# Question 1

An EPM Administrator would like to enable a Threat Protection policy, however, the policy protects an application that is not installed on all endpoints.

What should the EPM Administrator do?

## Options:

**A-** Enable the Threat Protection policy and configure the Policy Targets.

**B-** Do not enable the Threat Protection policy.

**C-** Enable the Threat Protection policy only in Detect mode.

**D-** Split up the endpoints in to separate Sets and enable Threat Protection for only one of the Sets.

## Answer:

D

# Question 2

Where would an EPM admin configure an application policy that depends on a script returning true for an end user's machine being connected to an open (no password protection) Wi-Fi?

## Options:

**A-** Advanced Policy - Application Control - Check Wi-Fi security

**B-** Advanced Policy - Options: Conditional enforcement - Apply Policy according to Script execution result

**C-** Default policies - Check if network access is secure

**D-** Advanced Policy - Access - Specify permissions to be set for Wi-Fi network security

## Answer:

B

# Question 3

**Question Type:** **MultipleChoice**

An EPM Administrator would like to enable CyberArk EPM's Ransomware Protection in Restrict mode. What should the EPM Administrator do?

## Options:

**A-** Set Block unhandled applications to On.

**B-** Set Protect Against Ransomware to Restrict.

**C-** Set Protect Against Ransomware to Restrict and Set Block unhandled applications to On.

**D-** Set Control unhandled applications to Detect.

## Answer:

C

# Question 4

**Question Type:** **MultipleChoice**

What unauthorized change can CyberArk EPM Ransomware Protection prevent?

**A-** Windows Registry Keys

**B-** Website Data

**C-** Local Administrator Passwords

**D-** Certificates in the Certificate Store

**Answer:**

D

# Question 5

**Question Type:** **MultipleChoice**

When working with credential rotation at the EPM level, what is the minimum time period that can be set between connections?

**Options:**

**A-** 1 hour

**B-** 5 hours

**C-** 24 hours

**D-** 72 hours

### Answer:
D

# Question 6

**Question Type:** **MultipleChoice**

When deploying Ransomware Protection, what tasks should be considered before enabling this functionality? (Choose two.)

### Options:
**A-** Add trusted software to the Authorized Applications (Ransomware protection) Application Group

**B-** Add trusted software to the Allow Application Group

**C-** Add additional files, folders, and/or file extensions to be included to Ransomware Protection

**D-** Enable Detect privileged unhandled applications under Default Policies

A, C

# Question 7

**Question Type:** **MultipleChoice**

Select the default threat intelligence source that requires additional licensing.

**Options:**

**A-** VirusTotal

**B-** Palo Alto WildFire

**C-** CyberArk Application Risk Analysis Service

**D-** NSRL

**Answer:**

B

# Question 8

How does EPM help streamline security compliance and reporting?

## Options:

**A-** Use of automated distribution of reports to the security team

**B-** Provides reports in standard formats such as PDF, Word and Excel

**C-** Print reports

**D-** Create custom reports

## Answer:

B