

Sicherheitsingenieur

FF09 IT-Infrastruktur, Betrieb und Sicherheit · ISCO-08 2529 · CBS 0812 Systemadministratoren und Netzwerkspezialisten · Dienstalter senior · Auch bekannt als: Ingenieur für Cybersicherheit, IT-Sicherheitsingenieur

Errichtet und verwaltet technische Sicherheitsmaßnahmen wie Zugriffsmanagement, Überwachung und Absicherung und testet die Ausfallsicherheit von Systemen.

Der Sicherheitsingenieur implementiert tatsächlich Sicherheitsmaßnahmen in der Umgebung und sorgt dafür, dass diese funktionsfähig bleiben – vom Identitätsmanagement bis hin zur Protokollierung und Erkennung. Im Gegensatz zum Sicherheitsbeauftragten handelt es sich hierbei um eine Rolle, die sowohl die Einrichtung als auch den Betrieb umfasst, und im Gegensatz zum Sicherheitsanalysten liegt der Schwerpunkt auf der Umsetzung und nicht auf der Untersuchung von Warnmeldungen. Die Auswahl konzentriert sich auf Sicherheitswerkzeuge, während der Engpass in der Abstimmung liegt: Eine Kontrollmaßnahme, die von den Betriebs- und Entwicklungsteams nicht unterstützt werden kann oder will, wird innerhalb weniger Wochen deaktiviert oder umgangen.

Kennzahlen für dieses Profil

25 Fähigkeiten · 4 Zu bewertende Kompetenzen · 5 Ausschlusskriterien · Schwerpunkt: Digitales, Daten und KI 71%, Kognitive Fähigkeiten und Problemlösung 10%, Selbstmanagement, Tatkraft und Belastbarkeit 9%

1 Zu messende Kompetenzen

Dies sind die Verhaltens- und Fähigkeitskonstrukte in diesem Profil. Zu jedem wird angezeigt, welcher hrmforce-Fragebogen es misst.

Zu messende Kompetenzen	Zielniveau	hrmforce-Instrument	Messmethode	Verhaltensanker auf Zielniveau
Genauigkeit und Liebe zum Detail Kompetenz (50-Framework): Genauigkeit	■■■■■ N5	Big Fifty, 360 Feedback	Persönlichkeitsfragebogen	Legt die Standards für Vollständigkeit und Richtigkeit fest, lässt Beispiele prüfen und weist Teams auf strukturelle Nachlässigkeiten hin.
Integrität und Zuverlässigkeit Kompetenz (50-Framework): Integrität	■■■■■ N5	Big Fifty (Integritätsskala), 360 Feedback, Strukturiertes Interview	Persönlichkeitsfragebogen	Legt die Integritätsstandards der Organisation fest, setzt diese auch gegenüber einflussreichen Parteien durch und erläutert die daraus resultierenden Entscheidungen öffentlich.

Zu messende Kompetenzen	Zielniveau	hrmforce-Instrument	Messmethode	Verhaltensanker auf Zielniveau
Disziplin und Einhaltung von Verpflichtungen Kompetenz (50-Framework): Fachgebiet	 N5	Big Fifty, 15PF, 360 Feedback	Persönlichkeitsfragebogen	Verankert den Standard für die zuverlässige Einhaltung von Arbeitsvereinbarungen und richtet sich an alle Mitarbeiter auf jeder Ebene, die diesen Standard vernachlässigen.
Stressresistenz Kompetenz (50-Framework): Stressresilienz	 N5	Big Fifty, 15PF, Mental Resilience (4C)	Persönlichkeitsfragebogen	Sorgt dafür, dass die Organisation auch in Krisenzeiten funktionsfähig bleibt, trifft Entscheidungen unter hoher Unsicherheit und setzt Maßstäbe für besonnenes Handeln unter Druck.

2 Vollständiges Kompetenzprofil

Alle Kompetenzen in diesem Profil, sortiert nach Gewichtung. Der unter jeder Kompetenz angegebene Verhaltensanker bezieht sich auf das Zielniveau.

