Lab 1

What is the CIA triad?

The CIA Triad is a foundational security model used to evaluate and design security controls. The 3 principles are defined as the following:

Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Example breaches:

- Data leaks
- Credential theft
- Eavesdropping
- Poor access control

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Examples:

- Changing bank records
- Tampering with logs to hide evidence
- Injecting false data

Confidentiality: Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorised disclosure of information.

Examples:

- DDoS attacks
- Ransomware encrypting files
- Hardware failure

In other words:

Integrity is any modification or destruction of information

Availability is any disruption of access or use of the information, meaning anytime a system is down or is withheld from being used/accessed

Confidentiality is unauthorised access to sensitive information such as private information and any proprietary information

<u>Passive and active attacks:</u>

passive attack attempts to learn or make use of information from the system but does not affect system resources

- The attacker observes, listens, or collects data without altering it.
- Aim: learn information, gather intelligence.
- Does not affect system resources.
- Hard to detect because nothing has changed.

For example:

- Network sniffing
- Traffic analysis

Active attack attempts to alter system resources or affect their operation

- The attacker modifies, disrupts, or damages system resources.
- Aim: cause harm, steal data, alter operations, or deny access.
- Usually detectable due to system changes or disruption.

For example:

- DDoS
- Ransomware
- Data tampering
- MITM (man-in-the-middle modifying data)

Section 1:

Case study A:

The 2017 Equifax Data Breach

https://archive.epic.org/privacy/data-breach/equifax/

A framework called struts announced a critical security flaw and released a patch, and although Equifax IT department received an alert to apply the patch, they failed to do so in a timely manner, thereby allowing the hackers to exploit the unpatched vulnerability in Equifax's online credit dispute portal.

1) Confidentiality is the primary principle of the CIA triad that was violated in this case study

2) The attackers gained unauthorized access to the sensitive and private information of 148 million Americans, 15.2 million British citizens and 19,000 Canadians. Stolen data included social security numbers, credit card numbers and addresses.

3) Availability was also integrity (in the CIA triad) as data was manipulated to hide theft. Company integrity was compromised as Equifax was sited for making inaccurate public statements regarding how many UK consumers were affected.

Case study D:

The 2021 Colonial Pipeline Ransomware Attack

https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

1) Availability is the primary principle of the CIA triad that was violated in The 2021 Colonial Pipeline Ransomware Attack

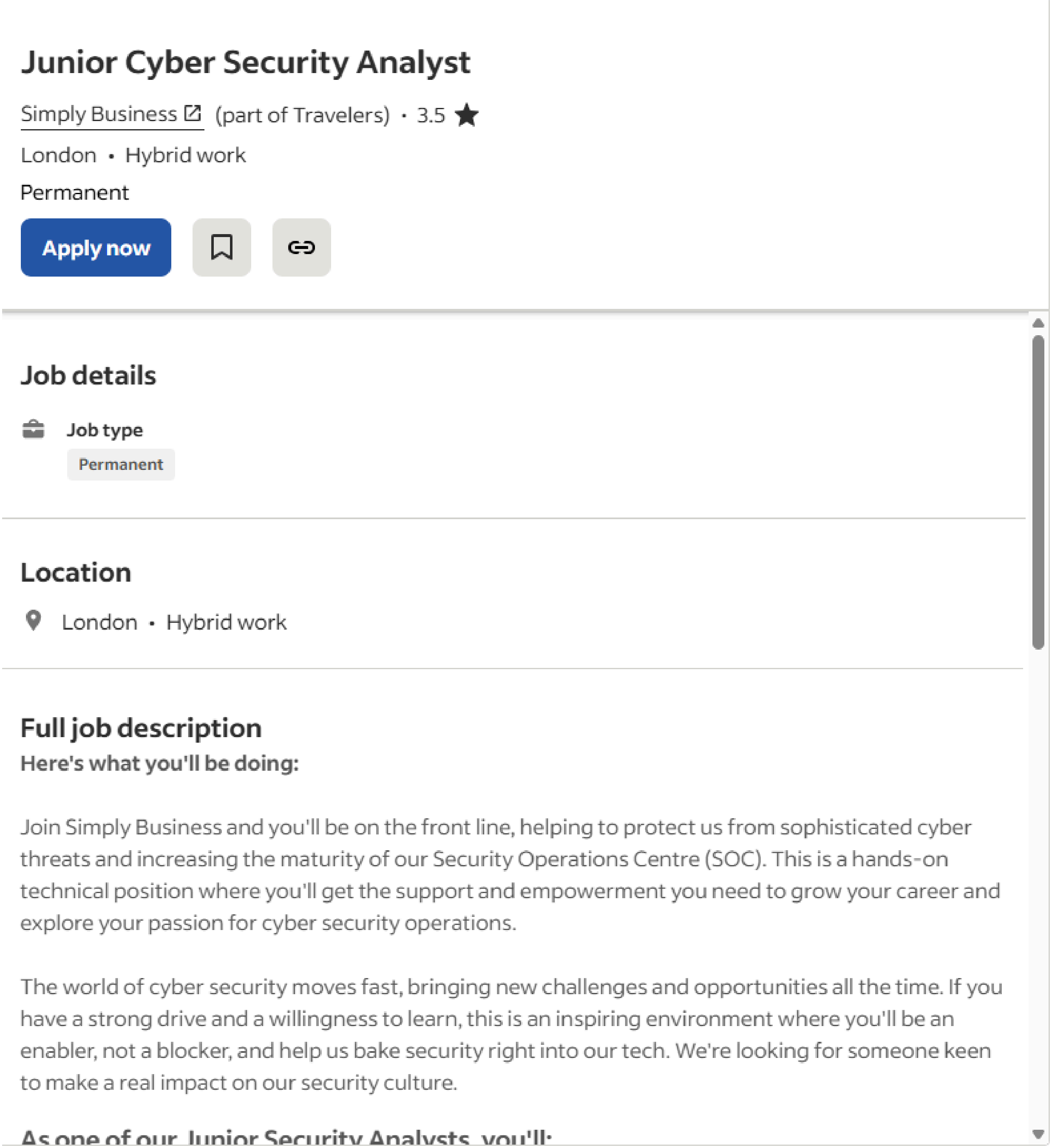
2) Fuel supply (a critical infrastructure) was unavailable to businesses and the public for multiple days. This shutdown had a massive operational and economic impact, as the pipeline that was shut down in response to the attack carried about 45% of the fuel used on the east coast

3) Confidentiality would be the secondary principle. This is because the attackers held about 100GB of sensitive corporate data before encrypting systems. Unauthorised access was gained and they threatened to leak this information.

