Security Analyst

FF09 IT infrastructure, operations and security · ISCO-08 2529 · CBS 0812 System administrators and network specialists · seniority medior · Also known as: SOC Analyst, Cyber Threat Analyst, Security Operations Analyst

Investigates alerts and logging for signs of attack, determines their severity and initiates the follow up steps during incidents.

The security analyst works in the monitoring chain and judges the stream of alerts coming out of detection systems. Unlike the security engineer, this role does not build the detection, and unlike the security officer it works at incident level rather than on policy. Selection asks mainly about tool experience, while the role depends on an investigative attitude and composure: most alerts are noise, and deciding under time pressure which one is real requires source evaluation and case building rather than routine.

Key figures for this profile

25 skills · 4 competencies to measure · 5 knockout skills · centre of gravity: Digital, data and AI 57%, Cognitive ability and problem solving 18%, Self-management, drive and resilience 9%

1 Competencies to measure

These are the behavioural and ability constructs in this profile. Each one shows which hrmforce questionnaire measures it.

Competencies to measure	Target level	hrmforce instrument	Assessment method	Behavioural anchor at target level
Stress tolerance Competency (50-framework): Stress resilience	▮▮▮▮▯ N4	Big Fifty, 15PF, Mental Resilience (4C)	Personality questionnaire	Keeps working in a structured way at peak load, keeps agreements with clients clear and flags early which results are at risk.

Competencies to measure	Target level	hrmforce instrument	Assessment method	Behavioural anchor at target level
Accuracy and attention to detail Competency (50-framework): Accuracy	N4	Big Fifty, 360 Feedback	Personality questionnaire	Builds check moments into the own process, keeps track of errors and prevents repetition by adjusting the method.
integrity and dependability Competency (50-framework): Integrity	N4	Big Fifty (Integrity Scale), 360 Feedback, Structured interview	Personality questionnaire	Reports a possible conflict of interest on own initiative and asks for review before a decision is taken.
Discipline and keeping commitments Competency (50-framework): Discipline	N4	Big Fifty, 15PF, 360 Feedback	Personality questionnaire	Commits only to what is feasible, tracks own commitments and informs those involved as soon as a deadline comes under pressure.

2 Full skill profile

Every skill in this profile, sorted by weight. The behavioural anchor under each skill belongs to the target level.

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	Security incident response Leads the organisation wide response team, decides on external communication and improves the runbook after every exercise.	N5	5	yes	Simulation	Knowledge test (client-specific), Work sample test
V	Problem analysis Splits a recurring complaint into possible causes, tests these with own data and names the most likely cause.	N4	5	yes	Assessment centre	Competency Check, Ability Scan
V	Critical thinking and source evaluation Detects fallacies and selective evidence in reports and states which conclusion the data do support.	N4	5	no	Work sample test	Competency Check, Work sample test
G	Stress tolerance Keeps working in a structured way at peak load, keeps agreements with clients clear and flags early which results are at risk.	N4	5	no	Personality questionnaire	Big Fifty, 15PF, Mental Resilience (4C)

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	Data analysis Selects analysis methods for an open question, turns raw data into a working file and supports every conclusion with figures.	N4	5	no	Work sample test	Ability Scan, Work sample test
K	Basic networking knowledge Deduces from symptoms in which network layer a problem sits and supports that with own measurements.	N4	5	yes	Knowledge test	Knowledge test (client-specific)
V	Incident management and troubleshooting Sets an investigation line for an unfamiliar disruption, restores the service and records cause and solution for reuse.	N4	5	yes	Work sample test	Work sample test, Knowledge test (client-specific)
V	Threat and risk analysis Independently performs a threat analysis on an application, prioritises risks and advises on measures with costs and effect.	N4	5	no	Work sample test	Knowledge test (client-specific), Work sample test
V	Access and identity management Designs roles and permissions for an application, carries out the periodic review and corrects excessive access.	N4	5	yes	Work sample test	Knowledge test (client-specific), Work sample test

