

AI CYBERSECURITY SKILLS SELF- ASSESSMENT CHECKLIST

Assess your capabilities, identify skill gaps, and plan your next step in AI security

A practical checklist for cybersecurity professionals, AI practitioners, and
aspiring specialists

1. Introduction

1.1 Purpose of the self-assessment checklist

This checklist helps you assess your current cybersecurity and AI security capabilities, recognise strengths, and identify areas that need practice. Use the results to build a focused learning plan and collect evidence of progress. This is a self-reflection tool, not a formal exam or validated measure of professional competence.

1.2 Who should use this checklist

Cybersecurity analysts and security operations professionals expanding into AI-enabled security.

IT, cloud, application security, and risk professionals who work with AI systems.

AI practitioners building security, privacy, and governance knowledge.

Students, career changers, and early-career professionals exploring AI cybersecurity roles.

Experienced practitioners planning a specialisation in AI security, threat analysis, or governance.

1.3 How to use the checklist

Rate each skill based on what you can demonstrate, not only what you have read.

Record a lab, incident, project, report, or example supporting each rating where possible.

If you have not had an opportunity to practise a skill, note that rather than guessing.

Calculate each area score and your overall score; compare them with your target role.

Select three priority skills and schedule practical learning activities.

Repeat the assessment after 8–12 weeks and compare ratings with new evidence.

1.4 Self-assessment rating scale

Rating	Level	Description
1	Beginner	Recognise some terms but need guidance to explain or perform the skill.
2	Developing	Understand basics and complete simple tasks with support.
3	Competent	Apply the skill independently in common, well-defined situations.

4	Proficient	Apply the skill reliably in complex situations and explain decisions.
5	Advanced	Handle novel or complex situations, evaluate trade-offs, and guide others.

2. Cybersecurity Skills Self-Assessment

Rate each skill from 1 to 5. Use the evidence column for a practical example, lab, tool, project, or report.

2.1 Cybersecurity Fundamentals

Skill statement	Rating (circle one)	Evidence / example
Understanding common cyber threats and attacks	1 2 3 4 5	
Identifying vulnerabilities and security risks	1 2 3 4 5	
Understanding security principles and best practices	1 2 3 4 5	
Knowledge of incident response basics	1 2 3 4 5	

Area total: ____ / 20 Average: ____ / 5 Notes: _____

2.2 AI and Machine Learning Fundamentals

Skill statement	Rating (circle one)	Evidence / example
Understanding basic AI and machine learning concepts	1 2 3 4 5	
Recognising how AI is used in cybersecurity	1 2 3 4 5	
Understanding the limitations of AI-generated results	1 2 3 4 5	
Identifying potential risks in AI-driven security systems	1 2 3 4 5	

Area total: ____ / 20 Average: ____ / 5 Notes: _____

2.3 AI-Powered Threat Detection

Skill statement	Rating (circle one)	Evidence / example

Understanding AI-driven threat detection tools	1 2 3 4 5	
Analysing unusual user or system behaviour	1 2 3 4 5	
Identifying suspicious patterns and anomalies	1 2 3 4 5	
Reviewing AI-generated alerts before taking action	1 2 3 4 5	

Area total: ____ / 20 Average: ____ / 5 Notes: _____

2.4 Security Operations and Incident Response

Skill statement	Rating (circle one)	Evidence / example
Understanding SOC workflows	1 2 3 4 5	
Reviewing and prioritising security alerts	1 2 3 4 5	

Using AI to support incident investigation	1 2 3 4 5	
Validating AI-generated incident response recommendations	1 2 3 4 5	

Area total: ____ / 20 Average: ____ / 5 Notes: _____

2.5 Generative AI and LLM Security

Skill statement	Rating (circle one)	Evidence / example
Understanding common generative AI risks	1 2 3 4 5	
Recognising prompt injection and data leakage risks	1 2 3 4 5	
Identifying insecure AI application configurations	1 2 3 4 5	