Section 2:

Job 1:

https://uk.indeed.com/viewjob?jk=3c271641b73866c5&from=shareddesktop_copy



Junior Cyber Security Analyst

Simply Business (part of Travelers) · 3.5 ★

London · Hybrid work

Permanent

Job details

Job type

Permanent

Location

London · Hybrid work

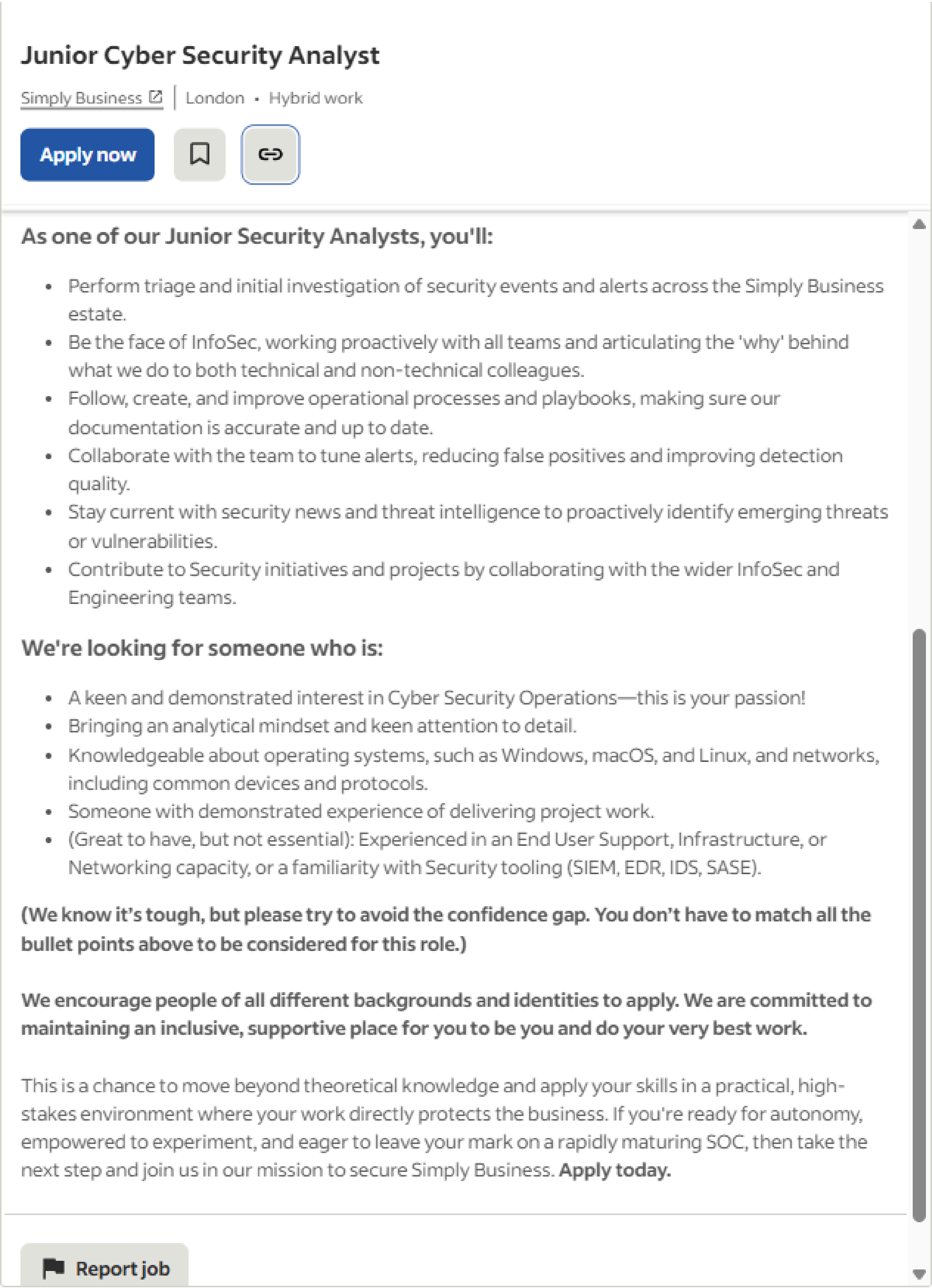
Full job description

Here's what you'll be doing:

Join Simply Business and you'll be on the front line, helping to protect us from sophisticated cyber threats and increasing the maturity of our Security Operations Centre (SOC). This is a hands-on technical position where you'll get the support and empowerment you need to grow your career and explore your passion for cyber security operations.

The world of cyber security moves fast, bringing new challenges and opportunities all the time. If you have a strong drive and a willingness to learn, this is an inspiring environment where you'll be an enabler, not a blocker, and help us bake security right into our tech. We're looking for someone keen to make a real impact on our security culture.

