Name: Santosh Kumar
Mobile: +91-9849023458

Email ID: santosh3518@gmail.com
Experience: 3.5 years
Domain: SOC (SIEM)
Residential: Hyderabad

Professional Experience:

April 2019 – Senior Security Analyst
Present Mind Tree, Hyderabad

- Analysis of notable triggered in Splunk using different tools mentioned and take necessary action.
- Based on the request we receive, search, fetch and share the required details with them.
- Dashboard, Lookups and report creation.
- Phishing analysis by performing containment and eradication.
- Basic troubleshooting in Zscaler
- Worked on weekly, monthly report and present in client meetings.
- Distributing threat intelligence news across the client.
- Feeding IOC's to intelligence management platform that helps enterprises easily enrich and operationalize their security data
- Phishing analysis by performing containment and eradication.
- Web content filtering
- Performing ADHOC scans and sharing the report
- Investigate the triggered offenses, then taking an appropriate action involving respective tower if necessary
- Log source integration to Splunk
- Use case creation and finetuning
- Trouble shoot the non-reporting log source
- Daily Splunk health check report
- Worked on SIEM monthly and weekly report.

March 2017 – Security Operations Center Engineer (SoC)
Jan 2019 Hasbro Inc, Rhode Island, USA

- Experience working in Security information and event management (SIEM).
- Analyzing Security logs from IDS, IPS, firewalls and Proxies checking for any suspicious events and escalating.
- Proactively manages IT security on behalf of customer to reduce the impact of security incidents and system compromises.
- Working as a L2 Analyst, actively investigates the latest in vulnerabilities, advisories, incidents, and penetration techniques and notifies concerned when appropriate.
- Respond in timely manner to support threat and other cases.
- Alerts concerned stakeholders of intrusions and potential intrusions and compromises to their IT environment
- Work with various business units to conduct vulnerability scanning in identifying, reporting and tracking system vulnerabilities and remediation efforts.
- Managing, monitoring and Knowledge on creating, Active channels, Active Lists.
- Checking health status for all devices, connectors that were integrated in ESM.
- Finding false positives, fine tuning and escalating Security events.
- Hands-on experience Monitoring Splunk and Arc Sight SIEM or similar enterprise-class SIEM.
- Alerts clients of intrusions and potential intrusions and compromises to their network infrastructure.
- Co-ordination with different stakeholders to mitigate /remediate security incidents.

Client: Bose, Boston **June 15 – Jan 2017**

Project: Light house

kiosk based application where user walk into store and have hands on experience of Bose products. Application interacts with peripheral device via Bluetooth. Application has default playlist (Spotify API) where user can select and play. The applications display product information (London & Dubai Store)

Role: Mobile Tester

Responsibilities:

- Responsible for understanding user scenarios, devising test plans, creating effective test cases and perform various test including Front-end Testing, Back-end Testing, **GUI testing**, Functional Testing, Smoke Testing and Regression Testing Involved in design and implementation of smoke and regression test suites.
- Identity key features and functionality of the application and devise effective test plan to uncover any potential errors/bugs that may interfere with the user experience and thus lower the quality of the products.
- Ensured Regression Test Bed is updated, ready for reuse, and stored in Test case repository.
- Testing **Spotify integration**

Client: Fidelity Investments, Smithfield, RI. **August 12 – April 15**

Project: CRM Application

CRM Application for internal user to manage their clients. We developed an CRM app which is used by field agent to help improve their sales.

Role: QA Functional Engineer

Responsibilities:

- Analyzed business requirements and functional documents, created the test strategy document that define the test environment, phases of testing, entrance and exit criteria into different phases of testing and resources required to conduct the effort.
- Involved in defining test automation strategy and test scenarios, created automated test cases, test plans and executed tests using Selenium WebDriver and JAVA.
- Involved in creation of automation framework in Selenium WebDriver using behavior driven approach like Jbehave, Cucumber.
- Created the Technical Test Plan in the initial phase and also during change requests.
- Created functional automation scripts for the report generation module using tools Selenium WebDriver and TestNG.

Education:

Graduated in Computer Science Engineering from JUNTU, Hyderabad 2010
Masters in Information Systems from Concordia University, USA 2012

Technical Skills and Tools

SIEM: *QRadar & Splunk*
EDR: *Crowd strike*
Content Filtering (Open DNS): *CISCO Umbrella*
Phishing Analysis: *Cofense, O365, Iron Port*
VA: *Qualys & Nessus*
Threat Intelligence Management tool: *Trustar*
Proxy: *Zscaler*

Declaration:

I hereby declare that all the information furnished above is true as per my knowledge.

Signature
Santosh