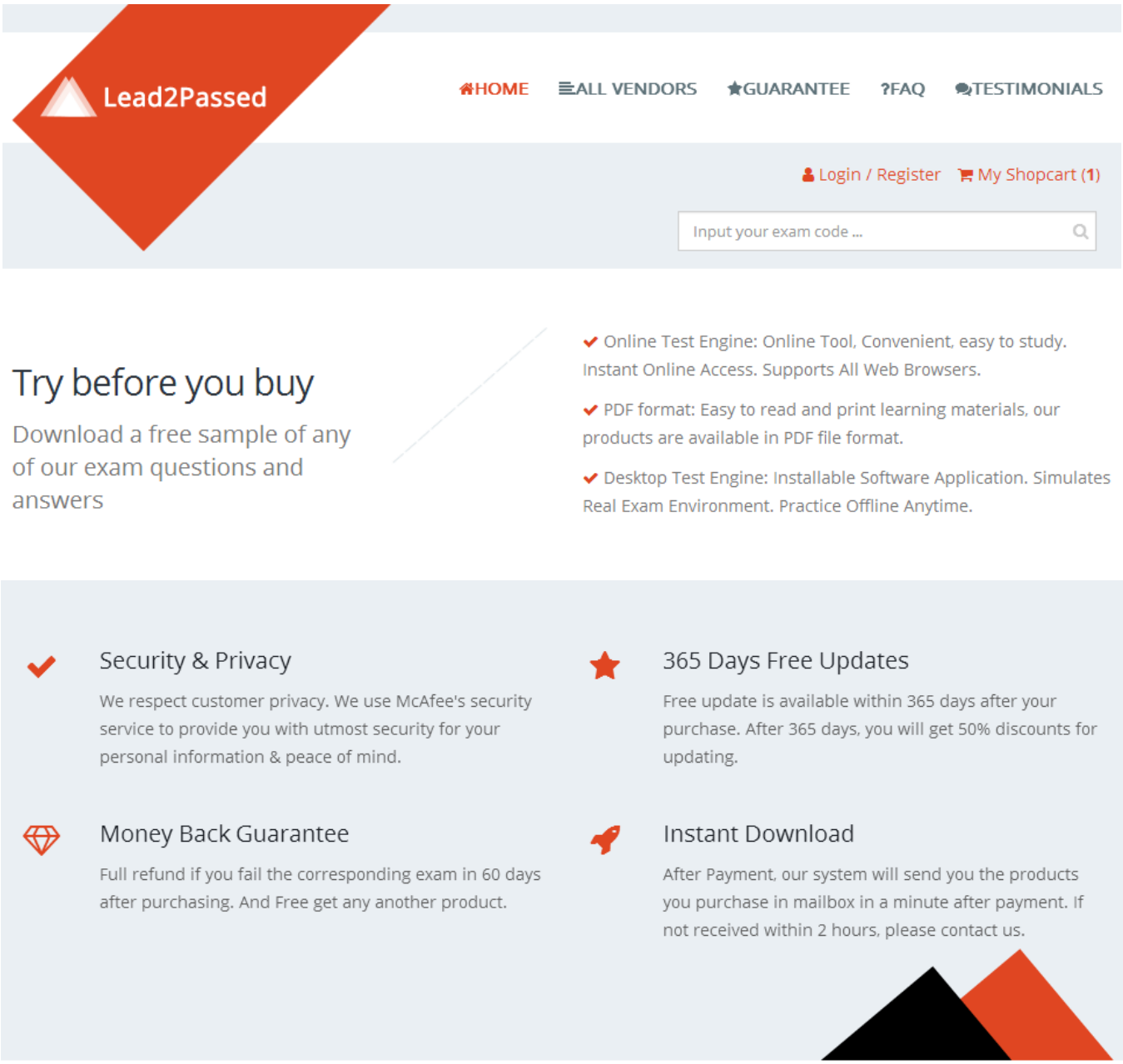
Lead2Passed



http://www.lead2passed.com

Valid Certification Exam Dumps Materials and Study Guide - Lead2Passed

Exam : **6V0-21.25**

Title : VMware vDefend Security for VCF 5.x Administrator

Vendor : VMware

Version : DEMO

NO.1 The VMware vDefend Management cluster is deployed by default with how many nodes?
A. One
B. Two
C. Three
D. Four
Answer: C
Explanation:
VMware vDefend (formerly NSX) architecture utilizes a Management Plane that is highly available. For production environments, the NSX Management cluster is deployed with exactly three nodes. This ensures high availability (HA) and fault tolerance for the management and control planes. If one node fails, the cluster maintains quorum and operations continue uninterrupted. While a single node can be deployed for lab or proof-of-concept environments, the default standard for a highly available production cluster is three nodes.

