Professional Services for Security Cyber Defense Simulation Service

At a glance

The Cyber Defense Simulation Service is a fun, dynamic event that provides hands-on experience for VMware Carbon Black Cloud products. The event allows customers to hunt and identify attacks in realistic scenarios.

Key benefits

- Address the holistic nature of security threats in all areas: people, process, and technology
- Learn techniques and skills to mitigate threats before, during, and after attacks
- Leverage real-world cyberwar exercises and incident response practices
- Highly secure and segmented platform allows hosting of malicious code and network activity in simulated environment
- Fun learning event for team building activities which does not require deep technical knowledge of the Carbon Black Cloud platform

SKU

PS-CBC-CYBR-DFS
(AMER and EMEA only)

SOW

This service is also available within a Statement of Work (SOW)
(AMER, EMEA, and APJ)

Overview

The cybersecurity landscape is in a perpetual state of change. It's no longer a matter of if an organization will encounter an attack, but when. Attackers may be inside a network for days, weeks, or months, preparing and executing attacks without detection. Attackers deliberately disguise and hide to evade automated defenses, making it harder than ever to protect endpoints with certainty.

An attacker's ability to proceed undetected leaves security staff stretched thin and struggling to keep systems safe. Traditional endpoint security can't be relied upon to prevent all modern attacks and adding agents and tools to a security stack adds unwanted complexity.

Threat hunting is an essential process for organizations to preempt destructive attacks. This process is a proactive approach to cybersecurity that identifies gaps in defenses to seek out and stop attacks before they ingrain deeply into an organization's IT environment. Threat hunting seeks out covert indicators of compromise (IOCs) to mitigate attacks before an adversary can achieve its objectives.

Continuously testing and developing skills to protect an organization from destructive attacks is crucial to honing security skills and staying ahead of cybercriminals.

Cyber Defense Simulation Service Description

The Cyber Defense Simulation Service is a fun, interactive game that gives participants exposure to threat hunting and incident response using the Carbon Black Cloud Native Endpoint Environment. During the event, participants work against the clock to answer questions and score points.

The event features the Carbon Black Cloud platform for threat hunting, investigation, and analysis. Typical exercises in the challenge facilitate understanding of the different stages of the cyber kill chain and swiftly plan how and where to stop each phase before becoming exposed to a larger targeted attack.

As per industry standard kill chains such as MITRE Attack and Lockheed, the theory is that by understanding each of these stages, defenders can better identify and stop attacks at each stage before they transition into a larger attack

surface. The more entry points at which threat actors can be intercepted, the more likely an organization will be able to deny them of data exfiltration.

The challenge assesses participants not only for threat hunting of abnormal behavior, but it also challenges participants to leverage other features and functionalities of the VMware Carbon Black Cloud Platform such as Carbon Black Live Response for data collection and root cause analysis, Carbon Black NGAV policies for enforcing protection activities and banning SHA/MD5/Hash/Binaries across the organization, and understanding of global threat detection by incorporating Carbon Black Cloud watchlists and audit and remediation queries.

The Cyber Defense Simulation challenge helps participants to develop skillsets across the threat hunting landscape, supporting SOC development and threat hunting.

Deliverables

The Cyber Defense Simulation challenge does not require deep technical knowledge of the Carbon Black Cloud platform.

- The event allows up to 15 participants at a time for the challenge
- The event starts with a planning session where VMware consultants research and understand the current skill set gaps and needs for the customer as per their Carbon Black implementation
- Following the planning session, a kickoff session is conducted where the details of the challenge, question format, and the overview of the Carbon Black Cloud environment is shared with participants
- As per Customer requirements, the challenge is conducted in one of three options:
    - Three-day event with 2.5 hours of support from a VMware consultant over Teams/Zoom/Slack
    - Four-day event with 2 hours of support from a VMware consultant over Teams/Zoom/Slack
    - Five-day event with 1.5 hours of support from a VMware consultant over Teams/Zoom/Slack
- After completion of the event, participants will present a summary of the work to VMware consultants for review and feedback
- A full simulation walkthrough will be provided to share best practices and methodologies for threat hunting, investigation, and triaging

Estimated Schedule and Scope

The estimated time needed for this service is as follows.

Preparation – 8 hours

- Initial coordination
- Kickoff meeting
- Event preparation
- Walkthrough

Event Support – 8 hours (event troubleshooting, hints, etc.)

- Lab maintenance (before and after event)
- Attack development and maintenance

Event Execution – 8 hours

- Hints and troubleshooting
- General event support
- May be spread over three, four, or five days dependent on customer options selected

Post Event Support – 8 hours

- Grading
- Analysis
- Reporting
- Creating post-event guide (challenge review, areas of improvement and focus, etc.)

Closure

- Closure email and/or call (may be included as part of post-event activities)

Scheduling

1. The event will be scheduled between the VMware Professional Services Project Manager and the customer during the project kick-off meeting. The event will be scheduled to begin no more than 120 days (4 months) following the project kick-off meeting.
2. Once the event begins, it is to be completed within five (5) consecutive working days.

Customer Requirements

The challenge does not require deep technical knowledge of the Carbon Black Cloud platform, but it does require basic knowledge. Customers are expected to attend the following:

- Pre-event planning workshop – up to 2 hours
- Event day simulation planning walkthrough – up to 2 hours
- Cyber Defense Simulation event – three, four, or five days based on option selected by customer
- Post-event workshop – up to 4 hours

Completion Criteria

The service is complete when any one of the following criteria are met:

- Completion of event and related workshops
- 12 months (365 days) after purchase date (service purchase expires)
- If PSO credits expire within the active service period, the service purchase expires at the same time credits expire unless a credit extension is requested. Customers must work with their Account Executive to determine a plan for all remaining credits on their account and to request an extension.

Out of Scope

- Any custom requirements from customers are out of scope for this engagement
- No modifications will be executed in the Cyber Defense Simulation environment that replicate with the customer ecosystem
- Any follow-up Professional Services work as an outcome of this engagement is out of scope for this service

Service Assumptions

- Customer Resources: Should the Customer request VMware to perform tasks that are dependent upon Customer resources or decisions, the Customer will make the required resources available or decisions final in a timely manner.
- Hardware Procurement: Procurement and installation of hardware (if any) is the responsibility of the Customer. VMware will provide recommendations and assistance.
- Working Hours: VMware resources will only be actively available during Americas business hours (9 am to 5 pm EST) and for the time blocks decided upon between the customer and VMware.

Learn more

Visit vmware.com/services.

- Project Management: VMware and the Customer's project management will work closely together to ensure that project scope remains consistent and to avoid any scope creep.
- Deliverable Language: The event, challenge, documentation, and work product(s) will be delivered in English.

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