T	Skill	Zielniveau	Gewicht	Knockout	Messmethode	hrmforce-Instrument
V	Problemanalyse Führt hartnäckige organisatorische Probleme auf einige wenige Grundursachen zurück und legt die Analysemethode fest, die andere Teams anwenden werden.	■■■■■ N5	5	ja	Assessment-Center	Competency Check, Ability Scan
K	Grundkenntnisse im Bereich Netzwerke Verbreitet Netzwerkwissen innerhalb der Organisation, legt Gestaltungsgrundsätze fest und prüft Netzwerkentwürfe von Anbietern.	■■■■■ N5	5	ja	Wissenstest	Wissenstest (kundenspezifisch)
V	Systemadministration und -überwachung Legt die Verwaltungs- und Überwachungsstandards der Organisation fest und entscheidet über die Gestaltung der Systemumgebung.	■■■■■ N5	5	ja	Arbeitsproben-Test	Wissenstest (kundenspezifisch), Arbeitsproben-Test
V	Störungsmanagement und Fehlerbehebung Entwirft den Vorfallmanagementprozess des Unternehmens, leitet die Reaktion auf größere Störungen und legt diese gegenüber der Geschäftsleitung und den Kunden Rechenschaft ab.	■■■■■ N5	5	ja	Arbeitsproben-Test	Arbeitsproben-Test, Wissenstest (kundenspezifisch)
V	Zugangs- und Identitätsmanagement Legt die Zugriffsrichtlinien der Organisation fest und ist für die Kontrolle der Berechtigungen bei Audits zuständig.	■■■■■ N5	5	ja	Arbeitsproben-Test	Wissenstest (kundenspezifisch), Arbeitsproben-Test

T	Skill	Zielniveau	Gewicht	Knockout	Messmethode	hrmforce-Instrument
G	Genauigkeit und Liebe zum Detail Legt die Standards für Vollständigkeit und Richtigkeit fest, lässt Beispiele prüfen und weist Teams auf strukturelle Nachlässigkeiten hin.	■■■■■ N5	4	nein	Persönlichkeitsfragebogen	Big Fifty, 360 Feedback
G	Integrität und Zuverlässigkeit Legt die Integritätsstandards der Organisation fest, setzt diese auch gegenüber einflussreichen Parteien durch und erläutert die daraus resultierenden Entscheidungen öffentlich.	■■■■■ N5	4	nein	Persönlichkeitsfragebogen	Big Fifty (Integritätsskala), 360 Feedback, Strukturiertes Interview
G	Disziplin und Einhaltung von Verpflichtungen Verankert den Standard für die zuverlässige Einhaltung von Arbeitsvereinbarungen und richtet sich an alle Mitarbeiter auf jeder Ebene, die diesen Standard vernachlässigen.	■■■■■ N5	4	nein	Persönlichkeitsfragebogen	Big Fifty, 15PF, 360 Feedback
G	Stressresistenz Sorgt dafür, dass die Organisation auch in Krisenzeiten funktionsfähig bleibt, trifft Entscheidungen unter hoher Unsicherheit und setzt Maßstäbe für besonnenes Handeln unter Druck.	■■■■■ N5	4	nein	Persönlichkeitsfragebogen	Big Fifty, 15PF, Mental Resilience (4C)
V	Informationssicherheit im Arbeitsprozess Legt die Richtlinien zur Informationssicherheit fest und überwacht organisationsweit, ob die Prozesse den festgelegten Anforderungen entsprechen.	■■■■■ N5	4	nein	Wissenstest	Wissenstest (kundenspezifisch)
V	Programmierung Legt Programmierstandards und die Wahl der Programmiersprachen für das Unternehmen fest und überprüft den Code anderer hinsichtlich Qualität und Wartbarkeit.	■■■■■ N5	4	nein	Arbeitsproben-Test	Arbeitsproben-Test, Wissenstest (kundenspezifisch)

T	Skill	Zielniveau	Gewicht	Knockout	Messmethode	hrmforce-Instrument
V	Nutzung von Cloud-Plattformen Legt die Cloud-Strategie des Unternehmens fest und entscheidet, welche Workloads wo platziert werden.	■■■■■ N5	4	nein	Wissenstest	Wissenstest (kundenspezifisch)
K	Sensibilisierung für Informationssicherheit Entwirft das Sensibilisierungsprogramm des Unternehmens, misst dessen Wirkung und passt den Ansatz auf der Grundlage der gemessenen Ergebnisse an.	■■■■■ N5	4	nein	Wissenstest	Wissenstest (kundenspezifisch)
V	Sichere Entwicklung Legt sichere Entwicklungsanforderungen im Unternehmen fest und beurteilt vor der Freigabe, ob Lösungen diese erfüllen.	■■■■■ N5	4	nein	Arbeitsproben-Test	Arbeitsproben-Test, Wissenstest (kundenspezifisch)
V	Bedrohungs- und Risikoanalyse Führt eigenständig eine Bedrohungsanalyse einer Anwendung durch, priorisiert Risiken und berät hinsichtlich Maßnahmen unter Angabe von Kosten und Wirkung.	■■■■■ N4	4	nein	Arbeitsproben-Test	Wissenstest (kundenspezifisch), Arbeitsproben-Test
V	Reaktion auf Sicherheitsvorfälle Begrenzt eigenständig den Schaden während eines Vorfalls, sichert Beweismittel und liefert einen nachvollziehbaren Ablauf der Ereignisse.	■■■■■ N4	4	nein	Simulation	Wissenstest (kundenspezifisch), Arbeitsproben-Test
V	Aus Fehlern und Vorfällen lernen Analysiert eigene Fehler sowie die des Teams, erörtert die Ursachen offen in der Arbeitsbesprechung und passt die Vereinbarungen entsprechend an.	■■■■■ N4	3	nein	Situational Judgement Test	360 Feedback, Competency Check

