1V0-81.20.VCEplus.premium.exam.54q

1V0-81.20

Associate VMware Security

Version 1.0

Exam A

QUESTION 1

Which VMware product allows you to query an endpoint like a database?

A. VMware NSX-T Data Center
B. VMware Carbon Black Audit & Remediation
C. VMware Workspace ONE UEM
D. VMware Carbon Black Endpoint Standard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2 Which three are industry best practices of Zero Trust framework? (Choose three.)

A. Employee machines need to have a passcode profile setup
B. Employee machines on Internal network are trusted and have access to all internal resources
C. Employee machines are checked for compliance before they get access to applications
D. Employees are not required to provide MFA to access internal resources over VPN
E. Employees get access to only the required resources to get their job done

Correct Answer: ACE
Section: (none)
Explanation

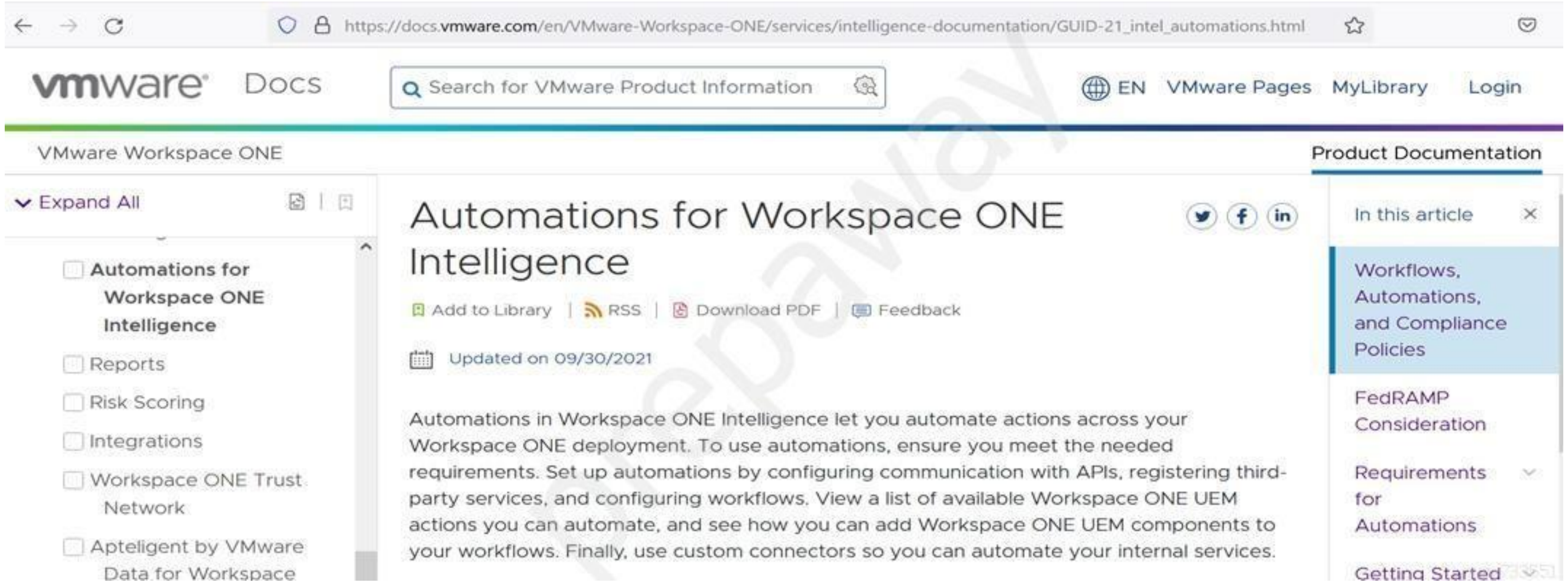
Explanation/Reference:

QUESTION 3 Which three default connectors are available in Workspace ONE Intelligence to execute automation actions? (Choose three.)

A. ServiceNow
B. vRealize Operations Manager
C. Slack
D. Log Insight
E. Workspace ONE UEM

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:


https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligence-documentation/GUID-21_intel_automations.html
vmware Docs
Search for VMware Product Information
EN
VMware Pages
MyLibrary
Login
VMware Workspace ONE
Product Documentation
Expand All
Automations for Workspace ONE Intelligence
Reports
Risk Scoring
Integrations
Workspace ONE Trust Network
Apteligent by VMware Data for Workspace
Add to Library | RSS | Download PDF | Feedback
In this article
Workflows, Automations, and Compliance Policies
FedRAMP Consideration
Requirements for Automations
Getting Started

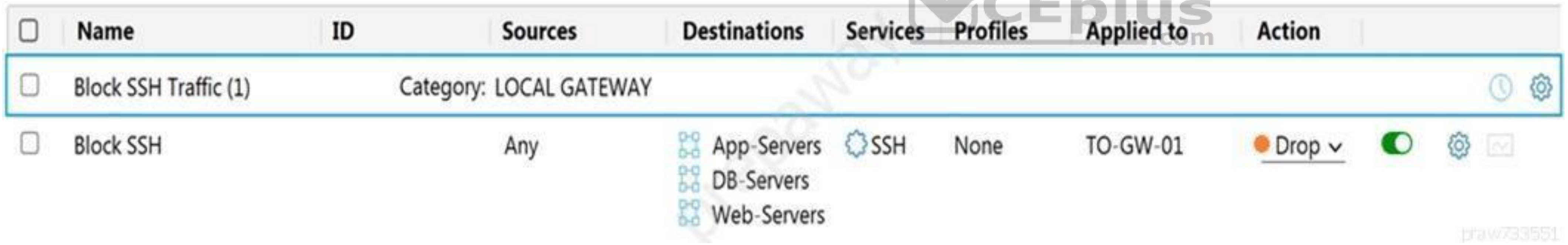
Automations for Workspace ONE Intelligence

Updated on 09/30/2021

Automations in Workspace ONE Intelligence let you automate actions across your Workspace ONE deployment. To use automations, ensure you meet the needed requirements. Set up automations by configuring communication with APIs, registering third-party services, and configuring workflows. View a list of available Workspace ONE UEM actions you can automate, and see how you can add Workspace ONE UEM components to your workflows. Finally, use custom connectors so you can automate your internal services.

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligence-documentation/GUID-21_intel_automations.html

QUESTION 4
Refer to the exhibit.



☐	Name	ID	Sources	Destinations	Services	Profiles	Applied to	Action
☐	Block SSH Traffic (1)	Category: LOCAL GATEWAY						
☐	Block SSH		Any	App-Servers DB-Servers Web-Servers	SSH	None	TO-GW-01	● Drop

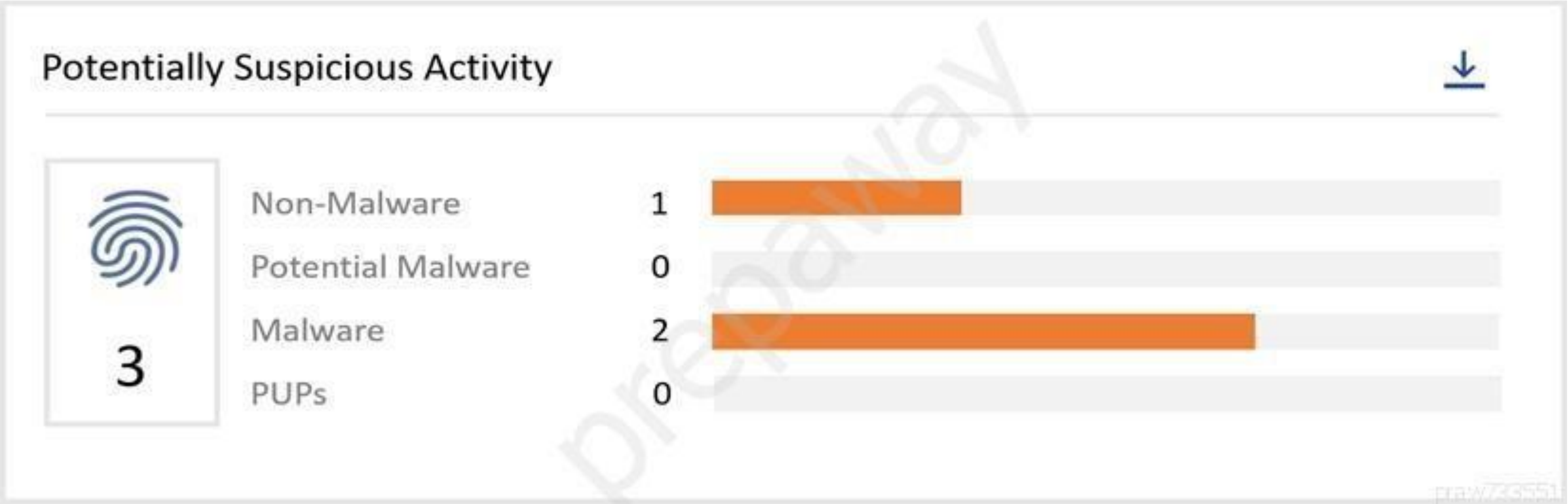
Which statement is true about the firewall rule?

A. It is a gateway firewall applied to a Tier-0 gateway that drops traffic on port 22
B. It is a distributed firewall applied to App-Services, DB-Servers and Web-Servers that rejects traffic on port 22
C. It is a distributed firewall applied to App-Services, DB-Servers and Web-Servers that drops traffic on port 22
D. It is a gateway firewall applied to a Tier-0 gateway that rejects traffic on port 22

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Refer to the exhibit.



From the VMware Carbon Black Cloud console, what page do you go to after clicking the Non-Malware bar in the Potentially Suspicious Activity chart?

A. Notifications page with the selected alert filtered
B. Reputations page with the selected reputation filtered
C. Investigate page with the selected reputation filtered
D. Alerts page with the selected alert filtered

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide.pdf (15)

QUESTION 6 Which four alert filters are available in the VMware Carbon Black Cloud Investigate page?
(Choose four.)

A. Watchlist
B. Target Value
C. Policy
D. Security Alert List
E. Effective Reputation
F. Alert Severity

Correct Answer: ABCF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 Which is a common solution to implement for inbound network attacks?

A. Load Balancer
B. Firewall
C. Proxy
D. Reverse Proxy

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 8 Which two are true about a VMware Service-defined Firewall?
(Choose two.)

A. A firewall that allows you to use 3rd party features like IDS/IPS, threat protection, anti-bot, and anti-virus solutions
B. A firewall that blocks external access into your internal network based on IP services
C. A firewall that enforces policy for North-South traffic
D. A firewall that is auto scalable as new workloads are deployed
E. A firewall that provides East-West protection between internal applications

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmware-nsx-service-defined-firewall.pdf

QUESTION 9 Which of the following is true about VMware Carbon Black Cloud Enterprise EDR watchlists?

A. They only update annually
B. You cannot customize them
C. They are made up of reports
D. Each watchlist is user specific

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Carbon-Black-EDR/7.5/VMware%20Carbon%20Black%20EDR%207.5%20User%20Guide.pdf

QUESTION 10 A technician has been asked to confirm a specific browser extension does not exist on any endpoint in their environment.

Which is the VMware Carbon Black tool to use for this task?