As one of our Junior Security Analysts, you'll:



Junior Cyber Security Analyst

Simply Business | London • Hybrid work

As one of our Junior Security Analysts, you'll:

- Perform triage and initial investigation of security events and alerts across the Simply Business estate.
- Be the face of InfoSec, working proactively with all teams and articulating the 'why' behind what we do to both technical and non-technical colleagues.
- Follow, create, and improve operational processes and playbooks, making sure our documentation is accurate and up to date.
- Collaborate with the team to tune alerts, reducing false positives and improving detection quality.
- Stay current with security news and threat intelligence to proactively identify emerging threats or vulnerabilities.
- Contribute to Security initiatives and projects by collaborating with the wider InfoSec and Engineering teams.

We're looking for someone who is:

- A keen and demonstrated interest in Cyber Security Operations—this is your passion!
- Bringing an analytical mindset and keen attention to detail.
- Knowledgeable about operating systems, such as Windows, macOS, and Linux, and networks, including common devices and protocols.
- Someone with demonstrated experience of delivering project work.
- (Great to have, but not essential): Experienced in an End User Support, Infrastructure, or Networking capacity, or a familiarity with Security tooling (SIEM, EDR, IDS, SASE).

(We know it's tough, but please try to avoid the confidence gap. You don't have to match all the bullet points above to be considered for this role.)

We encourage people of all different backgrounds and identities to apply. We are committed to maintaining an inclusive, supportive place for you to be you and do your very best work.

This is a chance to move beyond theoretical knowledge and apply your skills in a practical, high-stakes environment where your work directly protects the business. If you're ready for autonomy, empowered to experiment, and eager to leave your mark on a rapidly maturing SOC, then take the next step and join us in our mission to secure Simply Business. **Apply today.**

Company research:

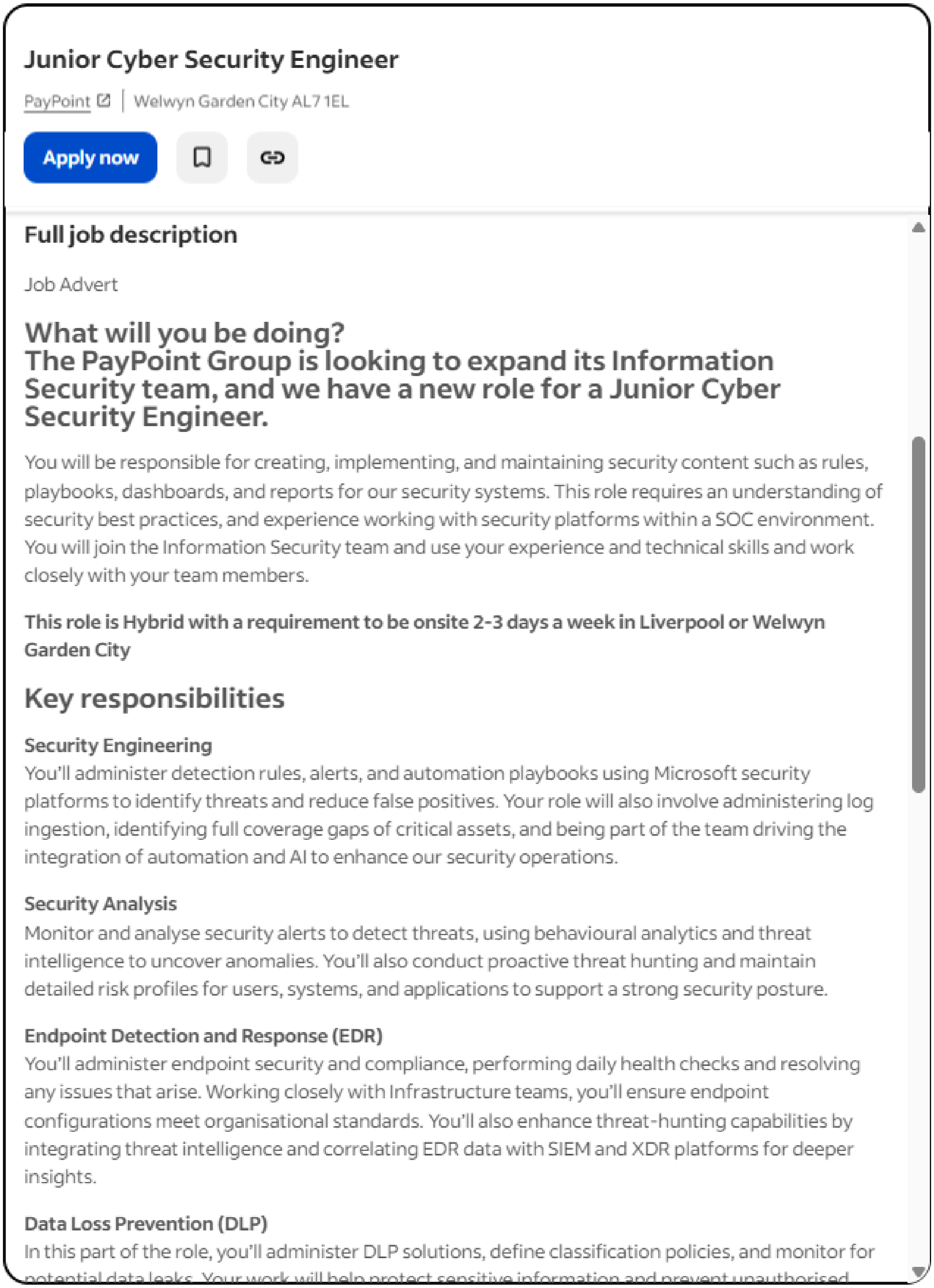
Based on employee reviews and some initial research, Simply Business is an insurance company that emphasises innovation, autonomy, and a supportive work environment. They have a reputation for strong culture and flexibility, with hybrid work options and a focus on internal development.