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	Information gathering and filtering Chooses sources independently for an open question, filters out duplicate and outdated data and justifies that choice.	N4	4	no	Work sample test	Competency Check, Work sample test
G	Accuracy and attention to detail Builds check moments into the own process, keeps track of errors and prevents repetition by adjusting the method.	N4	4	no	Personality questionnaire	Big Fifty, 360 Feedback
G	integrity and dependability Reports a possible conflict of interest on own initiative and asks for review before a decision is taken.	N4	4	no	Personality questionnaire	Big Fifty (Integrity Scale), 360 Feedback, Structured interview
G	Discipline and keeping commitments Commits only to what is feasible, tracks own commitments and informs those involved as soon as a deadline comes under pressure.	N4	4	no	Personality questionnaire	Big Fifty, 15PF, 360 Feedback
V	Information security in the work process Weighs security risks when setting new working agreements, adjusts measures and addresses colleagues on unsafe behaviour.	N4	4	no	Knowledge test	Knowledge test (client-specific)

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	Using cloud platforms Independently configures cloud services for an application, arranges permissions and backups and keeps costs and usage in view.	N4	4	no	Knowledge test	Knowledge test (client-specific)
K	Information security awareness Explains to colleagues how threats work, judges doubtful cases independently and adapts own behaviour to new threats.	N4	4	no	Knowledge test	Knowledge test (client-specific)
V	Learning from mistakes and incidents Analyses own errors and those of the team, discusses the cause openly in the work meeting and adjusts the agreements.	N3	3	no	Situational Judgement Test	360 Feedback, Competency Check
V	Professional currency and specialist literature Tracks sources and guidelines structurally, weighs their quality and adapts the own working method to new insights.	N3	3	no	Portfolio or evidence	Portfolio, Knowledge test (client-specific)
V	Writing technical documentation Writes complete documentation for a system or process, tests it with an unfamiliar reader and maintains versions.	N3	3	no	Work sample test	Work sample test, Portfolio

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	System administration and monitoring Independently manages a system environment, sets monitoring thresholds and removes recurring causes of disruptions.	N3	3	no	Work sample test	Knowledge test (client-specific), Work sample test
V	Release management and deployment Draws up a rollout plan with a fallback option, aligns with stakeholders and verifies after rollout that the service works.	N3	3	no	Work sample test	Knowledge test (client-specific), Work sample test
V	Process automation Describes a process in steps, automates the repeatable steps and builds in checks on errors and exceptions.	N3	3	no	Work sample test	Work sample test, Portfolio
V	Emergency and crisis organisation Independently fills a role in a crisis team, keeps the situation picture current and ensures decisions are recorded.	N3	3	no	Simulation	Work sample test, Competency Check
V	Service calls and telephone contact Settles unusual questions within a single call, keeps call time under control and audibly summarises the agreement made.	N3	2	no	Work sample test	Work sample test, Communication Styles

T	Skill	Target level	Weight	Knockout	Assessment method	hrmforce instrument
V	Data classification and retention Determines classification and retention period for an information flow and checks whether clean up happens as planned.	N3	2	no	Knowledge test	Knowledge test (client-specific), Work sample test

3 Levels per seniority

The same profile with the job family seniority adjustment applied. Target levels are clamped to 1 to 5.

Skill	junior	medior	senior
Security incident response	N5	N5	N5
Problem analysis	N3	N4	N5
Critical thinking and source evaluation	N3	N4	N5
Stress tolerance	N4	N4	N4
Data analysis	N3	N4	N5
Basic networking knowledge	N3	N4	N5
Incident management and troubleshooting	N3	N4	N5
Threat and risk analysis	N4	N4	N4
Access and identity management	N3	N4	N5
Information gathering and filtering	N3	N4	N5
Accuracy and attention to detail	N3	N4	N5
integrity and dependability	N3	N4	N5
Discipline and keeping commitments	N3	N4	N5
Information security in the work process	N3	N4	N5
Using cloud platforms	N3	N4	N5
Information security awareness	N3	N4	N5
Learning from mistakes and incidents	N2	N3	N4
Professional currency and specialist literature	N2	N3	N4
Writing technical documentation	N2	N3	N4
System administration and monitoring	N3	N3	N3
Release management and deployment	N2	N3	N4
Process automation	N2	N3	N4
Emergency and crisis organisation	N2	N3	N4

Skill	junior	medior	senior
Service calls and telephone contact	**N2**	**N3**	**N4**
Data classification and retention	**N2**	**N3**	**N4**