A. Enterprise EDR
B. EDR
C. Audit and Remediation
D. Endpoint Standard

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

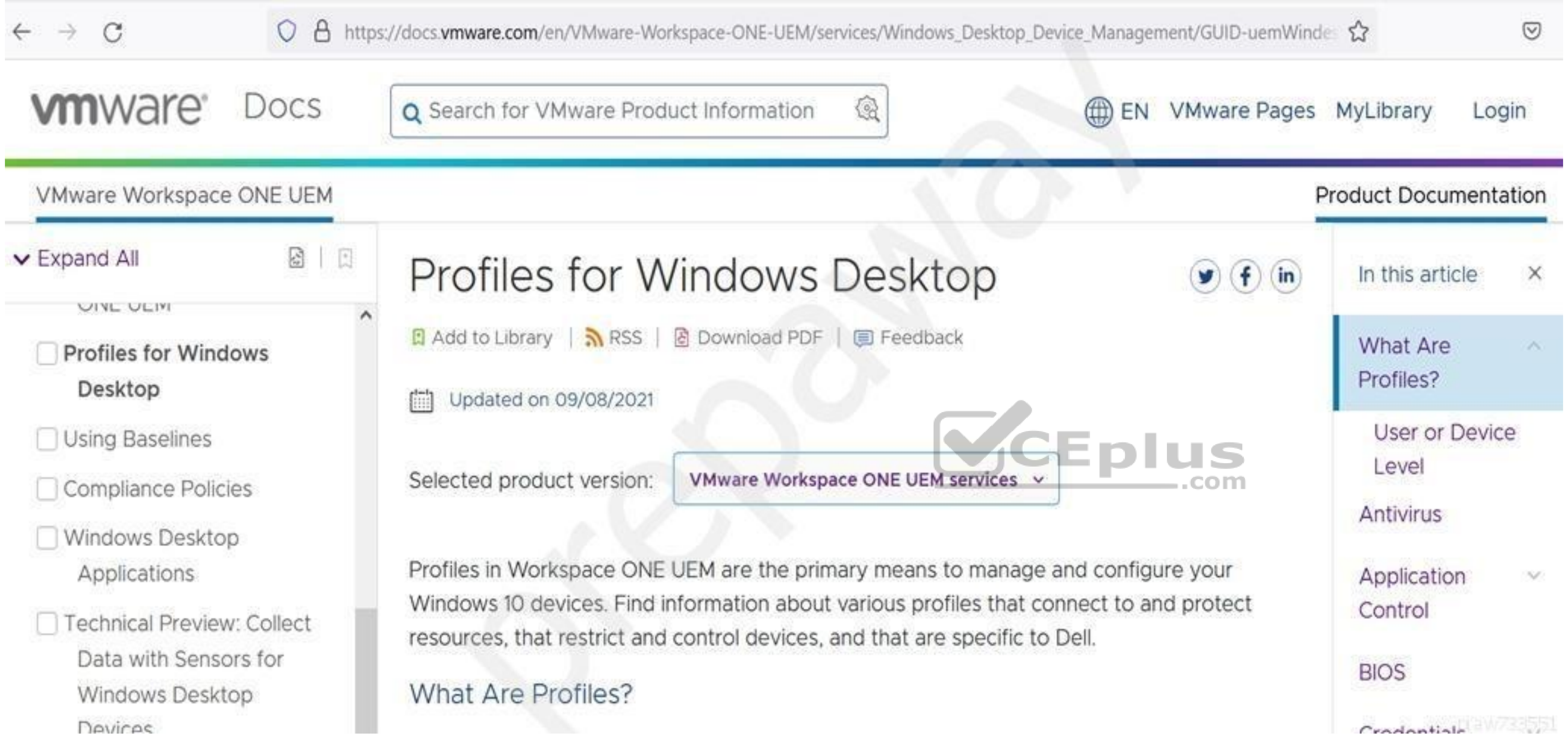
QUESTION 11 Which three Workspace ONE UEM capabilities are used to configure security policies on Windows 10 desktops?
(Choose three.)

A. Application Profiles

B. Custom XML
C. Custom Attributes
D. Baselines
E. Native Profiles

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:


https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Windows_Desktop_Device_Management/GUID-uemWinde
vmware Docs
Search for VMware Product Information
EN
VMware Pages
MyLibrary
Login
VMware Workspace ONE UEM
Product Documentation
Expand All
ONE UEM
Profiles for Windows Desktop
Using Baselines
Compliance Policies
Windows Desktop Applications
Technical Preview: Collect Data with Sensors for Windows Desktop Devices
Add to Library
RSS
Download PDF
Feedback
In this article
What Are Profiles?
User or Device Level
Antivirus
Application Control
BIOS
Credentials

Profiles for Windows Desktop

Updated on 09/08/2021

Selected product version: VMware Workspace ONE UEM services

Profiles in Workspace ONE UEM are the primary means to manage and configure your Windows 10 devices. Find information about various profiles that connect to and protect resources, that restrict and control devices, and that are specific to Dell.

What Are Profiles?

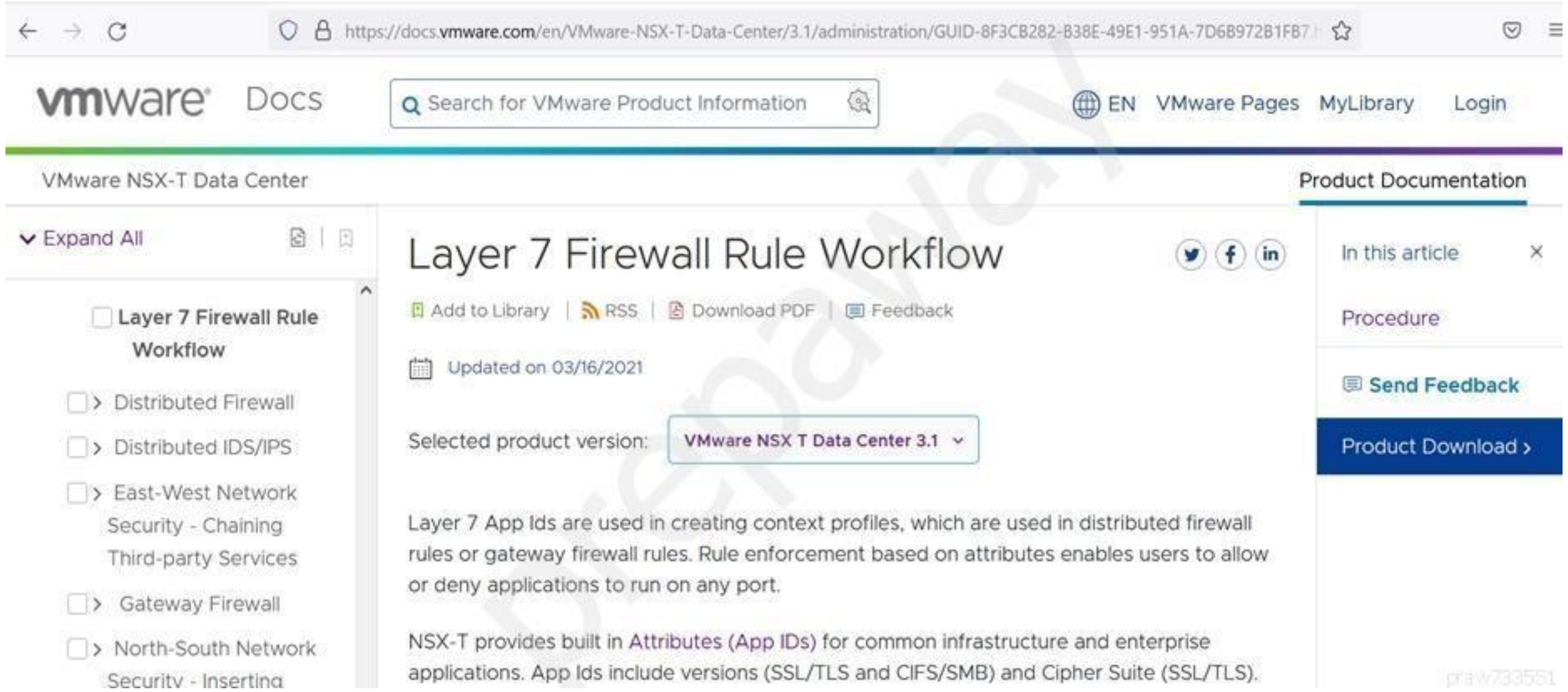
Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Windows_Desktop_Device_Management/GUID-uemWindeskProfiles.html

QUESTION 12 Which would require a Layer 7 Firewall?

A. block a specific port
B. block a subnet range
C. block a host
D. block a specific application

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:



https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/administration/GUID-8F3CB282-B38E-49E1-951A-7D6B972B1FB7.

vmware Docs | Search for VMware Product Information | EN | VMware Pages | MyLibrary | Login

VMware NSX-T Data Center | Product Documentation

Expand All

- Layer 7 Firewall Rule Workflow
- Distributed Firewall
- Distributed IDS/IPS
- East-West Network Security - Chaining Third-party Services
- Gateway Firewall
- North-South Network Security - Inserting

Layer 7 Firewall Rule Workflow

Add to Library | RSS | Download PDF | Feedback

Updated on 03/16/2021

Selected product version: VMware NSX T Data Center 3.1

Layer 7 App Ids are used in creating context profiles, which are used in distributed firewall rules or gateway firewall rules. Rule enforcement based on attributes enables users to allow or deny applications to run on any port.

NSX-T provides built in Attributes (App IDs) for common infrastructure and enterprise applications. App Ids include versions (SSL/TLS and CIFS/SMB) and Cipher Suite (SSL/TLS).

In this article | Procedure | Send Feedback | Product Download ›

Reference: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/administration/GUID-8F3CB282-B38E-49E1-951A-7D6B972B1FB7.html

QUESTION 13 VMware's Intrinsic Security layer includes functionality for which control points?

A. networks, workloads, endpoints, identity, and clouds
B. applications, workloads, devices, identity, virtual infrastructure
C. networks, containers, devices, users, and VMware Cloud
D. applications, users, networks, data center perimeter, vSphere

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.globalknowledge.com/en-gb/resources/articles/what-is-intrinsic-security

QUESTION 14 Which three are key features of VMware Carbon Black Cloud Enterprise EDR? (Choose three.)

A. self-service security remediation
B. continuous and centralized recording
C. attack chain visualization and searchD. live response for remote remediation
E. frequent Antivirus pattern updates

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-enterprise-edr-datasheet.pdf (2)

QUESTION 15 What are three core characteristics of VMware's Intrinsic Security solution? (Choose three.)

A. integrated
B. extensible
C. unified
D. content-centric
E. centrally managed
F. built-in

Correct Answer: ACF
Section: (none)
Explanation

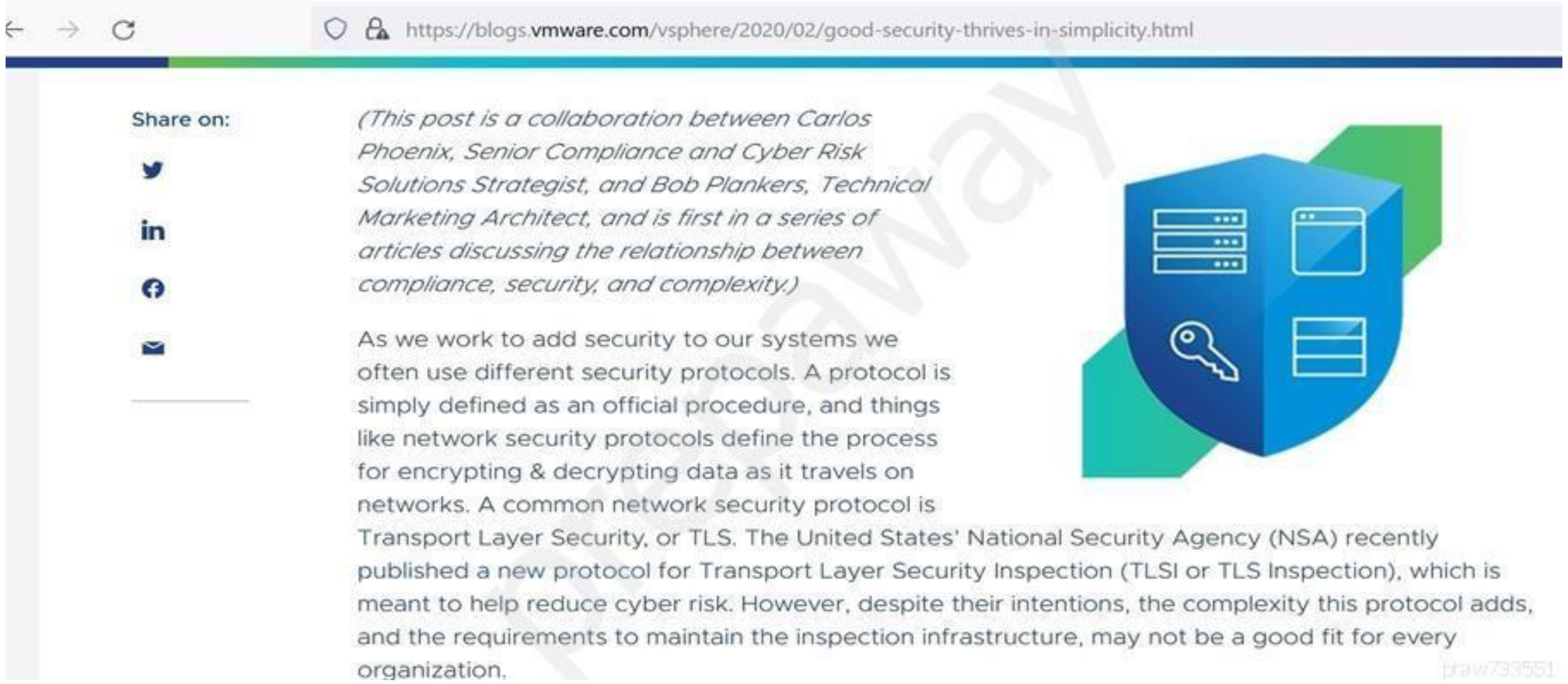
Explanation/Reference:

QUESTION 16 What is the safe course of action for a USB disk of unknown ownership and origin?

