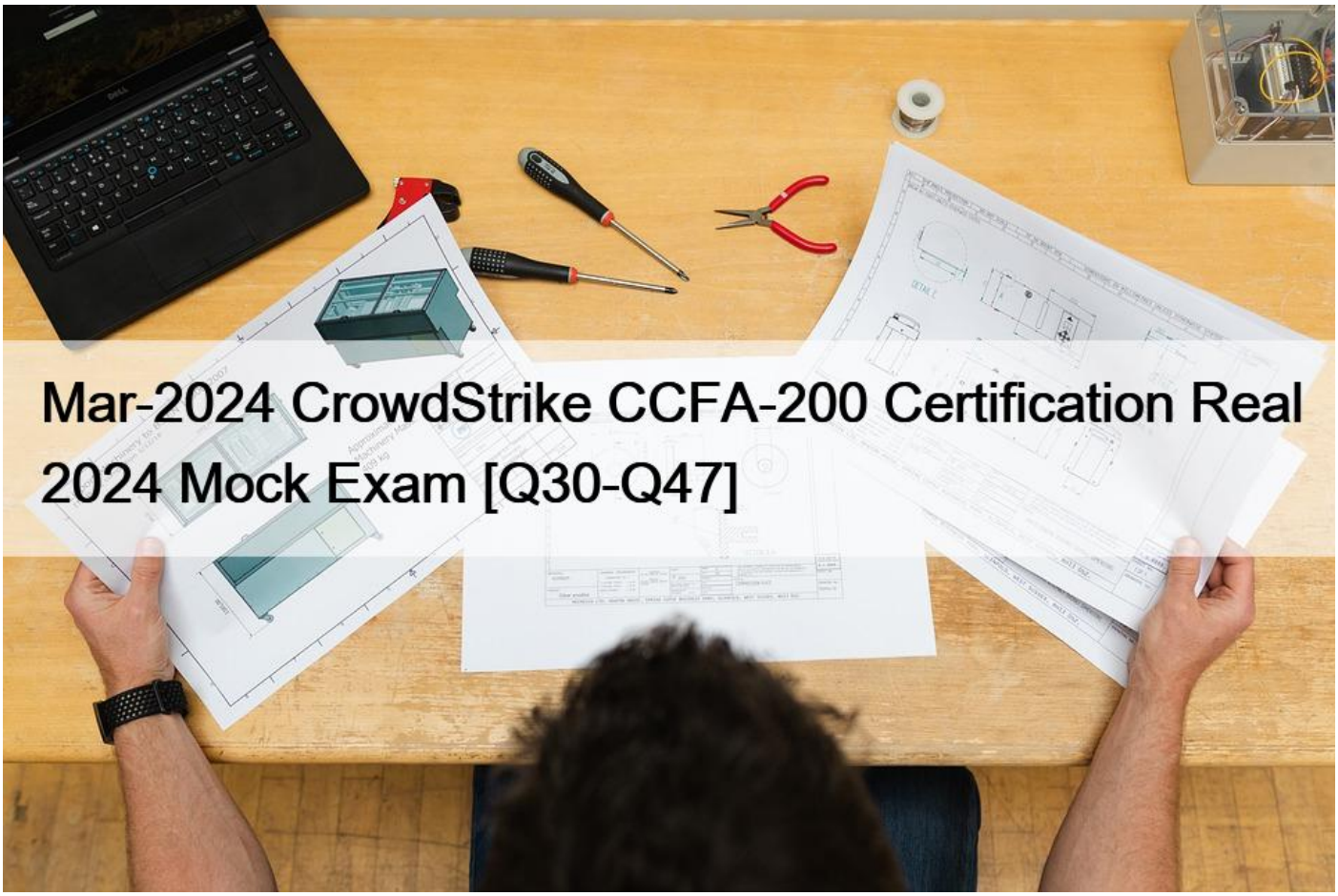
Mar-2024 CrowdStrike CCFA-200 Certification Real 2024 Mock Exam [Q30-Q47



Mar-2024 CrowdStrike CCFA-200 Certification Real 2024 Mock Exam
CCFA-200 Exam Questions and Valid PMP Dumps PDF

The CCFA-200 exam is a comprehensive assessment that covers a wide range of topics related to CrowdStrike Falcon. It includes questions on the platform's features, capabilities, and best practices for configuration and deployment. Candidates must also demonstrate their ability to analyze and respond to real-world cyber threats, using the tools and techniques provided by CrowdStrike Falcon.