T	Skill	Zielniveau	Gewicht	Knockout	Messmethode	hrmforce-Instrument
V	Aktueller Fachstand und Fachliteratur Erfasst Quellen und Leitlinien systematisch, bewertet deren Qualität und passt die eigene Arbeitsweise an neue Erkenntnisse an.	 N4	3	nein	Portfolio oder Nachweise	Portfolio, Wissenstest (kundenspezifisch)
T	Versionskontrolle und Arbeitsabläufe für die Zusammenarbeit Verwaltet Zweige und führt Zusammenführungen eigenständig durch, löst Konflikte und prüft die Änderungen von Kollegen inhaltlich.	 N4	3	nein	Arbeitsproben-Test	Arbeitsproben-Test
V	Erstellung technischer Dokumentationen Verfasst die vollständige Dokumentation für ein System oder einen Prozess, testet diese mit einem Laien und pflegt die verschiedenen Versionen.	 N4	3	nein	Arbeitsproben-Test	Arbeitsproben-Test, Portfolio
V	Release-Management und Bereitstellung Erstellt einen Einführungsplan mit einer Ausweichlösung, stimmt diesen mit den Beteiligten ab und überprüft nach der Einführung, ob der Dienst ordnungsgemäß funktioniert.	 N4	3	nein	Arbeitsproben-Test	Wissenstest (kundenspezifisch), Arbeitsproben-Test
V	Funktions- und Anwendungsmanagement Verwaltet eigenständig eine Anwendung, priorisiert Änderungswünsche gemeinsam mit den Anwendern und testet neue Versionen, bevor diese in Betrieb genommen werden.	 N4	3	nein	Arbeitsproben-Test	Wissenstest (kundenspezifisch), Arbeitsproben-Test
V	Prozessautomatisierung Beschreibt einen Prozess in einzelnen Schritten, automatisiert die wiederholbaren Schritte und integriert Prüfungen auf Fehler und Ausnahmen.	 N3	3	nein	Arbeitsproben-Test	Arbeitsproben-Test, Portfolio

T	Skill	Zielniveau	Gewicht	Knockout	Messmethode	hrmforce-Instrument
V	Datenklassifizierung und -aufbewahrung Legt die Klassifizierung und die Aufbewahrungsfrist für einen Informationsfluss fest und überprüft, ob die Bereinigung wie geplant erfolgt.	 N4	2	nein	Wissenstest	Wissenstest (kundenspezifisch), Arbeitsproben-Test
V	IT-Lieferanten- und Vertragsmanagement Führt Besprechungen mit Lieferanten zu Leistung und Kosten durch, dokumentiert Vereinbarungen und greift ein, wenn Vereinbarungen nicht eingehalten werden.	 N3	1	nein	Strukturiertes Interview	Strukturiertes Interview, Portfolio

3 Stufen nach Dienstalter

Dasselbe Profil unter Berücksichtigung der Dienstaltersanpassung für die Berufsgruppe. Die Zielstufen sind auf 1 bis 5 begrenzt.

Skill	medior	senior
Problemanalyse	N4	N5
Grundkenntnisse im Bereich Netzwerke	N4	N5
Systemadministration und -überwachung	N4	N5
Störungsmanagement und Fehlerbehebung	N4	N5
Zugangs- und Identitätsmanagement	N5	N5
Genauigkeit und Liebe zum Detail	N4	N5
Integrität und Zuverlässigkeit	N4	N5
Disziplin und Einhaltung von Verpflichtungen	N4	N5
Stressresistenz	N4	N5
Informationssicherheit im Arbeitsprozess	N4	N5
Programmierung	N4	N5
Nutzung von Cloud-Plattformen	N4	N5
Sensibilisierung für Informationssicherheit	N4	N5
Sichere Entwicklung	N4	N5
Bedrohungs- und Risikoanalyse	N4	N4
Reaktion auf Sicherheitsvorfälle	N4	N4
Aus Fehlern und Vorfällen lernen	N3	N4
Aktueller Fachstand und Fachliteratur	N3	N4
Versionskontrolle und Arbeitsabläufe für die Zusammenarbeit	N3	N4
Erstellung technischer Dokumentationen	N3	N4
Release-Management und Bereitstellung	N3	N4
Funktions- und Anwendungsmanagement	N3	N4
Prozessautomatisierung	N3	N3
Datenklassifizierung und -aufbewahrung	N3	N4
IT-Lieferanten- und Vertragsmanagement	N2	N3