A. Do not connect the USB to any computer as it may be a USB Killer device
B. Connect the USB device to your computer and allow the DLP software to protect it
C. Connect the USB to a non-Windows device and examine it
D. Connect the USB to an air gapped system and examine it

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:



https://blogs.vmware.com/vsphere/2020/02/good-security-thrives-in-simplicity.html

(This post is a collaboration between Carlos Phoenix, Senior Compliance and Cyber Risk Solutions Strategist, and Bob Plankers, Technical Marketing Architect, and is first in a series of articles discussing the relationship between compliance, security, and complexity.)

As we work to add security to our systems we often use different security protocols. A protocol is simply defined as an official procedure, and things like network security protocols define the process for encrypting & decrypting data as it travels on networks. A common network security protocol is Transport Layer Security, or TLS. The United States' National Security Agency (NSA) recently published a new protocol for Transport Layer Security Inspection (TLSI or TLS Inspection), which is meant to help reduce cyber risk. However, despite their intentions, the complexity this protocol adds, and the requirements to maintain the inspection infrastructure, may not be a good fit for every organization.

Reference: https://blogs.vmware.com/vsphere/2020/02/good-security-thrives-in-simplicity.html **QUESTION 17** When using VMware Carbon Black Live Response, what command will show all active processes?

A. `dir`
B. `list`
C. `ls`
D. `ps`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18 What types of hosts are supported for hosting both NSX-T Data Center managers and host transport nodes?

A. vSphere ESXi 6.7U1 or higher, KVM on CentOS Linux
B. vSphere ESXi 6.7U1 or higher, KVM on RHEL 7.6, Ubuntu 18.04.2 LTS
C. vSphere ESXi 6.5, KVM on RHEL 7.6, Ubuntu 18.04.2 LTS
D. vSphere ESXi 6.7U1 or higher, CentOS KVM 7.6, RHEL KVM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19 When considering the Device Details page in Workspace ONE UEM, what three sub menus can you check for changes in compliance? (Choose three.)

A. Profiles
B. Troubleshooting
C. Updates
D. Status History
E. Compliance

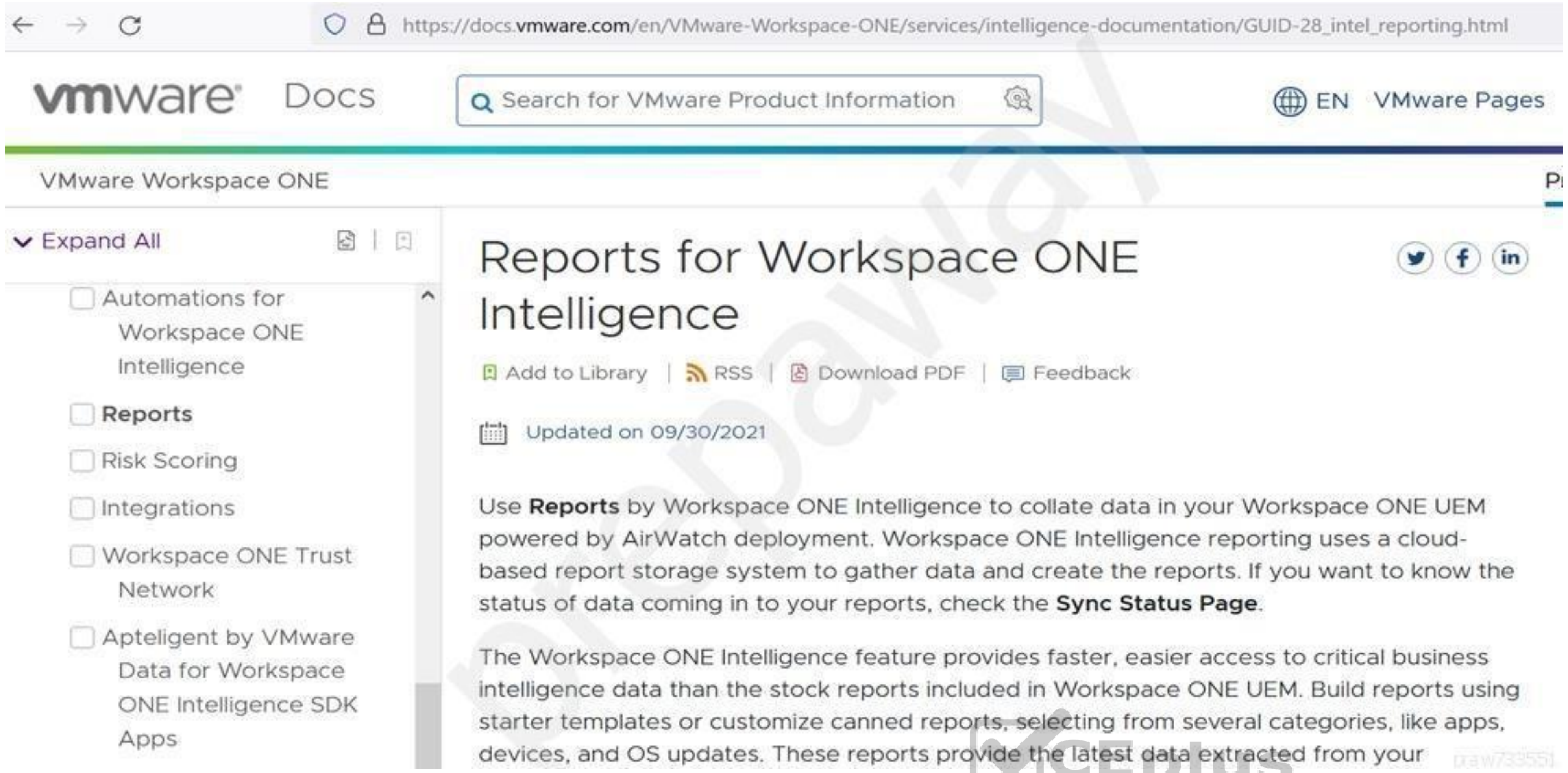
Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/WS1_UEM_Managing_Devices.pdf

QUESTION 20 When you share a report in Workspace One Intelligence with a specified user, how is the report shared?

A. Desktop Notification
B. Console Message
C. SMS
D. Email

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Explanation:


https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligence-documentation/GUID-28_intel_reporting.html
vmware Docs
Search for VMware Product Information
EN VMware Pages
VMware Workspace ONE
Expand All
Automations for Workspace ONE Intelligence
Reports
Risk Scoring
Integrations
Workspace ONE Trust Network
Apteligent by VMware Data for Workspace ONE Intelligence SDK Apps
Add to Library | RSS | Download PDF | Feedback

Reports for Workspace ONE Intelligence

Updated on 09/30/2021

Use **Reports** by Workspace ONE Intelligence to collate data in your Workspace ONE UEM powered by AirWatch deployment. Workspace ONE Intelligence reporting uses a cloud-based report storage system to gather data and create the reports. If you want to know the status of data coming in to your reports, check the **Sync Status Page**.

The Workspace ONE Intelligence feature provides faster, easier access to critical business intelligence data than the stock reports included in Workspace ONE UEM. Build reports using starter templates or customize canned reports, selecting from several categories, like apps, devices, and OS updates. These reports provide the latest data extracted from your

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligence-documentation/GUID-28_intel_reporting.html

QUESTION 21 What are the four valid options for a Windows compliance rule based on firewall status in a Workspace ONE environment? (Choose four.)

A. Good
B. Snoozed
C. Not Monitored
D. Deferred
E. Bad
F. Poor

Correct Answer: ACDE
Section: (none)
Explanation

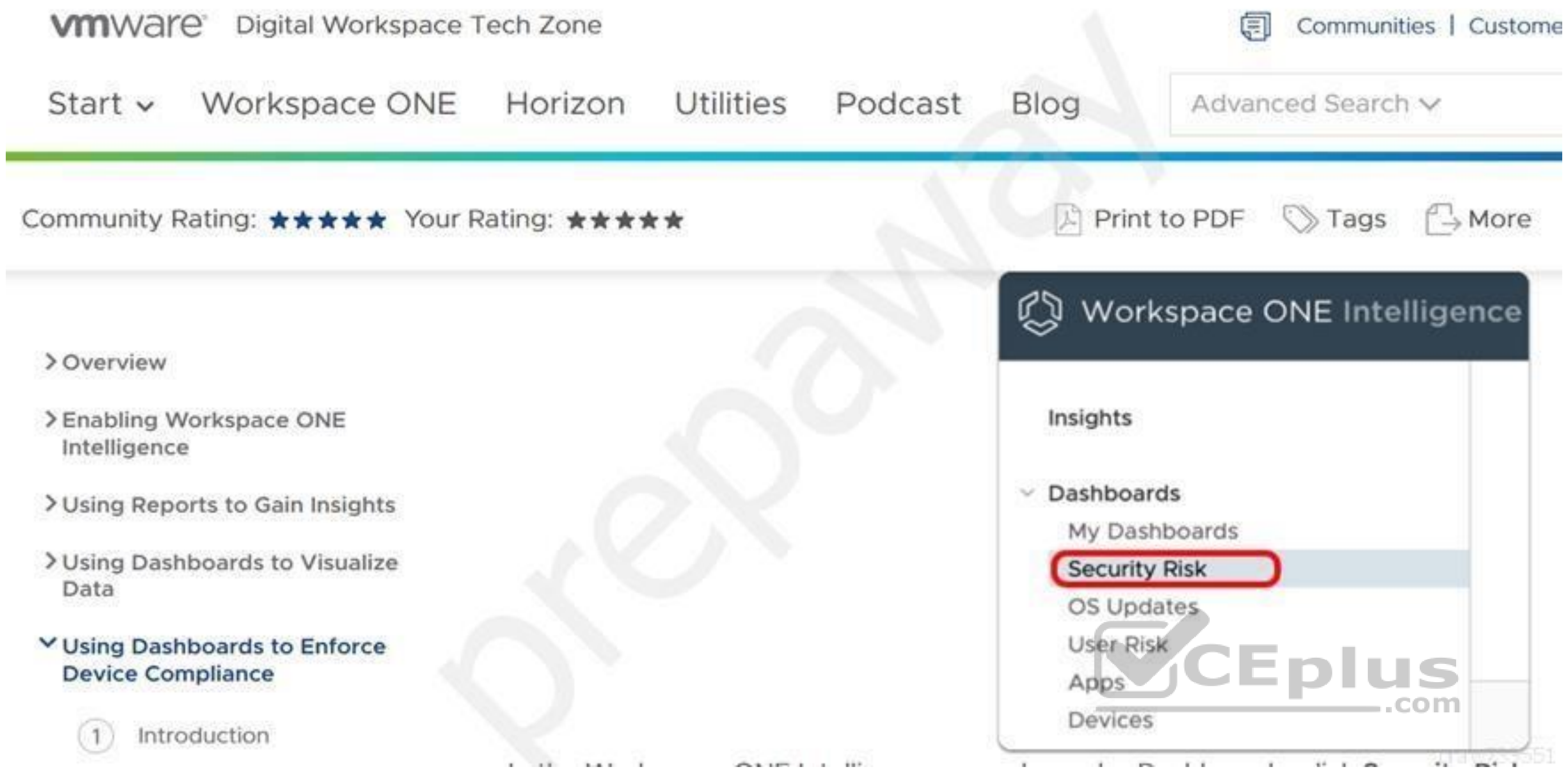
Explanation/Reference:

QUESTION 22 In Workspace ONE Intelligence, which two are default components of the security risk dashboard? (Choose two.)

A. Compromised Devices
B. Threats Summary
C. Web Apps
D. Desktop Apps
E. OS Updates

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:


vmware Digital Workspace Tech Zone
Communities | Custome
Start
Workspace ONE
Horizon
Utilities
Podcast
Blog
Advanced Search
Community Rating: ★★★★★ Your Rating: ★★★★★
Print to PDF
Tags
More
Overview
Enabling Workspace ONE Intelligence
Using Reports to Gain Insights
Using Dashboards to Visualize Data
Using Dashboards to Enforce Device Compliance
1 Introduction
Workspace ONE Intelligence
Insights
Dashboards
My Dashboards
Security Risk
OS Updates
User Risk
Apps
Devices

Reference: https://techzone.vmware.com/getting-started-workspace-one-intelligence-reports-and-dashboards-workspace-one-operational#_1066726

QUESTION 23 Micro segmentation is under which pillar of trust in VMware's 5 pillars of Zero Trust?

A. User
B. Session/Transport
C. Application
D. Device

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://events.afcea.org/Augusta20/CUSTOM/pdf/Dell%20Technologies%20-%20ZeroTrust.pdf

QUESTION 24
Which two choices are advantages for using baselines in Workspace ONE UEM? (Choose two.)
A. ability to apply a network security standard to a device
B. ability to use industry standard settings to a device
C. ability to apply drive updates to a device
D. ability to apply Windows Update patches to a device
E. ability to audit network security compliance to a device

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25 Which parameter ensures an endpoint will stay connected with the designated VMware Carbon Black Cloud tenant?

