TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **JN0-636**

Title : Security,Professional (JNCIP-SEC)

Version : DEMO

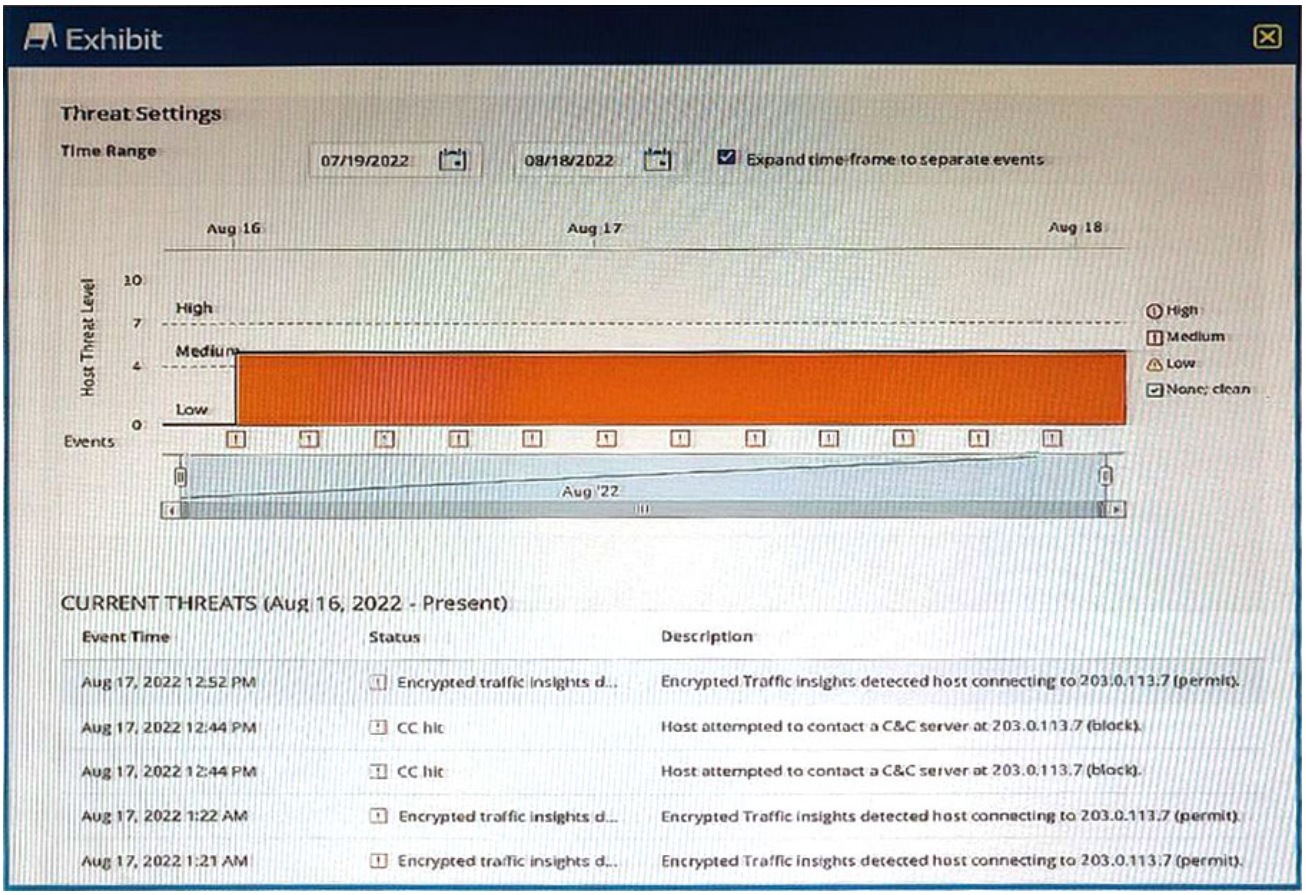
1.SRX Series device enrollment with Policy Enforcer fails To debug further, the user issues the following commandshow configuration services security—intelligence url
https://cloudfeeds.argon.juniperaecurity.net/api/manifeat.xml
and receives the following output:
What is the problem in this scenario?
A. The device is directly enrolled with Juniper ATP Cloud.
B. The device is already enrolled with Policy Enforcer.
C. The SRX Series device does not have a valid license.
D. Junos Space does not have matching schema based on the
Answer: C

2.You are asked to deploy filter-based forwarding on your SRX Series device for incoming traffic sourced from the 10.10 100 0/24 network in this scenario, which three statements are correct? (Choose three.)
A. You must create a forwarding-type routing instance.
B. You must create and apply a firewall filter that matches on the source address 10.10.100.0/24 and then sends this traffic to your routing
C. You must create and apply a firewall filter that matches on the destination address 10 10.100.0/24 and then sends this traffic to your routing instance.
D. You must create a RIB group that adds interface routes to your routing instance.
E. You must create a VRF-type routing instance.
Answer: A B D

3.You are asked to provide single sign-on (SSO) to Juniper ATP Cloud.
Which two steps accomplish this goal? (Choose two.)
A. Configure Microsoft Azure as the service provider (SP).
B. Configure Microsoft Azure as the identity provider (IdP).
C. Configure Juniper ATP Cloud as the service provider (SP).
D. Configure Juniper ATP Cloud as the identity provider (IdP).
Answer: B C

4.You want to identify potential threats within SSL-encrypted sessions without requiring SSL proxy to decrypt the session contents.
Which security feature achieves this objective?
A. infected host feeds
B. encrypted traffic insights
C. DNS security
D. Secure Web Proxy
Answer: B

5.Exhibit



You are using ATP Cloud and notice that there is a host with a high number of ETI and C&C hits sourced from the same investigation and notice that some of the events have not been automatically mitigated. Referring to the exhibit, what is a reason for this behavior?

A. The C&C events are false positives.

B. The infected host score is globally set bellow a threat level of 5.

C. The infected host score is globally set above a threat level of 5.

D. The ETI events are false positives.

Answer: D