NO.2 Which one of the following are the ICMP Timer Variables that can be customized within the vDefend Distributed Firewall?
A. First Packet, and Error Reply
B. First Packet, Single, and Multiple
C. Last Packet, and Static and Dynamic Errors
D. First Packet, Open, Established, Closing, Fin Wait, and Closed
Answer: A

NO.3 Which of the following are vDefend Advanced Threat Prevention capabilities? (Select all that apply)
A. Network Traffic Analysis (NTA)
B. Malware Analysis/Sandboxing
C. Network Detection and Response (NDR)
D. Intrusion Detection/Protection Systems (IDS/IPS)
E. Gateway Firewall
Answer: A,B,C,D

NO.4 In a vDefend NDR campaign, "hosts" refers to which of the following?
A. vSphere hosts
B. Workloads
C. VCF nodes
D. NSX-prepared cluster hosts
Answer: B
Explanation:
Within the VMware vDefend Network Detection and Response (NDR) UI and alerting systems, the term "hosts" is used from a cybersecurity perspective, not an infrastructure perspective. It refers directly to the network endpoints or virtual machines-specifically, your Workloads-that are participating in the analyzed traffic. It does not refer to the underlying physical hypervisors (like vSphere ESXi hosts or VCF nodes) that run the compute layer. NDR monitors these workload "hosts" to correlate suspicious activities into broader threat campaigns.

NO.5 Which of the following represent operational inefficiencies for application owners when it comes to security implementation? (Select all that apply)
A. Lack of visibility in hybrid cloud environments
B. Lack of automation across tools and platforms
C. Lack of communication between infrastructure and application teams
D. Lack of application awareness for network-based security policies
Answer: B,C,D
Explanation:
In modern data centers, implementing micro-segmentation often fails due to operational silos and inefficiencies rather than technology limitations. Application owners typically struggle with a lack of automation across disjointed security tools (Option B), a historical lack of communication between the infrastructure/network teams and the application developers (Option C), and traditional network-based security policies (like IP addresses and VLANs) that lack contextual awareness of the actual applications they are protecting (Option D). vDefend Security Intelligence is designed specifically to solve these exact inefficiencies by providing deep application visibility and automated rule recommendations.

NO.6 Which of the following are valid logon detection methods for IDFW? (Select all that apply)
A. Guest Introspection
B. Event Log Scrapping
C. Identity Access Management
D. Single Sign On (SSO)
Answer: A,B
Explanation:
The VMware vDefend Identity Firewall (IDFW) allows administrators to create distributed firewall rules based on Active Directory user identities rather than just IP addresses. To do this, vDefend must accurately map a user's login to a specific VM's IP address. It achieves this mapping through two primary supported logon detection methods:
Guest Introspection: An agent-based method utilizing VMware Tools installed on the guest OS to detect logons locally.
Event Log Scraping: An agentless method where vDefend integrates directly with Active Directory to scrape security event logs and track authentication events across the network.

NO.7 Which of the following are important components to cyber security design? (Select all that apply)
A. Proactive protection
B. Deep visibility
C. Recovery
D. Kernel remediation and upgrade
Answer: A,B,C
Explanation:
A robust, modern private cloud cybersecurity design framework focuses on three core pillars: Proactive Protection (implementing micro-segmentation and strict zero-trust access controls to prevent breaches before they happen), Deep Visibility (gaining granular insights into all East-West

traffic flows and application dependencies to identify anomalies), and Recovery (ensuring the environment can quickly isolate compromised workloads and restore services). Kernel remediation and upgrades (Option D) fall under general IT lifecycle patching and OS maintenance, not the overarching architectural pillars of network cybersecurity design.

NO.8 Which of the following is NOT true in the context of Malware Prevention?

A. Static Analysis is good at catching the benign files and good at catching the obvious malicious files

B. Static Analysis determines if dynamic analysis is needed

C. All the files are sent to NSX advanced threat prevention service for dynamic analysis

D. Dynamic Analysis provides full visibility into subject behavior and system memory

Answer: C

Explanation:

Option C is the false statement. Sending every single file crossing the network to the cloud sandbox (dynamic analysis) would consume a massive amount of network bandwidth and severely impact performance. Instead, vDefend Malware Prevention uses a highly efficient pipeline: it first checks the file hash, then performs local Static Analysis to catch obvious malware and clear benign files. It is only when the local static analysis deems a file "suspicious" or "unknown" that it is forwarded to the Advanced Threat Prevention cloud service for deep, behavior-based Dynamic Analysis (sandboxing).