A. Company Code
B. Organization Group ID
C. Device Serial Number
D. User ID

Correct Answer: D
Section: (none)
Explanation

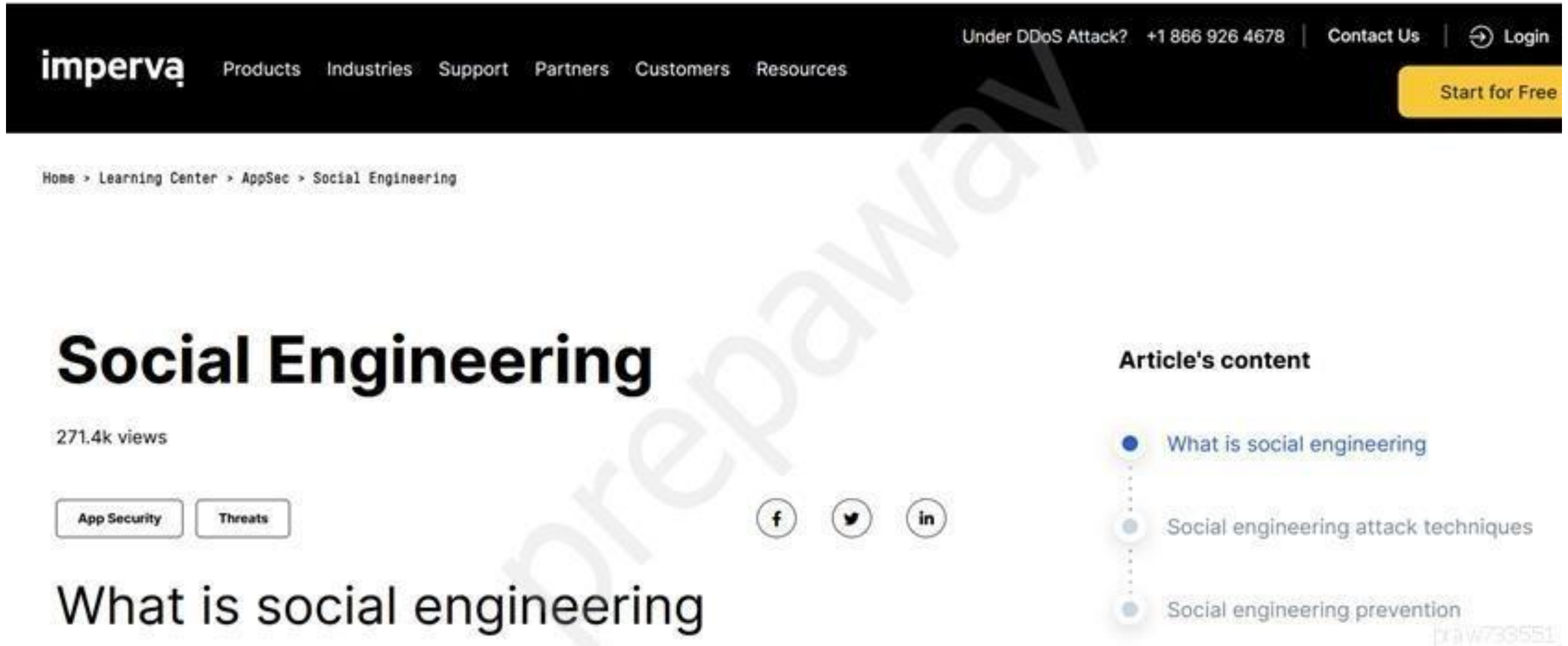
Explanation/Reference:

QUESTION 26 What is the term used to describe a type of social engineering attack aimed at a specific person or specific type of person?

A. Phishing
B. Whaling
C. Tailgating
D. Spear Phishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:



Social Engineering

271.4k views

What is social engineering

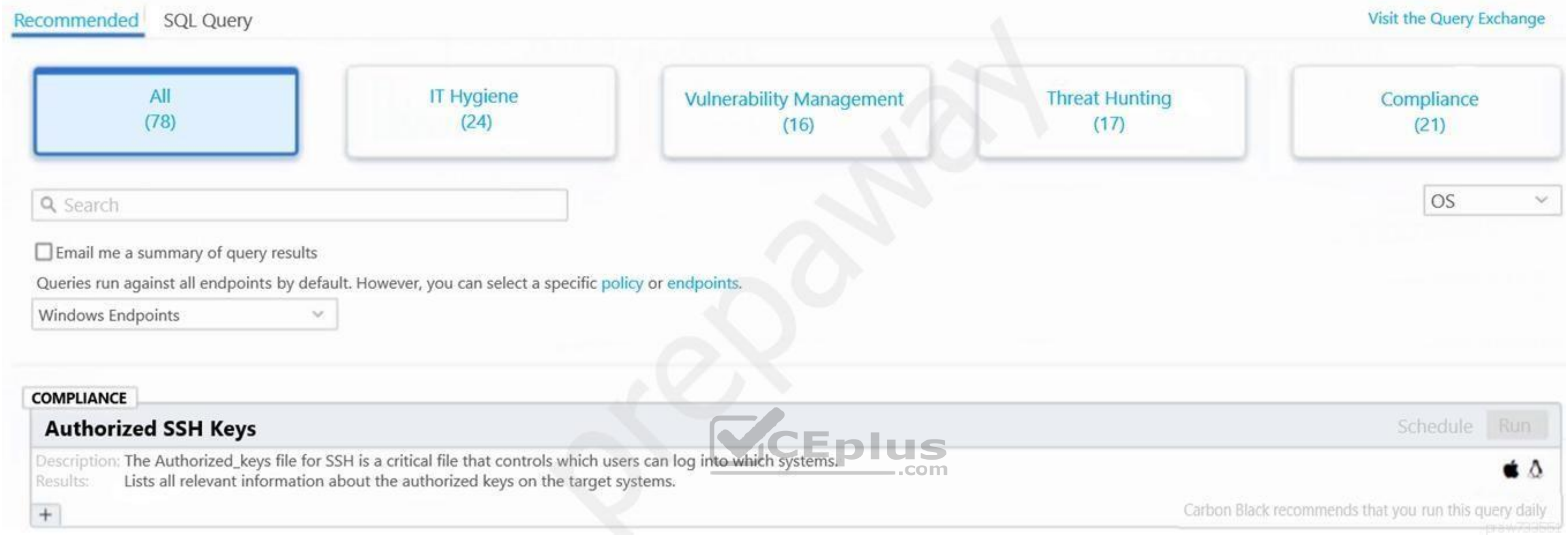
Article's content

- What is social engineering
- Social engineering attack techniques
- Social engineering prevention

Reference: https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Phishing,curiosity%20or%20fear%20in%20victims

QUESTION 27 Refer to the exhibit.

When attempting to run the recommended query for all Authorized SSH Keys in an organization, you see this view in the console.



☐ Email me a summary of query results

Queries run against all endpoints by default. However, you can select a specific policy or endpoints.

Windows Endpoints

Authorized SSH Keys

Description: The Authorized_keys file for SSH is a critical file that controls which users can log into which systems.

Results: Lists all relevant information about the authorized keys on the target systems.

Carbon Black recommends that you run this query daily

Why are you not able to run the query?

A. You must schedule the query first, before you can run the query
B. The policy Windows Endpoints have no devices
C. You need the ‘Use Recommended Query’ permission set in your role
D. There are no Mac or Linux sensors in the selected policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

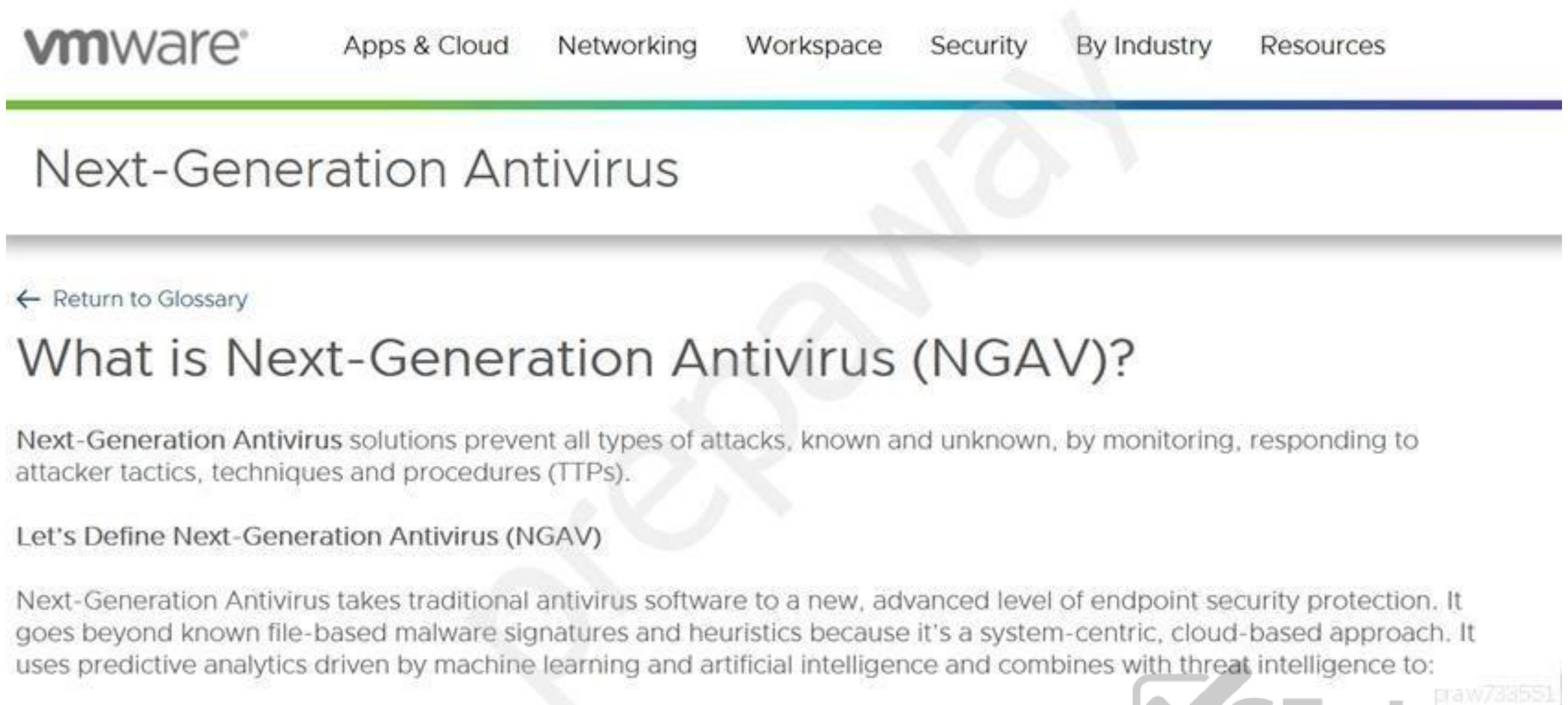
QUESTION 28 What is a unique benefit of Next Generation Antivirus over standard Antivirus?

A. signature based heuristics
B. predictive analytics
C. file based heuristics
D. reactive analytics

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:



Next-Generation Antivirus

What is Next-Generation Antivirus (NGAV)?

Next-Generation Antivirus solutions prevent all types of attacks, known and unknown, by monitoring, responding to attacker tactics, techniques and procedures (TTPs).

