TEKTUT

FREE GUIDE

Your First Steps in Cyber Security

What a cyber analyst actually does — and three things you can try right now, in your browser, for free.

NO EXPERIENCE NEEDED | BROWSER ONLY | 15 MINUTES

BEFORE WE START

You don’t need to be a tech person.

Most people who become cyber analysts did not grow up programming. They were not IT kids. Many came from completely different careers — teaching, the military, banking, customer service, engineering. What they had in common was curiosity, attention to detail, and the willingness to learn a structured skill.

Cyber security is not about being a hacker in a dark room. The reality is far more interesting — and far more accessible — than that.

ALREADY HAVE WHAT IT TAKES?

Before you read on, ask yourself one question: have you ever noticed something suspicious in an email and thought ’that doesn’t look right’? That instinct — spotting something out of place — is the single most important skill a cyber analyst has.

THE REALITY

What a cyber analyst actually does.

A junior cyber analyst — the role you would be working toward — typically spends their day inside a Security Operations Centre, or SOC. Think of it like air traffic control, but for a company’s data and systems.

TIME	TASK	IN PLAIN ENGLISH
Morning	**Alert triage**	Review security alerts that fired overnight. Decide which are real threats and which are false alarms.
Mid-morning	**Phishing investigation**	Analyse suspicious emails reported by staff. Check links, senders, attachments for anything malicious.
Midday	**Team huddle**	Brief stand-up with the team. Share what you found, discuss anything unusual, stay aligned on priorities.
Afternoon	**Log investigation**	Dig deeper into one or two alerts. Piece together what happened, when, and why — like detective work.
End of day	**Documentation**	Write up your findings. Clear, accurate notes matter — they feed into compliance reports and help the next shift.

NO CODING REQUIRED

Notice there is no programming in that list. Junior analysts rarely write code. The job is about observation, investigation, communication and clear thinking — skills that transfer from almost any background.

THE SKILLS

What employers actually look for at entry level.

Here is what comes up consistently in junior analyst job descriptions — and what we train at TekTut:

SKILL	WHY IT MATTERS	CAN YOU LEARN IT?
Attention to detail	Spotting the one suspicious thing in hundreds of normal events	Yes — it sharpens with practice
Understanding networks	Knowing how data moves so you can spot when something moves wrong	Yes — CompTIA Network+
Security fundamentals	Understanding threats, defences, and how attackers think	Yes — CompTIA Security+
Log reading	Making sense of system records to reconstruct what happened	Yes — covered in CySA+
Clear written communication	Writing reports that non-technical managers understand	Yes — you may already have this
Curiosity	The drive to keep asking 'why?' until you find the answer	Hard to teach — but you can develop it

> "The best analysts I have worked with came from non-technical backgrounds. They ask better questions, communicate more clearly, and spot things that people who have always been in IT simply stop noticing."

— Tom Sinclair, Lead Instructor, TekTut Academy

THE REAL BARRIER

Most people are ready to start learning cyber security sooner than they think. The biggest barrier is usually not ability — it is uncertainty about whether this world is really for them. The next section answers that question practically.

YOUR FIRST WINS

Three things to try right now — no experience needed.

Everything below works in any web browser. No software to install. No account needed. Each one takes under 10 minutes and gives you a genuine taste of what real analysts do every single day.

Read the brief explanation before each win — it tells you why this matters in the real world. Then try it. That moment of 'I just did that' is exactly the feeling we want you to have.

WIN 01	Check if your email has been in a data breach
WIN 02	Analyse a suspicious link without clicking it
WIN 03	See what information a website reveals about itself

THESE ARE REAL ANALYST TOOLS

These activities are not games or simulations — they are real tools that security professionals use. When you look up a domain's DNS records or check an IP reputation, you are doing what an analyst does. The only difference is they do it dozens of times a day.

YOUR FIRST WINS

WIN 01

Check if your email has been in a data breach

BROWSER ONLY — NO INSTALL NEEDED 5 minutes

Why this matters to a real analyst:

Data breaches happen constantly — millions of usernames and passwords leaked from compromised websites. One of the first things a SOC analyst does when investigating a potential account takeover is check whether the victim's credentials appear in known breach databases. Have I Been Pwned is the most trusted public tool for this — it is used by governments, IT teams, and security professionals worldwide.

