NAMISH CHATURVEDI

AWS Cyber Security Analyst | Information Security Team@Monese | Tallinn, Estonia

SUMMARY

- ✔ 6+ Years of experience in Cloud security, threat hunting, detections and IR, forensics analysis and automation
- ✔ Actively plays CTFs: Ranked under top 500 in Hackthebox.eu Hall of Fame
- ✔ 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 like IAM, WAF & Shield VPC, S3, Elasticsearch, CloudFront, EC2, Route53, etc
- ✔ 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-world 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
- ✔ Pursuing OSCP certification

EXPERIENCE

AWS Cyber Security Analyst at Monese

January 2020 – Present

- $ 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 ELK stack 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 forensics data collection from EC2 sources using SSM agent and lambda
- $ Automating security incident process to accelerate the remediation process(revoke IAM access, isolate EC2, etc)
- $ Automating forensics data collection from EKS clusters using open source tools and lambda

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
- $ Performing *triages* on the basis of events triggered by detections found in OCI environment
- $ 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
- $ Automating live *forensics* process to be performed on OCI boxes
- $ 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
- $ Performs static/dynamic code testing, manual code inspection, threat modeling, design reviews and vulnerability assessment of internal web applications

$ Network penetration testing using Nessus and Metasploit
$ Automate AWS environment assessment and monitoring using Scout2
$ Automate log gathering, analysis and alerting using AWS Redshift, Kinesis, CloudWatch, SQS and Telegram
$ 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
$ Develop architecture for our web services security platform which supports authentication, authorization, isolation and policy management
$ Automate malware scanning for S3 buckets using BinaryAlert and cloud auditing and alerting using Security Monkey
$ 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

CDAC Bengaluru [2013 – 2014]

PG Diploma - IT Infrastructure, System and Security

NIT, Raipur [2008 – 2012]

B. Tech - Electronics and Telecommunication

PERSONAL INFORMATION

Mail ID	–	namishelex01@gmail.com
Mobile No.	–	*+372 5806 9145*
LinkedIn	–	*linkedin.com/in/namishc*
Twitter	–	*@NamishSir*
Hobbies	–	*Playing computer games & badminton, playing my ukulele, OSINT*
Languages	–	*English, Hindi*
DOB	–	*01-05-1991*
Location	–	*Tallinn, Estonia*