Understanding the OWASP Top 10 for LLM Applications	1 2 3 4 5	
---	-----------	--

Area total: ____ / 20 Average: ____ / 5 Notes: _____

2.6 Cloud, Application and Data Security

Skill statement	Rating (circle one)	Evidence / example
Understanding cloud security fundamentals	1 2 3 4 5	
Identifying application vulnerabilities	1 2 3 4 5	
Applying data protection principles	1 2 3 4 5	
Recognising risks when integrating AI with business systems	1 2 3 4 5	

Area total: ____ / 20 Average: ____ / 5 Notes: _____

2.7 AI Governance, Risk and Compliance

Skill statement	Rating (circle one)	Evidence / example
Understanding responsible AI principles	1 2 3 4 5	
Identifying privacy, bias and transparency risks	1 2 3 4 5	
Understanding AI risk assessment and governance	1 2 3 4 5	
Recognising relevant security and compliance requirements	1 2 3 4 5	

Area total: ____ / 20 Average: ____ / 5 Notes: _____

2.8 Scripting, Automation and Technical Skills

Skill statement	Rating (circle one)	Evidence / example
Understanding basic scripting concepts	1 2 3 4 5	

Using automation to support security workflows	1 2 3 4 5	
Interpreting security logs and technical data	1 2 3 4 5	
Evaluating automated security actions before implementation	1 2 3 4 5	

Area total: ____ / 20 Average: ____ / 5 Notes: _____

3. Calculate Your Assessment Score

3.1 Record your score for each skill area

Each area has four skills. Add the ratings for a total from 4 to 20; divide by four for the average.

Skill area	Total score	Average	Priority / notes
1 Cybersecurity Fundamentals	___ / 20	___ / 5	
2 AI and Machine Learning Fundamentals	___ / 20	___ / 5	
3 AI-Powered Threat Detection	___ / 20	___ / 5	
4 Security Operations and Incident Response	___ / 20	___ / 5	

5 Generative AI and LLM Security	___ / 20	___ / 5	
6 Cloud, Application and Data Security	___ / 20	___ / 5	
7 AI Governance, Risk and Compliance	___ / 20	___ / 5	
8 Scripting, Automation and Technical Skills	___ / 20	___ / 5	

3.2 Calculate your overall score

There are 32 skill statements. Add all ratings for a total from 32 to 160, then divide by 32 for the overall average out of 5.

Calculation	Your result
Sum of all 32 ratings	___ / 160
Overall average = total ÷ 32	___ / 5

Skills rated 1 or 2	_____
Skills rated 4 or 5	_____

Example: a total of 112 gives an average of 3.5 out of 5. Use the score as a reflection aid, not as a stand-alone hiring or certification decision.

3.3 Identify your strongest skills

Strong skill	Rating	Evidence / result	How I can use this strength
1.			
2.			
3.			

3.4 Identify your biggest skill gaps

Skill gap	Rating	Why it matters	First improvement step
1.			

2.			
3.			

4. Understand Your Results

Use your average as a starting point, then review individual ratings. A strong overall score can hide a critical gap in incident response, privacy, or LLM security.

4.1 Beginner: Build your cybersecurity and AI foundations

If most ratings are 1, focus on common attacks, security principles, networking and logs, introductory AI/ML concepts, and safe lab practices. Practise explaining key terms in your own words.

4.2 Developing: Strengthen practical knowledge

If many ratings are 2, turn concepts into guided practice: work through beginner labs, review sample alerts, follow an incident-response walkthrough, and learn how AI outputs can be wrong or incomplete.

4.3 Competent: Apply skills through hands-on exercises

If many ratings are 3, practise complete workflows independently. Investigate sample alerts, validate AI recommendations against evidence, test an AI application in an authorised lab, and document findings.

4.4 Proficient: Develop advanced technical capabilities

If many ratings are 4, practise complex scenarios, threat modelling, secure AI integration, detection tuning, automation safeguards, and incident exercises. Seek peer review and measure the quality of decisions.