1 Go to haveibeenpwned.com

Open your browser and navigate to haveibeenpwned.com. This site is run by Troy Hunt, one of the most respected names in cyber security.

2 Enter your email address

Type in your own email address and click pwned? The site checks it against a database of over 12 billion compromised accounts.

3 Read the result

If it finds a match, it will tell you which breaches your email appeared in, when they happened, and what data was exposed — passwords, phone numbers, addresses.

4 Check the Passwords tab

Click the Passwords link at the top and enter a password you use (or have used). It will tell you if that exact password has appeared in a breach. This does NOT send your password anywhere — it uses a clever technique called k-anonymity.

WHAT WOULD AN ANALYST DO WITH THIS?

If your email appears in a breach, that is not unusual — most people's do. What matters is whether you are still using those credentials anywhere. This is exactly the conversation a cyber analyst has with employees after an incident.

WIN 02

Analyse a suspicious link without clicking it

BROWSER ONLY — NO INSTALL NEEDED

5–8 minutes

Why this matters to a real analyst:

Phishing — where attackers trick people into clicking malicious links — is the number one way organisations get compromised. Analysts are constantly checking URLs that employees have reported as suspicious. The golden rule: never click a link you do not trust. Instead, you analyse it safely from a distance.

1 **Go to VirusTotal**
Navigate to virustotal.com. This is a free tool owned by Google that checks URLs, files and IP addresses against 70+ security engines simultaneously.

2 **Click the URL tab**
Select the URL tab at the top of the search bar.

3 **Paste a suspicious-looking URL**
Try copying a link from a spam email (without clicking it), or use this test URL: http://malware.wicar.org/data/eicar.com — this is a safe, intentionally flagged test file used in security training.

4 **Read the analysis**
VirusTotal will show you how many security vendors flagged the URL as malicious, what category they put it in, and any related threat intelligence. A real analyst uses this as a first-pass check before investigating further.

YOU JUST USED OSINT

Security analysts call this OSINT — Open Source Intelligence. Using publicly available tools to gather information without touching the target directly is a core analyst skill. You just used it.

WIN 03

See what information a website reveals about itself

BROWSER ONLY — NO INSTALL NEEDED

5 minutes

Why this matters to a real analyst:

When an analyst investigates a suspicious website or email, one of the first steps is looking up the domain — who registered it, when, where it is hosted, what IP address it points to. This information is publicly available and often reveals whether a site is legitimate or a freshly-registered phishing domain.

1 **Go to whois.domaintools.com**

Navigate to whois.domaintools.com — a WHOIS lookup tool used by security researchers and analysts daily.

2 **Look up a domain you know**

Try entering bbc.co.uk or amazon.co.uk. You will see when the domain was registered, who owns it (sometimes hidden behind privacy protection), and where it is hosted.

3 **Now look up a suspicious example**

Notice the registration date. Legitimate companies register domains years in advance. Phishing sites are often registered days or hours before an attack. A brand-new domain claiming to be your bank is a major red flag.

4 **Check the IP address**

Copy the IP address shown and paste it into abuseipdb.com. This tells you whether that IP has been reported for malicious activity. Another tool in a real analyst's daily toolkit.

WHAT YOU JUST DID

You have just done what is called domain reconnaissance — building a picture of a target using public records. Analysts do this dozens of times a day when investigating phishing emails or suspicious traffic on the network.

WHAT'S NEXT

You have already started.

You have just done things that real analysts do. You checked breach data, analysed a suspicious URL, and researched a domain using public records. That is not nothing — that is a foundation.

The structured path from here is clear. CompTIA certifications are the most widely recognised entry-level credentials in UK cyber security hiring. TekTut's Cyber Analyst route takes you through all three — Network+, Security+, and CySA+ — in six months, with live sessions, mentor support, and a direct path to your first role.

01	02	03
CompTIA Network+	**CompTIA Security+**	**CompTIA CySA+**
How networks work	Core security skills	Analyst qualification

The route is structured. The timeline is realistic. The outcome — a job as a junior cyber analyst — is achievable for someone with no IT background. We know because we have seen it happen.

Take the next step

Take our free 8-question Career Route Quiz to find out which path fits you — or book a free 15-minute call with a course advisor.

tektut.academy

CompTIA Authorized Partner · CPD Certified · tektut.academy