**[Your Full Name]**  
📍 [City, Country] | 📧 [Your Email] | 📱 [Your Phone Number] | 🔗 [LinkedIn Profile] | 💻 [GitHub/Portfolio]

**🎯 Professional Summary**

Results-driven Cybersecurity Professional with over [X] years of experience in securing enterprise networks, systems, and applications. Skilled in vulnerability management, incident response, and threat analysis. Proven ability to collaborate with cross-functional teams to enhance security postures and protect sensitive data. Looking to leverage expertise in [specific skill/technology] to contribute to [company’s] cybersecurity initiatives.

**🛠️ Core Skills**

* Network Security & Firewall Management
* Vulnerability Management & Penetration Testing
* SIEM & Threat Detection Tools: Splunk, SolarWinds, ELK Stack
* Incident Response & Forensics
* Data Loss Prevention (DLP) & Encryption
* Endpoint Security & EDR Solutions (CrowdStrike, Carbon Black)
* Cloud Security (AWS, Azure, GCP)
* Programming & Scripting: Python, PowerShell, Bash

**🎓 Education**

**Bachelor of Science in Computer Science**  
[Your University Name], [City, Country] | [Year of Graduation]  
Relevant Courses: Network Security, Ethical Hacking, Cryptography, Cloud Security

**🏆 Certifications**

* Google Cybersecurity Professional Certificate – Coursera | 2024
* Certified Information Systems Security Professional (CISSP) – [Year]
* CompTIA Security+ | [Year]
* Certified Ethical Hacker (CEH) | [Year]
* Certified Incident Handler (GCIH) | [Year]

**💼 Professional Experience**

**Senior Detection Engineer**  
Confidential Company (Remote) | Mar 2022 – Present

* Developed and implemented advanced threat detection rules for enterprise applications and networks using [technologies]
* Led incident response efforts to mitigate security incidents and reduce downtime
* Collaborated with cross-functional teams to improve overall security posture and incident response capabilities
* Regularly conducted vulnerability assessments and provided actionable recommendations for remediation

**Cybersecurity Analyst**  
[Company Name], [Location] | Jan 2020 – Mar 2022

* Managed daily security operations and monitoring using SIEM tools (Splunk, ELK)
* Performed vulnerability scans using tools like Nessus and OpenVAS
* Conducted penetration testing on internal and external systems to identify vulnerabilities and weaknesses
* Assisted with compliance efforts (e.g., GDPR, HIPAA) and ensured adherence to security best practices

**💻 Projects & Achievements**

**Automated Threat Detection System**

* Developed an automated detection system using Python and Splunk to identify and alert on potential threats in real-time
* Reduced manual monitoring efforts by 30% and improved detection accuracy

**Cloud Security Framework Implementation**

* Designed and implemented security controls for AWS and Azure environments, including IAM roles, encryption, and access management
* Enhanced security compliance for cloud-based applications

**🌐 Languages**

* English – Professional Proficiency
* Urdu – Native
* [Other, if any]

**📌 References**

Available upon request.