4 Die Kompetenzskala

Ebene	Bezeichnung	Autonomie	Komplexität	Umfang	Kenntnisumfang
N1	Geführt	arbeitet unter Aufsicht und befolgt Anweisungen	Routine, jeweils eine Variable nach der anderen	eigene Aufgabe	Grundlegendes Verständnis der Terminologie
N2	Anwendung	arbeitet selbstständig innerhalb festgelegter Rahmenbedingungen	vertraute Situationen mit geringen Abweichungen	die eigene Rolle	praktische Kenntnisse, wendet Standardverfahren an
N3	Beherrscht	legt den eigenen Ansatz fest und holt proaktiv Input ein	mehrere Variablen, gewisse Mehrdeutigkeiten	eigenes Team oder eigener Prozess	fundierte Kenntnisse, wägt Alternativen ab
N4	Fortgeschritten	leitet andere an und entscheidet über die Vorgehensweise	komplex, mit widersprüchlichen Interessen	mehrere Teams oder eine Abteilung	fundierte Kenntnisse, berät andere
N5	Führung	legt den Standard und die Richtlinien fest	strategisch, unter hoher Unsicherheit	Organisation, Wertschöpfungskette oder Berufsfeld	Autorität, fördert die Entwicklung des Berufsstandes

5 Verhaltensanker pro Kompetenz

Die Ankerpunkte befinden sich bei N1, N3 und N5. N2 und N4 sind bewusst nicht als Ankerpunkte festgelegt: Die Bewerter interpolieren zwischen diesen Punkten gemäß der O*NET-Konvention.

Skill	N1	N3	N5
Problemanalyse Teilt ein Problem in einzelne Teile auf, trennt Ursachen von Wirkungen und gibt an, welche Informationen erforderlich sind, um weiterzukommen.	Gibt genau an, was bei einer Störung abweicht und welche Daten fehlen, und meldet dies dem Vorgesetzten.	Gliedert eine wiederholt auftretende Beschwerde in mögliche Ursachen auf, prüft diese anhand eigener Daten und benennt die wahrscheinlichste Ursache.	Führt hartnäckige organisatorische Probleme auf einige wenige Grundursachen zurück und legt die Analysemethode fest, die andere Teams anwenden werden.
Grundkenntnisse im Bereich Netzwerke Verfügt über ein umfassendes Verständnis der Funktionsweise von Netzwerken, einschließlich Adressierung, Routing, Ports und Namensauflösung, und kann angeben, wo Verbindungsprobleme auftreten können.	Erläutert, aus welchen Teilen eine Verbindung besteht, und führt eine vorgegebene Prüfung durch, beispielsweise einen Konnektivitätstest.	Leitet anhand von Symptomen ab, in welcher Netzwerkschicht ein Problem vorliegt, und untermauert dies durch eigene Messungen.	Verbreitet Netzwerkwissen innerhalb der Organisation, legt Gestaltungsgrundsätze fest und prüft Netzwerkentwürfe von Anbietern.

