CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

Certified Identity Specialist CCIS Exam Guide

Description

The CrowdStrike Certified Identity Specialist (CCIS) exam is the final step toward the completion of CCIS certification. This exam evaluates a candidate's knowledge, skills and abilities to manage domain security with identity-based solutions, administer policy rules and actions, automate responses to identity threats, and manage risk across the authentication landscape in the domain.

A successful CrowdStrike Certified Identity Specialist:

- Understands the tenets of identity protection and Zero Trust
- Enforces policies and policy rules to protect against identity-based risks
- Investigates identity-based detections and incidents
- Configures and maintains connectors between Falcon Identity Protection and MFA/IDAAS
- Assesses and manages user risk
- Implements authentication and security best practices for network segments in the domain
- Performs proactive threat hunting on identity-based detections
- Manages the overall identity-based security posture of the domain
- Tunes detection settings, risk configurations and more to customize Falcon Identity Protection for their domain

CrowdStrike Certification Program

Requirements

All exam registrants must (without exception):

- Accept the **CrowdStrike Certification Exam Agreement**
- Be at least 18 years of age
- Purchase a CrowdStrike exam voucher

Contact your CrowdStrike Account Executive to request a quote or purchase a CrowdStrike exam voucher through Pearson VUE.

University Subscription

It is **strongly suggested** that all exam registrants have an active subscription to CrowdStrike University and have confirmed access to their CrowdStrike University account.

- CrowdStrike certification-aligned courses are available to learners with an active CrowdStrike University account.
- A unique CrowdStrike Certification ID, training transcripts and printable certification documents are available through CrowdStrike University learning management system.

NOTE: All exam takers can view and print their CrowdStrike certification exam score report through Pearson VUE.

Required Certification Candidate Competence and Abilities

- Candidates should have at least six (6) months of experience with CrowdStrike Falcon in a production environment.
- Candidates should read English with sufficient accuracy and fluency to support comprehension. Exams are suitable for non-native English speakers.

About the Exam

Assessment Method

The CCIS exam is a 90-minute, 60-question assessment. Exam questions have been specifically written in a way that eliminates tricky wording and/or double negative questions. This exam passed several rounds of editing by both technical and non-technical experts and has been tested by a wide variety of candidates.

Initial Certification

To be eligible for certification, candidates must:

- Achieve passing score on the CCIS certification exam
- Refrain from any misconduct

In the event of misconduct by the candidate, CrowdStrike may invalidate the score and consider any suspicious action a violation of the **CrowdStrike Certification Exam Agreement**.

When a candidate has completed the exam and the candidate's official exam score has been posted, the certification candidate may view the official exam score at Pearson VUE.

Retake Policy

Candidates who do not pass an exam on their first (1st) attempt:

- Must wait 24 hours to retake the exam (wait time begins after the exam)
- Should review the exam objectives, training course materials and associated recommended reading listed in this document.

After the second (2nd) attempt, a candidate will need to wait seven (7) days for the third (3rd) attempt and any subsequent attempts. Wait time begins the day after the attempt.

Candidates that want to retake the exam should consider re-sitting the applicable recommended course(s) and gain additional experience with CrowdStrike Falcon before trying again.

Retakes beyond the fourth (4th) attempt will be considered on a case-by-case basis. CrowdStrike reserves the right to deny a retake beyond the fourth attempt.

Retaking Previously Passed Exams

Candidates will not be permitted to retake any exam they have previously passed unless directly related to a recertification requirement approved by CrowdStrike.

Beta Exams

Candidates will not be permitted to retake beta exams.

Exam Challenge

If a certification candidate believes there is an error on an exam or that specific questions on the CCFA exam are invalid, contact certification@crowdstrike.com to request an evaluation of your claim. The certification candidate must submit a claim within three (3) days of taking the exam for it to be considered. CrowdStrike will generally respond to your submission within fifteen (15) business days.

Recertification

Certification exams are not tied to product versions. The following life cycle will apply to recertification moving forward, beginning with the date the certification was issued:

- CrowdStrike Certified Falcon Administrator (CCFA): 3 years
- CrowdStrike Certified Falcon Responder (CCFR): 3 years
- CrowdStrike Certified Falcon Hunter (CCFH): 3 years
- CrowdStrike Certified Cloud Specialist (CCCS): 3 years
- CrowdStrike Certified Identity Specialist (CCIS): 3 years

Exam Preparation

Recommended Training

CrowdStrike strongly recommends certification candidates complete the **CSU LP-IP: Identity Specialist** courses in CrowdStrike University to prepare for the CCCS exam. To learn more about these courses, view the **CrowdStrike Training Catalog**.

