

# CERTPARK



## QUESTION & ANSWER



CERTPARK.COM

Accurate Study Guides,  
High Passing Rate!  
provides update  
free of charge  
in one year!



<https://www.certpark.com>

**Exam** : **156-315.81**

**Title** : Check Point Certified  
Security Expert - R81.20

**Version** : DEMO

1. Identify the API that is not supported by Check Point currently.

- A. R81 Management API-
- B. Identity Awareness Web Services API
- C. Open REST API
- D. OPSEC SDK

**Answer: C**

**Explanation:**

Check Point currently supports four types of APIs: R81 Management API, Identity Awareness Web Services API, OPSEC SDK, and Gaia REST API. The Open REST API is not a valid option.

Reference: Check Point APIs

2. SandBlast Mobile identifies threats in mobile devices by using on-device, network, and cloud-based algorithms and has four dedicated components that constantly work together to protect mobile devices and their data.

Which component is NOT part of the SandBlast Mobile solution?

- A. Management Dashboard
- B. Gateway
- C. Personal User Storage
- D. Behavior Risk Engine

**Answer: C**

**Explanation:**

SandBlast Mobile has four components: Management Dashboard, Gateway, Behavior Risk Engine, and On-Device Network Protection. Personal User Storage is not part of the SandBlast Mobile solution.

Reference: SandBlast Mobile Architecture

3. What are the different command sources that allow you to communicate with the API server?

- A. SmartView Monitor, API\_cli Tool, Gaia CLI, Web Services
- B. SmartConsole GUI Console, mgmt\_cli Tool, Gaia CLI, Web Services
- C. SmartConsole GUI Console, API\_cli Tool, Gaia CLI, Web Services
- D. API\_cli Tool, Gaia CLI, Web Services

**Answer: B**

**Explanation:**

You can communicate with the API server using three command sources: SmartConsole GUI Console, mgmt\_cli Tool, and Gaia CLI. Web Services are not a command source, but a way to access the API server using HTTP requests.

Reference: Check Point Management APIs

4. What makes Anti-Bot unique compared to other Threat Prevention mechanisms, such as URL Filtering, Anti-Virus, IPS, and Threat Emulation?

- A. Anti-Bot is the only countermeasure against unknown malware
- B. Anti-Bot is the only protection mechanism which starts a counter-attack against known Command & Control Centers
- C. Anti-Bot is the only signature-based method of malware protection.
- D. Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a

Command & Control Center.

**Answer:** D

**Explanation:**

Anti-Bot is a post-infection malware protection that detects and blocks botnet communications from infected hosts to Command & Control servers. It is different from other Threat Prevention mechanisms that prevent malware from entering the network or executing on the hosts.

Reference: Anti-Bot Software Blade

5.Which TCP-port does CPM process listen to?

A. 18191

B. 18190

C. 8983

D. 19009

**Answer:** D

**Explanation:**

The CPM process is the core process of the Security Management Server that handles all management operations. It listens to TCP-port 19009 by default.

Reference: CPM process