servicenow

ServiceNow Zertifizierter Implementierungsspezialist – Security Incident Response Prüfungsspezifikation

Release San Diego – Aktualisiert am 30. März 2022

servicenow

Einführung

Die Spezifikation der Prüfung zum von ServiceNow zertifizierten Implementierungsspezialisten für Security Incident Response definiert Zweck, Zielgruppe, Testoptionen, Prüfungsinhalte, Test-Framework und Voraussetzungen, die erfüllt sein müssen, um zertifizierter Implementierungsspezialist für Security Incident Response zu werden.

Zweck der Prüfung

Durch eine erfolgreiche Prüfung zum zertifizierten Implementierungsspezialisten für Security Incident Response wird der Nachweis erbracht, dass die Kandidaten über die nötigen Kompetenzen und die wichtigsten Kenntnisse verfügen, um bei der Konfiguration, Implementierung und Wartung von ServiceNow Security Incident Response mitzuwirken.

Zielgruppe der Prüfung

Die Prüfung zum zertifizierten Implementierungsspezialisten für Security Incident Response steht Kunden, Partnern und Mitarbeitern von ServiceNow ebenso wie anderen Personen offen, die daran interessiert sind, von ServiceNow zertifizierter Implementierungsspezialist für Security Incident Response zu werden.

Prüfungsvorbereitung

Die Prüfungsfragen beruhen auf offiziellen Schulungsmaterialien, der Website mit der ServiceNow-Dokumentation zu ServiceNow Security Incident Response und der Developer Site von ServiceNow. Lernmaterialien, die an anderer Stelle online veröffentlicht werden, sind inoffiziell und sollten nicht zur Vorbereitung auf die Prüfung verwendet werden.

Von ServiceNow als Prüfungsvoraussetzung angegebener Schulungspfad

Zur Vorbereitung auf die Prüfung zum zertifizierten Implementierungsspezialisten – Security Incident Response setzt ServiceNow die Absolvierung folgender obligatorischer Schulungen voraus. Informationen in folgenden ServiceNow-Schulungskursen enthalten Quellmaterial für diese Prüfung.

- Security Operations – Grundlagen
- Security Incident Response – Implementierung

Besuchen Sie den Zertifizierungspfad für CIS-SIR in Now Learning.

Nach Abschluss des Kurses „Security Incident Response – Implementierung“ haben Kandidaten Anrecht auf Erhalt oder Kauf eines nicht übertragbaren Gutscheincodes für die Registrierung zur Prüfung zum zertifizierten Implementierungsspezialisten für Security Incident Response.

Empfohlene Kenntnisse und Schulungen

Zur Vorbereitung auf die Prüfung empfiehlt ServiceNow den Abschluss der folgenden Schulungen und Zertifizierungen.

- ServiceNow – Grundlagen
- Now Platform – Implementierung
- Automated Test Framework – Grundlagen
- Flow Designer – Grundlagen
- IntegrationHub – Grundlagen
- Mobile Development – Grundlagen
- Service Portal – Grundlagen
- Common Service Data Model – Grundlagen
- Configuration Management Database – Grundlagen
- Now Experience UI Builder – Grundlagen
- Configuration Compliance – Grundlagen
- Was ist neu im Store für Security Operations?

Zusätzliche Ressourcen

Außerdem können die folgenden zusätzlichen Ressourcen nützlich für die Kandidaten bei der Vorbereitung auf die Prüfung sein.

- Leitfaden für Kandidaten – eine Ressource, die Sie durch den gesamten Zertifizierungsprozess führt

- Dokumentation zu San Diego Security Operations
- Dokumentation zu San Diego Security Incident Response
- Security Operations – Community-Forum

Sonstige empfohlene Erfahrung

- Drei (3) bis sechs (6) Monate praktische Erfahrung durch Teilnahme an einem Bereitstellungsprojekt für ServiceNow Security Incident Response oder durch Wartung der Security Incident Response-Anwendungssuite in einer ServiceNow-Instanz
- Allgemeine Vertrautheit mit branchenüblichen Begriffen, Akronymen und Abkürzungen

servicenow

Prüfungsumfang

Der Prüfungsinhalt ist in Lernbereiche unterteilt. Diese entsprechen den wichtigsten Themen und Aktivitäten, die bei ServiceNow-Implementierungen vorkommen. In jedem Lernbereich wurden spezifische Lernziele bestimmt, die in der Prüfung getestet werden.

Die folgende Tabelle zeigt die Lernbereiche, Gewichtungen und Unterthemen, die bei dieser Prüfung ausgewertet werden, und den Prozentsatz der Fragen, die auf die einzelnen Bereiche entfallen. Die aufgeführten Unterkompetenzen sind NICHT als vollständige Liste der Prüfungsinhalte zu verstehen.