Let's Define Next-Generation Antivirus (NGAV)

Next-Generation Antivirus takes traditional antivirus software to a new, advanced level of endpoint security protection. It goes beyond known file-based malware signatures and heuristics because it's a system-centric, cloud-based approach. It uses predictive analytics driven by machine learning and artificial intelligence and combines with threat intelligence to:

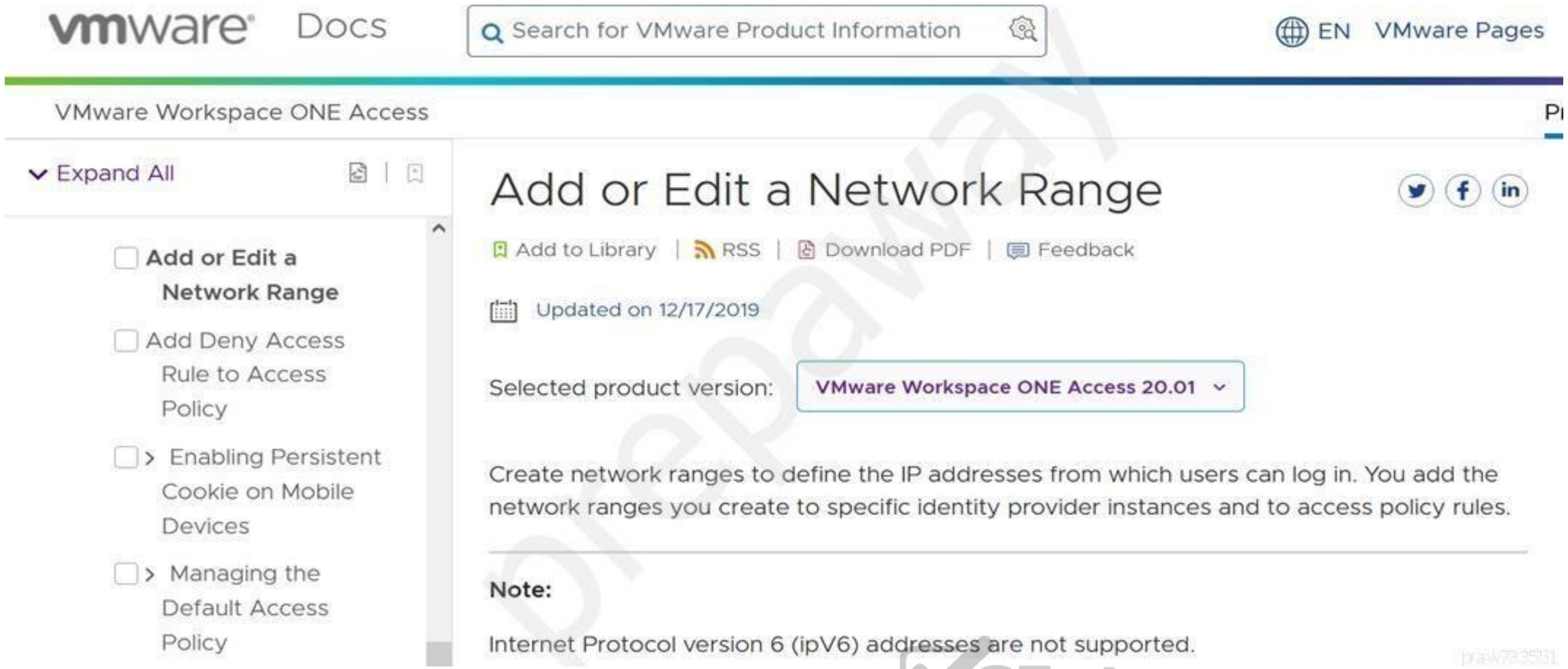
Reference: https://www.vmware.com/topics/glossary/content/next-generation-antivirus-ngav

QUESTION 29
What is the default user's network range when creating a new access policy rule in Workspace ONE Access?

A. 10.0.0.0/8
B. ALL RANGES
C. 192.168.0.0/16
D. LOCAL SUBNET

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:


vmware Docs
Search for VMware Product Information
EN VMware Pages
VMware Workspace ONE Access
Expand All
Add or Edit a Network Range
Add Deny Access Rule to Access Policy
Enabling Persistent Cookie on Mobile Devices
Managing the Default Access Policy
Add to Library | RSS | Download PDF | Feedback

Add or Edit a Network Range

Updated on 12/17/2019

Selected product version: VMware Workspace ONE Access 20.01

Create network ranges to define the IP addresses from which users can log in. You add the network ranges you create to specific identity provider instances and to access policy rules.

Note:

Internet Protocol version 6 (ipV6) addresses are not supported.

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-Access/20.01/ws1_access_authentication/GUID-3D7AB065-E2ED-4525-B575-2A576BAA3CC3.html

QUESTION 30 In VMware Carbon Black Cloud Endpoint Standard, which items are available in the Event view?

A. Hashes, Reputations
B. Emails, Policies, OS, Locations
C. Connection, IP/Port
D. IDs, Indicators/TTPs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 31 Which option would be considered an example of a Hardware Based Exploit?

A. SQL Injection
B. Social Engineering
C. Jail Breaking
D. Denial of Service

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: https://www.kaspersky.com/resource-center/definitions/what-is-jailbreaking

QUESTION 32 Network Security teams can leverage Micro-Segmentation for which purpose?

A. deny attackers the possibility to breach the data center perimeter
B. deny attackers the opportunity to move laterally within the internal network
C. replace the need to leverage traditional network segmentation
D. prevent a successful attack to any of the systems attached to the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33 Which three common mitigations for social engineering attacks? (Choose three.)

A. user training
B. filtering Email attachments
C. update Antivirus software
D. remove applications
E. blocking execution of suspicious files

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34 In Workspace ONE Intelligence, which of the following is a role that can be assigned to an administrator account?

A. Super User
B. Helpdesk
C. Read-only
D. Automater

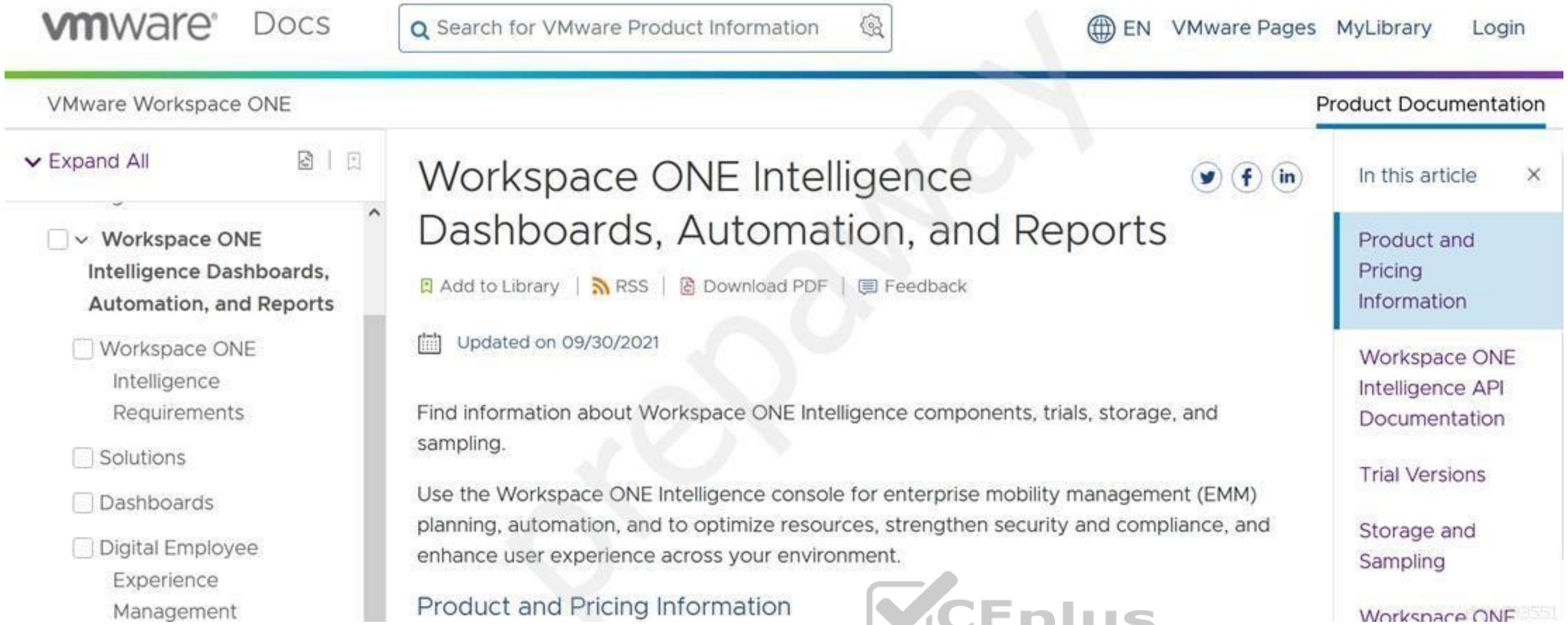
Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 35
In Workspace ONE UEM, from which menu would you access Workspace ONE Intelligence?

A. Apps & Books
B. General Settings
C. Device
D. Monitor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:



vmware Docs
Search for VMware Product Information
EN VMware Pages MyLibrary Login
VMware Workspace ONE
Product Documentation
Expand All
Workspace ONE Intelligence Dashboards, Automation, and Reports
Workspace ONE Intelligence Requirements
Solutions
Dashboards
Digital Employee Experience Management
Add to Library | RSS | Download PDF | Feedback
In this article
Product and Pricing Information
Workspace ONE Intelligence API Documentation
Trial Versions
Storage and Sampling
Workspace ONE

Workspace ONE Intelligence Dashboards, Automation, and Reports

Updated on 09/30/2021

Find information about Workspace ONE Intelligence components, trials, storage, and sampling.

Use the Workspace ONE Intelligence console for enterprise mobility management (EMM) planning, automation, and to optimize resources, strengthen security and compliance, and enhance user experience across your environment.

Product and Pricing Information

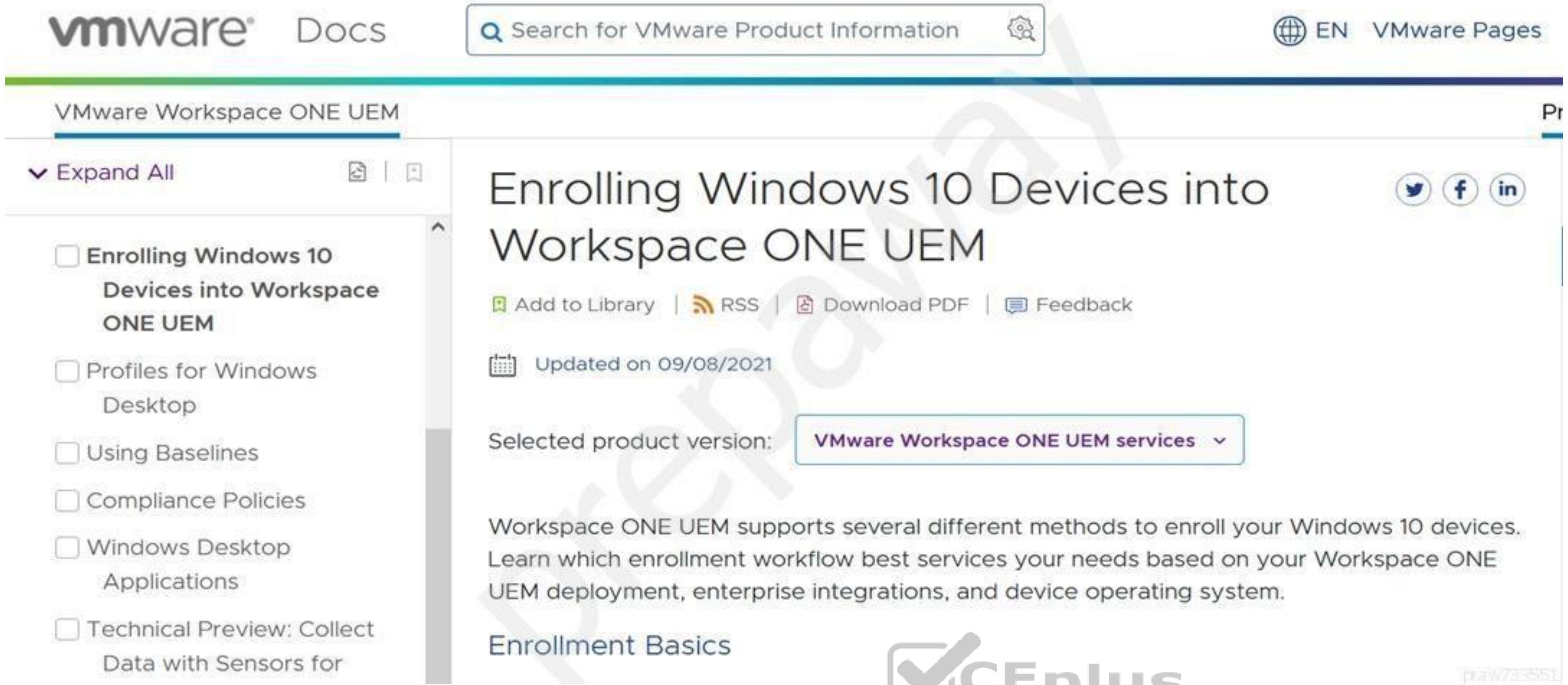
Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligence-documentation/GUID-01_intel_intro.html#:~:text=Access%20Workspace%20ONE%20Intelligence&text=Access%20the%20reports%20by%20navigating,console%2C%20follow%20the%20required%20steps

QUESTION 36 Which VMware application enrolls an endpoint into Workspace ONE?

A. Workspace ONE Web
B. CB Defense Sensor
C. VMware Horizon Client
D. Workspace ONE Intelligent Hub

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:



□ Enrolling Windows 10 Devices into Workspace ONE UEM
□ Profiles for Windows Desktop
□ Using Baselines
□ Compliance Policies
□ Windows Desktop Applications
□ Technical Preview: Collect Data with Sensors for

Enrolling Windows 10 Devices into Workspace ONE UEM

Add to Library | RSS | Download PDF | Feedback

Updated on 09/08/2021

Selected product version: VMware Workspace ONE UEM services

Workspace ONE UEM supports several different methods to enroll your Windows 10 devices. Learn which enrollment workflow best services your needs based on your Workspace ONE UEM deployment, enterprise integrations, and device operating system.