Skill	N1	N3	N5
Systemadministration und -überwachung Stellt den reibungslosen Betrieb der Systeme sicher, indem er Einstellungen, Updates und Berechtigungen verwaltet, Überwachungsmaßnahmen einrichtet und auf Signale reagiert, bevor die Nutzer davon betroffen sind.	Führt geplante Wartungsaufgaben und Aktualisierungen gemäß dem Runbook durch und meldet Abweichungen bei den Überwachungssignalen.	Verwaltet eigenständig eine Systemumgebung, legt Überwachungsschwellenwerte fest und beseitigt wiederkehrende Ursachen für Störungen.	Legt die Verwaltungs- und Überwachungsstandards der Organisation fest und entscheidet über die Gestaltung der Systemumgebung.
Störungsmanagement und Fehlerbehebung Erfasst Störungen, ermittelt deren Ursache durch gezielte Maßnahmen, stellt den Betrieb wieder her und hält Melder sowie Beteiligte auf dem Laufenden.	Erfasst eine Störung lückenlos, durchläuft die Standardschritte und eskaliert den Fall, sobald die eigenen Maßnahmen nicht zum Erfolg führen.	Leitet eine Untersuchung zu einer unbekannten Störung ein, stellt den Betrieb wieder her und dokumentiert Ursache und Lösung zur späteren Wiederverwendung.	Entwirft den Vorfalldatenmanagementprozess des Unternehmens, leitet die Reaktion auf größere Störungen und legt diese gegenüber der Geschäftsleitung und den Kunden Rechenschaft ab.
Zugangs- und Identitätsmanagement Erteilt Zugriffsrechte je nach Rolle und Bedarf, überprüft regelmäßig, wer auf welche Daten zugreifen darf, und entzieht die Rechte bei Änderungen oder beim Ausscheiden.	Bearbeitet Zugriffsanfragen gemäß dem festgelegten Rollenschema und protokolliert jede Änderung.	Entwirft Rollen und Berechtigungen für eine Anwendung, führt regelmäßige Überprüfungen durch und korrigiert übermäßige Zugriffsrechte.	Legt die Zugriffsrichtlinien der Organisation fest und ist für die Kontrolle der Berechtigungen bei Audits zuständig.
Genauigkeit und Liebe zum Detail Arbeitet sorgfältig, überprüft die eigene Arbeit auf Fehler und hält sich an die Vereinbarungen bezüglich der Vollständigkeit und Richtigkeit der Daten.	Überprüft die eigene Arbeit anhand einer Checkliste und korrigiert festgestellte Fehler, bevor die Arbeit weitergeleitet wird.	Baut Kontrollmomente in den eigenen Prozess ein, verfolgt Fehler und verhindert deren Wiederholung durch Anpassung der Vorgehensweise.	Legt die Standards für Vollständigkeit und Richtigkeit fest, lässt Beispiele prüfen und weist Teams auf strukturelle Nachlässigkeiten hin.
Integrität und Zuverlässigkeit Handeln im Einklang mit geltenden Standards und Vereinbarungen, auch ohne Aufsicht, sowie Transparenz hinsichtlich eigener Interessen, Fehler und zweifelhafter Fälle.	Hält sich an getroffene Vereinbarungen und Verhaltensregeln und meldet eigene Fehler dem Vorgesetzten.	Meldet von sich aus einen möglichen Interessenkonflikt und bittet um eine Überprüfung, bevor eine Entscheidung getroffen wird.	Legt die Integritätsstandards der Organisation fest, setzt diese auch gegenüber einflussreichen Parteien durch und erläutert die daraus resultierenden Entscheidungen öffentlich.
Disziplin und Einhaltung von Verpflichtungen Hält sich auch ohne Aufsicht an Vereinbarungen, Abläufe und Verpflichtungen und meldet rechtzeitig, wenn sich eine Verpflichtung als nicht erfüllbar erweist.	Erscheint zur vereinbarten Zeit mit der vereinbarten Arbeit und meldet etwaige Verzögerungen dem Vorgesetzten.	Verpflichtet sich nur zu dem, was machbar ist, behält den Überblick über die eigenen Verpflichtungen und informiert die Beteiligten, sobald eine Frist unter Druck gerät.	Verankert den Standard für die zuverlässige Einhaltung von Arbeitsvereinbarungen und richtet sich an alle Mitarbeiter auf jeder Ebene, die diesen Standard vernachlässigen.

Skill	N1	N3	N5
Stressresistenz Liefert auch unter Zeitdruck, bei Widerständen oder unerwarteten Wendungen stets Arbeit von gleichbleibender Qualität und bewahrt im Umgang mit anderen einen sachlichen Ton.	Arbeitet auch bei steigendem Druck weiter an der aktuellen Aufgabe und fragt den Vorgesetzten, welche Aufgabe warten kann.	Arbeitet auch bei höchster Auslastung strukturiert weiter, hält Vereinbarungen mit Kunden klar fest und weist frühzeitig darauf hin, welche Ergebnisse gefährdet sind.	Sorgt dafür, dass die Organisation auch in Krisenzeiten funktionsfähig bleibt, trifft Entscheidungen unter hoher Unsicherheit und setzt Maßstäbe für besonnenes Handeln unter Druck.
Informationssicherheit im Arbeitsprozess Wendet im Arbeitsalltag Sicherheitsmaßnahmen an, wie z. B. den sicheren Austausch, die Klassifizierung und die Speicherung von Informationen, und weist auf riskante Arbeitspraktiken hin.	Hält sich an die Sicherheitsvorschriften für den Austausch und die Speicherung von Informationen und meldet einen vermuteten Vorfall unverzüglich.	Wägt Sicherheitsrisiken bei der Festlegung neuer Arbeitsvereinbarungen ab, passt Maßnahmen an und spricht Kollegen auf unsicheres Verhalten an.	Legt die Richtlinien zur Informationssicherheit fest und überwacht organisationsweit, ob die Prozesse den festgelegten Anforderungen entsprechen.
Programmierung Verfasst, liest und optimiert Programmcode in mindestens einer Programmiersprache, gliedert ein Problem in einzelne Schritte auf und testet die eigene Lösung.	Passen bestehenden Code gemäß den Anweisungen an, führen ihn aus und melden Fehlermeldungen, die nicht eigenständig behoben werden können.	Entwickelt eigenständig eine Funktion oder ein Modul auf der Grundlage der Anforderungen, wählt geeignete Strukturen aus und sorgt dafür, dass der Code lesbar und getestet bleibt.	Legt Programmierstandards und die Wahl der Programmiersprachen für das Unternehmen fest und überprüft den Code anderer hinsichtlich Qualität und Wartbarkeit.
Nutzung von Cloud-Plattformen Richtet Dienste in einer Cloud-Umgebung ein und verwaltet diese, regelt Zugriffsrechte und Kosten und wählt je nach Anforderungen zwischen den verfügbaren Diensttypen aus.	Nutzt vorhandene Cloud-Dienste gemäß den Anweisungen und meldet ungewöhnliches Verhalten oder unerwartete Kosten an den Administrator.	Konfiguriert eigenständig Cloud-Dienste für eine Anwendung, richtet Berechtigungen und Backups ein und behält Kosten und Nutzung im Blick.	Legt die Cloud-Strategie des Unternehmens fest und entscheidet, welche Workloads wo platziert werden.
Sensibilisierung für Informationssicherheit Kennt die gängigsten Bedrohungen wie Phishing, Ransomware und Täuschungsversuche, erkennt deren Anzeichen und weiß, welche Maßnahmen in solchen Fällen zu ergreifen sind.	Erkennt eine offensichtliche Phishing-Nachricht, klickt nicht darauf und meldet die Nachricht über den dafür vorgesehenen Kanal.	Erläutert Kollegen, wie Bedrohungen funktionieren, beurteilt zweifelhafte Fälle eigenständig und passt das eigene Verhalten an neue Bedrohungen an.	Entwirft das Sensibilisierungsprogramm des Unternehmens, misst dessen Wirkung und passt den Ansatz auf der Grundlage der gemessenen Ergebnisse an.
Sichere Entwicklung Entwickelt Software, bei der Eingaben validiert, vertrauliche Daten geschützt und bekannte Sicherheitslücken vermieden werden, und überprüft dies durch gezielte Tests.	Befolgt die Richtlinien zur sicheren Programmierung bei eigenen Änderungen und fragt nach, wenn eine Richtlinie unklar ist.	Erkennt Schwachstellen in Design und Code, behebt diese und integriert Sicherheitstests in die eigene Arbeitsweise.	Legt sichere Entwicklungsanforderungen im Unternehmen fest und beurteilt vor der Freigabe, ob Lösungen diese erfüllen.