4 The proficiency scale

Level	Label	Autonomy	Complexity	Scope	Depth of knowledge
N1	**Guided**	works under supervision and follows instruction	routine, one variable at a time	own task	basic understanding of terminology
N2	**Applying**	works independently within set frameworks	familiar situations with limited variation	own role	working knowledge, applies standard approach
N3	**Proficient**	sets own approach and seeks input proactively	several variables, some ambiguity	own team or process	thorough knowledge, weighs alternatives
N4	**Advanced**	directs others and decides on the approach	complex, with conflicting interests	several teams or a department	in-depth knowledge, advises others
N5	**Leading**	sets the standard and the policy	strategic, under high uncertainty	organisation, value chain or profession	authority, advances the profession

5 Behavioural anchors per skill

Anchors sit at N1, N3 and N5. N2 and N4 are deliberately not anchored: raters interpolate between them, following the O*NET convention.

Skill	N1	N3	N5
Security incident response Acts on a security incident following the runbook by containing it, preserving evidence, recovering and informing the right parties in time.	Reports a suspected incident immediately, touches nothing and follows the coordinator's instructions.	Independently limits damage during an incident, preserves evidence and delivers a traceable timeline of events.	Leads the organisation wide response team, decides on external communication and improves the runbook after every exercise.
Problem analysis Breaks a problem into parts, separates causes from effects and states which information is needed to move forward.	States precisely what deviates in a malfunction and which data are missing, and puts this to the supervisor.	Splits a recurring complaint into possible causes, tests these with own data and names the most likely cause.	Traces persistent organisational problems back to a few root causes and sets the analysis method that other teams will use.

Skill	N1	N3	N5
Critical thinking and source evaluation Tests claims for logic, evidence and the interest of the source and thereby distinguishes facts from opinions and assumptions.	Asks what a claim is based on and checks whether the source is named and can be found.	Detects fallacies and selective evidence in reports and states which conclusion the data do support.	Sets the assessment criteria for sources and claims, including for texts made by artificial intelligence, and enforces them organisation wide.
Stress tolerance Keeps delivering work of the same quality under time pressure, opposition or unexpected turns and maintains a businesslike tone with others.	Keeps working on the current task as pressure rises and asks the supervisor which task can wait.	Keeps working in a structured way at peak load, keeps agreements with clients clear and flags early which results are at risk.	Keeps the organisation workable in crises, takes decisions under high uncertainty and sets the standard for composed action under pressure.
Data analysis Prepares and analyses data sets to find patterns, relationships and outliers and connects the outcomes to the original question.	Carries out a predefined analysis step on a supplied data set and records the outcome in the agreed format.	Selects analysis methods for an open question, turns raw data into a working file and supports every conclusion with figures.	Sets the organisation's analysis standards, reviews the analyses of others and establishes new analysis methods in the profession.
Basic networking knowledge Knows how networks work at a high level such as addressing, routing, ports and name resolution and states where a connection problem may arise.	Explains which parts make up a connection and performs a provided check such as a connectivity test.	Deduces from symptoms in which network layer a problem sits and supports that with own measurements.	Disseminates networking knowledge in the organisation, sets design principles and reviews network designs from suppliers.
Incident management and troubleshooting Takes in disruptions, establishes the cause through targeted steps, restores the service and keeps reporters and stakeholders informed.	Logs a disruption completely, works through the standard steps and escalates as soon as own steps do not work.	Sets an investigation line for an unfamiliar disruption, restores the service and records cause and solution for reuse.	Designs the organisation's incident process, leads the response to major disruptions and accounts for it to management and clients.