4.5 Advanced: Focus on specialisation and strategic leadership

If many ratings are 5, deepen a specialisation such as LLM red teaming, AI security engineering, threat detection, or governance. Mentor others and connect technical controls to business risk. Keep ratings evidence-based.

5. AI Cybersecurity Career Readiness

Role requirements vary by employer, industry, seniority, and regulation. Use these profiles as starting points, then compare them with current job descriptions.

5.1 AI Security Engineer

Secures AI applications, APIs, identities, data flows, and deployment configurations.

Relevant skills: LLM security, cloud/application security, data protection, scripting, threat modelling.

Current strengths	Areas to develop	Evidence / next action
-------------------	------------------	------------------------

5.2 AI Threat Analyst

Investigates suspicious activity, interprets threat intelligence, detects anomalies, and validates AI-assisted findings.

Relevant skills: Cybersecurity fundamentals, threat detection, log analysis, critical review of AI output.

Current strengths	Areas to develop	Evidence / next action
-------------------	------------------	------------------------

5.3 AI SOC Analyst

Triages alerts, correlates events, supports investigations, and validates automated recommendations.

Relevant skills: SOC workflows, incident response, alert prioritisation, automation safeguards.

Current strengths	Areas to develop	Evidence / next action
-------------------	------------------	------------------------

5.4 Generative AI Red Teamer

Tests AI applications with authorisation for prompt injection, data exposure, unsafe outputs, and control weaknesses.

Relevant skills: LLM risks, application security, structured testing, safe evidence handling.

Current strengths	Areas to develop	Evidence / next action
-------------------	------------------	------------------------

5.5 AI Governance Specialist

Assesses AI risks, documents controls, and coordinates compliance and oversight.

Relevant skills: Governance, privacy, bias/transparency, risk assessment, stakeholder communication.

Current strengths	Areas to develop	Evidence / next action
-------------------	------------------	------------------------

Career readiness comparison

Target role	Relevant skill areas	Current evidence	Top gap / next action
AI Security Engineer			
AI Threat Analyst			
AI SOC Analyst			

Generative AI Red Teamer			
AI Governance Specialist			

6. Personal Skills Development Plan

6.1 Select three priority skills to improve

Choose skills based on risk, role requirements, and current ratings. Prioritise critical gaps even if they are not your lowest-rated items.

6.2 Set specific learning objectives

Make each objective observable. Example: “Complete an authorised prompt-injection lab, document three findings, and explain one mitigation for each by the target date.”

6.3 Identify hands-on labs or practice projects

Review and triage synthetic security alerts.

Analyse sample authentication or application logs and explain suspicious patterns.

Create a threat model for a simple AI-enabled application.

Test a deliberately vulnerable demo AI application in an authorised environment.

Write an incident report based on a simulated event.

Create a small script to parse non-sensitive sample logs and validate its output.

Draft a risk register for an AI feature, including privacy, security, and human-oversight controls.

6.4 Set target completion dates

6.5 Track progress and reassess skills

Priority skill	Specific learning objective	Lab / project / support	Measure of success	Target date	Status
1.					Not started
2.					Not started
3.					Not started
Review date	Practice completed	Evidence / feedback	Updated rating (1-5)	Next action	

7. Practical Action Checklist

Use only authorised environments and synthetic or approved data. Do not test systems without explicit permission.

7.1 Practise analysing security alerts

Use a training dataset or simulated alerts.

Record the alert, context, possible explanations, and evidence needed.

Prioritise the alert and explain your reasoning.

Independently validate any AI-generated conclusion before recommending action.

Alert / scenario	Evidence reviewed	Assessment / priority	Validation needed	Outcome
---------------------	----------------------	--------------------------	----------------------	---------

7.2 Explore AI-powered threat detection tools

Choose a vendor demo, training lab, or approved tool.

Identify what signals the tool uses and what the alert means.

Review false-positive and false-negative possibilities.

Record where analyst judgement or more evidence is needed.

