

Survya Singh – CISSP, Sec+

Sr. SOC Threat Analyst

Mob: (469)-493-6829 | Email: singh.surya@gmail.com

Web: <https://survy.com> | LinkedIn: <https://www.linkedin.com/in/surya/>

SUMMARY

- Experienced IT Security professional with 5 years of diversified experience in security operations, threat intelligence, financial fraud analysis, and python scripting.
- Proficient in problem solving and debugging issues through packet analysis and root cause analysis.
- CISSP, Security+ certified. Hold a master's degree in cyber security.

EXPERIENCE

Citibank North America – Irving, TX

Oct 2017 - Present

Sr. SOC Threat Analyst

- Working as an SOC security analyst in Global SOC team and responsible for monitoring the security incidents in Citi IT networks.
- Perform monitoring, research, assessment and analysis on 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.
- 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 analysis by using 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.
- 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.

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.
- 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.

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 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.

PROFICENCIES

- **Certifications:** CISSP, Security+, CEH, WSU Cyber Security Analytics, Splunk Certified Core User, Qualys Certified, Venafi Security Certified, Oracle Certified Java Programmer (SCJP 6).
- **Skills:** ArcSight SIEM, Splunk, Palo Alto, Arbor, Archer, SAS, Vulnerability Assessment, Venafi, Qualys, PKI & SSH keys Management, Threat Intelligence, Linux, TCP/IP, Python Scripting and Excel Macros.

EDUCATION

Wright State University – Dayton, OH

Aug 2015 – Aug 2017

Master's in cyber security - GPA: 3.9/4

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

SRM University – Chennai, TN

Aug 2008 – Mar 2012

Bachelor of Technology – GPA: 3.3/4