Recommended Reading

CrowdStrike strongly recommends certification candidates review the following CrowdStrike Falcon support documentation titles to prepare for the CCIS exam:

- Identity Protection Overview
- Identity-based Incidents, Detections, and Risks
- Identity Protection Reports
- Identity Protection System Notifications
- Identity Protection Insights
- Identity Protection Threat Hunter
- Identity Protection Administration
- Identity Protection Policy
- Identity Protection in Falcon Fusion Workflows
- Integrating Identity Protection with AD FS
- Integrating Identity Protection with PingFederate
- Identity Protection APIs
- Zero Trust Assessment

Exam Scope

The following topics provide a general guideline for the content likely to be included on the exam; however, other related topics may also appear on any specific delivery of the exam.

1. Zero Trust Architecture
2. Identity Protection Tenets
3. Falcon Identity Protection Fundamentals
4. Domain Security Assessment
5. Risk Assessment
6. User Assessment
7. Threat Hunting and Investigation
8. Risk Management with Policy Rules
9. Configuration and Connectors
10. MFA and IDAAS Configuration Basics
11. Falcon Fusion for Identity Protection
12. GraphQL API

Scope Changes

To better reflect the content of the exam and for clarity purposes, the guidelines below may change at any time without notice. Such changes may include, without limitation, adding or deleting an available CrowdStrike certification, modifying certification requirements, and making changes to recommended training courses, testing objectives, outline and exams, including, without limitation, how and when exam scores are issued. The certification candidate agrees to meet (and continue to meet) the program requirements, as amended, as a condition of obtaining and maintaining the certification.

Exam Objectives

The following subtopics and learning objectives provide further guidance on the content and purpose of the exam:

1.0 Zero Trust Architecture

- **1.1** Describe what the NIST SP 800-207 framework for Zero Trust architecture defines
- **1.2** Describe the security need and impetus for the Zero Trust architecture
- **1.3** Describe the implementation of the Zero Trust architecture within Falcon Identity Protection
- **1.4** Describe the fundamental principles of Zero Trust (continuous validation, etc.)
- **1.5** Describe the difference between a traditional "wall-and-moat" security model and a modern Zero Trust model
- **1.6** Describe some of the key use cases for Falcon Zero Trust
- **1.7** Describe how a Falcon user's Zero Trust Assessment (ZTA) score is calculated

2.0 Identity Protection Tenets

- **2.1** Describe the identity protection architecture employed at CrowdStrike as a part of the Falcon Identity Protection platform
- **2.2** Describe how Falcon Identity Protection inspects traffic in the domain
- **2.3** Describe how Falcon Identity Protection complements traditional EDR solutions
- **2.4** Describe how Falcon Identity Protection helps secure against the human elements of security vulnerability
- **2.5** Describe how Falcon Identity Protection empowers the team to mitigate and prevent identity-based exploits and attacks
- **2.6** Identify key differences between Falcon Identity Protection log-free detections and traditional EDR solutions
- **2.7** Describe the threat landscape and the need for identity-based security solutions

3.0 Falcon Identity Protection Fundamentals

- **3.1** Identify the menu categories (monitor, enforce, explore and configure) of Falcon Identity Protection
- **3.2** Describe the contents of each menu category (monitor, enforce, explore and configure) within Falcon Identity Protection
- **3.3** Identify the goal of each menu category (monitor, enforce, explore and configure)
- **3.4** Recognize the availability of specific tools limited by product subscription for Identity Threat Detection vs. Identity Threat Protection (ITD vs. ITP)
- **3.5** Describe the purpose of Falcon Identity Protection in general security terms

- **3.6** Explain how Falcon Identity Protection works to mitigate threats that bypass traditional MITRE ATT&CK framework vectors
- **3.7** Describe the Falcon roles working within Falcon Identity Protection and the features available to those roles

4.0 Domain Security Assessment

- **4.1** Explain what the Risk Score represents in the domain
- **4.2** Describe how the Score Trend is represented and how to affect the score
- **4.3** Explain the Risk Matrix and how risks are represented
- **4.4** Describe how to lower the domain risk score
- **4.5** Explain and describe how to prioritize addressing risks in the domain
- **4.6** Describe where Falcon Identity Protection fits in the security model
- **4.7** Explain the factors that contribute to the domain risk score
- **4.8** Describe what "Severity," "Likelihood" and "Consequence" mean in terms of potential risk factors related to identity
- **4.9** Define the goals in the Domain Security overview and how they relate to identity protection outcomes
- **4.10** Describe how to change the "Goal" and what each goal in the domain security overview is geared toward
- **4.11** Describe how to change "Scope" and what that does for the Overview dashboard

5.0 Risk Assessment

- **5.1** Describe the categories of entity risk (low, medium, high) and their thresholds
- **5.2** Demonstrate how to move a user from higher to lower risk
- **5.3** Describe the elements that contribute to higher Risk Scores
- **5.4** Explain the Risk Analysis dashboard
- **5.5** Explain the Event Analysis dashboard
- **5.6** Apply filters for targeted risk analysis
- **5.7** Explain how to generate custom insights with filters
- **5.8** Describe how to create a custom report
- **5.9** Explain the difference of when one creates a custom insight versus a custom report
- **5.10** Describe how to export and schedule custom reports

