Training: Red Hat
RH415 Red Hat Security: Linux in Physical, Virtual, and Cloud

FORM OF TRAINING	MATERIALS	PRICE	DURATION
Traditional	Hardcopy	2050 EUR	4 days
Traditional	CTAB Tablet	2150 EUR	4 days

LOCATIONS

Krakow - 5 Tatarska Street, II floor, hours: 9:00 am - 4:00 pm
Warsaw - 17 Bielska Street, hours: 9:00 am - 4:00 pm

TRAINING GOALS:

Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415) is designed for security administrators and system administrators who need to manage the secure operation of servers running Red Hat® Enterprise Linux®, whether deployed on physical hardware, as virtual machines, or as cloud instances.

This course is based on Red Hat Enterprise Linux 7.5, Red Hat Satellite 6.3, Red Hat Ansible® Engine 2.5, Red Hat Ansible Tower 3.2, and Red Hat Insights.

Audience for this course:

- System administrators, IT security administrators, IT security engineers, and other professionals responsible for designing, implementing, maintaining, and managing the security of Red Hat Enterprise Linux systems and ensuring their compliance with the organization's security policies.

CONSPECT:

- Manage security and risk
  - Define strategies to manage security on Red Hat Enterprise Linux servers.
- Automate configuration and remediation with Ansible
  - Remediate configuration and security issues with Ansible Playbooks.
- Protect data with LUKS and NBDE
  - Encrypt data on storage devices with LUKS and use NBDE to manage automatic decryption when servers are booted.
- Restrict USB device access
  - Protect system from rogue USB device access with USBGuard.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
EUR: PL 81 2490 0005 0000 4600 6014 6631
USD: PL 63 2490 0005 0000 4600 6562 3381

- Control authentication with PAM
  - Manage authentication, authorization, session settings, and password controls by configuring pluggable authentication modules (PAMs).
- Record system events with audit
  - Record and inspect system events relevant to security, using the Linux kernel's audit subsystem and supporting tools.
- Monitor file system changes
  - Detect and analyze changes to a server's file systems and their contents using AIDE.
- Mitigate risk with SELinux
  - Improve security and confinement between processes by using SELinux and advanced SELinux techniques and analyses.
- Manage compliance with OpenSCAP
  - Evaluate and remediate a server's compliance with security policies by using OpenSCAP.
- Automate compliance with Red Hat Satellite
  - Automate and scale your ability to perform OpenSCAP checks and remediate compliance issues using Red Hat Satellite.
- Analyze and remediate issues with Red Hat Insights
  - Identify, detect, and correct common issues and security vulnerabilities with Red Hat Enterprise Linux systems by using Red Hat Insights.
- Perform a comprehensive review
  - Review the content covered in this course by completing hands-on review exercises.

REQUIREMENTS:

Red Hat recommends these prerequisites:

- Be a Red Hat Certified Engineer (RHCE), or demonstrate equivalent Red Hat Enterprise Linux knowledge and experience.

Difficulty level

CERTIFICATE:

Participants will obtain certificates signed by Red Hat.

TRAINER:

Red Hat Certified Instructor.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

ADDITIONAL INFORMATION:

Recommended next exam or course:

RH403 Red Hat Satellite 6 Administration

- Recommended for those interested in learning more about Red Hat Satellite

DO407 Automation with Ansible I and DO409 Automation with Ansible II: Ansible Tower

- Recommended for those who want to use DevOps practices to ensure security

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
EUR: PL 81 2490 0005 0000 4600 6014 6631
USD: PL 63 2490 0005 0000 4600 6562 3381