Why they are a good fit:

- Their mission to protect small businesses aligns well with cyber security values: safeguarding people’s livelihoods
- The environment appears collaborative and growth-oriented, which is ideal for an entry-level SOC analyst
- Hybrid work provides flexibility while still allowing hands-on engagement with security teams
- The role emphasises learning and development, which suits someone entering the field with high motivation

Job 2:

https://uk.indeed.com/jobs?q=Junior+penetration+tester&l=London%2C+Greater+London&from=searchOnHP%2Cwhereautocomplete&vjk=a5ed231338987bfd



Junior Cyber Security Engineer

PayPoint | Welwyn Garden City AL7 1EL

Full job description

Job Advert

What will you be doing?
The PayPoint Group is looking to expand its Information Security team, and we have a new role for a Junior Cyber Security Engineer.

You will be responsible for creating, implementing, and maintaining security content such as rules, playbooks, dashboards, and reports for our security systems. This role requires an understanding of security best practices, and experience working with security platforms within a SOC environment. You will join the Information Security team and use your experience and technical skills and work closely with your team members.

This role is Hybrid with a requirement to be onsite 2-3 days a week in Liverpool or Welwyn Garden City

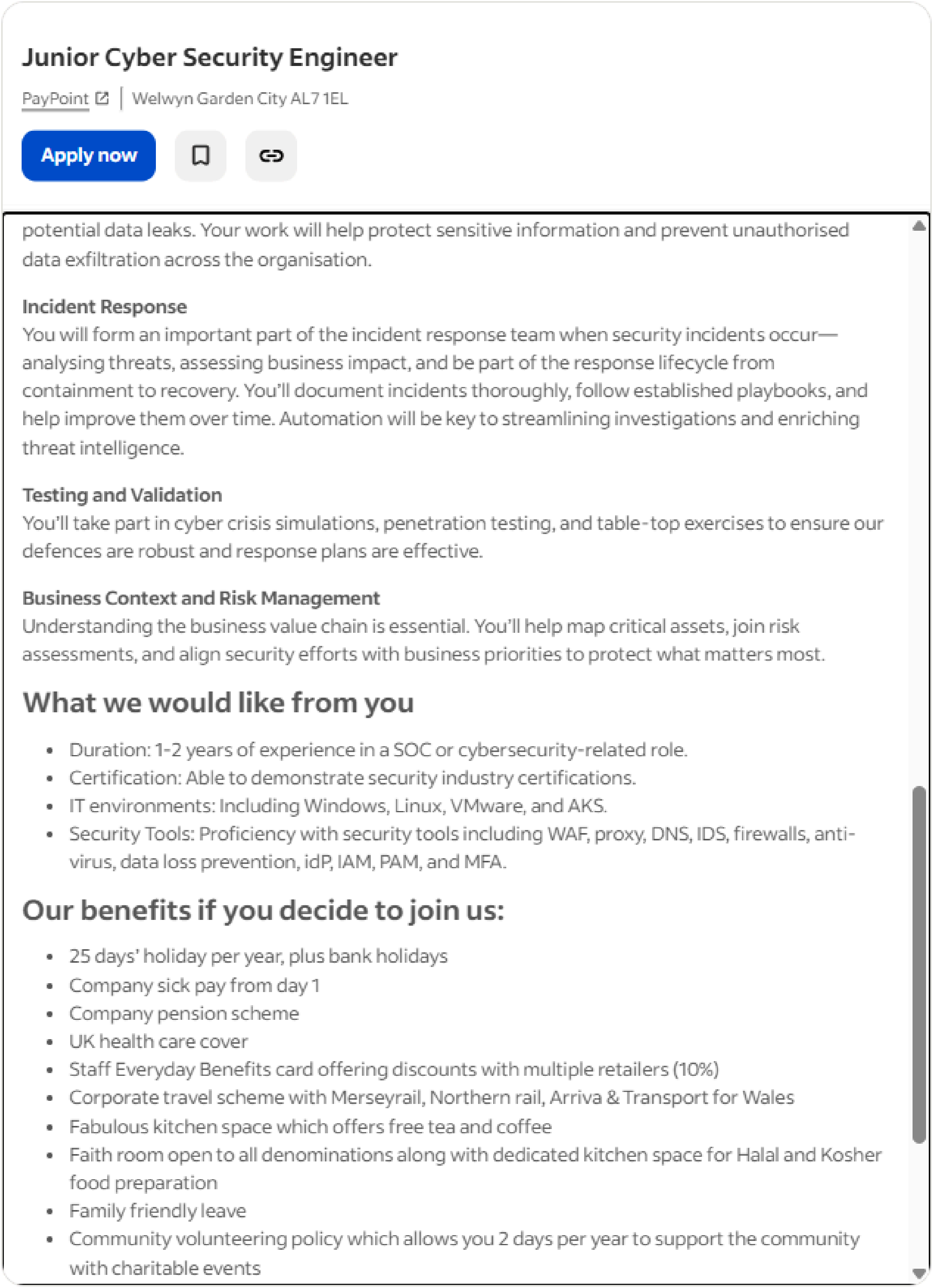
Key responsibilities

Security Engineering
You'll administer detection rules, alerts, and automation playbooks using Microsoft security platforms to identify threats and reduce false positives. Your role will also involve administering log ingestion, identifying full coverage gaps of critical assets, and being part of the team driving the integration of automation and AI to enhance our security operations.

Security Analysis
Monitor and analyse security alerts to detect threats, using behavioural analytics and threat intelligence to uncover anomalies. You'll also conduct proactive threat hunting and maintain detailed risk profiles for users, systems, and applications to support a strong security posture.

Endpoint Detection and Response (EDR)
You'll administer endpoint security and compliance, performing daily health checks and resolving any issues that arise. Working closely with Infrastructure teams, you'll ensure endpoint configurations meet organisational standards. You'll also enhance threat-hunting capabilities by integrating threat intelligence and correlating EDR data with SIEM and XDR platforms for deeper insights.

