Vendor: CrowdStrike

Exam Code: CCFA-200

Exam Name: CrowdStrike Certified Falcon Administrator

Version: DEMO

QUESTION 1
What command should be run to verify if a Windows sensor is running?

A. regedit myfile.reg
B. sc query csagent
C. netstat -f
D. ps -ef | grep falcon

Answer: B
Explanation:
The command that should be run to verify if a Windows sensor is running is sc query csagent. This command will display the status and information of the csagent service, which is the Falcon sensor service. The other commands are either incorrect or not applicable to Windows sensors.

QUESTION 2
Which option allows you to exclude behavioral detections from the detections page?

A. Machine Learning Exclusion
B. IOA Exclusion
C. IOC Exclusion
D. Sensor Visibility Exclusion

Answer: B
Explanation:
IOA Exclusion says - Stop all behavioral detections and preventions for an IOA that's based on a CrowdStrike-generated detection.

QUESTION 3
What are custom alerts based on?

A. Custom workflows
B. Custom event based triggers
C. Predefined alert templates
D. User defined Splunk queries

Answer: C
Explanation:
Scheduling a Custom Alert for your environment consists of three steps: choosing the template you'd like to configure, previewing the search results, then scheduling the alert. Use Custom Alerts to configure email alerts using predefined templates so you're notified about specific activity in your environment. When an alert runs and finds results, it sends an email to specified recipients instead of generating a new detection. Custom Alerts let you set up email alerts based on predefined templates that cover a wide range of topics including Real Time Response session initiation, host containment, OS security settings, and more that are not yet covered by notification workflows.

QUESTION 4
When creating an API client, which of the following must be saved immediately since it cannot be viewed again after the client is created?

A. Base URL

B. Secret
C. Client ID
D. Client name

Answer: B
Explanation:
When creating an API client, the secret must be saved immediately since it cannot be viewed again after the client is created. The secret is a randomly generated string that is used to authenticate the API client along with the client ID. The other options are either incorrect or can be viewed or modified later.

QUESTION 5
You notice there are multiple Windows hosts in Reduced functionality mode (RFM). What is the most likely culprit causing these hosts to be in RFM?

A. A Sensor Update Policy was misconfigured
B. A host was offline for more than 24 hours
C. A patch was pushed overnight to all Windows systems
D. A host was placed in network containment from a detection

Answer: C
Explanation:
The most likely culprit causing multiple Windows hosts to be in Reduced Functionality Mode (RFM) is a patch that was pushed overnight to all Windows systems. RFM occurs when the sensor detects a change in the operating system that requires a reboot to complete. A patch is one of the common causes of such a change. The other options are either incorrect or not related to RFM.

QUESTION 6
Which of the following is TRUE of the Logon Activities Report?

A. Shows a graphical view of user logon activity and the hosts the user connected to
B. The report can be filtered by computer name
C. It gives a detailed list of all logon activity for users
D. It only gives a summary of the last logon activity for users

Answer: D
Explanation:
The Logon Activities Report shows a graphical view of user logon activity and the hosts the user connected to, but it only gives a summary of the last logon activity for users. It does not give a detailed list of all logon activity for users, nor can it be filtered by computer name. The other options are either incorrect or not true of the report.

QUESTION 7
Which of the following roles allows a Falcon user to create Real Time Response Custom Scripts?

A. Real Time Responder ?Administrator
B. Real Time Responder ?Read Only Analyst
C. Real Time Responder ?Script Developer
D. Real Time Responder ?Active Responder

Answer: A
Explanation:
Real Time Responder - Administrator (RTR Administrator) - Can do everything RTR Active Responder can do, plus create custom scripts, upload files to hosts using the put command, and directly run executables using the run command.

QUESTION 8
What model is used to create workflows that would allow you to create custom notifications based on particular events which occur in the Falcon platform?

A. For - While statement(s)
B. Trigger, condition(s) and action(s)
C. Event trigger(s)
D. Predefined workflow template(s)

Answer: B
Explanation:
The model that is used to create workflows that would allow you to create custom notifications based on particular events which occur in the Falcon platform is trigger, condition(s) and action(s). This model allows you to specify what event will trigger the workflow, what condition(s) must be met for the workflow to execute, and what action(s) will be performed by the workflow. The other options are either incorrect or not related to creating workflows.

QUESTION 9
An analyst is asked to retrieve an API client secret from a previously generated key. How can they achieve this?