Enrollment Basics

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Windows_Desktop_Device_Management/GUID-uemWindeskDeviceEnrollment.html

QUESTION 37 Least Privilege is a common method for minimizing the risk of what kind of threat?

A. Insider Threats
B. Spear Phishing
C. Distributed Denial of Service
D. Man in the Middle

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.beyondtrust.com/blog/entry/what-is-least-privilege

QUESTION 38 Which VMware Carbon Black Cloud function allows an administrator to remotely run commands on protected endpoints?

A. Live Query
B. Alert Triage
C. Investigate
D. Live Response

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide.pdf (26)

QUESTION 39
Which NSX functionality allows technology partners to integrate third-party solutions to examine North-South and East-West network traffic?

A. Guest Introspection
B. Network Introspection
C. Gateway Firewall
D. Distributed Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
An organization using VMware Carbon Black makes use of an unsigned third party application that is critical to business function. Unfortunately, the application has a reputation of Potentially Unwanted Program and is prevented from running based on the policy.

What Approved list mechanism will allow this application to run in your environment while maintaining the most secure posture?

A. MD5 Hash based
B. Certs based
C. IT Tools based
D. SHA-256 Hash based

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.carbonblack.com/gbouw27325/attachments/gbouw27325/product-docs-news/3221/1/VMware%20Carbon%20Black%20App%20Control%20User%20Guide%20v8.6.pdf

QUESTION 41 Which three are components of the NSX-T Software-defined Firewall? (Choose three.)

A. NSX Distributed IDS
B. NSX Identity Firewall
C. NSX Edge Firewall
D. NSX Intelligence
E. NSX Distributed Firewall
F. NSX Identity Manager

Correct Answer: ADE
Section: (none)
Explanation

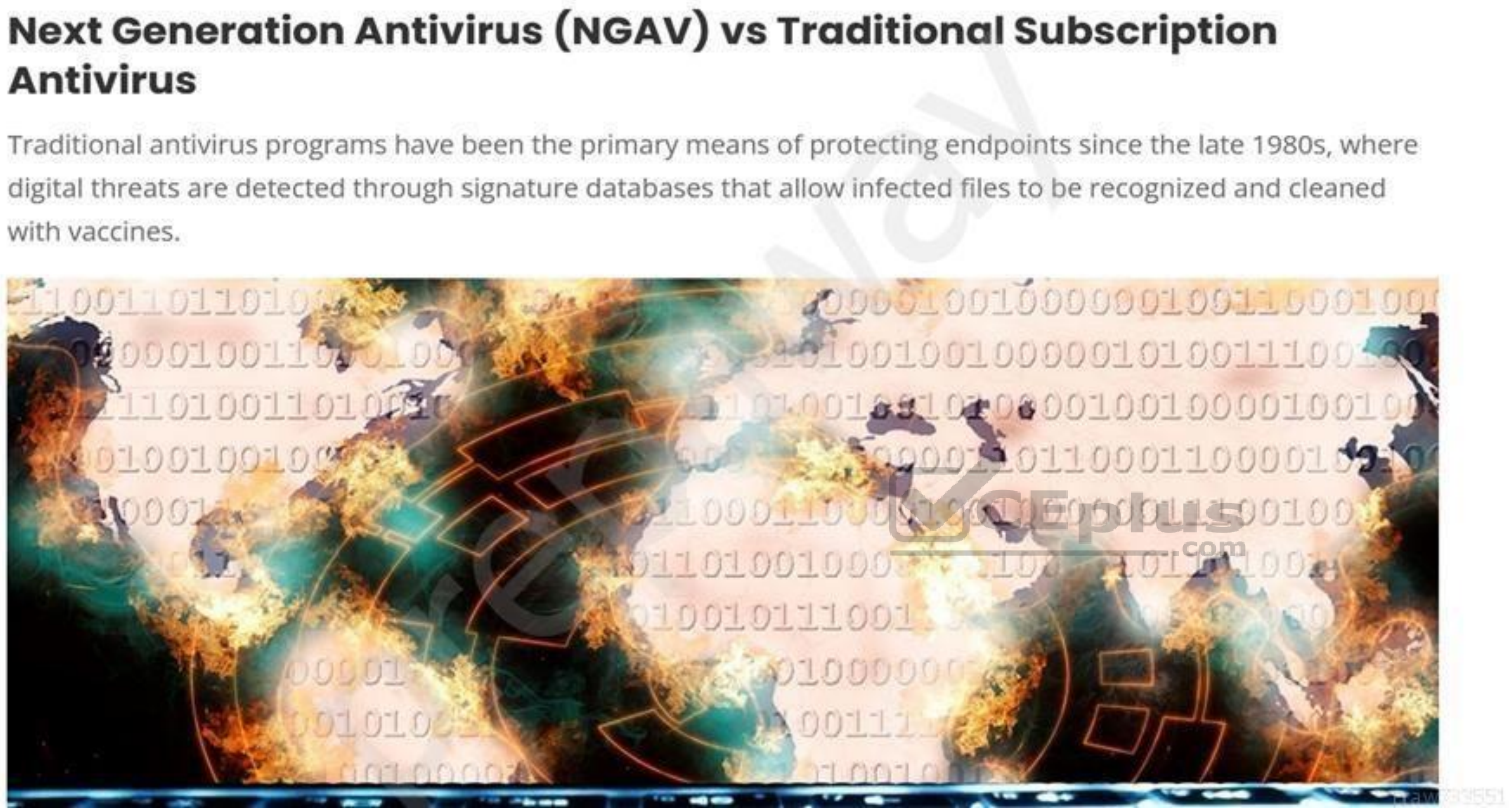
Explanation/Reference:
Reference: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-datasheet.pdf

QUESTION 42 What is one of the limitations of traditional Antivirus when compared to Next Generation Antivirus?

A. Traditional AV does not need a client installed on the machines to function
B. Traditional AV focuses on signature or definition based threats
C. Traditional AV requires integration with a SIEM to use the next generation features
D. Traditional AV does not provide a dashboard

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:



Next Generation Antivirus (NGAV) vs Traditional Subscription Antivirus

Traditional antivirus programs have been the primary means of protecting endpoints since the late 1980s, where digital threats are detected through signature databases that allow infected files to be recognized and cleaned with vaccines.

Reference: https://cipher.com/blog/next-generation-antivirus-ngav-vs-traditional-subscription-antivirus/

QUESTION 43 In VMware Carbon Black Cloud, which reputations have the highest priority during analysis?

A. Known Priority
B. Trusted Allow List
C. Company Allow List
D. Ignore

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 44 If the Compromised Protection switch is enabled in Workspace ONE UEM, what is the expected behavior on compromised devices in the environment?

A. A tag is assigned to the compromised devices and the admin gets notification
B. Compromised devices are automatically Enterprise Wiped
C. A block is set for all network connections except to the VMware servers
D. Devices are marked as non-compliant and the admin gets a notification

Correct Answer: D
Section: (none)
Explanation

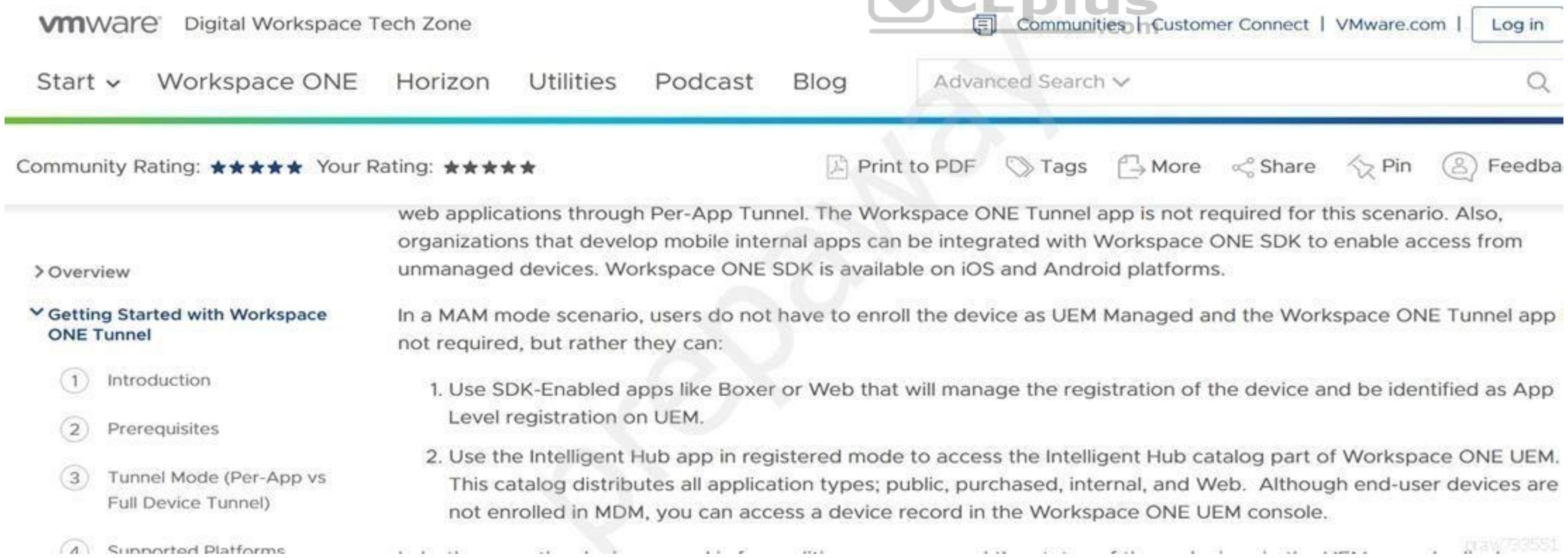
Explanation/Reference:

QUESTION 45 In a Workspace ONE deployment, Per App Tunnel uses the Native Platform API for which platforms?

A. iOS & Android only
B. iOS, Android, MacOS & Windows
C. iOS & MacOS only
D. Android & Windows only

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:


vmware Digital Workspace Tech Zone
Communities | Customer Connect | VMware.com | Log in
Start
Workspace ONE
Horizon
Utilities
Podcast
Blog
Advanced Search
Community Rating: ★★★★★ Your Rating: ★★★★★
Print to PDF
Tags
More
Share
Pin
Feedba
> Overview
Getting Started with Workspace ONE Tunnel
1 Introduction
2 Prerequisites
3 Tunnel Mode (Per-App vs Full Device Tunnel)
4 Supported Platforms

web applications through Per-App Tunnel. The Workspace ONE Tunnel app is not required for this scenario. Also, organizations that develop mobile internal apps can be integrated with Workspace ONE SDK to enable access from unmanaged devices. Workspace ONE SDK is available on iOS and Android platforms.

In a MAM mode scenario, users do not have to enroll the device as UEM Managed and the Workspace ONE Tunnel app not required, but rather they can:

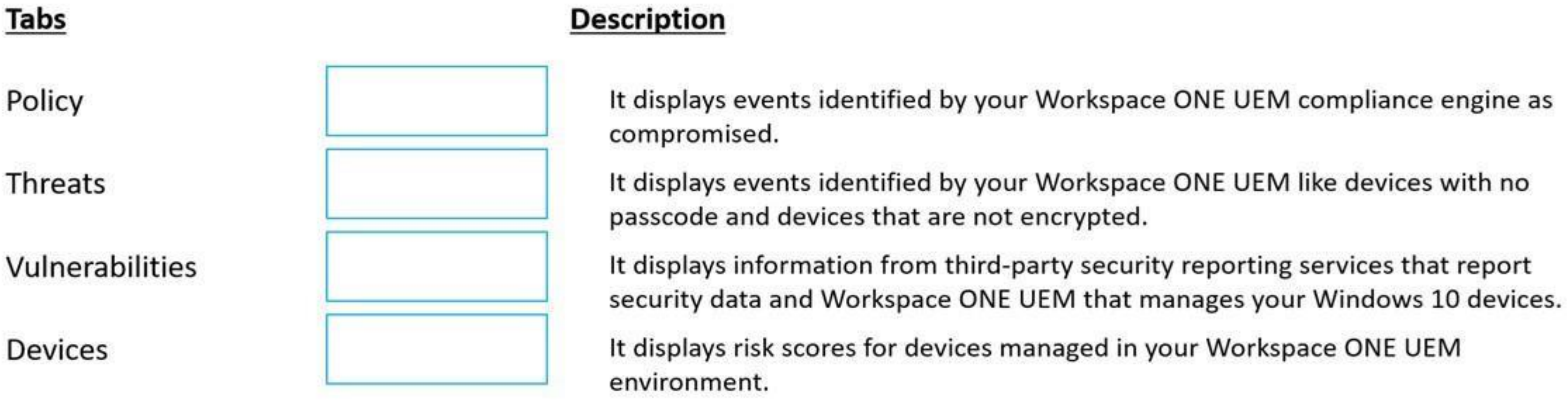
1. Use SDK-Enabled apps like Boxer or Web that will manage the registration of the device and be identified as App Level registration on UEM.
2. Use the Intelligent Hub app in registered mode to access the Intelligent Hub catalog part of Workspace ONE UEM. This catalog distributes all application types; public, purchased, internal, and Web. Although end-user devices are not enrolled in MDM, you can access a device record in the Workspace ONE UEM console.

