

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

AT A GLANCE

The primary objective of this service is to assist the 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

VSEC-CB-EDR-HEDR-PS-THADN

Service includes threat hunting sessions using the customer's VMware Carbon Black EDR or Hosted EDR setup for up to 3,000 Carbon Black EDR or Hosted EDR Endpoints. The customer is expected to have Carbon Black EDR sensors installed and communicating with the EDR or Hosted EDR servers.

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). REMOTE ONLY

Service Assumptions

CUSTOMER RESOURCES: Should Customer request VMware to perform tasks that are dependent upon Customer resources or decisions, Customer will make such resource available or decisions final in a timely manner.

HARDWARE PROCUREMENT: Procurement and installation of hardware is the responsibility of Customer. VMware will provide recommendations and assistance.

WORKSITE: The Software Related Services tasks may be performed on-site or remotely. An approximate travel schedule will be mutually agreed. Travel expenses are not included in the packaged offering and will be quoted separately and agreed mutually between Customer and VMware.

ON-SITE TRAVEL: In weeks where both parties have agreed that an on-site resource is prudent, travel for VMware consultants will occur on Mondays and Thursdays unless otherwise agreed. It is expected that consultants will travel to Customer's facility on Monday morning, arriving on site as early on Monday as possible, as dictated by flight options and travel time. The consultants will work on-site through Thursday and will schedule return travel on Thursday evenings, as available. Travel expenses are not included in this Datasheet.

WORKING HOURS: Engagements that require consultants to work in excess of 40 hours per week, to work on weekends or major national holidays and/or to travel outside of this schedule will be considered exceptions to this policy and will be reviewed and approved by VMware and Customer as required.

PRE-REQUISITES: Pre-requisites must be completed for all installation components before any installation activities will be performed. Should Customer not purchase the associated software for deployment, the services deliverable line items associated with those software components will not be delivered.

PROJECT MANAGEMENT: VMware and the Customer's project management will work closely together to ensure that project scope remains consistent and issues are resolved on a timely basis.

DELIVERABLE LANGUAGE: All work, documentation and work product(s) will be provided in English.

USE-CASE SCOPE: The scope of the use-cases will be considered locked upon completion of Deliverable 1.1 (See Service Deliverables Table below) and will be delivered within a single production deployment phase. Any alteration to the use-case scope thereafter may necessitate a change request.

Responsibilities

All supplier and Customer responsibilities are listed in the Deliverables section. The ownership is defined as follows:

- Primary Owner = VMware: VMware is responsible for delivery, with minimal assistance from Customer's project team.
- Joint: VMware and Customer's project team are jointly responsible for delivery.
- Primary Owner = CUSTOMER: Customer is responsible for delivery, with minimal assistance from VMware.

Completion Criteria

The project will be deemed complete when any of the criteria below are met.

1. Completion of all service deliverables included in the Deliverables section.
2. Consumption of up to seven (7) hours of Consulting Services inclusive of meetings and email correspondence; effort associated with this allocation of hours shall only be allocated to tasks defined in Datasheet.
3. Passage of eight (8) weeks after project kick-off (Deliverable 1.1).

Deliverables

ID	Description	Tool/Deliverable	Primary Owner	Comments
Phase 1: Plan				
1.1	Review key success criteria for Customer's deployment	-	Joint	VMware to document
1.2	Review Datasheet	-	CUSTOMER	Understand service assumptions, scope, and completion criteria
1.3	VMware Summarizes Key Next Steps and Requirements for Phase 2 (Execute)	-	VMWare	VMware to deliver follow-up documentation confirming deliverables from Phase 1 (Plan) and next steps for Phase 2 (Execute)
Phase 2: Execute				
2.1	Configuration Assistance	Create up to fifteen (15) policies and/or rules	Joint	Conduct knowledge transfer workshops of the following topics: threat hunting, threat intelligence feeds, watchlist tuning, Q&A
2.2	Alerts and Watchlist Hits	Review and triage up to fifteen (15) alerts and watchlist hits	Joint	Assist with alert notifications and triage
Phase 3: Close				
3.1	Customer Support Transition	Project closure email	VMware	Transition to support

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.
- Troubleshooting integration or infrastructure issues when deemed to be non-Company product issues

LEARN MORE

Visit vmware.com/services.

FOR MORE INFORMATION

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

Prerequisites Checklist

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

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.

