servicenow

ServiceNow Certified Implementation Specialist – Security Incident Response 試験仕様書

San Diego リリース – 2022 年 3 月 30 日更新

servicenow

はじめに

この ServiceNow Certified Implementation Specialist – Security Incident Response 試験仕様は、試験の目的、対象者、テストオプション、試験内容と範囲、試験の枠組みに加えて、Certified Implementation Specialist – Security Incident Response の認定を得るための前提条件を定めたものです。

試験の目的

Certified Implementation Specialist – Security Incident Response 試験は、ServiceNow Security Incident Response 実装の構成、実装、メンテナンスに役立つスキルと重要な知識を合格者が備えていることを認定するものです。

試験対象者

Certified Implementation Specialist – Security Incident Response 試験は、ServiceNow のお客様、パートナー、従業員のほかに、 ServiceNow Certified Implementation Specialist – Security Incident Response となることに興味のある方を対象としています。

試験準備

試験の問題は、公式の ServiceNow トレーニング教材、 ServiceNow Security Incident Response - ServiceNow ドキュメントサイト、ServiceNow 開発者サイトに基づいています。オンラインで公開されているその他の学習教材は公式ではなく、試験準備用としては推奨されません。

ServiceNow トレーニングパスの前提条件

Certified Implementation Specialist – Security Incident Response 試験の準備として、以下の前提トレーニングコースを完了する必要があります。以下の ServiceNow トレーニングコースで提供される情報には、試験のソース資料が含まれています。

- Security Operations Fundamentals
- Security Incident Response Implementation

Now Learning の CIS-SIR の認定パスを参照してください。

Security Incident Response Implementation コースを完了すると、Certified Implementation Specialist – Security Incident Response 試験に登録するためのバウチャーコード (譲渡不可) を取得または購入する資格が得られます。

推奨される知識および教育

試験の準備として、以下のトレーニングコースの完了と認定の取得を推奨します。

- ServiceNow Fundamentals
- ServiceNow Platform Implementation
- Automated Test Framework Fundamentals
- Flow Designer Essentials
- IntegrationHub Essentials
- Mobile Development Essentials
- Service Portal Fundamentals
- Common Service Data Model Fundamentals
- Configuration Management Database Fundamentals
- Now Experience UI Builder Fundamentals
- Configuration Compliance Essentials
- What's New in the Store for Security Operations

その他のリソース

上記に加えて、以下の追加リソースが試験準備に役立つ場合があります。

- Candidate Journey Guide – 認定プロセス全体をガイドするリソース

- San Diego Security Operations ドキュメント
- San Diego Security Incident Response ドキュメント
- Security Operations Community Forum

推奨されるその他の経験

- ServiceNow Security Incident Response 展開プロジェクトまたは ServiceNow インスタンスでの ServiceNow Security Incident Response アプリケーションスイートのメンテナンスに参加した 3 ～ 6 か月間の現場体験
- 業界の用語、略語、頭文字語についての一般的な知識

試験範囲

試験の内容は、重要なトピックと ServiceNow 実装中に行うアクティビティに対応する学習分野ごとに分かれています。それぞれの学習分野において、具体的な学習目標が示され、試験内でテストされます。

以下の表に、この試験で評価される学習分野、重み付け、サブトピックと、各分野の問題が占める割合 (%) を示します。記載したサブスキルは試験内容に含まれますが、これらに限定されるわけではありません。

	学習分野	試験における割合 (%)
1	**Security Incident Response の概要** • Security Incident Response について • データの可視化 • お客様の目標を理解して期待に応える	**15%**
2	**セキュリティインシデントの探索と Threat Intelligence** • セキュリティインシデントを作成する方法の理解 • Threat Intelligence の理解 • MITRE ATT&CK フレームワーク	**14 %**
3	**セキュリティインシデントと Threat Intelligence データ連携** • ServiceNow ストアおよび共有 • 構築済みデータ連携の管理 • カスタム統合の作成	**14 %**
4	**Security Incident Response の管理** • セキュリティアナリストワークスペース • Standard Automated Assignment Options • エスカレーションパスの定義 • セキュリティタグ • プロセス定義と選択	**15 %**
5	**リスク計算とインシデントの事後応答** • セキュリティインシデント算出グループおよびリスクスコア • インシデントの事後レビュー	**12 %**
6	**セキュリティインシデントの自動化** • 自動 Security Incident Response の概要 • フローとワークフローを使用したセキュリティインシデントの自動化 • Playbook の自動化 (ナレッジ記事と Runbook) • ユースケース: ユーザーから報告されたフィッシング v2	**30 %**
	合計	**100 %**

