servicenow

ServiceNow Certified Implementation Specialist - Security Incident Response Exam Specification

Paris Release – Updated October 1, 2020

servicenow

Introduction

The ServiceNow Certified Implementation Specialist - Security Incident Response Exam Specification defines the purpose, audience, testing options, exam content coverage, test framework, and prerequisites to become Certified Implementation Specialist - Security Incident Response certified.

Exam Purpose

The Certified Implementation Specialist - Security Incident Response exam certifies that a successful candidate has the skills and essential knowledge to implement Security Incident Response applications.

Exam Audience

The Certified Implementation Specialist - Security Incident Response exam is available to ServiceNow customers, partners, employees, and others interested in becoming a ServiceNow Certified Implementation Specialist - Security Incident Response.

Exam Preparation

Exam questions are based on official ServiceNow training materials for both required prerequisite and required courses, the ServiceNow documentation site, and the ServiceNow developer site. Study materials posted elsewhere online are not official and should not be used to prepare for the examination.

Prerequisite ServiceNow Training Path

ServiceNow requires the completion of the following prerequisite training course(s) in preparation for the Certified Implementation Specialist - Security Incident Response exam. Information provided in the following ServiceNow training course(s) contain source material for the exam.

- ServiceNow Fundamentals
- ServiceNow Get Started with Now Create
- ServiceNow Platform Implementation
- CMDB Fundamentals
- Security Operations (SecOps) Fundamentals
- Security Incident Response (SIR) Implementation - *Upon completion, the candidate will be eligible to collect a voucher for the Certified Implementation Specialist - Security Incident Response exam.

Recommended Knowledge & Education

ServiceNow recommends completion of the following Training Course(s) and Certification(s) in preparation for the exam.

- Certified System Administrator
- CIS-Security Incident Response Certification Test Prep
- Automated Test Framework (ATF) Fundamentals
- Flow Designer Fundamentals
- IntegrationHub Fundamentals
- Mobile Development Fundamentals
- Service Portal Fundamentals

Additional Resources

In addition to the above, the candidate may find the following additional resources valuable in preparation for the exam.

- Orlando Security Incident Response Documentation
- ServiceNow Security Operations Now Community Forums
- Glossary of Terms for Security Operations with Wikipedia Links

Additional Recommended Experience

- Three (3) to six (6) months field experience participating in a ServiceNow Security Incident response deployment project or maintaining the SIR application suite in a ServiceNow instance.
- General familiarity with industry terminology, acronyms, and initialisms

Exam Scope

Exam content is divided into Learning Domains that correspond to key topics and activities typically encountered during ServiceNow implementations. In each Learning Domain, specific learning objectives have been identified and are tested in the exam.

The following table shows the learning domains, weightings, and sub-skills measured by this exam and the percentage of questions represented in each domain. The listed sub- skills should NOT be considered an all-inclusive list of exam content.

	Learning Domain	% of Exam
1	**Security Incident Response Overview** • Introducing Security Incident Response • Understanding Customer Goals • Meeting Customer Expectations	**15%**

2	**Create Security Incidents** • Security Incident Response Setup Assistant • Using the Security Incident Catalog • Manual Creation of Security Incidents • Email Parsing **Risk**	**10%**
3	**Security Incident and Threat Intelligence Integrations** • ServiceNow Store and Share • Managing Pre-Built Integrations • Creating Custom Integrations	**14%**
4	**Security Incident Response Management** • Standard Automated Assignment Options • Definition of Escalation Paths • Security Tags • Process Definitions and Selection	**15%**
5	**Risk Calculations and Post Incident Response** • Security Incident Calculator Groups and Risk Scores • Post Incident Reviews	**13%**
6	**Automation and Standard Processes** • Automation with Workflows, Knowledge Articles, and Runbooks • Using Flow Designer • Implementing Playbooks	**30%**
7	**Data Visualization** • Data Visualization: Dashboards and Reporting	**3%**
	Total	**100%**

Exam Registration

Each candidate must register for the exam via the ServiceNow Webassessor website using a voucher obtained by completing the Security Incident Response (SIR) Implementation training prerequisite. Voucher codes are nontransferable and provides the candidate eligibility to sit for the Certified Implementation Specialist - Security Incident Response exam only.

During the registration process, each test taker has the option of taking the

exam at an Authorized Testing Center or as an online-proctored exam. In both testing venues, the Certified Implementation Specialist exam is done through a consistent, friendly, user interface customized for ServiceNow tests.

The Kryterion testing network is worldwide and all locations offer a secure, comfortable testing environment. Candidates register for the exam at a specific date and time so there is no waiting and a seat is reserved in the testing center.

Each candidate can also choose to take the exam as an online-proctored exam. This testing environment allows a candidate to take the test on his or her own system provided that certain requirements are met.

NOTE: A special accommodation version of the exam is available. Contact certification@servicenow.com for more information. Depending on the accommodation, there may be a 30-day lead time before testing.

Exam Structure

The exam consists of approximately 60 questions. For each question on the examination, there are multiple possible responses. The person taking the exam reviews the response options and selects the *most correct* answer to the question.

Multiple Choice (single answer)

For each multiple-choice question on the exam, there are at least four possible responses. The candidate taking the exam reviews the response options and selects the one response most accurately answers the question.

Multiple Select (select all that apply)

For each multiple-select question on the exam, there are at least four possible responses. The question will state how many responses should be selected. The candidate taking the exam reviews the response options and selects ALL responses that accurately answer the question. Multiple-select questions have two or more correct responses.

Exam Results

After completing and submitting the exam, a pass or fail result is immediately calculated and displayed to the candidate. More detailed results are not provided to the candidate.

Exam Retakes

If a candidate fails to pass an exam, they may register to take the exam again up to three more times at a cost.

servicenow

Sample Question(s)

Sample Item #1:

Which role is needed to install the Security Incident Response application?

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

Correct Answer: B

Sample Item #2:

Security Incident Response can be defined as:

A. The action plan taken to mitigate security incidents and imminent security threats
B. The change plan taken to fulfill requests raised through the Security Incident Catalog
C. The reaction plan taken to capture and record security incidents
D. The prevention activities to respond to imminent security threats

Correct Answer: A

Sample Item #3:

In which ServiceNow module can you find pre-built integrations?

A. Integrations
B. Sightings Search Configuration
C. Integration Configurations
D. Integration Status

Correct Answers: C

Sample Item #4:

Which process definition is set as default for security incident response application?

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

D. NIST Stateful

Correct Answer: D

Sample Item #5:

Which of the following statements best describes what Security Incident Calculators are used to do?

A. Set specific values according to matched conditions
B. Determine the Security Incident Risk Score
C. Calculate the cost of an incident
D. Calculate the time spent in the various incident states

Correct Answer: A, B

Sample Item #6:

A flow executes when what is met?

A. A trigger condition
B. IntegrationHub activation
C. Response Task state is Active
D. NIST Ready State

Correct Answer: A

Sample Item #7:

Identify three key Security Incident Response reporting audiences:

A. Security Analysts
B. Security Managers
C. CIOs/CISOs
D. Facilities Managers
E. Human Resources Managers

Correct Answers: A, B, C