2014 Latest Pass4sure&Lead2pass Symantec ST0-085 Dumps (41-50)

QUESTION 41
Which statement is true about rules in a Symantec Security Information Manager solution?

A. Rules can be created that escalate events to incidents, based on policies defined on each asset.
B. The Rules Editor can create policies on each asset to determine what rules are executed when an event occurs.
C. Rules can be configured on each asset that will launch a vulnerability scan when a specific type of event occurs.
D. The Rules tab can be used on the console to automatically identify available ports on an asset.

Answer: A

QUESTION 42
Which two ratings does the Information Manager Assets Table use to quantify the importance of the device and help determine how to escalate security incidents related to that device? (Select two.)

A. Confidentiality
"Pass Any Exam. Any Time." - www.actualtests.com 18
Symantec ST0-085 Exam
B. Criticality
C. Severity
D. Priority
E. Integrity

Answer: AE

QUESTION 43
What are two ways the Assets Table can reduce the reporting of false positive security incidents using built-in functionality? (Select two.)

A. assigns proper CIA values to each asset in the table
B. schedules daily updates of vulnerability information from Symantec's LiveUpdate service
C. populates the Policies tab with policies that apply to each asset
D. uses a supported vulnerability scanner to help prioritize incidents
E. configures normalization of event data captured by the collectors

Answer: CD

QUESTION 44
How can you determine which ports are potentially vulnerable on a given host in the Assets Table?

A. by running the NetScan user action on the asset
B. by looking at the Services tab on the asset
C. by viewing the Details tab for the asset
D. by running the Host Information report on the asset

Answer: B

QUESTION 45
What information is reported by the Nessus scanner when it scans a range of network addresses?
"Pass Any Exam. Any Time." - www.actualtests.com 19
Symantec ST0-085 Exam

A. configuration data of discovered devices
B. vulnerabilities of discovered network devices
C. patch levels installed on discovered devices
D. the SANS risk level of each discovered device

Answer: B

QUESTION 46
Which service provides Symantec Security Information Manager with updated intelligence about threats?

A. Symantec Security Information Manager
B. DeepSight Global Intelligence Network
C. Symantec Enterprise Security Manager
D. Symantec Endpoint Protection

Answer: B

QUESTION 47
What does the Correlation Engine do once custom rules are properly defined?

A. Correlates events against the rule criteria, analyzes conclusions and creates impending incidents.
B. Analyzes events against the rule criteria, correlates with existing conclusions and creates the impending incident.
C. Analyzes events against the rule criteria, creates conclusions and correlates conclusions into incidents.
D. Applies individual rules to events, analyzes conclusions and correlates events into incidents.

Answer: A

QUESTION 48
From the Information Manager Console, which procedure allows a Symantec Security Information Manager (SSIM) to forward events to another SSIM appliance?

A. System tab --> Appliance Configuration tab --> create new Forward event --> input IP address of remote appliance --> define Event Criteria
B. System tab --> Event Configuration tab --> create new Forward event --> input IP address of remote appliance --> define Event Criteria
C. Appliance Configuration tab --> Event Configuration tab --> create new Forward event --> input IP address of remote appliance --> define Incident Criteria
D. System tab --> Maintenance tab --> create new Forward event --> input IP address of remote "Pass Any Exam. Any Time." - www.actualtests.com 25
Symantec ST0-085 Exam
appliance --> define Incident Criteria

Answer: A

QUESTION 49

Which task does Symantec Security Information Manager perform relating to Incident Management?

A. Creates a vulnerability category.
B. Performs remediation on the attack.
C. Projects and documents future attacks.
D. Reports incidents to the SANS Internet Storm Center.
E. Assigns incidents to a team member.

Answer: E

QUESTION 50
When multiple incidents involving the same issue are merged, what does Information Manager do?

A. saves the original incidents and creates a new incident
B. closes the original incidents and creates a new incident
C. deletes the original incidents and creates a new incident
D. reports the original incidents to the SANS Internet Storm Center, closes the incidents and creates a new incident

Answer: B

If you want to pass Symantec ST0-085 successfully, donot missing to read latest lead2pass Symantec ST0-085 practice exams.
If you can master all lead2pass questions you will able to pass 100% guaranteed.

http://www.lead2pass.com/ST0-085.html