CrowdStrike CCFA-200 certification is a valuable credential for anyone looking to advance their career in cybersecurity. With the growing demand for skilled cybersecurity professionals, individuals who hold this certification will be well-positioned to take advantage of new career opportunities and to make a meaningful impact in the field.

NO.30 Which of the following can a Falcon Administrator edit in an existing user’s profile?
* First or Last name
* Phone number

* Email address
* Working groups

NO.31 You are beginning the rollout of the Falcon Sensor for the first time side-by-side with your existing security solution. You need to configure the Machine Learning levels of the Prevention Policy so it does not interfere with existing solutions during the testing phase. What settings do you choose?
* Detection slider: Extra Aggressive

Prevention slider: Cautious
* Detection slider: Moderate

Prevention slider: Disabled
* Detection slider: Cautious

Prevention slider: Cautious
* Detection slider: Disabled

Prevention slider: Disabled

NO.32 The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks. Which statement is TRUE concerning Falcon sensor certificate validation?
* SSL inspection should be configured to occur on all Falcon traffic
* Some network configurations, such as deep packet inspection, interfere with certificate validation
* HTTPS interception should be enabled to proceed with certificate validation
* Common sources of interference with certificate pinning include protocol race conditions and resource contention

NO.33 When would the No Action option be assigned to a hash in IOC Management?
* When you want to save the indicator for later action, but do not want to block or allow it at this time
* Add the indicator to your allowlist and do not detect it
* There is no such option as No Action available in the Falcon console
* Add the indicator to your blocklist and show it as a detection

NO.34 The Logon Activities Report includes all of the following information for a particular user EXCEPT _____.
* the account type for the user (e.g. Domain Administrator, Local User)
* all hosts the user logged into
* the logon type (e.g. interactive, service)
* the last time the user’s password was set

NO.35 Which of the following prevention policy settings monitors contents of scripts and shells for execution of malicious content on compatible operating systems?
* Script-based Execution Monitoring
* FileSystem Visibility
* Engine (Full Visibility)
* Suspicious Scripts and Commands

Explanation

The prevention policy setting that monitors contents of scripts and shells for execution of malicious content on compatible operating systems is Script-based Execution Monitoring. Script-based Execution Monitoring is a feature that enables the Falcon sensor to monitor and prevent malicious script execution on Windows systems.

The feature uses machine learning and behavioral analysis to detect suspicious scripts or commands executed by various script interpreters, such as PowerShell, WScript, CScript, or Bash. You can enable or disable Script-based Execution Monitoring in the Prevention Policy for Windows hosts1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NO.36 When a host is placed in Network Containment, which of the following is TRUE?
* The host machine is unable to send or receive network traffic outside of the local network
* The host machine is unable to send or receive network traffic except to/from the Falcon Cloud and traffic allowed in the Firewall Policy
* The host machine is unable to send or receive any network traffic
* The host machine is unable to send or receive network traffic except to/from the Falcon Cloud and any resources allowlisted in the Containment Policy

NO.37 Which is the correct order for manually installing a Falcon Package on a macOS system?
* Install the Falcon package, then register the Falcon Sensor via the registration package
* Install the Falcon package, then register the Falcon Sensor via command line
* Register the Falcon Sensor via command line, then install the Falcon package
* Register the Falcon Sensor via the registration package, then install the Falcon package

NO.38 When a Linux host is in Reduced Functionality Mode (RFM) what telemetry and protection is still offered?
* The sensor would provide protection as normal, without event telemetry
* The sensor would provide minimal protection
* The sensor would function as normal
* The sensor provides no protection, and only collects Sensor Heart Beat events

Explanation

When a Linux host is in Reduced Functionality Mode (RFM), the sensor would provide minimal protection.

