Harpreet Singh

Hoshiarpur, Punjab, India | 8872728323 | Mail | LinkedIn | GitHub

Summary

SOC Level 2 / Cloud Security Engineer with a proven track record of transitioning from monitoring to high-level incident response and **Detection Engineering**. Expert in **AWS/OCI infrastructure**, performing deep-dive **Root Cause Analysis (RCA)** on escalated threats, and architecting scalable **SIEM/Observability** pipelines using the **ELK Stack and OpenSearch**. Leverages **CCNA-level networking** and **AI-driven security automation** to reduce false positives and harden cloud-native environments.

Education

I.K.G.P.T.U ▌ Hoshiarpur, PB, India Graduated June 2024

B.Tech (C.S.E) CGPA: 8.2

Core Competencies

- **SOC L2 Operations:** Advanced Incident Response, Root Cause Analysis (RCA), Handling Escalations (Phishing, Malware).
- **Cloud Security Architecture:** AWS IAM, GuardDuty, WAF, CloudTrail, OCI Observability & DevOps.
- Detection **Engineering:** SIEM Design (ELK/OpenSearch), Log Ingestion (Logstash, Data Prepper), Sysmon, GROK patterns.
- **Network Security & Automation:** VPC Hardening, Routing (OSPF, EIGRP), Python-based Security Automation.

Professional Experience

Security Analyst (L2) | Cywarden, India **August** 2024 – Present

- **Lead L2 Response & Investigations:** Serve as the escalation point for complex security incidents, performing **Root Cause Analysis (RCA)** for phishing and malware threats across AWS-native environments.
- **Architected Cloud SOC Framework:** Designed a 24/7 monitoring framework for multi-tenant AWS environments using **GuardDuty, CloudWatch, and WAF** to provide continuous visibility.
- **SIEM Engineering & Optimization:** Deployed and maintained a centralized SIEM on the **ELK stack**, configuring Elastic Agent and Sysmon logging to improve detection coverage and telemetry.
- **Observability Pipeline Development:** Implemented a scalable security analytics platform using **OpenSearch and Data Prepper**, integrating APM through efficient log and trace ingestion.
- **ETL & Log Enrichment:** Optimized ingestion processes using **GROK for structured parsing**, ensuring high-fidelity alerts for faster incident response.
- **Infrastructure Hardening:** Enforced AWS security best practices by implementing granular **IAM policies, security groups, and encryption**.

Cyber Security Intern | Hoping Minds, Mohali, Punjab, India January 2024 – June 2024

- Gained hands-on experience in **Vulnerability Assessment (VAPT)**, threat analysis, and Risk Management.
- Evaluated Cloud Security Posture Management (CSPM) and AWS Cloud configurations to identify security gaps.

Personal Projects and Certifications

➢ **Secure Banking System** February 2024-June 2024

- **Developed a secure REST API** for banking applications, integrating **AES encryption** to protect transaction data and authentication tokens.
- **Implemented a custom VPN layer** to establish secure, encrypted communication tunnels for all financial data transfers.
- **Hardened system architecture**, resulting in a **40% reduction in potential security breaches** and improved overall reliability.
- **Applied secure coding and cryptographic principles** to build and validate financial infrastructure against common web vulnerabilities.

➢ **GuardianX** July 2024Present

- **Engineered a Python-based security tool** featuring signature-based virus scanning and automated port scanning to enhance malware protection.
- **Optimized detection logic** to achieve a **70% reduction in false positives** during testing, ensuring high-fidelity alerting for SOC environments.
- **Improved threat identification** by 30%, successfully identifying and blocking over 200 distinct malware variants.

➢ **MULTI-BUILDING NETWORK ARCHITECTURE** Jul 2022-Aug 2022

- **Architected and simulated a large-scale university network** using Cisco Packet Tracer to ensure high availability and performance.
- **Configured and managed servers** to centralize network resources and services across multiple physical locations.
- **Optimized network routing and switching** to achieve seamless connectivity and robust infrastructure design.

Certificates

- **SIEM Fundamentals**: Google Chronicle (10/2024 – Present).
- **The Cybersecurity Threat Landscape**: LinkedIn (10/2024 – Present).
- **Python Developer**: HackerRank (10/2023 – Present).
- **Cisco Certified Network Associate**: O7 soln (07/2023 – Present).

- **Oracle Cloud Infrastructure**: 2025 Certified Generative AI Professional.
- **Oracle Cloud Infrastructure**: Certified DevOps Professional.
- **Oracle Cloud Infrastructure**: Certified Observability Professional.

Technical Skills & Certifications

- **Cloud & SIEM:** AWS (EC2, S3, RDS, IAM, GuardDuty, CloudTrail, Config, WAF, CloudWatch), Elastic Stack (ELK), OpenSearch, Sysmon, Data Prepper, Logstash, Google Chronicle CSPM.
- **Offensive Security:** Nmap, Burp Suite, Metasploit, sqlmap, Dirsearch, Kali Linux, VAPT.
- **Networking:** Cisco Packet Tracer, Routing Protocols (RIP, OSPF, EIGRP), LAN/WAN Design, Troubleshooting.
- **Languages:** Python, GO, C

Skills & Extracurricular

Soft skills: Leadership, Quick Adaptability, Quick learner, Problem Solving.

Interests: Chess, Current Affairs, Strategic Gaming, Technology Trends, History, Cybersecurity Innovations, Philosophy, Cosmology and the Origins of the Universe

Languages

English (Fluent) | Punjabi (Native) | Hindi (Fluent)