5: Identity and Access Management
- Domain 6: Security Assessment and Testing
- Domain 7: Security Operations
- Domain 8: Software Development Security

RSA University is not affiliated with ISC2 or its subsidiaries. Participation in this course does not guarantee the successful completion of the ISC2 CISSP exam. RSA University uses approved content in the areas of the Common Body of Knowledge and has used the ISC2 CISSP Exam Outline -121417 – Final as a reference as to technical depth and topics on the exam. Course costs do not include exam fees or facilitate exam registration or delivery. Exam schedules are available in ISC2.org.

FIND OUT MORE
Certified Network Defender (CND)

At-A-Glance
Certified Network Defender & Exam

Overview
Certified Network Defender (CND) is a vendor-neutral, hands-on, instructor-led comprehensive network security certification training program. It is a skills-based, lab intensive program based on a job-task analysis and cybersecurity education framework presented by the National Initiative of Cybersecurity Education (NICE). The course has also been mapped to global job roles and responsibilities and the Department of Defense (DoD) job roles for system/network administrators. The course is designed and developed after extensive market research and surveys.

The program prepares network administrators on network security technologies and operations to attain Defense-in-Depth network security preparedness. It covers the “protect, detect, and respond” approach to network security. The course contains hands-on labs, based on major network security tools and techniques which will provide network administrators real world expertise on current network security technologies and operations. The study-kit provides you with over 10 GB of network security best practices, assessments and protection tools. The kit also contains templates for various network policies and a large number of white papers for additional learning.

Audience

Delivery Type and Duration
- Classroom (delivered live or virtual) 5 days
- Virtual Classroom (live learning delivered remotely) 5 days
- On-Demand Learning (iLearn / self-paced classroom experience) 5 days

Prerequisite Knowledge/Skills
Students should have a basic knowledge of computer science and networks.

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

- Learn about various network security controls, protocols, and devices
- Determine appropriate location for IDS/IPS sensors, tuning IDS for false positives and false negatives, and configurations to harden security through IDPS technologies
- Implement secure VPN for their organization
- Identify various threats to wireless network and learn how to mitigate them
- Monitor and conduct signature analysis to detect various types of attacks and policy violation activities
- Perform risk assessment, vulnerability assessment/scanning through various scanning tools and generate detailed reports on it
- Identify the critical data, choose appropriate back up method, media and technique to perform successful backup of organization data on regular basis
- Provide first response to the network security incident and assist IRT team and forensics investigation team in dealing with an incident.
- Troubleshoot their network for various network problems
- Identify various threats on organization network
- Design and implement various security policies for their organizations
- Learn the importance of physical security and able to determine and implement various physical security controls for their organizations
EC Council Certified Threat Intelligence Analyst (CTIA)

At-A-Glance
The Certified Threat Intelligence Analyst training is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence. It addresses all the stages involved in the Threat Intelligence Life Cycle.

Overview
Certified Threat Intelligence Analyst (C|TIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats.

C|TIA is a method-driven program that uses a holistic approach, covering concepts from planning the threat intelligence project to building a report to disseminating threat intelligence. These concepts are highly essential while building effective threat intelligence and, when used properly, can secure organizations from future threats or attacks.

This attention to a realistic and futuristic approach makes C|TIA one of the most comprehensive threat intelligence certifications on the market today. This program provides the solid, professional knowledge that is required for a career in threat intelligence, and enhances your skills as a Threat Intelligence Analyst, increasing your employability.

Audience
- Ethical Hackers
- Security Practitioners
- Threat Intelligence Analysts, Associates, Researchers
- Threat Hunters
- SOC Professionals
- Digital Forensic and Malware Analysts
- Incident Response Team Members
- Individuals interested in preventing cyber threats

Delivery Type and Duration
- Classroom (delivered live or virtual) 3 days
- Virtual Classroom (live learning delivered remotely) 3 days
- On-Demand Learning (iLearn / self-paced classroom experience) 3 days

Prerequisite Knowledge/Skills
Students should be familiar with the following:
- A minimum of 2 years working experience in information security.