Reference: https://techzone.vmware.com/deploying-vmware-workspace-one-tunnel-workspace-one-operational-tutorial#_1223703

QUESTION 46
DRAG DROP

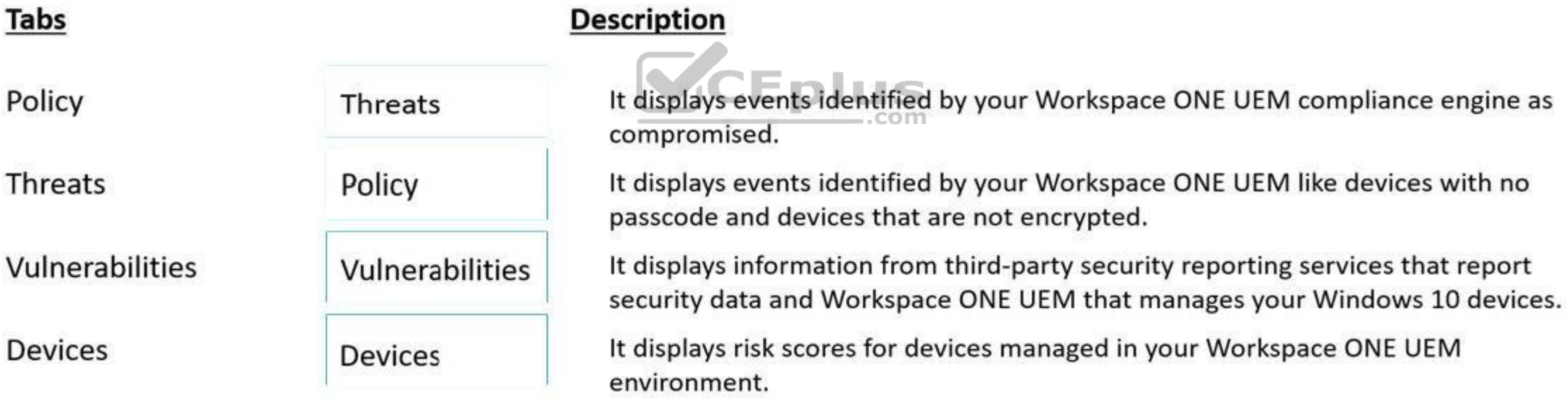
Match each Workspace ONE Intelligence Security Risk Module tab on the left with its description on the right by dragging the tab's name into the correct box.

Select and Place:



Tabs		Description
Policy		It displays events identified by your Workspace ONE UEM compliance engine as compromised.
Threats		It displays events identified by your Workspace ONE UEM like devices with no passcode and devices that are not encrypted.
Vulnerabilities		It displays information from third-party security reporting services that report security data and Workspace ONE UEM that manages your Windows 10 devices.
Devices		It displays risk scores for devices managed in your Workspace ONE UEM environment.

Correct Answer:



Tabs		Description
Policy	Threats	It displays events identified by your Workspace ONE UEM compliance engine as compromised.
Threats	Policy	It displays events identified by your Workspace ONE UEM like devices with no passcode and devices that are not encrypted.
Vulnerabilities	Vulnerabilities	It displays information from third-party security reporting services that report security data and Workspace ONE UEM that manages your Windows 10 devices.
Devices	Devices	It displays risk scores for devices managed in your Workspace ONE UEM environment.

Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
In VMware Carbon Black Cloud, what is the search field you would use when searching for a command line?

A. `command_line:`
B. `full_cmdline:`
C. `process_cmdline:`
D. `process_commandline:`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide.pdf (29)

QUESTION 48 Which attack technique probes the environment for openings on devices or the firewall?

A. Port Scan
B. Denial of Service
C. Living off the Land
D. Phishing

Correct Answer: A
Section: (none)
Explanation

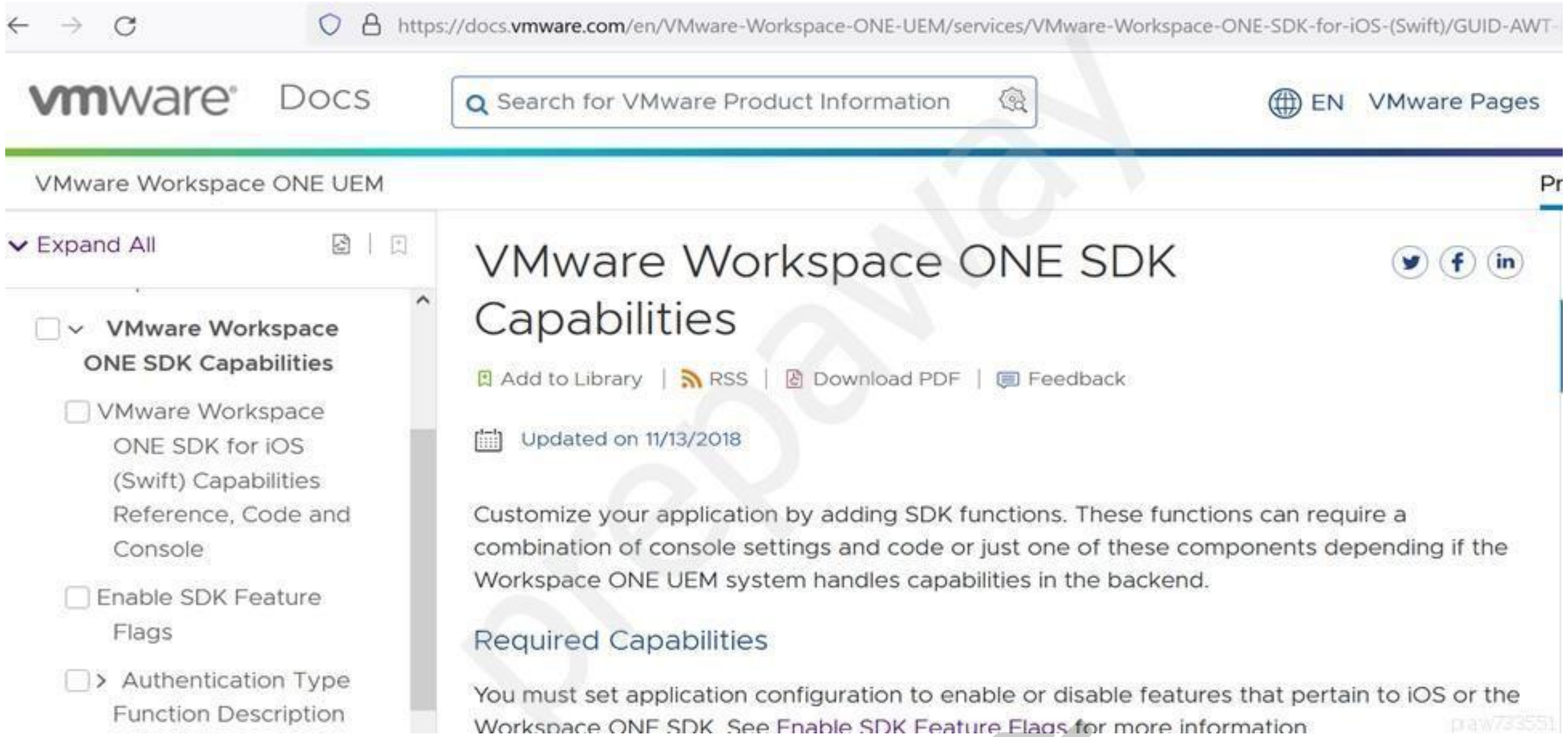
Explanation/Reference:

QUESTION 49 Which three are VMware Workspace ONE SDK capabilities? (Choose three.)

A. data loss prevention
B. find my device
C. single sign-on
D. geofencing
E. application blacklist

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:



https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/VMware-Workspace-ONE-SDK-for-iOS-(Swift)/GUID-AWT-

vmware Docs
Search for VMware Product Information
EN VMware Pages
VMware Workspace ONE UEM
Pr
Expand All
VMware Workspace ONE SDK Capabilities
VMware Workspace ONE SDK for iOS (Swift) Capabilities Reference, Code and Console
Enable SDK Feature Flags
Authentication Type Function Description
Add to Library | RSS | Download PDF | Feedback

VMware Workspace ONE SDK Capabilities

Updated on 11/13/2018

Customize your application by adding SDK functions. These functions can require a combination of console settings and code or just one of these components depending if the Workspace ONE UEM system handles capabilities in the backend.

Required Capabilities

You must set application configuration to enable or disable features that pertain to iOS or the Workspace ONE SDK. See Enable SDK Feature Flags for more information.

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/VMware-Workspace-ONE-SDK-for-iOS-(Swift)/GUID-AWT-KS-SDK-IOSSWIFT-CAPABILITIES.html

QUESTION 50
In VMware Carbon Black Cloud, which two of these statements are true of the Permissions section of the Prevention tab under Policies? (Choose two.)

A. assigns access rights to specific applications
B. deny or close Applications or Actions
C. take precedence over blocking and isolation
D. allows specific operations or applications
E. assigns access rights to specific individuals

Correct Answer: AD
Section: (none)
Explanation

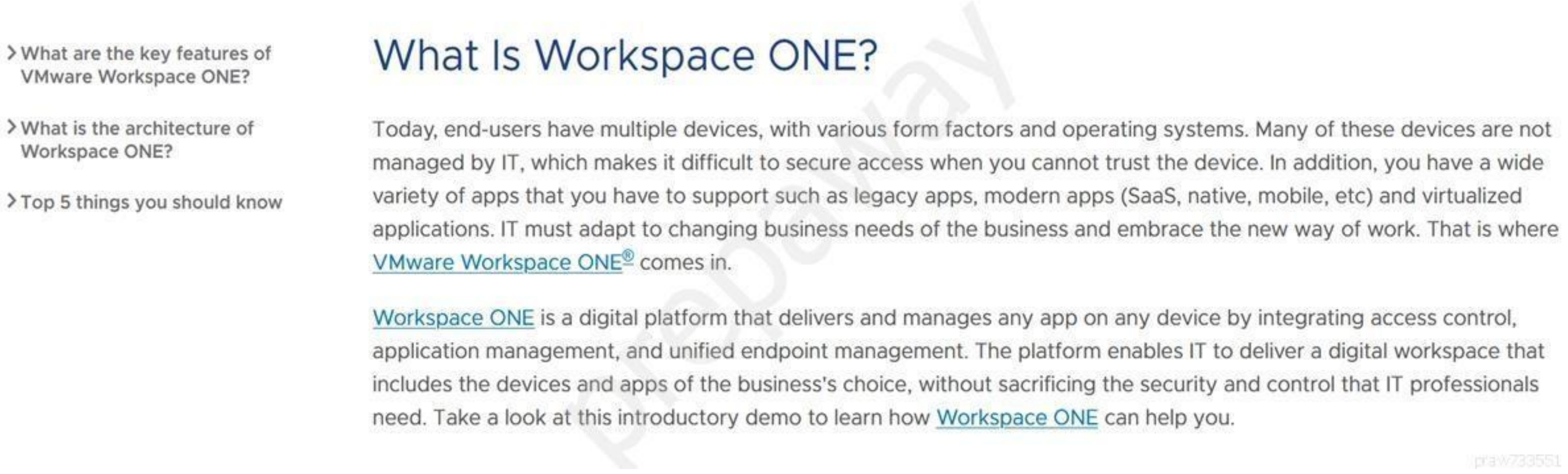
Explanation/Reference:

QUESTION 51
Which Workspace ONE feature incorporates network range, device platform, and authentication method into decision making when evaluating an access request from a user?

A. Sensors
B. Compliance Policies
C. Access Policies
D. Restriction Profiles

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:



- What are the key features of VMware Workspace ONE?
- What is the architecture of Workspace ONE?
- Top 5 things you should know

What Is Workspace ONE?

Today, end-users have multiple devices, with various form factors and operating systems. Many of these devices are not managed by IT, which makes it difficult to secure access when you cannot trust the device. In addition, you have a wide variety of apps that you have to support such as legacy apps, modern apps (SaaS, native, mobile, etc) and virtualized applications. IT must adapt to changing business needs of the business and embrace the new way of work. That is where VMware Workspace ONE® comes in.

