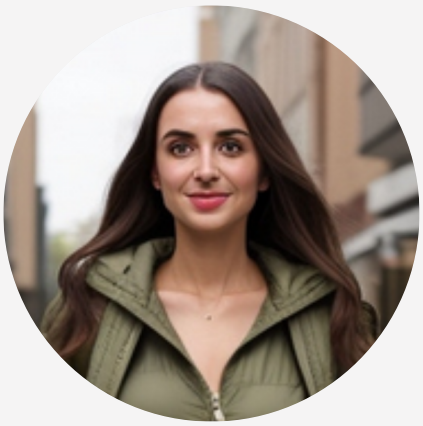

(206) 345-6789

sarah.lee@gmail.com

Seattle, WA

EDUCATION

Master of Science in Cybersecurity

University of Washington, United States

2009 - 2013

Certified Information Systems Security Professional (CISSP)

ISC2, Certification Date: October 2019

Certified Ethical Hacker (CEH)

EC-Council, Certification Date: January 2018

Cisco Certified Network Associate Security (CCNA Security)

Cisco Systems, Certification Date: December 2016

SKILLS

- Network security architecture and design
- Firewalls (Palo Alto, Fortinet, Cisco)
- Intrusion detection/prevention (IDS/IPS)
- Penetration testing and vulnerability assessments
- Incident response and forensics
- Risk management and compliance
- Network encryption (SSL, IPSec)

SARAH LEE

SENIOR NETWORK SECURITY ENGINEER

PROFESSIONAL SUMMARY

Network Security Engineer with over 15 years of experience safeguarding critical networks from cyber threats. Expertise in designing, implementing, and monitoring firewalls, intrusion detection systems, and other network security solutions. Proven track record in identifying vulnerabilities and mitigating risks in enterprise environments.

EXPERIENCE

April 2018 - December 2024

Senior Network Security Engineer

Microsoft Corporation / United States, Redmond, WA

- Architected and deployed secure network infrastructures to protect company assets from external and internal cyber threats.
- Led security incident response teams during network breaches, minimizing impact and restoring operations within 24 hours.
- Conducted vulnerability assessments and penetration testing, identifying weaknesses and implementing remediation plans.
- Trained junior engineers on security best practices, creating a culture of security awareness within the team.

January 2010 - March 2018

Network Security Engineer

AT&T Cybersecurity / United States, Bellevue, WA

- Developed and maintained network security policies and procedures for enterprise clients.
- Managed network security tools, such as firewalls, VPNs, and anti-virus software, ensuring 99.9% uptime.
- Performed risk analysis and vulnerability assessments, applying patches and updates to prevent data breaches.