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Use a method-driven holistic approach to identify and mitigate business risks
- Demonstrate mastery of the knowledge and skills required for threat intelligence

FIND OUT MORE
EC Council: Certified Ethical Hacking (CEH)

At-A-Glance
Certified Ethical Hacking Course & Exam

Overview
Cyber Security as a profession is evolving, the barrier to entry is rising, the demand for Skilled Cyber professionals continues to grow, but it is being refined, demanding a higher level of skill and ability.

This course will immerse you into a “Hacker Mindset” in order to teach you how to think like a hacker and better defend against future attacks. It puts you in the driver’s seat with a hands-on training environment employing a systematic ethical hacking process.

You are constantly exposed to creative techniques of achieving optimal information security posture in the target organization; by hacking it! You will learn how to scan, test, hack and secure target systems. The course covers the Five Phases of Ethical Hacking, diving into Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

Audience

Delivery Type and Duration
- Classroom (delivered live or virtual) 5 days
- Virtual Classroom (live learning delivered remotely) 5 days
- On-Demand Learning (iLearn / self-paced classroom experience) 5 days

Prerequisite Knowledge/Skills
Students should have some knowledge of computer networks, computer science

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

- Key issues plaguing the information security world, incident management process, and penetration testing.
- Various types of footprinting, footprinting tools, and countermeasures.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks.
- Different types of Trojans, Trojan analysis, and Trojan countermeasures.
- Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures.
- Packet sniffing techniques and how to defend against sniffing.
- Social Engineering techniques, identify theft, and social engineering countermeasures.
- Session hijacking techniques and countermeasures.
- Different types of webserver attacks, attack methodology, and countermeasures.
- Different types of web application attacks, web application hacking methodology, and countermeasures.
- SQL injection attacks and injection detection tools.
- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
• Mobile platform attack vector, android vulnerabilities, mobile security guidelines, and tools.
• Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures.
• Various cloud computing concepts, threats, attacks, and security techniques and tools.
• Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.
• Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
• Perform vulnerability analysis to identify security loopholes in the target organization’s network, communication infrastructure, and end systems.
• Different threats to IoT platforms and learn how to defend IoT devices securely.
EC Council Certified Security Analyst (ECSA)

At-A-Glance
Certified Security Analyst Course & Exam

Overview
The ECSA pentest program takes the tools and techniques you learned in the Certified Ethical Hacker course (CEH) and enhances your ability into full exploitation by teaching you how to apply the skills learned in the CEH by utilizing EC-Council’s published penetration testing methodology. It focuses on pentesting methodology with an emphasis on hands-on learning.

The new ECSAv10 includes updated curricula and an industry recognized comprehensive step-by-step penetration testing methodology. This allows a learner to elevate their ability in applying new skills learned through intensive practical labs and challenges. Unlike most other pen testing programs that only follow a generic kill chain methodology; the ECSA presents a set of distinguishable comprehensive methodologies that are able to cover different pentesting requirements across different verticals. It is a highly interactive, comprehensive, standards based, intensive 5-days training program that teaches information security professionals how professional real-life penetration testing are conducted.

Audience

Delivery Type and Duration
- Classroom (delivered live or virtual) 5 days
- Virtual Classroom (live learning delivered remotely) 5 days
- On-Demand Learning (iLearn / self-paced classroom experience) 5 days

Prerequisite Knowledge/Skills
Prior to exam, students must either:

- Attend official training via an EC-Council accredited training channel Or
- Possess a minimum of 2 years of working experience in a related InfoSec domain

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

- Network Penetration Testing: Identify security issues in network design and implementation
- Web Application Penetration Testing: Detect security issues in web applications that exists due to insecure design and development practices
- Social Engineering Penetration Testing: Identify employees that do not properly authenticate, follow, validate, handle, the processes and technology
- Wireless Penetration Testing: Identify misconfigurations in organization’s wireless infrastructure including WLAN, Mobile,
- Cloud Penetration Testing: Determine security issues in organization’s cloud infrastructure
- Database Penetration Testing: Identify security issues in the configuration of database server and their instances

FIND OUT MORE
At-A-Glance
Computer Hacking Forensic Investigator Course & Exam

Overview
CHFI v9 covers detailed methodological approach to computer forensic and evidence analysis. It provides the necessary skillset for identification of intruder's footprints and gathering necessary evidence for its prosecution. All major tools and theories used by cyber forensic industry are covered in the curriculum. The certification can fortify the applied knowledge level of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, computer and network security professionals, and anyone who is concerned about the integrity of the network and digital investigations.

