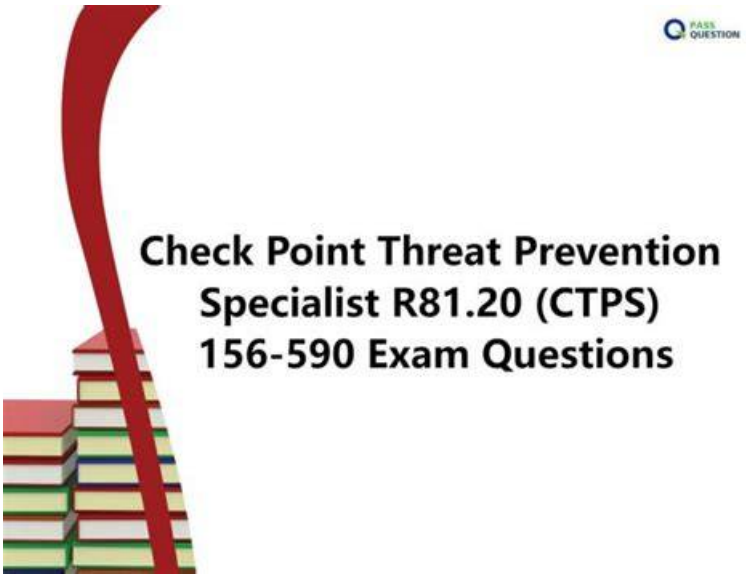
CheckPoint 156-590: Check Point Certified Threat Prevention Specialist (CTPS) braindumps PDF & Testking echter Test



Um Sie beim Kauf der CheckPoint 156-590 Prüfungssoftware beruhigt zu lassen, wenden wir die gesicherteste Zahlungsmittel an. Paypal ist das größte internationale Zahlungssystem. Und wir bewahren sorgfältig Ihre persönliche Informationen. Wenn Sie Fragen über die CheckPoint 156-590 Prüfungsunterlagen oder Interesse an anderen Prüfungssoftwaren haben, könnten Sie diret mit uns online kontaktieren oder uns E-Mail schicken. Wir tun unser Bestes, um Ihnen bei der CheckPoint 156-590 Prüfung zu helfen.

CheckPoint 156-590 Exam Syllabus Topics:

Section	Weight	Objectives
Threat Prevention Dashboard and Monitoring	10%	- Troubleshooting Threat Prevention issues - Threat Prevention statistics and trends - Threat Prevention logs and reporting - Using SmartConsole for monitoring
Threat Prevention Overview and Architecture	10%	- Check Point Threat Prevention solution overview - Threat Prevention architecture and components - Security Gateway integration with Threat Prevention
Threat Emulation (SandBlast)	15%	- Threat Emulation policy configuration - Threat Emulation architecture and deployment - Zero-day threat protection - File emulation process and verdicts
Anti-Bot and Anti-Virus	15%	- Anti-Virus scanning methods (streamed vs. traditional) - Bot detection mechanisms - Bot and malware signature updates - Configuring Anti-Bot and Anti-Virus policies
Threat Prevention Policy	20%	- Profile-based vs. rule-based configurations - Threat Prevention action settings - Creating and configuring Threat Prevention profiles - Applying Threat Prevention policy layers
IPS (Intrusion Prevention System)	20%	- IPS policy configuration and tuning - IPS architecture and deployment modes - IPS exceptions and whitelisting - IPS logging and alerts - IPS signatures and protections

Threat Extraction	10%	- Threat Extraction policy configuration - PDF, Office document, and archive sanitization - Threat Extraction (Sanboxing) concepts

>> 156-590 Testking <<

156-590 Buch & 156-590 Unterlage

Wir It-Pruefung sind die professionellen Anbieter der Schulungsunterlagen zur CheckPoint 156-590 Zertifizierungsprüfung. Seit langem betrachten wir It-Pruefung das Angebot der besten Prüfungsunterlagen zur CheckPoint 156-590 Zertifizierungsprüfung als unser Ziel. Verglichen zu anderen Webseiten, wir It-Pruefung sind immer von anderen vertraut. Warum? Weil wir It-Pruefung vieljährige Erfahrungen haben, aufmerksam auf die IT-Zertifizierung-Studie machen und viele Prüfungsregeln sammeln. Damit können wir It-Pruefung sehr hohe Hit-Rate haben. Das gewährleistet die Durchlaufrate.

CheckPoint Check Point Certified Threat Prevention Specialist (CTPS) 156-590 Prüfungsfragen mit Lösungen (Q64-Q69):

64. Frage
You have to issue a Log filter to view IPS logs generated for user John Doe.
Which of the following is the correct filter?