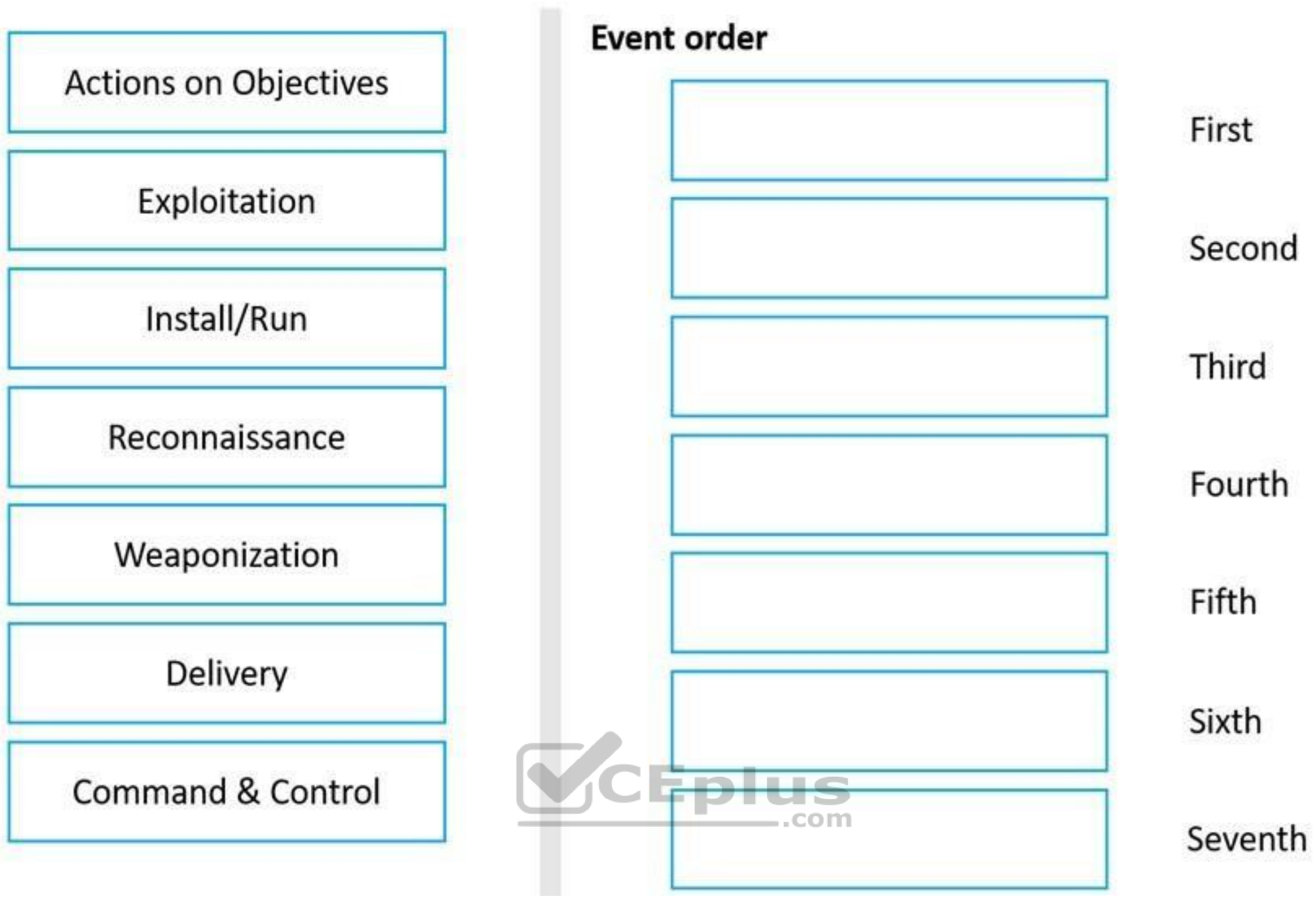
Workspace ONE is a digital platform that delivers and manages any app on any device by integrating access control, application management, and unified endpoint management. The platform enables IT to deliver a digital workspace that includes the devices and apps of the business's choice, without sacrificing the security and control that IT professionals need. Take a look at this introductory demo to learn how Workspace ONE can help you.

Reference: https://techzone.vmware.com/resource/what-workspace-one

QUESTION 52
DRAG DROP

Drag and drop the Cyber Kill events on the left into their proper sequential order on the right.

Select and Place:



Actions on Objectives

Exploitation

Install/Run

Reconnaissance

Weaponization

Delivery

Command & Control

Event order

First

Second

Third

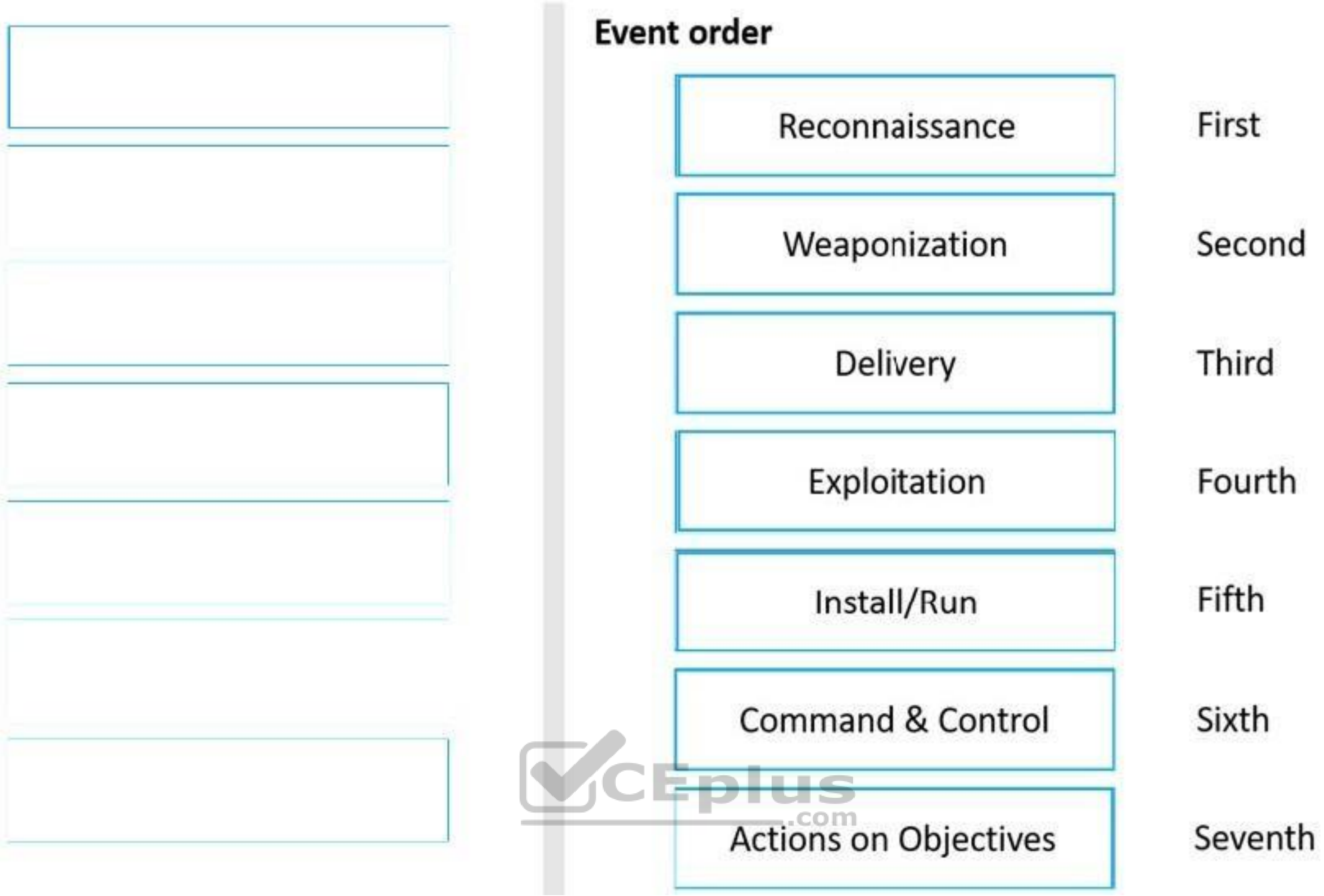
Fourth

Fifth

Sixth

Seventh

Correct Answer:



Event order

Reconnaissance	First
Weaponization	Second
Delivery	Third
Exploitation	Fourth
Install/Run	Fifth
Command & Control	Sixth
Actions on Objectives	Seventh

Section: (none)
Explanation

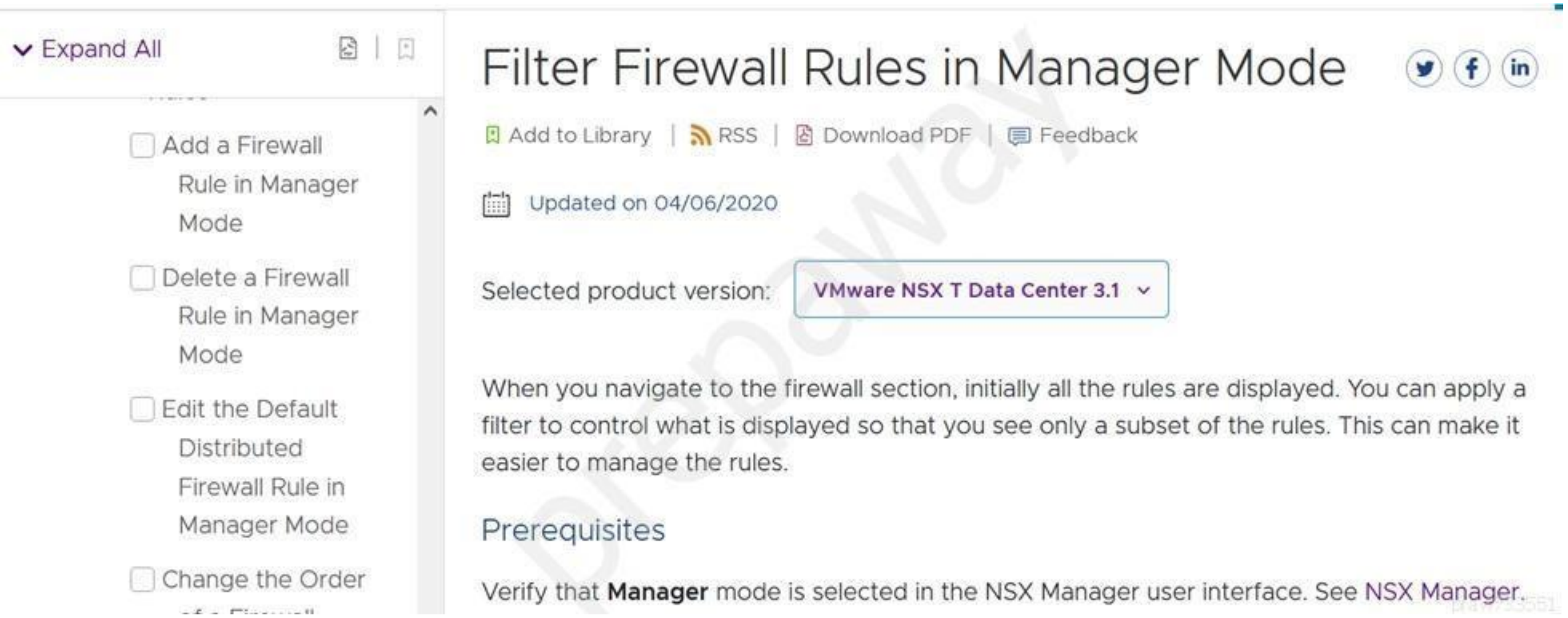
Explanation/Reference:

QUESTION 53 When filtering firewall rules after selecting an object to filter by, which four columns does the filter search? (Choose four.)

A. Services
B. Action
C. Protocol
D. Log
E. Applied To
F. Source
G. Destinations

Correct Answer: AEFG
Section: (none)
Explanation

Explanation/Reference:
Explanation:



□ Add a Firewall Rule in Manager Mode

□ Delete a Firewall Rule in Manager Mode

□ Edit the Default Distributed Firewall Rule in Manager Mode

□ Change the Order

Filter Firewall Rules in Manager Mode

Updated on 04/06/2020

Selected product version: VMware NSX T Data Center 3.1

When you navigate to the firewall section, initially all the rules are displayed. You can apply a filter to control what is displayed so that you see only a subset of the rules. This can make it easier to manage the rules.

Prerequisites

Verify that **Manager** mode is selected in the NSX Manager user interface. See NSX Manager.

Reference: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/administration/GUID-BF564729-868B-4136-9AD0-857C47078FB3.html

QUESTION 54 Which shell command line syntax represents less suspicious danger than the others?

A. `sc create`
B. `-Enc`
C. `clear`
D. `net user`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: