TUTIVRA

CAREER TOOLKIT · GUIDED CYBERSECURITY PROJECTS

8 guided projects that turn "no experience" into proof.

Step-by-step portfolio projects for SOC, incident response, vulnerability management, IAM, GRC, cloud, detection engineering and application security. Each one produces a piece of work you can show, explain and defend in an interview.

8	7	Free	3–8 hrs
guided projects	target roles	tools & labs	per project

© Tutivra · tutivra.com · For personal use by the purchaser. Worked examples use a fictional company and synthetic data and are labeled as training examples. Build and document your own work; never present an example as your own experience.

START HERE

How to use this pack

Hiring managers can't see your GPA or your study hours. They can see a project that shows how you think. Every project here follows the same pattern: a realistic scenario, clear steps, the evidence to capture, a worked example of finished work, and the words to use on your resume and in interviews.

Project 1 · SOC alert triage casebook	SOC Analyst · Beginner
Project 2 · Phishing investigation & response	SOC / IR · Beginner
Project 3 · Vulnerability-to-remediation lifecycle	Vulnerability Mgmt · Beginner
Project 4 · IAM joiner-mover-leaver review	IAM Analyst · Beginner
Project 5 · GRC control assessment & vendor risk	GRC Analyst · Beginner
Project 6 · Cloud configuration review	Cloud Security · Beginner+
Project 7 · Detection rule development & validation	SOC / Detection · Intermediate
Project 8 · Web application security assessment	AppSec · Beginner+

Which projects should I do?

YOUR TARGET ROLE	DO THESE, IN ORDER
SOC Analyst / Cybersecurity Analyst	1 → 2 → 7
Incident Response Analyst	2 → 1 → 7
Vulnerability Management Analyst	3 → 8 → 6
IAM Analyst	4 → 5 → 6
GRC Analyst	5 → 4 → 3
Cloud Security	6 → 4 → 3
Application Security	8 → 3 → 7

Two or three finished, well-documented projects beat eight half-finished ones. Going for AI security roles? Pair these with the **AI Security Track**.

GROUND RULES (READ BEFORE STARTING)

- **Only test what you own or are authorized to use:** your own lab, a free vendor sandbox, or a purpose-built training platform.
- **Never use real personal, employer or customer data.** Every scenario uses the fictional company Kestrel Supply Co.
- **Separate observations from conclusions.** "7 failed logins then a success" is an observation; "compromised account" is a conclusion that needs evidence.
- **The worked examples show the standard, not the answer.** Your evidence, wording and findings must be your own.

The scenario company used in every project

Kestrel Supply Co. (fictional) is a 900-employee distribution company with offices in two states. It uses Microsoft 365 and Entra ID for identity, Windows laptops, a few Linux servers, a customer web portal, a small Azure footprint, and several SaaS vendors. A 4-person security team relies on junior analysts to triage alerts, review access and track risks. That's the job you're practicing.

PROJECT 1 · SOC ANALYST

SOC alert triage casebook

Triage is the core SOC skill: look at an alert, gather context, decide what it means, and write it up so the next person can act. You'll build a small casebook of triaged alerts from your own lab.

Time	Level	Tools	Output
3–5 hours	Beginner	Wazuh or Microsoft Sentinel, Windows Event Viewer, spreadsheet	3-case casebook + evidence log

The scenario

Kestrel's SIEM raises an alert: *multiple failed sign-ins followed by a success* on a finance user's laptop. Your job is to decide whether it's a forgotten password or something worse, and document your reasoning.

Steps

1. **Set up a safe lab.** One Windows VM sending logs to Wazuh (free) or a Sentinel trial workspace. Create a dedicated lab account and note what "normal" sign-in looks like.
2. **Generate benign test activity.** On your own lab machine only: several failed sign-ins, then a success. Optionally use a vendor training dataset instead.
3. **Collect the evidence.** Timestamps, username, host, source IP (if present), Windows Event IDs (4625 failed, 4624 success) and logon type.
4. **Build a timeline.** Put events in order. Is this a typo burst or a machine-speed pattern? Same source or many?
5. **Correlate and note gaps.** What else would you check in a real environment (MFA result, new device, what happened after login)? Write down what's missing before deciding severity.
6. **Write the triage ticket:** disposition (true positive / benign true positive / false positive), confidence, rationale and escalation threshold.
7. **Repeat for two more cases** (e.g. a new local admin account, suspicious PowerShell) to make a 3-case casebook.

Evidence to capture

- ☐ Dashboard filtered to your lab host showing time, rule, source and severity
- ☐ Timestamped evidence log (spreadsheet)
- ☐ One triage ticket per case
- ☐ Decision table: observation → interpretation → action

WORKED EXAMPLE · TRAINING ONLY

CASE SOC-001 · Simulated sign-in anomaly

OBSERVATION	INTERPRETATION	ACTION
7 × Event 4625 over 4 minutes, then 1 × 4624, same lab account and host	Pattern worth validating; consistent with a typo burst *or* guessing	Check source and logon type
Logon type 2 (interactive), local console, business hours	Points toward a user at the keyboard, not remote guessing	Confirm with account owner
No new processes or admin activity after login	No evidence of follow-on activity	Close as benign true positive; tune threshold

Disposition: Benign true positive (training scenario). Confidence: medium. **Escalate if:** remote logon type, unfamiliar source, or post-login admin activity.

Resume bullet (only once you've done it)

"Built a home SOC lab with [Wazuh/Sentinel] and documented [3] alert triage cases using Windows Event IDs 4624/4625, timelines and evidence-based dispositions with escalation criteria."

Interview talking points

- **"Walk me through how you triage an alert."** Use this case: understand → gather context → validate → decide → document.
- **"Why didn't you just disable the account?"** Because the evidence didn't support it yet. Act on evidence, and know your escalation threshold.

References: Wazuh quickstart · Microsoft Sentinel incident training · CyberDefenders blue team labs

You just finished 1 of 13 guided projects.

If this project helped, the full Career Toolkit gives you everything else you need to land your first security role.

IN THE FULL TOOLKIT	WHAT IT GIVES YOU
12 more guided projects	Phishing investigation, vulnerability prioritization, IAM access review, GRC vendor assessment, cloud configuration review, detection engineering, web app security, plus 5 AI security projects
AI Security Track	3 AI career pathways, a 90-day plan, 35+ AI job titles and the 5 AI projects
16 resume documents	8 role templates + 8 completed examples, including AI Security and Vulnerability Management
Interview Question Bank	105 questions with what the interviewer is testing and strong answer outlines
Career Launch Playbook	8 career pathways, plus the Career Changer Translation Guide for 10 backgrounds
Job search system	100+ hidden job titles, 15 staffing firms, 50+ employers known for early-career hiring, outreach templates and a tracker

Get the complete Career Toolkit: one-time $39, instant download.
tutivra.com/toolkit

Free tools: find your role at tutivra.com/quiz · build job searches at tutivra.com/jobs