- A. user:John Doe AND (action:drop OR action:reject OR action:block)
- B. user:"John Doe" AND (action:drop OR action:reject OR action:block)
- C. user:"John-Doe" AND (action:drop OR action:reject OR action:block)
- D. user:'John Doe' AND (action:drop OR action:reject OR action:block)

Antwort: B

Begründung:
The correct answer is C. user:"John Doe" AND (action:drop OR action:reject OR action:block) . Check Point log-query syntax uses field-based filters in the form field:value , Boolean operators such as AND and OR , and parentheses to group multiple criteria. The official Query Language Overview states that the basic syntax is [Field:] < Filter Criterion > , and that Boolean operators can combine multiple filters. It also shows action filtering examples such as blade:"application control" AND action:block, and explains that multiple Boolean expressions can be grouped in parentheses.
Because the user name contains a space, the value must be enclosed in double quotation marks: user:"John Doe". Without quotes, the query parser treats the words as separate criteria, which makes option B incorrect.
Option A uses a hyphenated value, which changes the user name. Option D uses single quotes, while Check Point examples and expected syntax use double quotes for phrase values. The action clause is correctly grouped with OR to match logs where the IPS-related enforcement action is drop, reject, or block. Reference topics: Logs & Monitor query language, field filters, quoted strings, Boolean operators, action filtering, IPS log investigation.

65. Frage
Task: Validate policy enforcement of a specific IPS profile.

Antwort:

Begründung:
See the Explanation.Explanation:
1- Trigger test traffic that matches a rule using the profile.
2- SmartConsole > Logs > Filter by Profile name.
3- Confirm protections are applied with expected action.
4- Use fw stat on gateway to view loaded policy.
5- Ensure profile assignment is correct in the policy rule.

66. Frage
What kind of information is stored in the Audit Log?

- A. An audit log is a portion of the traffic log which has been filtered by filter expression defined by the administrator.
- B. An audit log is a record of actions taken by administrators.
- C. An audit log is a record of system event logs on the Security Gateway.
- D. An audit log is a record of system event logs on the Security Management Server.

Antwort: B

Begründung:
The correct answer is A. An audit log is a record of actions taken by administrators . In Check Point management architecture, audit logs are different from traffic logs, threat logs, or operating-system event logs.
A traffic log records inspected network connections and blade decisions. A threat log records Threat Prevention detections, preventions, packet captures, forensic details, and blade-specific events. An audit log records administrative activity performed in the management environment. The uploaded Check Point glossary material defines an Audit Log as a log that contains administrator actions on a Management Server, including login and logout, creation or modification of an object, and installation of a policy.
This is operationally important because audit logs support accountability and change control. When investigating a policy change, exception addition, blade enablement, profile modification, or installation event, the audit trail shows which administrator performed the action and when it occurred. Option B is incorrect because system event logs are not the same as audit logs. Option C describes a filtered view of logs, not an audit record. Option D is incorrect because gateway system logs are operational logs from enforcement points, while audit logs are management-plane administrative records. Reference topics: Audit Logs, administrator actions, Management Server accountability, policy installation auditing, change tracking.

67. Frage
Which of the following protocols can be scanned by Anti-Virus?

- A. Telnet
- B. RemoteDesktop
- C. CIFS
- D. SNMP

Antwort: C

Begründung:
The correct answer is C. CIFS . Check Point Anti-Virus scans file-transfer and content-bearing protocols, not arbitrary management or terminal protocols. The official Anti-Virus settings documentation lists the protocols Anti-Virus can scan as Web HTTP/HTTPS , FTP , SMB , and Mail SMTP or POP3 , with additional support for IMAP and POP3.
CIFS is closely associated with Microsoft file sharing and the SMB protocol family. In the exam context, CIFS maps to the file-sharing traffic class that Anti-Virus can inspect through SMB scanning. This is why CIFS is the correct option. Remote Desktop is an interactive remote-control protocol, not a file-inspection protocol for Anti-Virus scanning in this question. SNMP is a monitoring and management protocol and does not normally carry files for malware inspection. Telnet is an interactive terminal protocol and is not an Anti- Virus file-scanning protocol. The certification distinction is that Anti-Virus inspection focuses on files and content objects crossing supported protocols, especially web downloads, FTP transfers, SMB/CIFS file access, and mail attachments. Reference topics: Anti-Virus Settings, protocol scanning, SMB/CIFS inspection, file-transfer inspection, Threat Prevention protected scope.

68. Frage
What is a function of SmartEvent?

- A. Generates logs for customizable views
- B. Runs on the Security Gateway generating events
- C. A Multi-Domain level log forwarding tool used to forward logs to syslog or similar external tools
- D. Correlates Security Gateway logs into easily understandable events

Antwort: D

Begründung:
The correct answer is D. Correlates Security Gateway logs into easily understandable events . SmartEvent is Check Point's event-correlation and analysis system. It does not simply generate raw logs; logs are generated by Security Gateways and other Check Point components. SmartEvent consumes those logs, analyzes them against event policies, identifies patterns, and produces higher-level events suitable for investigation, dashboards, reports, and incident workflows. Check Point documentation explains that the

SmartEvent Correlation Unit analyzes each log entry from a Log Server, looks for patterns according to the installed Event Policy, and forwards identified events to the SmartEvent Server.
This directly eliminates the distractors. SmartEvent does not run on the Security Gateway as the log- generating enforcement component. It does not generate logs merely so views can be customized; rather, it indexes, correlates, and presents logs and events. It is not principally a Multi-Domain syslog-forwarding tool.
Its architectural value is correlation: it transforms large volumes of gateway logs into meaningful security events, reducing analyst workload and enabling threat timelines, reports, executive summaries, and incident management. Reference topics: SmartEvent Architecture, SmartEvent Correlation Unit, Event Policy, Log Server analysis, threat-event correlation.

69. Frage
......