Skill	N1	N3	N5
Bedrohungs- und Risikoanalyse Ermittelt Risiken, Schwachstellen und Folgen für ein System oder einen Prozess, wägt die Eintrittswahrscheinlichkeit gegen die Auswirkungen ab und benennt geeignete Maßnahmen.	Führt anhand einer vorgegebenen Liste von Bedrohungen eine Risikoanalyse durch und übermittelt das Ergebnis an den Fachspezialisten.	Führt eigenständig eine Bedrohungsanalyse einer Anwendung durch, priorisiert Risiken und berät hinsichtlich Maßnahmen unter Angabe von Kosten und Wirkung.	Ermittelt die Risikobereitschaft und die Analysemethode des Unternehmens und legt dem Vorstand das Sicherheitsrisikobild dar.
Reaktion auf Sicherheitsvorfälle Reagiert auf einen Sicherheitsvorfall gemäß dem Runbook, indem er diesen eindämmt, Beweismittel sichert, Daten wiederherstellt und die zuständigen Stellen rechtzeitig informiert.	Meldet einen vermuteten Vorfall unverzüglich, rührt nichts an und befolgt die Anweisungen des Koordinators.	Begrenzt eigenständig den Schaden während eines Vorfalls, sichert Beweismittel und liefert einen nachvollziehbaren Ablauf der Ereignisse.	Leitet das unternehmensweite Einsatzteam, trifft Entscheidungen zur externen Kommunikation und verbessert das Runbook nach jeder Übung.
Aus Fehlern und Vorfällen lernen Untersucht nach einem Fehler oder Vorfall, was geschehen ist, benennt die Ursache, ohne die Schuld auf andere abzuwälzen, und passt die Arbeitsweise in diesem Punkt an.	Meldet einen eigenen Fehler unverzüglich dem Vorgesetzten und führt die Aufgabe gemäß der korrigierten Anweisung erneut aus.	Analysiert eigene Fehler sowie die des Teams, erörtert die Ursachen offen in der Arbeitsbesprechung und passt die Vereinbarungen entsprechend an.	Stellt sicher, dass Vorfälle unternehmensweit sicher gemeldet werden, lässt die Ursachen systematisch analysieren und lässt die daraus gewonnenen Erkenntnisse in Richtlinien und Standards einfließen.
Aktueller Fachstand und Fachliteratur Verfolgt die Entwicklungen im eigenen Berufsfeld anhand von Fachliteratur, Leitlinien und Netzwerken und lässt relevante neue Erkenntnisse in die eigene Praxis einfließen.	Erfasst die erhaltenen beruflichen Informationen und ermittelt, welche Aspekte für die eigene Arbeit von Bedeutung sind.	Erfasst Quellen und Leitlinien systematisch, bewertet deren Qualität und passt die eigene Arbeitsweise an neue Erkenntnisse an.	Bewerten den Stand der Forschung, wägen widersprüchliche Forschungsergebnisse ab und legen fest, welche Leitlinien die Organisation künftig befolgen wird.
Versionskontrolle und Arbeitsabläufe für die Zusammenarbeit Arbeitet mit einem Versionskontrollsystem, nutzt Zweige und Zusammenführungsanfragen und sorgt dafür, dass der Änderungsverlauf für das Team nachvollziehbar bleibt.	Führt Änderungen mit einer klaren Beschreibung in dem gemäß der Teamvereinbarung festgelegten Zweig ein.	Verwaltet Zweige und führt Zusammenführungen eigenständig durch, löst Konflikte und prüft die Änderungen von Kollegen inhaltlich.	Legt die Vorgehensweise bei der Versionskontrolle und der Codeüberprüfung im Unternehmen fest und sorgt für deren teamübergreifende Einhaltung.
Erstellung technischer Dokumentationen Verfasst Handbücher, Supportdokumentationen und Entscheidungsprotokolle, denen ein Leser ohne Vorkenntnisse Schritt für Schritt folgen kann und die stets auf dem neuesten Stand bleiben.	Füllt eine Dokumentationsvorlage mit den einzelnen Schritten einer Aufgabe aus und lässt den Text von einem Kollegen überprüfen.	Verfasst die vollständige Dokumentation für ein System oder einen Prozess, testet diese mit einem Laien und pflegt die verschiedenen Versionen.	Legt den Dokumentationsstandard des Unternehmens fest und stellt sicher, dass die Dokumentation Bestandteil jeder Lieferung ist.