6.0 User Assessment

- **6.1** Describe the attributes and data points associated with users in Falcon Identity Protection
- **6.2** Explain the difference between a user, an endpoint and an entity

- **6.3** Describe the difference between human and programmatic accounts
- **6.4** Describe the icons and their meaning when identifying users
- **6.5** Explain what the default insights do in the Users view
- **6.6** Explain how to create custom filters in the Users view
- **6.7** Describe how high-risk users are baselined
- **6.8** Explain the risk baselining process and various timelines needed for accurate baselines
- **6.9** Describe the various risky types of accounts (stale, never logged in, compromised password etc.) and the risks they pose
- **6.10** Explain how to add custom lists to the Compromised Password directory
- **6.11** Explain what risks users with elevated privileges pose and how to assess those users
- **6.12** Explain the user watchlist and honeytoken accounts
- **6.13** Describe the use cases for a honeytoken account

7.0 Threat Hunting and Investigation

- **7.1** Describe an identity-based detection
- **7.2** Describe an identity-based incident
- **7.3** Describe the investigation pivots available from an identity-based incident
- **7.4** Explain the difference between an identity-based incident and detection
- **7.5** Describe how to pivot to related entities
- **7.6** Explain how to navigate an identity-based incident tree
- **7.7** Describe the evolution of an incident over time as more detections accumulate
- **7.8** Describe the information contained in the different types of identity-based detections
- **7.9** Explain the key information highlighted in various detections
- **7.10** Describe how to filter and search for detections
- **7.11** Demonstrate how to investigate the history of an incident and potential incident type changes
- **7.12** Explain how to enable/disable detection exclusions
- **7.13** Describe how to add exceptions to detection exclusions
- **7.14** Describe the logic behind detection exclusions
- **7.15** Describe the use cases for enabling or disabling detection types
- **7.16** Describe the difference between a detection-based risk and an analysis-based risk

8.0 Risk Management with Policy Rules

- **8.1** Describe the purpose of policy rules and policy groups
- **8.2** Demonstrate the policy rule creation process
- **8.3** Explain the purpose of the various triggers and conditions within a policy rule
- **8.4** Explain how to enable and disable policy rules

- **8.5** Explain how to group, ungroup and manage groups of rules
- **8.6** Describe how to apply any changes made to policy rules
- **8.7** Describe the Falcon role(s) necessary to write and manage policy rules

9.0 Configuration and Connectors

- **9.1** Describe how to monitor the domain controllers (DCs) in the domain (visibility into the DCs reporting and endpoints per DC)
- **9.2** Describe how to create and manage subnets
- **9.3** Explain how to enforce policy rules using subnets
- **9.4** Explain the risk configuration settings
- **9.5** Describe how to add exceptions to risk configurations
- **9.6** Explain the two types of connectors (MFA, IDaaS)
- **9.7** Explain the two types of MFA connectors (Cloud MFA, On-Premises RADIUS MFA)
- **9.8** IIdentify the supported MFA and IDaaS connectors
- **9.9** Describe where to find connector setup documentation
- **9.10** Describe how to enable authentication traffic inspection (ATI) on DCs in the domain
- **9.11** Describe the available configuration options within Falcon Identity Protection policies as it relates to data captured by the Falcon sensor
- **9.12** Describe what business privileges are, and how they impact entities
- **9.13** Explain how configured blocklisted/allowlisted countries impact detections

10.0 Multi-factor Authentication (MFA) and Identity-as-a-service (IDaaS) Configuration Basics

- **10.1** Explain how to access the IDaaS and MFA configuration settings
- **10.2** Explain the configuration fields associated with the various connectors
- **10.3** Describe how to configure the settings for MFA connectors
- **10.4** Describe how to enable third-party MFA for Falcon Identity Protection
- **10.5** Describe how Falcon Identity Protection extends on capabilities of existing MFA providers and does not intend to replace it

11.0 Falcon Fusion for Identity Protection

- **11.1** Describe the building blocks of a Falcon Fusion workflow
- **11.2** Explain how to define triggers
- **11.3** Explain how to add conditions
- **11.4** Explain what various conditions do and how to combine them to limit the scope of a workflow
- **11.5** Describe how to create custom, templated, scheduled and on-demand workflows

- **11.6** Describe how to create branching workflows and loops
- **11.7** Create workflows in Falcon Fusion to accomplish specific goals
- **11.8** GraphQL API

12.0 Describe where you can find Identity API (GraphQL) documentation

- **12.1** Create an API key specific to Falcon Identity Protection
- **12.2** Describe the differences between the different Falcon Identity Protection API permissions
- **12.3** Pivot from a Threat Hunter search into GraphQL
- **12.4** Build a simple query that returns all privileged users with high risk