試験の登録

ServiceNow は、Webassessor プラットフォームを使用して試験の登録を行う Kryterion と提携しています。メインライン試験は、Kryterion のテストセンターまたはオンライン (Kryterion の監督者が試験予約を監視する) で受けることができます。

試験に登録するには、Webassessor アカウントを作成し、自分の Now Learning アカウントにリンクする必要があります。

ServiceNow は、障害のある方または英語を第 2 言語とする方 (ESL) のために、資格試験の受験期間中に合理的な配慮を行います。

servicenow

注：特別な設備を用意した試験を提供しています。詳細については、certification@servicenow.com までお問い合わせください。設備の種類によっては、試験まで 30 日間のリードタイムをいただく場合があります。

試験の構成

この試験は 45 問の問題で構成されています。

複数の選択肢 (解答は 1 つ)

複数の選択肢がある問題では、4 つ以上の解答候補が提示されます。受験者は解答の選択肢を確認して、問題の解答として最も正しいものを選択します。

複数選択式問題 (該当するものをすべて選択)

複数の解答を選択する問題では、4 つ以上の解答候補が提示されます。解答をいくつ選択すればよいかは、問題に記載されています。受験者は解答の選択肢を確認して、問題の解答として正しいものをすべて選択します。部分点は与えられません。

試験結果

試験を完了して送信すると、すぐに合否結果が計算されて表示されます。

受験者へのより詳しい結果の提供は行われません。

再受験

不合格だった場合、バウチャーがなくても再受験できます。Webassessor で試験の登録と支払いを行います。詳細については、『Candidate Journey Guide』の「試験の管理ポリシー > 再試験」を参照してください。

例題

例題 1：次のうち、Security Incident Response アプリケーションをインストールするために必要なロールはどれか？

A. *sn_si.admin*
B. *admin*
C. *sn_sec_cmn.admin*
D. *sn_si.write*

正解：B

例題2：次のうち、Security Incident Response の定義として適切なものはどれか？

A. *セキュリティインシデントおよび差し迫ったセキュリティ脅威を緩和するために実行されるアクション計画*
B. *セキュリティインシデントカタログから生成された要求を満たすために実行される変更計画*
C. *セキュリティインシデントを捕捉して記録するために実行される対応計画*
D. *差し迫ったセキュリティ脅威に対処するために実行される対応計画*

正解：A

例題3: 構築済みの統合があるのはどの ServiceNow モジュールか？

A. *統合*
B. *サイティング検索構成*
C. *データ連携設定*
D. *データ連携ステータス*

正解：C

例題4：Security Incident Response アプリケーションのデフォルトとしてどのプロセス定義が設定されているか？

A. *NIST Open*
B. *SANS Open*
C. *SANS Stateful*
D. *NIST Stateful*

正解：D

例題5: 次のうち、セキュリティインシデント算出ツールの使用目的に関する記述として最も適切なものはどれか？

A. *一致した条件に従って特定の値を設定する*
B. *セキュリティインシデントリスクスコアを決定する*
C. *インシデントのコストを計算する*
D. *さまざまなインシデント状態での経過時間を計算する*

正解：A

例題6：フローは、何が満たされたときに実行されるか？

A. *トリガー条件*
B. *IntegrationHub アクティベーション*
C. *応答タスクステータスがアクティブであること*
D. *NIST 準備完了ステータス*

正解：A

例題7：3 人の主要な Security Incident Response レポート対象者を次の中から特定しなさい。

A. セキュリティアナリスト
B. セキュリティマネージャ
C. CIO/CISO
D. 施設管理者
E. 人事マネージャー

正解：A、B、C

詳細情報

www.servicenow.com