Ashish R Bhandari

Security Engineer | Troubleshooter | Software Explorer

+91 77189 72307

aashishrbhandari@gmail.com

Mumbai, India

github/aashishrbhandari

I am a Security Engineer, who loves to explore Softwares from different angles (Security, Frontend, Backend), I keep on improving my skills by reading, researching and developing (small projects), i try to learn the concepts in a way that i can EXPLAIN it to others. This helps me to increase my Knowledge & Experience. I always try to learn concepts from different ways so that i can fully decode and relate with it. I am very much curious to learn something new and always try to challenge myself.

Work Experience

Security Analyst — API Holdings

09/2022 - Preset

My Analysis till now *`No Problem can be solved without proper data & management`*
My Day starts with checking mail showing any Network related challenges faced at any location, and trying to figure out the possible existing area of the flaw. DNS, ISP, Service being down, Firewall Access Restriction, SD-WAN Tunnel etc.
First: Before beginning Security Review I should be well aware of Location Network Architecture, so that I can then identify the challenge and point out and work on the flaw. Before actually implementing Security Control, I should make sure the Architecture is in place. I be in close touch with Network Team, to understand any problem faced and I help them resolve it.
Second: I then began my work on implementation of the Security Controls at Firewall, SDWAN, WIFI, I make sure that I explain Local IT Executive the changes & possible problem that might come up after the change and how with Simple SOP you can gather the details and help speed up the resolution.
Third: I am in charge of the Cloud Firewall POC, where i use my checklist to test & understand the security control & how easy it is to implement it in that solution. I also discover new usecases as I test & research.
Other: as listed below

Core:

- Firewall Management: Security Review and Implementation
- Review, Implement, Manage: Sonciwall, FortiGate Firewall across All Locations
- Cloud Firewall POC & Implementation: NetSkope, ZScaler, Prisma Access, Cisco Umbrella, Checkpoint
- New Network Infrastructure: Setup, Testing & Review
- Co-ordinating with the Network & Infrastructure team to identify & help resolve any blocker or challenges

Other Tasks:

- Security Review & Implementation: JumpCloud, Site247-NCM, GMS-Sonicwall, IBM-QRadar, OpenVPN
- Troubleshooting: Firewall, OpenVPN
- Communicating with Vendor to resolve Network Infrastructure Problems.

Core Skills:

- Good in Understanding & Structuring Problems
- Good & Curious in Finding & Validating the Solution

Job Skills:

Firewall Review | Scripting | Troubleshooting | Network Arch Testing & Validating | DNS Security

Security Engineer — SafeSquid Labs

06/2019 - 09/2021

↳ Jr. Security Engineer (05/2018 - 06/2019)

My Role requires me to be flexible enough to understand the Enterprise Security Requirements, Understand how Web Apps work. I have to understand, troubleshoot & test Internet Apps working and should able to apply policy based restrictions on it.
I Work Closely with the NOC & SOC team to identify problems faced due to website/application broken functionality, which can be caused by Inline Content-Filtering Solution(Firewall/IDPS/AV Scanner).
I handle the Application Security Testing part where i provide a detailed report on the Security Vulnerabilities of the Product. One part of my work focuses on finding the Bugs & issues related to product found in the testing phase or at the client side.

Core:

- Testing using **#OWASP Top 10**, **#SANS Top 25** Methodology.
- Internal Application Security Testing (Burp Suite, Fiddler, Postman, MitmProxy, Curl & Manual Approach)
- Conduct VAPT on Product as well as on all Services including Web, Network & API VAPT

Responsibilities:

- As a SOC Analyst, I keep on hunting for different types of use cases that happen at client setup
- Leading Multiple Projects and Team, being able to help customer in all the phases and beyond
- Product Demonstration, Demonstrating New Ways of Applying Security Restrictions, Webinars, Requirement Gathering.

Job Skills:

Security Testing | Web Development | Scripting | Content-Filtering | Troubleshooting | DLP | DNS Security | Fuzzing

Network Engineer — EKids India

06/2017 - 05/2018

Maintain Security Restrictions, Network Setup, troubleshooting, AD Management are my keys roles along with Computer & Network device maintainence.

- Maintain the Cyberoam Firewall: Creating Network Restriction Policies
- Logging and Monitoring Events to understand flaw in the Network Restriction Policies
- Microsoft AD User Group management

Job Skills:

Hardware & Software Troubleshooting | DNS Security | Networking

Skills & Tools

Skills:

Security Testing | Troubleshooter | Networking | Web Dev(Frontend+Backend) | DNS Security | Java | Python | JavaScript | NodeJS | Scripting | Linux | Code Review

Tools:

Curl | OpenSSL | Wireshark | Tcpdump | Browser Developer Tools | BurpSuite | Fiddler | NMap | MITM Proxy | Pi-Hole(DNS)

Education

BSc (Spec. in IT) 2014-2017
Patkar Varde College(Goregoan)

HSC (With Maths) 2012-2014
Thakur College(Kandivali)

SSC 2012
Children's Academy(Kandivali)

Awards & Laurels

Buildbox Training
Rapid Game Development(College Tech WebSession)
Trained Students on how to use Buildbox and create their own games.

Bootstrap Session
Web Development(College Tech WebSession)
I showed how a simple login form, or a simple website can be retransformed and made attractive & responsive just by importing bootstrap and using it classes

JavaScript World
Web Development(College Tech WebSession)
I taught form validation, different event handlers, where to use and how they help etc.

Personal Qualities

- Listening, Understanding & Analyzing Problems
- Software Lover & Explorer
- Problem Solving & Observational Skills
- Love Teaching what i know
- Internet Surfer & Explorer

Exploring

Cloud Firewall:
NetSkope | ZScaler | Prisma Access | Cisco Umbrella

CTF Player:
TryHackMe | HackTheBox | PortSwigger | OffSec Playground

Perimeter Security Soln:
Proxy | Firewall | IDPS

Tech Lover:
Adguard | Pi-Hole | Diladele | Simplewall | SafeSquid