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

VMware Carbon Black EDR Administrator

Kód:	DÉLKA:	CENA:
VMW_VCBEDRA	8 Hours (1 den)	Kč bez DPH 10,000.00

Description

Školení je vedeno virtuálně v anglickém jazyce.
Cena školení je 380 EUR bez DPH - tato cena bude při fakturaci přepočtena aktuálním kurzem.
This one-day course teaches you how to use the VMware Carbon Black® EDR™ product and leverage the capabilities to configure and maintain the system according to your organization's security posture and policies. This course provides an in-depth, technical understanding of the Carbon Black EDR product through comprehensive coursework and hands-on scenario-based labs.

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
- Describe the Carbon Black EDR server installation process
- Manage and configure the Carbon Black EDR sever based on organizational requirements
- Perform searches across process and binary information
- Implement threat intelligence feeds and create watchlists for automated notifications
- Describe the different response capabilities available from the Carbon Black EDR server
- Use investigations to correlate data between multiple processes

Určeno pro

System administrators and security operations personnel, including analysts and managers

Vstupní znalosti

There are no prerequisites for this course.

Program

1 Course Introduction
- Introductions and course logistics
- Course objectives

2 Planning and Installation
- Hardware and software requirements
- Architecture
- Data flows
- Server installation review
- Installing sensors

3 Server Administration
- Configuration and settings
- Carbon Black EDR users and groups

4 Process Search and Analysis
- Filtering options
- Creating searches
- Process analysis and events

5 Binary Search and Banning Binaries
- Filtering options
- Creating searches
- Hash banning

6 Search best practices
- Search operators
- Advanced queries

7 Threat Intelligence
- Enabling alliance feeds
- Threat reports details
- Use and functionality

8 Watchlists
- Creating watchlists
- Use and functionality

9 Alerts / Investigations / Response
- Using the HUD
- Alerts workflow
- Using network isolation
- Using live response

Termíny školení

Termíny školení na vyžádání, kontaktujte nás prosím

Dodatečné informace

Školení je možné zajistit na míru. Kontaktujte nás pro bližší informace.