CHFI provides necessary skills to perform effective digital forensic investigation. It is a comprehensive course covering major forensic investigation scenarios that enables students to acquire necessary hands-on experience on various forensic investigation techniques and standard forensic tools necessary to successfully carryout computer forensic investigation leading to prosecution of perpetrators. CHFI presents a methodological approach to computer forensic including searching and seizing, chain-of-custody, acquisition, preservation, analysis and reporting of digital evidence.

Audience
- Police and other law enforcement personnel
- Defense and Military personnel
- e-Business Security professionals
- Systems administrators
- Legal professionals
- Banking, Insurance and other professionals
- Government agencies
- IT managers

Delivery Type and Duration
- Classroom (delivered live or virtual) 5 days
- Virtual Classroom (live learning delivered remotely) 5 days
- On-Demand Learning (iLearn / self-paced classroom experience) 5 days

Prerequisite Knowledge/Skills
Students should have a basic knowledge of computer science and networks.

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Perform incident response and forensics
- Perform electronic evidence collections
- Perform digital forensic acquisitions
- Perform bit-stream Imaging/acquiring of the digital media seized during the process of investigation.
- Examine and analyze text, graphics, multimedia, and digital images
- Conduct thorough examinations of computer hard disk drives, and other electronic data storage media
- Recover information and electronic data from computer hard drives and other data storage devices
- Follow strict data and evidence handling procedures
- Maintain audit trail (i.e., chain of custody) and evidence integrity
- Work on technical examination, analysis and reporting of computer-based evidence
- Prepare and maintain case files
- Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images and other files
- Gather volatile and non-volatile information from Windows, MAC and Linux
• Recover deleted files and partitions in Windows, Mac OS X, and Linux
• Perform keyword searches including using target words or phrases
• Investigate events for evidence of insider threats or attacks
• Support the generation of incident reports and other collateral
• Investigate and analyze all response activities related to cyber incidents
• Plan, coordinate and direct recovery activities and incident analysis tasks
• Examine all available information and supporting evidence or artefacts related to an incident or event
• Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents
• Conduct reverse engineering for known and suspected malware files
• Perform detailed evaluation of the data and any evidence of activity in order to analyze the full circumstances and implications of the event
• Identify data, images and/or activity which may be the target of an internal investigation
• Establish threat intelligence and key learning points to support pro-active profiling and scenario modelling
• Search file slack space where PC type technologies are employed
• File MAC times (Modified, Accessed, and Create dates and times) as evidence of access and event sequences
• Examine file type and file header information
• Review e-mail communications including web mail and Internet Instant Messaging programs
• Examine the Internet browsing history
• Generate reports which detail the approach, and an audit trail which documents actions taken to support the integrity of the internal investigation process
• Recover active, system and hidden files with date/time stamp information
• Crack (or attempt to crack) password protected files
• Perform anti-forensics detection
• Maintain awareness and follow laboratory evidence handling, evidence examination, laboratory safety, and laboratory security policy and procedures
• Play a role of first responder by securing and evaluating a cybercrime scene, conducting preliminary interviews, documenting crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, reporting of the crime scene
• Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred
• Apply advanced forensic tools and techniques for attack reconstruction
• Perform fundamental forensic activities and form a base for advanced forensics
• Identify and check the possible source/incident origin
• Perform event correlation
• Extract and analyze logs from various devices such as proxies, firewalls, IPSes, IDSes, Desktops, laptops, servers, SIM tools, routers, switches, AD servers, DHCP servers, Access Control Systems, etc.
• Ensure that reported incident or suspected weaknesses, malfunctions and deviations are handled with confidentiality
• Assist in the preparation of search and seizure warrants, court orders, and subpoenas
• Provide expert witness testimony in support of forensic examinations conducted by the examiner
EC Council Certified Incident Handler (ECIH)

At-A-Glance
Certified Incident Handler Course & Exam

Overview
The EC-Council Certified Incident Handler (ECIH) program is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students will learn how to handle various types of incidents, risk assessment methodologies, and various laws and policies related to incident handling. After attending this course, they will be able to create incident handling and response policies as well as deal with various types of computer security incidents.