Skill	N1	N3	N5
Release-Management und Bereitstellung Plant und führt die Einführung neuer Versionen durch, überprüft den Betrieb vor und nach der Einführung und stellt sicher, dass ein Rollback möglich bleibt.	Führt die Schritte eines Einführungsplans durch und meldet unverzüglich, wenn ein Schritt nicht zum erwarteten Ergebnis führt.	Erstellt einen Einführungsplan mit einer Ausweidlösung, stimmt diesen mit den Beteiligten ab und überprüft nach der Einführung, ob der Dienst ordnungsgemäß funktioniert.	Legt die Freigaberichtlinien des Unternehmens fest, entscheidet über Einführungszeiträume und optimiert strukturell die Vorlaufzeit von Änderungen.
Funktions- und Anwendungsmanagement Stellt sicher, dass eine Anwendung funktionsfähig und für die Nutzer geeignet bleibt, indem er Anforderungen erfasst, Einstellungen verwaltet und Änderungen mit dem Anbieter abstimmt.	Bearbeitet Nutzeranfragen zu einer Bewerbung gemäß den Anweisungen und erfasst die Anfragen im dafür vorgesehenen Register.	Verwaltet eigenständig eine Anwendung, priorisiert Änderungswünsche gemeinsam mit den Anwendern und testet neue Versionen, bevor diese in Betrieb genommen werden.	Legt fest, wie das funktionale Management organisiert ist, und entscheidet über die Lebensdauer von Anwendungen.
Prozessautomatisierung Analysiert einen wiederkehrenden Arbeitsprozess, entwickelt oder beauftragt die Automatisierung seiner einzelnen Schritte und überprüft, ob das Ergebnis zuverlässig bleibt.	Führt eine bestehende Automatisierung durch und meldet, wenn das Ergebnis von den Erwartungen abweicht.	Beschreibt einen Prozess in einzelnen Schritten, automatisiert die wiederholbaren Schritte und integriert Prüfungen auf Fehler und Ausnahmen.	Legt die Automatisierungsstrategie des Unternehmens fest und entscheidet, welche Prozesse automatisiert werden und welche nicht.
Datenklassifizierung und -aufbewahrung Klassifiziert Informationen nach Vertraulichkeitsgrad und Wichtigkeit, ordnet ihnen Aufbewahrungsfristen zu und stellt sicher, dass die Löschung und Archivierung tatsächlich erfolgen.	Weist gemäß dem Schema eine Klassifizierungskategorie zu und leitet unklare Fälle an den Administrator weiter.	Legt die Klassifizierung und die Aufbewahrungsfrist für einen Informationsfluss fest und überprüft, ob die Bereinigung wie geplant erfolgt.	Entwirft die Klassifizierungs- und Aufbewahrungsrichtlinien der Organisation und berücksichtigt diese bei Audits und bei der Aufsicht.
IT-Lieferanten- und Vertragsmanagement Verwaltet Vereinbarungen mit IT-Lieferanten hinsichtlich Lieferung, Leistung und Kosten, überwacht die Einhaltung der Vereinbarungen und spricht Abweichungen gegenüber den Lieferanten an.	Prüft Rechnungen und erbrachte Leistungen anhand des Vertrags und meldet Abweichungen an den Vertragsmanager.	Führt Besprechungen mit Lieferanten zu Leistung und Kosten durch, dokumentiert Vereinbarungen und greift ein, wenn Vereinbarungen nicht eingehalten werden.	Legt die Lieferantenrichtlinien des Unternehmens fest, schließt die wichtigsten Verträge ab und entscheidet über Kündigungen oder einen Wechsel.