Skill	N1	N3	N5
Threat and risk analysis Maps threats, weaknesses and consequences for a system or process, weighs likelihood against impact and names appropriate measures.	Completes a risk inventory using a given list of threats and submits the outcome to the specialist.	Independently performs a threat analysis on an application, prioritises risks and advises on measures with costs and effect.	Determines the organisation's risk appetite and analysis method and accounts for the security risk picture to the board.
Access and identity management Grants permissions based on role and necessity, periodically reviews who can access what and withdraws rights on change or departure.	Processes access requests according to the established role scheme and records every change.	Designs roles and permissions for an application, carries out the periodic review and corrects excessive access.	Sets the organisation's access policy and accounts for the control of permissions in audits.
Information gathering and filtering Searches purposefully for data in several sources, selects what is relevant to the question and leaves other information out.	Looks up the requested data in the designated sources and delivers them in full and with source references.	Chooses sources independently for an open question, filters out duplicate and outdated data and justifies that choice.	Designs the information flows for the whole field, decides which sources are authoritative and cuts redundant reporting.
Accuracy and attention to detail Works carefully, checks own work for errors and keeps to agreements about completeness and correctness of data.	Goes through the own work with a checklist and repairs errors found before the work is passed on.	Builds check moments into the own process, keeps track of errors and prevents repetition by adjusting the method.	Sets the standards for completeness and correctness, has samples checked and addresses teams on structural sloppiness.
integrity and dependability Acting in line with applicable standards and agreements, also without supervision, and being transparent about own interests, mistakes and doubtful cases.	Keeps to agreements and rules of conduct made and reports an own mistake to the manager.	Reports a possible conflict of interest on own initiative and asks for review before a decision is taken.	Sets the organisation's integrity standards, enforces them also with influential parties and explains the resulting choices publicly.

Skill	N1	N3	N5
Discipline and keeping commitments Sticks to agreements, procedures and commitments even without supervision, and reports in good time when a commitment turns out to be unachievable.	Arrives at the agreed time with the agreed work and reports any delay to the supervisor.	Commits only to what is feasible, tracks own commitments and informs those involved as soon as a deadline comes under pressure.	Anchors the standard for reliable follow through in working agreements and addresses anyone at any level who lets that standard slip.
Information security in the work process Applies security measures in daily work such as safe sharing, classifying and storing information and flags risky working practices.	Follows the security rules for sharing and storing information and reports a suspected incident immediately.	Weighs security risks when setting new working agreements, adjusts measures and addresses colleagues on unsafe behaviour.	Sets information security policy and monitors organisation wide that processes meet the requirements set.
Using cloud platforms Sets up and manages services in a cloud environment, arranges permissions and costs and chooses between available service types based on requirements.	Uses existing cloud services as instructed and reports unusual behaviour or unexpected costs to the administrator.	Independently configures cloud services for an application, arranges permissions and backups and keeps costs and usage in view.	Determines the organisation's cloud strategy and decides which workloads are placed where.
Information security awareness Knows the most common threats such as phishing, ransomware and deception, recognises their signals and knows which action is then expected.	Recognises an obvious phishing message, does not click and reports the message through the designated channel.	Explains to colleagues how threats work, judges doubtful cases independently and adapts own behaviour to new threats.	Designs the organisation's awareness programme, measures its effect and adjusts the approach based on measured results.
Learning from mistakes and incidents Investigates after an error or incident what happened, names the cause without shifting blame and changes the working method on that point.	Reports an own error to the supervisor at once and repeats the task following the corrected instruction.	Analyses own errors and those of the team, discusses the cause openly in the work meeting and adjusts the agreements.	Ensures incidents are reported safely across the organisation, has causes analysed structurally and works the lessons into policy and standards.

Skill	N1	N3	N5
Professional currency and specialist literature Follows developments in the own profession through literature, guidelines and networks and works relevant new insights into own practice.	Reads the professional information received and names which part matters for the own work.	Tracks sources and guidelines structurally, weighs their quality and adapts the own working method to new insights.	Assesses the state of the field, weighs conflicting research and determines which guidelines the organisation will follow from now on.
Writing technical documentation Writes manuals, support documentation and decision records that a reader without prior knowledge can follow step by step and that stay current.	Completes a documentation template with the steps of a task and has the text checked by a colleague.	Writes complete documentation for a system or process, tests it with an unfamiliar reader and maintains versions.	Sets the organisation's documentation standard and ensures documentation is part of every delivery.
System administration and monitoring Keeps systems running by managing settings, updates and permissions, sets up monitoring and acts on signals before users are affected.	Performs scheduled maintenance tasks and updates according to the runbook and reports deviations in monitoring signals.	Independently manages a system environment, sets monitoring thresholds and removes recurring causes of disruptions.	Sets the organisation's administration and monitoring standards and decides on the design of the system environment.
Release management and deployment Plans and carries out the rollout of new versions, checks operation before and after and ensures a rollback stays possible.	Executes the steps of a rollout plan and reports immediately when a step does not give the expected result.	Draws up a rollout plan with a fallback option, aligns with stakeholders and verifies after rollout that the service works.	Sets the organisation's release policy, decides on rollout windows and structurally improves the lead time of changes.
Process automation Analyses a recurring work process, builds or commissions automation of its steps and checks that the outcome stays reliable.	Runs an existing automation and reports when the outcome differs from what was expected.	Describes a process in steps, automates the repeatable steps and builds in checks on errors and exceptions.	Determines the organisation's automation agenda and decides which processes are and are not automated.