RFM is a mode that limits the sensor’s functionality due to license expiration, network connectivity loss, or certificate validation failure. When a Linux sensor is in RFM, it will only provide basic prevention capabilities, such as blocking known malware hashes and preventing script execution from the /tmp directory. The sensor will not send any telemetry or detection events to the Falcon platform, and will not receive any policy or update changes from the Falcon cloud1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NO.39 What is the name for the unique host identifier in Falcon assigned to each sensor during sensor installation?
* Endpoint ID (EID)
* Agent ID (AID)
* Security ID (SID)
* Computer ID (CID)

NO.40 Once an exclusion is saved, what can be edited in the future?
* All parts of the exclusion can be changed
* Only the selected groups and hosts to which the exclusion is applied can be changed
* Only the options to “Detect/Block” and/or “File Extraction” can be changed
* The exclusion pattern cannot be changed

NO.41 Which is a filter within the Host setup and management > Host management page?
* User name

* OU
* BIOS Version
* Locality

Explanation

OU (organizational unit) is a filter within the Host setup and management > Host management page. The Host management page allows you to view and manage all the hosts in your environment that have Falcon sensors installed. You can filter the hosts by hostname, group, OS version, sensor version, last seen date, health events, detections, and preventions. You can also filter by OU, which is a logical grouping of hosts based on their Active Directory domain structure1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

NO.42 On which page of the Falcon console can one locate the Customer ID (CID)?

* Hosts Management
* API Clients and Keys
* Sensor Dashboard
* Sensor Downloads

Explanation

The page of the Falcon console where one can locate the Customer ID (CID) is API Clients and Keys. The API Clients and Keys page allows you to create and manage API clients and keys for accessing the Falcon platform programmatically. The Customer ID (CID) is a unique identifier for your organization that is required for authenticating your API requests. You can find your CID at the top of the API Clients and Keys page2.

References: 2: Cybersecurity Resources | CrowdStrike

NO.43 What information does the API Audit Trail Report provide?

* A list of analyst login activity
* A list of specific changes to prevention policy
* A list of actions taken via Falcon OAuth2-based APIs
* A list of newly added hosts

Explanation

The information that the API Audit Trail Report provides is a list of actions taken via Falcon OAuth2-based APIs.

The API Audit Trail Report allows you to view and audit the activity and usage of the Falcon APIs by different API clients and users in your organization.

You can use this report to monitor who accessed what data, when, and how via the Falcon APIs2.

References: 2: Cybersecurity Resources | CrowdStrike

NO.44 Which of the following is TRUE of the Logon Activities Report?

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

NO.45 Which of the following options is a feature found ONLY with the Sensor-based Machine Learning (ML)?

* Next-Gen Antivirus (NGAV) protection

* Adware and Potentially Unwanted Program detection and prevention
* Real-time offline protection
* Identification and analysis of unknown executables

NO.46 You have a Windows host on your network in Reduced functionality mode (RFM). While the system is in RFM, which of the following is TRUE?
* System monitoring will be unavailable
* Event reporting will be unavailable
* Prevention patterns will not be triggered
* Some detection patterns and preventions will not be triggered

Explanation

The option that is true when a Windows host is in Reduced Functionality Mode (RFM) is that some detection patterns and preventions will not be triggered. RFM is a mode that limits the sensor’s functionality due to license expiration, network connectivity loss, or certificate validation failure. When a Windows sensor is in RFM, it will only provide basic prevention capabilities, such as blocking known malware hashes and preventing script execution from the %TEMP% directory. The sensor will not send any telemetry or detection events to the Falcon platform, and will not receive any policy or update changes from the Falcon cloud. This means that some detection patterns and preventions that rely on telemetry, machine learning, or cloud analysis will not be triggered.

References: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

NO.47 You have been asked to troubleshoot why Script Based Execution Monitoring (SBEM) is not enabled on a Falcon host. Which report can be used to determine if this is an issue with an old prevention policy?
* Host Update Status Report
* Custom Alerting Audit Trail
* Prevention Policy Debug
* SBEM Debug Report

Explanation

The report that can be used to determine if Script Based Execution Monitoring (SBEM) is not enabled on a Falcon host due to an old prevention policy is Prevention Policy Debug. The Prevention Policy Debug report allows you to view and compare the prevention policy settings applied to each host in your environment. You can use this report to identify any hosts that have outdated or inconsistent prevention policy settings, such as SBEM, which is a feature that monitors and prevents malicious script execution on Windows systems1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike