Survya Singh – CISSP

Security Operations Engineer
Seattle, WA -98119
Mob: (469)-493-6829 | Email: survya.singh@gmail.com | Web: https://survya.com | LinkedIn: https://www.linkedin.com/in/survya/

SUMMARY

- An experienced security professional with six years of diversified experience in security operations, threat hunting, financial fraud analysis, and python scripting. Proficient in security Monitoring, Detection, and Response (MDR) capability.

EXPERIENCE

Amazon – Seattle, WA Jul 2019 – Present
Security Operations Engineer

- Responsible for continuous monitoring, detection, and response against anomalous behavior or threat for securing Amazon GO and Book stores infrastructure.
- Build and scaled security operations team's visibility and capability by implementing EDR solution, onboarding logs to the SIEM platform, and created IRP documents to standardize response procedure.
- Designed, built, and implemented NSM (network security monitoring) solutions frugally using open source technology (Snort, Bro, and AWS SSM) for Amazon retail stores.
- Took ownership for designing and running Threat Hunting program for Amazon Go and Book stores and published daily reports.

Citibank North America – Irving, TX Oct 2017 – Jun 2019
Sr. SOC Threat Analyst

- Worked as a senior SOC security analyst in the Global SOC team and responsible for monitoring and analyzing security incidents in Citibank.
- Perform monitoring, research, assessment, and analysis of Intrusion Detection and Prevention tools, Anomaly Detection systems, Firewalls, Antivirus systems, and proxy devices.
- Responsible for handling of SOC interaction with other groups within Citi during shift hours, such as providing analysis of any possible security incident, coordinating with other groups for threat research, and incident response.
- Performed monitoring of financial data across Citibank and created an automated SAS script for identifying financial fraud globally. Developed macro based excel tool for automating email drafting for security incident escalation.

NiSource Columbia Gas – Columbus, OH May 2017 – Aug 2017
Cyber Security Intern

- Optimized checkpoint firewall rules by using Firemon Security Manager Tool.
- Performed threat hunting by analyzing logs from Palo Alto next-generation Firewall.

Southwest Airlines – Dallas, TX Jan 2017 – Apr 2017
Cyber Security Intern

- Enhanced security of server to server communication by remediating 50K weak SSH keys with 2048 bits SSH keys.
- Performed daily task of rotating, issuing, and managing SSH keys and PKI SSL certificates in Venafi Trustworthy tool.

DSW Inc. - OH, USA May 2016 – Aug 2016
Cyber Security Intern

- Documented SOP's for Qualys vulnerability assessment tool, Tripwire FIM tool, CyberArk, and Proofpoint.
- Took responsibility for coordinating with the operations team in the patching of Severity 5 & 4 vulnerabilities, thus enhancing the overall IT security. Performed daily tasks of Ad-hoc vulnerability assessment using Qualys tool and managed several vulnerability dashboards.

Accenture Services – Pune, MH Apr 2012 – Jul 2015
Software Engineering Analyst

- Developed a standardized TATC framework for testing of middleware web services using Parasoft SOA Test tool.
- Performed tasks like test case identification, test scenario creation, test execution, requirement gathering, and defect identification and management, and lead a team of 4 quality analysts.

PROFICIENCIES

- **Skills:** CrowdStrike, Splunk, ArcSight SIEM, Snort, Bro, AWS SSM, AWS EC2, AWS CloudWatch, Proofpoint, Archer, Threat Hunting, Threat Intelligence, Linux, TCP/IP, SAS, Python Scripting and Excel Macros.
- **Certifications:** OSCP- In Progress, CISSP, Security+, Splunk Core User Certified, WSU Cyber Security Analytics, CEH, Qualys Certified, Venafi Security Certified, Oracle Certified Java Programmer (SCJP 6).

EDUCATION

Wright State University – Dayton, OH Aug 2015 – Aug 2017
MS in cyber security **- GPA: 3.9/4**

SRM University – Chennai, TN Aug 2008 – Mar 2012
Bachelor of Technology – **GPA: 3.3/4**