Skill	N1	N3	N5
Emergency and crisis organisation Works according to crisis plans during incidents, fills a role in the crisis organisation and ensures situation assessment, decision making and recording.	Knows own role in the emergency plan and carries out the assigned tasks according to instruction during an exercise.	Independently fills a role in a crisis team, keeps the situation picture current and ensures decisions are recorded.	Designs the crisis organisation and the training and exercise cycle and leads the evaluation after a real emergency.
Service calls and telephone contact Handling client contacts by telephone and chat with a fixed structure, controlled questioning and a closing that contains a concrete agreement.	Answers according to the script, registers the question in the system and transfers the caller to the right colleague.	Settles unusual questions within a single call, keeps call time under control and audibly summarises the agreement made.	Designs conversation models and quality standards for the contact centre and reviews recordings to support coaching and system choices.
Data classification and retention Classifies information by sensitivity and importance, links retention periods to it and ensures deletion and archiving actually happen.	Assigns a classification label according to the scheme and refers unclear cases to the administrator.	Determines classification and retention period for an information flow and checks whether clean up happens as planned.	Designs the organisation's classification and retention policy and accounts for it in audits and supervision.

6 Assessment methods and validity

The validities are the corrected meta-analytic estimates from Sackett, Zhang, Berry and Lievens (2022) in the Journal of Applied Psychology, which replace the older Schmidt and Hunter (1998) figures. The spread matters as much as the mean: with a high SD, validity varies strongly by context.

Assessment method	rho	SD	What it is
Simulation	-	-	Simulated work situation, usually digital, with standardised scoring.
Assessment centre	**0.29**	**0.09**	Multiple exercises, multiple assessors, dimension-wise scoring.
Work sample test	**0.33**	**0.09**	The candidate performs a representative work sample under standardised conditions.
Personality questionnaire	**0.40**	**0.15**	Self-report of behavioural preferences. At hrmforce the Big Fifty and the 15PF.
Knowledge test	**0.40**	**0.13**	Test of declarative job knowledge, usually assembled per client.
Situational Judgement Test	**0.12**	**0.11**	Scenario with response options, scored on knowledge or behavioural tendency.
Portfolio or evidence	-	-	A collection of prior work or results, assessed against fixed criteria.

7 Assessment instruments for this job

hrmforce instrument	Skills	What it measures
Work sample test	**14**	Representative work sample under standardized conditions
Knowledge test (client-specific)	**12**	Professional knowledge test, customized for each client
Competency Check	**5**	Behavioral-Level Competency Assessment
360 Feedback	**4**	Multiple assessments based on behavioral anchors
Big Fifty	**3**	Personality questionnaire, 150 items, 25 factors
Portfolio	**3**	Evaluation of prior work against fixed criteria
Ability Scan	**2**	Aptitude Test: Verbal, Numerical, and Abstract Reasoning Skills
15PF	**2**	Personality Profile, a shorter alternative to the Big Fifty
Mental Resilience (4C)	**1**	Mental Resilience According to the 4C Model

hrmforce instrument	Skills	What it measures
Big Fifty (Integrity Scale)	1	
Structured interview	1	Behavioral interview with a fixed structure
Communication Styles	1	Preferred communication style

8 How to use this profile

1. Agree the profile with the hiring manager before the first candidate is measured. Weights shifted afterwards make the outcome indefensible.
2. Choose the assessment method per skill from the Assessment method column. Combine at most three methods per candidate.
3. Calibrate the assessors in a two-hour session using the anchors in chapter 5. Anchors without rater training deliver little.
4. Fill in the match calculator and discuss the gaps in the development conversation. Type A and type G are selection criteria, not one-quarter development goals.

Source: hrmforce Skills Framework 2.0, version 2.0.0, built 2026-09-08. Crosswalks to 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 and the Dutch CBS occupational classification BRC 2014 edition 2025. This profile is a starting point, not a standard: align it with your own organisation before selecting on it.