The IT incident management training program will enable students to be proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats. In addition, students will learn about computer forensics and its role in handling and responding to incidents. The course also covers incident response teams, incident management training methods, and incident recovery techniques in detail. The ECIH certification will provide professionals greater industry acceptance as the seasoned incident handler.

Audience
- Incident handlers
- Risk assessors
- Pen testers
- Forensic Investigators
- System admins/engineers
- Firewall admins
- Vulnerability auditors
- IT managers and professional

Delivery Type and Duration
- Classroom (delivered live or virtual) 3 days
- Virtual Classroom (live learning delivered remotely) 3 days
- On-Demand Learning (iLearn / self-paced classroom experience) 3 days

Prerequisite Knowledge/Skills
Students should have basic knowledge of general computer science and network topics.

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Principles, processes and techniques for detecting and responding to security threats/breaches
- Perform as a liaison to legal and regulatory bodies
- Learn to handle incidents and conduct assessments
- Cover various incidents like malicious code, network attacks, and insider attacks

FIND OUT MORE
EC Council Advanced Penetration Testing (APT)

At-A-Glance
Advanced Penetration Testing (APT) Course and Exam

Overview
The ECCAPT consists of entire network segments that replicate an enterprise network — this is not a computer game simulation; this is an accurate representation of an enterprise network that will present the latest challenges. Licensed Penetration Tester (Master) Licensed Penetration Tester (Master) to the penetration tester. Since the targets and technology continue to change, the ECCAPT is dynamic and machines and defenses will be added as they are observed in the wild. Finally, the targets and segments are progressive in nature, once you get into one machine and or segment, the next one will challenge you even more. The ranges are designed to teach professional-level skills to identify the attack surface of targets within a required time frame and, once this has been accomplished, to gain access to the machines and escalate privileges as required. The greater the variety of targets you encounter with and without defenses, the better of a professional penetration tester you will become.

The practical environment ranges progress in difficulty and reflect real enterprise network architecture. This environment includes defenses and challenges which you must defeat and overcome. This training format has helped thousands of penetration testers globally and is proven to be effective. Everything presented in the course is through an enterprise network environment that must be attacked, exploited, evaded, and defended.

Audience
- Penetration Testers
- Network Administrators
- IT Auditors
- Information Security Engineers
- Security Consultants

Delivery Type and Duration
- Classroom (delivered live or virtual) 3 days
- Virtual Classroom (live learning delivered remotely) 3 days
- On-Demand Learning (iLearn / self-paced classroom experience) 3 days

Prerequisite Knowledge/Skills

Eligibility Criteria
To be eligible to apply to sit for the LPT (Master) Exam, candidate must either.
- Hold an ECSA / ECSA (Practical) or LPT certification in good standing (Your USD100 application fee will be waived);
- Have a minimum of 2 years working experience in pentesting (You will need to pay USD100 as a non-refundable application fee);
- Have any other approved industry certifications such as OSCP or GPEN cert (You will need to pay USD100 as a non-refundable application fee)

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Demonstrate a repeatable and measurable approach to penetration testing.
- Perform advanced techniques and attacks to identify SQL injection, cross site scripting (XSS), LFI, RFI vulnerabilities in web applications.
- Submit a professional and industry accepted report that achieves management and technical buy-in
- Learn proprietary EC-Council penetration testing methodologies
- Write exploit codes to gain access to a vulnerable system or application
- Exploit vulnerabilities in operating systems
- Understand and demonstrate adversarial thinking
EC Council Certified Chief Information Security Officer (CCISO)

At-A-Glance
Certified Chief Information Security Officer (CCISO) Course & Exam

Overview
EC-Council’s CCISO Program has certified leading information security professionals around the world. A core group of high-level information security executives, the CCISO Advisory Board, contributed by forming the foundation of the program and outlining the content that would be covered by the exam, body of knowledge, and training. Some members of the Board contributed as authors, others as exam writers, others as quality assurance checks, and still others as trainers. Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program.

The Certified CISO (CCISO) program is the first of its kind training and certification program aimed at producing top-level information security executives. The CCISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view. The program was developed by sitting CISOs for current and aspiring CISOs.

