NAMISH CHATURVEDI

PRODUCT SECURITY ENGINEER | PRODUCT & CLOUD SECURITY@SNOWFLAKE | WARSAW, POLAND

SUMMARY

✔ 9+ 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
✔ Understanding of Cloud architectures, data center management & operations and implementation of different layers of security on an enterprise scale
✔ Hands-on experience of configuration and security management on AWS applications
✔ Hands-on experience on tools like NMap, Nessus, Burp Suite, ZAP, W3AF, Metasploit
✔ Hands-on experience on VAPT of Web and Mobile applications
✔ Familiarity with cyber-crimes and cyber-attacks, responsible groups and updated with sec-domain news
✔ Learning analysis and ML implementation on gathered application and network logs
✔ Automate vulnerability assessment of random web platforms using RaspberryPi
✔ Won Blackberry App Challenge in Feb'2012

EXPERIENCE

Product Security Engineer at Snowflake

October 2021 – Present

$ Managing audit, deployment and maintenance of the configuration across all commercial Snowflake product deployments
$ Managing audit, deployment and maintenance of the security agents on hosts across all 3 cloud providers (AWS, Azure and GCP)
$ Managing audit, deployment and maintenance of the security agents on hosts across all k8s clusters as a daemonset
$ 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
$ Automated the monitoring and reporting process of any malfunctioning of security agents
$ Building and managing the service readiness process of security agents from scratch in Snowflake
$ Implemented tenable solution across SF commercial deployments for vulnerability assessment
$ Involved in hiring process for building Poland cloud security team

AWS Cyber Security Analyst at Monese

January 2020 – August 2021 (1 year 8 months)

$ Managing AWS information security controls and reports for ISO and PCI audits
$ Automated AWS scanning and notification 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
$ Implementing MISP threat intelligence gathering to feed data into SIEM
$ 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
$ Creating dashboards for ease of *managing and auditing detections* in splunk
$ Creating *remote cli automation* tool for directly running queries on splunk parallelly in different regions
$ 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
- $ Performing *timeline analysis* and report generation of periodic purple team exercises

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
- $ System, application and database monitoring, analysis and alerting using Prometheus and Grafana
- $ 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, HTML
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]

PERSONAL INFORMATION

Mail ID	–	namishelex01@gmail.com
Mobile No.	–	*+48 572530821*
LinkedIn	–	https://linkedin.com/in/namishc
Twitter	–	*@NamishSir*
Hobbies	–	*Playing computer games & badminton, playing my ukulele, OSINT*
Languages	–	*English, Hindi*
DOB	–	*01-05-1991*
Location	–	*Warsaw, Poland*