Tool / feature	Signal or alert	Potential limitation	How to validate	Learning note
----------------	-----------------	----------------------	-----------------	---------------

7.3 Test an AI application for common security risks

Use a deliberately vulnerable training app or environment you are authorised to test.

Review input handling, access controls, data exposure, and prompt-injection resilience using benign tests.

Avoid accessing real secrets or other users' data.

Record observed behaviour, potential impact, and safe remediation recommendations.

Test area	Test prompt / action	Expected safe behaviour	Observed result	Finding / remediation
Prompt injection				
Sensitive data handling				
Access control				

Unsafe or unsupported output				
------------------------------	--	--	--	--

7.4 Review an AI security incident scenario

Scenario: a security assistant flags an unusual sign-in and recommends disabling an account. The alert contains limited context, and the user has a legitimate travel pattern.

Practise validating evidence before acting.

List evidence to collect: sign-in history, device details, MFA events, and related alerts.

Identify the risks of acting immediately and of ignoring the alert.

Write a decision path including verification, escalation, and containment options consistent with policy.

Explain which parts of the AI recommendation you accept, reject, or need to verify.

Question	Your notes
Evidence needed	
Possible false-positive explanation	
Risk of immediate action	

Risk of inaction	
Validation / escalation steps	
Final recommendation and rationale	

7.5 Document practical projects and learning outcomes

Record what you did, the environment, finding, recommendation, and lesson learned.

Do not include credentials, private data, or sensitive production details.

Date	Project / activity	Skills demonstrated	Evidence / result	Lesson / next step
------	-----------------------	------------------------	----------------------	-----------------------

Final Review and Next Steps

Review completed assessment areas

I rated all eight skill areas and all 32 skill statements.

I calculated each area score and my overall average.

I identified strengths and supporting evidence.

I identified skill gaps and considered role relevance.

I compared my skills with at least one target role.

I selected three priority skills and measurable learning objectives.

I scheduled practice and set target dates.

I chose a date to reassess my skills.

Identify remaining skill gaps

Remaining gap	Why it matters	How I will address it	Target date

Update your AI cybersecurity learning plan

Review progress every 8–12 weeks. Update ratings when you have new evidence such as a completed lab, project, peer review, or demonstrated improvement. Adjust your plan when your target role or responsibilities change.

Review date	Skill rating changed	Evidence supporting change	Plan adjustment
-------------	-------------------------	-------------------------------	-----------------

Explore professional development and certification options

Choose learning options that match your skill gaps and career direction. Consider structured courses, supervised labs, security community activities, portfolio projects, and relevant certifications. Before enrolling, check the current syllabus, prerequisites, assessment method, and recognition.

GSDC option: consider exploring the Certified Generative AI in Cybersecurity certification if its current scope aligns with your goals. Review the official program details against the skills you want to develop. Completing a certification alone does not establish practical competence.

Next Steps

Choose one skill gap and schedule a hands-on practice session.

Complete one authorised lab or small project and save a safe, sanitised record.

Ask a peer, mentor, or manager to review your reasoning and evidence.

Reassess after 8–12 weeks and update your plan.

My first priority skill is _____. I will practise by _____ before
_____. I will measure progress by _____.

CERTIFICATION IN GENERATIVE AI IN CYBERSECURITY

**AGENTIC AI DEVELOPER
CERTIFICATION BASED ON REAL-
WORLD AGENT FRAMEWORKS TO
DESIGN, BUILD, AND DEPLOY
AUTONOMOUS AI SYSTEMS.**



ABOUT GSDC CERTIFICATION



LIFETIME VALIDITY

GSDC Certification is an globally accredited certification with lifetime validity.



EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.



CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.



LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

LEARNING OBJECTIVE

- Make an impact in the cutting-edge field of artificial intelligence.
- Validate your generative AI application skills.
- Encourage the development of generative AI technologies.

Enroll now with the
code **LEARN20** To
avail **20%** discount

Enroll Now



www.gsdcouncil.org