Data Loss Prevention (DLP)
In this part of the role, you'll administer DLP solutions, define classification policies, and monitor for potential data leaks. Your work will help protect sensitive information and prevent unauthorised



Junior Cyber Security Engineer

PayPoint | Welwyn Garden City AL7 1EL

potential data leaks. Your work will help protect sensitive information and prevent unauthorised data exfiltration across the organisation.

Incident Response
You will form an important part of the incident response team when security incidents occur—analysing threats, assessing business impact, and be part of the response lifecycle from containment to recovery. You'll document incidents thoroughly, follow established playbooks, and help improve them over time. Automation will be key to streamlining investigations and enriching threat intelligence.

Testing and Validation
You'll take part in cyber crisis simulations, penetration testing, and table-top exercises to ensure our defences are robust and response plans are effective.

Business Context and Risk Management
Understanding the business value chain is essential. You'll help map critical assets, join risk assessments, and align security efforts with business priorities to protect what matters most.

What we would like from you

- Duration: 1-2 years of experience in a SOC or cybersecurity-related role.
- Certification: Able to demonstrate security industry certifications.
- IT environments: Including Windows, Linux, VMware, and AKS.
- Security Tools: Proficiency with security tools including WAF, proxy, DNS, IDS, firewalls, anti-virus, data loss prevention, idP, IAM, PAM, and MFA.

Our benefits if you decide to join us:

- 25 days' holiday per year, plus bank holidays
- Company sick pay from day 1
- Company pension scheme
- UK health care cover
- Staff Everyday Benefits card offering discounts with multiple retailers (10%)
- Corporate travel scheme with Merseyrail, Northern rail, Arriva & Transport for Wales
- Fabulous kitchen space which offers free tea and coffee
- Faith room open to all denominations along with dedicated kitchen space for Halal and Kosher food preparation
- Family friendly leave
- Community volunteering policy which allows you 2 days per year to support the community with charitable events

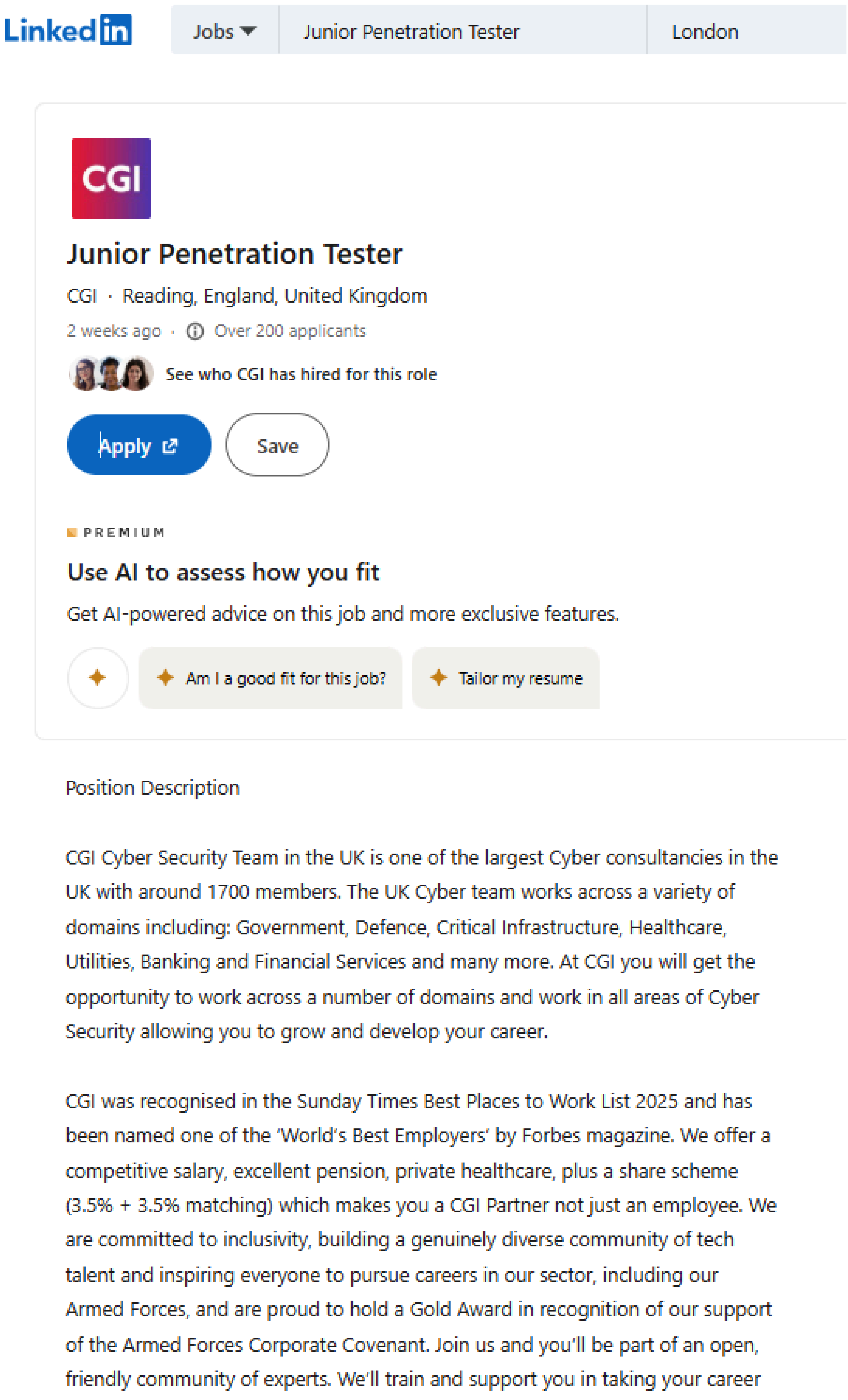
PayPoint Group is a well established organisation with a strong emphasis on secure digital services and business resilience. Their cyber security function appears highly structured and technical, making it a good fit to develop hands on engineering and SOC skills. The hybrid schedule and opportunities for automation, threat hunting, and security engineering make this role a good match for those who want to build a technical cyber security foundation.

