Manuals+ — User Manuals Simplified.

LUMIFY Carbon Black EDR Install Configure Manage User Guide

CLOUD COMPUTING AND VIRTUALISATION
VMware Carbon Black EDR: Install,
Configure, Manage

Contents

VMWARE AT LUMIFY WORK

VMware is the world leader in server virtualisation technolog ies. Lumify Work is a VMware Education Reseller Partner (VERP), offering training in vSphere, vRealize, vSAN, Horizon, NSX-T, Workspace ONE, Carbon Black, and other VMware technolog ies and platforms.

LENGTH	PRICE (Incl. GST)	VERSION
3 days	$3,960	7.x

WHY STUDY THIS COURSE

This course provides you with the knowledge, skills, and tools to achieve competency in installing, conf iguring, and managing the VMware Carbon Black® EDR™ environment. This course introduces you to product features, capabilit ies, and workf lows for managing endpoint security. Hands-on labs enable learners to reinforce topics by performing operat ions and tasks within the product in a training environment.

Product Alignment

- VMware Carbon Black® EDR™ 7.7

WHAT YOU'LL LEARN

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

- Describe the architecture of a Carbon Black EDR implementat ion
- Perform the installat ion, upgrade, and conf igurat ion of the Carbon Black EDR server
- Describe the purpose and use of mult iple datastores in the server
- Perform live queries across endpoints to gather addit ional data
- Perform effect ive searches across the dataset to f ind security art ifacts related to the endpoints
- Manage Threat Intelligence Feeds and Watchlists
- Describe connectors in Carbon Black EDR
- Troubleshoot server and sensor problems
- Analyse data found in the Heads-Up Display
- Manage invest igat ions to group and summarise security incidents and art ifacts
- Perform the different response capabilit ies available to users in Carbon Black EDR
- Use the Carbon Black EDR API to automate tasks

My instructor was great being able to put scenarios into real world instances that related to my specific situation.
I was made to feel welcome from the moment I arrived and the ability to sit as a group outside the classroom to discuss our situations and our goals was extremely valuable.

I learnt a lot and felt it was important that my goals by attending this course were met.
Great job Lumify Work team.

AMANDA NICOL
IT SUPPORT SERVICES MANAGER – HEALTH WORLD LIMITED
Lumif y Work Customised Tra ining
We can also deliver and customise this training course for larger groups saving your organisation time, money and resources.
For more information, please contact us on 1 800 853 276.

COURSE SUBJECTS

1. **Course Int roduct ion**
   - Introduct ions and course logist ics
   - Course object ives

2. **Planning and Archit ect ure**
   - Describe the architecture and components of Carbon Black EDR
   - Ident ify the communicat ion requirements for Carbon Black EDR

3. **Server Inst a llat ion, Upgrade, and Adm inist rat ion**
   - Install the Carbon Black EDR server
   - Describe the opt ions during the installat ion process
   - Install a Carbon Black EDR sensor
   - Conf irm data ingest ion in the Carbon Black EDR server
   - Ident ify built-in administrat ion tools
   - Manage sensor groups
   - Manage users and teams

4. Server Dat ast ores
   - Describe the datastores used in Carbon Black EDR
   - Interact with the available datastores

5. **Live Query**
   - Describe live query capabilit ies
   - Perform queries across endpoints

6. **Searching and Best Pract ices**
   - Describe the capabilit ies and data available in the process search

7. **Threat Int elligence Feeds and Wat chlist s**
   - Perform process searches to f ind specif ic endpoint act ivity
   - Describe the capabilit ies and data available in the binary search
   - Perform binary searches to f ind applicat ion data
   - Describe the query syntax and advanced use cases
   - Perform advanced queries across the dataset
   - Def ine Threat Intelligence Feeds
   - Manage the available Threat Intelligence Feeds
   - Describe the use of Watchlists

- Manage Watchlists in the environment

8. **Connect ors in Carbon Black EDR**
   - Conf igure connectors in Carbon Black EDR
   - Troubleshoot connectors

9. **Troubleshoot ing**
   - Ident ify the available troubleshoot ing scripts in the Carbon Black EDR server
   - Run troubleshoot ing scripts to ident ify problems
   - Generate a sensor log bundle
   - Ident ify the locat ion of sensor registry keys

10. **Head-Up Display**
    - Ident ify panels relat ing to endpoint data
    - Analyse endpoint data provided by the panels
    - Ident ify panels relat ing to operat ions data

11. Invest igat ions
    - Analyse operat ions data provided by the panels
    - Ident ify panels relat ing to server data
    - Analyse server data provided by the panels
    - Def ine alert generat ion in Carbon Black EDR
    - Manage alerts
    - Describe invest igat ions
    - Explore data used in an invest igat ion
    - Manage invest igat ions
    - Manage invest igat ion events

12. Responding t o Endpo int Incident s
    - Describe isolat ion in Carbon Black EDR
    - Manage isolat ing endpoints
    - Describe live response capabilit ies
    - Manage live response sessions
    - Describe hash banning
    - Manage banned hashes

13. Overview of Post man and t he Carbon Black EDR API
    - Explain the use of the API
    - Different iate the APIs available for Carbon Black EDR
    - Explain the purpose of API tokens
    - Create an API token
    - Explain the API URL
    - Create a valid API request
    - Import a collect ion to Postman
    - Init iate an API request from Postman
    - Perform operat ions manually using Postman
    - Analyse the use cases for Postman
    - Show basic automat ion tasks using the API and curl
    - Compare the usage of curl with Postman

WHO IS THE COURSE FOR?

- Security analyst, threat hunters, or incident responders
- Security professionals who work with enterprise and endpoint security tools

PREREQUISITES

- There are no prerequisites for this course.

The s upply of this cours e by Lumify Work is governed by the booking terms and conditions . Pleas e read the terms and conditions carefully before enrolling in this cours e, as enrolment in the cours e is conditional on acceptance of thes e terms and conditions .
https://www.lumifywork.com/en-au/courses/vmware-carbon-black-edr-install-configure-manage/

Call 1800 853 276 and
speak to a Lumify Work
Consultant today!

✉ **training@lumifywork.com**

🌐 **lumifywork.com**

facebook.com/LumifyWorkAU

linkedin.com/company/lumify-work

twitter.com/LumifyWorkAU

youtube.com/@lumifywork

Documents / Resources

LUMIFY Carbon Black EDR Install Configure Manage [pdf] User Guide
Carbon Black EDR Install Configure Manage, Black EDR Install Configure Manage, EDR Install Configure Manage, Install Configure Manage, Configure Manage, Manage

References

- ⊛ **Lumify Work | Lumify Work AU**
- **User Manual**