



Enterprise Computing Solutions - Education Services

NABÍDKA ŠKOLENÍ

Prosím kontaktujte nás zde

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: training.ecs.cz@arrow.com

Phone: +420 597 488 811

Kód:	DÉLKA:	CENA:
VMW_VCBEDRAA	8 Hours (1 den)	Kč bez DPH 11,000.00

Description

Školení je vedeno virtuálně v anglickém jazyce.

Cena školení je 410 EUR bez DPH - tato cena bude při fakturaci přepočtena aktuálním kurzem.

This one-day course teaches you how to use the advanced features of the VMware Carbon Black® EDR™ product. This usage includes gaining access to the Linux server for management and troubleshooting in addition to configuring integrations and using the API. This course provides an in-depth, technical understanding of the Carbon Black EDR product through comprehensive coursework and hands-on scenario-based labs. This class focuses exclusively on advanced technical topics related to the technical back-end configuration and maintenance.

Cíle

By the end of the course, you should be able to meet the following objectives:

- Describe the components and capabilities of the Carbon Black EDR server
- Identify the architecture and data flows for Carbon Black EDR communication
- Identify the architecture for a cluster configuration and Carbon Black EDR cluster communication
- Describe the Carbon Black EDR server data types and data locations
- Use the API to interact with the Carbon Black EDR server without using the UI
- Create custom threat feeds for use in the Carbon Black EDR server
- Perform the integration with a syslog server
- Use different server-side scripts for troubleshooting
- Troubleshoot sensor-side configurations and communication

Určeno pro

System administrators and security operations personnel, including analysts and managers

Vstupní znalosti

This course requires completion of the following course:

- VMware Carbon Black EDR Administrator

Program

1 Course Introduction	2 Architecture	3 Server Datastores
• Introductions and course logistics	• Data flows and channels	• SOLR database
• Course objectives	• Sizing considerations	• Storage configurations and data aging
4 EDR API	• Communication channels and ports	• Partition states
• CBAPI overview	5 Threat Intelligence Feeds	• Postgres
• Viewing API calls in the browser	• Feed structure	• Modulestore
• Utilizing the API to access data	• Report indicator types	6 Syslog Integration
	• Custom threat feed creation and addition	• SIEM support
		7 Troubleshooting
		• Server-side scripts
		• Server logs
		• Sensor operations

Termíny školení

Termíny školení na vyžádání, [kontaktujte nás prosím](#)

Dodatečné informace

Školení je možné zajistit na míru. [Kontaktujte nás pro bližší informace.](#)