Is this company a good fit for me?

Yes, as I want to develop more technical engineering and SOC skills. I am also interested in security tooling and detection engineering. The hybrid schedule is reasonable, and the company's role in secure digital transactions aligns with my career goals. Although my dream career path is not incident response, rather I want to get into penetration testing.

Job 3:

https://uk.linkedin.com/jobs/view/junior-penetration-tester-at-cgi-4332981514?position=1&pageNum=0&refId=ykA0h2BVXz1pjVNei6ssOA%3D%3D&trackingId=XDvgIF0qOmBhrogv%2BQd8wA%3D%3D&original_referer=https%3A%2F%2Fuk.linkedin.com%2Fjobs%2Fjunior-penetration-tester-jobs



Junior Penetration Tester

CGI · Reading, England, United Kingdom

2 weeks ago · ⓘ Over 200 applicants

See who CGI has hired for this role

PREMIUM

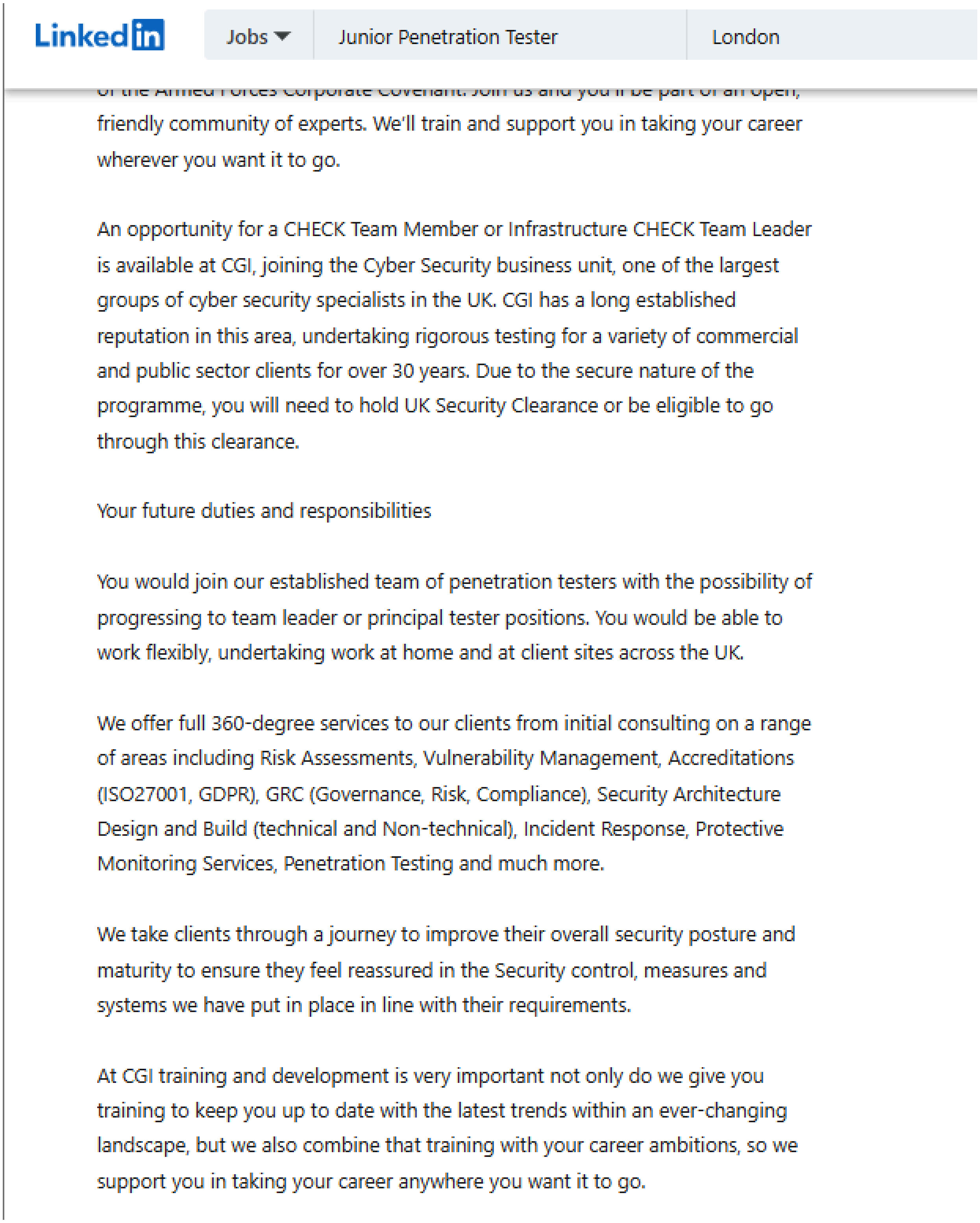
Use AI to assess how you fit

Get AI-powered advice on this job and more exclusive features.

Position Description

CGI Cyber Security Team in the UK is one of the largest Cyber consultancies in the UK with around 1700 members. The UK Cyber team works across a variety of domains including: Government, Defence, Critical Infrastructure, Healthcare, Utilities, Banking and Financial Services and many more. At CGI you will get the opportunity to work across a number of domains and work in all areas of Cyber Security allowing you to grow and develop your career.

CGI was recognised in the Sunday Times Best Places to Work List 2025 and has been named one of the 'World's Best Employers' by Forbes magazine. We offer a competitive salary, excellent pension, private healthcare, plus a share scheme (3.5% + 3.5% matching) which makes you a CGI Partner not just an employee. We are committed to inclusivity, building a genuinely diverse community of tech talent and inspiring everyone to pursue careers in our sector, including our Armed Forces, and are proud to hold a Gold Award in recognition of our support of the Armed Forces Corporate Covenant. Join us and you'll be part of an open, friendly community of experts. We'll train and support you in taking your career



of the Armed Forces Corporate Covenant. Join us and you'll be part of an open, friendly community of experts. We'll train and support you in taking your career wherever you want it to go.

