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 Advanced Analyst

Kód:	DÉLKA:	CENA:
VMW_VCBEDRAAN	8 Hours (1 den)	Kč 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 VMware Carbon Black® EDR™ product during incident response. Using the SANS PICERL framework, you will configure the server and perform an investigation on a possible incident. This course provides guidance on using Carbon Black EDR capabilities throughout an incident with an in-depth, hands-on, scenario-based lab.

Cíle

By the end of the course, you should be able to meet the following objectives:
- Utilize Carbon Black EDR throughout an incident
- Implement a baseline configuration for Carbon Black EDR
- Determine if an alert is a true or false positive
- Fully scope out an attack from moment of compromise
- Describe Carbon Black EDR capabilities available to respond to an incident
- Create addition detection controls to increase security

Určeno pro

Security operations personnel, including analysts and incident responders

Vstupní znalosti

This course requires completion of the following course:
- VMware Carbon Black EDR Administrator

Program

1 Course Introduction
- Introductions and course logistics
- Course objectives

2 VMware Carbon Black EDR & Incident Response
- Framework identification and process

3 Preparation
- Implement the Carbon Black EDR instance according to organizational requirements

4 Identification
- Use initial detection mechanisms
- Process alerts
- Proactive threat hunting
- Incident determination

5 Containment
- Incident scoping
- Artifact collection
- Investigation

6 Eradication
- Hash banning
- Removing artifacts
- Continuous monitoring

7 Recovery
- Rebuilding endpoints
- Getting to a more secure state

8 Lessons Learned
- Tuning Carbon Black EDR
- Incident close out

Termíny školení

Termíny školení na vyžádání, kontaktujte nás prosím

Dodatečné informace

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