	Lernbereich	% der Prüfung
1	**Security Incident Response – Übersicht** • Einführung in Security Incident Response • Datenvisualisierung • Kundenziele verstehen und Kundenerwartungen erfüllen	**15 %**
2	**Security Incidents und Threat Intelligence erkunden** • Erstellung von Security Incidents • Threat Intelligence verstehen • MITRE-ATT&CK-Framework	**14 %**
3	**Integrationen für Security Incident und Threat Intelligence** • ServiceNow Store und Freigabe • Verwaltung vorgefertigter Integrationen • Benutzerdefinierte Integrationen erstellen	**14 %**
4	**Verwaltung von Security Incident Response** • Security Analyst Workspace • Standardoptionen für die automatisierte Zuweisung • Definition von Eskalationspfaden • Sicherheits-Tags • Prozessdefinitionen und -auswahl	**15 %**
5	**Risikoberechnungen und Reaktion nach Incidents** • Rechnergruppen und Risikopunktzahlen für Security Incidents • Überprüfungen nach Incidents	**12 %**
6	**Security Incident – Automatisierung** • Automatisierung von Security Incident Response – Übersicht • Security Incident – Automatisierung mit Flows und Workflows • Playbook-Automatisierung (Wissensartikel und Runbooks) • Anwendungsfall: Von Benutzer gemeldetes Phishing v2	**30 %**
	Gesamt	**100 %**

Prüfungsregistrierung

ServiceNow arbeitet mit Kryterion zusammen und nutzt zur Prüfungsregistrierung deren Plattform Webassessor. Unsere Mainline-Prüfungen werden in Kryterion-Prüfungszentren angeboten oder können überall online abgelegt werden, während eine Kryterion-Aufsichtsperson den Prüfungstermin überwacht.

Um sich für eine Prüfung registrieren, müssen Sie ein Webassessor-Konto erstellen und dieses mit Ihrem Now Learning-Konto verknüpfen.

Für Personen mit Behinderung oder Englisch als Zweitsprache bietet ServiceNow angemessene Vorkehrungen für die Teilnahme an der Zertifizierungsprüfung.

HINWEIS: Es ist eine Prüfungsversion für Personen verfügbar, die spezielle Vorkehrungen benötigen. Weitere Informationen erhalten Sie unter certification@servicenow.com. Je nach Art der besonderen Vorkehrungen ist eine 30-tägige Vorlaufzeit vor der Prüfung erforderlich.

Aufbau der Prüfung

Die Prüfung besteht aus 45 Fragen.

Multiple-Choice (eine Antwort)

Bei jeder Multiple-Choice-Frage in der Prüfung gibt es mindestens vier Antwortmöglichkeiten. Die Prüfungskandidaten sehen sich die Antwortmöglichkeiten an und wählen die zutreffendste Antwort auf die Frage aus.

Mehrfachauswahl (alle zutreffenden Antworten auswählen)

Für jede Prüfungsfrage mit Mehrfachauswahl gibt es mindestens vier Antwortmöglichkeiten. In der Frage wird angegeben, wie viele Antworten auszuwählen sind. Prüfungskandidaten sehen sich die Antwortmöglichkeiten an und wählen ALLE zutreffenden Antworten auf die Frage aus. Eine Teilgutschrift ist nicht vorgesehen.

Prüfungsergebnisse

Nach Abschluss und Übermittlung der Prüfung wird sofort berechnet, ob das Ergebnis „Bestanden“ oder „Nicht bestanden“ ist, und das Ergebnis wird den Kandidaten angezeigt.

Die Kandidaten erhalten keine genaueren Informationen über die Ergebnisse.

Wiederholungsprüfungen

Wenn ein Kandidat eine Prüfung nicht besteht, ist kein Gutschein erforderlich, um die Prüfung zu wiederholen. Anmeldung und Bezahlung für die Prüfung erfolgen in

Webassessor. Weitere Informationen finden Sie in der Wiederholungsrichtlinie des Leitfadens für Kandidaten.

Beispielfragen

Beispielelement Nr. 1: Welche Rolle ist erforderlich, um die Anwendung Security Incident Response zu installieren?

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

Richtige Antwort: B

Beispielelement Nr. 2: Security Incident Response lässt sich definieren als:

A. *Aktionsplan zur Minimierung von Security Incidents und sich abzeichnenden Sicherheitsbedrohungen*
B. *Change-Plan zum Erfüllen von Anforderungen, die durch den Security Incident-Katalog ausgelöst wurden*
C. *Reaktionsplan, der zur Erfassung und Aufzeichnung von Security Incidents eingeführt wurde*
D. *Antwortplan zur Reaktion auf bevorstehende Sicherheitsbedrohungen*

Richtige Antwort: A

Beispielelement Nr. 3: In welchem ServiceNow-Modul finden Sie vorgefertigte Integrationen?

A. *Integrationen*
B. *Sichtungssuche – Konfiguration*
C. *Integrationskonfigurationen*
D. *Integrationsstatus*

Richtige Antwort: C

Beispielelement Nr. 4: Welche Prozessdefinition gilt standardmäßig für die Anwendung Security Incident Response?

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

Richtige Antwort: D

Beispielelement Nr. 5: Welche der folgenden Aussagen beschreibt am besten, wofür Security Incident-Rechner verwendet werden?

A. *Festlegung bestimmter Werte anhand von abgeglichenen Bedingungen*
B. *Festlegung der Risikopunktzahl von Security Incidents*
C. *Berechnung der Kosten eines Incidents*
D. *Berechnung der Zeit, die ein Incident in seinen verschiedenen Status verbracht hat*

Richtige Antwort: A

Beispielelement Nr. 6: Bei Erfüllung welcher Bedingung wird ein Flow ausgeführt?

A. *Auslöserbedingung*
B. *IntegrationHub-Aktivierung*
C. *Status der Antwortaufgabe „Aktiv“*
D. *NIST-Status „Bereit“*

Richtige Antwort: A

Beispielelement Nr. 7: Nennen Sie drei wichtige Zielgruppen für die Berichterstellung in Security Incident Response:

A. *Sicherheitsanalysten*
B. *Sicherheitsmanager*
C. *CIOs/CISOs*
D. *Facilities-Manager*
E. *Human Resources-Manager*

Richtige Antworten: A, B, C

Weitere Informationen:

www.servicenow.com