An opportunity for a CHECK Team Member or Infrastructure CHECK Team Leader is available at CGI, joining the Cyber Security business unit, one of the largest groups of cyber security specialists in the UK. CGI has a long established reputation in this area, undertaking rigorous testing for a variety of commercial and public sector clients for over 30 years. Due to the secure nature of the programme, you will need to hold UK Security Clearance or be eligible to go through this clearance.

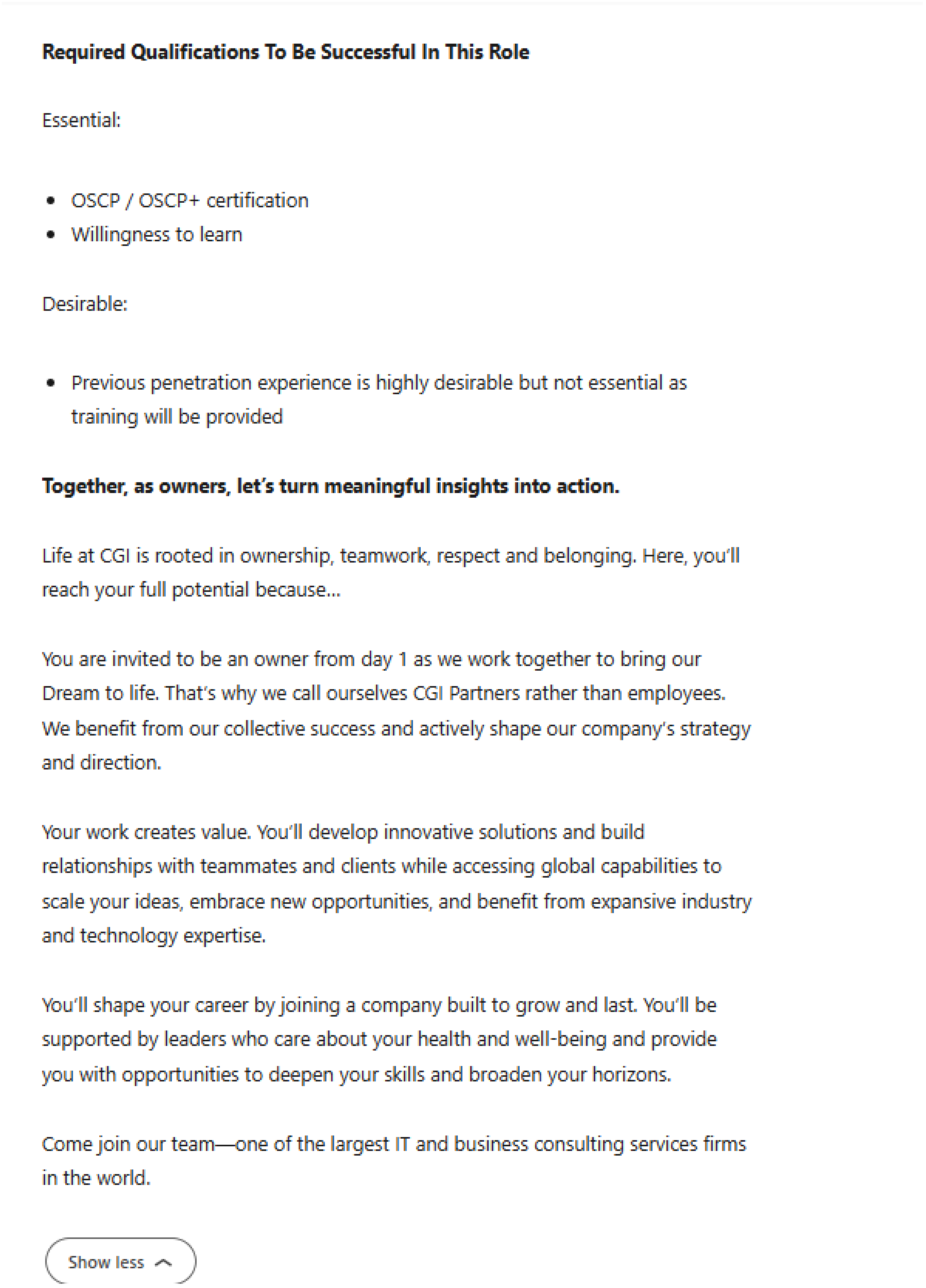
Your future duties and responsibilities

You would join our established team of penetration testers with the possibility of progressing to team leader or principal tester positions. You would be able to work flexibly, undertaking work at home and at client sites across the UK.

We offer full 360-degree services to our clients from initial consulting on a range of areas including Risk Assessments, Vulnerability Management, Accreditations (ISO27001, GDPR), GRC (Governance, Risk, Compliance), Security Architecture Design and Build (technical and Non-technical), Incident Response, Protective Monitoring Services, Penetration Testing and much more.

We take clients through a journey to improve their overall security posture and maturity to ensure they feel reassured in the Security control, measures and systems we have put in place in line with their requirements.

At CGI training and development is very important not only do we give you training to keep you up to date with the latest trends within an ever-changing landscape, but we also combine that training with your career ambitions, so we support you in taking your career anywhere you want it to go.



Required Qualifications To Be Successful In This Role

Essential:

- OSCP / OSCP+ certification
- Willingness to learn

Desirable:

- Previous penetration experience is highly desirable but not essential as training will be provided

Together, as owners, let's turn meaningful insights into action.