Audience
• Security professionals seeking to prove their readiness for executive positions.
• Existing CISOs who want to demonstrate their knowledge and skills in the profession

Delivery Type and Duration
- Classroom (delivered live or virtual) 5 days
- Virtual Classroom (live learning delivered remotely) 5 days
- On-Demand Learning (iLearn / self-paced classroom experience) 5 days

Prerequisite Knowledge/Skills
Applicants who would like to sit for the CCISO Exam will be required to fill out and return the Exam Eligibility Application proving that in addition to the training, they also have 5 years of IS management experience in 3 of the 5 CCISO Domains. Once that application has been approved, instructions for purchasing a Pearson VUE voucher will be issued.

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Drivers that Influence Governance
- Corporate Governance Activities
- Information Security Governance Activities
- Governance and Ethical Decision Making
- Risk Management
- Risk Treatment
- Risk Management Frameworks
- Audit Management
- Information Security Portfolio/Program/Project Management
- Security Operations
- Access Control
- Physical Security
- Network and Communications Security
- Threat & Vulnerability Management
- System and Application Security
- Encryption Concepts and Technology
- Strategic Planning
- Financial Management
- Vendor Risk Management

FIND OUT MORE
Additional Resources
How to Access On-Demand Learning
1. Navigate to https://community.rsa.com/community/training

2. Choose a product of interest and click on the product icon

3. From the Delivery Type dropdown menu, select the On-Demand type you wish to view, then select the course you are interested in from the list.

4. If you already have an EMC2 account, press the Access Training button on the course description page. If this is your first course with us, follow instruction here https://community.rsa.com/docs/DOC-41111 to register and create an account.

To see a demonstration video of how to access RSA University free On-Demand Learning, go to https://community.rsa.com/docs/DOC-43443

Check out RSA University YouTube channel for free On-Demand Videos https://www.youtube.com/channel/UC8zA1d5y_C_wAUcyr83-ndw
Don’t see training for the topic you are looking for? Make a request for new course offerings here: https://www.surveymonkey.com/r/RSA_Course_Request
# RSA NetWitness Platform and Information Security Matrix

<table>
<thead>
<tr>
<th>Course Title</th>
<th>Part Number</th>
<th>Delivery Modalities</th>
<th>Duration</th>
<th>Price (USD)</th>
<th># TCs*</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA NetWitness Platform Training Credit</td>
<td>ED-NW-TRAINCREDIT</td>
<td>-</td>
<td>-</td>
<td>$1</td>
<td>1</td>
</tr>
<tr>
<td>RSA NetWitness Platform Foundations</td>
<td>ED-NW-FND1115-ODC</td>
<td></td>
<td>3 days</td>
<td>$3000</td>
<td>3000</td>
</tr>
<tr>
<td>RSA NetWitness Platform Content Creation</td>
<td>ED-NW-CONCRE1115-ODC</td>
<td></td>
<td>2 days</td>
<td>$2000</td>
<td>2000</td>
</tr>
</tbody>
</table>

