

VMware Carbon Black EDR or Hosted EDR Threat Hunting Add-On

AT A GLANCE

The primary objective of this service is to assist customer on optimizing with the VMware Carbon Black EDR or Hosted EDR purchase.

A VMware Consultant will work jointly with the Customer team via remote working sessions to work with you on threat hunting sessions based on VMware Carbon Black EDR or Hosted EDR product.

KEY BENEFITS

- Rapid time to value on your newly purchased VMware Carbon Black EDR or Hosted EDR product.
- Increase security posture and visibility, decrease incident response time, and lock out malicious attacks before they have a chance to infiltrate your data.

Overview

The VMware Carbon Black EDR or Hosted EDR Threat Hunting Add-On service assists you with optimizing the Carbon Black EDR or Hosted EDR to your environment.

This service is ideal for organizations who have already setup the initial Carbon Black EDR or Hosted EDR environment and desire optimize the setup based on VMware best practice guidance.

Part Number / SKU	Service Description
VSEC-CB-EDR-HEDR-PS-THADN	VMware Carbon Black EDR or Hosted EDR-PS-Threat Hunting Add-On (REMOTE ONLY)

Project Scope

The scope of the service includes the following:

VSEC-CB-EDR-HEDR-PS-THADN

VMware Carbon Black EDR or Hosted EDR Threat Hunting Add-On (REMOTE ONLY)

Service includes threat hunting sessions using customer's VMware Carbon Black EDR or Hosted EDR setup for up to 3000 Carbon Black EDR or Hosted EDR Endpoints.

Customer is expected to have Carbon Black EDR sensors installed and communicating with the EDR or Hosted EDR servers.

Specification	Parameters	Description
Knowledge Transfer workshop(s)	Up to (7) seven hours	Conduct Knowledge transfer workshops of the following: threat hunting, threat intelligence feeds, watchlist tuning, Q&A.

Outcomes

Customer will be able to accomplish the following outcomes after the project:

- Improve SOC/IR effectiveness and efficiency via an enriched centralize and customizable threat intelligence platform
- Improve insights on complex attack sequence via real-time continuous recording of events in all deployed endpoints or workloads
- Ability to response to incidents quickly with continuous visibility across the enterprise

Estimated Schedule

VMware consulting services will be performed according to a schedule agreed to by both parties. Typically, consulting services are performed during normal business hours and workdays (weekdays and non-holidays).

Project Activities

The activities for this engagement are organized in phases below.

Phase 1: Initiate

The VMware Project Manager coordinate project initiation via email with key Customer and VMware stakeholders. Topics include the following:

- Project scope and objectives.
- Project deadlines, estimated timelines, scheduling, and logistics.
- Identification of key Customer team members with whom VMware will work to perform the tasks defined in this datasheet.
- Participating team members are confirmed, and contact details are exchanged to schedule execution phase.

Deliverables

- Project Initiation Email

Phase 2: Execute

The key activities for this phase are organized in the following sub-phases:

2.1 Execute: Knowledge Transfer

VMware conducts knowledge transfer sessions covering the design, implementation, and operational considerations relating to the scope of this project. VMware does the following:

- Conducts up to seven (7) hours of knowledge transfer sessions for appropriate Customer representatives.
- Provides an adoption guide document(s) containing operational guidance for the specified solutions.

Note: For the avoidance of doubt, the Knowledge transfers herein do not comprise VMware product training or certification courses as offered by the VMware Education unit -(<http://mylearn.vmware.com/mgrreg/index.cfm>).

Deliverables

- Adoption guide document
- Knowledge transfer workshop presentation
- Up to seven (7) hours of knowledge transfer sessions

Phase 3: Close

The VMware Project Manager sends email to the Customer covering project status, next steps, and how to engage further with VMware.

Deliverables

- One (1) closure email

Out of Scope

The following are the out of scope items for this project.

General

- Installation and configuration of custom or third-party applications and operating systems on deployed virtual machines.
- Operating system administration including the operating system itself or any operating system features or components.
- Management of change to virtual machines, operating systems, custom or third-party applications, databases, and administration of general network changes within Customer control.
- Remediation work associated with any problems resulting from the content, completeness, accuracy, and consistency of any data, materials, or information supplied by Customer.
- Installation or configuration of VMware products not included in the scope of this document.
- Installation and configuration of third-party software or other technical services that are not applicable to VMware components.
- Configuration of VMware products used for the service other than those implemented for the mutually agreed to use cases.
- Customer solution training other than the defined knowledge transfer session.

Carbon Black EDR or Hosted EDR Threat Hunting Add On

- Remediation/removal of unauthorized, malicious, or unwanted files.
- Investigation and analysis of potential malware and threats.
- Configuring more than one administration console.
- Building of custom scripts or feeds.
- Performing custom threat feed configuration.
- Customer solution training other than the defined in scope services.
- Developing custom documentation.
- Troubleshooting integration or infrastructure issues when deemed to be non-Company product issues.

Prerequisites Checklist

Customer is responsible for executing all items discussed in the Service Checklist prior to starting of the Execution phase.

Endpoints/Workloads minimum operating environment:

- CPU - 2 Cores Minimum: 1.5 GHz, Recommended: 2 GHz
- Memory - Minimum: 1 GB. Recommended: 2 GB for Windows 10 and Windows Server 2016 or higher
- Network - Minimum: 100 Mbit, Recommended: 1 Gbit
- Disk Space - Minimum: 100 MB of free disk space on the system volume, Recommended: 500 MB plus an additional 600 MB if local scanning is enabled

LEARN MORE

Visit vmware.com/services.

FOR MORE INFORMATION

Contact a Professional Services expert at vmware.com/company/contact.html.

Participation of the following Customer stakeholders is required for the Service to be performed:

- Enterprise Architect
- Infrastructure Architect
- IT Operations Manager
- IT Security Manager

TERMS AND CONDITIONS

This datasheet is for informational purposes only. VMWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DATASHEET. All VMware service engagements are governed by the VMware Professional Services [General Terms and Conditions](#). If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc. If you are outside the United States, the VMware contracting entity will be VMware International Limited.

If you purchase this packaged service outside of the ELA, the service must be delivered and accepted within the first 12 months of the purchase, or the service will be forfeited. Pricing for this service includes travel and other expenses. For detailed pricing, contact your local VMware representative.

