

NAMISH CHATURVEDI

DevSecOps Engineer | Box | Warsaw, Poland

namishelex01@gmail.com

<https://linkedin.com/in/namishc>

[@NamishSir](#)

SUMMARY

- ✓ 11+ Years of experience in Cloud security, threat hunting, detections and IR, forensics analysis and automation
- ✓ Actively played CTFs: Ranked under top 500 in Hackthebox.eu Hall of Fame in 2017-18
- ✓ BSI, India certified ISO/IEC 27001 Information Security Lead Implementer
- ✓ Familiarity with cyber-crimes and cyber-attacks, responsible groups and updated with sec-domain news
- ✓ Learning analysis and AI implementation on gathered application and network logs
- ✓ Automate vulnerability assessment of random web platforms using RaspberryPi
- ✓ Won Blackberry App Challenge in Feb'2012

EXPERIENCE

DevSecOps Engineer at Box

January 2024 - Present

- \$ Managing audit, deployment and maintenance of the security agents on all 3 cloud providers (AWS, Azure and GCP)
- \$ Managing audit, deployment and maintenance of the security agents deployed on k8s clusters
- \$ Managing the vulnerability management framework for cloud and platform environment
- \$ Building a security-focused AI+RAG model for security control management and automation.

Product Security Engineer at Snowflake

October 2021 – December 2023

- \$ Managing audit, deployment and maintenance of the security agents on all 3 cloud providers (AWS, Azure and GCP)
- \$ Managing audit, deployment and maintenance of the security agents deployed on k8s clusters
- \$ Auditing and modifying the security controls across all 3 cloud providers using terraform (AWS, Azure and GCP)
- \$ Automated the initial triage and support evidence collection for security agent from hosts and k8s clusters
- \$ Automated the business-sensitive operational tasks of creating and decommissioning of accounts
- \$ Implemented tenable solution across SF commercial deployments for vulnerability assessment

AWS Cyber Security Analyst at Monese

January 2020 – August 2021 (1 year 8 months)

- \$ Automated AWS cloud misconfiguration scanning and alerting using prowler, lambda and slack
- \$ Built a scalable, performance-tuned and fault-tolerant SIEM architecture using Snowflake with terraform
- \$ Built security threat detections over cloudtrail, DB, VPN, VPC, Vault, application and ELB log sources
- \$ Automating security incident process to accelerate the remediation process(revoke IAM access, isolate EC2, etc)

Senior Security Analyst at Oracle Cloud Infrastructure

December 2018 – January 2020 (1 year 1 month)

- \$ Managing security detections, automation and log analysis of *Oracle Cloud Infrastructure*
- \$ *Automating* the deployment of Splunk detections and alerting in different regions
- \$ Creating a *secret finder solution* to scrap all the confluence pages and search for any secrets spilled by collaborators
- \$ Writing new detections and tuning old detections to improve performance and avoid benign positives for Linux environments
- \$ Performing *threat hunts* for finding new vulnerabilities and tuning audit rules for in-depth logging

Senior Security and Cloud Engineer at Goodera

March 2017 – December 2018 (1 year 10 months)

- \$ Sole person for cloud, security and compliance administration and management
- \$ Enhancing security standards, policies, and controls for product and cloud resources using manual approach and using open-source tools
- \$ Automate cloud logs analyzing, security monitoring and alerting using ELK stack
- \$ Automate hardening of production level OS with CIS benchmark standards using ansible
- \$ Provide technical advice to internal organizations in the area of information security, specializing in application-level security and secure coding techniques

Software Development Engineer in Test - II at Freecharge

March 2016 - March 2017 (1 year 1 month)

- \$ Web application functional, performance and security testing
- \$ Static, dynamic and runtime testing of mobile applications
- \$ Performing Web UI and API automation using Java and Selenium
- \$ Introductory experience in PCI-DSS compliance management

QA Engineer at Chainalytics

February 2014 - March 2016 (2 years 2 months)

- \$ Web UI and API automation using Java and Selenium
- \$ Performance testing of all the feature consuming APIs using JMeter
- \$ Thorough functional and business logic testing on web application

SKILLS

COMPLIANCE	–	ISO 27001, GDPR
VULNERABILITY SCAN	–	NMAP, ETTERCAP, NESSUS
LANGUAGES	–	PYTHON, SHELL SCRIPT, JAVASCRIPT
DATABASES	–	MYSQL, MONGODB, REDSHIFT, REDIS
WEB APPLICATION SCAN	–	NIKTO, SSLSCAN, SSLYZE, ZED ATTACK PROXY, BURPSUITE
PLATFORMS	–	WINDOWS, UBUNTU, KALI, RESPBIAN, AMAZON LINUX

EDUCATION

PG Diploma - IT Infrastructure, System and Security	CDAC Bengaluru [2013 – 2014]
B. Tech - Electronics and Telecommunication	NIT, Raipur [2008 – 2012]