

Cybersecurity analyst (fresher)

Company: [Company name]

Location: [Location] | Work mode: [Work mode]

Employment type: Full-time | CTC: [CTC for the full-time role]

Joining: [Joining date] | Apply by: [Apply by]

About [Company name]

[About your company]

About the role

As a fresher cybersecurity analyst in the [Team] team at [Company name], you will watch security alerts, check suspicious emails and logins, and write up what you find. A senior analyst decides what is serious and leads any incident; you collect the facts, follow the runbook and escalate on time. The role focuses on security monitoring and incident triage rather than penetration testing, and it suits someone patient, curious and careful with notes. Working pattern: [business hours only / rotating shifts, including nights and weekends].

What you will do

- Monitor the SIEM alert queue, in a tool such as Splunk or Microsoft Sentinel, and sort each alert as a false alarm, needing more checks or an escalation, following the team's runbook
- Check phishing emails reported by staff by reading the sender, headers, links and attachments with approved tools, record the verdict and reply to the person who reported it
- Review suspicious sign-ins, such as an unusual hour, place or device, or many failures followed by a success, ask the user to confirm through a separate channel if the runbook allows, and escalate a suspected account takeover to a senior at once
- Search firewall, server and sign-in logs for the lines that answer a senior's question, and save them with timestamps in the ticket
- Check endpoint security alerts by finding the machine and the user, noting whether the threat was blocked or cleaned, and passing anything unclear to a senior
- Help a senior review vulnerability scan findings, record the affected system and supporting evidence, track the fix agreed with the system owner and re-check using the approved procedure
- Write incident notes in the ticket tool that say what happened, when, what was checked and who was told, and hand open items to the next analyst or shift with the same notes
- Escalate to the senior analyst through the escalation chart with a short summary of the evidence, and wait for approval before any step that changes a system, such as isolating a machine or disabling an account
- Help with access reviews by listing who can reach each system, asking the owners to confirm the list and recording the removals they ask for
- Draft short awareness material for staff, such as a phishing reminder or a password-manager tip, for a senior to review

What we are looking for

- Networking basics: IP addresses, ports, DNS, how HTTP and HTTPS work, and what happens between typing a web address and seeing the page
- Windows and Linux basics: users and permissions, processes and services, and where each system keeps its logs

- Core security ideas: confidentiality, integrity and availability, the difference between a threat, a vulnerability and an exploit, and how phishing, malware and brute-force logins work
- Ability to read a log line (time, source, user, action, result) and spot a repeating pattern
- Clear written English: incident notes that separate facts from guesses and give times
- Calm, careful habits: follows a runbook, asks when unsure and escalates early rather than acting alone
- Practical work you can describe: a home lab, a college lab or a practice-platform exercise, with what you found and what you did
- Willingness to work only on the systems and accounts you are given, and to keep company data private

Good to have

- Hands-on time with Wazuh or another open-source SIEM, at home, in a college lab or on a practice platform
- Awareness of the MITRE ATT&CK framework, used to name what an attacker may be trying to do
- Wireshark basics for reading a packet capture
- Simple scripting in Python, Bash or PowerShell to filter a log file
- An entry-level certificate or course such as CompTIA Security+, which is welcome but not required

Who can apply

Final-year students and graduates of B.E./B.Tech in computer science, IT or electronics fit well, as do BCA, B.Sc (computer science or IT) and MCA candidates and those with a B.Sc or M.Sc in cybersecurity or digital forensics. Candidates from other streams can apply if they show networking basics and practical lab work.

How to apply

Apply through this job post by [\[Apply by\]](#). Shortlisted candidates will hear from us about the next steps.

Cybersecurity analyst intern

Company: [Company name]

Location: [Location] | Work mode: [Work mode]

Employment type: Internship | Duration: [Internship duration] | Stipend: [Stipend for the internship]

Joining: [Joining date] | Apply by: [Apply by]

About [Company name]

[About your company]

About the role

[Company name] runs a cybersecurity internship where students see how a security team spends an ordinary day. You will shadow analysts, sort sample alerts, check reported emails in a test mailbox and write notes, all under supervision and on systems your mentor assigns. Working pattern: [business hours only]. You finish by presenting one runbook page or awareness tip to the team.

What you will do

- Shadow an analyst for the first weeks, then sort a set of closed low-risk alerts with usernames and addresses masked, and compare your verdicts with the analyst's
- Check sample phishing emails in a test mailbox with a mentor and write down what you checked: sender, headers, links and attachment
- Read one day of masked or test sign-in logs and list the unusual logins you find, with the times as evidence
- Update the tracker of vulnerability scan findings with owner, due date and re-check status
- Write one page of the runbook for a common alert, such as repeated failed logins, and test it with an analyst
- Set up a small test lab with an open-source SIEM such as Wazuh, on a machine or virtual machine your mentor provides, and show one alert from log to ticket
- Prepare a one-page awareness tip for staff, such as spotting a phishing email, and present it to the team

What we are looking for

- Studying for a degree, or a recent graduate; computer science, IT, electronics and cybersecurity fit well, and other streams can apply with networking basics
- Knows networking basics: IP addresses, ports, DNS and HTTP
- Has done at least one hands-on exercise, in a college lab, a home lab or on a practice platform, and can describe it
- Writes short, clear notes that say what was seen and when
- Agrees to work only on the systems and test accounts the mentor assigns, and to keep company data confidential

Who can apply

Final-year students and graduates of B.E./B.Tech in computer science, IT or electronics fit well, as do BCA, B.Sc (computer science or IT) and MCA candidates and those with a B.Sc or M.Sc in cybersecurity or digital forensics. Candidates from other streams can apply if they show networking basics and practical lab work.

How to apply

Apply through this job post by [Apply by]. Shortlisted candidates will hear from us about the next steps.

Screening questions to add to your job post

1. **A colleague forwards you an email that asks them to 'verify your account' through a link. What are your first steps?** Look for an answer that avoids the link, checks the sender's address and where the link really goes, asks whether anyone else received it or clicked it, and escalates at once if someone has entered a password.
2. **Briefly distinguish a threat, a vulnerability and an exploit.** Look for a threat as something that could cause harm, a vulnerability as a weakness, and an exploit as the method that takes advantage of a weakness. Plain words matter more than textbook wording.
3. **A user signs in at 3 a.m. from a city they have never visited. Why does it matter, and what would you check?** Look for an unusual time and place treated as a possible sign of stolen credentials, not proof, since travel or a VPN can explain it. Then look for checks on the user's usual pattern, the device, earlier failures and what happened after the sign-in. A case that cannot be confirmed goes to a senior.
4. **What do you look for in a log full of failed logins?** Look for one account or many, one source address or many, the timing, and a success after the failures. Naming Windows events 4625 (failed logon) and 4624 (successful logon) is a useful extra, not a requirement.
5. **How would you explain 'use a password manager' to a colleague who is not technical?** Look for plain, friendly words: one strong, different password for every site, kept in one locked place. Listen for whether the answer avoids jargon and avoids blaming the colleague.
6. **An alert fires on a server while your senior is in a meeting. What do you do?** Look for an answer that follows the runbook, notes the facts and times, and uses the escalation contact instead of waiting or acting alone. Disabling accounts or isolating machines without approval goes against the runbook, so ask what approval the candidate would seek.