Personal Information

Name: **Sachin Pansare**
Nationality: **Indian**
Experience: **4.5 Years**

Email:**pansaresachin2810@gmail.com**
Phone:**+91-9833200241**

Objective

To obtain an Information Security position that utilizes my experience, knowledge and skills to bring value to the organization.

Skills

- Understanding of organization's security goals and objectives.
- Understanding of Red team assessments ,Risk Assessment & management, Disaster Recovery Planning.
- Hands on experience with Computer Forensic methodology using various tools.
- Knowledge and demonstrable experience of Security Information Event Management systems (Qradar, SageNet).
- Hands on experience with integrating Network devices and security systems with the monitoring tool like SIEM.
- Familiarity with industry standard such as OWASP,CIS,ISO 27001.
- Good hands on knowledge of Web Application Penetration Testing.
- Good experience working in mixed Windows/Linux/Mac OSX, and virtualized environments.
- Good knowledge of security issues inherent in corporate environments like phishing, DDoS attacks and Malware.
- Respond to threats including isolation and remediation.
- Good analytical skills and remediate security issues.

Information Security Tools Handled

- **Perimeter Level:-** Cisco Umbrella, Checkpoint Firewall, FireEye NX, Radware DDos Protector.
- **SIEM :-** Qradar, SageNET.
- **Sandboxing :-** Check Point Sandblast, Cuckoo Sandbox.
- **Computer Forensic :-**Process Hacker, Pestudio, OSForensics, EnCase, VMWare Fusion,Wireshark
- **Vulnerability Scanning :-** Nexpose.
- **Endpoint Security :-** Symantec Promisec, Carbon Black Response, Carbon Black Protection(Bit9).
- **Email Security :-** Proofpoint Email, FireEye Email Protection.
- **Malware Protection :-** Cisco AMP.
- **Device Encryption:-** Datalocker Encrypted USB, BitLocker Encrypted Laptops.
- **User Password Security:-** Dashlane.
- **Patch Management:-** Ivanti.
- **Privilege Account Management:-** Beyond Trust
- **Web Application Penetration Testing :-** HTTRACK, Burp Suit , Acunetix

Education

- **K. J. Somaiya College** - Mumbai, India — Aug 2012- May 2014
  Master of Science **–** Information Technology

- **S. K. Somaiya College** - Mumbai, India — May 2009- April 2012
  Bachelor of Science – Information Technology

Experience

Wipro Technology — December 2014 – October 2017
Cyber Security Analyst — Pune, India.

Roles and Responsibility:

- **Project Implementation:**
  - Implementing Checkpoint Sandblast appliance (TE2000X) for protection against zero-day attack such as ransomware and many more.
  - Implementing Proofpoint email security for Client.

- **Incident Response:**
  - Worked on Radware DDoS protector to monitor if any DoS attack on infrastructure.
  - Blocking malicious IP address on Checkpoint firewall.
  - Worked on Cisco AMP for prevention against any advance malware protection.
  - Using Promisec end point security tool to determine if user has installed any non-work related software and if so ask for business justification.
  - Design and manage reports that provide added value to the management.
  - Analysing Qradar offenses and investigating on the basis of historical logs, payload information, bidirectional traffic and other log details.
  - Collecting information from log details to build new use cases and creating the same under higher level supervision.
  - Creating daily and weekly Qradar automated reports, analysing and discussing the same with management and client.
  - Blocking malicious sender/ip on Proofpoint.
  - Work with IT team to integrate different network device with SIEM system to collect logs and identity monitoring activities.
  - Performing Vulnerability scanning using Nexpose to determine any vulnerability in infrastructure.
  - Application security and URL filtering based on customer requirement.
  - Preparing documentation for Incident Response and for day to day activity.
  - Identify severity level of vulnerabilities with proof of concept / Evidence

Crane Co.(Crane Process Flow Technology):
Information Security Analyst

October 2017 – present
Pune, India

Roles and Responsibility:

- **Project Implementation:**
  - Implementing Cisco Umbrella infrastructure for safe internet access.
  - Implementing FireEye NX appliances to determine any active connection from inside to attacker.
  - Implementing Carbon Black Response and Carbon Black Protection for end point security using SCCM and on-premise deployment.
  - Implementation of Isolated network in organization for detailed malware analysis.

- **Process Improvement and Documentation :**
  - Created new incident response process for FireEye ETP.
  - Created new incident response process for FireEye NX.
  - Created new incident response process for Phish Alarm Button.

- **Incident Response:**

  - Understanding of CIS Controls 7 (Centre for Internet Security) to design and deploy security program.
  - Knowledge about MITRE ATT&CK™ Framework working on implementation with CB.
  - Working on Phish email alerts and Riskware Callback alert.
  - Investigate potential or actual security violations or incidents in an effort to identify issues and areas that require security measures or policy changes.
  - Performing penetration testing on organization's web application to determine infrastructure security.
  - Isolating end point using CB response if in case end point is compromised.
  - Working on CB Response alerts if any malicious process or md5 is running on end point system.
  - Working on CB Protection alerts if any non-work related software getting installed on system.
  - Designing Phishing camping for internal users to assess Cyber Security Awareness in Wombat Security tool.
  - Creating watchlist in CB Response.
  - Blocking malicious domain on Cisco Umbrella.
  - Working with different BU's to assess Ivanti patch management progress.
  - Working with BU team to ensure all security tools are installed on end point.
  - Monitoring encrypted USB progress and allocation of USB to user.
  - Working with BU team to determine EMET is installed on system or not.
  - Document all activities related to a security incident and provide support with status updates during the life cycle of the incident to SOC team.
  - Educate business unit managers, IT team and end user about common security risks and controls.
  - Preparing reports and presentation to showcase security program progress.

Training

- CB Response Introductory Analyst Training — March 2018
- CB Protection Administrator Training — June 2018
- Proofpoint Technical Training — May 2015

Certifications

- EC-Council Certified Security Analyst- (ECSA)v10 — December 2018
- Certified Ethical Hacker-(CEH)v9 — May 2018
- Check Point Certified Security Administrator (CCSA) — May 2017
- Cisco Certified Network Associate (CCNA). — January 2017

Workshops

- Attended ISACA seminar, 12 January 2019,Pune,India

Achievement

- Identified and utilized variety of learning materials, resources and technology methods for one of the major account which turned to Service Improvement Plan: PRAGATI (2016-17/PRAGATI/80175).
- Transition mentor for three different major account.
- Awarded for securing 1st position in stack in the month of June 2016

Strength:

- High level of patience, enthusiastic, complete involvement and goal oriented.
- Ability to give quantitative output with presenting and cope up with the workload.
- Positive approach towards work environment with flair of learning through exploration.

Additional Personal Information:

NAME :	**Sachin Maruti Pansare**
Date of Birth:	28th October 1991
Alternate Contact No	+91 8830517478
Alternate Email Address	panusachu@gmail.com

Declaration

I hereby declare that all the details furnished above are true to the best of my knowledge and I am solely responsible for any discrepancy.