A. The API client secret can be viewed from the Edit API client pop-up box
B. Enable the Client Secret column to reveal the API client secret
C. Re-create the API client using the exact name to see the API client secret
D. The API client secret cannot be retrieved after it has been created

Answer: D
Explanation:
The API client secret cannot be retrieved after it has been created. The secret is only displayed once when the API client is created, and it cannot be viewed or edited later. Therefore, it is important to save the secret securely and use it along with the client ID to authenticate the API client. The other options are either incorrect or not possible.

QUESTION 10
Which port and protocol does the sensor use to communicate with the CrowdStrike Cloud?

A. TCP port 22 (SSH)
B. TCP port 443 (HTTPS)
C. TCP port 80 (HTTP)
D. TCP UDP port 53 (DNS)

Answer: B
Explanation:
The sensor uses TCP port 443 (HTTPS) to communicate with the CrowdStrike Cloud. This port

and protocol are used to securely send and receive data between the sensor and the cloud, such as detections, policies, updates, commands, etc. The other options are either incorrect or not used by the sensor.

QUESTION 11
What is the most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM)?

A. Falcon console updates are pending
B. Falcon sensors installing an update
C. Notifications have been disabled on that host sensor
D. Microsoft updates

Answer: D
Explanation:
The most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM) is Microsoft updates. RFM occurs when the sensor detects a change in the operating system that requires a reboot to complete. Microsoft updates are one of the common causes of such a change. The other options are either incorrect or not related to RFM.

QUESTION 12
On which page of the Falcon console would you create sensor groups?

A. User management
B. Sensor update policies
C. Host management
D. Host groups

Answer: D
Explanation:
The only place where create host groups is in " Host and setup management > host Groups> Create a group" In Sensor Update policies you can only asign a group of host to the policy not creating a group of hosts.

QUESTION 13
While a host is Network contained, you need to allow the host to access internal network resources on specific IP addresses to perform patching and remediation. Which configuration would you choose?

A. Configure a Real Time Response policy allowlist with the specific IP addresses
B. Configure a Containment Policy with the specific IP addresses
C. Configure a Containment Policy with the entire internal IP CIDR block
D. Configure the Host firewall to allowlist the specific IP addresses

Answer: B
Explanation:
While a host is Network contained, the administrator can allow the host to access internal network resources on specific IP addresses to perform patching and remediation by configuring a Containment Policy with the specific IP addresses. This policy allows users to specify which ports, protocols and IP addresses are allowed or blocked during network containment. The other options are either incorrect or not related to network containment.

QUESTION 14
Which of the following is TRUE regarding Falcon Next-Gen AntiVirus (NGAV)?

A. Falcon NGAV relies on signature-based detections
B. Activating Falcon NGAV will also enable all detection and prevention settings in the entire policy
C. The Detection sliders cannot be set to a value less aggressive than the Prevention sliders
D. Falcon NGAV is not a replacement for Windows Defender or other antivirus programs

Answer: C
Explanation:
The Detection sliders cannot be set to a value less aggressive than the Prevention sliders in Falcon Next-Gen AntiVirus (NGAV). This is because prevention is a subset of detection, and it would not make sense to prevent threats that are not detected. The other options are either incorrect or not true of Falcon NGAV.

QUESTION 15
What is the purpose of using groups with Sensor Update policies in CrowdStrike Falcon?

A. To group hosts with others in the same business unit
B. To group hosts according to the order in which Falcon was installed, so that updates are installed in the same order every time
C. To prioritize the order in which Falcon updates are installed, so that updates are not installed all at once leading to network congestion
D. To allow the controlled assignment of sensor versions onto specific hosts

Answer: D
Explanation:
The purpose of using groups with Sensor Update policies in CrowdStrike Falcon is to allow the controlled assignment of sensor versions onto specific hosts. This allows users to manage the sensor updates for different hosts based on their needs and preferences, such as testing, staging or production. The other options are either incorrect or not related to using groups with Sensor Update policies.

QUESTION 16
What impact does disabling detections on a host have on an API?

A. Endpoints with detections disabled will not alert on anything until detections are enabled again
B. Endpoints cannot have their detections disabled individually
C. DetectionSummaryEvent stops sending to the Streaming API for that host
D. Endpoints with detections disabled will not alert on anything for 24 hours (by default) or longer if that setting is changed

Answer: C
Explanation:
Disabling detections on a host will stop the DetectionSummaryEvent from sending to the Streaming API for that host. This means that the host will not send any detection events to the Streaming API, which is used to stream data from the Falcon Cloud to external applications or systems. The other options are either incorrect or not related to disabling detections on a host.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**