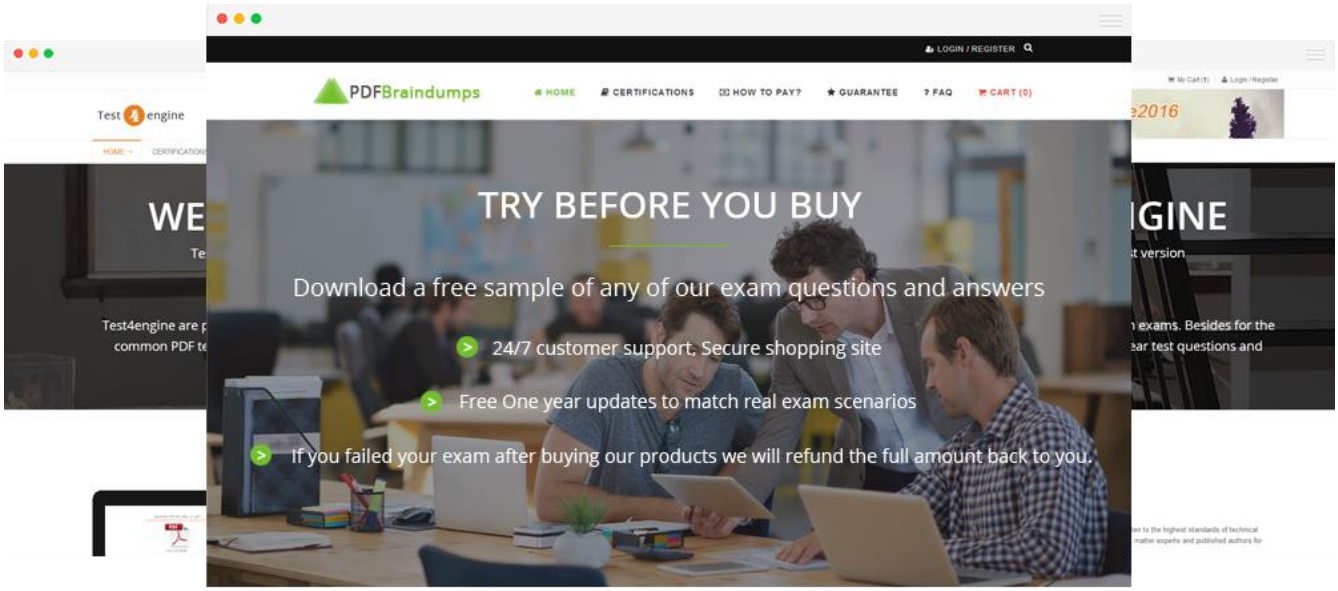
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

Exam : **C2150-400**

Title : IBM Security Qradar SIEM Implementation v 7.2.1

Vendor : IBM

Version : DEMO

NO.1 What is the result when adding host definition building blocks toQRadar?
A. Creates Offenses
B. Reduces false positives
C. Makes searches run faster
D. Authorizes QRadar Services
Answer: B

NO.2 Which tab in the QRadar web console allows flows to be monitored and investigated?
A. Admin
B. Assets
C. Offenses
D. Network Activity
Answer: C
Reference:ftp://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/CoreDocs/QRadar_71MR1_GettingStartedGuide.pdf(page 10, offenses tab)

NO.3 Which two search filters are available on theQRadarconsole while making an asset search? (Choose two.)
A. PCI Severity. NERC Severity
B. Vulnerability CVSS Base Score. Vulnerability Risk Score
C. Vulnerability on Open Port, Vulnerability on Open Service
D. Vulnerability on Open Port, Vulnerability External Reference
E. Vulnerability on Source Port, Vulnerability on Destination Port
Answer: B,E

NO.4 A user ofQRadarwishes to have a report showing the number of bytes per packet they see with their flows. The user decides to create a Custom Flow Property for this application.
Which type of custom property is required for this to be accomplished?
A. Regex Custom Property
B. Advanced Custom Property
C. Computation Custom Property
D. Calculation Based Custom Property
Answer: A

NO.5 A mail server typically communicates with 50 hosts per second in the middle of the night and then suddenly starts communicating with 1.000 hosts a second. The administrator wants to get an email alert whenever this situation is being observed.
Which type of rule should an administrator create to monitor this situation?
A. Flow Rule
B. Anomaly Rule
C. Threshold Rule
D. Behavioral Rule
Answer: C

NO.6 Which two authentication methods for theQRadarUser Interface are valid? (Choose two.)
A. SecureID
B. Digital Signatures
C. Password Authentication Protocol (PAP)
D. Remote Authentication Dial In User Service (RADIUS)
E. Terminal Access Controller Access-Control System (TACACS)
Answer: D,E

NO.7 Which character is used for naming subgroups when using the option Add Group in the Network Hierarchy editor?
A. +(plus)
B. . (period)
C. \ (Backslash)
D. /(Forward Slash)
Answer: B

NO.8 What is a benefit of enabling indexes on event properties?
A. Improved Offense Correlation
B. Improved search performance
C. Improved Performance of Custom Rules
D. Improved accuracy of auto-discovery log sources
Answer: B