

# Survya Pratap Singh

## Sr. SOC Analyst

3515 Coker Street, Irving TX -75062

Mob: 937-581-6431 | email: [singh.surya@gmail.com](mailto:singh.surya@gmail.com)

Website: <https://survya.com> | LinkedIn: <https://www.linkedin.com/in/survya/>

Experienced and passionate IT Security professional with 4.5 years of diversified experience in SOC, vulnerability assessment, threat intelligence, financial fraud analysis, and python scripting.

## Experience

Oct.2017- **Citi Bank** - TX, USA

Present Sr. SOC Analyst/ AVP

- Working as an L1 security analyst in Global SOC team and responsible for monitoring the security incidents in Citi IT networks.
- The daily task involved analyzing and investigating ArcSight security event logs and creating cases in Archer for further escalation.
- Working with several security tools like SilverTail, Iovation, Splunk, and SAS for analyzing ArcSight events and determining financial fraud in Citi bank worldwide.
- Developed an automation tool in excel macros for analysis SAS data and generating security escalation emails, which saves three minutes per case creation.

May.2017 - **NiSource Columbia Gas** - OH, USA

Aug.2017 *Cyber Security Intern*

- Optimized checkpoint firewall rules by using Firemon Security Manager Tool.
- Performed threat analysis by using Palo Alto next-generation Firewall.

Jan.2017- **Southwest Airlines** - TX, USA

May.2017 *Cyber Security Intern*

- Enhanced security of server to server communication by remediating 50K weak SSH keys with 2048 bits SSH keys.
- Improved security of PKI SSL certificates across various applications by replacing SHA-1 certificates with SHA-256 certificates.
- Performed daily task of rotating, issuing and managing SSH keys and PKI SSL certificates in Venafi Trustworthy tool.
- Automated manual processes for generating weekly SSH key remediation metrics using Excel Macros, which helped in increasing the team productivity.

May.2016- **DSW Inc.** - OH, USA

Aug.2016 *Cyber Security Intern*

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

May.2012- **Accenture Services** - MH, India

Aug.2015 Software Engineering Analyst – Banking Client

- Developed a standardized TATC framework for testing of middleware web services using Parasoft SOA Test tool.
- Performed task like test case identification, test scenario creation, test execution, requirement gathering and defect identification and management, and lead a team of 4 quality analysts.
- Received the "Accenture Financial Services Zenith Propel Award" at Accenture India Delivery Center level in 2014 and "Performer of the Quarter" award in 2013.

## Proficiencies

**Skills:** ArcSight SIEM, SilverTail, Archer, SAS, Vulnerability Assessment, Venafi, Qualys, PKI & SSH keys Management, Threat Intelligence, Linux, TCP/IP, Python Scripting and Excel Macros.

**Certificates:** WSU Cyber Security Analytics, CompTIA Security+, Certified Ethical Hacker (CEH V8), Qualys Certified, MCITP -2008 R2, Venafi Security Certified, Oracle Certified Java Programmer (SCJP 6), CISSP- In Progress.

## Education

Aug.2015- **Wright State University** - Dayton OH, USA

Jul.2017 *Master's in cyber security* - **GPA: 3.88/4**

- Concentration: Cyber Network Security, Host Computer Security, Cloud Computing Security, Information Security.
- Java Programmer Assistant in CS department for assisting undergrad student with their programming projects

### **Projects:**

DDOS Attack Detection Tool, Social Media Reconnaissance Tool developed in Python, and Android Weather Forecast application.