

Your first ninety days

The role is the reward for everything else. This is how you make the first three months count, and how you turn them into a record you can use.

Nobody expects you to contribute meaningfully in month one. They do expect you to learn deliberately, ask good questions, and write things down. Almost everything that makes the first ninety days go badly comes from waiting to be told rather than going and finding out.

1 · THE CONVERSATION TO HAVE IN WEEK ONE

Most people never explicitly ask what success looks like. Then they are surprised at their probation review.

Book thirty minutes with your manager in the first week and ask these. Write the answers down in their words, and re-read them at day 60.

- ☐ What does good look like in this role, in your words?
- ☐ What is the thing most likely to go wrong in my first three months?
- ☐ Who should I meet that I would not think to ask for?
- ☐ What is the team's biggest frustration right now?
- ☐ Where do you want me spending my time by month three?
- ☐ What is not written down that I need to know?

WHAT MY MANAGER SAID GOOD LOOKS LIKE, IN THEIR WORDS

2 · STAKEHOLDER MAP

Security is a function that only works through other people. Map them early, before you need anything from them.

Who	Name	What they need from security	Met on
Your line manager			
Your manager's manager			
IT operations lead			
The busiest engineering team			
Whoever owns risk or compliance			
Service desk lead			

A peer who joined in the last year			
------------------------------------	--	--	--

3 · THE NINETY DAYS

Tick as you go. The target dates matter more than the order.

DAYS 1-30

Orientation. Read, ask, and resist the urge to fix anything yet.

TARGET DATE

- ☐ Read all team policies, standards, and process documentation

Done when: Summary notes produced for key documents

- ☐ Understand the current threat landscape and team priorities

Done when: Can describe the top three team priorities without prompting

- ☐ Identify key stakeholders outside the team

Done when: Stakeholder map drafted with names, roles, and relationships

- ☐ Meet key contacts in IT operations and relevant business units

Done when: At least five cross-functional relationships established

- ☐ Understand how security decisions are made and risk is accepted

Done when: Can describe the governance process and key decision-makers

- ☐ Complete organisation-specific onboarding and access setup

Done when: All systems access in place; compliance training complete

DAYS 31-60

Contribution. Take ownership of something small and finish it.

TARGET DATE

- ☐ Take ownership of first specific work task or project

Done when: Deliverable completed, reviewed, and submitted

- ☐ Produce first written output (report, risk assessment, or briefing)

Done when: Document reviewed by manager before circulation

- ☐ Attend and actively contribute to team meetings and governance processes

Done when: Have spoken in at least one meeting with something substantive

- ☐ Complete security-tool-specific training for team's primary toolset

Done when: Proficient in the team's core tools without assistance

- ☐ Build working relationship with IT operations team

Done when: Have had at least two substantive conversations with IT ops contacts

- ☐ Identify one quick-win contribution aligned to team priorities

Done when: Quick win identified, proposed to manager, and in progress

DAYS 61-90

Direction. Work out where you add most value, and say so.

TARGET DATE

- ☐ Book 30-60-90 day review meeting with manager
Done when: Meeting scheduled; prepared discussion points
 - ☐ Operating independently on primary day-to-day responsibilities
Done when: Completing core work without requiring guidance on routine tasks
 - ☐ Established working relationships with all key stakeholders
Done when: Can describe each stakeholder's priorities and communication preferences
 - ☐ Clear view of the team's security roadmap and my contribution to it
Done when: Can articulate the next six months of team priorities unprompted
-

4 • KEEP A RUNNING NOTE

Five things worth writing down as they happen. This is the single habit that separates a good first year from an average one.

- ☐ Anything you had to ask twice — it is missing documentation
 - ☐ The steps you worked out for a task nobody had written down
 - ☐ Names, roles and what each person actually needs from security
 - ☐ Every acronym and system name that was not explained to you
 - ☐ Decisions you saw made, and the reasoning behind them
-

Why it matters. Everything you write down here becomes three things later: documentation the team did not have, evidence for your probation and appraisal, and — when you next interview — the specific, dated examples that competency questions are asking for. The version of you sitting in an interview in two years will not remember any of this unless you wrote it down now.

5 • NINETY-DAY REFLECTION

Answer honestly and keep the sheet. It is the raw material for your next appraisal and your next interview.

How has my understanding of this role changed since I started?

Which two or three skills do I most need to develop in the next six months?

What does success look like for me at the twelve-month mark?

What would I tell someone starting this role after me?

Already thinking about the next move?

The question bank covers every domain, and the interview workbook is free alongside it — including a story worksheet you can start filling in now, while the examples are fresh.

ronanblake.co.uk/downloads

From The Honest Guide to Breaking Into UK Cybersecurity, chapter six.