© 2021 RSA Security LLC or its affiliates. All rights reserved.
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Part Number</th>
<th>Delivery Modalities</th>
<th>Duration</th>
<th>Price (USD)</th>
<th># TCs*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to RSA NetWitness Platform</td>
<td></td>
<td></td>
<td>90 min</td>
<td>$0</td>
<td>0</td>
</tr>
<tr>
<td>RSA NetWitness Platform 11.5: What’s New</td>
<td></td>
<td></td>
<td>15 min</td>
<td>$0</td>
<td>0</td>
</tr>
<tr>
<td>RSA NetWitness UEBA (User and Entity Behavior Analytics) Overview</td>
<td></td>
<td></td>
<td>45 min</td>
<td>$0</td>
<td>0</td>
</tr>
<tr>
<td>RSA NetWitness Orchestrator Built on ThreatConnect - Fundamentals</td>
<td></td>
<td></td>
<td>180 min</td>
<td>$0</td>
<td>0</td>
</tr>
<tr>
<td>RSA NetWitness Log Parser Tool</td>
<td></td>
<td></td>
<td>30 min</td>
<td>$0</td>
<td>0</td>
</tr>
<tr>
<td>RSA NetWitness Platform ESA Fundamentals</td>
<td>ED-NW-TRAINCREDIT (Qty: 200)</td>
<td></td>
<td>60 min</td>
<td>$200</td>
<td>200</td>
</tr>
<tr>
<td>RSA NetWitness Platform ESA EPL Rules</td>
<td>ED-NW-TRAINCREDIT (Qty: 200)</td>
<td></td>
<td>90 min</td>
<td>$200</td>
<td>200</td>
</tr>
<tr>
<td>RSA NetWitness Lua Parsers for Logs</td>
<td>ED-NW-TRAINCREDIT (Qty: 200)</td>
<td></td>
<td>60 min</td>
<td>$200</td>
<td>200</td>
</tr>
<tr>
<td>RSA NetWitness Endpoint YARA Rules</td>
<td>ED-NW-TRAINCREDIT (Qty: 200)</td>
<td></td>
<td>45 mins</td>
<td>$200</td>
<td>200</td>
</tr>
<tr>
<td>RSA NetWitness Orchestrator Built on ThreatConnect - Incident Response</td>
<td>ED-NW-LAB-NWOTCIR</td>
<td></td>
<td>4 hours</td>
<td>$500</td>
<td>500</td>
</tr>
<tr>
<td>RSA NetWitness Log Parser Creation</td>
<td>ED-NW-LAB-LOGPARS</td>
<td></td>
<td>4 hrs.</td>
<td>$500</td>
<td>500</td>
</tr>
<tr>
<td>RSA NetWitness Logs Event Source Configuration</td>
<td>ED-NW-LAB-LOGESC</td>
<td></td>
<td>3 hrs.</td>
<td>$500</td>
<td>500</td>
</tr>
<tr>
<td>RSA Certified Information Systems Security Professional (CISSP) Certification Review</td>
<td>ED-IST-CISSP-110</td>
<td></td>
<td>5 days</td>
<td>$3750</td>
<td>-</td>
</tr>
<tr>
<td>EC Council Certified Network Defender Bootcamp &amp; Exam</td>
<td>ED-IST-CND-110</td>
<td></td>
<td>5 days</td>
<td>$3750</td>
<td>-</td>
</tr>
<tr>
<td>EC Council Certified Threat Intelligence Analyst (CTIA)</td>
<td>ED-IST-CTIA-110</td>
<td></td>
<td>3 days</td>
<td>$2250</td>
<td>-</td>
</tr>
<tr>
<td>EC Council: Certified Ethical Hacking Bootcamp &amp; Exam</td>
<td>ED-IST-CEH-110</td>
<td></td>
<td>5 days</td>
<td>$3750</td>
<td>-</td>
</tr>
<tr>
<td>EC Council Certified Security Analyst Course &amp; Exam</td>
<td>ED-IST-ECSA-110</td>
<td></td>
<td>5 days</td>
<td>$3750</td>
<td>-</td>
</tr>
<tr>
<td>EC Council Computer Hacking Forensic Investigator Course &amp; Exam</td>
<td>ED-IST-CHFI-110</td>
<td></td>
<td>5 days</td>
<td>$3750</td>
<td>-</td>
</tr>
<tr>
<td>EC Council Certified Incident Handler Course &amp; Exam</td>
<td>ED-IST-ECIH-110</td>
<td></td>
<td>3 days</td>
<td>$2250</td>
<td>-</td>
</tr>
<tr>
<td>EC Council Advanced Penetration Testing Course &amp; Exam</td>
<td>ED-IST-APTLPT-110</td>
<td></td>
<td>3 days</td>
<td>$2250</td>
<td>-</td>
</tr>
<tr>
<td>EC Council Certified Chief Information Security Officer (CCISO) Course &amp; Exam</td>
<td>ED-IST-CCISO-110</td>
<td></td>
<td>5 days</td>
<td>$3750</td>
<td>-</td>
</tr>
</tbody>
</table>

Note: All prices referenced here are in $US Dollars. Please consult with your local RSA or RSA Partner Rep for pricing in your local region for any private classroom (on-site pricing).

* Each Training Credit (TC) has a $1.00 USD value denomination.