Nizar Al Noor

Security Operations Center Analyst

An Information Security Professional with over 2 years of experience of working in Live Security Operations Center and be the first line of defense for cyber attacks and security incidents

sachwani.nizar@gmail.com

+966503186703

Riyadh, Saudi Arabia

linkedin.com/in/nizar-al-noor-20453a93

nizar.sachwani

WORK EXPERIENCE

Senior Cyber Defense (SOC) Analyst

Symantec

08/2017 – Present *Riyadh, Saudi Arabia*

Achievements/Tasks

- Working on Managed Security Services using Symantec MSS Platform & HP ArcSight SIEM in a 24/7 rotating shift environment
- Working on Fire Eye to analyze & prevent possible breaches and malware infections in the network
- Provide initial level mitigation for DDOS Attacks on clients using Arbor APS
- Catering of Spam & Phishing Emails reported by the clients or users

Contact: Srivatsa Venkatesh (Team Leader) – +966503046158

Senior SOC Analyst

Bank AL Habib

06/2016 – 02/2017 *Karachi, Pakistan*

Achievements/Tasks

- Helped setup a 24/7 Security Operations Center based on rotating shifts & acted as a Team Leader
- Worked on IBM QRadar SIEM to help detect potential threats and security alerts
- Helped design the SOC Manual and Standard Operating Procedures based on the best practices
- Worked on the Fire Eye HX, EX and NX component to help prevent the potential breaches via malware infection, emails and network intrusions

Contact: Hussein Hasan Ali (CISO/HOD Info Security) – +923351370826

SOC Analyst / Senior SOC Analyst

Rewterz Information Security

08/2015 – 05/2016 *Karachi, Pakistan*

Achievements/Tasks

- Worked on Malware Analysis using a wide variety of Sandboxing & Reverse Engineering Tools
- Working in a 24/7 based Security Operations Center for the client
- Using McAfee ESM & Splunk as the main sources of security incidents and logs
- Wrote Incident Reports and Executive Summaries to provide the client a clear insight of the working of the Security Operations Center
- Performed Automated Vulnerability Assessment of Critical Assets using Nessus

Contact: Faisal Arsalan (HR Manager) – +923453114266

EDUCATION

Bachelors in Computer Sciences (BSCS)

FAST - NUCES, Karachi, Pakistan

08/2011 – 07/2015 *Karachi, Pakistan*

Courses

- Network Security
- Information Systems Security
- Computer Programming
- Computer Networks

SKILLS

Security Operations Center | Managed Security Services | Log Analysis | Malware Analysis | Vulnerability Assessment | Security Incident Response | Linux

PERSONAL PROJECTS

Malware Analysis Using Reverse Engineering (02/2015 – 04/2015)

- Setup a Custom Lab to analyze different kinds of malwares

Android Based Home Automation System (02/2015 – 04/2015)

- Home Automation based on Android Application

NUCES Academia (08/2014 – 05/2015)

- An online portal created for students featuring lectures, live chats with instructors and virtual classrooms

ACHIEVEMENTS

Attended Kaspersky Fraud Prevention Workshop

Studying for CCNA Cyber Operations Certification

Attended AlienVault USM and IBM QRadar Training

LANGUAGES

English	●●●●●
Urdu	●●●●●
Arabic	●●○○○

INTERESTS

Security Operations | Malware Analysis | Log Analysis | Humanitarian Causes | Social Work | Scouting