6 Bewertungsmethoden und Validität

Bei den Validitätswerten handelt es sich um die korrigierten metaanalytischen Schätzungen von Sackett, Zhang, Berry und Lievens (2022) aus dem „Journal of Applied Psychology“, die die älteren Zahlen von Schmidt und Hunter (1998) ersetzen. Die Streuung ist ebenso wichtig wie der Mittelwert: Bei einer hohen Standardabweichung (SD) variiert die Validität stark je nach Kontext.

Messmethode	rho	SD	Was ist das?
Assessment-Center	0.29	0.09	Mehrere Übungen, mehrere Bewerber, bewertungsdimensionenbezogene Benotung.
Wissenstest	0.40	0.13	Test zur Überprüfung des deklarativen Fachwissens, der in der Regel kundenspezifisch zusammengestellt wird.
Arbeitsproben-Test	0.33	0.09	Der Bewerber führt unter standardisierten Bedingungen eine repräsentative Arbeitsprobe durch.
Persönlichkeitsfragebogen	0.40	0.15	Selbstauskunft zu Verhaltenspräferenzen. Unter hrnforce finden Sie den „Big Fifty“ und den „15PF“.
Simulation	-	-	Simulierte Arbeitssituation, in der Regel digital, mit standardisierter Bewertung.
Situational Judgement Test	0.12	0.11	Szenario mit Antwortmöglichkeiten, das hinsichtlich Wissen oder Verhaltenstendenzen bewertet wird.
Portfolio oder Nachweise	-	-	Eine Sammlung früherer Arbeiten oder Ergebnisse, die anhand festgelegter Kriterien bewertet wurden.
Strukturiertes Interview	0.42	0.19	Verhaltensorientiertes Vorstellungsgespräch mit festgelegten Fragen und einer Bewertungsskala pro Frage.

7 Assessment-Instrumente für diesen Beruf

hrnforce-Instrument	Kompetenzen	Was damit gemessen wird
Wissenstest (kundenspezifisch)	15	Fachwissenstest, individuell auf jeden Kunden zugeschnitten
Arbeitsproben-Test	13	Repräsentatives Arbeitsbeispiel unter standardisierten Bedingungen
360 Feedback	4	Mehrere Bewertungen auf der Grundlage von Verhaltensankern
Portfolio	4	Bewertung bisheriger Arbeiten anhand festgelegter Kriterien
Big Fifty	3	Persönlichkeitsfragebogen, 150 Items, 25 Faktoren
Competency Check	2	Kompetenzbeurteilung auf Verhaltensebene
Strukturiertes Interview	2	Verhaltensorientiertes Vorstellungsgespräch mit fester Struktur
15PF	2	„Personality Profile“, eine kürzere Alternative zum „Big Fifty“
Ability Scan	1	Eignungstest: Verbale, numerische und abstrakte Denkfähigkeiten
Big Fifty (Integritätsskala)	1	

hrmforce-Instrument	Kompetenzen	Was damit gemessen wird
Mental Resilience (4C)	1	Psychische Belastbarkeit gemäß dem 4C-Modell

8 So verwenden Sie dieses Profil

1. Stimmen Sie das Profil mit dem Personalverantwortlichen ab, bevor der erste Kandidat bewertet wird. Nachträglich vorgenommene Gewichtsadjustierungen machen das Ergebnis nicht mehr vertretbar.
2. Wählen Sie die Bewertungsmethode pro Kompetenz aus der Spalte „Bewertungsmethode“ aus. Kombinieren Sie maximal drei Methoden pro Bewerber.
3. Führen Sie in einer zweistündigen Sitzung eine Kalibrierung der Bewerter anhand der Ankerwerte aus Kapitel 5 durch. Ankerwerte ohne Schulung der Bewerter sind kaum aussagekräftig.
4. Füllen Sie den Übereinstimmungsrechner aus und besprechen Sie die Lücken im Entwicklungsgespräch. Typ A und Typ G sind Auswahlkriterien, keine Entwicklungsziele für das erste Quartal.

Quelle: hrmforce Skills Framework 2.0, Version 2.0.0, erstellt am 2026-09-08. Zuordnungen zu ESCO v1.2.1, O*NET 31.0, Lightcast Open Skills, SFIA 9, DigComp 3.0, EntreComp, LifeComp, GreenComp, AILit, WEF Future of Jobs 2025, ISCO-08 sowie zur niederländischen CBS-Berufsklassifikation BRC 2014, Ausgabe 2025. Dieses Profil dient als Ausgangspunkt und stellt keinen Standard dar: Passen Sie es an Ihre eigene Organisation an, bevor Sie darauf basierend eine Auswahl treffen.