Life at CGI is rooted in ownership, teamwork, respect and belonging. Here, you'll reach your full potential because…

You are invited to be an owner from day 1 as we work together to bring our Dream to life. That's why we call ourselves CGI Partners rather than employees. We benefit from our collective success and actively shape our company's strategy and direction.

Your work creates value. You'll develop innovative solutions and build relationships with teammates and clients while accessing global capabilities to scale your ideas, embrace new opportunities, and benefit from expansive industry and technology expertise.

You'll shape your career by joining a company built to grow and last. You'll be supported by leaders who care about your health and well-being and provide you with opportunities to deepen your skills and broaden your horizons.

Come join our team—one of the largest IT and business consulting services firms in the world.

CGI’s Cyber Security Team is one of the largest in the UK. They work across diverse sectors such as Government, Defence, Critical Infrastructure, Healthcare, and Finance. As a Junior Penetration Tester, I would join an established CHECK team and perform security assessments for both public and private sector clients.

Key responsibilities:

- Conduct penetration testing engagements for clients across multiple industries.
- Work within an established team with opportunities for progression to lead or principal tester roles.
- Undertake a mix of on-site and remote testing across the UK.
- Provide clients with full security assessment services across:
    - Risk assessments
    - Vulnerability management
    - Technical and non-technical security reviews
    - Security architecture assessments
    - Incident response
    - Protective monitoring services
- Help clients improve their overall security posture through structured testing and advising.
- Engage in continuous training and development to stay updated with the latest trends in cyber security

Is this company a good fit for me?

This company is a perfect fit for me as they are exactly what I am looking for, in terms of my dream job. Although it is not as “entry” level as the job title may seem as they require OSCP which can be difficult to get and is not beginner level for cyber security certifications.

Skills gap table:

Required Skill / Qualification	I Have This Skill	Evidence / Example	How to Develop
Interest in Cyber Security Operations	Yes	Currently studying Networks & Systems Security; pursuing penetration testing career	Continue labs in this course, start some individual learning in HackTheBox and TryHackMe. Can also get certifications such as Security+ or Google Cybersecurity Cert

Analytical mindset & attention to detail	Yes	Shown in coursework and technical documentation	Practice log analysis. Look into detection engineering basics
Knowledge of Windows, macOS, Linux	Developing	Basic Linux usage from labs and previous courses. Familiar with Windows environments. Used some CLI with Dynamic Web Module for our virtual machine.	Complete Linux labs, practise command line, use TryHackMe Linux modules.
Knowledge of networking and protocols	Developing	Completed networking modules/ Also familiar with TCP/IP	Wireshark labs, Nmap scanning exercises, TryHackMe networking pathways
Experience with documenting processes	Yes	University coursework and GitHub lab documentation for other Assignments in other modules	Improve documentation quality in my portfolio
Understanding of SIEM/EDR/IDS (optional)	No	No direct hands-on experience yet	Learn open-source SIEM tools (e.g., Wazuh). Complete Splunk Boss of the SOC basics, TryHackMe: “Security Operations” room
Experience delivering project work	Developing	Some experience from previous projects. Some group projects and some individual, uploaded to Github	Complete course mini-project and document process clearly
| Security Engineering (Creating detection rules, playbooks, dashboards)	No	Not yet performed rule writing or playbook automation	Learn Microsoft Sentinel basics; TryHackMe “SIEM” and “Detection Engineering” paths; practise writing basic KQL queries |
Endpoint Detection & Response (EDR) & Data Loss Prevention (DLP)	No	Not yet worked with enterprise EDR or DLP tools	Learn CrowdStrike/Wazuh fundamentals. Try free Microsoft Defender labs. study common DLP policies and classifications
OSCP / OSCP+ certification	No	Currently no offensive security certifications	Begin with TryHackMe Offensive Pathway. Then move to PWK/OSCP

			preparation labs
Penetration testing fundamentals	Developing	Some experience through course content and labs.; interest in offensive security	Practice on HackTheBox / TryHackMe. study OWASP Top 10. do hands-on web and network hacking labs

Action plan:

Gain hands-on experience with SIEM tools

- Start with Wazuh, Splunk Free Edition, or Elastic Security
- Complete SOC-oriented labs (TryHackMe: SOC Level 1 Pathway)

Strengthen Linux & networking fundamentals

- Complete Linux command line labs weekly
- Use Wireshark and Nmap regularly to understand packet flows and scanning

Build incident triage and investigation skills

- Practise analysing logs
- Participate in detection engineering labs or cyber ranges
- Study MITRE ATT&CK and common alert types

Develop Detection Engineering & Automation Skills

- Learn how detection rules are structured (e.g., KQL for Microsoft Sentinel).
- Experiment with writing simple analytics rules or alerts based on log data.
- Explore automation concepts using tools like Sentinel playbooks or open-source SOAR tools.
- Study behaviour-based detection to improve tuning and reduce false positives.

Gain Familiarity with Endpoint Security & DLP Concepts

- Learn how EDR tools work (e.g., Defender for Endpoint, CrowdStrike).
- Explore free DLP labs or documentation to understand policy creation, monitoring, and classification.
- Study common endpoint misconfigurations and how they affect security posture.
- Complete hands-on EDR exercises through cyber ranges or vendor training portals.

Build Offensive Security & Penetration Testing Skills

- follow the TryHackMe Offensive Security, Pentester Path, or Hack The Box Starting Point / Pro Labs.
- Study and practise the OWASP Top 10, including exploitation of common web vulnerabilities (SQLi, XSS, IDOR, RCE).
- Learn fundamental penetration testing methodologies (PTES, OSSTMM, NIST 800-115).
- Gain experience with common tools: Burp Suite, Nmap, Metasploit, Gobuster, Nikto, Responder, BloodHound, etc.
- Build a portfolio of solved boxes/challenges to demonstrate technical capability.
- Begin preparing for OSCP or similar certification by practising privilege escalation, buffer overflows, and post-exploitation techniques.