AMMAD ALI BUTT

Information Security | SOC Analyst

CONTACT

+92 343 3064432

ammad.butt021@gmail.com

ammad-butt

PROFILE

An Information Security Engineer with experience of working in various areas of security which includes Security Monitoring, Vulnerability Assessment, Endpoint Security, Malware Analysis and Threat Hunting. Operational task also includes Audits, Secure Network Design and Application Security Testing.

Along with the security tools and techniques, I like to work with the latest technologies including Cloud computing, Automation, Virtualization and ELK Stack which help to provide better and in depth understanding of Infrastructure to secure.

AREAS OF EXPERTISE

- Security Operation Center (SOC)
- Threat Hunting
- Malware Analysis
- SIEM Solutions
- Vulnerability Assessment and Patch Management
- Endpoint Security Solutions
- Network and Web Application Firewall (WAF)
- Application Security and Testing
- Ethical Hacking
- OS Virtualization

EDUCATION

NED University of Engineering and Technology
MS Information Security 2018
CGPA: 3.49 / 4

Institute of Business Management - CCSIS
BS Computer Science 2017
CGPA: 3.57 / 4

Bahria College Karsaz Karachi
Intermediate 2013
Subject – Pre Engineering

EXPERIENCE

Security Operations Engineer
AFINITI, Pakistan *Sept 2019 – Present*

Responsibilities:

- Leading SecOps domain in Information Security department.
- Incident Investigation and Response
- Security Monitoring and Investigation on IBM QRadar
- Reporting on Symantec Endpoint Security.
- Investigation of Suspicious Emails, Incidents and coordinating with respective teams for resolution.
- Correlating events from various security tools and improving detection.
- Threat Hunting and Malware Analysis
- RnD on Auditing and Logging to improve detection of malicious activities.
- L2 Support for security operations including review of Change Requests, Network Segmentations and Configuration Review.
- Documenting SOPs / Procedures for SecOps teams.
- Vulnerability Assessment of infrastructure and coordinating with various teams for patch management.

AMMAD ALI BUTT

CERTIFICATIONS

- CCNA Routing and Switching (*Certified)*
- CEHv10 (*Training Only*)
- Autopsy Training by Basis Technology
- Fortinet NSE1 and NSE2

ACHIEVEMENTS

- Merit Certificate for achieving second highest CGPA during bachelor's degree.
- Head of Event Management for Organizing Seminars, workshops and Events in university.
- Participated in multiple IT competition nationwide held in various universities including GIKI and IST Islamabad.

INTERSETS

- Blogging
- Sports
- Traveling
- Photography
- Gaming

PERSONAL DETAILS

- Location: Karachi, Pakistan
- Languages: English (Fluent)
  Urdu (Native)
- Nationality: Pakistani
- Religion: Islam
- Marital Status: Single

MORE EXPERIENCE

Information Security Engineer
GADITEK, Pakistan *May 2017 – Aug 2019*

Responsibilities:

- Managing McAfee ESM (SIEM) i.e Adding Data Sources, Alarms, Alerts and Tuning rules.
- Performing Vulnerability Assessment using Rapid7 Nexpose.
- Policy review and update on KasperSky Endpoint Security.
- Security Review of Network Firewall and Cloudflare (WAF).
- Threat Modeling and Risk Assessment (Desktop Applications and SDKs).
- Static Source Code Analysis (Automated Tools)
- Application Security Testing and validating reported bugs from BugCrowd.
- Secure Network Designs for on premises and cloud infrastructure.
- On demand security review of AWS, BitBucket, Customer Support portals and network devices.
- Managing Identify Management System (OKTA)
- User awareness trainings and sessions with different teams.
- Coordinating with DevOps and Backend team for security review and secure software development practices.